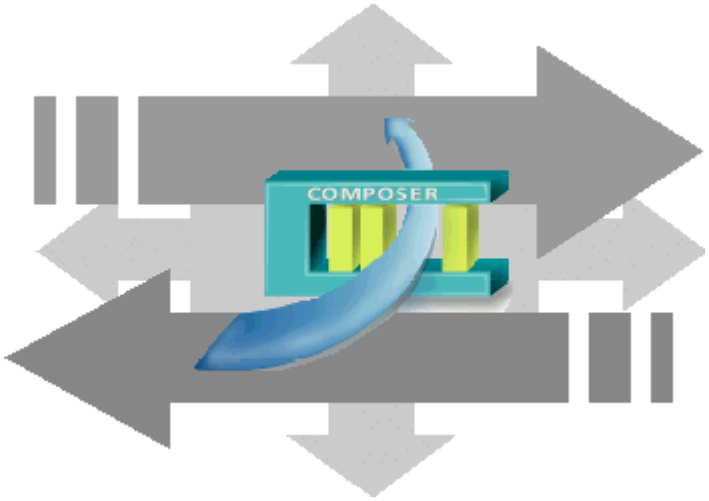
SIEMENS



DMS8000 MP4.20

Access Control Connectivity Guide

- SiPass

Building Technologies

Fire Safety & Security Product

Data and design subject to change without notice. / Supply subject to availability.
© 2009 Copyright by
Siemens Building Technologies AG

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

Table of contents

About this document

Purpose of this document

This manual is a guide to the configuration procedures for the integration of SiPass Access Control system in the DMS8000 systems: MM8000 management station and MK8000 OPC server. It is specifically for those individuals responsible for the commissioning of the management station, such as technical project managers, engineers, and commissioning personnel.

This guide is part of the general DMS8000 documentation set which includes the Composer Technical Manual, the other DMS8000 Connectivity Guides (Network/Fire/Intrusion, Video, and OPC), and the Installation, Configuration and Commissioning manual (ICC) for each specific product.

Target audience

This documentation is intended for the following users:

- Project Managers
- Project Engineers
- Commissioning Personnel

Individuals performing the operations described in this manual are expected to have prior expertise and training in the field of security, at least a moderate level of familiarity with the Siemens Building Technologies product line, and experience with the installation, configuration, and commissioning of security management systems.

Documentation resource information

A new document has been created to assemble in one place important information regarding documentation resources. This document contains the following:

- Comprehensive definitions of the target audiences for Siemens FS DMS documents
- Training program information including the Siemens intranet link
- A complete list of all available DMS8000 documents
- Instructions for how to obtain a document via the Siemens intranet using the STEP Documentation Repository System
- A map of relevant documents for each target audience group
- Customer Support links & resources
- A glossary containing definitions of all terms and acronyms used in DMS8000 documentation

To access the *DMS8000 MP4.20 Documentation Resource Information Guide* (STEP #A6V10089056), go to the link and follow the instructions below:

https://workspace.sbt.siemens.com/content/00001123/default.aspx

1. Click on the "STEP WEB Client" image: 

Choose "04 Fire -3F" from the "Product Segment" box and select “Activate filter”.
2. Select “All” in the Documents section of the Quick Search page and select “Advanced Search”.
3. Enter the document number in the “Brochure No.” field (A6V10089056) and press “Enter”.

Operational and safety regulations

Before beginning work on the DMS8000 systems, you must have read and understood the related documents, in particular the Safety Regulations included in the Installation, Configuration, and Commissioning manual (ICC) for each specific product.

Liability disclaimer for damage or injuries

Before products are delivered, they are tested to ensure they function correctly when used properly. Siemens disclaims all liability for damage or injuries caused by the incorrect application of the instructions, or the disregard of danger advisories. This disclaimer applies in particular to personal injuries or damage caused by:

– Improper and/or incorrect use.
– Disregard of safety instructions in the documentation or on the product.
– Poor maintenance or a lack of maintenance.

We have checked the contents of this manual for agreement with the hardware and software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual are reviewed regularly and any necessary corrections included in subsequent editions. Suggestions for improvement are welcome.

Modification index

Version	Date	Notes
A6V10062451_a_en	06.2009	Corresponds with DMS8000 MP4.20
A6V10062451_a_en	06.2008	Corresponds with DMS8000 MP4.15
A6V10062451_a_en	06.2007	Corresponds with DMS8000 MP4.10
009424_b_en	06.2006	Corresponds with DMS8000 MP3.20

1 Introduction

This is a guide to the software configuration procedures for the integration of Si-Pass Access Control systems in the MM8000 Management Station and MK8000 OPC server.

For a complete guide to the configuration process, this manual should be used with the DMS8000 Network, Fire and Intrusion Guide, and with the Installation, Configuration and Commissioning manual (ICC) of the specific product.

SiPass

SiPass is an access control system that monitors and controls access to a site. It is a complete system that packages all access control needs into a single application.

DMS8000 products and SiPass can coexist in the same installation; SiPass and MM8000/MK8000 servers can run on the same machine or on different networked PCs. Client functions may also be combined on the same PC.

→ The exact SiPass software version to use in the integrated systems is indicated in the latest MM8000 or MK8000 Release Notes.

Software License

A specific license id required for enabling the SiPass integration functions in MM8000.

→ Please refer to the local sales support for more details about MM8000 licenses.

1.1 What has been changed in MP4.20 configuration tools

Access Control tools have not changed in MP4.20.

In MP4.20, the **SiPass Entro** units are supported applying the same configuration procedure. The related devices (ACC-lite central controllers, DC12/DC22 and DC800 door controllers, PD30/40 readers, and IOR6 I/O relays) are also supported. All objects are imported during the standard import/alignment procedures.

