

# SIEMENS



## Access Control

### SiPass integrated

### Installation Guide

MP 2.80

## Copyright

Technical specifications and availability subject to change without notice.

We reserve all rights in this document and in the subject thereof. By acceptance of the document the recipient acknowledges these rights and undertakes not to publish the document nor the subject thereof in full or in part, nor to make them available to any third party without our prior express written authorization, nor to use it for any purpose other than for which it was delivered to him.

Edition: 30.09.2020

Document ID: A6V11144323

© Siemens Switzerland Ltd, 2020

# Table of Contents

<b>1</b>	<b>Document Updates after Previous Release .....</b>	<b>6</b>
<b>2</b>	<b>Introduction.....</b>	<b>7</b>
2.1	Advanced Security Solution .....	7
2.2	Certificates and Authentication .....	7
2.2.1	Machine Certificates .....	8
2.2.2	Self-signed Certificates .....	8
2.2.3	Certificate Thumbprint .....	8
2.3	Authentication Management Wizard .....	8
2.4	Accounts and Privileges .....	9
2.5	Finding a Computer Name .....	11
<b>3</b>	<b>Microsoft SQL Server.....</b>	<b>12</b>
3.1	Installing Microsoft SQL Server.....	13
3.2	Installing Microsoft SQL Server Express .....	15
3.3	Installing Management Studio Express.....	16
3.4	Configuring the SQL Server Maximum Memory .....	16
3.5	Configuring the SQL Server Protocols .....	17
<b>4</b>	<b>Before Installation .....</b>	<b>18</b>
4.1	Pre-requisites .....	18
4.2	Pre-installation Checklist.....	20
<b>5</b>	<b>Installing SiPass integrated.....</b>	<b>22</b>
5.1	License .....	22
5.1.1	License Management System .....	23
5.2	Installation Types .....	25
5.2.1	Complete Installation .....	25
5.2.2	Custom Installation .....	25
5.2.2.1	Remote MongoDB and RabbitMQ Configuration .....	26
5.2.3	SiPass integrated Clients.....	27
5.2.3.1	Types of Clients.....	27
5.2.4	High Security Option .....	27
5.3	Installing with Self-signed Certificates .....	28
5.3.1	SiPass Server and Local Client Installation.....	29
5.3.1.1	Generating and Applying Self-signed Certificate for SiPass Server and all Local Clients .....	32
5.3.1.2	Installing a Local Client with Self-signed Certificate after Server installation .....	33
5.3.2	Remote Client Installation .....	34
5.3.2.1	Generating Self-signed Certificate for the Remote Client .....	34
5.3.2.2	Installing a SiPass integrated Remote Client with Self-signed Certificate .....	35
5.3.2.3	Importing Certificate to the Remote Client .....	36
5.3.2.4	Assigning privileges to Certificate Private Key .....	37

5.4	Installing with Machine Certificates .....	38
5.4.1	SiPass Server and Local Client Installation .....	38
5.4.1.1	Selecting and Applying Machine Certificate for SiPass Server and all Local Clients.....	41
5.4.1.2	Installing a Local Client after Server Installation .....	41
5.4.2	Remote Client Installation .....	42
5.4.2.1	Saving Certificate Thumbprint of the Remote Client .....	42
5.4.2.2	Adding the Remote Client in SiPass Server.....	43
5.4.2.3	Saving Server Thumbprint for the Remote Client .....	43
5.4.2.4	Installing a SiPass integrated Remote Client with Machine Certificates .....	44
5.4.2.5	Adding the Server Certificate to the Remote Client .....	45
5.5	Certificate Expiry and Renewal .....	45
5.5.1	Renewing the Certificate on SiPass Server.....	46
5.5.1.1	Generating New Certificates for Remote Client .....	47
5.5.2	Renewing the Certificate on SiPass Remote Client .....	48
5.5.2.1	Updating Remote Client Certificate Thumbprint in SiPass Server .....	49
5.6	Installing Additional Components.....	50
<b>6</b>	<b>Installing SiPass integrated Web Site.....</b>	<b>51</b>
6.1	Pre-Installation Checklist.....	51
6.1.1	IIS Installation Instructions .....	51
6.2	Web Site Setup .....	53
6.2.1	Local SiPass Web Site Installation .....	54
6.2.2	Independent SiPass Web Site Installation.....	55
<b>7</b>	<b>SiPass integrated Web Client .....</b>	<b>57</b>
7.1	Post Installation Procedure .....	57
7.1.1	Enabling the HTTPS Security Communication for neXus SDK .....	58
7.1.2	Enabling the Secure Communication for RabbitMQ and MongoDB .....	58
7.1.3	Considerations in launching the SiPass integrated Web Client application .....	58
7.1.3.1	Launching the SiPass integrated Web Client application .....	59
7.1.4	Installing the neXus SDK .....	62
7.1.4.1	Launching the neXus SDK .....	62
7.1.5	Data Retention in Activity Feed .....	63
7.1.6	Restarting SiPass integrated Web Client Server Machine for More Number of Access Area .....	63
7.2	RESTful API Services .....	64
7.2.1	Deployment Instructions .....	64
7.2.2	Starting, Stopping, and Disabling SiPass integrated webclient services.....	64
7.3	Security Risk .....	65
7.4	Exporting the SiPass certificate .....	66
<b>8</b>	<b>SiPass integrated Services .....</b>	<b>67</b>
<b>9</b>	<b>Uninstalling or Reinstalling SiPass integrated .....</b>	<b>68</b>

10 Upgrading SiPass integrated ..... 69

10.1 SiPass integrated Backup / Restore Path .....69

10.2 Performing the Backup / Restore .....70

10.2.1 Steps .....71

11 Password Management ..... 72

12 Appendix ..... 73

12.1 SiPass integrated Port Reference.....73

12.1.1 Internal Server Ports used by Web Client .....73

12.2 Windows Settings.....74

12.3 Connection of Enrolment readers .....77

12.4 Troubleshooting.....78

12.4.1 Troubleshooting Fargo HDP 8500 Printer and  
Embedded Encoder .....81

12.4.1.1 Printer Issues.....81

12.4.1.2 Encoder Issues.....81

# 1 Document Updates after Previous Release

The following updates have been done to this document as below:

Section	Details
Pre-requisites [→ 18]	Updated information on the pre-requisites required for installing SiPass integrated MP2.80
License [→ 22]	Updated information on the new SiPass Licensing process.
License Management System [→ 23]	New sub-section describing the Siemens <b>License Management System</b> – the new way to manage <i>SiPass integrated License Subscriptions</i> from MP2.80 onward.
Upgrading SiPass integrated [→ 69]	Updated information on upgrading from previous versions of SiPass integrated to MP2.80.
SiPass integrated Port Reference [→ 73]	New Appendix sub-section listing the Ports used by SiPass integrated clients and APIs. <b>Note:</b> This information is also present in the SiPass integrated Network Guide.

## 2 Introduction

Congratulations on choosing the SiPass® integrated access control and security solution. SiPass integrated is the leading access control software on the market. This Installation Manual explains how to install the SiPass integrated software.



Be aware that while SiPass integrated is tested thoroughly in combination with different versions of Windows and other third-party applications, it is possible that a third-party application running on the same computer as the SiPass integrated Server or Client may cause unpredictable results. It is recommended that you test your environment fully, before going live with your SiPass integrated system.

This section provides an overview of the SiPass integrated installation process. This includes the various system components that need to be installed and configured prior to and following the installation of the SiPass integrated software. It is recommended that this summary be used as a guide only, and users unfamiliar with the installation process consult the relevant sections of this manual for more information.

Use the checklist in section **SiPass Server Install Checklist** of this document to manually tick off items as you proceed through the installation. This will ensure nothing is missed and will assist in troubleshooting.

### 2.1 Advanced Security Solution

Designed to meet demanding requirements of the modern day, SiPass integrated offers a high-security solution, based on authentication and authorization. While the authentication between the peers (client/server) is done through certificates using the x.509 standard, the authorization is through user logon credentials.

This is how it works:

- A Certification Authority (CA) signs the certificates for the peers
- The SiPass integrated Server and Remote Clients are installed after mutually authenticating the certificates during installation
- During everyday operation, the certificates are checked and validated (being signed by the same Certification Authority) at each login

### 2.2 Certificates and Authentication

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.



For ensuring maximum security, it is recommended to,

- use trustworthy certificates (e.g. issued by VeriSign or Siemens or any other recognized Certificate

Authority).

- set the exportable option for the private key, if the certificate is issued by the Certificate Authority.

### 2.2.1 Machine Certificates

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.

### 2.2.2 Self-signed Certificates

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 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.

### 2.2.3 Certificate Thumbprint

The Certificate Thumbprint is the unique identifier for a certificate. More than one certificate can exist with the same name but the certificate thumbprint is different, hence giving a unique identity to each certificate.

## 2.3 Authentication Management Wizard

The SiPass integrated Authentication Management wizard helps you to choose an existing certificate or generate a new certificate, and apply to SiPass integrated for authentication.

The wizard runs automatically during the installation. To run the wizard after installing SiPass integrated, right-click on *SiPass.CertificatePicker.exe* file from the SiPass installation directory and select **Run as Administrator**.

**Note:** *SiPass.CertificatePicker.exe* must be in the same directory as *AscoServer.exe* and *SiPass.exe* (the installation directory).



## 2.4 Accounts and Privileges

- **Privileges:** Ensure that the person carrying out the installation has local Administrator privileges on which SiPass integrated is being installed.

Also, for SiPass server installations with a pre-installed SQL Server, ensure that SQL Sysadmin role is enabled for the person carrying out the installation.

- **Windows Account:** Before installing SiPass integrated, you must configure the standard Windows user account(s) on the SiPass integrated Server and Client computers that will be used by the SiPass integrated operators.
- **SiPass integrated Installer Account and Run-time Account: Configure as below.**

Account Type	SQL Sysadmin	Local Admin
<b>Installer Account</b> (The account required to install SiPass integrated)	Yes	Yes
<b>Run-time Account</b> (The account required to operate SiPass integrated)	No	Optional

- **Domain User/Local User environment**

SiPass integrated Service User Account can be of the following types:

For example:

- Domain User - **Domainname\DomainUserAccountIdentifier**
- Local user - **LocalUserAccountIdentifier**



**Domain User/Local User environment** configuration is required only for installation purpose. After the installation is complete, this configuration can be removed.

### Set the Local Security Policy

1. In the **Run** command, type **secpol.msc**. The **Local Security Policy** console window opens.
2. From the left pane do the following.
3. Under **Security Settings**, expand **Local Policies**.
4. Select and click **Users Rights Assignment**.
5. In the right pane, search the policy **Allow log on locally**.
6. Verify the groups mapped for Allow log on locally security setting. For e.g. the groups mapped here are **Users/Administrators/Users/BackupOperators** groups

## Set the Local Users and Groups(Local)

1. In run command, type **lusrmgr.msc** and press **Enter** key. The **Local Users and Groups(Local)** window opens.
2. Add domain user(**DomainUserAccountIdentifier**)/local user(**LocalUserAccountIdentifier**) which will be used as a SiPass integrated service user account to any one of the groups that is mentioned in Allow log on locally policy, that is, **Users/Administrators/Users/BackupOperators** groups.



It is recommended to add the domain user/local user under the Administrators or Users Group.

**Unavailability of domain user account/local user account, under any of the Groups defined under the Local User and Groups management console, shall cause incomplete installation of few services.**

3. After the installation is complete, the domain user(**DomainUserAccountIdentifier**)/local user(**LocalUserAccountIdentifier**) can be removed/retained from the Local Security Policy settings as described under the section **Set the Local Security Policy**.

- **Workgroup environment**

In this scenario, the SiPass server and Remote Client computers must have identical (exactly same) Windows Account (Username and Password) details to work together.

1. Create a Windows account for running the SiPass service.  
**Note:** The operator must not be logged in with the service account to install SiPass.
  2. Run the standard SiPass integrated installation.  
⇒ The *SiPass Service Log On* dialog is displayed.
  3. Enter the Windows Account Login (**domain\username or computername\username**) in the **Account Name** field and the password (created to run the SiPass service) in the **Password** field.
- **Workgroup environment with DNS function:** This is a scenario when the internet router is run behind the Workgroup computers. In this case, the Computer Name and the router ID may get mixed up. The following points should be noted:
    - The real name (computer name in the network) can be fetched by pinging `-a <ip address>`. This is used as the **Full Computer Name** in the *Configurations* section of the *Client Configuration* dialog while configuring Client Certificates..
    - During Client Configuration on server side, the *Client Name* must match the real name of the client computers.
    - The *Server Name* used in the client setup must match the real name of the Server computer.
    - The Server Name must be identical as the *Subject Name* of the certificate.

## 2.5 Finding a Computer Name

Throughout this Installation Manual, you will be required to enter the name of a particular computer on the network in order to carry out a procedure. This name must be the same as that given to the computer when its operating system was installed.

Before you can locate the name of the computer / workstation, you must be logged on to that computer / workstation and must have Windows open.

### To find a computer name:

1. Select **Control Panel** from the Windows **Start** menu.
  - ⇒ The *Control Panel* will appear.
2. Double click on the **System** icon.
  - ⇒ The *System Properties* dialog will appear, displaying the *General* tab by default.
3. Click the *Computer Name* tab.
  - ⇒ The Network Identification details will appear.
  - ⇒ The *Computer Name* tab displays the Computer Name together with the Domain Name (if you are connected to a domain-type network).

When performing any procedure in this Installation Manual that needs this information, the Computer Name must be typed exactly as it appears in this dialog.

## 3 Microsoft SQL Server

Microsoft SQL Server is the system that meets the numerous and complex database needs of SiPass integrated. Microsoft SQL Server provides the level of software security necessary to safeguard the records created and modified in SiPass integrated.

The following table indicates the supported SQL Server software on which SiPass integrated will run:

SQL 2019 Express	SQL 2019	SQL 2019 Enterprise
SQL 2017 Express	SQL 2017	SQL 2017 Enterprise



If you are using SQL Server 2017 Express, it is recommended to install the cumulative update provided in the SiPass integrated Software bundle at the following location:

*SQL Server Express\SQL Server 2017 Express\Cumulative Update*

The following information must be noted carefully:

- SQL 2017 is compatible with WINDOWS 10 (64-bit), Windows Server 2016 and Windows Server 2019.
- If there are no SQL server versions installed on the computer where SiPass integrated is installed, a runtime version of Microsoft SQL Server 2017 Express will be installed.
- Sites with multiple clients and higher activity (for example, a large number of doors / cardholders / or event transactions, involving more than 5 clients, 100 doors, or 10000 cardholders) are recommended to purchase a higher performance version of SQL optimized for both scalability and performance.

**See the Microsoft website for more information regarding SQL versions and performance.** Failure to install the appropriate version of SQL Server may have an adverse impact upon the performance of SiPass integrated.

## 3.1 Installing Microsoft SQL Server

It is recommended to have the latest version of Microsoft SQL Server installed to take advantage of the new features that improve server management and application downtime.

### Note:

- The SQL Server and the SiPass integrated server must be installed on the same computer.
- After installation, ensure you also install the latest service pack and apply the correct settings as outlined in the previous chapter.

### To Install SQL Server:

#### Prerequisites:

- ▷ Check that the region setting of the computer is same as the region setting for MS SQL Server installation.
  - ▷ Create a domain/local account to be used for SQL system administrator.
1. Log in to the computer using this account and run the Microsoft SQL Server setup.
  2. On the left panel, click **Installation**.
  3. Select **New SQL Server stand-alone installation** or **add features to an existing installation** from the right panel of the dialog.
    - ⇒ The *SQL Server Setup* dialog is displayed next. This dialog displays the Setup Support Rules that identifies problems that might occur when SQL Server Setup support files are installed. When the operation is complete, click **Next**.
  4. In the next dialog, select the **Enter the product key** option. Enter a product key in the field provided in this dialog.
  5. Click **Next**.
    - ⇒ The next dialog displays the License Terms. Read this and tick the **I accept the license terms** checkbox.
  6. Click **Next**. A dialog to *Setup Support Rules* will be displayed.
  7. Click **Next** to continue. The *Setup Role* dialog will appear next.
  8. Select the features you wish to install.
    - ⇒ We recommend clicking **SQL Server Feature Installation**: Database Engine Services, Client Tools Connectivity and Management Tools - Basic. To select a different installation path click the ... **button** of the **Shared feature directory** field to select a path for each component that you are installing.
  9. Click **Next** to navigate to the **Instance Configuration** dialog.
  10. Select the **Default Instance** or **Named Instance** option and click **Next**
    - ⇒ The *Disk Space Requirements* dialog displayed next will review the disk space summary for the features selected.
  11. Click **Next** to navigate to the *Server Configuration* dialog.

