

EcoStruxure Building Operation

Security Expert SmartConnector

Installation & User Guide

February 2025



Prepared By:

Global Integration Solution Centre

EcoStruxure Building Operation

Security Expert SmartConnector

Installation & User Guide

February 2025

Copyright © 2025 Schneider Electric. All rights reserved.

The Schneider Electric brand and any registered trademarks of Schneider Electric Industries SAS referred to in this guide are the sole property of Schneider Electric SA and its subsidiaries. They may not be used for any purpose without the owner's permission, given in writing. This guide and its content are protected, within the meaning of the French intellectual property code (Code de la propriété intellectuelle français, referred to hereafter as "the Code"), under the laws of copyright covering texts, drawings and models, as well as by trademark law. You agree not to reproduce, other than for your own personal, non-commercial use as defined in the Code, all or part of this guide on any medium whatsoever without Schneider Electric's permission, given in writing. You also agree not to establish any hypertext links to this guide or its content. Schneider Electric does not grant any right or license for the personal and non-commercial use of the guide or its content, except for a non-exclusive license to consult it on an "as is" basis, at your own risk. All other rights are reserved.

Trademarks and registered trademarks are the property of their respective owners.

Contents

1	Introduction	6
1.1	Architecture.....	6
2	Versions & Prerequisites.....	8
2.1	SmartConnector Service Version.....	8
2.2	Security Expert Version	8
2.3	Prerequisites.....	8
2.4	Licensing	9
2.5	Security Expert Prerequisites	9
2.6	Quick Start Installation Sequence	10
3	SmartConnector Framework Installation.....	11
3.1	Download the SmartConnector Framework	11
3.2	Install the SmartConnector Framework	13
3.2.1	Install SmartConnector Framework	13
3.2.2	Validate SmartConnector Framework	15
3.2.3	Change Default Credentials	17
3.2.4	Install SmartConnector Framework Runtime License.....	18
4	Security Expert SmartConnector Extension Installation	22
4.1	Downloading the Security Expert SmartConnector	22
4.2	Installing Security Expert SmartConnector Extension	23
4.3	Install and License Security Expert SmartConnector Extension	24
4.4	Configure Security Expert SmartConnector Discovery Extension Processors.....	26
4.5	Configure Security Expert SmartConnector Alarm Update Extension Processors	30
4.6	Configure Schedule on Alarm Update Processor	31
4.7	Assign a Schedule to Security Expert Update Alarms Processors	32
5	Host Security Expert Objects in EcoStruxure Building Operation.....	33
5.1	Create Security Expert EWS Interface in EBO.....	33
5.2	Host Security Expert Objects in EcoStruxure Building Operation	35
6	Troubleshooting.....	36
6.1	SmartConnector Log File	36
6.2	Framework Licensing Error.....	37
6.3	SmartConnector Extension Licensing Error	38
6.4	SQL Authentication Error.....	38

6.5	Security Expert Communication Error	38
6.6	EWS Communication Errors	39
7	Appendix A – Hierarchy of points	40
7.1	Folders	40
7.2	Doors	40
7.3	Salto Door Objects.....	41
7.4	Floors	41
7.5	Inputs.....	42
7.6	Outputs.....	42
7.7	Miscellaneous Alarms.....	42
7.8	Areas.....	43
7.9	Data Values.....	44
7.10	Trouble Input.....	44
8	Appendix B – Filtering Alarms	44
9	Appendix C – SQL User Roles	45
10	Appendix D – Security Expert Cross Controller Operations.....	46
11	Appendix E – Security Expert Multi-Site Configuration	46
12	Revision History	47
13	References	48
14	SmartConnector Maintenance.....	49
14.1	Maintenance Processor Installation.....	49
14.2	Maintenance Schedule Creation	51
14.3	Assign a Schedule to the Maintenance Processors	52

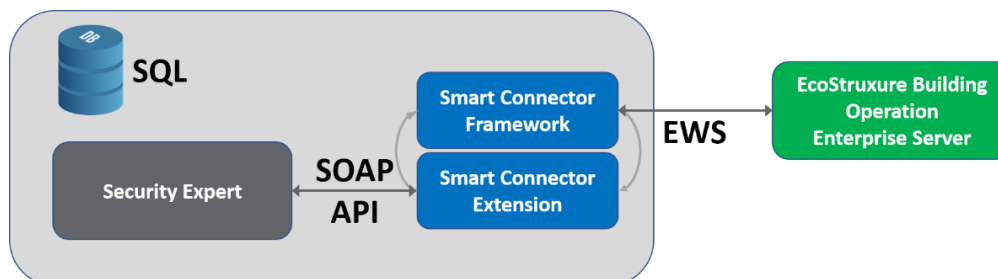
1 Introduction

This document outlines the installation and configuration of the Security Expert SmartConnector Extension required to integrate Security Expert with EcoStruxure Building Operations. This document assumes that EcoStruxure Building Operations and Security Expert systems have already been installed and are functional as independent systems.

Document	Description
SmartConnector Installation and Configuration Guide	Complete installation guide for SmartConnector Framework that covers in more depth – installation and configuration options, troubleshooting information on the SmartConnector Framework. This manual will be downloaded during the installation process.
Security Expert SmartConnector Extension	This manual

1.1 Architecture

A Basic overview of the architecture is that SmartConnector Framework and Extension will communicate to the Security Expert Server and the EcoStruxure Building Operation Enterprise Server to share data and alarms.

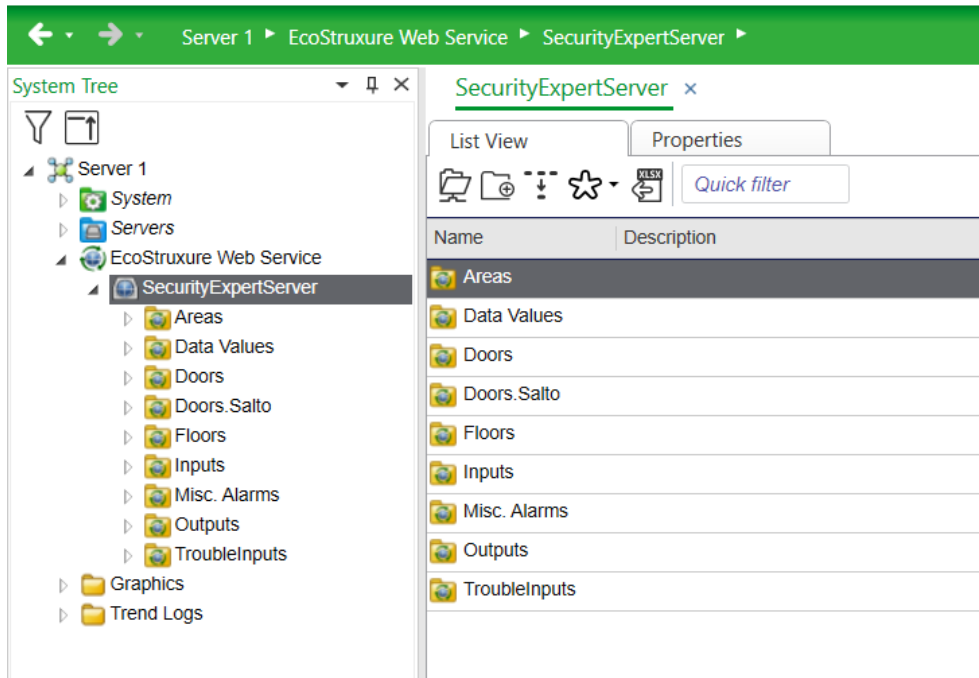


SmartConnector Framework is responsible for communication to the EcoStruxure Building Operation Enterprise Server using EcoStruxure Web Services (EWS)

Security Expert SmartConnector Extension is responsible for communication to the Security Expert Server using a SOAP Application Program Interface (API)

SmartConnector Framework and Security Expert SmartConnector Extension work together to share data between Security Expert and EcoStruxure Building Operation. Additionally, the SmartConnector Framework provides a user interface to configure communication to the Enterprise Server. The SmartConnector Framework provides extensibility to EcoStruxure Building Operation for additional functionality (processors) to communication with other system, such as in this case the Security Expert Extension.

Once SmartConnector Framework and Security Expert SmartConnector Extension have been installed and configured the two independent systems, will be able to share data values and alarming.



2 Versions & Prerequisites

2.1 SmartConnector Service Version

The processors have been configured to operate with the SmartConnector version 2.5.5.108, use with any other version of the SmartConnector framework is not supported.

2.2 Security Expert Version

The processors can support EcoStruxure Security Expert systems operating with version 4.3.370.1 and Security Expert SOAP version 1.7.0.0 or greater.

2.3 Prerequisites

In order to install the Security Expert SmartConnector Extension, we must first install and license the SmartConnector Framework. There are multiple configuration options as to where the SmartConnector Framework can be installed – for use in this document; the SmartConnector Framework and Extension will be installed on the same machine as the EcoStruxure Enterprise Server and SQL Express. For additional options using SQL or remote servers not containing the Enterprise Server refer to the SmartConnector Installation and Configuration Guide.

The following prerequisites must be performed before you start the installation and configuration of the SmartConnector Framework and Security Expert SmartConnector Extension.

- Security Expert System - Installed, Configured and Functional
- EcoStruxure Building Operation Enterprise Server - Installed, Configured and Functional - The minimum EWS Version supported is 1.2.
- Microsoft .NET v4.7 or later must be installed on the Enterprise Server
- SQL Express is installed on the Enterprise Server or server for SmartConnector installation

Note: If SQL is installed on a remote machine follow the detailed instructions in the *SmartConnector Framework Installation and Configuration Guide.pdf*

- The specified user must have at least the “public” and “dbcreator” user roles in the SQL server

Note: Additional Installation options for installing the SmartConnector Framework can be located in the *SmartConnector Installation and Configuration Guide*.

2.4 Licensing

The EcoStruxure Security Expert SmartConnector extension does not have a license cost, but to deploy the SmartConnector solution, a SmartConnector deployment license is required.

Use this part number to place orders for the SmartConnector Deployment license:

Part Number	Product Name	Description
SXWSWCDL100001	SW-SMART-CONNECT	SmartConnector Deployment License

2.5 Security Expert Prerequisites

The following tasks need to be carried out in EcoStruxure Security Expert before deployment of the SmartConnector.

Create an operator in EcoStruxure Security Expert this operator will be used to access the EcoStruxure Security Expert system and will also be used to acknowledge all alarms.

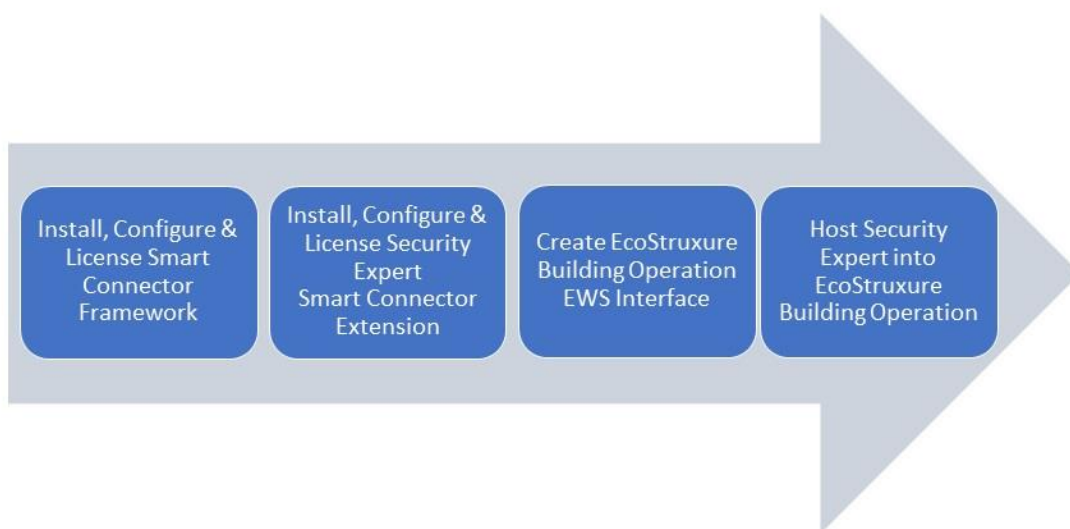
For any alarms which are required to be delivered to EcoStruxure Building Operation an event filter must be configured in the EcoStruxure Security Expert. Create a new event filter and add any events from the list of available. The record filter tab can be used to restrict the event filter to certain objects.

