SIEMENS
Ingenuity for life

SiPass integrated MP2.95

Software Installation & Update V1.1

www.siemens.com/SiPass

SiPass integrated MP2.95

Software Installation & Update V1.1

Table of contents

1. PC requirements

SiPass Server System Requirements:

Operation System	Windows 10 /11 Pro/Ent. (64-bit)	Windows Server 2019 / 2022
SiPass MP 2.90	✓	✓

Note:
SiPass 2.80 only supporting 64 bit operating systems

Microsoft SQL	SQL 2019 Express, Standard, Enterprise	SQL 2022 Express, Standard, Enterprise
SiPass MP 2.90	✓	✓

- Memory 8 GB (minimum), 16GB Recommended
- Hard Disk Drive 1 TB or more recommended
- 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 can use a licensed SQL-Server or the free of cost SQL-Express variant. (page12)
Dependent of the SiPass system size, the licensed or Express SQL-variant must be used.

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 doors, 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.

SQL-Express can be installed automatically by the SiPass installation.

The licensed SQL-Server must be installed manually in front of the SiPass installation.
For the SQL database installation please refer to the “SiPass integrated Installation Manual”.
This folder is located at each SiPass DVD in \Documentation\Installation and User Information.

3. SQL / SQL Express Database installation

Manual SQL-installation:
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 SQL Express.

Attention:
! Since SiPass 2.90, it is possible to use an external SQL server.
So, the SQL server can be installed on the SiPass Server PC or
the SQL-Server can be external now!
(Courseware „SiPass with remote SQL")

4. Java Runtime environment

The SiPass version 2.95 will need no Java Runtime, mustn't be installed.

5. IIS installation

The Internet Information Service (IIS) is needed for the SiPass Web-clients usage.
Since SiPass 2.80 the setup will activate the necessary ISS settings automatically.
No additional settings must be activated as in older SiPass versions before.

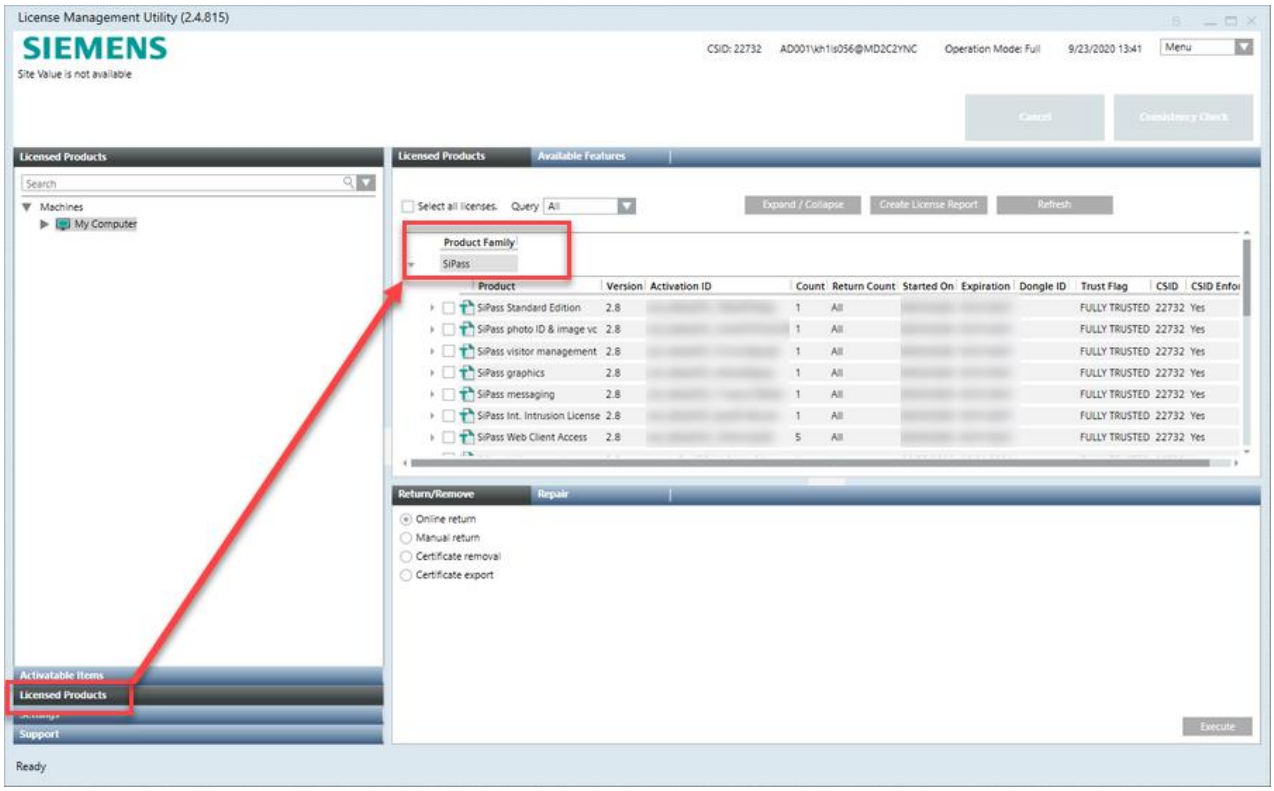
6. SiPass License

Since SiPass 2.80 the LMS license managemant tool LMU is used.
During the SiPass setup the LMU application will not be installed. We recommend to setup LMU and also activate the license before start SiPass setup.
(SiPass 2.90 will use the LMU version 2.6)

LMU training can be found here: https://siemens-learning-sipartnerportal.sabacloud.com/Saba/Web_spf/EU2PRD0112/common/ledetail/AAA-00005041/latestversion
(If the link does not work navigate to myLearning and search for LMU)

It is recommended to mount the SiPass DVD ISO to setup SiPass.
For the LMU-installation the DVD should not be mounted. Reason is that the LMU-Installation must write the installation result (log-file) to the installation folder.

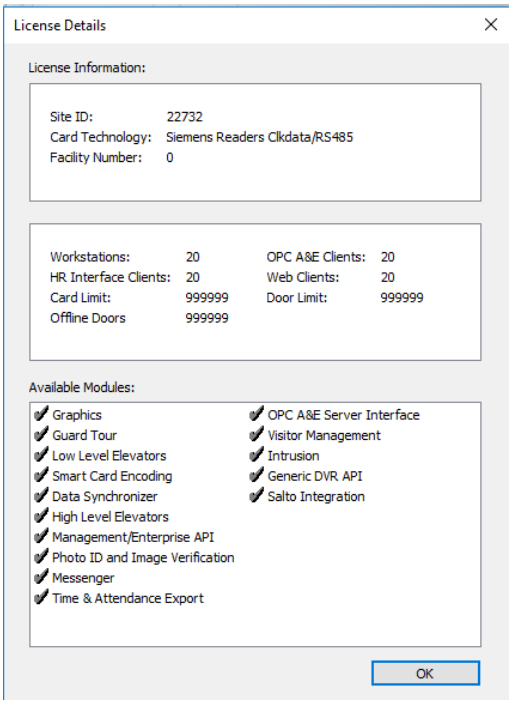
Therefore:
Copy the LMU setup file to a folder location where it is possible to write the setup log file.
The LMU setup can be found on SiPass DVD folder: \Prerequisites



LMU support handled via the standard product support process.

How to order / upgrade guide: SiPass how to order and Upgrade Guide - ID: 109784510 - Industry Support Siemens

7. Engineer License



with the LMS licensing a new SiPass License was introduced, the SiPass Engineering License.
What is the use case for the Dongle based license?

Q: Is this Engineering License needed to setup a customer system?
A: No is not

Q: Does the Engineering License enable additional engineer features?
A: No

Q: Is it needed to order additional the HW Dongle?
A: Yes, Order number: S55802-Y148

Q: Has the SiPass Engineering License a expire date?
A: Yes, after activation the Engineering License can be used for 12 month

Q: Can I renew the SiPass Engineering License with a SUR order?
A: No, new SAP order have to be placed (P54511-P110-A1-L)

What is the use case for the Engineering License?

- Test / Lab setups (if the build in DEMO mode of SiPass is not sufficient)
- commissioning on customer site => Subscription expire date of the customer license first set after site setup, customer have full 12 month Software subscription status
- customer demos (if the build in DEMO mode of SiPass is not sufficient)
- POC
- API development

The dongle is used also for Desigo CC and often called Desigo CC Dongle because this was the product which used it the last years. But in general this is a LMS Dongle and any system under LMS can use this dongle (CMD.04 LMS Micro Dongle):

Any SiPass license option can be activated:

- online (trusted store)
- offline
- dongle (if this is needed or whished by the customer)

<u>The SiPass Engineering License can only be activated via dongle (no online trusted store activation possible.</u>

8. SiPass integrated Server/Client installation

Since SiPass 2.80 the setup has been simplified by following items:

- No need to enter license details anymore
- Card technology, Facility and Site code can be individual selected during setup (no longer part of the license)
  Change is also possible afterwards via the Credential Profile dialogue if no card is assigned to the Credential Profile
- IIS will be installed and configured automatically
- Since SiPass version 2.95 no Java Runtime needed.

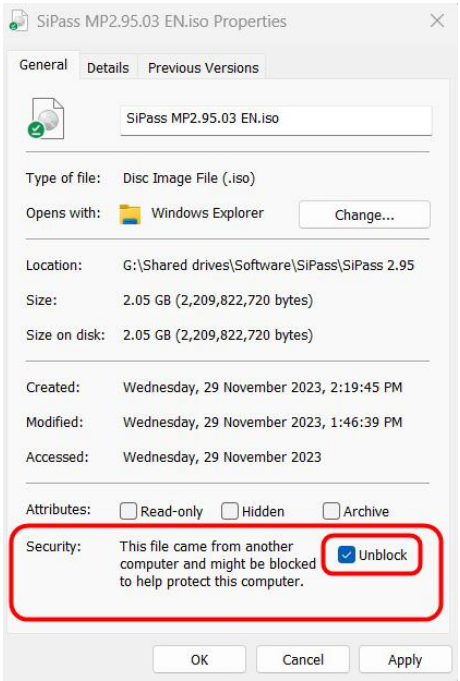
During setup SiPass all options will be installed also if LMU was installed before and the SiPass options activated.
If e.g. HR API is not part of the license the corresponding service will not be started.

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

Preparation: Allocate the "SiPass Service User"

The SiPass-Services will be started with a standard windows account.
This standard windows account will be called "SiPass Service User".
To make it easy, also name the dependent standard windows account for example "SiPassServiceUser".
As preparation the "SiPass Service User" can be allocated in front of the SiPass installation.
During the SiPass installation the "SiPass Service User" must be selected.
(also have a look the page 14)

<u>Note:</u> In front of the SiPass installation from ISO-File!



In front of the SiPass installation, the ISO-File must be unblocked.
Open the properties of the ISO-File.
If the "Unblock" tick-box is shown, the ISO-File is blocked.
Then tick "Unblock" and "Apply"!

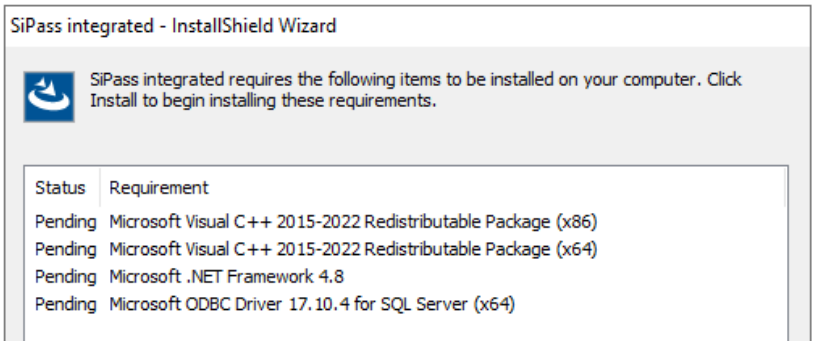
If SiPass will be installed with a blocked ISO-File, often the SiPass-Server-Service can't be started!

Implicit "Unblock" ISO-File!

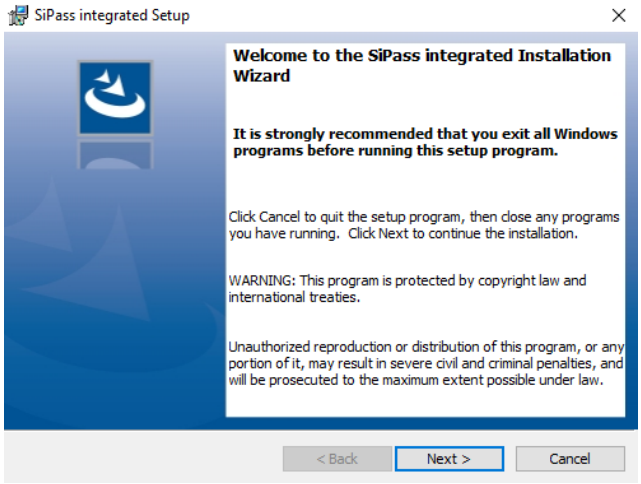
It is recommended to mount the DVD ISO or copy the full SiPass DVD to C:\ and start the installation from there.

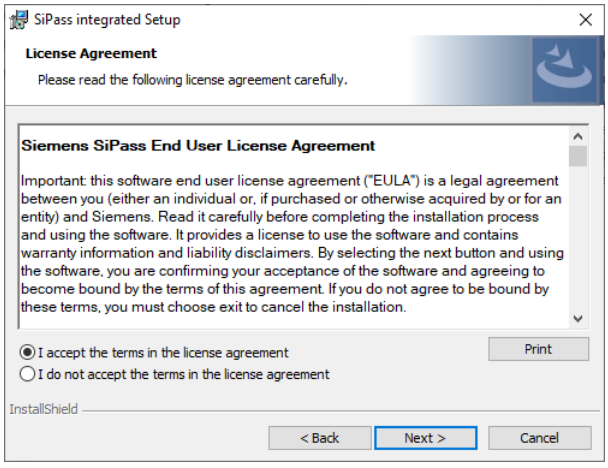
To start the SiPass integrated setup please execute the **„Install.exe“** from the DVD image root as Administrator (right click -> run as Administrator).

The setup checks first the PC environment an install necessary system application.
Microsoft not allowing a hidden installation of some applications.
This is the reason all need to confirm terms and conditions one by one, e.g.

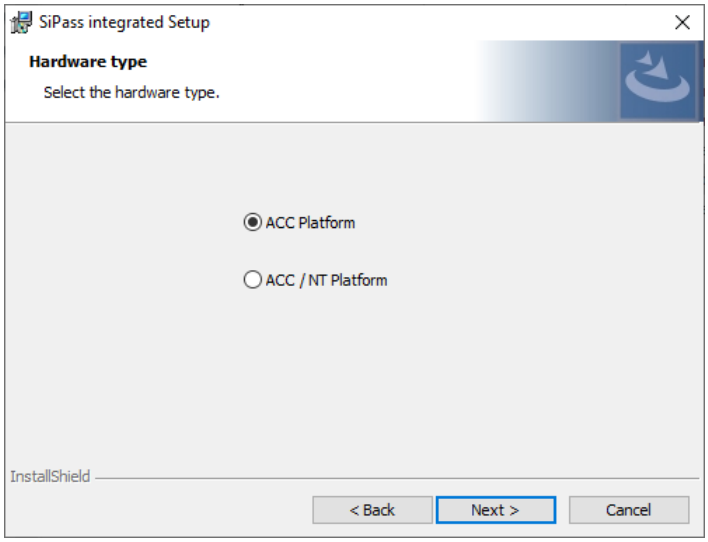


After the pre-setup is finished the SiPass integrated setup starts with the Welcome dialog.
On the next page the license agreement has to be accepted.