12. In the *Service Account* tab, make the following selections under the Service field:
  - SQL Server Agent
  - SQL Server Database Engine
  - SQL Server Browser
13. Click **Next**. The *Database Engine Configuration* dialog is displayed next.
14. Select the desired option for authentication: **Windows Authentication Mode (recommended for maximum security)** or **Mixed Mode (less secure)**
15. Click **Add Current User** for SQL Server administrators.
16. Click **Next**. The *Error Reporting* dialog will be displayed.
17. Click **Next**. The *Installation Configuration Rules* dialog will be displayed.
18. Click **Next** when the operation is complete. The *Ready to Install* dialog will be displayed.
19. Review the components to be installed and click **Install** to begin the installation. This step can take up to one hour, depending on the features that have been chosen.
  - ⇒ The *Complete* dialog will display the location where a Summary Log File has been saved.
20. Click **Close**.
21. Restart your computer.

## 3.2 Installing Microsoft SQL Server Express

SQL Server Express is a smaller free and re-distributable alternative to SQL Server. Unlike the SQL Server, service pack updates are built into a new installation program, and are not patches that apply to an existing installation.

It does have some limitations:

- 4GB Maximum database size
- 1GB Maximum memory
- A separate install for management of the database

### To Install SQL Server Express:

1. Run the Microsoft SQL Server Express Setup.
2. The *SQL Server Installation Centre* dialog will be displayed. On the left panel, click **Installation**.
3. Next, select **New SQL Server stand-alone installation** or **add features to an existing installation** from the right panel of the dialog.
4. The *SQL Server Setup* dialog is displayed next. This dialog displays the Setup Support Rules that identify problems that might occur when SQL Server Setup support files are installed. When the operation is complete, click **Next** to continue to **Installation Type**.
5. Select the **Perform a new installation of SQL Server** option.
6. Click **Next** to continue to **Feature Selection**.
7. Select the features you wish to install. We recommend clicking **Database Engine Services** and **Client Tools Connectivity**.
8. To select a different installation path click the ... button of the **Shared feature directory** field to select a path for each component that you are installing.
9. Click **Next** to continue to **Instance Configuration**.
10. Select the **Default Instance** or **Named Instance** option.
11. Click **Next** to continue to **Server Configuration**.
12. In the **Account Name** field, select **Network Service** from the drop-down list for the Log On account.
13. From the **Startup Type** drop-down list, select **Automatic for both services**.
14. Click **Next** to continue to **Database Engine Configuration**.
15. Select the desired option for authentication: **Windows Authentication Mode (recommended for maximum security)** or **Mixed Mode (less secure)**.
16. Enter an 'sa' password in the **Enter password** and **Confirm password** fields.
17. Click **Next**.
18. Review the components to be installed and click **Install** to begin the installation. This step can take up to one hour, depending on the features that have been chosen.



After installation, ensure that you also install the latest service pack and apply the correct settings as outlined in the previous chapter.

### 3.3 Installing Management Studio Express

SQL Server Express does not come with the management studio that is installed with the full version of SQL Server. Management Studio Express overcomes this limitation and lets you manage your SQL Express database.

#### To install Management Studio Express:

1. Run the setup file.
2. Click **New installation or add features to an existing installation**.
3. Read the EULA, tick the box **I accept** and click **Next**. Setup support files will be automatically installed at this point.
4. Ensure **Management Tools-Basic** and **SQL Client Connectivity SDK** are both checked, then Click **Next**.
5. Accept the default values on the **Error Reporting** screen, then click **Next** to begin the installation
6. Click **Close** to complete the installation. If prompted, restart your computer to apply the changes made during the installation before starting the application.

### 3.4 Configuring the SQL Server Maximum Memory

To ensure smooth operation of SiPass integrated, it is important to configure SQL Server so that it does not utilize too much memory.

#### To configure the Maximum memory in SQL Server:

1. Click the Start button and select **Programs > Microsoft SQL Server > SQL Server Management Studio**.
2. Check the correct server name is entered in the **Server name** field, and click **Connect**.
3. If the current windows user does not have enough privileges you can change the authentication from **Windows Authentication** to **SQL Server Authentication**.
4. Right click the SQL Server you are connected to, located at the top of the tree, and select **Properties**. The *Server Properties* window will appear.
5. Click the *Memory* tab.
6. Enter a value for the Maximum server memory. This can be set to whatever you wish, but be sure to leave memory for other processes on the system. We recommend a setting of half the total RAM on the computer.
  - ⇒ **Note: You can set a maximum memory for SQL Server standard and enterprise editions (and NOT for the Express version which has a maximum memory limit of 1GB).**
  - ⇒ Click **OK** to save your changes.
7. You will need to restart the SQL Server for the changes to take effect.



## 3.5 Configuring the SQL Server Protocols

To ensure the operation of SiPass integrated and reporting it is important to configure SQL Server for the correct protocols.

### To configure the SQL Server Protocols:

1. Click the **Start** button and select **Programs > Microsoft SQL Server > Configuration Tools > SQL Server Configuration Manager** to display the *SQL Server Configuration Manager* dialog.
2. Expand the *SQL Server Network Configuration*, located at the top of the tree by clicking on the cross, and then select *Protocols for MSSQLSERVER*. The Protocols will appear in the right hand pane.
3. Ensure the following protocols are enabled:
  - Shared Memory
  - TCP/IP
4. To enable each protocol, right click on its name and select the **Enable** option.
5. Close the SQL Server Configuration Manager.
6. You will need to restart the SQL Server for the changes to take effect.

## 4 Before Installation

### 4.1 Pre-requisites

Before installing SiPass integrated, ensure that the following prerequisites are installed in the system.

- **Java Development Kit 11 (64 bit):** SiPass integrated **MP 2.80** Server Component requires Java as a pre-requisite. Both the versions of Java mentioned below are supported and depending on the Java License you wish to use, one of the following can be installed before installing SiPass integrated:
  - **Oracle Java Development Kit SE 11**



The latest Oracle Java SE 11 can be downloaded from the link

<https://www.oracle.com/java/technologies/javase-jdk11-downloads.html>

**Note:** Java auto-update is automatically installed with Oracle Java SE 11. You can accept the latest update notifications to always keep it updated. However, if the update notification feature is disabled on your computer for some reason, you should enable it manually. For more information, see [https://java.com/en/download/help/java\\_update.xml](https://java.com/en/download/help/java_update.xml)

If you do not wish to enable the update notification, it is recommended to frequently check your installed Java version and update it manually.

- **Amazon Corretto 11 (an OpenJDK build)**



#### (1) Amazon Corretto version 11

The free OpenJDK 11 build can be downloaded from the link

<https://corretto.aws/downloads/latest/amazon-corretto-11-x64-windows-jdk.msi>

- Internet Information Services (IIS) 7 & above (for Server and Website only)
- **Browsers:** Chrome and Firefox. Recommended browser versions are:
  - Chrome greater than 83.0.4103.61
  - Firefox 76.0.1



#### **NOTICE**

IIS feature will be automatically enabled during SiPass Server and Website installation..

**The following must be installed/uninstalled manually:**

- License Management System (LMS) (Available in the *Prerequisites* folder in the SiPass integrated software bundle)
- neXus SDK 5.3.0.8 (for **Web Credential Design, Imaging and Printing**)
- If **MongoDB 3.4.6** and **RabbitMQ 3.7.7** are installed separately on a remote machine, the port binding must be done manually using the specific ports. MongoDB with port **8757** and RabbitMQ 3.7.7 with port **8756** respectively. Initially, MongoDB/RabbitMQ authentication and SSL communication will be disabled. Refer to **IP Sec and Network Guide** for configuring the inbound connection for port 8757 and port 8756.



If **MongoDB 3.4.6**, **RabbitMQ 3.7.7**, and **Erlang OTP 20.3** are uninstalled manually, ensure that the installation folder, registry entries, and other related services of the corresponding components are completely removed. By default, the installation folder will be as follows:

**MongoDB** - %systemdrive%\Program Files\MongoDB  
**RabbitMQ** - %systemdrive%\Program Files\RabbitMQ  
**Erlang OTP** - %systemdrive%\Program Files\erl9.3

- WE Installation Helper R101 (for **TBS Server** and **Terminal Enrollment**)
- Enrollment Module 10 (for **USB Enrollment**)



In the **Enrollment Module 10** installation folder, navigate to the **Service>Settings>Public>Service.Enrollment.ini** file. Ensure “Use Https” is set as true and “Port” has value 8282. Open **ServerCommunication.WebEdition.ini** file, and map the **EndpointIP** as the IP of the TBS Server. Restart the Enrollment Module 10 windows service.

**The following are installed automatically and must not be uninstalled at any time to ensure uninterrupted operation of SiPass integrated:**

- .NET Framework 4.8
- Microsoft ODBC Driver 13 for SQL Server
- Microsoft OLE DB Driver for SQL Server (v18)
- Microsoft SQL Server Compact 4.0 SP1
- Microsoft Visual C++ 2015-2019 Redistributable
- OPC Core Components Redistributable (v3.0.102)
- Microsoft .NETCore 2.2.5 Hosting
- SQL Server 2014 Express LocalDB
- Apache Tomcat 9.0.37



**NOTICE**

No other third party applications must be hosted in **Apache Tomcat 9.0 Tomcat\_SiPassintegratedTomcat** server.

- MongoDB 3.4.6
- Erlang OTP 20.3
- RabbitMQ 3.7.7
- Microsoft Application Request Routing 3.0
- IIS URL Rewrite Module 2.0

## 4.2 Pre-installation Checklist

The following checklist is recommended to be used for ensuring all necessary installation steps have been performed.

- **Windows Operating System:** Install the Windows Operating System (and appropriate Service Pack) on to a computer that meets all the system requirements as outlined in the SiPass integrated Release Notes.
- **Microsoft Windows Updates:** Ensure that all the latest updates and patches are installed for the respective MS Windows Operating System, before and after SiPass integrated installation.
- **Computer Configuration:** Ensure that the computer has been correctly configured on your computer network. All appropriate permissions, shared resources, drives, and other network devices should be configured correctly.
- **Date and Time:** SiPass server time and Remote Client time **MUST BE SYNCHRONIZED** under workgroup environment. Ensure that Windows Time service is running and the time is synchronized with an Internet time server under Date and Time Setting of the computer. **The maximum UTC time difference between client and server computers must be less than 5 minutes.**
- **.NET Framework:** The SiPass installation will automatically install .NET Framework. However, you must ensure that all the latest updates and patches are installed at all times.
- **MS SQL:** Install 2019 or 2017 version of Microsoft SQL Server (and appropriate Service Pack). If you prefer Microsoft SQL Express, the SiPass installation can install it. For recommended MS SQL versions, see section Microsoft SQL Server [→ 12] in this document.
- **SQL Memory Properties:** Configure the SQL Server Memory Properties [→ 16].
- **Peripheral Devices:** Install any additional peripheral devices that may be required. This includes printers (which may be networked), Video capture cards and cameras.
- **Internet Browser:** In order to browse the SiPass integrated Web Client, ensure that you have a minimum version of Mozilla Firefox or Google Chrome browser as outlined in section Pre-requisites.
- **Internet Information Services (IIS):** With SiPass integrated MP2.80 onward, IIS is installed and enabled automatically if SiPass Website feature is installed.

If you choose to install it manually later, see the IIS Installation Instructions [→ 51] section for details, or contact your IT administrator for IIS Setup support. The IIS installation must be done by a user with local administrator permissions.

- **User Account Control (UAC):** Ensure that you have turned off User Account Control (UAC) on the SiPass integrated computer.

**Note:** Ensure that you have logged on as an administrator or have been allocated local administrator privileges on the workstation where the SiPass integrated software is being installed.

- **Ports required by SiPass integrated:** Refer to the Appendix sub-section SiPass integrated Port Reference [→ 73] in this document for information on the ports used by SiPass integrated clients and APIs. For detailed information on setting up the network, see the document Network Guide in the SiPass integrated software bundle.

- Ensure that you have sufficient hard disk space available to install the software. Ensure that you have sufficient RAM (memory) to run SiPass integrated, SQL and other modules simultaneously. See the *System Limits and Capabilities* manual in the SiPass integrated software bundle.
- It is strongly recommended that you exit all Windows programs before running the SiPass integrated setup program.
- Install SiPass integrated onto the computer. If choosing the custom installation option, ensure that all the desired options are selected when performing the installation.
  - If SiPass integrated is being re-installed or upgraded, ensure that you have backed up your existing database so that you can restore it later.
  - If the Database option is selected during the installation, any existing database will be overwritten and all existing data will be lost.
  - If SiPass integrated is being re-installed, ensure previous versions have been uninstalled.
- Install any additional SiPass integrated Clients. If these additional clients are to be installed on a computer other than the server, ensure that it has been configured correctly and meets the requirements as outlined in the SiPass integrated Product Sheets and/or System Limits document.
- Assign appropriate read/write privileges to the SiPass integrated folder to each Windows account used to run SiPass integrated.
- Configure and set up SiPass integrated. Refer to the SiPass integrated *Configuration Client User Guide* and *Operation Client User Guide* for more information.




---

**To enable high security in the system, a secured installation and network communication is highly recommended.**

For ensuring **maximum security**, follow and implement as many recommendations as possible given in the document - *Security Recommendations* in the SiPass integrated software bundle.

---

## 5 Installing SiPass integrated

SiPass integrated is shipped with an easy-to-use installation program.

The SiPass integrated software installation can be performed in a number of ways depending upon the requirements of your facility.



---

Before attempting to install SiPass integrated, you should always consult the *Release Notes* in the documentation set of the SiPass integrated software bundle.

For ensuring maximum security, it is recommended to use trustworthy certificates (e.g. issued by VeriSign or Siemens or any other recognized Certificate Authority).

---

**Note:** If you have selected the **Complete** installation option, or the **Custom installation option with Configuration Client**, the account that runs SiPass integrated installation must have Windows administrator rights.

### 5.1 License

From Version MP2.80 onward, "SiPass integrated License" is a **subscription-based service** managed by a central tool - **Siemens License Management System (LMS)**.

- If you do not have a SiPass integrated license, you can order a new one for MP2.80.
- If you have an existing license for a previous release and are upgrading to MP2.80,
  - You must still order a new license.
  - Your existing license will be modified and applied in the new License Management Service (LMS) from where, you can activate your product.
  - Depending on the costs paid for the previous license, the new MP2.80 license will be issued for the standard upgrade fee (or any other amount as per your current agreement), the way upgrades have been done in the past.

**Contact Siemens Support in your region for help with this matter.**



---

**Note:**

SiPass integrated is always by your side and will keep working even when the subscription expires. However, it is recommended to renew your subscription as soon as possible to stay up to date on the latest product features, security updates and access to support.

When your subscription is about to expire, the status bar in SiPass integrated *Configuration Client* and *Operation Client* will start showing a reminder 7 days before the expiry. You can also check the subscription status any time by clicking **Help > About** from the top menu bar.

Contact Siemens Support in your region for help with renewing the subscription.

---

### 5.1.1 License Management System

Siemens License Management System (LMS) is required for a new subscription, renewing an existing subscription on expiry and/or managing an active subscription between different devices. With LMS, you can order the following:

<b>LMS Product</b>	An LMS product consists of one or more LMS features in varying quantities, and must be selected when ordering a new SiPass integrated license. Multiples of the same product can be ordered.
<b>LMS Feature</b>	A single feature, or a collection of features included in an LMS Product.

**Example:**

The product *SiPass Standard Edition* consists of the following features:

- si\_sipass\_1000\_card\_extension – quantity 1
- si\_sipass\_extension8doors – quantity 3
- si\_sipass\_Web\_Client – quantity 1
- si\_sipass\_workstation – quantity 1

This means that the product *SiPass Standard Edition* contains 1000 cards, 24 doors, 1 web client and 1 workstation.

