

SiPass integrated MP2.75/2.76 Software Installation & Update V1.2

Intern © Siemens AG 2019

www.siemens.com/SiPass

ZIN



SiPass integrated MP2.75/2.76 Software Installation & Update V1.2

Table of contents

1. PC requirements	. 3
2. Database information	. 4
3. SQL / SQL Express Database installation	. 5
4. IIS installation	. 5
5. SiPass License example	. 6
6. SiPass integrated installation	. 7
7. Renew certificate	19
7.1 Renew self-signed certificate	19
7.2 Renew remote client certificate (based on the self-signed Server certificate)	20
7.3 Renew Machine certificate	22
8. Manage the SiPass Certificates	23
8. DEMO installation	26
8.1 DEMO features	27
9. SiPass integrated login	28
10. SiPass Client installation	29
10.1 Client certificate invalid/expired	34
11. Update of SiPass features	36
12. SiPass integrated Upgrade Paths	38
13. SiPass integrated Web Client	40
14. Recommended SQL database settings	44

1. PC requirements

Operation System	Windows 7 (Pro&Ent.) SP1 (32- bit & 64- bit)	Windows 8.1 (32-bit & 64-bit)	Windows 10 Pro/Ent.	Windows Server 2008 R2 (SP2)	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019
SiPass MP 2.75	1	1	1	1	1	1	Since 2.76

SiPass Server System Requirements:

Note:

SiPass 2.76 only supporting 64 bit operating systems

Microsoft SQL	SQL 2017*	SQL 2017* Express	SQL 2016*	SQL 2016* Express	SQL 2014	SQL 2014 Express	SQL 2012 SP2	SQL 2012 SP2 Express
SiPass MP 2.75	1	1	1	\checkmark	1	1	1	1

* SQL 2016/2017 is not compatible with 32 Bit OS like Win 7, 8 or 10. Windows 7 in general is incompatible with SQL 2016/2017

- Memory 8 GB (minimum), 16GB Recommended
- Hard Disk Drive 100 MB
- Ports Ethernet 100Mbit / 1000Mbit (1000 Mbit Recommended)
- Intel core i5 or higher (5th generation or above)

Please also check:

Please check always the documentaions located at each SiPass DVD concerning latest information related to supported Operating System and Database versions. Also take care for *"Release notes"* and *"System limits"*.



2. Database information

SiPass setup offers the possibility to install SQL express in front for the SiPass installation (see page 10). If Windows Server 2016 or Windows 10 is used SQL Express 2017 will be installed, SQL 2014 SP2 Express for any other compatible operating system.

The SQL Express Edition database applications have been limited by Microsoft. As the database transactions increase, the performance of database application will decrease.

As a rule of thumb, a SiPass integrated Server used in conjunction with either of these versions of SQL should not exceed <u>10,000 cardholder</u> or <u>100 readers</u>, or <u>5 workstation clients</u>. Whilst some trade-offs can be made between these numbers or lower traffic sites can quite happily exist, larger installations should purchase the full SQL Server database license to ensure the integrity of their system at all times.

For the SQL database installation please refer to the "SiPass integrated Installation Manual".



3. SQL / SQL Express Database installation

Manual SQL-installation:

Because during the manual SQL installation some points must be considered! See "SiPass integrated Installation Guide.pdf"

Automatic SQL-installation:

If the SQL-Server is not preinstalled at the SiPass-Server the SiPass setup will automatically install SQL2014 SP2 or 2017 Express.

Attention:

! The SQL server and the SiPass Server have to be installed on the same PC!

4. IIS installation

The Internet Information Service (IIS) is needed if the SiPass Web-clients will be used. IIS must be enabled before SiPass integrated setup is started. For Windows 10 following steps must be performed:

- 1. Navigate to "Program and Features"
- 2. Select "Turn Windows features on or off"
- 3. Select and expand "Internet Information Services"
- 4. Select and expand "World Wide Web Services"
- 5. At section "Application Development Features", select the following options: - .NET Extensibility

 - ASP.NET
 - ISAPI Extensions
 - ISAPI Filters
- 6. After the setup of the IIS the SiPass integrated setup can be started



5. SiPass License example

The license is containing all options ordered via SAP, the SiPass integrated order form is needed additional. During the installation the license information has to be entered exactly as defined in the license.

The information in the last square (Modules) will be added automatically from the setup application.

The license has to fit for the SiPass integrated software version! <u>E.g. a license from SiPass 2.70 can't be used for SiPass 2.75.</u> But any 2.75 license can be used to setup 2.76 (CCTV stations have to be 0)

Copy and paste is faster than entering it Product Name: SiPass ACC 2.75 manually: Version: 2.75 Site Name: License Information: SiPass Training Site Name: SiPass Training Serial Number: 3723 Serial Number: Licence Kev: W1PXA-YK2DE-54MAJ-3MP5D-VY1A1 3723 Card Technology: Siemens Readers ClkData/RS485 Licence Key: Facility 1: 0 Site 1: 0 W1PXA-YK2DE-54MAJ-3MP5D-VY1A1 Number of Buses Workstations 20 0 *Configuration and Operation Client HR Interface Clients Number of CCTV Stations 0 1 counted independed. OPC A&E Clients 0 Web Clients 20 With the license example at the left it is Card Expansion Door Expansion 500 50 possible to start 20 times a Config and 20 times a Operation Client. Modules: Photo ID and Image Verification Graphics on on Guard Tour off off Messenger Low Level Elevators Time & Attendance Export on on Smart Card Encoding OPC A&E Server Interface off on 3rd Party DVR Interface off Visitor Management on Data Synchronizer Apogee Interface off on High Level Elevators off Siemens Corporate Card off off MM8000 Interface Intrusion on Unrestricted Page 6 Generic DVR API off Management Station API on SALTO Integration on

Example Trainings license



6. SiPass integrated installation

Make sure you have the customer license on hand.

