# **EcoStruxure<sup>™</sup> Secure Connect** Quick Start Guide

02/2025

EIO000003800.04





# Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this document are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owner.

This document and its content are protected under applicable copyright laws and provided for informative use only. No part of this document may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof.

# **Table of Contents**

Safety Information	4
About the Document	5
EcoStruxure Secure Connect	8
Use Case Components	9
Installation Overview	13
Step 1: Connecting to the GateManager	14
Step 2: Creating User Accounts	16
Step 3: Enabling the SiteManager Connection of the HMIGTO	
Appliance to GateManager	18
Step 4: Registering an Appliance on GateManager	20
Step 5: Creating an Agent	22
Step 6: Installing LinkManager	25
Step 7: Starting LinkManager and Connecting to Device	27
Glossary	33

# **Safety Information**

## **Important Information**

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** 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** 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.

# **About the Document**

# **Document Scope**

This document describes how to quickly install, configure, and test EcoStruxure Secure Connect. EcoStruxure Secure Connect provides secure remote access to devices as if you were on site.

**NOTE:** Read and understand this document before installing, operating, or maintaining your EcoStruxure Secure Connect.

EcoStruxure Secure Connect users should read through the entire document to understand all features.

# Validity Note

This document has been updated for the release of Vijeo Designer 6.2 SP7, SoMachine 4.3 and EcoStruxure Operator Terminal Expert 3.0.

The EcoStruxure Secure Connect offer is compatible with the EcoStruxure Machine Expert software, which is the successor of the SoMachine software. At the time of writing this document, the latest available version of EcoStruxure Machine Expert is 2.0.

# **General Cybersecurity Information**

In recent years, the growing number of networked machines and production plants has seen a corresponding increase in the potential for cyber threats, such as unauthorized access, data breaches, and operational disruptions. You must, therefore, consider all possible cybersecurity measures to help protect assets and systems against such threats.

To help keep your Schneider Electric products secure and protected, it is in your best interest to implement the cybersecurity best practices as described in the Cybersecurity Best Practices document.

Schneider Electric provides additional information and assistance:

- Subscribe to the Schneider Electric security newsletter.
- Visit the Cybersecurity Support Portal web page to:
  - Find Security Notifications.
  - Report vulnerabilities and incidents.
- Visit the Schneider Electric Cybersecurity and Data Protection Posture web page to:
  - Access the cybersecurity posture.
  - Learn more about cybersecurity in the cybersecurity academy.
  - Explore the cybersecurity services from Schneider Electric.

## **Product Related Cybersecurity Information**

Use this product inside a secure industrial automation and control system. Total protection of components (equipment/devices), systems, organizations, and networks from cyber attack threats requires multi-layered cyber risk mitigation measures, early detection of incidents, and appropriate response and recovery plans when incidents occur. For more information about cybersecurity, refer to the Harmony HMI/iPC Cybersecurity Guide:

http://www.se.com/ww/en/download/document/EIO0000004948/

#### 

# POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Change default passwords at first use to help prevent unauthorized access to device settings, controls and information.
- Disable unused ports/services and default accounts, where possible, to minimize pathways for malicious attacks.
- Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).
- Apply the latest updates and hotfixes to your Operating System and software.
- Use cybersecurity best practices (for example: least privilege, separation of duties) to help prevent unauthorized exposure, loss, modification of data and logs, interruption of services, or unintended operation.

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

## **Related Documents**

Title of documentation	Reference number
Cybersecurity Best Practice	<b>Refer to</b> General Cybersecurity Information, page 5
HMI/IPC Cybersecurity Guide	EIO000004948 (ENG)

You can download the manuals related to this product, such as the other software manual, from the Schneider Electric download center (www.se.com/ww/en/download).

# Information on Non-Inclusive or Insensitive Terminology

As a responsible, inclusive company, Schneider Electric is constantly updating its communications and products that contain non-inclusive or insensitive terminology. However, despite these efforts, our content may still contain terms that are deemed inappropriate by some customers.

## **Trademarks**

 ${\rm Microsoft}^{\circledast}$  and  ${\rm Windows}^{\circledast}$  are registered trademarks of Microsoft Corporation in the United States and/or other countries.

Product names used in this manual may be the registered trademarks owned by the respective proprietors.

# **EcoStruxure Secure Connect**

## **Overview**

EcoStruxure Secure Connect allows technicians and programmers to remotely monitor, diagnose, control, and program devices. This can significantly reduce the cost of maintaining devices and maximize device uptime. Remote access to the device is achieved by means of a private, point-to-point connection. Access to this connection is strictly controlled and all data sent and received on the connection is encrypted.

## **Supported Models**

For a complete list of appliances that support EcoStruxure Secure Connect, refer to the Supported Model List in the EcoStruxure Secure Connect Catalog.

https://www.se.com/ww/en/download/document/DIA5ED2190101EN/

**NOTE:** Available models differ depending on the screen editing software you are using. Please check the supported models of EcoStruxure Secure Connect with your screen editing software (that is, Vijeo Designer or EcoStruxure Operator Terminal Expert).

