SIEMENS

Access Control

SiPass integrated

Operation Client User Guide

MP 2.80

A6V101068659

Smart Infrastructure

30.09.2020

Copyright

Edition: 30.09.2020

Document ID: A6V101068659

Table of Contents

1 About this Guide

This guide provides an overview of SiPass integrated Operation Client. The document also provides technical information required for the System Administrator, Operator and the User to operate SiPass integrated on a day-to-day basis.

Objective

The objective of this document is to teach the implementer the various processes involved in operating the SiPass integrated system using the Operation Client.

2 Document Updates after Previous Release

The following updates have been done to this document as below:

SiPass integrated MP2.80

Section	Details
Purging the Cardholder Information [→ 96]	New section that describes the *Purge Cardholder Details* function used for clearing the Cardholder and related Audit Trail information if required by any privacy regulation for the region where SiPass integrated is installed.
Customizing System Preferences: Audit Trail Tab [→ 21]	Added description for the new checkbox – **Latest message on top** that keeps the latest entry on top and scrolls the Audit Trail window up as soon as a new entry comes in.
Cardholders Adding a Custom Report to Cardholder Search [→ 51]	New section describing how to add a customized report to the Cardholder Search Function.
Cardholders Definition Tab [→ 27]	Section updated for adding description of the new **Send QR Code** button.
Viewing Options for Site Plan [→ 109]	New section describing the different viewing options while working with a site plan.
Proximity Reports [→ 143]	New section that describes the *Proximity Report* function to identify and track cardholders who were close at one or more locations around the same time.
Audit Trail Reports [→ 140]	Section updated with information about the new *Audit Trail – Cardholder Changes (Custom Fields)* report that involves events related to accessing cardholder information with previously defined custom fields.
Host Event Tasks Report Fields [→ 150] (Host Event Tasks Report Fields)	Section updated to include information on the enhanced e-mail report formatting through Host Event Task.

SiPass integrated MP2.76 HF06, MP2.76 SP1 HF08 and MP2.76 SP2 HF05

The above mentioned Hotfixes include the update as listed below. Note that more hotfixes in future can include this change and the relevant document for each hotfix must be consulted for accurate information.

Section	Details
Proximity Reports [→ 143]	New section that describes the *Proximity Report* function to identify and track cardholders who were close at one or more locations around the same time.

SiPass integrated MP 2.76 SP2

Section	Details
Privacy Mode for Aperio Basic Lock [→ 87]	New section that describes the *Privacy Mode* function for the Aperio Lock.

SiPass integrated MP 2.76 SP1

Section	Details
Cardholder and Access Management: Personal Tab [→ 31]	Section updated to include the new **Manager Email Address** field description.
Actioning an Alarm [→ 106]	Note added to tell the user that the maximum lenghth of the message in the **Log of action taken** field is 256 characters.
Importing Cardholder Images [→ 47] Importing a Cardholder’s Photograph or Signature [→ 198]	Sections updated to inform the user about the supported image resolution while importing images for a cardholder or visitor.

SiPass integrated MP 2.76

Section	Details
Reports: Hubs Report Fields [→ 127]	New section that lists field descriptions for the new *Hubs* report in the Components report group.
CCTV	All references to CCTV removed from the document.

SiPass integrated MP 2.75

No modifications

SiPass integrated MP 2.70 Service Pack 1

Section	Details
Introduction and Starting Up: Certificate Expiry and Renewal [→ 13]	New section that explains how SiPass integrated monitors the certificate for validity and informs the user before its expiry date. The process to renew the certificate is also explained in this section.
Introduction and Starting Up: Setting Up Favorites [→ 18]	New section that describes how you can add the most frequently accessed menu items as favorites in one place.
Monitoring Your Site: Status Bar [→ 98]	New section that describes the information displayed by the status bar.
Biometric Integration: Configuring an Enrollment Reader for the Bioscrypt functionality [→ 178] Configuring an Enrollment Reader for Configuration II [→ 181]	• Added support for *Omnikey CardMan 5×22* readers. • Added step for Mifare DESFire card configuration in both Omnikey reader types.
Reports: Elevators [→ 152]	Section updated with new report types: • Destination Control Elevator Readers • Elevator Controller Details
Reports: Audit Trail Report Types [→ 143]	New section that lists the mapping between the *Audit Trail Type* filter numerical value and the specific Report Type Description.

3 Introduction and Starting Up

Congratulations on choosing SiPass integrated to be your access control software solution. SiPass integrated is the leading access control and security management software in the market that monitors and controls access to your site, using a personal computer running the latest Windows operating system.

The graphical user interface of SiPass integrated is designed to support the complex and demanding needs of security staff and operators. You can quickly and easily navigate the system and use the many functions provided. SiPass integrated is a complete system that packages all your access control needs into an easy-to-use application.

The SiPass integrated system allows you to effectively and efficiently monitor your building site and the people who access it. The system also allows dial-up communication via modems, meaning that fewer resources are required to monitor a large number of sites.

3.1 Online Help and SiPass integrated License Information

SiPass integrated provides an interactive Online Help reference manual under the **Help** menu. The menu also provides an **About** option that opens the SiPass integrated dialog which gives information like Site Name, Serial Number and Computer System Details.

Clicking the **License Details** button opens up another dialog which displays detailed information about Site, Workstations, Clients, Card Limit and available modules as per the respective SiPass integrated license.

Note: Creating a new Operator Login utilizes one SiPass integrated workstation license.

You can also have more information about SiPass integrated on the internet through the hyperlink given on the dialog.

3.2 Password Management

SiPass integrated is installed and configured by the Siemens Commissioning Engineer with the default password provided by Siemens. **For ensuring maximum security, you will be asked to change the default password to a secure password of your choice while logging in to SiPass integrated Operation Client for the first time.**

Note: If you logged in to the SiPass integrated Configuration Client first and have already changed the password, you will not be asked to change the password during the first login on the Operation Client. If you cancel the *Change Password* dialog three times, it will be closed and displayed again during your next login attempt.

A secure password can be created with the following properties:

- At least three characters long
- At least three of uppercase characters / lowercase characters / numbers / non-alphabet characters

You can change the password at any time later following the steps below:

1. Run the SiPass integrated Operation Client through the Windows **Start Menu**.
2. On the *Welcome* dialog, click the **Change Password** button.
   ⇨ The *Change Password* dialog is displayed. Enter the required information:
3. Type the username in the **User Name** field.
4. Type the existing password in the **Old Password** field.
5. Type an appropriate password in the **New Password** field. Memorize it so there are no login issues in future.
6. Type the new password again in the **Confirm Password** field.
7. Click **OK**.
8. The *Welcome* dialog is displayed again.
9. Login with the new password.

3.3 Certificate Expiry and Renewal

Every certificate has a validity period after which, it expires and must be renewed. This is to ensure that existing certificate information gets replaced with new one after regular intervals and security is maintained at all times.

Using the *SiPass Authentication Management* tool, you can renew a certificate on SiPass Server and Local Clients installed on a single computer, or on any SiPass integrated Remote Clients installed on separate computers.

SiPass integrated Server / Client starts giving you **warning messages 30 days prior to the certificate's expiry date.** You can close the message and log on to the system but you will keep getting reminders about renewing the certificate.

If you do not renew the certificate in 30 days, you will not be able to log on to SiPass integrated after the certificate has expired. You MUST renew the certificate in this case.

If the certificate of the Server for a Remote Client has expired, starting up the client will give you an error message about Server not being available. In this case, the Server Certificate must be renewed to work with this remote Client.

3.3.1 Renewing the Certificate on SiPass Server

1. Go to the SiPass integrated installation folder on the computer.
2. Right-click the *SiPass.CertificatePicker.exe* file and select the **Run as Administrator** option from the menu.
   - ⇨ The *Authentication Management* dialog is displayed.
3. Click **Next**.
   - ⇨ A message is displayed informing you that the SiPass integrated service will be stopped before making any changes.
4. Click **OK** and wait for the service to close.
5. To generate and install a self-signed certificate, tick the **Generate Self-Signed Certificate** checkbox.
   - ⇨ OR
6. Select your own certificate from the available certificate list on the screen.
   - ⇨ **Note:** If you select a certificate having expiry date in the next seven days, a warning message is displayed. Click **OK** to close the message and select another certificate.
7. Click **Finish**.
   - ⇨ A message is displayed asking if you wish to copy Windows Account Permissions from the previous certificate to the new certificate.
8. Click **Yes** if you want to import the permissions else click **No** and set the permissions yourself later.
   - ⇨ Now a message asks you if you wish to remove the existing (expired) certificate from the system.
9. Click **Yes** to remove it or **No** to keep it on the system.
   - ⇨ The new certificate is generated and applied to the SiPass server and any local clients. A message is displayed confirming that the certificate has been successfully applied.

If you have performed this operation on a computer that has SiPass Server installed, the message will also mention that the certificate configuration on Remote Clients should also be updated.

Follow the steps given in the next section to update the Remote Client certificate information.

10. Click **OK** to close the message.
    - ⇨ Another message will ask you if you wish to restart the SiPass Service on this computer.
11. Click **OK** to restart the SiPass service or **No** to close the message without restarting the service.

3.3.1.1 Generating New Certificates for Remote Client

Each Remote Client has its unique thumbprint. After renewing the certificate of the SiPass server, the thumbprint must also be updated in each Remote Client to authenticate the server again.

Follow the steps below to generate new certificates for the SiPass Remote Clients.

1. Run the SiPass integrated Configuration Client on the computer where SiPass server is installed.
2. From the **System** menu, click **Client Configuration …**
   - ⇨ The *Client Configuration - New* dialog is displayed. The existing Remote Clients for this SiPass server will be listed on the left pane on the dialog.
3. Click the **Generate All Self-Signed Certificates…** button.
   - ⇨ A message appears informing you that this step will generate self-signed certificates for all client records in the system, and update the thumbprint entries. It also asks if you wish to proceed with this step.
4. Make a choice **as desired**:
   - ⇨ If you click **Yes**, no further steps are required.
   - – Proceed to Step 5.
   - ⇨ If you do not want to generate certificates for all clients at once and click **No**. In this case:
   - – Select the Remote Client name from the left pane on the dialog. The **Full computer name** and **Certificate Thumbprint** fields will be populated with the information for that computer.
   - – Click the **Generate Self-Signed Certificate** button.
   - – Proceed to step 5.
5. When prompted, select a destination folder for saving the new client certificates. Sub-folders will be created inside this folder based on the client computer name. The functionality makes it easier to generate all client certificates in one go after expiry when server certificate is renewed.
   - ⇨ A message informs you that the certificate generation process has completed.
6. Click **OK**.
   - ⇨ The new client certificates will be available in the respective sub-folders inside the main folder you specified earlier. Now you can copy these certificates to individual client computers and authenticate. See section Renewing the Certificate on SiPass Remote Client [→ 15].
7. Click **Close** to close the *Client Configuration – New* dialog.

3.3.2 Renewing the Certificate on SiPass Remote Client

Each Remote Client has its unique thumbprint. After updating the Certificate information for SiPass Server, you must now update this in the existing remote Client Computer also to ensure both remain mutually-authenticated.

1. Go to the SiPass integrated installation folder on the Remote Client computer.
2. Right-click the *SiPass.CertificatePicker.exe* file select the **Run as Administrator** option from the menu.
   - ⇨ The *Authentication Management* dialog is displayed.
3. Click **Next**.
4. Click the folder icon next to the **Import Client & Server Certificate From** field.
5. Locate the folder created for saving the new certificates in the Generating New Certificates for Remote Client [→ 14] section. Select the sub-folder inside this that has the name of the Remote Client computer for which, you are currently renewing the certificate.
6. The **Import Client & Server Certificate From** field will be populated with the location of this folder.
7. Click **Finish**.
   - ⇨ A message is displayed asking if you wish to copy Windows Account Permissions from the previous certificate to the new certificate.
8. Click **Yes** if you want to import the permissions else click **No** and set the permissions yourself later.
   - ⇨ Now a message asks you if you wish to remove the existing (expired) certificate from the system.
9. Click **Yes** to remove it or **No** to keep it on the system.
   - ⇨ The new certificate is generated and applied to the remote client. A message is displayed confirming that the certificate has been successfully applied.
   - ⇨ It also informs that this Remote Client must be authenticated again in the SiPass system by updating the certificate configuration on SiPass integrated server computer through the Configuration client. The thumbprint of the new certificate of the Remote Client computer is also given in the message box which can be copied for authenticating in the server depending on the scenarios as below:
   - ⇨ **Scenario 1: I**f you updated the certificate configuration in SiPass Server first and then authenticated the client, you do not need to perform any additional step.
   - – Click **OK** to close the message.
   - ⇨ **Scenario 2:**If you updated the certificate configuration in the Remote Client computer first, the thumbprint for this client must also be updated in the server to authenticate the client again as genuine client for that server. Go to section Updating Remote Client Certificate Thumbprint in SiPass Server [→ 16] for the next steps.
   - – Copy the Certificate Thumbprint for the Remote Client and save it locally.
   - – Click **OK** to close the message.

3.3.2.1 Updating Remote Client Certificate Thumbprint in SiPass Server

On the SiPass server computer:

1. Run the SiPass integrated Configuration Client.
2. From the **System** menu, click **Client Configuration …**
3. The *Client Configuration - New* dialog is displayed.
4. Select the name of the computer (where SiPass integrated client is installed and for which, you are currently updating the certificate configuration) from the list of Remote Clients in the left hand pane of the dialog.
5. The **Full Computer Name** field is populated.
   - ⇨ **Note:** If the Remote Client computer is connected to SiPass server computer through a VPN connection, tick the **Only check thumbprint for authentication** checkbox.
6. Paste the thumbprint of the remote client computer (saved locally in the previous secton) in the **Certificate Thumbprint** field.
7. Click **Save**.
   - ⇨ The Remote Client certificate information is updated.
   - ⇨ You can also delete an existing Client Configuration and add the Remote Client with the new certificate information as a new client.

3.4 Navigating the Interface

The Graphical user interface (GUI) of SiPass integrated Operation Client consists of three separate panels and a toolbar.

- **Horizontal Tool Bars**

  The application displays the main menu bars: File, Edit, View, Options, Window and Help.

  Depending upon the features selected, SiPass integrated displays several Drop-down Menus and Buttons on its horizontal tool bars.

- **Navigation Panel**

  Found on the left of the Operation client user interface, this panel contains the tree structure of the functional categories.

- **Main Panel**

  This panel is used to view data. Custom Pages, Live Audit Trail Windows, Reports, etc, can be arranged and grouped here.

3.5 Customizing Views

SiPass integrated allows customization of the views to suit your individual requirements.

⟐ From the **View** menu, select Current View and then click on **Customize View** option.

- ⇨ The *Customize Views* dialog is displayed listing available areas for which, the views can be customized.

See section Customizing Views [→ 114] for more information on customizing each available information option.

3.6 Saving Current Layout

While working with multiple windows and sub-windows, you might customize the display of information as per your requirements. SiPass integrated gives you the option to save the size and layout so that the next time you start Operation Client, everything is displayed like it was when you exited the application.

1. Go to **File** menu and click the **Save Current Layout** option.
   - ⇨ A message is displayed telling you that doing ths would over write the previously saved layout setting.
2. Click **OK**.
   - ⇨ The most recent layout is now saved and will be loaded next time you start the SiPass integrated Operation Client.

3.7 Setting Up Favorites

You can save a preferred layout and add the most frequently accessed menu items as favorites in one place. The **My Favorites** folder in the navigation pane on the left is used to set the favorites. Follow the steps below:

1. On the left hand pane, right-click on the **My Favorites** item.
2. Click the **Setting my favorites …** menu option.
   - ⇨ The *My favorites* dialog is displayed.
3. Select the items most frequently accessed by you from the options in the *Available* list box on the left side. Expand any item by clicking the **+** symbol to select an item listed under the tree.
4. Click the **>** symbol to add this item to the *Selected* list box on the right side. You can also double-click an item to directly move it to the *Selected* list box. To remove an item, select it and click the **<** symbol.
5. Click **Save**.
6. Click Close.
   - ⇨ The selected items are now listed under **My favorites** in the left side pane.

Note: If you wish to see only the items added as Favorites, click the Hide default client tree view checkbox on the My favorites dialog before closing. This will hide all other options in the left pane of the Operation Client and only the items under My favorites will be visible.

3.8 System Preferences

System Preferences allow you to customize the SiPass integrated user interface and system operation to your own preferences. There are three tabs for defining System Preferences. If you have installed the optional *Photo ID and Image verification* Module, a fourth tab is present (*Imaging*) on client machines.

The system preferences are operator specific and changes made to the default preferences and will only affect the operator who made those changes.

In addition to the customizable system settings, SiPass integrated will remember the size and position of the *Audit Trail* window from each operator’s last session.

3.8.1 Customizing System Preferences

Customizing System Preferences will provide you with an enhanced and personalized Audit Trail view.

1. Select **Preferences** from the **Options** menu to display the *General* tab.
2. Complete the *General* tab system preferences. The section General Tab details the various the fields / options displayed on this tab.
3. To alter the Audit Trail preferences, choose the *Audit Trail* tab and complete the preferences displayed on this tab.
   – The Audit Trail information appears in a window on the main screen of SiPass integrated and, due to the limitations of screen size, only a limited amount of information can be viewed at any one time. It may be necessary to scroll across to view events that do not completely fit within the window.

3.8.1.1 General Tab

The following table explains the settings available on the *General* Tab.

Setting	Context	Description
Default Card & Operator Expiry Date	System(Local)	Specifies the date that will appear by default in the Cardholder and Operator definition screens. To disable the expiry date so that the card or operator privileges will never expire, de-select the checkbox.
Visitor default validity time (days)	System	Specifies the default time in days for visitors cards.
Operator Lockout Timeout	Operator	Specifies the time in minutes before workstation lockout is activated. You must re-enter your password to re-activate SiPass integrated, once your workstation has become locked. A value of 0 doesn’t lock out the workstation.
Home Plan	User	Specifies the site plan that will automatically open when a user logs on.
Accept Unique Pins Only	System	When checked, each PIN Number assigned to a Cardholder in the Cardholder dialog must be unique.
Number of Generated PINs in PIN selection dialog	System	Specifies the number of PINs displayed on the PIN selection dialog. To change the number of PINs displayed select a number from the dropdown list.
PIN Duress Extension	System	Specifies the number of digits added to the cardholders’ standard PIN in order to form a Duress PIN. This is formed by increasing or decreasing the last number of the cardholder’s standard PIN. For example, if the cardholder’s PIN is 1234, by selecting a PIN Duress Extension of 2, the duress PIN becomes 1232 or 1236.
Confirm on Save	Operator	When checked, the Save Confirmation dialog will appear when saving a modified Database record.
Confirm on Delete	Operator	When checked, the Delete Confirmation dialog will appear when deleting a Database record.
Clear on Save (Cardholder window only)	System	When checked, it will clear the cardholder window once it has been saved.
Save <None> Workgroup by Default (Cardholder window only)	System	When checked, if no Workgroup has been selected for a cardholder, no workgroup, i.e. ‘<None>’ will be allocated to the cardholder by default.
Employee Number Enforced	System	When checked, an employee number must be entered when a new cardholder is added in the system.
Display Higher Priority Alarm	System	When checked, allows alarms of a higher priority to be displayed in the Action Alarm dialog, if an alarm is already being actioned by an operator. The operator may select the higher priority alarm and choose to action it instead.
Popup Windows On Top	System	When checked (default), allows windows to pop-up on one another.
Number of Concurrent Cardholder Dialogs	Operator	Specifies the number cardholder dialogs that can be opened in the Operation Client. Maximum: 5. Minimum: 1 (default).
Number of Concurrent Visitor Dialogs	Operator	Specifies the number visitor dialogs that can be opened in the Operation Client. Maximum: 5. Minimum: 1 (default).
Default Access Type on Cardholder access assignment	System	Specifies the default Access type (per workstation) in *Access Assignment* dialog. Default type: Access Group.

3.8.1.2 Audit Trail Tab

The following table explains the settings available on the *Audit Trail* tab.

Setting	Description
Maximum Lines Buffered	Specifies the number of information rows displayed in the *Active Audit Trail* window. The maximum number of lines that can be displayed is 15000. For optimum performance, the value is set to 500 lines by default in SiPass integrated version MP2.80. For the earlier versions, this is set to 5000 by default. • A database restore between MP 2.80 to MP 2.80 will retain the default as 500, unless it was not changed from 500 before taking the backup. • A database restore from an earlier version will reset it to 5000 (the default value in the earlier releases). In this case, it should be manually reset to 500 (or a suitable value under 500) to avoid any live audit trail performance issues. **Note:** It is recommended that you increase this value only if required, as it might result in performance issues in the Operation Client live Audit Trail display. If you need more historical Audit Trail data, you can generate an Audit Trail report, when required.
Latest message on top	Keeps the latest entry on top and scrolls the Audit Trail window up as soon as a new entry comes in, making the Live Audit Trail grid always focused on the latest entries. Live Audit Trail grid column sorting / grouping is not allowed. The Audit Trail data is displayed in the order it is received. Sorting by Columns is allowed only for Audit Trail Snapshot

*

4 Site Management

After you have created all the components at your site using the *Components* dialog, you must then configure the parts of the system that define how and when components operate.

4.1 Time Schedules

Time Schedules define when certain events should occur at your site. For example, cardholders can be denied access after business hours by creating a Time Schedule that gives them access during office hours only. The SiPass integrated system provides you with three pre-defined Time Schedules.

They are indicated in the following table:

Time Schedule	Description
Always (point unsecure)	Access at all times, including weekends and holidays - effectively, no access control.
Never (point always secure)	No Time Schedules defined. Access is never granted.
System Function (non busy intervals)	Access between 2:00 am and 3:00 am everyday including holidays.

4.1.1 Creating a Time Schedule

The SiPass integrated system allows you to created about 65,000 different Time Schedules, with a maximum of 20 independent time intervals defined for each Time Schedule.

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Time Schedule** list item.
   ⇨ The Time Schedule dialog is displayed.
3. Enter a unique name identifying the Time Schedule into the **Time Schedule** field. You can enter up to 40 characters, in any combination of upper and lower case letters, and numbers.
   – You can also search for a time schedule by clicking the **Search** button.
4. Define the time intervals that will make up the Time Schedule.
5. To add the time interval to the **Time Intervals** list, choose **New**.
   – Time Schedules can also be defined by selecting the **Graph View** button. You may enter more than one time interval for each day. However, the start and stop times on any given day must not overlap
6. Click **Save**.

Creating a Time Schedule for a single day

1. Enter the name for your Time Schedule into the **Time Schedule** field.
2. Select **User** from the **Day Type** drop-down list.
3. Set the **Start Time** to 12:00 am and **Start Day** to Monday.
4. Set the **Stop Time** to 12:00 am and **Stop Day** to Tuesday.
5. Choose **Add**.
6. Click **Save**.

Creating a Time Schedule using Graph View

1. Enter a unique name identifying the Time Schedule into the **Time Schedule** field. You can enter up to 40 characters, in any combination of upper and lower case letters, and numbers.
2. Select the **Graph View** Button.
3. Double-click to select the start day and time of your time interval and drag the cursor to create the Time Schedule.
4. To define further time intervals for the Time Schedule, repeat the above step. However, keep in mind that the start and stop times on any given day must not overlap.
5. Choose **OK**.
6. The time interval will be created in the **Time Intervals** list.
7. Choose **Save**.

4.1.1.1 Time Schedule interval definition

The following table explains the options available when defining Time Intervals.

Option	Description
Day Type	Specifies the days that the Time Schedule includes. There is no default day type. To select a day type, choose the drop down arrow and select a new type from the list. The following day types may be selected: • **Weekday**: Allows you to assign a start time and stop time for each weekday (Monday through Friday). • **Weekend**: Allows you to assign a start time and stop time for each day of the weekend (Saturday and Sunday). • **Holiday1**: Allows you to assign a start time and stop time for a single day. • **Holiday2**: Allows you to assign a start time and stop time for a single day. • **User**: Allows you to define a Time Schedule that nominates the start and stop days and the start and stop times for any day.
Start Day	Start day for a particular time interval. To select a start day, choose the drop down arrow and select a new day from the list. The start day is only available when the user day type has been selected.
Stop Day	Stop day for a particular time interval. To select a stop day, choose the drop down arrow and select a new day from the list. The stop day is only available when the user day type has been selected.
Start Time	Start time for a particular time interval. If there is more than one interval being defined, the time interval will start at this time on each day. The start time, by default, is 8:00 am. To change the start time, select the hours, minutes or seconds and use the up-down arrows to set the correct time.
Stop Time	Stop time for a particular time interval. If there is more than one interval being defined, the time interval will stop at this time on each day. The stop time, by default, is 5:00 pm. To change the stop time, select the hours, minutes or seconds and use the up-down arrows to set the correct time.

4.2 Creating a Holiday

Holidays allows dates that are exceptional to the normal rules to be defined in the Time Zone records; For example, Christmas Day or New Year's Day. This allows cardholders access to be controlled without having to change Time Zone definitions every time a holiday occurs.

Only one holiday can be defined for a single date.

▷ Ensure that you have installed the appropriate bus drivers and have configured each bus.

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Holiday** list item.
   ⇨ The *Holidays* dialog is displayed with the default calendar (and any existing calendars) listed in the tree view on the left.
3. Click the **New** button on bottom left of the dialog to create a new holiday calendar.
4. Enter a unique name for the calendar in the **Calendar name** field.
5. From the **Available units** list box, select the ACCs that will observe the holiday.
6. Click the **Add >>** button.
   ⇨ The ACC will appear in the **Selected** list.
7. Go to the *Calendar View* tab.
8. Double click the date (for which you wish to create a holiday) from the months displayed on the tab.
   ⇨ The *Holiday Configuration* dialog is displayed.
9. Enter a unique name for the holiday in the **Name** field.
   – You may enter up to 40 characters, any combination of upper / lower case letters.
10. Select the type of Holiday from the **Type** drop-down box. SiPass integrated allows you to define eight types of Holidays. You can change the effects of a holiday by modifying the relevant Time Schedule(s) in the Time Schedule dialog.
11. Enter a description for the holiday (if required) into the **Description** field.
12. Click **OK**.
13. The *Holidays* dialog is displayed again with the date for which you created a holiday, highlighted in a different color.
14. Click **Save**.
    ⇨ The new holiday calendar will be displayed in the Calendars tree view on left side of the *Holidays* dialog.
    – To see all holidays created for a calendar, select a calendar and go to the *List View* tab.

4.3 Log Book

The Log Book allows operators to make a record of a site’s activities, using a simple heading-based log system. When certain events at your site occur, the operator can open the log book, select the appropriate topic, and log their observations or the action taken. This creates a permanent record that can be recorded at a later stage.

To configure the Log Book you have to create a set of topics, used to categorize log entries. This section explains how to create these topics and add entries to the Log Book.

4.3.1 Adding a topic to the Log Book subjects

The Look Up Table allows you to create the necessary topics for the Log Book.

Please refer the section Lookup Data for detailed information on how this can be done.

4.3.2 Making an Entry into a Log Book

Once you have created topics to be used for the Log Book Entries, operators can use them to log entries regarding activities at your site

1. Double click **Log Entry** from the **navigation pane on left hand side**.
   - ➪ The *Log Book Entry* dialog is displayed listing the **Operator Name**, **Date** and **Time** fields as non-editable fields. The operator can only select from the **Subject** combo box and only modify the **Description** field.
2. Select a subject from the drop down list in the **Subject** combo box by highlighting it in the displayed list.
3. Your choice of subject will be displayed in the combo box and the **Save** button will be enabled.
4. Complete the appropriate comments in the **Description** field as free text.
5. Click **Save**.

➪ Each entry will be logged individually.

➪ A report can be generated that prints all Log Book Entries.

5 Cardholder and Access Management

5.1 Personnel Management

SiPass integrated operators and cardholders make up the personnel at a SiPass integrated site. Operators are grouped by **Operator Groups**, and Cardholders are grouped according to **Work Groups**. This information is defined in the SiPass integrated system.

The SiPass integrated system contains information about the personnel who use the site and about the site itself. The system uses this information to accurately monitor events, and to display detailed information about personnel to authorized operators. For these reasons, it is essential to keep the SiPass integrated system up-to-date.

5.1.1 Cardholders

SiPass integrated allows authorized personnel and their movements at your site to be identified and tracked. To effectively track cardholder movements, new cardholders' details must be entered into the system and those records updated when their details or access privileges change.

In addition to the default tabs, the *Cardholder* dialog also supports customizable cardholder fields, called pages. These controls provide the functionality and the opportunity to collect a significant amount of additional cardholder information.

Once the information about a cardholder has been entered into the system and access privileges have been established, that cardholder's access to the site can be monitored and controlled. If the *Photo ID and Image verification Module* is installed, photo ID access cards can be created which can incorporate a cardholder's photograph and signature.

5.1.1.1 Cardholder Tabs and Tab Fields

The sections that follow will detail the fields available on the various tabs of the *Cardholder* dialog.

Once a cardholder has been saved, the following four fields will appear at the base of the *Cardholder* dialog, and will remain visible while the operator navigates any of the dialog's tabs:

- **Last Name**: Displays the last name of the cardholder;
- **First Name**: Displays the first name of the cardholder;
- **Card No**: Displays the card number of the cardholder.

If this field is displayed as ***Card No**, it implies that at least one other card has been assigned to this cardholder. The details of the additional card/s can be found on the *Advanced* tab.

- **Updated**: Displays the Date and Time at which this cardholder was last updated.

Definition Tab

The fields and controls on this tab are explained in the table below.

Item	Description
Photo Panel	Found under Access Control on this tab, this panel displays the stored photograph of the cardholder, if one already exists.
Last Name	Specify the cardholder's last name. You may enter up to 30 characters, in any combination of upper and lower case letters and numbers.
First Name	Specify the cardholder's first name. You may enter up to 20 characters, in any combination of upper and lower case letters and numbers.
Employee Number	This field must be entered if the Employee Number Enforced option has been enabled in *System Preferences*. You may enter up to 16 characters in any combination of upper and lower case letters and numbers.
View Modification History	This button displays the *View Modification History* dialog.
Workgroup	Specify the workgroup to which the cardholder will be assigned. To change the workgroup, select a new workgroup from the drop-down list. If you have not defined any workgroups in the SiPass Database, you may select **None** from the list. It is recommended that cardholders be re-assigned to an appropriate workgroup at a later stage. **Note**: Only partitioned Workgroups will be displayed in this field.
Define Workgroup	This button brings up the *Workgroup* dialog.
Search	This button displays the *Search Cardholder* dialog.
Next	This button displays the next cardholder in sequential card number order, to the one presently displayed.
Previous	This button displays the previous cardholder in sequential card number order, to the one presently displayed.
Credentials Window	This box displays the credential details of cards configured to the cardholder.
Card Number	This field should contain a cardholder's number that is unique to the system. The number of digits in the card number, and the maximum number of cardholders, will be dependent on the SiPass card technology that you purchased with your license.
Credential Profile	Displays the Credential Profile of the card
PIN	Indicates the cardholder's Personal Identification Number. To select a PIN for the current cardholder, click on the button on the right next to the field which will display a list of PIN's available for use. This field will be updated immediately when the cardholder's card number is entered. The cardholder may use their PIN if particular readers at your site have been configured for both Card and PIN. This field will be hidden unless the operator has the "See PIN" Operator Privilege assigned.
Void	When checked, all cards that are assigned to the cardholder card become void. The cardholder will not have access to any point at your site.
Start Date	Specifies the cardholder's start date. To change the date, click the drop down arrow from the Start Date field below, and select a new date from the displayed calendar. See explanation at the end of the table.
End Date	Specifies the cardholder's end date. To change the date, click the drop down arrow of the End Date field below, and select a new date from the displayed calendar. To disable the end date (the cardholder will always exist in the database), simply un-tick the checkbox. See explanation at the end of the table.

Item	Description
PIN Error Disabled	If this checkbox is ticked, it implies that this card has been made void because the PIN was entered incorrectly 3 times. The operator can un-tick this checkbox, which configures the card to be valid for PIN access again.
Add	This button adds a new row of card credentials in the Credentials box.
Delete	This button deletes a selected row of card credentials in the Credentials box.
Credential Profile	This button displays the *Cardholder's Credential Profile* dialog.
Send QR Code	Generates a QR code based on the base card number for any card technology and sends it to the cardholder or visitor by e-mail. • The Subject name of the e-mail is "QR Code for <First Name> <Last Name>" • The content of the email includes the start/end date of the credential • The attachment has the <First Name> <Last Name> as the file name If QR code was sent successfully, the Audit Trail displays the activity. If there is no e-mail address for the cardholder, the QR Code is not sent and an error message is displayed.
Status	Indicates the status of the cardholder's card. The following describes the possible status: • **Valid**. Access will be granted. • **Work Group void**. The workgroup to which the cardholder belongs has been voided and all members belonging to that group will be denied access privileges. • **Void**. The Void Card check box for the cardholder has been selected. Access will be denied. • **Expired**. The end date of the cardholder's card has passed. Access will be denied. • **Before start date**. The start date on the cardholder's card has not yet been reached. Access will be denied.
Supervisor	Ticking this checkbox nominates the cardholder as a "Supervisor" for doors that are configured with the Dual Custody mode of operation. Some doors require a standard cardholder and a Supervisor to present an access card before access will be granted. Ticking this checkbox means that when this cardholder badges his card at a reader, the door will unlock for the Extended Latch Time rather than the normal latch time, permitting easier access. The Extended Latch Time is configured in the *Components* dialog.
Void Cardholder	Ticking this checkbox voids all the cards belonging to the cardholder, which will deny him access to the site.
Isolate	When checked, the employee is allowed to secure any area (to which they have been granted access), even if inputs are not sealed.
Self Authorize	Ticking this checkbox will allow the cardholder to gain access to a door configured with the Dual Custody mode of operation, without needing the accompaniment of a subsequent cardholder before the door is unlocked.
APB Exclusion	Ticking this checkbox will exclude the cardholder from any Anti-Passback areas that have been created.
Re-Entry Exclusion	Ticking this checkbox will exempt the cardholder from Timed Re-entry rules for areas that are operating in the Anti-Passback mode "Timed Re-entry".
Visitor	This checkbox indicates that the cardholder is a visitor to the site rather than a permanent cardholder.
Accessibility	Ticking this checkbox means that when this cardholder badges his card at a reader, the door will unlock for the Extended Latch Time rather than the normal latch time, permitting easier access. The Extended Latch Time is configured in the *Components* dialog.
Access Control Window	Displays the Access Privileges configured for the cardholder.

Item	Description
Access Privileges button	Opens *the Access Assignment* dialog to allow changes to access privileges.
Read	This button allows you to view the encoded cardholder information on a valid card. A dialog will appear containing the information held on the badged card.
Assign	This button allows you to assign a card to a cardholder. This is a toggle-state button.
Read and Search	This button allows you to read the encoded cardholder information on a valid card, and then search for the card number on the system. This is a toggle-state button.
Encode	This button encodes a smart card with the details of the selected cardholder. The number entered in the Card Number field can be encoded onto the smart card if a smart card reader is attached to the PC and Smart Card Encoding has been configured from the System menu.
Cancel Salto Key	Cancels the SALTO System key assigned to the cardholder.
New	This button displays a new *Cardholder* dialog with empty fields.
Save	This button saves all the information configured on this dialog.
Delete	This button deletes this cardholder and all his/her assigned cards, from the database.

ℹ

Operators may need to change the start or end date of cardholders.

When changed:

- Other Cardholder Credentials which have the same start or end date prior to these changes, are updated in addition.

- For Cardholder Credentials which have an earlier start or end date than the one entered; the operator will be prompted with a message notifying them that the new date is greater than the initial date, and asks if the operator would like to continue.

- If cardholder's end date is greater than 50 years in the future, the **End Date** check box will be un-ticked for that cardholder after saving the details.

Advanced Tab

The fields and controls on this tab are explained in the table below.

Item	Description
Work Group Name	Lists the names of the workgroups that the cardholder is assigned to.
Partitioning	Specifies if the corresponding work group is a Partitioning Work Group.
Use for Anti-Passback	Specifies the workgroup that should be used for the Anti-Passback area count.
Choose	Displays the *Cardholder's Work Groups* dialog.
Fingerprints Window	Displays details of fingerprints captured by the system.
Index	Specifies which finger was used for the fingerprint capture.
Saved	Specifies whether the captured fingerprint is saved in the system.
Encoded	Specifies whether the fingerprint is encoded to card.
Credential Profile	Specifies the credential profile assigned to the card with this fingerprint
Delete	Deletes the selected fingerprint data for the cardholder.
Smart Card Data (Profile)	Displays the Smart Card Profile configured for the cardholder.
Profile Viewer	Dislays the *Profile Viewer* dialog.
General Data	Space for entering general data about the cardholder.

Personal Tab

The fields and controls on this tab are explained in the table below.

Item	Description
Title	Cardholder’s title. You may enter up to 20 characters, in any combination of upper and lower case letters and numbers.
Date of Birth	Cardholder’s date of birth. You may enter the date of birth in any format.
Address	Cardholder’s home address. You may enter up to 60 characters, in any combination of upper and lower case letters and numbers.
Payroll Number	Cardholder’s payroll number. You may enter up to 16 characters, in any combination of upper and lower case letters and numbers.
Phone Number	Cardholder’s home phone number. You may enter up to 16 characters, in any combination of upper and lower case letters and numbers.
Mobile Number	Cardholder’s mobile phone number. You may enter up to 16 characters, in any combination of upper and lower case letters and numbers. Note: In order to utilize the Message Forwarding to Mobiles feature of SiPass integrated, the following format is to be used for all mobile phone numbers: • The first part of the number should be the Country Code • The second part should be the local mobile phone number, excluding any leading zero. • The mobile phone number entered should not contain any spaces. For example, a fictitious mobile phone number 0123 123 123, should be entered in the following format: 61123123123, where 61 is the country code and the rest is the local mobile phone number.
Mobile Service Provider	Cardholder’s mobile service provider. Select a mobile service provider from the pre-defined list. Service providers are configured in the Service Providers dialog, available from the Messaging option which is available from the System menu.
Pager Number	Cardholder’s pager number. You may enter up to 16 characters, in any combination of upper and lower case letters and numbers.
Pager Service Provider	Cardholder’s pager service provider. Select a pager service provider from the pre-defined list. Service providers are configured in the Service Providers dialog, available from the Messaging option which is available from the System menu.
E-mail Address	Cardholder’s email address. Begin the Email address with SMTP (Simple Mail Transfer Protocol). E.g.: SMTP.username@emailprovider.com
Use Email address in Message Forwarding	Tick this checkbox if you want the cardholder’s details to be available in the Event Task Effect for Message Forwarding – Forward to Email(s).
Manager Email Address	Email address of the Cardholder’s manager (if any).
Username	Enter a unique username for the cardholder in this field. Note: Only cardholders who have a username and password can be configured as Organizers for Venue Bookings.
Password	Enter a unique password for the cardholder in this field. Note: Only cardholders who have a username and password can be configured as Organizers for Venue Bookings.

Vehicle Tab

The fields and controls on this tab are explained in the table below.

