

SiPass integrated MP2.70 Good to know V1.2

MK FI

Intern © Siemens AG 2018

www.siemens.com/buildingtechnologies



SiPass integrated MP2.70

Good to know

V1.2

Table of contents

Glo	ssary	,,,,,,, _	3
1.	SiPa	ass Service Log On: User is not accepted	4
1	.1.	Windows User (used for setup SiPass) is not a SQL sysadmin	5
1	.2.	SiPass Service User is SQL sysadmin	6
1	.3.	Windows user not correct created	6
2.	SiPa	ass Web Client within a domain environment	7
3.	Beh	avior of the Remote Client with different firewall settings	8
3	5.1	Test connection	8
3	5.1.	Firewall settings	9
3	.2.	Server/Client port information	9
3	.3.	Firewall setting for ACC communication	10
3	5.4.	Different firewall settings and the resulting behavior on the Remote Client	10
4.	Beh	avior of the Web Client with firewall settings	13
5.	Cer	tificate behavior	14
6.	Con	itact page	15



Glossary

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

FW	Fire wall	
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)	



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.

BiPass 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:	••••••				
	BiPass integrated Setup				
InstallShield	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.				
	InstallShield				

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.

📑 Install	Onen	
	0	Run as administrator
		Run as different user
		Troubleshoot compatibility Copy as path
		Send to +
		Сору
		Create shortcut
		Properties

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.

Object Explorer 👻 무 🗙	🗧 Login Properties - SIPASS\la	s
Connect - 📲 🖳 🔳 🍸 🖒 📓	Select a page	Script 👻 📑 Help
 MHFR228CV\SQLEXPRESS (SQL Server: Databases Security Logins ##MS_PolicyEventProcessin ##MS_PolicyTsqlExecutionL NT Service\MSSQL\$SQLEXP NT SERVICE\SQLWriter NT SERVICE\SQLWriter NT SERVICE\Winmgmt NT-AUTORITÄT\SYSTEM sa SIPASS\administrator SIPASS\las VORDEFINIERT\Benutzer Server Roles 	General Server Roles User Mapping Securables Status	Server role is used to g
Geregentials Geregentials Geregentials	Connection	
⊞ ☐ Replication ☐ Management ☐	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.

Object Explorer 👻	Login Properties - SIPASS\SS	U
Connect	Select a page General Server Roles User Mapping Securables Status	Script Help Server role is used to grant Server roles: bulkadmin dbcreator diskadmin processadmin public securityadmin 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 Properties ? × General Member Of Profile					
General Member Of Profile SiPass 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	SiPass Service User Properties ? X				
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	General Member Of Profile				
Full name: SiPass Service User Description: SiPass Service User User must change password at next logon User cannot change password Password never expires	SiPass Service User				
Description: SiPass Service User User must change password at next logon User cannot change password Password never expires	Full name: SiPass Service User				
User must change password at next logon User cannot change password Password never expires	Description:	SiPass Service User			
Account is disabled					

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/#/	P → 🚔 C 🧭 SiPass integrated ×
fully qualified computer name https://mhfr228cv.sipass.com:5443/sipass	
	Siemens
	Username
	Password
	Language English 👻
	Login

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/#/	P → S Zertifikatfehler C SiPass integrated ×
only computer name https://mhfr228cv:5443/sipass	
	Siemens
	Username
	Password
	Language
	O 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. Fire wall settings

With the following correct fire wall 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 fire wall settings	Remote Client fire wall settings
Setup inbound fire wall rules which <u>allow</u> the inbound connections for <i>AscoServer.exe</i> and for the default SiPass TCP ports : <i>8741, 8742, 8743, 8744,</i> <i>4200, 135, 445</i>	Setup inbound firewall rules which <u>allow</u> the inbound connections the default SiPass TCP ports : <i>8741, 8742, 8743,</i> <i>8744 ,4200, 135, 445</i>

3.2. Server/Client port information

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

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				

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.



3.3. Fire wall 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 fire wall 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, 8743, 8744, 4200, 135, 445	Inbound FW rule for TCP Ports : 8741, 8742, 8743, 8744, 4200, 135, 445	Working	Working
3	Active, Inbound FW rule for AscoServer.exe and 8741, 8742, 8743, 8744	Inbound FW rule for: 8741, 8742, 8743, 8744	Working	Working
4	Active, inbound FW rule for AscoServer.exe and 8741, 8742, 8743, 8744	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.