The SmartConnector extension supports only one event filter to be configured all matching events will be delivered as alarms to EcoStruxure Building Operation. If you require to filter the alarms being delivered to EcoStruxure Building Operation, see *Appendix B* Filtering alarms.

2.6 Quick Start Installation Sequence

The following overview provides the steps necessary to install and configure the system. The subsequent chapters will provide detailed information for each step in the process.

1. Install, Configure and License the **SmartConnector Framework**
2. Install, Configure and License the **Security Expert SmartConnector Extension**
3. Create **EWS Interface** in EcoStruxure Building Operation to communicate to **Security Expert Server**
4. Host **EWS objects** in EcoStruxure Building Operation from **Security Expert Server**



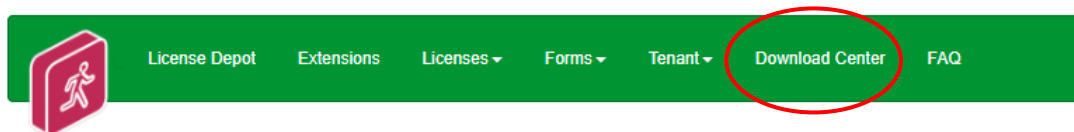
3 SmartConnector Framework Installation

The first step in the process is to download SmartConnector Framework software from <http://www.smartconnectorserver.com>, once downloaded you will install the SmartConnector Framework software, obtain the machine thumbprint, license the Framework to the machine thumbprint and finally configure the Framework system. Once the SmartConnector Framework has been installed, configured and licensed we can extend the Framework by adding the Security Expert SmartConnector Extension.

3.1 Download the SmartConnector Framework

The following steps will assist in downloading the SmartConnector Server Framework.

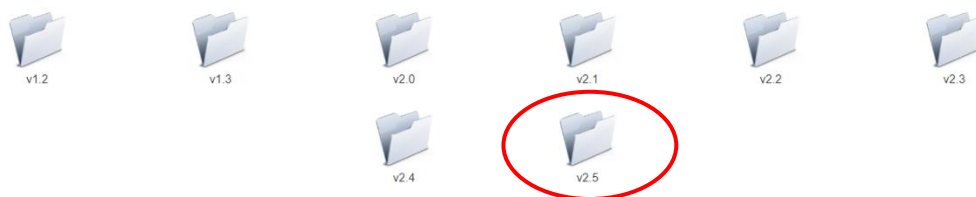
1. Go to <http://www.smartconnectorserver.com>
2. Request credentials to logon to the web site
3. Log on to the web site
4. From the menu, select Download Center from the menu



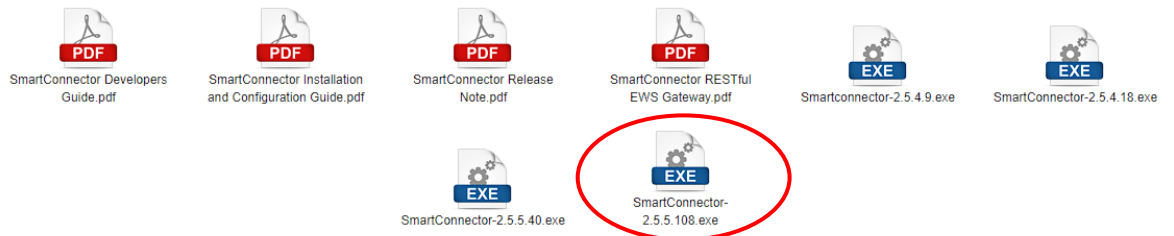
5. Select SmartConnector icon



6. Select the folder version (v2.5)



7. Select version SmartConnector (v2.5.5.108)
(Note: make sure Popups are not blocked by your browser)



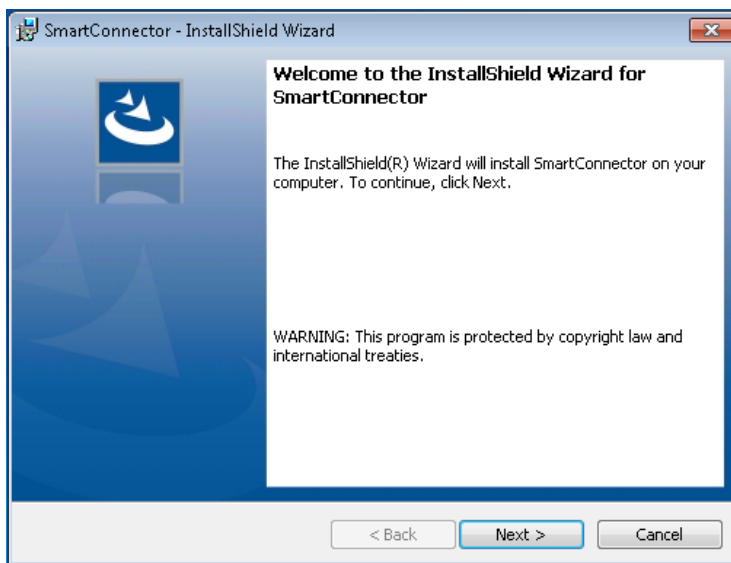
8. Save the SmartConnector v2.5.5.108.exe download file
9. Select the *SmartConnector Installation and Configuration Guide.pdf*
10. Save the *SmartConnector Installation and Configuration Guide.pdf* download file

3.2 Install the SmartConnector Framework

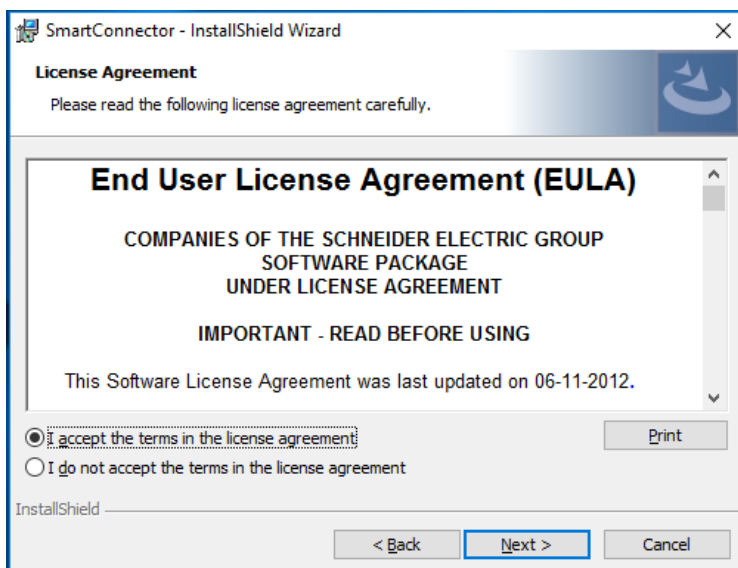
To install the SmartConnector Framework, execute the setup file that was just downloaded. Run SmartConnector-v2.5.5.108.exe – You must run this as an *Administrator*.

3.2.1 Install SmartConnector Framework

1. Locate the downloaded file SmartConnector-v2.5.5.10.exe
2. Right click on the file SmartConnector-v2.5.5.10.exe
3. Select Run as Administrator

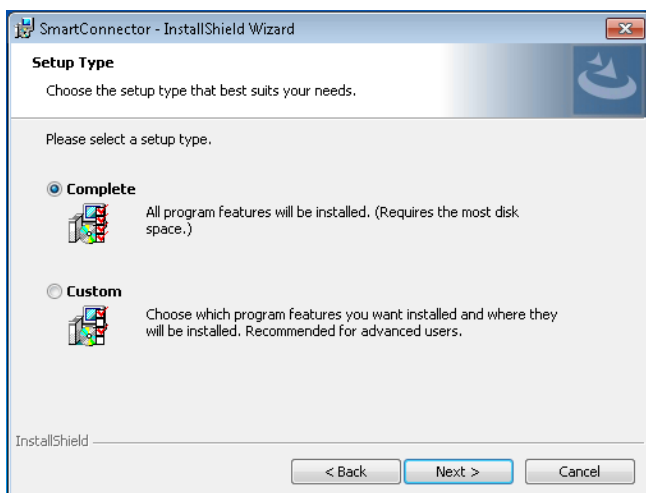


4. Click **Next**.
5. Review and accept the terms to the End User License Agreement

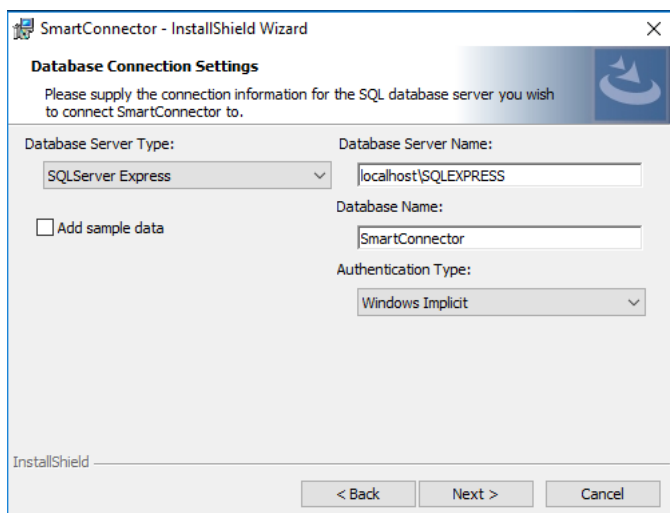


6. Click **Next**.

7. Choose the Setup Type you wish to perform. If this is a new installation, **you must choose Complete.**
8. Click **Next.**



9. Enter the required information for the database server where you will install the database to:

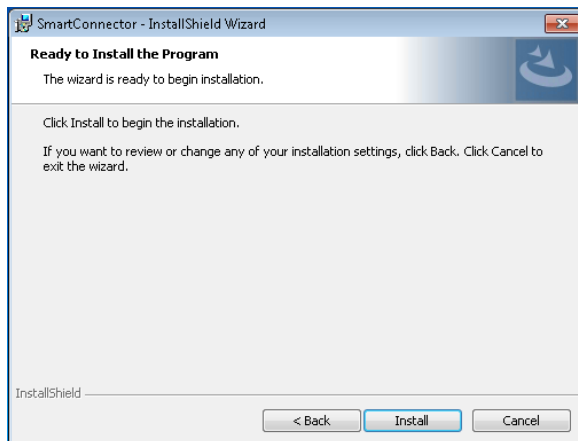


- i) You can **uncheck** – “Add sample data”.
For this manual example we are using SQL express and a local Windows user.
- ii) Select the Database Server Type: **SQLServer Express.**
- iii) Select the Authentication Type: **Windows Implicit.**

Note: The logged in user must have at least the “public” and “dbcreator” user roles in the local SQL server. In this configuration SmartConnector runs under the NT Authority\System account. See Appendix C.

For additional SQL installation options, refer to the *SmartConnector Installation and Configuration Guide* previously downloaded.

- iv) Click **Next** to display the final confirmation dialog shown below.