## **Use Case**

This quick start guide presents a typical use case for the deployment of EcoStruxure Secure Connect. It describes how to install and configure the components of an EcoStruxure Secure Connect solution, then use them to control a programmable logic controller (PLC) located on a remote work site from a laptop computer located in a local office.

The following figure shows the use case:



#### NOTE:

- The HMIGTO appliance and the M251 Logic Controller must be on the same network at the work site. Modify IP addresses that appear in this guide to those used on your network.
- This document illustrates one possible use case. EcoStruxure Secure Connect supports many different device types and architectures. Adapt the steps in this document to correspond to your environment.

# **Use Case Components**

# **Overview**

The following sections describe the components of the use case solution.

## Licenses

You must have a license to use EcoStruxure Secure Connect.

This document assumes the use of a 30-day free trial license, which includes:

- 1 x EcoStruxure Secure Connect GateManager license
- 1 x EcoStruxure Secure Connect SiteManager Extended 5 agents license
- 1 x EcoStruxure Secure Connect LinkManager license
- 1 x EcoStruxure Secure Connect LinkManager Mobile license

**NOTE:** This document refers to Trial license usage. The Trial license needs to be followed by Pack purchase to maintain the EcoStruxure Secure Connect service.

### **HMI/iPC** Appliance

This use case assumes the use of a Harmony<sup>™</sup> HMIGTO touchscreen display unit compatible with the latest version of the Vijeo Designer configuration software (Vijeo Designer 6.2 SP7 or later).

**NOTE:** The HMIGTO appliance must have Internet access. For HMI appliances with no Web browser in the application, you can check this as follows:

- 1. Temporarily connect a PC at the same network connection point
- 2. Set the PC network settings to those of the HMI appliance
- 3. Start an Internet browser on the PC and check you can access Web pages.

This may require retrieving settings or obtaining authorization from the IT infrastructure of the work site. Only outbound authorization is required in most cases.

For a complete list of appliances that support EcoStruxure Secure Connect, refer to the Supported Model List in the EcoStruxure Secure Connect Catalog.

https://www.se.com/ww/en/download/document/DIA5ED2190101EN/

## SiteManager

The SiteManager software runs on the HMIGTO appliance. It is installed on the appliance as part of Vijeo Designer RunTime.

To be registered with the GateManager component, SiteManager requires outgoing access to specific ports and protocols. The following outbound rules must be granted on the HMIGTO appliance:

- TLS through Web proxy (TLS to remote IP address and port of Web proxy)
- HTTPS (HTTP over TLS) to remote IP address of GateManager, remote port 443
- TLS over HTTP to remote IP address of GateManager, remote port 80

SiteManager has a Web user interface. It listens locally for incoming connections to the Web user interface. Access is restricted to the following HMIGTO appliance user:

• TLS to loopback IP, local port 11444

### LinkManager

The LinkManager software is installed on a laptop computer in the office and is typically used by PLC programmers and service engineers. LinkManager allows secure remote access to devices.

This use case assumes:

- A laptop computer running Windows 10, 64-bit edition
- A Windows user account on the laptop computer with administrator privileges.
- Access to the Internet using the HTTPS protocol. This may need to be configured on the corporate firewall and/or the personal firewall on the PC.

#### GateManager

The GateManager software runs on a Schneider Electric-hosted network server. You use GateManager to create secure, encrypted connections between appliances on the work site and the LinkManager software running on personal computers in the office. The Web-based user interface requires use of the HTTPS protocol. When you request a trial license, or purchase a license, a secure, private customer domain folder on the server is automatically created. Login credentials of a GateManager administrator account on this customer domain are then provided to you by email.

It is the role of the GateManager administrator to configure this domain. This involves:

- · Attaching purchased licenses to SiteManager appliances.
- Creating subdomains for organizing equipment based on their purpose, access level, physical location, and so on.
- Verifying for the entire customer domain the network status of all SiteManager and LinkManager components.
- Creating and managing other GateManager administrator accounts (only available with GateManager Premium Access) and LinkManager user accounts.
- Setting up and managing audit logs, alerts, and automated actions (only available with GateManager Premium Access).

#### 

#### EQUIPMENT DAMAGE

- Before any maintenance action, ensure by phone that you have on-site agreement.
- Before any update, ensure that you have a stable Internet and electricity environment.
- In 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.

## Device

This use case assumes the use of a TM251MESE logic controller, which has a configurable Ethernet interface. The device must be physically connected to the HMIGTO appliance with an Ethernet cable. Make a note of the Ethernet configuration details (IP address and subnet mask) of the device.

EcoStruxure Secure Connect supports a wide range of Schneider Electric devices.

## **Programming Software**

This use case assumes the use of SoMachine V4.3 programming software, installed on the same laptop computer as the LinkManager software.

EcoStruxure Secure Connect only establishes a connection to the appliance. Therefore, any programming software can be used provided that the network requirements (open ports, and so on) are met.

#### **Internet Browser**

An Internet browser is required to access the Web-based user interfaces of LinkManager, SiteManager, and GateManager.