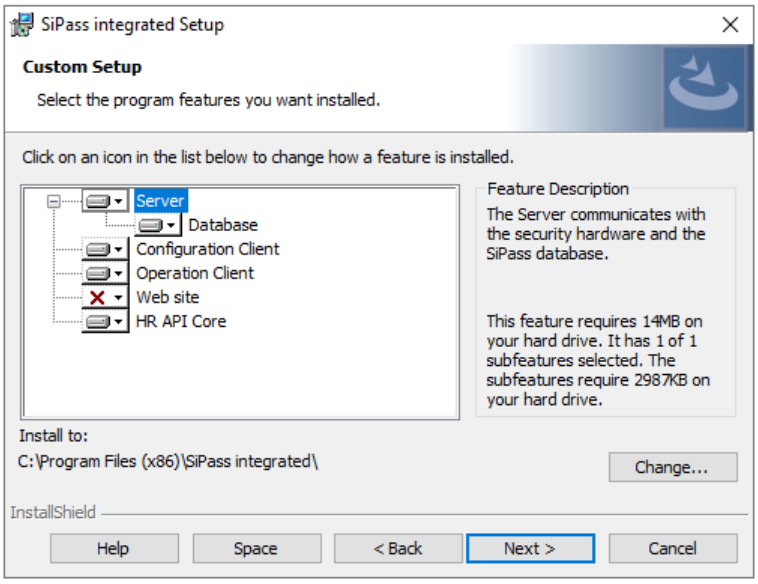
In the next dialog has to be defined which hardware platform is used, because SiPass integrated can still migrate an older systems called Advantage NT.



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

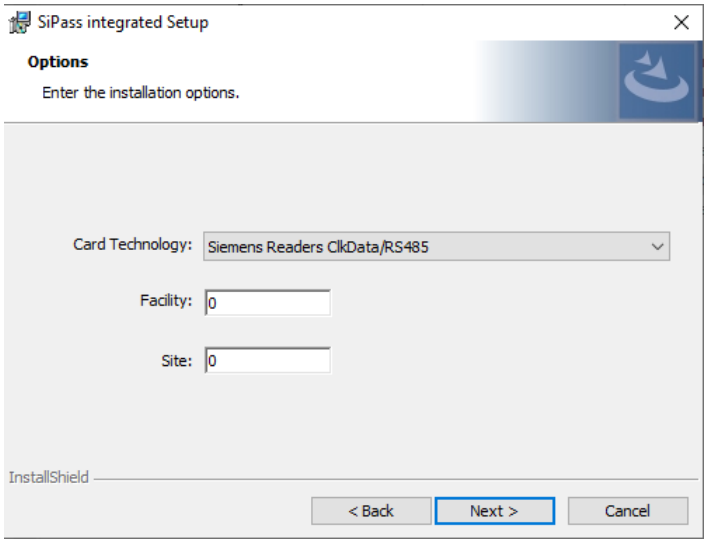
The ACC/NT Platform is for SiPass in conjunction with the “Advantage NT” and ACC controllers.

Select the features for the installation.
Since the SiPass version 2.90 the Webserver “Website” installation can be deactivated.
If later Web-clients will be needed, it is possible to additional install the Webserver any time it is needed.



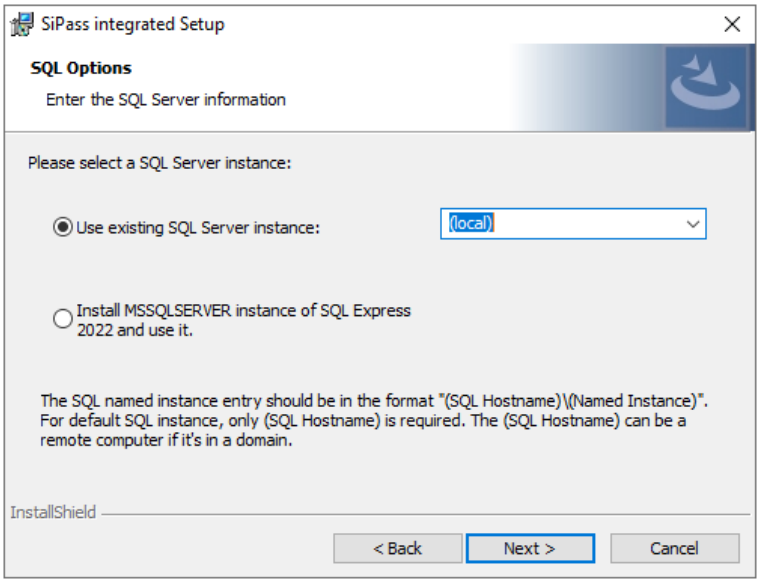
The installation path can be defined via “Change”, if the “Server” is selected.

This the new setup dialogue to define Card Technolgy, Facility and Site code.
Simply choose what is needed.

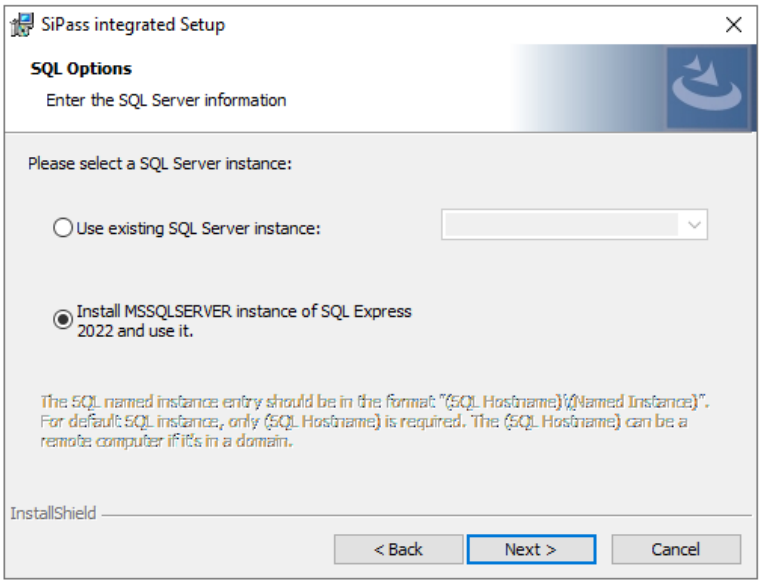


If you have chosen wrong card tech, it can then be changed via the Operation Client Credential Profile dialogue.
Consider, a change is only possible if no card is assigend to the credential profile.

Click Next and select the SQL Instance you want to use for the SiPass integrated system.
Since SiPass 2.90 the SQL-Server must not be on the same PC as the SiPass-Server.
(For an external SQL-Server have a look to the courseware “SiPass with remote SQL”)



If no SQL is available at the SiPass Server PC or the existing SQL installation is not compatible with SiPass integrated, SiPass setup offering to install SQL Express.



Each SQL database installation needs to have an “SA” administrator set.
SiPass integrated setup 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.

It is needed to accept the terms in the license agreement for SQL Express setup.

Info “SiPass Service User”:----------

The SiPass Server Service has to be started by its **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 a Host Event Task.

Attention: As “SiPass Service User” don’t use the User who is at the moment used for the Windows login! This will create an error.

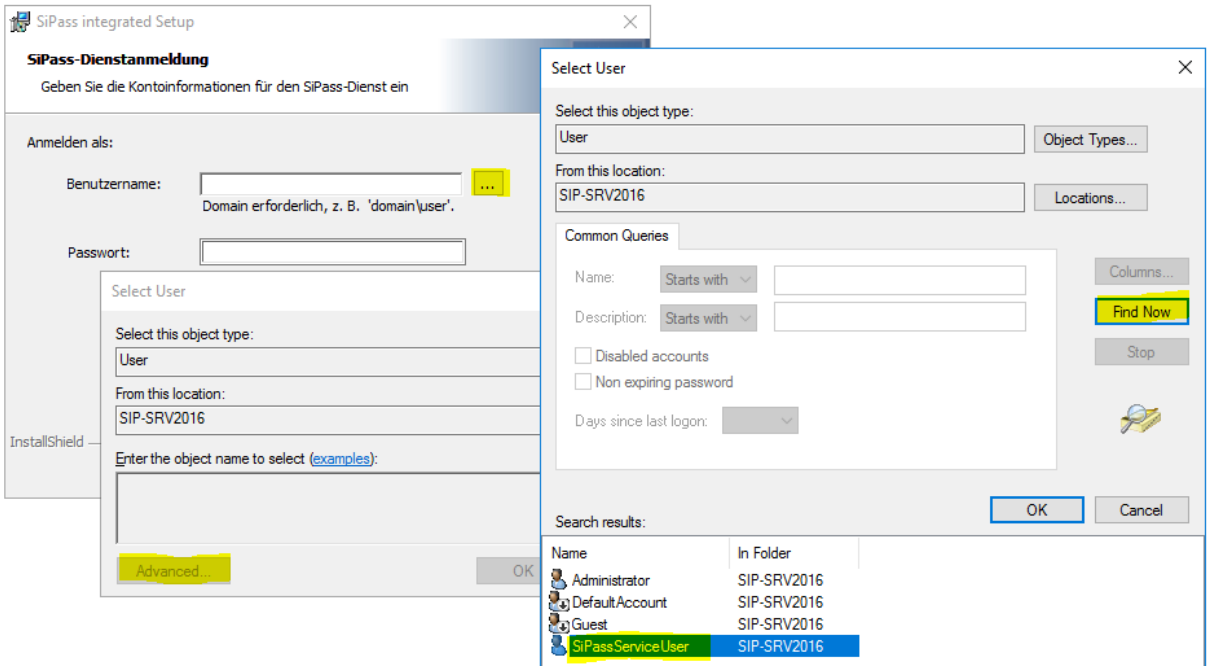
Please note: It is not possible to change the SiPass Service User afterwards.
If this is required SiPass need to be reinstalled with the new Windows User for the SiPass Service (create an backup of the database before you reinstall SiPass).

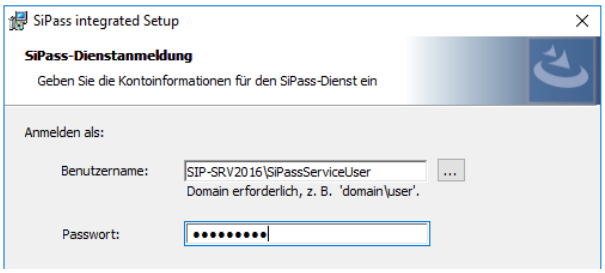
Since SiPass version 2.95 it is possible to change the SiPass Service User password.
Therefore, the followings steps needed:

- stop all SiPass services.
- change SSU password at the AD or Local Users and Groups
- change the PW at all SiPass Services (Properties \ Log On)
- start SiPass services.

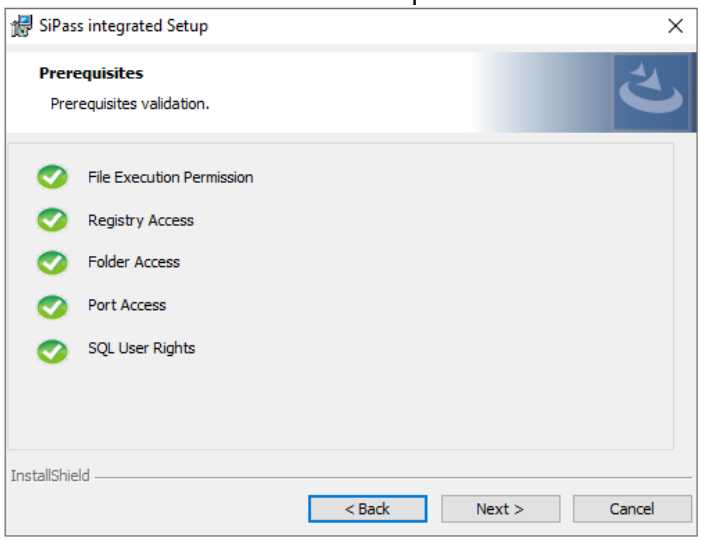
Tip: enter “LUSRMGR.msc” to the Run
Dialogue (open with WIN + R) and create the needed User (if a domain is used the Domain- or Active Directory-Administrator need to create this Windows user).

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.

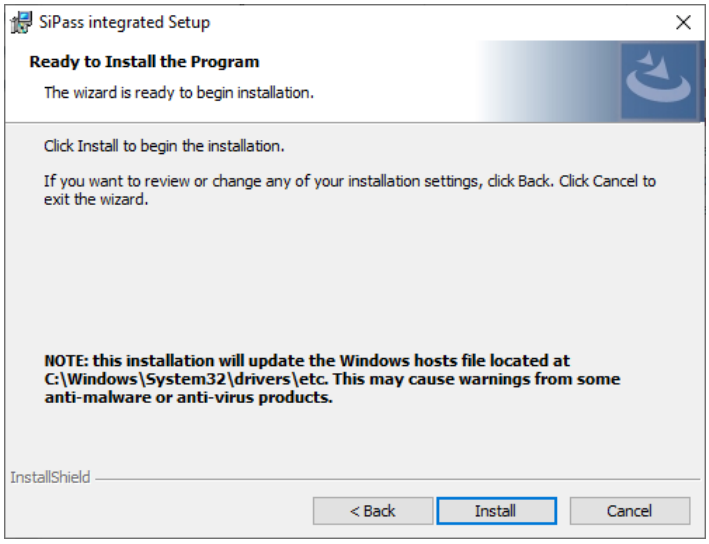




Since 2.95 the installation requirements will be checked.

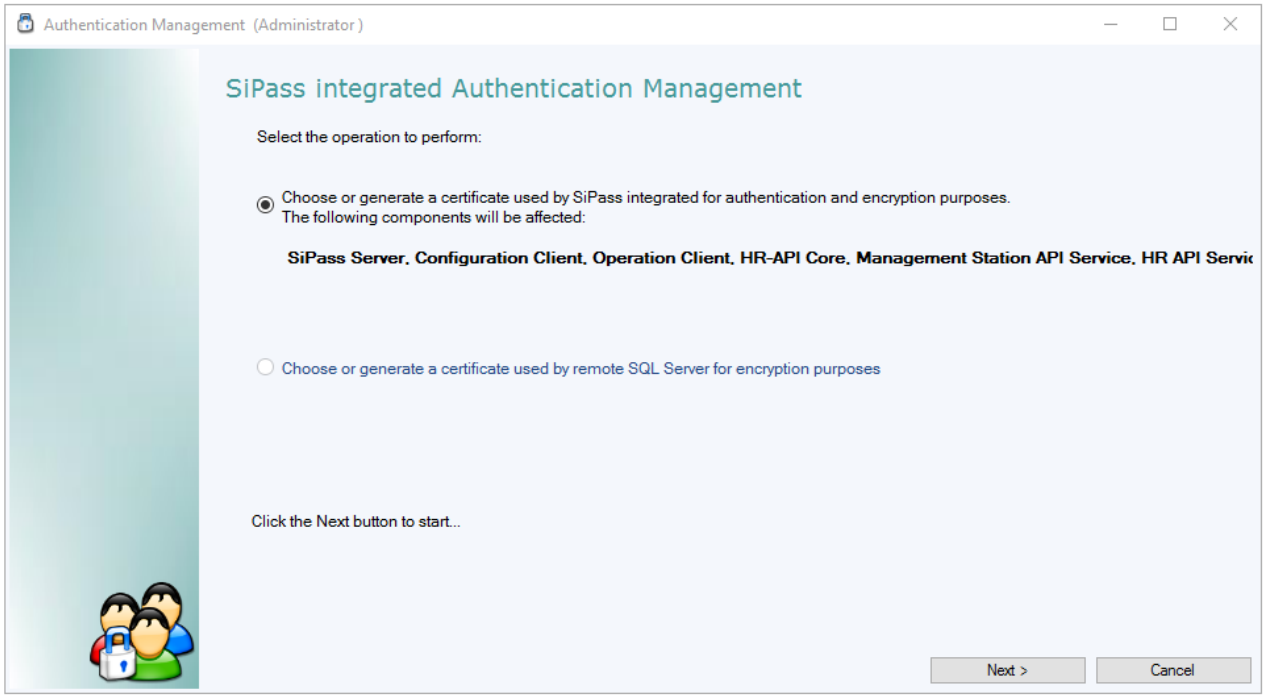


The "Ready to Install the Program" dialog is displayed.