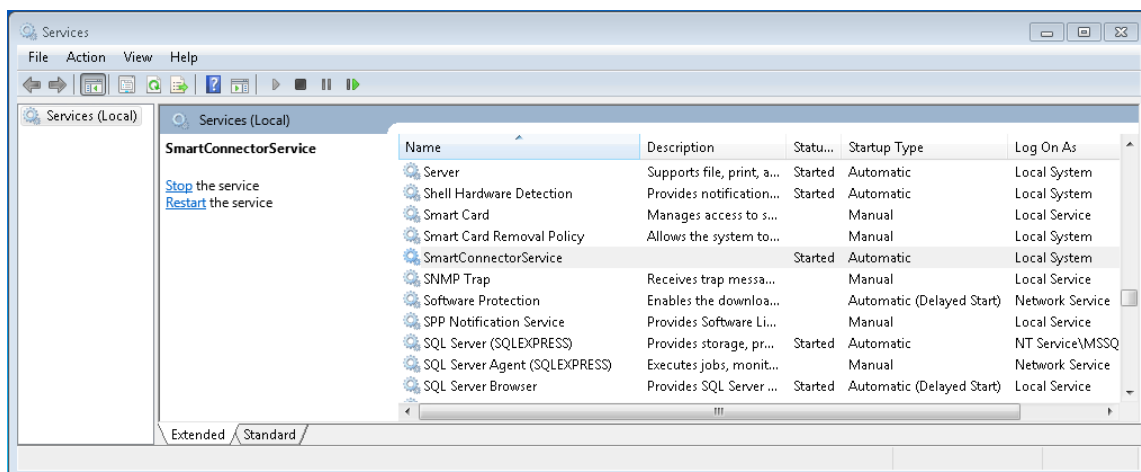
10. Click **Install** to complete the installation and create the default database.
11. Click **Finish**.

3.2.2 Validate SmartConnector Framework

To review the service installation, you should perform the following:

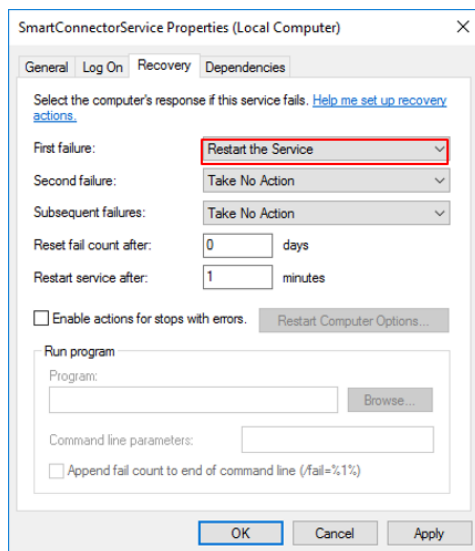
1. Open the Windows Services dialog.
2. Find the entry for “SmartConnectorService”. It should have a Status of “Started” or “Running” and a Startup Type of “Automatic” as shown below.

If SmartConnector and the connected database server are located on the same physical server, we recommend changing that the Startup Type to “Automatic (Delayed Start)”.



3. Right click the “SmartConnectorService” entry and choose Properties.
4. Click the **General Tab**.
5. Confirm the Startup Type is **Automatic**.
6. Click the **Log On** tab.

7. Confirm that the “Local System account” is selected. This may be different depending on the database authentication type you chose earlier.
8. Click the Recovery tab.
9. Set First failure: to **Restart the Service**
We recommended that you choose at least one recovery action in the event that the SmartConnector Service experiences a failure. At a minimum, “Restart the Service” should be selected.



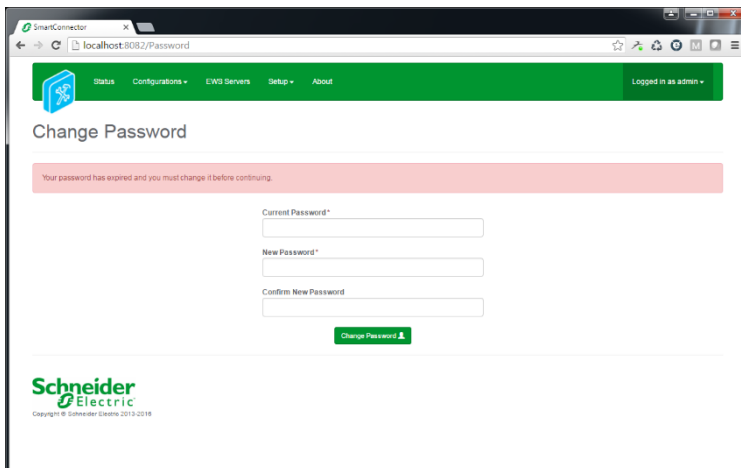
10. Select **OK** to save all changes.

3.2.3 Change Default Credentials

By default, SmartConnector will enable SmartConnector Portal on the local machine. Using SmartConnector Portal, you must change the default password to a new password.

1. Open a web browser.
2. Navigate to <http://localhost:8082>
3. At the [Login Page](#), enter the default user credentials of admin and Admin!23.

At this point you will be presented with the Change Password Page as show below.



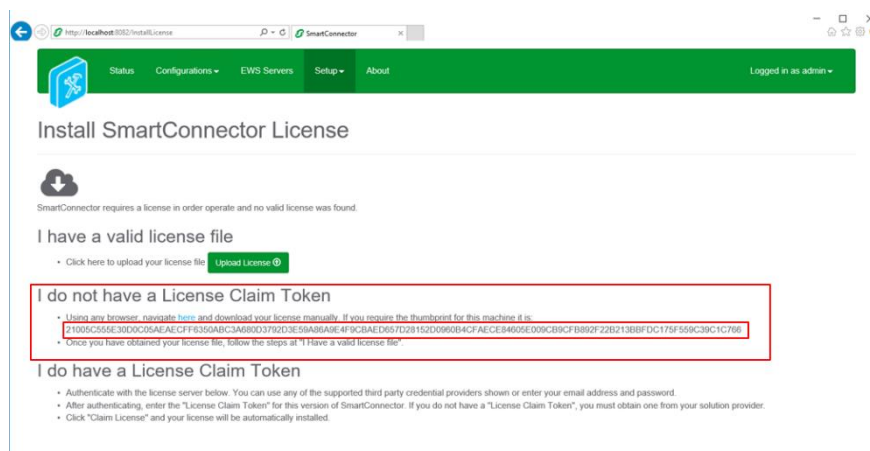
4. Enter the default password as the Current Password.
5. Enter a new password. Portal passwords are required to be at least 6 characters in length and contain a mix of upper case, lower case, numeric, and at least one non-alphanumeric character.
6. Confirm the password you entered in step 5.
7. Click **Change Password**.
8. Re-authenticate (Login) with your Username and new password.

3.2.4 Install SmartConnector Framework Runtime License

SmartConnector Framework requires a license in order to run. After changing the default password, navigating to any page of SmartConnector Portal will return the user to the Install License page where a runtime license must be installed.

I. SmartConnector Connected to the Web

If the Windows machine with SmartConnector Framework detects an active internet connection, the Install SmartConnector License page will automatically be displayed. Once authenticated with the License Manager, you only need to enter a License Claim Token to “claim” the runtime license and it will be automatically installed. Alternatively, the user may click “Upload License” to manually upload an already obtained license file. License Claim tokens and license files can be obtained from www.smartconnectorserver.com.



II. SmartConnector Not Connected to the Web

If SmartConnector fails to detect an active internet connection, the Install License page shown below will be displayed.

Directions are provided on how to download a license file from

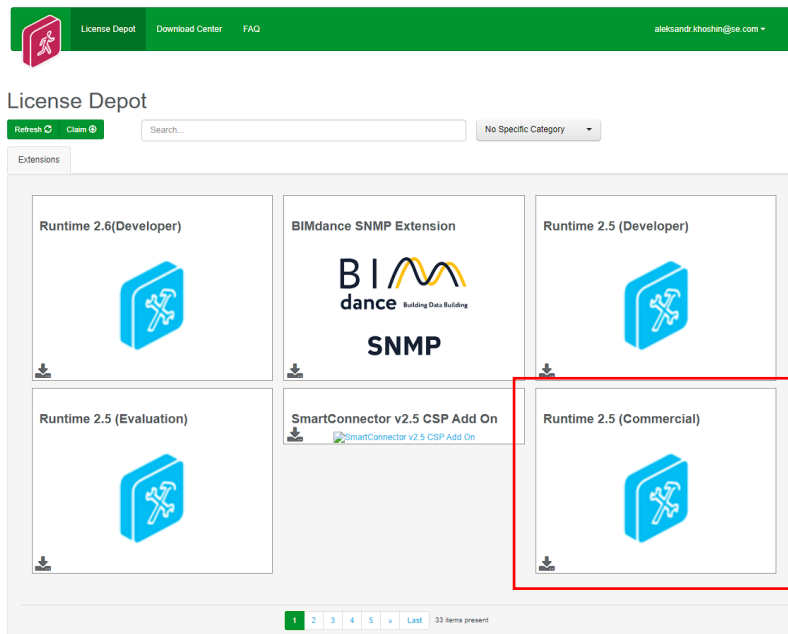
www.smartconnectorserver.com.


III. Obtain a license when you do not have a Claim Token

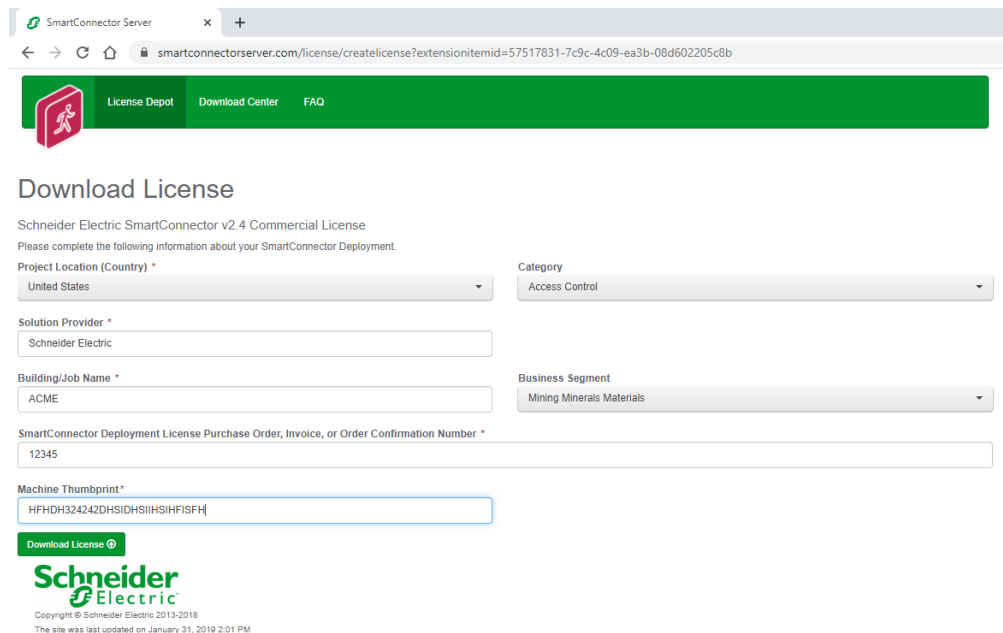
If you do not have a claim token, then you can download a License for SmartConnector Framework via a file and the Thumbprint of the machine SmartConnector Framework has been installed on.

1. From the “I do not have a License Claim Token section of the SmartConnector License page”.
2. Copy the Machine Thumbprint into the Windows clipboard for use later.
3. Click on the navigate here button in this section, this will connect you to the License Depot web page.

4. Log on to the License depot web page with your smartconnectorserver.com credentials.
5. Change the page until you see the Runtime v2.5 commercial license.



