

# EcoStruxure Secure Connect Advisor Quick Start Guide

12/2018



EIO0000003800.00

[www.schneider-electric.com](http://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, EcoStruxure Operator Terminal Expert, and EcoStruxure Machine Expert are 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, and 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.

© 2018 Schneider Electric. All rights reserved.

---

# Table of Contents

---



Safety Information .....	5
About the Book .....	7
EcoStruxure Secure Connect Advisor .....	9
Use Case Components .....	10
Installation Overview .....	14
Step 1: Connecting to the GateManager .....	14
Step 2: Creating User Accounts .....	17
Step 3: Enabling the SiteManager Connection of the HMIGTO to GateManager .....	20
Step 4: Registering an Appliance on GateManager .....	24
Step 5: Creating an Agent .....	26
Step 6: Installing LinkManager .....	31
Step 7: Starting LinkManager and Connecting to Device .....	33
Glossary .....	41



---

# 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.

---

# About the Book

---



## At a Glance

### Document Scope

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

**NOTE:** Read and understand this document and all related documents (*see page 7*) before installing, operating, or maintaining your EcoStruxure Secure Connect Advisor.

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

### Validity Note

This document has been updated for the release of Vijeo Designer V6.2 SP7, SoMachine V4.3 and EcoStruxure Operator Terminal Expert V3.0.

### Related Documents

Title of Documentation	Reference Number
EcoStruxure Secure Connect Advisor User Guide for GateManager	<a href="#">EIO0000002449 (ENG)</a> <a href="#">EIO0000002563 (FRE)</a> <a href="#">EIO0000002564 (GER)</a> <a href="#">EIO0000002565 (ITA)</a> <a href="#">EIO0000002566 (SPA)</a> <a href="#">EIO0000002567 (CHS)</a>
EcoStruxure Secure Connect Advisor Troubleshooting Guide for LinkManager (Starting and Connecting)	<a href="#">EIO0000002450 (ENG)</a> <a href="#">EIO0000002568 (FRE)</a> <a href="#">EIO0000002569 (GER)</a> <a href="#">EIO0000002570 (ITA)</a> <a href="#">EIO0000002571 (SPA)</a> <a href="#">EIO0000002572 (CHS)</a>
EcoStruxure Secure Connect Advisor Troubleshooting Guide for SiteManager	<a href="#">EIO0000002452 (ENG)</a> <a href="#">EIO0000002578 (FRE)</a> <a href="#">EIO0000002579 (GER)</a> <a href="#">EIO0000002580 (ITA)</a> <a href="#">EIO0000002581 (SPA)</a> <a href="#">EIO0000002582 (CHS)</a>

Title of Documentation	Reference Number
EcoStruxure Secure Connect Advisor User Guide for Security Setting	<a href="#">EIO0000002451 (ENG)</a> <a href="#">EIO0000002573 (FRE)</a> <a href="#">EIO0000002574 (GER)</a> <a href="#">EIO0000002575 (ITA)</a> <a href="#">EIO0000002576 (SPA)</a> <a href="#">EIO0000002577 (CHS)</a>
EcoStruxure Secure Connect Advisor Premium Domain Admin Guide for GateManager	<a href="#">EIO0000002732 (ENG)</a> <a href="#">EIO0000002733 (FRE)</a> <a href="#">EIO0000002734 (GER)</a> <a href="#">EIO0000002735 (SPA)</a> <a href="#">EIO0000002736 (ITA)</a> <a href="#">EIO0000002737 (CHS)</a>

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

---

## EcoStruxure Secure Connect Advisor

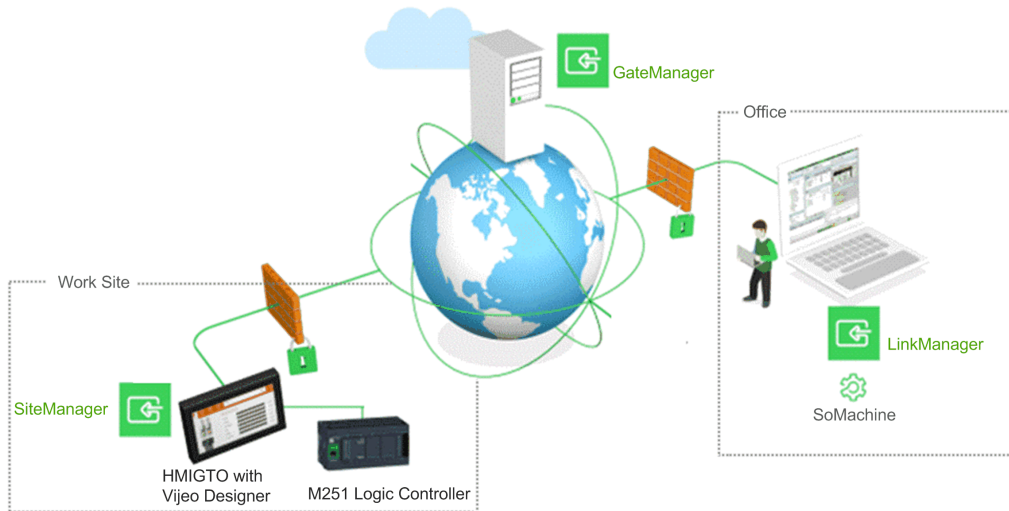
### Overview

EcoStruxure Secure Connect Advisor 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.

### Use Case

This quick start guide presents a typical use case for the deployment of EcoStruxure Secure Connect Advisor. It describes how to install and configure the components of an EcoStruxure Secure Connect Advisor 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 all IP addresses that appear in this guide to those used on your network.

**NOTE:** This document illustrates one possible use case. EcoStruxure Secure Connect Advisor 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 Advisor. The following license types are available:

License Type	Description
EcoStruxure Secure Connect Advisor	Allows an EcoStruxure Secure Connect Advisor user to log in to the EcoStruxure Secure Connect Advisor user interface on their PC and access devices in their customer domain.
EcoStruxure Secure Connect Advisor SiteManager Basic	Allows a secure remote connection to the appliance and offers full control over that appliance only.
EcoStruxure Secure Connect Advisor SiteManager Extended 5 Agents	Provides a secure remote connection to the appliance, offering full control over the appliance and full control over any asset within a subnetwork accessible from that appliance (up to 5 assets).
EcoStruxure Secure Connect Advisor SiteManager Extended 10 Agents:	Provides a secure remote connection to the appliance, offering full control over the appliance and full control over any asset within a subnetwork accessible from that appliance (up to 10 assets).

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

- 1 x EcoStruxure Secure Connect Advisor license
- 1 x EcoStruxure Secure Connect Advisor SiteManager Extended 5 agents license

### HMI/iPC Appliance

This use case assumes the use of a Magelis™ HMIGTO touchscreen display unit compatible with the latest version of the Vijeo Designer configuration software (Vijeo Designer V6.2 SP 7 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 Advisor, refer to Supported Model List (*see EcoStruxure Secure Connect Advisor, User Guide, For GateManager*).

---

## 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 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 and LinkManager user accounts.
- Setting up and managing audit logs, alerts, and automated actions (only available with GateManager Premium Access).

### WARNING

#### 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 Advisor supports a wide range of both Schneider Electric and third-party devices.

## Programming Software

This use case assumes the use of SoMachine Version 4.3 programming software, installed on the same laptop computer as the LinkManager software.

EcoStruxure Secure Connect Advisor 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 version 67. Any recent version of Apple Safari, Mozilla Firefox, Microsoft Edge, or Internet Explorer 9 (or later) 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.

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

The screenshot shows a configuration window titled "Secure Connect SiteManager Embedded" with a teal background. At the top, there is a yellow header bar with a lock icon and the title. Below the header, the "Access Control" section has two radio buttons: "Enabled" (selected) and "Disabled". Underneath, the "Connection Status" is indicated by a red square. The "SME Version" is displayed as "17393" in a grey box. Below this are several input fields: "Server Address", "Domain Token", "Appliance Name", "Proxy Address", "Proxy User", and "Proxy Password". At the bottom of the window, there are three buttons: "Factory Default", "Apply Change", and "Cancel".