A SiPass integrated MP (Marked Package) update will need a new license! (Exception is an update from 2.75 to 2.76)

For customer installations use the customer license not the "DEMO"-license. The "DEMO"-license will install features which will not be uninstalled during the license-update.

For more detailed information please refer to the "SiPass integrated Installation Manual".

Info:

It is possible that the setup requires a restart of the PC. If the installation will not automatically continue just restart the installation again.

SiPass 2.76 requires a manually Java installation in front to the SiPass setup. The setup file for Java can be found on each SiPass DVD image: \SiPass integrated DVD image\Prerequisites\Java Runtime Environment 8.

To start the SiPass integrated setup please execute the **"Install.exe"** from the DVD image root as <u>Administrator (right click -> run as Administrator)</u>.

The setup checks first the PC environment an install necessary system application.

Microsoft not allowing a hidden installation of the below listed applications. This is the reason all need to confirm terms and conditions one by one.

SiPass inte	grated - InstallShield Wizard			
نا ۲	Pass integrated requires the following items to be installed on your computer. Click istall to begin installing these requirements.			
Status	Requirement			
Pending	Microsoft .NET Framework 4.7.1			
Pending	Microsoft Visual C++ 2017 Redistributable Package (x86)			
Pending	Pending Microsoft Visual C++ 2013 Redistributable Package (x86, all)			
Pending	Microsoft ODBC Driver 13 for SQL Server (x86)			
	Install Cancel			

After the pre-setup is finished the SiPass integrated setup starts with the Welcome dialog. On the next page the license agreement has to be accepted.



😸 SiPass integrated Setup	×	😸 SiPass integrated Setup
<u>ح</u>	Welcome to the SiPass integrated Installation Wizard	License Agreement Please read the following license agreement carefully.
	It is strongly recommended that you exit all Windows programs before running this setup program.	Siemens SiPass End User License Agreement
ΔA	Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation.	Important: this software end user ilcense agreement (EULA) is a legal agreement between you (either an individual or, if purchased or otherwise acquired by or for an entity) and Siemens. Read it carefully before completing the installation process and using the software. It provides a license to use the software and contains warranty information and liability disclaimers. By selecting the next button and using
	WARNING: This program is protected by copyright law and international treaties.	the software, you are confirming your acceptance of the software and agreeing to become bound by the terms of this agreement. If you do not agree to be bound by these terms, you must choose exit to cancel the installation.
	Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.	I accept the terms in the license agreement Print I do not accept the terms in the license agreement
	< Back Next > Cancel	InstallShield < Back Next > Cancel

In the next dialog has to be defined which hardware platform is used, because SiPass integrated can migrate an older systems called Advantage NT.

😸 SiPass integrated Setup	
Hardware type	4
Select the hardware type.	0
	ACC Platform
	C ACC / NT Platform
InstallShield	
	< Back Next > Cancel

The ACC platform is for SiPass integrated in conjunction with ACC door controllers: ACC AP, AC5102, AC5200, AC5100 or the Granta Controller.

The ACC/NT Platform is for SiPass in conjunction with the "Advantage NT" and ACC door controllers.

On the next dialog you have to enter license information (see 5. SiPass License example).



😸 SiPass integrated Setu	e San	BiPass integrated Setu	μ		8
License Options Enter the license inform	ation.	License Options Enter the license inform	mation.		さ
Site Name:	SiPass Training	Workstations:	20	Number of Busses:	0
Serial Number:	3723	HR Interface Clients:	1	Number of CCTV Stations:	0
License Key:	W 1PXA - YK2DE - 54MAJ - 3MP5D - VY1A1	OPC AE Clients:	0	Web Clients:	20
Card Technology:	Siemens Readers ClkData/RS485	Card Expansion:	50	Door Expansion:	500
Site:	0 Facility: 0				
InstallShield	< Back Next > Cancel	InstallShield		< Back Next >	Cancel

The installed features and options for "Typical" and "Complete" installation will be explained in the original "SiPass Installation Manual".

To configure the installation choose "Custom" (always recommended).



In the "Custom Setup" dialog you can select the features you want to install.





The following symbols are used in the "Custom Setup" dialog:



This package will be installed as part

All the system features of this package will be installed

No system features will be installed

The installation path can be defined if the "Server" is selected.

関 SiPass integrated Setup	— ×-
Custom Setup Select the program features you want installed.	と
Click on an icon in the list below to change how a feature is in:	stalled. Feature Description The Server communicates with the security hardware and the SiPass database. This feature requires 7893KB on your hard drive. It has 1 of 1 subfeatures require 2752KB on your hard drive.
Install to: C:\Program Files\SiPass integrated\	Change
Help Space < Back	Next > Cancel

Click Next and select the SQL Instance you want to use for the SiPass integrated system.



📅 SiPass integrated Setup	
SQL Options Enter the SQL Server information	さ
Please select a local SQL Server instance:	
Use existing SQL Server instance:	(local) 🔻
Install MSSQLSERVER instance of SQL Expression	ess 2014 SP2 and use it.
If you wish to install a SQL Server version o not yet done so, you must exit the installati desired SQL Server product.	ther than SQL Express 2014 SP2, and have on by choosing Cancel and install your
InstallShield	Back Next > Cancel

If no SQL is available at the SiPass Server PC or the existing SQL installation is not compatible with SiPass integrated, SiPass setup can install a SQL 2014 Express (Win 7, 8.1, Server 2012) or SQL 2017 Express (Win 10 or Server 2016).

😸 SiPass integrated Setup	•••
SQL Options Enter the SQL Server information	と
Please select a local SQL Server instance:	
O Use existing SQL Server instance:	-
Install MSSQLSERVER instance of SQL Express 2	014 SP2 and use it.
If you wish to install a SQL Server version other not yet done so, you must exit the installation b desired SQL Server product.	than SQL Express 2014 SP2, and have y choosing Cancel and install your
InstallShield < Back	Next > Cancel

Each SQL database installation needs to have an "SA" administrator set.