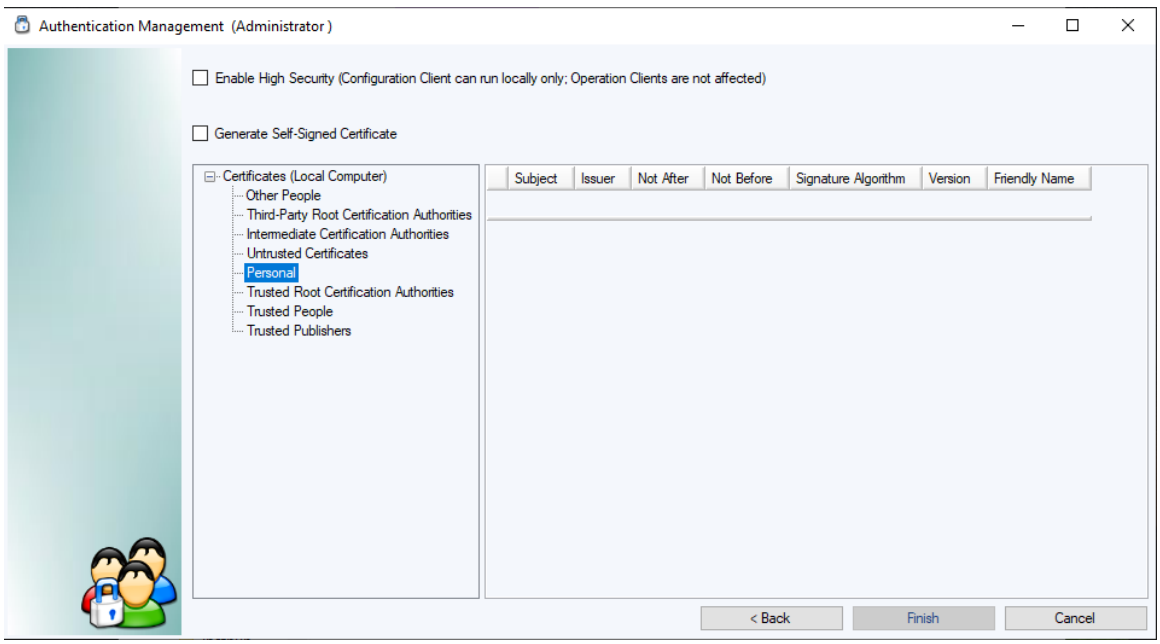
Now the SiPass setup install all the needed stuff, this will take some minutes.

SiPass Authentication Management Wizard is displayed to select existing Certificates or create SiPass “Self Signed” certificates.



Two Certificate options can be used

1. Applying an existing Machine Certificate
   Use of already existing certificates of the PC
2. Generate and apply Self-Signed Certificate
   Certifates for SiPass will be generated



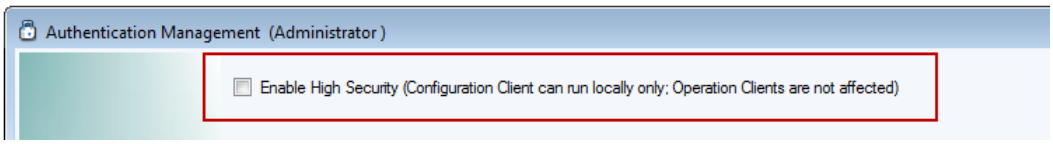
You can install SiPass integrated Server and Remote Clients using a Machine Certificate or a Self-signed Certificate. While the basic process remains the same in both cases, the difference lies in how the certificate identity is authenticated among the Server and Client Computers.

Self signed certificates (see page 18)
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 19)
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.

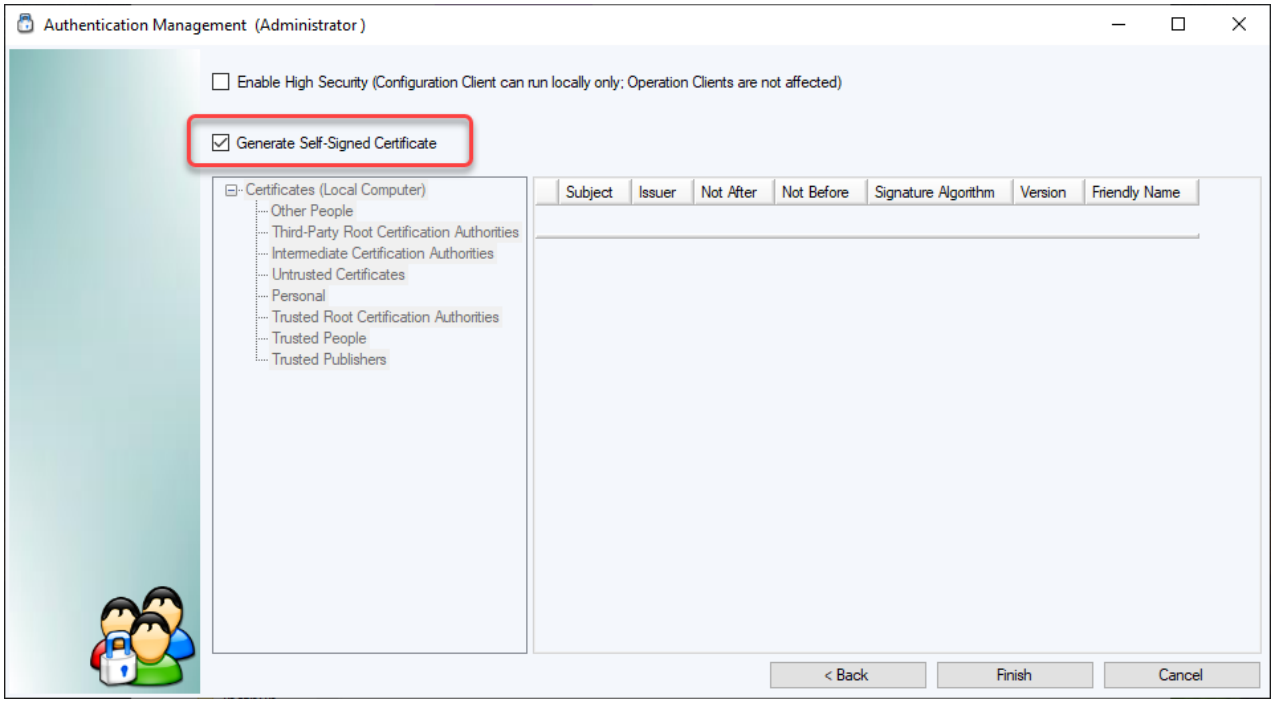


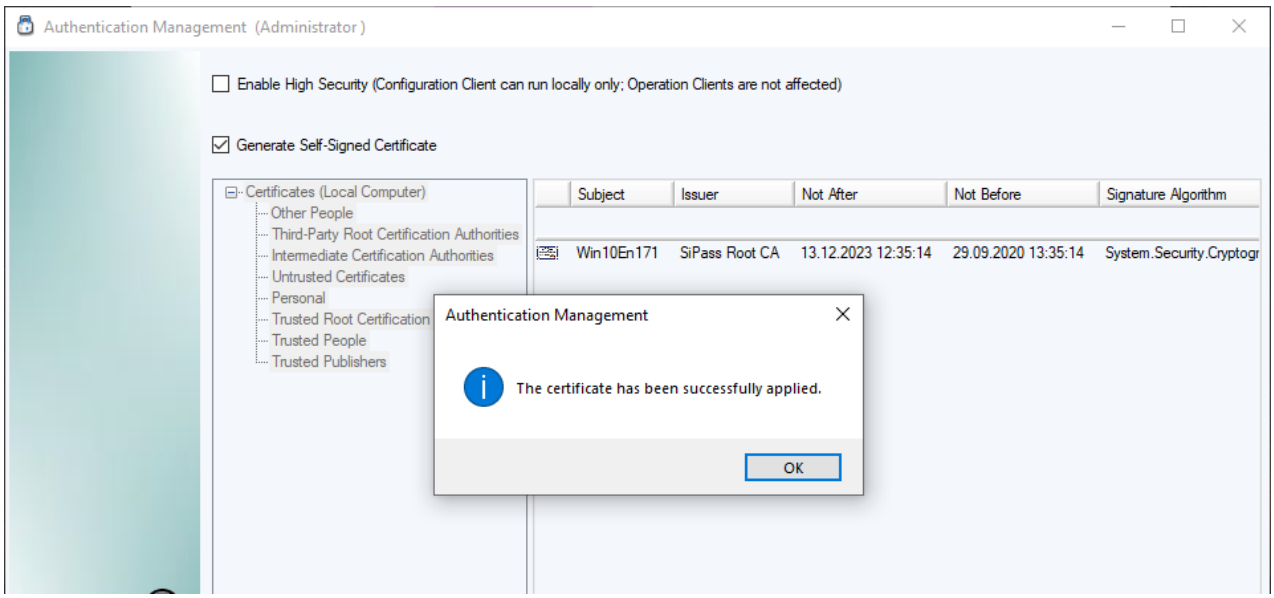
If you select Enable High Security, the Configuration Client can only run on the SiPass Server PC itself and not from a Remote Client.

Use Self signed certificates

Select Generate Self-Singed Certificate and click to 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.



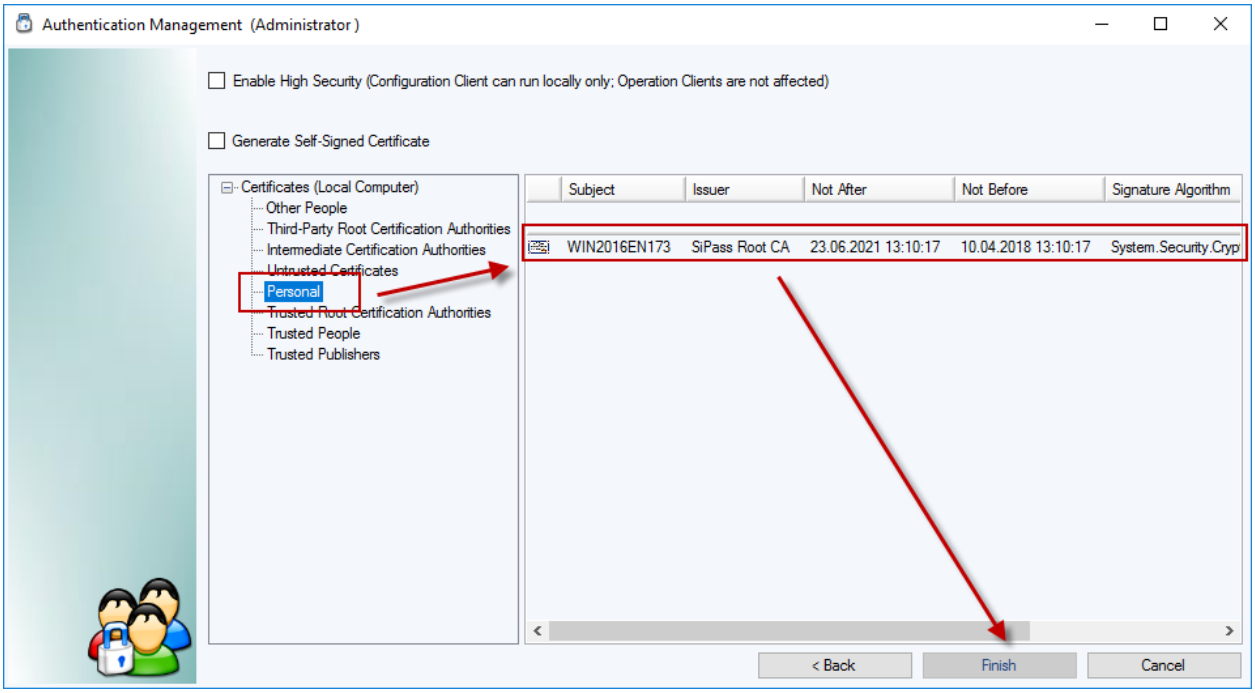


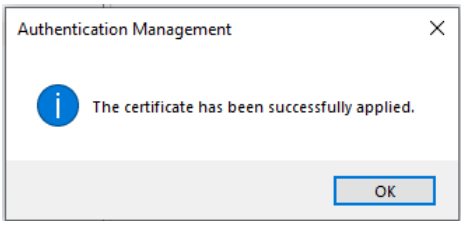
Use Machine certificates

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).

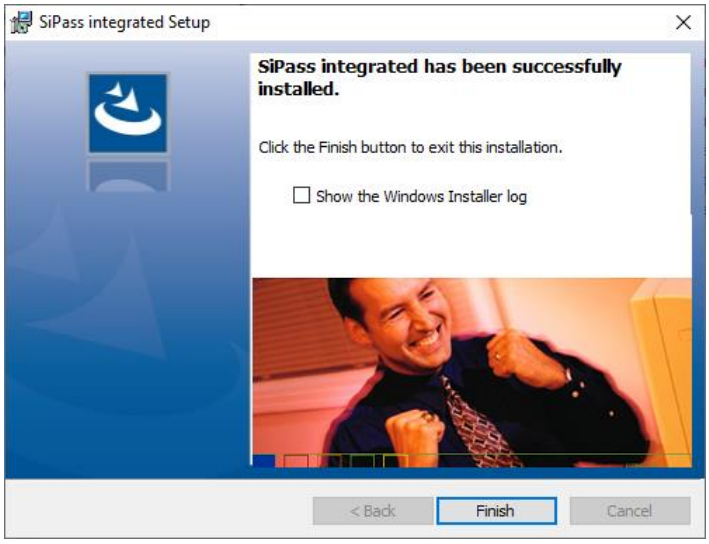
Note: Only the certificates with a private key are listed here.

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



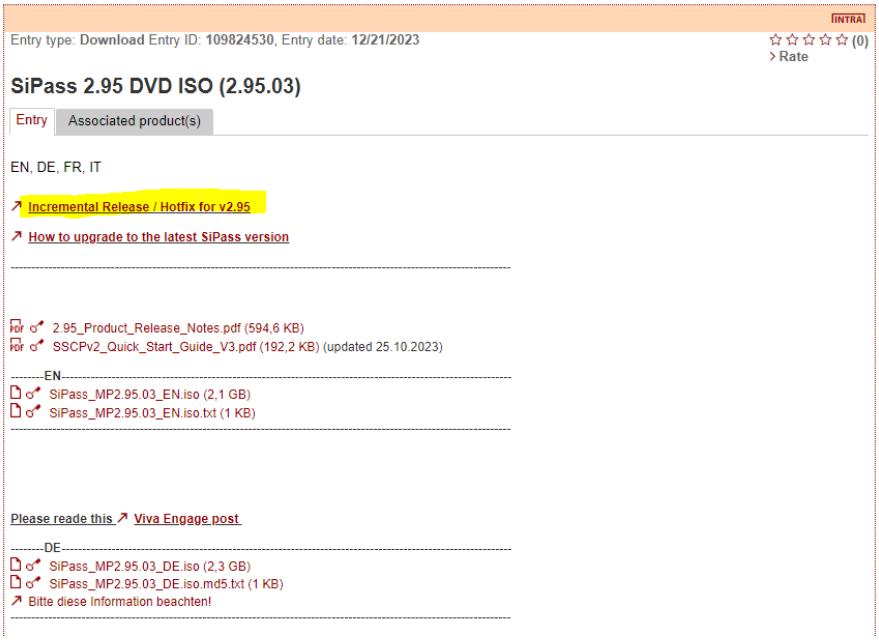


Setup of SiPass integrated successfully completed.