**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

#### 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 (*see page 14*)
2. Create GateManager and LinkManager user accounts (*see page 17*)
3. Enable the SiteManager connection of the HMIGTO to GateManager (*see page 20*)
4. Register the HMIGTO appliance with SiteManager (*see page 24*)
5. Create an agent (*see page 26*)
6. Install LinkManager (*see page 31*)
7. Log in to LinkManager and test the connection (*see page 33*).

## Step 1: Connecting to the GateManager

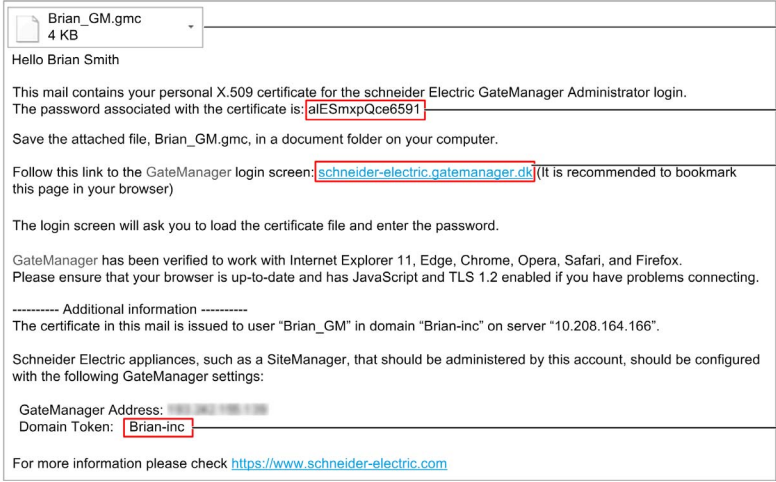
### Overview

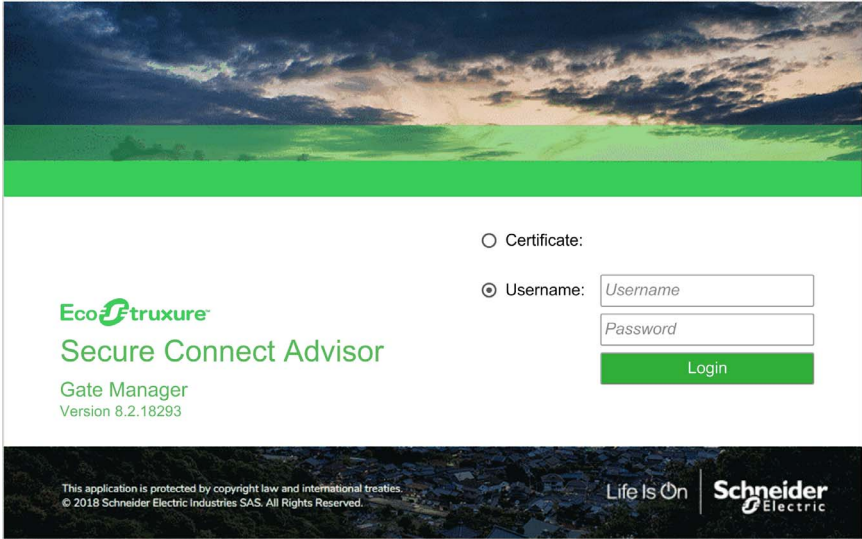
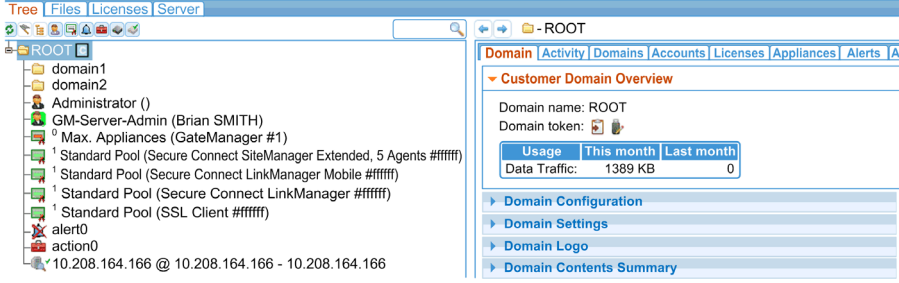
The first step is to request a trial license for EcoStruxure Secure Connect Advisor, then log in to the GateManager user interface using the credentials provided. This step can be done on the laptop computer in the office or any other computer.

### Obtaining a Trial License

Step	Action
1	Go to the EcoStruxure Secure Connect Advisor trial web site. If you are in Europe: <a href="https://eu.gatemanager.schneider-electric.com/trial">https://eu.gatemanager.schneider-electric.com/trial</a> If you are in North America: <a href="https://us.gatemanager.schneider-electric.com/trial">https://us.gatemanager.schneider-electric.com/trial</a>
2	Enter the information requested, then click <b>Sign up</b> . <b>Result:</b> A message is sent to the email address you provide.

## Logging In to GateManager

Step	Action
1	<p data-bbox="330 256 1156 305">Open the email that you receive, which contains all the information you need to log in to GateManager. For example:</p> <div data-bbox="330 313 1108 792" style="border: 1px solid gray; padding: 5px;">  <p data-bbox="330 326 532 358">Brian_GM.gmc 4 KB</p> <p data-bbox="330 367 450 383">Hello Brian Smith</p> <p data-bbox="330 399 1019 431">This mail contains your personal X.509 certificate for the schneider Electric GateManager Administrator login. The password associated with the certificate is: alESmXPQce6591</p> <p data-bbox="330 448 831 464">Save the attached file, Brian_GM.gmc, in a document folder on your computer.</p> <p data-bbox="330 480 1071 513">Follow this link to the GateManager login screen: schneider-electric.gatemanager.dk (It is recommended to bookmark this page in your browser)</p> <p data-bbox="330 529 831 545">The login screen will ask you to load the certificate file and enter the password.</p> <p data-bbox="330 561 1092 594">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.</p> <p data-bbox="330 610 577 626">----- Additional information -----</p> <p data-bbox="330 626 991 643">The certificate in this mail is issued to user "Brian_GM" in domain "Brian-inc" on server "10.208.164.166".</p> <p data-bbox="330 659 1092 691">Schneider Electric appliances, such as a SiteManager, that should be administered by this account, should be configured with the following GateManager settings:</p> <p data-bbox="330 708 598 724">GateManager Address: [REDACTED]</p> <p data-bbox="330 724 522 740">Domain Token: Brian-inc</p> <p data-bbox="330 756 776 773">For more information please check <a href="https://www.schneider-electric.com">https://www.schneider-electric.com</a></p> </div> <ol data-bbox="330 800 1249 930" style="list-style-type: none"> <li>1 Attached certificate file, with a .gmc (GateManager Certificate) extension</li> <li>2 Password to use with the certificate</li> <li>3 Web site address to use to log in to the GateManager user interface</li> <li>4 This domain token value is later used in the Vijeo Designer RunTime of the HMIGTO appliance. It is used to register the appliance in the GateManager customer domain.</li> </ol>
2	Save the GateManager certificate attached to the email to the local file system.