SiPass integrated setup 2.75 set the SA password in the background.

This PW is not needed to know and can be changed, if required by the customer, with help of the SQL Management Studio.



Since MP 2.75 the SiPass Server Service have to be started by a <u>own</u> (dedicated) Windows Account. A Windows standard user account is sufficient (non-admin rights required). Depending on Host Event Task functions it could be necessary to assign the SiPass Service User Administrator rights. E.g. if a DB backup is performed via HET.

The current logged in Windows User is not accepted and an error messages is occurring.

Please note: It is at the moment not possible to change the SiPass Service User afterwards. If this is required SiPass need to be reinstalled with the new Windows User for the SiPass Service.

Tip: enter "LUSRMGR.msc" to the Run Dialogue and create the needed User (if a domain is used the Domain Administrator need to create this Windows use).

😸 SiPass integrated Setu	
SiPass Service Log On Enter the SiPass service	e account information
Log on as:	
User name:	TESTWIN7SL176\SSU must include domain e.g. 'domain \user'.
Password:	•••••
InstallShield	
	< Back Next > Cancel

If you click on —, Windows will open the User selection window where you can search for all user that are configured on the Server PC via the Advanced option.

Select User	Select User
Select User Select this object type: User Object Types From this location: TESTWIN7SL176 Locations Enter the object name to select (examples): Check Names Advanced OK Cancel	Select User Image: Comparison of the second sec
	Name (RDN) In Folder Administrator TESTWIN7SL176 Guest TESTWIN7SL176 HomeGroupU TESTWIN7SL176 Siemens TESTWIN7SL176 SU TESTWIN7SL176 USER TESTWIN7SL176



On the next dialog you can change the Ports for the communication between Sever, Web Client, Web UI and Management station.

The default port numbers must be changed if those are allocated to another application on your system.

闄 SiPass integrated Setup	—
Port numbers for SiPass integrated service Specify the port numbers.	s ~
Various SiPass integrated services below will be a port numbers specified here. You can accept the are already allocated to another application. The than 65535.	vailable to the dients and Web Site at the default port numbers shown unless they port numbers must be positive, and less
SiPass server port:	8741
SiPass server callback port:	8742
Web Service port:	8743
Management Station Service port:	8744
HR API Service Port:	8745
InstallShield	
< E	lack Next > Cancel

only 2.75 not for 2.76.

For more details take a look in the original SiPass[®] integrated MP2.76 IP Security and Network Guide.

The "Ready to Install the Program" dialog is displayed.

😸 SiPass integrated Setup	🔡 SiPass integrated Setup
Ready to Install the Program The wizard is ready to begin installation.	Installing SiPass integrated The program features you selected are being installed.
Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.	Please wait while the InstallShield Wizard installs SiPass integrated. This may take several minutes. Status:
InstallShield	InstallShield
< Back Install Cancel	< Back Next > Cancel



SiPass Authentication Management Wizard is displayed.



Two Certificate options can be used

- 1. Applying an existing Machine Certificate
- 2. Generate and apply Self-Singed Certificate





You can install SiPass integrated Server and Remote Clients using a Machine Certificate or a Self-signed Certificate. While the basic process remains the same in both cases, the difference lies in how the certificate identity is authenticated among the Server and Client Computers.

Self signed certificates (see page 16)

Can be generated through several available tools. However, it is recommended to use the SiPass integrated Authentication Management Wizard for the purpose.

Note: The CA (certification authority) signature is not strong enough to ensure maximum security but this method gives you an automated way of generating and applying the certificates on both the computers and requires minimal manual effort.

Machine certificates (see page 17)

In a Windows domain of an organization, each computer gets a specific machine certificate installed (which is based on a trusted CA). This ensures maximum security at each level.

Note: This method is recommended for ensuring maximum security. However, it requires some effort from the user to look for the installed machine certificate in the Windows Certificate store, copy the Certificate Thumbprint and provide it manually during the authentication process.



If you select Enable High Security, the <u>Configuration Client</u> can only run on the SiPass Server PC itself and not from a Remote Client.



Use Self signed certificates

Select Generate Self-Singed Certificate and click on finish (it take some moments until the certificate are created and applied).

A new certificate is generated and applied to SiPass integrated server and local clients.

The certificate generated in this step will bear the full computer name in its subject.

All the remote clients will use a "child" of this self-signed certificate.





Use Machine certificates

The tree view on the left lists all the different certificate stores you can pick from. Select a certificate store in the left hand side tree view and then select a certificate in the grid on right hand side (populated with all the certificates within this store).

Note: Only the certificates with a private key are listed here.

Click Finish to apply the certificate and start the Installation. The selected machine certificate is applied to SiPass integrated server and any local client.







Setup of SiPass integrated successfully completed.



If the Installer log should be displayed, enable the option before click the Finish button.



7. Renew certificate

The SiPass self signed certificate is 1170 days valid, 30 days before the certificate expires the operator gets an info that the certificate needs to be renewed.

With hep of the *SiPass*.*CertificatePicker.exe* a new self-signed certificate can be created and assigned to Server and Client. This tool is located inside the SiPass installation folder (C:\Program Files (x86)\SiPass integrated).

7.1 Renew self-signed certificate

Start the tool as <u>Administrator</u>. The following dialog will appear.

🗟 Authentication Management (Administrator)					-	\Box \times
Enable High Security	/ (Configuration Client can	run locally only; Operation Cli	ents are not affecte	d)		
Generate Self-Signed	d Certificate					
⊡ · Certificates (Local C	Computer)	Subject	Issuer	Not After	Not Before	Signature Algorithr
Other People	t Cartification Authoritica					
- Internediate Ce	artification Authorities	Win10Ent64EN172	SiPass Root CA	24.09.2022 13:20:13	12.07.2019 13:20:13	System.Security.Cr
Untrusted Certi	ficates	Win10Ent64EN172	SiPass Root CA	29.09.2022 15:55:23	17.07.2019 15:55:23	System.Security.Cr
Trusted Root C Trusted People Trusted Publish	The SiPass integrated Ai	utnentication Managemen s integrated service will nee here are made. Do you wan if you plan to restart the si	t d to be restarted t to stop the servic ervice later)?	if any ce now		
			Yes	No		
		<				>
				Back	Finish	Cancel

We recoment to stop the SiPass-service in front. After that activate that option "Generate Self-Signed Certificate".

