



## Industrial VPN Router USER MANUAL

This manual covers the StrideLinx platform available from 2017 through 2021.

For details covering the StrideLinx Cloud 2.0 platform available after April 2021, please [click here](#) to link to that manual.

The StrideLinx Cloud 2.0 manual includes details describing the [Activation Code](#) model of Data Logging, Cloud Notify and other add-on features.

For information on the migration wizard from the original platform to StrideLinx Cloud 2.0, [click here](#).





## ⚡ WARNING ⚡

Thank you for purchasing automation equipment from AutomationDirect.com<sup>®</sup>, doing business as, AutomationDirect. We want your new automation equipment to operate safely. Anyone who installs or uses this equipment should read this publication (and any other relevant publications) before installing or operating the equipment.

To minimize the risk of potential safety problems, you should follow all applicable local and national codes that regulate the installation and operation of your equipment. These codes vary from area to area and usually change with time. It is your responsibility to determine which codes should be followed, and to verify that the equipment, installation, and operation is in compliance with the latest revision of these codes.

At a minimum, you should follow all applicable sections of the National Fire Code, National Electrical Code, and the codes of the National Electrical Manufacturer's Association (NEMA). There may be local regulatory or government offices that can also help determine which codes and standards are necessary for safe installation and operation.

Equipment damage or serious injury to personnel can result from the failure to follow all applicable codes and standards. We do not guarantee the products described in this publication are suitable for your particular application, nor do we assume any responsibility for your product design, installation, or operation.

Our products are not fault-tolerant and are not designed, manufactured or intended for use or resale as on-line control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of the product could lead directly to death, personal injury, or severe physical or environmental damage ("High Risk Activities"). AutomationDirect specifically disclaims any expressed or implied warranty of fitness for High Risk Activities.

For additional warranty and safety information, see the Terms and Conditions section of our catalog. If you have any questions concerning the installation or operation of this equipment, or if you need additional information, please call us at 770-844-4200.

This publication is based on information that was available at the time it was published. At AutomationDirect we constantly strive to improve our products and services, so we reserve the right to make changes to the products and/or publications at any time without notice and without any obligation. This publication may also discuss features that may not be available in certain revisions of the product.

## Trademarks

This publication may contain references to products produced and/or offered by other companies. The product and company names may be trademarked and are the sole property of their respective owners. AutomationDirect disclaims any proprietary interest in the marks and names of others.

Copyright 2017, AutomationDirect.com<sup>®</sup> Incorporated  
All Rights Reserved

No part of this manual shall be copied, reproduced, or transmitted in any way without the prior, written consent of AutomationDirect.com<sup>®</sup> Incorporated. AutomationDirect retains the exclusive rights to all information included in this document.

## ⚡ ADVERTENCIA ⚡

Gracias por comprar equipo de automatización de **AutomationDirect.com**<sup>®</sup>. Deseamos que su nuevo equipo de automatización opere de manera segura. Cualquier persona que instale o use este equipo debe leer esta publicación (y cualquier otra publicación pertinente) antes de instalar u operar el equipo.

Para reducir al mínimo el riesgo debido a problemas de seguridad, debe seguir todos los códigos de seguridad locales o nacionales aplicables que regulan la instalación y operación de su equipo. Estos códigos varían de área en área y usualmente cambian con el tiempo. Es su responsabilidad determinar cuales códigos deben ser seguidos y verificar que el equipo, instalación y operación estén en cumplimiento con la revisión mas reciente de estos códigos.

Como mínimo, debe seguir las secciones aplicables del Código Nacional de Incendio, Código Nacional Eléctrico, y los códigos de (NEMA) la Asociación Nacional de Fabricantes Eléctricos de USA. Puede haber oficinas de normas locales o del gobierno que pueden ayudar a determinar cuales códigos y normas son necesarios para una instalación y operación segura.

Si no se siguen todos los códigos y normas aplicables, puede resultar en daños al equipo o lesiones serias a personas. No garantizamos los productos descritos en esta publicación para ser adecuados para su aplicación en particular, ni asumimos ninguna responsabilidad por el diseño de su producto, la instalación u operación.

Nuestros productos no son tolerantes a fallas y no han sido diseñados, fabricados o intencionados para uso o reventa como equipo de control en línea en ambientes peligrosos que requieren una ejecución sin fallas, tales como operación en instalaciones nucleares, sistemas de navegación aérea, o de comunicación, control de tráfico aéreo, máquinas de soporte de vida o sistemas de armamentos en las cuales la falla del producto puede resultar directamente en muerte, heridas personales, o daños físicos o ambientales severos (“Actividades de Alto Riesgo”). **AutomationDirect.com** específicamente rechaza cualquier garantía ya sea expresada o implicada para actividades de alto riesgo.

Para información adicional acerca de garantía e información de seguridad, vea la sección de Términos y Condiciones. Si tiene alguna pregunta sobre instalación u operación de este equipo, o si necesita información adicional, por favor llámenos al número 770-844-4200 en Estados Unidos.

Esta publicación está basada en la información disponible al momento de la publicación. En **AutomationDirect.com** nos esforzamos constantemente para mejorar nuestros productos y servicios, así que nos reservamos el derecho de hacer cambios al producto y/o a las publicaciones en cualquier momento sin notificación y sin ninguna obligación. Esta publicación también puede discutir características que no estén disponibles en ciertas revisiones del producto.

## Marcas Registradas

Esta publicación puede contener referencias a productos producidos y/u ofrecidos por otras compañías. Los nombres de las compañías y productos pueden tener marcas registradas y son propiedad única de sus respectivos dueños. **Automationdirect.com**, renuncia cualquier interés propietario en las marcas y nombres de otros.

**PROPIEDAD LITERARIA 2017, AUTOMATIONDIRECT.COM<sup>®</sup> INCORPORATED**  
Todos los derechos reservados

No se permite copiar, reproducir, o transmitir de ninguna forma ninguna parte de este manual sin previo consentimiento por escrito de **AutomationDirect.com**<sup>®</sup> Incorporated. **AutomationDirect.com** retiene los derechos exclusivos a toda la información incluida en este documento. Los usuarios de este equipo pueden copiar este documento solamente para instalar, configurar y mantener el equipo correspondiente. También las instituciones de enseñanza pueden usar este manual para propósitos educativos.



## ⚡ AVERTISSEMENT ⚡

Nous vous remercions d'avoir acheté l'équipement d'automatisation de **AutomationDirect.com**<sup>®</sup>, en faisant des affaires comme, **AutomationDirect**. Nous tenons à ce que votre nouvel équipement d'automatisation fonctionne en toute sécurité. Toute personne qui installe ou utilise cet équipement doit lire la présente publication (et toutes les autres publications pertinentes) avant de l'installer ou de l'utiliser.

Afin de réduire au minimum le risque d'éventuels problèmes de sécurité, vous devez respecter tous les codes locaux et nationaux applicables régissant l'installation et le fonctionnement de votre équipement. Ces codes diffèrent d'une région à l'autre et, habituellement, évoluent au fil du temps. Il vous incombe de déterminer les codes à respecter et de vous assurer que l'équipement, l'installation et le fonctionnement sont conformes aux exigences de la version la plus récente de ces codes.

Vous devez, à tout le moins, respecter toutes les sections applicables du Code national de prévention des incendies, du Code national de l'électricité et des codes de la National Electrical Manufacturer's Association (NEMA). Des organismes de réglementation ou des services gouvernementaux locaux peuvent également vous aider à déterminer les codes ainsi que les normes à respecter pour assurer une installation et un fonctionnement sûrs.

L'omission de respecter la totalité des codes et des normes applicables peut entraîner des dommages à l'équipement ou causer de graves blessures au personnel. Nous ne garantissons pas que les produits décrits dans cette publication conviennent à votre application particulière et nous n'assumons aucune responsabilité à l'égard de la conception, de l'installation ou du fonctionnement de votre produit.

Nos produits ne sont pas insensibles aux défaillances et ne sont ni conçus ni fabriqués pour l'utilisation ou la revente en tant qu'équipement de commande en ligne dans des environnements dangereux nécessitant une sécurité absolue, par exemple, l'exploitation d'installations nucléaires, les systèmes de navigation aérienne ou de communication, le contrôle de la circulation aérienne, les équipements de survie ou les systèmes d'armes, pour lesquels la défaillance du produit peut provoquer la mort, des blessures corporelles ou de graves dommages matériels ou environnementaux («activités à risque élevé»). La société **AutomationDirect** nie toute garantie expresse ou implicite d'aptitude à l'emploi en ce qui a trait aux activités à risque élevé.

Pour des renseignements additionnels touchant la garantie et la sécurité, veuillez consulter la section Modalités et conditions de notre documentation. Si vous avez des questions au sujet de l'installation ou du fonctionnement de cet équipement, ou encore si vous avez besoin de renseignements supplémentaires, n'hésitez pas à nous téléphoner au 770-844-4200.

Cette publication s'appuie sur l'information qui était disponible au moment de la publication. À la société **AutomationDirect**, nous nous efforçons constamment d'améliorer nos produits et services. C'est pourquoi nous nous réservons le droit d'apporter des modifications aux produits ou aux publications en tout temps, sans préavis ni quelque obligation que ce soit. La présente publication peut aussi porter sur des caractéristiques susceptibles de ne pas être offertes dans certaines versions révisées du produit.

## Marques de commerce

La présente publication peut contenir des références à des produits fabriqués ou offerts par d'autres entreprises. Les désignations des produits et des entreprises peuvent être des marques de commerce et appartiennent exclusivement à leurs propriétaires respectifs. **AutomationDirect** nie tout intérêt dans les autres marques et désignations.

**Copyright 2017, AutomationDirect.com<sup>®</sup> Incorporated**  
Tous droits réservés

Nulle partie de ce manuel ne doit être copiée, reproduite ou transmise de quelque façon que ce soit sans le consentement préalable écrit de la société **AutomationDirect.com<sup>®</sup> Incorporated**. **AutomationDirect** conserve les droits exclusifs à l'égard de tous les renseignements contenus dans le présent document.





---

# Industrial VPN Routers USER MANUAL



**Please include the Manual Number and the Manual Issue, both shown below, when communicating with Technical Support regarding this publication.**

**Manual Number:** SE-SLVPN-USER-M  
**Issue:** 1st Edition, Revision S  
**Issue Date:** 04/21

Publication History		
Issue	Date	Description of Changes
1st Edition	11/17	Original Issue
Revision A	12/17	Minor updates and clarifications
Revision B	04/18	Rebranded to StrideLinx
Revision C	05/18	New platform features, updates and clarifications
Revision D	09/18	Added Cloud Notify, other minor updates and clarifications
Revision E	10/18	Added WAN redundancy, other minor updates and clarifications
Revision F	11/18	Minor updates and clarifications
Revision G	05/19	Added Micro800 support, BACnet support, Push notifications, Log on trigger, clarified subscription services and WAN redundancy.
Revision H	06/19	Added VPN connections on mobile devices.
Revision I	07/19	Updated cellular bands
Revision J	10/19	Added note to remove USB stick prior to factory reset.
Revision K	12/19	Clarification of Factor setting in data tags, other minor updates and corrections
Revision L	03/20	Added SE-SL3001 and SE-SL3011-4GG routers
Revision M	08/20	Added description of timestamp localization for alarm notifications.
Revision N	09/20	Changed "passcode" to "password" in 2FA section to match GUI.
Revision O	10/20	Added details on router ports, protocols, and server connections
Revision P	01/21	Clarified antenna connections.
Revision Q	01/21	Added Appendix K covering MELSEC support. Renumbered existing appendices.
Revision R	03/21	Clarified WiFi SSID character restrictions in Troubleshooting.
Revision S	04/21	Added notice about StrideLinx Cloud update and new manual.





# TABLE OF CONTENTS

---

## Chapter 1: Hardware

<b>Introduction</b> .....	<b>1-3</b>
The Purpose of This User's Manual .....	1-3
Technical Support.....	1-3
<b>Conventions Used</b> .....	<b>1-3</b>
<b>Product Overview StrideLinx Industrial VPN Router</b> .....	<b>1-4</b>
Product Family .....	1-4
What's in the Box? .....	1-4
Hardware Overview.....	1-5
Specifications .....	1-6
Dimensions .....	1-8
Compatible Accessories.....	1-8
<b>Installation</b> .....	<b>1-9</b>
Installation and Removal Procedures .....	1-9
Wiring.....	1-10
<b>Operation</b> .....	<b>1-12</b>
LED Status Indicators.....	1-12
Reset to Factory Default .....	1-13
<b>SIM Card Registration</b> .....	<b>1-14</b>
AT&T SIM Card Registration.....	1-14
T-Mobile SIM Card Registration.....	1-16
<b>StrideLinx Router Connectivity Requirements for Local IT</b> .....	<b>1-17</b>
How does the StrideLinx router connect? (ports, protocols & servers) .....	1-17
How to grant the StrideLinx router access? .....	1-17
Servers & domains .....	1-18
Ports & protocols .....	1-18
MAC or IP Address Filtering.....	1-18
<b>Agency Approvals</b> .....	<b>1-19</b>

## Chapter 2: StrideLinx Platform

<b>Overview</b> .....	<b>2-4</b>
Terms of Use .....	2-4
Data Fair Use Policy .....	2-4
<b>Getting started</b> .....	<b>2-5</b>
Create a User Account.....	2-5
Login.....	2-5
Choose Company.....	2-5
<b>User Interface</b> .....	<b>2-6</b>
<b>Registering Your Device</b> .....	<b>2-6</b>
Login.....	2-7
Generate a Configuration File.....	2-7
Register Your StrideLinx Router.....	2-11
Activate Your StrideLinx Router .....	2-12
Edit Router Info and Set Location .....	2-12
Save/Load Config Files for Router Transfer .....	2-13
<b>Configure LAN as WiFi Access Point (Hotspot)</b> .....	<b>2-14</b>
<b>Configure Redundant WAN Access</b> .....	<b>2-15</b>
<b>Installing VPN Client Software</b> .....	<b>2-19</b>
Download Installer .....	2-19
Run Setup .....	2-19
Run VPN Client .....	2-19
Confirm Windows TAP Ethernet Driver Installed .....	2-19
Reconnect to StrideLinx Platform .....	2-19
Support.....	2-19
<b>Connect to Your Router by VPN</b> .....	<b>2-20</b>
Regarding VPN Connections .....	2-20
Device Status.....	2-21
<b>Connect to Devices Behind the StrideLinx Router</b> .....	<b>2-22</b>
HTTP/VNC/Data Logging Services and Shortcuts .....	2-22
<b>Using StrideLinx on Your Mobile Device</b> .....	<b>2-25</b>
iOS Client.....	2-25
Android Client.....	2-26
Access via Web.....	2-26

**Reducing Router Bandwidth** ..... 2-27

**Organization: Companies, Device Categories & User Groups**..... 2-28

    Overview..... 2-28

    Companies..... 2-28

    Device Categories..... 2-28

    User Groups ..... 2-30

**Access and Permissions** ..... 2-31

**Two-factor Authentication** ..... 2-32

    Setting Up Two-factor Authentication ..... 2-32

    Backup Codes ..... 2-35

    Logging In ..... 2-35

    Disabling Two-factor Authentication..... 2-36

    User Access Token ..... 2-36

**Transfer a Device** ..... 2-36

    To Assign a Device Key..... 2-37

**Chapter 3: Controller Connection Examples**

**Video Examples**..... 3-3

**CLICK PLC Connection via Cellular Router SE-SL3011-4G** ..... 3-4

    Before You Begin..... 3-4

    Setup ..... 3-4

**BRX PLC Connection via WiFi Router SE-SL3011-WF** ..... 3-7

    Before You Begin..... 3-7

    Setup ..... 3-7

**C-more® HMI Connection via Wired Router SE-SL3011** ..... 3-10

    Before You Begin..... 3-10

    Setup ..... 3-10

**Chapter 4: Data Logging**

**Cloud Data Logging** ..... 4-3

    Why Cloud Data Logging? ..... 4-3

    How Does the Cloud Data Logger Work?..... 4-3

    Configure Cloud Data Logging On Your Device..... 4-3

    Set Up Datalogging Subscription ..... 4-4

    Set Up Data Sources for a Device Using Modbus Protocol..... 4-5

## Table of Contents

---

<b>Cloud Logging Web App</b> .....	<b>4-11</b>
Dashboards .....	4-11
Download Logged Data .....	4-17
Status Info .....	4-18
Tag Configuration .....	4-19
Trigger Configuration .....	4-21
Test Utility .....	4-23
<b>Pausing, Deactivating, &amp; Terminating Your Datalogging Subscription</b> .....	<b>4-24</b>
Activate / Deactivate Datalogging .....	4-24
Pause / Resume Datalogging.....	4-24
Terminating a Subscription.....	4-24

## Chapter 5: Cloud Notify

<b>Cloud Notify</b> .....	<b>5-3</b>
Why Cloud Notify?.....	5-3
How Does the Cloud Notify License Work? .....	5-3
Configure Cloud Notify On Your Device.....	5-3
Set Up Cloud Notify License.....	5-4
Set Up Data Sources For Alarm Notifications .....	5-5
Router Conditions for Alarm Notifications .....	5-10
Formatting the Alarm Notification Email .....	5-11
<b>Cloud Notify Web App</b> .....	<b>5-12</b>
Main Screen .....	5-12
Adding Alarms.....	5-13
Export Alarm Configurations .....	5-14
Managing Alarm Recipients.....	5-15
What Happens When an Alarm is Triggered?.....	5-16
Message Center.....	5-17
Configuring Your Mobile Device to Receive Push Notifications.....	5-19

## Appendix A: Accessories & Add-on Subscriptions

<b>Antennas</b> .....	<b>A-3</b>
4G LTE Antennas (for P/N SE-SL3011-4G and SE-SL3011-4GG).....	A-3
WiFi Antennas, IEEE 802.11 b/g/n 2.4 GHz (for P/N SE-SL3011-WF) .....	A-4
<b>Add-on Subscriptions &amp; Licenses</b> .....	<b>A-5</b>



Service Level Agreement ..... A-6  
 Cloud Logging ..... A-6  
 Cloud Notify ..... A-7  
 Data Top-up ..... A-7  
 Premium Branding ..... A-7