Step	Action
3	<p>Click the GateManager link in the received email (or copy and paste the link into a Web browser) to access the GateManager Login window:</p> 
4	<p>Select the <b>Certificate</b> option.</p> <p><b>NOTE:</b> Logging in with a certificate offers improved cybersecurity and is the only option recommended by Schneider Electric.</p>
5	<p>Click <b>Choose a file</b>, then browse and select the GateManager certificate you saved previously.</p>
6	<p>Enter the password contained in the received email.</p>
7	<p>Click <b>Login</b>.</p> <p><b>Result:</b> The GateManager user interface is displayed:</p> 

---

## Step 2: Creating User Accounts

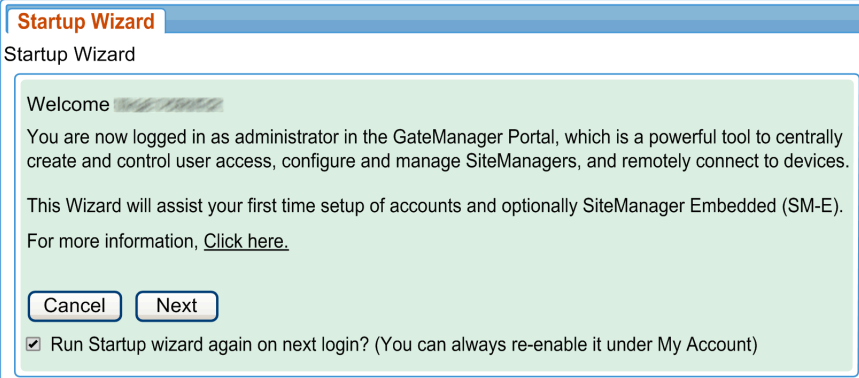
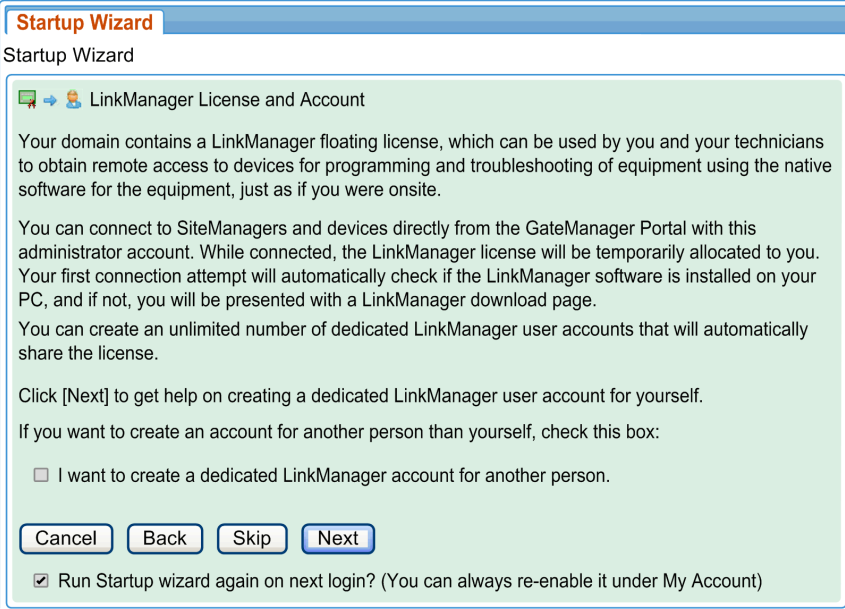
### Overview

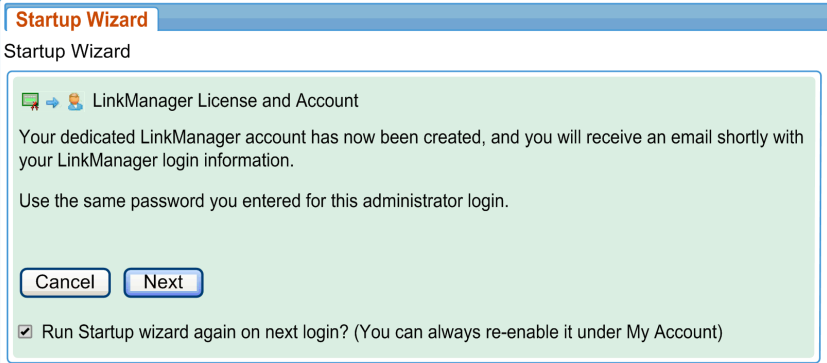
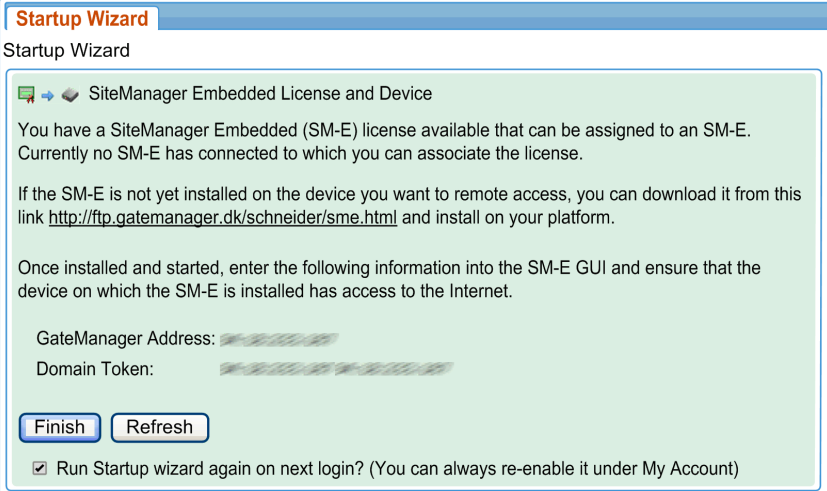
Once you have accessed the GateManager user interface, the next step is to create user accounts:

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	<p>The first time you log in to the GateManager user interface, a wizard screen is displayed on the right:</p> 
2	<p>Click <b>Next</b>. The following wizard screen is displayed:</p> 

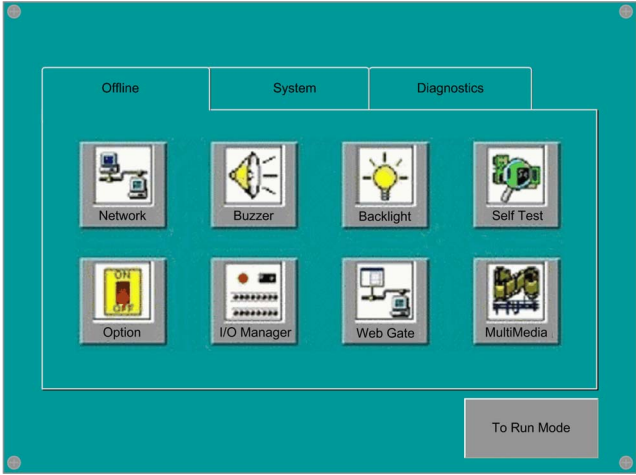
Step	Action
3	<p>Click <b>Next</b>. The following wizard screen is displayed:</p>  <p><b>Result:</b> An email is sent to the address you specified when requesting the trial license (<i>see page 14</i>). You will use this email later to install LinkManager (<i>see page 31</i>).</p>
4	<p>Click <b>Next</b>. The final page of the wizard is displayed:</p> 
5	Click <b>Finish</b> .