This document assumes the use of Google Chrome. Any recent version of Mozilla Firefox or Microsoft Edge can also be used.

## **Configuring a Proxy Server**

Depending on the network policies in place at the work site, outgoing connections to the Internet may be restricted (IP address range blocked, port range blocked, protocol types blocked, and so on). Both the SiteManager and LinkManager components may require a Web proxy to access the Internet.

If this is the case, contact the network administrator of your work site for help in setting up the connection to the Internet to use a Web proxy.

۲	Secure Connect SiteManager Emb	pedded		(
	Access Control	• Enabled	O Disabled	
	Connection Status			
	SME Version		17393	
	Server Address			
	Domain Token			
	Appliance Name			
	Proxy Address			
	Proxy User			
	Proxy Password			
F	actory Default	Apply Chan	ge Cancel	

The SiteManager user interface, for example, allows you to configure a Web proxy:

**Proxy Address**. IP address of the Web proxy. An IP address, optionally followed by a colon (:) and a port number. For example, *10.11.0.100:9400* or *10.0.11.0.100* (port 80 is used by default).

Proxy User. Web proxy user name, if any.

Proxy Password. Password for the Web proxy user name, if any.

# **Installation Overview**

# **Installation Steps**

# **A**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.

#### Perform the steps in the following order:

- 1. Connect to the GateManager user interface, page 14
- 2. Create GateManager and LinkManager user accounts, page 16
- 3. Enable the SiteManager connection of the HMIGTO appliance to GateManager, page 18
- 4. Register the HMIGTO appliance with SiteManager, page 20
- 5. Create an agent, page 22
- 6. Install LinkManager, page 25
- 7. Log in to LinkManager and test the connection, page 27.

# Step 1: Connecting to the GateManager

# **Overview**

The first step is to request a trial license for EcoStruxure Secure Connect, then log in to the GateManager user interface using the credentials provided. This step can be done on the laptop computer in the office or any other computer.

# **Obtaining a Trial License**

Step	Action
1	Contact your reseller to obtain a Trial license or visit the product page on se.com.
2	If you are using the product enquiry form on the product page, then enter the information requested, and click <b>Request now</b> .
	Nosale. A mossage is sent to the chair address you provide.

# Logging In to GateManager

Step	Action
1	Open the email that you receive, which contains all the information you need to log in to GateManager. For example:
	Brian_GM.gmc       1         Hello Brian Smith       1         This mail contains your personal X.509 certificate for the schneider Electric GateManager Administrator login.       2         Save the attached file, Brian_GM.gmc, in a document folder on your computer.       2         Follow this link to the GateManager login screen:       gatemanager.schneider-electric.com It is recommended to bookmark this page in your browser)       3         The login screen will ask you to load the certificate file and enter the password.       GateManager has been verified to work with Internet Explorer 11, Edge, Chrome, Opera, Safari, and Firefox.       Please ensure that your browser is up-to-date and has JavaScript and TLS 1.2 enabled if you have problems connecting.         ———— Additional information ———       The certificate in this mail is issued to user "Brian_GM" in domain "Brian-inc" on server "10.208.164.166".         Schneider Electric appliances, such as a SiteManager, that should be administered by this account, should be configured with the following GateManager settings:       4         GateManager Address:       4         Domain Token:       Brian-inc         4       4         5       Password to use with the certificate         8       Web site address to use to log in to the GateManager user interface         4       This domasin taken your browser is later used in the Vision Designer Dup Time of the UMICTO
	appliance. It is used to register the appliance in the GateManager customer domain.
2	Save the GateManager certificate attached to the email to the local file system.
3	Click the GateManager link in the received email (or copy and paste the link into a Web browser) to access the GateManager Login window:



# **Step 2: Creating User Accounts**

## **Overview**

Once you have accessed the GateManager user interface, the next step is to create user accounts:

GateManager Account Type	Description
Domain Administrator	An option provided by the Premium Access add-on. Allows customers to administer their own customer domain. Allows the creation of sub-domains to manage customers and/or have complete control over which LinkManager users can assess which agents.
Basic Administrator	Standard administrator role managing the customer domain. Performs tasks such as license management and controlling LinkManager.
LinkManager User	The user role for a technician or expert: the physical person who establishes the connection from the laptop computer to the HMIGTO appliance.

Before starting, take time to consider these roles within your organization. There may be more than one role per person, depending on the size of your organization. For example, if the GateManager Basic Administrator Account and LinkManager User accounts are to be used by the same physical person, only one account is required. Otherwise, two separate accounts are required.

