SiPass integrated MP2.75

Good to know V1.3

www.siemens.com/buildingtechnologies

SiPass integrated MP2.75

Good to know

V1.3

Table of contents

Glossary

This glossary will give you a quick overview over the used terms and abbreviations.

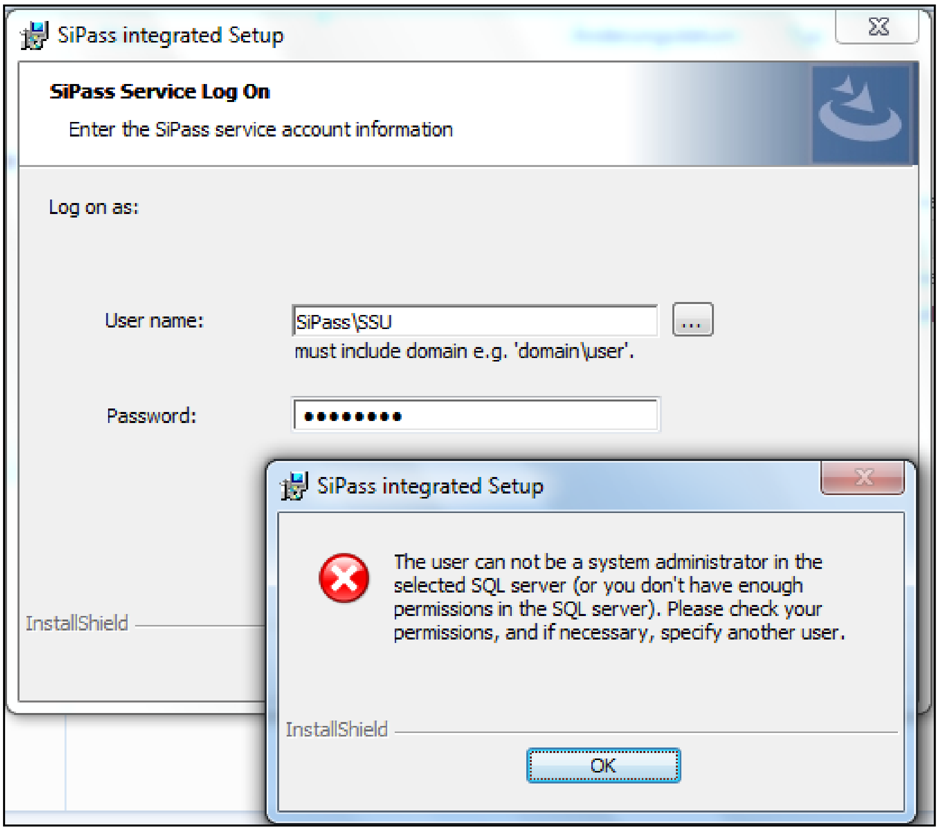
FW	Firewall
Inbound FW rule	A firewall setting for inbound traffic as seen from the perspective of the affected system.
WCF	Windows Communication Foundation (WCF) is a framework for building service-oriented applications. Using WCF, you can send data as asynchronous messages from one service endpoint to another.
Host PC	The PC where the SiPass service is installed and running
Remote Client	SiPass integrated Client connected via network to the SiPass host (SiPass service)

Change history:

Version	Content
1.3	

1. SiPass Service Log On: User is not accepted

During the installation process you will be asked to enter user credentials used to start the SiPass Service. In some circumstances you might be confronted with the following error message.



SiPass integrated Setup

SiPass Service Log On

Enter the SiPass service account information

Log on as:

User name: SiPass\SSU

must include domain e.g. 'domain\user'.

Password: ••••••••

SiPass integrated Setup

The user can not be a system administrator in the selected SQL server (or you don't have enough permissions in the SQL server). Please check your permissions, and if necessary, specify another user.

One possible reason for this behavior is that the Windows User you are using for the SiPass installation is not a SQL sysadmin.

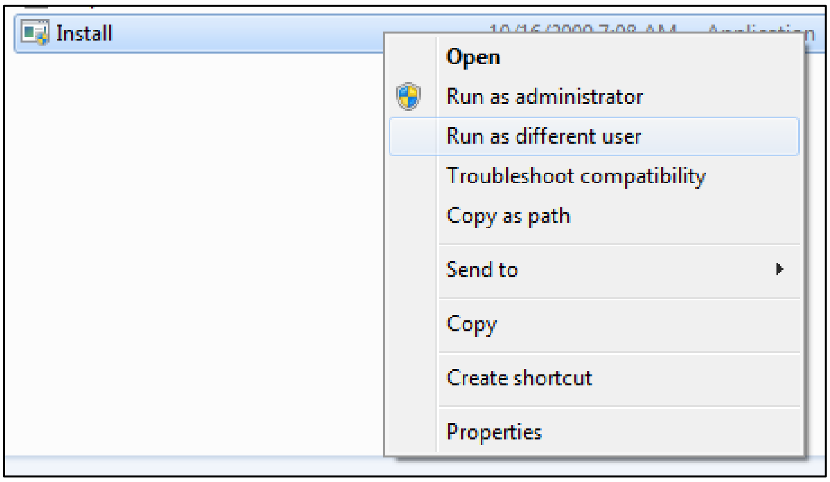
Another possible reason is that the SiPass Service User is a SQL sysadmin.

Third known reason is a not proper created Windows account assigned to start the SiPass service.