No.	D. Server Remote Client		Behavior Remote	Behavior Remote	
	Firewall	Firewall	Operation Client	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 In- bound 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 In- bound FW rule	Off	Microsoft Visual C++ Runtime Library Runtime Error! Program:am Files\SiPass integrated\SiPassConfigurationClient.exe abnormal program termination	SiPass integrated Configuration Client	
8	Active, Inbound FW rule for: 8741, 8742, 8743, 8744	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	
9	Off, no Inbound FW rule	Active, Inbound FW rule for: 8741, 8742, 8743, 8744	SiPass integrated The server (mhfr228cv) is not available it may be still starting up. Retry?	SiPass integrated Configuration Client	



No.	Server	Remote Client	Behavior Remote	Behavior Remote
	Firewall	Firewall	Operation Client	Configuration Client
10	Active, Inbound FW rule for: 8741,8742, 8743,8744	Active, Inbound FW rule for: 8741,8742, 8743,8744	Starting with AT, Cardholder/Visitor generates fol- lowing error. The other functions are working. SiPass integrated Operation Client An error has occured Additional information: L-> 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, 8743, 8744	Active, Inbound FW rule for: 4200, 8741, 8742, 8743, 8744	Working	SiPass integrated Unknown error
12	Active, Inbound FW rule for: 8741,8742, 8743,8744	Active, Inbound FW rule for: 4200, 8741, 8742, 8743, 8744	Starting with AT, Cardholder/Visitor generates following error. The other functions are working. SiPass integrated Operation Client An error has occured Additional information: L-> One or more exceptions occurred while firing the topic 'UITreeView_AfterSele (Microsoft.Practices.CompositeUI)	SiPass integrated
13	Active, Inbound FW rule for: 4200,8741, 8742,8743, 8744	Active, Inbound FW rule for: 8741,8742, 8743,8744	Working	SiPass integrated Unknown error
14	Active, Inbound FW rule for: 135, 4200, 8741, 8742, 8743, 8744	Active, Inbound FW rule for: 135, 4200, 8741, 8742, 8743, 8744	Working	SiPass integrated Unknown error



4. Behavior of the Web Client with firewall settings

No.	Server	Remote Client	Behavior Remote	
	Firewall	Firewall	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	Active, no Inbound FW rule	Not Working	
	8741, 8742, 8743, 8744		_	
4	Inbound FW rule for Port 5443	Active, no Inbound FW rule	Not Working	
			A Upphie to connect to the Cinese conver	
			• Onable to connect to the Sipass server.	



5. Certificate behavior

No.	SiPass Server		Remote Client	Behavior Remote	Behavior Remote
				Operation Client	Configuration Client
1	Correct created Clien qualified name of the	t certificate with full e Remote PC SiPass com	Installed with the full qualified host name of the Server PC and correct imported child certificate	Working	Working
2			(e.g. Win7EntDE-172) Correctly imported Server child certificate	Working	Working
3			Installed with the full qualified host name of the Server PC and correct imported child certificate		
4	Child certificate was created with the Remote PC name (e.g. Win7EntDE-175)		Installed with the Server PC name (e.g. Win7EntDE-172 Correctly imported Server child certificate	Working	Working
No.	SiPass Server	Remote Client	Behavior Remote	Behavior Remote	
			Operation Client	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 certificate is invalid. The client w	with the server. Probably the server vill 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 connecti certificate is invalid. The clien	on with the server. Probably the server It will close now.



6. Contact page

BT CPS S&C MK&B CSFS MCH- Customer Support Center

Technical support for the SiPass integrated software and associated firmware is managed by the CPS FS Customer Support Center.

For support relating directly to the hardware you will need to contact Vanderbilt.

Hotline Europe: Phone: +49 89 9221 8000 Fax: +49 89 9221 6000 support.eu.i-bt@siemens.com fs.support.sbt@siemens.com

Hours of operation:

Monday - Thursday:	08:00 A.M 05:00 P.M. CET
Friday:	08:00 A.M 03.00 P.M. CET

Hotline South & North America: Phone: +1 800 877 7545 https://support.industry.siemens.com/my/WW/en/requests#createRequest

Hours of operation: Monday – Friday:

08:00 A.M. - 05:00 P.M. Central Time