6. Select the  download button to obtain the License file.
7. Complete the Download License form.

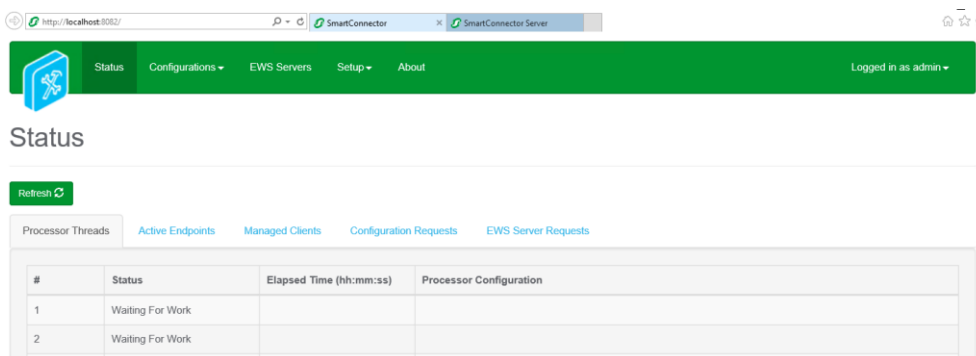


The screenshot shows the 'Download License' form on the SmartConnector Server website. The form is titled 'Download License' and is for 'Schneider Electric SmartConnector v2.4 Commercial License'. It asks for the following information:

- Project Location (Country):** United States
- Category:** Access Control
- Solution Provider:** Schneider Electric
- Building/Job Name:** ACME
- Business Segment:** Mining Minerals Materials
- SmartConnector Deployment License Purchase Order, Invoice, or Order Confirmation Number:** 12345
- Machine Thumbprint:** HFHDH32424DHSIDHSIHSIFSFH

At the bottom of the form, there is a 'Download License' button. Below the form, the Schneider Electric logo is displayed, along with the copyright information: 'Copyright © Schneider Electric 2013-2018. The site was last updated on January 31, 2019 2:01 PM'.

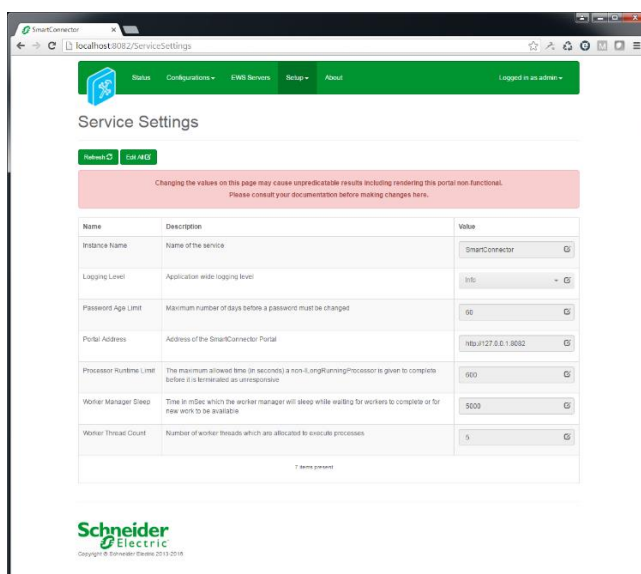
8. Paste in the machine thumbprint from the Windows clipboard (copied earlier).
9. Save the downloaded License file.
10. Return to the Install SmartConnector License page.
11. Select Upload License.
12. SmartConnector Framework is now successfully licensed.
13. The SmartConnector Framework status page will appear.




IV. Confirm Settings

SmartConnector installs the service with some default settings. After changing the password, you should confirm the system settings meet the criteria for how SmartConnector Framework will be used.

1. Open any web browser.
2. Navigate to <http://localhost:8082>
3. Authenticate with the credentials you used in the prior section.
4. From the menu, click **Setup -> Service Settings**.



- To edit any field, you can either click the edit icon  in that field or click the Edit All button to enable all fields for editing.
- The default settings will be acceptable for the initial installation of SmartConnector Framework.
- Users should use good security practices to define the expiration time for user Passwords.

The EWS Portal address can also be modified here from the default port used 8082.

5. Review and/or change values as desired. Unless otherwise noted, changes made here will take effect without a service restart.

Instance Name	– Appears in the browser tab and can be useful to distinguish which SmartConnector instance you are looking at if you are connecting to multiple deployed instances from a single browser.
Logging Level	– Maximum level SmartConnector will log. Possible values are <i>None, Error, Status, Info, Debug, Trace, All</i> . This setting is used in conjunction with Logging Filters to control how much information is captured in the log files.
Password Age Limit	– The maximum number of days before a Portal user’s password will expire.
Portal Address	– Address of SmartConnector Portal. For security concerns, the default value will be 127.0.0.1 which means the portal can only be accessed from the local machine. If broader access is required, this value can be modified by using the “+ syntax” e.g. http://+:8082 . This will allow access to any IP or DNS which resolves to the local machine. If you plan to secure the endpoint with a certificate, then the protocol shown here should be changed to https to match. Entering an empty value will disable the portal. Use caution! Consult the Security Considerations for suggestions on how best to configure this.
Processor Runtime Limit	– The maximum amount of time a Processor Configuration is given to complete before it is deemed to be unresponsive and is terminated. Unless otherwise instructed this value should not need to be modified.
Worker Manager Sleep	– The amount of time that the Worker Manager will idle before determining if there are Processors that need to be invoked. Unless otherwise instructed this value should not need to be modified.
Worker Thread	Count – The number of concurrent Processors that can be executed. This number may be increased but is largely dependent on the host machine’s number of logical processors. To determine the number of logical processors, open a command prompt and enter the command: WMIC CPU Get DeviceID, NumberOfCores, NumberOfLogicalProcessors. While you can set this value greater than the number of logical processors, it represents the number of concurrent workers that can run without potential operating system queuing. You will need to restart the SmartConnector Service for this change to take effect.

6. After you have made the necessary changes, click Save to save them to the database.

4 Security Expert SmartConnector Extension Installation

Schneider Electric Buildings group places all SmartConnector Extensions in the Marketplace. The steps below will walk you through how to connect and download the Security Expert SmartConnector Extension.

4.1 Downloading the Security Expert SmartConnector

1. Visit the Schneider Electric Exchange Shop:

<https://exchange.se.com/shop>

2. Search for 'Security Expert' in the search box:

Shop Exchange

Access hundreds of apps, design guides, datasets and more.

Security Expert

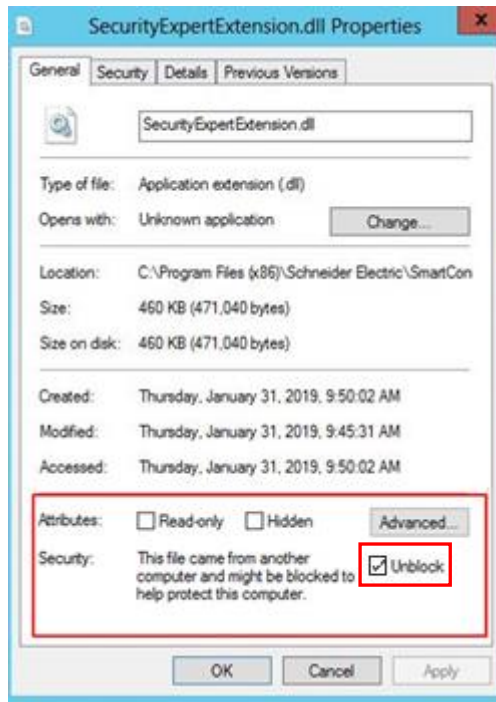


3. Search for Security Expert in the search box.
4. Click to open the Security Expert SmartConnector.
5. Click on the download button to download the SmartConnector extension file.

The screenshot shows the Schneider Electric Exchange Shop interface. At the top, there is a navigation bar with 'Schneider Electric Exchange' and links for 'HOME', 'COLLABORATE', 'DEVELOP', and 'SHOP'. Below the navigation bar, there is a search bar containing the text 'Security Expert'. To the right of the search bar, there is a 'Download' button highlighted with a red box. Below the search bar, there is a product card for 'EcoStruxure™ Security Expert SmartConnector'. The card includes a small image of the product, the product name, a description, and a 'Free' label. Below the product card, there is an 'Overview' section with a 3D building model and a list of features.

4.2 Installing Security Expert SmartConnector Extension

1. Extract the files from the zip file to a temporary directory.
2. Right click on each file and select Properties.
3. Verify the file is not blocked – see screen shot below; if the file is blocked, select Unblock.



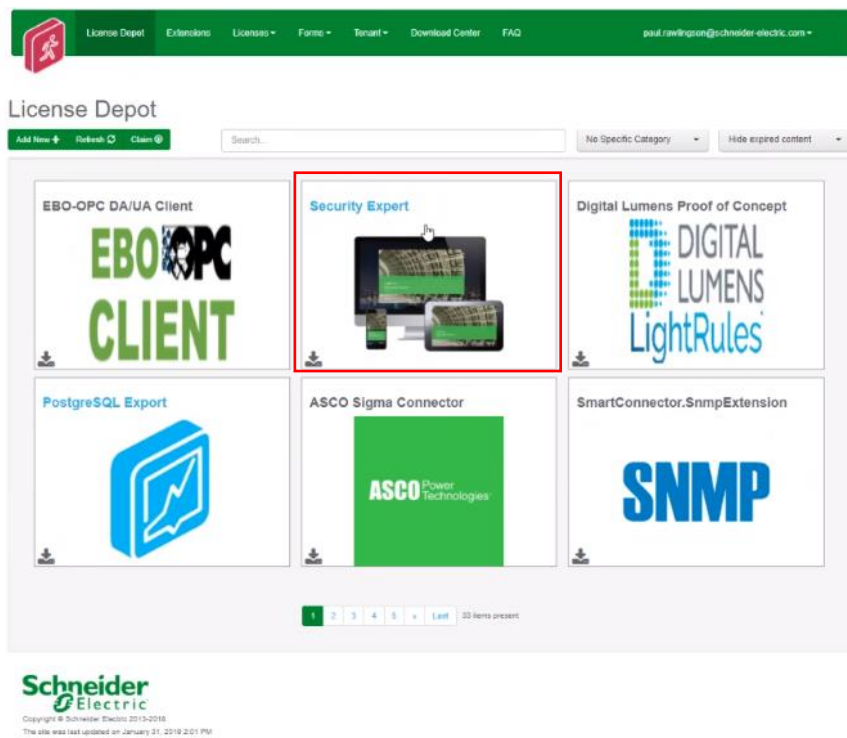
4. Copy the files to the installed directory for SmartConnector Framework (e.g. *C:\Program Files (x86)\Schneider Electric\SmartConnector*).

4.3 Install and License Security Expert SmartConnector Extension

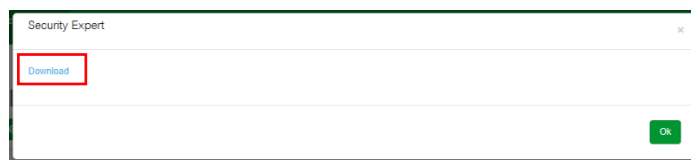
1. Visit the License Claim website at the link below:
<https://www.smartconnectorserver.com/Marketplace>

Note: You must be logged in to access the license claim page. If you are not logged in, you will be directed to do so.

2. Enter "Security Expert" into the search box of webpage.
3. Click on the Security Expert download licence button.



4. From the popup box click on the download button.



- Fill in the form with the details from your site.

License Depot Download Center FAQ

Download License

Security Expert Licence

Name *

Contact Email address *

Comments

Deployment Site *

Machine Thumbprint *

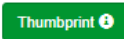
Download License


Schneider Electric
Copyright © Schneider Electric 2013-2018
The site was last updated on January 31, 2019 2:01 PM

To get the machine thumb print go to the SmartConnector web page on your machine and login to:

<http://localhost:8082>

Select setup -> License



Click on the thumbprint button  and copy the thumbprint number.