The following questions we recoment to answer with "Yes".

SiPass integrated Authentication Management	×		
Would you like to copy the Windows account from the previous certificate to the new certific	permissions ate?		
	SiPass integrated	Authentication Management	×
Yes	? It app Would	ears SiPass is currently using a self-signed certificate. I you like to remove it?	
		Yes No Cancel	



If the procedure was successful you will get the following information.



From this point the remote clients can't connect any more to the SiPass server. To solf this problem also at the remote clients the certificate must be renewed.

7.2 Renew remote client certificate (based on the self-signed Server certificate)

Start the SiPass Configuration-client and open the Client-configuration dialog. It is possible to create for all clients the new certificates in one step.

a Client Configuration - New		-		\times
Win 10Ent 174 Win 10Ent 175 Win 10Ent 176	Configurations Full computer name: [Certificate Thumbprint: Only check thumbprint for authentication Generate Self-Signed Certificate			
Generate All Self-Signed Certificates	New Save Server Thumbprint Save	Delete	Ck	ose

Choose "generat all self-signed certificates" and create a new folder. In this new folder each client will get a separate folder allocated. Now copy the new created remote client certificate to the respective remote client.

At the remote client start the SiPass.CertificatePicker.exe as Administrator.



🗗 Authentication Management (A	Administrator)	_	
Impo	nt Client & Server Certificates	s From:	• 🖻
Server C	ertificate Thumbprint:	6CF11D305EE11855900A990D9A05D90B6762FB47	
- Cer 	trificates (Local Computer) Other People Third-Party Root Certification Intermediate Certification A Untrusted Certificates Personal Trusted Root Certification A Trusted People	Browse For Folder Not Before	Signature Algorithr System.Security.Ci
	Trusted Publishers	 Local Disk (C:) inetpub PerfLogs Program Files Program Files (x86) TEMP Users 	
2		Make New Folder	Cancel

Now just select the correct certificate for this client and agree with two times Yes.

SiPass integrated Authentication Management	×	
Would you like to copy the Windows account from the previous certificate to the new certific	permissions cate?	
	SiPass integrated Authentication Management	\times
Ja		
	? It appears SiPass is currently using a self-signed certificate. Would you like to remove it?	
	Ja Nein Abbrechen	

The now shown certificate-thumbprint is only a information, no additional actions needed.



7.3 Renew Machine certificate

Also for this function the <u>SiPass.CertificatePicker.exe</u> will be used as described above. Instead of creating or importing a new certificate the existing new certificate has just to be selected. After that, in the Client Configuration the thumbprint of this new certificate has to be entered. Now the SiPass Server certificate is changed.

At the remote client side the certificate selection and the possibility to enter the Server certificate thumbprint is in the same dialog.

Start the <u>SiPass.CertificatePicker.exe</u> select the new certificate and enter the Server certificate thumbprint.

Authentication Manage	jement (Administrator)							
Import Client & Server Certificates From:								
	Server Certificate Thumbprint:	74C7F	F959	EC9CB58C73EB5107	9755A153B1C2844	С		
	⊡ · Certificates (Local Computer) … Other People … Third-Party Root Certification Authori	ies		Subject	Issuer	No	ot After	Not Befo
	Intermediate Certification Authorities	e		Win10Ent64EN173	SiPass Root CA	06	.10.2022 13:27:38	24.07.20



8. Manage the SiPass Certificates

For the following described steps it is mandatory to use a Windows Administrator account.

To manage the SiPass Certificates you have to open the MMC console. Open Run (Win +R) and enter "mmc" followed by "OK". The empty Windows Console started

Click on File-> Add/Remove Snap-in-> Select "Certificates" and click on Add.

T I PROVIDE THE REPORT OF THE		
Ctrl+O		
Ctrl+S		
	There are no items to s	how in this view.
Add or Remove Snap-ins		×
You can select snap-ins for this console from th	ose available on your computer and configure the sele	ted set of spap-ins. For
extensible snap-ins, you can configure which e	xtensions are enabled.	
Available snap-ins:	Selected snap-ins:	
Snap-in Vendor	Console Root	Edit Extensions
ActiveX Control Microsoft Cor		Remove
Cettificates Microsoft Cor	=	
Component Services Microsoft Cor		Move Up
Computer Managem Microsoft Cor		Move Down
Device Manager Microsoft Cor Disk Management Microsoft and	Add >	
Event Viewer Microsoft Cor		
Folder Microsoft Cor		
Group Policy Object Microsoft Cor		
IP Security Monitor Microsoft Cor		
IP Security Policy M Microsoft Cor	-	Advanced
Description:		
The Certificates snap-in allows you to browse	the contents of the certificate stores for yourself, a se	rvice, or a computer.
	Add or Remove Snap-ins You can select snap-ins for this console from th extensible snap-ins, you can configure which e Available snap-ins: Snap-in ActiveX Control ActiveX Con	Add or Remove Snap-ins There are no items to s Add or Remove Snap-ins You can select snap-ins for this console from those available on your computer and configure the select extensible snap-ins, you can configure which extensions are enabled. Available snap-ins: Selected snap-ins: Snap-in Windows from the extensions of the extension of th



In the new opened window select "Computer account" and click Next. Select "local computer" and click on Finish.