## **Creating the Accounts**

Step	Action
1	The first time you log in to the GateManager user interface, a wizard screen is displayed on the right:
	Startup Wizard
	Startup Wizard
	Welcome You are now logged in as administrator in the GateManager Portal, which is a powerful tool to centrally create and control user access, configure and manage SiteManagers, and remotely connect to devices. This Wizard will assist your first time setup of accounts and optionally SiteManager Embedded (SM-E). For more information, <u>Click here.</u>
	Run Startup wizard again on next login? (You can always re-enable it under My Account)
2	Click <b>Next</b> . The following wizard screen is displayed:

Step	Action			
	Startup Wizard			
	Startup Wizard			
	a → S LinkManager License and Account			
	Your domain contains a LinkManager floating license, which can be used by you and your technicians to obtain remote access to devices for programming and troubleshooting of equipment using the native software for the equipment, just as if you were onsite.			
	You can connect to SiteManagers and devices directly from the GateManager Portal with this administrator account. While connected, the LinkManager license will be temporarily allocated to you. Your first connection attempt will automatically check if the LinkManager software is installed on your PC, and if not, you will be presented with a LinkManager download page. You can create an unlimited number of dedicated LinkManager user accounts that will automatically			
	share the license.			
	Click [Next] to get help on creating a dedicated LinkManager user account for yourself.			
	If you want to create an account for another person than yourself, check this box:			
	I want to create a dedicated LinkManager account for another person.			
	Cancel Back Skip Next			
	Run Startup wizard again on next login? (You can always re-enable it under My Account)			
3	Click <b>Next</b> . The following wizard screen is displayed:			
	Startup Wizard			
	Startup Wizard			
	📮 🤿 🤱 LinkManager License and Account			
	Your dedicated LinkManager account has now been created, and you will receive an email shortly with			
	your Linkmanager login information.			
	Use the same password you entered for this administrator login.			
	Run Startup wizard again on next login? (You can always re-enable it under My Account)			
	<b>Result:</b> An email is sent to the address you specified when requesting the trial license, page 14. You will use this email later to install LinkManager, page 25.			
4	Click Next. The final page of the wizard is displayed:			
	Startup Wizard			
	Startup Wizard			
	SiteManager Embedded License and Device			
	You have a SiteManager Embedded (SM-E) license available that can be assigned to an SM-E. Currently no SM-E has connected to which you can associate the license.			
	If the SM-E is not yet installed on the device you want to remote access, you can download it from this link <u>http://ftp.gatemanager.dk/schneider/sme.html</u> and install on your platform.			
	Once installed and started, enter the following information into the SM-E GUI and ensure that the device on which the SM-E is installed has access to the Internet.			
	GateManager Address:			
	Finish Refresh			
	Run Startun wizard again on payt login? (You can always re anable it under My Assault)			
5	Click Finish.			

# Step 3: Enabling the SiteManager Connection of the HMIGTO Appliance to GateManager

## **Overview**

The next step is to enable the SiteManager software on the HMIGTO appliance and establish a network connection between the appliance—physically located on the work site—and the GateManager server.

# Activating and Configuring the SiteManager Software

Step	Action
1	On the HMIGTO appliance, enter the Vijeo Designer RunTime <b>Configuration</b> menu.
2	Select the Offline tab: Offline System Diagnostics
3	Click the Network button. Result: The Network window appears: Network Ethernet 1 IP Address: Definition of the second of the
4	Click the Secure Connect button.
	Result: The Secure Connect SiteManager Embedded window appears.
5	Set the Access Control option to Enabled:

Step	Action
	Secure Connect SiteManager Embedded
	Access Control    Enabled  Disabled
	Result: Additional fields are displayed:
	Secure Connect SiteManager Embedded
	Access Control    Enabled  Disabled
	Connection Status
	SME Version 17393
	Server Address
	Domain Token
	Appliance Name
	Proxy Address
	Proxy User
	Factory Default Apply Change Cancel
6	Specify the following items:
	<ol> <li>In the Server Address field, type the IP address of the GateManager server. This address is contained in the email you received when registering your trial version</li> </ol>
	of EcoStruxure Secure Connect. Refer to Logging in to GateManager, page 14. 2. In the <b>Domain Token</b> field, type the domain token assigned to you, "Brian-Inc".
	This is contained in the email you received when registering your trial version of EcoStruxure Secure Connect. Refer to Logging in to GateManager, page 14.
	3. In the <b>Appliance Name</b> field, type a unique name for your appliance, for example "MyHMIGTO". This name is later used to identify the appliance in the
	If the HMI has been previously configured, it is strongly recommended to click the
	factory default button in the bottom left of the window to return SiteManager to its factory default settings.
	<b>NOTE:</b> If your appliance uses a proxy server, you may also need to complete the <b>Proxy Address</b> , <b>Proxy Server</b> , and <b>Proxy Password</b> fields. Refer to Configuring a Proxy Server, page 11.
7	Click the Apply Change button.
	<b>Result:</b> You return to the <b>Network</b> window. In a few seconds, the indicator next to the <b>Secure Connect</b> button turns green to indicate a successful connection to your domain on the GateManager server:
	Secure Connect Not Attached to a Domain
8	Click Return on the Network window.

# Step 4: Registering an Appliance on GateManager

# **Overview**

Every HMI/iPC appliance and device deployed as part of a EcoStruxure Secure Connect solution must be associated with a license you have purchased. This association is made in the GateManager user interface.

