EcoStruxure Secure Connect Advisor

Premium Domain Admin Guide For GateManager

12/2017

EIO0000002732.02

www.schneider-electric.com

Schneider Electric

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

You agree not to reproduce, other than for your own personal, noncommercial use, all or part of this document on any medium whatsoever without permission of Schneider Electric, given in writing. You also agree not to establish any hypertext links to this document or its content. Schneider Electric does not grant any right or license for the personal and noncommercial use of the document 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.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When devices are used for applications with technical safety requirements, the relevant instructions must be followed.

Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this information can result in injury or equipment damage.

TRADEMARKS

Schneider Electric has made every effort to supply trademark information about company names, products, and services mentioned in this manual.

Vijeo Designer, Vijeo XD, Vijeo XL, Vijeo Design'Air and SoMachine are either registered trademarks or trademarks of Schneider Electric.

iPC (Industrial Personal Computer) is either registered trademark or trademark of Schneider Electric.

Microsoft, Windows, Windows Vista, Windows Server, Internet Explorer, Windows Media, Excel, Visio, DirectX, Visual Basic, Visual C++, and Visual Studio are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

GateManager, LinkManager, SiteManager, are registered trademarks of Secomea A/S.

All other brands and products referenced in this document are acknowledged to be the trademarks or registered trademarks of their respective holders.

Table of Contents

Safety Information 5
About the Book 9
Chapter 1 Introduction 11
Prerequisites on Using This Guide 12
Concept of EcoStruxure Secure Connect Advisor 13
Operating Environment 15
Supported Model List 16
License and System Configuration 17
Chapter 2 Premium Domain Admin Guide 21
First Time Login to the GateManager Web Graphical User Interface (GUI) 22
SiteManager Configuration Backup 25
Accessing the Web GUI of a SiteManager 26
Accessing the Web GUI of a LinkManager 27
Organize Equipment in Domains and Provide LinkManager Access to Specific Equipment 28
Understanding Audit Logs 36
Working with Alerts 37
Working with Actions 40
Combining Alerts and Actions 42
Working with the Replace Appliance Function 44
GateManager Administrator GUI FAQ 45
Glossary 47

Safety Information

Important Information

NOTICE

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result** in minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

PLEASE NOTE

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

BEFORE YOU BEGIN

Do not use this product on machinery lacking effective point-of-operation guarding. Lack of effective point-of-operation guarding on a machine can result in serious injury to the operator of that machine.

⚠ WARNING

UNGUARDED EQUIPMENT

- Do not use this software and related automation equipment on equipment which does not have point-of-operation protection.
- Do not reach into machinery during operation.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

This automation equipment and related software is used to control a variety of industrial processes. The type or model of automation equipment suitable for each application will vary depending on factors such as the control function required, degree of protection required, production methods, unusual conditions, government regulations, etc. In some applications, more than one processor may be required, as when backup redundancy is needed.

Only you, the user, machine builder or system integrator can be aware of all the conditions and factors present during setup, operation, and maintenance of the machine and, therefore, can determine the automation equipment and the related safeties and interlocks which can be properly used. When selecting automation and control equipment and related software for a particular application, you should refer to the applicable local and national standards and regulations. The National Safety Council's Accident Prevention Manual (nationally recognized in the United States of America) also provides much useful information.

In some applications, such as packaging machinery, additional operator protection such as point-of-operation guarding must be provided. This is necessary if the operator's hands and other parts of the body are free to enter the pinch points or other hazardous areas and serious injury can occur. Software products alone cannot protect an operator from injury. For this reason the software cannot be substituted for or take the place of point-of-operation protection.

Ensure that appropriate safeties and mechanical/electrical interlocks related to point-of-operation protection have been installed and are operational before placing the equipment into service. All interlocks and safeties related to point-of-operation protection must be coordinated with the related automation equipment and software programming.

NOTE: Coordination of safeties and mechanical/electrical interlocks for point-of-operation protection is outside the scope of the Function Block Library, System User Guide, or other implementation referenced in this documentation.

START-UP AND TEST

Before using electrical control and automation equipment for regular operation after installation, the system should be given a start-up test by qualified personnel to verify correct operation of the equipment. It is important that arrangements for such a check be made and that enough time is allowed to perform complete and satisfactory testing.

⚠ WARNING

EQUIPMENT OPERATION HAZARD

- Verify that all installation and set up procedures have been completed.
- Before operational tests are performed, remove all blocks or other temporary holding means used for shipment from all component devices.
- Remove tools, meters, and debris from equipment.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Follow all start-up tests recommended in the equipment documentation. Store all equipment documentation for future references.

Software testing must be done in both simulated and real environments.

Verify that the completed system is free from all short circuits and temporary grounds that are not installed according to local regulations (according to the National Electrical Code in the U.S.A, for instance). If high-potential voltage testing is necessary, follow recommendations in equipment documentation to prevent accidental equipment damage.

Before energizing equipment:

- Remove tools, meters, and debris from equipment.
- Close the equipment enclosure door.
- Remove all temporary grounds from incoming power lines.
- Perform all start-up tests recommended by the manufacturer.

OPERATION AND ADJUSTMENTS

The following precautions are from the NEMA Standards Publication ICS 7.1-1995 (English version prevails):

- Regardless of the care exercised in the design and manufacture of equipment or in the selection and ratings of components, there are hazards that can be encountered if such equipment is improperly operated.
- It is sometimes possible to misadjust the equipment and thus produce unsatisfactory or unsafe operation. Always use the manufacturer's instructions as a guide for functional adjustments. Personnel who have access to these adjustments should be familiar with the equipment manufacturer's instructions and the machinery used with the electrical equipment.
- Only those operational adjustments actually required by the operator should be accessible to the operator. Access to other controls should be restricted to prevent unauthorized changes in operating characteristics.

About the Book

At a Glance

Document Scope

This document helps you get started with hosted GateManager of EcoStruxure Secure Connect Advisor in relation to the GateManager Domain Administration.

This guide assumes that you have a subscription to a Schneider Electric Connect Pack or Trial and have ordered the GateManager PREMIUM up-grade, and then had your GateManager administrator account upgraded with Domain Administration features.

This document does not explain all the features and possibilities of the GateManager Domain Administrator, but only the more commonly used features for administering SiteManager and LinkManager.

NOTE: Read and understand this document and all related documents before installing, operating, or maintaining your EcoStruxure Secure Connect Advisor.

The Vijeo Designer (VJD) or Vijeo XD (VXD) users should read through the entire document to understand all features. See *Vijeo Designer* or *Vijeo XD*.

Validity Note

This document has been updated for the release of Vijeo Designer V6.2 SP6, SoMachine V4.3 and Vijeo XD V3.0.

Related Documents

Title of Documentation	Reference Number
EcoStruxure Secure Connect Advisor User Guide for GateManager	*EIO0000002449 (ENG)* *EIO0000002563 (FRE)* *EIO0000002564 (GER)* *EIO0000002565 (ITA)* *EIO0000002566 (SPA)* *EIO0000002567 (CHS)*
EcoStruxure Secure Connect Advisor Troubleshooting Guide for LinkManager (Starting and Connecting)	*EIO0000002450 (ENG)* *EIO0000002568 (FRE)* *EIO0000002569 (GER)* *EIO0000002570 (ITA)* *EIO0000002571 (SPA)* *EIO0000002572 (CHS)*

Title of Documentation	Reference Number
EcoStruxure Secure Connect Advisor User Guide for Security Setting	*EIO0000002451 (ENG)* *EIO0000002573 (FRE)* *EIO0000002574 (GER)* *EIO0000002575 (ITA)* *EIO0000002576 (SPA)* *EIO0000002577 (CHS)*
EcoStruxure Secure Connect Advisor Troubleshooting Guide for SiteManager	*EIO0000002452 (ENG)* *EIO0000002578 (FRE)* *EIO0000002579 (GER)* *EIO0000002580 (ITA)* *EIO0000002581 (SPA)* *EIO0000002582 (CHS)*

You can download these technical publications and other technical information from our website at http://www.schneider-electric.com/en/download

Chapter 1
Introduction

What Is in This Chapter?

This chapter contains the following topics:

Topic	Page
Prerequisites on Using This Guide	12
Concept of EcoStruxure Secure Connect Advisor	13
Operating Environment	15
Supported Model List	16
License and System Configuration	17

Prerequisites on Using This Guide

Prerequisites

Prerequisites on using this guide are:

- You have administrator privileges to install a program on your Windows PC.
- Your PC has outgoing access to the Internet through https. This applies to both your corporate firewall and any personal firewall installed on your PC.
- You have a SiteManager Embedded license.
- You have received, by email, a GateManager `Domain Administrator` certificate with a link to the GateManager `Web` portal.

Concept of EcoStruxure Secure Connect Advisor

What Is EcoStruxure Secure Connect Advisor?

When you want to display or operate on a personal computer or smart device, the screens of display units in remote locations, you need a system to prevent unauthorized access from external sources.

With EcoStruxure Secure Connect Advisor serving the role of router, as long as you have an Internet connection, you can construct such a system.