Item	Description
Car Rego 1	Registration number of the cardholder’s first vehicle. You may enter up to 10 characters, in any combination of upper and lower case letters and numbers.
Car Model 1	Model of the cardholder’s first vehicle. You may enter up to 20 characters, in any combination of upper / lower case letters and numbers.
Car Color 1	Color of the cardholder’s first vehicle. You may enter up to 15 characters, in any combination of upper / lower case letters and numbers.
Car Rego 2	Registration number of the cardholder’s second vehicle. You may enter up to 10 characters, in any combination of upper / lower case letters and numbers.
Car Model 2	Model of the cardholder’s second vehicle. You may enter up to 20 characters, in any combination of upper / lower case letters and numbers.
Car Color 2	Color of the cardholder’s second vehicle. You may enter up to 15 characters, in any combination of upper and lower case letters and numbers

Tracking Tab

The fields and controls on this tab are explained in the table below.

Item	Description
Card Trace	When checked, this check box allows all the valid card transactions performed by the cardholder to appear in the Audit Trail as special exception alarms.
DateTime Card Last Used	This field will display Date and Time details about when a card was last used
Card Number Last Used	This field displays the card number that was last used
Point Name	This field displays the access point details where the card was last used
Last Anti-Passback Location	This field displays details about the anti-passback location where the card was last used
Anti-Passback Credential Profile	This dropdown field displays the Card number and Credential Profile of all the cards assigned to the cardholder.
Forgive Card button	This button “forgives” a cardholder and permits them to exit or enter an area, where normally this would produce an Anti-Passback violation. A forgive feature permits access for the first use of a card at either an Entry or Exit reader.
Remove Card from APB button	This button removes the card from the Anti-Passback area.
Add Card to APB button	This button adds the card to the Anti-Passback area.

Control Tab

The fields and controls on this tab are explained in the table below.

Item	Description
Card Number / Credential Profile	Drop down list to choose card/s assigned to the cardholder.
Access	Drop down list to choose between Access Points / Access Points Groups that will be displayed directly below this field.
Output	Displays a drop down list to choose between Outpoint Points / Output Point Group / Notification Zones / Notification Zone Groups that will be displayed directly below this field.
Add button	Adds the selections of the Access and Output fields to the Output Control section below.
Remove button	Removes selections from the Output Control section below.
Card field	Details the chosen card.
Access Point / Group field	Details the chosen Access Point / Group
Output Point / Group field	Details the chosen Output Point / Group
Time Schedule	Details the chosen Time Schedule
Filter Against Access Privileges checkbox	This selection filters this particular cardholder against all the access privileges configured for the same cardholder.

Imaging Tab

The fields and controls on this tab are explained in the table below.

Item	Description
Front Side tab	This tab will display a preview of the Card Template selected.
Reverse Side tab	This tab will display a preview of the Card Template selected.
Photo radio button	This button is used to display the image configured for the cardholder.
Signature radio button	This button is used to display the signature configured for the cardholder.
Live button	This button will connect the screen on this tab to video capture driver, to display a live image.
Capture button	The button captures the live image.
Import button	This button will bring up the Windows ‘Open’ dialog. The user can select a Graphics Image file from this dialog.
Export button	This button will import export the Graphics Image to a required location.
Contrast scale	This scale can be used to adjust the contrast level of the image displayed on the tab.
Brightness scale	This scale can be used to adjust the brightness level of the image displayed on the tab.

Item	Description
Card Template	This drop-down list displays the available Card Templates that can be selected.
Insert Card	This command is given to the Card Printer to insert a card for printing.
Eject Card	This command is given to the Card Printer to eject a card.
Print	This command is given to the Card Printer to print a card.

Custom Tabs

While some sites require minimal information concerning their cardholders, others may require very detailed information.

SiPass integrated allows you to customize cardholder records to suit your requirements in two ways:

- By adding additional pages to the *Cardholder / Visitor* dialog. Such additional pages are known as **Custom Pages**. Operators can design Custom Pages using the *Advanced Security Programming* feature of SiPass integrated. See the SiPass integrated *Configuration Client User Guide* for more information.
- By customizing the layout of existing Predefined Pages of the *Cardholder / Visitor* dialog.

The Advanced Security Programming feature can be accessed through the SiPass integrated Configuration Client.

Configuring Custom Tabs on the Cardholder Dialog

An operator can design and create **Custom Tabs** for the *Cardholder* dialog.

These tabs are created by designing **Custom Pages** using the **Advanced Security Programming feature in the SiPAss integrated Configuration Client**. For detailed information on how to create Custom Pages, refer the SiPass integrated Configuration Client User Guide.

The following steps are only required if Customizable Cardholder Fields have been created for the *Cardholder* dialog.

1. Choose the first customizable tab, in this case.
2. Complete each of the fields in the tab. Some fields can be populated from drop-down lists.

If there are any compulsory fields among the customizable fields, it is essential that they be completed. Failure to complete compulsory controls will generate an error.

3. New categories to the Custom Cardholder Fields can be added under the existing fields. Simply select a blank category from the drop down box in the field you’d like to add the category to and type in the name. When you have finished select Save.
4. When done, choose **OK**, You will be returned to the normal view of the Cardholder Custom Page.
5. Select any additional customizable tabs and complete the controls.
6. Click **Save**.

5.1.1.2 Adding Cardholders

This section provides simple instructions on how to add a cardholder to SiPass integrated.

▷ **Navigation from Main Menu:** *Operation > Cardholder > Definition* tab

1. Display the *Definition* tab of the *Cardholder* dialog. For descriptions on fields of this tab, refer Definition Tab [→ 27].
2. Complete the Cardholder’s Identification details.
   - ⇨ A single row of cardholder credentials appears in the **Credentials** section of this dialog. You can save a cardholder without a card number, by deleting this default row, and then clicking **Save**.
   - ⇨ Once the cardholder has been saved their **Last Name**, **First Name** and **Card Number** is displayed along the bottom of the *Cardholder* dialog, for all the tabs associated with this dialog. This helps you concentrate on the cardholder whose details you are entering or modifying, without the need to constantly refer back to the *Definition* tab.
3. Click **Save**.
   This new cardholder is saved in the SiPass integrated system.
   If you would like to create access privileges for the cardholder, or configure this cardholder record in any other way, proceed to the sections that follow.

Configuring the DEFINITION Tab

The sections that follow provide detailed instructions on how to perform specific configurations on the *Definition* tab of the *Cardholder* dialog.

For a quick-reference guide on the main fields to be configured, refer the section Definition Tab [→ 27].

Configuring Cardholder Identification Details

This section describes how to add/modify cardholder identification details on the *Definition* tab of the *Cardholder* dialog.

▷ **Navigation:** *Cardholder & Access Management > Cardholder > Definition* tab

1. Display the *Definition* tab of the *Cardholder* dialog. For descriptions on fields of this tab, refer Definition Tab [→ 27].
2. Complete the Cardholder’s Identification details.
   - ⇨ A single row of cardholder credentials appears in the **Credentials** section of this dialog. You can save a cardholder without a card number, by deleting this default row, and then clicking *Save*.
   - ⇨ Once the cardholder has been saved their **Last Name**, **First Name** and **Card Number** is displayed along the bottom of the *Cardholder* dialog, for all the tabs associated with this dialog. This helps you concentrate on the cardholder whose details you are entering or modifying, without the need to constantly refer back to the *Definition* tab.
3. Click **Save**.
   This new cardholder is saved in the SiPass integrated system.

Assigning Cardholder to Partition Workgroup

Navigation: *Cardholder & Access Management* > *Cardholder*.

1. Click the *Definition* tab.
2. Open or Create a new record for the cardholder who is to be assigned a partition workgroup.
3. Select a Work Group from the **Work Group** drop down field. You can also click the *…* button to select from the list of partition workgroups.
   – **NOTICE! Note:** Only Partition Workgroups are listed in this field. For details on Partition workgroups, refer the section Partition Workgroups [➞ 61]
4. Click **Save**.

⇨ The cardholder will be assigned to the selected partition workgroup.

Configuring Cardholders' Card & Card Credentials

The **Credentials** section of this tab is used to configure and display cards and card credentials for a cardholder. An operator can configure multiple cards for a cardholder.
Note: A maximum of 5 cards can be assigned to each cardholder.
On creating a new cardholder, a single row of cardholder credentials appears in the *Credentials* section of this dialog.

To Configure Card Credentials:

Navigation: *Cardholder & Access Management* > *Cardholder*.

1. Click the *Definition* tab.
2. Open or Create a new record for the cardholder who needs to be configured a card.
3. Click **New** to add a new credentials row. Or, you can configure the default row of this section.
4. In the **Card Number** field, enter a card number that is unique to the system. The field can be filled by badging the respective card, and clicking the **Assign Card** button.
5. Select a **Credential Profile** for the card. If you wish to create or edit a credential profile, click the **Credential Profile** button on this tab.
   For details on creating a Credential Profile, refer the section Credential Profile [➞ 57].
6. In the **PIN** field, type in a PIN number, or select a PIN from the drop down list. This is the cardholder’s Personal Identification Number for this card.
   ⇨ **Note:** The PIN length can be changed even when a credential profile is active for an existing cardholder as below (the ACC must be initialized again after making this change):
   – If PIN length is reduced, the PIN will be cropped at the end (i.e. 123456 => 1234)
   – If PIN length is extended, leading 0 will be added to the PIN (i.e. 1234 => 001234)
7. If the **Void** checkbox is ticked, the card will be made void. The cardholder will not be able to access the site, using this card.
8. In the **Start Date** field, type or select the date when the card can be used for access by the cardholder.
9. In the **End Date** field, type or select the date after when the cardholder can no longer use this card for access.

10. To disable the end date, simply un-tick the checkbox of the **End DateTime** field below.
11. Save your changes.

⇨ This newly configured card credentials will be saved in the system.

⇨ The number of digits in the **Card Number**, and the maximum number of cardholders, will depend on the SiPass card technology purchased with the license.

⇨ The drop down list of the *PIN field* is updated when a cardholder’s card number is entered. The cardholder may use their PIN if particular readers at the site are configured for both *Card* and *PIN*. This field will be hidden if the operator does not have the ‘See PIN’ operator privilege assigned.

Setting Unlimited End Date & Time for Card

The following action allows configures the cardholder’s access for an indefinite Date or Time.
As a result of this action, the **End DateTime** field of the *Cardholder* dialog becomes disabled for the particular cardholder.

Navigation: *Cardholder & Access Management* > *Cardholder*.

1. Click the *Definition* tab.
2. Open or Create a new record for the cardholder to be configured with this feature.
3. Tick the checkbox of the **End DateTime** field.
4. Click **Save**.

Voiding a Cardholder

The following action voids all the cards assigned to the cardholder, and none of his/her cards can be used to access the site.

Navigation: *Cardholder & Access Management* > *Cardholder*.

1. Click the *Definition* tab.
2. Open or Create a new record for the cardholder who is to be made void.
3. Tick the **Void Cardholder** checkbox.
4. Click **Save**.

Isolating a Cardholder

Isolating a cardholder means that the cardholder will be allowed to secure any area (to which they are granted access), even if input points of the area are not sealed.

Navigation: *Cardholder & Access Management* > *Cardholder*.

1. Click the *Definition* tab.
2. Open or Create a new record for the cardholder who is to be isolated.
3. Tick the **Isolate** checkbox.
4. Click **Save**.

Configuring APB Exclusion

The following action configures the cardholder to be excluded from an Anti-Passback areas that have been created.

Navigation: *Cardholder & Access Management* > *Cardholder*.

1. Click the *Definition* tab.
2. Open or Create a new record for the cardholder who is to be configured APB Exclusion.
3. Tick the **APB Exclusion** checkbox.
4. Click **Save**.

Configuring Extended Latch Time Accessibility

The following action can be configured to allow easier access for the cardholder. When a cardholder badges his/her card at a reader, the door will unlock for the Extended Latch Time, rather than the normal Latch Time. You can configure the Extended Latch Time in the *Components* dialog.

Navigation: *Cardholder & Access Management* > *Cardholder*.

1. Click the *Definition* tab.
2. Open or Create a new record for the cardholder who is to be configured with this feature..
3. Tick the **Accessibility** checkbox.
4. Click **Save**.

Configuring Cardholder as Supervisor

The following action configures the cardholder as a Supervisor for doors that are configured with the Dual Custody mode of operation. For more information, refer **Supervisor** checkbox description in the section Definition Tab [→ 27].

Navigation: *Cardholder & Access Management* > *Cardholder*.

1. Click the *Definition* tab.
2. Open or Create a new record for the cardholder who is to be configured as a supervisor.
3. Tick the **Supervisor** checkbox.
4. Click **Save**.

Configuring Self-Authorization

This action allows the cardholder to gain access to a door configured with the Dual Custody mode of operation, without needing the accompaniment of a subsequent cardholder before the door is unlocked.

Navigation: *Cardholder & Access Management* > *Cardholder*.

1. Click the *Definition* tab.
2. Open or Create a new record for the cardholder who is to be configured with self-authorization privileges.
3. Tick the **Self Authorize** checkbox.
4. Click **Save**.

Configuring Re-Entry Exclusion

This action exempts the cardholder from Timed Re-entry rules for areas that are operating in the Anti-Passback mode ‘Timed Re-entry’.

Navigation: *Cardholder & Access Management > Cardholder*.

1. Click the *Definition* tab.
2. Open or Create a new record for the cardholder who is to be configured with Re-entry Exclusion.
3. Tick the **Re-Entry Exclusion** checkbox.
4. Click **Save**.

Configuring Private Access Privileges

The following actions are required to configure Private Access Privileges for the cardholder. For more information on Private Access Privileges, refer the section Assigning Cardholder's Private Access Privileges [➞ 71].

Navigation: *Cardholder & Access Management > Cardholder*.

1. Click the *Definition* tab.
2. Open or Create a new record for the cardholder who is to be assigned a partition workgroup.
3. Ensure that cardholder identification and partition workgroup details are defined.
4. Click the **Access Privileges** button. The *Access Assignment* dialog is displayed.
5. Proceed to configure access privileges for the cardholder. For more information on assigning Private Access Privileges for a cardholder, refer the section Assigning Cardholder's Private Access Privileges [➞ 71].
6. The private access privileges assigned to a cardholder will be visible in **Private** tree hierarchy of the **Access Control** window of this tab.
7. Click **Save**.

Reading a Card

This action allows the operator to view the encoded cardholder information on a valid card. A dialog will appear containing the information held on the badged card.

Navigation: *Cardholder & Access Management > Cardholder*.

1. Click the *Definition* tab.
2. Open the record for the cardholder whose card is to be read.
3. Click the **Read** drop-down button, and select a required reader.
   The *Read Card* dialog is displayed.
4. Placed the card on the reader.
   The card details will be displayed on your system.

Assigning a Card

This action allows you to assign a card to a cardholder. This is a toggle-state button.

Navigation: *Cardholder & Access Management* > *Cardholder*.

1. Click the *Definition* tab.
2. Open or Create a new record for the cardholder who is to be assigned a card.
3. Badge a card at a configured reader, and click the **Assign** button.
   The card number is displayed in the **Card Number** field.
4. Click **Save**.

Reading and Searching Card

This action allows you to read the encoded cardholder information on a valid card, and then search for the card number on the system. This is a toggle-state button.

Navigation: *Cardholder & Access Management* > *Cardholder*.

1. Click the *Definition* tab.
2. Badge a card at a configured reader, and click the **Read & Search** button.

⇨ The card information will be displayed on the *Definition* tab.

Configuring the ADVANCED Tab

The sections that follow provide detailed instructions on how to perform specific configurations on the *Advanced* tab of the *Cardholder* dialog.

For a quick-reference guide on the main fields to be configured, refer the section Advanced Tab [→ 30].

Configuring Cardholder's Non-Partition Workgroup/s

The **Work Groups** section of this tab will list the Partition work group that the cardholder is assigned to (from the *Definition* tab). The partition work group will have its corresponding **Partitioning** checkbox ticked. This indicates that this is the Partition work group.

To assign the cardholder to a Non-Partition work group, follow the instructions below.

Navigation: *Cardholder & Access Management* > *Cardholder*.

1. Open or Create a new record for the cardholder who is to be assigned a non-partition workgroup.
2. Click the *Advanced* tab.
3. Click the **Choose** button.
   The Cardholder’s *Work Groups* dialog is displayed.
4. Select an object/s from **the Available Non-Partition Work Groups** list, and click **Add**.
   If you want to create a work group, click the **Define Work Group** button, and configuring the dialog that appears.
5. Click **OK**.
   The non-partition work group is listed in the *Advanced* tab.
6. Click **Save**.

Note: You can remove the cardholder from this non-partition work group, by clicking the **Choose** button, and removing the work group from the list of selected work groups.

Configuring Cardholder's Anti-Passback Count Workgroup

Navigation: *Cardholder & Access Management* > Cardholder.

1. Open or Create a new record for the cardholder who is to be configured with this feature.
2. Click the *Advanced* tab.
3. Click the **Choose** button.
   The Cardholder’s *Work Groups* dialog is displayed.
4. In the **Work Groups** section of this tab;
   Tick the **Use Anti-Passback** checkbox for the partition / non-partition work group that should include this cardholder in its anti-passback count.
5. Click **Save**.
6. **Note**: Only one work group can be selected for the cardholder’s anti-passback count.

Saving Cardholder's Fingerprints

▷ In order to enable the fields of this section, ensure that a Bioscrypt reader is configured and connected to the system.

▷ The **Finger Prints** section of the *Advanced* tab displays details of the cardholder’s fingerprints.

▷ A maximum of 2 fingerprints can be saved for each cardholder.

▷ **Navigation:** *Cardholder & Access Management* > Cardholder.

1. Open or Create a new record for the cardholder whose fingerprints are to be saved.
2. Click the *Advanced* tab.
3. Capture the cardholder’s fingerprint using the bioscrypt reader configured to the system.
   Note: You can repeat this step to capture additional fingerprints. However, only 2 of these prints can be saved in the system.
4. The **Finger Prints** section of the *Advanced* tab will display a new row for the captured fingerprint. If you have captured multiple fingerprints, select the rows that you do not require, and click the **Delete** button to remove these rows.
5. In the **Index** field, click to select the finger name that was used for the fingerprint capture.
6. In the **Credential Profile** field, select a credential profile to which this fingerprint should be saved.
7. Click the **Save** button on the *Cardholder* dialog.

⇨ The fingerprint/s will be saved in the SiPass integrated system. This system indicates this by displaying a ticked **Saved** checkbox for the fingerprint that was saved.

Encoding Cardholder's Fingerprint/s to Card

You can select a cardholder's fingerprint/s that is saved in the system, and encode it to a card.

Navigation: *Cardholder & Access Management* > *Cardholder*.

1. Open or Create a new record for the cardholder whose fingerprints are to be encoded to card.
2. Click the *Advanced* tab.
3. Ensure that you have captured, configured and saved a cardholder's fingerprints in the system. For more information on how to do this, refer the section Configuration Type B: Fingerprint Acquisition.
4. Place the card to be encoded on the Enrolment Reader, and click the **Encode** button on the *Cardholder* dialog.
5. The fingerprint/s will be encoded to the card.

⇨ This system indicates this by displaying a ticked **Encoded** checkbox for the fingerprint that was encoded to a card.

Configuring Cardholder's Smart Card Data

You can configure Smart Card profile for a cardholder in the Smart Card Data section of this tab.

Navigation: *Cardholder & Access Management* > *Cardholder*.

1. Open or Create a new record for the cardholder for whom smart card data is to be configured.
2. Click the *Advanced* tab.
3. Cick the **Profile** drop down button, and select a profile from the list.
   If you wish to create/modify an existing smart card profile, click the **Profile Viewer** button.
4. Click **Save**.

Configuring Cardholder's General Data

You can enter any general data for the cardholder that will be stored in the system database.

Navigation: *Cardholder & Access Management* > *Cardholder*.

1. Open or Create a new record for the cardholder whose general data is to be configured.
2. Click the *Advanced* tab.
3. In the **General Data** field of this tab, type in the information required.
4. Click **Save**.

Configuring the PERSONAL Tab

The sections that follow provide detailed instructions on how to perform specific configurations on the *Personal* tab of the *Cardholder* dialog.

For a quick-reference guide on the main fields to be configured, refer the section Personal Tab [→ 31].

Configuring Cardholder's Personal Details

You can enter a cardholder’s personal details in relevant fields of this tab. The cardholder’s personal details are not essential when creating a cardholder record. These fields can be used to narrow a match when attempting to locate a cardholder record in the database or to positively identify the cardholder.

Navigation: *Cardholder & Access Management* > *Cardholder*.

1. Open or Create a new record for the cardholder whose personal details are to be configured.
2. Click the *Personal* tab.
3. Complete the **Title**, **Date of Birth**, **Address** and **Payroll Number** fields of this tab. For details on each of the field, refer the section Personal Tab [→ 31].
4. Click **Save**.

Configuring Cardholder's Contact Details

You can enter a cardholder’s contact details in relevant fields of this tab.

Navigation: *Cardholder & Access Management* > *Cardholder*.

1. Open or Create a new record for the cardholder whose contact details are to be configured.
2. Click the *Personal* tab.
3. Complete the **Phone Number**, **Mobile Number**, **Mobile Service Provider**, **Pager Number**, **Pager Service Provider**, **Email Address** fields of this tab. For details on each of the field, refer the section Personal Tab [→ 31].
4. Click **Save**.

Configuring Cardholder's User Details

You can enter a cardholder’s **Username** and **Password** in the **User Details** section of the *Personal* tab. Cardholders with these details configured can be configured as Organizers of Venue Bookings in the system.

Navigation: *Cardholder & Access Management* > *Cardholder*.

1. Open or Create a new record for the cardholder whose user details are to be configured.
2. Click the *Personal* tab.
3. Enter a name in the **Username** field.
4. Enter a password in the **Password** field.
5. Click **Save**.

Configuring the VEHICLE Tab

The sections that follow provide detailed instructions on how to perform specific configurations on the *Vehicle* tab of the *Cardholder* dialog.

For a quick-reference guide on the main fields to be configured, refer the section Vehicle Tab [→ 32].

Configuring Cardholder's Vehicle Details

You can add details about the cardholder’s vehicle into the system through this tab. Note that these details are not essential when creating a cardholder record. However, they can be used to narrow a match when attempting to locate a cardholder in the database.

Navigation: *Cardholder & Access Management* > *Cardholder*.

1. Open or Create a new record for the cardholder whose vehicle details are to be configured.
2. Click the *Vehicle* tab.
3. Complete the fields under the *Vehicle* tab. For details on the various fields in the *Vehicle* tab, please refer the section Vehicle Tab [→ 32].
4. Click **Save**.

Configuring the TRACKING Tab

The sections that follow provide detailed instructions on how to perform specific configurations on the *Tracking* tab of the *Cardholder* dialog.

For a quick-reference guide on the main fields to be configured, refer the section Tracking Tab [→ 33].

Configuring a Card to be Traced

You can specify if the cardholder’s card transactions are to appear as special alarms in the system, on this tab.

Navigation: *Cardholder & Access Management* > *Cardholder*.

1. Open or Create a new record for the cardholder whose card is to be configured for trace.
2. Click the *Tracking* tab.
3. Tick the **Card Trace** checkbox.
4. Click **Save**.

This action allows all valid card transactions performed by the cardholder to appear in the Audit Trail as special exception alarms. Traced cardholder numbers that appear in audit trail will be pre-pended with the hash symbol, ‘#’.

The last Date and Time, Card Number, Point Name and Anti-Passback Location that was used by the cardholder will also be displayed on this tab. For more details on these fields, refer section Tracking Tab [→ 33].

Exempting Cardholder from Anti-Passback Violation

Navigation: *Cardholder & Access Management* > *Cardholder*.

1. Open or Create a new record for the cardholder whose card is to be exempted from anti-passback violation.
2. Click the *Tracking* tab.
3. Select the required card from the **Anti-Passback Credential Profile** drop down list.
4. Click **Forgive Card**.
5. Click **Save**.

Adding/Removing Card from Anti-Passback Area

Navigation: *Cardholder & Access Management* > *Cardholder*.

1. Open or Create a new record for the cardholder whose card is to be configured.
2. Click the *Tracking* tab.
3. Select the required card from the **Anti-Passback Credential Profile** drop down list.
4. To remove the card from the anti-passback area count, click **Remove Card from APB**.
5. To add a card to the anti-passback area count, click **Add Card to APB**.
6. Click **Save**.

Configuring the CONTROL Tab

For a quick-reference guide on the main fields to be configured, refer the section Control Tab [→ 33]. The *Control* tab can be used to configure the system to control a specific card-holder’s access to points in the site. At a system-level, this is done by using this tab to link specific readers (Access points) to door latches or output relays (Output points).

Navigation: *Cardholder & Access Management* > *Cardholder*.

1. Open or Create a new record for the cardholder whose access is to be configured.
2. Click the *Control* tab.
3. The **Output Control** box of this tab has four fields. For more information on these fields, refer the section Control Tab [→ 33].
4. From the **Card** field, select a card you wish to configure for an output link.
   – **Note**: By selecting the **All Card** option on the **Card Number** drop down menu, the user can configure a specific output link to all the cardholder’s cards.
5. From the **Access Point Group** field drop-down box, select one or more Access Points or Access Point Groups you want to link to a notification zone. The available points or point groups will appear in the list of this field. Multiple points can be selected by using CTRL + left click.
6. From the **Output Point / Group** drop-down box, select the output point or output point group you want to be activated. The available points or point groups will appear in the list below. Select one or more points or point groups from the list. Multiple output points can be selected by using CTRL + left click.

7. Select the **Time Schedule** during which the selected output points or groups may be activated.
8. Click **Add**. The linked access points and output points/groups will be added to the **Output Control** list.
9. Repeat the previous steps for every output point or group link you want to assign to this cardholder.
10. Click **Save**.

⇨ When the cardholder badges his or her card at one of the selected access points during the nominated Time Schedule, the output points will be unsecured. If the output points are already unsecured, there will be no effect.

Configuring the IMAGING Tab

The sections that follow provide detailed instructions on how to perform specific configurations on the *Imaging* tab of the *Cardholder* dialog.

For a quick-reference guide on the main fields to be configured, refer the section Imaging Tab [→ 34].

Importing Cardholder Images

The *Imaging* tab will only appear if the *Video Imaging and Card Printing Module* is installed. The *Imaging* tab allows you to capture a photograph or signature of a cardholder from a live video image, or import from an existing file. This photograph or signature can then be printed onto the cardholder's access card or viewed on-screen, together with the cardholder record.

Navigation: *Cardholder & Access Management > Cardholder*.

1. Open or Create a new record for the cardholder for whom images are to be imported.
2. Click the *Imaging* tab.
3. Select the **Import** button to display the Windows *Open* dialog.
4. Select the desired image file from those displayed in the list. The image will be displayed in the left-hand panel of the dialog.
5. Suitably crop and position the image in the template.

> Generally used image formats like JPG, BMP, PNG and TIF can be uploaded in SiPass integrated. Graphic Interchange Format (GIF) files are licensed and cannot be used with SiPass integrated.
>
> **Images with a maximum resolution of up to 4500x4000 are supported.** A resolution higher than this may result in error.

Capturing Cardholder Photographs

Once you have installed SiPass' *Photo ID and Image Verification Module* and have configured the image preferences, you can begin capturing cardholder images.

▷ Ensure that the video capture card has been installed and configured.

▷ Create an employee record for the employee whose image is to be captured.

▷ Ensure that a card template has been created.

▷ **Navigation:** *Cardholder & Access Management* > Cardholder.

1. Open or Create a new record for the cardholder whose photograph is to be captured.
2. Click the *Imaging* tab.
3. Click **Live**.

   ⇨ The imaging panel will display a live video image on screen.
4. Position the camera and employee so that the employee's picture is displayed clearly (in focus) on screen. Refer to the video camera's user guide for detailed instructions concerning its operation and settings.
5. Click **Capture**.
6. The live video image will appear on screen as a still image. A cropping tool will appear overlaid on the captured photo, and a contrast and brightness slider will also appear.
7. By positioning the cursor over one of the handles located at the corner of the cropping rectangle, you can change the size of the cropped area by dragging the rectangle to the desired size.
8. By positioning the cursor anywhere inside the cropping area, you can hold down the left mouse button and drag to move the cropped area. The part of the captured image that appears within the rectangle will appear in the photo field on the card template.
9. Use the **Contrast and Brightness** sliders, to adjust the image quality. The higher up the scale, the greater the Contrast and/or Brightness, and vice versa.
10. Click **Save** when complete.

Capturing Cardholder Signature

Once you have installed SiPass' Photo ID and Image Verification Module and have configured the image preferences, you can begin capturing cardholder signatures.

Ensure that the signature capture pad has been installed and configured.

1. Create an employee record for the employee whose signature is to be captured.
2. Ensure that a card template has been created.
3. Navigate to *Cardholder & Access Management* > *Cardholder* from the navigation pane.
4. Open or Create the record for the cardholder whose signature is being captured.
5. Click the *Imaging* tab.
6. Enable the **Signature** radio button by clicking on it once.
7. Choose **New Signature**. Sign the capture pad using the pen provided.
8. Use the **Contrast** and **Brightness** sliders to adjust the signature.
9. Click **Save**.

Importing Cardholder's Photograph or Signature

Once you have installed SiPass' *Photo ID Module* and have configured imaging preferences, you can begin importing photographs and signatures of cardholders.

1. Create an employee record for the cardholder whose image will be captured.
2. Ensure that the cardholder photograph or signature exists.
3. Navigate to *Cardholder & Access Management* > *Cardholder* from the navigation pane.
4. Open or Create the database record for the cardholder whose photograph or signature is being imported.
5. Click the *Imaging* tab. If a previous image of the employee signature exists in the employee's record, it will automatically be recalled when the *Imaging* tab has been selected.
6. Select the **Photo** radio button to import the cardholder's photograph or select the Signature radio button to import a signature.
7. Click the **Import** button.
8. Select the image file to import.
9. Click the **Open** button or double click on the file name.
10. By positioning the cursor over one of the handles located at the corner of the cropping rectangle, you can change the size of the cropped area by dragging the rectangle.
11. Use the **Contrast** and **Brightness** sliders, to adjust the image quality - the higher up the scale, the greater the Contrast and/or Brightness, and vice versa.
12. Click **Save**.

5.1.1.3 Searching for a Cardholder

SiPass integrated allows you to search the Database for a specific cardholder.

This can be done in two ways:

- Search based on details provided

– OR –

- Search by selecting a cardholder from the *Search Cardholder* dialog.

Both these methods have been discussed in detail in the two sections that follow.

Search Based on Details Provided

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Cardholder** list item.
3. Enter all or part of the details known about the cardholder into the respective fields displayed on the *Definition* tab.
4. To narrow the search as much as possible, enter all the data you can about the cardholder for whom you are searching. The more search criteria you enter, the more effective and quicker the search.
5. You can also use wildcards to search for cardholder details as specified in the table provided below in this section.
6. Click **Search** to begin the **Database** search.
   ⇨ The *Search Cardholder* dialog will appear if more than one cardholder record matches the search criteria. If only one record matches the search criteria, then that cardholder's information will be displayed directly in the *Definition* tab.
7. To skip to the next record, choose **Next**, or to go back a record, choose **Previous**.
8. When more than one cardholder is found as a result of a search, the order in which the cardholder's appear in the *Search Cardholder* dialog can be changed by clicking on the appropriate column header, sorting the order by **Card Number**, **Last Name**, **First Name, Employee Number** and **Card Status**.
9. To select a cardholder from the *Search Cardholder* dialog, double-click anywhere on the listed record or select the cardholder record and choose **OK.**

⇨ The selected cardholder's record will be retrieved from the Database and appear in the *Definition* tab.

Character	Description
%	Matches any string of zero or more characters
-	Matches any one character
[token]	Brackets can enclose a range or a set of numbers or letters, such as [1-9] or [klmnopq]. To format tokens use the following: • A 'range' token This token is formed with a start character and stop character. – Start is the beginning of the character range. – "" is a special character indicating a range. – Stop is the end of the character range. • A 'set' token: has discrete values in any order and it is inside brackets, it can be in any order, i.e., [ab6bc], and [abcde] are types of token sets.
^ token	The caret (^) before a token indicates that any characters following the caret will not be included in the search. For example: [^c-g] means that the search will not include any character which is a 'c' or a 'g'.

Search and Select a Cardholder from the 'Search Cardholder' Dialog

The operator can also use the *Search Cardholder* dialog to select a cardholder.

This can be done in the following manner:

1. Select the *Definition* tab on the *Cardholder* dialog.
2. Click **Search**. This action will display the **Search Cardholder** dialog and will list all the cardholders.
3. The cardholders can be segregated on the basis on the following field filters:
   - Card Number
   - First Name
   - Last Name
   - Workgroup
   - Workgroup Description
   - Workgroup Status
   - Access Group
   - Start Date
   - End Date
   - Card Status
   - Employee Number
   - Credential Profile
   - Visitor
4. Click under each Field cell. This will bring up a drop-down filter field. You can type specific information related to this field to search for a cardholder/(s). The cardholders filtered according to this data, will be displayed below.
5. Further, you can search for cardholder by making a required selection from the **Report Type** field. This action will display a report of cardholders that are filtered according to the option selected. For example, selecting Valid Cardholders will display all the cardholders whose status is displayed as Valid in the *Cardholder* dialog.
6. Viewing and selecting a cardholder from *Search Cardholder* dialog list can be done in the following ways:
   - Right-click and select **View Cardholder**. This action displays the details of the selected cardholder on the *Definition* tab, while keeping the *Search Cardholder* dialog displayed.
   - Right-click and select **View Cardholder and Close Search**. This action displays the details of the selected cardholder on the *Definition* tab, and closes the *Search Cardholder* dialog.
   - Double-click on a cardholder in the list. The details of the selected cardholder will be displayed on the *Definition* tab, and the *Search Cardholder* dialog will be closed.

NOTICE! If you click **View Cardholder** without performing a new search, the previous search result is displayed. To ensure that you get an updated cardholder search report every time, it is recommended to run a new search before viewing the result.

5.1.1.4 Adding a Custom Report to Cardholder Search

You can add a customized report to the Cardholder Search Function.

Pre-requisite: Create the required Customized Reports based on any Predefined Cardholder report. See the Reports [➙ 113] section for more details.

1. From the left-hand navigation pane, double-click **Cardholder**.

   ➪ The *Cardholder* dialog is displayed.

2. Click the **Search** button on the right-hand side of the dialog.

   ➪ The *Search Cardholder* dialog is displayed.

3. Click the **…** button (next to the Filter Type dropdown list.

   ➪ The *Select Custom Reports* dialog is displayed, listing all the custom reports created earlier.

4. Check the tick-boxes for the custom reports that you wish to add to the Cardholder Search.

5. Click **OK**.

   ➪ The *Search Cardholder* dialog box is displayed again.

6. Click the **Filter Type** dropdown list.

   ➪ The customized reports that you selected above will now be available in this list.

5.1.1.5 Configuring Multiple Cards for a Cardholder

The **Credentials** section of the *Definition* tab lists all the cardholder’s cards.

If only one card has been assigned to the cardholder, it will still be displayed on this tab.

For more information, refer the section Configuring Cardholders' Card & Card Credentials [➙ 37].

5.1.1.6 Unused Cards

SiPass integrated can track cards that have not been used recently.

The operators need to follow these processes to apply this feature:

- **Configure a Report**:

  The operator tracks and views Unused Card(s) by configuring a Customized or Predefined report in SiPass integrated.

- **Convert the Report into an Actionable Report**:

  The operator converts the Customized or Predefined Report into an Actionable Report, by assigning an action to it. This action can be either to void an Unused Card(s), or Cardholder(s) of these unused cards.

- **Trigger a Host Event Task**:

  In the Host Event Task dialog, the operator selects the created Actionable Report to trigger the action that voids Unused Card(s), or Cardholder(s).

These processes are discussed in detail, in the sections that follow.

Tracking Unused Cards using Customized / Predefined Reports

It is possible to configure SiPass integrated to generate reports of cards that are unused for a specific number of days. This feature will allow operators to track and view details of these cards.

This is particularly useful when configuring cardholders with multiple cards. It gives the operator the ability to track, not just the cardholder, but each of his cards also.

Configuring SiPass to generate reports of unused cards is done in SiPass integrated.

This can be done in two ways:

- By configuring a Customized Report that displays all the inactive cards, filtered using specific parameters.

– OR –

- By using a Pre-defined Report that displays all the inactive cards using a 30-Day Threshold.

The steps required for both these options are provided below.

Tracking Unused Cards using a Customized Report

1. In the **Navigation** panel on left, select and right-click **Customized Reports**.
2. Select **New Report**. This action will display the **Report Wizard** application.
3. Click **Next**.
4. Enter a **Name** for the report, and click **Next**.
5. Select **Cards – Inactive** from the **Record Type** field.
6. From the **Available Fields** section, add all the fields required for this report.
7. Click **Next**.
8. Specify the filter conditions in this dialog.

ℹ For more information on how to specify Filter Conditions, refer the section Filter Conditions.

9. Click **Finish**.

⇨ This action will display the report on the SiPass Operation Client panel.

Tracking Unused Cards using a Predefined Report

On selecting this option, the system generates a report for all the cards that have been unused since the last 30 days.

1. In the **Navigation** panel on left, select and expand **Predefined Reports**.
2. Select and expand **Cardholder**.
3. Right-click the **Inactive Cards – 30 Day Threshold** report.

ℹ The steps required to covert this Predefined Report to an Actionable Report by assigning a **Void Card / Cardholder** action to it, are the same as those described in the section above.

Converting the Report into an Actionable Report

This sub-section explains how an operator can convert this Customized Report to an Actionable Report, by assigning an action to it. This action can be to void unused cardholder(s) / card(s).

1. Select and right-click on this report on the **Navigation** panel.
2. Select **Customize Current View**.
3. In the dialog that appears, select **Available Actions**.
4. Tick the **Void Cardholder** checkbox to void a cardholder of an inactive card(s). Further, click on this option to highlight it.
5. Tick the **Void Card** checkbox to void an inactive card. Further, click on this option to highlight it.
6. Select the **Set as Default** button.
7. Click **Apply**, and **OK**.

⇨ The customized report has been converted to an Actionable Report.

The steps required to covert this Predefined Report to an Actionable Report by assigning a **Void Card / Cardholder** action to it, are the same as those described in the section above.

Configuring a Host Event Task based on the Actionable Report

This section explains how an operator can select the Actionable Report as a Target, to void Unused Cards, or Cardholder(s) of these unused cards.

1. Select **Program > Event Tasks > Host**.
2. After entering an **Event Name** and **Time Schedule**, configure all the fields of the **Trigger** section.
3. From the **Target** field, select **Actionable Report**.
4. From the **Report** field, select a specific **Actionable Report**.
5. Enter a required message in the **Message** field.
6. Click **Save**.

⇨ The system has now been configured to void Unused Card(s) or Cardholders(s) of unused cards, based on the Actionable Report selected.

5.1.2 Visitors

SiPass integrated includes an extensive Visitor Management function. Visitors in SiPass can be regarded as temporary cardholders: the same information needs to be captured as for permanent cardholders, but additional information such as card issue status and length of stay also needs to be recorded.

The Visitor interface is therefore extremely similar in appearance and functionality to the Cardholder dialog. Access privileges and personal data need to be assigned and collected, Visitor facial and signature images can be captured and printed onto a card, and custom visitor fields for additional data can be created. You can also create custom fields specifically for Cardholders, Visitors, or both.

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.

A Visitor type is available in the Workgroups dialog, allowing you to create workgroups specifically for the purpose of organizing visitor groups.

All visitor transactions are recorded in the Audit Trail and an extensive Visitor reporting facility is available to produce documentation of visitor histories.