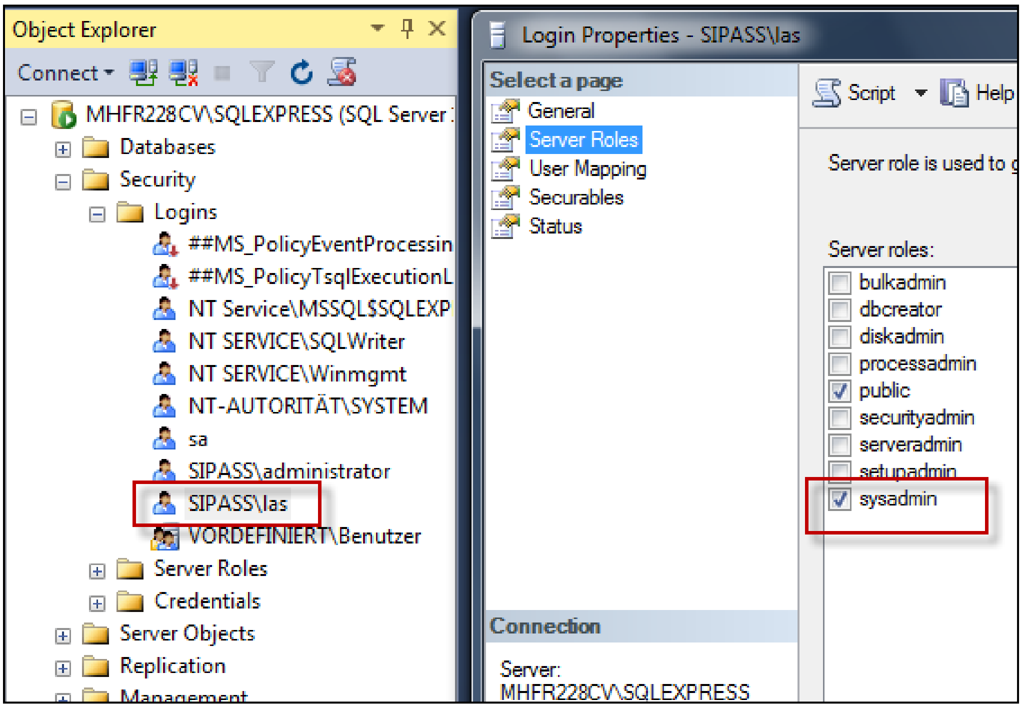
The solutions to the above problem can be found on the following pages.

1.1. Windows User (used for setup SiPass) is not a SQL sysadmin

First option:
Start the SiPass Setup with a Windows User which is SQL sysadmin. For this purpose hold the [SHIFT]-Key and right click on the application file. Please select Run as different user in the appearing context menu.



Second Option:
Open the “Microsoft SQL Server Management Studio”, navigate to the Windows User account which you want to modify (setup SiPass):
Computer name -> Security -> Logins -> ‘User account’
Assign the Server Role of a ‘sysadmin’ to the User account.



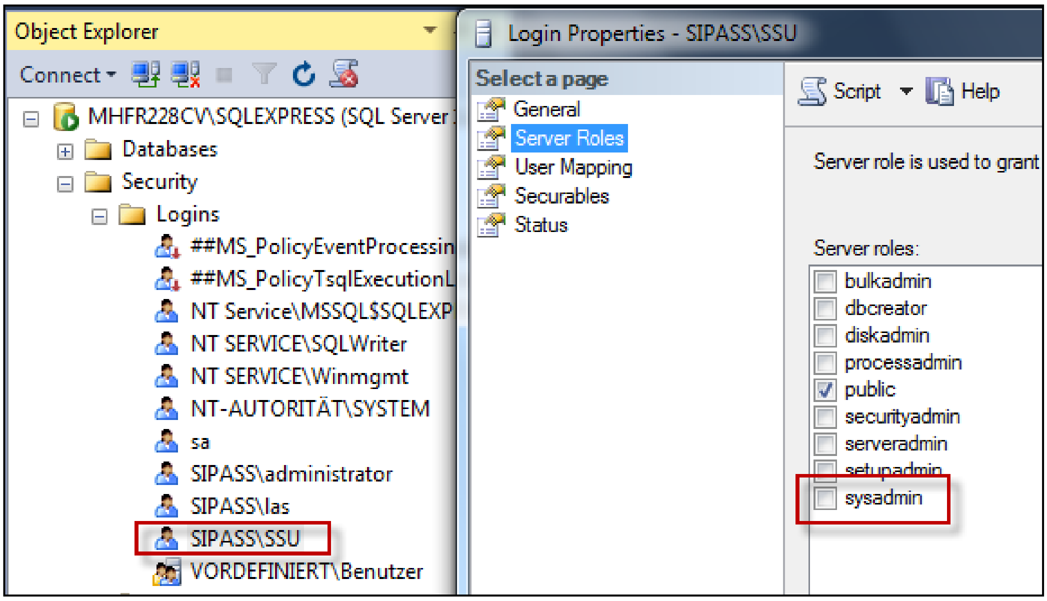
Server role is used to g

Server roles:
☐ bulkadmin
☐ dbcreator
☐ diskadmin
☐ processadmin
☑ public
☐ securityadmin
☐ serveradmin
☐ setupadmin
☑ sysadmin

Server:
MHFR228CV\SQLEXPRESS

1.2. SiPass Service User is SQL sysadmin

Open the “Microsoft SQL Server Management Studio”, navigate to the Windows “SiPass Service User” account:
Computer name -> Security -> Logins -> SiPass Service User account (SSU).
Withdraw the Server Role of a sysadmin from the SiPass Service User account.