EcoStruxure Secure Connect Advisor is structured to connect safely display units on the work site (SiteManager), with computers or smart devices in the office (LinkManager), over a server (GateManager).

- GateManager:
  Server for creating a safe encrypted connection between display units on the work site (SiteManager) and personal computers or smart devices in the office (LinkManager). You can use GateManager to check the network connection status of SiteManager and LinkManager. The GateManager `Administrator` registers the SiteManager and LinkManager and allows access to the network.
- SiteManager:
  Display unit having SiteManager Embedded running is called SiteManager. Setup for accessing the network is handled from the software; SiteManager Embedded.

- LinkManager:
  Software installed on the computers. It allows remote access to SiteManager and/or devices represented by agents on the SiteManager. Setup for accessing the network is handled by GateManager. For remote monitoring and operation, you can use data collection and remote monitoring software as the LinkManager.
  Different configurations are possible depending on the package which you purchase. Refer to the license that comes with each package:
  - Webgate
  - SoMachine
  - Vijeo Designer
  - Vijeo XD

⚠ WARNING

EQUIPMENT DAMAGE

- Before performing maintenance, ensure by phone that you have on-site agreement.
- Before any update, ensure that you have a stable Internet and electricity environment.
- More particularly, do not use 3G through a mobile phone setup as tethering hotspot for any update.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Operating Environment

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

This product must be installed and configured by qualified software installation staff with administrator rights.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

The following table lists the system requirements for EcoStruxure Secure Connect Advisor.

Requirements	Description
Models for SiteManager	For a list of the display unit models that support EcoStruxure Secure Connect Advisor, refer to Supported Model List *(see page 16)*.
PC for GateManager/LinkManager	Windows PC/AT compatible machine
Operating system	• GateManager/LinkManager Windows 8/Windows 8.1/Windows 7/Windows Vista (All editions for 32/64 bit versions). • SiteManager For information about the operating system installed on a display unit, refer to its corresponding hardware manual.
Other non-operating-system programs	Browsers: Internet Explorer 9 or later, Google Chrome, Apple Safari, Mozilla Firefox.
Network settings	Port/Protocol: SiteManager runs all its communication using one of the following ports or protocols. Use in an environment that supports the port or protocol. • Port 11444 • Port 443 with HTTPS/TLS • Port 80 with TLS over HTTP • TLS through Web-proxy For details, refer to EcoStruxure Secure Connect Advisor Troubleshooting Guide for LinkManager (LinkManager connection methods).

Supported Model List

You can register the following display units as SiteManager:
- Magelis industrial PC (iPC) series
- Magelis HMI series

NOTE: Available models differ depending on the screen editing software you are using. For more information, refer to the manuals that came with your screen editing software.

IPC Series

For details about the reference, refer to the corresponding hardware manual for your display unit.

iPC	Model	Part number series
S-Panel iPC	S-Panel iPC Performance and Optimized	HMIPSP, HMIPEP, and HMIPSO
Box iPC	Box iPC Modular and Display Universal and Performance	HMIBMU and HMIBMP
	Box iPC Universal	HMIBSU

HMI Series

For details about the reference, refer to the corresponding hardware manual for your display unit.

HMI	Model	Part numbers
HMIGTU	HMIGTU terminals*1	HMIG3U HMIG5U HMIG5U2
HMIGTO	HMIGTO terminals	HMIGTO1310 HMIGTO2310 - HMIGTO2315 HMIGTO3510 HMIGTO4310 HMIGTO5310 - HMIGTO5315 HMIGTO6310 - HMIGTO6315
*1 For the display modules you can mount, refer to the Hardware Manual.		

NOTE: Vijeo XD supports only HMIGTU.

License and System Configuration

License Format

License formats are divided largely into two groups:

- SiteManager Embedded Basic
- SiteManager Embedded Extended

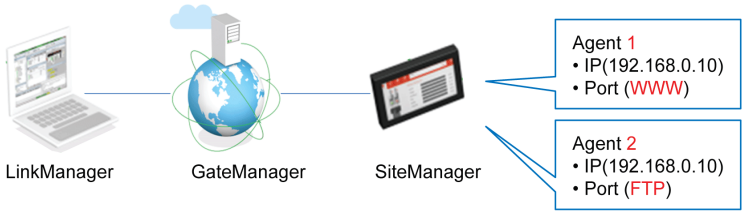
NOTE: The combination of licenses, which you purchase changes the system configurations you can have.

SiteManager Embedded Basic

Only for accessing a display unit itself, you can register up to 2 Agents (access methods) per display unit.

When the display unit has multiple Ethernet interfaces, you can set up an Agent for each interface.

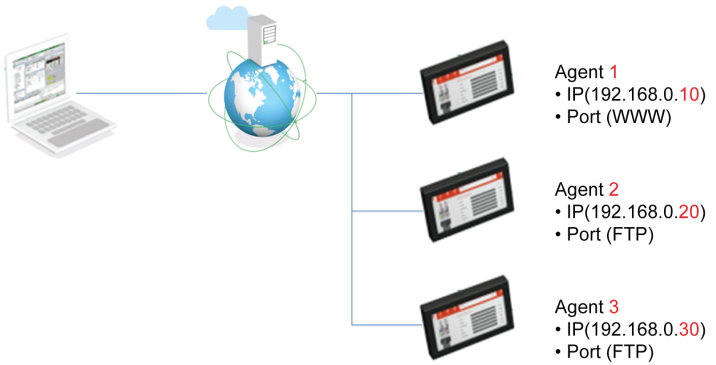
When different ports are used with a single interface, you can set up an Agent for each port.



SiteManager Embedded Extended

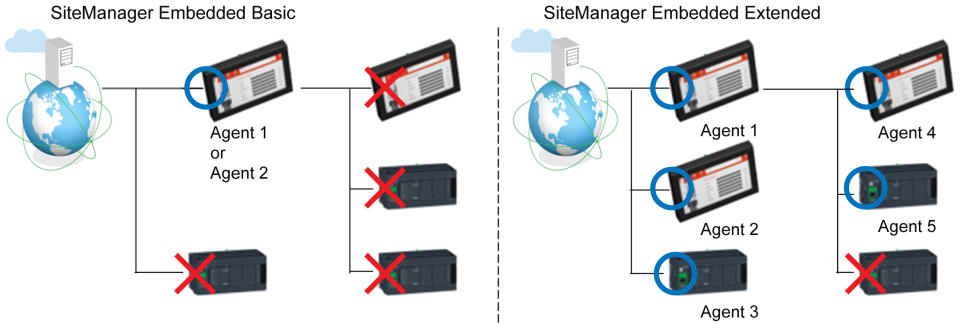
You can access external IP devices (such as PLCs, IPCs, Server, Web camera, and so on) on the same network as the display unit, and register Agents.

As you can connect multiple devices with different IP addresses, you can also register multiple Agents.



NOTE:

- All the ports are open by default. Change to the port as used by your application. Make changes to settings from the SiteManager GUI (**Edit** from **Device Agents**).
- The devices without a registered Agent are not accessible from EcoStruxure Secure Connect Advisor.



Standard Package Content

Package name	Data traffic per month	Amount of LinkManager for PC	Amount of SiteManager
Free trial (30 days)	N/A	1 x license included	1 x SiteManager Embedded Extended 5 License *6
Pack 1 *1*2*4	1 GB *5	1 x license included	15 x SiteManager Basic licenses *7
Pack 2 *1*2*3*4	5 GB *5	3 x license included	25 x SiteManager Basic licenses *7
Pack 3 *1*3	10 GB *5	5 x license included	40 x SiteManager Basic licenses *7

*1 One package per customer account. One customer can have multiple accounts. Each package is charged as a renewable service on a yearly basis, except for the trial package. Customers may request termination of their yearly contract at least one month in advance of the end date. At the end date of a terminated contract, the customer account is closed and all associated options are lost.

*2 Pack 1 can be upgraded to pack 2 or 3 at any time during the yearly subscription period. Pack 2 can be upgraded to pack 3 at any time during the yearly subscription period.

*3 Pack 2 and 3 can be downgraded at the beginning of a renewed yearly subscription period, only after the customer provides a list of LinkManager to be deactivated at least one month in advance of the contract renewal date.

*4 A subsequent package upgrade on the same customer account can only be requested six months after the last package downgrade was performed.

*5 Excess data cannot be carried over to the next month. The data traffic is calculated per month and over usage will be invoiced at the end of the yearly package subscription period, or at the renewal date of the yearly package subscription period.

*6 SiteManager Embedded Extended 5 gives access to the on-site touch panel and five of its connected drives and PLCs.

