

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

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

SiPass Server System 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	✓	✓	✓	✓	✓	✓	Since 2.76

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	✓	✓	✓	✓	✓	✓	✓	✓

* 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 10,000 cardholder or 100 readers, or 5 workstation clients. 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!

E.g. a license from SiPass 2.70 can't be used for SiPass 2.75.

But any 2.75 license can be used to setup 2.76 (CCTV stations have to be 0)

Example Trainings license

Product Name:	SiPass ACC 2.75
Version:	2.75

Copy and paste is faster than entering it manually:

License Information:	
Site Name:	SiPass Training
Serial Number:	3723
Licence Key:	<u>W1PXA-YK2DE-54MAJ-3MP5D-VY1A1</u>
Card Technology:	Siemens Readers ClkData/RS485
Site 1:	0
Facility 1:	0

Site Name:
SiPass Training

Serial Number:
3723

Licence Key:
W1PXA-YK2DE-54MAJ-3MP5D-VY1A1

Workstations	20	Number of Buses	0
HR Interface Clients	1	Number of CCTV Stations	0
OPC A&E Clients	0	Web Clients	20
Card Expansion	50	Door Expansion	500

*Configuration and Operation Client counted independed.
With the license example at the left it is possible to start 20 times a Config and 20 times a Operation Client.

Modules:			
Graphics	<input checked="" type="checkbox"/>	Photo ID and Image Verification	<input checked="" type="checkbox"/>
Guard Tour	<input type="checkbox"/>	Messenger	<input type="checkbox"/>
Low Level Elevators	<input checked="" type="checkbox"/>	Time & Attendance Export	<input checked="" type="checkbox"/>
Smart Card Encoding	<input checked="" type="checkbox"/>	OPC A&E Server Interface	<input type="checkbox"/>
3rd Party DVR Interface	<input type="checkbox"/>	Visitor Management	<input checked="" type="checkbox"/>
Data Synchronizer	<input checked="" type="checkbox"/>	Apogee Interface	<input type="checkbox"/>
High Level Elevators	<input type="checkbox"/>	Siemens Corporate Card	<input type="checkbox"/>
MM8000 Interface	<input type="checkbox"/>	Intrusion	<input checked="" type="checkbox"/>
Generic DVR API	<input type="checkbox"/>	Management Station API	<input checked="" type="checkbox"/>
SALTO Integration	<input checked="" type="checkbox"/>		

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:

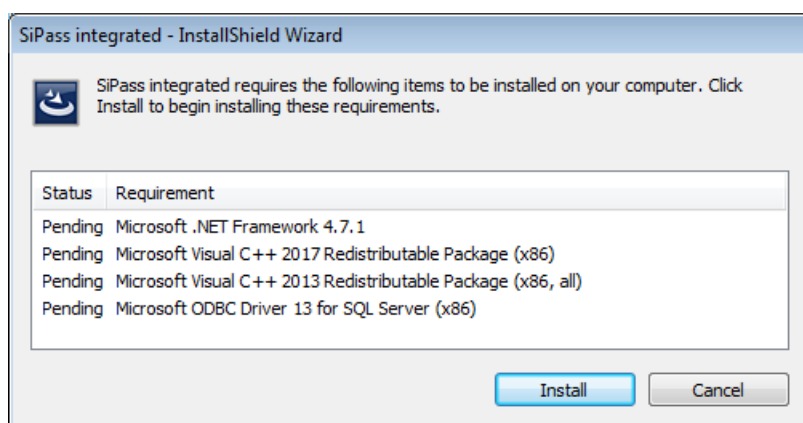
\\SiPass integrated DVD image\Prerequisites\Java Runtime Environment 8.

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

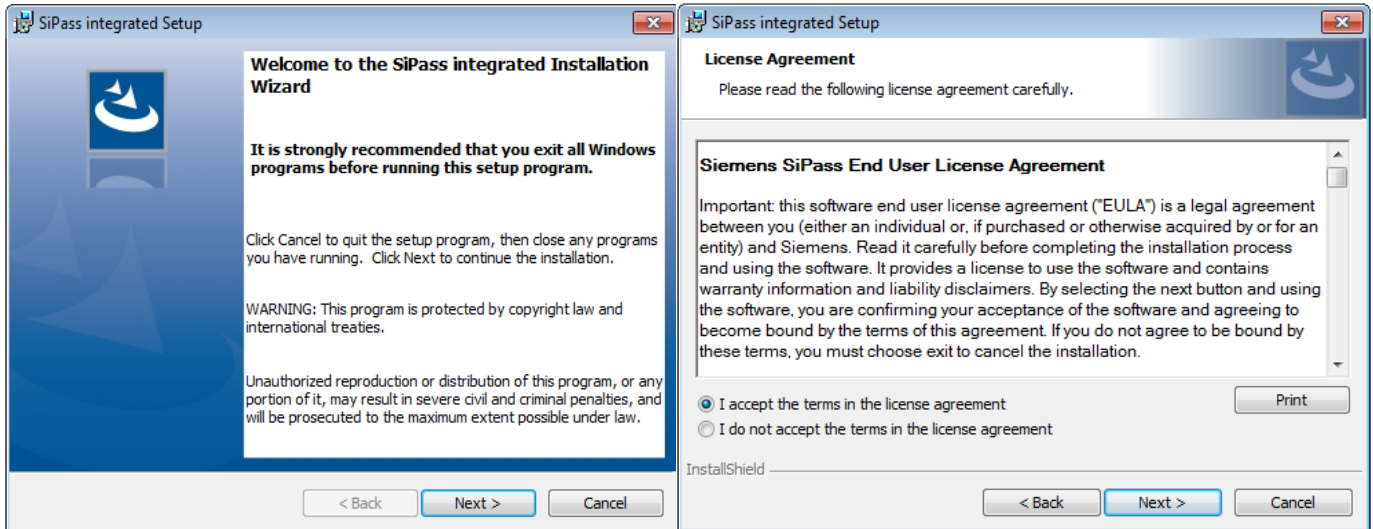
The setup checks first the PC environment and install necessary system application.

Microsoft not allowing a hidden installation of the below listed applications.

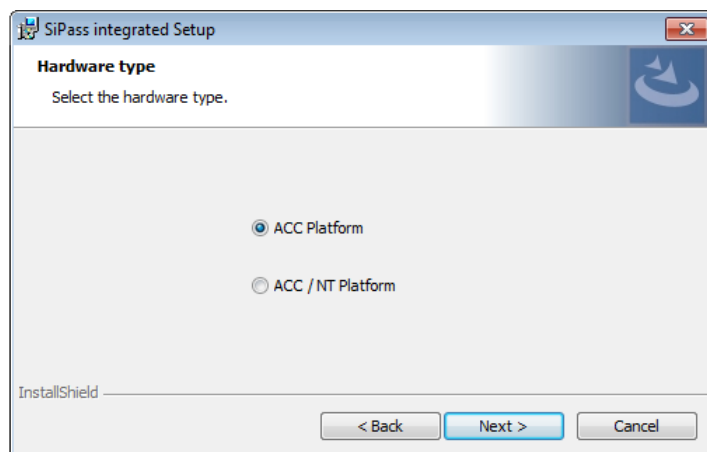
This is the reason all need to confirm terms and conditions one by one.



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.



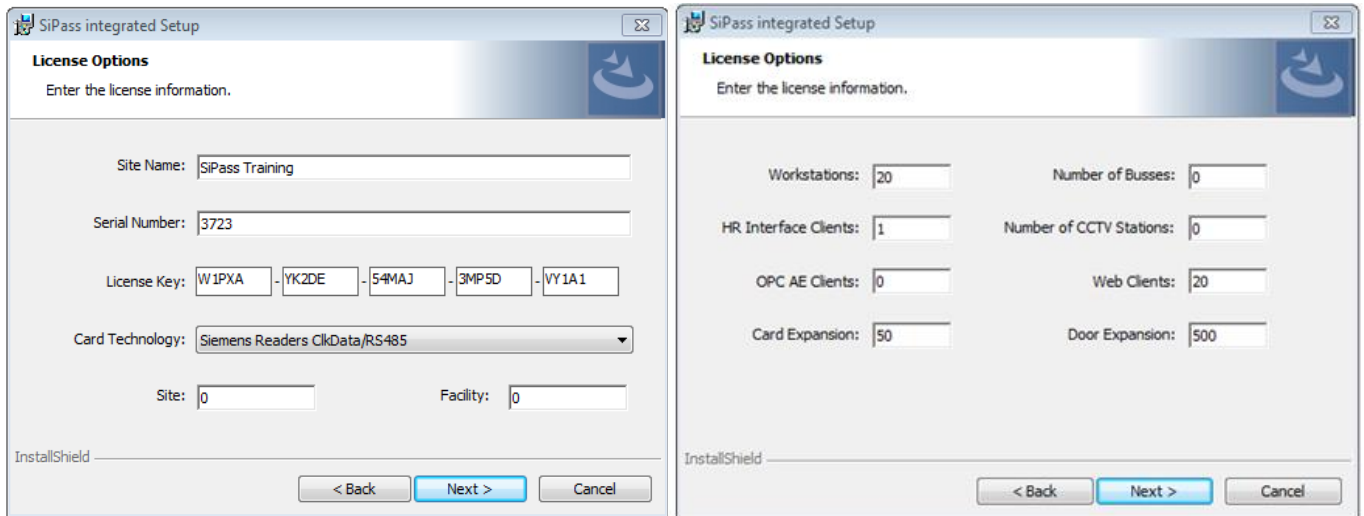
In the next dialog has to be defined which hardware platform is used, because SiPass integrated can migrate an older systems called Advantage NT.



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

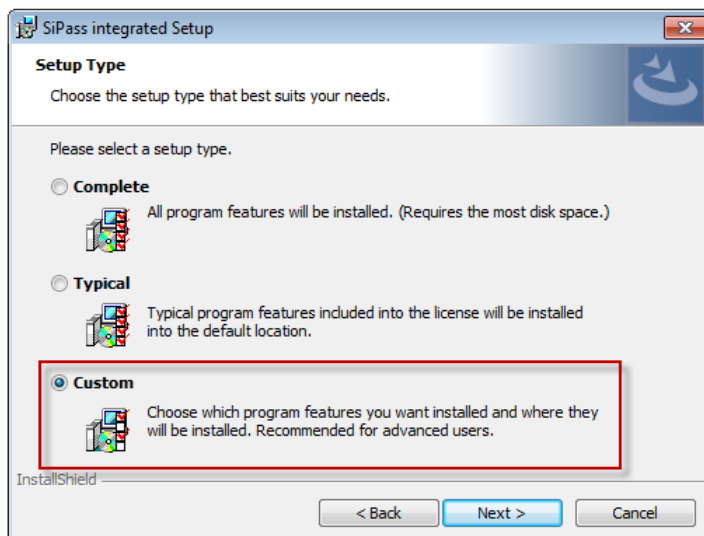
The ACC/NT Platform is for SiPass in conjunction with the "Advantage NT" and ACC door controllers.

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

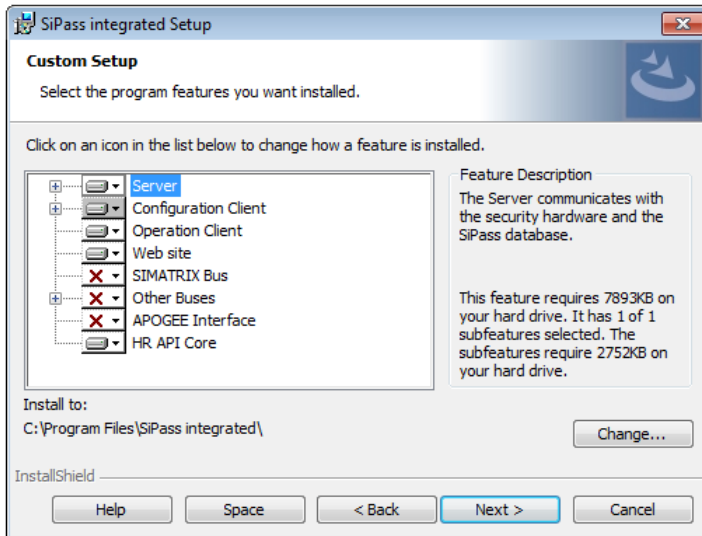


The installed features and options for "Typical" and "Complete" installation will be explained in the original "SiPass Installation Manual".