To enhance the *SiPass Standard Edition* above, you can increase the number of cardholders by purchasing a *SiPass 10000 Card Extension* product. This contains “quantity 10” of the feature *si\_sipass\_1000\_card\_extension* and adds 10,000 cardholders to your license.

**Note:** When activating the SiPass license modules, only the LMS features are checked for.

The LMS package must be installed separately, before (recommended) or after installing SiPass integrated. You will need it installed for activating the subscription later.

**Note:** The *LMS installation package* is available in the *Prerequisites* folder in the SiPass integrated software bundle.

Once you have obtained a new license subscription for SiPass integrated MP2.80 from your regional Siemens Support, you will get an e-mail mentioning the **Activation Key** and **Entitlement Key**. These are the keys which include your subscription validity and the SiPass integrated features purchased. Store this information securely to prevent misuse of your license.

Once you have everything in place,

1. Start the LMS application.
2. For activating, renewing or managing your subscription, or troubleshooting regarding the LMS Application, see the *LMU.chm* help file located at *C:\ProgramData\Siemens\LMS\Documentation* (or any other drive where you installed the LMS).
3. Login to SiPass integrated and start using normally after license activation.



---

**The number of computers where you can install SiPass integrated cannot exceed the number of devices allowed in your subscription.**

If you have already installed on the maximum number of computers allowed and wish to install SiPass integrated on some other computer, you must first return the subscription through the LMS application on an already installed computer and then activate the subscription on the computer where you wish to install SiPass integrated now.

---



---

RESTful MS-API and HR-API services must be manually started, if the license is enhanced to introduce the HR-API or MS-API license feature.

---



---

**Note:**

If a software update needs to be performed for the LMU on a computer where both SiPass and LMU are installed, the SiPass services must first be stopped manually to apply the update.

---



## 5.2 Installation Types

### 5.2.1 Complete Installation

A Complete Installation will automatically select each module and option available.

### 5.2.2 Custom Installation

A Custom installation will allow you to install any combination of the following:

Client Options	Description
<b>Server</b>	The Server is required for communicating with the security hardware and the SiPass integrated database.
<b>APOGEE Interface</b>	Allows you to interface with Siemens APOGEE Building Automation System.
A SiPass integrated Client is normally installed on the server computer and may also be installed on other computers that form part of the access control system. The clients below are installed on a computer to provide a GUI (Graphical User Interface) for the system's operator(s).	
<b>Configuration Client</b>	The SiPass integrated user interface for site setup and configuration.
<b>Operation Client</b>	This is the SiPass integrated user interface for daily operation of site activities.
<b>Web Site</b>	The SiPass integrated web user interface for security operators and administrators.
<b>HR-API Core</b>	This type of Client is installed on a computer to provide an interface to third-party Human Resource databases that can be used to help populate SiPass integrated.

**Note:** The **Server** feature requires selecting at least the **Configuration Client** option for proceeding with the installation.



The **Web UI API**, **RESTful Management Station API** and **RESTful HR-API** are installed with every installation option given above.

Multiple MS-API clients can use the RESTful Management Station API interface, which can be installed on Remote Client computers, separately from the SiPass integrated Server. Only one login can be done at a time on "RESTful Management Station API" service. The additional installations allow multiple MS-API clients to run and connect to SiPass server, each client connecting to their own "RESTful Management Station API" service.

For installing the **RESTful Management Station API** separately, refer to the *SiPass integrated RESTful Management API Installation guide*.

### 5.2.2.1 Remote MongoDB and RabbitMQ Configuration

If you selected the “Custom” installation type, or performing a SiPass integrated upgrade, the *MongoDB and RabbitMQ Configuration* dialog is displayed after entering the Username and Password for the SiPass service account. With this dialog, a remote hostname can be configured for either RabbitMQ or MongoDB, as well as the Username / Password.

You can click **Next** with no changes.

- In this case, the default values (local Server name and credentials) are used
- Both RabbitMQ and MongoDB will be installed locally with the requested Username / Password
- This will also occur automatically for the **Complete** installation type

**Note:** See the Appendix sub-section Internal Server Ports used by Web Client [→ 73] for more information on the ports used by MongoDB and RabbitMQ, along with a list of other ports used by SiPass integrated Web Client.

**In case when it is required to use the MongoDB / RabbitMQ services running somewhere else,** you can modify the Server name and Credential settings in the MongoDB and RabbitMQ Configuration dialog to ensure a successful remote connection.



#### **NOTICE**

After installing SiPass integrated, MongoDB and RabbitMQ should be secured with SSL communication.

While setting the Remote MongoDB password, user must avoid the special characters like double quotes (“), greater-than symbol (>), less-than symbol (<)

## 5.2.3 SiPass integrated Clients

SiPass integrated allows you to install clients on more than one computer in a network. A remote client provides the GUI (Graphical User Interface) that is used by the SiPass integrated operator to administer and monitor your access control and security system. Only one client of each type can be installed on any single computer in your system.

### 5.2.3.1 Types of Clients

#### Local Client

When any or both of the Configuration Client and Operation Client is installed on the same computer on which, the SiPass server is installed. The client is connected to the server directly in this case.

#### Remote Client

When any or both of the Configuration Client and Operation Client is installed on a computer other than the one where SiPass server is installed. The client is connected to the server through the network in this case.

#### Before You Begin

- Ensure that your License Agreement permits you to configure an additional Client. If your License only allows the installation of a single Client, please contact your distributor to obtain an additional License.
- Ensure that you have installed the SiPass integrated Server software.
- If you are installing a Client on a workstation other than the Server, ensure that the target workstation has been configured on the same network.
- Identify the name of the computer where the SiPass integrated Server has been installed.
- It is recommended that you exit all Windows programs before running the SiPass integrated setup program.

## 5.2.4 High Security Option

For all installation types, you get the option to enable high-security for SiPass integrated that adds higher immunity against external security threats.

**In the high security mode, the SiPass Configuration Client and MS-API Client can connect to the SiPass integrated server ONLY AS LOCAL clients (on Server site) (SiPass Operation Clients are not affected).**

#### Enabling the high security option

The option can be enabled during the SiPass integrated installation by ticking the **Enable High Security** checkbox in the *Authentication Management Wizard*.

To enable high security after the SiPass integrated installation, run the Authentication Management Wizard by running the *SiPass.CertificatePicker.exe* file from the SiPass integrated installation directory on the computer where SiPass integrated server and local client are installed.

## 5.3 Installing with Self-signed Certificates

Certificates properties:

Certificate Type	Key Length	Hashing Algorithm
SiPass Generated Certificate	2K	SHA-2

Encryption:

SiPass integrated Client	Encryption for Data Transfer
Configuration Client	TLS, Genuine Channels, DCOM NTLM
Operation Client	TLS, Genuine Channels



---

### Web Site feature and Certificates

If you choose to generate a self-signed certificate during SiPass integrated installation and connect to the SiPass Web Site using a browser (on a PC that does not have a SiPass client installed), the web site certificate will not be trusted in this case and a warning will be shown. Depending on the browser, you may not be able to proceed with using the SiPass web site.

To prevent this from happening, it is recommended that if you are using the SiPass Web Site feature, an existing official certificate (either predefined company certificate, or official purchased certificate) is selected during the SiPass integrated installation.

---

### 5.3.1 SiPass Server and Local Client Installation

1. Start the **Windows** operating system.
2. Locate the SiPass integrated installer folder on a disk, network share or portable media.
3. Right-click on the *Setup.exe* file (in root folder) and select the **Run as Administrator** option from the menu.
  - ⇒ SiPass integrated Setup will now check for any pre-requisites not installed on your computer.



Some pre-requisites will be installed by the setup automatically (or by asking you to click and confirming the installation). However, the Java Development Kit 11 (64-bit) must be installed manually. In this case, exit the SiPass integrated installation and install JDK 11 first. Java JDK tested version is 11.0.8

See the Pre-requisites [→ 18] section in this document (or SiPass integrated Release Notes) for more information.

If you closed the SiPass integrated setup for installing JDK 11, run it again by right-clicking on the *Setup.exe* file (in root folder) and select the **Run as Administrator** option from the menu. If you installed JDK before running the SiPass integrated setup, continue with the installation wizard.

Once all the pre-requisites are installed, the *Welcome to the SiPass integrated Installation Wizard* will appear. From this point onward in the SiPass integrated installation, you may exit by choosing the Cancel button.

1. Click **Next >**.
  - ⇒ The *License Agreement* dialog is displayed describing the SiPass integrated End User License Agreement (EULA). It is recommended that you read, understand and agree to the terms and conditions mentioned here.
2. To agree to the EULA terms and proceed with installation, select the **I accept the terms in the license agreement** option.
3. Click **Next**.
  - ⇒ The *Hardware Type* dialog is displayed.
4. Select the SiPass integrated platform (ACC or ACC / NT) that you wish to install by checking the option that corresponds to your license.
5. Click **Next**.
  - ⇒ The *Options* dialog will appear.
6. Complete the fields to set your base credential profile during the setup. Note that the **License Key** and other information is included in your subscription activation through the LMS.
  - **Card Technology:** The access card format that you have purchased with your SiPass integrated license
  - **Site:** Site Code used
  - **Facility:** Facility Code used



Refer to the information provided with your SiPass integrated subscription for more details about completing the *Options* dialog.

7. Click **Next**.
  - ⇒ The **Setup Type** dialog will appear.
8. Select the type of installation you want (Custom / Complete).
9. If you have chosen the Custom installation, the *Select Features* dialog will appear with the following choices:
  - Server
  - Configuration Client
  - Operation Client
  - Website
  - APOGEE Interface
  - HR-API Core
  - ⇒ **Note:** Refer to the table given in *Custom Installation* section of this document to learn more about these features and options. The **Server** feature requires selecting at least the **Configuration Client** option for proceeding with the installation.
  - ⇒ If you have chosen a *Complete* installation, the *Select Features* dialog will not appear.
10. Select which features are to be installed by clicking on the hard drive icon for a particular feature and selecting *Will be installed on the local hard drive* from the drop down menu.
11. Specify the destination for the SiPass integrated software.
  - A default directory, usually **C:\Program Files (x86)\SiPass integrated\**, will be nominated by the Install Wizard. You may designate any hard drive as the host.
  - To change the default destination directory, choose the **Change** button and select a new location from the Change Current Destination Folder dialog.
  - ⇒ **Note:** You cannot specify a network drive or remote computer for the SiPass integrated installation directory.
12. Click **Next**. The *SQL Options* dialog will appear.
  - If you want to use an existing SQL Server instance, select the **Use existing SQL Server instance:** option, and from the drop-down list, select the instance (**Local**) that will host the SiPass SQL database.
  - If there is no previous instance of SQL Server installed on your computer, select the **Install MSSQLSERVER instance of SQL Express 2017 and use it** option.
  - To install any other SQL Server version, exit the installation by choosing Cancel and install your desired SQL Server product.
  - ⇒ See section Microsoft SQL Server [→ 12] for more information on supported SQL versions with different Operating Systems.
13. Click **Next**.
  - ⇒ The *SiPass Service Log On* dialog will be displayed.
14. Enter the Username and Password for the SiPass service account
  - ⇒ **Note:**
    - This is the minimum required Windows standard account (non-admin).
    - If HR API subscription/callback is required, the SiPass user should have administrator rights.
15. Click **Next**.

If you selected the “Custom” installation type, or performing a SiPass integrated upgrade, the *MongoDB and RabbitMQ Configuration* dialog is displayed (See section Remote MongoDB and RabbitMQ Configuration for more information).

- Click **Next** to go ahead with no changes (default values are used)
- Or, enter the details as below:

#### MongoDB

- **Server** – Provide the full computer name where MongoDB is installed.
- **Username** – Provide the username to connect with MongoDB.
- **Password** - Provide the password to connect with MongoDB.

#### RabbitMQ

- **Server** – Provide the full computer name where RabbitMQ is installed.
- **Username** – Provide the username to connect with RabbitMQ.
- **Password** - Provide the password to connect with RabbitMQ.

If you selected the **Complete installation type**, or you have entered the required values on the *MongoDB and RabbitMQ Configuration* dialog, the *Ready to Install the Program* dialog is displayed.

- Click **Install**.
  - The Installation will proceed and the installation progress indicator will appear.
  - The *SiPass Authentication Management Wizard* is displayed.
- Do one of the following:

To generate and apply self-signed certificate for SiPass server and all local clients	Click here [→ 32]
Install a Local Client after server installation	Click here [→ 32]

### 5.3.1.1 Generating and Applying Self-signed Certificate for SiPass Server and all Local Clients

In this step, the self-signed certificates are generated and applied on the SiPass Server and any or all of the Configuration Client, Operation Client and Web Client (depending on features selected on the *Setup Type* dialog) installed on the same computer where the SiPass Server is installed.

Continuing the steps from the previous section, on the *SiPass integrated Authentication Management Wizard* screen:

1. Click **Next**.
  - ⇒ The *Authentication management* dialog is displayed.
2. Tick the **Generate Self-Signed Certificate** checkbox.
3. Click **Finish**.
  - ⇒ A message in the bottom left corner of the *Authentication management* dialog is displayed, informing you that the certificate is being generated and applied. The other actions on the dialog are disabled till you see a message confirming that a new certificate has been generated and applied to SiPass integrated server and any local client selected for installation.
4. Click **OK** to close the message.
  - The certificate generated in this step will bear the full computer name in its subject.
  - All the clients use self-signed certificates.
  - ⇒ The SiPass integrated installation is continued. When completed, the *Setup Complete* dialog will appear.
5. Click **Finish**.
6. Restart the SiPass service.
  - ⇒ Congratulations! You have now successfully installed SiPass integrated.



### 5.3.1.2 Installing a Local Client with Self-signed Certificate after Server installation

As a minimum requirement for SiPass Server installation, a local Configuration Client must be installed on the same computer as the server. However, at any point of time, a local Operation Client can also be installed on the computer where the SiPass server and Configuration Client are already installed.

In this case, the self-signed certificate is generated again during the local Operation Client installation and applied on the SiPass integrated Server and the local Configuration Client also.

**To install a local Operation Client, follow the steps below:**

1. Click **Next**.
  - ⇒ Continuing the steps from the section SiPass Server and Local Client Installation, on the *SiPass integrated Authentication Management Wizard* screen:
2. Click **Next**.
  - ⇒ The *Authentication management* dialog is displayed.
3. Tick the **Generate Self-Signed Certificate** checkbox.
4. Click **Finish**.
  - ⇒ A message in the bottom left corner of the Authentication management dialog is displayed, informing you that the certificate is being generated and applied. The other actions on the dialog are disabled till you see a message confirming that a new certificate has been generated and applied to SiPass integrated server and any local client selected for installation.
5. Click **OK** to close the message.
  - The certificate generated in this step will bear the full computer name in its subject.
  - All the clients use self-signed certificates.
  - ⇒ The SiPass integrated installation is continued. When completed, the *Setup Complete* dialog will appear.
6. Click **Finish**.
7. Restart the SiPass service.
  - ⇒ Congratulations! You have now successfully installed SiPass integrated.

## 5.3.2 Remote Client Installation

### 5.3.2.1 Generating Self-signed Certificate for the Remote Client

After the SiPass server is installed, the SiPass integrated Configuration Client on the Server computer is used to generate a self-signed certificate that will be provided to the client computer during installation.

Since this certificate is generated (and hence, signed) by the Certification Authority (CA) of the server computer, installing this self-signed certificate on the remote client computer authenticates it as the genuine client of the respective server computer.

#### Steps

- ▷ **Prerequisite:** To generate Client certificates through the SiPass integrated Configuration Client, the client must be run locally (on server site) with the SiPass integrated server.
- ▷ For this operation the Configuration Client must be run in *Administrator* mode.
- 1. Right-click on the SiPass integrated Configuration Client icon on the computer where SiPass server is installed and select **Run as Administrator**.
- 2. From the **System** menu, click **Client Configuration ...**
  - ⇒ The *Client Configuration - New* dialog is displayed.
- 3. Type the name of the computer (where SiPass integrated client will be installed) in the **Full computer name** field.
  - ⇒ **Note:** If the Remote Client computer is connected to SiPass server computer through a VPN connection, tick the **Only check thumbprint for authentication** checkbox.
- 4. Click the **Generate Self-Signed Certificate...** button (which is enabled when the Self-signed certificate has been generated for SiPass integrated during server installation).
- 5. When the Windows browsing dialog is displayed, select an empty folder or create a new one on the local hard drive to store the self-signed certificate generated for the client. These files will be required during the SiPass integrated installation on the client computer.
  - ⇒ **Note:** This folder must 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.
  - ⇒ Once you specify the location to store the certificate, a message is displayed confirming that the certificate has been generated successfully.
- 6. Click **OK** to close the message.
  - ⇒ The **Certificate Thumbprint** field on the *Client Configuration - New* dialog is now populated.
  - ⇒ **Note:** If a client's certificate is generated, the server thumbprint is also included. In case you wish to save only the server thumbprint without generating the self-signed certificate, click the **Save Server thumbprint...** button and specify an empty folder to save the thumbprint file.
- 7. Click **Save**.
  - ⇒ The Client Computer is listed on left hand side of the *Client Configuration - New* dialog. To delete an existing Client Configuration, select it from the left pane of the dialog and click **Delete**.
- 8. Click **Close** to close the *Client Configuration - New* dialog.