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

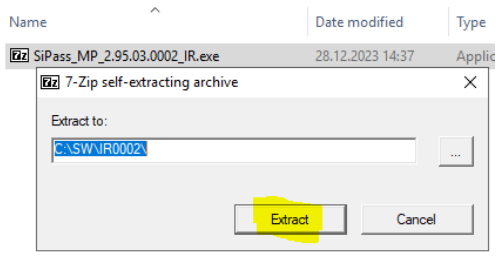
IMPORTANT:
Do not forget to apply the latest patch before you start configure the system.
A link can be found always inside the SISO download container of 2.95.
SiPass 2.95 DVD ISO (2.95.03) - ID: 109824530 - Industry Support Siemens

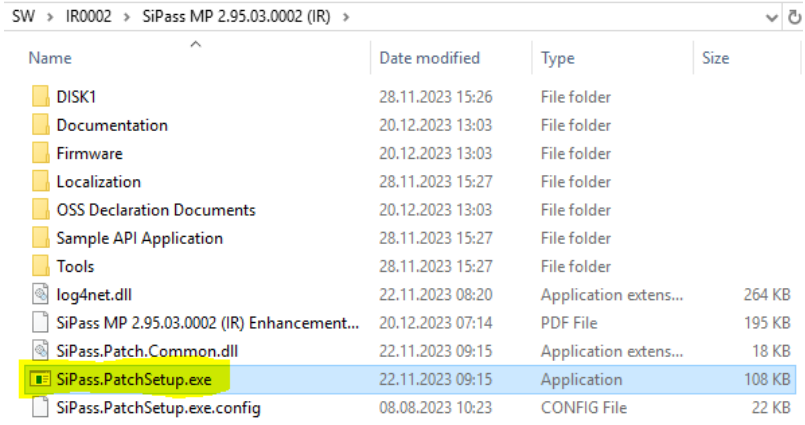


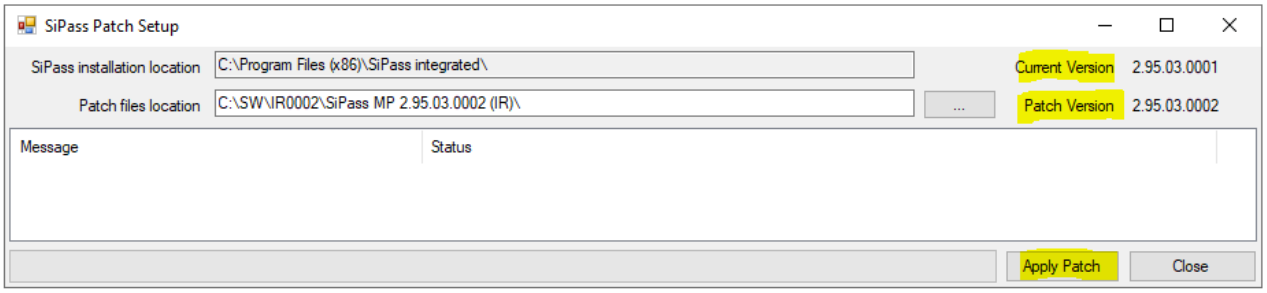
➔ continue with “login” at chapter 12.

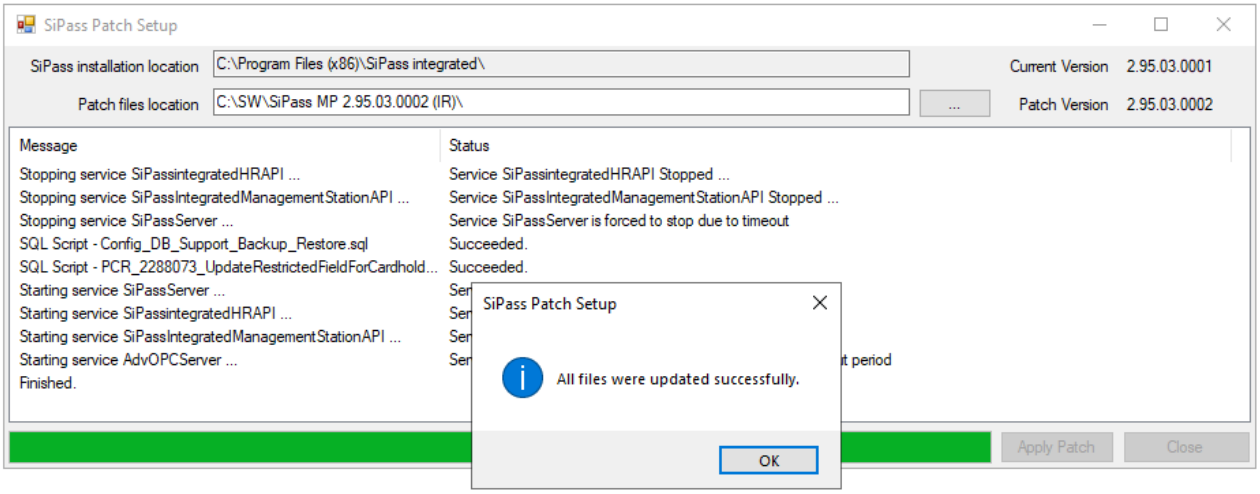
Example: SiPass 2.95.03, Incremental Release 0002.

IR=Incremental Release; HF=Hotfix
Always use the latest Release, doesn't matter if the latest version is a IR or HF.









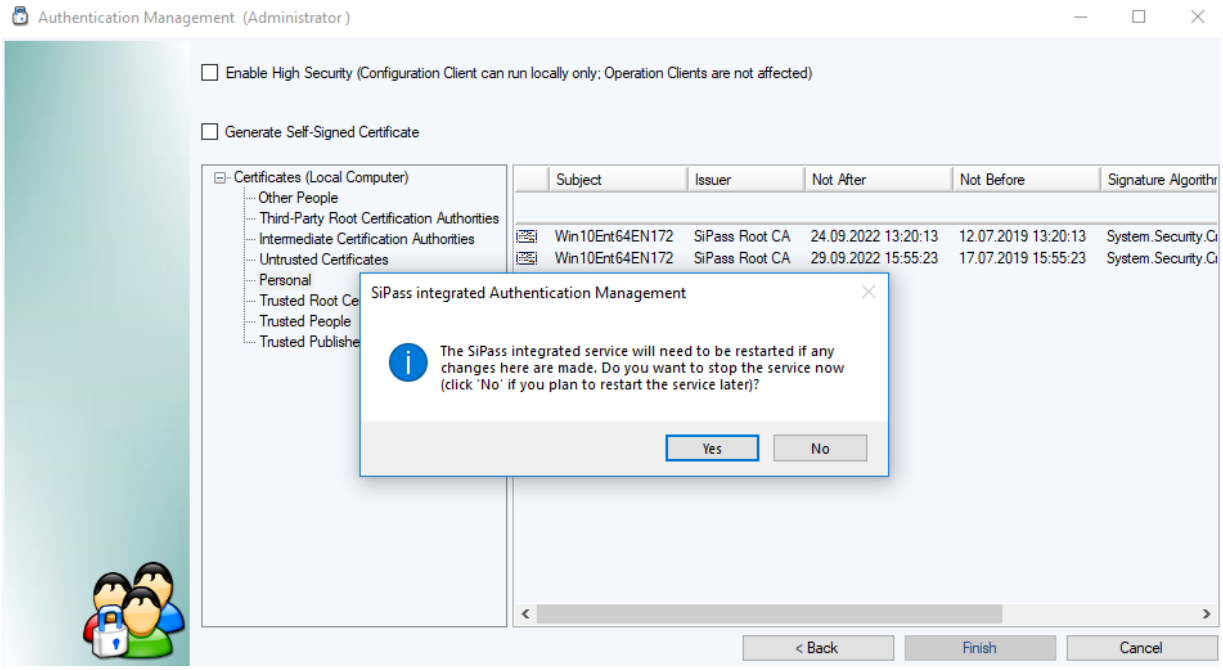
9. Renew certificate

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).

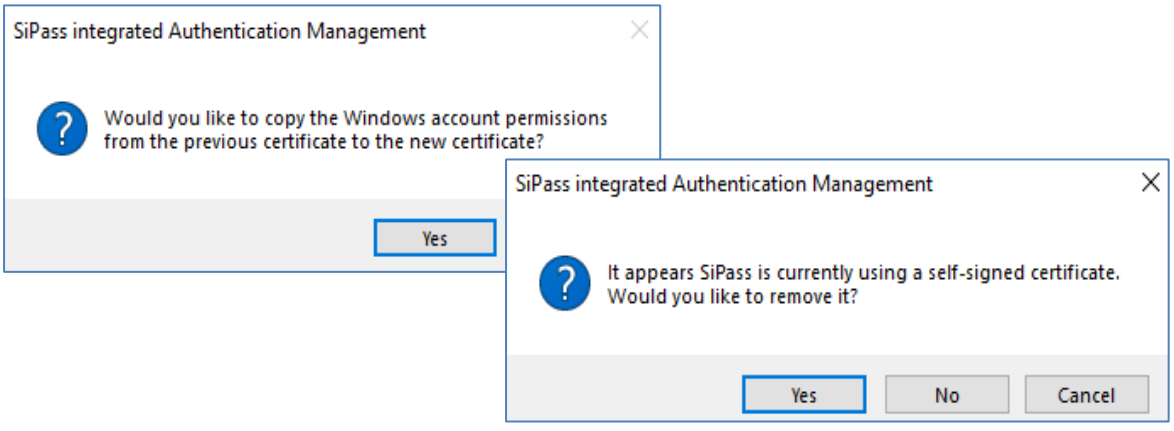
9.1 Renew self-signed certificate

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

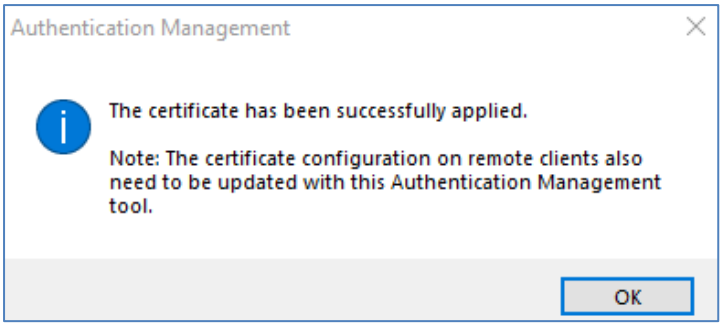


We recommend to stop the SiPass-service in front.
After that activate that option “Generate Self-Signed Certificate”.

The following questions we recommend to answer with “Yes”.



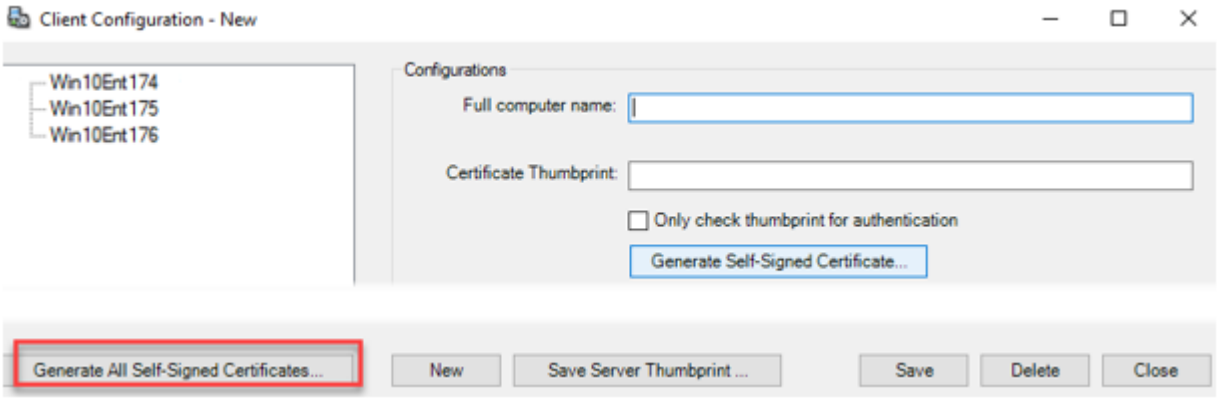
If the procedure was successful you will get the following information.



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.

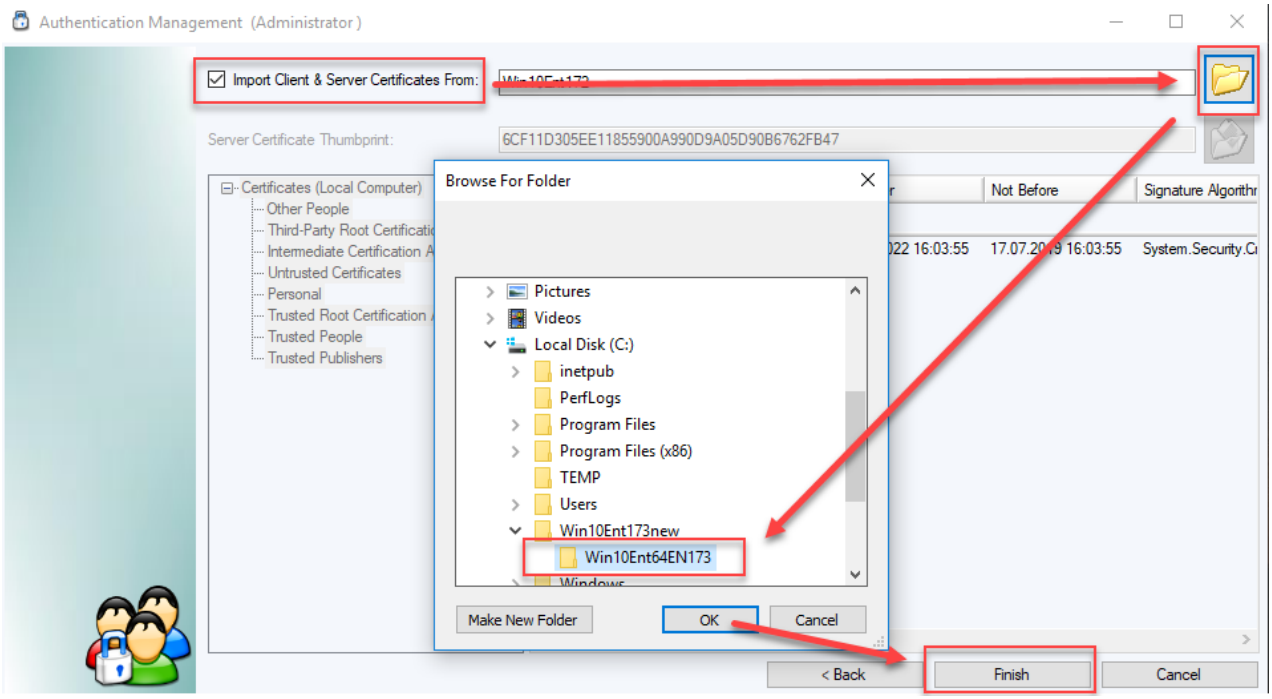
9.2 Renew remote client certificate (based on the self-signed Server certificate)

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.

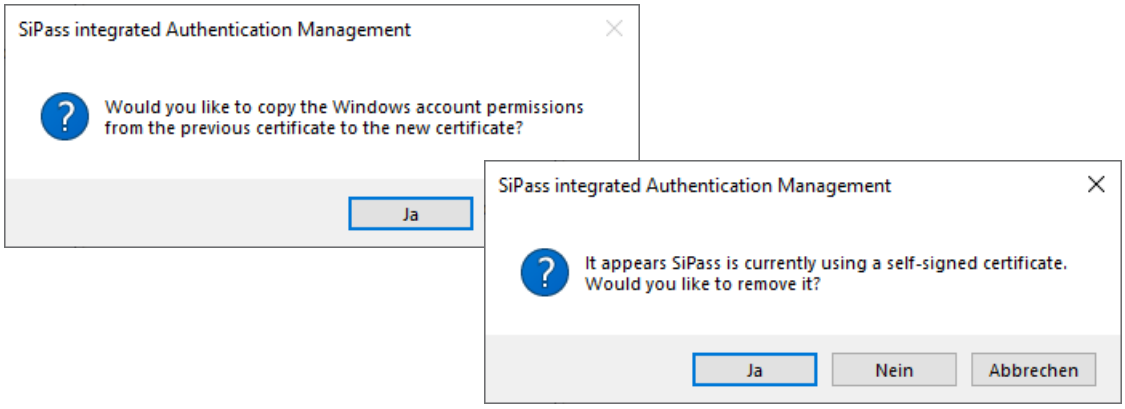


Choose "generate all self-signed certificates" and create a new folder.
In this new folder each client will get a separate folder allocated.
Now copy the new created remote client certificate to the respective remote client.

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.