**Appendix B: Troubleshooting**

**Troubleshooting Overview ..... B-3**  
**My StrideLinx Router Doesn't Come Online ..... B-3**  
 Internet Connection ..... B-3  
 Connectivity ..... B-3  
 Network Settings ..... B-3  
 Configuration ..... B-3  
 StrideLinx Router Log File ..... B-5  
**I Can't Connect to the StrideLinx Router ..... B-5**  
 VPN Client ..... B-5  
 TAP Adapter ..... B-5  
 VPN Client Log File ..... B-6  
**I Can't Connect to My Device(s) Behind the StrideLinx Router ..... B-6**  
 VPN Connection ..... B-6  
 IP Range ..... B-6  
 Default Gateway ..... B-6  
 Timeout Setting ..... B-6  
 Programming Software Does Not Allow Multiple Programming Connections ..... B-6  
 I Don't Know How to Configure My Device ..... B-6  
 I Am Unable to Configure My Device ..... B-7  
 Check Your Settings ..... B-7  
 I Still Can't Connect to My Device ..... B-7  
**I Can't Connect to My HTTP/VNC Server ..... B-7**  
 Accessibility ..... B-7  
 HTTP/VNC Server ..... B-7  
 Password ..... B-7  
 StrideLinx Router Settings ..... B-7  
 Specific Service and Server Settings ..... B-8  
**Wireless Connectivity ..... B-8**

## Appendix C: Safety and Security Considerations

Security Considerations for Control Systems Networks.....	C-3
Safety Guidelines.....	C-4
Plan for Safety .....	C-4
Digital Input Safety Lockout .....	C-5

## Appendix D: Data Logging Address Notation – AutomationDirect Devices

StrideLinx Modbus to AutomationDirect PLC Address Maps .....	D-3
CLICK PLCs .....	D-3
DirectLogic PLCs .....	D-6
Do-more PLCs .....	D-8
Productivity Series PLCs.....	D-10

## Appendix E: StrideLinx Network Security

Introduction: Intended Audience.....	E-3
Solution explained.....	E-3
StrideLinx Router.....	E-3
StrideLinx Platform.....	E-3
StrideLinx Client.....	E-3
Overview.....	E-3
Controls Network Security .....	E-5
Remote access.....	E-5
Local access.....	E-5
Company Network Security .....	E-6
Connectivity.....	E-6
Remote access.....	E-7
Local access.....	E-7
StrideLinx Platform Security.....	E-7
Servers .....	E-7
StrideLinx platform.....	E-7
VPN Client Security .....	E-8

## Appendix F: Capabilities of Connected AutomationDirect Devices

Network Topology.....	F-3
Network with StrideLinx VPN router using wired or WiFi network connectivity .....	F-4

Network with StrideLinX VPN router using 4G cellular network connectivity ..... F-5

Device Capabilities..... F-6

**Appendix G: Set Up Data Source Using Siemens S7 protocol**

Set up data source for a device using Siemens S7 protocol ..... G-3

**Appendix H: Set Up Data Source Using OPC UA protocol**

Set up data source for a device using OPC UA protocol ..... H-3

**Appendix I: Set Up Data Source Using EtherNet/IP protocol**

Set up data source for a device using EtherNet/IP protocol ..... I-3

Error Messages ..... I-13

**Appendix J: Set Up Data Source Using BACnet/IP protocol**

Set up data source for a device using BACnet/IP protocol..... J-3

**Appendix K: Set Up Data Source Using MELSEC protocol**

Set up data source for a device using MELSEC protocol ..... K-3

PLC settings ..... K-4

Select a communication protocol..... K-9

**Add variables (new, import) ..... K-11**

Manually add new variables ..... K-11

Import variables from a file (or device)..... K-12

**Test variables ..... K-13**

**Connecting StrideLinX to Q series Ethernet module QJ71E71-100 with MELSEC Protocol..... K-14**

**Appendix L: Custom Branding**

Custom branding.....L-3

Basic branding .....L-3

Premium branding .....L-6

**Appendix M: Terms of Use**

IXON B.V. Terms of Use..... M-3

Annex I ..... M-11

# HARDWARE

---



# CHAPTER 1

## In this Chapter...

<b>Introduction</b> .....	1-3
The Purpose of This User's Manual .....	1-3
Technical Support .....	1-3
<b>Conventions Used</b> .....	1-3
<b>Product Overview StrideLinx Industrial VPN Router</b> .....	1-4
Product Family .....	1-4
What's in the Box? .....	1-4
Hardware Overview .....	1-5
Specifications .....	1-6
Dimensions .....	1-8
Compatible Accessories .....	1-8
<b>Installation</b> .....	1-9
Installation and Removal Procedures .....	1-9
Wiring .....	1-10
<b>Operation</b> .....	1-12
LED Status Indicators .....	1-12
Reset to Factory Default .....	1-13
<b>SIM Card Registration</b> .....	1-14
AT&T SIM Card Registration .....	1-14
T-Mobile SIM Card Registration .....	1-16
<b>StrideLinx Router Connectivity Requirements for Local IT</b> .....	1-17
How does the StrideLinx router connect? (ports, protocols & servers) .....	1-17
How to grant the StrideLinx router access? .....	1-17
Servers & domains .....	1-18
Ports & protocols .....	1-18
MAC or IP Address Filtering .....	1-18
<b>Agency Approvals</b> .....	1-19

This manual covers the StrideLinx platform available from 2017 through 2021.

For details covering the StrideLinx Cloud 2.0 platform available after April 2021, please [click here](#) to link to that manual.

The StrideLinx Cloud 2.0 manual includes details describing the [Activation Code](#) model of Data Logging, Cloud Notify and other add-on features.

For information on the migration wizard from the original platform to StrideLinx Cloud 2.0, [click here](#).

## Introduction

### The Purpose of This User's Manual

Thank you for purchasing our StrideLinx™ series Industrial VPN Router. This manual describes AutomationDirect.com's StrideLinx industrial VPN routers, their specifications and included components, and provides you with important information for installation, connectivity and setup.

### Technical Support

We strive to make our manuals the best in the industry. We rely on your feedback to let us know if we are reaching our goal. If you cannot find the solution to your particular application, or, if for any reason you need technical assistance, please call us at:

770-844-4200

Our technical support group will work with you to answer your questions. They are available Monday through Friday from 9:00 a.m. to 6:00 p.m. Eastern Time. We also encourage you to visit our web site where you can find technical and non-technical information about our products and our company.

<https://www.AutomationDirect.com>

If you have a comment, question or suggestion about any of our products, services, or manuals, please let us know.

## Conventions Used



---

*When you see the “notepad” icon in the left-hand margin, the paragraph to its immediate right will be a special note. The word **NOTE**: in boldface will mark the beginning of the text.*

---



---

*When you see the “exclamation mark” icon in the left-hand margin, the paragraph to its immediate right will be a warning or a caution. This information could prevent injury, loss of property, or even death (in extreme cases). The words **WARNING** or **CAUTION**: in boldface will mark the beginning of the text.*

---

## Product Overview StrideLinx Industrial VPN Router

1

The StrideLinx series of industrial VPN routers is the hardware component for the StrideLinx platform. The StrideLinx router makes it convenient to remotely connect to your equipment, while the built-in firewall keeps your equipment safe from outside threats.

Beyond remote access, StrideLinx also enables you to customize your platform to send alarms & notifications, log data locally or to the cloud, and brand the StrideLinx platform as your own. These options are provided as add-on services so you get exactly what you need at the best possible price. Datalogging, alarms, and notifications options are not supported by model SE-SL3001.

Configuration is as easy as inserting a USB memory stick, which contains your configuration file, into the StrideLinx router's USB port. Generate the configuration file from the Tools menu in your StrideLinx platform account.

### Product Family

StrideLinx routers are available in variants with the following communication modes:

StrideLinx Industrial VPN Router Models			
Part #	Ethernet	WiFi	4G LTE
SE-SL3001 <sup>1</sup>	✓		
SE-SL3011			
SE-SL3011-WF	✓	✓	
SE-SL3011-4G (AT&T) <sup>2,3</sup>	✓		
SE-SL3011-4GG (global) <sup>3</sup>			✓

1. SE-SL3001 does not support data logging or notifications.
2. Certified for AT&T; compatible with T-Mobile and other carriers using the same cellular bands.
3. Refer to specifications tables for supported cellular bands.

### What's in the Box?

In the package you will find the following contents:

- StrideLinx router
- USB stick used for configuration
- Female 4-pin plug-in connector with screw connection, model Weidmuller BL 5.08/04/180 SN BK BX or equivalent
- Product insert

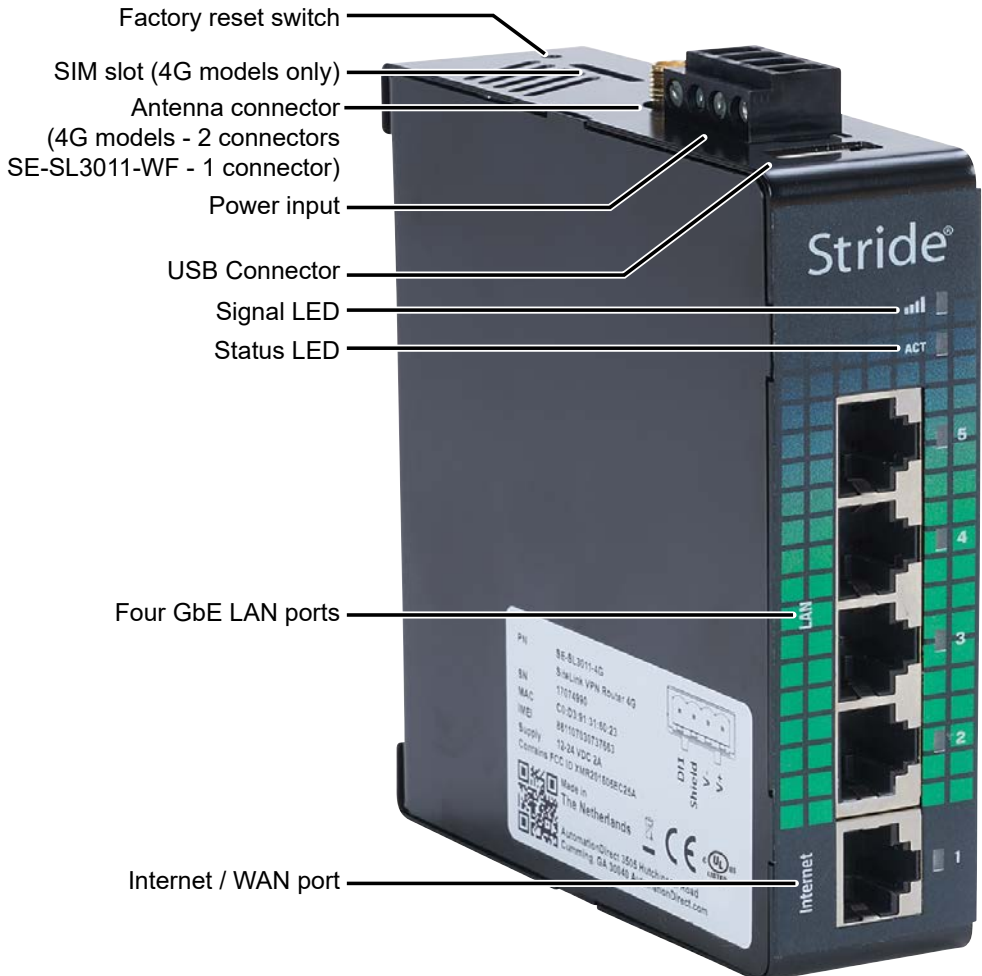
External antennas are required for WiFi and 4G models. Antennas sold separately.

Models that support 4G connections require a SIM card and cellular service (provided by others). Detailed instructions are shown in section "[SIM Card Registration](#)" on page 1-14.



## Hardware Overview

The StrideLinx router is created with performance and a multitude of hardware capabilities in mind.



**SAFETY NOTICE:** The StrideLinx VPN router allows the user to connect to remote industrial controls equipment from Ethernet, Wi-Fi, or cellular network connections. The remote user may fully operate and monitor the local control system and affect the function and control of the application just as the local operator controls it. Proper Control, Security and Safety Procedures should be considered and implemented when utilizing the remote access feature. See Appendix C and Appendix E.



## Specifications

1

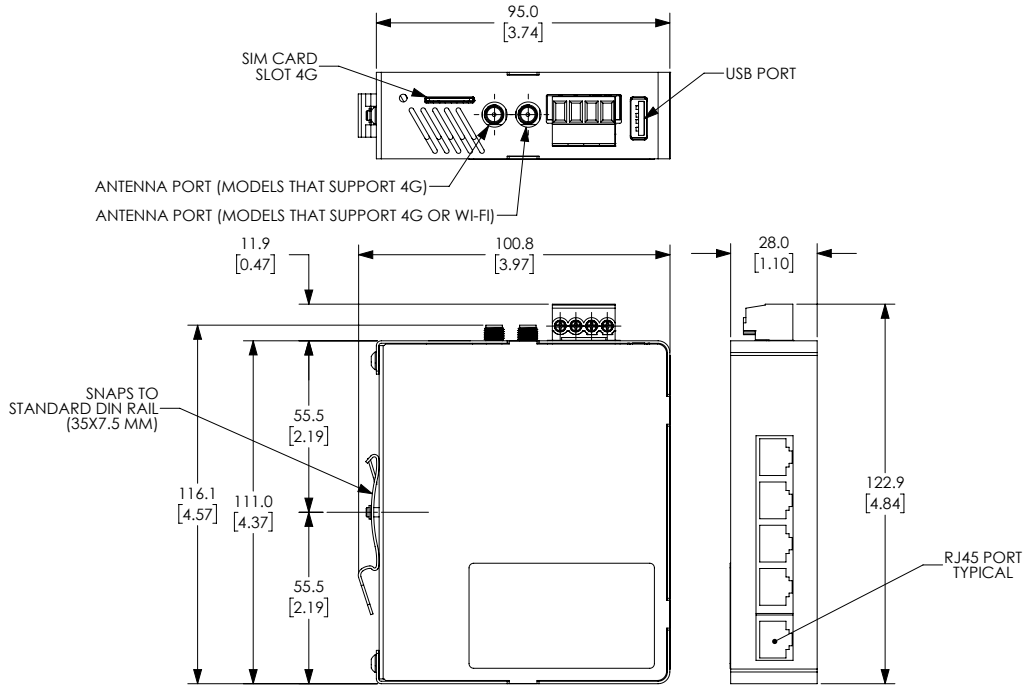
General Specifications	
USB	USB 2.0 (for configuration only)
Processor	MIPS 800 MHz
Digital Input for Local Control	Yes
Operating temperature	-20°C to +65°C [-4°F to +149°F]
Storage temperature	-20°C to +65°C [-4°F to +149°F]
Relative humidity	10 to 95% non-condensing
Operating altitude	Maximum 2000m
Storage altitude	Maximum 3000m
Environmental Air	For use in Pollution Degree 2 Environment. No corrosive gases permitted.
EMI	FCC CFR47 Part 15, EN55022/CISPR22, Class B
EMS	IEC61000-4-2 (ESD): ± 8kV (contact), ± 15kV (air) IEC61000-4-3 (RS): 10V/m (80MHz ~ 2GHz) IEC61000-4-4 (EFT): Power Port ± 4kV; Data Port: ± 2kV IEC61000-4-5 (Surge): Power Port: ± 2kV/DM, ± 4kV/CM; Data Port ± 2kV IEC61000-4-6 (CS): 10V (150kHz ~ 80MHz)
RoHS and WEEE	RoHS (Pb free) and WEEE compliant
Packaging and Protection	Metal case, IP20
Mounting	DIN rail
Certification	CE, cULus, RoHS, REACH, AT&T (SE-SL3011-4G), FCC
Warranty	2 years
Agency Approvals	UL/cUL 60950-1, CE

Power Details	
Input Voltage	Class 2 LPS Power Supply 12-24 VDC
Maximum Input Power	10W
Maximum Input Current	2A
Internal Voltage Protection	29V max
Reverse Polarity Protection	Yes
Isolation	1.5 kV

Ethernet Interface	
Ethernet ports	Five GbE (4x LAN, 1x WAN)
Port Type	Shielded RJ45
Auto-Crossover	Yes, allows you to use straight-through or crossover wired cables
Auto-Sensing Operation	Yes, full and half duplex
Auto-Negotiating Speed	Yes
Flow Control	Automatic
Operating Mode	Store and forward wire speed switching, non-blocking
Devices Supported	All IEEE 802.3 compliant devices are supported
Protection	Built-in 1.5 kV magnetic isolation
Cable Requirements	Twisted pair (Cat5e or better) (shielded recommended)
Max. Cable Distance	100 meters
4G LTE Specifications for SE-SL3011-4G Only	
Cellular Bands (AT&T)	LTE-FDD: B2, B4, B12 WCDMA: B2, B4, B5
Speed	LTE-FDD: Max. 150 Mbps (DL)/Max. 50 Mbps (UL) WCDMA: Max. 384 kbps (DL)/Max. 384 kbps (UL)
Antenna Connection	Two (2) SMA plugs (male)
Antenna Connector Torque	3–5 lb-in [0.3–0.6 N·m]
SIM size	Standard SIM (2FF)
FCC ID	XMR201605EC25A
4G LTE Specifications for SE-SL3011-4GG Only	
Cellular Bands (Global)	LTE FDD: B1,B2,B3,B4,B5,B7,B8,B12,B13,B18,B19,B20,B25,B26,B28 LTE TDD: B38,B39,B40,B41 WCDMA: B1,B2,B4,B5,B6,B8,B19 GSM: B2,B3,B5,B8 GPRS: B2,B3,B5,B8
Speed	LTE-FDD: Max. 150 Mbps (DL)/Max. 50 Mbps (UL) LTE-TDD: Max. 130 Mbps (DL)/Max. 30 Mbps (UL) WCDMA: Max. 384 kbps (DL)/Max. 384 kbps (UL) GSM (EDGE): Max. 296 kbps (DL)/Max. 236.8 kbps (UL) GPRS: Max 107 kbps (DL)/Max. 85.6 kbps (UL)
Antenna Connection	Two (2) SMA plugs (male)
Antenna Connector Torque	3–5 lb-in [0.3–0.6 N·m]
SIM size	Standard SIM (2FF)
FCC ID	XMR201903EG25G
WiFi Specifications (P/N SE-SL3011-WF Only)	
WiFi IEEE 802.11 Version	b/g/n
WiFi Modes	Station (Client) Mode and Access Point
Speed	72 Mbps
Antenna Connection	RP-SMA plug (male)
Antenna Connector Torque	3–5 lb-in [0.3–0.6 N·m]
FCC ID	XPYLILYW1

## Dimensions

units: mm [in]



StrideLinx router dimensions



**NOTE:** Maintain 25mm [1 inch] clearance around device.

## Compatible Accessories

SE-SL3011-4G, SE-SL3011-4GG and SE-SL3011-WF require antennas, purchased separately. The routers that support 4G have two standard SMA screw antenna connectors for 4G LTE antennas and the SE-SL3011-WF router contains an RP-SMA screw antenna connector for a 2.4 GHz WiFi antenna.