Certificates snap-in	×		
This snap-in will always manage certificates for: My user account Service account Computer account	Select Comput Select the co This snap-ir	er mputer you want this snap-in to manage. will always manage: omputer: (the computer this console is running on) * computer: Browse	×
< Back Next >	Allow ti only ap	e selected computer to be changed when launching from the command line. This plies if you save the console.	

Expand Certificates -> Personal -> Certificates, here you find all personal "Certificates". Also the certificate generated by SiPass (SiPass Root CA).

ᡖ Console1 - [Console Root\Certif	ficates (Local Computer)\Personal\C	ertificates]		
🚟 File Action View Favorites	s Window Help			
🗢 🔿 🙍 📰 📋 🗟 🛸	?			
Console Root	Issued To	Issued By	Expiration Date	Intendec
 Certificates (Local Compute Personal 	😭 WIN2016EN173	SiPass Root CA	23.06.2021	<all></all>
Certificates				
> In Trusted Root Certificatic				
s 🧮 Enterprise Trust				

To Change the access rights for the users of the certificate select the certificate -> click with right mouse button-> Select "All Tasks"-> "Manage Private Keys..."

Console1 - [Console Root\Certi	ficates (Local C	Computer)\Perso	onal\Ce	rtificates]	
🚟 File Action View Favorite	s Window	Help			
🗢 🔿 📶 🔏 🖬 🗙 (🗐 🔒 🛛 🖪				
Console Root	Issued To	^		Issued By	Expiration Da
Certificates (Local Compute Personal	WIN2016F	Open		SiPass Root CA	23.06.2021
 Certificates Trusted Root Certificatic 		All Tasks	>	Open	
 Enterprise Trust Intermediate Certificatic Trusted Publishers 		Cut Copy		Request Certificate with New Renew Certificate with New	/ Key Key
> 🧮 Untrusted Certificates > 🛗 Third-Party Root Certific		Delete		Manage Private Keys	
 Trusted People Client Authentication Is: 		Help		Export	
> 📔 Preview Build Roots					



In the new open window you can add user/user groups to the certificate.

Only "Read rights" are necessary!

With this step a user will be added who is not member of a already existing user-group and is no administrator.

Permissions for TestWin7SL176 p	orivate keys	×
Security		
Group or user names:		
SYSTEM Siemens (TESTWIN7SL176\Si SSU (TESTWIN7SL176\SSU) Administrators (TESTWIN7SL1 Users (TESTWIN7SL176\User	emens) 76'\Administrator s)	s)
	Add	Remove
Permissions for Users	Allow	Deny
Full control Read Special permissions		
For special permissions or advanced click Advanced.	settings,	Advanced
ОК	Cancel	Apply

Delete a unused certificate:

In case the installation of SiPass fails it could be possible that 2 or more SiPass Root CA certificates listed in the mmc-console.

Not used certificates can be deleted vis right click to the certificate. Keep the latest certificate. How to check: double click => Details => Valid from





8. DEMO installation

Any SiPass integrated installation can be installed as DEMO installation.

To install a demo version the following entries need to be made. All other entries are made automatically during the installation process.

• Enter into the Serial Number field "DEMO" in capital letters.

• <u>Define your Card Technology</u> select "**Siemens Readers ClkData/RS485**". This card technology will work for Siemens OSDP (e.g. ARxxS-MF) or for CerPass reader protocol (e.g. AR618x-MX).

😸 SiPass integrated Setu	p 🔀
License Options Enter the license inform	nation.
Site Name:	
Serial Number:	DEMO
License Key:	
Card Technology:	Siemens Readers ClkData/RS485
Site:	0 Facility: 0
InstallShield	< Back Next > Cancel

The License Key entries made automatically during installation click "Next". To check the License Key entry go to "Back" to return to these page.

SiPass setup entered itself the License Details.

Ĩ	😸 SiPass integrated Setu	p 💽
	License Options	4
e	Enter the license inform	nation.
	Site Name:	Demo
	Serial Number:	DEMO
5	License Key:	H7C76 - YEN23 - HV4KX - PXJZU - NYJS1
:	Card Technology:	Siemens Readers ClkData/RS485
ŀ	Site:	6 Fadity: 0
۱	InstallShield	
		< Back Next > Cancel

Click "NEXT"->To configure the installation choose "Custom"-><u>Please disable the APOGEE</u> Interface. (only for 2.75)



8.1 DEMO features

The following dialog will show the system features that are available with the demo version:

SiPass integrated Setup		×
Enter the license information.		C
Workstations: 3	Number of Busses:	2
HR Interface Clients: 1	Number of CCTV Stations:	1
OPC AE Clients: 2	Web Clients:	3
Card Expansion: 15	Door Expansion:	128
InstallShield		
	< Back Next >	Cancel

- ✓ 3 workstations
- ✓ 2 buses are available to connect other systems or devices (only 2.75)
- ✓ 1 HR interface
- ✓ MS API
- ✓ DVR API
- ✓ 1 CCTV client is available to control the video matrix (only 2.75)
- ✓ 2 OPC clients (receiving alarms from an OPC A&E server)
- ✓ 3 Web Clients
- ✓ 15 Card Expansion
- ✓ 128 Door Expansions

System features like "Graphic" or "Photo ID and Image Verification" will be added automatically.

During the installation this system features will not be displayed.

The activated system features can be checked with the licence sheet or afterwards with help of the Info dialog (Help->About).

cense Details			×
License Information:			
Site Name:	Demo		
Serial Number:	DEMO		
Card Technology:	Siemens R	Readers Clkdata/RS485	
Facility Number:	0		
Workstations:	3	Number of Buses:	2
HR Interface Client	s: 1	Number of CCTV Stations:	1
OPC A&E Clients:	2	Web Clients:	3
Card Limit:	15	Door Limit:	128
Available Modules:		OPC A&E Server Inter	face
Guard Tour		Visitor Management	
V Low Level Elevators	s	APOGEE Interface	
Smart Card Encodir	ng	🖋 Intrusion	
🖋 3rd Party DVR Inte	rface		
🖋 Data Synchronizer			
High Level Elevator	s		
Photo ID and Image	e Verificati	on	
W Messenger			
Fime & Attendance	Export		

Unrestricted Page 27



9. SiPass integrated login

Since MP 2.70 SiPass integrated is spitted in a Configuration Client and an Operation Client.