- MHFR228CV\SQLEXPRESS (SQL Server
  - Databases
  - Security
    - Logins
      - ##MS_PolicyEventProcessin
      - ##MS_PolicyTsqlExecutionL
      - NT Service\MSSQL$SQLEXP
      - NT SERVICE\SQLWriter
      - NT SERVICE\Winmgmt
      - NT-AUTORITÄT\SYSTEM
      - sa
      - SIPASS\administrator
      - SIPASS\las
      - SIPASS\SSU
      - VORDEFINIERT\Benutzer

General
Server Roles
User Mapping
Securables
Status

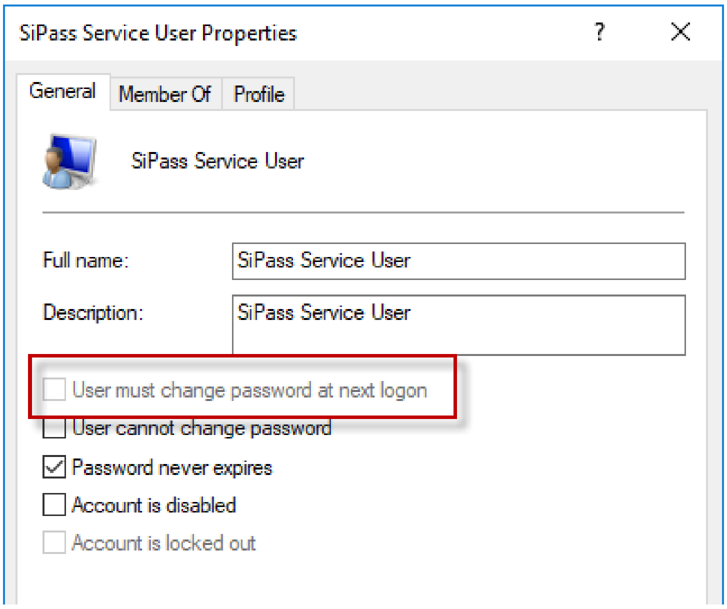
Server role is used to grant

Server roles:

□ bulkadmin
□ dbcreator
□ diskadmin
□ processadmin
☑ public
□ securityadmin
□ serveradmin
□ setupadmin
□ sysadmin

1.3. Windows user not correct created

The SiPass Service User Windows account was created but the option "User must change password ant next logon” is still set.



SiPass Service User

Full name: SiPass Service User

Description: SiPass Service User

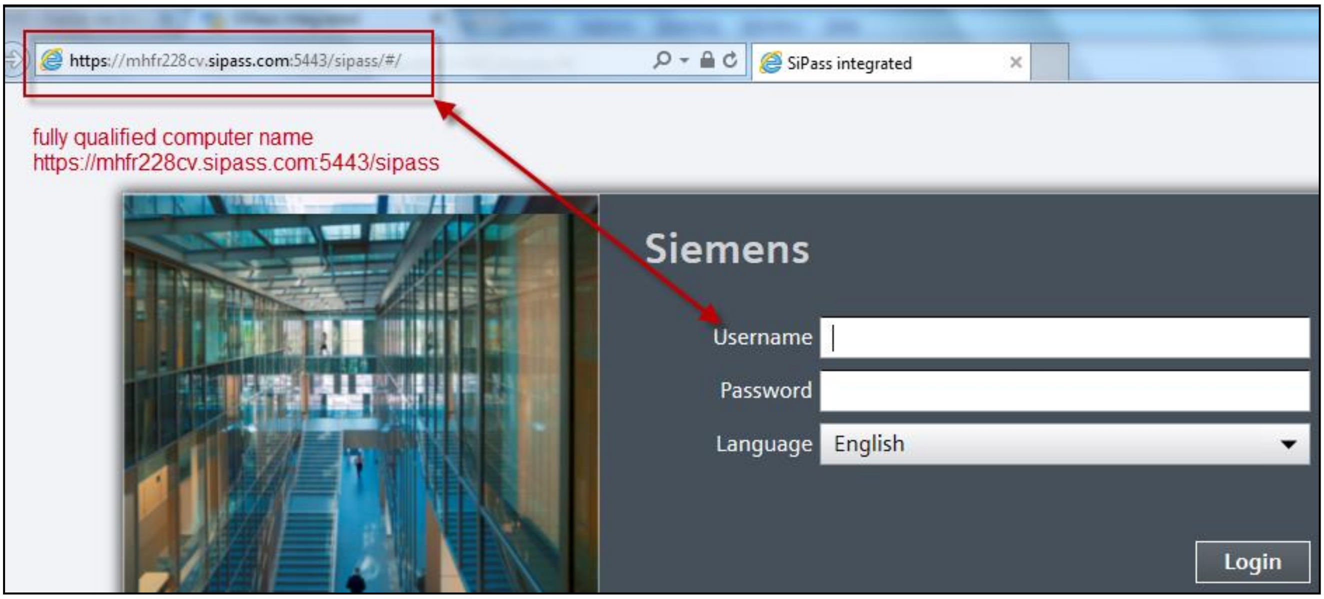
□ User must change password at next logon
□ User cannot change password
☑ Password never expires
□ Account is disabled
□ Account is locked out

Enter “lusrmgr.msc” to the Run dialogue (Windows key + R), open Users, select the “SiPass Service User” Windows User and remove this option.