*7 SiteManager Basic gives access to the on-site touch panel. For OEM machine builders the amount of SiteManager is increased at yearly package renewal to allow continued remote support to their end-customers (for Pack 1, 15 new SiteManager licenses on package renewal, for Pack 2, 25 new SiteManager licenses on package renewal, for Pack 3, 40 new SiteManager licenses on package renewal)

Extending a Standard Package [*8]

Option name	Quantity	Description
Data package	1 GB per month	Extra data traffic over the subscription plan.
LinkManager	1 x license	LinkManager to add remote PCs.
SiteManager Basic	5 x licenses	SiteManager activations on-site HMI.
SiteManager Embedded Extended 5	1 x license	SiteManager access to five connected drives, cameras, PLCs, and so on.
SiteManager Embedded Extended 10	1 x license	SiteManager access to ten connected drives, cameras, PLCs, and so on.
GateManager Premium Access	1 x license per customer account	Premium functionality in the GateManager cloud.
User statistics	1 x license per customer account	View statistics of user login and data usage.
[*8] options can be added to all standard packages, except the trial package.		

NOTE: There are SiteManager Embedded Extended 5 and SiteManager Embedded Extended 10. You can set up five IP addresses with SiteManager Embedded Extended 5, and ten IP addresses with SiteManager Embedded Extended 10.

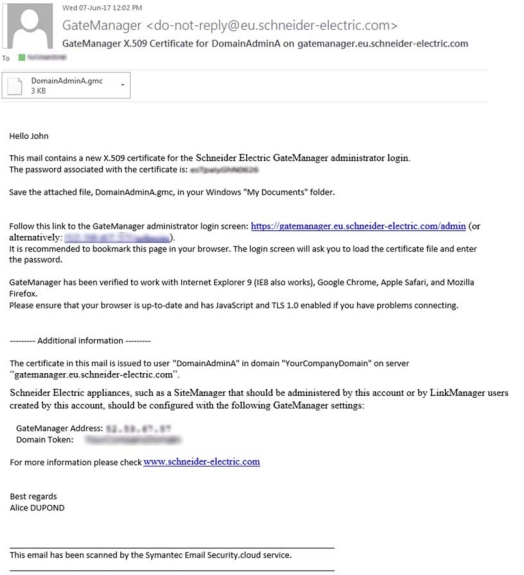
Chapter 2
Premium Domain Admin Guide

What Is in This Chapter?

This chapter contains the following topics:

Topic	Page
First Time Login to the GateManager Web Graphical User Interface (GUI)	22
SiteManager Configuration Backup	25
Accessing the Web GUI of a SiteManager	26
Accessing the Web GUI of a LinkManager	27
Organize Equipment in Domains and Provide LinkManager Access to Specific Equipment	28
Understanding Audit Logs	36
Working with Alerts	37
Working with Actions	40
Combining Alerts and Actions	42
Working with the Replace Appliance Function	44
GateManager Administrator GUI FAQ	45

First Time Login to the GateManager Web Graphical User Interface (GUI)

Step	Action
1	When the administrator account was initially created for you, an email was automatically sent to you. It would look like this: 

Wed 07-Jun-17 12:02 PM

GateManager <do-not-reply@eu.schneider-electric.com>

GateManager X.509 Certificate for DomainAdminA on gatemanager.eu.schneider-electric.com

To [redacted]

DomainAdminA.gmc
3 KB

Hello John

This mail contains a new X.509 certificate for the Schneider Electric GateManager administrator login.
The password associated with the certificate is: [redacted]

Save the attached file, DomainAdminA.gmc, in your Windows "My Documents" folder.

Follow this link to the GateManager administrator login screen: https://gatemanager.eu.schneider-electric.com/admin (or alternatively: [redacted]).
It is recommended to bookmark this page in your browser. The login screen will ask you to load the certificate file and enter the password.

GateManager has been verified to work with Internet Explorer 9 (IE8 also works), Google Chrome, Apple Safari, and Mozilla Firefox.
Please ensure that your browser is up-to-date and has JavaScript and TLS 1.0 enabled if you have problems connecting.

--------- Additional information ---------

The certificate in this mail is issued to user "DomainAdminA" in domain "YourCompanyDomain" on server "gatemanager.eu.schneider-electric.com".

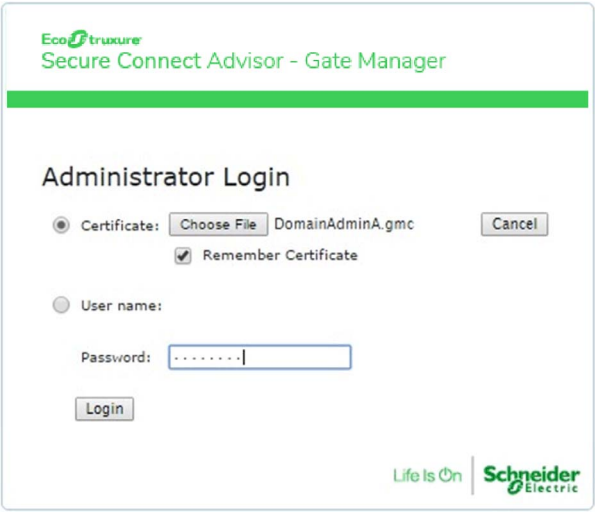
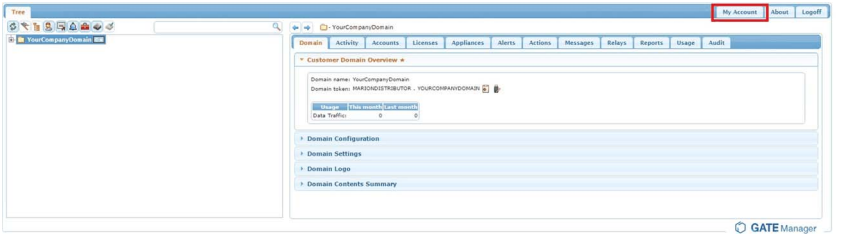
Schneider Electric appliances, such as a SiteManager that should be administered by this account or by LinkManager users created by this account, should be configured with the following GateManager settings:

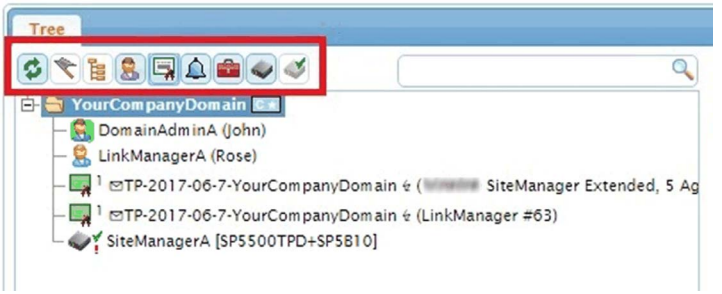
GateManager Address: [redacted]
Domain Token: [redacted]

For more information please check www.schneider-electric.com

Best regards
Alice DUPOND

This email has been scanned by the Symantec Email Security.cloud service.

Step	Action
2	Follow the link in the email to open the GateManager login screen, and browse for the certificate you saved.  **NOTE:** The GateManager administrator portal requires minimum MS Internet Explorer 9, Apple Safari, Firefox, or Google Chrome.
3	In your first login, you see an empty tree. You should consider changing your password under **My Account**. This makes the GateManager server issue a new email with a new certificate. Your existing certificate is then invalidated. 

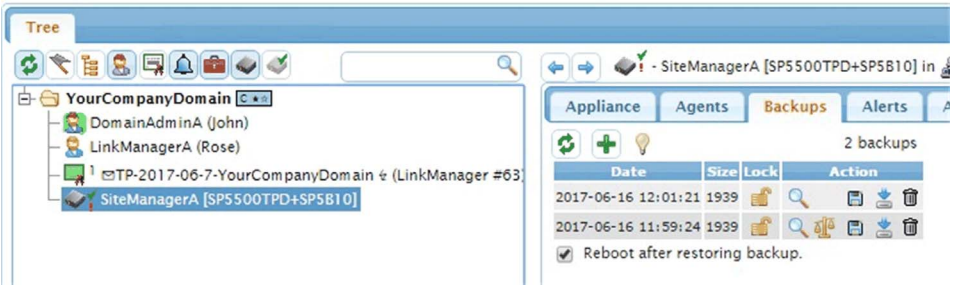
Step	Action
4	The items are as default displayed in the tree view. In order to hide items in the tree view, you can **click the icons** above the tree. When an icon has a blue background, it means that the item is activated and the associated objects are shown in the tree. The icon mouse-over message indicates the function of an item. When you log in again, the settings of the icons are saved in a cookie on your PC and your tree-view is restored. This allows you to customize your favorite view according to the functions you use most often. 

SiteManager Configuration Backup

With GateManager you do not need to setup configuration backup.

When a modification is made to the SiteManager configuration, the GateManager server creates automatically a new backup of the configuration.