An improved description of the procedure to **change the user account used to launch the SiPass server** is provided at p.15.

Also, a brief section about how to **simulate** the SiPass system for MM8000 tests is provide at p.17.

2 Configuring SiPass Access Control System

2.1 SiPass integration

The DMS8000 systems MM8000 and MK8000 can support the integration of SiPass access control system in order to provide for a comprehensive security solution.

Currently, the integrated solution with MM8000 management station can:

- Substitute the existing MM8000 functionalities for the SiPass functions related to door event management, thus harmonising the entire event treatment of the safety and security devices.
- Handle the AC users and access permissions configuration using the SiPass software integrated into the MM8000 user interface.
- Allow for basic door statuses and control commands from the MM8000 text pages and graphic maps.
- Store the security-relevant AC transactions (e.g. access denied) in the MM8000 history database.
- Support the connectivity to ACC controllers over a LAN network.

Instead, the integrated solution with MK8000 OPC server can:

- Allow for door statuses and control commands to be mapped in OPC items.

2.2 SiPass Driver

The Access Control integration requires a basic communication infrastructure between MM8000/MK8000 and SiPass software; this is actually a software driver.

In Composer, the SiPass Driver should be added to the MM8000/MK8000 main station in order to enable the SiPass configuration functions.

The Fig 1 below illustrates how to add the SiPass driver to the MM8000 configuration:

1. In the MM8000 physical configuration, select the main station name:

Supervisor System Settings → MM8000 System → Physical configuration → <Station name>

In the MK8000 project, the selection is quite similar:

MK8000 System → MK8000 → Physical configuration → <Station name>

2. Click the button A to add the driver (see Fig 1).

→ *A new node is added. No further configuration is required by the driver.*

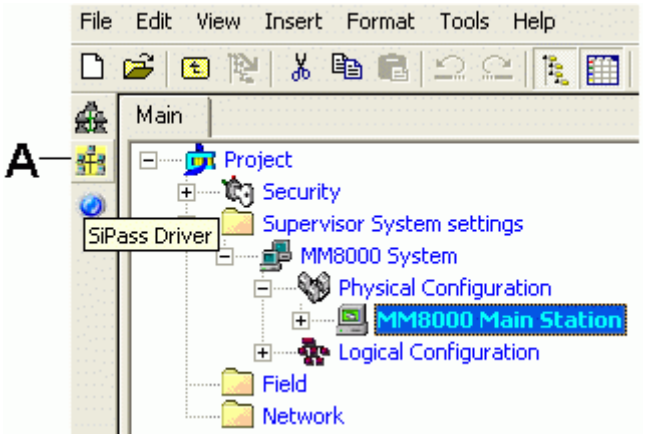


Fig 1 Adding the SiPass Driver (A)

Note: The Composer plug-in #252401 is required.

2.3 Configuration checklist of SiPass

Verify that you have satisfied the items needed in the first checklist before proceeding to the configuration procedure that follows.

ITEMS NEEDED FOR CONFIGURATION

☐ The SiPass system should be configured and reachable, either locally (on the same PC as MM8000/MK8000) or over the network, for importing the SiPass database into the Composer structure.
Alternatively, the SiPass export file (.XML) should be created, using the utility available in MM8000/MK8000 (SiPass Export Tool), and then imported off-line into Composer.

☐ Plug-ins needed:
- Plug-in #252501, which must be installed before you can configure your system.

2.4 Configuration procedure

The following are the configuration procedures for SiPass.

Adding the SiPass Driver

1. Open the Composer project.
2. If not already done, add the **SiPass Driver** (→ see 2.2 at pag.5).

Adding the folder for the Access Control

- Optionally, add one or more folders.

Adding the SiPass subsystem

1. Select the destination folder.
2. In the left-hand bar, select the **Access Control** folder 
and then the **SiPass** icon  .

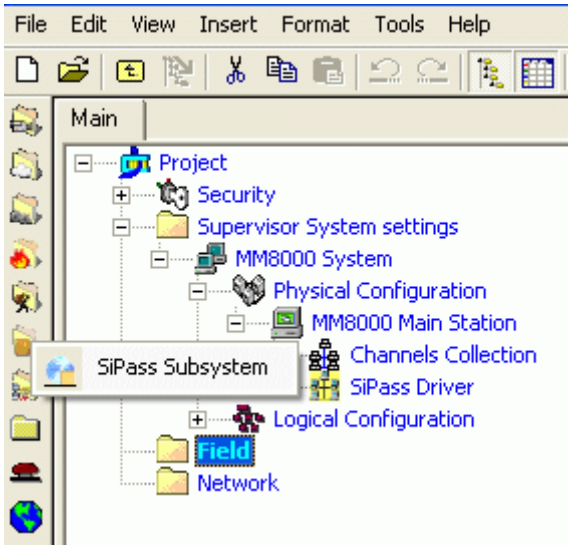


Fig 2 Adding the SiPass subsystem

Linking the SiPass subsystem to the SiPass Driver

You have now to link the subsystem to the Driver.

1. Select the **SiPass subsystem** node.
2. Drag and drop it on the **SiPass Driver** (Fig 3).

A new link node appears.

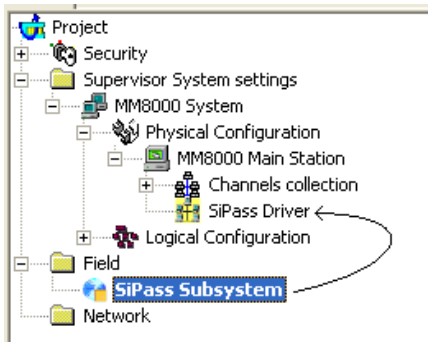


Fig 3 Linking the SiPass subsystem

Setting the SiPass server address

In this step, you have to specify the network name or address of the SiPass server.