Now Windows will accept the assigned User, no need to cancel the setup of SiPass itself.

2. SiPass Web Client within a domain environment

If you are using the SiPass Web Client within a domain environment it is necessary to use the fully-qualified host name (FQHN).

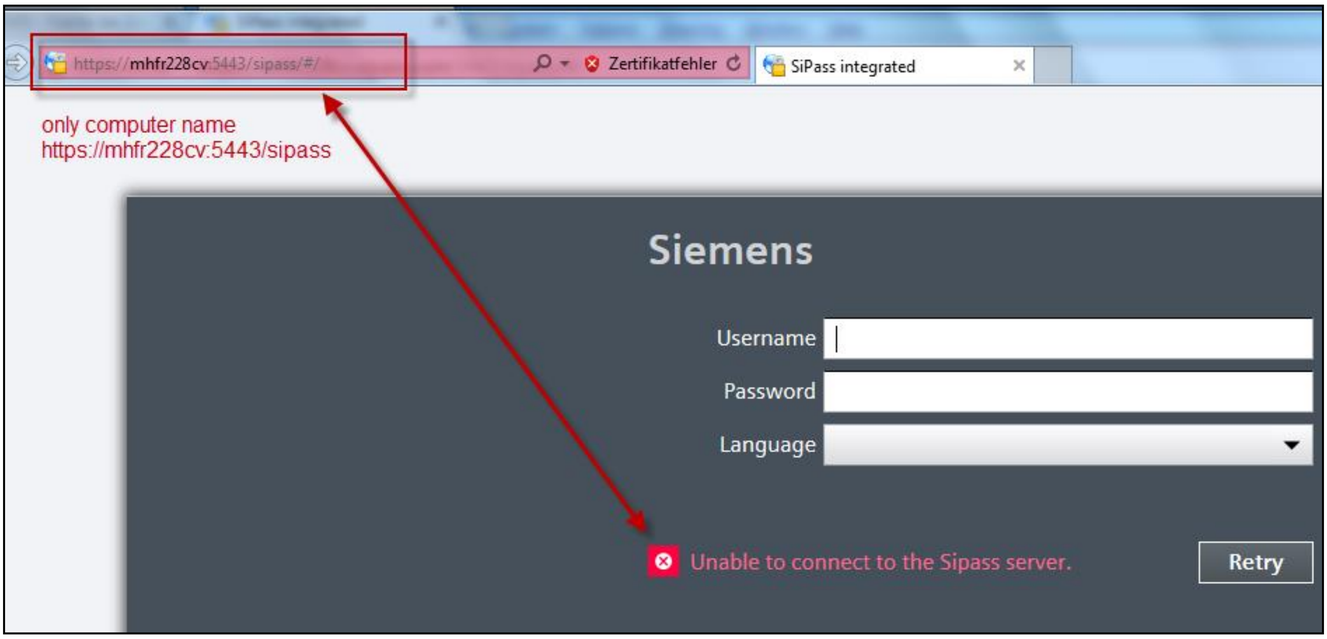


https://mhfr228cv.sipass.com:5443/sipass/#/

fully qualified computer name
https://mhfr228cv.sipass.com:5443/sipass

As shown in the picture above, the FQHN is e.g. “*mhfr228cv.sipass.com*”

If you would use just the host name “*mhfr228cv*” without the domain, the error message “Unable to connect to the SiPass server” will appear. See picture below.



https://mhfr228cv:5443/sipass/#/

Zertifikatfehler

only computer name
https://mhfr228cv:5443/sipass

Unable to connect to the Sipass server.

3. Behavior of the Remote Client with different firewall settings

In this chapter the possible behaviors and error messages which can appear during the login process from a remote client computer are shown.

The testing was done with different firewall settings (Windows OS) for the SiPass Server computer firewall and for the Remote Client computer firewall. The resulting behavior of the Remote Client was tested within a domain environment. Windows 7 was used as Server and Client operating system.

3.1 Test connection

The easiest way to test the connection between the SiPass Server and the Remote Client computer is to turn both firewalls off. If both SiPass Operation Client and SiPass Configuration Client are working on the Remote Client computer, you can assume that the installation of the Remote Client computer was successful and that the general connection between both computers is established correctly.

Attention: Only use this procedure, if you are sure that it won't affect your overall system security. If you are in doubt, please ask your system administrator for permission. For security reasons we do not recommend the described procedure.

Alternatively you can ping each computer from the other to test the connection. Therefore you can use the Windows command line. Use the following command:
ping <IP address of other computer> (e.g. ping 192.168.1.125).

Attention: This procedure only works if the corresponding firewall settings for echo request and echo response are being activated!

If the other computer is responding, you can assume that connection between both computers is established correctly.

3.1. Firewall settings

With the following correct firewall settings the connections within your SiPass system work properly. Both the Remote Operation Client and the Remote Configuration Client will work as expected.