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



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

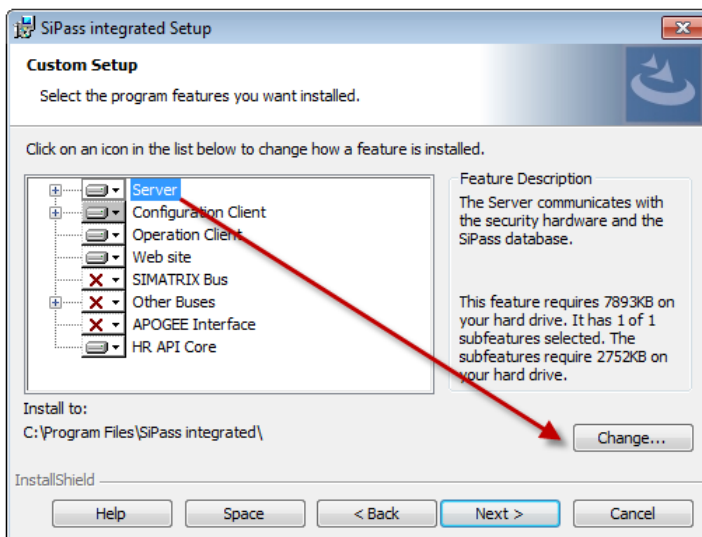


The following symbols are used in the „Custom Setup“ dialog:

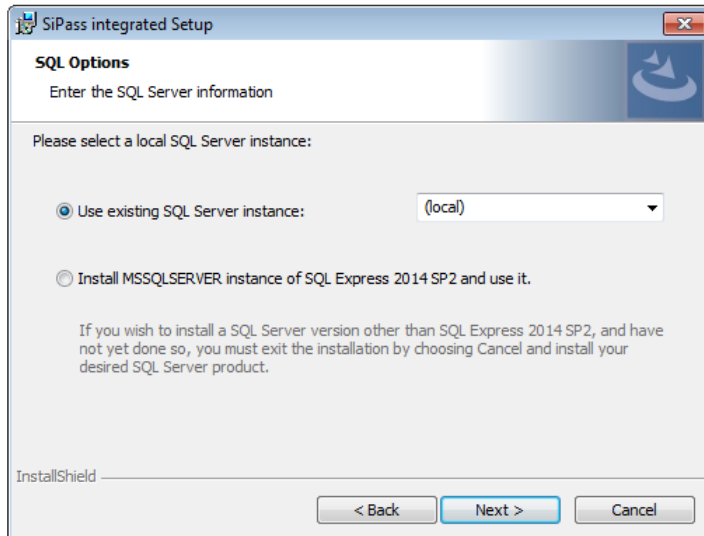


This package will be installed as part
All the system features of this package will be installed
No system features will be installed

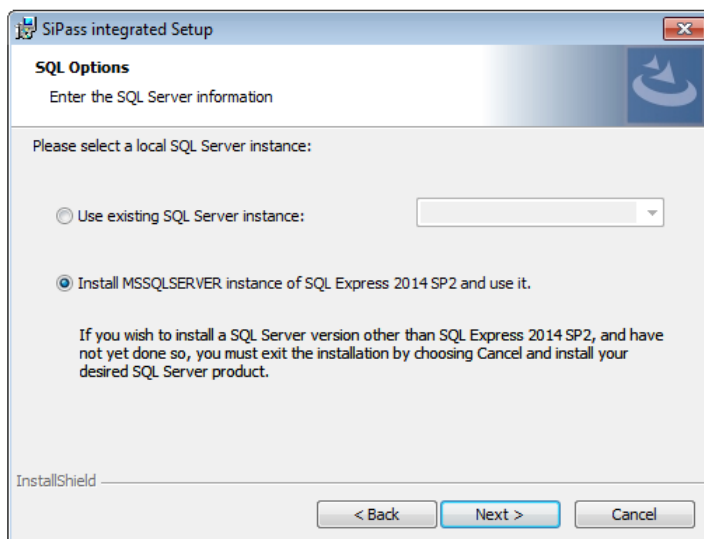
The installation path can be defined if the “Server” is selected.



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



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).



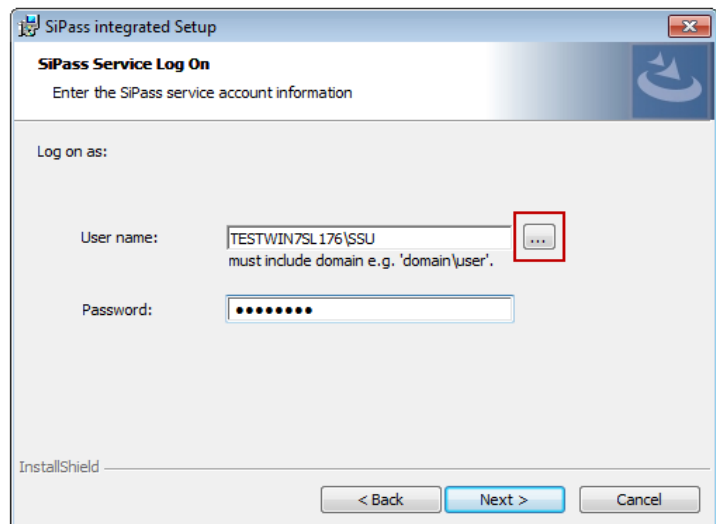
Each SQL database installation needs to have an "SA" administrator set. SiPass integrated setup 2.75 set the SA password in the background. This PW is not needed to know and can be changed, if required by the customer, with help of the SQL Management Studio.


Since MP 2.75 the SiPass Server Service have to be started by a **own** (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.

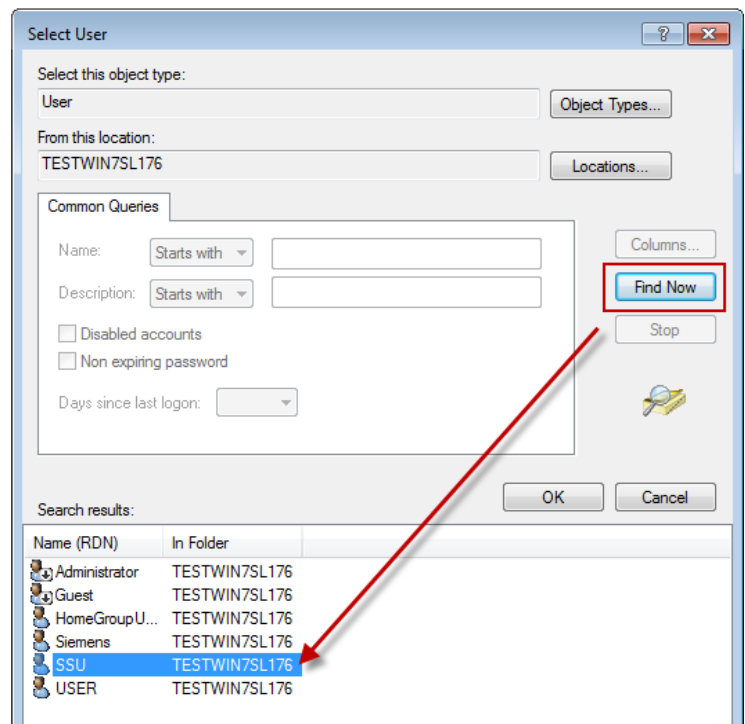
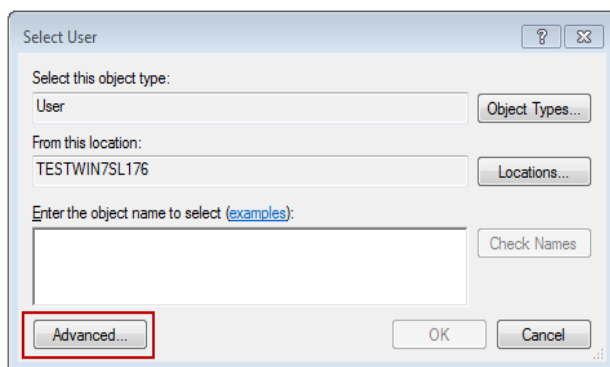
The current logged in Windows User is not accepted and an error messages is occurring.

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).

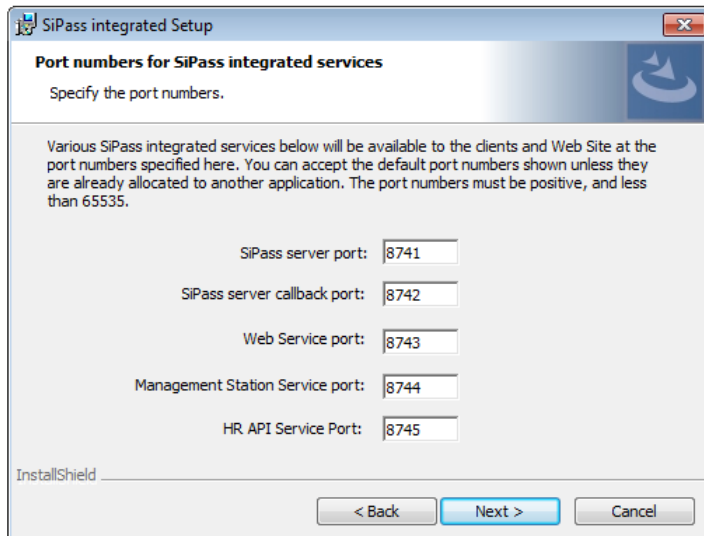


If you click on , Windows will open the User selection window where you can search for all user that are configured on the Server PC via the Advanced option.



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

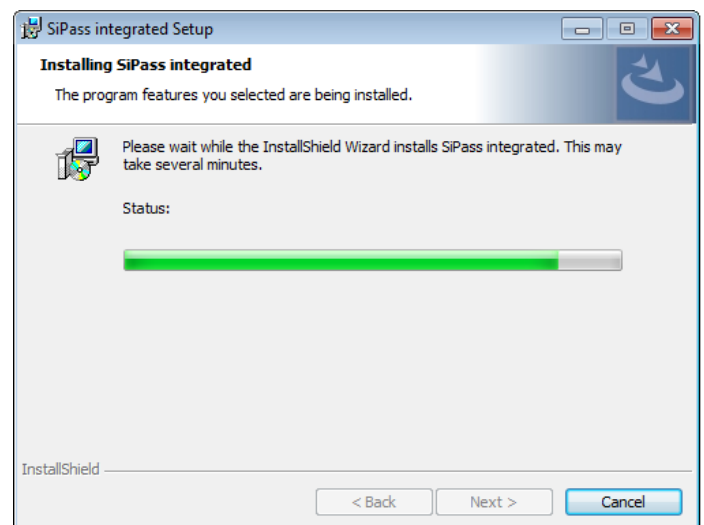
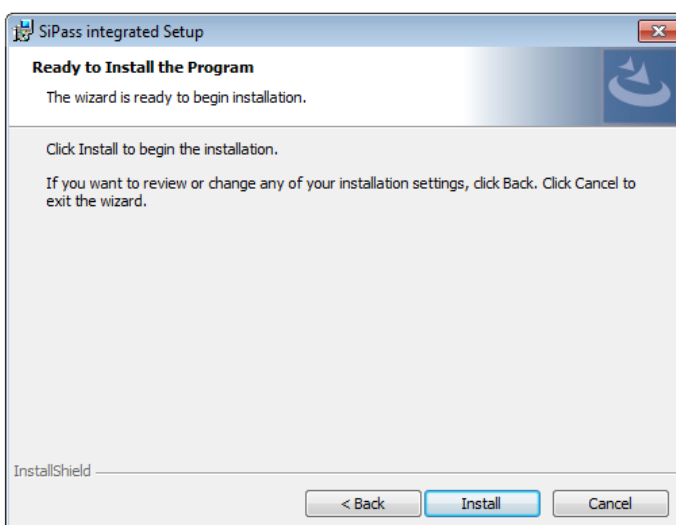
The default port numbers must be changed if those are allocated to another application on your system.