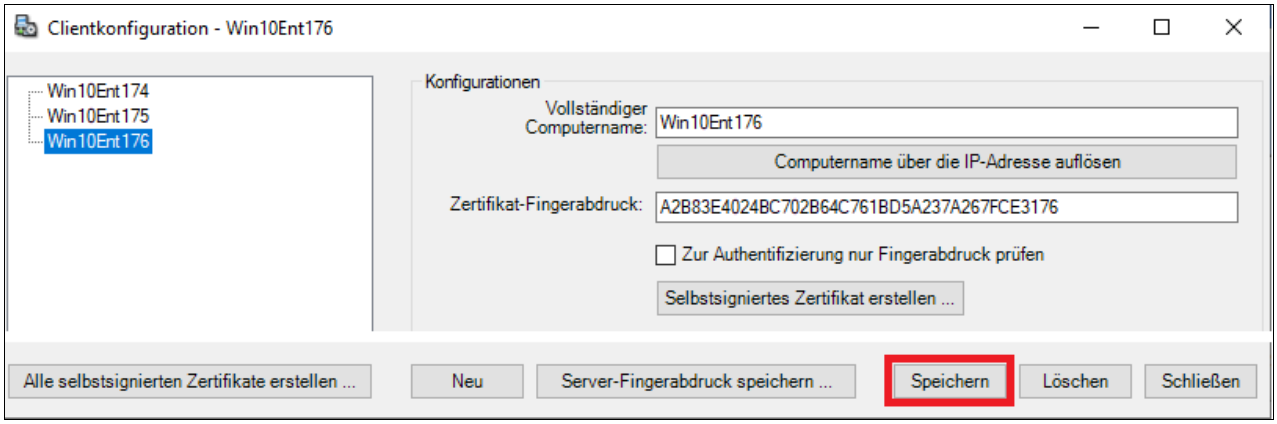


The now shown certificate-thumbprint is only a information, no additional actions needed.

9.3 Renew Machine certificate

SiPass Server side:
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. For the SiPass Server the certificate is changed now.

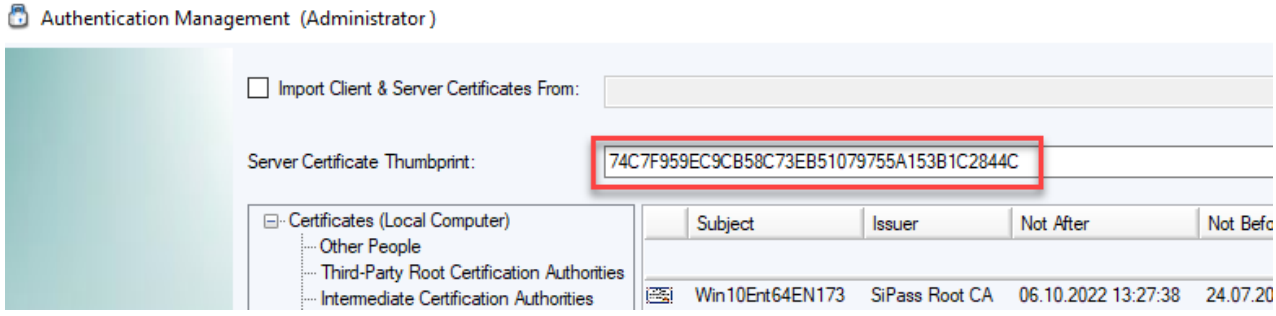
If remote clients connected, it is needed to enter at the "Client configuration" for each client the "Thumbprint" of the new remote-client-certificates



Remote client side:

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.



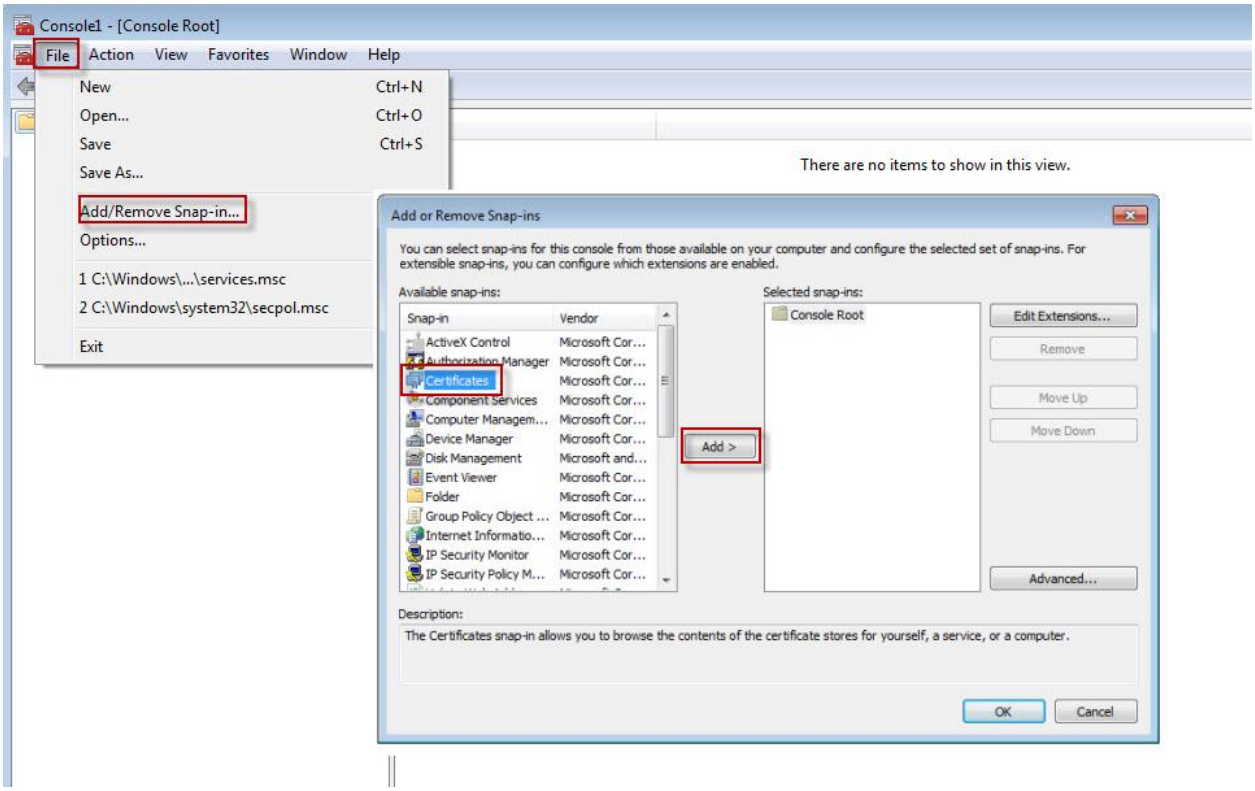
If the Server Thumbprint is not known:
In the "Client Configuration" mask is a button to store the Server-Thumbprint.

10. Manage the SiPass Certificates

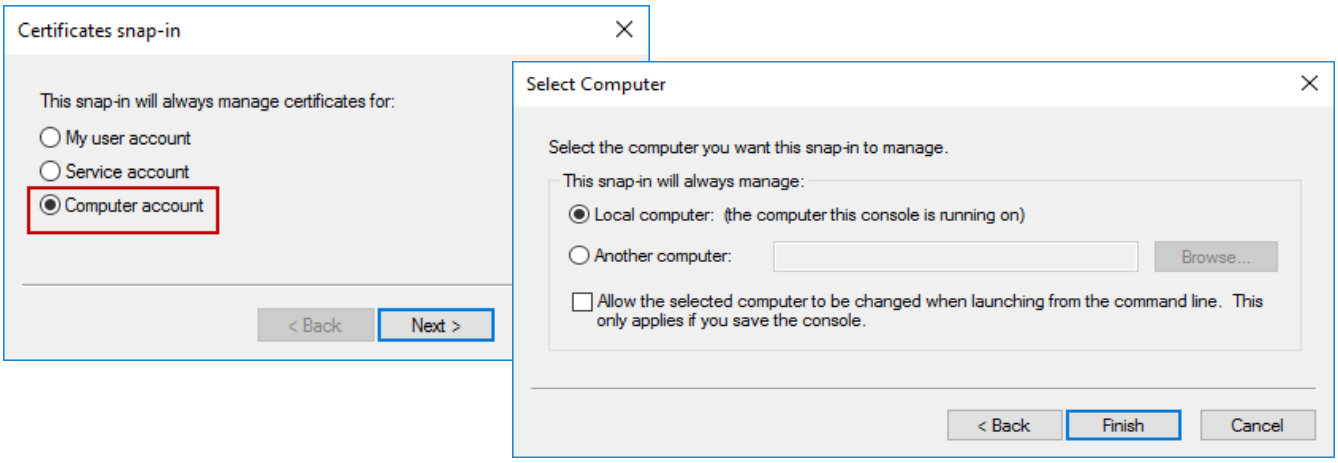
For the following described steps it is mandatory to use a Windows Administrator account.

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

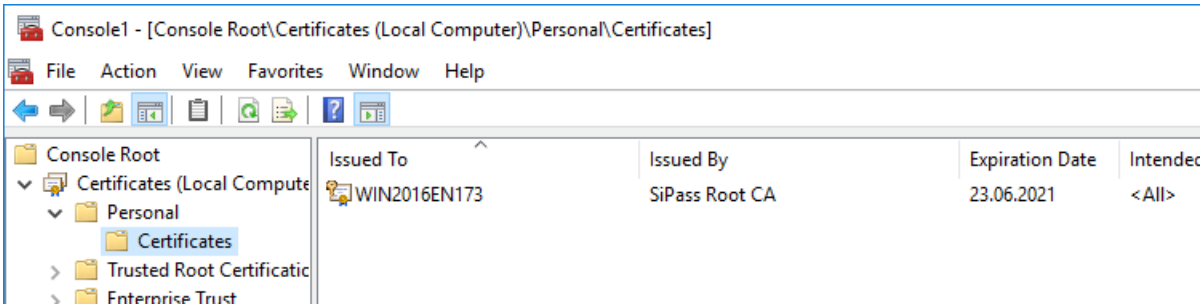
Click on File-> Add/Remove Snap-in-> Select “Certificates” and click on Add.



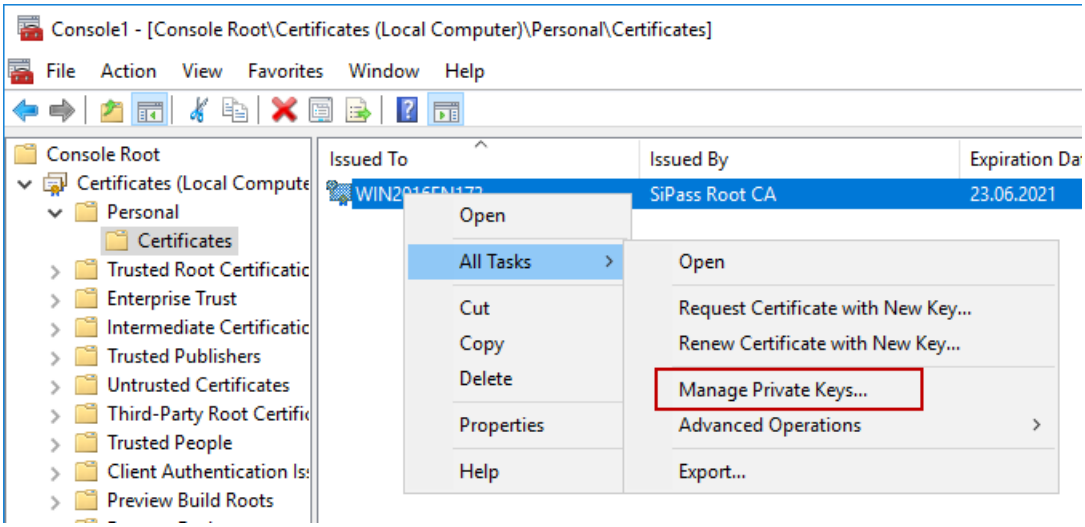
In the new opened window select “Computer account” and click Next.
Select “local computer” and click on Finish.



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



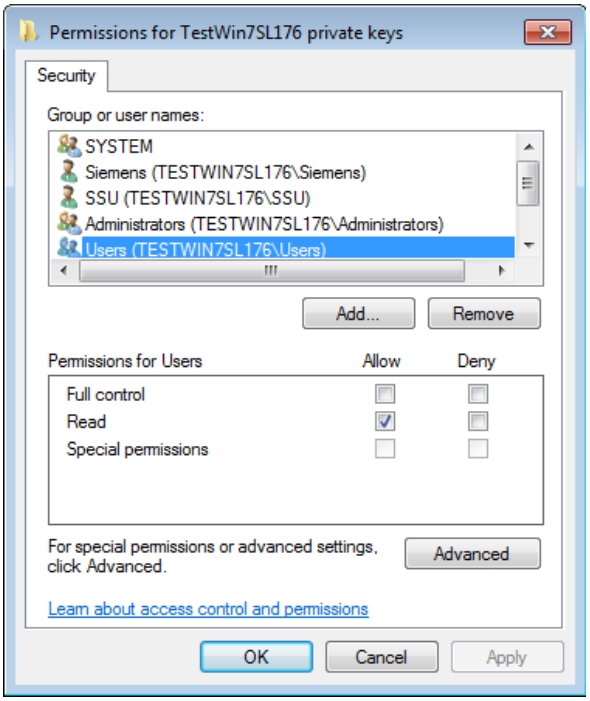
To Change the access rights for the users of the certificate select the certificate -> click with right mouse button-> Select “All Tasks”-> “Manage Private Keys…”



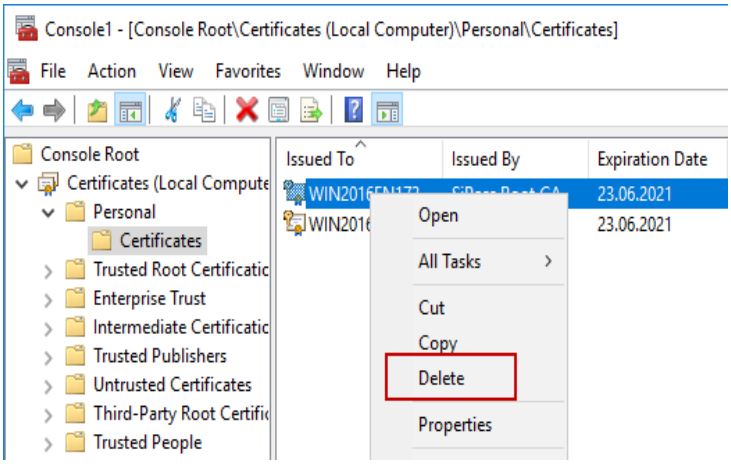
In the new open window you can add user/user groups to the certificate.

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.