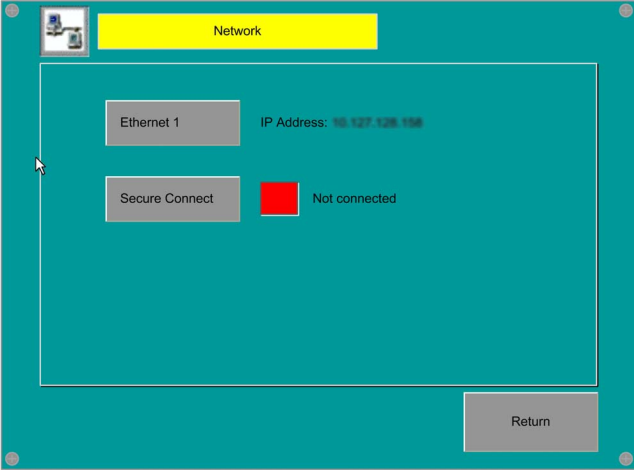
## Step 3: Enabling the SiteManager Connection of the HMIGTO to GateManager

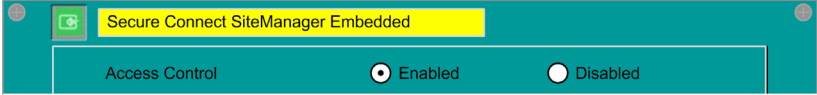
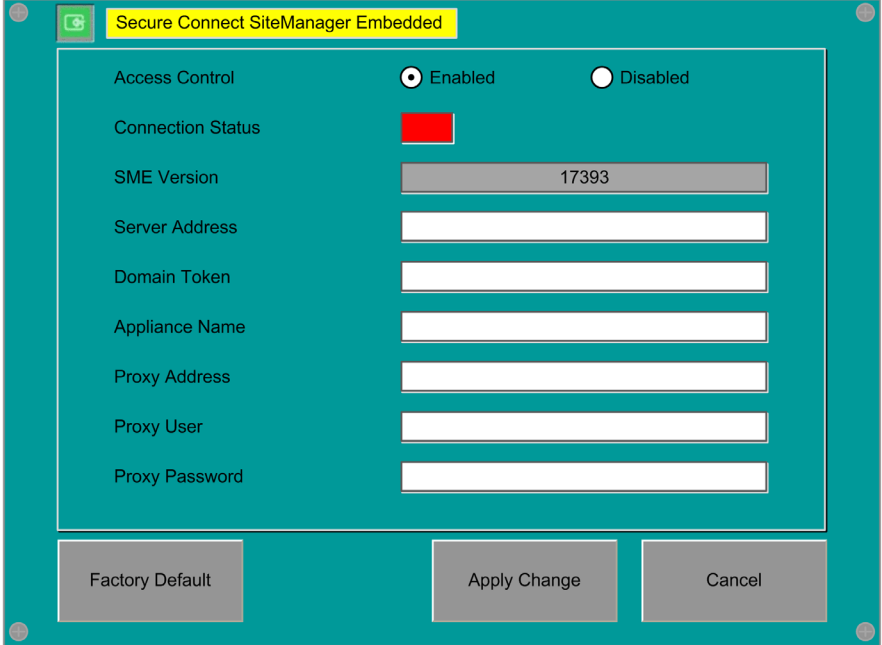
### Overview


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 <b>Offline</b> tab:  The screenshot shows a teal-colored configuration menu with three tabs at the top: 'Offline', 'System', and 'Diagnostics'. The 'Offline' tab is selected and highlighted. Below the tabs, there are eight icons arranged in two rows of four. The first row contains icons for 'Network', 'Buzzer', 'Backlight', and 'Self Test'. The second row contains icons for 'Option', 'I/O Manager', 'Web Gate', and 'MultiMedia'. A 'To Run Mode' button is located at the bottom right of the menu.

Step	Action
3	<p>Click the <b>Network</b> button.</p> <p><b>Result:</b> The <b>Network</b> window appears:</p> 
4	<p>Click the <b>Secure Connect</b> button.</p> <p><b>Result:</b> The <b>Secure Connect SiteManager Embedded</b> window appears.</p>

Step	Action
5	<p data-bbox="330 203 727 227">Set the <b>Access Control</b> option to <b>Enabled</b>:</p>  <p data-bbox="330 381 692 406"><b>Result:</b> Additional fields are displayed:</p> 

Step	Action
6	<p>Specify the following items:</p> <ol style="list-style-type: none"> <li>1. In the <b>Server Address</b> field, type the IP address of the GateManager server. This address is contained in the email you received when registering your trial version of EcoStruxure Secure Connect Advisor. Refer to Logging in to GateManager (<i>see page 15</i>)</li> <li>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 Advisor. Refer to Logging in to GateManager (<i>see page 15</i>)</li> <li>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 GateManager user interface.</li> </ol> <p>If the HMI has been previously configured, it is strongly recommended to click the <b>Factory Default</b> button in the bottom left of the window to return SiteManager to its factory default settings.</p> <p><b>NOTE:</b> If your appliance uses a proxy server, you may also need to complete the <b>Proxy Address, Proxy Server, and Proxy Password</b> fields. Refer to Configuring a Proxy Server (<i>see page 13</i>).</p>
7	<p>Click the <b>Apply Change</b> button.</p> <p><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:</p>  <p>The screenshot shows a teal-colored bar containing a grey button labeled 'Secure Connect' on the left. To its right is a small green square, followed by the text 'Not Attached to a Domain'.</p>
8	<p>Click <b>Return</b> on the <b>Network</b> window.</p>



## Step 4: Registering an Appliance on GateManager

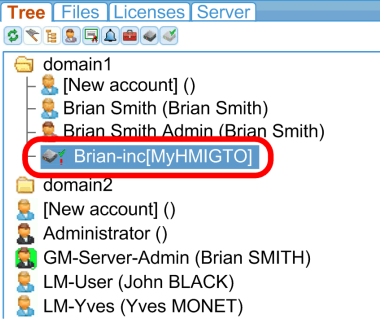
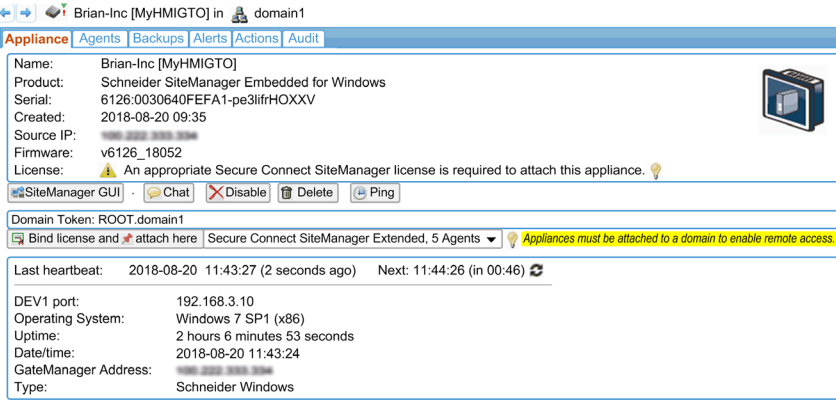
### Overview

Every HMI/iPC appliance and device deployed as part of a EcoStruxure Secure Connect Advisor 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

**NOTE:** This may already have been done when using the wizard to create user accounts (*see page 18*).

Step	Action
1	If you are not already logged in, log in to the GateManager user interface (see Connection to GateManager ( <i>see page 14</i> )).
2	<p>In the <b>Tree</b> tab on the left, find the following entry:</p>  <p>1 Number of available licenses remaining 2 Number of SiteManager agent licenses available</p> <p>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 (<i>see page 26</i>) describes how to create the rule for this use case. Either a <b>SiteManager Extended, 5 Agents</b> license (included in the trial version) or a <b>SiteManager Extended, 10 Agents</b> license (<i>see page 10</i>) 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 Advisor web site or contact your reseller to purchase additional licenses.</p>

Step	Action
3	<p>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 (<i>see page 20</i>):</p>  <p>The properties of the appliance appear in the <b>Appliance</b> tab on the right.</p> 
4	<p>Click <b>Bind license and attach here</b>.</p> <p><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.</p>