**NOTE:** Two antennas will provide best performance, including improved and more predictable throughput and improved resistance to interference. If only one antenna is connected to a 4G router, it must be connected to the MAIN antenna connector, closer to the front of the router.

For compatible antennas, see Appendix A or visit [www.AutomationDirect.com](http://www.AutomationDirect.com).

# Installation

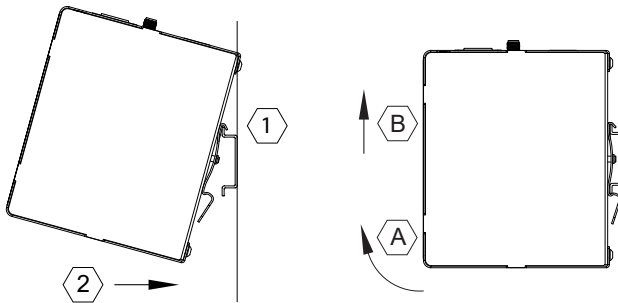
## Installation and Removal Procedures



**NOTE:** These devices are open-type and are meant to be installed in an enclosure which is only accessible with the use of a tool and suitable for the environment.

### *Installing and Removing from DIN rail*

The StrideLinx router can be easily installed on a standard DIN rail. (1) Hang the device on the rail and (2) push the unit down until you feel a click. To remove the unit, (A) pull/rotate the device up and (B) lift off the rail.



### *Installing the SIM Card (for SE-SL3011-4G and SE-SL3011-4GG)*

The SIM card slot uses a standard (size 2FF) SIM card.



**WARNING:** DO NOT insert or remove the SIM card when power is applied to the router.

To insert, push the SIM card into the slot until you feel a click; this is approximately 1mm inside the device. Release the card and the card will stay in the device. The end of the SIM card should be aligned with the outside of the enclosure.

To remove, push the SIM card firmly into the slot until you hear a click. Releasing will then cause the SIM card to partially eject, allowing you to easily take out the card.

## Guidelines for Installing the StrideLinx Router

When designing the layout of your system, always separate the devices that generate high voltage and high electrical noise from the low-voltage, logic-type devices such as the StrideLinx router. Also consider the heat-generating devices and locate the electronic-type devices in the cooler areas of your cabinet. Reducing the exposure to a high-temperature environment will extend the operating life of the StrideLinx router.

Consider also the routing of the wiring for the devices in the panel. Avoid placing low-voltage signal wires and communications cables in the same tray with AC power wiring and high-energy, rapidly-switched DC wiring.

The StrideLinx router is designed to be cooled using natural convection. For proper cooling, you must provide a clearance of at least 25 mm [1 inch] above and below the device. Also, allow at least 25 mm [1 inch] of depth between the front of the device and the inside of the enclosure.

## Wiring

### Wiring Guidelines



---

**WARNING:** To minimize the risk of potential safety problems, you should follow all applicable local and national codes that regulate the installation and operation of your equipment. These codes vary from area to area and it is your responsibility to determine which codes should be followed, and to verify that the equipment, installation, and operation are in compliance with the latest revision of these codes.

*Equipment damage or serious injury to personnel can result from the failure to follow all applicable codes and standards. We do not guarantee the products described in this publication are suitable for your particular application, nor do we assume any responsibility for your product design, installation, or operation.*

*If you have any questions concerning the installation or operation of this equipment, or if you need additional information, please call technical support at 1-800-633-0405 or 770-844-4200.*

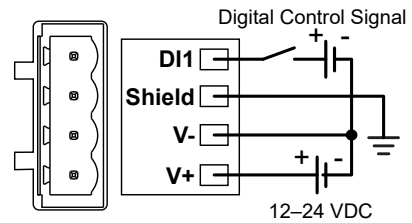
*This publication is based on information that was available at the time it was printed. At Automationdirect.com® we constantly strive to improve our products and services, so we reserve the right to make changes to the products and/or publications at any time without notice and without obligation. This publication may also discuss features that may not be available in certain revisions of the product.*

---

Proper grounding and wiring of all electrical equipment is important to help ensure the optimum operation of the StrideLinx router and to provide additional electrical noise protection for your application.

The StrideLinx router comes with a female 4-pin plug-in connector with screw connection (type: Weidmuller BL 5.08/04/180 SN BK BX).

Wiring Details	
Wire Size Range	18–12 AWG
Wire Strip Length	7mm [0.28 in]
Terminal Screw Torque	0.4 N·m [3.5 lb·in]
Max Wire Length	3m [9.84 ft]
Min Ground Conductor	16 AWG



### Power Supply

The StrideLinx router can be powered from the same DC source that is used to power your other devices. To maintain the UL listing, this must be a Limited Power Supply (LPS) or Class 2 power supply. A DC voltage in the range of 12 to 24 VDC needs to be applied between the V+ terminal and the V- terminal as shown above. A recommended DC power supply is AutomationDirect.com part number PSL-24-030.

### Digital Input (DI1)

The digital input may be configured to restrict remote access to the router when the input is in either an ON or OFF state. Instructions for enabling can be found in the “StrideLinx platform” chapter. The V- from the power supply is used as common ground.

This feature can provide an extra level of security or safety, by allowing remote connections only when certain conditions are met, such as when an operator is present or safety interlocks are engaged. The input can be wired directly through a switch, or a series of interlocks, or can be controlled via PLC for more complex control conditions.

A video providing an overview of using the StrideLinx router’s Digital Input as a part of your safety lockout procedures is accessible by clicking the thumbnail at the right, or by copying the following URL to your browser:

<https://www.AutomationDirect.com/VID-CM-0034>



Digital Input Specifications	
Type	Optocoupler
DI Voltage Range	0–29 VDC
DI OFF State Voltage Range	0–3 VDC
DI ON State Voltage Range	7–29 VDC
DI ON State Current Range	2–5 mA (typically)

### Shield

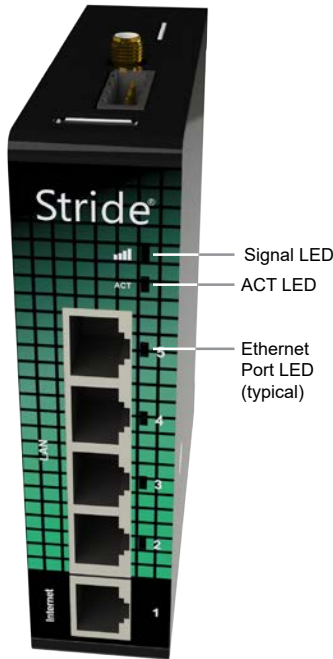
Connect the Shield pin of the StrideLinx router to the protective earth conductor (PE) with minimum 16 AWG copper wire.

## Operation

# 1

### LED Status Indicators

The StrideLinx router has two LEDs for router status, and one LED per Ethernet port.



Signal LED (SE-SL3011-4G, -4GG & -WF models)		
Color	Mode	Description
Red	Blinking continuously	No reception
Red	Blinking 2 pulses	SIM card invalid, PIN invalid or PUK required
Red	Constant	Low reception
Purple	Constant	Medium reception
Blue	Constant	Good reception
Blue	Blinking	Initializing

ACT LED		
Color	Mode	Description
Red	Constant	Booting or not registered
Red	Blinking 1 pulse	Waiting for internet access
Red	Blinking 3 pulses	LAN/WAN conflict <sup>1</sup>
Red	Blinking 4 pulses	The router was removed from the StrideLinx platform <sup>2</sup>
Red	Blinking 5 pulses	The router was already registered to the StrideLinx platform <sup>3</sup>
Blue	Blinking 1 pulse	Connecting to StrideLinx platform
Blue	Blinking 2 pulses	Setting up VPN connection
Blue	Constant	VPN connection active

*1. The network range on the LAN side is in conflict with the settings on the WAN side. The router cannot reliably access the internet because of this. Changing the LAN side IP range generally resolves the conflict.*

*2. If you want to access the device again, you will have to reconfigure it via a USB stick.*

*3. This means someone removed the router from the company after registration without performing a factory reset. Fix this by performing factory reset and configuring the router.*

Ethernet activity LEDs		
Color	Mode	Description
Blue	Constant	Link up
Blue	Blinking	Data activity

## Reset to Factory Default



---

**WARNING:** This action cannot be undone. You'll have to re-register your device on the StrideLinx platform and complete the configuration steps before connecting by VPN.

---

To reset the router:

1. If you want to save the router settings before you reset the router, use the “Save as Template” feature on the StrideLinx platform.
2. Remove the router from the Devices list.
3. Remove the USB flash drive from the router.



---

**NOTE:** Be sure to remove the USB stick before pressing the reset button to ensure a previous configuration file doesn't interfere with the reset to factory default.

---

4. Revert the router back to factory default settings by pressing and holding the reset button on top for 15 seconds until the ACT LED lights steady Red. Wait for the StrideLinx router to restart.
5. Create a configuration file.
6. Load the new configuration file into the router via a USB flash drive.

The router will now appear as a “new device” in your company.



# 1 SIM Card Registration

The routers that support 4G connections require SIM card and cell service intended for data applications. The specifications for each model that supports 4G include information on which bands and frequencies are supported.

AutomationDirect can only support AT&T connections, as described in the following section.

## AT&T SIM Card Registration



**NOTE:** AutomationDirect recommends that users purchase the AT&T M2M SIM cards intended for data applications like the StrideLinx router. The following section provides instruction on acquiring an AT&T M2M SIM card. AutomationDirect can only offer support for AT&T 4G connections using an AT&T M2M SIM card purchased at the link below.

To begin, open the AT&T marketplace web page at <https://marketplace.att.com/data-plans>. “IoT Data Plans” should be selected (1).

Select “View Details” under AT&T IoT Data Plans – LTE North America (2).

A screenshot of the AT&amp;T IoT Marketplace website. The page title is "IoT Solutions". On the left, there are filters: "SELECTED FILTERS" includes "IoT Data Plans" (marked with a red circle 1 and a clear button), and "IoT Solutions" includes "IoT Data Plans" (checked, marked with a red circle 1). The main content area shows three product cards for "AT&amp;T IoT Data Plans - LTE International", "AT&amp;T IoT Data Plans - LTE North America", and "AT&amp;T IoT Data Plans - LTE-M US". Each card features the AT&amp;T logo, a "NEW Featured Product" badge, and a price of "\$2.99". The "AT&amp;T IoT Data Plans - LTE North America" card has a red circle 2 over its "View Details" button. The top navigation bar includes the AT&amp;T logo, a hamburger menu, "IoT Marketplace", a shopping cart icon, and "Login".

Select Connectivity (data per device per 30 days) (3). Be sure to scroll down in the drop down window to see all choices – up to 10GB/device (4).

Select Number of SIM Cards (5).

Select Device “IXON – StrideLinX VPN Router 4G” (6).

Add to Cart & Checkout

Once you have your SIM cards you must log into your AT&T account and register the SIM cards – Go to Management – Register SIMs (7).

Find the SIM card ICCID on the card and name it, if desired (8). Click Register SIMs (9).

The SIM card is now ready to be installed into the StrideLinX router. Configuration of the 4G router to use the AT&T APN is covered in the “Registering Your Device” section of Chapter 2.

## T-Mobile SIM Card Registration

**1**

While AutomationDirect does not offer technical support for this setup, the StrideLinx 4G router can be used with a T-Mobile prepaid 4G data plan.

To do so, first visit a T-Mobile store and purchase an LTE data plan and SIM card for a hotspot device.

The T-Mobile SIM card must be activated by calling T-Mobile before use in the StrideLinx 4G router.

Once the SIM card has been activated, install it into the router as described earlier in this chapter.

Configuration of the 4G router to use the T-Mobile APN is covered in the “Registering Your Device” section of Chapter 2.

## StrideLinx Router Connectivity Requirements for Local IT

The StrideLinx VPN router allows the user to connect to remote industrial controls equipment from Ethernet, Wi-Fi, or cellular network connections. The remote user may fully operate and monitor the local control system and affect the function and control of the application just as the local operator controls it. Proper Control, Security and Safety Procedures should be considered and implemented when utilizing the remote access feature. See Appendix C for an overview of security and safety considerations, and see Appendix E for a more detailed look at StrideLinx network security.

### How does the StrideLinx router connect? (ports, protocols & servers)

The StrideLinx router uses outgoing ports to establish a secure connection to the StrideLinx Platform. This means there is no need to open any incoming ports in your firewall.

### How to grant the StrideLinx router access?

#### *Easy method: automatic updates*

You may create an **exception** in your firewall **for the domain name** and ports & protocols, mentioned below, to grant the StrideLinx router the access it needs.

With time, some servers may be removed or added to benefit the service. We try to keep these changes to a minimum.

**If we add a server**, we simply add a DNS record. Your firewall will re-check the domain once the TTL expires. Within an hour your firewall will be up-to-date and allow traffic to the new IP address.

Likewise, **if we remove a server**, we will remove its DNS record, and your firewall will block any traffic to this IP address.

#### *Alternative method: manual updates*

You can execute a **DNS lookup** (nslookup) request at the domain name mentioned below, to get an IP list of all servers currently required by the StrideLinx solution. You can then create exceptions to these IP addresses, in combination with the ports and protocols mentioned below, to grant the StrideLinx router the access it needs.

With time, some servers may be removed or added to benefit the service. We try to keep these changes to a minimum.

Please keep your firewall rules/exceptions up to date by periodically performing a DNS lookup and checking for changes to maintain optimal remote service accessibility.

## Servers & domains

The StrideLinx router connects to different servers: **REST API**, **MQTT**, and **OpenVPN servers**, which include the following domains:

- \*.ixon.cloud
- \*.ixon.net
- \*.ayayot.com (phonetic IIoT)

For your convenience, we provide a domain name that resolves to an always up-to-date IP list of all current servers:

- whitelist.ixon.cloud.

## Ports & protocols

Below is an overview of the ports and protocols that the StrideLinx router utilizes.

StrideLinx Router Ports and Protocols			
Direction	Port	Transport	Application
Outbound	443	TCP	HTTPS, MQTT/TLS, OpenVPN <sup>(1)</sup>
Outbound	8443 <sup>(2)</sup>	TCP	HTTPS
Outbound	53 <sup>(3)</sup>	TCP & UDP	DNS <sup>(3)</sup>

*1. The very first packet may be considered unencrypted as the OpenVPN handshake takes place prior to the TLS handshake. For this reason an exception may be required on firewall rules that block non-SSL traffic over SSL ports.*

*2. Only used when stealth mode is activated for connectivity via a censored internet connection (e.g. when located in China).*

*3. DNS requests are often handled by local DNS servers. In those cases the listed DNS port can be ignored.*

## MAC or IP Address Filtering

Your local network may be configured to only allow internet access to specific devices, based on the MAC address or IP address. The MAC address can be obtained from the label on the side of the StrideLinx router or in the Devices Info tab of your StrideLinx account. The IP address can be set to a static IP address. However, by default the IP address is set to be obtained automatically via DHCP.

## Agency Approvals

### Applicable European Directives

The StrideLinX router is in conformity with the provisions of the following European Directives.

Applicable European Directives	
<i>Directive</i>	<i>Description</i>
EMC Directive 2014/30/EU	Product safety
Radio Equipment Directive 2014/53/EU	Use of the radio spectrum
RoHS Directive 2011/65/EU including amendment 2015/863	Restriction of hazardous substances
REACH Directive	Regulation and registration of chemicals
WEEE Directive 2012/19	Waste of electronic equipment

### Applicable Safety Standards

The StrideLinX router was tested and passed the following standards.

Applicable Safety Standards	
<i>Standards</i>	<i>Description</i>
EN 55032	Electromagnetic Compatibility of Multimedia Equipment
EN 301 489-1	EMC Standard for Radio Equipment and Services, Part 1: Common technical requirements
EN 301 489-3	EMC Standard for Radio Equipment and Services, Part 3: Specific conditions for Short-Range Devices
EN 61000-4-2	Electrostatic discharge immunity test
EN 61000-4-3	Radiated, Radio-frequency, Electromagnetic Field Immunity Test 80-1000 MHz
EN 61000-4-4	Burst Immunity Test
EN 61000-4-5	Surge Immunity Test
EN 61000-4-6	Immunity to Conducted Disturbances, Induced by Radio-frequency Fields
IEC 60950-1 + Amendment 1 and Amendment 2	Information Technology Equipment Safety, Part 1: General Requirements - Edition 2
UL 60950-1	Information Technology Equipment Safety, Part 1: General Requirements - Edition 2
CSA C22.2 No. 60950-1-07 + Amendment 1 and Amendment 2	Information Technology Equipment Safety, Part 1: General Requirements - Edition 2

## FCC Compliance

The product described in this User Manual complies with Part 15 of the FCC Rules. The StrideLinx router is a class B Information Technology Equipment (ITE) device.

Operating is subject to the following conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.