The default User Name and password for both Clients is: User Name: siemens Password: spirit

logon to SiPass integ	rated, enter your User Name and Password.	To logon to SiPas usemame and pas	s integrated Operation Client, enter your ssword.
User Name:	Siemens		
Password:	•••••	User Name:	Siemens
		Password:	

Configuration Client Login

Operation Client Login

After the first login it is required to change the password.



Note:

Please create an own customer login and do not overhand the Siemens login to any customer.



10. SiPass Client installation

The following steps will explain to install the Client with Self-Singed Certificate.

If you want to install with Machine Certificate, please refer to chapter 7 or the SiPass integrated MP2.75 Installation Manual from the DVD.

Start the <u>Configuration Client</u> at the SiPass Server and open the Client Configuration option at the System tab.



Enter the Full Computer Name of the Client PC and click on Generate Self-Signed Certificate. Click on Save and select an empty folder where the Certificate should be stored. (always make new folder for each new client)

a Client Configuration - New*	-		×
Configuration - New Configurations Full computer name: Win10Entx64172 Certificate Thumbprint: Only theck thumbprint for authentication Generate Self-Signed Certificate			
Generate All Self-Signed Certificates New Save Server Thumbprint Save	Delete	Cl	ose



SiPass create the Client Certificate and the Server Thumbprint in the folder you selected. The folder should be accessible from the remote client computer.

You can manually copy this folder to the client computer or save it to a shared network drive or remotely access the server computer from the client computer.

After using the certificate, remember to delete this folder permanently to ensure security of information.

SiPass int	egrated	×
1	The certificate has been generated successfully! All necessary files have been copied to the selected folder. The content of the folder is sensitive. This folder will have to be available on the client machine at the time of the SiPass client installation/configuration.	
	ОК]

There are 3 files inside the Certificate folder

Name	
 cacert.pem client.pfx server.thumbprint 	



<u>**Tipp:</u>** Test the connection to the server in front of the SiPass Client setup. e.g.: *ping* [Server PC name] ; e.g. : *ping sipasssrv* (Ping only works if firewall is down) If SiPass is installed inside a Domain environment it is mandatory to use the full qualified computer name, here an example: MDXXZXXX.ad001.siemens.net</u>

The SiPass integrated Client is installed in the same manner as the SiPass server. Please note:

The SiPass server is responsible for the license check.

The same customer license which has been used setup the Server, has to be used for the SiPass client installation. Also use the same installation-files.

Select Custom installation.

During the SiPass client installation the "Server", "Web site" and the "HR API Core" option has to be deselected.







Attention:

Enter in the Server field the **Name** of the SiPass Server PC.

🖟 SiPass integrated Set	tup			×
SiPass integrated Se Enter the location of	erver the SiPass integra	ated Server		と
This question is asked to uninstall and reinst	only during initial all SiPass integrat	installation. To ed.	change the server loca	tion you will have
	Server name:	WIN2016EN17 (IP address is	73 not supported)	
SiPass serv	ass server port: ver callback port:	8741 8742	These have to be the specified during serve	port numbers er installation.
InstallShield		< Back	Next >	Cancel

(At the 2.76 installation no ports will be shown.)

SiPass Client installation in a Workgroup environment:

All the Windows users of the Client PC have to be exist at the SiPass Server PC as Windows user (Password must be set for the Windows user).

Info: If the Windows user is not known at the SiPass Server-PC, it is not possible to start the SiPass Client ("The Server is starting up or is not available" error messages appears).

If a SiPass Client will be installed in a Domain:

The Windows user of the SiPass Client PC must have at least local user rights at the Windows SiPass Server PC.



SiPass Authentication Management Wizard is displayed.

Select on the Client in the Authentication Management Wizard the Folder that contains the Client Certificate and click on Finish.

🔁 Authentication Management (Administrator)				- 🗆	\times
Import Client & Server Certificates F	rom:				\triangleright
Server Certificate Thumbprint:					
- Cettficates (Local Computer) - Other People - Third-Party Root Certificatio - Intermediate Certificatio - Intermediate Certificates - Personal - Trusted Root Certification A - Trusted People - Trusted Publishers - Trusted Publishers - Second	Browse For Folder Program Files (x86) ProgramData Recovery System Volume Information TEMP Client cert Users DVD Drive (D:) Make New Folder OK	Cancel	e Algorithm Version F	Fiendly Name	
		< Back	Finish	Cance)

The Certificate is not applied to the SiPass Client PC.





Setup of SiPass integrated Client successfully completed.



10.1 Client certificate invalid/expired

If the certificate does not match with the Server certificate you will get the following error message.



In this case you have to start the SiPass.CertificatePicker.exe from the SiPass integrated directory as Administrator and assign the correct certificate.



sk (C:) 🕨 Program Files 🕨 SiPass integra	ated > - 47 Search
n New folder	
Name	Date modified Type
SiPass.CertificatePicker	22.04.2017.12:23 Δαα
SiPass.CertificatePicker.exe.	Open
SiPass.CertificatePicker.Fun	Run as administrator
SiPass.CertificatePicker.Func	Troubleshoot compatibility
SiPass.Client.Asp.Layout.dll	Pin to Taskbar
SiPass.Client.ASP.Shell	Pin to Start Menu
SiPass.Client.ASP.Shell.exe.c	Restore previous versions

Please select the folder where the certificate is stored and click on Finish.

hentication Management		
✓ Import Client & Server Co	ertificates From:	
Server Certificate Thumbprin	t: B65D89DAFF1E2595EA1AEABF484C630	B5AE7277F
Certificates (Local Com Other People	puter) Subject	Issuer





11. Update of SiPass features

This chapter explains how to add further features to SiPass, not how to install a new version.