---

## Step 5: Creating an Agent

### Overview

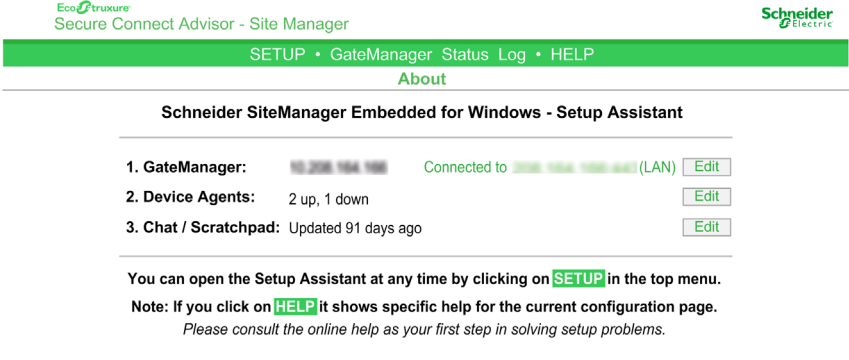
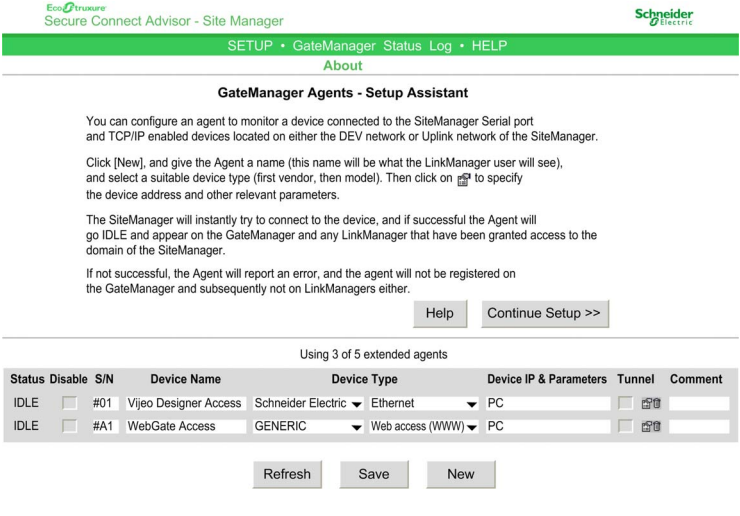
The next step is to create an agent that will allow direct access to the Ethernet interface of the TM251MESE logic controller at the work site.


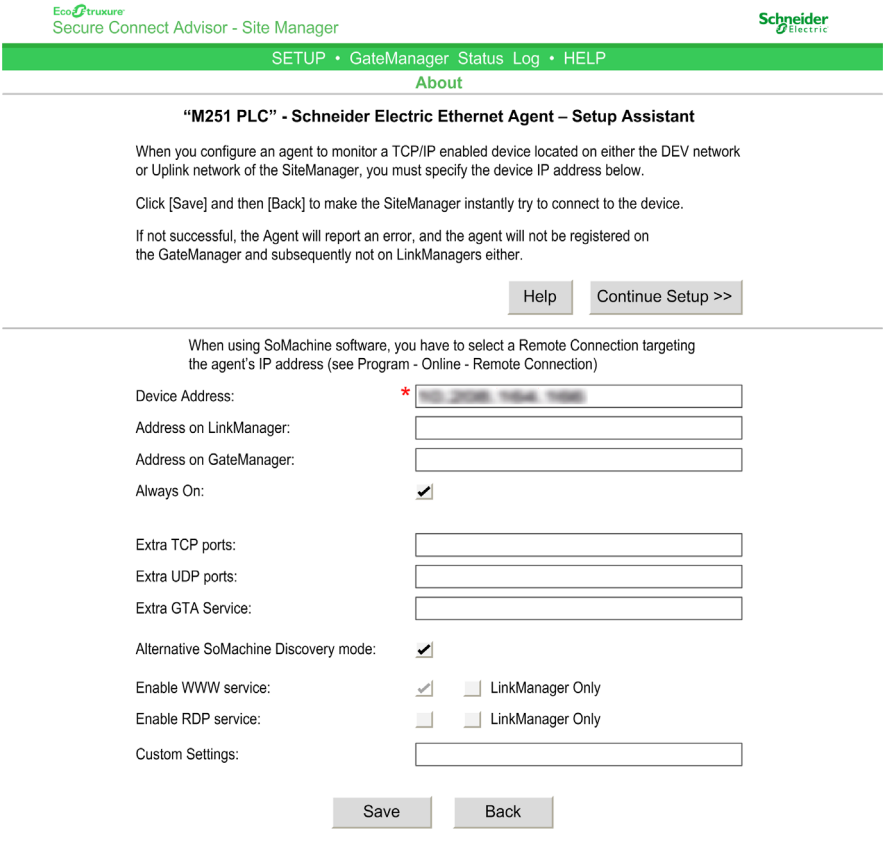
An agent is a user-defined rule containing all the parameters necessary for LinkManager to connect to an individual device. To connect to 5 devices, for example, you would need to create 5 different agents. The license in the trial version is an extended 5 license: up to 5 agents can be used with this 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.

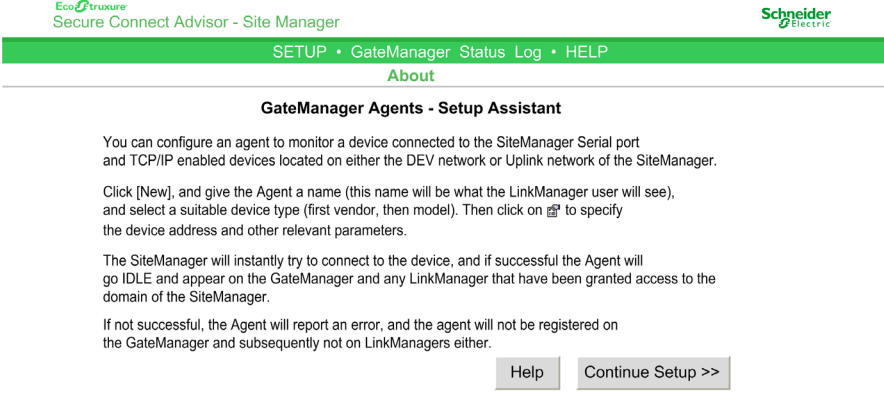
It is also possible for multiple agents to connect to the same device: for example one to establish an FTP connection to the device, and another to build a Vijeo Designer project transfer connection to the device.

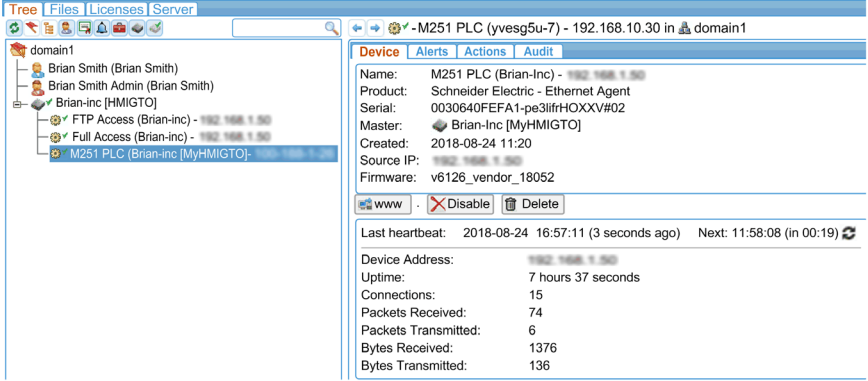
## Creating an Agent

Proceed as follows:

Step	Action																								
1	<p>On the PC logged in to the GateManager user interface (<i>see page 15</i>), right-click on the <b>MyHMIGTO</b> appliance in the <b>Tree</b> tab on the left and choose <b>Open SiteManager GUI</b>.  <b>Result:</b> The SiteManager user interface opens in a new browser tab:</p> 																								
2	<p>Click the <b>Edit</b> button next to <b>Device Agents</b>.  <b>Result:</b> A list of existing agents appears:</p>  <table border="1" data-bbox="362 1175 1103 1247"> <thead> <tr> <th>Status</th> <th>Disable</th> <th>S/N</th> <th>Device Name</th> <th>Device Type</th> <th>Device IP &amp; Parameters</th> <th>Tunnel</th> <th>Comment</th> </tr> </thead> <tbody> <tr> <td>IDLE</td> <td><input type="checkbox"/></td> <td>#01</td> <td>Vjeo Designer Access</td> <td>Schneider Electric</td> <td>Ethernet</td> <td>PC</td> <td></td> </tr> <tr> <td>IDLE</td> <td><input type="checkbox"/></td> <td>#A1</td> <td>WebGate Access</td> <td>GENERIC</td> <td>Web access (WWW)</td> <td>PC</td> <td></td> </tr> </tbody> </table>	Status	Disable	S/N	Device Name	Device Type	Device IP & Parameters	Tunnel	Comment	IDLE	<input type="checkbox"/>	#01	Vjeo Designer Access	Schneider Electric	Ethernet	PC		IDLE	<input type="checkbox"/>	#A1	WebGate Access	GENERIC	Web access (WWW)	PC	
Status	Disable	S/N	Device Name	Device Type	Device IP & Parameters	Tunnel	Comment																		
IDLE	<input type="checkbox"/>	#01	Vjeo Designer Access	Schneider Electric	Ethernet	PC																			
IDLE	<input type="checkbox"/>	#A1	WebGate Access	GENERIC	Web access (WWW)	PC																			
3	Click <b>New</b> .																								