# Associating the HMIGTO Appliance with a SiteManager License

Action Step 1 If you are not already logged in, log in to the GateManager user interface (see Connection to the GateManager, page 14). 2 In the Tree tab on the left, find the following entry: Standard Pool (Secure Connect SiteManager Extended, 5 Agents #ffffff) 2 1 Number of available licenses remaining 2 Number of SiteManager agent licenses available A SiteManager agent is a user-defined rule for building a remote connection to either the SiteManager appliance or a device connected to the SiteManager appliance on the work site. Creating an Agent, page 22 describes how to create the rule for this use case. Either a SiteManager Extended, 5 Agents license (included in the trial version) or a SiteManager Extended, 10 Agents license, page 9 is required for this use case. Make sure that there is at least one available license. If the license icon is red and 0 appears ( , there are no more available licenses. In this case, return to the EcoStruxure Secure Connect web site or contact your reseller to purchase additional licenses.

**NOTE:** This may already have been done when using the wizard to create user accounts, page 16.

Step	Action
3	In the <b>Tree</b> tab on the left, select the appliance to register. Appliances are labeled with the domain prefix and appliance name you assigned in Vijeo Designer RunTime when configuring the connection to GateManager, page 18:
	Tree       Files       Licenses       Server         Image: Server       Image: Server       Image: Server         I
	Brian Smith Admin (Brian Smith)     Brian-inc[MyHMIGTO]     domain2     [New account] ()
	<ul> <li>Administrator ()</li> <li>GM-Server-Admin (Brian SMITH)</li> <li>LM-User (John BLACK)</li> <li>LM-Yves (Yves DUPONT)</li> </ul>
	The properties of the appliance appear in the <b>Appliance</b> tab on the right.
	Appliance         Agents         Backups         Alerts         Actions         Audit           Name:         Brian-Inc (MvHMIGTO)         Brian-Inc (MvHMIGTO)         Brian-Inc (MvHMIGTO)         Brian-Inc (MvHMIGTO)
	Product: Schneider SiteManager Embedded for Windows Serial: 6126:0030640FEFA1-pe3lifrHOXXV Created: 2018-08-20 09:35 Source IP:
	Firmware: v6126_18052 License: An appropriate Secure Connect SiteManager license is required to attach this appliance. ?
	Domain Token: ROOT.domain1
	🔄 Bind license and 🖈 attach here Secure Connect SiteManager Extended, 5 Agents 👻 🖗 Appliances must be attached to a domain to enable remote access.
	Last heartbeat: 2018-08-20 11:43:27 (2 seconds ago) Next: 11:44:26 (in 00:46)
	DEV1 port:         192.163.3.10           Operating System:         Windows 7 SP1 (x86)           Uptime:         2 hours 6 minutes 63 seconds           Date/time:         2 018-08-20 11:43:24           GateManager Address:         Type:
4	Click Bind license and attach here.
	<b>Result:</b> The appliance is associated with the SiteManager licence.
	Notice that the number of available licenses in the <b>Tree</b> view on the left is reduced by 1.

# **Step 5: Creating an Agent**

# **Overview**

The next step is to create an agent that will allow direct access to the Ethernet interface of the TM251MESE logic controller at the work site.

An agent is a user-defined rule containing all the parameters necessary for LinkManager to connect to an individual device. To connect to 5 devices, for example, you would need to create 5 different agents. The license in the trial version is an extended 5 license: up to 5 agents can be used with this appliance, permitting up to 5 extended devices behind the iPC/HMI appliance. Extended devices are those accessible from the iPC/HMI appliance over the network of the work site.

It is also possible for multiple agents to connect to the same device: for example one to establish an FTP connection to the device, and another to build a Vijeo Designer project transfer connection to the device.

## **Creating an Agent**

Step	Action
1	On the PC logged in to the GateManager user interface, page 14, right-click on the <b>MyHMIGTO</b> appliance in the <b>Tree</b> tab on the left and choose <b>Open SiteManager GUI</b> .
	Result: The SiteManager user interface opens in a new browser tab:
	Eco@Fuxuurer Secure Connect - Site Manager Schneider
	SETUP • GateManager Status Log • HELP
	ADOUT
	Schneider Sitemanager Embedded for Windows - Setup Assistant
	1. GateManager: Connected to (LAN) Edit
	2. Device Agents: 2 up, 1 down Edit
	3. Chat / Scratchpad: Updated 91 days ago Edit
	You can open the Setup Assistant at any time by clicking on SETUP in the top menu.
	Note: If you click on HELP it shows specific help for the current configuration page.
	Please consult the online help as your first step in solving setup problems.
2	Click the <b>Edit</b> button next to <b>Device Agents</b> .
	<b>Result:</b> A list of existing agents appears:
	Eco <b>O</b> truxurer Secure Connect - Site Manager Schneider
	SETUP • GateManager Status Log • HELP
	About
	GateManager Agents - Setup Assistant You can configure an agent to monitor a device connected to the SiteManager Serial port and TCPUR explored setup control and citizen to DCR converts or Linkin explored of the SiteManager
	Click [New], and give the Agent a name (this name will be what the LinkManager user will see), and select a suitable device type (first vendor, then model). Then click on mark to specify
	The SiteManager will instantly try to connect to the device, and if successful the Agent will go IDLE and appear on the GateManager and any LinkManager that have been granted access to the densities of the DickManager.
	ournam for the Supervanager. If not successful, the Agent will report an error, and the agent will not be registered on the CateManager and subsequently not on LinkManagers either.
	Help     Continue Setup >>
	Using 3 of 5 extended agents
	Status Disable S/N         Device Name         Device Type         Device IP & Parameters         Tunnel         Comment
	IDLE #01 Vijeo Designer Access Schneider Electric    Ethernet    PC
	IULE #A1 WebGate Access GENERIC
	Refresh Save New
3	Click New.