SiPass Server firewall settings	Remote Client firewall settings
Setup inbound firewall rules which allow the inbound connections for ***AscoServer.exe*** and for the default SiPass TCP ports: ***8741, 8742, 8743, 8744*, 8745*, 4200, 135, 445***	Setup inbound firewall rules which allow the inbound connections the default SiPass TCP ports: ***8741, 8742, 8743, 4200, 135, 445***

3.2. Server/Client port information

The table below lists the Server ports that are used to communicate with clients.

Port Number	**Role**
Ports connecting to Configuration Client	
135	RPC End Point Mapper, Responds to Client Requests for Dynamic endpoints
445	SMB (Server Message block) port - used when SiPass RPC communication is through named pipes
4200	SiPass integrated .Net Remoting Services
Ports connecting to Operation Client	
4200	SiPass integrated .Net Remoting Services
8740, 8741	Connection to SiPass Web Services
8742	Incoming connections from server to port
Port connecting to Web Client	
8743	Connection to Web UI API Web Services
Port connecting to MS API	
8744*	Connection to Management Station API Web Services
Port connecting to HR API	
8745*	Connection to HR API Web Services

Note: RPC dynamically allocated ports can be changed in Windows from default range.

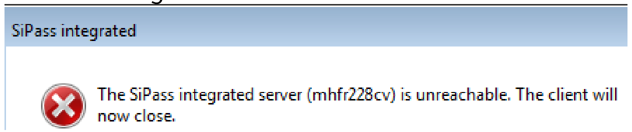
The port numbers are categorised according to the type of client connecting to them. For example, if there is no Operation Client being used, then port 8741 will not be opened up on the firewall for the server.

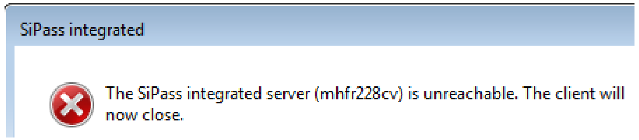
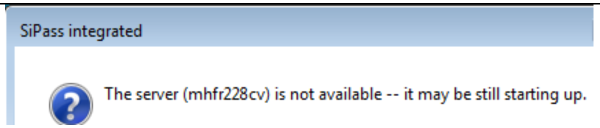
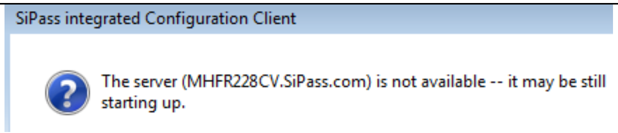
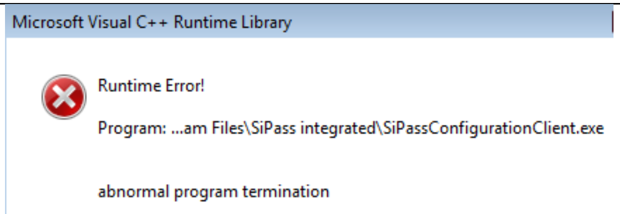
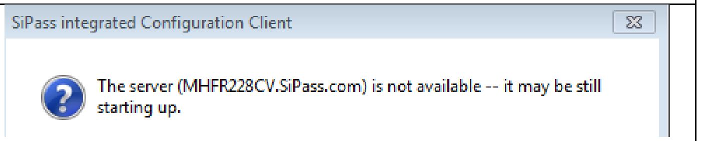
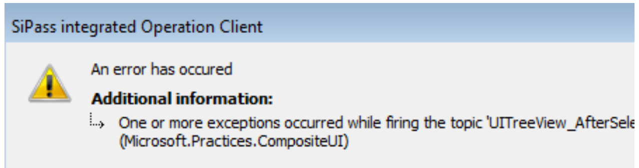
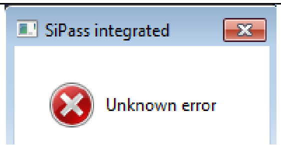
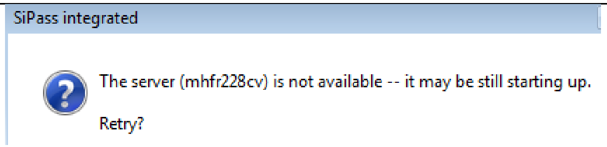
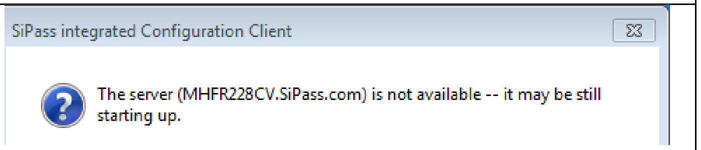
*) only need to consider if HR or MS Web services used

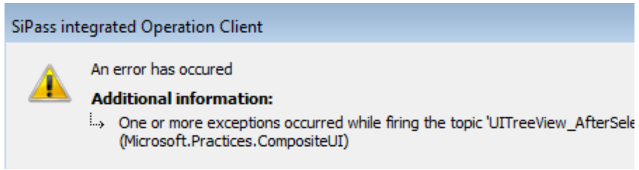
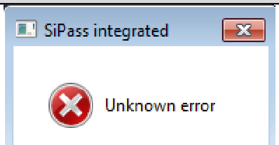
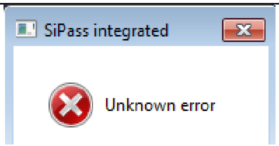
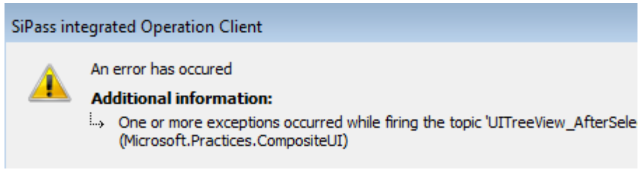
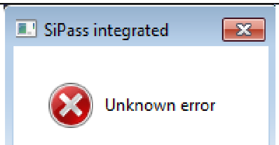
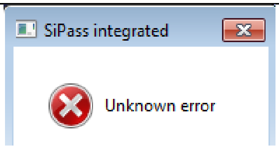
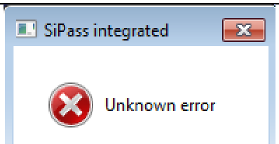
3.3. Firewall setting for ACC communication