1. Select the **SiPass Subsystem** node.
2. Select the **Node** tab.

   Note: Here you can customise the node name in the **Description** field.
3. In the **Computer Name** field, enter the IP address of the SiPass server PC.

   There are two possible cases:

   – The SiPass server is the same as for MM8000/MK8000. In this case, the default IP address 127.0.0.1 is valid in any case.

   – The SiPass server is another PC on the network. If so, enter the IP address or the PC name.

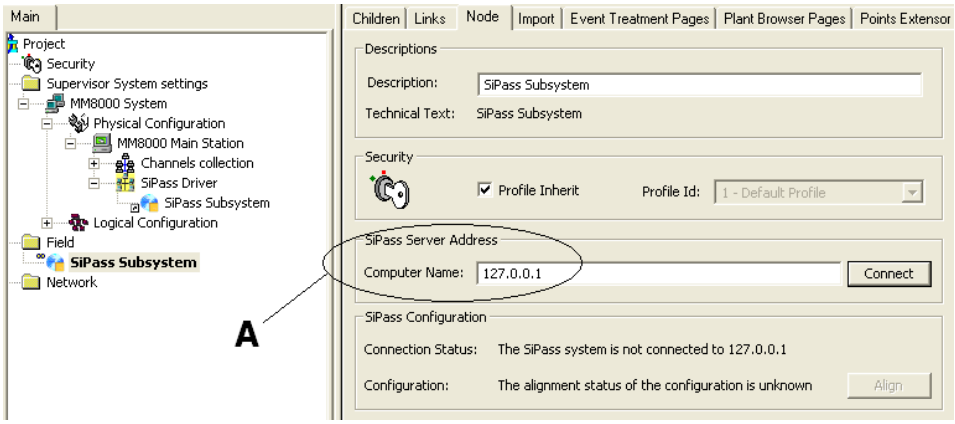


Fig 4 Setting the SiPass Server IP address

A	Enter the PC name or IP address of the SiPass server. Note that the value 127.0.0.1 is always valid if the SiPass and MM8000/MK8000 servers are installed on the same PC.

Setting up the SiPass configuration structure

The SiPass configuration can be imported into Composer in order to allow a fast and seamless alignment process between the two systems.

There are two ways to import the configuration:

A. On-line mode: the SiPass server is accessible over the network and the configuration data can be acquired directly.

B. Off-line mode: the SiPass server is not yet accessible over the network and the configuration data can be acquired by means of an export file.

Importing the SiPass configuration: on-line mode

In the first case, once the SiPass server name is properly set, you can proceed as follows:

1. Click the **Connect** button.

   ➔ *A connection with the SiPass server is established.*

   In a few seconds, the **Connection Status** will indicate the successful connection (Fig 5).

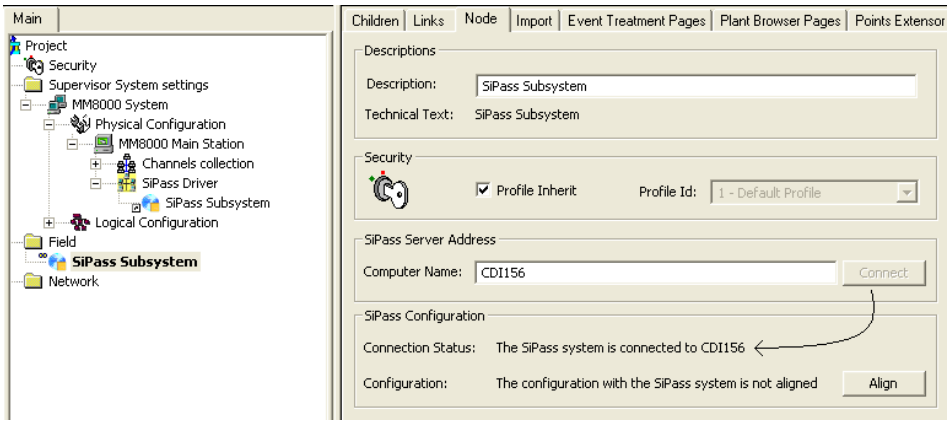


Fig 5 Connecting to SiPass server for on-line configuration

If the connection fails, an error message appears (Fig 6). In this case, check that:

– The network connection is working (e.g. use the Ping command).

– On the server machine, the SiPass software is running properly.

Fig 6 Error in connecting to SiPass server

2. Click the **Align** button.

➔ *The SiPass configuration data is transferred over the network to Composer.*

In a few seconds, the configuration status message will show "**system is aligned**" and the SiPass structure will become available in the Composer tree (Fig 7).