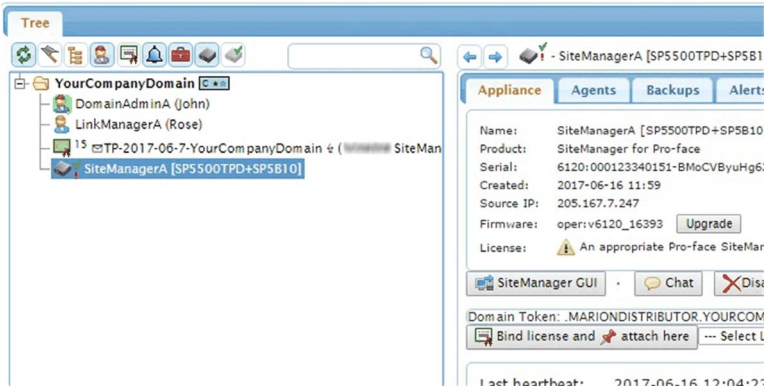
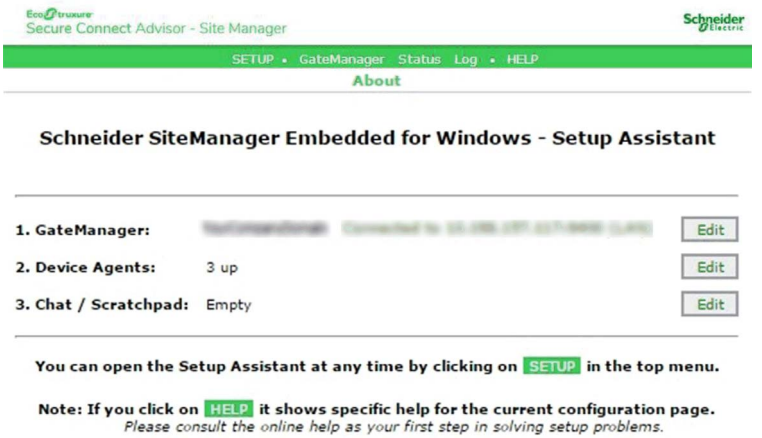
You can view the configuration by placing the cursor on a SiteManager and select the **Backups** tab:



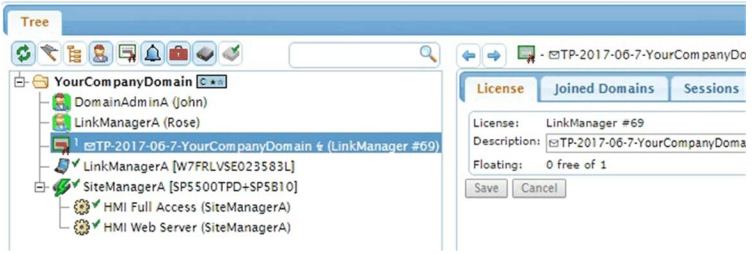
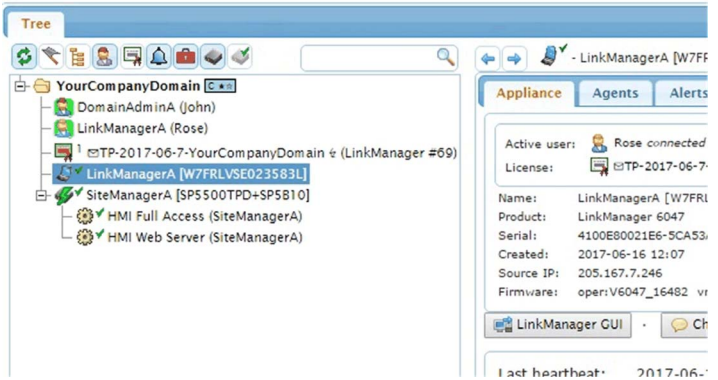
The GateManager stores always the 3 most recent configurations and overwrite the oldest. If you want to maintain a particular configuration, you can select the **Lock** function, which prevents the configuration from being overwritten.

A useful feature is that you can use the scale symbol  to compare differences between two configuration backups.

Accessing the Web GUI of a SiteManager

Step	Action
1	A SiteManager that has not been managed via the GateManager administrator GUI (Graphic User Interface) before is marked with a red exclamation mark ❗. Before you can connect to the Web GUI of the SiteManager, you need to attach it to the GateManager and bind a license to it. 
2	This brings you to the configuration interface of the SiteManager.  Refer to the EcoStruxure Secure Connect Advisor User Guide for GateManager for an introduction to configuring SiteManager network settings and setting up Device Agents. *You can download the guide from the location.*

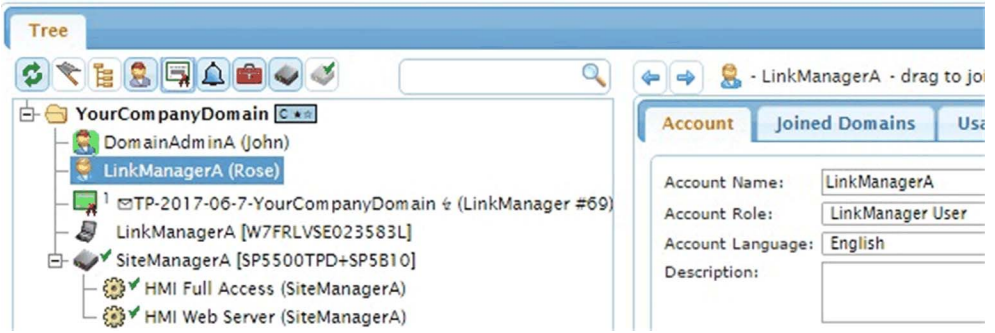
Accessing the Web GUI of a LinkManager

Step	Action
1	When a LinkManager is connected to the GateManager server, you see a number of things: 
2	If you select the laptop icon, you see the **LinkManager GUI** button.  **NOTE:** If you click it, it is redirected to the administrator interface of the LinkManager. You are not able to remote control the user console.

Organize Equipment in Domains and Provide LinkManager Access to Specific Equipment

One of the key features of the GateManager, is the ability to create domains for organizing equipment based on purpose, access level, customer, location, and so on. You can create accounts for which differentiated access to the various domains are defined.

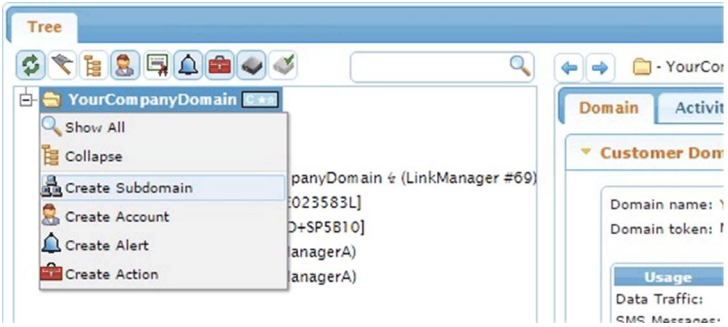
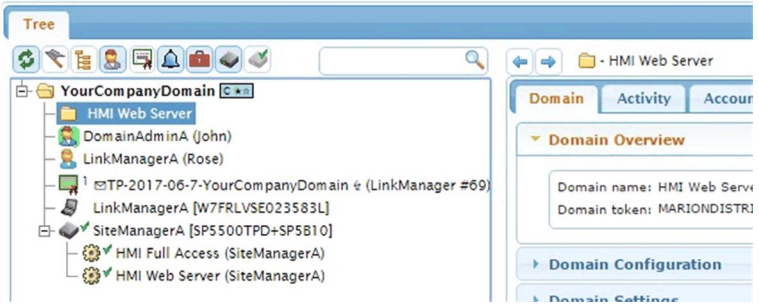
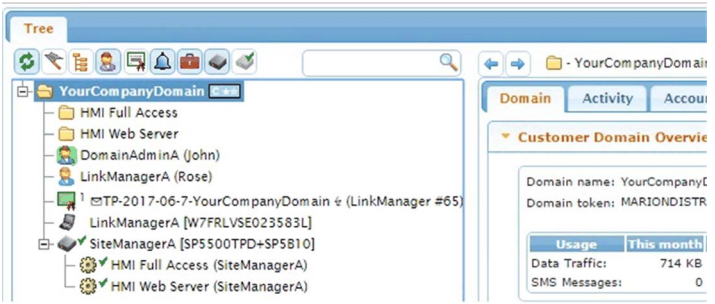
For example, the LinkManager user LinkManagerA who, due to being created in the root domain (YourCompanyDomain), has access to any device that may appear in this domain and any subdomain.