Proceed as follows:

Step	Action							
4	Specify the following information:							
	• Device Name: M251 PLC							
	Device Type: Schneider Electric / Ethernet							
	<b>NOTE:</b> The <b>Device Type</b> list box contains the default agent definitions for access to all supported devices (port rules, and so on).							
	The <b>GENERIC</b> device type provides full access to the device.							
	<b>PC</b> in the <b>Device IP &amp; Parameters</b> column refers to the IP address of the appliance. <b>PC</b> can also be selected for HMI appliances.							
5	Click the <b>Parameter Details</b> button 🖆 to display additional parameters:							
	Eco 2 tructure Secure Connect - Site Manager							
	About							
	"M251 PLC" - Schneider Electric Ethernet Agent – Setup Assistant							
	When you configure an agent to monitor a TCP/IP enabled device located on either the DEV network or Uplink network of the SiteManager, you must specify the device IP address below.							
	Click [Save] and then [Back] to make the SiteManager instantly try to connect to the device.							
	If not successful, the Agent will report an error, and the agent will not be registered on							
	the GateManager and subsequently not on LinkManagers either.							
	Help Continue Setup >>							
	When using SoMachine software, you have to select a Remote Connection targeting the anext's IP address (see Program - Online - Remote Connection)							
	Device Address:							
	Address on LinkManager:							
	Address on GateManager:							
	Always On:							
	Extra TCP ports:							
	Extra UDP ports:							
	Extra GTA Service:							
	Alternative SoMachine Discovery mode:							
	Enable WWW service:							
	Enable RDP service:							
	Custom Settings:							
	Save Back							
	Specify:							
	<ul> <li>Device Address. The IP address of the M251 programmable logic controller</li> </ul>							
	Always On. Selected							
	Alternative SoMachine Discovery mode. Selected							
6	Click Save then Continue Setup.							
	<b>Result:</b> The new agent is added to the list of agents. If SiteManager can communicate with the device, the device status changes to <b>IDLE</b> after a few seconds, indicating that a connection has been made to the device but data is not yet being exchanged:							
	EcoOrtrawere Secure Connect - Site Manager Scheeder							
	SETUP • GateManager Status Log • HELP							
	About GateManager Agents - Setup Assistant							
	You can configure an agent to monitor a device connected to the SiteManager Serial port							
	and TCP/IP enabled devices located on either the DEV network or Uplink network of the SiteManager.							
	Click [New], and give the Agent a name (this name will be what the LinkManager user will see), and select a suitable device type (first vendor, then model). Then click on  the device address and other relevant parameters.							
	The SiteManager will instantly try to connect to the device, and if successful the Agent will go IDLE and appear on the GateManager and any LinkManager that have been granted access to the domain of the SiteManager.							
	If not successful, the Agent will report an error, and the agent will not be registered on the GateManager and subsequently not on LinkManagers either.							
	Heip Continue Setup >>							
	Using 3 or 5 extended agents Status Disable S/N Device Name Device Type Device IP & Parameters Tunnel Comment							
	IDLE       #01       Vijeo Designer Access       Schneider Electric ▼       Ethernet       PC       200         IDLE       #A1       WebGate Access       GENERIC       Web access (WWW) ▼       PC       200							
	IDLE #02 M251 PLC Schneider Electric V Ethernet V Month on + SOM							
	Refresh Save New							

Step	Action						
7	Click Continue Setup.						
8	Close the browser tab to return to the GateManager user interface.						
9	In the Tree tab on the left, select the new agent, which appears below the MyHMIGTO appliance: Tree Files Leanses Server C Tree Files Leanses Server C Tree Files Leanses Server C Tree Files Leanses (Bran-Inc) Bran Smith (Brian Smith) Brian Smith (Brian Smith) C Brian-Inc (MyTO) C TP Access (Brian-Inc) - Product: Schneider Electric - Elment Agent Sorial: 0030640FEAT-bpa3iftHOXXV#02 Master: D Brian-Inc (MyHMIGTO) C Teated: 2018-08-24 11:20 Source IP SiZe vendor 18052 Www · Clabele Delete Last heartbeat: 2018-08-24 16:57:11 (3 seconds ago) Next: 11:58:08 (in 00:19) Device Address: Uptime: 7 hours 37 seconds Connections: 15 Packets Transmitted: 6 Bytes Received: 1376 Bytes Transmitted: 136						
	<b>Result:</b> The status of the device appears in the <b>Device</b> tab on the right.						