- Click on the download licence  button and download the licence file.
- Go to the SmartConnector portal <http://localhost:8082>
- Select setup -> **License**
- Select **Add+**
- Select *Security Expert License template.lic* license file.
- Select **Open**

Status Configurations EWS Servers Setup About Logged in as admin

Licenses

Refresh Thumbprint Add

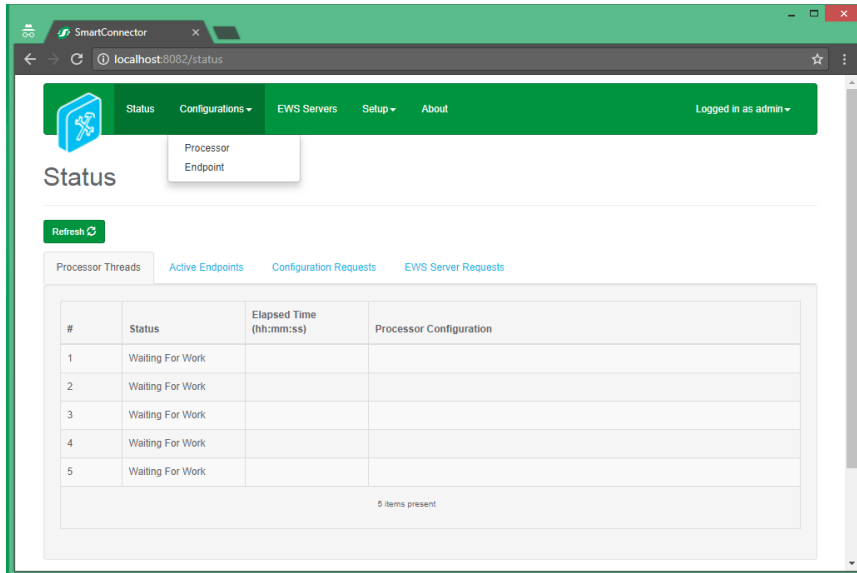
	Assembly Name	Assembly Version	Features	Licensed To	Expiration Date
	Mongoose.Service.exe	2.5.*	No custom features		Never expires
	SecurityExpertExtension	1.**	No custom features		Never expires

2 items present

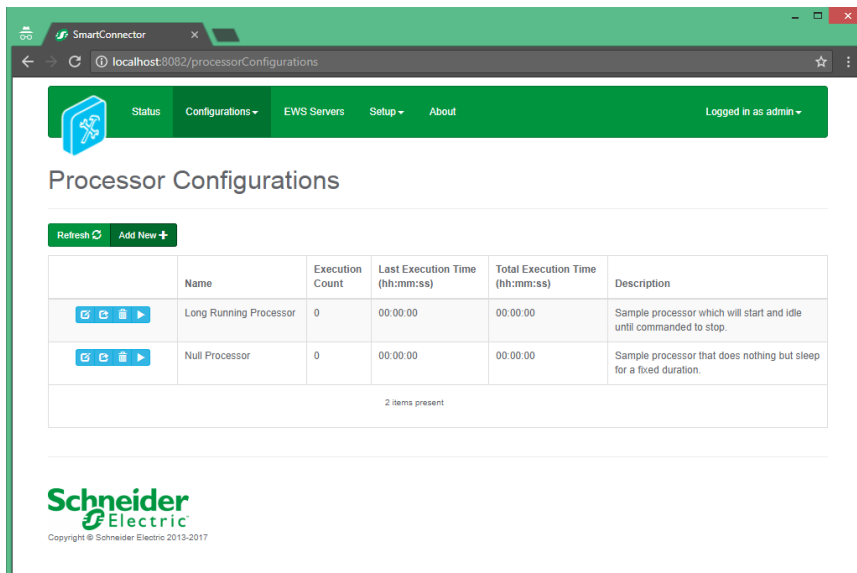
You have successfully licensed the Security Expert SmartConnector Extension.

4.4 Configure Security Expert SmartConnector Discovery Extension Processors

1. Log into the **SmartConnector Portal**. If it the SmartConnector is installed on the same machine use localhost:8082
2. Select **Configurations -> Processor**



3. From the Processor Configurations Page, press Add New + Button.



4. From the **Add Processor Configuration** Page, Select the **SecurityExpertExtension** Assembly
5. Select the **Next** Button.
6. Choose the **SecurityExpertExtension.DiscoveryProcessor** class and press the **Next** Button.
7. Give a Name and a Description for this configuration and Press the **Finish** Button.

8. On the **Process Configuration** Page, Click on the **Details** Tab.

Processor Configuration

Name: Security Expert Discovery Processor | Is Active: True

Description: Discovers all value items (and specified Event Filter alarms) from Security Expert

Processor | **Details** | Control | History | Schedule

Expand All | Collapse All

- Details
 - Security Expert Settings
 - Ews Server
 - Event Filter

9. Click the + symbol to expand the Security Expert Setting Node.

Details

- Security Expert Settings
 - Soap Endpoint *
https://ak-soap-sx.gisclab.co.uk:8040/SecurityExpertSOAPService/service.svc
 - Use Tls *
True
 - Use Ca Cert *
True
 - Certificate Path
C:\cert\SOAPSX.cer
 - Operator User Name *
admin
 - Operator Password
~ Encrypted ~
 - Database Site Id *
1
- Ews Server
- Event Filter

Update the following properties:

- **SOAP Endpoint:** Enter the SOAP address from the Security Expert machine.

- **Use TLS:** Select “True” or “False” from the drop-down list if you want to use TLS.
- **Use CA Cert:** Select “True” or “False” from the drop-down list if you want to use HTTPS communication with certificate.
- **Certificate path:** Specify the path to the encryption certificate.
- **Operator Username:** Enter the Security Expert Operator details.
- **Operator Password:** Enter the Security Expert Operator details.

Note: The Username and Password **MUST** match an Operator that has been created in Security Expert.

- **Database Site Id:** Enter the database Id of the Security Expert site

Sites						
General	Display	Active Directory	Site Defaults	User Photos Export	Biometrics	Salto
Name	Database ID	Created Date	Last Modified	Last Modified By		
Schneider Electric	1	20/08/2018 14:56:51	27/11/2020 07:01:28	Admin		

10. Expand the **EWS Server** Node and update the following properties:

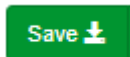
- EWS Address. Example <http://localhost:51350/EcoStruxure/DataExchange>
Note: this URL must match wherever you have installed the SmartConnector Framework and Security Expert Extension.
- Realm: **(Default)** SecurityExpert
- Server Name: **(Default)** SecurityExpertServer
- Username (your username).
- Password (your password).

Note: The Username & Password specified above is the EWS User that EcoStruxure Building Operation will authenticate with when connecting to the SmartConnector Framework – This is not an EBO User or a Security Expert Operator. The password must be a complex password.

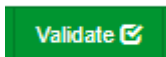
11. Expand the **Event Filter** node and update the following properties:

Event Filter Id: Enter the database id of the event filter which has been configured in Security Expert

12. Click the Save button.



13. Then click the validate button fix any errors which are displayed.



14. Click the start button to run the discovery process.




Note: The Discovery Processor only needs to be run once unless new objects are created in Security Expert – In this case you will also need to perform an EBO EWS Host of the new objects.

4.5 Configure Security Expert SmartConnector Alarm Update Extension Processors

1. From the Processor Configurations Page, press Add New + Button.
2. From the **Add Processor Configuration** Page, Select the **SecurityExpertExtension** Assembly.
3. Select the **Next** Button.
4. Choose the **SecurityExpertExtension.UpdateAlarmProcessor** class and press the **Next** Button.
5. Give a Name and a Description for this configuration and Press the **Finish** Button.
6. Click on the EWS Servers Button.



7. Click on the edit button on the Security Expert server.

	Name	URL
	SecurityExpertServer	http://localhost:51350/EcoStruxure/DataExchange?singleWsd

1 item present

8. Make a note of the EWS ID.

EWS Server

Stop ■

Contents Host

Refresh Edit Add Delete

SecurityExpertServer

Id: 4

Page Size: 1000

Address: <http://localhost:51350/EcoStruxure/DataExchange>

Realm: SecurityExpert

Auto Start: True

Allow Cookies: False

Max Received Message Size: 4000000

- Go back to the configurations page and edit the alarm update processor enter the EWS ID into the settings and click save.

Processor Configuration

Name
Security Expert Alarm Update Processor

Description
Pulls in alarms from Security Expert and updates alarm states.

Processor Details Control History Schedule

Expand All Collapse All

Details

Ews Server Id

Ews Server Id *

4

4.6 Configure Schedule on Alarm Update Processor

The following procedure will create schedules that will be used to execute the alarm update processor.

- Select **Setup -> Configuration Schedules**.
- From the **Configuration Schedules** page, select **Add New +**
- Enter 'Every 1 Seconds' in the **Description** field.
- Select the current date and time from the **Start Date** field.
- Select **Time Interval** from the **Type** field.
- Enter '1' in the **Interval Gap** field.
- Select **Seconds** from the **Interval Gap Units** field.
- Select **Save** to save the Schedule.

Description *
Every One Second

Start Date *
01/01/2020 12:00 AM

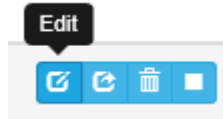
Type
Time interval

Interval Gap
1

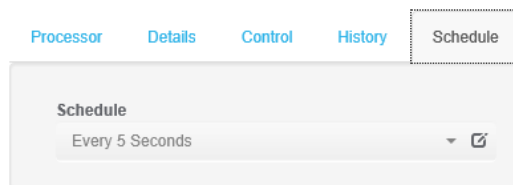
Interval Gap Units
Seconds

4.7 Assign a Schedule to Security Expert Update Alarms Processors

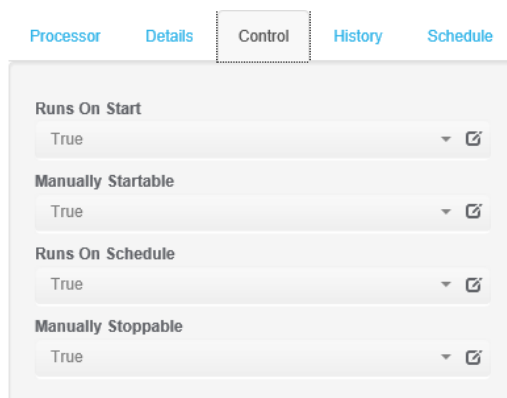
1. Select **Configurations** -> **Processor**.
2. Select **Edit** in the **UpdateAlarmsProcessor** page.



3. From there, navigate to and select the **Schedule** tab from the top.
4. Select the **“Every 5 Second”** schedule from the **Schedule** field.



5. Select the **Control** tab



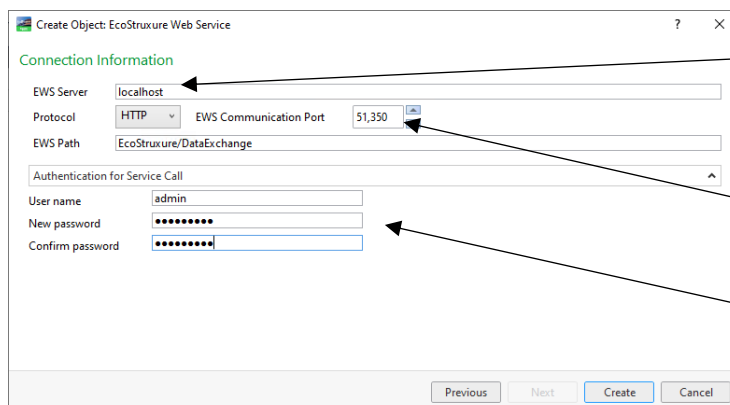
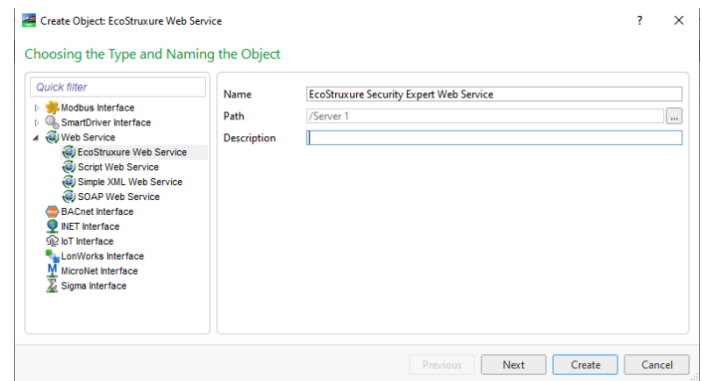
6. In the **Runs On Start** field select **True**.
7. In the **Runs On Schedule** field select **True**.
8. Select **Save** to save the changes to the Processor Configuration.