---

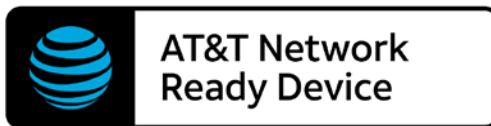
**WARNING for WiFi and 4G models: The antenna used with this transmitter must be installed with a separation distance of at least 20cm from all persons and must not be co-located or operated in conjunction with any other antennas or transmitters. Only an antenna tested with the wireless transmitter or a similar antenna with equal or lesser gain may be used.**

---

## Certifications

The StrideLinx router has been tested and certified for:

- CE certification
- FCC verification
- cULus listed (UL File #E495151)
- AT&T certification (SE-SL3011-4G)



Model SE-SL3011-4G Only

# STRIDELINX PLATFORM

---



## In this Chapter...

<b>Overview .....</b>	<b>2-4</b>
Terms of Use .....	2-4
Data Fair Use Policy .....	2-4
<b>Getting started .....</b>	<b>2-5</b>
Create a User Account.....	2-5
Login.....	2-5
Choose Company.....	2-5
<b>User Interface .....</b>	<b>2-6</b>
<b>Registering Your Device .....</b>	<b>2-6</b>
Login.....	2-7
Generate a Configuration File.....	2-7
Register Your StrideLinx Router .....	2-11
Activate Your StrideLinx Router .....	2-12
Edit Router Info and Set Location .....	2-12
Save/Load Config Files for Router Transfer .....	2-13
<b>Configure LAN as WiFi Access Point (Hotspot) .....</b>	<b>2-14</b>
<b>Configure Redundant WAN Access.....</b>	<b>2-15</b>
<b>Installing VPN Client Software.....</b>	<b>2-19</b>
Download Installer .....	2-19
Run Setup .....	2-19
Run VPN Client .....	2-19
Confirm Windows TAP Ethernet Driver Installed .....	2-19
Reconnect to StrideLinx Platform .....	2-19
Support.....	2-19
<b>Connect to Your Router by VPN.....</b>	<b>2-20</b>
Regarding VPN Connections .....	2-20
Device Status.....	2-21



<b>Connect to Devices Behind the StrideLinx Router .....</b>	<b>2-22</b>
HTTP/VNC/Data Logging Services and Shortcuts .....	2-22
<b>Using StrideLinx on Your Mobile Device .....</b>	<b>2-25</b>
iOS Client.....	2-25
Android Client.....	2-26
Access via Web.....	2-26
<b>Reducing Router Bandwidth .....</b>	<b>2-27</b>
<b>Organization: Companies, Device Categories &amp; User Groups.....</b>	<b>2-28</b>
Overview.....	2-28
Companies.....	2-28
Device Categories.....	2-28
User Groups .....	2-30
<b>Access and Permissions .....</b>	<b>2-31</b>
<b>Two-factor Authentication .....</b>	<b>2-32</b>
Setting Up Two-factor Authentication .....	2-32
Backup Codes .....	2-35
Logging In .....	2-35
Disabling Two-factor Authentication .....	2-36
User Access Token.....	2-36
<b>Transfer a Device .....</b>	<b>2-36</b>
To Assign a Device Key.....	2-37

This manual covers the StrideLinx platform available from 2017 through 2021.

For details covering the StrideLinx Cloud 2.0 platform available after April 2021, please [click here](#) to link to that manual.

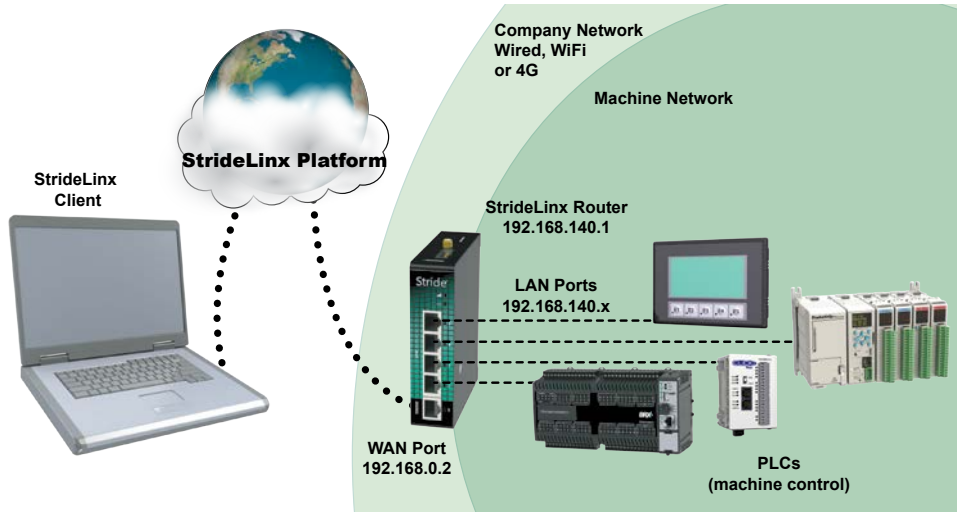
The StrideLinx Cloud 2.0 manual includes details describing the [Activation Code](#) model of Data Logging, Cloud Notify and other add-on features.

For information on the migration wizard from the original platform to StrideLinx Cloud 2.0, [click here](#).

## Overview

The StrideLinx Platform is a secure and powerful platform based on a worldwide network of servers. It is focused on delivering and enhancing innovative remote service.

The following example illustrates how a typical StrideLinx setup might be configured.



As shown in the example above the StrideLinx router will isolate a local machine network (e.g., 192.168.140.x range) from the corporate network (e.g., 192.168.0.x range). To prevent network routing problems you must make sure the StrideLinx router's IP address is in a different subnet than the company network.

### Terms of Use

The StrideLinx platform is powered by IXON, B.V., and use of the service requires acceptance of IXON's Terms of Use. A copy of the Terms of Use is included in Appendix M for your convenience.

### Data Fair Use Policy

A StrideLinx user may access, program and monitor any device on the local machine network by VPN. The intended use of the StrideLinx platform is secure remote access to industrial control equipment for remote service. A monthly allowance of 5GB data traffic per company account is included, and is sufficient in most cases to accomplish remote service.

When the platform is used for other purposes, the data traffic may exceed the 5GB allowance. The StrideLinx platform includes optional Data Top-up subscriptions to increase the monthly limit. See "[Add-on Subscriptions and Licenses](#)" in Appendix A for more details.

If the data traffic for a company reaches the monthly limit, further data traffic will be throttled to 50kbit/sec. This is adequate to access and program a PLC.

Although data usage is affected by the number of users accessing the platform, we expect the most significant data usage to be from an IP camera connected on the platform.

Any Cloud Logging subscription data does not count toward the monthly data traffic allowance, and is not subject to throttling.

## Getting started

These steps will get you up and running with the StrideLinx Platform (<https://www.StrideLinx.com>).

### 1. Create a User Account

To start using the StrideLinx Platform, you will need a user account. There are two ways of setting up an account.

- You can create a user account and a new company by filling out the registration form at <https://www.StrideLinx.com>.
- You can join an existing company by being invited by a user already in that company.

In both cases you will receive a confirmation e-mail. Complete your account registration by following the verification link inside.



---

**NOTE:** No e-mail? Be sure to check your spam folder if you haven't received an e-mail in your inbox.

---

### 2. Login

Once you have a user account, it's very easy. Just go to the login page and log in with your e-mail address and password combination.



---

**NOTE:** Forgot your password? You can use the recovery form to request a password recovery e-mail. We will then send you instructions for setting up a new password.

---

### 3. Choose Company

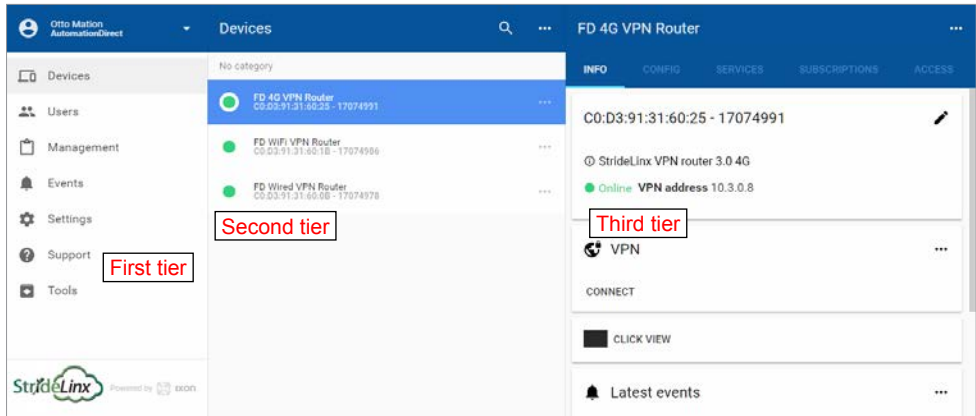
If you have just created your user account, it is probably linked with only one company. In that case your company is automatically chosen and this step will not show up.

However, if your user account is linked to more than one company, you must choose the company you want to use. During login you will see a list of companies you are linked to.

That's it! You are now logged in. The next section provides a brief overview of the StrideLinx platform user interface, and the subsequent section walks you through registering your router on the StrideLinx Platform.

## User Interface

For convenience we have named the areas of the platform as shown in the following graphic. When viewed on a device with a screen width less than 1280 pixels, the first-tier menu is hidden by default and accessible by clicking on the menu icon (☰) in the upper left corner.



## Registering Your Device

These steps will guide you through the process of registering your StrideLinx router to the StrideLinx Platform. Videos to walk you through the process of setting up each type of router (wired, WiFi, and 4G LTE) are accessible by clicking the thumbnails below, or copying the URL to your browser. All routers can be configured as a wired router by using the Ethernet WAN port for connectivity.

*Complete Setup of Wired Router (any model)*

<https://www.AutomationDirect.com/VID-CM-0020>



*Complete Setup of Wireless Router (SE-SL3011-WF)*

<https://www.AutomationDirect.com/VID-CM-0021>



*Complete Setup of 4G LTE Router  
(SE-SL3011-4G or SE-SL3011-4GG)*

<https://www.AutomationDirect.com/VID-CM-0022>



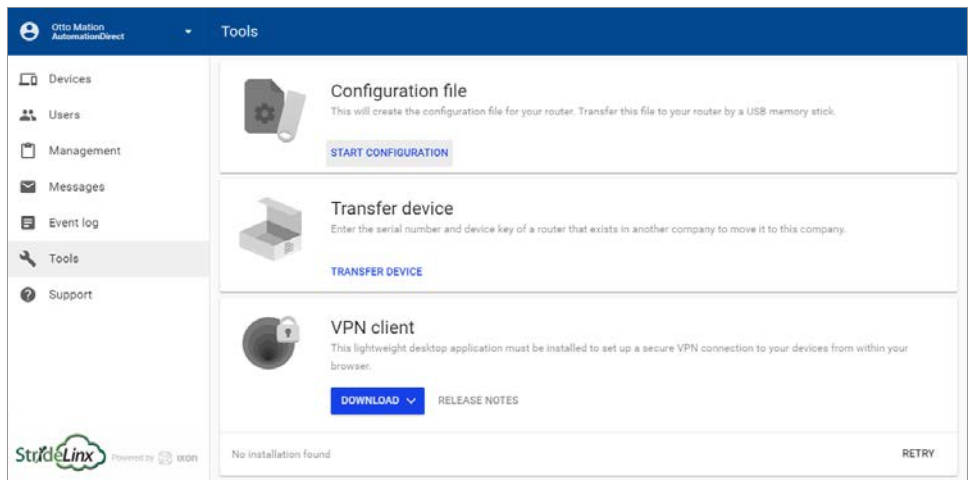
## 1. Login

Go to the login page at [www.StrideLinx.com](http://www.StrideLinx.com) and log in with your e-mail address and password. A user account is required. If you don't already have one, you need to create a user account before you can proceed.

The device you log in from (your PC or laptop) to configure your router must have an available USB port.

## 2. Generate a Configuration File

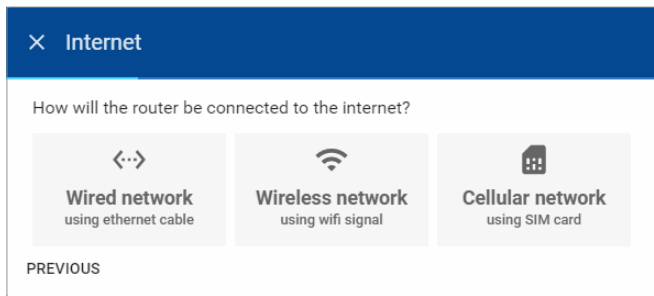
Note that a few details regarding the machine network internet connection will be needed to complete configuration of a new router. Please read through this section and make sure the relevant information is available before beginning a new configuration. Once you are successfully logged in and ready to proceed, choose “Tools” from the navigation menu. Click on the START CONFIGURATION button to open the configuration file wizard.



A dialog box will confirm that the new router will be registered to the company to which you are currently logged in. Click NEXT to continue.

## Configure the Internet Settings

Select the method by which your router will connect to the internet (i.e., Wired, Wireless, or Cellular). After the router is configured and activated, a second connection method can be added for WAN redundancy. The WAN redundancy feature is intended to take advantage of two independent internet sources and will not failover automatically when the two connection types access the internet by the same modem/company router.



**NOTE:** All models can be configured to connect to the internet via wired connection. On the 4G models and WiFi model, set up your preferred primary internet connection method now; a fallback connection method for WAN redundancy can be configured through the StrideLinx platform after the initial setup is complete. If a WiFi model is configured to use a wired WAN connection, its WiFi connection may be configured as a wireless access point.

### Configure a Wired WAN Network

The router will be configured by default to have its IP address and DNS server assigned via DHCP, and to disable the Digital Input control of the VPN. Usually these settings are appropriate and you may click NEXT and skip ahead to the “[Configure LAN IP Address](#)” subsection. Unlike the network settings for the devices connected behind this router, the router’s network settings usually function best when configured for DHCP. If your network conditions require static network settings on the WAN port, though, click SHOW MORE.

#### Manually Configure WAN IP Address

After clicking SHOW MORE on the WAN setup dialog box, click “Use the following IP address.”

Enter the desired static IP address for the WAN (internet) side of the router (IPv4 only).

The network mask defaults to 255.255.255.0. If this needs to change, click the dropdown arrow to the right of the network mask and select the correct mask from the list.

Enter the default gateway the router should use to access the internet.



**CAUTION:** The LAN IP address and WAN IP address need to be on separate subnets. The address range 10.3.x.x is reserved for communications between the server and the router. Addresses in this range may not be configured by the user.



**NOTE:** Configuring a static IP address will also require that you set a custom DNS server.

### *Manually Configure DNS Server*

After clicking SHOW MORE on the WAN setup dialog box, click “Add a custom DNS server”. This radio button will already be selected if a static IP address has been entered.

Enter the IP address of the preferred DNS server (IPv4 only).

### *Configure Digital Input for Wired Connection*

The Digital Input feature allows you to enable or disable the VPN connection based upon an external digital signal supplied to the router. Electrical details for the Digital Input can be found in the “Wiring” subsection of the “Hardware” chapter of this manual.

Disabling the VPN connection disables remote programming, but allows remote monitoring including data logging.

By default, the Digital Input is disabled. When creating the INITIAL configuration file, the user may choose to enable this feature. To use this feature, click the dropdown arrow to the right of the Digital Input field and select an option from the dropdown box. Available options are:

- Disabled (Digital Input state is ignored. VPN router functions normally.)
- Disable VPN connection when input is high
- Disable VPN connection when input is low

### *Configure Proxy Server*

If your network requires the router to connect to the internet through a proxy server, please click the switch to enable this feature, and enter configuration information as follows.

Enter the IP address of the proxy server (IPv4 only), and enter the proxy server port number.

If authentication is required for the proxy server, click the dropdown arrow to the right of the Authentication field and select “Basic authentication” then enter a username and password for the proxy server.

### *Configure a WiFi WAN Connection*

After selecting “Wireless network” as the method to connect to the internet, enter the name (SSID) of the wireless network and enter the WiFi password if needed, then click NEXT.

The wireless router has its internet-facing IP address and DNS server assigned via DHCP.

The Digital Input control of the VPN is disabled by default. When creating the INITIAL configuration file, the user may choose to enable this feature. If you wish to enable the Digital Input, click SHOW MORE in the upper right corner of the dialog box. The available options are:

- Disabled (Digital Input state is ignored. VPN router functions normally.)
- Disable VPN connection when input is high
- Disable VPN connection when input is low



### *Configure a 4G WAN Network*

After selecting “Cellular network” as the method to connect to the internet, enter the Access Point Name (APN) associated with the cellular network to which the SIM card is configured. The APN should be obtained from the cellular provider. Standard APNs for AT&T and T-Mobile are as follows:

- AT&T: m2m.com.attz
- T-Mobile: fast.t-mobile.com

Enter the PIN code for the SIM card if applicable, then click NEXT.

The mobile router has its internet-facing IP address and DNS server assigned by the mobile network.

The Digital Input control of the VPN is disabled by default. When creating the INITIAL configuration file, the user may choose to enable this feature. If you wish to enable the Digital Input, click SHOW MORE in the upper right corner of the dialog box. The available options are:

- Disabled (Digital Input state is ignored. VPN router functions normally.)
- Disable VPN connection when input is high
- Disable VPN connection when input is low

### *Configure LAN IP Address*

The VPN router creates a separate subnet on the LAN side. At this stage in the router setup, only the router’s IP address (IPv4 only) on the LAN subnet needs to be entered. After the router is connected to the StrideLinx platform, DHCP server, network mask, and internet access settings can be configured through the platform.



---

**NOTE:** *The LAN IP address and WAN IP address need to be on separate subnets.*

---

After entering the LAN IP address, click NEXT to continue.

### Download the Configuration File

Click the DOWNLOAD button to download the configuration file (ixrouter.conf) to your computer. Save the file to the root directory of a USB memory stick after the download is complete.

We include a USB memory stick with your StrideLinx router, but you can use any USB stick you prefer.

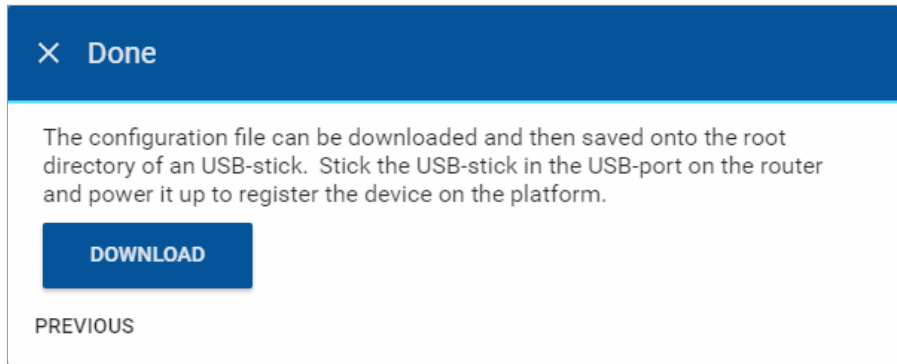
Click the X beside DONE to close the dialog box after the download is complete.




---

**NOTE:** Make sure that the file is named `ixrouter.conf` and that it is placed in the root directory of the memory stick.

---




---

**Problems downloading the configuration file?** If nothing happens when you click on the download button, make sure you are using a supported browser and that your browser does not automatically block download prompts. If the browser directly opens the configuration file in a new page, you can save the configuration file by pressing `ctrl + s` and saving the page source as `ixrouter.conf`.

---

### 3. Register Your StrideLinx Router

To register your router on the StrideLinx Platform, you must plug the USB stick with the configuration file into your StrideLinx router.

Next, make sure the router has the necessary hardware connected to allow internet access as specified in the configuration file (i.e., WAN port ethernet cable, WiFi antenna, or mobile network antennas and SIM card).

Finally, boot up the router by attaching the power cable.

The LED on the router will start blinking now, indicating that it's running the registration procedure. This usually takes somewhere between 20-30 seconds to complete.