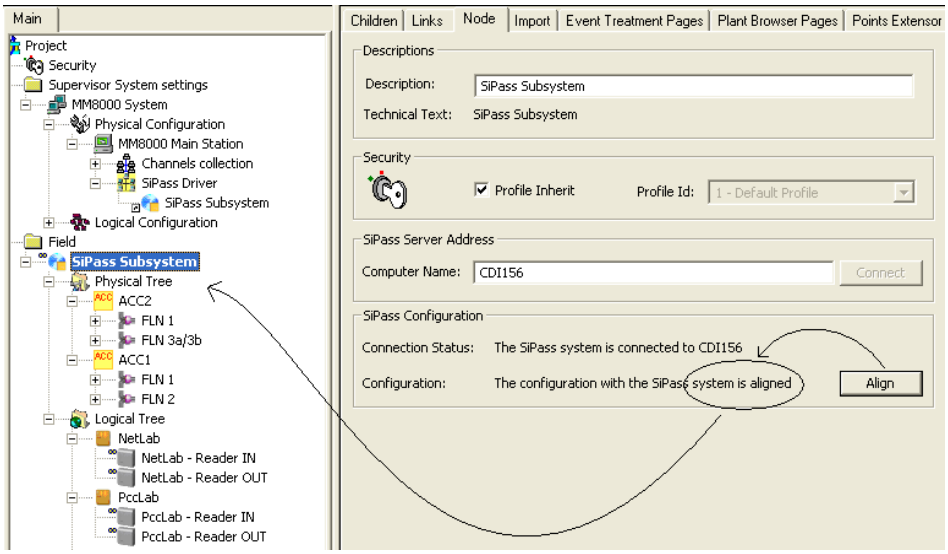


Fig 7 Transferring SiPass configuration

3. While the connection with SiPass stays active, any modification in the SiPass configuration is detected by Composer. If the configuration status shows "**system not aligned**" again, it means that a new import is necessary: just press the button Align as described above. The modified objects will be imported without affecting the remaining part of the structure.

Importing the SiPass configuration: off-line mode

If the SiPass server cannot be directly connected to the PC running Composer, an off-line mode is available. On the SiPass server, you need to run the utility program **SiPass Export Tool**, available on the MM8000/MK8000 CD, and create an export file (there is no need to install the entire MM8000 or MK8000 on the SiPass server).

The SiPass Export Tool can create an XML file containing the SiPass configuration, which can then be imported into Composer. The Fig 8shows the simple utility interface: you just need to indicate the SiPass IP address or name (the default value 127.0.0.1 is valid if running locally on the server) and the export file name, then click Create file to proceed.

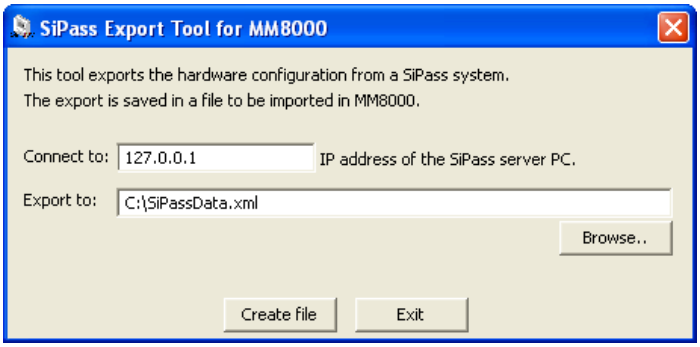


Fig 8 Exporting SiPass configuration

Then, the resulting XML file can be imported into Composer with the following procedure:

1. Select the **SiPass Subsystem** node.

2. Select **Tools→Import** or right-click the SiPass node and select Import (Fig 9).

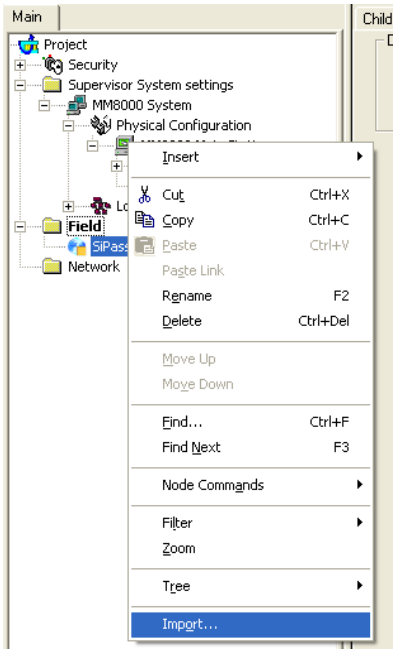


Fig 9 Start SiPass off-line import

➔ *After a confirmation request, the software presents a browsing window to search for the file to import (a file with extension XML is expected).*

3. Using standard Windows controls, do the following:

– Locate the file

– Select it and click **Open** (Fig 10)

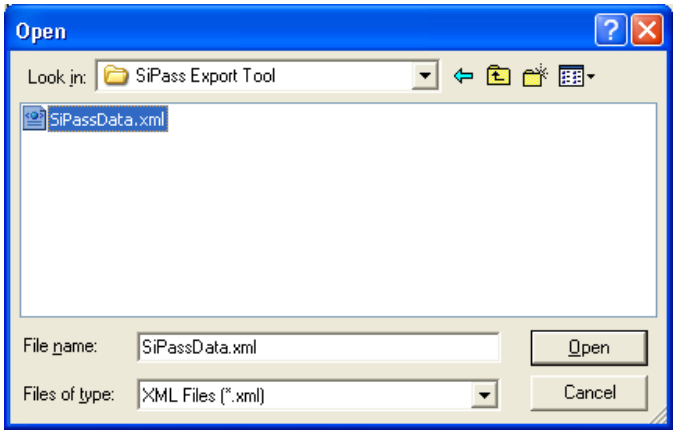


Fig 10 Selecting the SiPass XML file

➔ *In a few moments, the SiPass structure is imported, and the node is represented in the Composer tree.*

Selecting the **Import** tab results in a page report being displayed. This page contains the detailed logs of the latest import procedure, including all the added (or removed) objects.

Customising the SiPass configuration point (MM8000 only)

Once the SiPass structure is imported, it is ready to be downloaded. However, in MM8000, customisations are possible as for the other points. Namely:

- In the **Point Extensor** tab of each individual point, customise the description and icon (Fig 11).