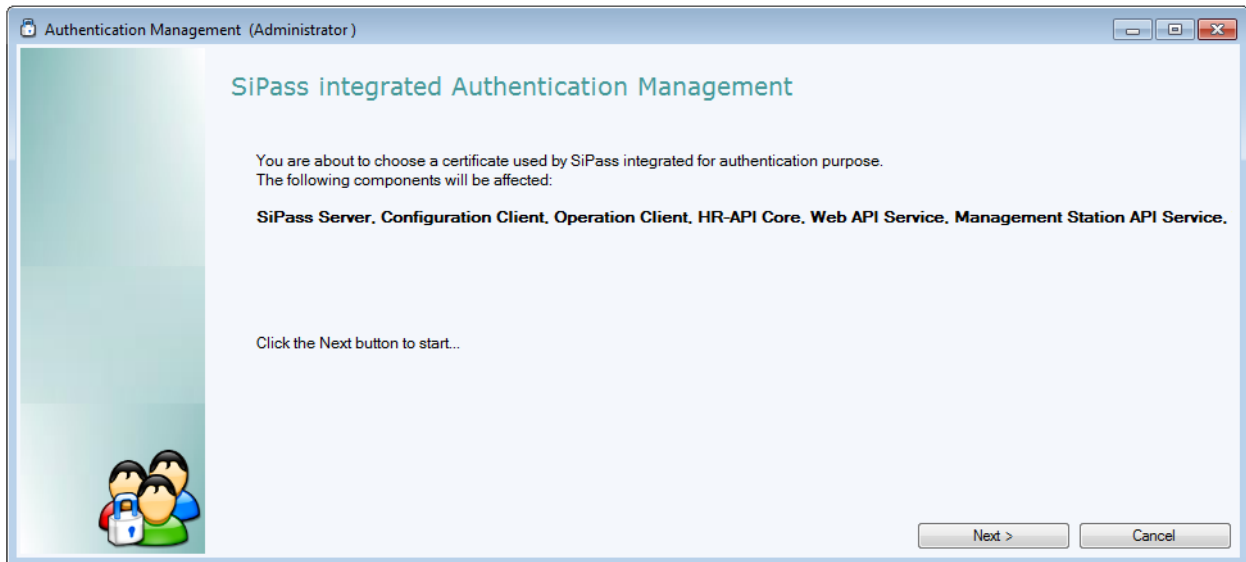
only 2.75 not for 2.76.

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.

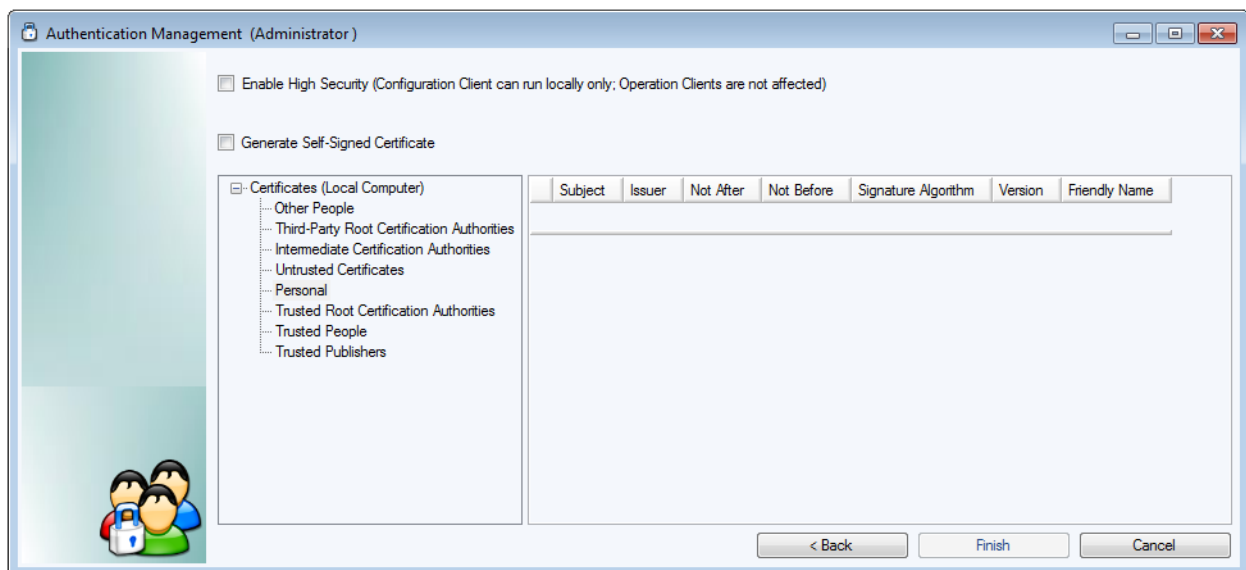


SiPass Authentication Management Wizard is displayed.



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)

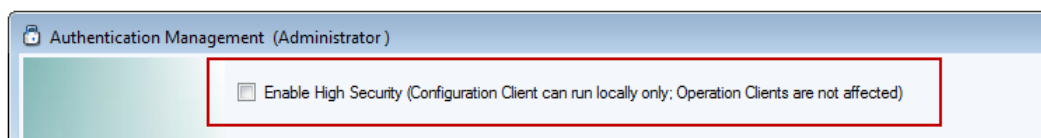
Can be generated through several available tools. However, it is recommended to use the SiPass integrated Authentication Management Wizard for the purpose.

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 Configuration Client can only run on the SiPass Server PC itself and not from a Remote Client.

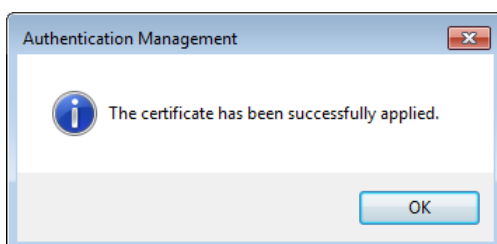
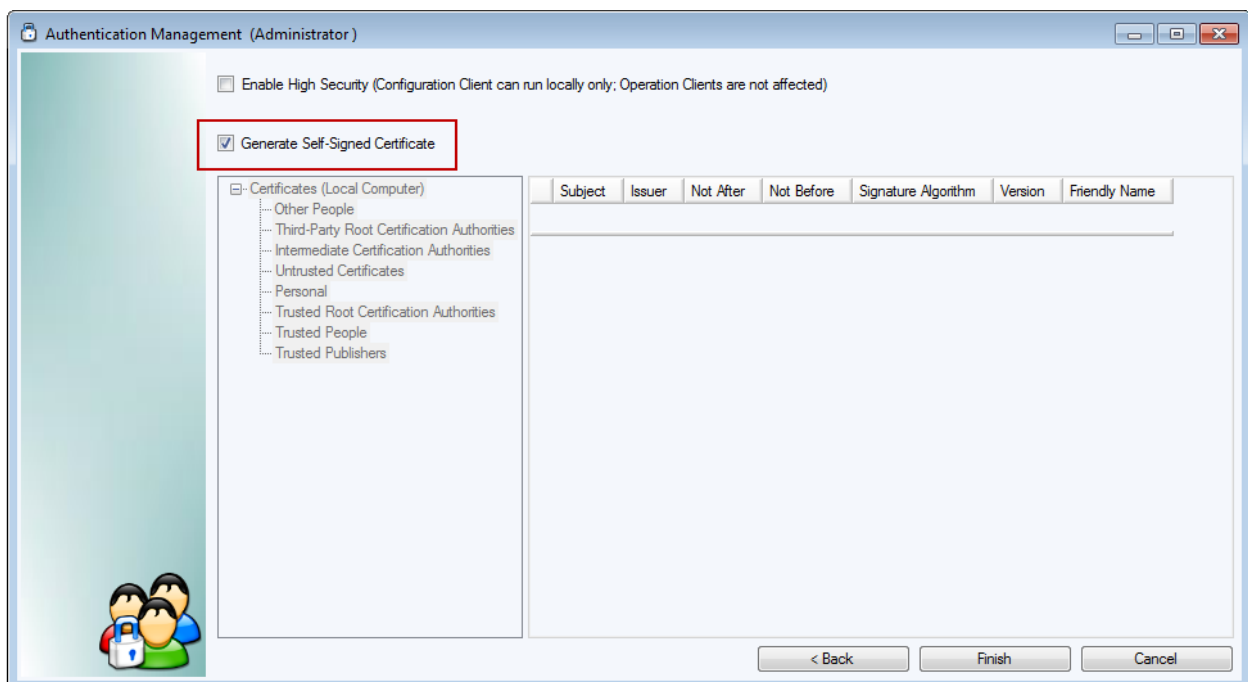
Use Self signed certificates

Select Generate Self-Signed 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.



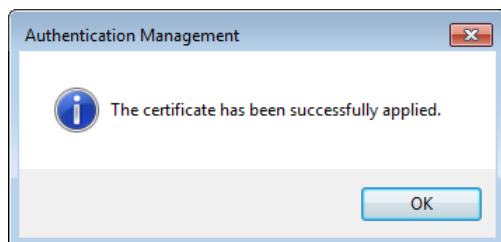
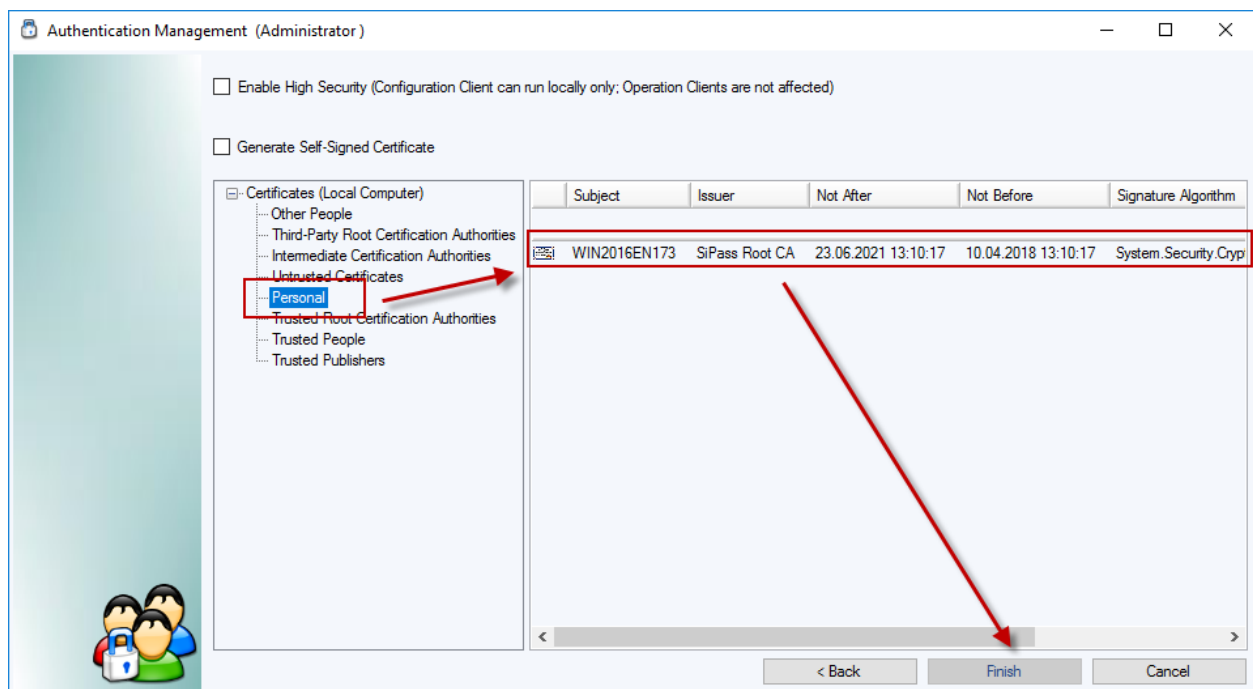
Use Machine certificates

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).

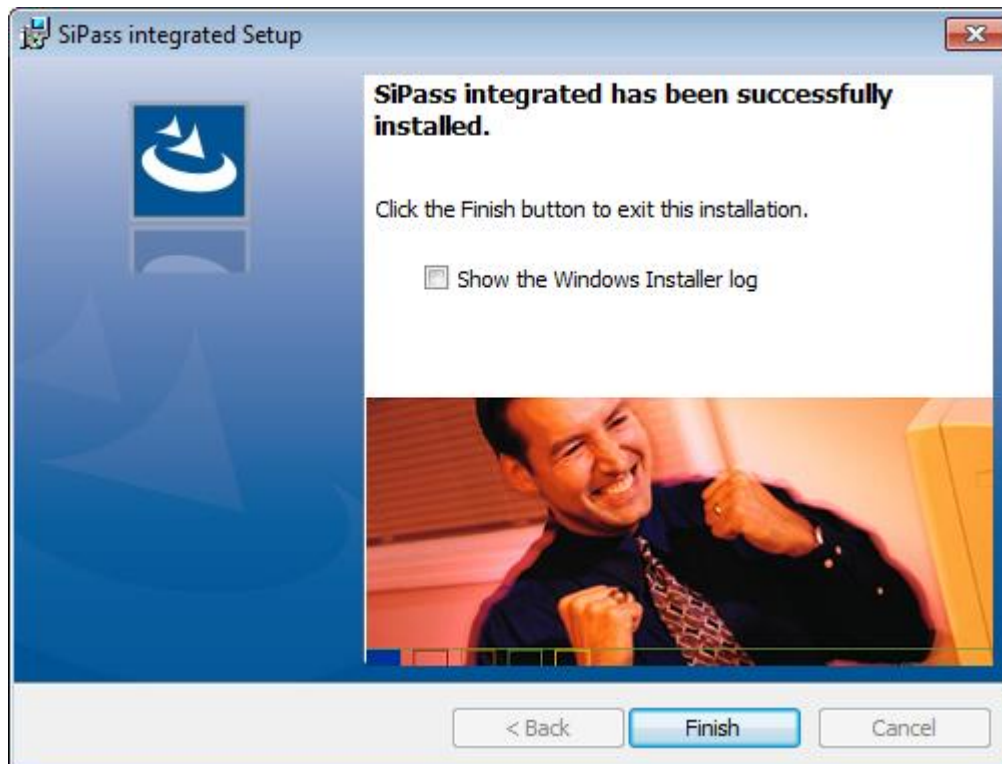
Note: Only the certificates with a private key are listed here.