Step	Action
4	<p>Specify the following information:</p> <ul style="list-style-type: none"> <li>● <b>Device Name:</b> M251 PLC</li> <li>● <b>Device Type:</b> Schneider Electric / Ethernet</li> </ul> <p><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).</p> <p>The <b>GENERIC</b> device type provides full access to the device.</p> <p><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.</p>
5	<p>Click the <b>Parameter Details</b> button  to display additional parameters:</p>  <p>When using SoMachine software, you have to select a Remote Connection targeting the agent's IP address (see Program - Online - Remote Connection)</p> <p>Device Address: <input type="text"/> *</p> <p>Address on LinkManager: <input type="text"/></p> <p>Address on GateManager: <input type="text"/></p> <p>Always On: <input checked="" type="checkbox"/></p> <p>Extra TCP ports: <input type="text"/></p> <p>Extra UDP ports: <input type="text"/></p> <p>Extra GTA Service: <input type="text"/></p> <p>Alternative SoMachine Discovery mode: <input checked="" type="checkbox"/></p> <p>Enable WWW service: <input checked="" type="checkbox"/> <input type="checkbox"/> LinkManager Only</p> <p>Enable RDP service: <input type="checkbox"/> <input type="checkbox"/> LinkManager Only</p> <p>Custom Settings: <input type="text"/></p> <p>Specify:</p> <ul style="list-style-type: none"> <li>● <b>Device Address.</b> The IP address of the M251 programmable logic controller</li> <li>● <b>Always On.</b> Selected</li> <li>● <b>Alternative SoMachine Discovery mode.</b> Selected</li> </ul>

Step	Action																																
6	<p>Click <b>Save</b> then <b>Continue Setup</b>.</p> <p><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:</p>  <p>Using 3 of 5 extended agents</p> <table border="1" data-bbox="362 748 1247 862"> <thead> <tr> <th>Status</th> <th>Disable</th> <th>S/N</th> <th>Device Name</th> <th>Device Type</th> <th>Device IP &amp; Parameters</th> <th>Tunnel</th> <th>Comment</th> </tr> </thead> <tbody> <tr> <td>IDLE</td> <td><input type="checkbox"/></td> <td>#01</td> <td>Vijeo Designer Access</td> <td>Schneider Electric</td> <td>Ethernet</td> <td>PC</td> <td><input type="checkbox"/> </td> </tr> <tr> <td>IDLE</td> <td><input type="checkbox"/></td> <td>#A1</td> <td>WebGate Access</td> <td>GENERIC</td> <td>Web access (WWW)</td> <td>PC</td> <td><input type="checkbox"/> </td> </tr> <tr> <td>IDLE</td> <td><input type="checkbox"/></td> <td>#02</td> <td>M251 PLC</td> <td>Schneider Electric</td> <td>Ethernet</td> <td>192.168.1.50 on + SOM</td> <td><input type="checkbox"/> </td> </tr> </tbody> </table> <p>Refresh Save New</p>	Status	Disable	S/N	Device Name	Device Type	Device IP & Parameters	Tunnel	Comment	IDLE	<input type="checkbox"/>	#01	Vijeo Designer Access	Schneider Electric	Ethernet	PC	<input type="checkbox"/>	IDLE	<input type="checkbox"/>	#A1	WebGate Access	GENERIC	Web access (WWW)	PC	<input type="checkbox"/>	IDLE	<input type="checkbox"/>	#02	M251 PLC	Schneider Electric	Ethernet	192.168.1.50 on + SOM	<input type="checkbox"/>
Status	Disable	S/N	Device Name	Device Type	Device IP & Parameters	Tunnel	Comment																										
IDLE	<input type="checkbox"/>	#01	Vijeo Designer Access	Schneider Electric	Ethernet	PC	<input type="checkbox"/>																										
IDLE	<input type="checkbox"/>	#A1	WebGate Access	GENERIC	Web access (WWW)	PC	<input type="checkbox"/>																										
IDLE	<input type="checkbox"/>	#02	M251 PLC	Schneider Electric	Ethernet	192.168.1.50 on + SOM	<input type="checkbox"/>																										
7	Click <b>Continue Setup</b> .																																

Step	Action
8	Close the browser tab to return to the GateManager user interface.
9	<p>In the <b>Tree</b> tab on the left, select the new agent, which appears below the <b>MyHMIGTO</b> appliance:</p>  <p><b>Result:</b> The status of the device appears in the <b>Device</b> tab on the right.</p>


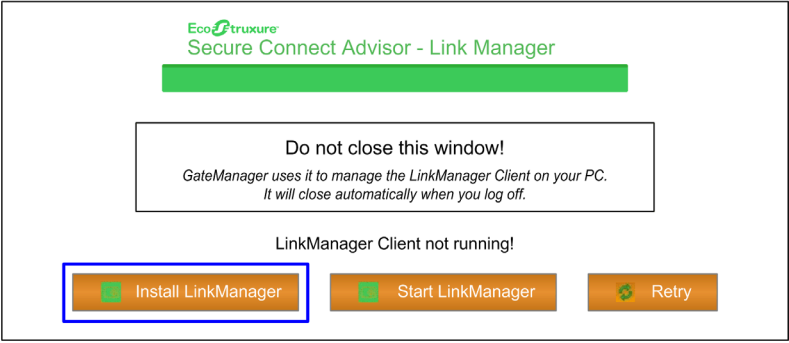
## Step 6: Installing LinkManager



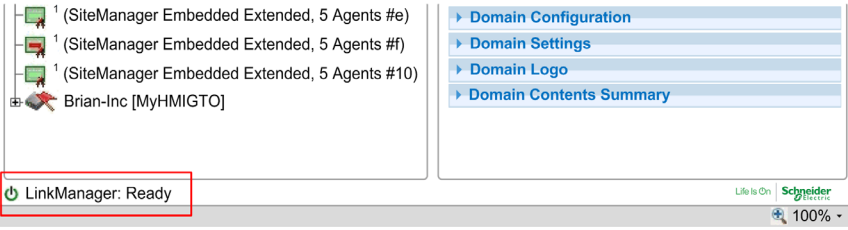
### Overview

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 ( <i>see page 14</i> )) on the laptop computer in the office.
2	<p>Click the Refresh icon in the bottom left corner of the GateManager window:</p>  <p><b>Result:</b> GateManager checks whether the LinkManager software is installed on the laptop computer.</p>
3	<p>The following window appears:</p>  <p>Click <b>Install LinkManager</b>.</p>
4	A message appears asking whether you want to save the setup file. Click <b>Run</b> to launch the setup program.