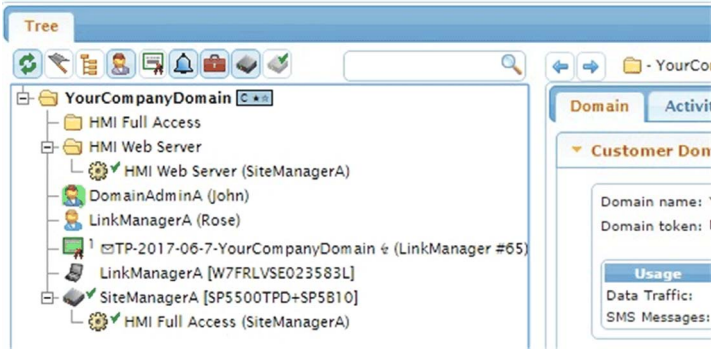
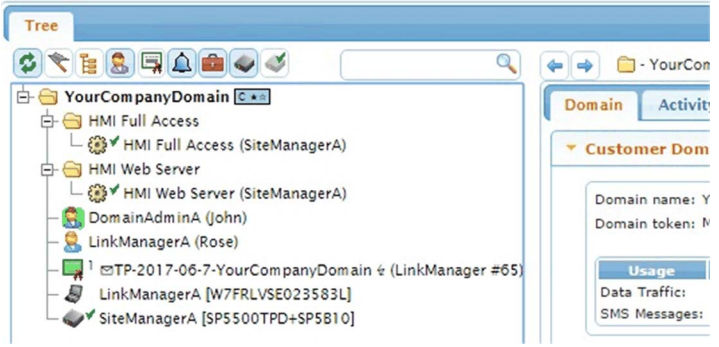


Follow the following steps to do this exercise:

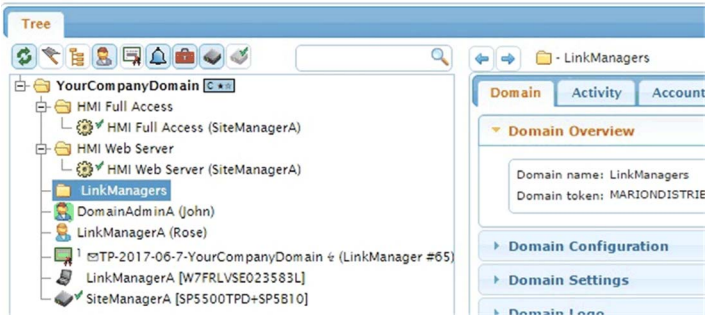
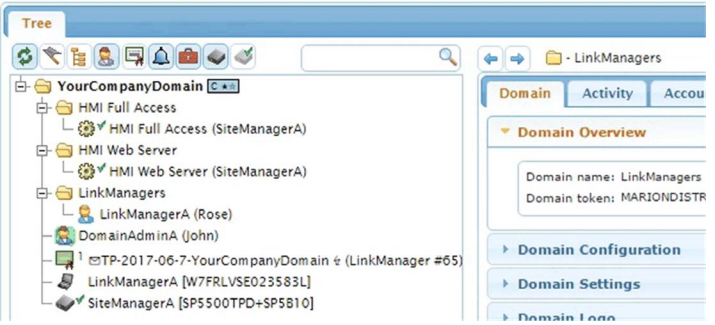
Step	Action
1	Create some domains, and move device agents configured on the SiteManager SiteManagerA into these domains.
2	Move LinkManager user LinkManagerA to a subdomain and grant the user access only to the agent **HMI Web Server**.
3	Create a new LinkManager user LinkManagerB, who has access to both the agents, **HMI Full Acces** and **HMI Web Server**. The user should not have access to the SiteManager.

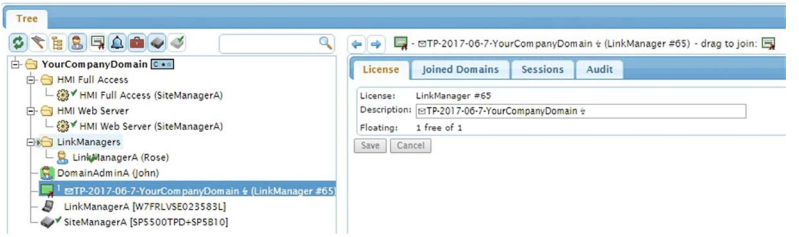
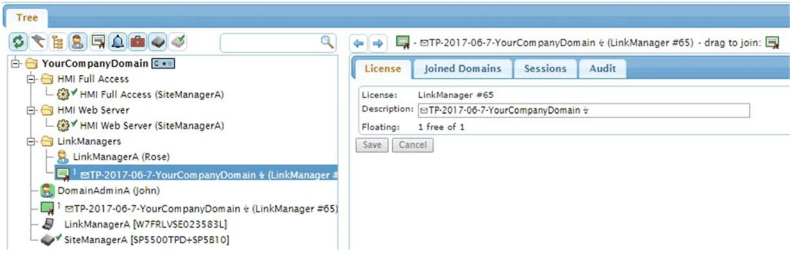
Create New Domains and Move Device Agents to Them

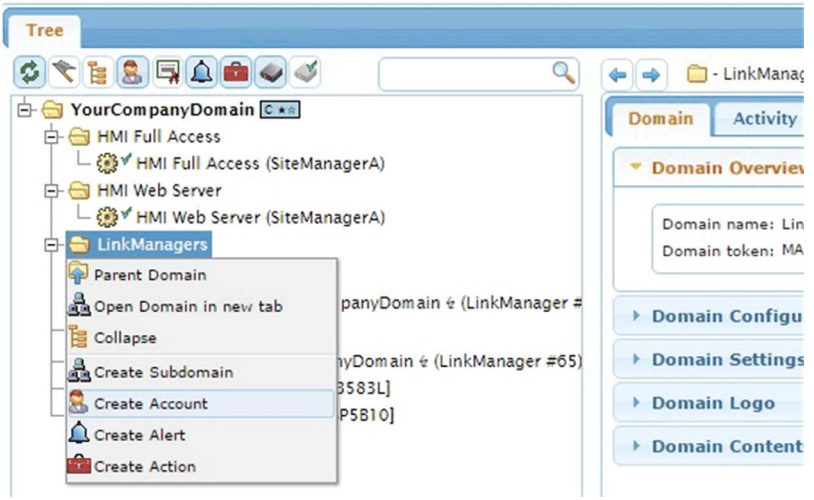
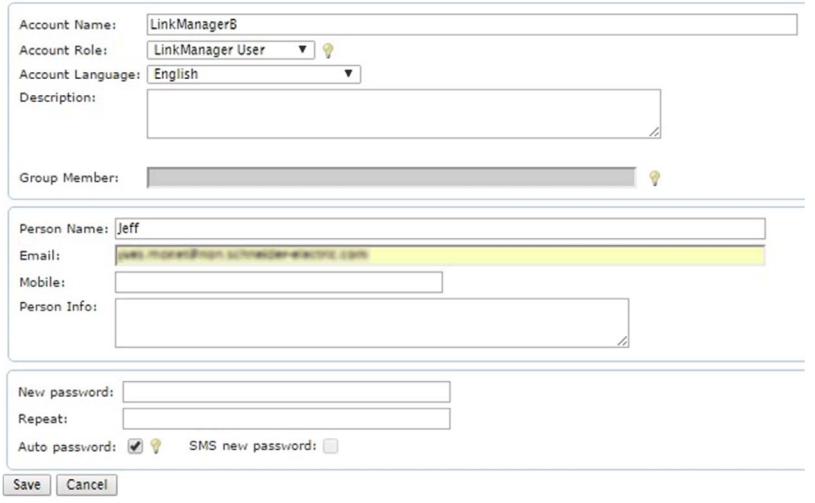
Step	Action
1	Right-click the root domain and select **Create Subdomain**. 
2	Name the new domain **HMI Web Server**. 
3	Use the same procedure to create the domain **HMI Full Access**. 

Step	Action
4	Select the agent **HMI Web Server** and while holding down the left mouse button, drag the agent to the domain **HMI Web Server**. 
5	Do the same for moving the agent **HMI Full Access** to the domain **HMI Full Access**.  **NOTE:** The SiteManager itself stays in the root domain.

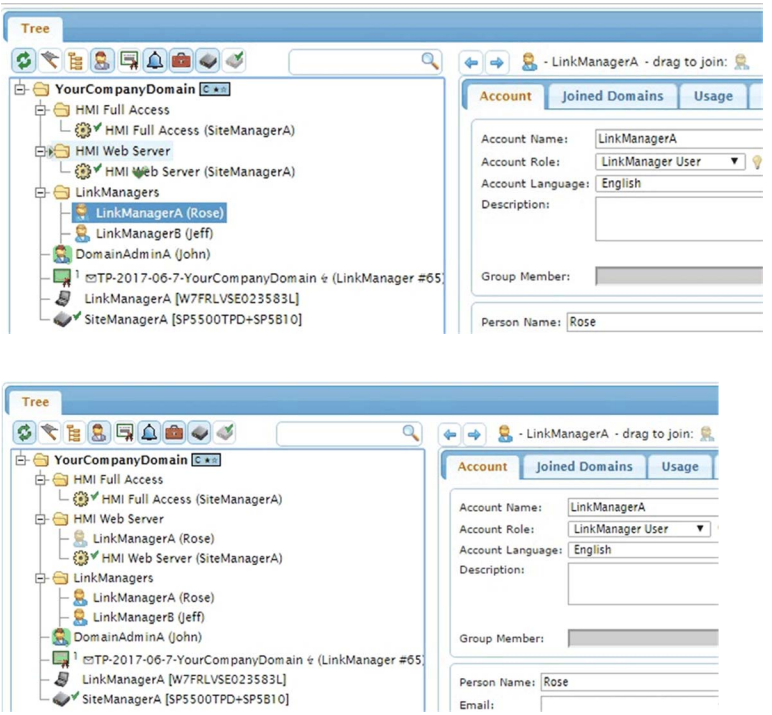
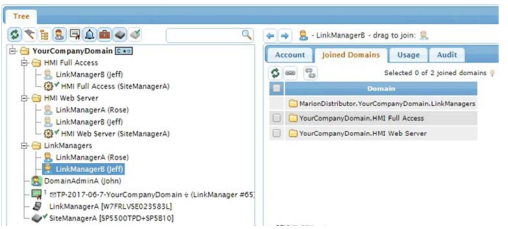
Create a Domain to Hold LinkManager Accounts

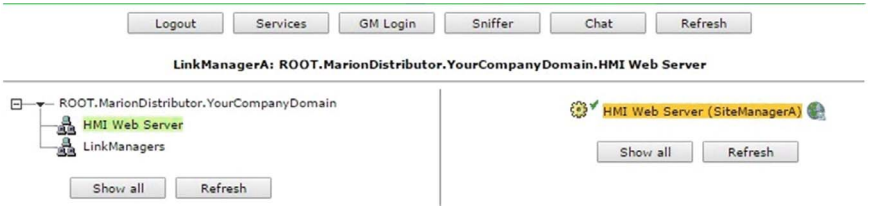
Step	Action
6	Right-click the root domain and select **Create Subdomain**, and create a domain called LinkManagers. 
7	Select the account LinkManagerA, and while holding down the left mouse button, drag the account into the new domain. 