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.

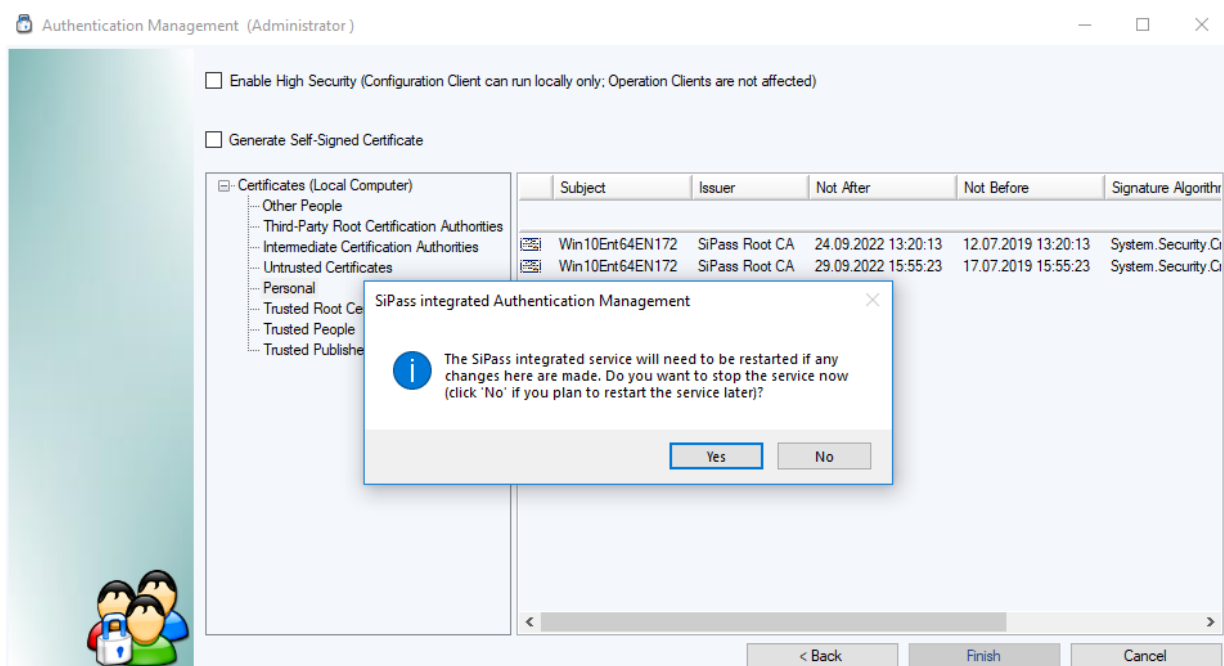
7. Renew certificate

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 help 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).

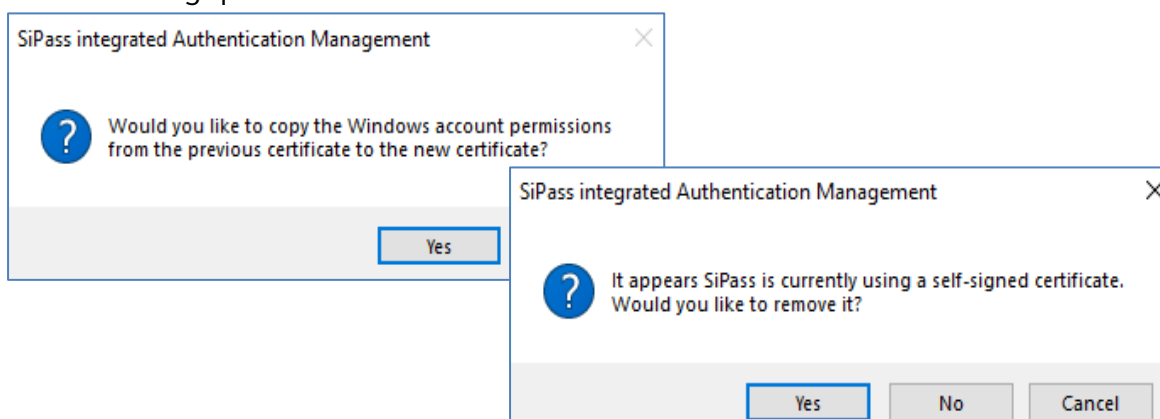
7.1 Renew self-signed certificate

Start the tool as *Administrator*.
The following dialog will appear.

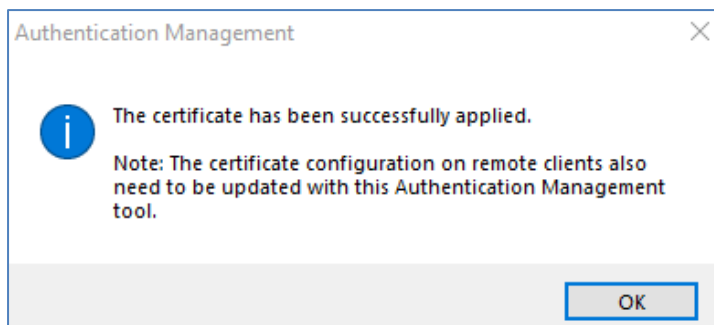


We recommend to stop the SiPass-service in front.
After that activate that option "Generate Self-Signed Certificate".

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



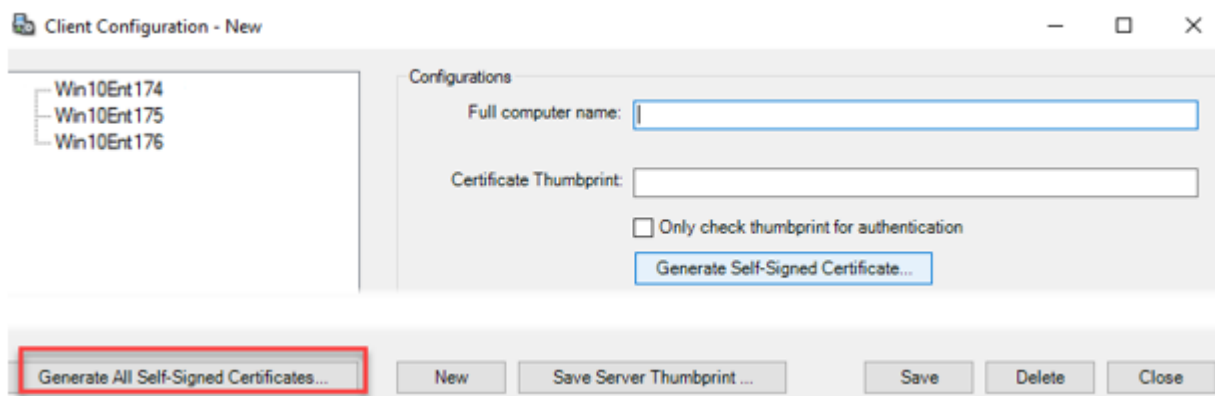
If the procedure was successful you will get the following information.



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

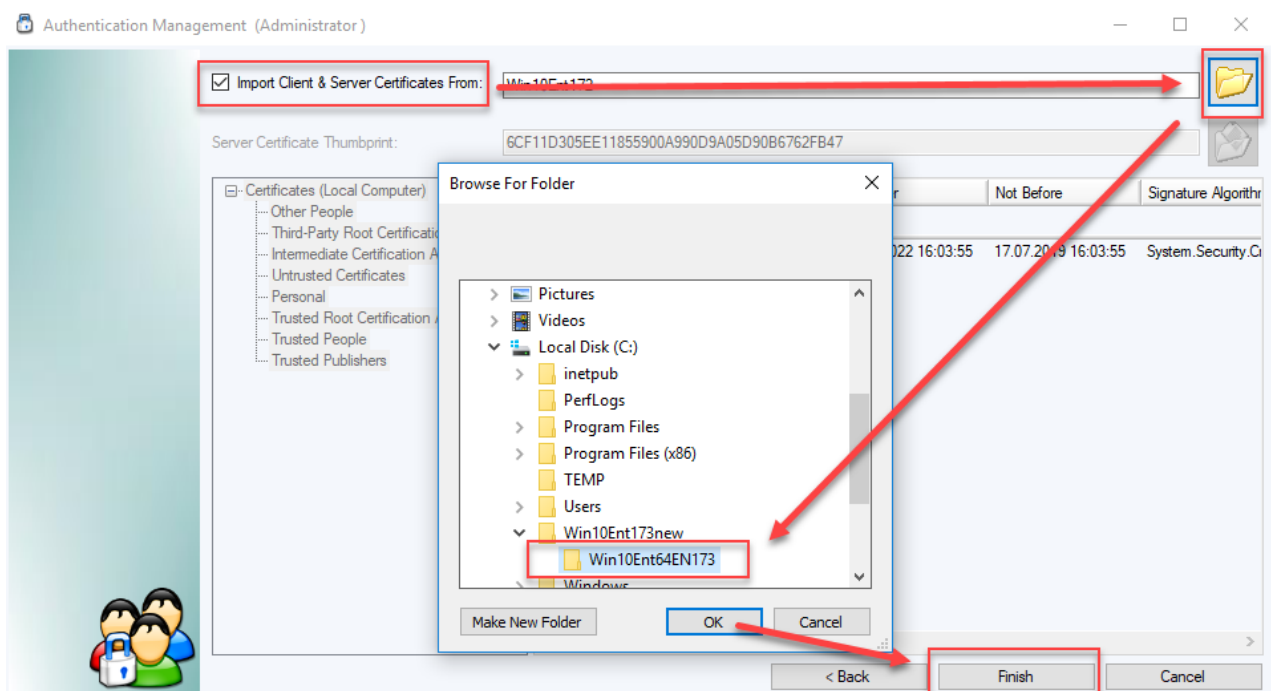
7.2 Renew remote client certificate (based on the self-signed Server certificate)

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.

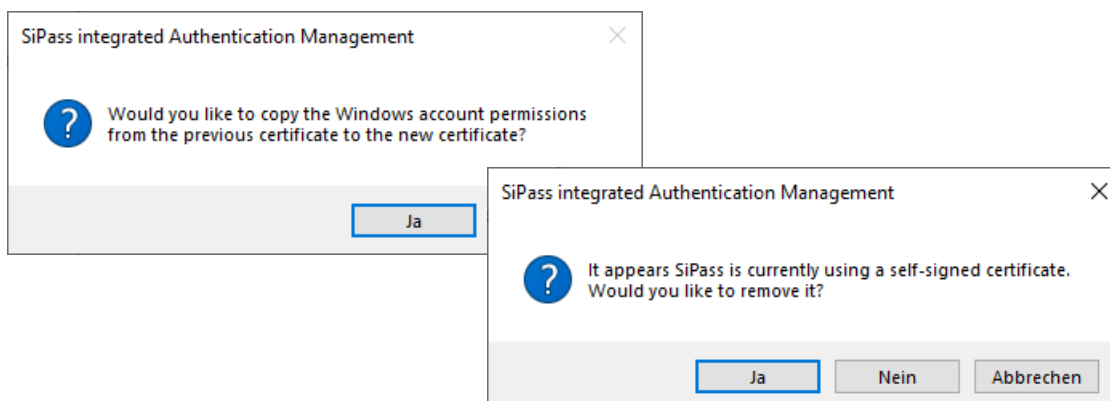


Choose "generat all self-signed certificates" and create a new folder. In this new folder each client will get a separate folder allocated. Now copy the new created remote client certificate to the respective remote client.

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



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



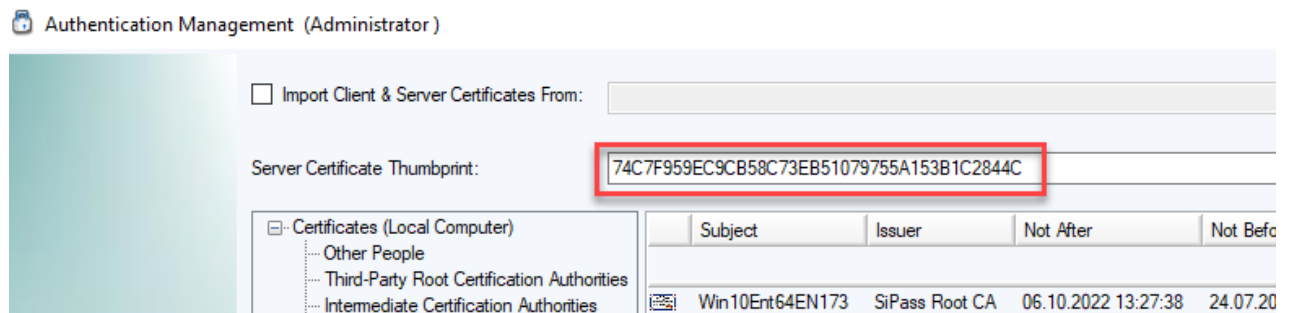
The now shown certificate-thumbprint is only a information, no additional actions needed.