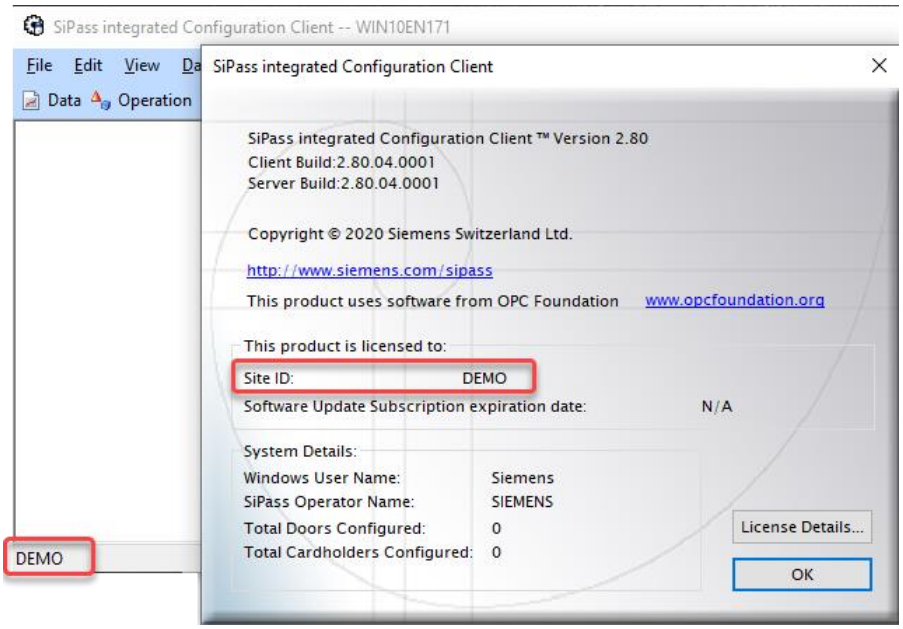
Delete a unused certificate:
In case the installation of SiPass fails it could be possible that 2 or more SiPass Root CA certificates listed in the mmc-console.
Not used certificates can be deleted vis right click to the certificate.
Keep the latest certificate. How to check: double click => Details => Valid from



11. DEMO installation

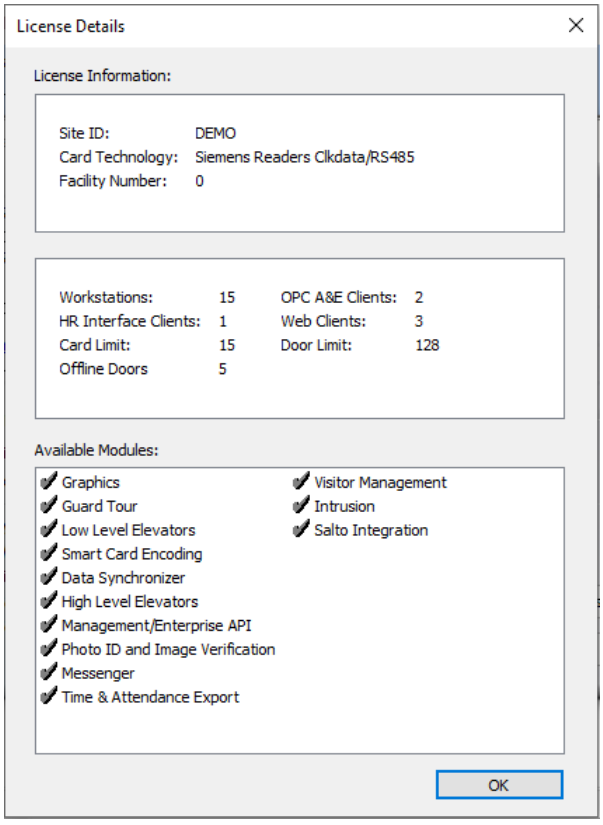
Any SiPass integrated installation is a DEMO installation.
If LMU is installed and a SiPass license avtivated SiPass will use the installed options.

Configuration or Operation Client will show DEMO until a CSID License is activated via LMU.
SiPass ask LMU every 10 minutes for a license update.



11.1 DEMO features

Theses are the 2.80 DEMO features (Help -> About -> License Details)



12. SiPass integrated login

Since MP 2.70 SiPass integrated has been spit into 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.

13. SiPass Client installation

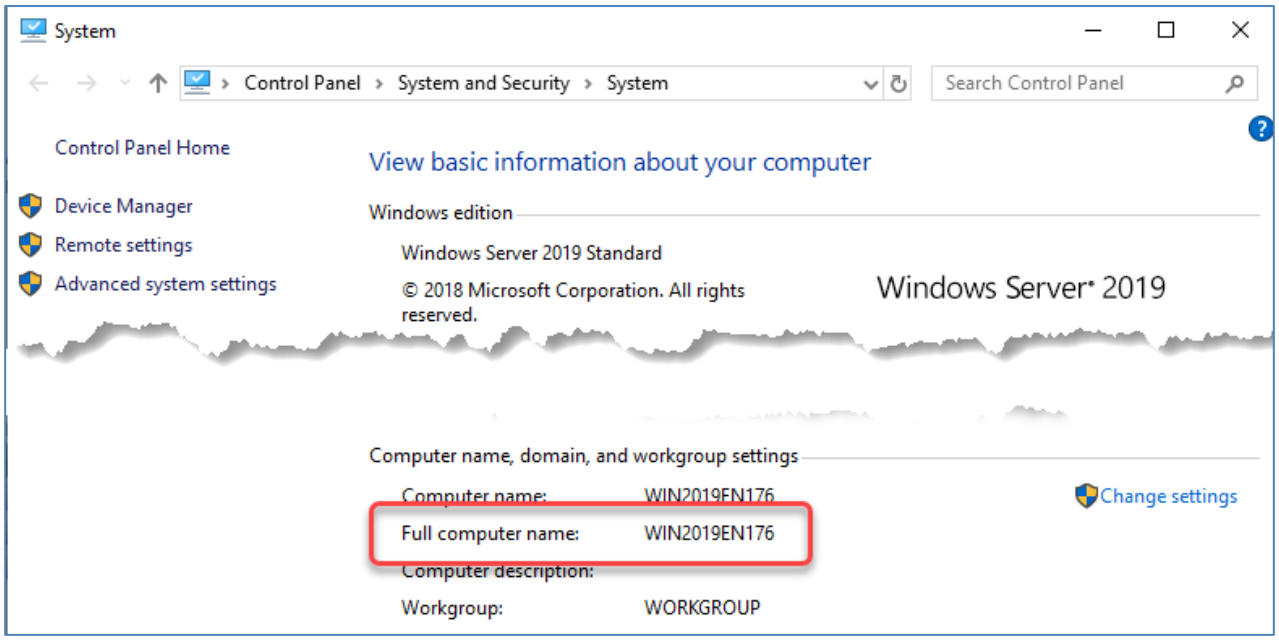
Feedbacks from the field show this is often not a simple task to perform.
With the enhancements we release inside 2.80 we hope it will be changed and at the end of the day all the installed remote clients up and running.

13.1. Client Connectivity Tool

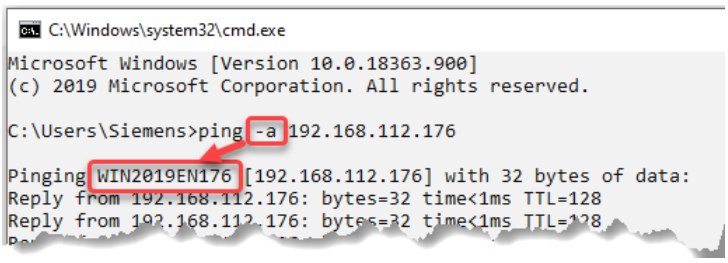
The new Client Connectivity Tool is located inside the tools folder of each SiPass DVD image. This is a powerful tool to check before setup the needed connectivity between future remote client PC and the SiPass server PC.

Copy it to the future remote client PC and run with Administrator rights: "SiPass.ConnectivityTool.exe".

Enter the Full computer name of the SiPass server PC, the name can be found at the Windows System dialogue (Windows Key + Break).

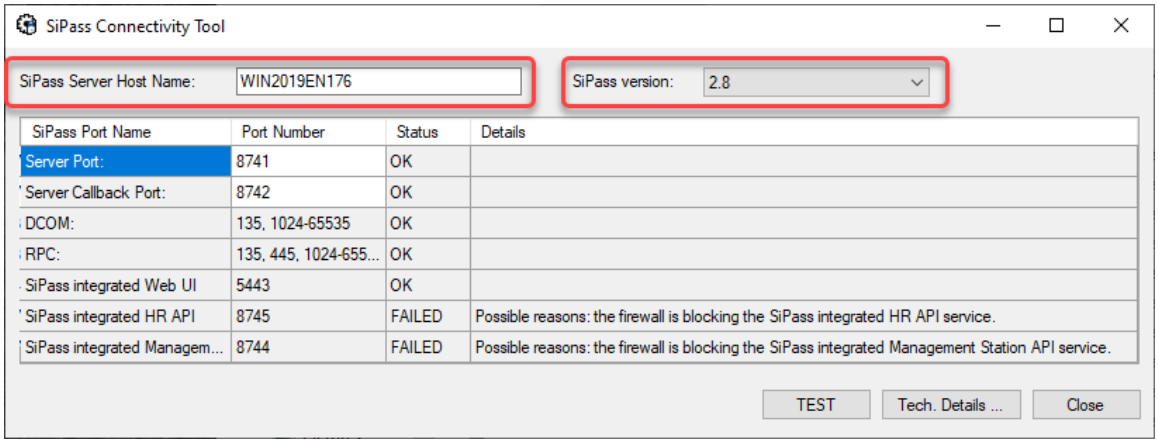


Alternative use the CMD command: ping -a [server IP address]
The result will be the correct server name which need to be entered into the Client Connectivity Tool and later during the SiPass remote client setup.



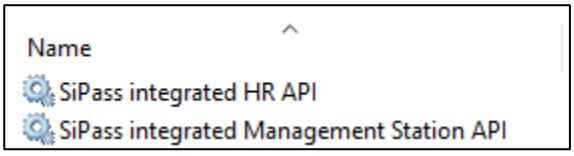
Workgroup environment with DNS function: This is a scenario when an internet router is run behind the Workgroup computers. In this case, the Computer Name and the router ID may get mixed up.

Enter the SiPass server PC name, select the correct SiPass version and run the test.



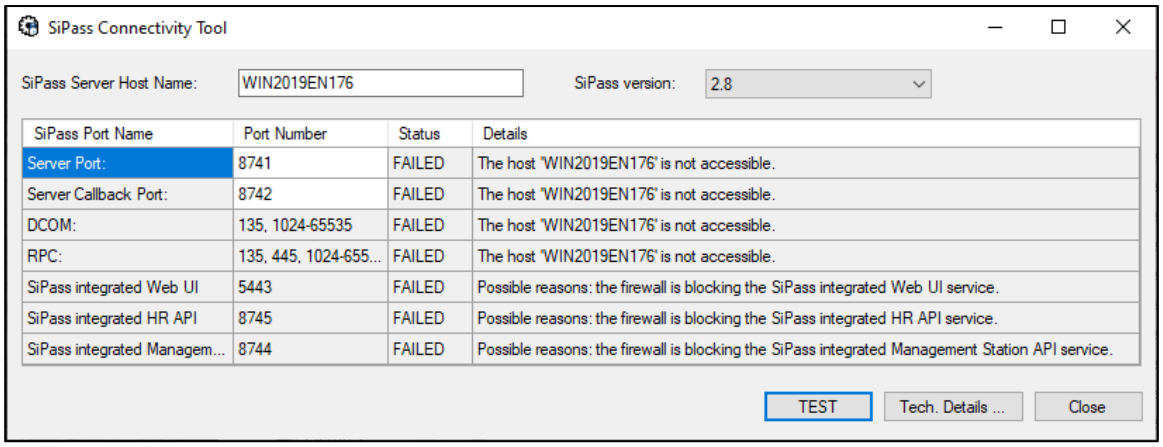
The above example shows a not started HR and MS API service. This can be ok if these two functions are not part of the licensed functions.

If they are licensed please check if the corresponding services are running and run the test again.



If the test shows a positive result start with the setup of the SiPass remote client.

The below test is resulting in a up and running Windows Firewall at the SiPass server PC with no exceptions.



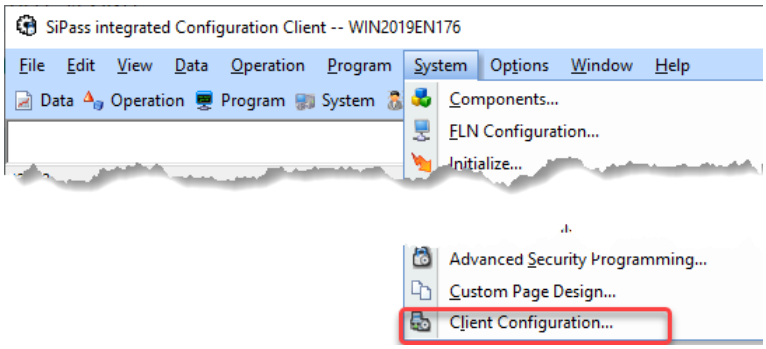
Take a screenshot and discuss the result with customer IT.

13.2 Remote Client setup

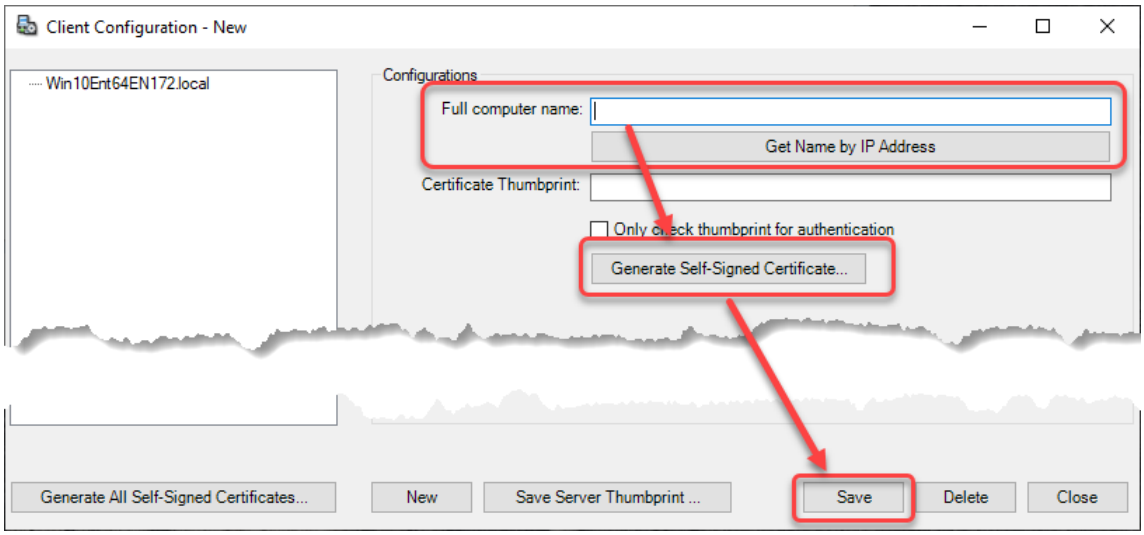
The following steps will explain how to install a remote Client with Self-Singed Certificate.

If you want to install with Machine Certificate, please refer to chapter 7 or the SiPass integrated MP2.80 Installation Manual from the DVD.

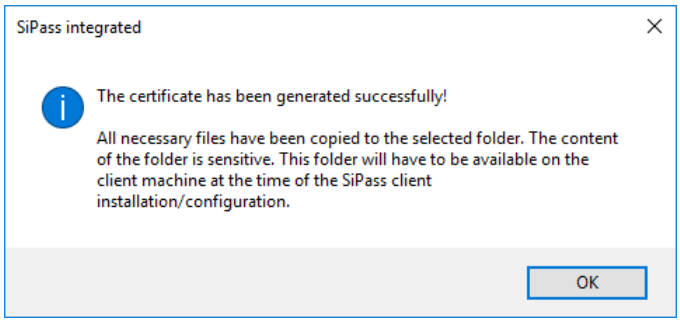
Start the Configuration Client and open the Client Configuration option at the System tab.



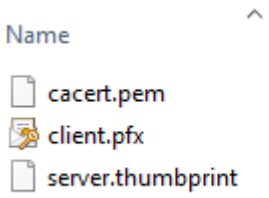
Since 2.80 it is possibility to enter the IP address of the Client PC and let SiPass Config Client search for the correct full computer name. Click afterwards Generate Self-Signed Certificate.
Alternatively enter the Full Computer Name of the Client PC manually and click on Generate Self-Signed Certificate.
Click on Save and select an empty folder where the Certificate should be stored. (always make new folder for each new client)



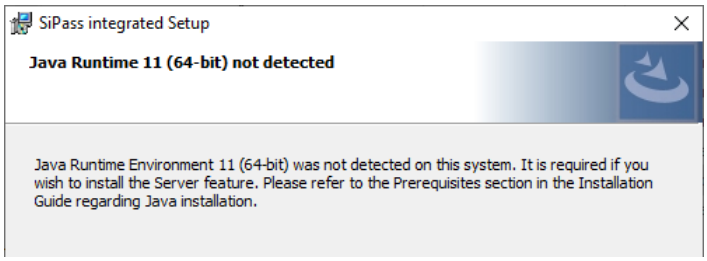
SiPass creates the Client Certificate and the Server Thumbprint in the folder you selected.
The folder should be accessible from the remote client computer.
You can manually copy this folder to the client computer or save it to a shared network drive or remotely access the server computer from the client computer.
After using the certificate, remember to delete this folder permanently to ensure security of information.