Step	Action
8	Ensure that a LinkManager license is available in the domain LinkManagers. In this case, you only have one **License Pool** called **YourCompanyDomain**, and which contains only one license. Drag the license into the LinkManagers domain. This, however, means that other LinkManager accounts that potentially could be created in the root domain **YourCompanyDomain** is not able to use the license. Leave the license in the root domain, and instead we **join** the license to the LinkManagers domain. Select the license, and drag the icon on the right, into the domain for which the license should be available:   Now the license can be used for LinkManager accounts in both the root domain, and the domain LinkManagers.

Step	Action
9	Create the LinkManager account LinkManagerB. Select the domain LinkManagers, right-click, and select **Create Account**. 
10	Fill in the minimum details for the account: 

Grant Domain Access to LinkManagers Using “Joined Domains”

Step	Action
11	Select the account icon for LinkManagerA on the right and drag it into the domain that the account should have access to: 
12	Select the account LinkManagerB, and do the same procedure for the account. Join the LinkManagerB account to both **HMI Web Server** and the **HMI Full Acces** domain: 

Step	Action
13	The result is that when the user LinkManagerA logs in with their LinkManager, the user is able to access only the **HMI Web Server** domain and connect only to the **HMI Web Server** agent:  When the user LinkManagerB logs in, the user can access to both the domains and then to both the agents: 

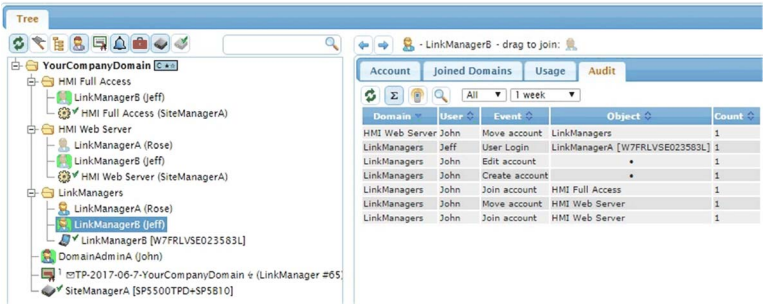
Understanding Audit Logs

The actions on the SiteManager made in the previous sections are logged on the GateManager.

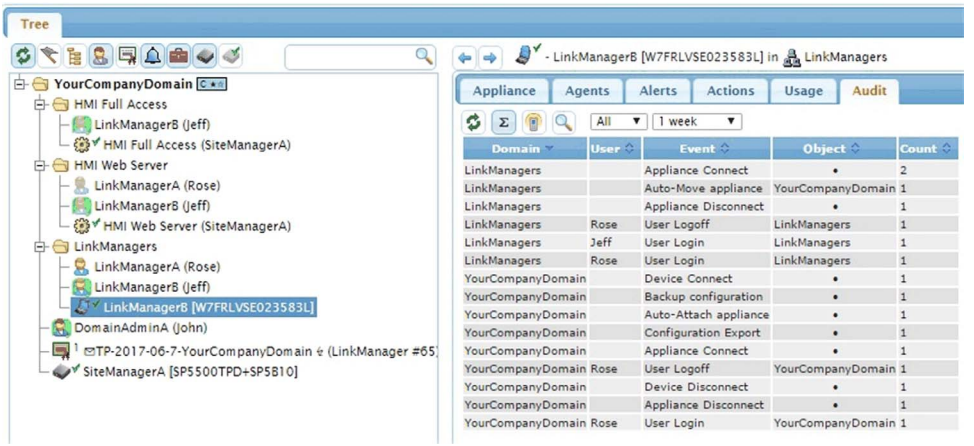
It does, however, require some explanation to understand what is logged where.

For example, if you want to check what devices the user LinkManagerB has connected to recently.

If you look at the account of LinkManagerB, you can see the events occurred on the account but you cannot see the actual work done by LinkManagerB:



Select the LinkManager appliance object of LinkManagerB, which represents the specific PC on which the account of LinkManagerB has been activated:



The reason for this is that the account of LinkManagerB could be installed on different PCs that are operated by different people.

Working with Alerts

Generally About Alerts

Alerts can be used to submit an alert to a specific email address.

Alert processing depends on the GateManager connection to the Schneider Electric HMI Appliances (GateManager) being available or not.

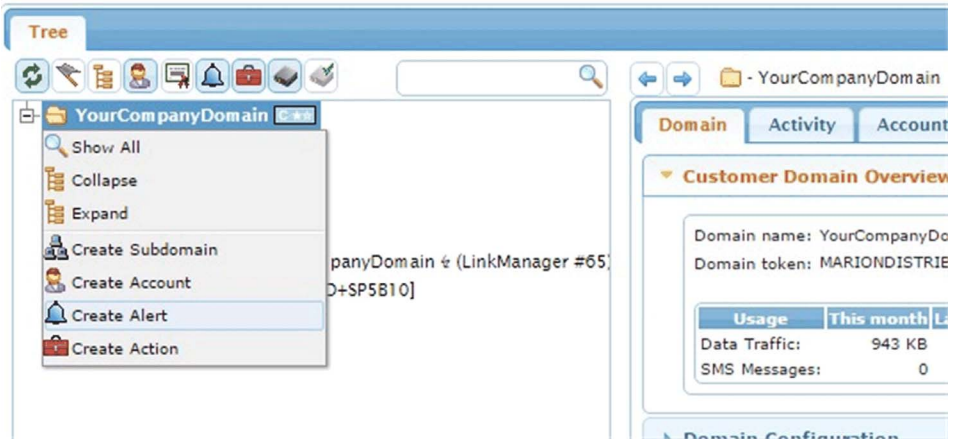
Alerts that are associated with equipment connected to the appliance (via an Input port on a SiteManager, or equipment connected by Ethernet, USB, or Serial), are delivered instantly via the Appliance GateManager connection, and result in the alert email being sent immediately (or based on the defined delay for the trigger).

Alerts that are associated with the Appliance itself, such as an **Appliance Disconnect** alert, is only triggered based on the following criteria:

- If the next expected heartbeat does not arrive (default up to 10 minutes).
- If the Appliance has sent an off-line heartbeat, and has not reconnected within 2 minutes (offline heartbeats are generated based on a controlled reboot/reconnect activated from the local Appliance Web menu or an applied GateManager reboot action, or as a result of an automatic reboot in conjunction with a firmware upgrade).