As a precaution, a backup should be made first!

If you want to install an additional feature, make sure that this feature will be included in the license. Otherwise a new license has to be ordered (updated).

The new license has to be installed at the server only.

In this Example for the training we increase the number of Workstations, Cards and Doors.

Proc	duct Name:	SiPass ACC 2.75				
	Version:	2.75				
License Information:						
Site Name:	SiPass Training					
Serial Number:	3723					
Licence Key:	PGXGQ-V1ALF-2PEPY-3ZRV4-DVUV1					
Card Technology:	Siemens Readers ClkData/RS485					
Site 1:	0 Facility 1: 0					
Workstati	ons 22	Number of Buses 0				
HR Interface Clie	nts 1	Number of CCTV Stations 0				
OPC A&E Clie	nts 0	Web Clients 20				
Card Expans	ion 52	Door Expansion 555				

Copy and paste is faster than entering it manually: Site Name: SiPass Training Serial Number: 3723 License Key: PGXGQ-V1ALF-2PEPY-3ZRV4-DVUV1



Start the **"Install.exe"** from the DVD root as <u>Administrator</u> (right click -> run as Administrator).

The setup will recognize that SiPass integrated is already installed and will provide the possibilities as shown in the dialog below.

Select "Modify" and proceed with the installation as usual.

😸 SiPass integrat	ed Setup							
Program Main	Program Maintenance							
Modify, repair,	or remove the program.							
Modify								
1 1	Change which program features are installed. This option displays the Custom Selection dialog in which you can change the way features are installed.							
🔘 Repair								
F	Repair installation errors in the program. This option fixes missing or corrupt files, shortcuts, and registry entries.							
Remove								
8	Remove SiPass integrated from your computer.							
InstallShield								
	< Back Next > Cancel							

The new license details has to be entered, SiPass server service has to be restarted and the new option will be enabled.

It is possible too to start the license update from the Programs and Features dialogue but if the User Account Control setting is set to high the license update will fail.

Options like the DataSynchronizer can't be added so easy.

If the Data Synchronizer feature should be added this steps necessary:

- backup DB and Audit trail
- Uninstall SiPass
- > Set it up with the new license detail
- Restore DB and AT



12. SiPass integrated Upgrade Paths

It is possible to upgrade from older SiPass integrated version to MP2.76.

Which versions can be updated directly or needs additional steps can also be found in the "SiPass installation manual" located on the official DVD.

	TARGETTES UPGRADE VERSION							
Current Version	SiPass integrated Version	MP 2.40	MP 2.50	MP 2.60	MP 2.65	MP 2.70	MP 2.75	MP 2.76
	MP 2.35	1	1	Х	Х	Х	Х	Х
	MP 2.40		1	Х	Х	Х	Х	Х
	MP 2.50			1	1	Х	Х	Х
	MP 2.60				1	1	1	Х
	MP 2.65					1	1	1
	MP 2.70						1	1
	MP 2.75							\checkmark

SiPass version update step by step:

- 1. A new SiPass version also requires a new software license, a new license needs to be ordered first (2.75 licenses are compatible with 2.76)
- Disconnect the ACCs by changing the ACC Port => all ACCs offline This is needed otherwise the ACCs sending still system events to the server and they are lost afterwards. The ACCs buffering now all the system events until the update is successful performed
- Backup the database using the SiPass integrated backup function This backup will be used later to restore again all the data Always use a new empty folder to not overwrite an existing backup. The Audit Trail is not included in the database backup Move or copy the SQL archive files (date.sqlarc) to a secure place outside of the SiPass integrated folder. The default location for these files is: C:\Program Files\SiPass integrated\DataFolder\Data\Archive
- 4. Close all running applications
- 5. Uninstall the current installed SiPass version (start the SiPass installation of the installed version and select "remove")
- 6. Check if the installed SQL version and Service pack is compatible with MP2.75/2.76. If not upgrade the SQL Database (see page 4)



- 7. Setup the new SiPass version (run as Administrator)
- 8. Check if a patch is available for the installed version and apply it
- 9. Start SiPass integrated Configuration client and restore the previous made SiPass database backup
- 10.Restart PC after restore
- 11.Login and check the restored DB together with the customer
- 12. Backup the database with the new SiPass version

Note:

The option "System Settings" has to be deselected before restoring the backup.

The deselection is also necessary if the PC name or the operating system has changed. Because the registry will be overwritten with the old license details and the SiPass server will not start up after the PC has been restarted.

ed	T	ESTWIN7SL175							
v	<u>D</u> at	a <u>O</u> peration <u>P</u> rogram <u>S</u> ystem	Opt	<u>t</u> ions <u>W</u> indow <u>H</u>	elp	Restore Database			— ×
ati		Backup	0	Log off system 📳 S	how	Enter the location of the dat	abase that you wish ti	o restore	
		Restore		<u>D</u> atabase		Postoro From			
		Purge	Sec.	<u>A</u> udit Trail		C:\Users\Siemens\Desk	op\Backup From MP:	2.50\2.bkp	Browse
		<u>A</u> rchive		<u>L</u> og Book					
	5	Batch Card Printing Monitor			۱ I	Database Option			
		Guard Tour Status				🔽 Database	📝 Images	System Settings	Client Configuration
	۲	<u>T</u> &A Data Export				🔽 Graphics Files	Local Settings		
									OK Cancel

13.Bring the ACCs back to communication => change the ACC port back. Download the current firmware to all devices (Explained in courseware "SiPass HW-installation"). The current firmware will be found on the original SiPass DVD

Note:

All the SiPass Clients have to be considered updating with the current SiPass integrated version amd patch.

Two items need to be clarified with the customer if the update was done from 2.65 or older:

- Request a SiPass Service user Windows account, never use a account assigned to a person.
- Clarify which certificate the customer want to use.