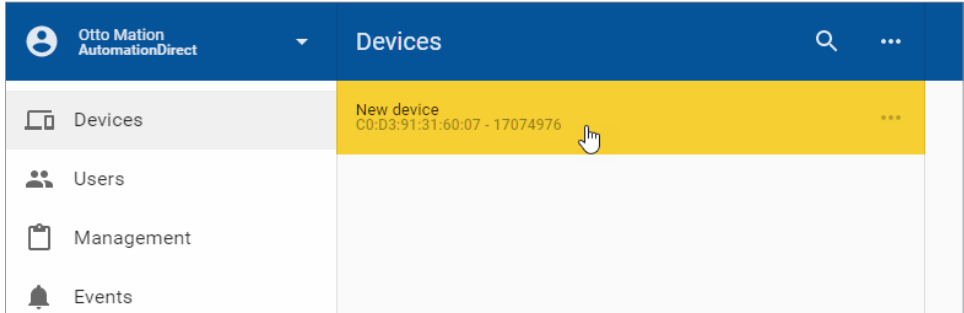

---

**NOTE:** It's best practice to remove the config file from the USB after the router has been registered so that on power up the router boots from the current configuration rather than the initial configuration.

---

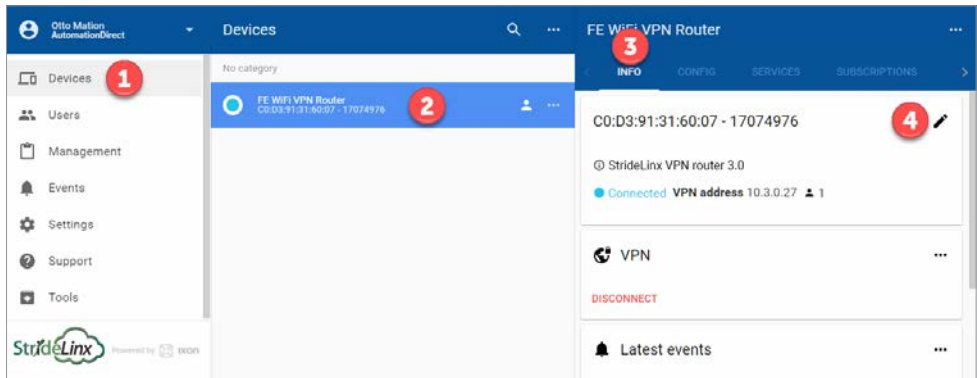
### 4. Activate Your StrideLinX Router

Once your router is registered it will show up as a new device on the devices page. Before you can start using the device, it must first be activated. You can trigger the activation form by clicking on the device's status icon in the list view. From then, activating the router is as simple as giving it a name and clicking the ACTIVATE button.



### Edit Router Info and Set Location

The name, description, category, and physical location of the activated router can now be set by (1) clicking Devices, (2) selecting the desired router, (3) clicking the INFO tab, and (4) clicking the Edit (pencil) icon to the right of the device identifier in the third-tier panel.

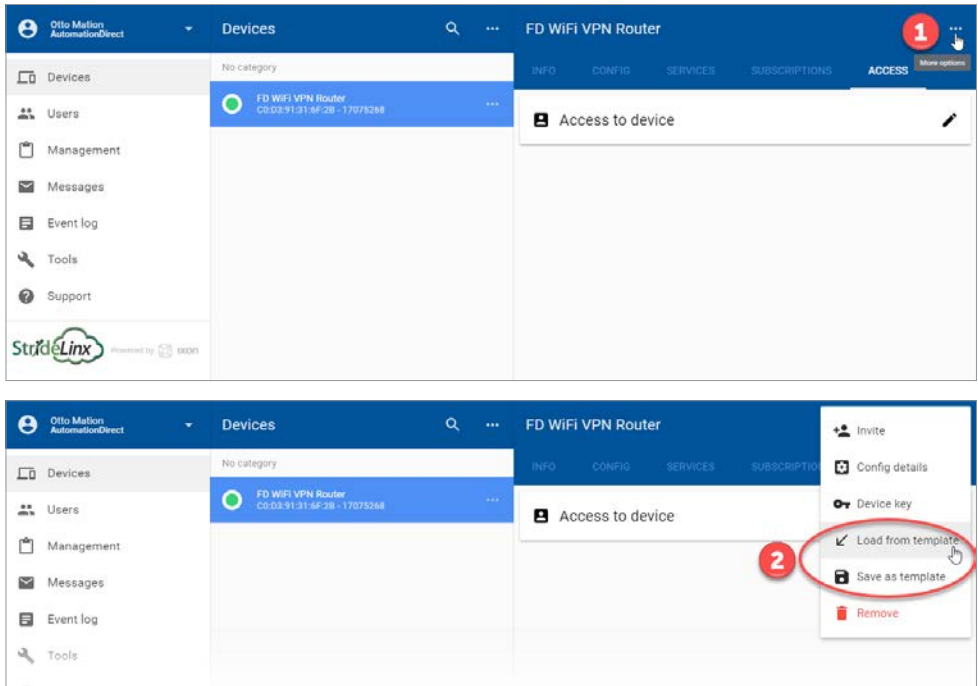


The device name and description may be edited for user convenience in identifying the router. The device category is discussed later in this chapter.

If a physical location is entered, the StrideLinX platform will use that location to determine the closest StrideLinX platform server to connect to the router. If no location is entered, the platform server will be selected based on the WAN IP address of the router.

## Save/Load Config Files for Router Transfer

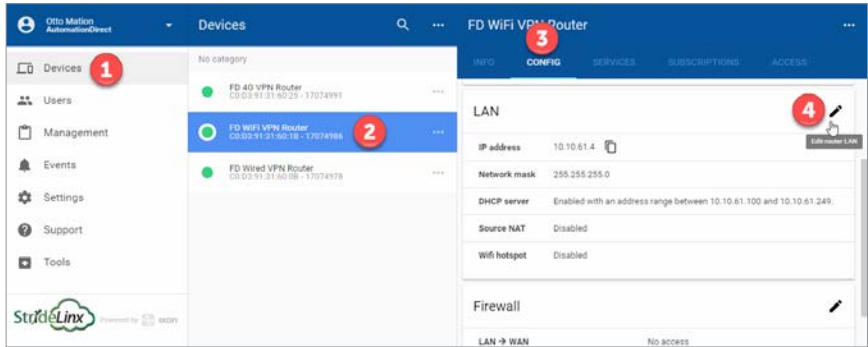
If you want to connect another StrideLinx router with the same router configuration settings, device connections and user permissions, you can do so by using the “Save as Template” and “Load from Template” features accessed from the ellipsis at the top of the device pane:



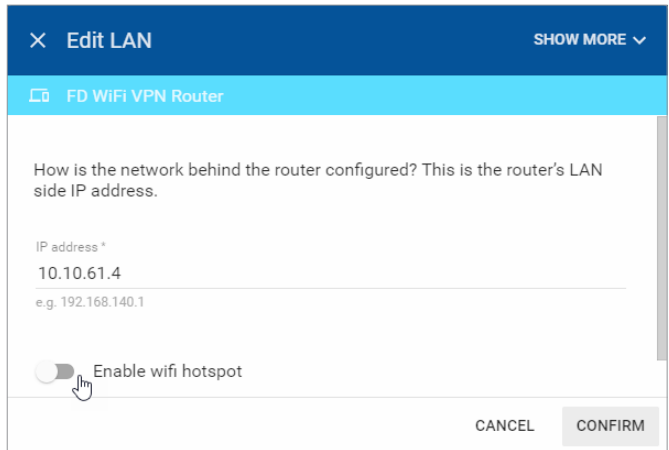
## Configure LAN as WiFi Access Point (Hotspot)

A WiFi StrideLinX router can be configured as a WiFi hotspot (access point) after it has been initially set up and connected to a StrideLinX Platform account. To begin, select Devices from the first-tier menu (1), select the router to be configured in the second-tier menu (2), select the CONFIG tab in the third-tier menu (3), and then click the pencil icon to the right of “LAN” (4).

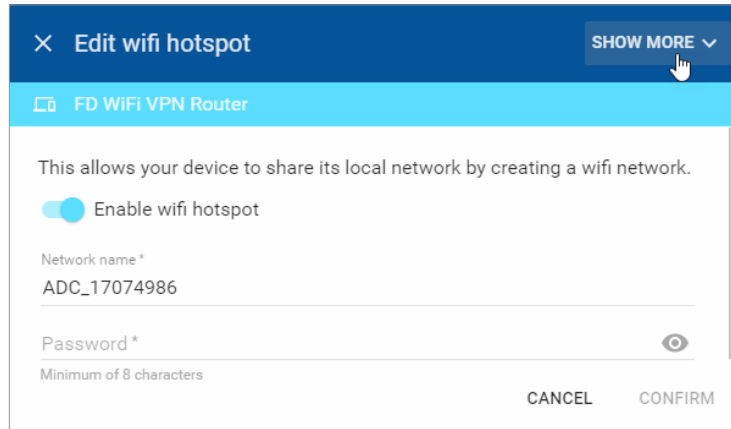
2



Click “Enable WiFi hotspot” to enable the feature and begin setting the hotspot configuration.



Enter the Network name (SSID) and password for the WiFi hotspot. If you wish to specify a WiFi channel for the hotspot, click SHOW MORE and then enter the channel number (1–11).

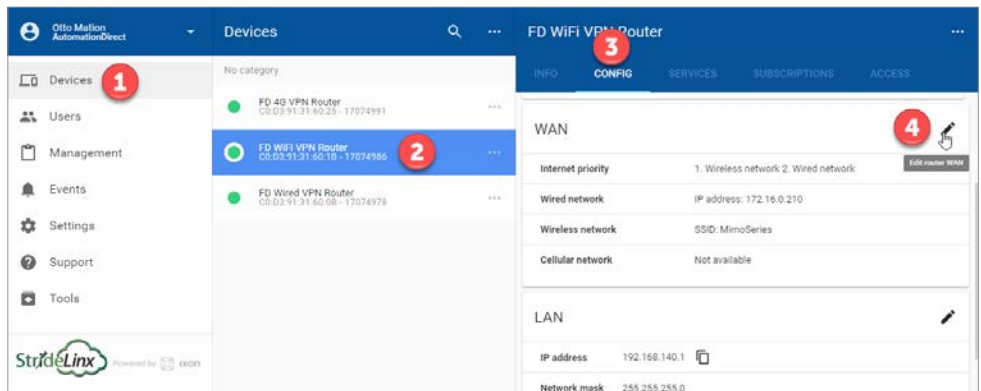


The WiFi hotspot is now enabled. To disable the hotspot, begin the same procedure and deselect “Enable WiFi hotspot” then click CONFIRM.

## Configure Redundant WAN Access

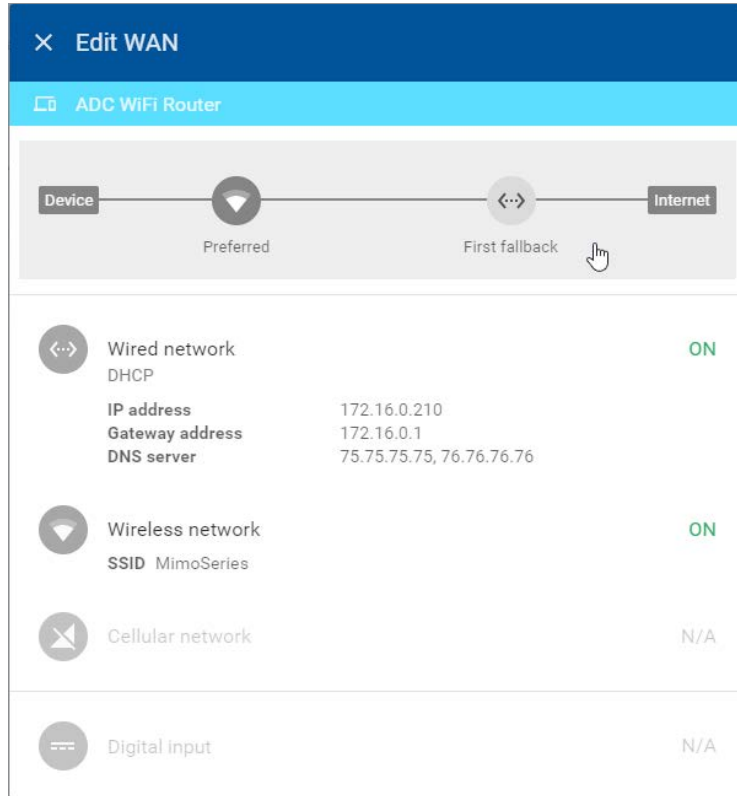
WiFi or cellular router models with internet access available via both the wireless network connection (WiFi or cellular) AND the wired WAN port may be configured with a primary internet (WAN) source and a secondary internet (WAN) source. When the router is configured with both sources, the secondary internet source will become active when the primary source becomes unavailable. This feature is intended to take advantage of two independent internet sources and will not failover automatically for WiFi routers when the two connection types access the internet by the same modem/company router.

To configure redundant WAN access, (1) click Devices, (2) select the router to be configured, (3) select the Config tab, then (4) click the Edit (pencil) icon in the WAN section of the display.

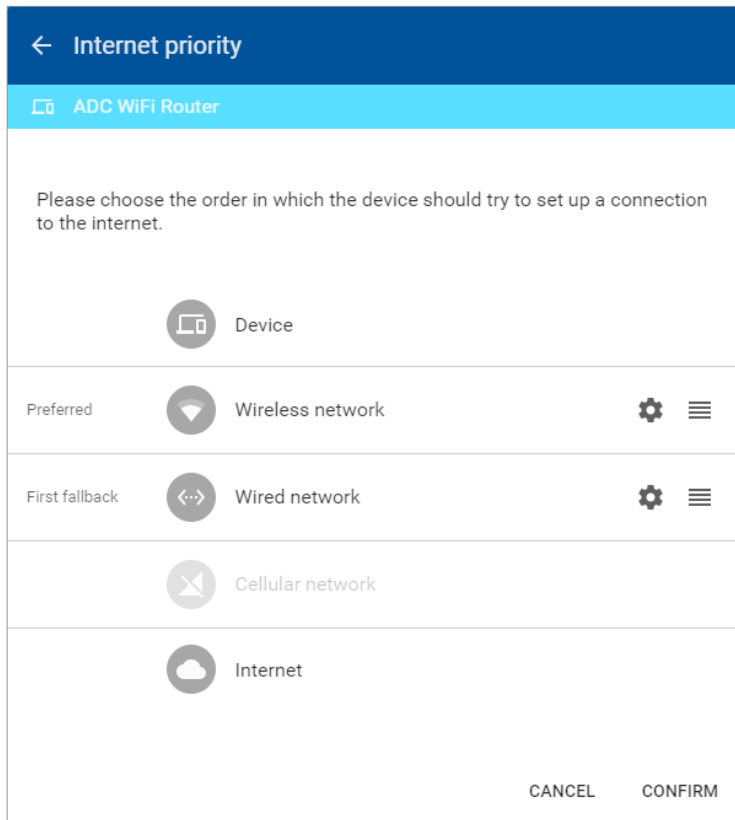


The Edit WAN screen shows a summary of the current WAN configuration. Settings for each available WAN connection can be adjusted by clicking on the connection information in the lower section of the display. (Note that Digital Input can only be set up during initial configuration.)

2



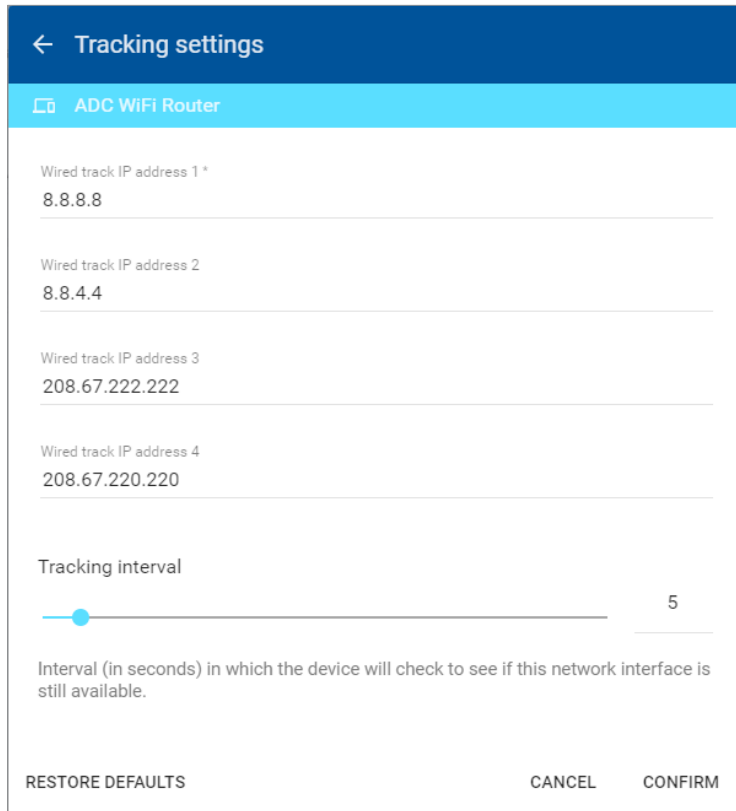
The diagram at the top of the screen indicates the order of preference of each configured WAN connection from the device to the internet. Click on this diagram to open the Internet Priority screen.



On the Internet Priority screen, the order of preference can be adjusted by clicking the icon on the far right (☰) of one of the WAN entries and dragging it upward (higher priority) or downward (lower priority).

Click on the setup (gear) icon to open the Tracking Settings dialog and set up how each WAN connection tracks its connectivity.





← Tracking settings

ADC WiFi Router

Wired track IP address 1 \*

8.8.8.8

Wired track IP address 2

8.8.4.4

Wired track IP address 3

208.67.222.222

Wired track IP address 4

208.67.220.220

Tracking interval

5

Interval (in seconds) in which the device will check to see if this network interface is still available.

RESTORE DEFAULTS CANCEL CONFIRM

The router will periodically check up to four public IP addresses to determine that the preferred WAN connection is available. The default IP addresses to track are public DNS servers. Any public IP address may be entered, but should be an address that is always on and will respond to ping requests.

The default tracking interval is 5 seconds. The interval can be adjusted between 1 and 60 seconds.

Finally, the new configuration must be pushed to the router. While pushing the new configuration, the router will disconnect for up to one minute.

## Installing VPN Client Software

Before you can set up a VPN connection to your router, you must install the VPN client software.