### 5.3.2.2 Installing a SiPass integrated Remote Client with Self-signed Certificate

1. Follow the procedure to start the SiPass integrated Installation.
2. Fill in the *Options* dialog with the same details as the original installation.
3. Click **Next** to continue.
4. Select **Custom** and click **Next** to continue to the *Select Features* dialog.
5. Select only the Client option(s) you are installing.
  - The Configuration Client and Operation Client can be installed and run on any local or remote client computer. **However, when the high-security installation option is selected, only the SiPass Configuration Client on server site can connect to the SiPass integrated server.**
  - The HR-API Core must be installed on the computer where the HR application or the HR application gateway is installed.
  - Ensure that the SiPass integrated Server option is marked with a red cross (described as *This feature will not be available.*) so that the server will NOT be installed.
  - Ensure other items in the dialog are also marked with a red cross.
6. Click **Next**.
  - ⇒ The *SiPass integrated Server* dialog will appear.
7. Type the full name or IP address of the SiPass integrated Server computer in the **Server** field. **Ensure that the port numbers on this dialog are exactly the same as for server installation.**
  - ⇒ **Note:** Unless a server name is provided in this field, the installation process will not proceed.
8. Click **Next**.
  - ⇒ The *Ready to Install the Program* dialog will appear.
9. Click **Install**.
  - ⇒ The SiPass integrated Client installation will proceed and the progress indicator will appear.
  - ⇒ After completion, the *Authentication Management Wizard* is displayed where a certificate can be selected/imported. This is the same certificate generated during the SiPass server installation that were saved separately in an empty folder of your choice.
  - ⇒ **Note:** The *Authentication Management Wizard* can also be run to add/renew the certificate on an installed remote client. Double-click the *SiPass.CertificatePicker.exe* file from the SiPass integrated installation directory on the computer where SiPass integrated client is installed and follow the process as mentioned below.
10. Continue with the steps described in the next section.

### 5.3.2.3 Importing Certificate to the Remote Client

1. On the *Authentication Management Wizard* screen, click **Next**.  
⇒ The *Authentication management* dialog is displayed.
2. Tick the **Import Client & Server Certificates From** checkbox.
3. Click the folder icon next to the field and locate the folder that contains the Server Certificate and Thumbprint files generated earlier on the server.
4. Click **Finish**.  
⇒ The certificate is applied and the following message is displayed: *The certificate has been successfully applied*.
5. Click **OK** to close the message.  
⇒ The SiPass integrated installation is continued. When completed, the *Setup Complete* dialog will appear.
6. Click **Finish**.  
⇒ Congratulations! You have now successfully installed SiPass integrated on the client computer.

**Note:**

- You can also load another Server Certificate Thumbprint for authenticating SiPass server on the client. To do this, run the *Authentication Management Wizard* and edit the pre-filled **Server Certificate Thumbprint** field filling-in the thumbprint value of that server computer, or locate a thumbprint file for that server computer stored separately.
- The permissions to the selected/imported certificate have been granted to both the current user and local Administrators. If the SiPass Client will be run by other users on this computer who are not System Administrators, then these users must be granted Read permissions (at least) to the certificate private key so they can be assigned additional privileges, if required later. See section *Assigning privileges to Certificate Private Key* [→ 36].

### 5.3.2.4 Assigning privileges to Certificate Private Key

The windows account which starts the SiPass clients must have the Read privileges to the certificate private key.

1. Click the Windows Start button, type *mmc* in the search box and press the **Enter** key to start the *Microsoft Management Console*.  
⇒ The *Console 1 - [Console Root]* dialog is displayed.
2. From the **File** menu, select **Add/Remove Snap-in** to display the *Add/Remove Snap-ins* dialog.
3. From the **Snap-in** list box on the left hand side, select **Certificates**.
4. Click the **Add >** button.  
⇒ The *Certificates snap-in* dialog is displayed.
5. Select **Computer Account** and click **Next**.  
⇒ The *Select Computer* dialog is displayed with the option **Local computer: (the computer this console is running on)** selected by default.
6. Click **Finish**.  
⇒ The *Add/Remove Snap-ins* dialog is displayed again with the **Console Root snap-in** tree listing **Certificates (Local Computer)** on right hand side of the list box.
7. Click **Ok** to close the dialog.
8. In the left pane of the *Microsoft Management Console* dialog, expand the **Certificates (local computer)** tree as below:
  - Personal
  - Certificates⇒ The certificate added by you will be displayed in the right section of the window.
9. Right-click with the mouse on the certificate and from the menu, select **All Tasks > Manage Private Keys...**  
⇒ The *Permissions for private keys* dialog will be displayed.
10. Tick the **Read** checkbox (if not already checked) to allow read permissions for the certificate private key.
11. Click **OK** to close the dialog.
12. Close the *Microsoft Management Console*. Click **Yes** if you want to save the list of certificate stores on the computer.  
⇒ The privileges are now assigned to the Certificate Private Key.

## 5.4 Installing with Machine Certificates

- **Prerequisite:** Certificates are already installed on all the computers on which SiPass integrated will be installed.



If using custom certificates specific to the installation site, the private key format should be RSA. Other formats might not be supported by the operating system.

- A Machine Certificate being used for SiPass integrated installation must meet the **requirements** below:
  1. Ensure the identity of a remote computer
  2. Allow secure communication on the Internet
  3. Prove your identity to a remote computer

### 5.4.1 SiPass Server and Local Client Installation

1. Start the **Windows** operating system.
2. Locate the SiPass integrated installer folder on a disk, network share or portable media.
3. Right-click on the *Setup.exe* file (in root folder) and select the **Run as Administrator** option from the menu.
  - ⇒ SiPass integrated Setup will now check for any pre-requisites not installed on your computer.



Some pre-requisites will be installed by the setup automatically (or by asking you to click and confirming the installation). However, the Java Development Kit 11 (64-bit) must be installed manually. In this case, exit the SiPass integrated installation and install JDK 11 first.

See the Pre-requisites [→ 18] section in this document (or SiPass integrated Release Notes) for more information.

If you closed the SiPass integrated setup for installing JDK 11, run it again by right-clicking on the *Setup.exe* file (in root folder) and select the **Run as Administrator** option from the menu. If you installed JDK before running the SiPass integrated setup, continue with the installation wizard.

Once all the pre-requisites are installed, the *Welcome to the SiPass integrated Installation Wizard* will appear. From this point onward in the SiPass integrated installation, you may exit by choosing the Cancel button.

1. Click **Next >**.
  - ⇒ The *License Agreement* dialog is displayed describing the SiPass integrated End User License Agreement (EULA). It is recommended that you read, understand and agree to the terms and conditions mentioned here.
2. To agree to the EULA terms and proceed with installation, select the **I accept the terms in the license agreement** option.
3. Click **Next**.
  - ⇒ The *Hardware Type* dialog is displayed.
4. Select the SiPass integrated platform (ACC or ACC / NT) that you wish to install by checking the option that corresponds to your license.

5. Click **Next**.

⇒ The *Options* dialog will appear.

6. Complete the fields to set your base credential profile during the setup. Note that the **License Key** and other information is included in your subscription activation through the LMS.

- **Card Technology:** The access card format that you have purchased with your SiPass integrated license
- **Site:** Site Code used
- **Facility:** Facility Code used



Refer to the information provided with your SiPass integrated subscription for more details about completing the *Options* dialog.

7. Click **Next**.

⇒ The **Setup Type** dialog will appear.

8. Select the type of installation you want (Custom / Complete).

9. If you have chosen the Custom installation, the *Select Features* dialog will appear with the following choices:

- Server
- Configuration Client
- Operation Client
- Website
- APOGEE Interface
- HR-API Core

⇒ **Note:** Refer to the table given in *Custom Installation* section of this document to learn more about these features and options. The **Server** feature requires selecting at least the **Configuration Client** option for proceeding with the installation.

⇒ If you have chosen a *Complete* installation, the *Select Features* dialog will not appear.

10. Select which features are to be installed by clicking on the hard drive icon for a particular feature and selecting *Will be installed on the local hard drive* from the drop down menu.

11. Specify the destination for the SiPass integrated software.

- A default directory, usually **C:\Program Files (x86)\SiPass integrated\**, will be nominated by the Install Wizard. You may designate any hard drive as the host.
- To change the default destination directory, choose the **Change** button and select a new location from the Change Current Destination Folder dialog.
- ⇒ **Note:** You cannot specify a network drive or remote computer for the SiPass integrated installation directory.

12. Click **Next**. The *SQL Options* dialog will appear.

- If you want to use an existing SQL Server instance, select the **Use existing SQL Server instance:** option, and from the drop-down list, select the instance (**Local**) that will host the SiPass SQL database.
- If there is no previous instance of SQL Server installed on your computer, select the **Install MSSQLSERVER instance of SQL Express 2017 and use it** option.
- To install any other SQL Server version, exit the installation by choosing Cancel and install your desired SQL Server product.
- ⇒ See section Microsoft SQL Server [→ 12] for more information on supported SQL versions with different Operating Systems.

13. Click **Next**.

⇒ The *SiPass Service Log On* dialog will be displayed.

14. Enter the Username and Password for the SiPass service account

⇒ **Note:**

- This is the minimum required Windows standard account (non-admin).
- If HR API subscription/call back is required, the SiPass user should have administrator rights.

15. Click **Next**.

If you selected the “Custom” installation type, or performing a SiPass integrated upgrade, the *MongoDB and RabbitMQ Configuration* dialog is displayed (See section Remote MongoDB and RabbitMQ Configuration for more information).

- Click **Next** to go ahead with no changes (default values are used)
- Or, enter the details as below:

**MongoDB**

- **Server** – Provide the full computer name where MongoDB is installed.
- **Username** – Provide the username to connect with MongoDB.
- **Password** - Provide the password to connect with MongoDB.

**RabbitMQ**

- **Server** – Provide the full computer name where RabbitMQ is installed.
- **Username** – Provide the username to connect with RabbitMQ.

**Password** - Provide the password to connect with RabbitMQ.

If you selected the **Complete installation type**, or you have entered the required values on the *MongoDB and RabbitMQ Configuration* dialog, the *Ready to Install the Program* dialog is displayed.

◆ Click **Install**.

- ⇒ The Installation will proceed and the installation progress indicator will appear.
- ⇒ The *SiPass Authentication Management Wizard* is displayed.
- ⇒ Do one of the following:

To select and apply machine certificate for SiPass server and all local clients	Click here [→ 40]
Install a Local Client after server installation	Click here [→ 41]



### 5.4.1.1 Selecting and Applying Machine Certificate for SiPass Server and all Local Clients

On the *SiPass integrated authentication management Wizard* screen:

1. Click **Next**.
  - ⇒ The *Authentication management* dialog is displayed. The tree view on the left lists all the different certificate stores you can pick from.
2. 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.
3. Click **Finish** to apply the certificate (To close the application without applying the certificate, click **Cancel**.).
  - ⇒ A message in the bottom left corner of the *Authentication management* dialog is displayed, informing you that the certificate is being applied. The other actions on the dialog are disabled till you see a message confirming that the certificate has been applied to SiPass integrated server and any local client selected for installation.
4. Click **OK** to close the message.
  - ⇒ The SiPass integrated installation is continued. When completed, the *Setup Complete* dialog will appear.
5. Click **Finish**.
6. Restart the SiPass service.
  - ⇒ Congratulations! You have now successfully installed SiPass integrated.

### 5.4.1.2 Installing a Local Client after Server Installation

On the *SiPass integrated authentication management Wizard* screen:

1. Click **Next**.
  - ⇒ The *Authentication management* dialog is displayed. The tree view on the left lists all the different certificate stores you can pick from.
2. 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.
3. Click **Finish** to apply the certificate (To close the application without applying the certificate, click **Cancel**.).
  - ⇒ A message in the bottom left corner of the *Authentication management* dialog is displayed, informing you that the certificate is being applied. The other actions on the dialog are disabled till you see a message confirming that the certificate has been applied to SiPass integrated server and any local client selected for installation.
4. Click **OK** to close the message.
5. The SiPass integrated installation is continued. When completed, the *Setup Complete* dialog will appear.
6. Click **Finish**.
7. Restart the SiPass service.
  - ⇒ Congratulations! You have now successfully installed SiPass integrated.

## 5.4.2 Remote Client Installation

### 5.4.2.1 Saving Certificate Thumbprint of the Remote Client

After the SiPass server is installed, the thumbprint of the machine certificate of the remote client computer is used for setting it up as the genuine client of that SiPass server installation.



This step is done on the remote client computer. You can go to this computer directly, or access it through the Remote Desktop Connection from the computer where the SiPass server is installed.

#### On the Remote Client computer

1. Click the Windows **Start** button, type *mmc* in the search box and press the **Enter** key to start the *Microsoft Management Console*.
  - ⇒ The *Console 1 - [Console Root]* dialog is displayed.
2. From the **File** menu, select **Add/Remove Snap-in** to display the *Add/Remove Snap-ins* dialog.
3. From the **Snap-in** list box on the left hand side, select **Certificates**.
4. Click the **Add >** button.
  - ⇒ The *Certificates snap-in* dialog is displayed.
5. Select **Computer Account** and click **Next**.
  - ⇒ The *Select Computer* dialog is displayed with the option **Local computer: (the computer this console is running on)** selected by default.
6. Click **Finish**.
  - ⇒ The *Add/Remove Snap-ins* dialog is displayed again with the **Console Root snap-in** tree listing **Certificates (Local Computer)** on right hand side of the list box.
7. Click **Ok** to close the dialog.
8. In the left pane of the Microsoft Management Console dialog, expand the **Certificates (local computer)** tree as below:
  - Personal
  - Certificates
  - ⇒ The certificate added by you will be displayed in the right section of the window.
9. Double click this certificate.
  - ⇒ The *Certificate* dialog is displayed.
10. Go to the *Details* tab and scroll down.
11. Click **Thumbprint** from the displayed fields.
  - ⇒ The thumbprint of the machine certificate of this Remote Client computer is displayed in the box below.
12. Select and copy the thumbprint value. Open any text editor and paste it there.
13. Remove all spaces manually.
  - ⇒ **Note:** Ensure each and every space is removed before proceeding further.
14. Save this as a text file and copy this file securely to the server computer. Remember to permanently delete this file once it is no longer required.

### 5.4.2.2 Adding the Remote Client in SiPass Server

In this step, the remote client certificate thumbprint from the previous step is used to add that computer as a trusted client in the server computer.

**Prerequisite:** To generate Client certificates through the SiPass integrated Configuration Client, the client must be run locally with the SiPass integrated server.

**On the SiPass server computer:**

1. Run the SiPass integrated *Configuration Client*.
2. From the **System** menu, click **Client Configuration ...**  
⇒ The *Client Configuration - New* dialog is displayed.
3. Type the name of the computer (where SiPass integrated client will be installed) in the **Full computer name** field.  
⇒ **Note:** If the Remote Client computer is connected to SiPass server computer through a VPN connection, tick the **Only check thumbprint for authentication** checkbox.
4. Paste the thumbprint of the remote client computer (from the previous steps) in the **Certificate Thumbprint** field.
5. Click **Save**.

The Client Computer is listed on left hand side of the *Client Configuration - New* dialog. To delete an existing Client Configuration, select it from the left pane of the dialog and click **Delete**.

### 5.4.2.3 Saving Server Thumbprint for the Remote Client

In this step, the certificate thumbprint of the server computer is saved for setting it up as the server during the remote client installation (in next section).