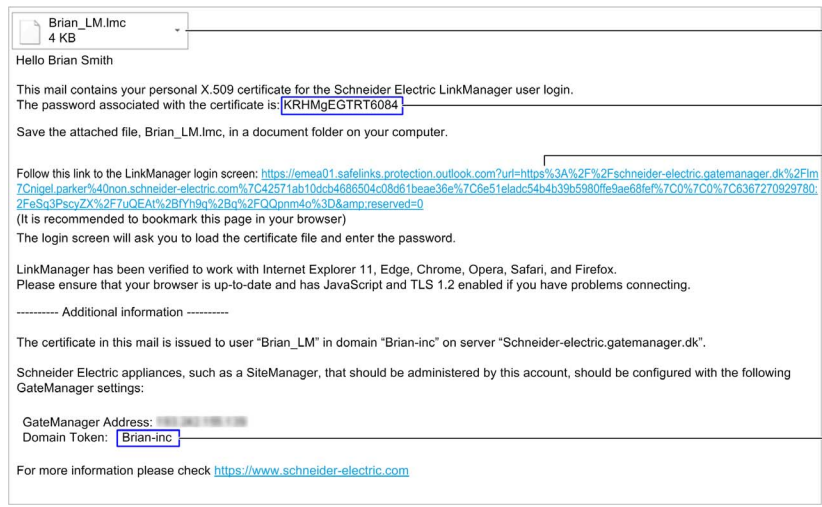
Step	Action
5	<p>Click <b>Run</b> on the security warning window that appears.</p> <p><b>Result:</b> The LinkManager software is installed on the laptop computer. When installation is complete, a LinkManager icon appears  in the Windows system tray in the bottom right of the screen.</p>
6	<p>Return to the GateManager window and click the Refresh icon in the bottom left of the window again:</p>  <p>This time, the installed LinkManager software is detected and the message changes to <b>LinkManager: Ready</b>:</p>  <p>LinkManager is now installed and ready for use.</p>

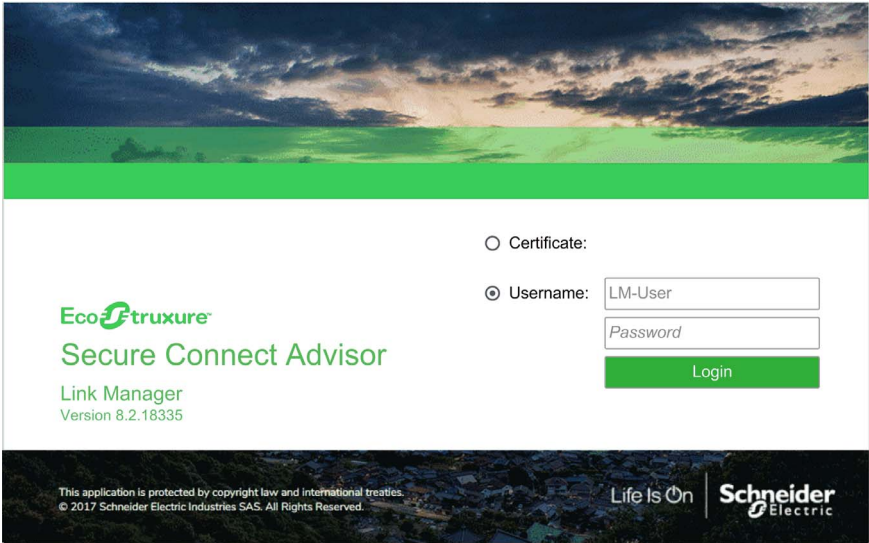
## Step 7: Starting LinkManager and Connecting to Device

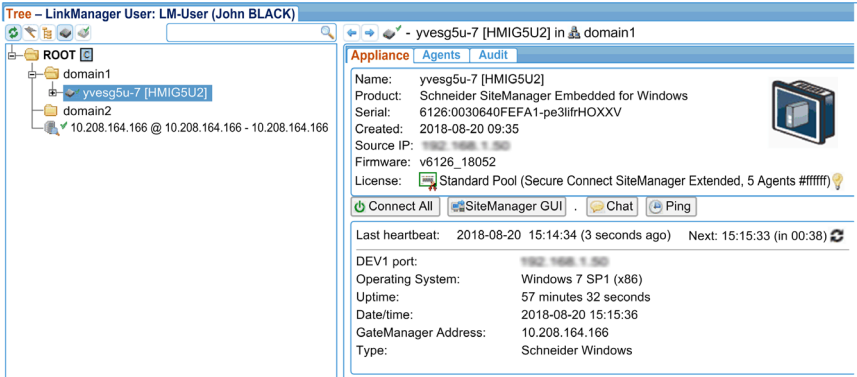
### Overview

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

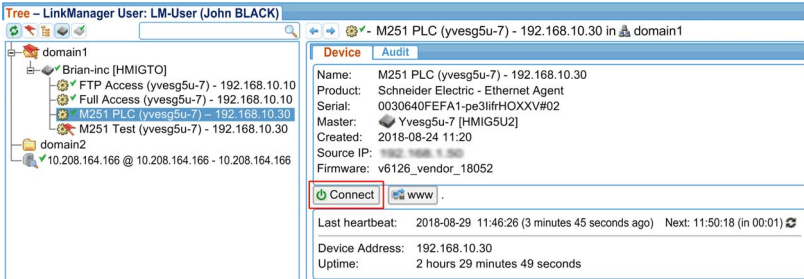
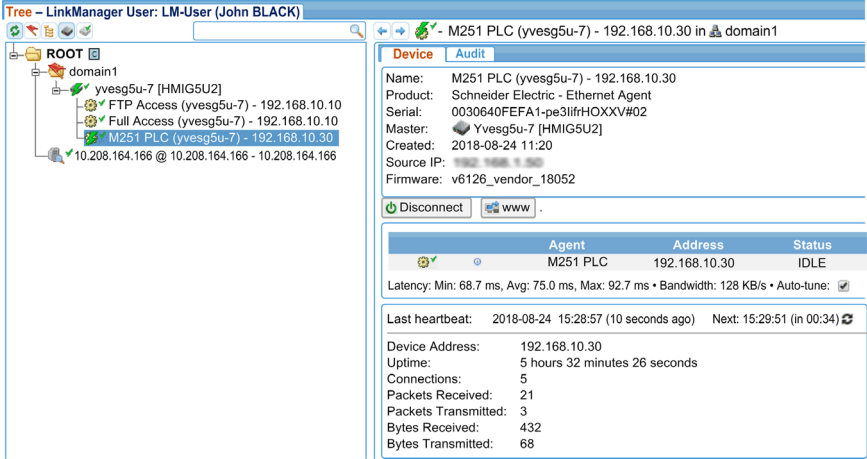
### Logging in to LinkManager

Step	Action
1	<p>Open the email you received after creating the LinkManager user account (see Creating User Accounts <i>(see page 18)</i>). For example:</p>  <p>1 Attached certificate file with a .lmc (LinkManager Certificate) extension.</p> <p>2 Password associated with the certificate</p> <p>3 Address to use to log in to the LinkManager user interface</p> <p>4 Domain token prefix used to identify appliances.</p>


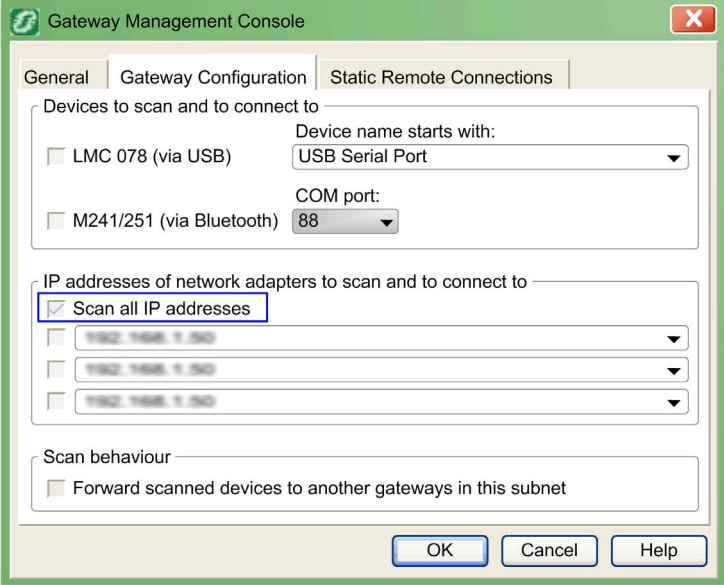

Step	Action
2	<p>The default Web browser is launched and the LinkManager login window appears:</p> 
3	<p>Select the <b>Certificate</b> option.</p> <p><b>NOTE:</b> Logging in with a certificate offers improved cybersecurity and is the only option recommended by Schneider Electric.</p>
4	<p>Click <b>Choose</b> and select the previously downloaded LinkManager certificate file.</p>
5	<p>Enter the password from the email you received.</p>