13. SiPass integrated Web Client

With SiPass integrated MP2.76 a new web interface for cardholder management is available.

Note: Each active Web Client has to be licensed. The Web Client behaves like installed SiPass Client, the number of licensed Clients can be used at the same time.

The IIS must be installed in front of the SiPass Server installation:

Internet-Information-Service activation, e.g.: for Windows 10

Navigate to "Programs and Features".

- Select at the left column "Turn Windows-feature on or off".
- Select the Internet-Information-Service (IIS).
- Expand the Internet-Information-Service (IIS).
- Under Webserver / Application Development select additional the features:
 - .NET Extensibility x.x
 - ASP.NET x.x
 - ISAPI Extentions
 - ISAPI-Filters

Compatible web-browsers for the Web Client:

- Firefox V49.0.1 oder höher
- IE11 V10.10240 oder höher
- Chrome V55.0.2xx oder höher

Available options are:

- ✓ Cardholders
- ✓ Visitor (licensed option)
- ✓ Access Levels
- ✓ Access Group
- ✓ Alarms
- ✓ Venues and Bookings
- ✓ Manual Override
- ✓ Activity feed (2.76)
- ✓ Area Monitoring (2.76

Card design and card-printing must be licensed and installed per Web-Client.



Die Funktion Webseite muss am SiPass integrated Server installiert sein. Ggf. über den Standard Installationsprozess hinzufügen.

Der Dienst SiPass integrated Web UI API auf dem SiPass Server muss gestartet sein.

The same operator credentials as the standard SiPass integrated client are used for login to the web interface.

If the Self Signed Certificate is used an exception need to be added before the SiPass Website can be used.

If Internet explorer is used it may be necessary to change the "Internet options" at the Tab "Security".

Enable "Trusted sites" and add the link to the SiPass web site as Trusted site.







SiPass Web Client with Firefox browser:

• Start Firefox

Web Client login page

- Open page: https://PC-Name :8743/API/Product
- Add exception
- This window will pop up:

This step is only at the first time necessary.

- Open Web Client: https://PC-Name :5443/sipass
- Web Client Login will appear with picture and language selection possibility.

Mit dieser XML-Datei sind anscheinend keine Style-Information

- - <Key>de</Key> <Name>Deutsch</Name>
 - <Name>Deutso </Language>
- Siemens SiPass integrated Username Password Language Deutsch

The SiPass integrated logins are also valid for the Web Client login.

l localnost:90/sipass/#/ X					
\leftarrow \rightarrow C (i) localhost:90/sipass/#/					☆ :
🔒 Home 🖉 Edit	_	_	🔲 siemens 🛛 ?	>	SIEMENS
Start		Configuration			
A Live Alarms Total Alarms High Others 0 0 0	Visitor	Access Level	About		
Cardholder	Manual Override	Access Group	Credential Design		
Venue & Booking	Þ	Venue & Venue Views			

Unrestricted Page 42



SiPass Web Client with Chrome browser:

- Start Chrome
- Open Web Client address: https://PC-Name :5443/sipass

(At the first time it can be possible that an exception has to be entered: Select ADVANCED and at the bottom klick to Proceed to <PC-Name>, acknowledge exception.)



Your connection is not private

Attackers might be trying to steal your information from **win2012sl171.sipass.cps.com** (for example, passwords, messages, or credit cards). <u>Learn more</u> NET::ERR_CERT_COMMON_NAME_INVALID

HIDE ADVANCED

Back to safety

This server could not prove that it is **win2012sl171.sipass.cps.com**; its security certificate does not specify Subject Alternative Names. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to win2012sl171.sipass.cps.com (unsafe)



The SiPass integrated logins are also valid for the Web Client login.



14. Recommended SQL database settings

To apply these settings the SQL Management Studio need to be used. SiPass setup will not install this tool during setup, have to installed manually. The Tool can be found at the DVD image: SQL Server Express\SQL Server SQL Server Management Studio v17.3.

Perform the below described steps only of you familiar with the SQL Management tool.

1. By default the recovery mode is FULL, recommended is the mode "SIMPLE

📙 Database Properties - asco4	1		
Select a page	Script 👻 📑 Help		
	Collation:	Latin1_Gener	al_CI_AS
Change Tracking	Recovery model:	Simple	
Pamiesione	Compatibility loval:	COL Server 2	014 (120)

2. "Auto Close" and "Auto Shrink" have to be set to "False"

Automatic	
Auto Close	False
Auto Create Incremental Statistics	False
Auto Create Statistics	True
Auto Shrink	False
Auto Update Statistics	True
Autor I Include Chattation Annual Includes	C-l

3. Set the "Autogrowth" value to 100 MB for asco4 and asco4_log

Database Properties - asco4						
Select a page	🔄 Script 🔻 💽	Help				
Filegroups	Database name:		asco4			
Change Tracking	Owner:		WIN7PRO64EN168\siemens			
Permissions	Use full-text in	ndexing				
	Database files:					
	Logical Name	File Type	Filegroup	Initial Size (MB)	Autogrowth / Maxsize	Path
	asco4	ROWS Data	PRIMARY	25	By 100 MB, Unlimited	C:\Progra
	asco4_log	LOG	Not Applicable	5	By 100 MB, Limited to 500 MB	C:\Progra

This prevent the DB to be fragmented if always 1 MB added to the DB.

- 4. Set the max size for the asco4_log file to 500 MB (see screenshot above)
- 5. Assign 50% of the installed RAM to the SQL itself (SQL Server Properties)

8192 MB is 50% of 16 GB RAM	=>	Server memory options Minimum server memory (in MB):
		0 Maximum server memory (in MB):
		8192

6. No SQL Backup job for the asco4 DB should be created. Recover/restore a SiPass system is only possible with the SiPass own backup. SQL Backups used in rare cases for fault analyses by the developers only.