7.3 Renew Machine certificate

Also for this function the SiPass.CertificatePicker.exe 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 SiPass.CertificatePicker.exe select the new certificate and enter the Server certificate thumbprint.

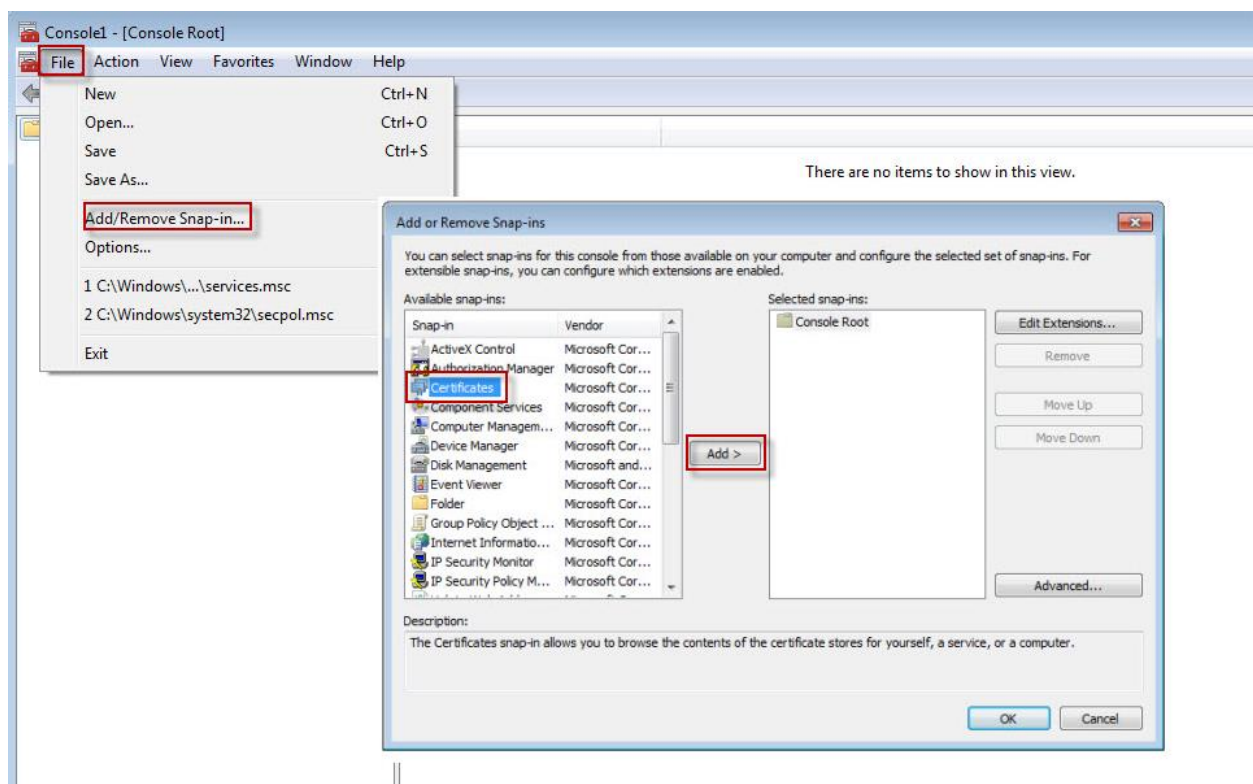


8. Manage the SiPass Certificates

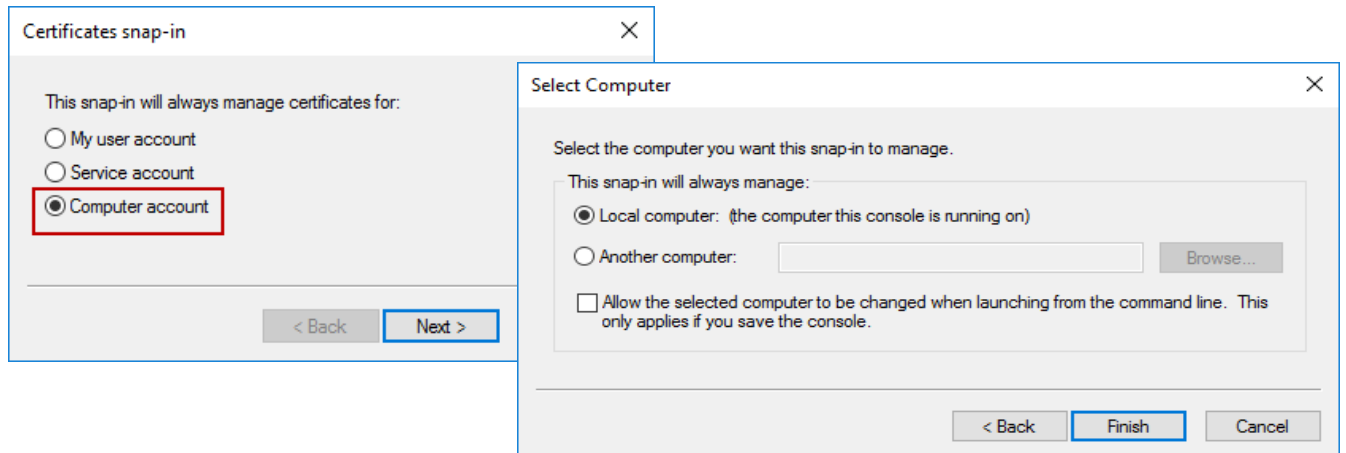
For the following described steps it is mandatory to use a Windows Administrator account.

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

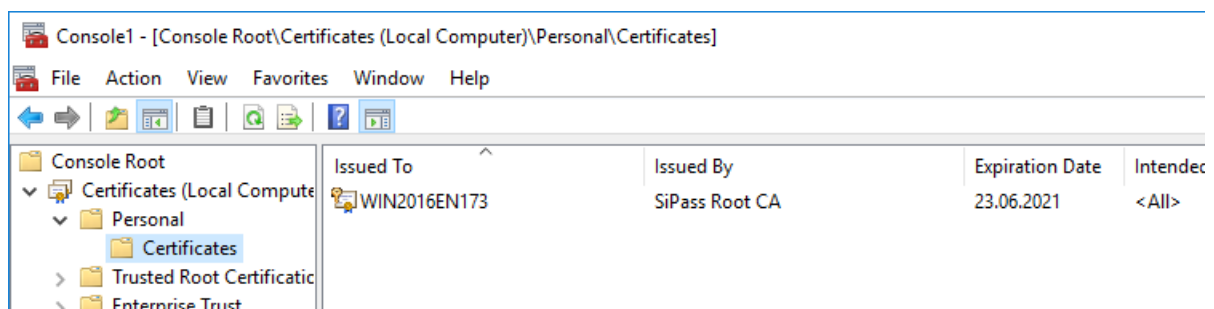
Click on File-> Add/Remove Snap-in-> Select "Certificates" and click on Add.



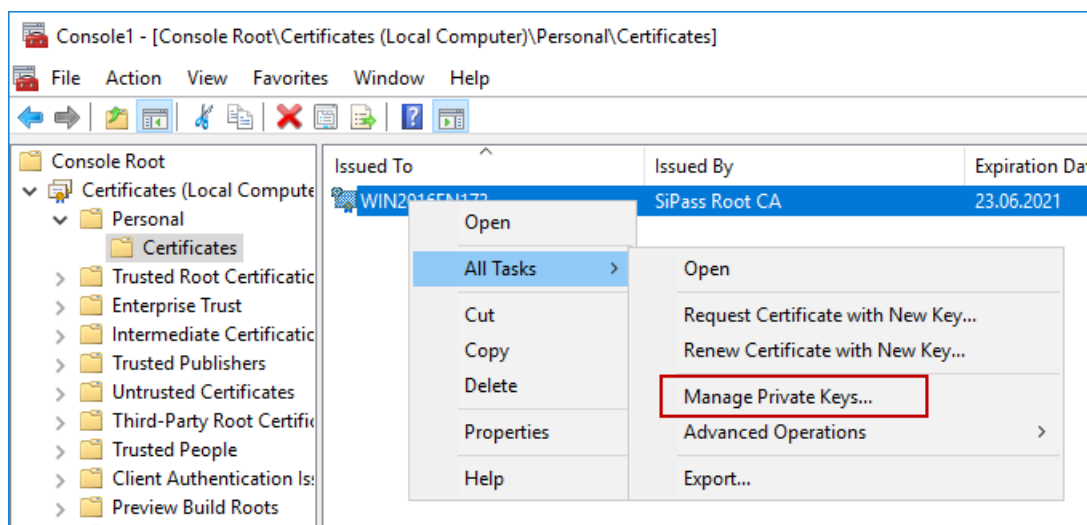
In the new opened window select "Computer account" and click Next. Select "local computer" and click on Finish.



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



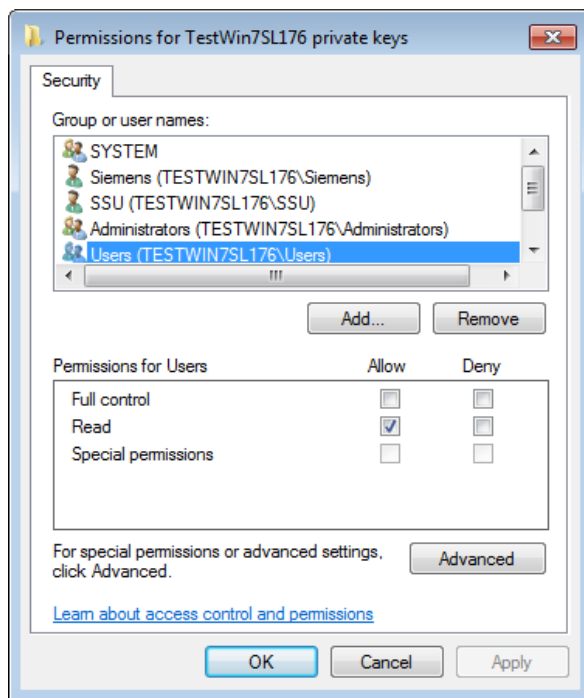
To Change the access rights for the users of the certificate select the certificate -> click with right mouse button-> Select "All Tasks"-> "Manage Private Keys..."



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.

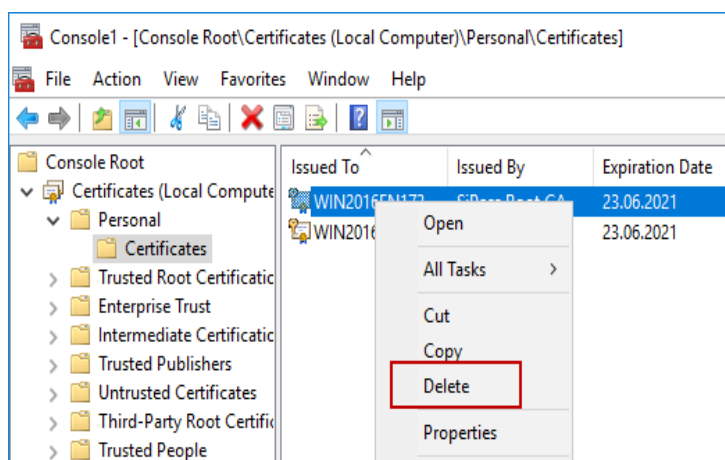


Delete a unused certificate:

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.
- Define your Card Technology 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 Setup

License Options
Enter the license information.

Site Name:

Serial Number:

License Key: - - - -

Card Technology:

Site: Facility:

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.

SiPass integrated Setup

License Options
Enter the license information.