No.	Server Firewall	ACC communication status
1	Off	Online, communication
2	Active, inbound FW rule for TCP 4343 (Default ACC bus port)	Online, communication
3	Active, no inbound FW rule	Offline, no communication

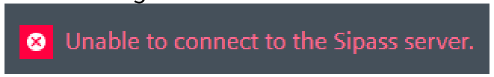
3.4. Different firewall settings and the resulting behavior on the Remote Client

No.	Server Firewall	Remote Client Firewall	Behavior Remote Operation Client	Behavior Remote Configuration Client
1	Off	Off	Working	Working
2	Active, inbound FW rule for **AscoServer.exe** and TCP Ports: **8741, 8742, 4200, 135, 445**	Inbound FW rule for TCP Ports: **8741, 8742, 4200, 135, 445**	Working	Working
3	Active, Inbound FW rule for **AscoServer.exe** and **8741, 8742**	Inbound FW rule for: **8741, 8742**	Working	Working
4	Active, inbound FW rule for **AscoServer.exe** and **8741, 8742**	Active, no Inbound FW rule	Slow start up, no Audit Trail, Cardholder search is not working. After some minutes the Client is disconnecting from the server.  The SiPass integrated server (mhfr228cv) is unreachable. The client will now close.	It is working, but slow. A bad overall operation performance.

No.	Server Firewall	Remote Client Firewall	Behavior Remote Operation Client	Behavior Remote Configuration Client
5	Off	Active, no Inbound FW rule	Slow start up, no Audit Trail, Cardholder search is not working. After some minutes the Client is disconnecting from the server.  SiPass integrated The SiPass integrated server (mhfr228cv) is unreachable. The client will now close.	It is working, but slow. A bad overall operation performance.
6	Active, no Inbound FW rule	Active, no Inbound FW rule	 SiPass integrated The server (mhfr228cv) is not available -- it may be still starting up.	 SiPass integrated Configuration Client The server (MHFR228CV.SiPass.com) is not available -- it may be still starting up.
7	Active, no Inbound FW rule	Off	 Microsoft Visual C++ Runtime Library Runtime Error! Program: ...am Files\SiPass integrated\SiPassConfigurationClient.exe abnormal program termination	 SiPass integrated Configuration Client The server (MHFR228CV.SiPass.com) is not available -- it may be still starting up.
8	Active, Inbound FW rule for: **8741, 8742**	Off	Starting with AT, Cardholder/Visitor generates following error. The other functions are working.  SiPass integrated Operation Client An error has occured **Additional information:** One or more exceptions occurred while firing the topic 'UITreeView_AfterSele (Microsoft.Practices.CompositeUI)	 SiPass integrated Unknown error
9	Off, no Inbound FW rule	Active, Inbound FW rule for: **8741, 8742**	 SiPass integrated The server (mhfr228cv) is not available -- it may be still starting up. Retry?	 SiPass integrated Configuration Client The server (MHFR228CV.SiPass.com) is not available -- it may be still starting up.

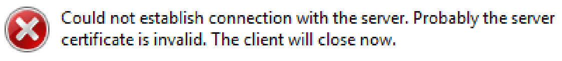
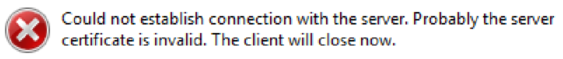
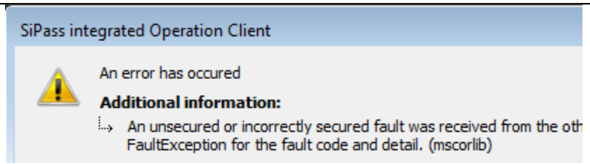
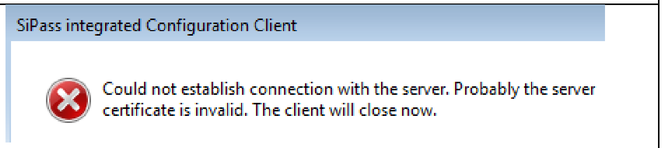
No.	Server Firewall	Remote Client Firewall	Behavior Remote Operation Client	Behavior Remote Configuration Client
10	Active, Inbound FW rule for: **8741, 8742**	Active, Inbound FW rule for: **8741, 8742**	Starting with AT, Cardholder/Visitor generates following error. The other functions are working.  SiPass integrated Operation Client An error has occured **Additional information:** One or more exceptions occurred while firing the topic 'UITreeView_AfterSele (Microsoft.Practices.CompositeUI)	 SiPass integrated Unknown error
11	Active, Inbound FW rule for: **4200, 8741, 8742**	Active, Inbound FW rule for: **4200, 8741, 8742**	Working	 SiPass integrated Unknown error
12	Active, Inbound FW rule for: **8741, 8742**	Active, Inbound FW rule for: **4200, 8741, 8742**	Starting with AT, Cardholder/Visitor generates following error. The other functions are working.  SiPass integrated Operation Client An error has occured **Additional information:** One or more exceptions occurred while firing the topic 'UITreeView_AfterSele (Microsoft.Practices.CompositeUI)	 SiPass integrated Unknown error
13	Active, Inbound FW rule for: **4200, 8741, 8742**	Active, Inbound FW rule for: **8741, 8742**	Working	 SiPass integrated Unknown error
14	Active, Inbound FW rule for: **135, 4200, 8741, 8742**	Active, Inbound FW rule for: **135, 4200, 8741, 8742**	Working	 SiPass integrated Unknown error