5 Host Security Expert Objects in EcoStruxure Building Operation

5.1 Create Security Expert EWS Interface in EBO

In order to create the EWS Interface for Security Expert in Building Operation, you will need to know the configuration of the EWS Endpoint, IP address (or Localhost) and the communication port number. In this example we will use the default settings

1. Select the Enterprise Server – *Server 1*
2. Select **New**
3. Select **Interface**
4. Select **Web Service**
5. Select **EcoStruxure Web Service**
6. Provide a **Name** and **Description** for the EWS Interface
Example: *Security Expert EWS Interface*
7. Select **Next**
8. Enter the EWS *Server name or IP address*
9. Select **HTTP** or **HTTPS**
10. Enter the **Port Number**
11. Enter the **EWS Path**
12. Enter the *EWS User* defined from the Security Expert SmartConnector Extension
13. Enter the *Password* for the EWS User defined in the Security Expert SmartConnector Extension



IP address or DNS name where the SmartConnector has been installed

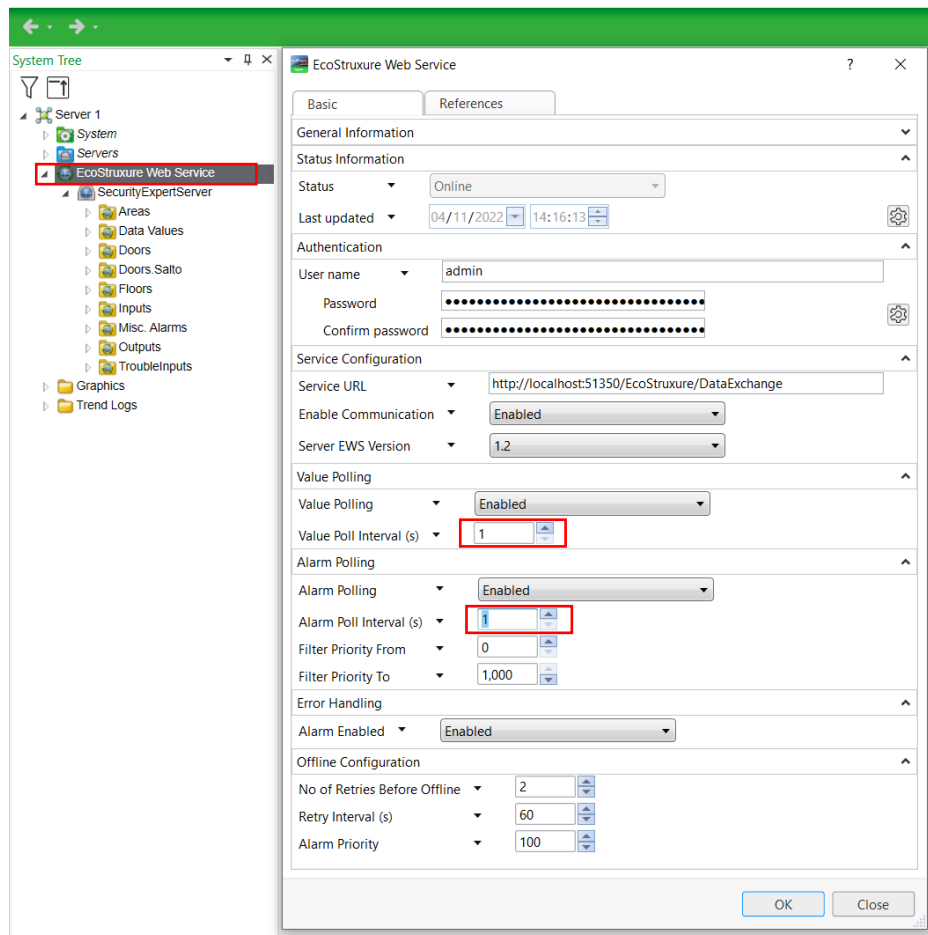
Port details as you have created in Section 4.3 step 10

User credentials as created in Section 4.3 step 10

14. Select **Create**

From the System Tree

1. Select the **EWS Interface** just created
2. Select **Properties** Tab
3. Verify that the **User** and **Password** match the setting in Security Expert SmartConnector Extension
4. Verify the **Service URL** matches the setting in the Security Expert SmartConnector Extension
5. Set the **Value Polling Interval** to 1 second
6. Set the **Alarm Polling Interval** to 1 second
7. Click **Save**



To verify communication is working properly check the following:

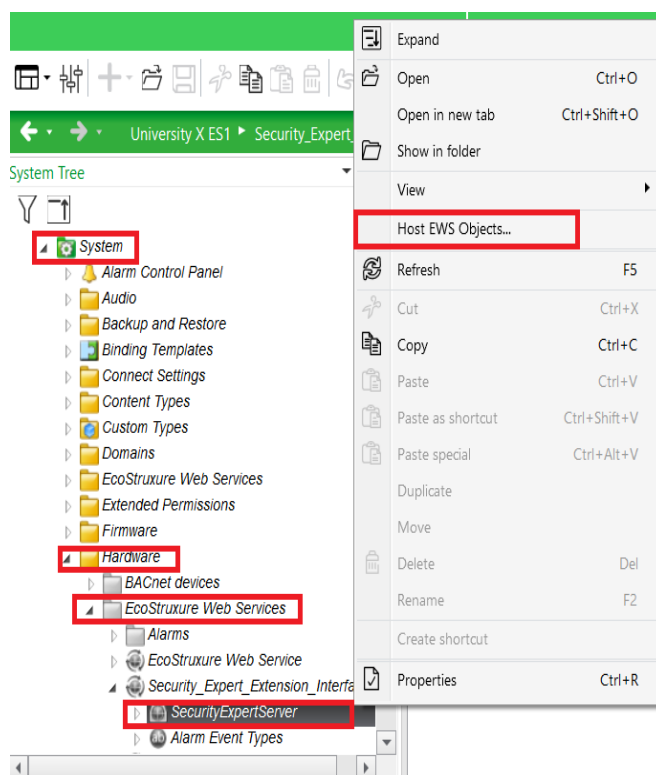
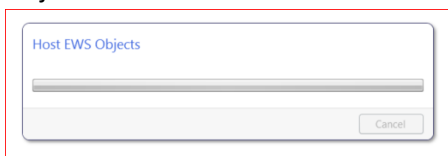
1. The version field of the EWS Interface properties page will populate with a value 1.2.
2. Wait 60 seconds and verify the interface does not go offline.

5.2 Host Security Expert Objects in EcoStruxure Building Operation

Host the EWS objects that are available from the Security Expert EWS Service, by performing the follow procedure. EcoStruxure Building Operation system will discover all objects available from Security Expert and create an object in the Building Operation database that can be used for programming, scheduling, or binding to graphics.

The following steps can be used to Host an EWS Interface

1. Open the Enterprise Server
2. Open the System folder
3. Open the Hardware folder
4. Open the EcoStruxure Web Services
5. Open the Security Expert EWS Interface
6. Right click on the Security Expert object
7. Select Host EWS Objects
8. Select the EWS Interface created in section 4.1
9. A dialog may appear “Hosting EWS Objects”
10. Upon completion of the Hosting process, close the System folder
11. Open the Security Expert EWS Interface created in section 4.1
12. The Security Expert objects will all be hosted



You can now use these objects as any other Building Operations object to bind to a program or a graphic.

6 Troubleshooting

6.1 SmartConnector Log File

SmartConnector includes integrated logging into log files where both SmartConnector extensions and the SmartConnector framework can log any messages that may be useful. These log files can be found generally in the directory **C:\ProgramData\SmartConnector\Logs** on the machine where SmartConnector is installed.

In general, if you are having problems with SmartConnector or the Security Expert extension, it may be necessary to increase the logging level, or enable additional logging filters.

1. To adjust the logging level, visit the **Service Settings** page and edit the *Logging Level setting*.

Service Settings

Refresh Edit All

Changing the values on this page may cause unpredictable results including rendering this portal non-functional. Please consult your documentation before making changes here.

Name	Description	Value
Instance Name	Name of the service	SmartConnector
Logging Level	Application wide logging level	Trace
Password Age Limit	Maximum number of days before a password must be changed	60
Portal Address	Address of the SmartConnector Portal	http://127.0.0.1:8082
Processor Runtime Limit	The maximum allowed time (in seconds) a non-ILongRunningProcessor is given to complete before it is terminated as unresponsive	600
Worker Manager Sleep	Time in mSec which the worker manager will sleep while waiting for workers to complete or for new work to be available	5000
Worker Thread Count	Number of worker threads which are allocated to execute processes	5

2. To adjust the logging filters, visit the **Logging Filters** page. The logging filters most likely to pertain to this solution is **Processor** and **Ews Serve**.

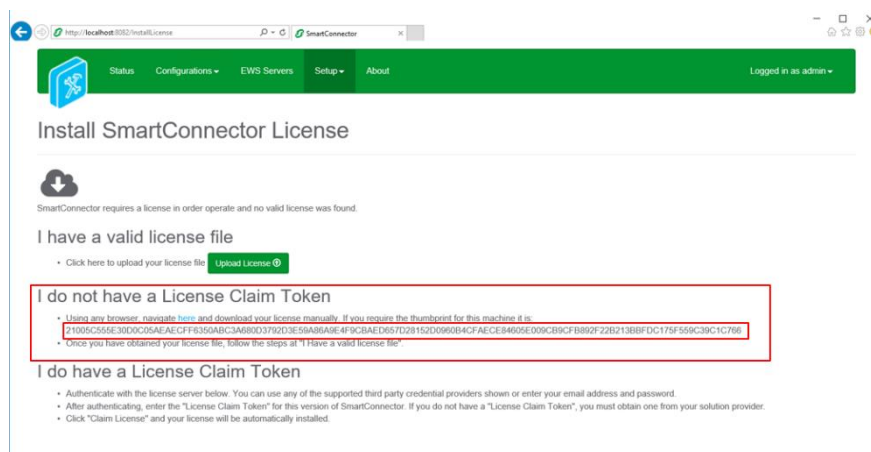
Logging Filters

Refresh Edit All Add Category All None

Category	Include in Logs
Api	False
Csp Client	False
Database	False
Ews Consume	False
Ews Serve	True
Licensing	False
Other	False
Portal	False
Processor	True

6.2 Framework Licensing Error

If you navigate to the SmartConnector portal and see a page similar to the below screenshot. This means that either you have not yet got a license for your SmartConnector framework, or your current license is no longer valid.



If you have not yet got a license for your SmartConnector framework:

Follow the instructions in the section Install SmartConnector Framework Runtime License.

If you have already got a license for your SmartConnector framework:

The SmartConnector framework license is bound to a machine thumbprint. This machine thumbprint is a key generated from multiple hardware components of your machine, including the current network adapter that was being used when the license was generated. If you have switched to a different network adapter (e.g. going from a hard-wired connect to a WIFI connection), then it is very likely this machine thumbprint has changed. Please follow the section Install SmartConnector Framework Runtime License using your new thumbprint.

6.3 SmartConnector Extension Licensing Error

If your Security Expert SmartConnector extension processors are not running, please verify that they contain a valid license by:

1. Navigate to the processor's configuration page.
2. Click on the 'Validate' button.
3. If the error displayed is "License not found." You will need to obtain a license for the extension.

If you have not yet got a license for your Security Expert SmartConnector extension

Follow the instructions in the section Install and License Security Expert SmartConnector Extension.

If you have already got a license for your Security Expert SmartConnector extension

The Security Expert SmartConnector extension license is bound to a machine thumbprint. This machine thumbprint is a key generated from multiple hardware components of your machine, including the current network adapter that was being used when the license was generated. If you have switched to a different network adapter (e.g. going from a hard-wired connection to a WIFI connection), then it is very likely this machine thumbprint has changed. Please follow the section Install and License Security Expert SmartConnector Extension using your new thumbprint.