Site Name:

Serial Number:

License Key: - - - -

Card Technology:

Site: Facility:

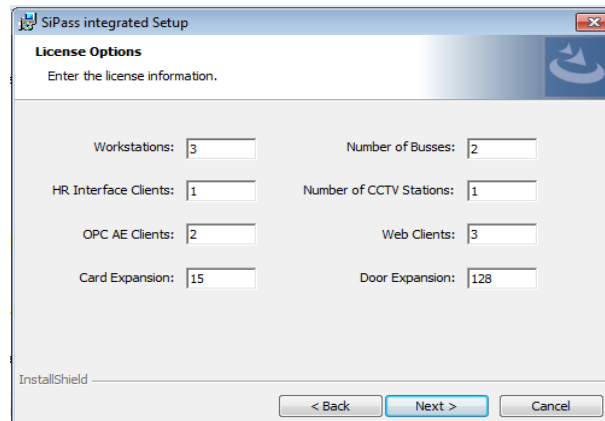
InstallShield

< Back Next > Cancel

Click „NEXT“->To configure the installation choose “Custom”->Please disable the APOGEE Interface. (only for 2.75)

8.1 DEMO features

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

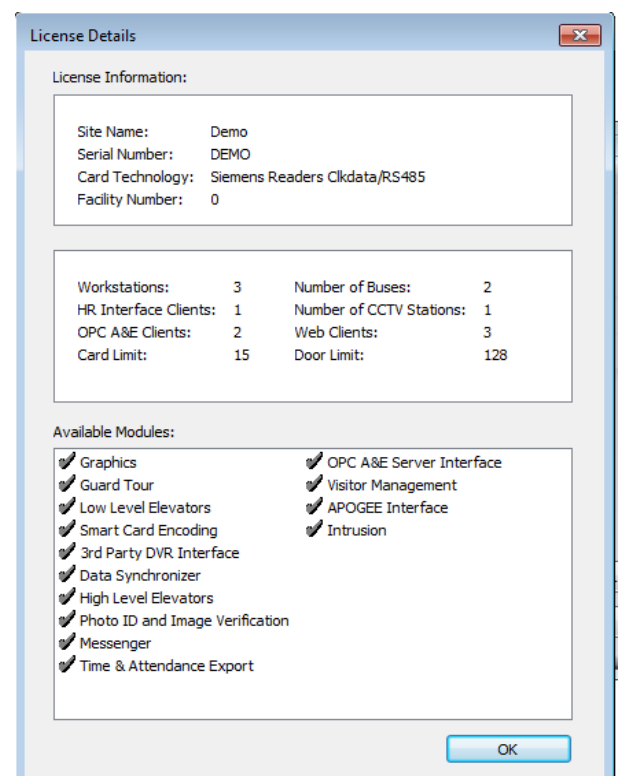


- ✓ 3 workstations
- ✓ 2 buses are available to connect other systems or devices (only 2.75)
- ✓ 1 HR interface
- ✓ MS API
- ✓ DVR API
- ✓ 1 CCTV client is available to control the video matrix (only 2.75)
- ✓ 2 OPC clients (receiving alarms from an OPC A&E server)
- ✓ 3 Web Clients
- ✓ 15 Card Expansion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

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

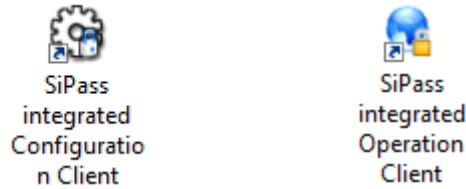
During the installation this system features will not be displayed.

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



9. SiPass integrated login

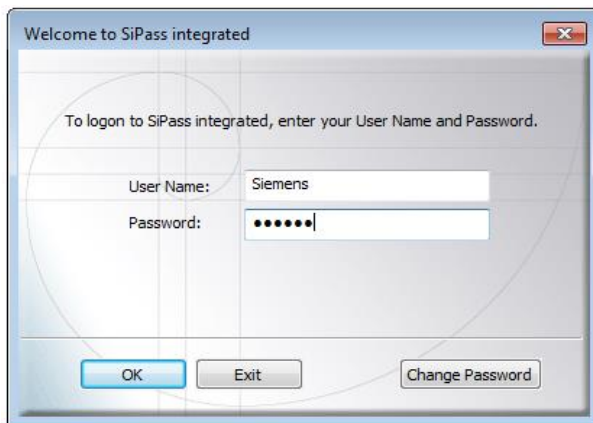
Since MP 2.70 SiPass integrated is spitted in a Configuration Client and an Operation Client.



The default User Name and password for both Clients is:

User Name: siemens

Password: spirit



Configuration Client Login



Operation Client Login

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



Note:

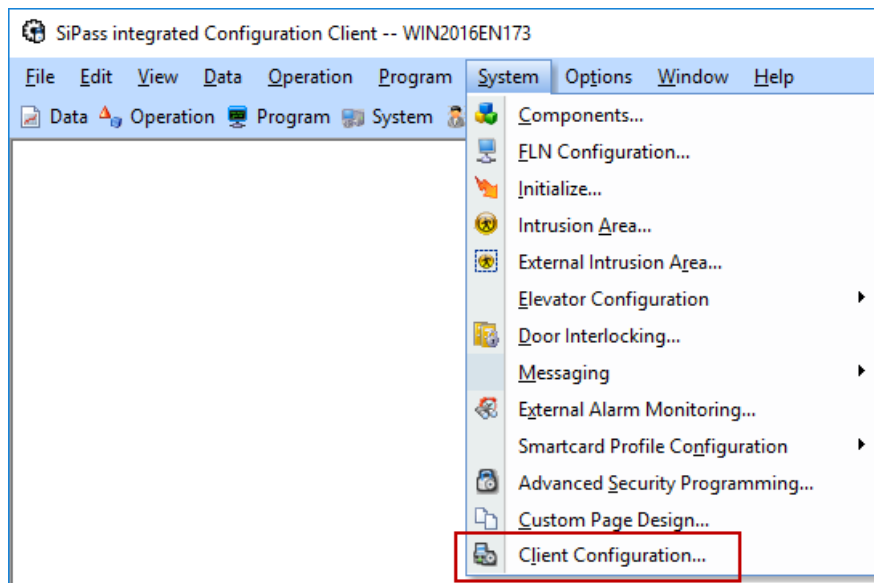
Please create an own customer login and do not overhand the Siemens login to any customer.

10. SiPass Client installation

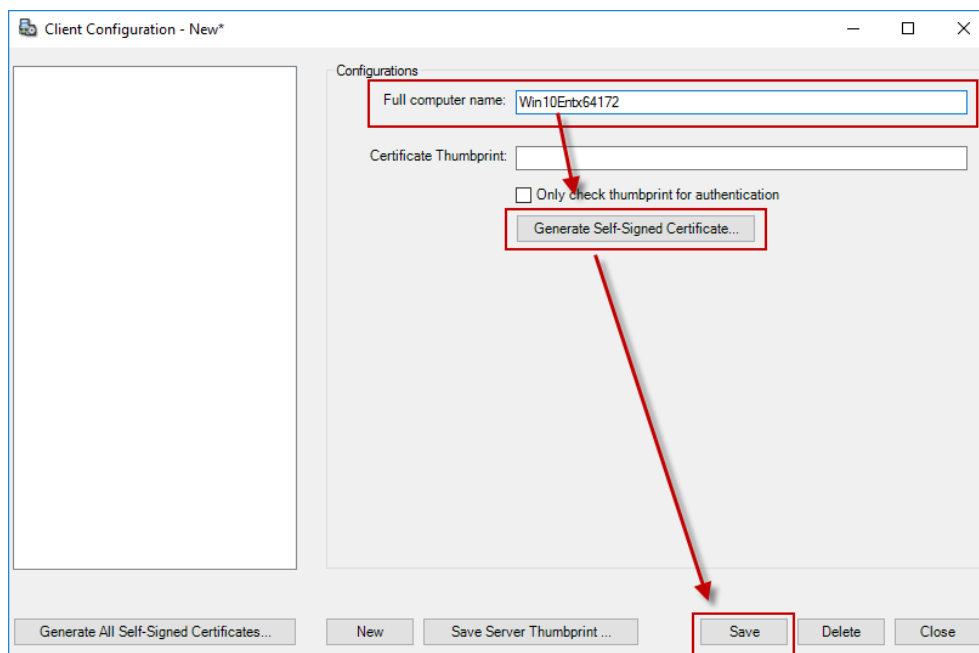
The following steps will explain to install the Client with Self-Signed Certificate.

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

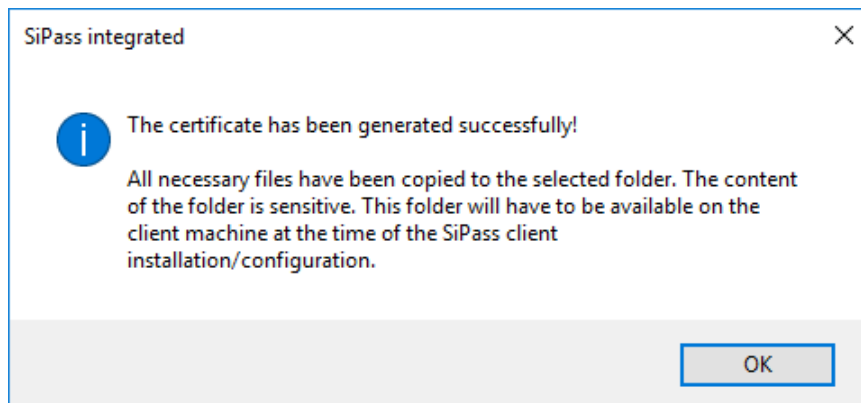
Start the Configuration Client at the SiPass Server and open the Client Configuration option at the System tab.



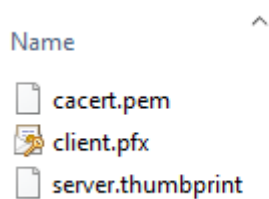
Enter the Full Computer Name of the Client PC and click on Generate Self-Signed Certificate. Click on Save and select an empty folder where the Certificate should be stored. (always make new folder for each new client)



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.



There are 3 files inside the Certificate folder



Tipp: 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

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

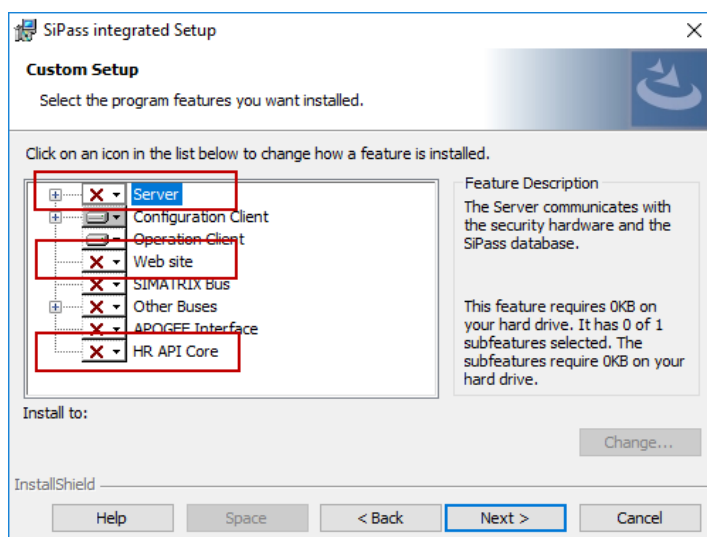
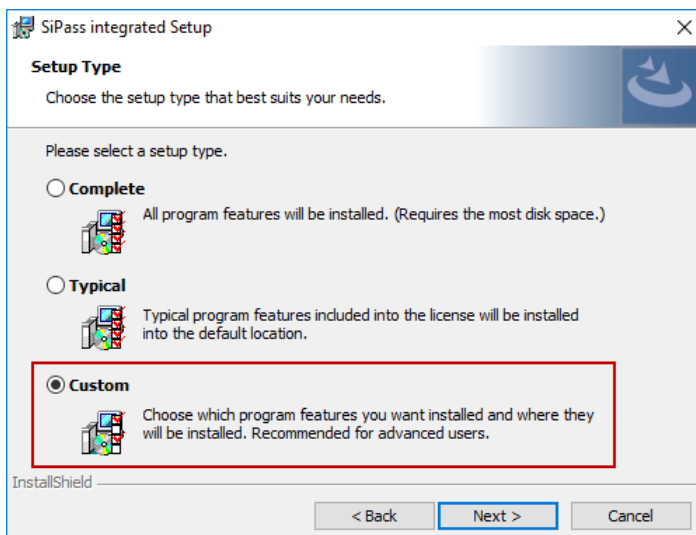
Please note:

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.

