

SiPass integrated MP2.70

Good to know

V1.2

SiPass integrated MP2.70

Good to know

V1.2

Table of contents

Glossary.....	3
1. SiPass 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. SiPass Web Client within a domain environment	7
3. Behavior of the Remote Client with different firewall settings.....	8
3.1 Test connection.....	8
3.1. Firewall settings.....	9
3.2. Server/Client port information	9
3.3. Firewall setting for ACC communication.....	10
3.4. Different firewall settings and the resulting behavior on the Remote Client	10
4. Behavior of the Web Client with firewall settings	13
5. Certificate behavior	14
6. Contact page.....	15

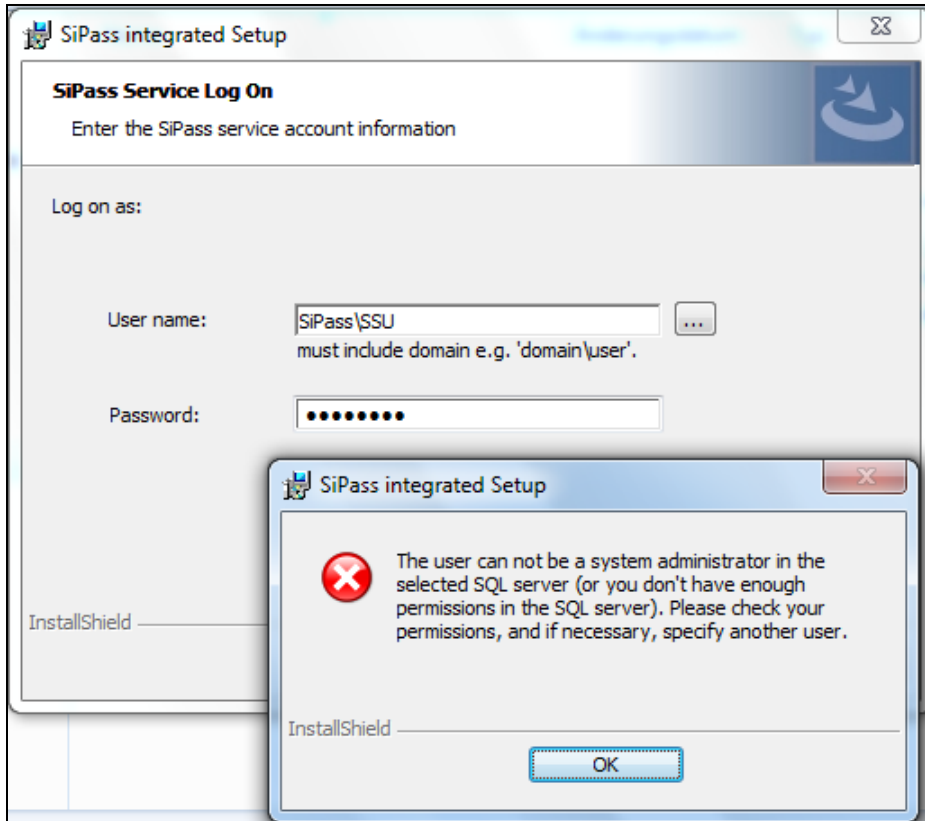
Glossary

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)

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.



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.

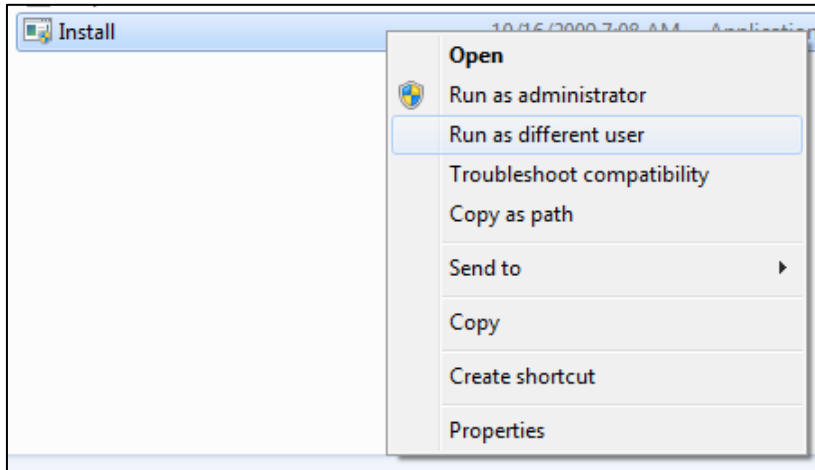
Third known reason is a not proper created Windows account assigned to start the SiPass service.