For PC connections, the VPN client is a light-weight application that runs in the background on your PC. It creates a virtual Ethernet port on your PC and handles all communication between your PC, the StrideLinx Platform and your browser.

2

### 1. Download Installer

You can find the download for the latest VPN client version for Windows, MacOS and Linux on the Tools page of the StrideLinx Platform website. The instructions here will focus on the Windows installer.

### 2. Run Setup

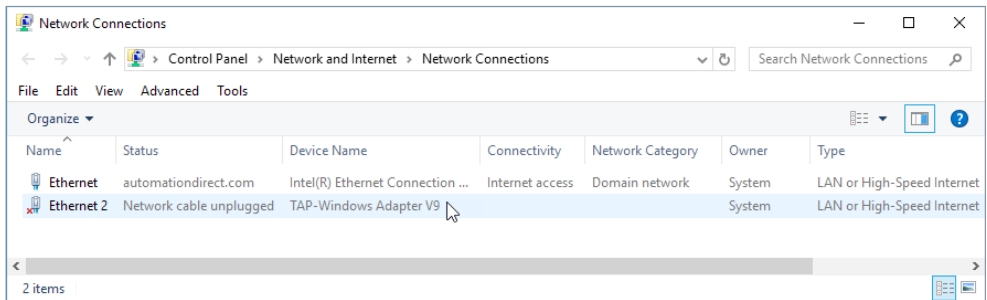
Double-click the Installer file (VPN\_Client-x64\_en-US.msi) to open the installation wizard and follow the installation steps.

### 3. Run VPN Client

The VPN client will launch automatically after the installation has completed.

### 4. Confirm Windows TAP Ethernet Driver Installed

Go to your PC network connections and confirm the Windows TAP Ethernet driver is present. If not, you will need to install a Windows TAP Ethernet driver before proceeding.



### 5. Reconnect to StrideLinx Platform

After the VPN client has been installed, refresh the [www.StrideLinx.com](http://www.StrideLinx.com) page in your web browser.

## Support

To help us support you, we sometimes need the log files from the VPN client. On a Windows PC you can find these at “C:\ProgramData\StrideLinx\VPN Client\Logs”. Usually, the most recent log file is the most relevant.

## Connect to Your Router by VPN

Once the VPN client is installed and running on your PC, you can set up a connection with your router by clicking on the CONNECT button in the StrideLinx Platform. The CONNECT button can be found on the device's details panel, as shown below.



**NOTE:** Can't click the connect button? Refer to the [troubleshooting section](#) of the manual.

When the connection is established the status icon will turn blue.





All traffic to the machine network will now be routed through the StrideLinx Platform and you will be able to access devices behind the router as if they were connected directly to your PC.

### Regarding VPN Connections

1. Keep in mind that a single TAP adapter (PC) is only able to make one VPN connection at a time.
2. A single user account may be connected via VPN:
  - a. TO a single router at a time
  - b. FROM a single PC or mobile device at a time
3. Multiple users (each from its own PC or mobile device) may be connected via VPN to a single router at a time.
  - a. Typically, the software connecting to the devices behind the router, e.g. Do-more! Designer or Productivity Suite, restricts user connections to a single user.

## Device Status

The current status of a device is indicated by the status-icon in the device list-view. It can also be found inside the info section on the device details page.

Device Status		
<i>Icon</i>	<i>Label</i>	<i>Description</i>
	Offline	The device is offline. You can't set up any kind of connection to the device.
	Online	The device is online. You can now set up a connection to the device.
	Connecting	The device is busy connecting.
	Connected	The device is connected through the VPN. Your PC now has access to the device's machine network.

## Connect to Devices Behind the StrideLinx Router

When your PC is connected to a StrideLinx router, a VPN connection is established between the PC and the machine network behind the StrideLinx router. All devices on the machine network behave as though they are located on the PC's local network.

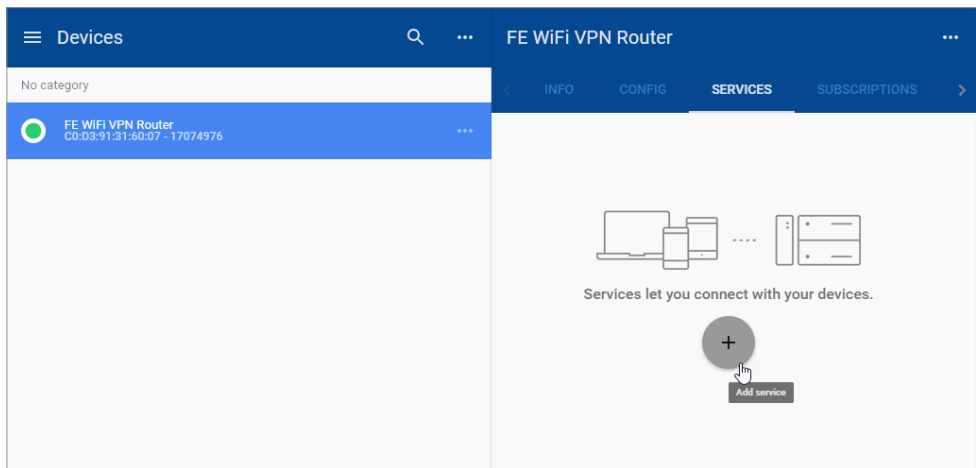
Alternatively, specific services on the machine network can be configured for access via the StrideLinx Platform without requiring a VPN connection, as described below.

### HTTP/VNC/Data Logging Services and Shortcuts

Once your device is registered and configured, you may want to set up a service that allows you to access your HTTP/VNC/Data Logging server(s) via the StrideLinx Platform.

#### *Managing Services*

Adding a service is quite simple. Select a router and then select “services” in the third-tier panel. From there you can view and modify all the device's existing services or add new ones. Shortcuts to services are displayed on a router's Info page providing easy access to all of the services for a specific router.



When adding a service you first specify the target of the service you wish to add by entering a name and IP address. Next, you select the service type (HTTP/VNC/Data Logging), enter any remaining details (i.e. a password if required), and click ADD.

Please refer to [Chapter 3](#) to configure the many device options from AutomationDirect.com.

### *Push Automatically Generated Port Forwarding*

When you add a service, a required port forwarding is automatically added to your router's CONFIG tab. A dot appears below the CONFIG tab to indicate that changes have been made that have not yet been synchronized to the router. Please click the CONFIG tab, then click the ellipsis to the right of the configuration sync message and click "Push config to device" to update the router.



*This is a secure VPN→LAN port forward inside the encrypted VPN tunnel so that StrideLinx users can access the HTTP server or VNC server of their control network devices by shortcut services in the StrideLinx platform.*

Any change to the router configuration (for example, changes to network settings or WiFi client settings) will be identified with this dot and must be pushed to the router in the same way.

The first screenshot shows the 'FE WiFi VPN Router' configuration page. The 'CONFIG' tab is selected, and a small red dot is visible below the 'CONFIG' tab label. A table of services is displayed, including an 'HTTP server' with IP address '192.168.140.100' and port '192.168.140.100:80/'.

The second screenshot shows the same configuration page, but a blue notification banner appears at the top stating: "This configuration is not in sync with the current configuration on the device." A red dot is now visible below the 'CONFIG' tab label.

The third screenshot shows the same configuration page with the notification banner. A context menu is open over the notification banner, showing three options: "Push config to device" (with a blue arrow icon), "Import config from device" (with a black arrow icon), and "Details" (with an information icon). The "Push config to device" option is highlighted by the mouse cursor.

### *Hypertext Transfer Protocol (HTTP or HTTPS)*

With an HTTP(S)-service you can remotely connect to any webserver hosted on your devices.

You can open the HTTP service in a new browser-window by clicking on the “open-in-new” icon in the top right corner or you can press-and-hold the CTRL key when you click on an HTTP service to directly open it in a new window.

### *Virtual Network Computing (VNC)*

With StrideLinx Platform you can remotely access your devices with a VNC server from within your browser. If you have a VNC server running on a computer, make sure you set your server’s encryption setting, if available, to also accept unencrypted connections.

Our in-browser VNC client has been optimized for use with smartphones or tablets. With two finger gestures you can pinch-zoom and pan around the screen.

### *Data Logging*

Datalogging and monitoring is available as an add-on service, subscribed to from your StrideLinx account. Note that model SE-SL3001 does not support data logging.

The setup process requires:

1. Enter credit card information in the Billing section. (Click your username, then click “Billing” in the 1st-tier menu.)
2. Activate the Data logging subscription for the desired router under SUBSCRIPTIONS in the third-tier panel for that device. Select the desired service level (number of data points per hour). Note that a 30-day free trial of the data logging service for one router is available from the SUBSCRIPTIONS panel as well.
3. After the Data logging service is activated, click the ellipsis in the Data logging box to expose the menu that includes adding/editing a data report or live data monitor. Selections to Pause, Upgrade and Deactivate the datalogging subscription are also available here.
4. Configure your device for Datalogging – select the Protocol and enter the Data Tags.
5. Configure data reports (log/record historical data) and/or data monitors (display live data)

A more detailed example of setting up data logging is shown in [Chapter 4](#).

## Using StrideLinx on Your Mobile Device

Apps are available on the iTunes App Store and the Google Play Store. Android and iOS devices can access services set up for connection through the StrideLinx Platform, or may establish a direct VPN connection through the StrideLinx router. Mobile VPN access requires router firmware versions v3.13 or newer. After upgrading the router firmware from version v3.12 or older, power cycle the router or cycle the VPN on and off. To cycle the VPN, go to Device->Info->VPN & click the 3 ellipses->Edit VPN Access. Turn off the “Use VPN” button, confirm changes. Do this again, but turn on the “Use VPN” button.

The apps allow access to the following:

- Connect to devices behind the router, for example, using the *C-more* Remote Access app.
- Router configuration
- User permission management
- Access token management
- Create & monitor data dashboards (note that model SE-SL3001 does not support data logging)
- View event logs



**NOTE:** The StrideLinx app may take an extended time to load, depending on the speed of the available data connection, when it is not already cached in your device's memory.

### iOS Client

The VPN client for iOS devices is available in the iTunes App Store at <https://itunes.apple.com/us/app/stride-sitelink/id1276487779?mt=8>, or by scanning the QR code to the right.



A video walking you through setting up and using the iOS mobile app to access the StrideLinx Platform data logging is accessible by clicking the thumbnail at the right, or by copying the following URL to your browser:

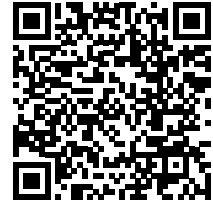
<https://www.AutomationDirect.com/VID-CM-0031>





## Android Client

The VPN client for Android devices is available in the Google Play Store at <https://play.google.com/store/apps/details?id=co.ixon.stridesitelink&hl=us>, or by scanning the QR code to the right.



A video walking you through setting up and using the Android mobile app to access the StrideLinx Platform data logging is accessible by clicking the thumbnail at the right, or by copying the following URL to your browser:

<https://www.AutomationDirect.com/VID-CM-0030>

**2**

## Access via Web

Alternatively, mobile devices not connected through a StrideLinx app can access services set up for connection through the StrideLinx Platform via the web at [www.StrideLinx.com](http://www.StrideLinx.com). You can also save the webpage as a WebApp on most devices.

### *Use as a WebApp*

The StrideLinx website can be saved as an app on most mobile devices, allowing access to StrideLinx from your home screen.

#### *On iOS Devices*

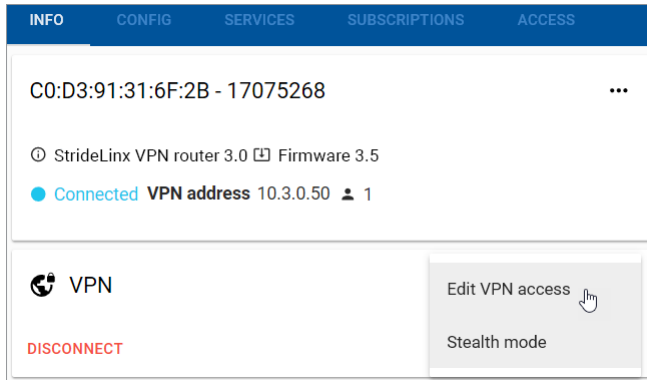
- Open the Safari browser
- Navigate to [www.StrideLinx.com](http://www.StrideLinx.com)
- Tap the menu-icon
- In the menu, tap on the “Add to Home Screen” option
- Choose “Add”
- The StrideLinx WebApp will now be accessible from your home screen

#### *On Android Devices*

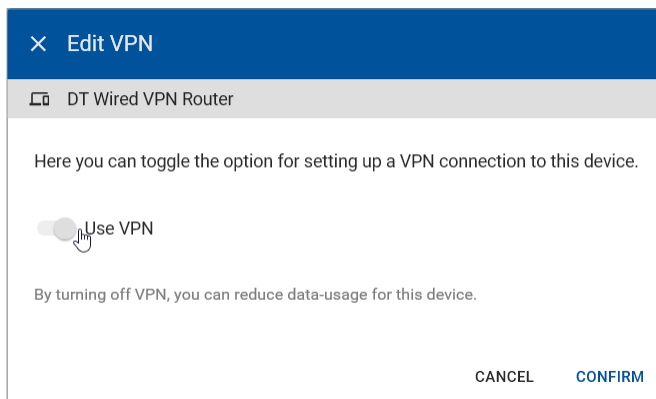
- Open the Chrome browser
- Navigate to [www.StrideLinx.com](http://www.StrideLinx.com)
- Tap the menu-icon (three dots)
- In the menu, tap on the “Add to Home Screen” option
- Choose “Ok”
- The StrideLinx WebApp will now be accessible from your home screen

## Reducing Router Bandwidth

Users can reduce the amount of StrideLinx router background data by turning off the router-to-cloud VPN so that the router operates in standby mode. In order to put the router in standby mode, log into your StrideLinx account and select the router. Click on the info tab, click the ellipses in the VPN section (to the right of the Connect button), and select “Edit VPN Access.”



Click the “Use VPN” toggle switch shown below to turn the router-to-cloud connection to standby mode. This will reduce the monthly bandwidth to about 5MB/mo. In order to access the router (by VPN or through the webservice/VNC server shortcuts) the user will have to turn this back on. This is a fairly simple step to save data if data consumption is of concern.



# Organization: Companies, Device Categories & User Groups

## Overview

A video providing an overview of the tools for organizing companies, users and devices within the StrideLinx Platform is accessible by clicking the thumbnail at the right, or by copying the following URL to your browser:

<https://www.AutomationDirect.com/VID-CM-0038>



## Companies

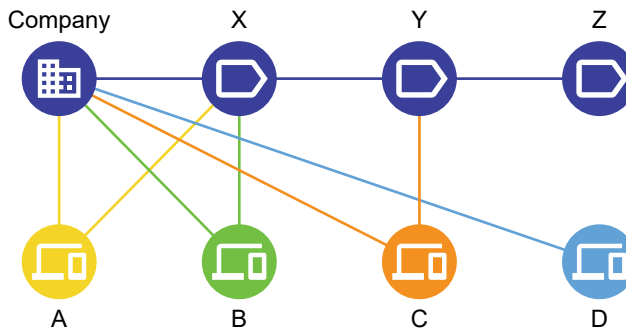
A user account may be associated with more than one company. The StrideLinx Platform will display the devices and settings for the currently active company, which can be changed at any time by selecting “Switch company” in the resultant 1st-tier menu after clicking your username.

Details about the current company, including the company name and location, can be edited by selecting “My company” from the 1st-tier menu. Click your username to expose the option. The company is identified by a unique code which is assigned by the StrideLinx system. This identifier is not configurable and is shown on the My Company page. The “Company name” is fully editable. It is possible, though not recommended, to configure multiple companies with the same or similar company names.

## Device Categories

Routers can be assigned to device categories. Categories allow you to manage employee or customer access with an initial setup saving time as additional users or routers are added. Users or user groups with access to a category will always be able to access all devices within that category. So if routers are removed from a category or a new router gets added, you don’t have to update the access rules.

In the example below you see a company with four routers (A, B, C and D) and three device categories (X, Y and Z). The lines in between show the connections among them.

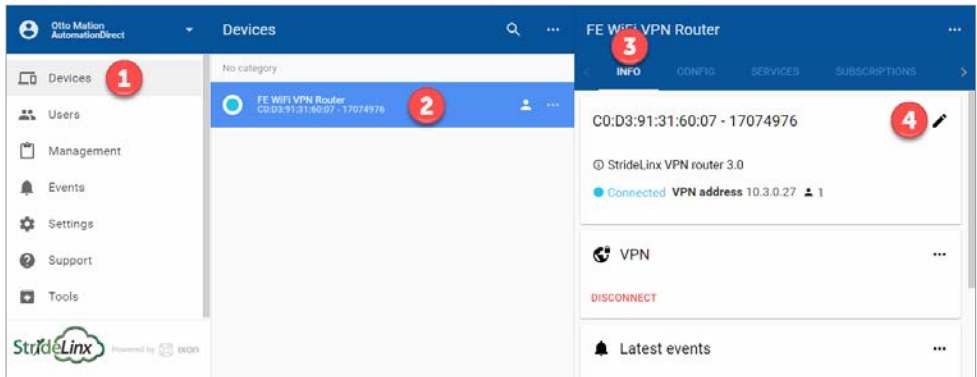


Routers can only be linked to one company and one category. For example routers A and B are linked to category X and router C is linked to category Y.

Routers don't have to be linked to a category, and categories don't have to contain any routers. For example router D is not assigned to any category, and category Z does not contain any routers.

A category is first created by selecting Management in the first-tier menu, then selecting DEVICE CATEGORIES in the second-tier menu. Finally, click CREATE A CATEGORY in the second-tier panel.

Once a category is created, routers may be assigned to it by (1) clicking Devices, (2) selecting the desired router, (3) clicking the INFO tab, and (4) clicking the Edit (pencil) icon to the right of the device identifier in the third-tier panel.

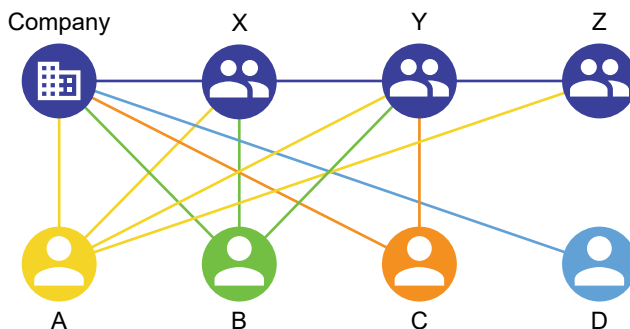


A device category can then be selected, along with editing the router name, description, and location.