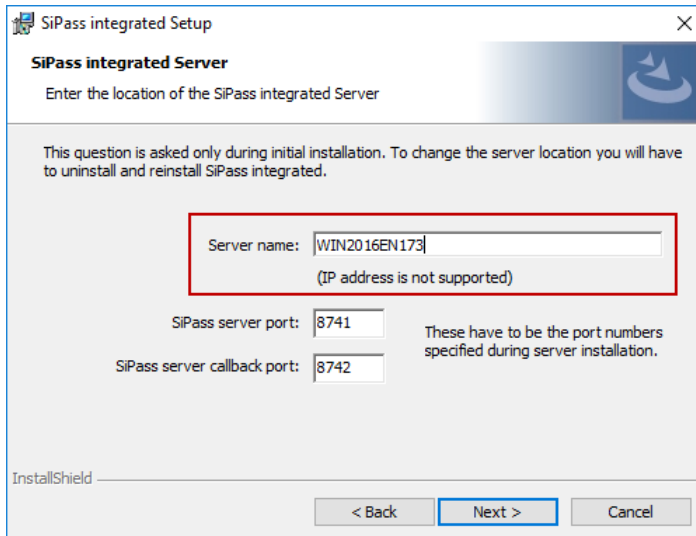
Select **Custom** installation.

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.



(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 exist at the SiPass Server PC as Windows user (Password must be set for the Windows user).

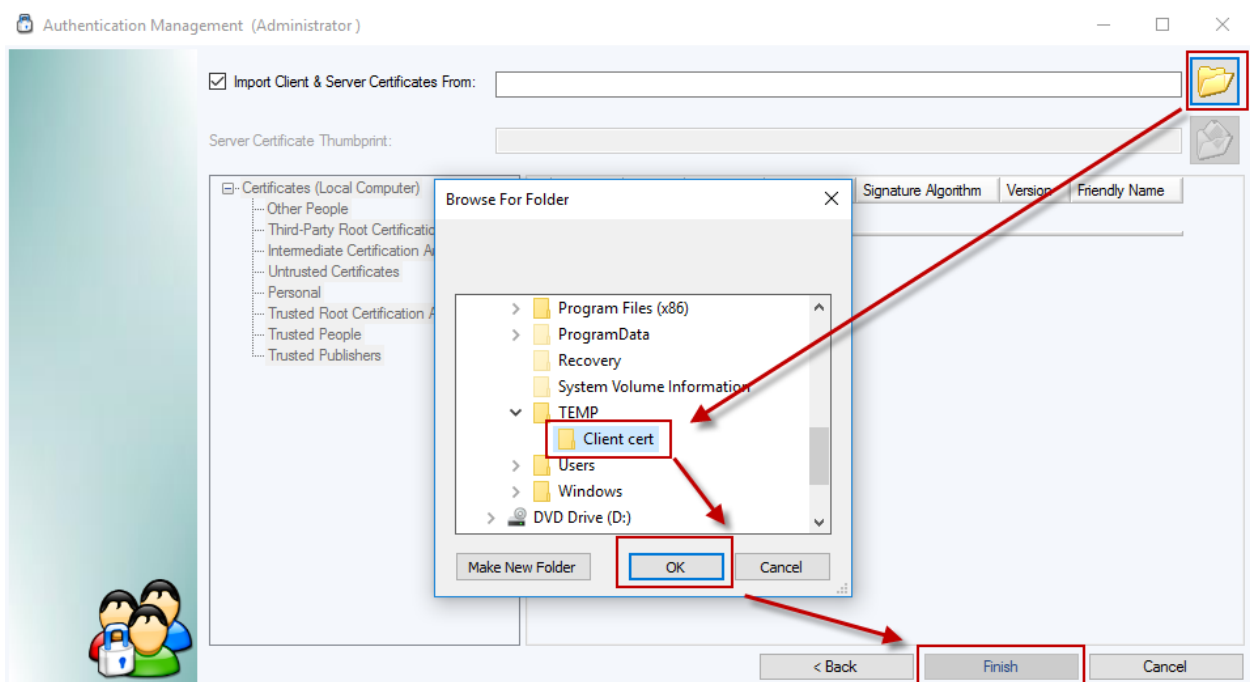
Info: If the Windows user is not known at the SiPass Server-PC, it is not possible to start the SiPass Client ("The Server is starting up or is not available" error messages appears).

If a SiPass Client will be installed in a Domain:

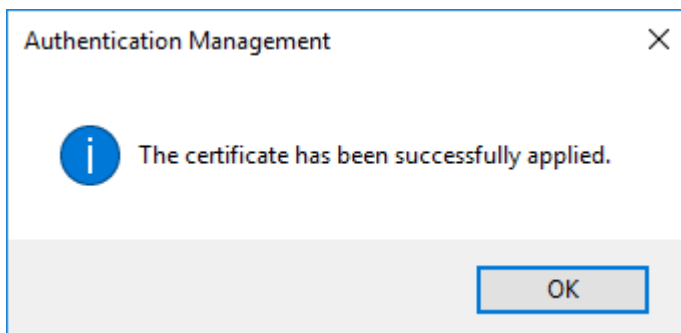
The Windows user of the SiPass Client PC must have at least local user rights at the Windows SiPass Server PC.

SiPass Authentication Management Wizard is displayed.

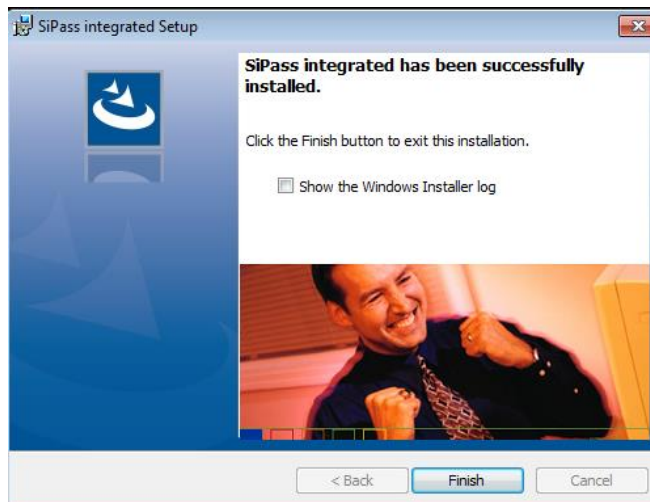
Select on the Client in the Authentication Management Wizard the Folder that contains the Client Certificate and click on Finish.



The Certificate is not applied to the SiPass Client PC.

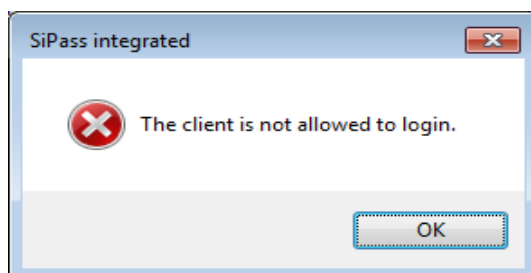


Setup of SiPass integrated Client successfully completed.

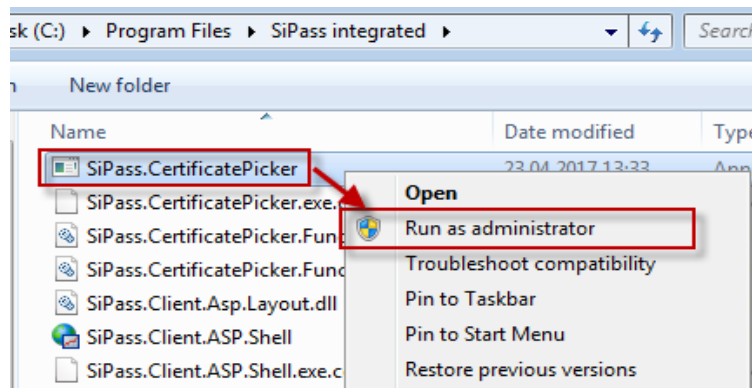


10.1 Client certificate invalid/expired

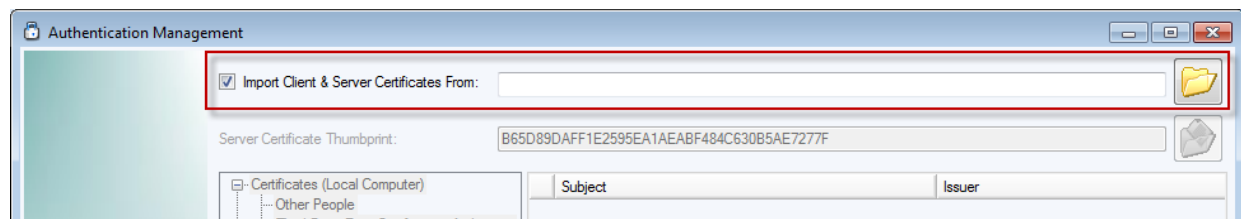
If the certificate does not match with the Server certificate you will get the following error message.



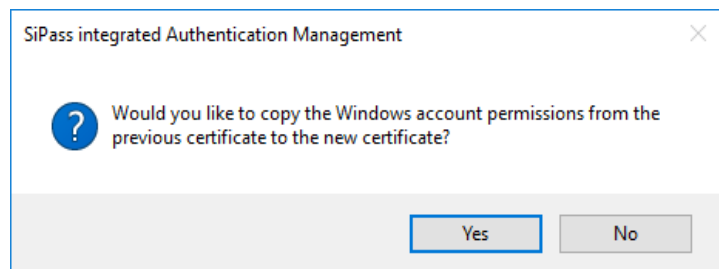
In this case you have to start the SiPass.CertificatePicker.exe from the SiPass integrated directory as Administrator and assign the correct certificate.



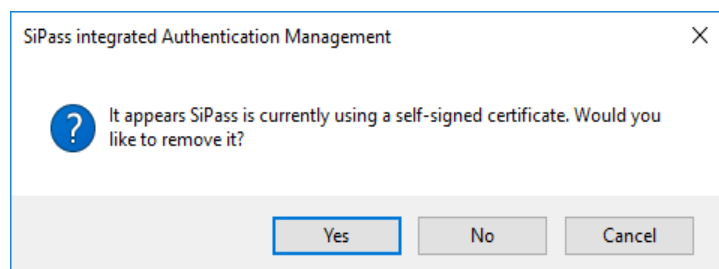
Please select the folder where the certificate is stored and click on Finish.



It is recommended to copy the existing Windows account permissions of the existing (old) certificate to the new one.

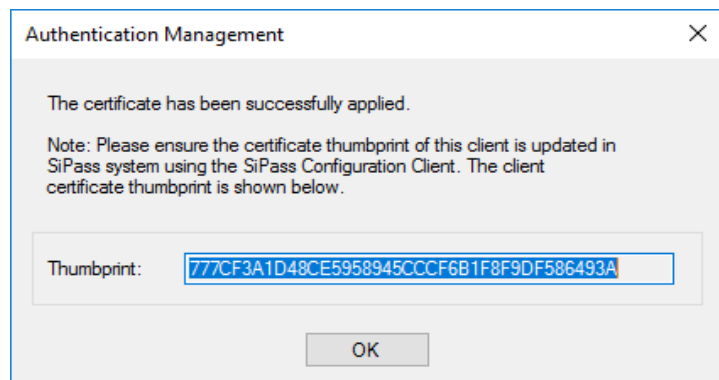


It is recommended to remove the old (not longer needed/used) Certificate.



The Client Certificate Thumbprint is only needed if Machine certificate is used.

If the new certificate was created by SiPass nothing have to be done with the Client Thumbprint.



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.

Product 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:	<input type="text" value="0"/>	Facility 1: <input type="text" value="0"/>

Workstations	<input type="text" value="22"/>	Number of Buses	<input type="text" value="0"/>
HR Interface Clients	<input type="text" value="1"/>	Number of CCTV Stations	<input type="text" value="0"/>
OPC A&E Clients	<input type="text" value="0"/>	Web Clients	<input type="text" value="20"/>
Card Expansion	<input type="text" value="52"/>	Door Expansion	<input type="text" value="555"/>

Copy and paste is faster than entering it manually:

Site Name: SiPass Training

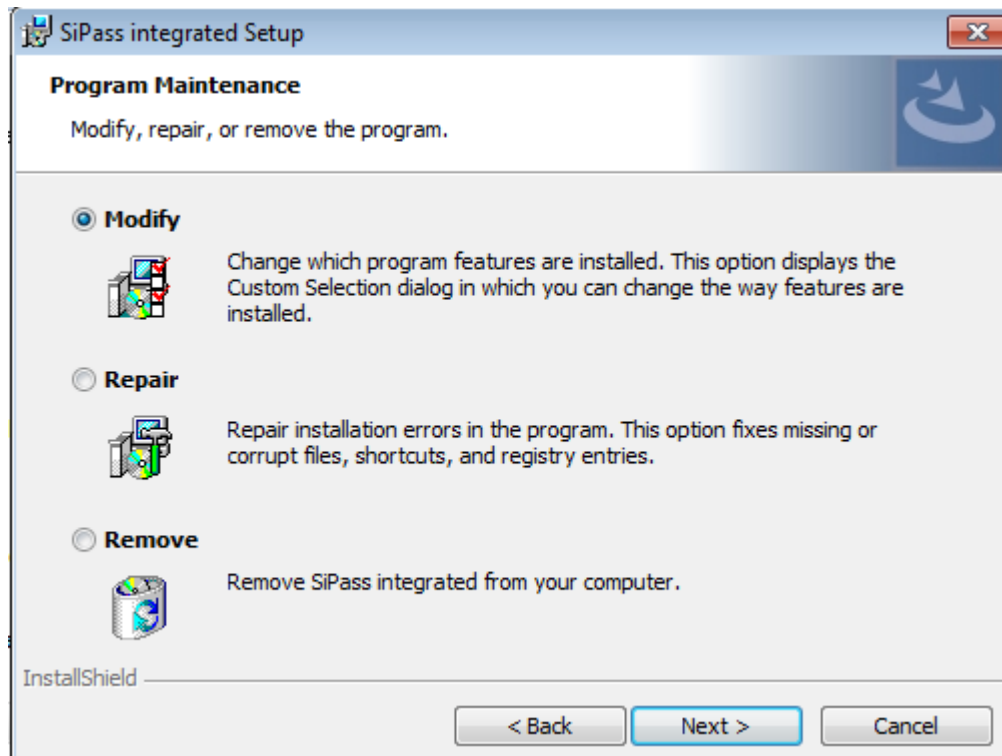
Serial Number: 3723

License Key: PGXGQ-V1ALF-2PEPY-3ZRV4-DVUV1

Start the „**Install.exe**“ from the DVD root as Administrator (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.