5.1.2.1 Adding a Visitor

There are pre-defined tabs available when adding a visitor – *Visitor Definition*, *Advanced*, *Personal*, *Tracking*,*Visitor Management*, *Control*, *Imaging* and *Visitor Details*. You can create additional tabs the **Custom Fields** feature of the SiPass integrated application.

▷ Ensure that all the access points, areas, Time Schedules and site management details have been configured. If you have the optional *Photo ID* and *Card Printing* modules installed and are going to print a visitor card, ensure you have designed a card template first.

▷ Ensure that field entries are not preceded by (white) spaces. This may cause unpredictable behavior in other areas of the application.

▷ **Navigation:** *Cardholder & Access Management* > *Visitor*.

1. Complete the *Visitor Definition* tab exactly as for a normal cardholder except for the visitor start and end dates, these vary.
   – The **Start Date** will be set to the current date, click on the drop down box to select a new date.
   – The **End Date** will also be set to the current date, unless changed.
   – In order to change the validity days, this can be done via the **System Preferences** option in the **Options** menu. Enter the number of days next to 'Visitor default validity time (days)'.
2. Select the *Advanced* tab and configure the cardholder's details as required (as described for a normal cardholder).
3. Select the *Personal* tab and complete the visitor's personal details (as described for a normal cardholder).
4. Select the *Tracking* tab and tick the **Card Trace** checkbox to enable tracking of the visitor.
5. Select the *Visitor Management* tab and complete the visitor management details:
   – **Select Cardholder**: Allows an existing cardholder with whom the visitor is meeting to be nominated.
   – **Remove Cardholder**: Removes the existing cardholder with whom the visitor is meeting to be nominated..

6. Select the *Control* tab and fill in the information as described for a normal cardholder.
7. Select the *Visitor Details* tab and fill in the required information.
8. Select the *Imaging* tab, if you intend to capture or import the Visitor's photograph or signature.

   ⇨ The *Imaging* tab will only appear if the *Photo ID and Image Verification* Module is installed. The *Imaging* tab allows you to capture a photograph or signature of a visitor from a live video image, or import from an existing file. This photograph or signature can then be printed onto the visitor's access card or viewed on-screen.

9. Complete the details in the *Visitor Details* tab as required.
10. If you have created any *Customizable Cardholder* Fields for the *Visitor* dialog, they must be completed.
11. Return to the *Visitor Definition* tab.
12. Click **Save**.

5.1.2.2 Issuing and Returning Visitor Cards

Once you have created the Visitor record with access privileges and personal details, Visitor cards can be issued or returned as required. Issuing a card requires that you nominate an existing cardholder to be the "sponsor" for the visitor.

Issuing a Visitor card

Navigation: *Cardholder & Access Management* > *Visitor*.

1. Use the **Search** button in the *Visitor Definition* tab to locate the Visitor record for whom you want to issue a card. Otherwise, create the new record as described in the previous procedure.
2. Select the *Visitor Management* tab.
3. Choose *Select Cardholder*.
4. Select an existing cardholder from the list who will "sponsor" the visit.

   – If you press an alphabet key on the keyboard, SiPass integrated will automatically scroll the list to the nearest cardholder surname beginning with that letter.

5. Choose **OK**.

   ⇨ You will be returned to the *Visitor Management* tab of the *Visitor* dialog and the selected cardholder will appear in the **First Name** and **Last Name** fields.

6. Choose **Issue** and **Save**.

   ⇨ The **Card Status** field will update to "Issued" and the **Issue Time** field will contain the current time.

7. Click **Save**.

⇨ The Visitor record will be updated with the Card Issue details.

Returning a Visitor card

1. Select **Visitor** from the **Operation** menu or toolbar.
2. Use the **Search** function in the *Definition* tab to locate the Visitor record for whom you want to return a card.
3. Use the **Next** function to navigate to the next record in the database. Use the **Previous** function to navigate to the preceding record.

4. Select the *Visitor Management* tab.
5. Choose **Return Save**.
   - ⇨ The Status field will be updated to “Returned” and the Return Time field will contain the current time.
6. Return to the *Definition* tab.
7. Click **Save**.

⇨ The Visitor record will be updated with the Card Return details.

5.1.2.3 Adding a Visitor to a list of Expected Visitors

A list of visitors expected to visit the site can be compiled and displayed at any time.

Navigation: *Cardholder & Access Management* > *ExpectedVisitor*.

1. Choose **Add**.
2. Select a visitor from the list of visitors displayed by highlighting their name.
   - ⇨ Only those visitors that are enrolled in the system will be available for selection. Before adding a visitor to the list of expected visitors ensure that you have enrolled the details of that visitor first.
3. Select the date and time the visitor is expected to arrive at the facility.
4. Select the date and time the visitor is expected to depart the facility.
5. Choose **OK**. Choose **Close**.

⇨ The Expected Visitors list will be updated and closed.

5.1.3 Credential Profile

The Credential Profile feature gives collections of workgroups the flexibility to use different card formats for access control and security. Cardholders can be configured with multiple cards of different credential profiles.

Components of the Credential Profile

The Credential Profile is defined by the following components:

- **Name**: This field details the name of the Credential Profile.
- **Card Technology**: This field details the Card Technology assigned to this credential profile.
- **Facility Code**: This field details the Facility Code of the credential profile.
- **Validity Code**: This field details the Validity Code of credential profile.
- **PIN Mode**: This field details the Operation Mode configured for the credential profile.
- **PIN Digits**: This field details the number of digits that can be configured for the card’s PIN Number.
- **In Use**: This field details if the card is in use. If ticked, it indicates that this Credential Profile has been applied to at least one card.

Once created, a Credential Profile can be configured to a cardholder’s card.

Two valid cards cannot have the same credential profile. When displayed as being ‘**In Use**’, the **Name**, **Card Technology**, **Facility Code** and **Validity Code** of that particular card cannot be modified.

Navigating to the Credential Profile

The *Credential Profile* dialog can be accessed in two ways:

◈ **Cardholder & Access Management** > **Credential Profile**.

OR

1. Select **Cardholder & Access Management** > **Cardholder**.
2. Next, click the *Definition* tab.
3. Click the **Credential Profile** button.

5.1.3.1 Adding / Deleting Credential Profiles

1. Select **Cardholder & Access Management > Credential Profile** from the main toolbar to display the *Cardholder's Credential Profile* dialog.
2. To add a credential profile, select **Add**.
   ⇨ A new row will be added to this dialog. Once configured and saved, each row corresponds to an individual Credential Profile.
3. Select a cell under the **Name** column. This field can be edited by typing into it.
4. Select a cell under the **Card Technology** column. This field can be configured by making a selection from the cell's drop-down list.
5. Select a cell under the **Facility Code** column. This field can be edited by typing into it.
6. Select a cell under the **Validity Code** column. This field can be edited by typing into it.
7. Select a cell under the **PIN Mode** column to configure an operation mode for the profile.
8. Select a cell under the **PIN Digits** column. This field can be edited by typing into it.
   ⇨ **Note:** The PIN length can be changed even when a credential profile is active for an existing cardholder as below (the ACC must be initialized again after making this change):
   – If PIN length is reduced, the PIN will be cropped at the end (i.e. 123456 => 1234)
   – If PIN length is extended, leading 0 will be added to the PIN (i.e. 1234 => 001234)
9. Select a cell under the **In Use** column.
   ⇨ This field will change depending on whether the Credential Profile has been assigned to a card. When assigned, it will display as **Yes**. If not, it will display as **No**.
10. To delete a Credential Profile, select the appropriate profile row and click **Delete**.

Operators can also access the *Cardholder's Credential Profile* dialog from the *Definition* tab on the *Cardholder / Visitor* dialog. Click the **Credential Profile** button on this tab to display the dialog. If more than one card configured to a cardholder has the same Credential Profile, only one of them will be valid.

5.1.4 Workgroup

Workgroups are logical groups to which selected cardholders belong. Generally, cardholders whose jobs are the same or similar will belong to the same Workgroup.

Types of Workgroups:

You may, or may not want to allow operators to have privileges to view/create/edit the partition functions of a workgroup. Based on whether want to confer these Operator Partitioning privileges to an operator, there are two kinds of workgroups that can be created:

- **Partition Workgroups**

Operator Partitioning is possible with Partition Workgroups. The ability to View / Create / Edit the Partition Workgroup depends on the operator privileges conferred to the operator group.

These partition workgroups can be used for assigning Access Control and Anti-Passback control.

A cardholder can be configured to only one partition workgroup.

The level of partition privileges the operator can configure to his/her operator group depends on the operator's own privileges.

For detailed information on these workgroups, refer the section Partition Workgroups [→ 61].

- **Non-Partition Workgroups**

Operator Partitioning is **not** possible with Non-Partitioned Workgroups.

A cardholder can be a member of multiple Non-Partition Workgroups.

They can be used for assigning Access and Anti-Passback control.

For detailed information on these workgroups, refer the section Non-Partition Workgroups [→ 63].

5.1.4.1 Work Group Fields

The sections that follow provide details of fields and other configuration options on the *Work Group* dialog.

Work Group Configuration Tab Fields Description

Field	Description
Work Group Name	Specifies a unique name for the work group. You may enter up to 40 characters, in any combination of upper and lower case letters and numbers.
Void Work Group checkbox	When checked, all cardholder cards belonging to this work group will be voided and all cardholders belonging to that work group will be denied access at all access points.
Partition Group checkbox	When checked, the work group created will be considered a Partition Work Group.
Clear Card Number (enabled for visitor only)	Tick this checkbox to clear the card number for a visitor under the visitor dialog.
Department	Indicates that the work group is an internal department.
Contractor	Indicates that the work group is an external contracting company.
Other	Indicates that the work group is a miscellaneous group that does not belong to either a department or contractor.
Visitor	Indicates that the work group is a dedicated group for visitors.
Clear Card Number (enabled for visitor only)	Tick this checkbox to clear the card number for a visitor under the *Visitor* dialog. This checkbox is enabled only when the **Visitor** checkbox is ticked.
Access Control box	Displays the access control details configured for the selected work group.
Disable Access Control checkbox	Tick this checkbox to temporarily disable any inherited access privileges for the selected workgroup. To re-enable the access privileges, un-tick this checkbox.
Access Privileges button	Clicking this button displays the *Access Assignment* dialog, where access privileges for the workgroup can be created or modified.

Contact Tab Field Description

Name	Specifies the name of the primary contact for the work group. You can enter up to 40 characters, in any combination of upper and lower case letters and numbers.
Title	Specifies the primary contact's title. You can enter up to 20 characters, in any combination of upper / lower case letters and numbers.
Addr	Specifies the primary contact's home address. You can enter up to 80 characters, in any combination of upper and lower case letters and numbers.
Phone	Specifies the primary contact's home phone number. You can enter up to 20 characters, in any combination of upper and lower case letters and numbers.
Fax	Specifies the primary contact's fax number. You can enter up to 20 characters, in any combination of upper and lower case letters and numbers.
Mob	Specifies the primary contact's mobile phone number. You can enter up to 20 characters, in any combination of upper and lower case letters and numbers.

5.1.4.2 Partition Workgroups

This section will explain the concept of Partition Workgroups.

Only Partition Workgroups can be used for Operator Partitioning.

Each cardholder can be configured to only ONE partition workgroup.

They can be used for assigning Access and Anti-Passback control.

Creating Partition Workgroups

For details on how to create Partition Workgroups, refer the section Creating Partition Workgroups [→ 62] of this manual.

Searching/Selecting Partition Workgroups

Once configured and saved, Partition Workgroups will be listed in the following dialogs:

- In the **Workgroup Name** dropdown field of the *Work Group* dialog. The ability to View / Create / Edit the Partition Workgroup depends on the operator privileges conferred to the operator group.
- In the **Workgroup Id** dropdown field of the *Cardholder* dialog. Only Partition Workgroups will be listed here. However, the ability to view these workgroups depends on the operator privileges conferred to the operator group.

Searching for a Cardholder belonging to a Partition Group

Operators can use the **Search** button on the *Cardholder* dialog to list or find a cardholder/s that belongs to a Partition Group.

ℹ In order for operators in an operator group to view cardholders belonging to Partition Workgroups assigned to them, they must be given operator privileges to **Customized** and **Pre-defined Cardholder reports**. These can be found within the **SiPass Explorer** items under **Partition Functions** displayed in the *Operator Group* dialog.

Creating a Partition Work Group

1. Select *Cardholder & Access Management* > *Work Group* from the main menu.
   - ⇨ The *Work Group* dialog is displayed. This dialog displays a tree view of all the available work groups, on its left panel.
2. Select the *Work Group Configuration* tab.
3. Enter a name for the work group in the **Work Group Name** field. You can search for existing work groups by clicking the **…** button.
   - – **Note**: This name should be as descriptive as possible. This will help SiPass operators identify the Work Group easily. Enter up to 40 characters, in any combination of upper and lower case letters and numbers.
4. By default, the **Partition Work Group** checkbox is ticked. This checkbox is enabled only when creating a new work group.
5. Select the **Group Type**. For more information on each option, refer the field descriptions of the **Group Type** in the section Work Group Configuration Tab Fields Description [→ 59].
6. Click **Save**.
   - ⇨ This workgroup will be saved as a Partition Work Group.
7. **From the perspective of an operator's privileges:** Partition workgroups can be selected on the *Operator Group* dialog for operator partitioning of the workgroup partition functions. You can view this partition workgroup list by navigating in the following manner from the main menu: *Cardholder & Access Management* > *Operator Group* > *Partition functions* > *Work Groups*

5.1.4.3 Non-Partition Workgroups

This section will explain the concept of Non-Partition Workgroups.

Non-Partition Workgroups are NOT available for Operator Partitioning.

They can be used for assigning Access and Anti-Passback control.

Creating Non-Partition Workgroups

For details on how to create Non-Partition Workgroups, refer the section Creating a Non-Partition Work Group [→ 64] of this manual.

Searching/Selecting Non-Partition Workgroups

Once configured and saved, Non-Partition Workgroups will be listed in the following dialogs:

- In the **Workgroup Name** dropdown field of the *Work Group* dialog.
- Clicking the **Work Groups** button of the *Advanced* tab in the *Cardholder* dialog will display the *Cardholder's Work Groups* dialog. The operator can view the Non-Partition Workgroups in this dialog, and select a workgroup/s to be configured for the cardholder. The selected Non-Partition workgroups will be listed in the **Work Groups** section of the *Advanced* tab.

Creating a Non-Partition Work Group

1. Select *Cardholder & Access Management* > *Work Group* from the main menu.

   ⇨ The Work Group dialog is displayed. This dialog displays a navigation tree on its left panel. Here, you can view the hierarchy of all the work groups available in the system.

2. Select the *Work Group Configuration* tab.
3. Enter a name for the work group in the **Work Group Name** field. You can search for existing work groups by clicking the **…** button.

   – This name should be as descriptive as possible. This will help SiPass operators identify the workgroup easily. Enter up to 40 characters, in any combination of upper and lower case letters and numbers.

4. Untick the **Partition Work Group** checkbox. This checkbox is enabled only when creating a new work group.
5. Select the **Group Type**. For more information on each option, refer the Field Descriptions of the Group Type box in the section Work Group Configuration Tab Fields Description [→ 59].
6. Click **Save**.

   ⇨ This workgroup will be saved as a Non-Partition Work Group.

7. **From the perspective of an operator's privileges:** Non-partition workgroups cannot be used for Operator Partitioning, and will not be listed in the *Operator Group* dialog for operator partitioning of the workgroup partition functions.

5.1.4.4 Configuring Workgroup Access Privileges

1. Select *Workgroup* from the *Operation* menu.
2. Find or create the workgroup record whose access privileges to be changed.
3. Click on the **Access Privileges** button. The *Access Assignment* dialog is displayed.
4. Click the *Access Assignment* tab.
5. From the **Access Type** field drop down list, select the access objects that should be included in the workgroup privileges.

   – If you wish to create new, or modify existing access levels and groups, click the *Access Group Definition* tab, and *Access Level Definition* tab, and configure these tabs as required.

6. The select access type object names will be listed in the adjacent box of the *Access Assignment* tab.
7. Select the access type object and click **Add**, to add them to the workgroup's access privileges.
8. Click **OK**. You will be returned to the *Work Group* dialog.

   ⇨ The selected access privilege is displayed in the **Access Control** section of this dialog.

9. Click **Save**.
10. For instructions on how to assign these workgroup access privileges to a bulk set of card/cardholders, refer the section Automatic Bulk Card Creation [→ 66].
11. For instructions on how to assign these workgroup access privileges to a specific cardholder, refer the section Assigning Cardholder's Workgroup Access Privileges [→ 73].

Temporarily Disabling Workgroup Access Privileges

It is possible to temporarily disable inherited access privileges for a specific workgroup. This means that all the cardholders belonging to this workgroup will not be able to use the access privileges of this workgroup, until its access privileges are re-enabled.

1. Select *Workgroup* from *Cardholder & Access Management* in navigation pane.
2. Find the workgroup record whose access privileges to be temporarily disabled.
3. Check the **Disable Access Control** checkbox.
4. Click **Save**.

⇨ The access privileges of the selected workgroup are temporarily disabled. To re-enable its access privileges, un-tick the **Disable Access Control** checkbox.

Modifying Workgroup Access Privileges

1. Click *Cardholder & Access Management* > *Work Group* from SiPass main menu to display the *Work Group* dialog.
2. Enter the name of the work group in the **Work Group Name** field, or click the **…** button to search for a work group. Alternatively, you can also select the work group from the left navigation tree.
3. Click the **Access Privileges** button of this dialog.
   ⇨ This displays the *Access Assignment* dialog.
4. Click the access privilege to be modified, in the **Access Control** box of this dialog.
5. Click the **Remove** button, or double-click the item. This will delete the item from the box.

⇨ You can now add new access privilege/s to the box if required.

5.1.4.5 Voiding a Workgroup

When a work group is made void, all cardholder cards belonging to this work group will be voided, AND all cardholders belonging to that work group will be denied access at all access points.

1. Click *Cardholder & Access Management* > **Work Group** from the navigation pane to display the *Work Group* dialog.
2. Enter the name of the work group in the **Work Group Name** field, or click the **…** button to search for a work group. Alternatively, you can also select the work group from the left navigation tree.
3. Tick the **Void Work Group** checkbox.
4. Click **Save**.

5.1.4.6 Deleting a Workgroup

1. Click *Cardholder & Access Management* > **Work Group** from the navigation pane to display the *Work Group* dialog.
2. Enter the name of the work group in the **Work Group Name** field, or click the **…** button to search for a work group. Alternatively, you can also select the work group from the left navigation tree.
3. Click **Delete**.
4. Click **Yes** to confirm your action.

⇨ This workgroup will be deleted from the system.

5.1.4.7 Configuring Card Profiles for Workgroups

1. Select the *Card Configuration* tab of the *Work Group* dialog.
2. Click the **Smart Card Profile** drop down list, and select a profile to be assigned to this work group.
3. Click the **Update Cardholders** button.
   ⇨ This action updates this smart card profile to the *Advanced* tab of the *Cardholder* dialog, for every cardholder in the selected work group.
   – **Note**: If the **Profile** field, detailed above, is cleared or left blank, the cardholders in the selected workgroup will no longer be configured with this smart card profile.
4. Click **Save** to save your configuration.

5.1.4.8 Automatic Bulk Card Creation

Once you have defined a Work Group it is possible to automatically create a set of cards and assign them to it. This way, you can automatically apply the same set of access control privileges to a set of cards.

Note: Bulk cards cannot be created automatically for non-partition workgroups.

▷ Ensure that you have created and saved the Work Group for which you wish to create a bulk set of cards automatically.

1. Choose **Work Group** from the **Operation** toolbar or menu.
2. From the **Work Group Name** drop-down box, select the name of the Work Group in which you wish to create a bulk set of cards.
3. Ensure that the correct Work Group details are complete, including the Work Group’s access control privileges (if required).
4. Enter the range of cards to be automatically created in the **Card Range** field. For example “11-15” will create cards 11, 12, 13, 14, and 15.
5. Choose the **Create Cards** button.
   ⇨ SiPass integrated will now begin creating all cards in the range specified. A *Status* dialog will appear indicating the status of the bulk creation of cards.
6. When finished, choose **Close**.

5.1.4.9 Configuring Cardholder Workgroup for Anti-Passback Assignment

1. Navigate to the *Advanced* tab of the *Cardholder* dialog for the cardholder to be configured for workgroup anti-passback count.
2. In the **Work Groups** section of this tab, tick the **Use for Anti-Passback** checkbox for the Partition / Non-Partition Workgroup that should be configured for the cardholder’s anti-passback count.
3. Click **Save**.

⇨ **Note**: Only one workgroup listed in this section can be used to be included in the cardholders anti-passback count.

5.2 Access Management

The level of access a cardholder has to various points at your site is determined by the access control privileges that they have been assigned. Cardholder access control is achieved by:

- Creating Time Schedules
- Defining Access Levels
- Defining Access Groups
- Assigning Access Privileges to Cardholders or Workgroups

While configuring access assignment for Cardholder/Visitor, Venue and Workgroups, the OSDP FLN Access Points may be displayed in the list of points available for selection.

These MUST NOT be selected for any access assignment..

5.2.1 Access Levels

An access level is a collection of access points or access point groups mapped to a Time Schedule.

An operator must have access privileges to all of the points in an access level, before they can modify, delete or assign the access level to access groups.

5.2.1.1 Configuring Access Levels

▷ Ensure that all the access points, point groups, areas/sub-areas and floors to which the cardholder will require access have been defined.

▷ Establish the Time Schedules during which the cardholders will require access.

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Access Level** list item.
   ⇨ The *Access Level Definition* dialog is displayed. Alternatively, you can also access this dialog by clicking the **Access Privileges** button on the *Cardholder* dialog.
3. Enter a name for the Access Level into the **Name** field.
4. Select the **Time Schedule** for which the selected access points will be unsecured, from the **Time Schedule** drop down box.
   – **Never**: The cardholder cannot gain access at any time
   – **Always**: The cardholder can gain access at the points, areas/sub-areas, groups or floors at all times
   – **System Function (non busy intervals)**: The event task can only be triggered between 2 am and 3 am every day of the year including holidays
5. Select whether you are adding access points or access point groups from the **Type** drop down box.
6. Select the point or point group in the bottom list that you want to add to the Access Level. Click the **Add** button to add it to the adjacent list.

The OSDP FLN Access Points may be displayed in this list and should not be selected for assigning to an Access level.

7. To remove an access type from this list, select it, and click the **Remove** button.
8. Repeat for every point or point group that you want to add to the access level.
9. Click **Save**.

5.2.1.2 Searching for an Access Level

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Access Level** list item.
3. In the **Search** field indicated by **<Search>** enter the name or part of the name of the Access level you are looking for.
4. Click on the Arrow button to begin your search.
   - ➪ A list of all matching access levels will appear in the list box.
5. Click on the **Cross** button to clear the search field and enter a new term for searching.

> ℹ This search field is dynamic and will automatically begin filtering the list of access levels based upon the letters you type into the field as you type.

5.2.2 Access Groups

An access group is a collection of access levels. Access groups are assigned to cardholders and workgroups to determine the level of access personnel have to entry points at your site. The following steps describe how an Access Group can be defined.

5.2.2.1 Configuring Access Groups

▷ Ensure you have defined all of the access levels required for your site.

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Access Group** list item.
   - ➪ The *Access Group Definition* dialog is displayed. Alternatively, you can also access this dialog by clicking the **Access Privileges** button of the *Cardholder* dialog.
3. Enter a name for the Access Group into the **Access Group Name** field.
   - ➪ A list of Access Levels will appear in the **Available Access Levels** list.
4. Select the access level you want in the Access Group and use the **Add** button to move them to the **Selected Access Levels** list.
5. Repeat for every access level you want to add to the group.
6. To remove an access level, select it from the **Select Access Levels** list, and click the **Remove** button.
7. Click **Save**.

5.2.2.2 Searching for an Access Group

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Access Group** list item.
3. In the **Search** field indicated by **<Search>** enter the name or part of the name of the Access Group you are looking for.
4. Click on the Arrow button to begin your search.
   - ⇨ A list of all matching access groups will appear in the list box.
5. Click on the Cross button to clear the search field and enter a new term for searching.

This search field is dynamic and will automatically begin filtering the list of access groups based upon the letters you type into the field as you type.

5.2.3 Access Assignment

Operators can assign *single* or *multiple* access rights to cardholders, workgroups or venues, without limitations on the number of access rights per cardholder. This can be done for any of the following access types: *Points*, *Point Groups*, *Access Levels*, *Access Groups*, *Floors*, *Floor Groups*, *Intrusion Areas*, *Intrusion Area Point Groups*.

Any of the above can be assigned either permanently, or temporarily (with a start and end date). Any combination of permanent access rights, or access rights with time constraint is possible. Overlapping access rights are also allowed. It is possible to have expired access rights automatically removed (and archived) from the cardholder definition screen.

When assigning access to workgroups; any modification to the access rights of a workgroup will immediately affect all cardholders belonging to this workgroup. Cardholders with multiple Workgroups assigned to them will inherit all access rights from all workgroups.

5.2.3.1 Configuring Access Privileges

As an operator, the access privileges you define and assign to a cardholder will determine the points through which they are able to gain entry to the site, and the time-schedules for entry. The SiPass integrated system allows operators to grant **Multiple Access Privileges** to a cardholder.

This means that cardholders can access a site using Multiple Access Privileges, configured by an operator in the following ways:

- Assigning a cardholder’s **Private Access Privileges**

The operator can assign Private Access Privileges for individual cardholder. For further details, refer the section Assigning Cardholder's Private Access Privileges [→ 71].

- Assigning **Work group Access Privileges**

The operator can assign a Work group to a cardholder. The cardholder can then access the site using the access privileges assigned to his/her work group.

If a cardholder has multiple workgroups assigned, he/she will can inherit and use the access privileges of all the workgroups assigned. For further details, refer the section Assigning Cardholder's Workgroup Access Privileges [→ 73].

- Assigning **Venue Booking Access Privileges**

The operator can assign access privileges to venue bookings for cardholder or entire workgroups. For further details refer the section Assigning Cardholder's Venue Booking Access Privileges [→ 80].

- The flexibility of SiPass integrated allows operators to grant cardholders **with a combination of Private, Workgroup and Venue Booking Access Privileges**.

Assigning Cardholder's Private Access Privileges

Ensure that all access types like points, point groups, areas/sub-areas, floors, venue bookings, etc., to which the cardholder will require access have been defined.

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Cardholder** list item.
   ⇨ The *Cardholder* dialog is displayed.
3. On the *Definition* tab, find an existing cardholder, or create a new cardholder for whom access privileges need to be defined. For more information, refer the section Adding Cardholders.
   – **NOTE**: Any existing private access privileges of a cardholder will be displayed in the **Private** tree of the **Access Control** box of this dialog. The steps required to add new access control privileges, or modify existing privileges, are available in the following section.
4. Click the **Access Privileges** button.
5. The *Access Assignment* dialog is displayed. Configure this dialog to assign private access privileges to the cardholder. For more information, refer the section Configuring the Access Assignment dialog [→ 71].

Configuring the Access Assignment dialog

The **Access Assignment** dialog can be used to assign *Private*, as well as *Workgroup* access privileges. Hence, the instructions provided below are applicable to both.

DIALOG DESCRIPTION

This dialog has three tabs:

- **Access Assignment**: You can use this tab to select and configure the Access Type items (points, levels, groups, etc) to be assigned to the cardholder / workgroup, and also specify the Time Schedule for access.
- **Access Group Definition**: You can use this tab to define new Access Groups.
- **Access Level Definition**: You can use this tab to define Access Levels.

1. Click the *Access Assignment* tab.
2. This tab has two main sections: **Configuration** and **Access Control**.
   - The **Configuration** section is where you must first define the access privileges for the cardholder / workgroup. This is then added to the **Access Control** section of this tab.
   - The **Access Control** section will list all the configured access privilege details.
   - **Note** : For cardholder / workgroup with existing access privileges:
   - The **Access Control** box will list the access control item details for cardholder / workgroup that already have access privileges assigned.
3. Select an item from the **Access Type** drop down list.
4. Click on an access object displayed in the adjacent box to highlight it.
5. Select the **Time Schedule** to be configured for the access object.
6. If you want to configure temporary access control privileges for a specific calendar period, continue to the next step.
7. If you want to restrict the access privileges defined for the cardholder / workgroup, to specific calendar period, proceed with the instructions a, b and c below. This means that the cardholder / workgroup will be able to access the site, using the access privileges you define, only during the specified Day/Month/Year period.
   - a. Tick the **Use Start Date and End Date** checkbox.
   - b. In the **Start** field, specify the Date/Month/Year and Time (Hour/Sec.), to define when the cardholder / work groups’ access privileges will begin. You can also click the dropdown arrow of this field, to make a selection.
   - c. In the **End** field, specify the Date/Month/Year and Time (Hour/Sec.), to define when the cardholder / workgroups’ access privileges will end.
   - **Important**: If you define a **Start Time** and **End Time**, which is longer than the time specified in the Time-Schedule, the cardholder will only be able to access the site only during the time specified in the Time Schedule. For example, consider that a Time Schedule configured for a point is 9:00 am – 5:00 pm. Next, the operator configures a cardholder / workgroups’ access privileges for the same point with a Start Date and End Date from 1/12/2015 - 2 am to 4/12/2015 – 10 pm. In such a situation, the cardholder will be able to access the site at the assigned point from the 1/12/2015 – 4/12/2015, but only between 9:00 – 5:00 pm.
8. If you selected **Intrusion Area Point** from the **Access Type** drop-down list, you will need to configure two additional fields on this tab: Control Mode and Arming Rights.

9. If you selected **Intrusion Area Point Group** from the **Access Type** drop down list, you will need to configure only the **Control Mode** field.
10. Click the **Add** button, to add the configured access type item to the **Access Control** box of this dialog. You can also double-click the item, or drag-and-drop it into the box below.
11. You can remove an item from the box by selecting it, and clicking the **Remove** button. Or, double-click to remove it from the box.
12. The **Access Control** box contains the following fields: **Name**, **Time-Schedule**, **Start**, **End**, **Control Mode** and **Arming Rights**. These fields display the configuration details you specified for each access privilege in the previous steps.
13. When complete, click **OK**.
    - ➪ All the access privileges you configured will be transferred to the selected cardholder / workgroup.

For Cardholder’s Private Access Assignment:

The *Cardholder* dialog will be displayed. Expand the **Private** tree item of the **Access Control** box of this dialog to view the configured private access privileges.

For Workgroup Access Assignment:

The *Work Group* dialog will be displayed. The *Access Control* box of this dialog displays the configured access privileges for the selected workgroup. Click **Save**.

Modifying Private Access Privileges

1. Open the *Access Assignment* dialog.
2. Click the access privilege to be modified, in the **Access Control** box of this dialog.
3. Click the **Remove** button, or double-click the item. This will delete the item from the box.

➪ You can now add a new, modified private access privilege to the box.

Assigning Cardholder's Workgroup Access Privileges

Cardholders can be assigned workgroup access privileges for Partition or Non Partition Workgroups.

The sections that follow provide instructions on how to configure such workgroup access control privileges.

Assigning Cardholder's Parition Workgroup Privileges

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Cardholder** list item.
3. Go to **Definition** tab, and create a new record, or open an existing record for a cardholder to be assigned partition workgroup access.
4. Click the **Workgroup** drop down list. This list displays the available partition workgroups.
5. Select a workgroup from the list and click **Save**.

Assigning Cardholder's Non-Partition Workgroup Privileges

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Cardholder** list item.
3. Go to the **Advanced** tab, and create a new record, or open an existing record for a cardholder to be assigned partition workgroup access.
4. In the **Work Groups** section of this tab; click the **Choose** button. The *Cardholder's Work Groups* dialog is displayed.
5. Select a workgroup from the **Available Non-Partition Work Groups** section.
6. Click **Add** and **OK**. This workgroup will be added to the *Advanced* tab of the *Cardholder* dialog.
7. Click **Save**.

The cardholder can now use the Access Control privileges configured to the selected Non-Partition Workgroup. The Access Control section of the *Definition* tab will display the assigned workgroup as part of the cardholder's workgroup access privileges.

Assigning Cardholder's Venue Booking Access Privileges

Operators can assign cardholders to venue bookings which will allow cardholders to inherit the access privileges of the specific venue they are configured to.

For more information, please refer the sections under the topic Assigning Cardholder's Venue Booking Access Privileges [→ 80].

5.2.3.2 Workgroup and Operator Access Privileges

It is possible for an operator to assign access groups to a cardholder, where the operator has actually not been granted privileges for those access groups.

For example, an administrator or high-level operator creates a workgroup called "Security" with access privileges for Access Group A. This workgroup is flagged to automatically grant access privileges to cardholders assigned to the workgroup.

Another operator group is created, that does not have access privileges to any Access Groups, but is granted access privileges to the Security workgroup. An operator belonging to this operator group can assign the workgroup "Security" to a new cardholder, effectively transferring access privileges for Access Group A to the cardholder even though their operator group has not been granted privileges for this Access Group.

This kind of scenario can be avoided by:

- Creating a single operator group for the creation of cardholders or
- Ensuring that all operator groups with "create" permissions for workgroups have been granted privileges to exactly the same access groups.

5.2.4 Offline Access

SiPass integrated allows you to configure cardholders that have access if the reader interface devices stop communicating with the ACC.

5.2.4.1 Defining Offline Access Groups

Offline Access Groups control who has access to which doors when the reader interfaces are offline.

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Offline Access Group** list item.
3. Click **New Offline Access Group**.
4. Enter a name for the group and click **Save**.

Your Offline Access Group is now created. You can assign cardholders to this group from the *Cardholder* dialog and add doors to the group from the Offline Mode configuration in the *FLN Configuration* dialog in the SiPass integrated Configuration Client.

5.2.4.2 Defining Offline Access Privileges

Offline Access Privileges are assigned in a similar way as regular access privileges.

An operator can configure 100 unique card numbers (as configured in SiPass integrated for cardholders) that can be granted access at doors controlled by a RIM device (devices like DRI/SRI/ERIs). When a RIM device is operating in the Offline mode, and a user badges a card, the device will check its internal list of 100 cards to see if the card: (a) Exists in the list of up to 100 cards, (b) Has access to that particular reader device.

If both conditions are met, the device will open the door and store a ‘Valid Card’ event; or if invalid, an ‘Invalid Card’ event.

If the door is opened and closed, it will also store a DoorFrame opened and closed message.

The system will warn the operator when the cardholder limit is reached. But please keep this in mind when assigning cardholders to groups.

The steps that follow detail how operators can configure Offline Access Privileges in the SiPass integrated system.

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Cardholder** list item.
3. Find or create the cardholder record whose access privileges you want to modify.
4. Click on the **Access Assignment** button.
5. Click **Offline Access Groups**.
6. Tick the checkboxes of the Offline Access Group you wish to add and click **Close** to close the dialog.
7. Select each Offline Access Group and click **Add** to view which doors it includes.
8. Click **OK** to return to the *Cardholder* dialog.
9. Click **Save**.

5.2.5 Venue Management

SiPass integrated's VENUE MANAGEMENT feature is a highly flexible and versatile tool that allows you create and manage venues in your site.

You can create access controlled venues on your site, which can be booked for the purpose of meetings, conferences, trainings, etc. Operators can configure organizers, participants, the time schedule of the venue bookings, and also control access privileges to cardholders for the venue.

This feature also lets you view various bookings across multiple venues and time periods which can help organizers plan and book venues efficiently.

In functionality, venue bookings allow you to create access privileges, for a special set of access privileges for a cardholders or workgroups, over a temporary period, after which the temporary privileges can be removed, if required.

Dialog Description

⟐ Click *Operation* > *Venue Management* from the main menu.

⇨ This displays the *Venue Booking Management* dialog.

Tabs: There are two tabs on this dialog:

- **Venue**: This tab is used to define a venue, and its access control configuration.
- **Venue Booking**: This tab is used to book a venue, and view/edit/delete existing bookings.

Left Panel: There are three expandable boxes in this panel:

- **Venues**: All venues configured in the system are listed here.
- **Calendar**: A monthly calendar, with the current day highlighted, is displayed here.
- **Views**: You can use this box to customize views of venue schedules and bookings for single or multiple venues side-by-side.

5.2.5.1 Creating a New Venue

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Venue Management** list item.

   ⇨ The *Venue Booking Management* dialog is displayed.
3. Click the **New Venue** button to define a new venue for your site.
4. Click the *Venue* tab.
5. Enter a name for the venue in the **Name** field.
6. Enter a description of the venue in the **Description** field.
7. Click **Save**.
8. The **Venues** tree panel on the left of this dialog displays all venues avail-able in the system.

Searching for existing venues:

1. Click the **…** button on this dialog.
2. Select a venue from the *Venue Search* dialog that appears.

The filtered text box at the top of this dialog can be used for filtering the venue bookings.

5.2.5.2 Configuring Access Control for Venue

You can control access to each venue by configuring its Access Assignment. This allows you to define and control all the points of entry and exit to the venue.

1. Open the *Venue Booking Management* dialog.
2. Create a new venue, or open an existing venue by clicking the **...** button. You can also select the desired venue from the venue tree view on the left panel of this dialog.
3. Select the **Define Access Privileges** button.
   ⇨ The *Access Assignment* dialog is displayed.
4. You can now configure and assign access privileges to this venue on this dialog. For further details, refer the section Configuring the Access Assignment dialog [→ 71].
5. The access privileges you define will be displayed in the **Access** box of this dialog.
6. Click **Save**.

5.2.5.3 Venue Booking

Venue Booking is a simple configuration that allows you to book a specific venue, configure Organizer/s, Participants, the start & end Date and Time of the booking, and also grant access control privileges to cardholders to access the venue.

Booking a Venue

▷ Ensure that the Venue to be booked is configured in the system.

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Venue Management** list item.
   ⇨ The *Venue Booking Management* dialog is displayed.
3. Select the venue in the **Venues** tree panel on the left.
4. Next, click the *Venue Booking* tab.
5. The Calendar is displayed on this tab. Select from the **Day**, **Work Week**, **Week** or **Month** buttons to view the Calendar accordingly.
   – **Day**: Displays 24 hours of the present day
   – **Work Week**: Displays all 24 hours from Monday – Friday of the present work week
   – **Week**: Displays all 7 days of the current work week by default. To display a different week, select it from the Calendar box on the adjacent left panel.
   – **Month**: Displays all the days of the month. Use the scroll bar to view days of the previous or following month/s.

Opening the Venue Booking Definition dialog

Option 1:

- You can highlight **Hours/Days/Weeks** on this calendar, and then right-click to display the **New Venue Booking** menu option. Select this option to display the *Venue Booking Definition* dialog.

Option 2:

- Click the **New Venue Booking** button on the *Venue Booking* tab. The *Venue Booking Definition* dialog is displayed.

Configuring the Venue Booking Definition dialog

1. Click the *Venue Booking* tab.
2. Enter a **Name** for the booking. If this booking authentication is required, tick the **Require Authentication** checkbox.
   - **Note**: The **Require Authentication** checkbox is related to the ‘organizers’ configured for this venue booking.

To allow an organizer/s to edit a booking:

1. Tick **the Require Authentication** checkbox
2. Add the cardholder as an organizer for the venue booking.
3. Ensure that this organizer has a Username and Password (configured in the Personal tab of the Cardholder dialog). If checkbox is ticked, and the organizer/s does not have a username and password configured, the booking can still be saved. But, the organizer/s can-not edit the booking until they are given a username and password.
   - ⇨ **Only a user logged into the system as an administrator can edit the booking without requiring a username and password.**
4. In the field below, enter a **Description** of the booking.
5. Select the Start Date and Start Time of the booking in the **Start Date** field.
6. Select the End Date and End Time of the booking in the **End Date** field.
7. Select the venue in the **Venue** field. By default, the venue selected on the *Venue Booking Management* dialog will populate this field. Click the **…** button to search and select another venue.
8. Click **Save**.