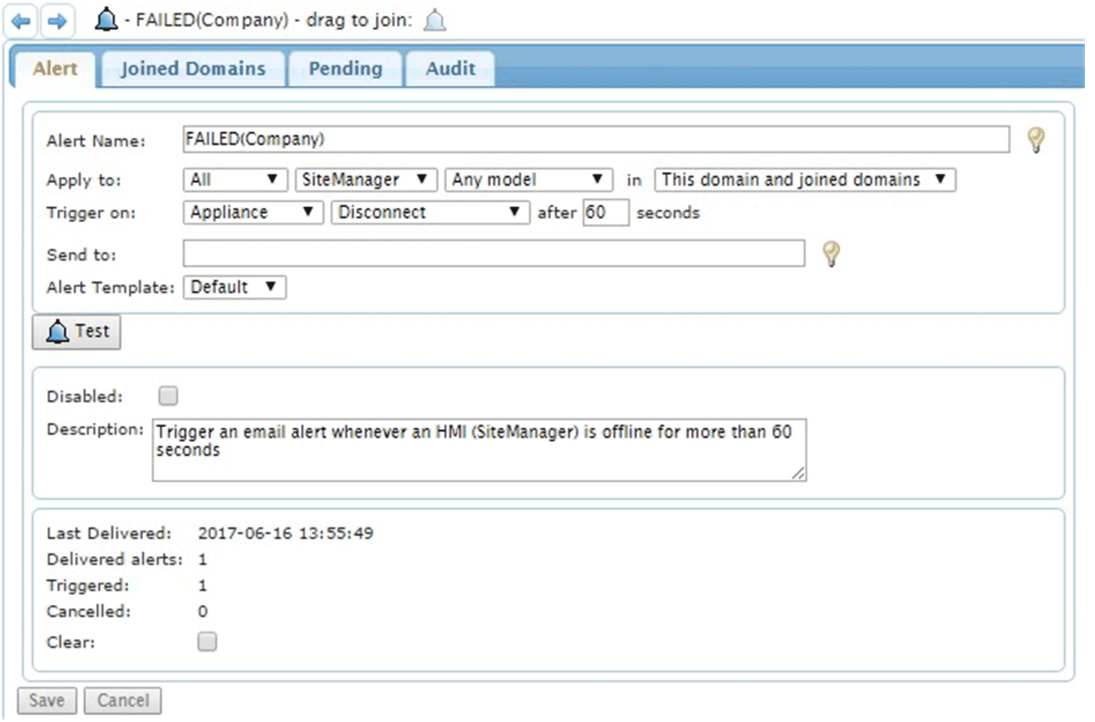
If a SiteManager is disconnected, and have **Disconnect** alerts associated with devices controlled by the Appliance (such as SiteManager agents), the alerts for these devices are triggered based on the above two criteria also. The devices may in fact be connected locally at the remote site, but since the GateManager cannot determine the cause for the general disconnect, it has no other choice than to trigger the device alerts also.

Alerts are created by Right clicking the domain where the alert should be created:



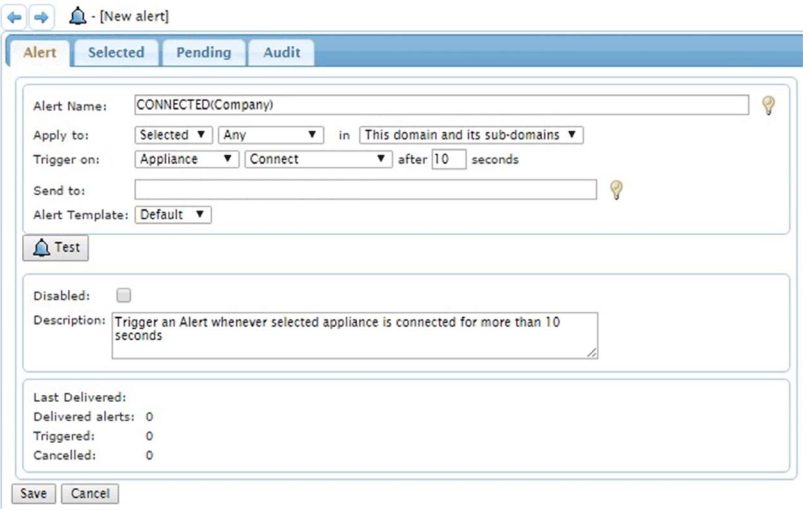
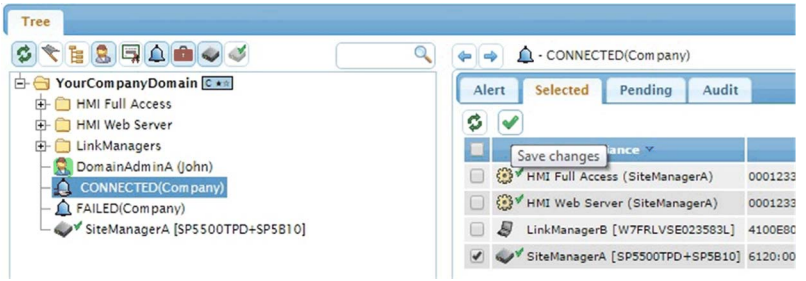
Example of a FAILED Alert (or Disconnect Alert)

Common names like **FAILED** or **Connected** are reserved words on the hosted server, so you have to extend the naming. In this case **FAILED Company** identifies clearly the alert when it is mailed to you.



Example of a Connected Alert for Selected Appliances

This example illustrates the creation of an **Alert** that is triggered when certain appliances are connected.

Step	Action
1	Create the **Alert** definition as follows: 
2	Click the **Selected** tab and check mark the appliances that should have this alert associated: 

NOTE: Combining the **Apply to** and **Trigger on** option should cover most of the needs for an alert.

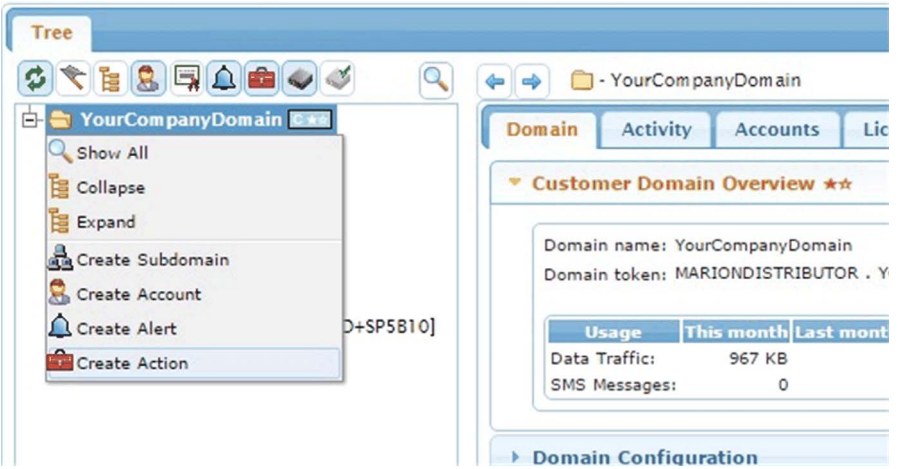
Working with Actions

With Actions you can perform firmware upgrades, restore configuration backup's or parts of configurations and/or rebooting appliances.

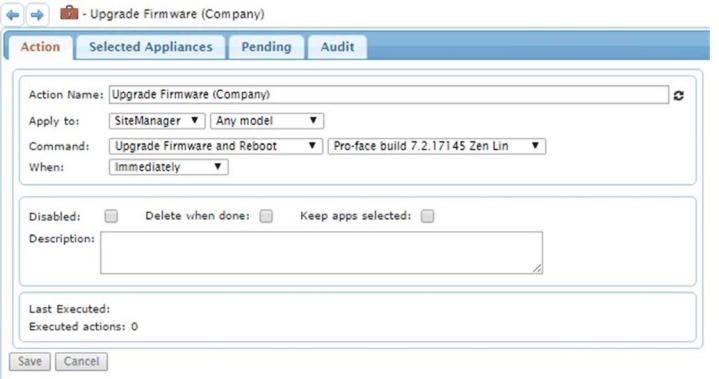
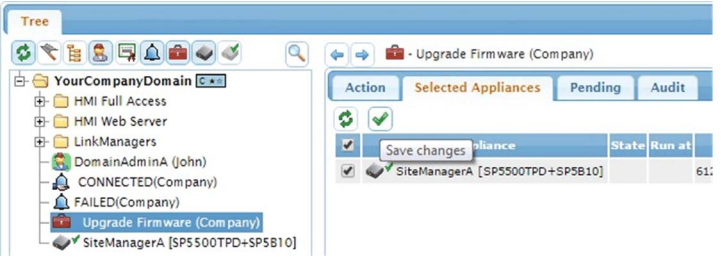
An Action is only performed on selected appliances so there is no risk of creating a firmware upgrade action. You cannot break anything by applying a wrong firmware to an Appliance.

Appliances are not upgraded before the appliance is selected. However you can combine Actions and Alerts (see next section).

To create an Action, remember to select the **Actions** icon at the top to make actions visible in the tree view. Right-Click on the domain where the action should be created:



Upgrade Firmware on Multiple Appliances

Step	Action
1	Create an Action for the models (SiteManager) and select the firmware to upgrade with: 
2	Click the **Selected Appliances** tab and select the appliances you want to upgrade: 
3	Press **Save Changes** icon  to execute the action. Appliances that are currently not connected are automatically upgraded the next time they come online. 

Combining Alerts and Actions

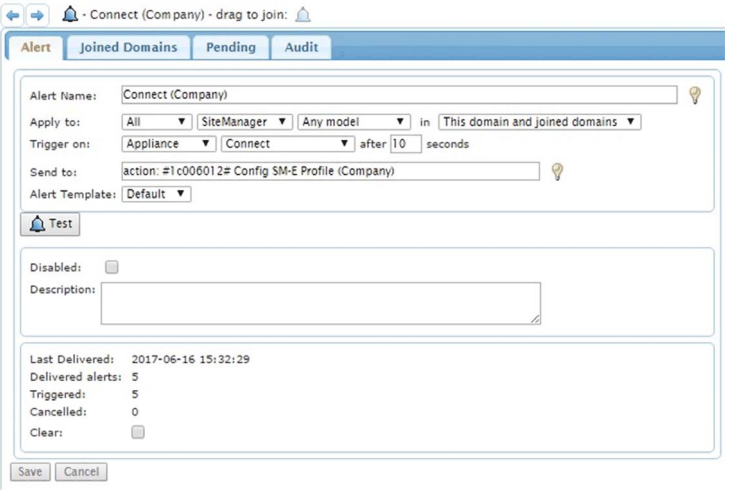
It is possible to create an alert that has triggers and action.