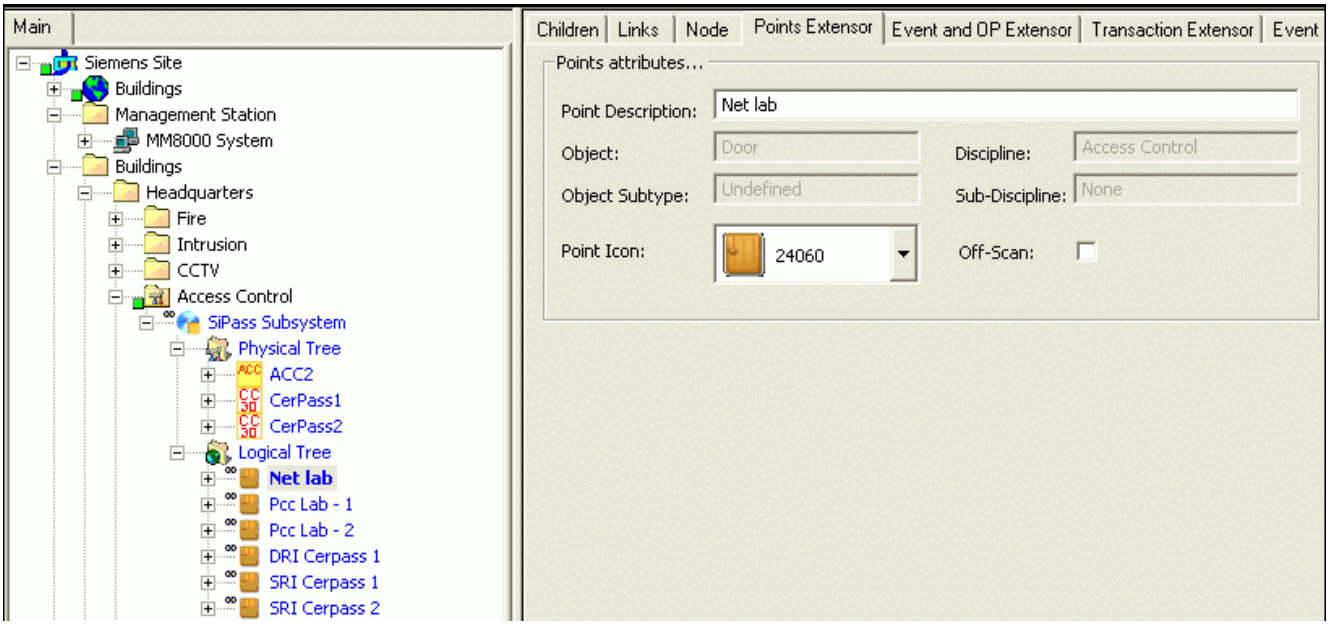


Fig 11 Customising individual SiPass points

- In the **Event and OP Extensor** tab of each individual point, customise the options of an event (e.g.: modifying the event settings for the properties as in Fig 14).