Adding / Removing Organizers:

1. In the **Organizers** section, click the **Add** button.
2. The *Search Cardholder* dialog will be displayed. Double-click on a cardholder to configure them as an organizer. You can select and configure multiple organizers for the same venue booking.
3. To delete this organizer/s, select the card-holder and click the **Remove** button.
   - For instructions on how to configure Venue Booking access privileges to individual cardholders, refer the section Assigning Venue Booking Privileges to Cardholders [→ 80].
   - For instructions on how to configure Venue Booking access privileges to workgroups, refer the section Assigning Venue Booking Privileges to Workgroups [→ 81].

Configuring a Recurrent Venue Booking

1. Open the *Venue Booking Definition* dialog.
2. Click the *Recurrence* tab.
3. Select from the following options available on this tab:

Recurrence pattern	Details	Range of recurrence
One Off	Select this option to configure this booking as a one-off booking that will not recur.	
Daily	• Select **Every__day(s)** to repeat this booking for a selected number of days. Enter the number of days for recurrence in this field. • Select **Every weekday** to configure this booking to recur every weekday	• Select **End after: ___ occurrences** to end the recurrence of the booking after a number of occurrences. Specify a number of occurrences in this field. • Select **End by** and select a date, to end the recurrence of the booking by the selected date
Weekly	• Select **Recur every __ week(s) on**:, and specify the number of weeks you want the booking to recur.	
Monthly	• Select **Day __ of every __ month(s)** to configure recurrence of the booking on a monthly basis. For example, for the fifth day of every month. • The __ __ **of every __ month(s)** to configure it for a specific recurrence. For example, for every third Thursday of every month.	

◈ Click **Save**.

Listing Current Bookings

- ◈ Click the Current Bookings button on the Venue Booking tab.
  - ➪ The bookings for all venues will be listed by Name, Start Date, End Date and Venue.

Search and Filter this list:

- ◈ You can search and filter this list by typing your search term in the filter box below each column.

Editing venue booking items on this list:

1. Each venue booking item can also be edited or deleted by double-clicking on the item, which will bring up the *Venue Booking Definition* dialog.
2. Or, by right-clicking on the item, and choosing **Edit Venue Booking** or the **Delete Venue Booking**.
3. **Note**: If the item chosen is configured as a recurring venue booking, a dialog will be displayed with the following options:
   - **Open this occurrence**: This option allows you to edit only Venue Booking for the specific date/time
   - **Open this series**: This option allows you to edit the venue booking to affect all the venue bookings in its recurrence series.

Single-Screen Display of Single/Multiple Venue Bookings

1. Click the **New Calendar View** button of the **Views** box in the left panel.
2. The *Calendar View* dialog is displayed.
3. Enter a name for the new view you want to create.
4. Select the venues whose bookings you want to view.
5. If you select multiple venues, their booking schedules will be displayed side-by-side.
6. Click *Save* and *Close*.

➪ The saved view will be displayed in the Views box. Select a view to display it in the Venue Booking tab.

Assigning Cardholder's Venue Booking Access Privileges

Operators can assign cardholders to venue bookings which will allow cardholders to inherit the access privileges of the specific venue they are configured to.

This can be done by in the following ways:

- **Assigning Venue Booking access privileges to Individual Cardholders to Venue Bookings** (as Organisers or Participants)
- **Assigning Venue Booking access privileges to Workgroups**

The sections that follow provide detailed instructions on the two options listed above.

Assigning Venue Booking Privileges to Cardholders

▷ Ensure that the Venue to be booked is configured in the system.

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Venue Management** list item.
   ⇨ The *Venue Booking Management* dialog.
3. Select the venue in the **Venues** tree panel on the left.
4. Next, click the *Venue Bookings* tab.
5. Double-click on an existing venue booking on this tab to open it. The *Venue Booking Definitio*n dialog is displayed.
6. In the **Participants** section, select the *Cardholder* tab and click the **Add** button.
   ⇨ The *Search Cardholder* dialog appears.
7. Select a cardholder on this dialog, and click the **Add** button to add individual cardholders.
8. To remove a participant, select the cardholder, and click the **Remove** button.
9. Click **Save**.

⇨ The cardholder will inherit the access privileges of the venue selected for this venue booking.

Assigning Venue Booking Privileges to Workgroups

▷ Ensure that the Venue to be booked is configured in the system.

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Venue Management** list item.
3. The *Venue Booking Management* dialog.
4. Select the venue in the **Venues** tree panel on the left.
5. Next, click the *Venue Bookings* tab.
6. Double-click on an existing venue booking on this tab to open it. The *Venue Booking Definitio*n dialog is displayed.
7. In the **Participants** section, select the *Work Group* tab and click the **Add** button.
   ⇨ The *Select Work Group …* dialog appears.
8. Select a work group on this dialog, and click the **OK** button to add individual workgroups.
9. To remove a work group, select it, and click the **Remove** button.
10. Click **Save**.

⇨ All the cardholders in the selected workgroups will inherit the access privileges of the venue selected for this venue booking.

Assigning Exclusive Access Control Privileges to Cardholders

A special set of access privileges can be specified for cardholders, that override their standard assigned access over a temporary period of time, after which these exclusive privileges are removed.

For this, a venue is defined as "Exclusive" and the assigned cardholders have access ONLY to the venue doors during the booking time period. All other access is disabled until again outside the booking time.

- Multiple venues can be configured as exclusive.
- A cardholder assigned to multiple exclusive venues (with overlapping time periods) will have access to all the venues (from start time of the earliest booking for a venue till end time of the last booking for a venue).

Note: Exclusive access permissions can change or reduce a cardholder's access depending on how these permissions are defined.

▷ Ensure that the Venue to be booked is configured in the system.

1. On the *Venue Booking Management* dialog, select the venue for which exclusive privileges will be specified.
2. Click the **Override Standard Access Rights** checkbox to define the venue as exclusive.
3. Click **Save**.

All cardholders assigned to the venue will now have exclusive access till the time the venue booking is valid.

Actions triggered by Venue Booking Time

The Advanced Security Programming (ASP) functionality in SiPass integrated includes venue booking as event trigger. After setting up a venue, you can configure an ASP activity to trigger an action, before or after every booking start or stop. This helps in creating different actions for the same venue based on the time the booking is made for that venue.

For example, an action can be configured to turn on the air conditioning ten minutes before the booking start time, or turn on the lighting 5 minutes before the booking start time, turn off the lighting and air conditioning two minutes after the booking stop time.

Note: In case of bookings with overlapping start and end times, care must be taken that an action for the start of next booking is not cancelled by the end time of the previous booking. For example, if the lights-on action is set to 11:00 am for Booking 2 but the lights-off action from Booking 1 is set to 11:02 am, the overlap in start and end trigger times of the two bookings will turn off the lights for booking 2.

More details of the event trigger properties can be found in the *SiPass integrated Reference Manual*.

5.2.6 Destination Control

If your SiPass integrated license includes the Destination Control function, you additionally get a high-quality access system with modern thyssenkupp elevators to enable smart and intelligent interfaces via keycard technology.

The features in this fully integrated security solution are tailored for the best in access, security and convenience:

- Customized access privileges
- Special effects during elevator travel
- Favorite floor selection
- Prioritized elevator call and landing
- Automated elevator provisioning
- Customisable time for elevator access
- Latest Access System Technology powered by SIEMENS

5.2.6.1 Defining Acces and Privileges

Assigning Caretaker/Technician Role

The Cardholder dialog includes the *High Level Elevator* tab used for assigning Caretaker or Technician role to the cardholder. Note that a cardholder can have only one of the roles out of 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 you choose the role assigned to the cardholder for the High Level Elevator. The available options are:

- **None**: Standard cardholder
- **Caretaker**: Nominates the cardholder as a Caretaker and allows access to designated floors. When the card is presented, the Caretaker can select multiple floors by badging the card only once (within the allowed time period). **Note**: A visitor cannot be assigned the Caretaker role. The option is not available while setting up the Elevator Role for a visitor in the Visitor dialog.
- **Technician**: Nominates the cardholder as a Technician and allows access to designated floors. When the card is presented, the system checks the commissioning of the elevator system. In case of a Landing Operating Panel (LOP) and Car Operating Panel (COP), the indicator light flashes yellow while the verification is in progress, and turns green if the setup is working fine. In case of a DSCT, the technician is required to confirm by pressing a button on the panel. In case of a fault, red indicator is flashed.

Assigning Special Effects

The *High Level Elevator* tab also helps you define any special effects like customized lighting and/or communication language in the elevator during the time the cardholder travels.

- The **Language** dropdown list allows you to choose the language for communication with the cardholder in the elevator. You can select any other language in the list for communicating with the cardholder in the selected role. Not selecting any option in the list keeps the language as English by default.
- The **Lighting** dropdown list allows you to choose the lighting effect in the elevator for the cardholder. You can select any special lighting effect in the list to be applied during the travel of this particular cardholder. Not selecting any option in the list keeps the default lighting.
  The information about the language and special effects is listed in the *Cardholder All Fields* report

High Level Elevator Lookup Data

The High Level Elevator Lookup Table is used to:

- Add new language support in Language lookup table
- Add new lighting effect support in Lighting lookup table

Adding a Custom Value in High Level Elevator Lookup Table

The High Level Lookup Data can be modified as follows:

1. Select **Look Up Table** by expanding the *Imported Data* List in the left side pane.
   ⇨ The main window opens up displaying a tree structure in the left pane.
2. Select **High Level Elevator** from the tree (click the + icon to expand the tree).

Adding a New value for the Language Lookup Data

1. Click **Language** in the High level Elevator sub-tree.
   ⇨ The *Language* dialog is displayed in the right pane of the window displaying the existing options for the Language lookup data.
2. Click an empty cell (preferably the **ID** field first) and enter an ID number for the new language.
3. Enter the name of the language in the **Name** field (this is displayed in the **Language** dropdown list on the *High Level Elevator* tab in SiPass Integrated).
4. Enter a short name of the language in the **Value** field (this is the value linked for the language in the database).
5. Click **Save**.
6. Click **Close**.
   ⇨ The new language is added to the High Level Elevator Lookup Data and is available in the **Language** dropdown list on the High Level Elevator tab of the Cardholder and Visitor dialogs in SiPass Integrated.

Adding a New Effect for the Lighting Lookup Data

1. Click **Lighting** in the High level Elevator sub-tree.
   - ⇨ The *Lighting* dialog is displayed in the right pane of the window displaying the existing options for the Lighting lookup data.
2. Click an empty cell (preferebly the **ID** field first) and enter an ID number for the new lighting effect.
3. Enter an appropriate name for the effect in the **Name** field (this is displayed in the **Lighting** dropdown list on the *High Level Elevator* tab in SiPass Integrated).
4. Enter a short name for the effect in the **Value** field (this is the value linked for the lighting effect in the database).
5. Click **Save**.
6. Click **Close**.
   - ⇨ The new lighting effect is added to the High Level Elevator Lookup Data and is available in the **Lighting** dropdown list on the *High Level Elevator* tab of the *Cardholder* and *Visitor* dialogs in SiPass Integrated.

The ACC must be initialized after adding any new lookup value to ensure that the lookup table is always synchronized with the ACC.

Assigning VIP Privileges

You can assign VIP privileges for the thyssenkrupp elevator banks by assigning the VIP floor to the cardholder and visitor.

Note: The VIP privileges do not apply to workgroup and venue access.

Before moving ahead, ensure that all access types like points, point groups, areas/sub-areas, floors, venue bookings, etc., to which the cardholder will require access have been defined.

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the *Cardholder* list item.
   - ⇨ The *Cardholder* dialog is displayed.
3. On the *Definition* tab, find an existing cardholder, or create a new cardholder for whom VIP privileges need to be defined.
4. Click the **Access Privileges** button in the *Access Control* section.
   - ⇨ The *Access Assignment* dialog is displayed.
5. Select **Floor Points** from the **Access Type** drop down list.
   - ⇨ This lists the thyssenkrupp elevator banks having VIP privileges (along with the floors and sides) in the grid on the right side of the dialog. You can identify a VIP-enabled bank with the bank name having the suffix - VIP. The floors for other banks are also listed in the grid.
6. If you wish to assign the cardholder access to a new floor (not assigned earlier) at this step, select the floor name and side from the grid and click **Add**. The selected floor is added to the list of floors to which the cardholder has access and is displayed in the Access Control section on the dialog.
   - ⇨ **Note:** If you do not wish to add any additional floors for the cardholder, skip this step.
7. When the cardholder has all the necessary floors listed in the *Access Control* section, select the bank having VIP privileges and click **Add**.
   - ⇨ The bank that the cardholder has VIP privileges for is now listed in the *Access Control* section for the cardholder. The VIP privileges apply to the cardholder only for the assigned floors of that elevator bank.
8. Click **OK** to close the Access Assignment dialog.
9. Click **Save** on the Cardholder dialog.

Assigning Favorite Floors for a Cardholder, Workgroup or Venue

You can set the favorite floor when assigning floors to Cardholder, Visitor, Workgroup or Venue.

Favorite Floors and Time Schedules

- If the same floor is assigned multiple times with different time schedules to the same cardholder/venue/workgroup, the ACC matches against all configured time schedules for that point to grant access.
- If a floor is set as favorite during Time Schedule 'A' and as a regular floor (not favorite) during Time Schedule 'B', it is only considered a favorite floor during Time Schedule 'A' even when the access is valid during Time Schedule 'B'.

Note: The following steps describe the process of assigning favorite floors to a cardholder. To assign favorite floors to a workgroup or venue, follow the steps below by adding access privileges through the Work Group dialog or Venue Management dialog.

Before moving ahead, ensure that all access types like banks, floors, venue bookings, etc., to which the cardholder will require access have been defined.

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Cardholder** list item.
   ⇨ The *Cardholder* dialog is displayed.
3. On the *Definition* tab, find an existing cardholder, or create a new cardholder for whom favorite floors need to be defined.
4. Click the **Access Privileges** button in the *Access Control* section.
   ⇨ The *Access Assignment* dialog is displayed.
5. Select **Floor Points** from the **Access Type** drop down list.
   ⇨ This lists the floors for all the elevator banks in the system in the grid on right side of the dialog.
   Note: The **Favorite Floor** checkbox is enabled only for the floors belonging to thyssenkrupp elevator banks.
6. To assign the cardholder access to a favorite floor, select the floor from the grid.
7. Tick the **Favorite Floor** checkbox and click **Add**.
   ⇨ The selected floor is added to the list of floors to which the cardholder has access and is displayed in the *Access Control* section. The *Favorite Floor* column in the section (read only) displays a check mark, indicating it is a favorite floor.
   Note: If you select multiple floors and the selection includes floors not belonging to a thyssenkrupp elevator bank, the **Favorite Floor** checkbox is disabled.
8. Click **OK** to close the *Access Assignment* dialog.
9. Click **Save** on the *Cardholder* dialog.
   ⇨ The audit trail in the main window will display the access privilege (favorite floor) that has been added.

Defining Favorite Floors in Access Levels

You can set one or more floors or floor side as favorite while defining Access Levels. The favorite option cannot be set for floors not belonging to a thyssenkrupp elevator bank, or for floor groups.

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Access Level** list item.
   - ⇨ The *Access Levels* dialog is displayed listing avalable access levels on the left.
3. Type a suitable name for the new access level in the **Access Level Name** field.
4. Select an appropriate time schedule for the access level from the **Time Schedule** dropdown list.
5. In the *Configuration* section, select **Floor Points** from the **Type** dropdown list.
   - ⇨ The available floors are listed in the list box below.
6. Select one or more floors to be added as favorite.
7. Tick the **Favorite Floor** checkbox and click **Add**.
   - ⇨ The selected floor is added to the Access Level and is displayed in the list box on the right side of the *Access Level Definition* dialog. The suffix - (Favorite) indicates it is a favorite floor.
8. Click **Save**.
9. Click **Close** to close the *Access Level Definition* dialog.

5.2.7 Privacy Mode for Aperio Basic Lock

With SiPass integrated MP2.76 SP2 onward, the *Privacy Mode* function is available that allows the Aperio door lock to be secured from the inside, making it impossible to enter the room from the outside, even with a valid pass.

Activating Privacy Mode

The Privacy Mode is activated by:

- Pressing the *Activator* push button on the Aperio Lock from the inside
- Locking the Dead Bolt on the Aperio Lock

When this mode is activated, SiPass integrated blocks the door access from the outside. The card access at the Reader Point and manual override commands to Lock/Unlock the Aperio Lock are disabled.

Deactivating Privacy Mode

It can be deactivated by any of the actions listed below:

- Releasing the *Activator* button on the Aperio Lock
- Unlocking the Dead Bolt from the inside
- Opening the interior Door Handle of the Aperio Lock
- Through SiPass integrated Operation Client
- A special pass (Supervisor Pass) in SiPass integrated Operation Client - *Cardholder* dialog > **Supervisor** checkbox

When any of the above actions takes place, the SiPass integrated clears the Door Blocked state, and the Reader Point and Latch Output are enabled.

Supervisor Override for Privacy Mode

When a cardholder configured as a *Supervisor* (the **Supervisor** checkbox on the *Cardholder* dialog is checked), badges his card at an Aperio Lock in Privacy Mode, the Privacy Mode and Door Blocked state are bypassed (disabled) and the access is allowed.

The Interior Door Handle, which is mapped to the REX input, is always freely accessible.

Due to this, when the Aperio Lock is in the Door Blocked state, the REX input will remain enabled.

Resetting the Privacy Mode after Supervisor Bypass

To set the Privacy Mode after the lock has been opened by the Supervisor:

- Press the *Activator p*ush button on the inside of the Aperio Lock to bring it back in the normal (unlocked) state or unlock the deadbolt
- Press the push button again or Lock the deadbolt again from the inside of the door

5.3 Anti-Passback

The SiPass integrated Anti-Passback functionality allows you to define a set of locations (called „Areas“) that cardholders must enter and exit in a specific sequence. This lets you force entry and exit travel through a site, and monitor exactly the number of cardholders entering a particular location.

The Anti-Passback features in SiPass integrated are flexible enough to suit the environment of any site. The following Anti-Passback alarms can be generated:

- Soft Anti-Passback
- Hard Anti-Passback
- Fail-soft Anti-Passback
- Area Count violations

Soft Anti-Passback

In this mode, cardholders must use their access card to gain entry to and exit from a defined locality. If a valid cardholder has presented their access card to enter a locality and not presented the card when exiting they are in breach of the Anti-Passback rules. The next time the cardholder attempts to enter that same locality a Soft Anti-Passback alarm will be raised. However, the cardholder **will** still be permitted entry into the area.

Hard Anti-Passback

In this mode, cardholders must use their access card to gain entry into and exit from a defined area. If a valid cardholder has presented their access card to enter an area and not presented the card when exiting they are in breach of the Anti-Passback rules. The next time the cardholder attempts to enter that same area a hard Anti-Passback alarm will be raised and that cardholder will not be permitted entry into the area.

Fail-Soft Anti-Passback

Depending on the size of the area governed by Anti-Passback rules, multiple ACCs may be required to share Anti-Passback data.

Fail-soft Anti-Passback mode dictates that if the connection between ACCs in an Anti-Passback Area is broken, then SiPass integrated will default to Soft Anti-Passback mode for that area. That is, access outside of the Anti-Passback rules will be permitted, but the violation will be recorded in the Audit Trail.

Area Count Violations

By applying a limit to the number of cardholders who may enter a specified area, you can:

- Raise an alarm when the area count has been reached.
- Raise an additional alarm when the area count has been exceeded.
- Trigger event tasks such as preventing further cardholders from entering a area that has reached its limit, or turning on an “Area Full” sign.

Timed Re-entry

Timed Re-entry is a feature of Anti-Passback that allows you to limit re-use of a card at certain readers or reader groups within a specified amount of time.

An attempt to re-enter an Area in “Timed Re-entry” mode within the duration will result in access being denied and a “Timed Re-entry Restricted” violation message reported to the Audit Trail.

Internal Readers Anti-Passback

This form of Anti-Passback enforces the use of entry and exit readers, before cardholders can access any other internal readers within that area. Cardholders must badge their card at an Entry Reader (log in to the area) before they can access any internal readers within that area. Soft or hard anti-Passback modes can be set to any of the internal readers within the area. When assigning access points to an area, any internal reader can be assigned as an access point to that area.

Delayed Reporting

Under normal access operation modes, a valid card badge is equivalent to a valid door entry in SiPass integrated. That is, if a valid card has been badged, to SiPass integrated this means that the cardholder has physically passed through the door.

However, it is possible for a cardholder to badge their card, but not actually proceed through the door. If this occurred at an Area configured for Anti-Passback, this would mean the Area Count would be incorrectly incremented or decremented, and the cardholder incorrectly located by the system.

To counteract this, access points used to enter defined Anti-Passback Areas should be assigned to the Operation Modes “Card Only Delayed Reporting” or “Card and PIN Delayed Reporting”. Access points assigned one of these modes will only recognize a valid access attempt if the associated door monitor registers that the door has opened after a valid badge.

Other Anti-Passback Features

Besides the standard access features provided by the Anti-Passback function, a number of other attributes can also be easily configured. These include:

Audit Trail Entries – All area transactions are immediately logged to the SiPass integrated audit trail. An additional area specific column can also be added to your audit trail view using the Operator Preferences feature of SiPass integrated.

Reports – You can generate reports regarding the localities at your site. More specifically you can generate reports on cardholders that are currently inside a specified area.

Distribution of Anti-Passback data across ACCs

It is recommended that, where possible, card readers set up to control access to an Anti-Passback system are not connected to different ACCs.

This will depend on how your site is structured; for reasons of complexity or physical size, it may not be feasible for all readers controlling access to an area or areas to be connected to a single ACC. While the performance of Anti-Passback controllers should not be affected, in these instances you should be aware of the behavior of the Global Anti Passback (GAP) system in case of communications failure.

ACCs communicate to each other the movements of cardholders across shared Anti-Passback areas. This process is completely transparent to the operator. However, if the connection between ACCs is disabled for some reason, cardholder movement data may not be sent. This means that ACCs may hold incorrect information about the whereabouts of a particular cardholder.

In this instance, Areas set to Hard Anti-Passback mode will default to that mode. This stops cardholders from entering and exiting areas until all communications are restored. Areas set to Fail-soft Anti-Passback mode will default to Soft Anti-Passback.

The above applies only to communications losses between ACCs that share Areas. If comms loss occurs between two ACCs with no Anti-Passback areas in common, operation will continue as normal.

5.3.1 Creating an Anti-Passback Cluster

SiPass integrated allows you to create clusters of ACCs in which Anti-Passback can operate. Once setup, a cluster of ACCs communicate among themselves to ensure that Anti-Passback operates across ACCs even when communications with the server are lost.

▷ Ensure that you have configured all ACCs that will form a cluster and have pre-planned your Anti-Passback areas so that you know which ACCs to include in the cluster.

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Anti Passback Area** list item.
3. Select the **New Cluster** button.
4. Enter a descriptive name for the Area into the **Cluster Name** field.
5. Click on an ACC from the Available Units List to highlight it and then select **Add** to add the ACC to the **Selected Units** list. Repeat this step until all ACCs to from the cluster have been selected.
6. Click **Save**.

⇨ This newly created cluster will appear in the tree view on the left hand side of the dialog.

5.3.2 Creating an Anti-Passback area

Anti-Passback revolves around the concept of an **Area**. An **Area** in SiPass integrated is defined as a space with at lease one entry and one exit point. An area can consist of two or more sub-areas.

A **Sub-Area** is simply an area that is located within another area. The sub-areas must operate in the same Anti-Passback mode as the area to which they belong.

Creating an area involves assigning the IN and OUT readers which are used to enter and exit the area, the Anti-Passback mode, and also giving the area a Count if required. The count of an area includes all cardholders currently located in an area, including all sub-areas of that area. This means that if a cardholder exits an area and enters a sub-area of that area, the count of the original area will remain the same, and the count of the sub-area will increase by one.

If a cardholder exits the sub-area and re-enters the area, the original area's count will still remain the same, and the sub-area's count will decrease by one.

i If Area details are changed, deleted or updated, the ACCs that handle Anti-Passback access to those areas must be re-initialized for the changes to take effect.

To create an Anti-Passback area

▷ Ensure that you have configured in SiPass integrated the Dual Reader Interface (DRI) or SRI devices used to access and exit the area(s).

▷ Ensure that you have configured your ACC cluster(s)

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Anti Passback Area** list item.

3. Select the **New Area** button.

   ⇨ The area definition screens will now appear showing the *Definition* Tab.

4. Complete the *Definition* tab details.
5. Select the *Member* tab.
6. Select “IN Reader” from the **Type** drop-down box.

   ⇨ The list of readers you have defined at the facility will be displayed in the **Available** List. Once the list is displayed, select the reader(s) and choose **Add** to move them to the **Selected** List.

7. Select “OUT Reader” from the **Type** drop-down box

   ⇨ The readers you have configured at the facility will appear in the **Available** List, minus those readers that have already been assigned as IN Readers for this area.

8. Select the readers from the **Available** List which permit exit from this area, and choose **Add** to move them to the **Selected** List.

   – If you selected “Timed Re-entry” as the Anti-Passback mode in step 3, it is not compulsory to choose any OUT readers for this area.

9. Select “Internal Reader” from the **Type** drop-down box.

   ⇨ The list of readers you have defined at the facility will be displayed in the **Available** List.

10. Once the list is displayed, select the reader(s) which will be the internal readers in the area, and choose **Add** to move them to the **Selected** List.

    – An internal reader is not an ‘IN’ or ‘OUT’ reader, it is only an internal reader for the area.

ℹ The "Aperio Wireless Access Point“ cannot be selected as In / Out / Internal reader for the Anti-passback function.

1. If you wish to set cardholder limits for each workgroup for your Anti-Passback area, select the *Workgroup* tab.
2. Highlight the workgroup to be added from the available list and click the **Add** button.

   ⇨ The workgroup will now be added to the selected list.

3. Configure the workgroup by setting the limit and enforce attributes.

   – **Capacity**: Sets the maximum number of cardholders that belong to that workgroup which can enter the Anti-Passback area.
   – **Enforce Capacity**: This checkbox forces the maximum count for that workgroup by denying entry to additional cardholders that belong to the workgroup when the capacity is reached, even if the overall Anti-Passback area has not reached its capacity.

4. Click **Save**.

ℹ Cardholders that belong to workgroups not specifically assigned a limit to the Anti-Passback area share the remainder of the overall limit.

5.3.2.1 Area Definition Configuration Fields

The fields used to configure the main definition of the Area tab are provided in the table that follows:

Field	Description
Area Name	Enter the name of the Anti-Passback area. This name will be displayed in system messages (e.g.: Audit Trail)
Mode	Select the mode of operation for the Anti-Passback area as described earlier.
Alarm Class	Select the alarm class that will apply to this Anti-Passback area from the Alarm Class drop down box.
Area Number	A read only field that indicates the ID for the Anti-Passback area.
Current Status	Displays the current status for the Anti-Passback area. To refresh the information select Load.
Mustering Anti-Passback Area	Tick this checkbox if the Anti-Passback area is a mustering area and will be used for reporting cardholders logged into the area during an emergency. This area will be included when a “Mustering Report” is generated.
Maximum Cardholders	Enter the maximum number of cardholders permitted to be logged into the area at any one time.
Enforce Maximum Cardholders	Tick this checkbox to enforce the maximum limit on the Anti-Passback area. This means that no further cardholders will be permitted to enter the area until another cardholder has first exited.
Enable Four Eyes Access	Tick this checkbox to enable four eyes access control for the Anti-Passback area. This allows you to set a time period for badging between the first and second badge of the two cardholders which are required in the specified area at any one time.
Four Eyes Timer	Enter the time in seconds, that will delay alarm generation after a first cardholder enters the Anti-Passback area, and before the second cardholder also enters. This entry can range from 1 second to 32767 seconds.
Include Cardholders in Anti-Passback sub-areas	Tick this checkbox if cardholders already logged in to sub-areas are also included in the four eyes count.
Trigger Alarm if no Cardholder	Tick this checkbox to generate an alarm when the Anti-Passback area becomes empty.
Re-entry Timeout	Only enabled when the mode selected is Timed Re-entry. Enter the time in minutes before a cardholder can re-use their access card at the re-entry doors. Please note that if an exit reader is configured in the Timed Re-entry configuration, cardholders badging to exit are automatically allowed to re-enter at any time.

5.3.3 Assigning a sub-area to an Anti-Passback area

You must define the IN and OUT readers for both sub-areas and the areas to which they belong. This means that some readers will be assigned twice.

▷ Ensure that you have configured all of the sub-areas to be assigned.

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Anti Passback Area** list item.
3. Select the Area from the *Name* dialog, or create a new area.
4. Select the *Member* tab.
5. Select **Sub area** from the **Type** drop-down box. The **Available** List will be populated with all defined areas, that have been assigned the same Anti-Passback mode as the current Area.
6. Select the Sub-area(s) you want to assign to this Area, and choose **Add** to move them to the selected list.
7. Click **Save**.

5.3.4 Viewing Cardholders in an Area

SiPass integrated allows you to view a detailed list of cardholder located in an area, in real-time.

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Anti Passback Area** list item.
3. Select from the **Area Name** drop-down box the area you want to view.
4. Select the *Area Data* tab.
5. Choose the **Load Cardholders** button to refresh the list with details of cardholders currently in that Area. The table at the end of this section explains each column in the list.
6. To refresh other properties within this dialog use the buttons provided:
   - **Load Current Count**:
     Updates the Current Count field.
   - **Reset Current Count**:
     Resets the Current Count field to zero and removes all cardholders from the area.
   - **Forgive All**:
     Forgives cardholders in all areas. Cardholders may enter/ exit any Anti-Passback area once only without violating Anti-Passback rules.

Forgiving a cardholder only operates for a single card badge. Once the cardholder has entered/exited an area after a forgive command has been granted, normal Anti-Passback rules immediately apply.

Column	Description
Card No.	The card number of the card holder
First Name	Cardholder’s first name
Last Name	Cardholder’s last name
Date	Date when the cardholder entered the area or sub-area
Time	Time when the cardholder entered the area or sub-area

5.3.5 Forgiving Anti-Passback Violations

To **Forgive** a cardholder is to allow them to enter or exit an area, where normally this would produce an Anti-Passback violation. The Forgive feature permits access for the first use of a card, whether at an Entry or an Exit Reader. Upon power-up, all cards will be in ‘forgive mode’ when the Anti-Passback mode has been applied.

In addition, single cardholders can be forgiven an Anti-Passback violation from the Audit Trail, manual command or Event Task, and all cardholders in an area can be forgiven simultaneously. Forgiving a cardholder only operates for a single card badge. Once the cardholder has entered or exited an area after a forgive command has been granted, normal Anti-Passback rules immediately apply.

Sending a manual Forgive command

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Manual Override** list item.
3. Choose the **APB Area** button.
4. Select **Forgive All Cards** to forgive every active card defined in SiPass integrated.
5. Alternatively, select **Forgive Card** to issue a forgive command to a single cardholder. The **Card Number** field will appear.
6. Choose **Send**.

If you are issuing a forgive command to a primary card number (that is, not a Tenant or 2nd Card Number), enter the card number into the Card Number field. If you are issuing a forgive command to a tenant or 2nd card number, the card number must be entered in the following format:

<number>,<facility>,<technology>

Where **number** = card number, **facility** = facility code, **technology** = card technology code.

For example: 0034,15,10

5.4 Purging the Cardholder Information

With SiPass integrated MP2.80 onward, cardholder data privacy has been strengthened to comply with **General Data Protection Regulation (GDPR)**, giving you the option to maintain data privacy and / or clear the cardholder information from SiPass integrated database and Audit Trail History.

The **Purge Cardholder Details** option allows you to search and delete a Cardholder and the Audit Trail data related to that specific cardholder from the database, if required. The Web Client will also clean the activity audit trail archive for the cardholder for whom, the details have been purged as above.

Note: For every data purge activity, ensure that all the services and message broker(RabbitMQ) are running, so that all the entries related to the Cardholder information are removed completely.

> You can also choose to implement data privacy for an Access Point so that the card event is not sent to SiPass server (which means no Audit Trail log). This can be done through the **Disable Card Event** checkbox from the *Reader* tab while setting up devices and access points in SiPass integrated Configuration Client. See the *Configuration Client User Guide* for more information.

5.4.1 Steps

1. From the left-hand side navigation pane, double-click **Purge Cardholder Details**.

   ⇨ The *Purge Cardholder Details* dialog is displayed.

2. In the *Search Fields* section of the dialog, click the **Cardholder** radio button (if not already selected) and enter the applicable parameters to search for the Cardholder for whom, you wish to purge (clear) the details.

   – Select a value for the **Field**:

   – First Name

   – Last Name

   – Card Number

   – Employee Number

   – Location

   – Message

   – Work group Name

◈ Select a value for the **Comparison Operator**:

   – Begins With

   – Contains

   – Equal To

- ◈ Type a **Value** specific to the Cardholder. For example, type the first name of the Cardholder if you selected *First Name* in the **Field** dropdown list above.
  - – To add a row to the Search Fields, click the **Add** button and enter the required values.
  - – To delete a row from the Search Fields, select the row containing the data and click the **Remove** button.
  - – To clear the entered values, select the applicable row from the Search Fields, and click the **Clear** button.

1. When all the values are entered / selected properly, click the **Search** button.
   - ⇨ The Cardholder record is displayed in the *Cardholder* section of the dialog.
2. Select the row containing the cardholder information and Click the **Delete Cardholder and Audit Data** button.
   - ⇨ A message appears to confirm the deletion of the cardholder data.
3. Click **Yes**.
   - ⇨ The Cardholder and related Audit data is deleted from SiPass integrated.
4. Click **Close** to return to the Operation client main window.

Note: The Cardholder Audit Trail data will be deleted from the database and audit archive files. However, the live Audit Trail data will not be deleted for the cardholder until the SiPass Server is restarted.

6 Monitoring Your Site

SiPass integrated allows you to monitor and control your site using a number of powerful and easy-to-use tools. Primarily, you monitor activity at your site with Active Audit Trail or a Site Plan. (To view, edit and operate any of your sites using Site Plans, you must have the optional *Graphics Module* installed.) Your site is constantly monitored in the background using the SiPass integrated alarm system, which immediately informs you of alarm situations.

6.1 Status Bar

The Status Bar at the bottom of the SiPass integrated Operation client screen gives quick information about the following:

- Outstading alarm count
- Total alarm count in the alarm queue
- Total number of configured ACCs
- Number of online ACCs
- Date / Time
- Operation Client Lock / Unlock status
- SiPass Server Online / Offline status

The Status Bar is displayed by default. To hide/unhide, go to the **View** menu and click the **Status Bar** option.

6.2 Active Audit Trail Window

The *Audit Trail - All* Window (main screen) allow you to monitor events that occur at your site as they happen. You can specify which events, and what specific information each event is displayed in the *Audit Trail - All* Window.

All database changes made by an operator are logged to the SiPass integrated audit trail, including brief information regarding the details for each change made.

The most recent event will always occur at the bottom of the viewer and, as new events appear, previous events will automatically be scrolled upwards. You may use the scroll bars located on the right-hand side of the viewer to view events or alarms that do not appear on your screen.

The Alarm Queue icon in the status bar displays a list of outstanding alarms waiting to be actioned or restored to normal. The Alarm Queue can be turned on or off without affecting the appearance or operation of the Audit Trail windows.

SiPass integrated allows you to perform the following tasks by right-clicking on an audit trail entry:

- View the details of a point associated with an audit trail entry
- View the details of a cardholder associated with an audit trail entry
- Allow entry to a cardholder that has violated Anti-Passback rules
- View a photograph of the cardholder stored in the database
- View a live image snapshot of the cardholder, if the Image Verification module is installed and the snapshot option enabled.
- View a DVR recording, if the DVR Interface module is installed.
- View details of a visitor associated with an audit trail entry.

An icon representing each event that appears in the Active Audit Trail window is located in the leftmost column.

6.3 Audit Trail Logs

To provide operators with a greater level of flexibility of Audit Trail views, SiPass integrated has been equipped with the innovative feature of Audit Trail Logs.

Operators can choose to fully utilize this feature by:

- Customizing audit trails by applying filters for the information displayed, and share these views with other operators. For example, in one log, the operator can choose to view only Card Transactions, or only Anti-Passback Area related Audit Trails.
- Opening multiple Audit Trail Logs
- Applying operator privileges at various levels for each Audit Trail Log
- Print and take Snapshots of Audit Trail Logs
- These features can be utilized through the SiPass integrated Operation Client. However, the assignment of operator privileges for Audit Trail Logs is done through the SiPass integrated Configuration Client.

Configuring multiple Audit Trail Logs

1. Select and right-click **Audit Trail Logs** from the **Navigation** panel on left.
2. Select **New Audit Trail Log**. This action will open the Report Wizard.
3. Click **Next**.
4. In the **Name** field, enter a name for the new Audit Trail view. Click **Next**.
5. From **Available Fields**, select the fields that you want displayed in the Custom Transaction Log. Click **Next**.
6. In the next screen, specify the filter conditions for the Custom Transaction Log.
7. Click **Finish**.

⇨ The new Audit Trail Log, with the specified fields and filter conditions, will be displayed under the Audit Trail Logs tree in the navigation panel on left.

Note: There is a limit of 20 views (which include Audit Trail Logs and Report Views) that can be displayed at the same time. If new views are to be displayed, older views will need to be closed.

6.3.1 Saving and Sharing Audit Trail Logs

When a Level 1 Operator creates or edits an Audit Trail Log, he can assign **View**, **Create** or **Edit** privileges for it to all the Level 2 Operators under him.

Note: For the purpose of understanding, the term Level 1 Operator refers to a person at the highest level of hierarchy.

Level 2 Operators refer to operators under the Level 1 Operator.

Level 3 Operators refer to operators under Level 2 Operators.

The level of permission a Level 2 Operator can assign to a Level 3 Operator depends on the kind of privileges assigned to him.

For example, a Level 2 Operator with Edit privileges can assign only Edit or View privileges to a Level 3 Operator. He cannot assign Create privileges.

Further, a Level 2 operator can configure privileges for Custom Transaction Logs to a Level 3 operator under him. But, he cannot assign privileges for Audit Trail Logs to another Level 2 operator. This can only be done by a Level 1 Operator.

6.3.2 Applying Direct Commands from Each Audit Trail

A number of direct commands can be given by right-clicking on any audit trail in a view.

The following are the options available to the operator on right-click:

- **Point**:

  This action displays the *Points* dialog.

- **Cardholder**:

  This action displays the respective *Cardholder* dialog.

- **Visitor**:

  This action displays the respective *Visitor* dialog.

- **Forgive**:

  This action "Forgives" a cardholder in an Anti-Passback area, and permits them to exit or enter an area, where normally this would produce an Anti-Passback violation. A forgive feature permits access for the first use of a card at either an Entry or Exit reader.

- **Remove From Anti-Passback**:

  This action removes the card from the Anti-pass back system.

- **View Image**:

  This action displays the image of the cardholder that has been saved on the *Cardholder* dialog.

- **View Snapshot:**

  This action displays the Image Verification snapshot that was taken.