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.

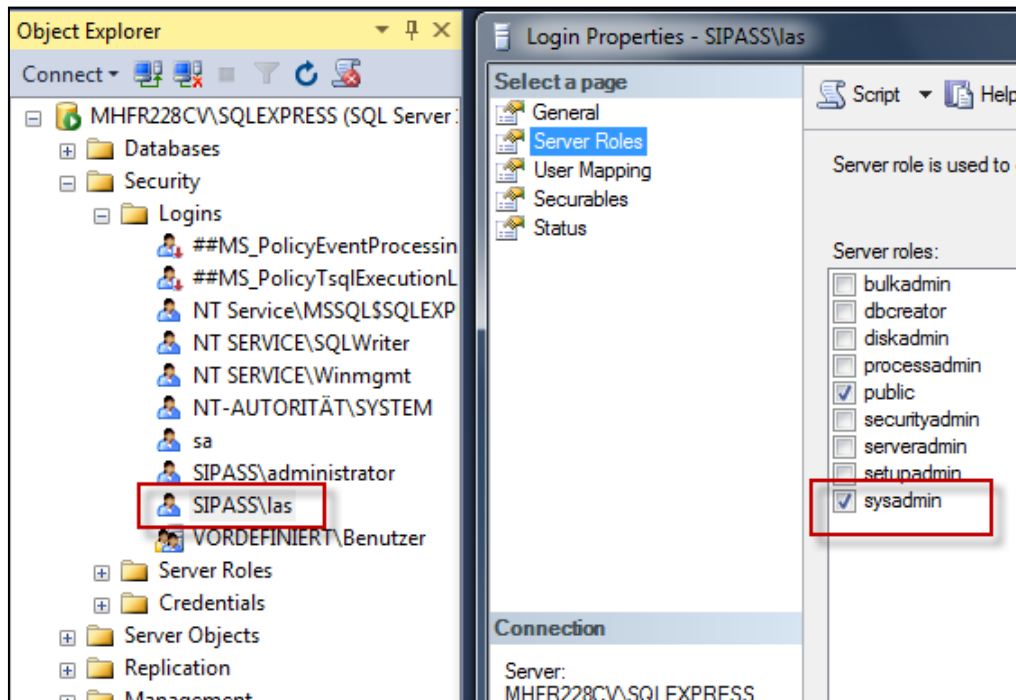


Second Option:

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.

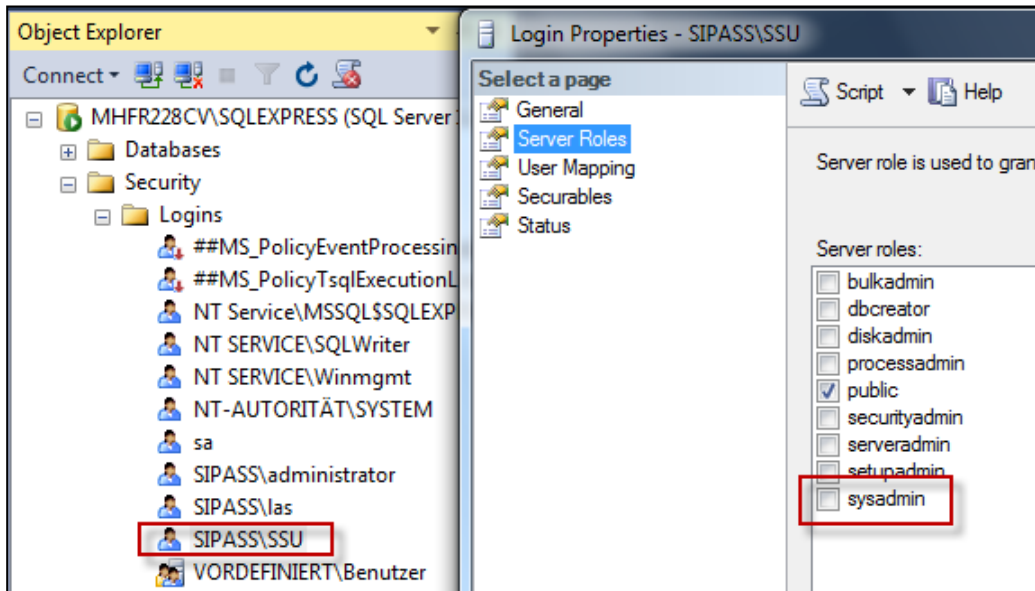


1.2. SiPass Service User is SQL sysadmin

Open the "Microsoft SQL Server Management Studio", navigate to the Windows "SiPass Service User" account:

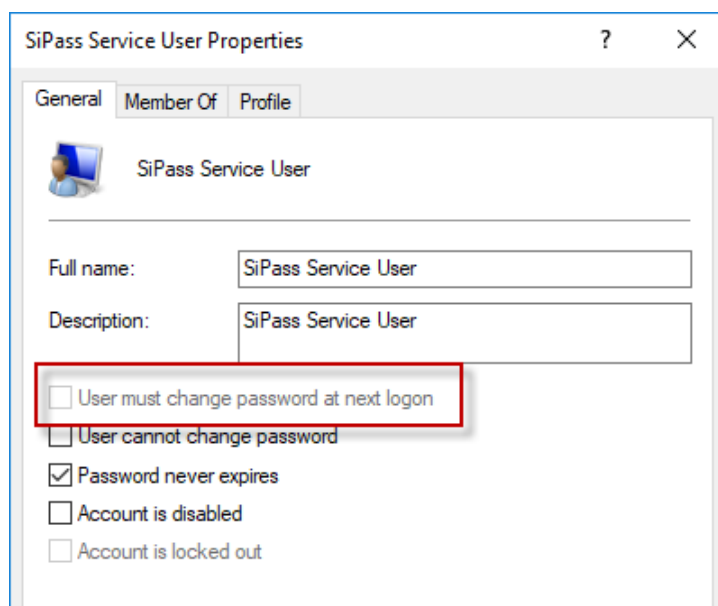
Computer name -> Security -> Logins -> SiPass Service User account (SSU).

Withdraw the Server Role of a sysadmin from the SiPass Service User account.



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.

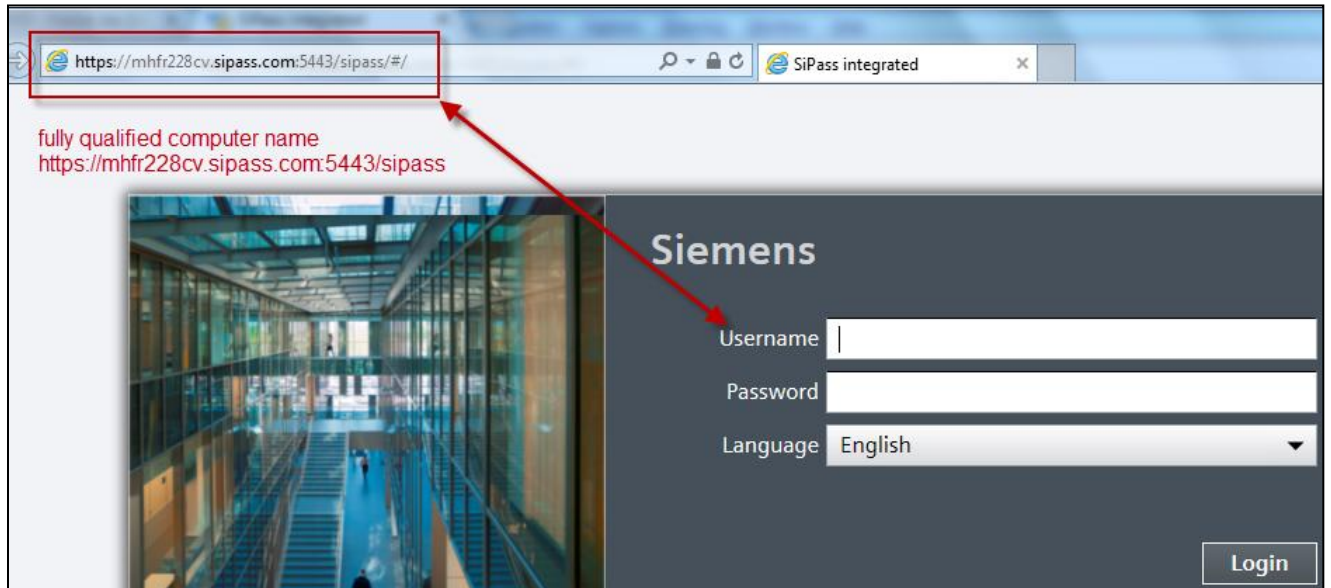


Enter "lusrmgr.msc" to the Run dialogue (Windows key + R), open Users, select the "SiPass Service User" Windows User and remove this option.