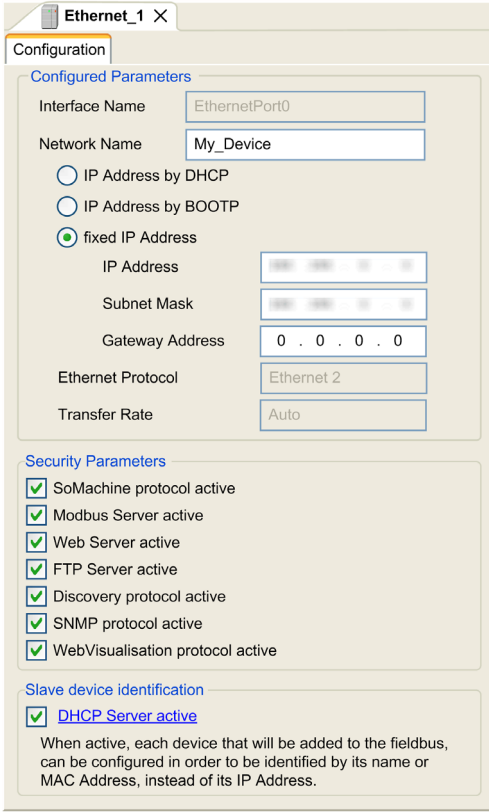
Step	Action
6	<p>Click <b>Login</b>.</p> <p><b>Result:</b> The Link Manager user interface appears:</p>  <p>The screenshot shows a web-based interface for Link Manager. On the left is a tree view with a 'ROOT' node containing 'domain1' and 'domain2'. Under 'domain1', there is a node for 'yvesg5u-7 [HMIG5U2]' with a status icon. Below this, a list of IP addresses is shown: '10.208.164.166 @ 10.208.164.166 - 10.208.164.166'. On the right, a detailed view for the selected appliance is displayed. It includes fields for Name, Product, Serial, Created, Source IP, Firmware, and License. Below these are buttons for 'Connect All', 'SiteManager GUI', 'Chat', and 'Ping'. A heartbeat section shows the last and next heartbeat times. A table of system details follows, including DEV1 port, Operating System, Uptime, Date/time, GateManager Address, and Type.</p> <p><b>NOTE:</b> The LinkManager user interface is very similar to that of the GateManager. Check that <b>LinkManager User:</b> appears in the top-left corner of the window.</p>

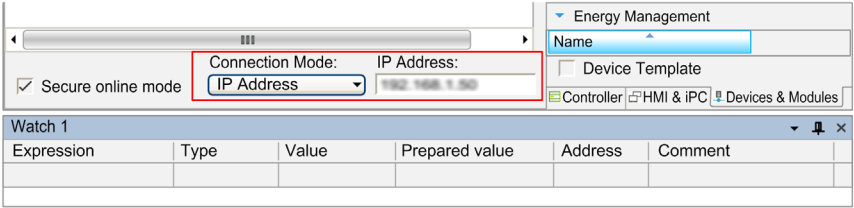

## Connecting to the M251 Programmable Logic Controller

Step	Action
1	<p>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. <i>(see page 26)</i></p> <p><b>Result:</b> The device properties appear in the <b>Appliance</b> tab on the right.</p>
2	<p>Click the <b>Connect</b> button on the right:</p>  <p><b>NOTE:</b> You could also select the <b>MyHMIGTO</b> appliance on the left, then click the <b>Connect All</b> button that appears on the right to connect all agents defined for the appliance simultaneously.</p> <p><b>Result:</b> The M251 programmable logic controller connection details appear:</p>  <p>A secure connection has now been established between LinkManager and the device.</p> <p><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).</p>

## Remotely Programming the M251 Programmable Logic Controller

Step	Action
1	<p>Right-click the SoMachine <b>Gateway Tray Application</b> icon  in the Windows system tray 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:</p>  <p>This ensures that SoMachine is configured to scan all IP addresses for incoming communications. Click <b>OK</b>.</p>
2	<p>Right-click on the <b>Gateway Tray Application</b> icon  in the Windows system tray again, and choose <b>Restart Gateway</b>.</p> <p><b>NOTE:</b> This step is important, as it establishes the connection between LinkManager and the remote HMIGTO appliance.</p>
3	<p>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 SoMachine online help if necessary.</p>

Step	Action
4	<p>In Logic Builder, go to the <b>Devices</b> tab on the left and double-click on the <b>Ethernet_1 (Ethernet Network)</b> node to display the Ethernet properties of the logic controller:</p> 
5	<p>Enter the <b>IP Address</b> and the <b>Subnet Mask</b> of the M251 programmable logic controller located on the work site.</p> <p><b>NOTE:</b> Verify that the values match those you entered when creating the agent (<a href="#">see page 26</a>).</p>
6	<p>In the <b>Gateway Address</b> field, enter the IP address of the HMIGTO appliance that is connected to the M251 programmable logic controller.</p>
7	<p>In the <b>Applications Tree</b> tab, create a new programmable object unit (POU):</p> <ol style="list-style-type: none"> <li>1. Right-click on <b>Application (MyController: TM251MESE)</b> and choose <b>Add Object → POU</b></li> <li>2. In the <b>Implementation language</b> list, choose <b>Instruction List (IL)</b>, then click <b>Add</b>.</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:</li> </ol> <pre data-bbox="330 1409 727 1458">%MW10 := %MW10 - 1; %MW11 := WSTRING_TO_WORD("51");</pre>

Step	Action
8	<p>In the <b>Devices Tree</b> tab on the left, double-click <b>Application (MyController: TM251MESE)</b>. At the bottom of the <b>Controller Selection</b> tab on the right, select <b>IP Address</b> in the <b>Connection Mode</b> list, and enter the IP address of the M251 logic controller:</p>  <p>The screenshot shows a software window with a toolbar at the top. Below the toolbar, there are several tabs: 'Energy Management', 'Name', 'Device Template', 'Controller', 'HMI &amp; IPC', and 'Devices &amp; Modules'. The 'Controller' tab is active, and within it, the 'Connection Mode' dropdown is set to 'IP Address'. The 'IP Address' field contains the value '192.168.1.50'. A red box highlights the 'Connection Mode' dropdown and the 'IP Address' field. Below this, there is a 'Watch 1' table with columns for 'Expression', 'Type', 'Value', 'Prepared value', 'Address', and 'Comment'. At the bottom of the window, there is a status bar with 'Last build: 0 0', 'Precompile: 0', and 'Current user: (nobody)'.</p>
9	<p>Click the <b>Login</b> button  on the toolbar, or choose <b>Online → Login</b>.</p>
10	<p>Click <b>Yes</b> on the window that appears to log in to the logic controller.</p>
11	<p>Click <b>OK</b> to transfer the new POU from the LinkManager laptop computer to the logic controller on the work site.</p>
12	<p>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!</p>



---

# Glossary



## A

### **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**

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

### **domain token**

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

## G

### **GateManager**

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

## H

### **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**

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.

### **subdomain**

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

## T

### **TLS**

Transport Layer Security