- **Playback (DVR)**:

  This action plays back the respective DVR recording from the audit trail.

6.3.3 Customizing Audit Trail Logs

The appearance of Audit Trail Logs and individual audit trails can be customized in a number of ways. This sections that follow will detail how this can be done.

6.3.3.1 Highlighting Audit Trail Logs with Colors

An operator may want certain filtered audit trails to be highlighted, to help differentiate them from the rest of the Audit Trail Logs on the screen.

To configure Audit Trail Log highlights:

1. Under the **Audit Trail Logs** tree in the navigation panel on left, right-click on a selected Audit Trial log report.
2. Select **Customize View** to open its dialog window.
3. When the *Customize Views* dialog appears, select **Automatic Formatting** from the **Views** panel.
4. Use the **Format Conditions** panel to set the conditions and appearance formats to customize the audit trail.

For more information on how to use this dialog for customization, refer the section Automatic Formatting [→ 119] of this manual.

6.3.4 Printing Audit Trail Logs

You can print a selected Audit Trail Log screen as below.

1. Select the Audit Trail Log screen that you would like to print.
2. Select the **Print Preview** button on the horizontal menu bar.
3. In the dialog that appears, click the **Print** button.

6.3.5 Snapshot Capture of Audit Trail Logs

The Snapshot Capture feature allows the operator to capture a snapshot of the Audit Trail Log.

This feature is particularly useful in cases where a large number of Audit Trails appear at a fast pace on the screen. In such a situation, it may be difficult for the operator to study a particular section of the Audit Trail Log, if required. Taking a snapshot allows the operator to save the Audit Trail log for reference or analysis.

To take a Snapshot of the Audit Trail Log:

1. Select the Audit Trail Log screen for which a snapshot is to be taken.
2. Select the **Snapshot** button from the horizontal menu bar on the top.

⇨ A capture screen of the snapshot appears at the bottom of that particular Audit Trail Log.

6.4 Controlling Points

SiPass integrated allows you to control points using a number of different tools. This flexibility allows you to send commands to individual points, areas and units, view detailed information regarding a individual point, and provides an overview of all the components configured at your site.

6.4.1 Querying a Point

SiPass integrated allows you to view a detailed description of single point, intrusion area, group or unit. This information can often help you to handle an alarm situation, or just keep you up-to-date with the state of your site.

You can only query a point, intrusion area, group or unit using a Site Plan.

6.4.2 Securing and Unsecuring a Point

SiPass integrated allows you to secure or unsecure a single point, area, unit or group. By doing this you are able to override the normal behavior of an individual point, area or group. You can only secure or unsecure an area, point or group using a Site Plan, or the **Manual Override** function.

The following table provides a brief outline of the actions triggered when you secure or unsecure an individual point, area or group:

Point Type	Unsecure	Secure
Input Point	If you unsecure an input point, it will become disabled. A disabled input point cannot register an alarm. You may wish to disable an input that is faulty, and continually enters an alarm state for example.	If you secure an input point, it will become enabled. An enabled input point can register an alarm. You might wish to enable an input point that was previously disabled.
Output Point	If you unsecure an output, it will become unlocked. Unlocking an output is a fast way of allowing access. If the output controls a monitored door, it will stop the alarm for that monitored input.	If you secure an output point, it will be locked. Locking an output is a fast way of stopping an alarm activated due to the point being unlocked.
Groups / Intrusion Areas	If you unsecure a group or Intrusion area, its individual points will be unsecured.	If you secure a group or area, its individual points will become secured.

6.4.3 Allowing Access to an Output Point

SiPass integrated allows you to override the normal behavior of an individual output point, to allow access to a particular location. For example, if a cardholder forgets their access card and needs to gain entry into a secure location, you can allow that cardholder to gain access by sending that point a manual ‘allow access’ command. This command initiates the same system processes as if they had actually used their card access. You can only allow access to an output point (door) using a Site Plan.

6.4.4 Manual Override

Manual override allows you to manually manipulate an individual point, intrusion area, floor or elevator by sending electronic messages through the system. Manual commands can also be used to perform diagnostic functions. These commands will often be sufficient to restore locations to their normal state, or to check the correct operation of a specific point.

To send a manual command:

1. Double click the **Manual Override** Area list item from the Navigation pane on left hand side.
2. Select a point, elevator, area or unit from the **Type** toolbar.
3. The **Commands** available for the type you select will appear inside a list box of commands.
4. Select the unit to which the point, point group, area, elevator or unit is associated (not available for Type = Unit) from the **Unit Name** field. The default selection “All Units” will display all the points, point groups, areas, and elevators available in the system.
5. Select the specific point, point group, intrusion area, elevator or unit to which you wish to send a command from the list box at the bottom of the *Manual Override* dialog.
6. Select the Command to be sent, from the list box of commands.
   - ⇨ Additional fields may need to be completed depending upon the type of command that you select.
   - ⇨ When the *Manual Override* dialog is first opened, the default setting opens with the **Access** button selected and the **Allow Access** command highlighted. An extra field to the right of the **Commands** drop down list (highlighted above) accompanies the following commands.
7. Enter the appropriate details in the additional field (if required). The command you have selected may require a “Duration” option:
   - **Until Time Schedule Change**:
     This command will apply until the next Time Schedule begins, or until the time entered in the **Duration** field expires, whichever occurs first. After this the component will revert to normal Time Schedule control. Entering a value of zero in the Duration field means that the command is effectively permanent; the command will apply until the next manual command is sent.
   - **Permanent**:
     This command will apply until the “Return to Time Schedule Control” command is sent to the component, or until the time entered in the Duration field expires.
8. Choose **Send**. The command will be sent and an event will be generated in the Audit Trail that indicates the type of action the command produced.

6.4.5 Using the Alarm Queue

The Alarm Queue displays a list of alarms with points, waiting to be restored to their normal state, or to be actioned. The Alarm Queue will automatically appear when an operator logs on AND there is an outstanding alarm.

◈ Double click the **Alarm Queue** list item from the Navigation pane on left hand side.

Once the window is displayed, you can view the information for each current alarm or action alarms that have not been actioned.

The following table describes the information contained in the Alarm Queue.

Column	Description
Priority	The priority of the alarm. Entries will be arranged according to their priority, as specified in their Alarm Class definition. Alarms of highest priority appear first, followed by standard priority, lowest priority and no priority..
Priority Desc	The description of the Alarm Priority, as recorded in the Alarm Priority dialog.
Date	The date the alarm was first triggered.
Time	The time the alarm was first triggered.
Location	The point, area, group or unit that triggered the alarm.
Status	A short message describing the status of the alarm. For example, “Waiting for normal” indicates the point, area, group or unit, which triggered the alarm, has been actioned but is waiting to be returned to its normal state.
Count	Number of times an alarm entered alarm and back to normal without being actioned.
Current State	A message describing the current state of the alarm. For example, “Door has been forced” indicates the door has been forcibly opened. This message is user-defined in the Alarm Class Definition dialog.

6.4.5.1 Alarm Handling Priority

Alarms are handled with priority as below:

1. When a lower priority alarm is triggered first, the action window pops up immediately. If a highest priority alarm is triggered after this, the highest priority action window cannot be seen as it is hidden under the current lower priority window.
2. Now, if the highest priority and lower Standard 1, Priority Two alarms trigger within few seconds after the lower priority alarm, the Highest Priority alarm action window is visible (as the highest takes precedence) the moment you clear the existing action window in point 1 above.

The **Display Higher Priority Alarm** checkbox on the *General* tab in the *System Preferences* dialog allows alarms of a higher priority to be displayed in the *Action Alarm* dialog, if an alarm is already being actioned by an operator. The operator may select the higher priority alarm and choose to action it instead.

6.5 Handling Alarms

When an alarm is triggered in SiPass integrated, the *Alarm Display* dialog will appear.

Once such an alarm has been triggered, there are a number of tools that you can use to handle the situation. Every alarm shown in the *Alarm Display* dialog requires the alarm event to be actioned. By actioning the alarm, you acknowledge that you know about the alarm condition and are doing something to rectify the situation.

An operator can select from a list of custom responses when actioning an alarm, or enter their own. After the alarm has been actioned, further tasks may need to be carried out in order to return the alarm to its normal state.

There are two types of alarm conditions that can occur:

- Restorable
- Non-restorable

6.5.1 Restorable Alarms

Restorable alarms occur when something has physically changed at your site. For example, if an alarm class for a door-frame existed on your SiPass integrated database, the alarm can be set to restorable. If the door has been forced, and triggered alarm, you can action that alarm. But, that input will not return to normal until the door is physically closed. If it is not returned to its normal state within the Time Period specified in the alarm-class record, the alarm will reactivate. The reactivated alarm will trigger the Alarm Display dialog to appear again, and the count will increment to one.

Sometimes a point, area, group or unit, which is restorable, will return to normal before you action the alarm. For example, an open boom gate might close; in which case, actioning the alarm would be sufficient to clear it.

To restore an alarm you may need to do one or more of the following:

- Physically change the situation at your site. For example, you may need to close a door that is obstructed.
- Unsecure (disable) the input point in SiPass integrated Configuration Client so that it no longer registers an alarm.
- Manually send a command through the system to restore the point, area, group or unit.
- Find out more about the point, area, group or unit registering an alarm.

6.5.2 Non-Restorable Alarms

Defining a Non-Restorable Alarm generally assumes that you want the operator to acknowledge a specific alarm once only. For example, you may define an alarm class so that a void card is detected at a reader connected to a main door. You want the operator to acknowledge that someone has attempted to gain access using a void card. If the alarm is not restorable, the point in alarm will be considered normal as soon as the alarm is actioned.

The related alarm will be cleared from the alarm queue.

6.5.3 Actioning an Alarm

When an alarm is triggered and an *Alarm Display* dialog appears, you must action the alarm. By actioning the alarm, you are logging a message to the system, indicating that you have acknowledged the alarm and are doing something about it.

Note: You can add a description for your response to the alarm in the **Log of action taken** field. The description can be up to 256 characters long after which, it will be truncated.

There are three ways you can action an alarm:

- Via the *Alarm Display* dialog
- Via the **Site Plan**
- Via the **Alarm Queue**

6.5.3.1 Method 1 - Alarm Display dialog

When the *Alarm Display* dialog appears the alarm status display appears in the upper left-hand corner of the *Alarm Display* dialog. This display informs you of the number of events currently in the alarm queue, the number of alarms that have been actioned and are waiting to be restored, and the location of the alarm that triggered the dialog and the reason for the alarm.

1. Select an appropriate alarm response from the **Pre-defined Alarm Response** drop-down box, or enter a new response. The text entered should briefly reflect the nature of the alarm and the action taken by the operator/security personnel.
2. Choose **Add Response** to add the response to the **Log of action taken** field. You may select or enter multiple alarm responses, by choosing **Add Response** after each entry. You must enter a response into the dialog before the **Action** button is enabled. You can choose **Edit Response** to open the *Alarm Responses* dialog, which allows you to create, modify and delete pre-defined alarm responses.
3. Choose **Action**. The *Alarm Display* dialog will be removed and an event will appear in the Audit Trail indicating that the alarm has been actioned. The contents of the Log of action taken field will also be displayed in the Audit Trail, to show what action has been taken in response to the alarm.
   - To silence the alarm before actioning it, you can enter the time (in seconds) into the secs field and choose Silence. The Alarm Display dialog will disappear and the alarm will be silenced. If the alarm has not been actioned before the silence time has expired, the alarm will re-trigger.
   - The action of silencing the alarm will appear in the Audit Trail as well as each time that the alarm re-activates.
   - More than one operator may receive the alarm at their Client PC. However, only one operator needs to action the alarm.

6.5.3.2 Method 2 - Site Plan

1. Choose **Plan**, from the *Alarm Display* dialog.
2. Select the point, area, or floor to be actioned by clicking on it.
3. Choose **Action** from the **Alarm** toolbar.
4. Select an appropriate alarm response from the **Pre-defined Alarm Response** drop-down box, or enter a new response.
5. Choose **Add Response** to add the response to the **Log of action taken** field.
   – You may select or enter multiple alarm responses, by choosing Add Response after each entry.
   – You must enter a response into the dialog before the **OK** button is enabled.
   – You can choose **Edit Response** to open the *Alarm Responses* dialog, which allows you to create, modify and delete pre-defined alarm responses.
6. Choose **OK**.

⇨ The alarm event will disappear from the **Alarm Queue** window and an Audit Trail event will be generated, informing the SiPass integrated operator(s) that the alarm has been actioned. The *Alarm Display* dialog will be removed.

⇨ If the alarm is restorable, and has not been restored to its normal state within the specified Time Schedule, the alarm will remain in the **Alarm Queue** window and continue to re-activate until it has been restored.

⇨ An event will appear in the Audit Trail that indicates the alarm has been actioned. The contents of the Log of action taken field will also be displayed in the Audit Trail, to show what action has been taken in response to the alarm.

⇨ More than one operator may receive the alarm at their client PC. However, only one operator needs to action the alarm.

ℹ To action alarms from Site Plans, the operator should have the appropriate Operator Privilege for Site Plans, and also privileges to the particular unit or point in concern.

6.5.3.3 Method 3 - Alarm Queue

All alarms that have been triggered and are waiting to be restored to their normal state or to be actioned appear in the *Alarm Queue* window. As well as being displayed in the Alarm Queue, the alarms are also displayed in the Audit Trail.

1. Double click the **Alarm Queue** list item from the Navigation pane on left hand side.

   ⇨ A message will appear in the Audit Trail indicating that you have crossed to the *Alarm Queue* Window.

2. Highlight the alarm to be actioned, by clicking on it. More than one alarm can be actioned at once, by using CTRL – Left Click to select multiple rows.
3. Choose **Action**.
4. Select an appropriate alarm response from the **Pre-defined Alarm Response** drop-down box, or enter a new response.
5. Choose **Add Response** to add the response to the Log of action taken field. You may select or enter multiple alarm responses, by choosing **Add Response** after each entry.
6. You must enter a response into the dialog before the **OK** button is enabled.

   – You can choose **Edit Response** to open the *Alarm Responses* dialog, which allows you to create, modify and delete pre-defined alarm responses.

7. Choose **OK**.

⇨ The alarm will disappear from the *Alarm Queue* window and an Audit Trail event will be generated, indicating the alarm has been actioned. The contents of the Log of action taken field will also be displayed in the Audit Trail, to show what action has been taken in response to the alarm.

⇨ If the alarm is restorable, and has not been restored to its normal state within the specified Time Schedule, the alarm will remain in the *Alarm Queue* window and continue to re-activate until it has been restored.

!

NOTICE

The operator privileges (from the System Functions found on the Operator Group dialog) required to configure various aspects of the Alarm Queue are stated below.

- Operators with View (v), Edit (e) and Create (c) privileges for the Alarm Queue can action alarms in the Alarm Queue. They can also use the ‘Add Reponse’ feature to add or delete a response to the Pre-defined Alarm Response.
- Only Operators with Edit (e) privileges can edit existing Pre-defined Alarm Responses.
- Operators with only View (v) permissions CAN action the alarm, and use an existing alarm response from the Pre-defined Alarm Response options.
- An operator without any privileges for the Alarm Queue, will not be able to view the Alarm Queue dialog.

⇨ Further, Alarm Queue Privileges do not affect the privileges for Site Plan Alarms.

6.6 Using Site Plans to Monitor your Site

Once you have created a site plan and added the appropriate symbols to that plan, it can be used to monitor your site. When an alarm has been triggered, the symbol representing the point, group, area or unit in question on the site plan will change color. It will remain that way until it has been actioned and, if necessary, returned to its normal state. A site plan can also be used to send manual commands to elements, allowing you to control many aspects of your site from the graphical plan.

6.6.1 Viewing Options for Site Plan

While working in Operation client, the Site Plan windows and Audit Trail windows might require arranging the information on the screen for the best possible view.

With SiPass integrated MP2.80 onward, a site plan can be opened outside the Operation Client main workspace window and dragged to any corner of the screen as required.

- To move an already open site plan outside the Operation client workspace, click on the **Topmost** option in the menu of the site plan window.
- To always open the site plan outside the Operation Client window, check the **Open Site Plan window in topmost mode** checkbox by clicking *Options > Preferences* in the Operation Client.
- To zoom-in / zoom-out on the information in a Site Plan, use **Ctrl + Mouse Wheel** (like standard Windows zoom).

6.6.2 Interpreting the Site Plan

When you have selected the correct site plan, you will be able to see the current status of each of its points, areas, groups and units. Each element is represented by a symbol that changes color according to its current status.

Important: The part of the symbol that is to change color according to status, must be filled with the standard RED when it is drawn.

Colour	Symbol
RED (SOLID)	Alarm symbol
RED (FLASHING)	Alarm Symbol
MAGENTA	Alarm Symbol
GREEN	Restored symbol
BLUE	Symbol remains as it was when it was unsecured.

By positioning the mouse pointer over a point on a site plan, a brief description of that point will appear, including the name of the point and its current state. By positioning the mouse pointer over a point on a site plan, and right clicking, the Query dialog will appear, displaying detailed information about that point.

6.6.3 Securing a Point or Area From a Site Plan

SiPass integrated allows you to send a manual command to secure a particular point or area using a Site Plan.

1. Expand the **Site Plan** folder list in the Navigation menu and select the plan that contains the appropriate points or area.
2. Select the point, area, or group to be secured by clicking on it.
3. Choose **Secure Location/ Group**.

⇨ The point, area or group will be secured.

6.6.4 Unsecure a Point or Area From a Site Plan

SiPass integrated allows you to send a manual command to unsecure a particular point or area using a Site Plan.

1. Expand the **Site Plan** folder list in the Navigation menu and select the plan that contains the appropriate points or area.
2. Select the point, area, or group to be unsecured by clicking on it.
3. Choose **Unsecure**.

⇨ The point, area or group will be unsecured.

6.6.5 Allow Access to an Output Point From a Site Plan

SiPass integrated allows you to override the normal behavior of an individual output point to allow access to a particular location. For example, if a cardholder forgets their access card and needs to gain entry into a secure area, you can allow that cardholder to enter the area by sending the output point a manual “allow” command.

1. Select the icon that represents the output point. The point should now appear highlighted on the site plan.
2. Choose **Allow Access**. The point will temporarily change state. For example, if you selected an output point at a door, the door will temporarily unlock for the configured time and then return to its normal state (locked).
3. Choose **Unsecure Location/ Group**.

6.6.6 Manually Controlling a Point from a Site Plan

You can manually manipulate an individual point, area, floor, or elevator by sending electronic messages through the system. Manual commands can also be used to perform diagnostic functions.

1. Choose the icon that represents the point to be manually controlled.
2. The point should now appear highlighted on the site plan.
3. Choose **Override**.
4. Select which component you wish to manually control by selecting the appropriate button from the **Type** toolbar. The Commands are always available by accessing the **Manual Override** function.
5. Select the unit to which the type is associated from the **Unit Name** field.
6. Select the specific point, point group, area, elevator or unit to which you wish to send a command, from the list box at the bottom of the dialog.
7. Select the **Command** to be sent from the **Commands** list box.
8. Choose **Send**.
   ⇨ The command will be sent to the respective component and an event will be generated in the Audit Trail indicating the resulting action.
9. Choose **Close** to return to the main screen.

6.6.7 Querying a Point From a Site Plan

SiPass integrated allows you to view a detailed description of a single point, area, group or unit. This information can often help you to handle an alarm situation, or just keep you up-to-date with the state of your site.

1. Select the icon that represents the point, area, group, or unit to be queried.
2. Right click on the selected point, area, group or unit.
   ⇨ The *Query* dialog will appear. View the details regarding the selected point, area, group or unit.
3. Choose **Close** when you have finished viewing the details.

6.6.7.1 Point Details

The following table explains the point details when querying a point.

Detail	Description
Location	The name of the point, area, group or unit that you are querying.
Type	Indicates the specific type of point, area, group or unit that you are querying.
Alarm Class	Specifies the Alarm Class that has been assigned to the point, area, group or unit.
Priority	Indicates the priority level of the Alarm Class assigned to the point, area, group or unit.
Time/Date	Indicates exactly when the selected item first went into alarm.
Alarm Count	Specifies exactly how many times this item has entered an alarm state without being actioned (after being restored).
Status	Brief description of the status of the point, area, group or unit. The status displayed here is defined in the alarm class definition.
Alarm State	The current state of the point, area, group or unit.
Enable	Indicates whether the point, area, group or unit is enabled or disabled. Alarms cannot go off at disabled points.
Last Alarm Comment	Displays the brief message entered by the operator about the last alarm occurring at this point, area, group or unit.

6.6.8 Actioning an Alarm from a Site Plan

SiPass integrated allows you to action an alarm using a site plan, after an alarm has been triggered and is to be acknowledged.

1. Select the alarm to be actioned from the **Alarm Queue** and choose **Site Plan**. A plan appears that displays the point, area, or floor where the alarm was activated. If the plan has been configured correctly, all points or areas currently in an un-actioned alarm state will be flashing red.
2. Select the point area, or floor to be actioned by clicking on it.
3. Choose **Action Alarm**.
4. Enter a message into the **Log of action** taken field. This will indicate that you have acknowledged the alarm and are taking action to investigate. This message is passed to the Audit Trail.
5. Choose **OK**.
   - ⇨ The alarm event will disappear from the **Alarm Queue** window (if the point has returned to a normal state) and an Audit Trail event will be generated, informing the SiPass operator(s) that the alarm has been actioned.

7 Reports

The SiPass integrated system contains a powerful reporting package, which allows you to create detailed reports on information contained in the Log Book. You can customize the information that appears in each report to suit your own needs. Any reports you produce will only contain data to which your operator group has privileges.

SiPass Predefined reports are available to access the whole range of reports available to SiPass integrated. It can be accessed via the **SiPass integrated Operation Client** navigation panel.

7.1 Customized & Predefined Reports

SiPass integrated allows you to browse and generate reports easily. This tool combines a powerful database and audit trail reports from SiPass integrated, with an intuitive visual interface called the SiPass Reporting Wizard to speed-up and streamline your reports.

It is also possible to arrange how the data is presented and customize reports even further than before. Reports come with a standard selection of data columns which can be removed or reordered, as well as a set of additional columns that can be inserted. Custom views can be added to change how the data in a report is displayed and these views are saved for future use.

There are two types of reports that an operator can create:

- **Customized Reports**
- **Pre-defined Reports**

7.1.1 Getting Started

7.1.1.1 Creating a New Report

SiPass integrated allows you to create customized reports for the information you receive, and the way in which it is received. Custom reports are based on pre-defined data sets such as Cardholder or Points, and can be saved under **Customized Reports** in the **Navigation** pane.

There are two ways to create a new report: Create a new report by itself or create a new report based on an existing report.

Creating a new report

1. Select **New > New Report** from the **File** menu.

   On the *Report Wizard* screen, click **Next** to continue.

2. Enter a name for your report and select a place in the **Navigation** tree for it to be saved.
3. Click **Next** to continue.
4. Select a **Record Type** and then the fields to include in your report.

   Use the left and right buttons to move fields in and out of the report.

5. Click **Next** to continue.
6. Specify filter conditions for your report. For more details please refer to the section Filter Conditions [→ 115].
7. Click **Finish** to complete your report.

Creating a new report from an existing report

1. From the File menu, select **New > New Report**.

   On the *Report Wizard* screen, click **Next** to continue.

2. Enter a name for your report and select a place in the **Navigation** tree for it to be saved.
3. Select the option **Create from an existing report**, and click **Next.**
4. Select a report to base your new report on, and click **Next** .
5. Select a **Record Type** and then the fields to include in your report.

   Use the left and right buttons to move fields in and out of the report.

6. Click **Next** to continue.
7. Specify filter conditions for your report. For more details please refer to the section Filter Conditions [→ 115].
8. Click **Finish** to complete your report.

7.1.1.2 Customizing Views

Customizing views ensures your report is easy to read and contains the information you required. Available views are required in a list in the **Current View** pane. To begin, perform the following operations:

1. Launch **SiPass Reporting**.
2. Use the **Tree** in the **Navigation** Pane to locate the component you wish to build a report on.
3. Right click the report you wish to customize and select **Customize View**.
4. Select a view to customize or create a new view.

The operator can customize a report view using the following options:

- **Display Fields**
- **Filter Conditions**
- **Available Actions**
- **Group By**
- **Sort Order**
- **Appearance**
- **Automatic Formatting**
- **Advanced**

The sections that follow explain each of these options, and how you can use them to customize your views.

Display Fields

The Modify Fields section defines which fields are included in your view, and the order in which they are displayed.

Modifying display fields

1. Select **Display Fields**. Two columns of fields will be displayed.
2. Select a field and use the **left** and **right** buttons to move the field in and out of the report.
   - The left hand column lists all the fields not being used, and the right hand column lists all those that will be displayed in the report.
3. Select a field in the right hand column and use the Up and Down buttons to modify the order of the field in the report.
   - Fields at the top of the list are displayed first, and will appear on the left hand side of the report.
4. Click **OK** or **Apply** to save your changes.

Filter Conditions

Filter conditions allow you to restrict the report to only display certain data. This is useful when you need only particular records, and not everything. SiPass integrated allows you to add several filters to narrow down the results and provide even more precise data.

Modifying filter conditions

1. Select **Filter Conditions**.
2. Click on the labeled filter button to create a filter.
3. Select a field to filter with and an operator for your filter action.

   Filter Condition Operators are explained in the section that follows.
4. Enter in the data that you wish to filter with and click the **Add Criterium** button.

   The data you can enter into the filter section.
5. Repeat steps 3-4 for any additional filters that are required.
6. Click **OK** or **Apply** to save your changes.

Filter condition operators

The available filter condition operators are explained in the table below:

Operator	Explanation
Equal to	Returns all records that exactly match the specified field value
Not equal to	Returns all records that do not match the specified field value
Greater than	Returns all records that are greater than the specified field value
Less than	Returns all records that are less than the specified field value
Less than or equal to	Returns all records that are lesser than or equal to the specified value
Greater than or equal to	Returns all records that greater than or equal to the specified field value
Between	Returns all records that are between the specified field values
Not between	Returns all records that are not between the specified field values
Contains	Returns all records that contain the specified field value
Does not contain	Returns all records that do not contain the specified field value
Begins with	Returns all records that begin with the specified field value
Ends with	Returns all records that end with the specified field value
Is null	Returns all records that have a null value for that field
Is not null	Returns all records that do not have a null value for that field
Is empty	Returns all records that do not have a value for that field, and are empty
Is not empty	Returns all records that have a value for that field, and are not empty
Any of	Returns all records that have a value that matches any of the specified values.
None of	Returns all records that have a value that matches none of the specified values.
*As Parameter	Returns all records that have a value that matches the parameter specified.

Current Date Relative Report Filter

SiPass integrated cardholder report capability helps you filter the search results for a date field relative to the current date. You can filter a report for comparing any date field with the current date through the new *Current Date* option in the **Date Field Filter** dropdown list, by entering the number of days, hours and minutes before or after the date on which, the report is running.

Any of the following filter condition operators can be selected for this purpose:

- Equal to
- Not Equal to
- Greater than
- Greater than or equal to
- Less than
- Less than or equal to

You can enter the number of days, hours and minutes before or after the date on which, the report is running. If you want to create a report prior to the date the report is running, enter a negative value (-) in the **Days** field.

Example

- Values entered as **Days = 2**, **Hours = 10** and **Minutes = 30**, create a report for 10:30 am of two days later to the date the report is running.
- Values entered as **Days = -1**, **Hours = 10** and **Minutes = 30**, create a report for 10:30 am of one day prior to the date the report is running.

Note: Time value is not supported (hours/minutes field disabled) if any of the *Equal to* or *Not Equal to* filter condition is selected.

*Parameterized Reports

If a report was created with at least one **As Parameter** filter condition, it is considered to be a **Parameterized Report**.

Available Actions

Operators can configure any of the following actions to a report, to create **Actionable Reports**:

- **Void Card**

Voids the particular card in the SiPass integrated system.

- **Void Cardholder**

Voids the cardholder in the SiPass integrated system.

- ***Resolve by Deleting**

The synchronization issue is resolved by deleting the entity/entities in concern.

- ***Resolve by taking external system version**

The synchronization issue is resolved by accepting the external system version.

- **Warn User**

When applied, this action will warn the operator when the details of the cardholder in concern is either updated or newly created in the *Cardholder* dialog.

- ***Resolve by taking SiPass version**

The synchronization issue is resolved by accepting the SiPass integrated version of the entity/entities in concern.

- ***Ignore Conflict**

The synchronization report entry is actioned to be ignored.

*****The operator does not have to customize actions for the 4 synchronization resolution actions described above. These actions will be available by default on the synchronization report, by right-clicking an entry in the report.

Setting an Available Action:

1. Select **Available Actions**.
2. Tick the checkboxes for the options that you want to customize for the report.
3. Select **Set as default**.
4. Click **OK** or **Apply**.

Group By

Group By allows you to arrange how the records returned by the report are organized. The records are sorted into groups with a common field value as specified by the user.

Setting a Group By condition

1. Select **Group By**.
2. Select a field to group by from the first drop down list
3. Select whether to sort the grouped items **Ascending** or **Descending** by clicking the appropriate option
4. Select any additional grouping in the other drop down lists, going from top to bottom.
5. Hide or display the name of the column that is used for grouping by toggling the checkbox labeled **Hide columns when grouped**.
6. Click **OK** or **Apply** to save your changes.

Sort Order

Sort Order allows you to sort the records by multiple fields. The sorting is done in order, with the top field that is selected being sorted first, and the bottom field being sorted last.

Setting a Sort Order

1. Select **Sort Order**.
2. Select a field to sort from the first drop down list.
3. Select whether to sort **Ascending** or **Descending** by clicking the appropriate option.
4. Select any additional sorting in the other drop down lists, going from top to bottom.
5. Click **OK** or **Apply** to save your changes.

Appearance

Making changes to the Appearance section lets you customize how the data is presented by modifying fonts, grid lines, icons and column size distribution.

Customizing Appearances

1. Select **Appearance**.
2. Select a font to use for the column headings by clicking the **Font** button in the **Column Headings** section.
3. Enable or disable **Automatic Column Sizing** by clicking the checkbox.
   – **Automatic Column Sizing** automatically fits all selected fields in the viewable area. It attempts to use an even distribution of column sizes.
4. Select a font to use for the row text by clicking the **Font** button in the **Rows** section.
5. Enable or disable row icons by clicking the **Show Icon** checkbox.
   – An icon is displayed next to each row by default. You can even select a different icon to display by clicking the icon graphic and picking one from the list.
6. Select a grid line type and style from the drop down lists in the **Grid lines** section.
   – **Grid lines** define what lines are shown and **Grid line** style defines whether the line is solid or dotted.
7. Enable or disable **Shade Group Headings** by clicking the checkbox.
   – This option will color the **Group By** headings grey in your printed report to help distinguish them.
8. Click **OK** or **Apply** to save your changes.

Automatic Formatting

Automatic Formatting allows you to create rules that automatically format text depending on specific criteria. This means that you can visually highlight specific data to make it easily visible without filtering out all other data.

For example, you may want to easily see which Units are online and which are offline. By using automatic formatting you can have all Units that are online displayed in the report with a green background, and all the offline ones displayed with a red background.

Setting up Automatic Formatting:

1. Select **Automatic Formatting**.
2. Click **New** to create a new **Format Condition**.
3. Enter a **Condition name**.
4. Enter a filter condition for when the formatting will be applied. This is a combination of a **Field**, a **Condition** and a **Value**. For more details on configuring filters please refer to the section Filter Conditions [→ 115].
5. Select formatting to make the filtered data stand out.
   – Select a font modifier, or a combination of them by ticking the checkbox next to Bold, Italic or Underline.
   – Click **Colors** and select a text and or background color to highlight the text.
6. Click **OK** or **Apply** to save your changes.

Advanced

The Advanced section allows you to set column properties. These properties control the behavior and display of the column in the report.

Multiple Page feature for all reports

SiPass integrated now implements the Multiple Page feature for all reports, if the configured row-limit per page has been exceeded. This presents operators with the advantage of viewing entire large reports.

When customizing the view of a report, the number of rows to be displayed per report is set to 100,000 by default. This value can be configured to a maximum limit of 300,000 rows per page.

For large reports that contain more than 300,000 rows, the rows that follow will be displayed in additional pages of the report.

This allows enables operators to view large reports, without limiting the number of report pages that can be displayed.

Configuring Advanced properties

1. Select **Advanced**.
2. Select a column.
3. Adjust the properties of the column as required.
4. Repeat steps 2 and 3 for each column that needs to be modified.
5. In the **Page Size** field, select the number of rows to appear per page, for the entire report.

By default, this value is set to 100,000. The maximum limit is 300,000 rows per page.

6. Click **OK** or **Apply** to save your changes.

Advanced fields

The available fields are explained in the table below:

Field	Explanation
Allow Drag	Determines whether the selected column can be dragged and repositioned within the report.
Allow Size	Determines whether the selected column can be resized within the report.
Allow Sort	Determines whether the selected column can be sorted within the report.
Caption	Sets the title of the column.
Image Size	Sets the dimensions of the image, in pixels, if one is in the column. The first number is the image width , and the second is the image height.
Width	Sets the width of the column in pixels.
Mode	Determines whether the sorting and filtering is done on the server or the client. We recommend the Server mode as it will be faster and transfer less data over the network.
Limit	Sets the maximum number of records that can be returned after a sort or filter operation.

7.1.1.3 Searching Reports for Data

SiPass integrated makes it possible to search for specific data within a report. This feature is embedded in every report, via the interface, and can be easily enabled or disabled.

▷ Before you begin, ensure that all the columns you want to include in your search are added to the report.

1. Open the report you wish to search within.
2. Click the **Find** button on the Tool Bar. A filter row will appear.
3. Type your search term(s) into the appropriate columns on the filter row and press the **Enter** key. Rows matching your search criteria will be displayed below.
   – Use the * character as a wildcard to fill in parts of the search you are unsure of.
   – Multiple keywords can be used in multiple columns to narrow your search.
4. Click the **Find** button again to make the filter row disappear and return to the regular report view.

For single reports containing multiple pages:

Using the **Find** button will only search through the report page currently displayed. All additional pages of the report should be displayed and searched through individually.

Search Criteria

This section details the search criteria that can be used to search for specific information within reports.

Search Symbols	Search Criteria Description	Example
=	**Equal To** This search criteria can find only numeric data.	**= 7.** This search will return all the rows with the value 7.
!=	**Not Equal To** This search criteria can find data that is not equal to the numeric or strings entered after it.	**!=7** This search will return rows with all values except 7.
>	**Greater Than** This search criteria can find data that is greater than the numeric or strings entered after it.	**>7** This search will return rows with all values greater than 7. **>B** This search will return rows with all strings that begin with alphabets that come after B. It will not return rows that contain strings beginning with the alphabet A.
<	**Less Than** This search criteria can find data that is less than the numeric or strings entered after it.	**<7** This search will return rows with values less than 7. **<B** This search will return rows with all strings that begin with alphabet A alone, as it comes before B. This search will not return strings that begin with alphabets that come after B.

Search Symbols	Search Criteria Description	Example
>=	**Greater Than or Equal To** This search criteria can find numeric or strings that are greater than or equal to the value entered after it.	**>=2** This search will return rows with all values greater than or equal to 2. **>= B** This search will return rows with all strings that begin with the alphabet B, and all the following alphabets. It will not return rows starting with the alphabet A.
<=	**Less Than or Equal To** This search criteria can find numeric or strings that are less than or equal to the value entered after it.	**<=2** This search will return rows with values less than or equal to 2. **<=C** This search will return rows with all strings that begin with alphabet C, and also rows that begin with the alphabets B and A. It will not return rows beginning with alphabets that come after C.
* *	**Contains** This search criteria can find numeric or strings that are entered between both the asterix symbols.	***20*** This search will return rows that contain the value 20. ***pin*** This search will return rows that contain the word „pin“.
*	**Ends With** This search criteria will find numeric and strings that end with value entered after the asterix.	***2** This search will return rows that end with the value 2. ***pin** This search will return rows that end with the word pin
*	**Begins With** This search criteria will find numeric and strings that start with the value entered before the asterix.	**2*** This search will return rows that begin with the value 2. **System*** This search will return rows that begin with the word System.
No Symbols Used	If search data is entered into the search field without any accompanying symbols, this search will be treated as using the Equal To symbol.	**Pin** This search will return rows that contain the word Pin.

7.1.1.4 Page Setup

Before printing or generating a print preview, you should configure your Page Setup. This is important to ensure that any reports you generate are properly formatted. This will need to be done once per session. If you close and open SiPass Reporting, you will need to configure these settings again.

Adjusting the Page Setup

1. Select **File > Page Setup**.
2. Select a paper **Size** and **Source** using the drop down boxes.
3. Select an **Orientation** of Portrait or Landscape.
4. Set the printing **Margins** for your report. The default setting is 1 inch.
5. Click the **Printer…** button to select your report printer.
6. Click **OK** to finish the Page Setup process.

For single reports containing multiple pages:

Using the **Print** button from the menu bar to print a report, will only print the report page currently displayed. All additional pages of the report should be displayed and printed individually.

7.1.1.5 Exporting Data

Once you have configured the data for your report, you can easily export it to four different formats:

- Tab delimited text file
- Excel file
- XML file
- CSV text file (Comma Separated Values)

Exporting a report

1. Generate the report you wish to export. For more details, refer the section Generating Reports.
2. Customize the report columns (for more details refer the section Customizing Views [→ 114]).
3. Select **File > Save As** from the menu.
4. Select a location to export the file.
5. Enter a name for the exported file.
6. Select a format.
7. Click **Save** to finish exporting the report.

For single reports containing multiple pages:

Using the **File > Save As** functions from the menu, will save and export only the page of the report that is currently displayed. All additional pages should be saved and exported individually.

7.1.2 Generating Reports

Unlike customized reports, the filters, view and other related information are already pre-defined for Predefined Reports. However, if any available pre-defined report needs to be customized, this can still be done by right-clicking the specific report and selecting **Customize View**.

This report can then be customized as described in the section Customizing Views [→ 114].

7.1.2.1 Components

The components category handles the physical components of your system. This includes Controllers (Units), Devices and Points.

Generating a Components report

▷ View the section Customizing Views [→ 114] for more detail on formatting your report.

1. Expand the **Components** item from the **Navigation** pane.
2. Select either **Units, Devices** or **Points.**
   - If selecting points choose either **All Points, Access Points, Input Points** or **Output Points**.
3. Customize the view of your report:
   - Right Click and select **Customize View.**
   - Suggested modifications include changing the columns, adding filters and grouping data.
4. Click **Print Preview**.
   - If the report looks fine click the **Print** button at the top left corner of the screen.
   - To make further modifications to the report, click the **Close Print Preview** button and return to step 4.

Units Report Fields

These are the available fields for the Units report. If all the fields are not visible on the report, click the **Field Chooser** button.

To add these fields to the report, select a field and drag it to the field bar of the report.

Colum	Description
Unit Name	Name of the controller \ unit
Number	Unique number of the controller \ unit
Type	Type of unit (e.g. ACC)
Status	Status of the controller \ unit
Enabled	Whether the controller \ unit is enabled or disabled
Bus Name	Bus that the controller \ unit is connected to.
Version	Controller \ unit firmware version or revision.
Server Name	Server name where the controller \ unit is connected
Equipment Description	Field can be used to described the equipment being configured
Serial Number	Serial number of the unit

Devices Report Fields

These are the available field columns for the Devices report.