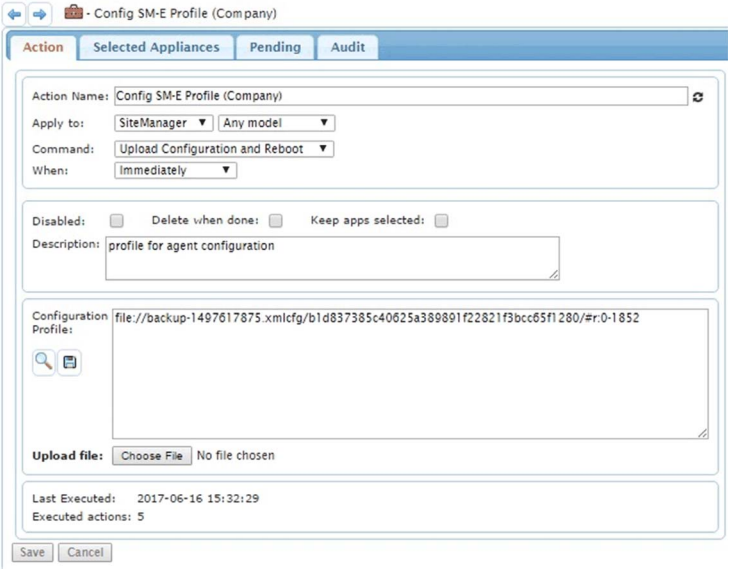
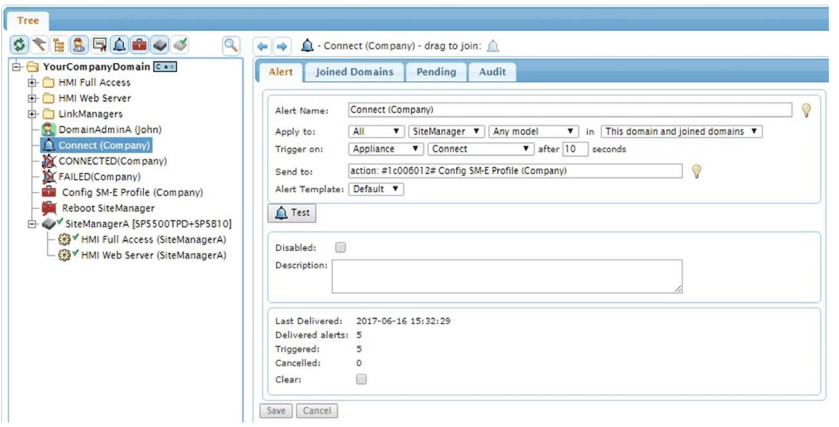
Example: The next time a SiteManager appliance connects to the GateManager it should get a new GateManager address, automatically reboot, and subsequently connect to another GateManager. This is useful when migrating from one GateManager to another.

Example: When a new SiteManager appliance appears in a domain it should be configured with a special configuration profile (For example, special Agent definitions on a SiteManager).

NOTE: You cannot append a single Agent to the existing table. A configuration profile overwrites always the entire section (For example, the Agent list).

The following example will apply a new SiteManager profile the next time a new SiteManager appliance appears in a specific domain.

Step	Action
1	Create an alert named **Connect (Company)** in the domain **YourCompanyDomain**. Settings are: Apply to: **All**, SiteManager, **Any models** Trigger on: **Appliances New** 

Step	Action
2	Create an Action that contains the add-on configuration part. Settings are: Apply to: SiteManager, **All models** Command: **Upload Configuration** and **Reboot** 
3	Combine the Action to the Alert by dragging the Action from the Domain-Tree to the **Send to** field of the **Alert**: 
4	Select the **Connect (Company)** alert in the Domain-Tree. With the mouse drag the **Config SM-E Profile (Company)** action to the **Send to** field in the right side window. Next time a SiteManager of any model show up in the **YourCompanyDomain** for the first time it will be applied the Configuration profile from the **Config SM-E Profile (Company)** action.

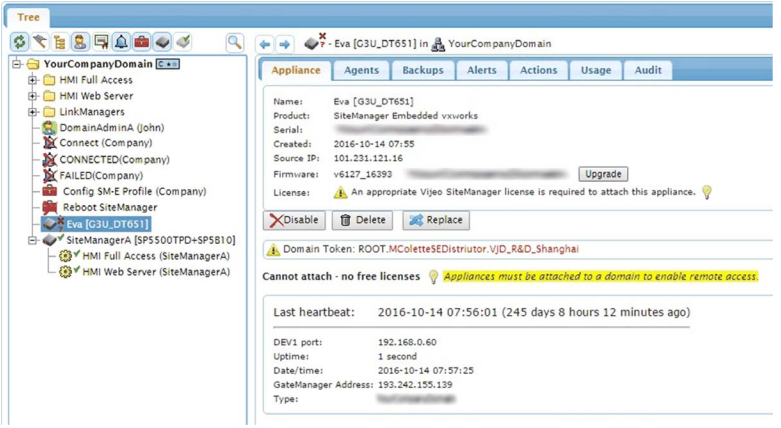
Working with the Replace Appliance Function

If you have a SiteManager appliance that needs to be replaced for any reason, you use the **Replace** function in GateManager.

The **Replace** function restores the configuration from the old appliance to the new one.

The settings are restored including VPN tunnels, Agent, passwords and certificates. The old and the new appliances do not have to be the same model. For example, an HMI Unit-1 can be replaced by an HMI Unit-2.

The **Replace** button shows only on flagged units (marked with a red cross):



Select the flagged appliance in the Tree-view and press the **Replace** button. A Wizard guides you through the replacement procedure.

GateManager Administrator GUI FAQ

Q1: Can any browser be used for accessing the GateManager administrator GUI?

A1: The GateManager administrator GUI is using advanced Java script, which should be supported by most web browsers. We recommend Google Chrome, Mozilla Firefox, Apple Safari (for Apple OS). Microsoft Internet Explorer is not recommended due to slow and flawed processing of Java script. However, IE 9-11 should work, while IE8 will not.

Q2: Can I use my tablet or smartphone?

A2: Yes. For Apple iPad and iPhone, Although not recommended you may need to change your administrator account to use user name and password only, since it may not be possible to store the x509 certificate onto the device. For newer Android based devices such as Samsung, you can store the certificate on the device. The drag and drop by default is disabled when GateManager detects a browser on an Android or iOS platform in order to prevent unintended reorganizing of contents. This can, however, be enabled under the **My Account** menu and is stored in a local cookie locally on the PC.

Q3: Can I load the x509 certificate into my browser, so I do not have to browse for it each time I login?

A3: Yes. GateManager uses a cookie to remember which file was used for the last login.

Q4: Can GateManager administrators at the same level replace or delete each other's accounts?

A4: Yes. We have chosen to allow this by design, in order to let administrators help each other in case a password is forgotten. If you need to have an overall administrator, you can decide to create a subdomain structure in which you create additional administrator accounts, and then have the initial administrator account in the **root-domain**.

Q5: I already have a subscription to a Schneider Electric Connect Pack or Trial. What do I need to gain GateManager Premium account?

A5: You need to purchase the option **GateManager Premium Access**. You can use the same login as your current pack subscription (your Premium account features will be available at the next login).

Glossary

A

Agent

Generic term for display units and external devices that SiteManager Embedded allowed to connect to the network. The number of units (Agents) you can register differs depending on your license.

D

device/PLC

Indicates a device, such as a PLC (Programmable Logic Controller), that connects to a display unit.

display unit

Indicates a touch-panel display unit manufactured by Schneider Electric for displaying the screen interface designed in Screen Editor & Logic Program Software.

G

GateManager

It is used for user administration and access control for LinkManagers, and acts as communication broker between LinkManagers and SiteManagers.

L

LinkManager

The software installed on your computer, allows remote access to SiteManager and/or devices represented by agents on the SiteManager.

LinkManager Mobile

A service on the GateManager, allows remote access to web enabled and VNC/RDP (Virtual Network Computing/Remote Desktop Protocol) devices from a browser.

S

SiteManager

Refers to display units on the work site connected to the EcoStruxure Secure Connect Advisor network.

SiteManager Embedded

Software used to set up access to the EcoStruxure Secure Connect Advisor network. This software may not be required as you can set up the network connection from the offline screen of some display units.

SiteManager Embedded Basic

One of the license formats required to use SiteManager Embedded. Allows access to the display unit and registration of up to two agents.

SiteManager Embedded Extended

One of the license formats required to use SiteManager Embedded. Allows access to external IP devices – such as PLCs, IPCs, server, Web camera, and so on, on the same network as the display unit, and registration of five agents or more.

screen editor & logic program software

Indicates software for HMI, VJD and VXD screen editor software.