4. Behavior of the Web Client with firewall settings

No.	Server Firewall	Remote Client Firewall	Behavior Remote Operation Client
1	Off	Off	Chrome: Working IE11: Working Firefox: Working
2	Inbound FW rule for Port 5443 +8743	Inbound FW rule for Port 5443 +8743	Chrome: Working. IE11: Working Firefox: Working
3	Inbound FW rule for AscoServer.exe and 8741, 8742	Active, no Inbound FW rule	Not Working
4	Inbound FW rule for Port 5443	Active, no Inbound FW rule	Not Working  Unable to connect to the Sipass server.

5. Certificate behavior

No.	SiPass Server	Remote Client	Behavior Remote Operation Client	Behavior Remote Configuration Client
1	Correct created Client certificate with full qualified name of the Remote PC e.g. Win7EntDE-175.SiPass.com	Installed with the full qualified host name of the Server PC and correct imported child certificate	Working	Working
2		Installed with Server PC name (e.g. Win7EntDE-172) Correctly imported Server child certificate		
3	Child certificate was created with the Remote PC name (e.g. Win7EntDE-175)	Installed with the full qualified host name of the Server PC and correct imported child certificate	Working	Working
4		Installed with the Server PC name (e.g. Win7EntDE-172 Correctly imported Server child certificate		

No.	SiPass Server	Remote Client	Behavior Remote Operation Client	Behavior Remote Configuration Client
5	Certificate changed e.g. expiration	Old certificate still in use	 Could not establish connection with the server. Probably the server certificate is invalid. The client will close now.	 Could not establish connection with the server. Probably the server certificate is invalid. The client will close now.
6	The time difference between the Server and the Remote Client computer is more than 5 minutes		 SiPass integrated Operation Client An error has occured **Additional information:** An unsecured or incorrectly secured fault was received from the oth FaultException for the fault code and detail. (mscorlib)	 SiPass integrated Configuration Client Could not establish connection with the server. Probably the server certificate is invalid. The client will close now.

6. SiPass Card technologies

This section outlines the card technologies supported by SiPass.
Progression of card details through the system:

1. Reader reads a card and passes the raw card data to a RIM e.g. DRI. This data will be in the form of a bit stream, obtained via one of a variety of physical interfaces e.g. Wiegand, Clock/Data, and serial interfaces like OSDP, CerPass (RS485) Reader.
2. The RIM interprets this bit stream to extract a Card number, a Facility, and a Revision according to a Card Technology configuration (also called a Reader Technology in SiPass).
3. The RIM will report the card details to the ACC.
4. The ACC will accept the card details and may change the Card Technology e.g. all Siemens readers will report cards into SiPass as "Siemens Readers Clkdata/RS485" Technology, irrespective of the actual device configuration e.g. Siemens RS485 UID.
5. This translated Card Technology is what should be configured inside SiPass and called Base or Tenant credential and loaded via initialize to the ACCs to be granted access to a door. With help of a Telnet session and the command "db" the support reader technology is listed, see below example

```
Username: SIEMENS
Password: ********
User SIEMENS logged in
db
Database State: Normal Operation
Primary Database COMPLETE.
Backup Mode: ONBOARD FLASH.
MaxSize [32000000] AvailSize [31982346].
Total Cards[5626] Pins[0] Collisions[0]
Prox26Bit[8] Fclt 0 CredProfId 2 PinLen 0: Used[426]
SiemensRdr[26] Fclt 0 CredProfId 1 PinLen 6: Used[5200]
Total Acccess Levels = 15
Total Access Groups = 8
Done
```

The ACC is accepting Siemens "Siemens Readers ClkData/RS485" and "HID Proximity 26 Bit"

The below table contain the important card technologies SiPass is supporting

Format Number	Reader Technology Name	Interface	Version Introduced	Comments	Base Card Technology Name	Facility Digits	Card Digits
8	HID Proximity 26 Bit	Wiegand			HID Proximity 26 Bit	3 (8bit)	5 (16bit)
9	HID Proximity 36 Bit Asco	Wiegand			HID Proximity 36 Bit Asco	6 (18bit)	5 (16bit)
10	HID Proximity Corporate 1000 35/48 Bit	Wiegand			HID Proximity Corporate 1000	4 (12bit)	7 (20bit)
11	HID Proximity SIEMENS Encrypted 52 Bit	Wiegand			HID Proximity SIEMENS 52bit	7 (20bit)	7 (20bit)
12	HID Proximity Siemens STG	Wiegand			HID Proximity Siemens STG	0	9 (29bit)
15	Mifare CSN32	Wiegand			Mifare CSN32	0	10 (32bit)
16	Mifare CSN40	Wiegand		8 bit checksum added to 32 bit card	Mifare CSN40	0	10 (32bit)
19	All HID Proximity*	Wiegand		Reports as the specific card technology – i.e. whichever format matched is the Card Technology that is reported.	Variable	Variable	Variable
24	Siemens Clk/data	Clock/Data			Siemens Readers ClkData/RS485	0	16