Colum	Description
Device Name	Name of the device.
Device Number	Number of the device on the FLN.
Type	Type of the device
Unit Name	Name of the ACC the device is attached to.
Unit Number	Number of the ACC the device is attached to.
FLN Name	Name of the FLN that the device is on.
FLN Number	Number of the FLN the device is on.
External Device Number	External number used to identify the device on APOGEE.
Equipment Description	Field can be used to describe the equipment being configured

Points Report Fields

These are the available field columns for Point reports.

Colum	Description
Point Name	Name of the point.
Point Number	Point number of the point.
Point Status	The last reported status of the point
Time Schedule	Time schedule associated with the point.
Point Type	Type of point (e.g. Access, Input, Output)
Unit Number	Number of the ACC that the point is attached to.
Unit Type	The type of Unit that the point is on.
FLN Number	Number of the FLN the point is on.
Device Number	Number of the device that the point is on.
Unit Name	Name of the ACC the point is on.
FLN Name	Name of the FLN the point is on.
Device Name	Name of the device the point is on.
Bus Name	The name of the bus the point is on
Server	The SiPass integrated server the ACC is communicating with
Alarm Class	The alarm class assigned to the point
Normal Task 1 Command	Internal Controller event task (NT hardware only)
Normal Task 1 Data	Internal Controller event task (NT hardware only)
Normal Task 2 Command	Internal Controller event task (NT hardware only)
Normal Task 2 Data	Internal Controller event task (NT hardware only)
Alarm Task 1 Command	Internal Controller event task (NT hardware only)
Alarm Task 1 Data	Internal Controller event task (NT hardware only)
Alarm Task 2 Command	Internal Controller event task (NT hardware only)
Alarm Task 2 Data	Internal Controller event task (NT hardware only)
Timer1	The setting of the first timer on the point, for output points this is delay 1
Timer2	The setting of the second timer on the point for output points this is delay 2
Operation	The operation mode of the point
External ID	The external ID of the point used by OPC systems.

Hubs Report Fields

These are the available field columns for the Hubs report.

Colum	Description
Hub Name	Name of the Aperio hub as entered during configuration.
Hub Number	Number of the Hub on the FLN.
Model	Model of the device
Status	Communication Status of the Hub.
Description	Description for the Aperio hub as entered during configuration.
Unit Name	Name of the ACC the device is attached to..
Unit Number	Number of the ACC the device is attached to.

7.1.2.2 Time Schedule

This category provides reports for time schedules and contains all the details of the time schedules including the start and end of the time periods.

Generating a Time Schedule report

▷ View the section Customizing Views [➙ 114] for more detail on formatting your report.

1. Expand the **Time Schedule** item from the **Navigation** Pane.
2. Select either **Time Schedules** or **Time Schedule Details**.
   - **Time Schedules** is an overview of the time schedule names.
   - **Time Schedule Details** shows all the details of each time schedule. The default view includes all time schedules that have valid time periods.
3. Double click the time schedules you want from the **Available Time Schedules** box and click **Display Selected** to show the details of only a few time schedules.
4. Customize the view of your report:
   - Right Click and select **Customize View**.
   - Suggested modifications include changing the columns, adding filters and grouping data.
5. Click **Print Preview**.
   - If the report looks fine click the **Print** button at the top left corner of the screen.
   - To make further modifications to the report click the **Close Print Preview** button and return to step 5.

Time Schedule Details Report Fields

These are the available field columns when building reports on Time Schedule Details.

Column	Description
Start Date	Day when the time schedule starts.
Stop Date	Day when the time schedule stops.
Start Time	Time when the time schedule starts.
Stop Time	Time when the time schedule stops.
Time Schedule ID	Number associated with the time schedule.
Time Schedule	Name of the time schedule.

7.1.2.3 Component Groups

The Component Groups category displays reports which show the component point groups that are defined in SiPass and the points they contain.

Generating a Component Groups report

▷ View the section Customizing Views [→ 114] for more details on formatting your report.

1. Expand the **Components Group** item from the **Navigation** Pane.
2. Select a group report from the list. The types of reports are explained below.
   – **Groups** displays an overview of the groups and what types they are.
   – **Points / Units / FLNs / Devices** displays the details of each group and the objects it contains.
3. Customize the view of your report:
   – Right Click and select **Customize View.**
   – Suggested modifications include changing the columns, adding filters and grouping data.
4. Click **Print Preview.**
   – If the report looks fine click the Print button at the top left corner of the screen.
   – To make further modifications to the report click the **Close Print Preview** button and return to step 4.

Point Group Report Fields

These are the field columns that are available when building reports on Point Group details.

Column	Description
Point Group Name	Name of the point group.
Point Group Type	The type of the point group (e.g. Access, Input, Output)
Point Name	Name of a point within the group.
Unit Name	Name of the ACC a point belongs to.
Unit Number	Number of the ACC a point belongs to.
FLN Number	Number of the FLN associated with the point.
Device Number	Number of the device that the point is on
Point Number	Number of the point
Clearance Required Action	Whether the Clearance Required flag is set for the point group.
Isolate Group Action	Whether the Isolate Group flag is set for the point group.
Group Alarm Timer	How long the number of alarms must be active to trigger the group alarm.
Group Alarm Count	How many points in the group must go into alarm before the group alarm is triggered.
Alarm Class Name	Name of the Alarm Class assigned to the group

Unit Group Report Fields

These are the field columns that are available when building reports on Unit Group details.

Column	Description
Unit Group Name	Name of the Unit Group.
Unit Name	Name of the Unit inside the group.
Unit Number	Number of the Unit inside the group.
Alarm Class Name	Name of the Alarm Class assigned to the group

FLN Group Report Fields

These are the field columns that are available when building reports on FLN Group details.

Column	Description
FLN Group Name	Name of the FLN Group.
FLN Name	Name of the FLN inside the group.
FLN Number	Number of the FLN inside the group.
Parent Unit	Unit the FLN is connected to.
Alarm Class Name	Name of the Alarm Class assigned to the group

Device Group Report Fields

These are the field columns that are available when building reports on Device Group details.

Column	Description
Device Group Name	Name of the Device Group.
Alarm Class Name	Name of the Alarm Class assigned to the group.
Device Name	Name of the Device inside the group.
Device Number	Number of the Device inside the group.
Parent FLN	The FLN the Device is connected to.
Parent Unit	The Unit the Device is connected to.

7.1.2.4 Access Levels

The Access Level category displays reports based on the access levels configured in SiPass integrated and the points they contain.

Generating an Access Levels report

▷ View the section Customizing Views [→ 114] for more details on formatting your report.

1. Expand the **Access Levels** item from the Navigation Pane.
2. Select either **All Access Levels, Access Level Points** or **Access Level Point Groups**.
   - All **Access Levels** displays an overview of the access levels and what types they are.
   - **Access Level Points** displays the details of each access level and the points it contains. The default view shows all the access levels.
   - **Access Level Point Groups** display the point groups which contain access points.
3. Customize the view of your report:
   - Modifications include changing the columns, adding filters and grouping data.
4. Click **Print Preview**.
   - If the report looks fine click the **Print** button at the top left corner of the screen
   - To make further modifications to the report click the **Close Print Preview** button and return to step 4.

Access Level Report Fields

These are the field columns that are available when building reports on Access level points.

Column	Description
Point Name	Name of a point within the access level
Time Schedule	Time schedule for the access level
Point Type	Type of point (e.g. Access)
Access Level Name	Name of the access level
Point Number	Number of a point within the access level
Unit Number	Number of the ACC the point belongs to
FLN Number	Number of the FLN the point is on
Device Number	Number of the device the point belongs to
Unit Name	Name of the ACC the point belongs to
FLN Name	The Name of the FLN the point is on
Device Name	The Name of the device the point belongs to

7.1.2.5 Access Groups

The Access Groups category displays the details of access groups as either points or levels.

Generating an Access Groups report

▷ View the section Customizing Views [→ 114] for more details on formatting your report.

1. Expand the **Access Groups** item from the **Navigation** Pane.
2. Choose either **All Access Groups, Access Group Points,** or **Access Group Levels**.
   - **All Access Groups** displays a list of the access group names.
   - **Access Group Points** displays the details of each access group and the points it contains. The default view shows all access groups.
   - **Access Group Levels** displays the access groups and the access levels they contain. The default view shows all the access groups.
3. Customize the view of your report:
   - Right Click and select **Customize View**,
   - Suggested modifications include changing the columns, adding filters and grouping data.
4. Click **Print Preview.**
   - If the report looks fine, click the **Print** button at the top left corner of the screen.
   - To make further modifications to the report click the **Close Print Preview** button and return to step 4.

Access Group Report Fields

These are the field columns that are available when building reports on Access level points.

Column	Description
Point Name	Name of a point within the access group
Point Type	Type of point (e.g. Access)
Access Group Name	Name of the access group
Point Number	Number of a point within the access group
Unit Number	Number of the ACC the point belongs to
FLN Number	Number of the FLN the point is on
Device Number	Number of the device the point belongs to
Unit Name	Name of the ACC the point belongs to
FLN Name	Name of the FLN the point is on
Device Name	Name of the device the point belongs to

7.1.2.6 Workgroups

The Workgroups category generates reports that display all the current work groups and any additional details about those workgroups that you need.

Generating a Workgroups report

▷ View the section Customizing Views [→ 114] for more details on formatting your report.

1. Expand the **Workgroups** item from the **Navigation** Pane.
2. Select **Workgroup Details**.
3. Customize the view of your report:
   – Right Click and select **Customize View**.
   – Suggested modifications include changing the columns, adding filters and grouping data.
4. Click **Print Preview**.
   – If the report looks fine, click the **Print** button at the top left corner of the screen.
   – To make further modifications to the report, click the **Close Print Preview** button and return to step 4.

Workgroup Report Fields

These are the field columns that are available when building reports on Work Groups.

Column	Description
Workgroup Name	Name of the work group.
Workgroup Type	Type of the work group (e.g. Visitor, Department, Contractor)
Workgroup Status	The status of the work group (e.g. Void, Valid)
Primary Contact Name	Name of the primary contact for the work group
Primary Contact Title	Title of the primary contact for the work group
Primary Contact Address	Address of the primary contact for the work group
Primary Contact Phone	Phone number of the primary contact for the work group
Primary Contact Fax	Fax number of the primary contact for the work group
Primary Contact Pager	Pager number of the primary contact for the work group
Secondary Contact Name	Name of the secondary contact for the work group
Secondary Contact Title	Title of the secondary contact for the work group
Secondary Contact Address	Address of the secondary contact for the work group
Secondary Contact Phone	Phone number of the secondary contact for the work group
Secondary Contact Fax	Fax number of the secondary contact for the work group
Secondary Contact Pager	Pager number of the secondary contact for the work group
Access Privileges	Access privileges assigned to the workgroup
Partition Group	Determines whether the workgroup is a Partition group

Note that the Workgroup name (not Workgroup ID) is used as a report filter. If the name of a workgroup is changed, the report includes events related to the new name only. Selecting Workgroup ID as report filter will not display the correct result.

7.1.2.7 Cardholders

The cardholder category handles all the card related reports. It has some default views that filter out visitors and different types of card status.

Generating a Cardholder report

▷ View the section Customizing Views [→ 114] for more details on formatting your report.

1. Expand the **Cardholders** item from the **Navigation** pane.
2. Select one of the **Cardholder, Visitor** or **Cardholder access reports**.
3. Customize the view of your report:
   – Right Click and select **Customize View**.
   – Suggested modifications include changing the columns, adding filters and grouping data.
4. Click **Print Preview**.
   – If the report looks fine, click the **Print** button at the top left corner of the screen.
   – To make further modifications to the report, click the **Close Print Preview** button and return to step 4.

Cardholder Reports

These are the field columns that are available for reports in the Cardholder category.

Report	Description
All Cardholders	All cardholders who are not visitors.
Valid Cardholders	Valid cardholders who are not visitors.
Invalid Cardholders	Void or expired cardholders who are not visitors.
All Visitors	All visitors in the system.
Valid Visitors	All valid visitors.
Invalid Visitors	Void or expired visitors.
Cardholders – Access Policies	Listing of cardholder access policies.
Cardholders Point Concise	Listing of cardholder access and point groups they have access to.
Cardholder Point Detail	Listing of the points the cardholder has access to.
Cardholder Filtered Point Access	List of cardholder details, that can be filtered by Card Number, or by Point Name.
Cardholders Last Known Location	List of all cardholders and their last known location.
Cardholders Offline Access Details	List of the cardholders configured with Offline Access privileges and their details
Cardholder All Fields	Lists all the cardholder fields.
Cardholders with images	Lists all cardholders that have an image.
Cardholders with no images	Lists all cardholders that don’t have an image.
All Cards	Lists all the cards configured to a cardholder
Cardholders Work Groups	Lists all the cardholders assigned to workgroups
Inactive Cards – 30-Day Threshold	Lists all the inactive cards in within a 30-day threshold
Card – Last Used Day	Lists all cardholders and displays their last location and when they last used their card.

Cardholder Report Fields

These fields are available when building reports on Cardholders.

To view these fields, select a report under **Cardholders** and then click the **Field Chooser** button on the top horizontal menu bar.

Column	Description
Card Number	Card number of the cardholder. The leading 0 of the Card Number is not displayed in the report.
First Name	First name of the cardholder
Last Name	Last name of the cardholder
Start Date	Defines the first day the card can be used.
End Date	Defines the last day the card can be used.
Card Status	Current status of the card (e.g. Void, Valid)
Work Group Name	Work group the cardholder is a part of
Workgroup Description	The description of the workgroup.
Workgroup Status	The status of the workgroup, either Void or Valid
Employee Number	Employee number of the cardholder
Title	Title of the cardholder; for example Mr or Mrs.
Date Of Birth	Cardholder’s date of birth
Address	Address of the cardholder
Payroll Number	A number for the cardholder that corresponds to your Payroll system.
Phone	Telephone number for the cardholder
Mobile	Mobile telephone number for the cardholder
Mobile Service Provider	Mobile service provider used for the cardholder
Pager	Pager number for the cardholder.
Pager Service Provider	Pager service provider used for the cardholder
Email	Cardholder’s email address
Use Email	Checkbox that determines whether the cardholder appears in the list of possible recipients for a Message Forwarding task
Car Rego 1	Registration number of the cardholder’s primary car.
Car Model 1	Model number of the cardholder’s primary car.
Car Color 1	Color of the cardholder’s primary car.
Car Rego 2	Registration number of the cardholder’s second car.
Car Model 2	Model number of the cardholder’s second car.
Car Color 2	Color of the cardholder’s second car.

Column	Description
Credential Profile	Credential Profile of the card/s assigned to the cardholder
Fingerprint Captured	Specifies if the cardholder’s fingerprint has been captured.
Fingerprint Encoded	Specifies if the cardholder’s captured fingerprint has been encoded.
WG Access Control Assignment	Specifies the Workgroup for access control assignment
WG Anti-Passback Group	Specifies the workgroup being used for the cardholder’s anti-passback
WG Partition Group	Specifies the partition workgroup configured for the cardholder.

Visitor Reports Fields

These are the field columns that are available when building reports on Visitors. To view these fields, select a visitor report under Cardholders and then click the Field Chooser button on the top horizontal menu bar.

Column	Description
Card Number	Card number of the visitor
First Name	First name of the visitor
Last Name	Last name of the visitor
Start Date	Defines the first day the card can be used.
End Date	Defines the last day the card can be used.
Issue Time	The time when the visitor card was issued
Return Time	Time when the visitor card was returned
Sponsor First Name	First name of the visitor’s sponsor
Sponsor Last Name	Last name of the visitor’s sponsor
Company	Company that the visitor is from
Visitor Card Status	Status of the visitor card (e.g. Void, Issued)
Card Status	Current status of the card (e.g. Void, Valid)
Work Group Name	Work group of the visitor
Workgroup Description	The description of the workgroup.
Workgroup Status	The status of the workgroup, either Void or Valid
Access Group Name	Access group assigned to the visitor
Employee Number	Employee number of the visitor
Title	Title of the visitor; for example Mr. or Mrs.
Date Of Birth	Visitor’s date of birth
Address	Address of the visitor
Payroll Number	A number for the visitor that corresponds to your Payroll system.
Phone	Telephone number for the visitor
Mobile	Mobile telephone number for the visitor
Mobile Service Provider	Mobile service provider used for the visitor r
Pager	Pager number for the visitor.
Pager Service Provider	Pager service provider used for the visitor

Column	Description
Email	Visitor’s email address.
Use Email	This checkbox determines whether the visitor appears in the list of possible recipients for a Message Forwarding task.
Temp Access Group Name	Temporary access group assigned to the visitor
Credential Profile	Credential Profile of the card/s assigned to the visitor

7.1.2.8 Audit Trail

The audit trail category displays all the possible audit trail reports.

Generating an Audit Trail report

▷ View the section Customizing Views [→ 114] for more details on formatting your report.

1. Expand the **Audit Trail** item from the **Navigation** pane.
2. Select a type of audit trail report.
3. Select the date range of audit trail you wish to view and click **Display**.
4. Customize the view of your report:
   - Right Click and select **Customize View**.
   - Suggested modifications include changing the columns, adding filters and grouping data.

   ⇨ **Note:** The Audit Trail Type filter accepts numerical value only. To know more about which number to enter for a specific Report type, see section Audit Trail Report Types [→ 143].
5. Click **Print Preview**.
   - If the report looks fine, click the **Print** button at the top left corner of the screen
   - To make further modifications to the report click the **Close Print Preview** button and return to step 5.

Audit Trail Reports

The following Audit Trail reports are available.

Report	Description
Audit Trail - All	Report containing all audit trail messages.
Audit Trail - Access	Report containing only audit trail concerning access events.
Audit Trail – Access Cardholder Detail	Report containing only audit trail that involves events related to accessing cardholder information.
Audit Trail – Cardholder Door Access	Report containing only audit trail that involves cardholders entering doors.
Audit Trail - Concise	Similar to All Audit Trail report but has fewer columns.
Audit Trail - Database Change	Report containing only audit trail concerning database changes.
Audit Trail – Image Verification	Report containing only audit trail concerning image verification events.
Audit Trail - Operator Log	Report containing only audit trail concerning operator actions.
Audit Trail – Visitor Access	Report containing only audit trail concerning visitor access events.
Audit Trail – Visitor Card History	Report containing only audit trail concerning visitor card changes.
Audit Trail – Time & Attendance Access	Report containing only audit trail concerning Time & Attendance access.
Audit Trail – Earliest and Latest Access	Report containing only audit trail concerning the earliest and latest access.
Audit Trail – Access Cardholder Detail (Custom Fields)	Report containing only audit trail that involves events related to accessing cardholder information with specific fields.
Audit Trail – Cardholder Changes (Custom Fields)	Report containing audit trail that involves events related to accessing cardholder information with previously defined custom fields.

Audit Trail Columns

These are the field columns that are available when building reports on Audit Trail.

Column	Description
Date Occurred	Date the event occurred at the Unit
Time Occurred	Time the event occurred at the Unit
Date Recorded	Date when SiPass recorded the message.
Time Recorded	Time when SiPass recorded the message.
Location	Location where the event occurred
First Name	First name of the cardholder or operator involved in the event
Last Name	Last name of the cardholder or operator involved in the event
Message	Message containing the details of the event
Server Name	Name of the server where the event originated
Bus	Name of the bus where the event originated
Workgroup	Workgroup associated with the cardholder in the event
Card Number	The card number of the cardholder involved in the event
Anti Passback Area	Anti Passback area involved in the event
Intrusion Area	The intrusion area involved in the event
Unit Number	The number of the Unit involved in the event
Point Number	Number of the point involved in the event
Type	Type of the point involved in the event
Category	Category of the event message
State Id	Id number of the state reported by the event
Audit Trail Type	Type of audit trail event
Date Occurred Server	Date when SiPass received the audit message from the ACC
Time Occurred Server	Time when SiPass received the audit message from the ACC
FLN Number	The number of the FLN involved in the event
Device Number	The number of the Device involved in the event
Card Facility	Facility number associated with the card event
Card Technology	Card technology associated with the card event
Employee Number	Employee number of the cardholder

Audit Trail Report Types

Filter Condition Numerical Value	Report Type Description
0	Undefined
1	Log On / Log Off
2	Comms Actions
3	Server Alarm
4	Alarm Action
5	Database Action
6	Event Task
7	Guard Tour
8	Batch Card Printing
9	Image Verification
10	Pager System
11	Forwarding Message
12	External Message
13	Bus Message
14	Actioning Message
15	DED System
16	External System
17	ACK Message
18	DVR Message
19	Email Message
20	Detailed Database Action

7.1.2.9 Proximity Reports

With the *Proximity Report* feature, SiPass integrated helps you to identify cardholders who were close at one or more locations around the same time. Two types of reports can be generated for this purpose:

- **Proximity Report:** for tracking all the cardholders who used one specific reader at, or after the specified date/time.
- **Extended Proximity Report:** for tracking all the cardholders who accessed any reader(s) (tracked by the initial *Proximity Report*) that a specific employee used after a specific start date/time.

Once a cardholder, or a group of cardholders has been identified and must be isolated, they can be voided. With their card void, the cardholder(s) will need to contact the security desk from where, they can be guided toward the next steps accordingly.

The following Audit Trail Access Type reports provide the option to generate Proximity reports.

- Audit Trail Access
- Audit Trail Access Cardholders Detail
- Audit Trail Cardholder Door Access
- Audit Trail Visitor Access
- Audit Trail - Access Cardholders Detail (Custom Fields)

Nested Proximity Reports

A Proximity Report can also be run from within a Proximity Report. In this case, each proximity report works on the first window’s original information which is passed along to the next one.

For example, Cardholder A (original person being tracked) is selected in the first window, Cardholder B from the second window (result of the first report), Cardholder C in the third window (result of the second report) and so on.

Steps

1. From the audit trail data displayed in a window for an *Audit Trail Access Type Report*, select the desired row entry from which, the proximity report must be run.
2. Right-click to display the menu options.
   – To list all the employees who used a specific reader at or after the specified start date/time, click **Begin Cardholder Proximity Report**
   – To list all the employees who used any reader that a specific employee used after a specific start date/time, click **Begin Extended Proximity Report**
   ⇨ Running either of the two commands generates the proximity records for the selected cardholder(s), beginning from the selected row’s date/time in the Audit Trail data.

Note: The Proximity Report only operates on the visible page in an Audit Trail Access report, so before running the proximity report, if extra pages are detected and the configured page size is less than 300,000, a warning message will be displayed informing the user to increase the report page size.

◈ To void the tracked cardholder(s), right-click a cardholder entry in the proximity report window and click **Reporting Actions > Void Cardholder**

7.1.2.10 APB Areas

The APB Areas category generates reports that display all the current Anti-Passback areas and any additional details that you need.

Generating an APB Area report

▷ View the section Customizing Views [→ 114] for more details on formatting your report.

1. Expand the **APB Area** item from the **Navigation** pane.
2. Select **All APB Areas** or **APB Area Details**.
3. Customize the view of your report:
   – Right Click and select **Customize View**.
   – Suggested modifications include changing the columns, adding filters and grouping data.
4. Click **Print Preview**.
   – If the report looks fine, click the **Print** button at the top left corner of the screen.
   – To make further modifications to the report, click the **Close Print Preview** button and return to step 4.

APB Areas Columns

These are the field columns that are available when building reports based on APB areas.

Column	Description
Area No	The number of the APB area
Cluster	The cluster the APB area is attached to
Name	The name of the APB area
Mode	The mode of the APB area, e.g. Soft Anti-Passback
Capacity	The maximum capacity of the area.
Enforce Capacity	Whether or not the maximum capacity is forced.
Mustering APB Area	Whether this area is a mustering APB area.
Enable Four Eyes	Whether Four Eyes mode is enabled on this area.
Include Cardholder in Sub area	Whether a cardholder in a sub area counts for Four Eyes mode.
Four Eyes Timer	The timer set for Four Eyes enabled mode.
Alarm If No Cardholder	Whether this area raises an alarm when there are no cardholders. This is a Four Eyes option.
Re-Entry Timeout	The timeout delay to allow cardholders to re-enter the area.

Column	Description
Type	The type of point in the APB area.
Point Name	The name of the point inside the APB area.
Unit Name	The name of the unit that the point is on.
Area Name	The name of the ABP area.

7.1.2.11 Intrusion Areas

The Intrusion Areas category generates reports that display all the current Intrusion areas and any additional details that you need.

Generating an Intrusion Area report

▷ View the section Customizing Views [→ 114] for more details on formatting your report.

1. Expand the **Intrusion Areas** item from the **Navigation** pane.
2. Select **Intrusion Area General Details** or **Intrusion Area Point Details**.
   - **General Details** shows basic information about the Intrusion Area.
   - **Point Details** shows the points in the Intrusion Area.
3. Customize the view of your report:
   - Right Click and select **Customize View**.
   - Suggested modifications include changing the columns, adding filters and grouping data.
4. Click **Print Preview**.
   - If the report looks fine, click the **Prin**t button at the top left corner of the screen
   - To make further modifications to the report, click the **Close Print Preview** button and return to step 4.

Intrusion Areas Report Fields

These are the field columns are available when building reports based on Intrusion areas.

Column	Description
Intrusion Area Name	The name of the Intrusion Area
Short Name	The short name of the Intrusion Area, used for intrusion terminals
Point Number	The point number of a point in the Intrusion Area
Time Schedule	The Time Schedule associated with the Intrusion Area
Entry Delay	The delay used when entering the area before raising an alarm. This is so that the user has enough time to disarm the area.
Exit Delay	The delay used when exiting the area before raising an alarm. This allows the user to exit when arming the area.
Type	Type of point included in the Intrusion Area

7.1.2.12 Alarms

The Alarms category contains reports to both display alarm classes and outstanding alarms.

Generating an Alarms report

▷ View the section Customizing Views [→ 114] for more details on formatting your report.

1. Expand the **Alarms** item from the **Navigation** pane.
2. Select the **Alarm Classes** or **Alarm Events Outstanding** type of report:
   - **Alarm Classes** shows all alarm classes and their details
   - **Alarm Events Outstanding** shows outstanding alarms of different types
3. Customize the view of your report:
   - Right Click and select **Customize View**
   - Suggested modifications include changing the columns, adding filters and grouping data.
4. Click **Print Preview**.
   - If the report looks fine, click the **Print** button at the top left corner of the screen
   - To make further modifications to the report, click the **Close Print Preview** button and return to step 4.

Alarms Class Report Fields

These are the field columns that are available when building reports based on Alarms.

Column	Description
Alarm Class Name	Name of the Alarm Class
Type	Type of Alarm Class
Priority	The priority assigned to the Alarm Class
Restorable Alarm	Whether the Alarm Class is Restorable or not
Timeout	The timeout of the Alarm Class before it re-alarms
Alarm Instruction File	The instruction file associated with the Alarm Class
Siren Sound File	The siren sound file that will play when this Alarm Class is triggered
Status	The status of the alarm state included in the Alarm Class
Description	The description of the alarm state included in the Alarm Class
Alarm or Restore	Lists whether the state included in the Alarm Class is an alarm or restore type
Symbol	The symbol associated with the alarm state included in the Alarm Class.

Alarms Events Outstanding Report Fields

These are the field columns that are available when building reports based on Alarms Events Outstanding.

Column	Description
Alarm on Bus	The Bus that is under alarm.
Alarm on Point Group	The Point Group that is under alarm.
Alarm on Point	The Point that is under alarm.
Alarm on Unit	The Unit that is under alarm.
Date Occurred	The date that the alarm occurred
Time Occurred	The time when the alarm occurred
Count	The number of times the alarm has occurred
Priority	The priority of the alarm that has occurred
Status	The current status of the alarm

7.1.2.13 Site Plans

The Site Plans report gives a list of all available site plans.

Generating a Site Plan report

1. View the section Customizing Views [→ 114] for more details on formatting your report.
2. Expand the **Site Plans** item from the **Navigation** pane.
3. Select the Site Plans report.
4. Customize the view of your report:
   – Right Click and select **Customize View**.
   – Suggested modifications include changing the columns, adding filters and grouping data.
5. Click **Print Preview**.
   – If the report looks fine, click the **Print** button at the top left corner of the screen.
   – To make further modifications to the report, click the **Close Print Preview** button and return to step 4.

7.1.2.14 Event Tasks

The Event Tasks category contains reports to both display controller based and host based event tasks.

Generating an Event Task report

▷ View the section Customizing Views [→ 114] for more details on formatting your report.

1. Expand the **Event Tasks** item from the **Navigation** pane.
2. Select **Controller Event Tasks** or **Host Event Tasks**.
3. Customize the view of your report:
   - Right Click and select **Customize View**.
   - Suggested modifications include changing the columns, adding filters and grouping data.
4. Click **Print Preview**.
   - If the report looks fine, click the **Print** button at the top left corner of the screen
   - To make further modifications to the report, click the **Close** button and return to step 4.

Controller Event Tasks Report Fields

These are the field columns that are available when building reports based on Controller Event Tasks.

Column	Description
Event Task	The name of the Event Task
Time Schedule	Time Schedule associated with the Event Task
Trigger Number	Number of triggers used in the Event Task
Trigger Type	The type of trigger used in the Event Task
Trigger Controller	The Controller associated with the trigger used in the Event Task
Trigger Source	The source of the trigger used in the Event Task
Trigger State	The state of the trigger used in the Event Task
Trigger Data	The data used for the trigger in the Event Task
Logical Operator	The logical operator joining the two triggers
Effect Type	The type of effect as a result of the Event Task
Effect Controller	The controller associated with the effect of the Event Task
Effect Target	The target associated with the effect of the Event Task
Effect Message	The AT Message specified with the effect of the Event Task
Effect Command	The command used by the effect of the Event Task
Effect Data	The data required by the effect of the Event Task
Effect Delay	The delay before the effect happens

Host Event Tasks Report Fields

These are the field columns that are available when building reports based on Host Event Tasks.

Column	Description
Event Task	The name of the Event Task
Time Schedule	Time Schedule associated with the Event Task
Trigger Source	The source type of the Event Task trigger
Trigger Location	The location of the Event Task trigger
Trigger State	The required state of the Event Task trigger
Trigger Date Occurred	The required date of the Event Task trigger
Trigger Time Occurred	The required time of the Event Task trigger
Additional Criteria Source	The source of an additional Event Task trigger
Additional Criteria Value	The required value of an additional Event Task trigger
Effect Target	The target type of the Event Task effect
Effect Location	The location of the Event Task effect
Effect Command	The command used in the Event Task effect
Effect Data	The required data for the Event Task effect
Message	The message displayed in the Audit Trail

The e-mail containing the report is sent in the following format:

- The e-mail Title (Subject) contains the text entered in the **Message** field on the *Host Event Task* dialog in SiPss integrated Configuration Client.
- The attachment to the e-mail is named the same as the name of the report for which, the Host Event Task has been created.

7.1.2.15 Guard Tour

This category contains reports about Guard Tours.

Generating a Guard Tour report

▷ View the section Customizing Views [→ 114] for more details on formatting your report.

1. Expand the **Guard Tour** item from the **Navigation** pane.
2. Select a report for either **Active Tours or Normal Tours**.
3. Customize the view of your report:
   – Right Click and select **Customize View**.
   – Suggested modifications include changing the columns, adding filters and grouping data.
4. Click **Print Preview**.
   – If the report looks fine, click the **Print** button at the top left corner of the screen.
   – To make further modifications to the report, click the **Close Print Preview** button and return to step 4.

Guard Tour Report Fields

These are the field columns that are available when building reports based on Guard Tours.

Column	Description
Tour Name	Name of the Guard Tour
Guard Name	Guard assigned to the tour
Tour Type	The type of tour, Ordered or Unordered
Total Expected Time	The total time expected for the tour
Total Tolerance Time	The total tolerance time allowed for the tour
Tour Stop Name	The name of a stop in the tour
Point Number	The number of a point included in the tour
Interval Time	The time expected between points in the tour
Tolerance Time	The tolerance time allowed between points in the tour
Sequence	The order of points in the tour
Enabled	Whether the tour is enabled or not

7.1.2.16 Holidays

The Holidays category contains reports about the defined Holidays in the system.

Generating a Holidays report

1. View the section Customizing Views [→ 114] for more details on formatting your report.
2. Expand the **Holidays** item from the **Navigation** pane.
3. Select **System Defined Holidays**.
4. Customize the view of your report:
   - Right Click and select **Customize View**.
   - Suggested modifications include changing the columns, adding filters and grouping data.
5. Click **Print Preview**.
   - If the report looks fine, click the **Print** button at the top left corner of the screen.
   - To make further modifications to the report, click the **Close** button and return to step 4.

Holidays Report Fields

These are the field columns that are available when building reports based on Holidays.

Column	Description
Holiday Name	Name of the Holiday
Holiday Date	The date when the Holiday occurs
Applicable Unit	The Unit that the Holiday affects

7.1.2.17 Elevators

The Elevators category contains reports about the defined floors and banks in the system.

Generating an Elevator report

▷ View the section Customizing Views [→ 114] for more details on formatting your report.

1. Expand the **Elevators** item from the **Navigatio**n pane.
2. Select the required report type from the following:
   - **Elevator Floor Details**
   - **Elevator Bank Details**
   - **Destination Control Elevator Readers**
   - **Elevator Controller Details**
3. Customize the view of your report:
   - Right Click and select **Customize View.**
   - Suggested modifications include changing the columns, adding filters and grouping data.
4. Click **Print Preview**.
   - If the report looks fine, click the **Print** button at the top left corner of the screen.
   - To make further modifications to the report, click the **Close Print Preview** button and return to step 4.

Elevators Report Fields

These are the field columns that are available when building reports based on Elevators.

Column	Description
Alarm Class	The alarm class assigned to the floor
Bank Name	The name of the elevator Bank
Component Type	Component Type used in Elevator controller, including LOP/COP/DSCT, in which the reader can be used as a Provision Reader
Certificate Thumbprint	The thumbprint of the certificate used for message encryption between SiPass integrated and Elevator controller
Comms Reporting ACC	The ACC used for audit trail reporting
Elevator Controller	The gateway responsible for communication with ACC
Elevator Component	Components related with thyssenkrupp Elevator Controller
Elevator Name	Name of the Elevator
Elevator Type	The type of Elevator – thyssenkrupp or Generic
Floor Name	The name of the floor
Input Point Name	The input point assigned to the floor
Output Point Name	The output point assigned to the floor
Poll Period (sec)	The time for polling between the controller and the ACC
Reader Name	The name of the reader assigned to the elevator
Response Max Time (sec)	The time for getting a response from the controller
Rise Number	The rise number of the floor
Time Schedule	The time schedule for the floor
Unit Name	The name of the unit the bank is attached to
URL	The Universal resource Locator (URL) to access the elevator controller

7.1.2.18 Operators

The Operators category contains reports about the operators and operator groups in the system.

Generating an Operator report

▷ View the section Customizing Views [→ 114] for more details on formatting your report.

1. Expand the **Operators** item from the **Navigation** pane.
2. Select a report from the list.
3. Customize the view of your report:
   – Right Click and select **Customize View**.
4. Suggested modifications include changing the columns, adding filters and grouping data.
5. Click **Print Preview**.
   – If the report looks fine, click the **Print** button at the top left corner of the screen.
   – To make further modifications to the report, click the **Close Print Preview** button and return to step 4.

Operators Reports

These are the reports available for operators.

Column	Description
Operator Details	Shows details about the operators in the system
Operators – System Function Access	Lists the operators and their System Function access
Operators – Point Group Access	Lists the operators and their Point Group access
Operators – Unit Group Access	Lists the operators and their Unit group access
Operators – FLN Group Access	Lists the operators and their FLN group access
Operators – Device Group Access	Lists the operators and their Device Group access
Operators – Work Group Access	Lists the operators and their Work Group access
Operators – Floor Plans Access	Lists the operators and their Floor Plans access
Operator Groups – System Function Access	Lists the operator groups and their System Function access
Operator Groups – Point Group Access	Lists the operator groups and their Point Group access
Operator Groups – Unit Group Access	Lists the operator groups and their Unit group access
Operator Groups – FLN Group Access	Lists the operator groups and their FLN group access
Operator Groups – Device Group Access	Lists the operator groups and their Device Group access
Operator Groups – Work Group Access	Lists the operator groups and their Work Group access
Operator Groups – Floor Plans Access	Lists the operator groups and their Floor Plans access
Operator Groups – Lockout Status	Lists the operator groups and whether they are locked out or not.

Operators Report Fields

These are the field columns that are available when building reports based on Operators.

Column	Description
User Name	User Name of the operator
Last Name	Last name of the operator
First Name	First name of the operator
Expiry Date	Expiry date of the operator
Operator Group	The operator group being referred to
Lockout Status	Whether the operator or operator group is locked out
System Function Accessible	The available system functions
Privilege	The privilege assigned to the function, for example create, edit, delete.
Group Accessible	The group that is accessible, can be a point group, unit group etc depending on the report
Workgroup Accessible	The workgroup that is accessible
Accessible Plans	Site Plans that are accessible

7.1.2.19 Database Analysis

The Database Analysis category contains reports that display additional data about the database.

Generating a Database Analysis report

▷ View the section Customizing Views [→ 114] for more details on formatting your report.

1. Expand the **Database Analysi**s item from the **Navigation** pane.
2. Select the **General** or **Bus** report.
3. Customize the view of your report:
   – Right Click and select **Customize View**.
   – Suggested modifications include changing the columns, adding filters and grouping data.
4. Click **Print Preview**.
   – If the report looks fine, click the **Print** button at the top left corner of the screen.
   – To make further modifications to the report, click the **Close Print Preview** button and return to step 4.

Database Analysis Report Fields

These are the field columns that are available when building reports based on Database Analysis.

Column	Description
SiPass Version	The version of SiPass integrated installed
SiPass Build Date	The build date of the SiPass integrated installation
SiPass Description	A brief date and description of the build
Employee Count	Total number of cardholders
Operator Count	Total number of operators
Minimum Card Number	Lowest card number used
Maximum Card Number	Highest card number used
Time Schedule Count	Total number of time schedules
Event Task Count	Total number of event tasks
Area Count	Total number of anti Passback areas
Alarm Class Count	Total number of alarm classes
Holiday Count	Total number of holidays
Unit Count	Total number of units
Bus Count	Total number of buses
Bus Name	Name of the bus
Bus Type	Type of bus
Number of Units	Number of units connected to the bus

7.1.2.20 Mustering

The Mustering category contains the mustering report.

Generating a Mustering report

▷ View the section Customizing Views [→ 114] for more details on formatting your report.

1. Expand the **Mustering** item from the **Navigation** pane.
2. Select **Mustering** Report.
3. Customize the view of your report.
4. Right Click and select **Customize View**.
   – Suggested modifications include changing the columns, adding filters and grouping data.
5. Click **Print Preview**.
   – If the report looks fine, click the **Print** button at the top left corner of the screen.
   – To make further modifications to the report, click the **Close Print Preview** button and return to step 4.

Mustering Report Fields

These are the field columns that are available when building a mustering report.

Column	Description
Workgroup Name	The name of the workgroup
Area Name	The Anti-passback area the cardholder is in
Last Name	The last name of the cardholder
First Name	The first name of the cardholder
Card Number	The card number of the cardholder
Employee Number	The employee number of the cardholder
Visitor	Indicates whether the cardholder is a visitor or not
Point Name	The name of the point the cardholder was last at

7.1.2.21 Credential Profiles

The Credential Profile category contains the Credential Profile report.

Generating a Credential Profile report

▷ View the section Customizing Views [→ 114] for more details on formatting your report.