## User Groups

Within a company users can have specific access and permissions. User groups make it possible to better organize users within a company. This improves clarity, but more importantly makes it easier to set access rules for your company's devices.

In the following example you see a company with four users (A, B, C and D) with three user groups (X, Y and Z). The lines in between show the connections among them.



A user can be linked to more than one user group. For example user B is linked to both groups X and Y while user C is only linked to group Y.

Users don't have to be linked to a user group. For example user D is not assigned to any user group. Users may be members of multiple companies, but user groups are only assigned on a per-company basis.

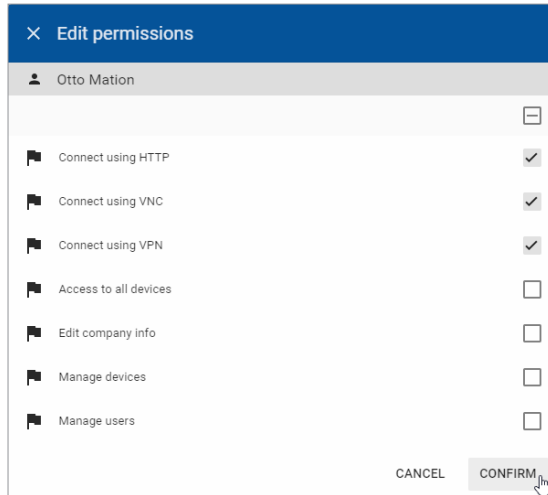
A user group is created by selecting Management in the first-tier menu, then selecting USER GROUPS in the second-tier menu. Finally, click the "Add User Group" button in the lower right to create a new user group.

To edit the assigned user groups for a user or selection of users, select Management in the first-tier menu, then select USERS in the second-tier menu. Select one or more users by clicking the check box beside each name. Finally, you can select the 'Edit groups' option. This will open a dialog with a list of all the available user groups.

For each user you can select user groups by toggling the input checkboxes. By clicking confirm the changes will get saved.

## Access and Permissions

Users and User groups may be assigned permissions restricted to a single device or a Category of devices. Access can also be given to a single router from the Devices – Router – Access tab.



Each user and user group has their own set of permissions within a company. Based on those permissions a user is allowed or not allowed to see and use specific modules of the platform. In combination with access rules you can very easily limit the functionality to the needs of a user. For example, you might want to give a specific user permission to use the VNC connection, but not allow him to edit any configuration settings for the router.

Here is a brief description of each permission.

- **Connect using HTTP:** allows/disallows users to see HTTP server shortcuts on the router – Info page.
- **Connect using VNC:** allows/disallows users to see VNC server shortcuts on the router – Info page.
- **Connect using VPN:** allows/disallows user to connect by VPN to a router’s local area network to access field devices. Disallowing may be useful when you want to prevent a user from programming field devices.
- **Access to all devices:** allows access to all routers in a company’s account. If this box is unchecked no routers will be visible. Access to device categories or specific routers can be granted so that all devices are not blocked.
- **Edit company info:** allows/disallows the user to edit the My company page info.
- **Manage devices:** allows/disallows the user to modify or edit router config settings and shortcuts to HTTP/VNC servers, data logging tags & reports/monitors. Also allows/disallows data logging subscriptions to be modified.
- **Manage users:** allows/disallows user management (inviting other users, setting user permissions).

## Two-factor Authentication

Two-factor authentication is an additional security feature that requires a second, one-time-use password, in addition to your configured password, for every login. This protects your account from access by someone who has learned your login name and password.

These one-time passwords are generated by an authentication app on a smartphone, and are valid for a short amount of time. The passwords are based on a key shared by the StrideLinx platform and a time-based encryption algorithm. Thus, access to the enrolled phone device provides a second authentication of your identity.

### Setting Up Two-factor Authentication

#### 1. Download an Authentication Application

To generate a valid one-time password, you need a mobile device with an authentication application installed on the device. Most commonly a mobile phone is used, but other devices like a tablet are also an option.



**CHOOSING A DEVICE:** You need access to your registered device to log in to your account, so choose a device you keep with you at all times. The authentication apps do not require a data connection to generate a valid one-time password and will continue to refresh their codes even in airplane mode.

There are a number of free authentication apps available for multiple device operating systems. Our examples show Google Authenticator.

#### 2. Enable Two-factor Authentication

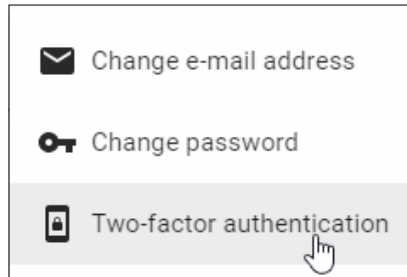
To enable two-factor authentication on the StrideLinx Platform, click your username at the top of the first-tier menu, then select “My profile.” Find the Login and Security block under My Profile in the 1st-tier menu after clicking your username.

The screenshot shows the user profile page for 'Oto Motion AutomationDirect'. The page is titled 'My profile'. The left sidebar contains navigation items: My profile, My company, Billing, Switch company, and Log out. The main content area is divided into sections: 'Login and security' (with a 'Security options' link), 'My access tokens', and 'My permissions'. The 'My access tokens' section contains a table with the following data:

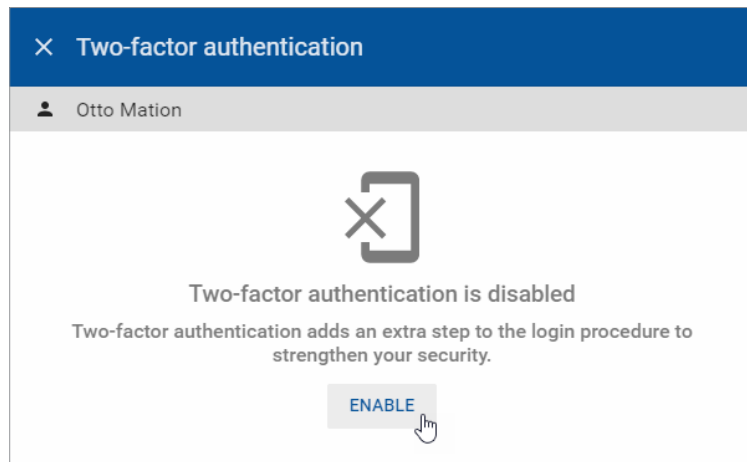
Device	OS	Browser	Expires	
Unknown device	Windows 10	Chrome 61.0.3163.79	in 7 days	REMOVE

The 'My permissions' section shows a table with one entry: 'Description' and 'Active' (with an up arrow).

Click the ellipsis icon, then click “Two-factor authentication” in the pop-up dialog. A dialog will appear notifying you that two-factor authentication is currently disabled.



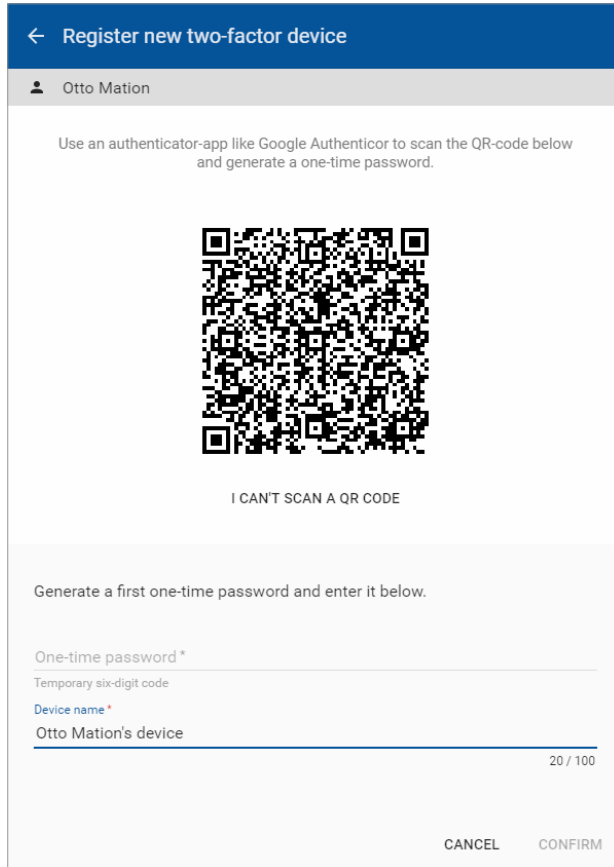
Click ENABLE to activate the feature.



In the resulting screen, a QR code is visible at the top of the dialog box. In the installed authentication app, choose to “Add a new account” or something similar. Google Authenticator allows you to scan a QR code with the camera of your device.

Point the device’s camera towards the screen so that the entire QR code falls in the window. After a few seconds, the application will notify that it has registered the QR code and will prompt you for a name for the account.






← Register new two-factor device

👤 Otto Mation

Use an authenticator-app like Google Authenticator to scan the QR-code below and generate a one-time password.



I CAN'T SCAN A QR CODE

Generate a first one-time password and enter it below.

One-time password \*  
Temporary six-digit code

Device name \*  
Otto Mation's device

20 / 100

CANCEL CONFIRM

If you can't scan a QR code on your device you can also manually enter the code needed to register your device. Click on "I can't scan a QR code" to display a 16-character code.

Afterward, by clicking on the name you gave this account, a 6-digit code (and often a timer) will be shown. Every 30 seconds, the timer resets and the code changes. After this time period, the previous code becomes invalid and the new code becomes valid.

In the dialog box on the website, enter the 6-digit one-time password visible on your device and enter a descriptive name for the device you registered.

Click on CONFIRM to verify if your device is registered properly and the one-time password is valid. If the one-time password provided during setup is valid, two-factor authentication is enabled for your account.

### *Problems Registering Your Device?*

If, after clicking “Confirm”, a message appears stating that the one-time password is incorrect, several things may have happened:

- You made a mistake entering the one-time password
- You waited too long after entering the one-time password before clicking CONFIRM. Note that these codes are only valid for a short amount of time.
- There was a problem in scanning the QR code or entering the 16-character code. In your app, remove the account. Then you can make a new account and scan the QR code or enter the code again.

### **Backup Codes**

Once your two-factor authentication setup is completed, you will receive an e-mail which contains five one-time-use backup codes. If your authentication device becomes unavailable for any reason, you can still use a backup code to enter your account. After entering your username and password on [www.StrideLinx.com](http://www.StrideLinx.com), you can choose to enter a backup code instead of generating a one-time password. You will be notified by e-mail when a backup code is used.

When you have used your last backup code to log in, new backup codes will be automatically generated and sent to your e-mail.




---

**LOSING YOUR DEVICE:** *If you have lost your phone, you should disable two-factor authentication by logging in with a backup code and following the steps under “Disabling two-factor authentication”. When you re-enable two-factor authentication, you can register a new device.*

---

**If you lose both your device and your backup codes, you will have no way of entering your account!**

---




---

**LOSING YOUR BACKUP CODES:** *If you have lost your backup codes, you can disable two-factor authentication by following the steps under “Disabling two-factor authentication”. If you later re-enable two-factor authentication, new backup codes will be sent to your e-mail address.*

---

**If you lose both your device and your backup codes, you will have no way of entering your account!**

---

### **Logging In**

When two-factor authentication is enabled, after entering your username and password as usual, you will be prompted to generate a one-time password. Open the authentication application installed on the registered device and choose the correct account to generate a 6-digit code.

If you wish to log in using a backup code, click the device icon to the right of the input for the one-time password to enter a backup code. Clicking the icon again will revert back to entering a one-time password.

## Disabling Two-factor Authentication

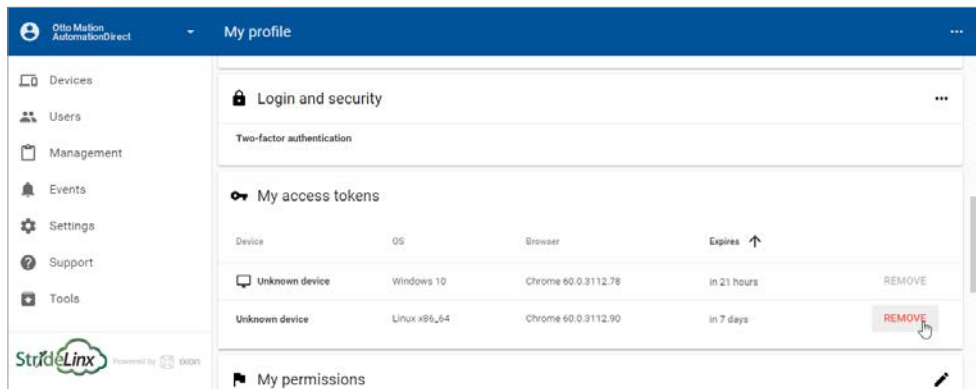
You can disable two-factor authentication by going to “Two-factor Authentication” under “Login and security” on the “My Profile” page. After clicking DISABLE, an e-mail will be sent to your email address where you can confirm or reject the disabling of two-factor authentication.

You can always re-enable two-factor authentication later with the same or a new device.

## User Access Token

A unique security access token is stored and valid for 7 days when a user has successfully logged in. A user is automatically logged in when returning to [www.StrideLinx.com](http://www.StrideLinx.com) on the same browser and with the same IP address within that 7-day window. If the IP address has changed or the user uses a different browser, the user has to log in again.

The Access Token for a device you have previously used to access the StrideLinx Platform may be removed to prevent automatic login. Browse to the My Profile page:



Note that you cannot remove the access token for the device you are currently using to access the StrideLinx Platform.

## Transfer a Device



**NOTE:** If a Datalogging or other subscription is assigned to a device, you will not be able to transfer that device unless the destination company has a license for that subscription available. A Cloud Notify license though will transfer with the router to which it is activated if that router is transferred to another company. Note that model SE-SL3001 does not support data logging.

A router is assigned to a single company. To assign a router to a different company, the router may be reset to default and reconfigured, or, the Transfer device utility will change the company assignment without changing any other configuration settings.

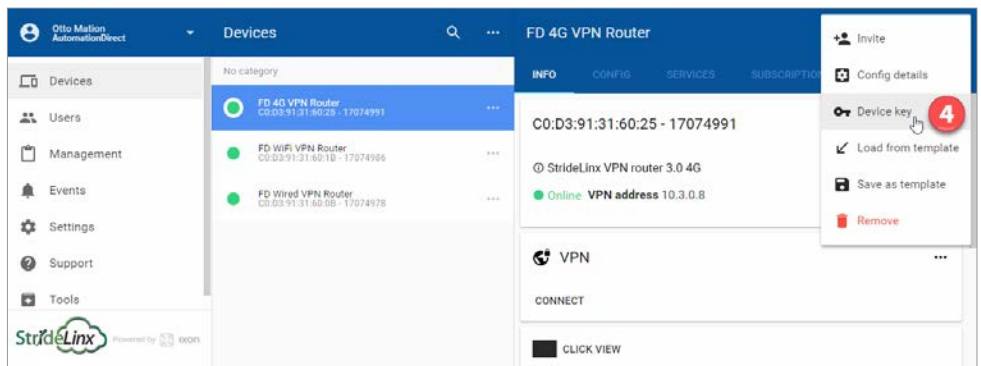
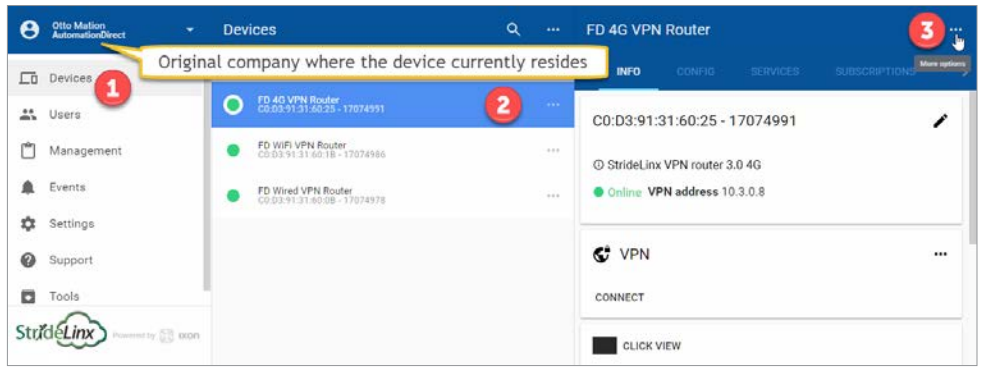
The Transfer Device utility is found on the Tools page on the Device menu.

The serial number and Device key for the router must be known. The Device Key is assigned to the router while you are logged in to the company where the router currently resides.

Note that in the StrideLinx system, the company to which a router is assigned is identified by a unique code rather than the company name. It is possible to have a duplicate company name.

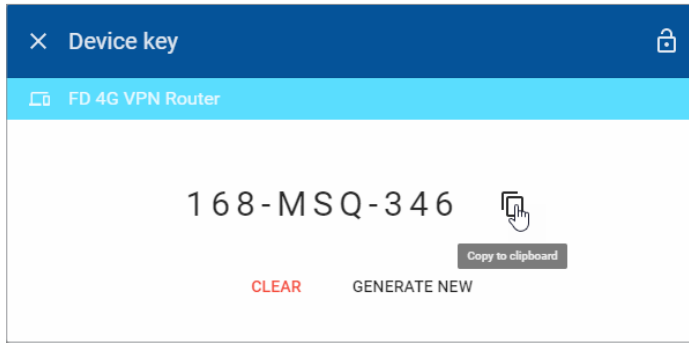
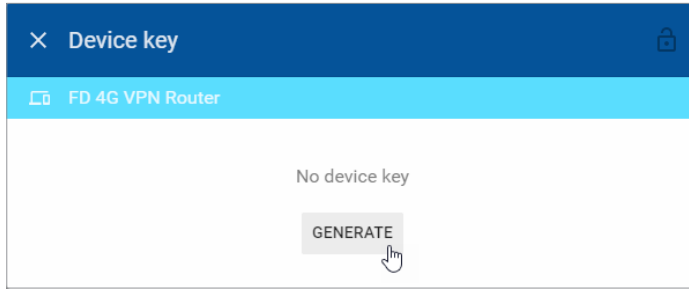
## To Assign a Device Key

When logged in to the original company where the router resides, from the Devices menu list, (1) select Devices. Then (2) click on the target router in the second tier. (3) Click the ellipsis to the right of the router name in the third-tier panel, and (4) click “Device key”.