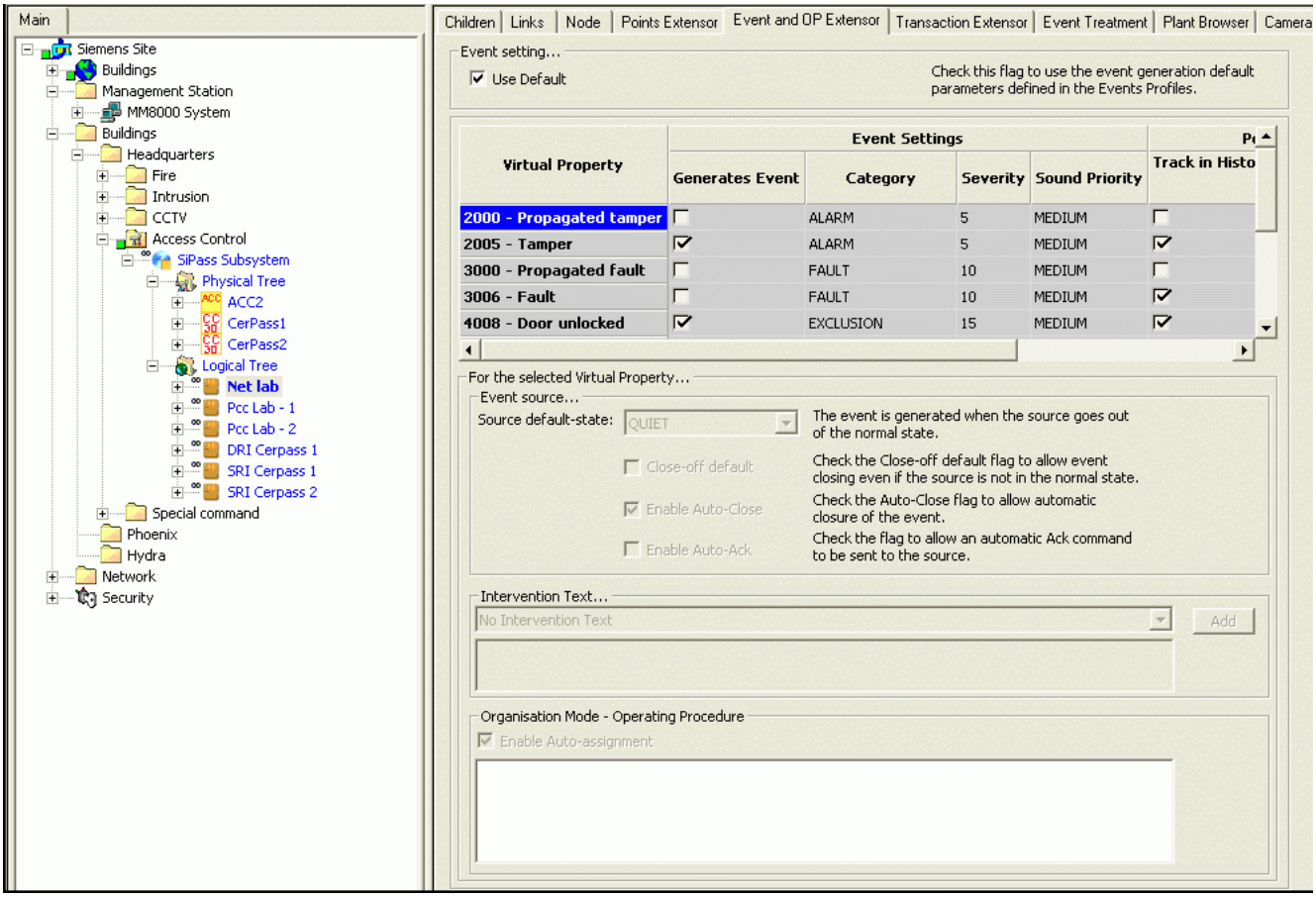


Fig 12 Customising individual SiPass points event setting

- In the **Transaction Extensor** tab of each individual point and transaction, customise the log options (e.g.: enabling/disabling properties as in Fig 13).

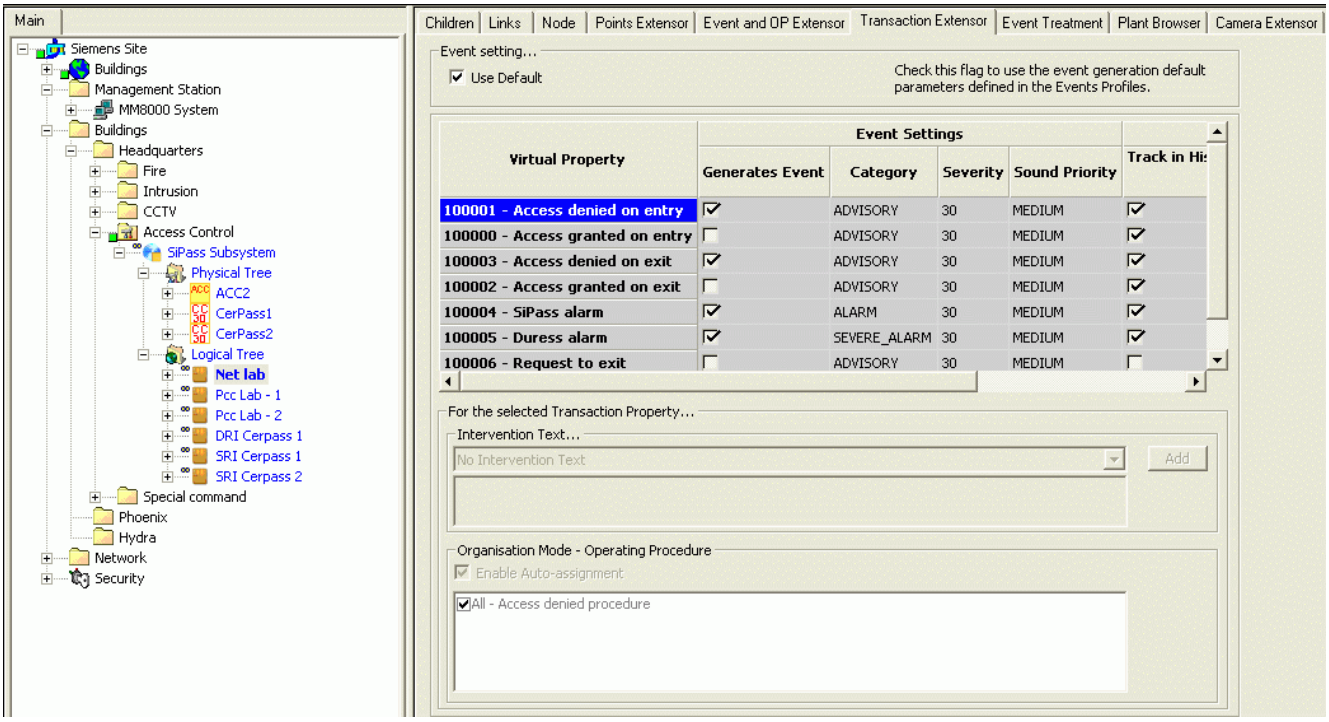


Fig 13 Customising individual SiPass log options

- In the **Style** tab of **MM8000 system - Logical configuration - User Data - Event and Points - Style**, customise the options of a class of points (e.g.: modifying the event settings for the properties of Door points as in Fig 14).