# Step 6: Installing LinkManager

# Overview

The next step is to install LinkManager on the laptop computer in the local office.

# Installing LinkManager

To install LinkManager:

Step	Action						
1	If you are not already logged in, log in to the GateManager user interface (see Connection to GateManager, page 14) on the laptop computer in the office.						
2	Click the Refresh icon in the bottom left corner of the GateManager window:						
	Image: Provide and the second sec						
	LinkManager: Click to Detect      Click to detect LinkManager Client.						
	<b>Result:</b> GateManager checks whether the LinkManager software is installed on the laptop computer.						
3	The following window appears:						
	EcoPtruxure Secure Connect - Link Manager						
	Do not close this window! GateManager uses it to manage the LinkManager Client on your PC. It will close automatically when you log off.						
	LinkManager Client not running!						
	Install LinkManager Start LinkManager 😽 Retry						
	Click Install LinkManager.						
4	A message appears asking whether you want to save the setup file. Click <b>Run</b> to launch the setup program.						

Step	Action					
5	Click <b>Run</b> on the security warning window that appears. <b>Result:</b> The LinkManager software is installed on the laptop computer. When installation is complete, a LinkManager icon appears in the Windows system tray in the bottom right of the screen.					
6	Return to the GateManager window and click the Refresh icon in the bottom left of the window again:					
	<ul> <li>Image: Segretize: Constraints of the segret sector of the segret sector of the sector o</li></ul>					

# Step 7: Starting LinkManager and Connecting to Device

# **Overview**

The final step is to log in to LinkManager on the laptop computer and view data generated by the device.

# Logging in to LinkManager

Step	Action					
Step 1	Action         Open the email you received after creating the LinkManager user account (see Creating User Accounts, page 16). For example:         Image: Creating User Account Intermet Explore 11. Edg. Chrome, Opera, Safari, and Firefox.         Please ensure that your browser is up-to-date and has JavaScript and TLS 1.2 enabled if you have problems connecting.         Image: Creatificate in this mail is issued					
2	4 Domain token prefix used to identify appliances. The default Web browser is launched and the LinkManager login window appears:					
3	Link Manager         Version         This application is protected by copyright law and international treatme.         2017 Schneider Electric Industries SAS. All Rights Reserved.         Life Is On         Select the Certificate option.         NOTE: Logging in with a certificate offers improved cybersecurity and is the only option recommended by Schneider Electric.					
4	Click Choose and select the previously downloaded LinkManager certificate file.					
L						

Step	Action						
5	Enter the password from the email you received.						
6	Click Login. Result: The Link Manager user interface appears:						
	Tree - LinkManager User: LM-User (John BLACK)         Image: Start St						

# Connecting to the M251 Programmable Logic Controller

Step	Action						
1	In the <b>Tree</b> tab on the left of the LinkManager use interface, expand the domain structure and select first the <b>MyHMIGTO</b> device, then the <b>M251 PLC</b> agent that you created earlier in GateManager, page 22. <b>Result:</b> The device properties appear in the <b>Appliance</b> tab on the right.						
2	Click the <b>Connect</b> button on the right:						
	Tree - LinkManager User: LM-User (John BLACK)         Image: Comparison of the state of the						
	Tree - LinkManager User: LM-User (John BLACK)         ROOT E       Image: Comparing the second s						
	A secure connection has now been established between LinkManager and the device. <b>NOTE:</b> You can also click the <b>WWW</b> button on the right to log in to the web site embedded in the M251 programmable logic controller. This allows you to directly monitor the controller, view diagnostics, and perform a number of maintenance operations (including stopping and starting the controller).						

# Remotely Programming the M251 Programmable Logic Controller

Step	Action							
1	1 Right-click the SoMachine <b>Gateway Tray Application</b> icon <b>1</b> in the Windows stray of the laptop computer and choose <b>Gateway Management Console</b> .							
	Go to the <b>Gateway Configuration</b> tab and select the <b>Scan all IP addresses</b> option if it is not already selected:							
	Gateway Management Console							
	General Gateway Configuration Static Remote Connections Devices to scan and to connect to Device name starts with: LMC 078 (via USB) USB Serial Port COM port: M241/251 (via Bluetooth) 88							
	IP addresses of network adapters to scan and to connect to							
	Scan behaviour Forward scanned devices to another gateways in this subnet							
	OK Cancel Help							
	This ensures that SoMachine is configured to scan all IP addresses for incoming communications. Click <b>OK</b> .							
2	Right-click on the <b>Gateway Tray Application</b> icon <b></b> in the Windows system tray again, and choose <b>Restart Gateway</b> . Or you can add a static route in the <b>Gateway Tray Application</b> :							
	Gateway Management Console							
	General Gateway Configuration Static Remote Connections							
	Remote IP address:							
	Add Connection           Address         State         Connection							
	Remote connections are static tunneling connections from the local PC to the given PLC.							
	As long as a remote connection is established a scan on the local gateway also lists the devices scanned by the PLC.							
OK Cancel Help								
	<ol> <li>Click the Static Remote Connections tab.</li> <li>In the Remote IP address field, enter the local IP address of the M251 programmable logic controller, then click Add connection.</li> <li>Click OK.</li> </ol>							