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

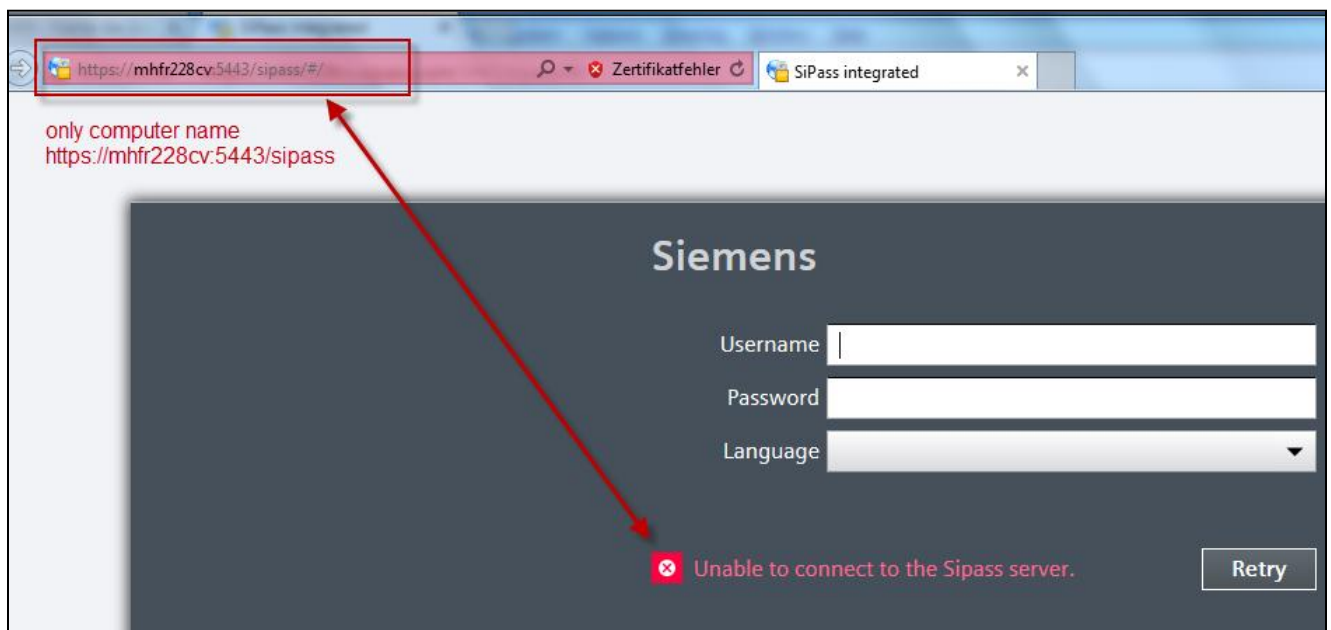
2. SiPass Web Client within a domain environment

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



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.



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.

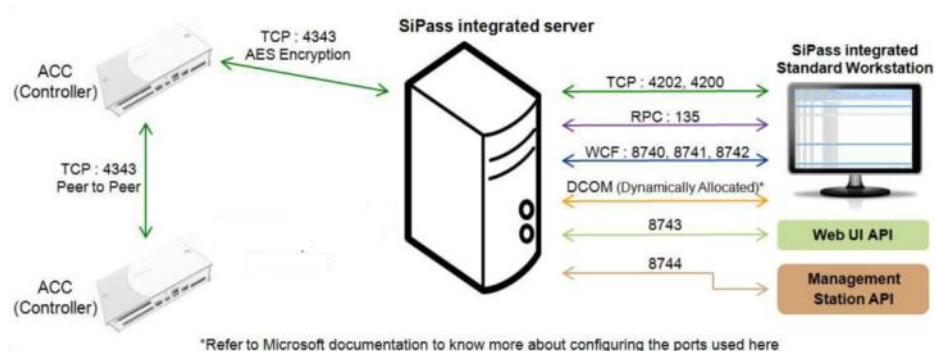
Alternatively you can ping each computer from the other to test the connection. Therefore you can use the Windows command line. Use the following command:
ping <IP address of other computer> (e.g. ping 192.168.1.125).

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 <u>allow</u> the inbound connections for <i>AscoServer.exe</i> and for the default SiPass TCP ports: 8741, 8742, 8743, 8744, 4200, 135, 445	Setup inbound firewall rules which <u>allow</u> the inbound connections the default SiPass TCP ports: 8741, 8742, 8743, 8744, 4200, 135, 445

3.2. Server/Client port information

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

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

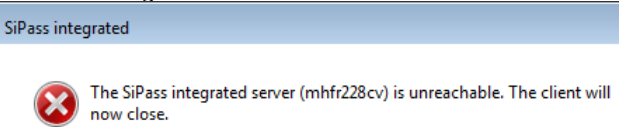
Note: RPC dynamically allocated ports can be changed in Windows from default range.