**Continuing the steps from the previous section...**

1. Click the **Save Server thumbprint...** button and specify an empty folder to save the server certificate's thumbprint into a file which can be used while selecting Certificates for remote client.
2. Click **Close** to close the *Client Configuration - New* dialog.

#### 5.4.2.4 Installing a SiPass integrated Remote Client with Machine Certificates

1. Follow the procedure to start the SiPass integrated installation.
2. Fill in the *Options* dialog with the same details as the original installation.
3. Click **Next** to continue.
4. Select **Custom** and click **Next** to continue to the *Select Features* dialog.
5. Select only the Client option(s) you are installing.
  - The Configuration Client and Operation Client can be installed and run on any local or remote client computer. **However, when the high-security installation option is selected, only the SiPass Configuration Client on Server site can connect to the SiPass integrated server.**
  - The HR-API Core must be installed on the computer where the HR application or the HR application gateway is installed.
  - Ensure that the SiPass integrated Server option is marked with a red cross (described as *This feature will not be available.*) so that the server will NOT be installed.
  - Ensure other items in the dialog are also marked with a red cross.
6. Click **Next**.
  - ⇒ The *SiPass integrated Server* dialog will appear.
7. Type the full name or IP address of the SiPass integrated Server computer in the **Server** field. **Ensure that the port numbers on this dialog are exactly the same as for server installation.**
  - ⇒ **Note:** Unless a server name is provided in this field, the installation process will not proceed.
8. Click **Next**.
  - ⇒ The *Ready to Install the Program* dialog will appear.
9. Click **Install**.
  - ⇒ The SiPass integrated Client installation will proceed and the progress indicator will appear.
  - ⇒ After completion, the *Authentication Management Wizard* is displayed where a certificate can be selected/imported. This is the same certificate saved in the section Saving Server Thumbprint for the Remote Client [→ 43] that was saved separately in an empty folder of your choice.
  - ⇒ **Note:** The Authentication Management Wizard can also be run to add/renew the certificate on an installed remote client. Double-click the *SiPass.CertificatePicker.exe* file from the SiPass integrated installation directory on the computer where SiPass integrated client is installed and follow the process as mentioned below.
10. Continue with the steps described in the next section.

### 5.4.2.5 Adding the Server Certificate to the Remote Client

On the Authentication Management Wizard screen,

1. Click **Next**.  
⇒ The *Authentication management* dialog is displayed.
2. Tick the **Import Client & Server Certificates From** checkbox.
3. Click the folder icon next to the field and locate the folder that contains the Server Certificate and Thumbprint files generated earlier on the server.
4. Click **Finish**.  
⇒ The certificate is applied and the following message is displayed: *The certificate has been successfully applied to SiPass Client*.
5. Click **OK** to close the message.  
⇒ The SiPass integrated installation is continued. When completed, the *Setup Complete* dialog will appear.
6. Click **Finish**.  
⇒ Congratulations! You have now successfully installed SiPass integrated on the client computer.

**Note:**

- You can also load another Server Certificate Thumbprint for authenticating SiPass server on the client. To do this, run the *Authentication Management Wizard* and edit the pre-filled Server **Certificate Thumbprint** field filling-in the thumbprint value of that server computer, or locate a thumbprint file for that server computer stored separately.
- The permissions to the selected/imported certificate have been granted to both the current user and local Administrators. If the SiPass Client will be run by other users on this computer who are not System Administrators, then these users must be granted Read permissions (at least) to the certificate private key so they can be assigned additional privileges, if required later. See section Assigning privileges to Certificate Private Key [→ 36].

## 5.5 Certificate Expiry and Renewal

Every certificate has a validity period after which, it expires and must be renewed. This is to ensure that existing certificate information gets replaced with new one after regular intervals and security is maintained at all times.

Using the *SiPass Authentication Management* tool, you can renew a certificate on SiPass Server and Local Clients installed on a single computer, or on any SiPass integrated Remote Clients installed on separate computers.



SiPass integrated Server / Client starts giving you **warning messages 30 days prior to the certificate's expiry date**. You can close the message and log on to the system but you will keep getting reminders about renewing the certificate.

If you do not renew the certificate in 30 days, you will not be able to log on to SiPass integrated after the certificate has expired. You **MUST** renew the certificate in this case.

If the certificate of the Server for a Remote Client has expired, starting up the client will give you an error message about Server not being available. In this case, the Server Certificate must be renewed to work with this remote Client.

### 5.5.1 Renewing the Certificate on SiPass Server

1. Go to the SiPass integrated installation folder on the computer.
2. Right-click the *SiPass.CertificatePicker.exe* file and select the **Run as Administrator** option from the menu.
  - ⇒ The *Authentication Management* dialog is displayed.
3. Click **Next**.
  - ⇒ A message is displayed informing you that the SiPass integrated service will be stopped before making any changes.
4. Click **OK** and wait for the service to close.
5. To generate and install a self-signed certificate, tick the **Generate Self-Signed Certificate** checkbox.
  - ⇒ OR
6. Select your own certificate from the available certificate list on the screen.
  - ⇒ **Note:** If you select a certificate having expiry date in the next seven days, a warning message is displayed. Click **OK** to close the message and select another certificate.
7. Click **Finish**.
  - ⇒ A message is displayed asking if you wish to copy Windows Account Permissions from the previous certificate to the new certificate.
8. Click **Yes** if you want to import the permissions else click **No** and set the permissions yourself later.
  - ⇒ Now a message asks you if you wish to remove the existing (expired) certificate from the system.
9. Click **Yes** to remove it or **No** to keep it on the system.
  - ⇒ The new certificate is generated and applied to the SiPass server and any local clients. A message is displayed confirming that the certificate has been successfully applied.



---

If you have performed this operation on a computer that has SiPass Server installed, the message will also mention that the certificate configuration on Remote Clients should also be updated.

Follow the steps given in the next section to update the Remote Client certificate information.

---

10. Click **OK** to close the message.
  - ⇒ Another message will ask you if you wish to restart the SiPass Service on this computer.
11. Click **OK** to restart the SiPass service or **No** to close the message without restarting the service.

### 5.5.1.1 Generating New Certificates for Remote Client

Each Remote Client has its unique thumbprint. After renewing the certificate of the SiPass server, the thumbprint must also be updated in each Remote Client to authenticate the server again.

**Follow the steps below to generate new certificates for the SiPass Remote Clients.**

1. Right-click on the SiPass integrated Configuration Client icon on the computer where SiPass server is installed and select **Run as Administrator**.
2. From the **System** menu, click **Client Configuration ...**
  - ⇒ The *Client Configuration - New* dialog is displayed. The existing Remote Clients for this SiPass server will be listed on the left pane on the dialog.
3. Click the **Generate All Self-Signed Certificates...** button.
  - ⇒ A message appears informing you that this step will generate self-signed certificates for all client records in the system, and update the thumbprint entries. It also asks if you wish to proceed with this step.
4. Make a choice **as desired**:
  - ⇒ If you click **Yes**, no further steps are required.
    - Proceed to Step 5.
  - ⇒ If you do not want to generate certificates for all clients at once and click **No**. In this case:
    - Select the Remote Client name from the left pane on the dialog. The **Full computer name** and **Certificate Thumbprint** fields will be populated with the information for that computer.
    - Click the **Generate Self-Signed Certificate** button.
    - Proceed to step 5.
5. When prompted, select a destination folder for saving the new client certificates. Sub-folders will be created inside this folder based on the client computer name. The functionality makes it easier to generate all client certificates in one go after expiry when server certificate is renewed.
  - ⇒ A message informs you that the certificate generation process has completed.
6. Click **OK**.
  - ⇒ The new client certificates will be available in the respective sub-folders inside the main folder you specified earlier. Now you can copy these certificates to individual client computers and authenticate. See section [Renewing the Certificate on SiPass Remote Client \[→ 47\]](#).
7. Click **Close** to close the *Client Configuration – New* dialog.

## 5.5.2 Renewing the Certificate on SiPass Remote Client

Each Remote Client has its unique thumbprint. After updating the Certificate information for SiPass Server, you must now update this in the existing remote Client Computer also to ensure both remain mutually-authenticated.

1. Go to the SiPass integrated installation folder on the Remote Client computer.
2. Right-click the *SiPass.CertificatePicker.exe* file select the **Run as Administrator** option from the menu.
  - ⇒ The *Authentication Management* dialog is displayed.
3. Click **Next**.
4. Click the folder icon next to the **Import Client & Server Certificate From** field.
5. Locate the folder created for saving the new certificates in the Generating New Certificates for Remote Client [→ 46] section. Select the sub-folder inside this that has the name of the Remote Client computer for which, you are currently renewing the certificate.
6. The **Import Client & Server Certificate From** field will be populated with the location of this folder.
7. Click **Finish**.
  - ⇒ A message is displayed asking if you wish to copy Windows Account Permissions from the previous certificate to the new certificate.
8. Click **Yes** if you want to import the permissions else click **No** and set the permissions yourself later.
  - ⇒ Now a message asks you if you wish to remove the existing (expired) certificate from the system.
9. Click **Yes** to remove it or **No** to keep it on the system.
  - ⇒ The new certificate is generated and applied to the remote client. A message is displayed confirming that the certificate has been successfully applied.
  - ⇒ It also informs that this Remote Client must be authenticated again in the SiPass system by updating the certificate configuration on SiPass integrated server computer through the Configuration client. The thumbprint of the new certificate of the Remote Client computer is also given in the message box which can be copied for authenticating in the server depending on the scenarios as below:
    - ⇒ **Scenario 1:** If you updated the certificate configuration in SiPass Server first and then authenticated the client, you do not need to perform any additional step.
      - Click **OK** to close the message.
    - ⇒ **Scenario 2:** If you updated the certificate configuration in the Remote Client computer first, the thumbprint for this client must also be updated in the server to authenticate the client again as genuine client for that server. Go to section Updating Remote Client Certificate Thumbprint in SiPass Server [→ 48] for the next steps.
      - Copy the Certificate Thumbprint for the Remote Client and save it locally.
      - Click **OK** to close the message.



### 5.5.2.1 Updating Remote Client Certificate Thumbprint in SiPass Server

On the SiPass server computer:

1. Run the SiPass integrated Configuration Client.
2. From the **System** menu, click **Client Configuration ...**
3. The *Client Configuration - New* dialog is displayed.
4. Select the name of the computer (where SiPass integrated client is installed and for which, you are currently updating the certificate configuration) from the list of Remote Clients in the left hand pane of the dialog.
5. The **Full Computer Name** field is populated.
  - ⇒ **Note:** If the Remote Client computer is connected to SiPass server computer through a VPN connection, tick the **Only check thumbprint for authentication** checkbox.
6. Paste the thumbprint of the remote client computer (saved locally in the previous section) in the **Certificate Thumbprint** field.
7. Click **Save**.
  - ⇒ The Remote Client certificate information is updated.
  - ⇒ You can also delete an existing Client Configuration and add the Remote Client with the new certificate information as a new client.

## 5.6 Installing Additional Components

If you purchased additional components, or did not install all of the components that you purchased originally, you can install those components (for example, the Messaging module or an additional Bus) onto your existing SiPass integrated system.

During the installation of a new component, SiPass integrated will automatically complete the fields in the License dialogs with the components and features currently installed. The only details you need to change are the new license key, and those new components which have been purchased. If you are installing additional components, you may be asked for your SiPass integrated installation setup files during installation.

### To Install Additional SiPass integrated Components:

1. Select **Control Panel** from the Windows Start Menu.
2. Double click **Add or Remove Programs**.
3. The *Add or Remove Programs* window will appear.
4. Select **SiPass integrated** from the list displayed.
5. Click **Change**.
  - ⇒ The *Application Maintenance* dialog will appear.
6. Select the **Modify** option.
  - ⇒ The *Hardware Type* dialog will appear.
7. Select the same hardware type as the installation to which you are adding a component.
8. Click **Next**.
  - ⇒ The *License Options* dialog will appear.
9. Enter the new License Key you obtained when ordering the additional component(s), as well as any changes made to the details in this dialog.
10. Click **Next**.
  - ⇒ The second *License Options* dialog will appear.
11. Change only the fields where you have purchased additional components.
12. Click **Next**.
  - ⇒ The *Select Features* dialog will appear. Like the License dialogs, when installing additional components the SiPass integrated Install Wizard will complete the dialog with the details of the current installation.
13. Select any additional features that you are installing for the first time.
14. Click **Next**.
  - ⇒ The *Ready to Modify* dialog will appear.
15. Click **Next**.
  - ⇒ The SiPass integrated installation will proceed, and the progress indicator will appear. After completion, the *Setup Complete* dialog will appear.
16. Click **Finish** to complete the installation.
17. Click **Yes** to restart the SiPass Service.
  - ⇒ **Note:** The changes you have made will be functional ONLY after the SiPass service is restarted.

## 6 Installing SiPass integrated Web Site

The sections of this chapter detail how to install the SiPass integrated Web Server in a separate machine.

### 6.1 Pre-Installation Checklist

This section provides details of a Pre-Installation Environment that should ideally be prepared for the SiPass integrated Web Server.

- **Internet Information Services (IIS):** With SiPass integrated MP2.80 onward, IIS is installed and enabled automatically if SiPass Website feature is installed.  
  
If you choose to install it manually later, see the IIS Installation Instructions [→ 51] section for details, or contact your IT administrator for IIS Setup support. The IIS installation must be done by a user with local administrator permissions.
- The Firewall should be configured to allow inbound connection for port 5443 (the default HTTPS port used by SiPass Web Site).



---

#### Web Site feature and Certificates

If you choose to generate a self-signed certificate during SiPass integrated installation and connect to the SiPass Web Site using a browser (on a PC that does not have a SiPass client installed), the web site certificate will not be trusted in this case and a warning will be shown. Depending on the browser, you may not be able to proceed with using the SiPass web site.

To prevent this from happening, it is recommended that if you are using the SiPass Web Site feature, an existing official certificate (either predefined company certificate, or official purchased certificate) is selected during the SiPass integrated installation.

---

#### 6.1.1 IIS Installation Instructions

This section provides instructions about *how* to install Internet Information Services (IIS) for the SiPass integrated Web Server.

Supported Operating Systems
Windows Server 2019
Windows Server 2016
Windows 10

**IIS Installation for Windows Server 2016 and Windows Server 2019**

1. Start the operating system on the workstation where the SiPass Server software is to be installed.
2. Open **Server Manager**.
3. In the **Configure this local server** menu, select **Add Roles and Features**. The *Add Roles and Features Wizard* displays.
4. Click the next button, select **Role-based or Feature-based Installation**.
5. Click the next button, select the destination server (local is selected by default).
6. Click the next button, select the **Web Server (IIS)** checkbox.
7. Click the next button, select the latest version of **.NET Framework Features** checkbox (if not selected by default).
8. Click **Next**, to confirm the Installation Selection.
9. Click **Install**.
  - ⇒ When the IIS installation completes, the wizard reflects the installation status.
10. Click **Close** to exit the wizard.


**IIS Installation for Windows 10**

1. Start the operating system on the workstation where the SiPass Server software is to be installed.
2. From the Windows **Start** menu, click **Settings**.
3. When the Windows *Settings* screen is displayed, click **System**.
4. On the *System* dialog, click **Apps & features**.
  - ⇒ The Apps currently installed in the computer are displayed on the right side.
5. Scroll down till the end and click **Programs and Features** under the *Related Settings* heading.
  - ⇒ **Note:** Alternatively, you can click the **Search** icon in the Windows Taskbar and search for Control Panel. Click **Control Panel** from search results and from the *Control Panel Items* dialog, click **Programs and Features**.
  - ⇒ The *Programs and Features* dialog is displayed.
6. On the left panel, click *Turn Windows features on or off*.
  - ⇒ The *Windows Features* dialog is displayed.
7. Enable **Internet Information Services** feature by selecting the **Internet Information Services** checkbox.
8. Expand **Internet Information Services > World Wide Web Services > Application Development Features**
9. In **Application Development Features**, enable the following features by selecting the respective checkboxes:
  - .NET Extensibility
  - ASP.NET
  - ISAPI Extensions
  - ISAPI Filters
10. Click **OK**.
  - ⇒ The IIS Setup configuration is complete.

To install SiPass integrated, right-click the SiPass **Setup.exe** file and select **Run as administrator** to begin installation.