1. Expand the **Credential Profile** item from the **Navigation** pane.
2. Select a **Credential Profile** report.
3. Customize the view of your report:
   – Right Click and select **Customize View**.
   – Suggested modifications include changing the columns, adding filters and grouping data.
4. Click **Print Preview**.
   – If the report looks fine, click the **Print** button at the top left corner of the screen
   – To make further modifications to the report, click the **Close Print Preview** button and return to step 4.

Credential Profile Report Fields

These are the field columns that are available when building a Credential Profile report.

Column	Description
Credential Profile	The Credential Profile of the card
Facility Code	The Facility Code of the card
Card Technology	The Card Technology of the card
Pin Mode	The PIN operation mode configured for the card
Pin Digits	The number of digits for the PIN of the card
Base Profile	The Base Profile of the card

7.1.2.22 Advanced Security Programming

The Virtual Components category contains the Virtual Components report.

Generating a Virtual Components report

▷ View the section Customizing Views [→ 114] for more details on formatting your report.

1. Expand the **Advanced Security Programming** item from the **Navigation** pane.
2. Select a report from the list.
3. Customize the view of your report:
   – Right-click and select **Customize View**.
4. Suggested modifications include changing the columns, adding filters and grouping data.
5. Click **Print Preview**.
   – If the report looks fine, click the **Print** button at the top left corner of the screen.
   – To make further modifications to the report, click the **Close Print Preview** button and return to step 4.

ASP Reports

These are the reports available for operators.

Column	Description
Flags	Displays details about virtual flags in the system
Counters	Displays details about virtual components in the system
Timers	Displays details about virtual timers in the system
Activity List	Displays all activities in the system
Activity Detais	Displays details about all activities in the system

ASP Components Profile Report Fields

These are field columns that are available when building reports based on Virtual Components.

Column		Description
Virtual Flags	Name	Displays the name of the virtual flag
	Unit	Displays the name of the unit configured for the virtual flag
	Default Value	Displays the default value of the flag
	Audit Trail Reporting	Specifies the Audit Trail for the flag
	Alarm Class	Specifies the alarm class configured
Virtual Counters	Name	Displays the name of the Virtual Counter
	Unit	Displays the unit configured for the virtual counter
	Default Value	Displays the default value of the counter
	Preset Value	Displays the preset value of the counter
	Max. Value	Displays the maximum value of the counter
	Count Mode	Displays the count mode
	Audit Trail Reporting	Specifies the Audit Trail for the counter
Virtual Timers	Name	Displays the name of the Virtual Timer
	Unit	Displays the unit configured for the virtual timer
	Period	Displays the period for which the timer is configured
	Timer Mode	Displays the mode of the timer
	Audit Trail Reporting	Specifies the Audit Trail for the timer

Activity List	Name	Displays the name of the activity
	Unit	Displays the unit configured for the activity
	Time Schedule	Displays the type of Time Schedule
	Description	Description of the activity
Activity Details	Type	Displays the type of flow
	Point Category	Displays the category configured for the flow
	Point Unit	Displays the point on which the flow is configured
	Point Location	Displays the location of the point
	Activity Name	Displays the name of activity the flow belongs to
	Activity Unit	Displays the unit configured for the flow
	Activity Time Schedule	Displays the type of time schedule of the activity that the flow belongs to

7.1.2.23 Upload

The Upload category contains the Upload report.

Generating a Upload report

▷ View the section Customizing Views [→ 114] for more details on formatting your report.

1. Expand the **Upload** item from the **Navigation** pane.
2. Select **Upload** report.
3. Customize the view of your report.
4. Right-click and select **Customize View**.
   – Suggested modifications include changing the columns, adding filters and grouping data.
5. Click **Print Preview**.
   – If the report looks fine, click the **Print** button at the top left corner of the screen.
   – To make further modifications to the report, click the **Close Print Preview** button and return to step 4.

Upload Report Fields

These are the field columns that are available when building an Upload report.

Column	Description
External System	The External system that is integrated with SiPass. (For example, SALTO)
Correlation ID	Details the ID of the object in the conflict
Conflict Description	Description of the conflict arising at the time of uploading with the external system

7.1.2.24 Venue

The Venue category contains the Venue report.

Generating a Venue report

▷ View the section Customizing Views [→ 114] for more details on formatting your report.

1. Expand the **Venue** item from the **Navigation** pane.
2. Select a report.
3. Customize the view of your report.
4. Right-click and select **Customize View**.
   - Suggested modifications include changing the columns, adding filters and grouping data.
5. Click **Print Preview**.
   - If the report looks fine, click the **Print** button at the top left corner of the screen.
   - To make further modifications to the report, click the **Close Print Preview** button and return to step 4.

Venue Report Fields

These are the field columns that are available when building an Venue report.

Column		Description
Venues	**Name**	Displays the name of the venue.
	Description	Displays a description of the venue.
Venue Access Policies	**Name**	Displays the name of the venue
	Description	Displays the description of the venue.
	Access Type	Displays the access type configured to the venue.
	Access Name	Displays the access name for the venue.
	Time Schedule	Displays the Time Schedule configured for the venue.
	Control Mode	Displays the control mode configured for the venue.
	Arming Rights	Displays the arming rights configured for the venue.
Venue Bookings	**Venue Name**	Displays the name of the booked venue.
	Booking Name	Displays the venue booking name.
	Description	Displays the description of the venue booking
	Start Time	Displays the Start Time of the venue booking.
	End Time	Displays the End Time of the venue booking.
Venue Booking Participants	**Venue Name**	Displays the name of the booked venue.
	Booking Name	Displays the venue booking name.
	Description	Displays the description of the venue booking.
	Type	Displays the venue booking participant.
	First Name	Displays the first name of the venue booking participants.
	Last Name	Displays the last name of the venue booking participants.
	Card Number	Displays the card number of the venue booking participants.

7.2 Scheduled Reporting

Reports within SiPass Reporting can be automatically generated and exported with an event task. This allows you to perform regular reporting without the ongoing manual effort. The host based events and reports can be scheduled in the SiPass integrated Configuration Client.

To view the Host Based Event Reports

◈ In the **Predefined Reports folder, go to Event Tasks and double click Host Event Tasks**.

⇨ The *Host Event Tasks* dialog is displayed on right hand side listing the default system function tasks along with any tasks scheduled in the Configuration Client.

7.3 Log Book Reports

The Log Book offers an integrated reporting tool to prepare daily activity reports by operators. At some sites, the preparation and submission of a Log Book report is mandatory, and in some circumstances, may even be a statutory requirement for operators monitoring the activities of a site.

Creating a Log Book Report is very similar to creating Database or Audit Trail reports The process of creating a report is roughly a three-step operation, but the exact number of steps required will depend upon how complex a report you want to create.

Step 1: Ordering Report Records

1. Expand the **Predefined Reports** folder list in navigation pane on left.
2. Double click **Log Book > Log Books**.
3. In the **Current View box on left, complete the** details.
   - **Start Date**: Contains two fields - **Date** and **Time** - which determine the oldest Time Schedule from which the Log Book information will be selected.
   - **Stop Date**: Contains two fields - **Date** and **Time** - which determine the most recent Time Schedule from which the Log Book information will be selected.
4. In the Log Books dialog on the right hand side, select whether the report will be sorted by **Operator Name** or **Subject** or **Description** or **Date/Time Occurred**.
5. Select the sort function to apply to this field by enabling the corresponding radio button. Choosing either **Ascending** or **Descending** will cause an icon to appear next to the selected field, indicating that records will be sorted in alphabetical or reverse alphabetical order according to your choice of radio button. Please note that the sort function does not have to be used.
   - **None**: When enabled, does not use the selected field to sort the information.
   - **Ascending**: When enabled, sorts the information by the specified field, in ascending order.
   - **Descending**: When enabled, sorts the information by the specified field, in descending order.

Step 2: Creating a Query

By creating a query, you can filter the records that will appear in the report, based on the criteria you select. If you do not wish to filter the records displayed in the report, simply proceed to step 3.

1. Choose the first constraint to be placed on the report information by selecting a field from the list.
2. Select the specific attribute to be used as the constraint. For example, if you chose to create a query based on operators, you may select the specific operator from the **Operator Name** drop-down list.
3. Select the **Query** filter to apply, from the **Filter** list. To change the filter, choose the drop down arrow and select a new filter from the list.
4. Choose **Add**. The specified data query will be added to the **Query** box.
5. If you want to enter more than one query, you can choose the way in which multiple queries are handled, by selecting the correct operand between each.
   - **And**: When selected, the report will display all results that match the combined queries entered, as if they were a single query. Using the AND function to filter between criteria belonging to the same field type (eg: points) will return a blank report).
   - **Or**: When selected, the report will display all results that match each query entered, as if they were separate queries.
6. For more complex reports, you can group queries together, using the ( ) button

⇨ If you select the **Remember Settings** checkbox before exiting the dialog or previewing the report, the current query will load when you next open the *Log Book Report* dialog.

Step 3: Printing, Previewing or Exporting your Report

Once you have selected the information on which to base your report, chosen the order in which records are to be displayed and created your query, you are ready to print, preview, or export your report.

7.3.1 Log Book Report Filters

The table below explains the available Log Book report filters.

Filter	Description
Equals	The report will display only those records that exactly match (except case) the entered criteria.
Not Equals	The report will display all the records that do not exactly match the entered criteria.
Like	Allows you to use a wild card in the query. For example, an entry of “Like %t%” for a cardholder’s First Name, would result in a report displaying all cardholders whose first name contains the letter “t”. You may also use “[]” to find a single character in a specified range (for example, “like [\]” ¬would search for the character \. The standard Windows wild card “*” does not work in this instance.
Less than	This query has two sub-functions. The first applies to numerical data, where the report displays all records that are numerically smaller than the entered data. The second applies to alphabetical data, where the report displays all records that alphabetically precede the entered criteria.
Less than or equal to	A combination of both the Equals and Less than query filters.
Greater than	This query has two sub functions. The first applies to numerical data, where the report displays all records that are numerically larger than the entered data. The second applies to alphabetical data, where the report displays all records that alphabetically follow the entered criteria.
Greater than or equal to	A combination of both the Equals and Greater than query filters.

7.4 Interactive Reports

Interactive Reports are run by the SiPass integrated system when the operator conducts a specific operation. Interactive Reports can be configured to run when adding and saving cardholders, and execute the report's underlying action.

7.4.1 How Does an Interactive Report Work

An operator can create an Interactive Report based on a Watchlist Report. The Watchlist Report should have an action assigned to it. This action will be triggered when the Interactive Report returns a non-empty result after being run.

For the Interactive Reports to be selectable, they must contain at least one parameter in the Filter Conditions. By default, when creating a report, it is configured as a Parameterized Report (every Watchlist column will be added as a parameter in the Filter Conditions by default).

A report that contains at least one **As Parameter** filter condition is considered to be a Parameterized Report.

Basically, the Interactive Report maps fields of a selected Watchlist Report to the fields of the *Cardholder* dialog. The Watchlist Report can have an action assigned to it, like the default Warn User action, for example.

When the user saves a cardholder, the cardholder fields are presented as parameters to the Interactive Report. The Interactive Report will then run using the given cardholder parameters. If the report generates a cardholder/s that matches the configured parameters, the configured action, like Warn User for example, will be executed. This means that the operator can be warned if he/she is editing a cardholder that exists on the Watchlist report.

Similarly, other actions assigned to the selected Watchlist Report can be triggered when the Interactive Report is run.

7.4.2 Configuring an Interactive Report

This section explains how the operator can configure an Interactive Report based on a Watchlist Report.

1. Select **Interactive Reports** from the **Navigation** pane.
2. Double click *Cardholder / Visitor dialogs.*
3. From the **Reports** drop down list, select a specific Watchlist report.
4. From the **Parameters** section that appears below, map the parameters of the existing report to the required fields of the *Cardholder* dialog.
5. Click **Save**.
   ⇨ The configured Watchlist appears under the **Selected List** section.
6. Click **Close**.

Once this configuration is saved, the report is run whenever the *Cardholder* dialog creates a new cardholder, or updates an existing cardholder. During this process, the existing parameter fields of the Watchlist Report are run against the mapped Cardholder dialog fields to check if matches can be found.

For example, an Interactive Report can be created for a Watchlist Report that has the default 'Warn User' action assigned to it.

On running the report, if the Watchlist parameter **First Name** is mapped to the **First Name** field of the *Cardholder* dialog, the Interactive Report checks for matching first names. If matching first names are found, a Watchlist Breach message will be generated when that particular cardholder is created, or their card/s updated.

7.4.3 Removing an Interactive Report

An Interactive Report can be deleted by selecting the report from the **Selected List** section, and clicking **Remove**.

ℹ If an operator wants to delete a Watchlist configured to an Interactive Report, the specific Interactive Report itself must be deleted / removed first.

7.4.4 Creating an Interactive Report during Watchlist Report Creation

The steps required to create an Interactive Report has been discussed in the section Configuring an Interactive Report [→ 169].

Alternatively, an Interactive Report can be generated while creating a new Watchlist Report, as described in the section Field Mapping a Watchlist Report.

8 Image Verification

SiPass integrated allows you to perform image verification on cardholders. This advanced functionality increases the security of your site, by allowing security operators to visually confirm the identity of personnel attempting access.

Image verification can be configured to be mandatory at particular access points, requiring the guard to manually verify identity before allowing access. It can also be configured to allow access according to cardholder access privileges, but automatically take a snapshot of the cardholder to be displayed on a selected monitor.

8.1 Operating Image Verification

Setting an access point's Image Verification mode to "Operator controlled" or "Host Verification" means that when an access card is badged at a reader, the *Image Verification* dialog will appear on the SiPass client. The security operator needs to manually verify that the live image matches the stored database image of the cardholder, before allowing or denying entry.

A cardholder must have access privileges to a point for the Image Verification screen to be displayed upon an access attempt. For example, if a person does not have privileges during a certain Time Schedule, or is using a void card, access will be denied by the hardware controller, and the Image Verification screen will not be displayed.

If an access point's Image Verification mode has been set to "View Only", the *Image Verification* dialog will still appear on screen. However, the dialog will be for viewing and snapshot purposes only. Access will be determined as normal.

An operator must have the appropriate privileges for both Image Verification and the access point, to be able to use the Image Verification dialog to view live images and confirm or deny entry at that point.

Performing Image Verification

1. When an access card is badged at an image verification access point, the *Image Verification* dialog will appear: The stored database photo appears on the left hand side, and the live snapshot appears on the right.
2. If you are satisfied that the live photo matches the database photo, choose **Allow**. The door will unlock and access will be permitted.
3. Otherwise, select the **Deny** button. The door will remain locked and the door controller will reset and wait for the next access attempt.

The door controller will wait a certain amount of time for a response from an operator. During this time, swiping any other card at the reader will have no affect. If there still has not been a response from an operator after this time, the controller will reset and access can be re-attempted. The timeout period can be configured by entering a value into the Host Verify Timeout field of the *Access* tab of the relevant device. The default is 60 seconds.

If an operator has not allowed or denied entry using Image Verification within 30 seconds, an audible alarm will sound. This can be silenced by choosing Silence. This event is not a SiPass alarm.

8.1.1 Operating Image Verification from the Audit Trail

If you have checked the **Save Image Snapshot** checkbox in the *Image Verification* tab of the *Components* dialog, each time an access attempt is made at an access point configured for image verification, a live snapshot of the cardholder will be saved to the database. Both the cardholder's image from the database and the saved snapshot can be viewed from the audit trail.

For example, a guard may observe from the audit trail that a cardholder has entered the site, but may not recall seeing that cardholder when he or she completed the last guard tour. The live snapshot of the access attempt can be recalled from the Audit Trail, to confirm whether that cardholder has indeed entered the site, or someone else has used the card to gain unauthorized access.

Stored snapshots can also be viewed in *Image Verification* reports.

Viewing a stored cardholder image from the Audit Trail

1. Locate the audit trail entry for which you wish to view a stored database image of a cardholder. The entry must be an access attempt by a valid cardholder.
2. Right click on the entry. A menu will appear.
3. Select **View** Image.
4. Choose the *Imaging* tab to see the stored database image of the cardholder.

Viewing a live Snapshot from the Audit Trail

1. Locate the audit trail entry for which you wish to view a live image. The audit trail entry must be an access attempt by a valid cardholder, at a point configured for image verification.
2. Right click on the entry. A menu will appear.
3. Select **View Snapshot**.
   - ⇨ The *Image Verification* dialog will appear, displaying only the live snapshot of the access attempt made at that point.
4. Choose **Close**.

9 Biometric Integration

9.1 Introduction

The Bioscrypt functionality allows operators to capture fingerprint templates and encode the fingerprint template into the smart card during enrollment.

An optional feature allows operators to capture and store the fingerprint template into the SiPass integrated database. This feature is configurable based on the individual country regulations regarding fingerprint storage.

This functionality allows operators to encode fingerprint templates as cardholder data into the smart card, while enrolling the card at the same simultaneously.

It supports the 1K and 4K Mifare cards, and the 2K, 4K and 8K DESFire Card Technology.

It utilizes the Triple DES (also known as 3DES), mechanism for encryption.

The Bioscrypt reader can be connected to RIM devices (DRI, ERI and SRI) for Access Control.

9.1.1 Prerequisites

Before proceeding to create a Bioscrypt components in SiPass integrated, the operator must ensure that the following prerequisites are available with the SecureAdmin application.

- Install the Server and Client of the **SecureAdmin version 4.1.9**.

ℹ After the SecureAdmin application is installed, the documentation for the application should also be available on your PC. Please refer the same for information on how to use the application.

- Register the **BIOSCRYPT V-Station** reader in SecureAdmin. Please refer the Secure Admin documentation for detailed information on how to register.
- Configure the **Wiegand** output for the BIOSCRYPT V-Station reader. This can be done through the following steps:

1. Navigate through **Device Settings** to locate the *Wiegand* tab of the BIOSCRYPT V-Station device.
2. In the *Miscellaneous Settings* section of this tab, check the **Activate Wiegand Output** checkbox.
3. Select **Always Output** in the adjacent dropdown field.
4. Next, operators can choose to configure either a Mifare Classic or Mifare DESFire card template. For details, refer the two sections that follow.
5. Click the **Wiegand Output Settings** button. Set **Verification Output.**
6. Proceed to create a **Site Key** to authenticate the Mifare Smart Card. A detailed guide for the same can be found in the **SecureAdmin** documentation.

   ⇨ While enrolling Mifare cards for a site, set the 'Key B' for Read/Write operations or select the **Use ESI Site Key encryption** option to prevent the default Key A being assigned to all the cards.

7. Set the **Site Key** and **Smartcard Layout** on the BIOSCRYPT V-Station reader. Refer the SecureAdmin documentation to set the Site Key.
8. Open the **SmartCard Device Manager** and ensure that the Use Wiegand String option is ticked for every device integrated into the system. **Overwrite Card Wiegand String** should also be ticked for Mifare DESFire card.

To configure the Mifare Classic card template:

▷ The custom format is used to send the **CSN** number of cards that use the Mifare Classic card technology.

1. Click the **Custom Wiegand Settings** button, and configure the template in the *Weigand Format* dialog displayed.
2. Enter the **Name** of the configuration.
3. Enter **Length** as 40.
4. In the **Weigand ID** settings, Enter **Start Position** as 0, **Length** as 32, **Heart Beat Value** as 0.
5. In the **User fields** settings, specify the following information:
   - Name – Successful code
   - Start Position – 32
   - Length – 8
   - Success Value – 0
   - Failure – 250
6. Click **Apply**.

ℹ This configuration is required only if the system is required to configure the Mifare Classic card.

To configure the Mifare DESFire card template:

▷ The Card Type has to be set to DESFire to configure a DESFire card. To select the card type as DESFire, perform the following steps:

1. Click the **Smart Card** tab from **SecureAdmin** to open the *Smart Card Device Manager dialog.*
2. Select **DESFire Smart Card** from the *Smart Card Type pop-up.*

▷ The custom format is used to send the UID number of cards that use the Mifare DESFire card technology.

1. Click the **Custom Wiegand Settings** button, and configure the template in the *Weigand Format* dialog displayed.
2. Enter the **Name** of the configuration.
3. Enter **Length** as 72.
4. In the **Weigand ID** settings, Enter **Start Position** as 0, **Length** as 64, **Heart Beat Value** as 0.
5. In the **User fields** settings, specify the following information:
   - Name
   - Start Position -64
   - Length-8
   - Success Value-0
   - Failure-250
6. Click **Apply.**

This configuration is required only if the system is required to configure the Mifare DESFire Classic card.

In case of L1 readers using Mifare DESFire cards, the Master key should not be modified. If changed, the key will not be read by the L1 reader.

9.2 Creating a Bioscrypt Credential Profile

1. Double click **Credential Profil**e from the left pane to display the Credential Profile dialog.
2. Select the **Base** card profile.
3. Verify if **Bioscrypt Credential** is checked for this profile.
   – **Note**: The Bioscrypt credential checkbox will appear in the *Credential Profile* dialog only after a bioscrypt system bus is created in the *Components* dialog.
4. Click **OK** to save this profile.

9.3 Determining the Bioscrypt / Enrollment Reader Configuration

The Bioscrypt reader and the Enrollment reader can be configured in SiPass integrated for the Bioscrypt functionality. The operators can decide if they require an enrollment reader, apart from the Bioscrypt reader; in which case, they will need to configure an enrollment reader in the *Enrollment Configuration* dialog. The enrollment reader has to be configured to import a Bioscrypt Profile.

The enrollment reader configuration in the remote client must be reconfigured after restoring the SiPass integrated database.

The steps required to configure a Bioscrypt and Enrollment reader in SiPass integrated are explained in the sections that follow.

9.3.1 Configuring the Bioscrypt reader in SiPass integrated

Please note that the configuration explained in this section is client-specific.

Configuring the Bioscrypt Reader in SiPass integrated

1. Select **Options > Enrollment Reader Configuration** on the SiPass integrated main menu.
2. Click the **Add** button.
3. From the **Select Type** drop down list, select **Bioscrypt Reader Configuration**.

Please note that the **Encode** button of the *Cardholder* dialog will be disabled if the Bioscrypt reader configuration is the only card reader added in the

Select Type field of the *Enrollment Reader Configuration* dialog.

4. Tick the **Reading** checkbox if you wish to use the Bioscrypt Reader only to read the card.
5. Or else, tick the **Encoding** checkbox if you wish to use the Bioscrypt Reader to encode the card. Ticking the **Encoding** checkbox ticks the **Reading** checkbox by default.

The options available in the *Fingerprint Enrollment* section of this dialog, determine the various functionalities that can be configured. The table below explains the options.

Configuration Option	Expected Configuration Action
Prompt to encode the fingerprint on card	When this option is ticked, the Bioscrypt device is used to encode the fingerprint template on the card. When this option is un-ticked, the system saves the acquired fingerprint to be stored in the SiPass database.
Use Card Serial Number as Template Identifier	When this option is ticked, the fingerprint template will be identified by the Card Serial Number (CSN) of the card. When this option is un-ticked, the fingerprint template will be identified by the card number given in the *Definition* tab of the *Cardholder* dialog. If no card number was specified, the user is notified that a card number is required to complete the card assignment operation.
Store the fingerprint for encoding later	When this option is ticked, the fingerprint will be saved to the database as part of the enrollment process.

For **Configuration Type A: Card Assignment** – **Prompt to encode the fingerprint on card** and **Use Card Serial Number as Template Identifier** options should be checked.

For **Configuration Type B: Fingerprint Accquisition** – **Use Card Serial number as Template Identifier** and **Store the fingerprint for encoding later** options should be checked.

1. In the *Communication Settings* section of this dialog, do the following:
2. Enter an appropriate value for the Bioscrypt device in the **Device ID** field. The Device ID value for Bioscrypt reader shall match the Device ID value set in the Communication tab of SecureAdmin.
3. Specify the type of connection to the Bioscrypt reader in the **Connect Using** field.
4. Enter the IP address of the Bioscrypt device in the **IP Address** field.
5. Click **Save** to save this configuration.

9.3.2 Configuring an Enrollment Reader for the Bioscrypt functionality

Configuring the enrollment reader for the Bioscrypt functionality

If you wish to use an enrollment reader as part of the Bioscrypt functionality, the reader needs to be configured in the Enrollment Reader configuration dialog.

> The option to use the enrollment reader to read, search and assign cards will be enabled in the *Cardholder* dialog, only when the enrollment reader is configured to the **Reading** mode in the *Enrollment Reader Configuration* dialog. This action ensures that the **Read**, **Assign** and **Read & Search** buttons of the *Cardholder* dialog will be made drop-down buttons, to allow selection of the reader device to be used.

1. Select **Options > Enrollment Reader Configuration** on the SiPass integrated main menu.
2. Click the **Add** button.
3. From the **Select Type** drop down list, select the enrollment reader to be used for this functionality. Options include the *Omnikey CardMan 5×21* and *Omnikey CardMan 5×22* readers both of which can read the Mifare Classic and Mifare DESFire smart cards.
4. Tick the **Reading** checkbox of the **Operation Mode** field.
5. In the **Profile Name** field, select the Bioscrypt profile from the drop down list.
6. Depending on the type of smart card you wish to configure, set the values as below:
   - **Mifare Classic:** Set the **Sector / Application** in the fields.
   - **Mifare DESFire:** Set the **AID / File** in the fields.

   ⇨ **Note:** In case of *Omnikey CardMan 5×22* reader, the AID should be set to the correct AID(hex) format = "000000" to fetch the UID in the Cardholder credential.
7. Select the port to be used for the enrollment reader in the **Port Name** field.
8. Click **Save** to save this configuration.

9.4 Configuring the Bioscrypt profile to a Work Group

This section details the steps required to configure a new workgroup with the Bioscrypt profile.

1. Double click **Work Group** from the left pane to open the *Work Group* dialog.
2. Configure a New Work Group.
3. Click the drop down arrow of the Profile field, and select the Bioscrypt smart card profile created.
4. Click **Save**.

9.5 Types of Bioscrypt Configuration in SiPass integrated

SiPass integrated can be configured to work with the Bioscrypt reader in two ways, each providing a different functionality. A brief explanation of each configuration type follows.

Card Assignment

This configuration type allows operators to use the SiPass integrated interface to select cardholders for whom fingerprints are required. The Bioscrypt reader is then used to obtain the cardholder's fingerprint, and assign a card with fingerprint details written to it.

In this case, the fingerprint template is not saved to the database. In is only saved to the card assigned.

Fingerprint Acquisition

The functionality of this configuration builds on the result of Configuration Type 1, where a cardholder is assigned a card containing their fingerprint information. However, in this type of configuration, SiPass integrated also saves the fingerprint to the database for future use.

9.5.1 Configuration Type A: Card Assignment

Through this configuration, the operator selects a cardholder in SiPass integrated, whose card will then be assigned and written with their fingerprint data using the Bioscrypt reader device. A summary of the configuration stages required for this scenario is detailed below.

Summary of Configuration Stages for Type I

▷ Ensure that you have installed the SecureAdmin client and server software.

▷ Ensure that you have created a Bioscrypt bus in SiPass integrated.

▷ Ensure that you have saved the custom card configuration in SiPass integrated.

1. Configure the Bioscrypt Enrollment Reader in SiPass integrated through the *Enrollment Reader Configuration* dialog. For further information, refer the section Configuring the Bioscrypt Reader for Configuration I [→ 180].
2. Use the *Cardholder* dialog to begin scanning a fingerprint on the Bioscrypt reader, and assigning a card with the fingerprint. For further information, refer the section Assigning Fingerprints and Cards with the Bioscrypt Reader [→ 180].

The sections that follow explain each of these configuration stages in detail.

9.5.1.1 Configuring the Bioscrypt Reader for Configuration I

The Bioscrypt reader can be configured to read and encode the fingerprint template onto a card in this type of configuration, without saving the card template to the database.

◈ Follow the steps described in the section Configuring the Bioscrypt reader in SiPass integrated [→ 176].

ℹ Ensure that **Prompt to encode the fingerprint on card** option is checked on *Enrollment Reader Configuration* dialog.

9.5.1.2 Assigning Fingerprints and Cards with the Bioscrypt Reader

Once operators have created a Bioscrypt bus, and the enrolled a Bioscrypt reader in SiPass integrated, they can proceed to assign cards with fingerprints using the Bioscrypt reader. This is done on the *Cardholder* dialog. The instructions that follow explain this process.

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Cardholder** list item.
   ⇨ The *Cardholder* dialog is displayed.
3. Click the **Assign** drop down button, and select **Assign fingerprint from Bioscrypt reader**. The drop-down appears only if multiple readers have been connected to SiPass integrated.
   ⇨ *Register Card with Fingerprint* dialog will be displayed.
4. Follow the instructions of the dialog to acquire a fingerprint.
5. When a satisfactory fingerprint has been obtained, the *Cardholder* dialog prompts to register the fingerprint with a card.
6. Place the card on the Bioscrypt reader to assign the fingerprint to the card.
   ⇨ The card number will be displayed on the *Cardholder* dialog. And an icon is displayed on the definition tab of the cardholder indicating that fingerprint is on the card.
7. Configure all other required cardholder details.
8. Click **Access Privileges** button, select the access points for the cardholder and click **OK.**
9. Click **Save**.

⇨ As a result of this configuration, the acquired fingerprint gets physically assigned to a card using the Bioscrypt reader. This is also indicated by an icon.

You can inspect the card after acquiring the fingerprint.

◈ In the *Cardholder* dialog, click **Read** drop-down and select **Inspect Bioscrypt Card.** *Read Card* dialog shows up. Place the card on the Bioscrypt reader.

⇨ The Bioscrypt reader reads the card and shows the biometrics stored on the card.

You can verify the card details by doing the following steps:

1. Badge the card on the Bioscrypt reader; follow the instruction on the reader and present fingerprint.
2. If the card is valid then it is notified to the user by an audit trail message which says **Valid**. If the card is invalid then it is notified to the user through an audit trail message which says **Invalid**.

9.5.2 Configuration Type B: Fingerprint Acquisition

This functionality allows the operator to use SiPass integrated to encode a card that has already been assigned fingerprints through the Bioscrypt reader.

A summary of the configuration stages required for this scenario is detailed below.

Summary of Configuration Stages for Type I

- ▷ Ensure that you have installed the SecureAdmin client and server software.
- ▷ Ensure that you have created a Bioscrypt bus in SiPass integrated.
- ▷ Ensure that the Bioscrypt Reader Configuration has been imported for the purpose of configuring the smart card profile.
- ▷ Ensure that a Bioscrypt profile has been configured for a work group. For more information, refer the section Configuring the Bioscrypt profile to a Work Group [→ 179]

Make sure, in the *Enrollment Reader Configuration* dialog, under the

Fingerprint Enrollment section, the **Use Card Serial Number as Template Identifier** is unchecked and **Store the fingerprint for encoding later** option is checked for this configuration.

1. Configure the Bioscrypt Enrollment Reader in SiPass integrated through the Enrollment Reader Configuration dialog. For further information, refer the section Configuring the Bioscrypt Reader for Configuration II. [→ 181]
2. Use the Cardholder dialog to begin scanning a fingerprint on the Bioscrypt reader, and assigning a card with the fingerprint. For further information, refer the section Card Enrollment with Bioscrypt Details.
3. The sections that follow explain each of these configuration stages in detail.

9.5.2.1 Configuring an Enrollment Reader for Configuration II

The Bioscrypt reader must be configured in SiPass integrated. This section details the steps required to do this.

It is important to note that the configuration explained in this section is client-specific.

1. Select **Options** > **Enrollment Reader Configuration** on the SiPass integrated main menu.
2. Click the **Add** button.
3. From the **Select Type** drop down list, select **Profile Reader – OmniKey CardMan 5×21 or OmniKey CardMan 5×22**. Ensure that the **Bioscrypt Reader Configuration** is also added as part of this drop down list. Ensure that the **Encoding** is checked.

Note that on selecting this reader type, the **Encoding** checkbox gets ticked by default and the **Profile** section of this dialog becomes enabled. The *OmniKey CardMan 5×21* and *OmniKey CardMan 5×22*readers are used to read both Mifare Classic and DESFire cards.

4. From the **Profile Name** drop down list, select the card profile to be used for the bioscrypt card enrollment.

5. Depending on the type of smart card you wish to configure, set the values as below:

   – **Mifare Classic:** Set the **Sector / Application** in the fields.
   – **Mifare DESFire:** Set the **AID / File** in the fields.

   ⇨ **Note:** In case of *Omnikey CardMan 5×22* reader, the AID should be set to the correct AID(hex) format = "000000" to fetch the UID in the Cardholder credential.

6. From the **Port Name** drop down list, specify the port name of the card reader.

7. Click **Save** and **Close**.

⇨ The enrollment reader will be now be enrolled in SiPass integrated.

9.5.2.2 Card Enrollment with Bioscrypt Details

Once operators have created a Bioscrypt bus, enrolled the Bioscrypt reader, and imported a Bioscrypt Profile in SiPass integrated, they can proceed to assign cards with fingerprints using the Bioscrypt reader. This is done on the *Cardholder* dialog. The instructions that follow will explain this process

Ensure that the Bioscrypt smart card profile is selected in the **Profile** field of the *Advanced* tab on the *Cardholder* dialog.

Assigning a fingerprint to the card

1. Expand the **Cardholder & Access Management** folder list from the Navigation pane on left hand side.

2. Double click the **Cardholder** list item.

   ⇨ The *Cardholder* dialog is displayed.

3. To assign a finger print to a card, place the card on the Enrollment Reader.

4. Click **Assign** to get the CSN number. The CSN number is displayed in the **Card Number** field of on the *Cardholder* dialog.

5. Enter the required cardholder details like the First Name, Last Name, Workgroup, etc.

6. Click the **Access Privileges** button, select the access points for the cardholder and click **OK.**

7. Click the **Assign** drop down button, and select **Acquire fingerprint for base card from Bioscrypt reader.**

8. Follow the instructions on the dialog to acquire a fingerprint.

9. You can repeat the previous step to capture additional fingerprints. However, only 2 fingerprints can be saved in the system.

10. The **Finger Prints** section of the *Advanced* tab will display a new row for the captured fingerprint. If you have captured multiple fingerprints, select the rows that you do not require, and click the **Delete** button to remove these rows.

11. In the **Index** field, click to select the finger name that was used for the fingerprint capture.

12. In the **Credential Profile** field, select a credential profile to which this fingerprint should be saved.

13. Click **Save**. The fingerprint/s will be saved in the SiPass integrated system. The system indicates this by displaying a ticked **Saved** checkbox for the fingerprint that was saved.

14. Click **Read & Search** button to read the contents of the card placed on the reader. An icon is displayed on the cardholder dialog which depicts fingerprint is on the card as well as on the disk.

15. Click **Encode**. The fingerprint/s will be encoded to the card. The SiPass system indicates this by displaying a ticked **Encoded** checkbox for the fingerprint that was encoded to a card.

    ⇨ Smart Card encoding successful message is displayed to the user.

⇨ As a result of this configuration, the fingerprint gets encoded to a card using the Bioscrypt reader.

You can inspect the card after acquiring the fingerprint.

◈ In the *Cardholder* dialog, click **Read** drop-down and select **Read card from Profile Reader – OmniKey CardMan 5×21.** *Read Card* dialog shows up. Place the card on the Bioscrypt reader.

⇨ The Bioscrypt reader reads the card and shows the biometrics stored on the card.

You can verify the card details by applying the following steps:

1. Badge the card on the Bioscrypt reader; follow the instruction on the reader and present fingerprint.

2. If the card is valid then it is notified to the user by an audit trail message which says **Valid**. If the card is invalid then it is notified to the user through an audit trail message which says **Invalid**.

10 DVR

The SiPass integrated DVR solution helps you to communicate with DVR equipment using a high level interface that allows control and maneuvering of the equipment connected to the DVR system, such as DVR units, cameras and auxiliary devices. With the DVR High Level Interface, you can view and record digital images from a SiPass workstation.

Whilst SiPass integrated supports many DVR systems, Siemens SISTORE DVR system is recommended for reliability and performance.

A DVR communicates with SiPass integrated workstations by TCP/IP protocol across an Ethernet network. This allows even greater flexibility when integrating your DVR camera system with the SiPass integrated access control and security system. You only need to connect a DVR to the network on which the desired SiPass DVR workstation is located.

If you only require the use of a single operator and therefore a single PC, the DVR Client files can be installed on the same machine that the SiPass server and Client are installed. If you require a separate SiPass workstation for viewing and recording functionality, the DVR Client files can be installed on a separate PC, along with a SiPass Client.

The SISTORE interface cannot be used to control PTZ type cameras, but can be used to control the recording mechanism on a SISTORE system.

DVR Configuration Summary

The following list provides a summary of the configuration and setup for the SiPass DVR option.

- Ensure that Windows and the same service pack have been installed on all PCs in the SiPass integrated access control and security network.
- If your access control and security network is to be configured using more than one PC, ensure that all machines are connected together using an appropriate communications protocol.
- Install the appropriate SiPass integrated software onto each PC in your access control and security network, ensuring that exactly the same version of SiPass integrated is used for all installed components.
- Ensure that the DVR system architecture has been planned in advance.
- Ensure that you have programmed the DVR unit using the System Administration software and that all DVR devices have been connected.
- Ensure that the DVR unit has been connected to the SiPass PC where the DVR bus service has been installed.
- Install the DVR Client files on the PC(s) where DVR images are to be viewed. Configure the DVR Client with the address and details of the DVR.
- Program and configure the DVR Bus and DVR using SiPass integrated.
- Program the necessary cameras and camera groups in SiPass integrated.

10.1 SiPass integrated DVR Client

SiPass integrated features a fully integrated DVR Client as part of its Graphical User Interface. The Client allows you to view live images, organize your DVR Camera system including sequences and presets, and record and playback live images, which are archived by date and time.

When the DVR Client is called from a SiPass integrated workstation to play back a recorded image or view a live image, the actual client will depend on the type of DVR System(s) you have installed at your facility.

- Ensure that all the DVR equipment has been configured in SiPass integrated Configuration Client.
- Ensure that the DVR unit and camera have been turned on and the System Administration software has been used to configure the DVR Switcher.
- Ensure that the SiPass Server and the network connection between the DVR workstations and any DVRs are running and operational.
- Ensure that the correct operator privileges have been assigned.

The SiPass DVR Client currently only applies to SISTORE CX / SX units that are Version 3.1 and higher.

The dedicated SiPass DVR GUI is opened by expanding the DVR folder in the navigation pane on left and selecting **Live DVR**. The following table show the function of each set of controls:

Control	Function
Camera List	Lists all of the cameras you have defined for DVR operation. The icons indicate the camera type.
Preset List	Lists all of the presets you have defined for the camera selected above.
Playback Controls	Allows you to select and play back a previous DVR recording event. Also allows you to record in real-time from the DVR Client.
PTZ Controls	A series of controls for manipulating PTZ cameras, camera focus, and auxiliary camera devices like wipers and lamps.
DVR Mode	Selects Live Video or Recorded Video mode.
DVR Units	Lists the DVR units that you have defined in the Components dialog.

Using the Camera Controls

The camera controls in the DVR Client allow you to move a PTZ camera using the mouse, and activate auxiliary devices.

Directing the camera using the mouse

As well as the compass on the right hand side of the DVR Client, cameras can also be manipulated using a mouse inside the viewing area.

By clicking and dragging the left mouse button, while the mouse pointer is positioned inside the viewing window, a camera can be moved in the direction of the mouse drag. The closer the mouse pointer is to the edge of the screen, the faster the camera will move.