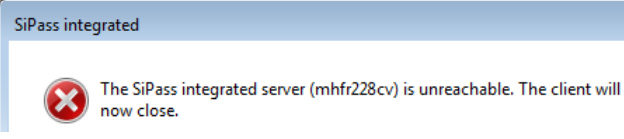
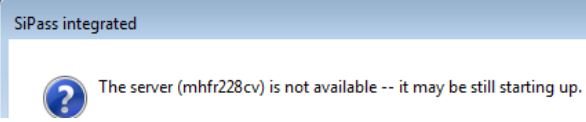
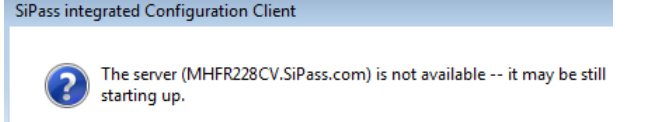
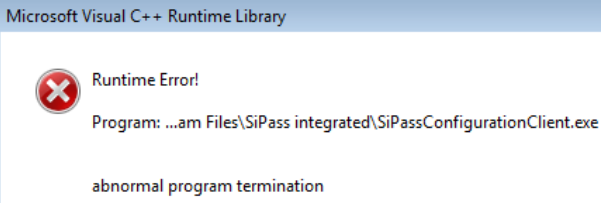
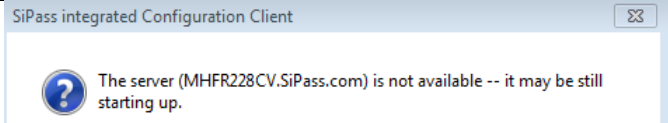

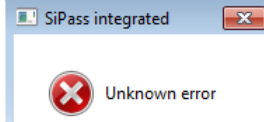
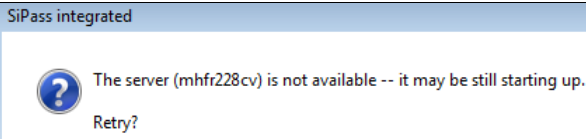
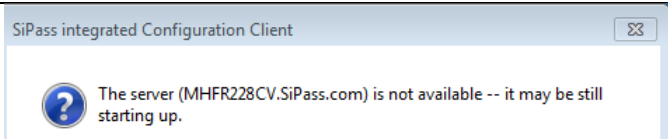
The port numbers are categorised according to the type of client connecting to them. For example, if there is no Operation Client being used, then port 8741 will not be opened up on the firewall for the server.

3.3. 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

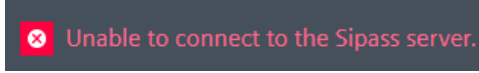
3.4. Different firewall settings and the resulting behavior on the Remote Client

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, 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. 	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	<p>Slow start up, no Audit Trail, Cardholder search is not working. After some minutes the Client is disconnecting from the server.</p> 	<p>It is working, but slow. A bad overall operation performance.</p>
6	Active, no Inbound FW rule	Active, no Inbound FW rule		
7	Active, no Inbound FW rule	Off		
8	Active, Inbound FW rule for: 8741, 8742, 8743, 8744	Off	<p>Starting with AT, Cardholder/Visitor generates following error. The other functions are working.</p> 	
9	Off, no Inbound FW rule	Active, Inbound FW rule for: 8741, 8742, 8743, 8744		

No.	Server Firewall	Remote Client Firewall	Behavior Remote Operation Client	Behavior Remote 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 following error. The other functions are working. 	
11	Active, Inbound FW rule for: 4200, 8741, 8742, 8743, 8744	Active, Inbound FW rule for: 4200, 8741, 8742, 8743, 8744	Working	
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. 	
13	Active, Inbound FW rule for: 4200, 8741, 8742, 8743, 8744	Active, Inbound FW rule for: 8741, 8742, 8743, 8744	Working	
14	Active, Inbound FW rule for: 135, 4200, 8741, 8742, 8743, 8744	Active, Inbound FW rule for: 135, 4200, 8741, 8742, 8743, 8744	Working	

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, 8743, 8744	Active, no Inbound FW rule	Not Working
4	Inbound FW rule for Port 5443	Active, no Inbound FW rule	Not Working 

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		<p>SiPass integrated Operation Client</p>  An error has occurred Additional information: ↳ An unsecured or incorrectly secured fault was received from the other side. See FaultException for the fault code and detail. (mscorlib)	<p>SiPass integrated Configuration Client</p>  Could not establish connection with the server. Probably the server certificate is invalid. The client 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