6.4 SQL Authentication Error

If SmartConnector cannot connect to its database, then the framework will fail to start. If you notice that the SmartConnector Server is not starting, or starting and instantly stopping, please review the SmartConnector logs for messages pertaining to SQL Authentication. If this is the case, you may need to make sure that your SQL Credentials are valid before starting the SmartConnector service.

6.5 Security Expert Communication Error

If the Security Expert SmartConnector extension is unable to make a valid connection to Security Expert. The SmartConnector log will display that this has occurred. If you are having problems where it seems you may not be getting the data that you expect, or no data at all. Please check the SmartConnector logs for information about what may be going on.

6.6 EWS Communication Errors

If EBO is unable to make a connection to the EWS server created by the Security Expert SmartConnector extension. First check the SmartConnector logs for any information, such as authentication or other errors. If no errors are shown in the log, check the following.

- The IP address/ hostname configured in EBO is valid for connecting to the EWS Server in SmartConnector.
- The port configured in the EWS Server in SmartConnector is the same port in EBO.
- The endpoint configured in the EWS Server in SmartConnector (everything after the port number e.g. <http://localhost:51350/EcoStruxure/DataExchange>) is the same as the endpoint in EBO.
- Firewall rules allow this connection to occur.

7 Appendix A – Hierarchy of points

EcoStruxure Building Operation will be able to host the following types of objects from the Security Expert system. Each type of object will have a Name of the object, a description of the object, an indication whether the value is able to be read or written and finally a comment column indicating the values expected values that the object might contain.

Users can also host the Alarm Items for the object which enables the user to customize the action to take place in EcoStruxure Building Operation when the alarm is active.

7.1 Folders

Name	Description	Read/Write
Doors	Doors in the building	Read Only
Floors	Floors in the system	Read Only
Salto	Salto Door Objects	Read Only
Inputs	Input objects	Read Only
Outputs	Output objects	Read Only
Misc. Alarms	Extra alarms	Read Only
Areas	Areas in the system	Read Only
Data Values	Data Values from system	Read Only
Trouble Input	Trouble Input Status	Read Only

7.2 Doors

Value Item	Description	Read/Write	Notes
Lock Status	Door Lock Status	Read Only	Possible Values: 0 -Locked 1 -Unlocked by user 2 -Unlocked by schedule 3 -Unlocked by user timed 4 -Unlocked by user latched 5 -Unlocked by exit device 6 -Unlocked by entry device 7 -Unlocked by Operator 8 -Unlocked by operator timed 9 -Unlocked by operator latched 10 -Unlocked by area 11 -Unlocked by fire alarm 12 -Unlocked by calendar action 13 -Unlocked by calendar action 14 -Unlocked by user using extended door time 15 -Unlocked by exit device using extended door time 16 -Unlocked by entry device using extended door time

			<p>17 -Unlocked by operator using extended door time</p> <p>18 -Locked using extended door time</p> <p>19 -Lockdown – Entry Allowed</p> <p>20 -Lockdown – Exit Allowed</p> <p>21 -Lockdown – Entry/Exit Allow</p> <p>22 -Full Lockdown</p> <p>23 -Not locked (in the locked state but not secure)</p> <p>24 -Not locked (in the locked by calendar action state but not secure)</p> <p>100 Set by SmartConnector so EBO can change Lock Status to any state</p>
--	--	--	---

Position Status	Door Position Status	Read Only	<p>Possible Values:</p> <p>0 -Secure</p> <p>1 -Open</p> <p>2 -Open alert</p> <p>3 -Left Open</p> <p>4 -Forced Open</p> <p>5 -Bonding fault</p>
Lock Control	Door Lock Control	Read/Write	<p>Possible Values:</p> <p>0 -Lock door</p> <p>1 -Unlock door</p> <p>2 -Unlock door latched</p> <p>3 -Door lockout entry</p> <p>4 -Door lockout exit</p> <p>5 -Door lockout entry exit</p> <p>6 -Door lockout clear</p>

7.3 Salto Door Objects

Value Item	Description	Read/Write	Notes
Lock Control	Door Lock Control	Write	<p>Possible values:</p> <p>0 -Open</p> <p>1 - Emergency Open</p> <p>2 - Emergency Close</p> <p>3- End Emergency</p> <p>*Salto model dependent not all values supported on all devices</p>

7.4 Floors

Value Item	Description	Read/Write	Notes
Floor # Activation Status	Activated or Deactivate floor	Read/Write	<p>Possible values:</p> <p>0 -Deactivate</p> <p>1 -Activate</p> <p>2 -Activate Timed</p>

7.5 Inputs

Value Item	Description	Read/Write	Notes
Status	Input's status	Read Only	Possible values: 0 -Closed/Off 1 -Open/on 2 -Tamper 3 -Short Circuit
Bypass	Input's bypass state	Read Only	Possible Values: 0 -Not bypassed 1 -input bypassed 2 -Siren Lockout 3 -Bypass latched
[Input Name] Bypass Control	Bypass Control	Read/Write	Possible Values: 0 -Remove Bypass 1 -Bypass until next disarm 2 -Bypass permanently

7.6 Outputs

Value Item	Description	Read/Write	Notes
Activation Status	Output's status	Read Only	0 = Off, 1 = On, 2 = Pulse On, 3 = On timed, 4 = On pulse timed
Activation Time	Time since activated	Read Only	Seconds (integer)
Activation Control	Activation control	Read/Write	0 = Deactivate, 1 = Activate, 2 = Activate timed

7.7 Miscellaneous Alarms

Alarm Item	Description	Read/Write	Notes
[Event Name]	Alarms that don't fit in other folders	Read Only	Dynamically created by Event Filter

7.8 Areas

Value Item	Description	Read/Write	Notes
Arm Status	Area Arm Status	Read Only	Possible values: 0 = Disarmed, 1 = Input(s) open waiting for user, 2 = Trouble Condition waiting for user 3 = Bypass error waiting for user, 4 = Bypass warning waiting for user, 5 = User count not zero waiting for user, 6 = Unknown, - = -, 127 = Unknown, 128 = Armed, 129 = Exit delay, 130 = Entry delay, 131 = Disarm delay, 132 = Code delay
24 Hr Status	24 Hour Area Status	Read Only	0 = Disabled, 1 = Busy, 128 = Enabled
Notification Bits Alarm activated	Extra area information	Read Only	True / False
Notification Bits Siren activated	Extra area information	Read Only	True / False
Notification Bits Alarms in memory	Extra area information	Read Only	True / False
Notification Bits Remote armed	Extra area information	Read Only	True / False
Notification Bits Force armed	Extra area information	Read Only	True / False
Notification Bits Instant armed	Extra area information	Read Only	True / False
Notification Bits Partial armed	Extra area information	Read Only	True / False
Arm Control	Arm or disarm an area	Read/Write	0 = Disarm area, 1 = Disarm 24 hour, 2 = Disarm all, 3 = Arm area, 4 = Force arm area, 5 = arm area instant, 6 = Force arm area instant, 7 = Walk test enable, 8 = Walk test disable, 9 = Silence alarm, 10 = Arm area stay, 11 = Arm area 24

7.9 Data Values

Value Item	Description	Read/Write	Notes
Data Values	Data values which are created in Security Expert	Read Only	Number

7.10 Trouble Input

Value Item	Description	Read/Write	Notes
Trouble Input	Trouble Input Status	Read Only	Possible values: 0 = Off 1 = On

8 Appendix B – Filtering Alarms

To filter unwanted alarms from EcoStruxure Building Operation carry out the following tasks:

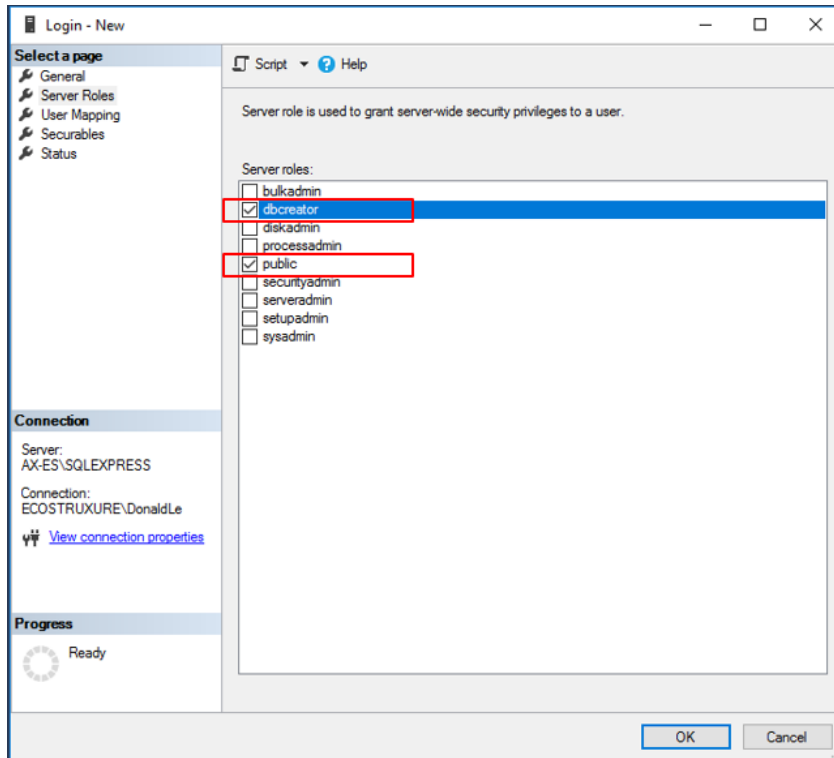
1. Navigate to the folder which contains the alarm object.
2. Open the alarm object.
3. Click on presentation tab.
4. Tick the box Auto Hide.

The screenshot shows the 'System Tree' on the left with the 'Door Forced Open' alarm object selected. The main window displays the 'Presentation' configuration tab for this alarm. The 'Auto hide' checkbox is checked, which will prevent the alarm from being displayed in the alarm banner.

This will stop the alarms from being displayed in the alarm banner.

9 Appendix C – SQL User Roles

The Windows user installing the SmartConnector Framework software must have 'dbcreator' and 'public' roles within SQL in order for SmartConnector Framework to install correctly. During the installation process of SmartConnector Framework the database tables necessary for configuring the system will be created.



Note: If the logged in Windows User did not have the proper SQL user roles during the installation process, the DB tables will not be created. You will need to *uninstall* then *reinstall* SmartConnector Framework to create the tables, once the Windows User has proper SQL roles defined. An attempt to perform an installation selecting "Modify" or "Repair" will not create the default DB for SmartConnector Framework.

10 Appendix D – Security Expert Cross Controller Operations

If Security Expert reassigns objects to other controllers, then the Discovery Processor will need to be run for that site. This can occur for example if say an area is modified so that it has more I/O connected and reassigned to a new controller. In this case the Ews Server hosted would be out of date . The area in this example would have a new parent. Deleting the host and running the Discovery Processor is required to update the changes in the Security Expert system. It would also be required to change the Ews Server Id in the associated Alarm Update Processor to match the newly created Ews server.

11 Appendix E – Security Expert Multi-Site Configuration

Support has now been added for supporting multiple Security Expert sites using multiple instances of the Security Expert SmartConnector extension.

Each Security Expert site now has its own Security Expert SmartConnector Extension.

A Discovery Processor is used to create the Ews Host Server for the required site.

The Alarm Update Process then has a new detail parameter called Ews Server Id that requires the Id of the discovered Ews server, to link it to the Alarm Update Processor.

The image below shows two instances of the Security Expert Extension processors to cover two different sites. Each site has its own settings.