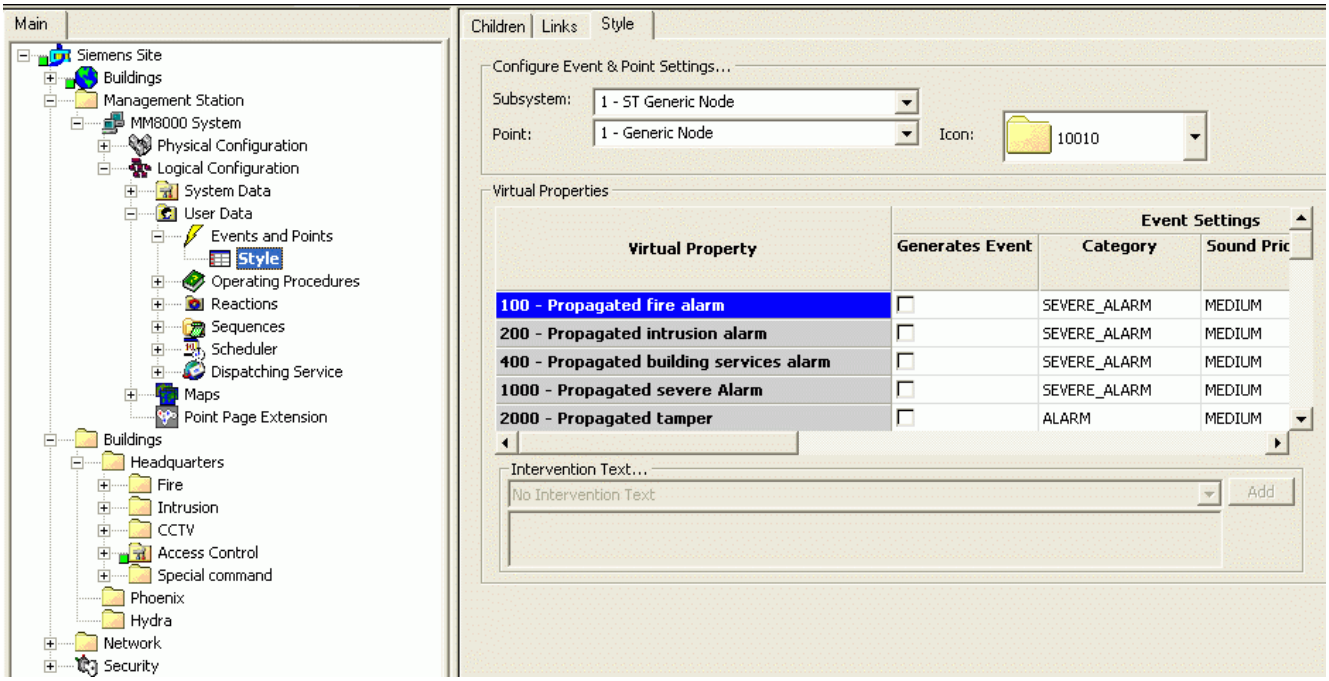


Fig 14 Customising event settings of SiPass Doors

2.5 Further SiPass configuration notes

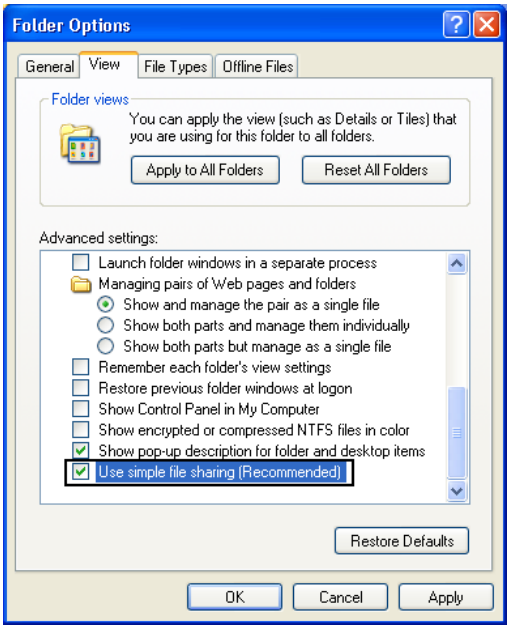
2.5.1 Tips and hints

- **SiPass configuration (MM8000 only)**. In order to work with MM8000, the SiPass configuration must include the following:
  - Users authorised on both MM8000 and SiPass have to be configured in both environments with balanced permissions (MM8000 security profiles and SiPass Operator Group functions).
  - In SiPass, the common Operator(s) must be enabled to Automatic Logon as Windows users. In the Operator form, click the **Use the Windows logon** option and then select the correspondent MM8000 Domain and User.
- **SiPass license**. In order to work with MM8000 or MK8000, SiPass requires a software license. Please refer to the SiPass documentation.

Known issues and limitations

- **SQL Server**. In the integrated system on the same server PC, the SQL Server (MSDE) has to be installed by SiPass, which must therefore be installed first.

  If you have installed MM8000/MK8000 before SiPass, do the following:
  - Uninstall MM8000 or MK8000 and reboot
  - Uninstall MSDE and reboot
  - Delete the MSDE folder, typically C:\Program Files\Microsoft SQL Server
  - Install SiPass
  - Re-install MM8000 or MK8000 (refer to the ICC manual).
- **Reader name, FLN name and structure**. This information cannot be acquired from SiPass; this prevents MM8000 and MK8000 from representing the entire physical structure of the devices.
- The **SiPass functions which are also available in MM8000** - e.g. event notification (message forwarding in SiPass), reactions and sequences (event tasks in SiPass) - should be clearly assigned to either of the two systems, according to specific requirements, thus preventing any functional overlap.
- In SiPass 2.40 and later, note that the **SiPassUser** password, required for MM8000 communication, must be in uppercase: **SIPASSPASSWORD**.
- In case of communication problems between MM8000 and SiPass, make sure not to check the Windows Explorer folder option: **Use Simple File Sharing** (select **Tools→ Folder Options** in the Explorer menu and then click the **View** tab as illustrated here below). This option should NOT be enabled on the SiPass server PC.