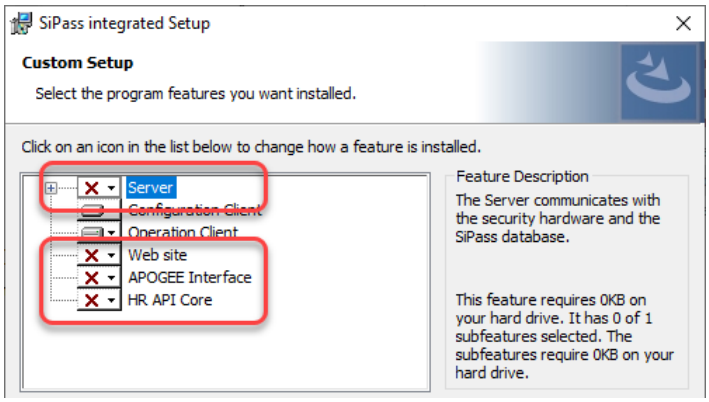
There are 3 files inside the Certificate folder



The SiPass integrated Client is installed in the same manner as the SiPass server.
LMU and Java Runtime is not needed at the Remote Client PC.
So this information can be ignored.

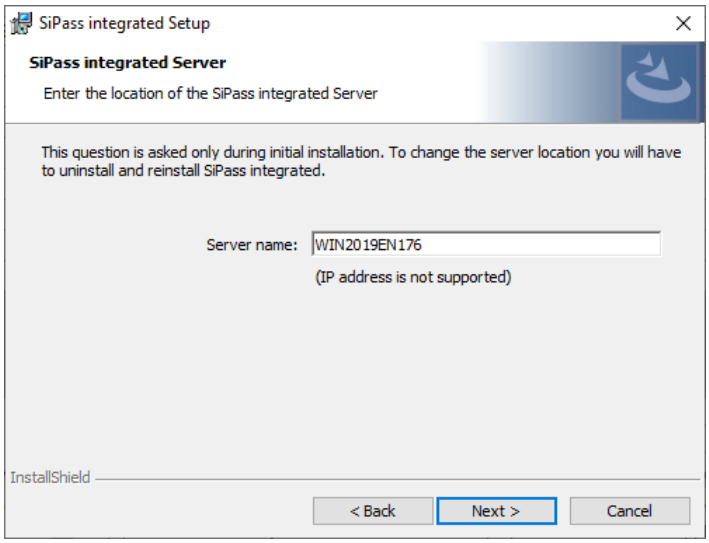


Select ***Custom*** installation.
During the SiPass client installation the “Server”, “Web site” and the “HR API Core” options have to be deselected.



Attention:

Enter in the Server name field the full computer name of the SiPass Server PC (see 10.1. Client Connectivity Tool) .



SiPass Client installation in a Workgroup environment:

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

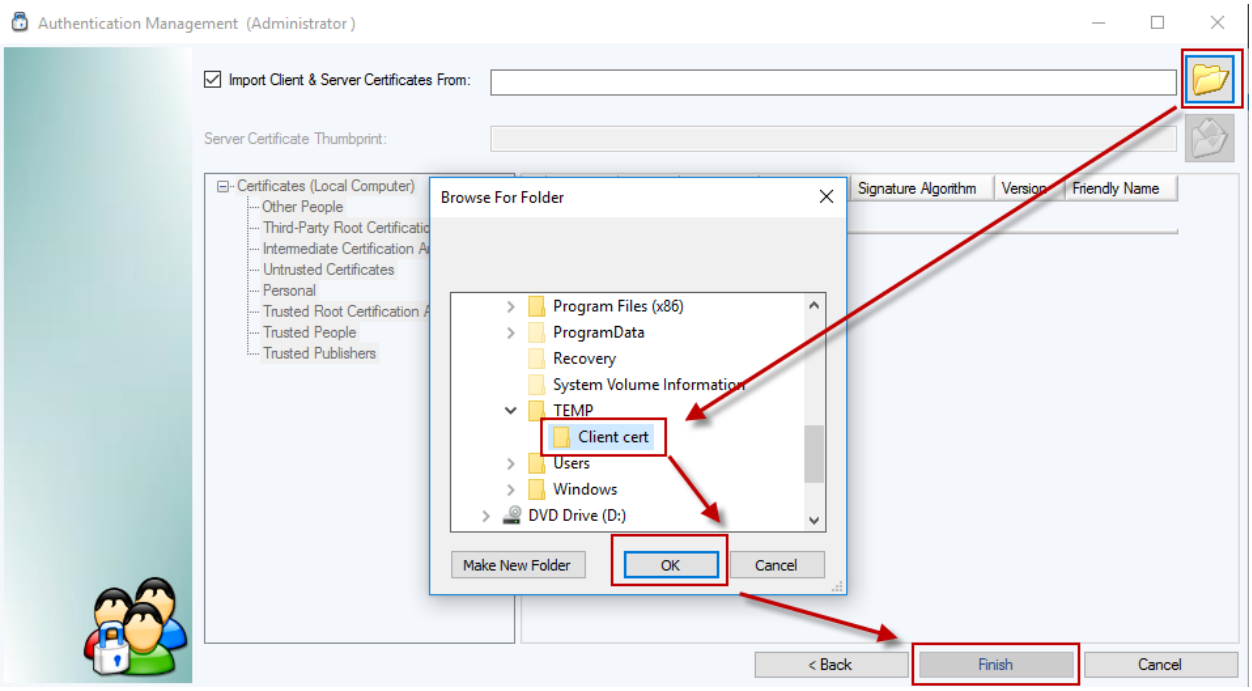
Info: If the Windows user is not known at the SiPass Server-PC, it is not possible to start the SiPass Client, following messages will be displayed: "The Server is starting up or is not available" error messages appears.

SiPass Client installation in a Domain environment:

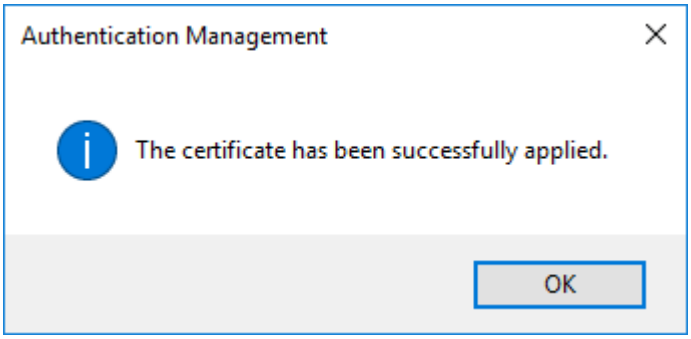
The Windows user of the SiPass Client PC must have at least local user rights at the Windows SiPass Server PC.

SiPass Authentication Management Wizard

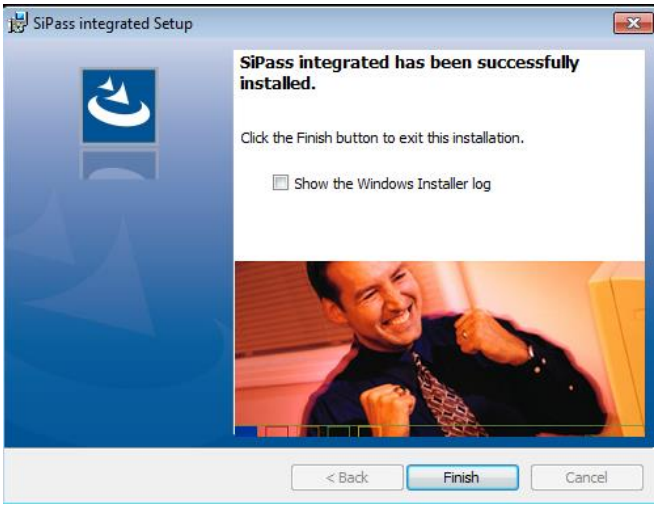
Select on the Client in the Authentication Management Wizard the Folder that contains the Client Certificate and click on Finish.



The Certificate is now applied to the SiPass Client PC.



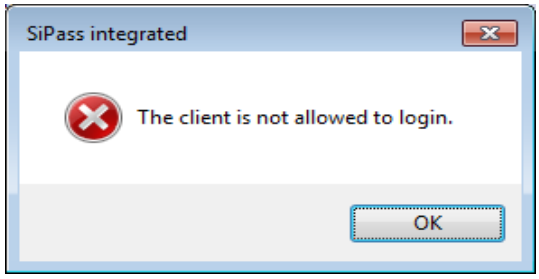
Setup of SiPass integrated Client successfully completed.



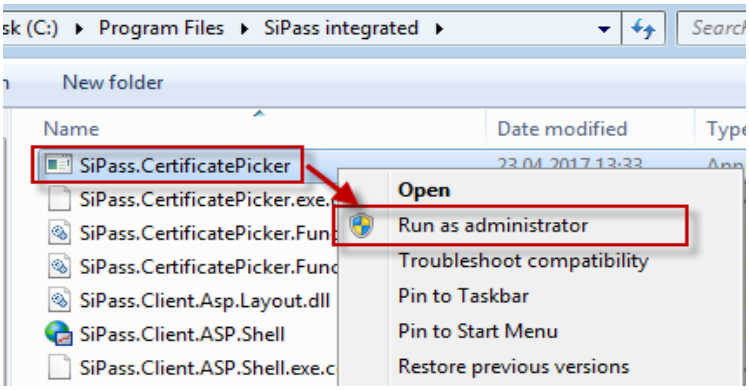
Apply the same patch as done at the server.
Otherwise the Client can not be used.

13.3 Client certificate invalid/expired

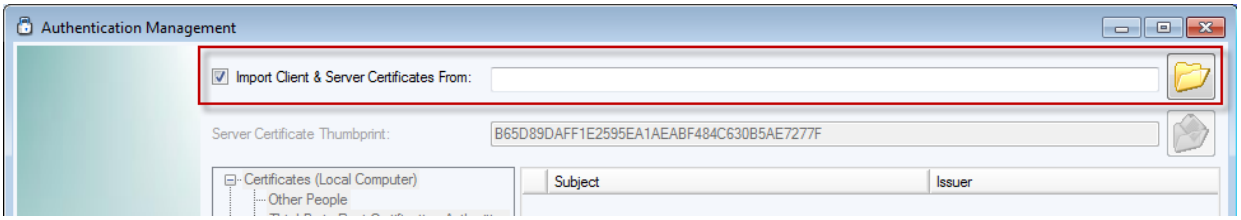
If the certificate does not match with the Server certificate you will get the following error message.



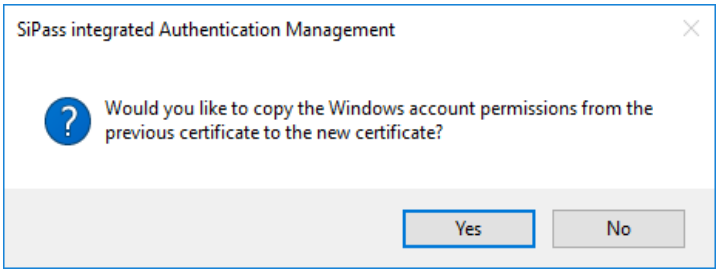
In this case you have to start the SiPass.CertificatePicker.exe from the SiPass integrated directory as Administrator and assign the correct certificate.
The SiPass.CertificatePicker.exe will be found in the SiPass integrated folder.



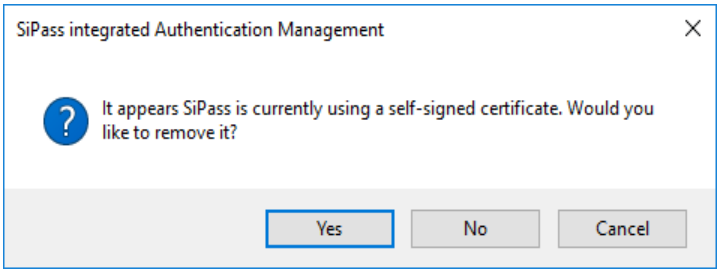
Please select the folder where the certificate is stored and click on Finish.



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

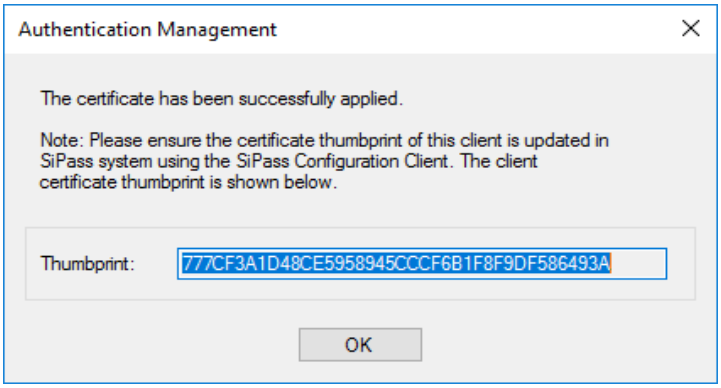


It is recommended to remove the old (not longer needed/used) Certificate.



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.



14. Update of SiPass features

Until 2.76 a new license had to be order and applied by calling the SiPass setup again and choose Modify.
Since 2.80, SiPass is using LMU and the license update is quite simple.
Order the needed options and activate it with help of LMU.
Wait 10 minutes and the function/expansion is applied to SiPass.

15. SiPass integrated upgrade path

It is possible to upgrade from older SiPass integrated version to MP2.90.

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

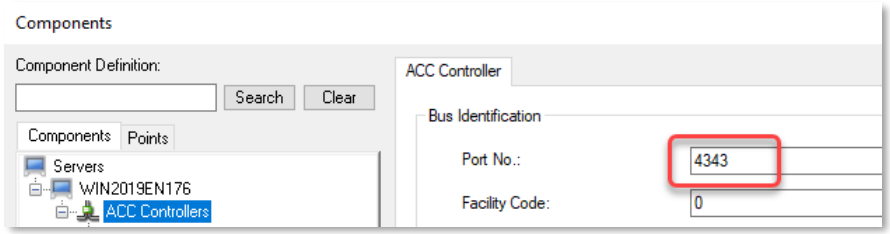
	TARGETTES UPGRADE VERSION											
Current Version	**SiPass integrated Version**	**MP 2.40 2.50**	**MP 2.60**	**MP 2.65**	**MP 2.70**	**MP 2.75**	**MP 2.76**	**MP 2.80**	**MP 2.85**	**MP 2.90**	**MP 2.95**	**MP x.xx**
	MP 2.35	✓	X	X	X	X	X	X	X	X	X	X
	MP 2.40	✓	X	X	X	X	X	X	X	X	X	X
	MP 2.50		✓	✓	X	X	X	X	X	X	X	X
	MP 2.60			✓	✓	✓	X	X	X	X	X	X
	MP 2.65 SP4				✓	✓	✓	✓	✓	✓	✓	✓
	MP 2.70					✓	✓	✓	✓	✓	✓	✓
	MP 2.75						✓	✓	✓	✓	✓	✓
	MP 2.76							✓	✓	✓	✓	✓
	MP 2.80								✓	✓	✓	✓
	MP 2.85									✓	✓	✓
	MP 2.90										✓	✓

The Support Center will also provide a "Database Upgrade Service", this will make sense espessially if older systems need to be upgraded.
SAP purchase order P54511-P200-A10 "SiPass Uprade Service".

15.1 SiPass upgrade step by step:

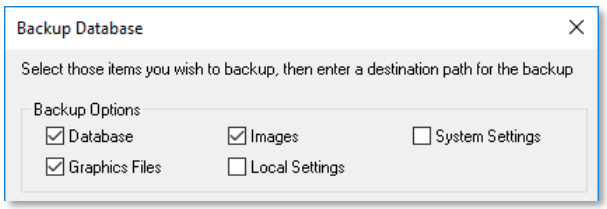
A new SiPass version will need a new license.
Since SiPass 2.80 a new software license needs to be ordered only via SAP without the well known software order form.
A CSID created during the SAP order or with help of the LMS Cocpit (https://lmscockpit.bt.siemens.com).
Based on a Excel sheet a migration tool are created, the tool helps to create a bill of material.
After a manual verification throug HQ logistic the LMS tool send an email to the requester and the SiPass LMS license can be activated via LMU.
If migration licenses are needed because a direct upgrade is not possible are they send in a separate email to the requester.