	Name	Execution Count	Last Execution Time (hh:mm:ss)	Total Execution Time (hh:mm:ss)	Description
	Security Expert Alarm Update Processor	101768	00:00:00	06:07:05	Pulls in alarms from Security Expert and updates alarm states.
	Security Expert Alarm Update Processor 3	34969	00:00:00	15:27:35	Pulls in alarms from Security Expert and updates alarm states.
	Security Expert Discovery Processor	46	00:02:40	00:23:27	Discovers all value items (and specified Event Filter alarms) from Security Expert
	Security Expert Discovery Processor 3	12	00:00:22	00:02:16	Discovers all value items (and specified Event Filter alarms) from Security Expert

4 items present

12 Revision History

Version	File Details	Date
1.0.0.0	Document Issued for Comments	17 December 2020
1.0.0.1	Document Update as per Beta Comments	20 January 2021
1.0.0.2	Document Update as per final comments	22 March 2021
1.0.0.3	Document Update for release	31 March 2021
1.0.0.4	Document Updated with Security Expert Version	06 July 2022
1.0.0.5	Document updated for release 1.1.0.8	30 October 2022
1.0.0.6	Document updated for release 1.2.0.17 (Added the functionality to use TLS and SSL certificates to communicate with SOAP)	3 February 2025
1.0.0.7	Document updated for release 1.2.0.22 Fix for Alarm updates for TLS after processor restart.	13 February 2025

13 References

SmartConnector Installation and Configuration Guide.pdf

SmartConnector Version 2.5 Release Notes.pdf

[SmartConnector Manuals](#)

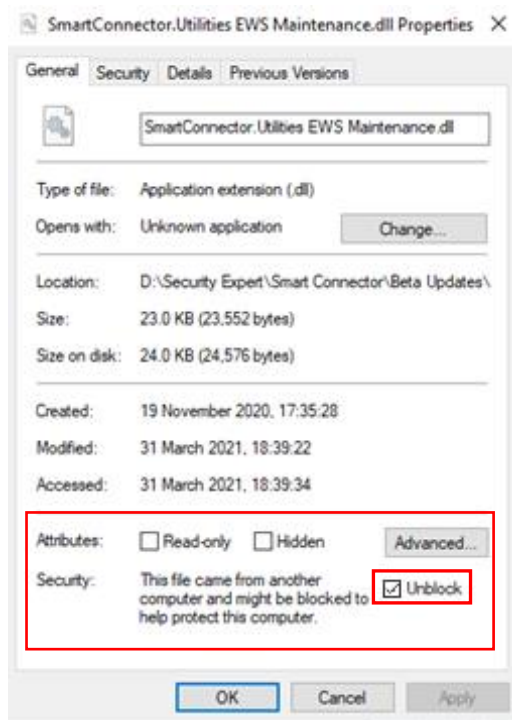
14 SmartConnector Maintenance

SmartConnector uses an SQL database which needs to have regular maintenance performed on it to keep the size of the database within an acceptable limit. To help with the task of carrying out database maintenance a SmartConnector extension has been created which can be scheduled to run every night and perform database maintenance.

14.1 Maintenance Processor Installation

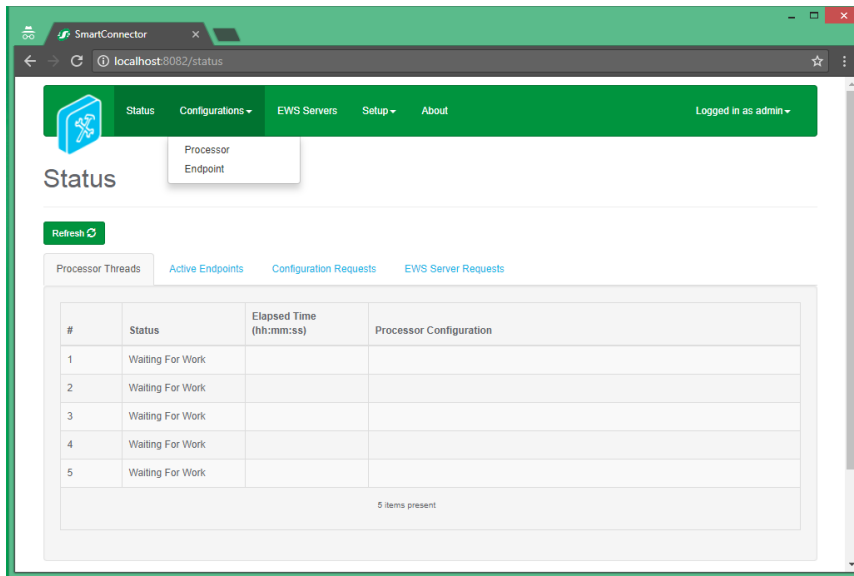
To install the Smart Connector EWS Maintenance processor follow the steps below.

1. Extract the files from the SmartConnector. Utilities EWS Maintenance zip file to a temporary directory
2. Right click on each file and select Properties
3. Verify the file is not blocked – see screen shot below; if the file is blocked, select Unblock.

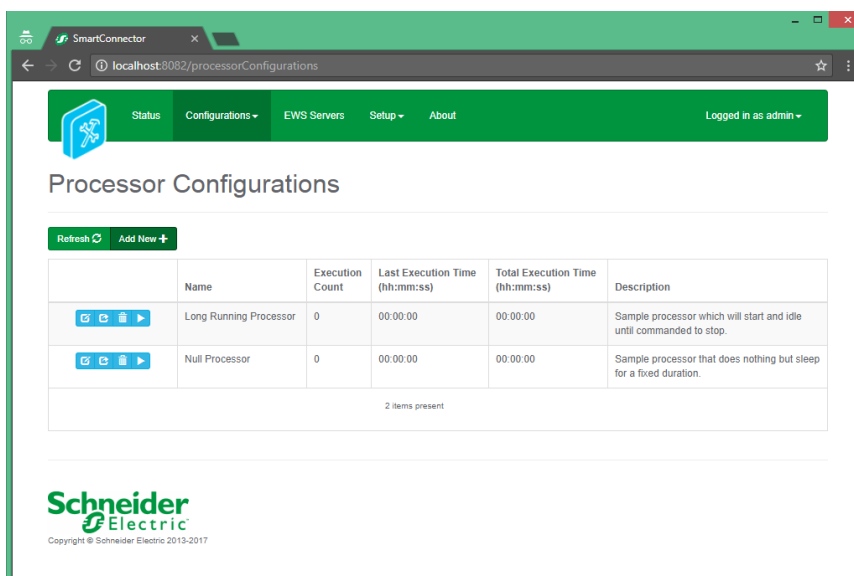


4. Copy the files to the installed directory for SmartConnector Framework (e.g. C:\Program Files (x86)\Schneider Electric\SmartConnector).
5. Log into the **SmartConnector Portal**. If the SmartConnector is installed on the same machine use localhost:8082

6. Select **Configurations -> Processor**



7. From the Processor Configurations Page, press Add New + Button.



8. From the **Add Processor Configuration** Page, Select the **SmartConnector.Utilities Extension Assembly**.

9. Give a Name and a Description for this configuration and Press the **Finish** Button.

10. On the **Process Configuration** Page, Click on the **Details** Tab.

11. Expand the **SmartConnector Ews Server settings** Node and update the following properties:

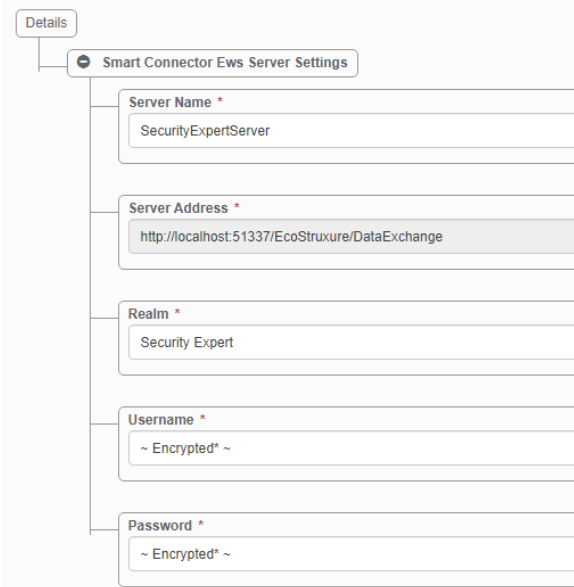
Server Name : EWS Server Name (**Default:** SecurityExpertServer)

Server Address : EWS Server Address (**Default**
<http://localhost:51350/EcoStruxure/DataExchange>)

Realm: EWS Realm (**Default:** SecurityExpert)

EWS Username: Username for EWS Server

EWS Password: Password for EWS Server



Details

Smart Connector Ews Server Settings

Server Name *
SecurityExpertServer

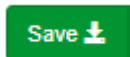
Server Address *
http://localhost:51337/EcoStruxure/DataExchange

Realm *
Security Expert

Username *
~ Encrypted* ~

Password *
~ Encrypted* ~

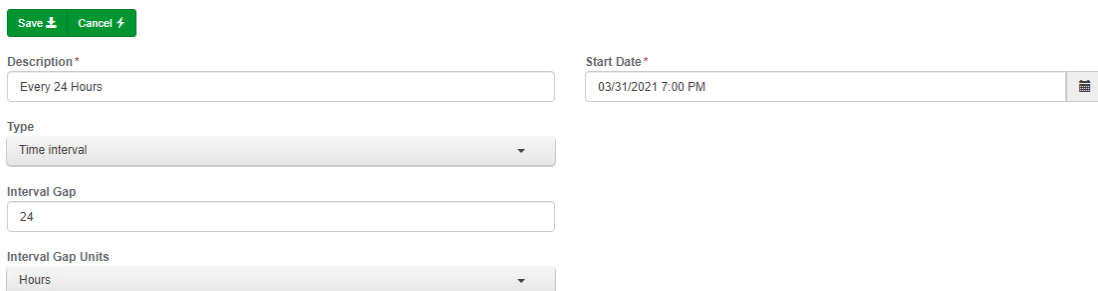
12. Click the Save button





14.2 Maintenance Schedule Creation

The following procedure will create schedules that will be used to execute the alarm update processor.

1. Select **Setup -> Configuration Schedules**.
2. From the **Configuration Schedules** page, select **Add New +**
3. Enter *'Every 24 Hours'* in the **Description** field
4. Select the current date and time from the **Start Date** field
5. Select **Time Interval** from the **Type** field
6. Enter *'24'* in the **Interval Gap** field
7. Select **Hours** from the **Interval Gap Units** field
8. Select **Save** to save the Schedule



Save  Cancel 

Description *
Every 24 Hours

Start Date *
03/31/2021 7:00 PM

Type
Time interval

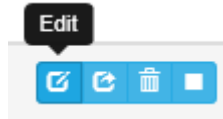
Interval Gap
24

Interval Gap Units
Hours

14.3 Assign a Schedule to the Maintenance Processors

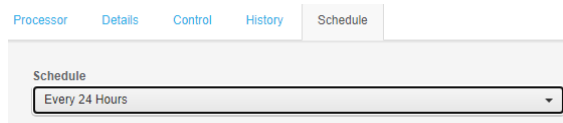
9. Select **Configurations** -> **Processor**.

10. Select **Edit** in the **SmartConnector Maintenance Processor** page.

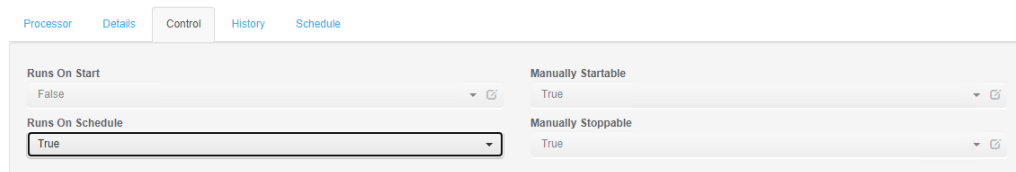


11. From there, navigate to and select the **Schedule** tab from the top

12. Select the **Every 24 Hours** schedule from the **Schedule** field.



13. Select the **Control** tab.



14. In the **Runs On Schedule** field select **True**.

15. Select **Save** to save the changes to the Processor Configuration.