## 6.2 Web Site Setup

The SiPass Web Site (Web Server) Setup is the main pre-requisites to using the SiPass Web Client.

	<b>NOTICE</b>
	<p>In the SiPass integrated server machine, an entry is made in the following path, ...\\Windows\\System32\\drivers\\etc\\hosts config, for the proper functioning of the SiPass integrated web application.</p> <p>Consequences</p>

There are two setup options available for installing the SiPass Web Site. These options allow you to access the SiPass server from the internal local network, or externally (e.g., from the Internet).

The client count is a combination of both servers.

- **Setup A: Installing a Local SiPass Web Site**  
With this option, the SiPass Web Server can be installed on a Local SiPass Server.
- **Setup B: Installing an Independent SiPass Web Site**  
With this option, the SiPass Web Site is installed on another server within the same subnet with IIS installed, but independent of the SiPass Server which is installed on a LAN network. This independent SiPass WEB Server can be published to the Internet, thus protecting the SiPass Server from Internet attack. Configuration of the firewall would generally be carried out by the IT department of SiPass integrated customer.



For both single box and multiple box installation, it is mandatory to restart the machine for which the OS type is **Windows Server 2016** and **Windows 10**.

## 6.2.1 Local SiPass Web Site Installation

Follow the instructions of how to perform a SiPass integrated Installation. For more information, refer the section Installing SiPass integrated.

1. Perform the SiPass integrated installation as described in this document till you see the *Setup Type* dialog.
2. Select **Custom**, and click **Next** to continue to the *Select Features* dialog.
3. Ensure that **Server**, is selected. Click the drop down arrow of this icon to select further options.
4. Ensure that **Client** is selected. Click the drop down arrow of this icon to select further options.
5. Ensure that **Web site** is selected.
6. Click **Next**. Click **Next**. Configure the setup of the *SQL Options* dialog that will appear, as in a standard installation setup.
  - ⇒ The *MongoDB and RabbitMQ Configuration* dialog is displayed (See section Remote MongoDB and RabbitMQ Configuration for more information).
7. Click **Next** to go ahead with no changes (default values are used), or enter the details as below:
  - **MongoDB**
    - **Server** – Provide the full computer name where MongoDB is installed.
    - **Username** – Provide the username to connect with MongoDB.
    - **Password** - Provide the password to connect with MongoDB.
  - **RabbitMQ**
    - **Server** – Provide the full computer name where RabbitMQ is installed.
    - **Username** – Provide the username to connect with RabbitMQ.
    - **Password** - Provide the password to connect with RabbitMQ.

When you have entered the required values on the MongoDB and RabbitMQ Configuration dialog, the *Ready to Install the Program* dialog is displayed. You will be prompted to confirm that you want to continue the installation.

- ◇ Click **Install**.
- ⇒ The installation will proceed and the installation progress indicator will appear. When completed, the *Setup Complete* dialog will appear.
- ◇ Click **Finish**.
- ⇒ Congratulations! You have now successfully installed SiPass integrated with the Web Server (Web Site).

## 6.2.2 Independent SiPass Web Site Installation

Follow the instructions to install SiPass integrated web site on a separate computer from where the SiPass Server is installed.

**Prerequisite:** A server certificate must be saved earlier for importing to the Client Computer on which, the Web Site is being installed. See below:

To generate a self-signed certificate for the remote computer	<a href="#">Click here</a>
To generate a machine certificate for the remote computer	<a href="#">Click here [→ 43]</a>

1. Perform the SiPass integrated installation as described in this document till you see the *Setup Type* dialog.
2. Select **Custom**, and click **Next** to continue to the *Select Features* dialog.
3. Deselect the **Server** feature. To do this, click the **Server** icon drop down arrow, and select the **This feature will not be available** option.
4. You can also select a **Client** if required.
5. Ensure that **Web site** is selected.
6. Click **Next**.

⇒ *The SiPass integrated Server* dialog is displayed.

7. In the **Server** field, enter the SiPass Server computer name or IP address.

The *MongoDB and RabbitMQ Configuration* dialog is displayed (See section Remote MongoDB and RabbitMQ Configuration for more information).

Click **Next** to go ahead with no changes (default values are used), or enter the details as below:

### MongoDB

**Server** – Provide the full computer name where MongoDB is installed.

**Username** – Provide the username to connect with MongoDB.

**Password** – Provide the password to connect with MongoDB.

### RabbitMQ

**Server** – Provide the full computer name where RabbitMQ is installed.

**Username** – Provide the username to connect with RabbitMQ.

**Password** – Provide the password to connect with RabbitMQ.

When you have entered the required values on the MongoDB and RabbitMQ Configuration dialog, the *Ready to Install the Program* dialog is displayed. You will be prompted to confirm that you want to continue the installation.

1. Click **Next**.
  - ⇒ The Authentication Management Wizard is displayed. Click **Next**.
  - ⇒ The *Authentication Management* dialog is displayed.
2. Tick the **Import Client & Server Certificates From** checkbox.
3. Click the folder icon next to the field and locate the folder that contains the Server Certificate and Thumbprint files generated earlier on the server.
4. Click **Finish**.
  - ⇒ A message in the bottom left corner of the *Authentication management* dialog is displayed, informing you that the certificate is being applied. The other actions on the dialog are disabled till you see a message confirming that the certificate has been applied to SiPass integrated server and any local client selected for installation.
5. Click **OK** to close the message.
  - ⇒ The SiPass integrated installation is continued. When completed, the *Setup Complete* dialog will appear.
6. Click **Finish**.
  - ⇒ Congratulations! You have now successfully installed SiPass integrated Web Site.

Note:

You can also load another Server Certificate Thumbprint for authenticating SiPass server on the client. To do this, run the *Authentication Management Wizard* and edit the pre-filled **Server Certificate Thumbprint** field filling-in the thumbprint value of that server computer, or locate a thumbprint file for that server computer stored separately.



## 7 SiPass integrated Web Client

### 7.1 Post Installation Procedure

After the installation of the SiPass integrated Web UI Client the user has to provide the following information in IIS:

1. On the **Start** menu, click **All Programs**, point to **Accessories**, and then click **Run**.
2. In the Open box, type **inetmgr** and then click **OK**
  - ⇒ A confirmation message displays as **Do you want to allow the following program to make changes to the computer?**
3. Click **Yes**
  - ⇒ The **Internet Information Services (IIS )Manager** dialog box displays.
4. Click **Sites** to expand the tree view and click **SiPass**.
  - ⇒ The **SiPass Features View** displays.
5. Perform the following instructions for **MIME Types**.

#### MIME Types

If **MIME types** are not available in the **IIS** folder, follow the below steps to add the MIME types:

1. Select and double click on the **MIME Types**.
2. The **MIME Types** display.
3. Right-click on the **MIME Type** and click **Add**.
4. The **Add MIME Type** dialog box displays.
5. Enter the **File name extension** as **.json**.
6. Enter the **MIME type** as **text/jscript**.
7. Click **Ok** to save the entered settings.
  - or...
8. Click **Cancel** to cancel the process.

#### Directory Browsing

In **Directory Browsing** ensure that the **Directory Browsing** is disabled. If it is not disabled, perform the following instructions:

1. Select and double click on the **Directory Browsing**.
  - ⇒ The **Directory Browsing** screen displays.
2. Click the **Disable** button on the **Action** pane.
  - ⇒ The **Directory Browsing** is disabled.

### 7.1.1 Enabling the HTTPS Security Communication for neXus SDK

The default port number for nexus sdk https communication is 54881.

### 7.1.2 Enabling the Secure Communication for RabbitMQ and MongoDB

RabbitMQ and MongoDB communications are secured with SiPass integrated Self-Signed Certificate. However, if user chooses an external certificate from a vendor, the certificate private key should be exportable from the Windows certificate store.

If the certificate private key is not exportable, you have to update the certificate private key in the following file,

```
<InstallationPath>\SiPass integrated\Web UI API\SiPass
integrated WebUIAPI\ActivityFeed\Certificate\server_key.pem
```

```
<InstallationPath>\SiPass integrated\Web UI API\SiPass
integrated
WebUIAPI\ActivityFeed\Certificate\server_certificate_key.pem
```

```
Example : C:\Program Files (x86)\SiPass integrated\Web UI
API\SiPass integrated
WebUIAPI\ActivityFeed\Certificate\server_key.pem
```



If the private key file is unavailable, self-signed certificate must be consumed.

### 7.1.3 Considerations in launching the SiPass integrated Web Client application

Before launching the application, if there is an existing SiPass integrated certificate, user has to ensure that the existing certificate is deleted.

#### To delete the existing SiPass integrated Certificate:

1. Click **START > Run**, type **mmc** in the Open field, and click **OK**.
  - ⇒ A message **Do you want to allow the following program to make changes to the computer?** displays.
2. Click **Yes**.
  - ⇒ The **Console -1 [Console Root]** dialog box opens.
3. In the tree view, click **Console Root** folder.
  - ⇒ The **Certificates (Local Computer)** displays.
4. Under **Certificates (Local Computer)**, click the **Trusted Root Certification Authorities** folder.
  - ⇒ The **Certificate** folder displays.
5. Double click the **Certificate** folder.
  - ⇒ The **Certificate** displays.
6. Right click the self-signed Sipass certificate and click **Delete**.
  - ⇒ The **Certificate** is deleted.

### 7.1.3.1 Launching the SiPass integrated Web Client application

User can launch the application through the following browsers: **Chrome** and **Firefox** using windows operating system. It is recommended to clear the Browser history before launching the SiPass integrated web client.

#### Steps to launch the application using different browsers:

Launching the application with different browsers have visible changes, however, it allows the user to access all the features, regardless of which browser they use.

##### Chrome

1. Browse with the certificate name and the port number that is specified for the Https binding. Eg:  
`https://<certificatename>:<sipassurlrouterportnumber>/sipass/`. Certificate name is the full computer name where the SiPass integrated Server is installed.



#### **NOTICE**

If user has their own certificate, the certificate name can be the full computer name where the SiPass integrated Server is installed.

2. Click **Advanced** and then click **Proceed**.  
⇒ System displays the content of the Language and image in the Login screen. User can now proceed with the login.

##### Firefox

If user browses with the certificate name and the port number that is specified for the Https binding. Eg:  
`https://<certificatename>:<sipassurlrouterportnumber>/sipass/`

1. Advanced dialog box opens.
2. Click Proceed/Add Exceptions.  
⇒ Login screen displays a message as Unable to connect to the SiPass server.
3. In a new tab, enter the link  
`https://<certificatename>:<sipassurlrouterportnumber>/sipass/api/` product and click Advanced and then click Proceed/Add Exceptions.
4. Refresh the login screen.  
⇒ System displays the content of the Language and image in the Login screen. User can now proceed with the login.

## Exporting and Importing Certificate

To counter the error message, user must export the certificate from the machine where the SiPass server is installed and import certificate in client machine.

1. Open **Run**, type *mmc*.  
⇒ The console window opens.
  2. Click **File** and select **Add/Remove Snap-in** from the drop down list.  
⇒ The **Add/Remove Snap-ins** window opens as shown below.
  3. Select **Certificate** from the **Available Snap-ins** list.
  4. Click **Add**, the **Certificate snap in** window opens.
  5. Select the **Computer account** option button from the list.  
⇒ The **Select Computer** window opens as shown below.
  6. By default, the **Local Computer** option button is selected.
  7. Click **Finish**. The certificate is added.
  8. Click **OK**, you can view the certificate in the console window.
  9. Expand the **Trusted Root Certification Authorities** node.
  10. Click **Certificates**, the certificates are listed.
  11. Right click on the certificate used for SiPass integrated, select **All Tasks** and click **Export** as shown below.
  12. **Certificate Export Wizard** opens, click **Next**.
  13. By default, **No, do not export the private key** option button is selected, click **Next**.
  14. The **DER enclosed binary X.509 (.cer)** type is selected, click **Next**.
  15. Enter the File Name and click **Browse**, to select the path.
  16. Select the path and click **Save**.
  17. The path gets selected, click **Next**.
  18. The export is completed.
  19. Click **Finish**.  
⇒ A confirmation message displays.
  20. Click **OK**.
- The exported certificate must be installed in the client machine working in Windows 10 operating system.
1. Open the Exported certificate from the local folder.  
⇒ The **Certificate** dialog box gets opened as shown below.
  2. Click the **Install Certificate** button.
  3. In the dialog box below, select **Local Machine** as the store Location.
  4. Click **Next**.
  5. Select the **Place all certificate in the following store** option.
  6. Click **Browse**, to select the **Trusted Root Certification Authorities** store
  7. Click **Next**.
  8. Click **Finish**.
  9. The certificate is imported successfully.

## Deployment Scenarios

### Single box installation

If SiPass integrated server along with SiPass URL Router and SiPass integrated Web UI hosted in IIS are installed in a single machine, the SiPass integrated installer will generate a self-signed certificate. The self-signed certificates are important to maintain secured communication between client and server.

The certificate that is generated will be applied to the SiPass server and SiPass integrated Web UI automatically.

### Certificate - Expired

If the certificate is expired, the certificate becomes invalid, and user will be prompted with the following messages.

During login, if SiPass certificate is expired, a message will be notified as:

**SiPass: 'SiPass integrated server certificate validity expired'** in the SiPass integrated web application. In addition, it does not allow the user to login.

During middle of any operation, if SiPass certificate is expired, the same message is notified as above. In this case, the user has to logout of the application.

### Certificate - About to Expire

#### SiPass

During login, an expiration notification message is displayed in the SiPass integrated web application - notification bar, 7 days before expiration, to let the user know that the specific certificates are about to expire.

**'SiPass integrated server certificate validity going to expire on <Date Time>'. Please contact Administrator. Incase left unattended, then user cannot login to web client.**

### Multiple box installation

#### Scenario

SiPass integrated server along with SiPass URL Router and SiPass integrated Web UI API are installed in a separate machine and SiPass integrated Web UI hosted in IIS are installed in a separate machine.

### Certificate - Expired

The same certificate is used in the SiPass integrated server and SiPass integrated Web UI. In this case, if the SiPass certificate is expired, a message will be notified as **'SiPass integrated server certificate validity expired'** in the SiPass integrated web application. In addition, it does not allow the user to login.

### Certificate - About to expire

If the SiPass certificate is about to expire, the expiration notification message is displayed in the SiPass integrated web application - notification bar, 7 days before expiration, to let the user know that the specific computer certificates are about to expire.

**'SiPass integrated server certificate validity going to expire on <Date Time>'. Please contact Administrator. Incase left unattended, then user cannot login to web client.**

If the user is using the Sipass server certificate or a different self-signed certificate in IIS, the administrator has to manually update the certificate on expiring or going to expire.



No message is notified regarding validity of the certificate to the user.

## neXus

In neXus, if the certificate is expired or going to expire, the Administrator needs to verify the validity of the neXus certificate and update the certificate accordingly.



No message is notified for neXus certificate validity.

The user is not restricted from working, even if the certificate is expired.

### 7.1.4 Installing the neXus SDK

The SiPass application requires neXus SDK to capture image and signature. Install the neXus SDK in the target machine where the SiPass web client is accessed.

#### To install neXus SDK Utility:

1. Navigate to the ISO path: `..\<Product version>_EN\Tools\neXusSDK`
  2. Run the **neXusSDK.exe** file.
- ⇒ The neXus SDK installation is complete.

	<b>NOTICE</b>
	Refer to neXus SDK manuals (which is available in the neXus SDK installation directory) to know more about <b>How to configure basic settings</b> .  Refer to the SiPass integrated web client User guide to know more about usage of SiPass application along with neXus SDK.

#### 7.1.4.1 Launching the neXus SDK

neXus SDK can be launched through the following browsers: **Chrome** and **Firefox**.

For the SiPass web client application to communicate with the nexus application, the Nexus URL <https://localhost:neXusport> should be launched atleast once in the browser where the SiPass web client is used.

	<b>NOTICE</b>
	neXusport - The port specified for https binding of neXus SDK during installation.

	<b>NOTICE</b>
	Exceptions needs to be handled for different browsers in the same way as mentioned above in the section <i>Steps to launch the application with different browsers</i> on page [→ 58].

After the exceptions are handled, system displays the status of the neXus card SDK API.

### 7.1.5 Data Retention in Activity Feed

By default, the data will be retained in **Activity Feed** for seven days. However this default seven days settings can manually be changed by following the procedure given below:

- Logon windows with the run-time account used for SiPass installation.