1. Disconnect the ACCs by changing the ACC Port => all ACCs offline

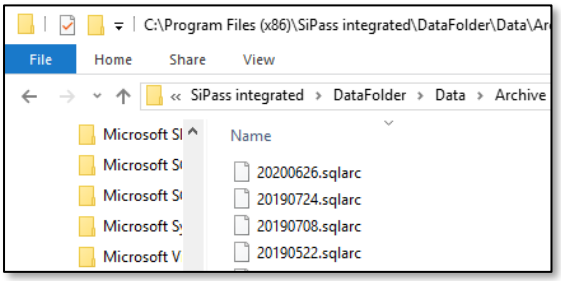


This is needed to stop the ACC sending events.
The new events, which will be not at the backup, will be stored at the ACC.

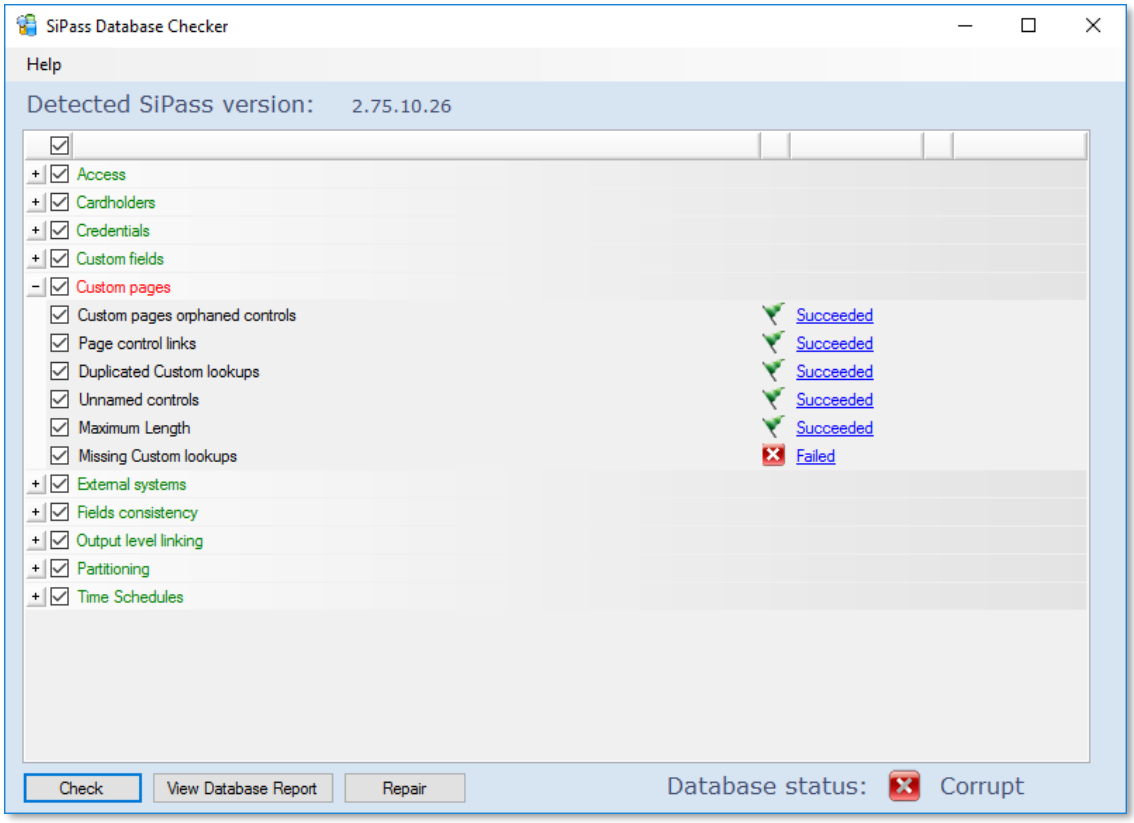
2. Backup the database using the SiPass integrated backup function



This backup will be used later to restore again all the data
Use always 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



3. Run the DB check tool and if needed repair the DB, the DB check tool can be found inside the Tools folder at each SiPass DVD image.
   If the check sowing errors use the Repair option.

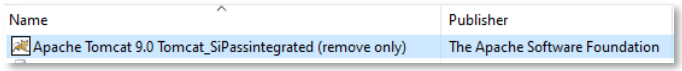


   After repair take a new DB backup (consider to use a new empty folder)
   If the error can't relaired contact the support desk, provide DB check file an if possible the DB backup itself.

4. Close all running applications

5. Uninstall the current installed SiPass version, start the SiPass installation (right klick => run as Administrator) of the installed version and select "remove".

6. If 2.76 is used: Unisstall "*Apache Tomcat 9.0 Tomcat_SiPassintegrated*"



   <u>If this application is not uninstalled the Web Client Activity Feed and Area Monitoring is not working.</u>

7. Check if the OS, the installed SQL version and Service pack is compatible with the SiPass version.

8. Setup LMU and activate the SiPass license

9. Setup the new SiPass version (run as Administrator)

10. Check if a patch is available for the installed version and apply it

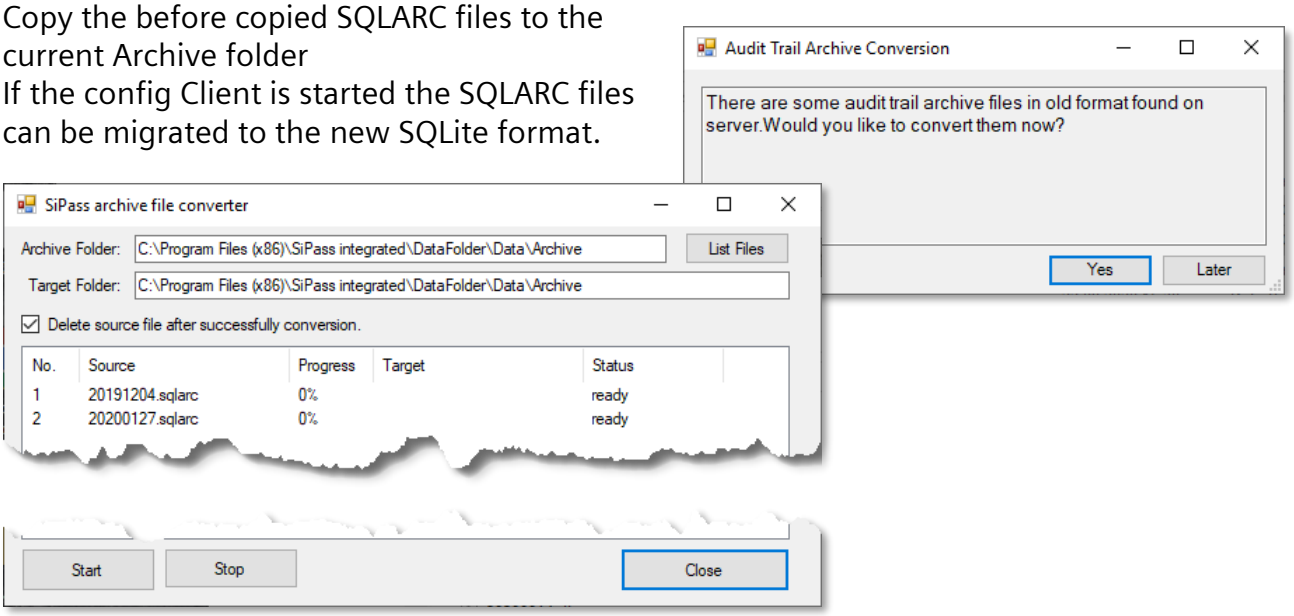
11. Start SiPass integrated Configuration client and restore the previous made SiPass database backup

12. Restart PC after restore DB

13. Login and check the restored DB together with the customer

14. Backup the database with the new SiPass version

15. Copy the before copied SQLARC files to the current Archive folder
    If the config Client is started the SQLARC files can be migrated to the new SQLite format.



    Recommended is to start with the SQLARC file of the last 3 days.
    After this step it is known how long it will take to migrate 3 days or archive files and if the migration task can be done inside the available time frame for all the other SQLARC files.
    Any time the Config Client is started the check for existing SQLARC files is performed and offers the migration.
    Reporting only working after the migration to the new format.

16. 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 iamge.

Note:
Since 2.80 the option “System Settings” and “Local Settings” are not longer used.
Printer and enrolment reader settings have to be re-set manually after the restore.

16. SiPass integrated Web Client

The SiPass Web Client is always part of any SiPass setup. It is not possible to setup SiPass without this option.

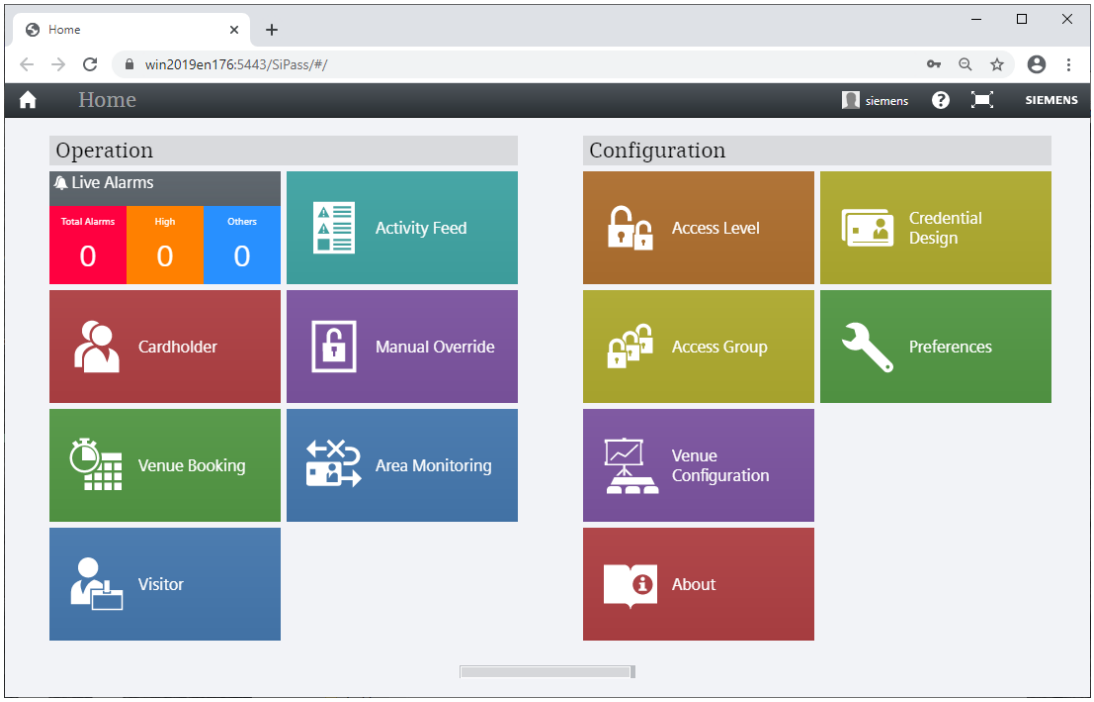
The Web Client offering following options:

- ✓ Cardholders
- ✓ Visitor (licensed option)
- ✓ Access Levels
- ✓ Access Group
- ✓ Alarms
- ✓ Venues and Bookings
- ✓ Manual Override
- ✓ Activity feed (since 2.95 not available)
- ✓ Area Monitoring (since 2.95 not available)

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

Web Client login page

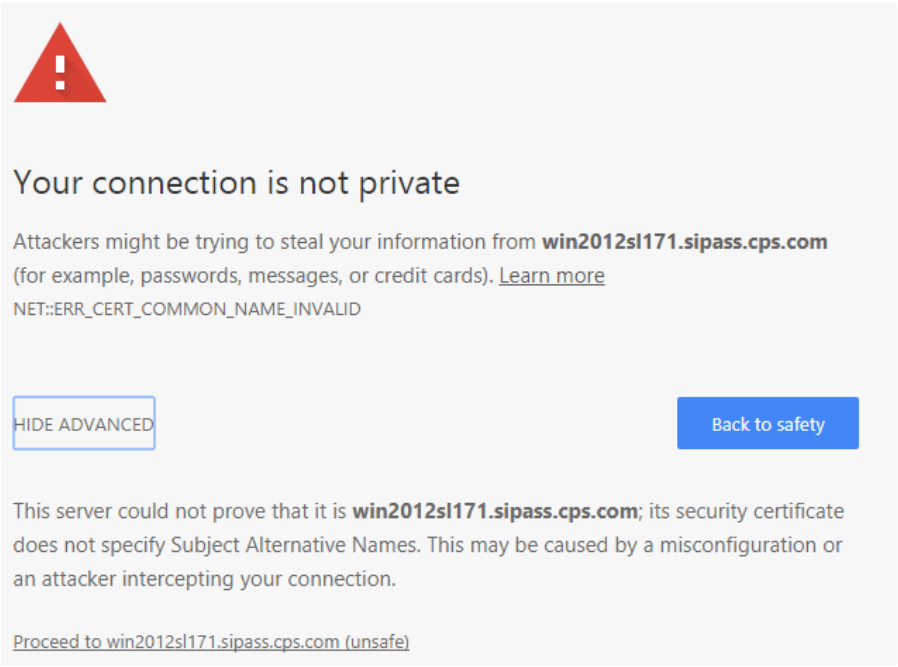
The SiPass integrated logins are also valid for the Web Client login.



SiPass Web Client with Chrome browser (recommended browser):

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

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



SiPass Web Client with Firefox browser:

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

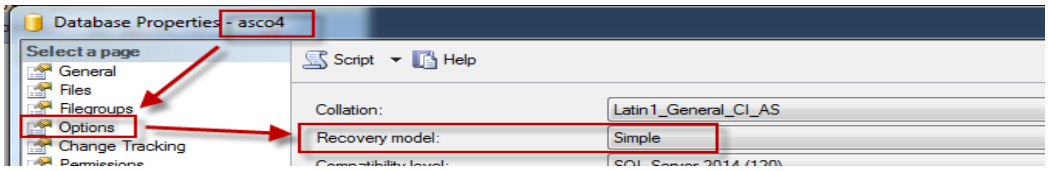
The above step is only required the first time!

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

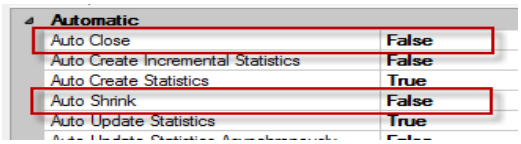
17. Recommended SQL database settings

To apply the recomended settings the SQL Management Studio needed 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 Management Studio v18.5.1.
Perform the below described steps only of you familiar with the SQL Management tool.

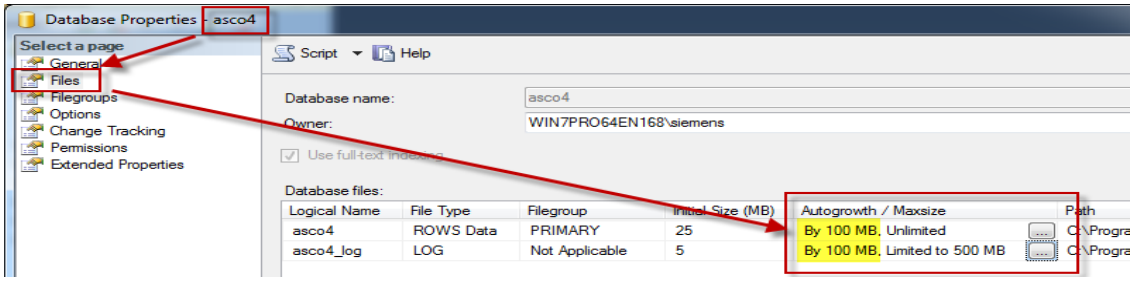
1. By default the recovery mode is FULL, recommended is the mode “SIMPLE



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

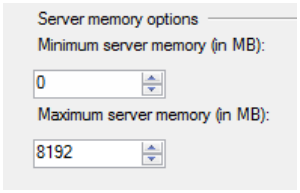


This prevent the DB to be fragmented if always 1 MB added to the DB.

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.