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.

Current Version	TARGETTES UPGRADE 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	✓	✓	X	X	X	X	X	X
MP 2.40		✓	X	X	X	X	X	X
MP 2.50			✓	✓	X	X	X	X
MP 2.60				✓	✓	✓	✓	X
MP 2.65						✓	✓	✓
MP 2.70							✓	✓
MP 2.75								✓

SiPass version update step by step:

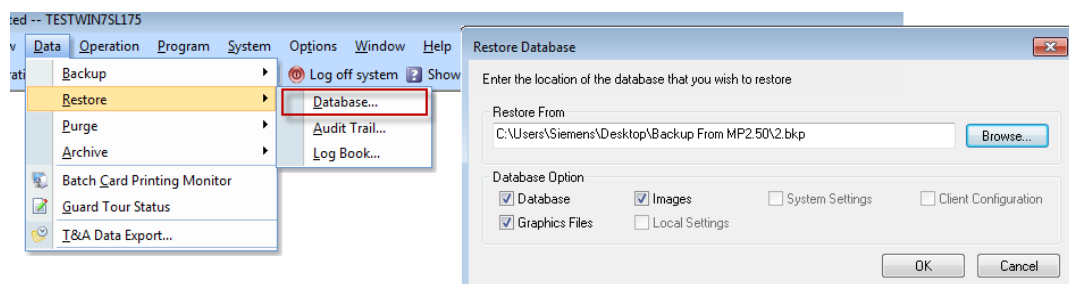
1. A new SiPass version also requires a new software license, a new license needs to be ordered first (2.75 licenses are compatible with 2.76)
2. Disconnect the ACCs by changing the ACC Port => all ACCs offline
This is needed otherwise the ACCs sending still system events to the server and they are lost afterwards. The ACCs buffering now all the system events until the update is successful performed
3. 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.



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 and 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.

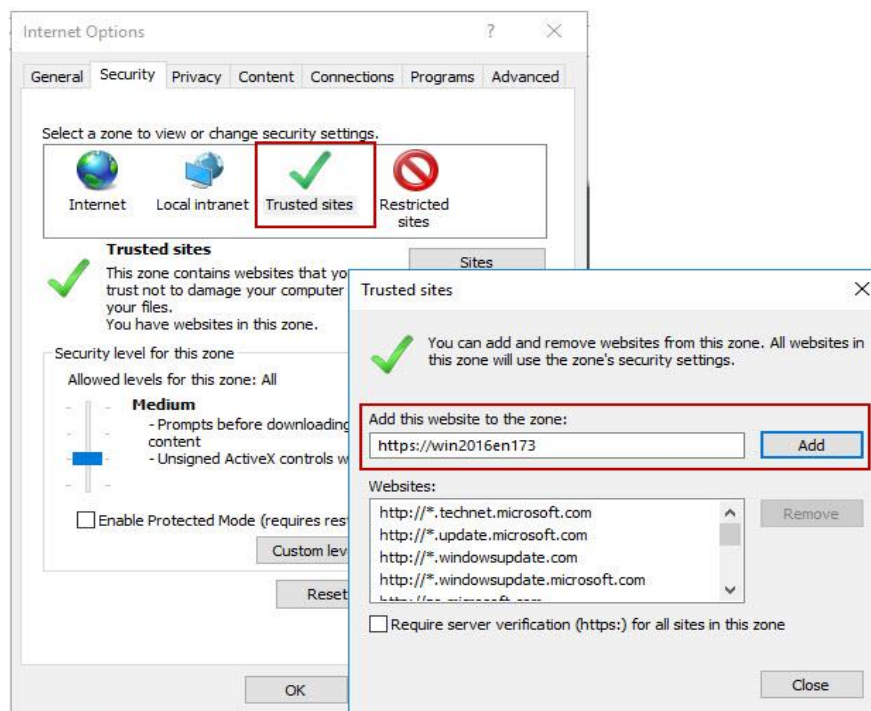
Die Funktion *Webseite* muss am SiPass integrated Server installiert sein. Ggf. über den Standard Installationsprozess hinzufügen.
Der Dienst *SiPass integrated Web UI API* auf dem SiPass Server muss gestartet sein.

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

```
Mit dieser XML-Datei sind anscheinend keine Style-Informationen

- <Product>
- <AvailableLanguages>
  - <Language>
    <Key>zh-cn</Key>
    <Name>Chinese (Simplified)</Name>
  </Language>
  - <Language>
    <Key>de</Key>
    <Name>Deutsch</Name>
  </Language>
```

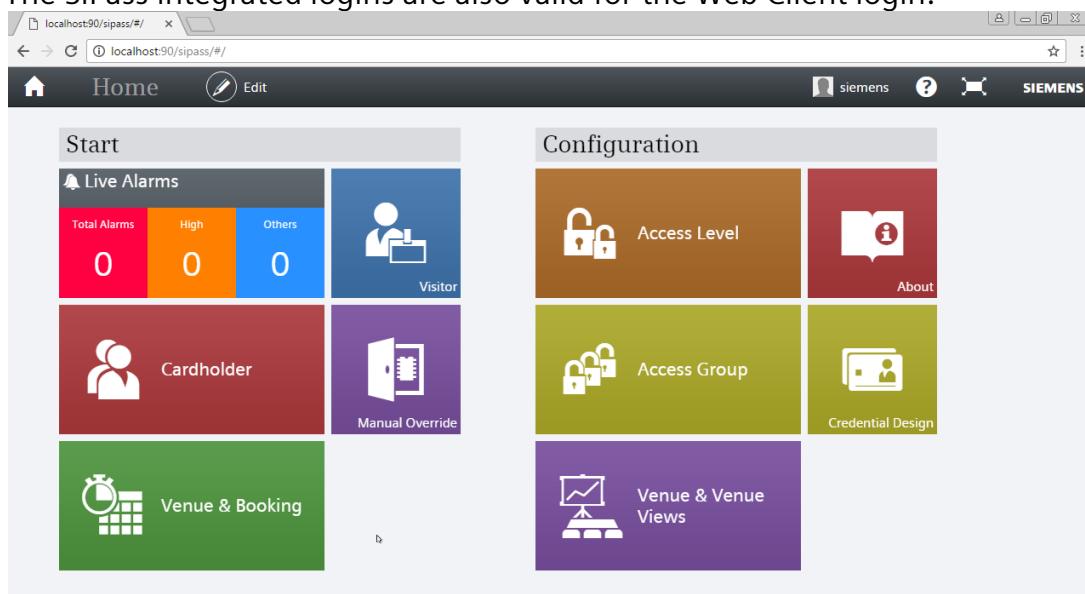
This step is only at the first time necessary.

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

Web Client login page



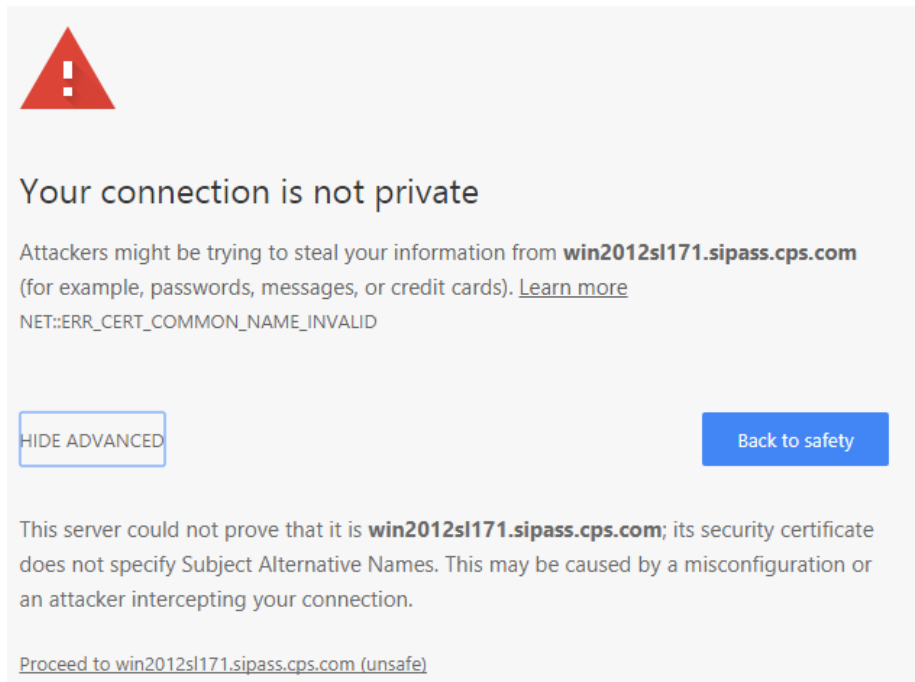
The SiPass integrated logins are also valid for the Web Client login.



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 click to *Proceed to <PC-Name>*, acknowledge exception.)



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

14. Recommended SQL database settings

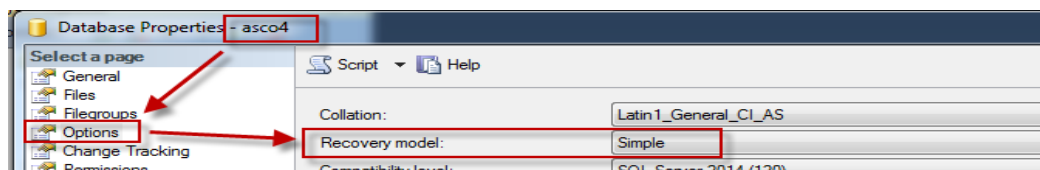
To apply these settings the SQL Management Studio need to be used.

SiPass setup will not install this tool during setup, have to installed manually.

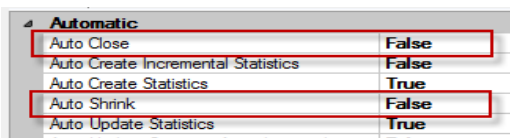
The Tool can be found at the DVD image: SQL Server Express\SQL Server SQL Server Management Studio v17.3.

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

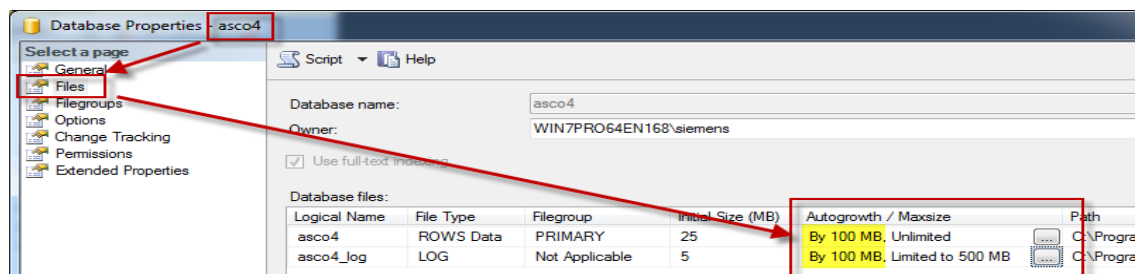
1. By default the recovery mode is FULL, recommended is the mode "SIMPLE"



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



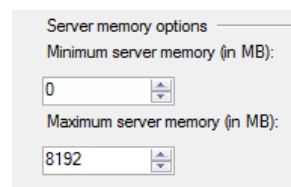
3. Set the "Autogrowth" value to 100 MB for asco4 and asco4_log



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 =>



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.