- Open command prompt and execute the below command

```
C:\>setx SISUITE_ACTIVITY_FEED_STORAGE_RETENTIONTIME  
"NO_OF_DAYS"
```

- Set the retention days in the "NO\_OF\_DAYS" field.

As the default setting is changed, you must restart the **Siveillance Activity Feed** from the service console to view the applied changes.

The data is automatically purged based on the retention period (in days) set sequentially based on times tamp value it was created.



#### **NOTICE**

After upgrading the SiPass integrated system, the default value gets updated in **PersistenceStorage\_RetentionTime** attribute.

### 7.1.6 Restarting SiPass integrated Web Client Server Machine for More Number of Access Area

For more\* number of Access Area in site, user can restart the SiPass integrated web client Server PC, as there is change made to the registry to accommodate the increased HTTP header size (32KB).

This applies for all the operating systems.

The registry value gets changed as shown below:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters]
```

```
"MaxRequestBytes"=dword:00008000
```

*more\* is approximately > 100 areas*

## 7.2 RESTful API Services

- Restarting the SiPass server service, will restart the Web UI API automatically.
- Stopping and Starting the Sipass Server service will require the Web UI API and its dependency services to start manually. Following are the dependency services:
  - Apache Tomcat 9.0 Tomcat\_SiPassintegrated
  - MongoDB\_SiPassintegrated
  - RabbitMQ\_SiPassintegrated
  - SiPass integrated Web UI API
  - SiPass integrated Activity Feed Interface
  - SiPass integrated PACS Management
  - SiPass integrated Unified Area Monitoring
  - SiPass integrated - Siveillance Dynamic UI
  - SiPass integrated - Siveillance Activity Feed
  - SiPass integrated - Siveillance Unified User Management
  - SiPass integrated UUM Interface
- When the SiPass server service is stopped first, the Web UI API, Management Station API, and the HR API service will be prompted to stop automatically.

### 7.2.1 Deployment Instructions

The following deployment instructions are common for all the RESTful services: Web UI API, HR API, and MS API.

- The firewall exceptions related to the application (if found) needs to be accepted.
- The inbound and outbound ports needs to be configured in order to access the API.
- Firewall block for the hosting URL and port needs to be changed accordingly.


### 7.2.2 Starting, Stopping, and Disabling SiPass integrated webclient services

While the SiPass integrated webclient is not under use, it is recommended to **Stop** and set the **Startup** Type as **Disabled** for the below mentioned webclient services in any order.

1. Apache Tomcat 9.0 Tomcat\_SiPassintegrated
2. MongoDB\_SiPassintegrated
3. RabbitMQ\_SiPassintegrated
4. SiPass integrated Web UI API
5. SiPass integrated Activity Feed Interface
6. SiPass integrated PACS Management
7. SiPass integrated Unified Area Monitoring
8. SiPass integrated - Siveillance Dynamic UI
9. SiPass integrated - Siveillance Activity Feed
10. SiPass integrated - Siveillance Unified User Management
11. SiPass integrated UUM Interface



## 7.3 Security Risk

	<b>⚠ WARNING</b>
	<p><b>Following are the recommendations to maintain data privacy:</b></p> <p>Access the SiPass web client in a restricted environment.</p> <p>Disable the <b>Manage Autofill settings</b> and <b>Manage Passwords features</b> in browser settings.</p> <p>Enable the <b>Set Your Computer to Lock Your Screen Automatically</b> feature in the Computer in which the SiPass integrated web client is browsed.</p> <p>The UAA default credentials can be modified in the <b>Unified User Management - Change Password</b> screen, however, the same needs to be updated in the <b>Preferences</b> screen also, so that the operators, operator groups, and privileges can be synchronized to the underlying UAA. Refer to <i>SiPass integrated web client user guide</i> for more information.</p>

### Disabling Transport Layer Security (TLS) 1.0

1. Open the  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\ registry key
2. If TLS 1.0 key is available, click the key; or create a new key with the name TLS 1.0
3. If the TLS 1.0 key exists, it must have a key called 'Client' and one 'Server' underneath. If it is not available, then create them as described in the previous step.
4. The 'Client' and 'Server' keys must be disabled TLS 1.0. Navigate to the 'Client' key and create a DWORD (32 bit) entry and call this 'Enabled' by setting its value as 0. Repeat, and create a new DWORD (32 bit) entry for the 'Server' key and call it 'Enabled' by setting the value as 0. This will disable TLS (all versions) for both client and server.
5. After completing the steps above, reboot the system.

### Disabling Transport Layer Security (TLS) 1.1

1. Open the  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\ registry key
2. If TLS 1.1 key is available, click the key; or create a new key with the name TLS 1.1
3. If the TLS 1.1 key exists, the key must have a key called 'Client' and one called 'Server' underneath. If it is not available, create them as described in the previous step.
4. The 'Client' and 'Server' keys have to be disable TLS 1.1, Navigate into the 'Client' key and create a DWORD (32 bit) entry and call this 'Enabled' by setting its value to 0. Repeat, and create a new DWORD (32 bit) entry for the 'Server' key and call it 'Enabled' by setting the value to 0. This will disable TLS (all versions) for both client and server.
5. After completing the steps above, reboot the system.

## 7.4 Exporting the SiPass certificate

If user is using an external system, where SiPass certificate is not registered, then user has to perform the following procedure to export the certificate.

API's child and root certificate that are given during SiPass installation, needs to be given during exporting the certificate.

### To export the child and root certificate:

1. Click > **START > Run**, type **mmc** in the **Open** field, and click **OK**.  
⇒ A message **Do you want to allow the following program to make changes to the computer?** displays.
2. Click **Yes**.  
⇒ The **Console -1 [Console Root]** dialog box opens.
3. From the **File** menu, select and click **Add or Remove Snap-ins**.  
⇒ The **Add or Remove Snap-ins** dialog box opens.
4. From the **Available snap-ins**, select **Certificates** and click **Add**.  
⇒ The **Certificates snap-in** dialog box displays.
5. Select **My User account** and click **Finish**.  
⇒ The selected certificate gets added under the **Selected snap-ins**.
6. Click **OK**.

### For Child certificate

1. In the **Console -1 [Console Root]** window, on the left side tree view, click **Certificates - Current User** and choose **Personal Folder** from the **Logical Store Name**.
2. Right click **Personal Folder** and point to **All Tasks** and click **Import** and select **SipassChild.cer**  
⇒ The **Certificate Import Wizard** displays.
3. Click **Next**.
4. Browse the File name and click **Next** and click **Finish**.

### For Root certificate

1. On the left side tree view, click **Certificates - Current User** and choose **Trusted root certification authorities Folder** from the **Logical Store Name**.
2. Right click **Trusted root certification authorities Folder** and point to **All Tasks** and click **Import** and select **SipassRoot.cer**  
⇒ The **Certificate Import Wizard** displays.
3. Click **Next**.
4. Browse the **File name** and click **Next** and click **Finish**.  
⇒ Exporting child and root certificate is complete.

## 8 SiPass integrated Services

When you install the SiPass integrated software, few background services are installed to allow SiPass integrated to function correctly (even if the client is not active). These services allow access control events and communications with system controllers to be maintained, even when the SiPass integrated client is not running.

By default, the services start automatically when the workstation on which they are installed is switched on. If necessary, you may change the default settings and configure these services to start manually. You may also stop these services at any time.



---

You must have local administrator privileges to change service settings.

---

The services that run for the proper operation of SiPass integrated are given below. The list gives the names as displayed on the *Services* dialog. On selecting a service on the dialog, a description is also available for each of these services.

- SiPassServer
- SiPass integrated Activity Feed Interface
- SiPass integrated HR API
- SiPass integrated Management Station API
- SiPass integrated PACS Management
- SiPass integrated Unified Area Monitoring
- SiPass integrated UUM Interface
- SiPass integrated Web UI API
- SiPass OPC A&E Server
- SiPass To Open Processor Gateway
- SiPass integrated - Siveillance Activity Feed
- SiPass integrated - Siveillance Dynamic UI
- SiPass integrated - Siveillance Unified User Management

Following 3rd-party services are also installed during SiPass setup:

- SQL Server
- Apache Tomcat 9.0 Tomcat\_SiPassintegrated
- MongoDB\_SiPassintegrated
- RabbitMQ\_SiPassintegrated

The SiPassServer is installed during the SiPass integrated installation, while the SQLServer service is installed during the SQL Server installation.

You will also see the “*World Wide Web Publishing Service*”. This is the Internet Information Service (IIS) which is installed with Windows Operating System.

## 9 Uninstalling or Reinstalling SiPass integrated

The uninstall program will remove the SiPass integrated application, application drivers, registry settings and directories from your computer. Any programs installed as prerequisites are also uninstalled automatically.

It is highly recommended that you back up your SiPass integrated database before performing any of the maintenance procedures described in this chapter.



---

If the computer on which you are operating has the SiPass integrated Server installed, and you perform a **Modify** operation, the SiPass Server will be restarted.

SiPass integrated does not support the **Repair** option.

---

### To uninstall SiPass integrated:

1. Select **Control Panel** from the Windows Start Menu.
2. Double click **Add or Remove Programs**.
  - ⇒ The *Add or Remove Programs* window will appear.
3. Select **SiPass integrated** from the list displayed.
4. Click **Remove**.
  - ⇒ The *Application Maintenance* dialog will appear.
5. Click **Yes** to confirm, and the uninstall process will begin.
  - ⇒ **Note:** The SiPass service will be automatically stopped to perform the uninstall process.

## 10 Upgrading SiPass integrated

### 10.1 SiPass integrated Backup / Restore Path



#### IMPORTANT

Due to the technical advancements, SiPass integrated MP2.80 does not support system upgrade from previous versions. A fresh install is required for this version.

However, you can perform a **database backup/restore from the previous versions, and also within the earlier versions** (see table below). Note that this table does not represent *upgrade compatibility* among different versions of SiPass integrated, for which, you should contact the Siemens Technical Support for your region.

**Note:** You can always perform a backup and restore within the same version if performing a fresh install. For example, backing up MP2.80 database, uninstalling, re-installing MP2.80 and restoring the MP2.80 database.

Version Currently Installed	Version You Want To Restore To					
		MP 2.65	MP 2.70	MP 2.75	MP 2.76	MP 2.80
	MP 2.60	Yes	Yes	Yes	No	No
	MP 2.65*	Yes	Yes	Yes	Yes	Yes
	MP 2.70	No	Yes	Yes	Yes	Yes
	MP 2.75	No	No	Yes	Yes	Yes
	MP 2.76	No	No	No	Yes	Yes
	MP 2.80	No	No	No	No	Yes



\*In case of MP2.80, the database can be restored from MP2.65 Service Pack 4 onward.



#### Note

The time taken to upgrade to another version of SiPass integrated depends on the number of Cardholder images, Site Plans and Card templates.

## 10.2 Performing the Backup / Restore

If you are backing-up / restoring from a previous version of SiPass integrated, and wish to maintain your existing database, several steps need to be followed to ensure a smooth transition between versions.

Before you begin:

- Ensure that you have read the new version of SiPass integrated Release Notes.
- Ensure that your system meets any new requirements for the version you are planning to install.
- Ensure you are familiar with backing up and restoring the SiPass integrated database.
- Ensure that you have installed the **latest Hotfix / Patch** for the current version of SiPass integrated for which the backup is being performed.
- Back up all components of your current SiPass integrated database.

**Note:** The *System* and *Local*/backup/restore options are no longer available to ensure enhanced data privacy and security.



When backing up the SiPass integrated database, the **Audit Trail is not backed up automatically**. You must perform a **manual back up** to save the Audit Trail data.

If the currently installed version of SiPass integrated is earlier than MP2.65 SP4, you might need to install an **intermediate version** before restoring to MP2.80. Contact your Siemens support personnel for more information and help.

---



From SiPass integrated MP 2.76 SP2 onward, only the custom services as below are used:

**Apache Tomcat 9.0 Tomcat\_SiPassintegrated**


**MongoDB\_SiPassintegrated**

**RabbitMQ\_SiPassintegrated**

---

## 10.2.1 Steps

1. Perform the back up for the installed version of SiPass integrated.  
⇒ **Note:** Don't forget to install the latest Hotfix / Patch for this version before taking the backup.
2. Exit the SiPass integrated application. Ensure that all remaining SiPass integrated Services have been stopped.
3. Uninstall the current version of SiPass integrated. This **MUST** be done before installing the new version.

	<b>NOTICE</b>
	<p><b>Apache Tomcat</b></p> <p>While upgrading from 2.76 SP2 to 2.8, <b>Apache Tomcat 9.0 Tomcat_SiPassintegrated</b> server component must be manually uninstalled.</p> <p>Before version 2.76 SP2, if no applications are hosted in <b>Apache Tomcat 9.0 Tomcat server</b>, the Apache Tomcat 9.0 Tomcat component can be uninstalled.</p>

4. Install the new version of SiPass integrated.
5. Log into the new version of SiPass integrated.
6. Restore the backed-up database.



### Important

After installing SiPass integrated MP2.80 and configuring remote clients, while restoring the database from MP2.70 / MP2.75 and/or MP2.76, the **Client Configuration** checkbox is also available (checked by default) to restore the Remote Client configuration data from the previous version. When checked, the remote client configuration is overwritten. If this is unchecked, the remote client configuration stays the same as done after installing MP2.80.

7. Check the SiPass integrated Audit Trail to ensure the database was successfully restored.
8. Exit out of SiPass integrated, restart your SiPass integrated Server and log back in for the changes to take effect.



All operators who belong to the "Administrator" operator group will be given privileges to the new database components. All other operator groups will not automatically be assigned privileges; you must manually assign new database privileges to the appropriate operator groups after restoring.



After performing the restore, on the **Operation client> System Preferences > Audit Trail** tab, the value of **Maximum Lines Buffered** field must be set accordingly as it may have been overwritten to the new default value of 500 from MP2.80 onward. See the *Introduction and Starting Up > System Preferences* section in SiPass integrated Operation client User Guide for more information.

## 11 Password Management

SiPass integrated is installed and configured by the Siemens Commissioning Engineer with the default password provided by Siemens. **For ensuring maximum security, you will be asked to change the default password to a secure password of your choice while logging in to any of the SiPass integrated Clients for the first time.**

**Note:** When you log in to a SiPass integrated Client first and change the password, you will not be asked to change the password during the first login on the other clients on the same computer. If you cancel the *Change Password* dialog three times, it will be closed and displayed again during your next first login attempt.

A secure password can be created with the following properties:

- At least three characters long
- At least three of uppercase characters / lowercase characters / numbers / non-alphabet characters

**You can change the password at any time later following the steps below:**

1. Run the SiPass integrated Operation Client or Configuration through the Windows **Start Menu**.
2. On the *Welcome* dialog, click the **Change Password** button.  
⇒ The *Change Password* dialog is displayed. Enter the required information:
3. Type the username in the **User Name** field.
4. Type the existing password in the **Old Password** field.
5. Type an appropriate password in the **New Password** field. Memorize it so there are no login issues in future.
6. Type the new password again in the **Confirm Password** field.
7. Click **OK**.
8. The *Welcome* dialog is displayed again.
9. Login with the new password.



## 12 Appendix

### 12.1 SiPass integrated Port Reference

The table below lists the ports that are used to communicate among server, clients and hardware devices. 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.

Port Number	Role
<b>Ports connecting to Configuration Client</b>	
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
Dynamically Allocated (Chosen from default range 49512-65535)	RPC Ports, can be changed in Windows from default range. <b>Note:</b> The TCP ports used by SiPass integrated are configured both within the software and in the Windows registry. DCOM (using RPC ports) can be configured in Windows to use a set range of port numbers when it dynamically allocates one.
<b>Ports connecting to Operation Client</b>	
8741	Connection to SiPass Web Services
8742	Incoming connections from server to client port
<b>Port connecting to Web Client</b>	
5443	SiPass UI port (SiPass URL Router)
<b>Port connecting to MS API</b>	
8744	Connection to Management Station API Web Services
<b>Port connecting to HR API</b>	
8745	Connection to HR API Web Services
<b>Port connecting to ACC</b>	
4343	ACC communications, both Server to ACC, and between ACCs.

#### 12.1.1 Internal Server Ports used by Web Client

The following ports can be added as exception, as required.

8756, 5656	RabbitMQ
8757	MongoDB
8743	Connection to Web UI API Web Services
8746	Unified User Management (UUM)
8747	Activity Feed Service Port
8748	Dynamic UI Port Number
8749	PACS Port Number
8750	Unified Area Monitoring Port number (UAM)
8751	Web Client Port
8752	Web Client TBS Port
8753, 8755	Unified Authorization (UAA)

## 12.2 Windows Settings



---

- During installation, SiPass integrated automatically configures the DCOM settings using 'Anonymous' and 'Everyone' groups.

- We recommend creating a Windows Users Group who will be using your SiPass integrated system, and using this group for DCOM authentication. If you are running over a workgroup environment, this group and its members must exist on both the server and client computers.

- The DCOM Configuration folder can be found in the **Tools** folder, which is available on the Installation CD

- By default local Administrators have full privileges on the Server PC to run the local client.

---

1. Search **Components Services** in the **Windows Search**.
2. Double-click the **Component Services** icon.
3. Double-click **Computers**.
4. Double-click the **My Computer** icon.
5. Double-click **DCOM Config**.
6. Right-click on the **advanTage Server** icon and select **Properties**.
7. Ensure the *Authentication Level* dropdown list is set to **Default**.

## To configure SiPass Server settings

- ▷ Ensure that you have already created your SiPass integrated Group in Windows, which contains the Windows user accounts that will be running SiPass integrated.
- 1. Click the Windows **Start** menu and select **Control Panel**. The *Control Panel* window will appear.
- 2. Double-click **Administrative Tools**.
- 3. Double-click **Components Services**.
- 4. Double-click the **Component Services** icon.
- 5. Double-click **Computers**.
- 6. Right-click on the **My Computer** icon and choose **Properties**.
- 7. Select the COM Security tab.
- 8. Click the **Edit Limits** button for Access Permissions.
- 9. Click **Add** then enter **your SiPass Group** and click **OK**.
- 10. Tick **Remote Access** for your SiPass Group
- 11. Click **OK**.
- 12. Click the **Edit Limits** button for the Launch and Activation Permissions.
- 13. Click **Add** then enter **your SiPass Group** and click **OK**.
- 14. Tick **Remote Activation** for your SiPass Group.
- 15. Click **OK**.
- 16. Double-click the **My Computer** icon.
- 17. Double-click **DCOM Config**.
- 18. Right-click on the **advanTage Server** icon and select **Properties**.
- 19. Select the **Security** tab.
- 20. Select **Customize** from the **Launch and Activation Permissions** section and click **Edit**.
- 21. Click **Add** then enter your SiPass Group and click **OK**.
- 22. Tick **Remote Activation** for your SiPass Group.
- 23. Click **OK**.
- 24. Select **Customize** from the **Access Permissions** section and click **Edit**.
- 25. Click **Add**.
- 26. Enter **your SiPass Group** and click **OK**.
- 27. Tick **Remote Access** for your SiPass Group.
- 28. Click **OK**.
- 29. Click **OK** again.
- 30. Close the open dialogs.
- 31. You will need to restart your SiPass Server service before these changes take effect.



The Local Security Policy setting for 'Network Access: Sharing and security model for local accounts' must be set to Classic. The DCOM Configuration folder can be found in the Tools folder, which is available on the Installation CD.

**To configure SiPass integrated Client settings (remote clients only):**

- ▷ Ensure that you have already created your SiPass Group in Windows, which contains the Windows user accounts that will be running SiPass integrated.
- 1. Click the Windows **Start** menu and select **Control Panel**. The *Control Panel* window will appear.
- 2. Double-click **Administrative Tools**.
- 3. Double-click **Components Services**.
- 4. Double-click the **Component Services** icon.
- 5. Double-click **Computers**.
- 6. Right-click on the **My Computer** icon and select **Properties**.
- 7. Select the *COM Security* tab.
- 8. Click the **Edit Limits** button for Access Permissions.
- 9. Click **Add** then enter **your SiPass Group** and click **OK**.
- 10. Tick **Remote Access** for your SiPass Group.
- 11. Click **OK**.
- 12. Click the **Edit Limits** button for Launch Permissions.
- 13. Click **Add**.
- 14. Enter your SiPass Group and click **OK**.
- 15. Tick all permissions for your SiPass Group.
- 16. Click **OK**.
- 17. Click **OK** again.
- 18. Close the open dialogs.

## 12.3 Connection of Enrolment readers

Enrolment readers can be connected by plugging into the USB port of the SiPass integrated Server or Remote Client computer.



Remote Desktop connection cannot be used to setup a reader. You must perform the setup on the computer to which, the Enrolment reader is connected directly and the SiPass client is installed locally.

1. Remove the reader from its packaging.
2. Connect the USB wire of the reader to the USB port in your computer.
3. **For Omnikey 5321 and Omnikey 5421 readers, a driver must be installed.** Go to the reader manufacturer's website to download and install the appropriate driver for your reader.
  - ⇒ The **Omnikey 5422** and **Omnikey 5022** readers do not need a driver to be installed separately
  - ◆ Configure the reader through SiPass integrated Operation Client. See the *Operation Client User Guide* in the SiPass integrated software bundle for more information about configuring the reader's profile.

## 12.4 Troubleshooting

The following troubleshooting table may help you to overcome errors during the installation of SiPass integrated or its associated peripheral devices.

Error	Solution
<p>"Insecure Certificate" browser error when using the Web Site feature:</p> <p>ERROR_CERT_COMMON_NAME_INVALID</p>	<p>If the SiPass integrated Server is using the self-signed certificate, then the self-signed certificate must be re-generated.</p> <p>Go to the SiPass integrated installation directory on the SiPass Server computer and double-click the <i>SiPass.CertificatePicker.exe</i> file.</p>
Audit trail not being displayed in Operation Client	<ul style="list-style-type: none"> <li>• Ensure all ports are shown as open when running the supplied SiPass Connectivity Tool</li> <li>• Check that a proxy is not interfering with audit trail callback connection. To attempt to bypass proxy, open the <i>bindings.config</i> file on the Server computer, change the "useDefaultWebProxy="true" value from true to false, and restart SiPass server.</li> </ul>
Unable to Open printer dialogue.	<p>Ensure that a printer has been configured in the <b>Print Setup</b> option under the SiPass integrated <b>File</b> Menu system.</p> <p>If this does not rectify the problem and does not allow the local client to be used, simply set the printer as a local printer and then return it to the network printer option.</p>
Reader Name not verified.	<p>When configuring readers in SiPass integrated and assigning the reader with an "Image Verification" mode of operation, the following symbols cannot be used in the name of that reader:</p> <p>/ \ : ? * &lt; &gt;  </p>
Smart Card reader not recognized during installation. (Error Message displayed)	<p>When installing a smart card reader that is not recognized, an error message will be displayed, stating that the reader cannot be selected, or is not available or not installed.</p> <p>To rectify the situation, uninstall the drivers and re-install them again.</p>

Error	Solution
SiPass integrated language different from the Operating system locale	<p>To prevent issues when SiPass integrated is installed in a language different from the locale of Operating System of your computer, the following steps must be performed:</p> <ul style="list-style-type: none"> <li>Browse to the SiPass integrated installation root directory on SiPass integrated Client and Server, and open the Configuration File: <ul style="list-style-type: none"> <li><i>AscoSrvr.exe.config</i> (SiPass Server)</li> <li><i>SiPassOpClient.exe.config</i> (SiPass Operation Client)</li> <li><i>SiPassConfigurationClient.exe.config</i> (SiPass Configuration Client)</li> </ul> </li> <li>Go to the setting &lt;add key="UseInstalledLanguage" value="true"/&gt;</li> <li>Modify the value for this setting to "false"</li> </ul> <p><b>Note:</b> The above steps must be performed after installing SiPass integrated.</p> <p><b>SiPass integrated Server:</b> Stop SiPass service, apply the changes and restart the service.</p> <p><b>SiPass integrated Client:</b> Apply the changes and restart the client computer.</p>
Audit Trail stops updating and operator name is missing from the details	<p>In case of extensive sites, when updating an operator group by assigning or removing thousands of point groups, the Audit Trail in the SiPass integrated client may stop updating. In this case, the operator name is also missing from the details.</p> <p><b>Note:</b> To rectify the issue, you can increase maximum mailbox size by adjusting the <i>MailBoxMaxItems</i> registry value between 1000 to 10000. If this value is set outside this range, the default value of 3000 is used.</p> <ul style="list-style-type: none"> <li>On the SiPass server PC, run <i>regedit</i> in a command prompt</li> <li>Navigate to the following registry key using the <i>regedit</i> tool:</li> </ul> <p><b>On a 64-bit Operating System</b></p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Landis &amp; Staefa\ADVANTAGE\Version4\Server\ServerConfigurations\&lt;ComputerName&gt;</p> <p><b>On a 32-bit Operating System</b></p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\Landis &amp; Staefa\ADVANTAGE\Version4\Server\ServerConfigurations\&lt;ComputerName&gt;</p> <p>where &lt;ComputerName&gt; is the name of the server.</p> <ul style="list-style-type: none"> <li>Locate the <i>MailBoxMaxItems</i> value and double-click it</li> <li>When given a choice to work with Hexadecimal or Decimal base, select Decimal, then enter a value between the allowed range 1000 to 10000.</li> <li>Click <b>OK</b></li> <li>Restart the SiPass server</li> </ul>

Error	Solution
SiPass integrated Management Station API, Web UI API and Web UI do not get removed if installation is rolled back before completion	<p>These services must be removed from the <i>Services.msc</i> window as described below:</p> <ul style="list-style-type: none"> <li>Go to command prompt</li> <li>Navigate to the Sipass integrated installation path (generally <i>C:\Program Files (x86)\SiPass integrated\</i>)</li> <li>Use the following command to delete the service:  <code>sc [&lt;ServerName&gt;] delete [&lt;ServiceName&gt;]</code> </li> </ul> <p>where</p> <p>&lt;ServerName&gt; = The name of the remote server on which the service is located. The name must use the Universal Naming Convention (UNC) format (for example, \\myserver). To run <i>sc.exe</i> locally, omit this parameter.</p> <p>&lt;ServiceName&gt; = The service name returned by the <b>getkeyname</b> operation</p> <p>? = Displays help at the command prompt</p> <p>The <i>sc</i> command deletes a service subkey from the registry. If the service is running or if another process has an open handle to the service, the service is marked for deletion.</p> <p>Service Name and path can be seen in General tab when the particular service is double clicked from the services.msc dialog</p> <p>If the dependency services of Web UI API still persists, please remove the below services using the above steps:</p> <ul style="list-style-type: none"> <li>SiPass integrated - Siveillance Activity Feed</li> <li>SiPass integrated - Siveillance Dynamic UI</li> <li>SiPass integrated - Siveillance User Management</li> <li>SiPass integrated Activity Feed Interface</li> <li>SiPass integrated PACS Management</li> <li>SiPass integrated Unified Area Monitoring</li> <li>SiPass integrated UUM Interface</li> </ul> <p><b>Note:</b> The above solution applies to Windows 10, Windows Server 2016, and Windows Server 2019.</p>
MongoDB_SiPassintegrated, RabbitMQ_SiPassintegrated  services are not started due to trusted certificate mapping during installation	<p>Reapply self-signed certificate using Certificate Picker. Once the certificate is applied, start the following services in the Service console:</p> <ul style="list-style-type: none"> <li>MongoDB_SiPassintegrated</li> <li>RabbitMQ_SiPassintegrated</li> <li>SiPass integrated - Siveillance Activity Feed</li> <li>SiPass integrated - Siveillance Dynamic UI</li> <li>SiPass integrated - Siveillance Unified User Management</li> <li>SiPass integrated UUM Interface</li> </ul>



## 12.4.1 Troubleshooting Fargo HDP 8500 Printer and Embedded Encoder

### 12.4.1.1 Printer Issues

#### **"Error: Please reset your printer"**

Any of the card movement related operations like *Insert Card* or *Eject Card* fail with "Error: Please reset your printer". This indicates that printer is no longer reachable using the IP address provided.

Follow the steps below to resolve the issue:

1. Restart the printer.
2. Verify that the printer IP address is reachable from the workstation.
3. Verify that the ports 5400 and 5402 are not blocked by Windows firewall or anti-virus.
4. Verify that there are no IP address conflicts over the network.

### 12.4.1.2 Encoder Issues

#### **Any of encoding related tasks fail with error:**

#### **"Can not select smart card!" (IP address issue)**

The error occurs when the printer is not reachable with the IP address provided and results in the following:

- Failure of any encoder related operations (Read, Assign, Read & Search or Encode)
- Display of error message : "Can not select smart card!"
- *"SiPassOpClient.log.txt"* file showing one of the following error message:

```
EstablishSession() - Could not establish ethernet
connection for encoder 'OMNIKEY 5x21 LAN B8120048-CL 0'.
SCardControl(, CM_IOCTL_ENCODER_CONNECT, ... ) failed.

[OMNIKEY Ethernet Driver] Error code '0xC1000005': A
timeout occurred during communication with the encoder
device.
```

Hint: Please verify that the IP address or Hostname of the ethernet encoder is reachable and that the outbound port '22222' is not blocked.

or

```
EstablishSession() - Could not establish ethernet
connection for encoder 'OMNIKEY 5x21 LAN B8120048-CL 0'.
SCardControl(, CM_IOCTL_ENCODER_CONNECT, ... ) failed.

[OMNIKEY Ethernet Driver] Error code '0xC1000002': The
OMNIKEY 5121 Ethernet Driver Service did not respond to
the user request.
```

Hint: This could mean that the previous attempt to establish ethernet session is in failure state. This is the continuation of it. Please verify that the IP address or Hostname of the ethernet encoder is reachable and the outbound port 22222 is not blocked.

To resolve the error, verify the following:

1. The printer IP address is reachable from the workstation, and the same IP address is setup in the LAN encoder using the *OMNIKEY 5121 Ethernet Encoder Utility*. This utility comes with *OMNIKEY 5121 Ethernet Encoder Driver - 2.0.0.1* and gets installed on the workstation.
2. *Port 22222* is not blocked by Windows firewall or anti-virus.

**Any of encoding related tasks fail with error:**

**"Can not select smart card!" (Multiple sessions with encoder)**

The error occurs when another workstation is accessing the printer's encoder remotely and results in the following:

- Failure of any encoder related operations (Read, Assign, Read & Search or Encode)
- Display of error message : "Can not select smart card!"
- "*SiPassOpClient.log.txt*" file showing one of the following error message:  
  

```
EstablishSession() - Could not establish ethernet
connection for encoder 'OMNIKEY 5x21 LAN B8120048-CL 0'.
SCardControl(, CM_IOCTL_ENCODER_CONNECT, ... ) failed.

[OMNIKEY Ethernet Driver] Error code '0xC1000006': The
encoder device is busy. The encoder is likely established
in a session with another server or workstation.

Hint: Ensure that only one remote workstation (OMNIKEY
Ethernet Driver) is connected to the 'OMNIKEY 5121
Ethernet Encoder'.
```

To resolve the error, follow the steps below:

1. Ensure that no other workstation is using the embedded encoder in 'Network Connection (Ethernet mode)'
2. Restart the printer

**Note:** If this does not resolve the issue, see section Switching between Local Connection (USB mode) Type and Network Connection (Ethernet mode) Type in *SiPass integrated Configuration Client User Guide* (Version MP 2.76).

#### **Error: OMNIKEY 5121 Embedded Encoder no longer detected by Windows in USB mode**

If 'OMNIKEY 5121 Embedded Encoder' was configured in 'Local Connection (USB mode)' and no longer appears in Windows Device Manager console, this means another workstation is using the embedded encoder of the printer in 'Network Connection (Ethernet mode)'.

Follow the steps below:

1. Ensure that no other workstation is using the embedded encoder in 'Network Connection (Ethernet mode)'.
2. Restart the printer.
3. Verify that the printer is connected to workstation via USB cable.
  - ⇒ The encoder should appear in the Windows Device Manager console under the 'Smart card readers' as 'OMNIKEY 5x21'.

Issued by  
Siemens Switzerland Ltd  
Smart Infrastructure  
Global Headquarters  
Theilerstrasse 1a  
CH-6300 Zug  
+41 58 724 2424  
[www.siemens.com/buildingtechnologies](http://www.siemens.com/buildingtechnologies)