Changing a camera title

The titles of cameras in the list on the left hand side can be changed from the DVR Client. Any changes will be updated in the *Components* dialog.

1. In the **Camera** list on the right hand side, double right-click on the camera title to be changed. The title will be highlighted and a cursor will appear.
2. Change the camera title by editing the title text.
3. Click on another camera. The highlighting will be removed.
4. Choose **Set** to save the title change.

10.1.1 Creating a Preset from the DVR Client

DVR Camera Presets can also be created from the SiPass DVR Client.

1. Expand the **DVR** folder in the navigation pane on left and double click the camera for which you want to define a preset, from the list under the **Live DVR** item.
   ⇨ The *DVR Operation* dialog is diaplayed.
2. In the **Preset** list, select a blank Preset, or an existing Preset if you wish to over-write it.
3. Use the Camera controls to set the camera position and focus to the desired setting.
4. Click the **Set** button. This will assign the current camera setting to this Preset Slot.
5. You can add or change Preset names by right double-clicking in the **Name** Column, and entering a new name.

10.1.2 Viewing and Recording from a DVR Camera

SiPass integrated allows you to select a camera and display live images from that camera on the DVR GUI screen.

1. Expand the **DVR>Live DVR** folder list from the Navigation pane on left hand side.
   ⇨ The configured DVR units with any Cameras and IP Cameras are displayed in a tree structure.
2. Double click any camera for which you want to view the live image.
   ⇨ The *DVR Operation* dialog displays the live image from the selected camera.
   ⇨ **Note:** To view cameras from a different DVR unit, select the new unit from the **DVR Unit** drop-down box. Any cameras defined for that unit will appear in the **Camera** list on the left hand side. To go to a preset for a select camera, simply choose the **Preset name** from the **Preset** list below.
3. To view a recording for a camera, select **Recorded Video** from the **Mode** dropdown list.
   ⇨ The dialog is now refreshed to support the viewing of recoded video.

10.1.3 Recording from the DVR Client

An operator can record a live video from the DVR Client.

1. Expand the **DVR** folder in the navigation pane on left and double click the camera from which you want to record the video, from the camera list under the **Live DVR** item.

   ⇨ The *DVR Operation* dialog is diaplayed.

2. Select **Live Video** from the drop-down list of the **Mode** field.
3. This action will display the live image from the selected camera. This mode generally appears by default on opening this dialog.
4. You can also select another DVR Unit connected to the camera you want to record, from the **DVR Unit** list at the top of the dialog. The list of cameras defined for this unit will appear in the **Camera** list.
5. Select the camera from the list from which you want to record a live image.
6. If the camera has PTZ functionality, use the PTZ Controls on the right hand side to move the camera into the desired recording position. You can use the PTZ controls to manipulate the camera and also select Presets while in recording mode.

   ⇨ **Note:** PTZ functions are not available when an IP camera is directly connected to SiPass integrated.

7. Choose **Start** in the **Recording** section.

ℹ The operator can add a comment to the video to be recorded by typing in the Comment field.

When you have finished recording, choose **Stop**. The recording event will be stored in the DVR event calendar and can be replayed from both the DVR Client and the Audit Trail.

10.1.3.1 Search and Playback of a DVR Recording

The DVR Client can be used to play back video images that you have recorded. This includes video images recorded by generic DVR units.

Further, SiPass integrated allows you to perform a filtered search for specific video images from a DVR unit.

The sections that follow explain how to perform a filtered search for video images, and how to playback these images.

Playing back a DVR recording using the DVR Main dialog

1. Expand the **DVR** folder in the navigation pane on left and double click the camera for which you want to define a preset, from the list under the **Live DVR** item.

   ⇨ The *DVR Operation* dialog is diaplayed.

2. Select **Recorded Video** from the drop-down list of the **Mode** field.
3. An operator can use the appropriate buttons in the **Playback** box to **Start**, move to the **Prev Frame**, move to the **Next Frame**, **Pause**, **Resume** and **Stop** a recorded video. The operator can also use the horizontal scroll bar in this box to navigate to different parts of the video.
4. To search for a recorded video by the Time of recording, select the **By Time** radio button in the **Search Criteria** box. You can select from the list available in this drop-down field. Click **Search**.
5. To search for a recorded video by the Comment attached to the recording, select the **By Comment** radio button in the **Search Criteria** box.
6. Click **Search**.
7. The search results of recorded video clips will appear in the **Video Clips** box. Click any clip in the list and use the options in the **Playback** box to view it.

Searching for recorded video clips

Searching for recorded video clips

1. Expand the **DVR** folder in the navigation pane on left and double click the camera for which you want to define a preset, from the list under the **Live DVR** item.

   ⇨ The *DVR Operation* dialog is diaplayed.

2. Select **Recorded Video** from the **Mode** dropdown field.
3. In the *Play Options* section, click the **Search Video Clips** radio button.
4. Configure the search criteria required. For more information on the search criteria, refer the table provided below.
5. Click the **Search** button.

⇨ The search results of the recorded video clips will be displayed in the Video Clips section.

The table that follows explains the Play Options, Search Criteria, Video clip listings and Playback options available to customize the viewing of recorded video.

Section	Available Options	Description
Play Options	Search video clips	This option allows the operator to search recorded video files by the **Camera**, **Time**, **Comment** search criteria on this dialog.
	Play by time	This option allows the operator to search recorded video files by **Camera** and the **Start time** of the video.
Search Criteria	Camera	This field lists all the cameras configured to the DVR unit selected in the DVR Unit field of this dialog. The operator can tick the checkbox corresponding to the camera, and the search will return all the video clips that were recorded by that camera.
	By Time	**Start time**: The search will return results of all the video files that were recorded after Start time specified in this field.
		End time: The search will return results of all the video files that end recording before the End time specified in this field.
	By Comment	This option allows operators to search for video clips based on the comment attached to the recorded video clips.
Video Clips	#	This field displays the video clip number.
	Camera	This field displays the name of the camera that recorded the video clip.
	Comment	This field displays the comment about the recorded video clip.
	Start Time	This field displays the exact time when the video started recording.
	Stop Time	This field displays the exact time when the video stopped recording.

	ClipStorageId	This filed displays the Clip Storage Identification number.
Playback*	**Speed**	This option allows you to increase or decrease the speed of the video clip being played.
	Start	This button starts playing the selected recorded video clip.
	Stop	This button stops playing the video clip.
	Play Backward	This button allows the operator to play the video clip backwards from its current play position.
	Prev Frame	This button moves the video clip being played to the previous frame.
	Pause	This button pauses the video clip being played.
	Next Frame	This button moves the video clip being played to the next frame.
	Play Forward	This button allows the operator to play the video clip forwards from its current play position.

*****Mouse-over on the buttons of this section will display the names of the individual buttons.

Playback recorded video clips

This section explains how to select and play recorded video clips that are returned after a search.

Playing a recorded video clip

1. Follow the instructions provided in the section Searching for recorded video clips [➙ 188] to perform a filtered search for recorded video clips.
2. The resulting video clips of the search will be listed in the *Video Clips* section of the *DVR Operation* dialog.
3. Select a video clip that you want to play.
4. Click the **Play** button in the *Playback* section of this dialog. Alternatively, double-click the required video clip in the *Video Clips* section.

⇨ The video clip that is selected will be played.

Using the Playback options to customize viewing the video

An operator can use the appropriate buttons in the Playback section to Play, move to the Prev Frame, move to the Next Frame, Pause, Resume and Stop a recorded video. For further information on these buttons, please table in the section Searching for recorded video clips [➙ 188].

The operator can also use the horizontal scroll bar in this section to navigate to different parts of the video.

10.1.4 Playing Back DVR Recordings from the Audit Trail

SiPass integrated features a DVR Playback option from the Audit Trail right-click menu.

1. Right-click on a DVR recording event from the Audit Trail.
2. Select the **Play Back** option.

⇨ The DVR Client will appear, and the recording you selected from the Audit Trail will begin playing in the viewing window.

10.2 Operating IP Camera from SiPass integrated

The DVR Client of SiPass integrated is used for controlling IP Cameras connected to the DVR system. Note that PTZ functions are not supported for any IP camera directly connected to SiPass integrated.

10.2.1 Viewing IP Camera video on the Live DVR dialog

Once an IP Camera has been configured on the *Components* dialog, its video can be viewed on the *Live DVR* dialog in the following manner:

▷ Ensure that the right IP address has been entered for the camera in the *Components* dialog.

1. Expand the **DVR>Live DVR** folder list from the Navigation pane on left hand side.
   ⇨ The configured DVR units with any Cameras and IP Cameras are displayed in a tree structure.
2. Double click the IP camera for which you want to view the live image.
   ⇨ The *DVR Operation* dialog displays the live image from the selected camera.

ℹ To use record the IP Camera video, the camera must first be configured as a Remote Video Source. For more information on this feature, refer the section Using IP Cameras as Remote Video Sources.

10.2.2 Using an IP Camera as a Remote Video Source

To use IP Cameras as Remote Video Sources, it should first be connected to a DVR Unit.

This functionality requires that the IP Camera be configured as the Remote Video Source on the SISTORE CX tool.

ℹ Ensure that the IP address entered in the SISTORE CX tool matches the IP address configured for the IP camera in the *Components* dialog.

10.2.3 Using an IP Camera for Cardholder Imaging

Once an IP Camera has been configured in the SiPass integrated Configuration Client, it can be used for the purpose of Cardholder image capture in the following manner:

Note: Ensure that the right IP address has been entered while configuring the camera.

1. Double-click the **Cardholder** item in the navigation panel on left.
   ⇨ The *Cardholder* dialog is displayed.
2. Click on the **Imaging** tab.
   ⇨ Live video from the IP Camera will appear when the **Live** button is clicked.
3. After live video appears a photo can be captured by clicking the **Capture** button.

10.3 Operating the SISTORE DVR Client

If you have installed the recommended DVR solution, Siemens SISTORE, at your facility, the viewing and recording process will be slightly different. This is because a separate DVR Graphical User Interface is used for SISTORE DVR systems within SiPass integrated.

This chapter gives only a brief description of the most important components of the SISTORE DVR user interfaces, and aims to introduce the operator to the basic functionality of the SISTORE Clients. For more information on configuring and using this DVR Client, it is highly recommended that you consult the User’s Guide that came with the DVR software.

10.3.1 Using the SISTORE AX Client to view live images

The following instructions show the basic usage of the SISTORE AX type DVR Client. This Client appears when you have SISTORE AX type DVR units installed at your site, and you trigger viewing from a SISTORE DVR camera through the *DVR Operation* dialog, an *Event Task*, or a *Graphic Map*.

SISTORE AX Client Controls

If you hold the mouse pointer over an icon on the SISTORE AX client GUI, a tool tip will appear giving a brief description of the command.

Control	Description
Select Site	Selects a SISTORE AX DVR unit from which to select and view camera images.
Select Camera	Select the camera to view from the current DVR unit.
Split-pane view	Select how many camera images to display on screen.
Full screen view	Displays the current camera image(s) using the entire screen space. Click anywhere on the screen to return to the client view.
PTZ/Lens Controls	Controls to zoom in/out, focus near/far, and open and close the iris.
Preset Controls	Choose whether to create a new preset from the current camera position (MEM) or go to an existing preset (POS).
Alarm on/off	This controls the reporting of alarm events of up to four types from a DVR unit; for example, Video Loss alarm.

10.3.2 Using the SISTORE AX Client to record and playback

The following instructions show the basic usage of the SISTORE AX type DVR Client to record images, and play back previously recorded images.

The “Search” Client appears when you have SISTORE AX type DVR units installed at your site, and you trigger viewing of a recorded image through the **Play Back** option from the Audit Trail right-click menu.

You may search for DVR Recording events by calendar/time search (Time Lapse search) or by Recording event (Event search); for example, by alarm event or motion detection.

SISTORE AX Search Client Controls (Time Lapse Mode)

If you hold the mouse pointer over an icon on the SISTORE AX client GUI, a tool tip will appear giving a brief description of the command.

Control	Description
Select Site	Selects a SISTORE AX DVR unit from which to select and view camera images.
Select Camera	Select the camera to view from the current DVR unit.
Split-pane view	Select how many camera images to display on screen.
Recording Calendar	Select a day to view images recorded by a camera (if any). Days marked in blue indicate recording events on that day.
Recording Time	Select a time from which to begin viewing by clicking a Time Schedule on the timeline with the mouse.
Reload Image	Reloads the current recorded image.
Go to Time	Opens a dialog from which you can enter an exact time during the selected day to being viewing.
Search Mode	Selects the mode to search for recorded sequences. There are two modes: Time Lapse Search – uses a calendar and timeline to select recordings for playback. Event Search – uses a query dialog to search for specific events by camera, motion detection and alarm response.
Play Controls	Controls to play, stop, forward and rewind the selected DVR recording.

SISTORE AX Search Client Controls (Event Mode)

If you hold the mouse pointer over an icon on the SISTORE AX client GUI, a tool tip will appear giving a brief description of the command.

Control	Description
New Event Query	Opens the Event Search dialog to create a new query to search for DVR Recordings.
Next Event	Cycles to next Recording in the Results list.
Event Query Results	Lists all matching results of the query.

10.4 Virtual Monitors

The Virtual Monitor feature allows operators to arrange and view a matrix of DVR images simultaneously.

1. Double click **Virtual Monitors** from the Navigation pane on left hand side.
   - ⇨ The *Virtual Monitors* dialog is displayed listing the camera systems available to provide DVR views in the **Cameras** panel on left. You can see individual cameras by expanding the tree hierarchy.
2. The right side panel displays windows where different DVR views can be played.
3. The operator can select the layout of the *Virtual Monitors* dialog.
4. To increase / decrease the number of windows, select **File > Load** and select from the selections available to alter the number of windows, as required.
5. To add a view to individual windows, select a camera from the **Cameras** panel.
6. Click and drag this camera, and drop it onto a selected window on the right. This action will play the live image of that camera on the selected window.
   - ⇨ **Note:** Alternatively, you can also right-click on a desired screen and select **Set Camera**. This action will display the *Select Camera Point* dialog from where you can select the IP camera. Click **OK** to display the video on the selected screen.

ℹ To use or record the IP Camera video, the camera must first be configured as a Remote Video Source. For more information on this feature, refer the section Using an IP Camera as a Remote Video Source [→ 192].

11 Video Imaging and Card Printing

SiPass integrated allows you to capture live images using a video or digital camera and store these images with the record or a cardholder. You can also import images from over 32 different file types. Once the Video Imaging and Card Printing Module has been installed, each operator can configure the image settings to their own preferences.

By using SiPass integrated to set the camera or video card properties, the settings will not be permanently recorded and will only be configured for the current session. It is recommended that you configure settings with the video capture card or digital camera’s own installation software.

11.1 Capturing Cardholder Photographs

Once you have installed SiPass' Photo ID and Image Verification Module and have configured the image preferences, you can begin capturing cardholder images.

▷ Ensure that the video capture card has been installed and configured.

▷ Create an employee record for the employee whose image is to be captured.

▷ Ensure that a card template has been created.

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Cardholder** list item.
3. Open or Create the record for the cardholder whose image is being captured.
4. Choose the *Imaging* tab. Choose **Live**.
   ⇨ The imaging panel will display a live video image on screen.
5. Position the camera and employee so that the employee's picture is displayed clearly (in focus) on screen. Refer to the video camera's user guide for detailed instructions concerning its operation and settings.
6. Choose **Capture**.
   ⇨ The live video image will appear on screen as a still image. A cropping tool will appear overlaid on the captured photo, and a contrast and brightness slider will also appear.
7. By positioning the cursor over one of the handles located at the corner of the cropping rectangle, you can change the size of the cropped area by dragging the rectangle to the desired size.
8. By positioning the cursor anywhere inside the cropping area, you can hold down the left mouse button and drag to move the cropped area. The part of the captured image that appears within the rectangle will appear in the photo field on the card template.
9. Use the **Contrast** and **Brightness** sliders, to adjust the image quality. The higher up the scale, the greater the Contrast and/or Brightness, and vice versa.
10. Choose the *Definition* tab, when finished.
11. Click **Save**.

11.1.1 Image Recall

Image details - employee photographs and signatures - are saved to each employee record. Any client terminal can access these records merely by opening the desired employee record and choosing the Imaging tab at the top of the dialog. The last saved image will be displayed.

11.2 Importing a Cardholder’s Photograph or Signature

Once you have installed SiPass’ Photo ID Module and have configured imaging preferences, you can begin importing photographs and signatures of cardholders.

▷ Create an employee record for the cardholder whose image will be captured.

▷ Ensure that the cardholder photograph or signature exists.

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Cardholder** list item.
3. **Open** or **Create** the database record for the cardholder whose photograph or signature is being imported.
4. Choose the *Imaging* tab. If a previous image of the employee signature exists in the employee’s record, it will automatically be recalled when the Imaging tab has been selected.
5. Select the **Photo** radio button to import the cardholder’s photograph or select the **Signature** radio button to import a signature.
6. Choose the **Import** button.
7. Select the image file to import.
8. Choose the **Open** Button or double click on the file name.
9. By positioning the cursor over one of the handles located at the corner of the cropping rectangle, you can change the size of the cropped area by dragging the rectangle.
10. Use the **Contrast** and **Brightness** sliders, to adjust the image quality - the higher up the scale, the greater the Contrast and/or Brightness, and vice versa.
11. Choose the *Definition* tab, when finished.
12. Click **Save**.

Generally used image formats like JPG, BMP, PNG and TIF can be uploaded in SiPass integrated. Graphic Interchange Format (GIF) files are licensed and cannot be used with SiPass integrated.

Images with a maximum resolution of up to 4500x4000 are supported. A resolution higher than this may result in error.

11.3 Card Printing

The SiPass integrated Video Imaging and Card Printing module also provides the tools you need to print access cards on-site. SiPass integrated allows you to print a single card from a cardholder's record, or print a group of cards based on selectable criteria. Card Printing is normally carried out as a function of the Video Imaging and Card Printing Module and requires a dedicated printer for the purpose. Card printing cannot be carried out on conventional printers. However, conventional printers can be used to proof card templates.

Depending upon your requirements, cards can be printed as single-sided or double-sided (duplex). Many card printers are capable of duplex printing.

!	*NOTICE*
	You should keep in mind that used printer ribbon contains negative images of data contained on cards. Ensure that you dispose of used printer ribbons according to your policy for handling confidential information.

11.3.1 Printing a Card

SiPass integrated allows you to print an access card for any cardholder in your database. This function would normally be carried when a cardholder is newly enrolled in SiPass integrated or when a new access card needs to be issued.

Printing a single card

▷ Ensure that a card printer has been correctly installed and configured.

▷ Ensure that the appropriate card template has been designed

1. Expand the Cardholder & Access Management folder list from the Navigation pane on left hand side.
2. Double click the **Cardholder** list item.
3. Create a new cardholder record or open the record of an existing cardholder.
4. Choose the *Imaging* tab.
5. Capture the cardholder's photograph
6. Choose **Print**. The card will be sent to the printer.

⇨ The cardholder's details are also automatically saved when cards are printed from the *Cardholder* dialog.

Printing a batch of cards

1. From the **Operation** menu, select **Batch Card Printing**.
2. Select the **Card Filter Options** that best describe the group of cards you wish to print, by selecting the checkbox and entering or choosing the appropriate data.
3. Choose the **Generate** button.

   ⇨ The list of cardholders that match your criteria will appear in the **Generated Card List** field.
4. From the displayed list, select those cardholders to be excluded from the batch print job by double clicking anywhere on their record.

   ⇨ The entry in the **Print** column for that record will now say “No”, indicating that a card will not be printed.
5. Select the required **Print Configuration**.
   - **Start Immediately**:
     Allows the SiPass Operator to choose whether to start the Batch Print job immediately or wait and start the print job manually from the *Batch Card Printing Monitor* window.
   - **Apply Request to Proceed Message After**:
     If selected, this option allows you to specify whether a confirmation to proceed with the batch print job appears. You can also specify the exact number of cards that are printed before the confirmation dialog next appears.
   - **Apply Card Template if none defined**:
     Allows you to specify a default card template for each cardholder in the SiPass integrated system that has not been assigned a template. This option will not be enabled if the **Card Template filter** option has been selected.
   - **Always Encode upon Question:**
     Allows you to encode and print all the cards configured for Batch Card Encoding / Printing. Leaving this checkbox un-ticked means that SiPass integrated will not encode any cards that require an operator decision. For example, an operator may have configured this dialog to encode and print a card with a card number that already exists in the system. Normally, this would bring up a dialog asking the operator to verify (Yes or No) if the card number should be used for the new card. There are other situations that may arise, requiring an operator decision. Such cards will not be encoded if this checkbox is left un-ticked. However, SiPass integrated will proceed with the batch card encoding and printing process for the remaining cards.
6. Choose **Proceed** to send the job to the batch print queue. A confirmation window will appear.
7. Select **Yes**.

   ⇨ The cards will begin printing automatically if the **Start Immediately** option has been selected. If this option has not been selected the print job will be paused and can be started from the *Batch Card Printing Monitor* window.
8. Choose **Close**.

⇨ If you have entered a value into the **Apply Request to Proceed Message After** field, a dialog will appear each time the specified number of cards have been printed.

11.3.1.1 Batch Printing Card Filters

The following table explains the available card filters for batch printing

Filter	Description
Card Range	This option allows you to select a range of cards based on specified card numbers. For example “12 - 56”, 10, 100 – 145”.
Only These Workgroups	This option allows you to select one or more workgroups to which cardholders belong. Simply select a single workgroup by clicking on it. To choose multiple workgroups hold down the CTRL key while selecting each workgroup.
Card Template	This option allows you to select a card template. All cardholders with the template associated with their database record will be included.
Custom Field	This allows you to select a custom field from a list of all defined custom fields in the system. Once selected, you will then be able to select a specific value associated with that custom field. All cardholders with a record that matches the selected custom field value will be included.
Cards Last Printed	This allows you to select cardholders based on the date and time their card was last printed, from the following conditions: –Before, On or before, After, or On or after Any cardholder whose card was printed in the selected range will be included, dependant upon the other criteria you have chosen.
Filter on Card Printed State	Allows you to select all cardholders that have or have not had their access card previously printed based on your selection.
Cardholder Modified	This allows you to select cardholders whose database record was changed based on the following conditions: –Before, On or before, After, or On or after Any cardholder whose record was changed within the selected range will be included, dependant upon the other criteria you have chosen.
Filter on Employee Modified State Since Last Printed	Allows you to select all cardholders whose database record has either been changed or remained unchanged since their card was last printed.
Filter Out Void Cards	Allows you to ignore all cardholders with a void status.

11.3.2 Batch Card Printing Monitor

This section shows how to open and use the *Batch Card Printing Monitor* window. This window allows you to monitor the progress of print jobs, and to pause, start, abort, or resume a batch card print job.

1. From the **Data** menu in the SiPass integrated Configuration Client, select **Batch Card Printing Monitor**. The *Batch Card Printing Monitor* window will appear displaying the status of each batch card print job that has been generated. The following describe each column in the window:
   - **Batch**: Batch card printer number – auto generated based on date and time.
   - **Status**: paused, queuing (another currently printing in a queue of batch jobs), printing, aborted.
   - **Progress**: The number of cards that have been printed out of the total number.
   - **Current**: Card number that is currently being printed.
   - **Printer**: Printer to which the job will be sent.
2. To start, pause, abort or resume card batch print jobs, right-click on the job you want to action. A menu will appear showing a list of options: **Start**, **Pause**, **Resume**, **Abort**. Select the action you want to perform on the print job.
3. Close the *Batch Card Printing Monitor* window when you have finished.

12 Imported Data

The Import Data feature of SiPass integrated has two main options in its tree view:

Watchlists

This innovative feature allows the operator to create a new watchlist, or import an existing source of data (a csv. or text file) into the SiPass integrated system.

An operator can create / import a set of cardholder details as a Watchlist. These details will be linked to the SiPass integrated system, and the operator can configure SiPass to alert operators if cardholders with matching or similar details are saved within, or already exist within the SiPass system.

Lookup Data

The Lookup Data feature is basically used for file import or export, to and from SiPass integrated. Files present under Lookup Data can be used to populate the ‘Drop-down List’ custom field for Custom Pages. (Refer the sections under Importing / Exporting Custom Pages of this manual for more information on File Import / Export, and the sections under Populating the Drop Down List Custom Field for information on the the Drop-down list custom field.)

12.1 Watchlists

Watchlists that are created in SiPass integrated, or imported from an external location, can be configured for two primary purposes:

A. To Perform a Warn User Configuration

When an operator adds a new cardholder, or updates the details of an existing cardholder, whose details match those provided in a watchlist, a warning message will be displayed.

The operator can then choose whether to proceed with the cardholder creation / update.

Please refer the section Warn User Configuration [→ 203] for more details.

B. To Generate Watchlist-linked Customized Reports

The operator can generate a Customized Report based on the data of a specific Watchlist Report. This Customized Report can be configured to perform the following functions:

- To trigger specific Reporting Actions
- To be used as an Actionable Report for Event Tasks.

Please refer the section Creating Watchlist-linked Customized Reports [→ 207].

12.1.1 'Warn User' Configuration

Overview of configuration stages

To configure the Warn User feature, an operator must follow the procedures mentioned below.

1. Create a new Watchlist report.
2. Map the fields of the Watchlist report to the fields of the *Cardholder* dialog.

Conditions triggering the warning message

Once configured the warning message is triggered and displayed when an operator does the following:

- Uses the *Cardholder* dialog to create a new cardholder, whose details match those that exist in a Watchlist report;
- Uses the *Cardholder* dialog to update the details of an existing cardholder, whose details match those that exist in a Watchlist report

Warning message displayed

Once this configuration is complete, an operator will be presented with the following warning message:

"*Action happened on Trigger Effect Entry: xyz*

A watchlist breach has occurred. Are you sure you want to continue?";

where **xyz** represents the name of the watchlist report that contains the cardholder's details.

12.1.1.1 Creating Watchlist Reports in SiPass integrated

Watchlist Reports can be created in SiPass integrated in two ways:

- Create a new Watchlist Report within SiPass integrated; OR
- Import an existing watchlist from an external location, to create a new Watchlist Report

Both these options have been discussed in the sections that follow.

Creating a new Watchlist Report

1. Select **Imported Data > Watchlists** from the **Navigation** panel on left.
2. Right-click **Watchlists** and select **New Watchlist Report**. This action will display the **Report Wizard.**
3. Enter a name for the watchlist in the **Name** field.
4. Select **External Data** from the **Create from data source** field.
5. Click **Next**.
6. In the next dialog, you can leave the **External File** field blank.
7. In the file columns and rows below, right-click on the cell **NoName**.
8. Select **Change Column**.

   ⇨ This will display the *Customize Column* dialog.
9. Specify the column name in the **Column Name:** field.

The following words/terms should not be used as Column Names: **rownumber**, **revision**, **instance**, **type**. Further, a column name should not start with the underscore symbol (_).

10. Select **the Column Type**: to be either **Text** or **Integer**.
11. Select the maximum length of characters in the column in the **Max Length:** field.
12. Click **OK**.

13. To add additional rows or delete rows from this file, right-click the first cell of the last row and select **Insert Row** or **Remove Row** as required.
14. To change, insert or remove columns, right-click any of the top-most cells and select **Change Column / Insert Column / Remove Column** as appropriate.
15. In the available cells, type in the information required for the watchlist. For example, if you want the watchlist to be based on the First Name and Last Name of cardholders, change 2 column names to First Name and Last Name. And then add the respective list of first and last names in the cells under the respective columns.
16. Click **Next**.
17. All the dialogs in the next field are selected by default. The operator can change the display fields if necessary.
18. Click **Next**.
19. All the fields selected in the next dialog are Filter Conditions. The operator can change the filter condition if necessary.
20. Click **Next**.
21. In the next dialog, map the **Parameter** field (which will appear in the Watchlist report) to the adjacent *Cardholder* dialog fields.

ℹ The operator can choose to skip this step, and proceed to click **Finish**. The field mapping can then be done on the *Interactive Reports* dialog. For more information on how to configure this mapping, refer the section Configuring an Interactive Report through Field-Mapping.

22. Click **Finish**.

⇨ This new watchlist will now be added and under **Watchlists** in the **Navigation** panel.

Importing Files to Create Watchlist Reports

The following steps detail how an operator can import a watchlist into SiPass integrated:

1. Select **Imported Data > Watchlists** from the **Navigation** panel of SiPass integrated.
2. Right-click **Watchlists** and select **New Watchlist Import**. This action will display the **Report Wizard**.
3. Click **Next**.
4. Enter a name for this watchlist in the **Name** field.
5. Select **External Data** from the **Create from data source** field.
6. Click **Next**.
7. In the next dialog, select the **…** button to select the external file from where the data should be imported.

ℹ The following words/terms should not be used as Column Names: **rownumber**, **revision**, **instance**, **type**. Further, a column name should not start with the underscore symbol (_).

8. Click **Next**.

9. All the fields in the next dialog are selected by default. The operator can change the display fields if necessary.
10. Click **Next**.
11. The fields selected in the next dialog are all Filter Conditions. The operator can change the filter condition if necessary.
12. Click **Next**.
13. In the next dialog, map the **Parameter** field (which will appear in the Watchlist report) to the adjacent *Cardholder* dialog fields.
14. Click **Finish**.

In some cases, the operator may import information to an existing watchlist. In such cases, ticking the **Overwrite existing ones** checkbox will overwrite any information that was present on the watchlist earlier. If this checkbox is left unticked, the list from the imported file will be added to the end of the existing watchlist.

⇨ This new watchlist will now be added and displayed under **Watchlists** in the **Navigation** panel.

12.1.1.2 Field Mapping a Watchlist Report

There are three ways in which Field Mapping can be performed for a Watchlist report:

Field Mapping performed during Watchlist report creation

1. After setting the Filter Conditions while creating the Watchlist report, click **Next**.
2. In the next dialog, map the **Parameter** fields (which will appear in the Watchlist report) to the adjacent fields of the *Cardholder* dialog.
3. Click **Finish**.

Field Mapping option chosen by selecting a Watchlist report

1. Expand the **Watchist** tree hierarchy of the **Navigation** panel.
2. Select and right-click a Watchlist report for which field mapping is to be done.
3. Select **Field Mapping**. This action displays the *Field Mapping* dialog.
4. Map the **Parameter** fields (which will appear in the Watchlist report) to the adjacent fields of the *Cardholder* dialog.
5. Click **Save** and **Close**.

Field Mapping performed on the Interactive Reports dialog

For detailed instructions on how to perform this configuration, refer the section Configuring an Interactive Report of this manual.

Once field mapping is complete, the watchlist has been configured for the Warn User feature. When operators create or update details of a cardholder matching the watchlist, a watchlist breach message will be displayed.

12.1.1.3 Modifying Existing Watchlist Data

1. From the **Watchlist** tree hierarchy, select a Watchlist report.
2. Right-click this report, and select **Modify Watchlist Data** to display the *Modify Watchlist Data* dialog. The watchlist data can now be modified as required.

Modifying the existing watchlist with a new import: Ticking the **Overwrite existing data** checkbox and then importing a new watchlist, will overwrite the data of the existing watchlist. If this checkbox is left unticked, the imported watchlist data will be added below the existing data.

12.1.2 Creating Watchlist-linked Customized Reports

1. Select **Customized Reports** from the **Navigation** panel.
2. Click **Next** when the Report Wizard appears.
3. Enter a **Name** for the Customized report.
4. Click **Next**.
5. Select a **Report Type**.

If the operator wishes to use this customized report to Void Cardholder/Card, the Record Type chosen must have valid Cardholder details. Details on how to Configure Void Cardholder / Card have been discussed in the sections under Void Cardholder/Card using Customized Reports.

6. Click the **Click here to add filter criterion** button.
7. Click **Choose Field**.
8. Select [Parameter Report] from the drop down list. The adjacent field automatically changes to **Matches**.
9. Click the adjacent empty field, and select the watchlist report that this customized report should be linked to.
10. Right-click the cells highlighted in blue below.
11. Select a field from the list (the list displays fields of the Report Type selected), to add to the Customized Report.
12. Click **Finish**.
13. The customized report will be displayed on the main panel of SiPass integrated.

12.1.3 Void Cardholder/Card using Customized Reports

An operator can void cardholders or cards using Customized Reports.

This can be done in two ways:

- **By enabling Reporting Actions from a customized report, to either Void Cardholder/Card**
- **By using Actionable Reports for Event Tasks that Void Cardholders/Cards**

Both these options are detailed in the sections that follow.

12.1.3.1 Void Cardholder/Card using Reporting Actions

1. Expand **Customized Reports** from the **Navigation** panel.
2. Select and right-click the watchlist-linked Customized Report created.
3. Select **Customize View**.
4. Select **Available Actions** from the **View** panel.
5. Tick the checkboxes corresponding to **Void Card** and **Void Cardholder**.
6. Click **OK**.
7. Select and right-click on a cardholder entry in the Customized report displayed.
8. Select **Reporting Actions > Void Cardholder** / **Void Card**, as required.

⇨ The cardholder or card will now be made void in SiPass integrated. The result of this action will be reflected in the Audit Trail, the *Cardholder* dialog and Credential Profile of the cardholder in concern.

12.1.3.2 Void Cardholder/Card using Host Event Tasks

1. Repeat steps 1 to 4 of the previous section Void Cardholder / Card using Reporting Actions [→ 208].
2. Tick the checkbox corresponding to either Void Cardholder / Card (depending on which action you want to configure), **AND** click on this action to highlight it.
3. The **Set as default** button now becomes enabled.
4. Click **OK**.
5. Next, select **Program > Event Task > Host** on the main SiPass integrated user interface.
6. Configure the **Trigger** for this Host Event Task.
7. Select **Actionable Report** for the Effect **Target** field.
8. From the drop-down list of the **Report** field, select the Customized Report that was configured earlier.
9. Click **Save**.

⇨ Upon meeting the Trigger criteria, the Host Event Task will perform the default action that was configured for the customized report ; that being either Void Cardholder or Void Card.

12.2 Lookup Data

The Lookup Data allows the operator to work with lists that can be linked to SiPass integrated for a number of purposes and can be used to:

- Import lists (in the row and column format)
- Export file lists from SiPass integrated to an external location
- Create new lists (in the row and column format)

The lists that are saved into the Lookup Data can be utilized for a number of purposes as follows:

- To create options for custom cardholder fields of the *Cardholder* dialog (Refer the section Populating the DROP DOWN LIST Custom Field of this manual for information on populating Drop-down lists.)
- To create Visitor Profiles and Listed Company fields for the *Visitor* dialog

12.2.1 Creating/Importing a New Lookup File

An operator can also create a new file, or customize existing files as follows:

1. Expand the Imported Data list item in the navigation panel on left.
2. Right-click **Lookup Table** list item in the tree.
3. Select **New/import Lookup Data**.
   ⇨ The *New/Import Lookup Data* dialog is displayed.
4. Enter a name for the new file in the **Display Name** field or click in the External File field, locate the external file and click **Import**.
5. In the file columns and rows below, right-click on the cell **NoName** and select **Change Column**.
   ⇨ The *Customize Column* dialog will be displayed.
6. Specify the column name in the **Column Name:** field.
7. Select the **Column Type**: to be either Text or Integer.
8. Select the maximum length of characters in the column in the **Max Length:** field.
9. Click **OK**.
10. To add additional rows or delete rows from this file, right-click the first cell of the last row and select **Insert Row** or **Remove Row** as required.
11. In the available cells, type in the required information. The information type should be as specified in Step 6 (Text or Integer).

The operator can only add rows to this file. Columns cannot be added.

12. Click **Save**.

13 Configuring Time and Attendance (T&A)

13.1 Overview

SiPass integrated offers a utility for exporting cardholder “clock-on” and “clock-off” data. This kind of data can be used in Human Resources applications to collect hours worked, for example. When this functionality is enabled, every valid entry on an entry/exit reader is automatically exported to an external text file, and you can choose exactly which cardholder and card data to save to file.

The T&A Calculation Interface exports all of the data you nominate for each valid card badge at entry and exit readers for the Clock-on and Clock-off areas you have selected.

The Advanced Security Programming in SiPass integrated (Operation Client) allows operators to configure multiple T&A Calculation Interfaces.

Before you begin:

The T&A Calculation Interface relies on SiPass “Areas” to collect card badging data. An area is a location that can be entered and exited through one or more secure doors. Before you can configure the T&A Calculation Interface, you must first:

- Ensure that all the areas, sub-areas and access points to which the cardholder will require access have been defined.
- Establish the Time Schedules during which the cardholders will require access.

13.2 Configuring a T&A Calculation

An operator can configure multiple T&A Calculation Interfaces with ASP. The steps required to configure an interface are as follows:

1. Select **T&A Calculation** from the **Navigation** panel on left side.
2. Enter a name for the interface in the **Name** field.
3. The **Clock-on** field indicates the area for which cardholder details should be recorded for the first valid card badge of the day.
4. The **Clock-off** field indicates the area for which cardholder details should be recorded for the last valid card badge of the day. A default area already exists, “Global Outside”, which means any location that is not inside your facility.

The Time Period for the attendance can be configured in the **Period** section of this dialog.

1. Select **Absolute** if wish to specify the exact Time and Date for which attendance data should be collected. This period can be specified using the **Begin Time:** and the **End Time:** drop down lists that appear on selecting **Absolute**.
2. Select **Relative** if you wish to specify a relative time period for which attendance data should be collected. This period can be specified using the **Begin Time: (days) (hours before)** and the **End Time: (days) (hours before)** drop down lists that appear on selecting **Relative**.
3. If you tick the **Use Begin/End time as CLOCK ON/OFF for single records** checkbox, data will be collected only for the time-period specified. For example, An Area A might be configured for T&A Calculation until the End Time: 12:33 pm on a particular day. If a cardholder in the area exists at 1:30 pm on that day, his last hour of presence in Area A will not be recorded. His attendance will be marked only up to 12:33pm.
4. If you tick the **Use Date as output prefix** checkbox, a Host Event Task configured for the **Target:** T&A Calculation Calc and **Command:** Save As will be affected in the following manner:
   - ⇨ If this checkbox is left unticked, any older T&A Calculation event tasks files created with the same file name will be overwritten.
   - ⇨ If this checkbox is ticked, the same file name will be prefixed with the date specified in the T&A Calculation Configuration dialog.
5. Click **Save** and **Close**.

13.3 Configuring a Time & Attendance Event Task

The steps required to configure a **Time & Attendance** Event Task are as follows:

1. Configure the **Event Name**, **Time Schedule** and **Trigger** fields on the *Host Event Task* dialog. **Note**: This event task can be configured with any trigger.
2. From the **Target** drop down list, select **T&A Calculation**.
3. From the **Report** field, select the required T&A Calculation report from the drop down list.
4. The following selections can be made from the **Command** drop down list:
   - **Print**:
   - ⇨ This command will print the selected T&A Calculation report.
   - **SaveAs**:
   - ⇨ This command will save the selected T&A Calculation report. From the **Type** drop down list, select if the file should be saved in the **CSV**, **TXT** or **XML** format.
   - **Email Forwarding**:
   - ⇨ This command will forward the selected T&A Calculation report to a specified cardholder’s email address. After selecting the **Email Forwarding** command, click the **+** button on this dialog.

This will bring up the *Search Cardholder* dialog from where you can select cardholders. The email will be forwarded to all the selected cardholders.

Note: To ensure that the event task forwards the email to the selected cardholders, tick the **Use E-mail Address in Message Forwarding** checkbox on the *Personal* tab of the *Cardholder* dialog, and click **Save**.

Index

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