*The All HID reader technology currently includes the following card formats:

- Custom Wiegand (If Custom Wiegand format is configured for the specific RIM device)
- 26-Bit Wiegand
- 36-Bit ASCO
- 35-bit HID Corporate 1000
- 52-bit Siemens Encrypted
- 31-bit Siemens STG

Format Number	Reader Technology Name	Interface	Version Introduced	Comments	Base Card Technology Name	Facility Digits	Card Digits
26	Siemens RS485	CerPass (RS485)			Siemens Readers Clkdata/RS485	0	20 (64bit)
28	HID Proximity 26 Bit	Wiegand		HID Proximity 26 Bit. This is a licence option that simple accepts multiple HID 26 bit cards with difference facilities (up to 20 configured per reader)	26-bit Multi Facility HID	3 (8bit)	5 (16bit)
30	Siemens Mifare GID	CerPass (RS485)		ASCII format – 8 characters, with a 1 digit revision	Siemens Mifare GID	0	19
31	Mifare Facility	CerPass (RS485)			Mifare Facility	6	16
32	Proximity 36 Bit Code Card	Wiegand			HID Proximity 36 Bit Asco	5 (16bit)	5 (16bit)
37	Custom Card (Wiegand)	Wiegand			Custom Wiegand	10 (32bit)	20 (64bit)
40	Siemens Entro	Device Specific			Siemens Entro	0	16
43	Wiegand52BCD	Wiegand			Custom Wiegand	0	NA
45	Siemens RS485 UID	CerPass (RS485)	2.4		Siemens Readers ClkData/RS485	10	20 (64bit)
47	iClass OSDP	OSDP (RS485)	2.5		iClass OSDP	10 (32bit)	20 (64bit)
48	SALTO	Wiegand	2.5	Translates to base licence. Can accept 32bit CSN, also 56 and 58 bit CSN	any	0	17 (56bit)

Format Number	Reader Technology Name	Interface	Version Introduced	Comments	Base Card Technology Name	Facility Digits	Card Digits
49	Siemens Clk/Data UID	Clock/Data	2.5		Siemens Readers ClkData/RS485	0	20 (64bit)
50	Siemens Clk/Data Extended	Clock/Data	2.5		Siemens Readers ClkData/RS485	0	20 (64bit)
76	ARxxS-MF OSDP	OSDP (RS485)	2.5	Only AR MF (NGCR) Readers can be used.	Siemens Readers ClkData/RS485		64bit
77	ARxxS-MF OSDP Custom	OSDP (RS485)	2.6	Card data passed through the Custom Wiegand formatter	Custom Wiegand	32bit	64bit
78	ARxxS-MF OSDP Raw	OSDP (RS485)	2.6	Used to report the raw bit stream from an OSDP reader, so that a Custom Card format may be constructed in SiPass	NA		Up to 128bits
79	ARxxS-MF OSDP Mifare Facility	OSDP (RS485)	2.6	Legacy Mifare Facility card	Mifare Facility	6	16
82	ARxxS-MF OSDP Siemens Mifare GID	OSDP (RS485)	2.6	ASCII format – 8 characters, with a 1 digit revision	Siemens Mifare GID	0	19
83	ARxxS-MF OSDP All HID Prox	OSDP (RS485)	2.65	Card data passed though the ALL HID Prox formatter (see Format Number 19)	Variable	Variable	Variable
85	ARxxS-MF OSDP ASCII	OSDP (RS485)	2.65	Card is encoded as up to 20 ASCII digits, to be compatible with the MX reader.	Siemens Readers ClkData/RS485		64bit

Format Number	Reader Technology Name	Interface	Version Introduced	Comments	Base Card Technology Name	Facility Digits	Card Digits
86	ARxxS-MF OSDP BCD Packed	OSDP (RS485)	2.65	Card is encoded with BCD nibbles, 2 nibbles per byte, to be compatible with the MX reader	Siemens Readers ClkData/RS485		16
87	ARxxS-MF OSDP BCD Unpacked	OSDP (RS485)	2.65	Card is encoded with BCD nibbles, 1 nibble per byte, to be compatible with the MX reader.	Siemens Readers ClkData/RS485		16
88	Europlex 34 Bit	Wiegand	2.65	LSB is first, so parsed in reverse order.	Custom Wiegand	12	20
89	Remec 37 Bit	Wiegand	2.65	LSB is first, so parsed in reverse order.	Custom Wiegand	12	20
90	OSDP General	OSDP (RS485)	2.70 SP1	All OEM Readers report as Siemens Readers.	Siemens Readers ClkData/RS485		Up to 64 bits
254	Raw Card (Wiegand)	Wiegand		Used to report the raw bit stream from a Wiegand reader interface, so that a Custom Card format may be constructed in SiPass.	NA	0	128 bits