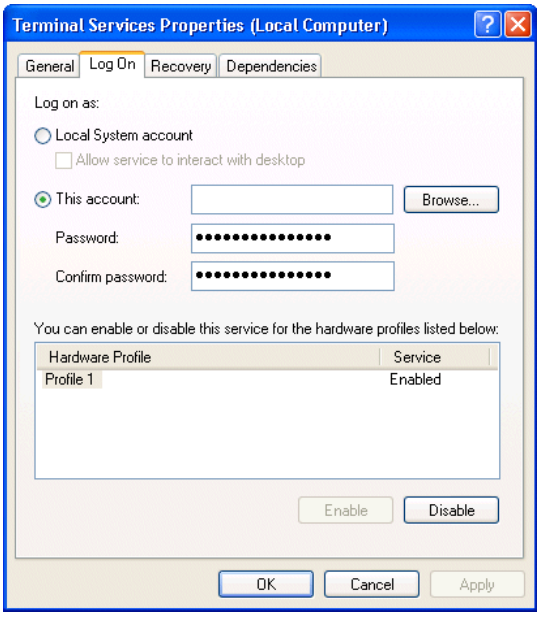
- **If the SiPass server does not run on the same PC as MM8000**, then specific installation steps are required on the networked PC where SiPass is installed:

  1) In the Windows user list, the SiPass PC should include the MM8000 *Internal User*, by default **DMS8000_Proc**. Use the same username and password as on the MM8000 PC. Refer to MM8000 ICC Manual (doc.no.A6V10062413_a_en).

  2) In the **SiPass Server Properties**, modify the Logon option in order to use the MM8000 *Internal User* as Logon account.

  Perform the following steps:

  1. Log on to the PC with the SiPass server.
  2. Right-click on **My Computer** and select:
     System Tools → Local User and Groups → Users
  3. Add the new user **DMS8000_PROC** and assign administrator rights (for detailed instructions, please refer to the Windows documentation).
  4. Right-click again on **My Computer** and select:
     Services and Applications → Services
  5. Double-click on the **SiPass** service and select the **Log On** tab.



6. Click the **This Account** button and then select **Browse**
7. In the **Select User** window, select the **Advanced** button
8. Select **Find Now** and then **DMS8000_PROC**
9. Restart the PC

From MM8000, select **Change Server** in the Composer Properties Management window, and select the SiPass server to connect.

2.5.2 SiPass alarm classes

In the integrated system, the use of SiPass **Alarm Classes** requires a special attention. In fact, MM8000/MK8000 can receive and then present the SiPass events only if:

- **Alarm Class Type** is Input (no Outputs, Access or any other type)
- **Alarm Handling** is set to “Require Acknowledging”
- **Alarm Options** do not include the “Restorable Alarm”
- The definition includes all the possible input states of the object (e.g.: **Door forced** and **Door held**, etc.)

In general, whenever possible, **we recommend not configuring any Alarm Classes in SiPass**. When necessary, specific needs cases can be handled as follows:

- For Input Alarm events, use SiPass Input activation status, assigning a category, e.g. Alarm, in the **Event and OP Extensor** tab of the Composer point.
- In other cases, you can use controller event tasks to activate an assigned input and then, in turn, use this input to generate a message to MM8000/MK8000.

This approach allows getting the current Input state properly displayed in MM8000 (or processed by MK8000) and the event being closed only when the corresponding Input is in quiet state. Also, the same event is used for subsequent triggers, i.e. if the input is re-activated while the event is still open. The event handling in MM8000 is therefore fully standard.

The table below presents the possible scenarios and the results for the system operator. Refer to this table for any further needs of Alarm Classes when discussing the issue with SiPass specialists.

	Effect in MM8000/MK8000	Effect in SiPass
No Alarm Classes defined	Event generation and transactions (within the documented limitations) as configured in Composer by default. Door alarms received and displayed as Severe Alarm.	No alarm pop-ups. Registrations in audit trail.
Alarm Class of any point type configured as: **No Acknowledge required**	No additional event.	No alarm pop-up. Registrations in audit trail.
Input Alarm Class configured as: **- Acknowledge required** **- Not Restorable**	Event generation; **point status is not visible**. Event closing always possible regardless of the point status. Subsequent events from this point are displayed as new events. **Input activation Advisory never receives and displays the Inactive point state.**	No alarm pop-up of this input. Registrations in audit trail.
Input Alarm Class configured as: **- Acknowledge required** **- Restorable**	Event generation; **point status is not visible**. Event closing always possible regardless of the point status. **Re-activated events (triggered by the Restorable "Once actioned … " option) are no more received.** Input activation Advisory receives and displays the Inactive point state.	No alarm pop-up of this input initial event. **Re-activated pop-ups are displayed if the input remains active.** Registrations in audit trail.
Alarm Class of any other type but Input configured as: **- Acknowledge required** **- Restorable**	None	**Alarm pop-up not removable → "freezing" SiPass client.**
Alarm Class of any other type but Input configured as: **- Acknowledge required** **- Not Restorable**	None	Alarm pop-up Registrations in audit trail.

Check latest MM8000 Release Notes for version compatibility and limitations.

2.5.3 SiPass Filed Simulator

A simulation function is available for simulating the SiPass events in MM8000. However, this is not part of the Field Simulator described in the Appendix A of MM8000 Installation, Configuration, and Commissioning manual (ICC).

Activating the SiPass simulator

The SiPass field simulator can be activated by selecting the **Children** tab of the **SiPass driver** and clicking the **Simulation** checkbox. The simulator is started automatically when MM8000 server restarts. It can also be started manually from the folder:

<installation folder>\Utilities\Field Simulator\SiPassSimulator.exe

The SiPass Simulators only works properly when:

- The actual SiPass server is NOT running. Make sure to stop the **SiPassServer** service in the Windows service list.
- The PC is physically connected to a LAN network (valid network cable plugged in).

Siemens Switzerland Ltd
Building Technologies Group

International Headquarters
Fire Safety & Security Products

Gubelstrasse 22
CH-6301 Zug

Tel +41 41 724 24 24
Fax +41 41 724 35 22

www.sbt.siemens.com