Step	Action						
	<b>NOTE:</b> This step is important, as it establishes the connection between LinkManager and the remote HMIGTO appliance.						
3	Start either <b>SoMachine Central</b> or <b>Logic Builder</b> , and create a new project. Add a TM251MESE logic controller to the project. Refer to the <i>M251 Programming Guide</i> in the EcoStruxure Machine Expert online help if necessary.						
4	In Logic Builder, go to the <b>Devices</b> tab on the left and double-click on the <b>Ethernet_1</b> (Ethernet Network) node to display the Ethernet properties of the logic controller:						
	Ethernet_1 X         Configuration         Configured Parameters         Interface Name       EthernetPort0         Network Name       My_Device         IP Address by DHCP       IP Address by BOOTP         IP Address       IP Address         IP Address       IP Address         Subnet Mask       IP Address         Gateway Address       0 . 0 . 0 . 0         Ethernet Protocol       Ethernet 2         Transfer Rate       Auto         Security Parameters       SoMachine protocol active         Web Server active       Web Server active         IP Solver active       Discovery protocol active         Simple Simple Protocol active       Simple Protocol active         Veb Visualisation protocol active       Simple Protocol active         VebVisualisation protocol active       Sintex device identification         VebVisualisation protocol active       PhCP Server active         VebVisualisation protocol active       When active, each device that will be added to the fieldbus, can be configured in order to be identified by its name or MAC Address, instead of its IP Address.						
5	Enter the <b>IP Address</b> and the <b>Subnet Mask</b> of the M251 programmable logic controller located on the work site.						
	<b>NOTE:</b> Verify that the values match those you entered when creating the agent, page 22.						
6	In the <b>Gateway Address</b> field, enter the IP address of the HMIGTO appliance that is connected to the M251 programmable logic controller.						
7	<ul> <li>In the Applications Tree tab, create a new programmable object unit (POU):</li> <li>1. Right-click on Application (MyController: TM251MESE) and choose Add Object &gt; POU</li> <li>2. In the Implementation language list, choose Instruction List (IL), then click Add.</li> <li>3. Add a new section to the existing application in the controller. For example, create a simple test POU containing a few lines of code: %MW10 := %MW10 - 1; %MW11 := WSTRING_TO_WORD("51");</li> </ul>						
8	In the <b>Devices Tree</b> tab on the left, double-click <b>Application (MyController:</b> <b>TM251MESE)</b> . At the bottom of the <b>Controller Selection</b> tab on the right, select <b>IP</b> <b>Address</b> in the <b>Connection Mode</b> list, and enter the IP address of the M251 logic controller:						

Step	Action					
	Connection Mode: IP Address:     IP Address      Watch 1				Energy Management Name Device Template Controller CHMI & IPC Devices & Modules	
	Expression 1	Туре	Value	Prepared value	Address	Comment
		La	ast build: 😮 0 😗	0 Precompile: 3		Current user: (nobody)
9	Click the Login button solution the toolbar, or choose Online > Login.					
10	Click <b>Yes</b> on the window that appears to log in to the logic controller.					
11	Click <b>OK</b> to transfer the new POU from the LinkManager laptop computer to the logic controller on the work site.					
12	In the <b>Application tree</b> tab, click the Start/Stop icon on the toolbar to start and stop running the POU on the logic controller.					
	You are now in control of the program running on the remote M251 programmable logic controller!					

## Glossary

#### Α

#### agent:

An object that contains all the parameters necessary for LinkManager to connect to a remote device. For example, an agent might specify use of the FTP protocol, the IP address of the device, and use of the standard FTP port number.

#### appliance:

An HMI/iPC display unit that LinkManager can connect to.

#### D

#### device:

A device, such as a Programmable Logic Controller (PLC), 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 or Logic Program Software.

#### domain token:

A text string provided to you when you register EcoStruxure Secure Connect. When concatenated with the appliance name, uniquely identifies appliances in your domain.

#### domain:

A private area of the GateManager software in which to configure and manage users, appliances, licenses, audit logs, alerts, automated actions, and so on.

#### G

#### GateManager:

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

#### Η

#### HTTPS:

Hyper Text Transfer Protocol Secure

#### L

#### LinkManager:

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

#### S

#### 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.

#### SiteManager Embedded:

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

#### SiteManager:

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

#### subdomain:

A logical division of a domain, useful for organizing equipment based on purpose, access level, physical location, and so on.

#### Т

#### TLS:

Transport Layer Security

Schneider Electric 35 rue Joseph Monier 92500 Rueil Malmaison France

+ 33 (0) 1 41 29 70 00

www.se.com

As standards, specifications, and design change from time to time, please ask for confirmation of the information given in this publication.

© 2025 Schneider Electric. All rights reserved.

EIO000003800.04