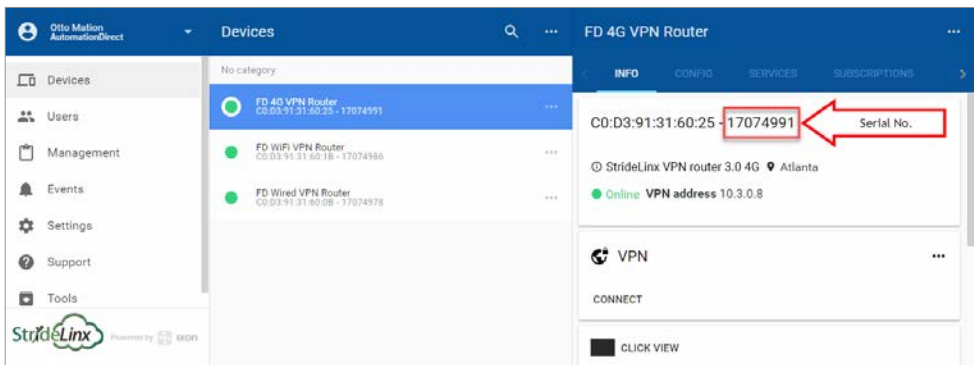


2

2



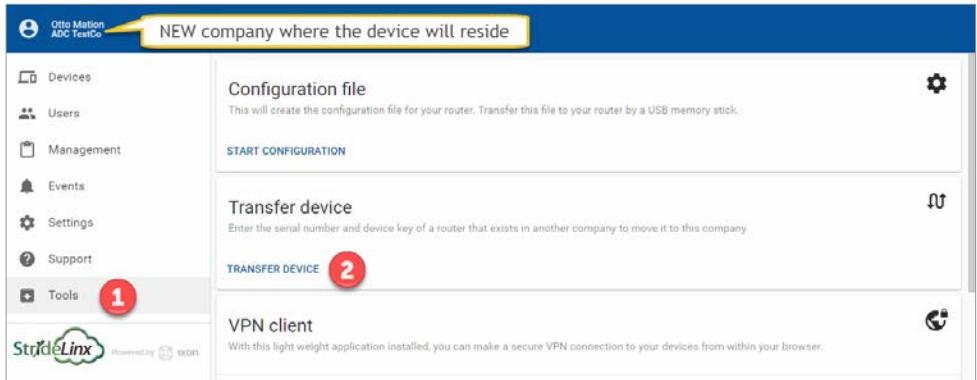
Click the GENERATE button, then click the Copy to Clipboard button. Paste this key into a notepad or word document. On the Device details third-tier panel, copy the device serial number.



Now, change to the destination Company. Select Tools on the Devices menu list, then click the TRANSFER DEVICE in the second-tier menu and paste the serial number and device key.

**If a Datalogging or other subscription is assigned to a device, you will not be able to transfer that device unless the destination company has a license for that subscription available. Note that model SE-SL3001 does not support data logging.**

2



× Transfer device

Serial number \*

Device key \*

Generated on the device details page

CANCEL    TRANSFER

The device should now be successfully transferred to the new company. If a message indicates that the transfer failed, the device may have a data logging or other subscription assigned to it. The new company must have the same subscription service available to assign to the device, or the service must be removed from the device prior to transfer.

# CONTROLLER CONNECTION EXAMPLES

---



## In this Chapter...

Video Examples.....	3-3
<b>CLICK PLC Connection via Cellular Router SE-SL3011-4G .....</b>	<b>3-4</b>
Before You Begin.....	3-4
Setup .....	3-4
<b>BRX PLC Connection via WiFi Router SE-SL3011-WF .....</b>	<b>3-7</b>
Before You Begin.....	3-7
Setup .....	3-7
<b>C-more® HMI Connection via Wired Router SE-SL3011 .....</b>	<b>3-10</b>
Before You Begin.....	3-10
Setup .....	3-10

**3**

This manual covers the StrideLinx platform available from 2017 through 2021.

For details covering the StrideLinx Cloud 2.0 platform available after April 2021, please [click here](#) to link to that manual.

The StrideLinx Cloud 2.0 manual includes details describing the [Activation Code](#) model of Data Logging, Cloud Notify and other add-on features.

For information on the migration wizard from the original platform to StrideLinx Cloud 2.0, [click here](#).



## Video Examples

Videos examples of remote programming several of our PLC and HMI products are accessible by clicking the thumbnails below, or copying the URL to your browser.

*Remote Programming a CLICK PLC*

<https://www.AutomationDirect.com/VID-CM-0023>



3

*Remote Programming a Productivity 2000 PLC*

<https://www.AutomationDirect.com/VID-CM-0024>



*Remote Programming a Do-more! BRX PLC*

<https://www.AutomationDirect.com/VID-CM-0025>



*Remote Programming a DirectLogic PLC*

<https://www.AutomationDirect.com/VID-CM-0027>



*Remote Programming a C-more® HMI Panel*

<https://www.AutomationDirect.com/VID-CM-0026>



## CLICK PLC Connection via Cellular Router SE-SL3011-4G

The cellular StrideLinx VPN router is a valuable option when:

- There is no existing internet available at the remote site, or
- The network policies at the remote site prohibit connection of third-party devices. Although the StrideLinx solution is IT friendly, using only outbound request for connection, it may be the case that local policies prohibit any such connection.

In such cases, if an AT&T phone can get a signal at the location of the router, your SE-SL3011-4G router can provide you the remote access you need.

This example will step you through connecting to a CLICK PLC via the cellular router, model SE-SL3011-4G



---

**NOTE: Regarding Ethernet access to a CLICK PLC**

*If you intend to take advantage of any methods of remote access to the PLC, you need to consider the security exposure in order to minimize the risks to your process and your PLC.*

*Security should always be carefully evaluated for each installation. Refer to the “Security Considerations for Control Systems Networks” section of Appendix B.*

---

### Before You Begin

1. Buy an AT&T M2M SIM card and know the APN and PIN
2. Know your CLICK network settings
3. Have your SE-SL3011-4G router, LTE antennas and USB stick available

### Setup

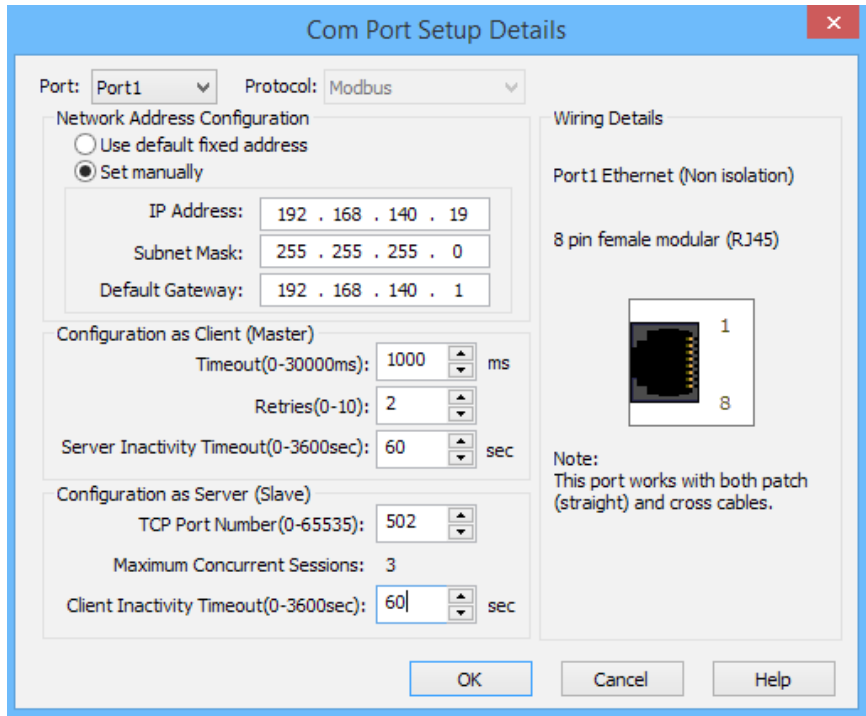
Remember that you can't browse across the VPN to the router's LAN network, so the CLICK must be configured and the network settings known before you configure your router.

### *Configure the CLICK Network Settings*

For our example, we'll configure CLICK as follows:

- IP Address: 192.168.140.19
- Subnet mask: 255.255.255.0
- Default Gateway: 192.168.140.1 (the router's LAN IP address) This must be on the same subnet as the CLICK

1. In the CLICK software, select Setup > Com Port Setup > Ethernet Port 1 Setup (button) and enter the IP address, subnet mask and default gateway settings.



2. Click OK in the setup dialog and the subsequent dialog.
3. Write the project to the PLC.

### *Configure Your SE-SL3011-4G Router*

1. You must contact AT&T to purchase a SIM card for your router. You may choose the M2M (data only) SIM card option rather than the typical phone (voice and data). You will need AT&T access; the M2M SIM card includes a selected amount of data and a valid length of time (rather than the monthly subscription typical for the phone SIM card)

*Steps 2 through 15 are outlined in detail in Chapter 2. If you have already completed router activation, please proceed to step 16.*

2. Create your StrideLinx account at [www.StrideLinx.com](http://www.StrideLinx.com), as discussed in Chapter 2.
3. Once you're logged in, Select "Tools" > START CONFIGURATION and confirm the appropriate company, then click NEXT.
4. Select "Mobile Network Using SIM Card"

5. Enter the APN and PIN associated with the SIM card, then click NEXT.
6. On the WAN information screen, Click SHOW MORE to configure the Digital Input VPN router access control if desired. Click NEXT when finished.
7. On the LAN information screen, enter the router port IP address, which must match the default gateway entered in the CLICK PLC setup (192.168.140.1 in this example).
8. Download the configuration file. Rename it ixrouter.conf if it has been saved with a suffix.
9. Copy ixrouter.conf to the root directory of your USB stick.
10. Install the VPN Client on your PC. (This step must be repeated for any new PC where you will use your StrideLinx account.)
11. Mount and wire your SE-SL3011-4G router, and connect the LTE antennas.
12. With Power DISCONNECTED from the SE-SL3011-4G router, plug the SIM card into the router.
13. Insert the USB stick into the router.
14. Power your router. Wait while the router writes the configuration and then registers itself to the StrideLinx Server. After the router is successfully registered and connected to the StrideLinx platform, the Status LED will be on steady blue and the Signal LED will be on steady blue/violet/red depending on network signal strength.



---

**NOTE:** *It's best practice to remove the config file from the USB after the router has been registered so that on power up the router boots from the current configuration rather than the initial configuration.*

---

15. Activate the router.
16. Now, your router will appear in the Devices list in your StrideLinx account.
17. Select the router from the list of devices, then click the CONNECT icon.

### *Configure the CLICK Software to Access the CLICK PLC via VPN*

1. Open the CLICK software on your PC and select the "Connect to PLC" button.
2. Select Port Type = Ethernet and select the Outside this LAN radio button, then the Add... button.
3. Enter a Link Name and the CLICK IP address defined previously (192.168.140.19 in this example), then click OK.
4. Highlight your target CLICK in the devices list, then click the CONNECT button.

You should now be successfully connected to the CLICK PLC from a remote PC through the VPN.

## BRX PLC Connection via WiFi Router SE-SL3011-WF

The WiFi StrideLinx VPN router is a valuable options when:

- Client mode - Wired internet access is not available to the equipment panel, or would be impractical to install.
- Access point mode - VPN connections to multiple devices is desired without wiring Ethernet cable to each.
- Client mode - Local operators want to limit access to a machine network by using their smartphone as a WiFi hotspot. This allows the StrideLinx WiFi router to connect as a client and establish a VPN connection to the platform on an as-needed basis.

This example will step you through connecting to a BRX PLC via the WiFi router, model SE-SL3011-WF, in client mode. Internet access will be via the WiFi connection, and the BRX PLC will be connected to a LAN port on the router. The router's Ethernet WAN port will be disabled.




---

### **NOTE: Regarding Ethernet access to a BRX PLC**

*If you intend to take advantage of any methods of remote access to the PLC, you need to consider the security exposure in order to minimize the risks to your process and your PLC.*

*Security should always be carefully evaluated for each installation. Refer to the "Security Considerations for Control Systems Networks" section of Appendix B.*

---

### Before You Begin

1. Know your BRX network settings
2. Know the SSID and password for the WiFi access point at your BRX location
3. Have your SE-SL3011-WF router, WiFi antenna and USB stick available

### Setup

Remember that you can't browse across the VPN to the router's LAN network, so the BRX PLC must be configured and the network settings known before you configure your router.

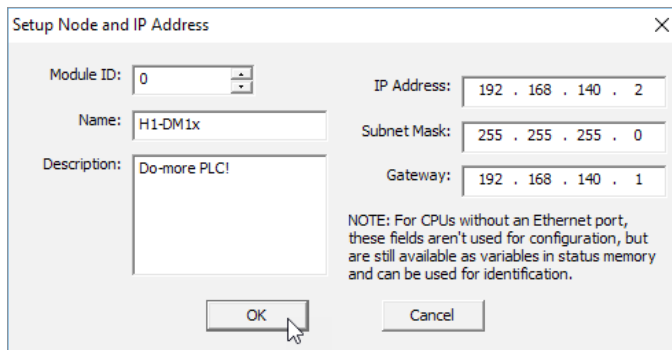
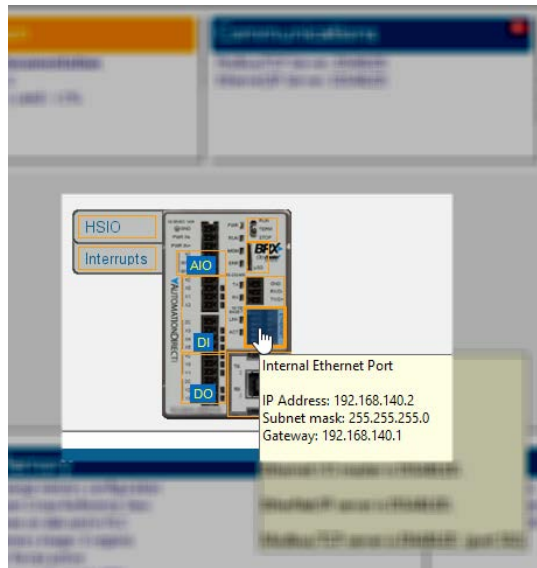
### *Configure the BRX PLC Network Settings*

For our example, we'll configure BRX PLC as follows:

- IP Address: 192.168.140.19
- Subnet mask: 255.255.255.0
- Default Gateway: 192.168.140.1 (the router's LAN IP address) This must be on the same subnet as the BRX PLC

1. In the Do-more! Designer software, connect to your BRX PLC.
2. Click on the ethernet port in the image of your PLC on the Do-more! Designer dashboard, select “Edit IP configuration” and enter the IP address, subnet mask and default gateway settings.

3



3. Click OK in the setup dialog.
4. Write the project to the PLC.

### Configure Your SE-SL3011-WF Router

1. Create your StrideLinx account at [www.StrideLinx.com](http://www.StrideLinx.com), as discussed in Chapter 2. *Steps 2 through 13 are outlined in detail in Chapter 2. If you have already completed router activation, please proceed to step 14.*
2. Once you're logged in, Select "Tools > Start Configuration" and confirm the appropriate company, then click NEXT.
3. Select "Wireless Network"
4. Enter the name (SSID) and password for the wireless network, then click NEXT.
5. On the WAN information screen, Click SHOW MORE to configure the Digital Input VPN router access control if desired. Click NEXT when finished.
6. On the LAN information screen, enter the Default Gateway address (Router port IP Address), which must match that entered in the BRX PLC setup (e.g., 192.168.140.1).
7. Download the configuration file. Rename it ixrouter.conf if it has been saved with a suffix.
8. Copy ixrouter.conf to the root directory of your USB stick.
9. Install the VPN Client on your PC. (This step must be repeated for any new PC where you will use your StrideLinx account.)
10. Mount and wire your SE-SL3011-WF router, and connect the WiFi antenna.
11. With Power DISCONNECTED from the router, insert the USB stick into the router.
12. Power your router. Wait while the router writes the configuration and then registers itself to the StrideLinx Server. After the router is successfully registered and connected to the StrideLinx platform, the Status LED will be on steady blue.



**NOTE:** It's best practice to remove the config file from the USB after the router has been registered so that on power up the router boots from the current configuration rather than the initial configuration.

13. Activate the router.
14. Now, your router will appear in the Devices list in your StrideLinx account.
15. Select the router from the list of devices, then click the CONNECT icon.

### Configure the Do-more! Designer Software to Access the BRX PLC via VPN

1. Open the BRX Do-more! Designer software on your PC and select "New Link" from the Links panel on the lower left of the Launchpad tab.
2. Click the "Link Editor..." button.
3. Select the PLC family (Do-more! BRX Series in this example) and PLC Type.
4. Click the "Port" tab, select Ethernet and enter the BRX IP address defined previously (192.168.140.19 in this example).
5. Enter a Name and Description for this PLC link, then click ACCEPT.
6. Double-click the new entry in the Links list to connect to the BRX PLC.

You should now be successfully connected to the BRX PLC from a remote PC through the VPN.

## **C-more**® HMI Connection via Wired Router SE-SL3011

The wired StrideLinx VPN router is a valuable options when:

- Adding a third-party device to the remote network is permitted.

This example will step you through connecting to a **C-more** HMI via the wired router, model SE-SL3011. Internet access will be via the wired WAN connection, and the **C-more** HMI will be connected to a LAN port on the router.



---

**NOTE: Regarding Ethernet access to a C-more panel**

*If you intend to take advantage of any methods of remote access to the panel, you need to consider the security exposure in order to minimize the risks to your process and your **C-more** panel.*

*Security should always be carefully evaluated for each installation. Refer to the “Security Considerations for Control Systems Networks” section of Appendix B.*

---

### Before You Begin

1. Know your **C-more** network settings.
2. Have your SE-SL3011 router and USB stick available.
3. Have an established StrideLinx platform account set up.

### Setup

Remember that you can't browse across the VPN to the router's LAN network, so the **C-more** HMI must be configured and the network settings known before you configure your router.

#### *Configure the C-more HMI Network Settings*

For our example, we'll configure **C-more** HMI as follows:

- IP Address: 192.168.140.19
- Subnet mask: 255.255.255.0
- Default Gateway: 192.168.140.1 (the router's LAN IP address) This must be on the same subnet as the **C-more** HMI



1. In the **C-more** HMI panel setup software, select Setup > Touch Panel Network > Ethernet Port.
2. Check Save Settings to Project, and select the Use the following IP address radio button.
3. Enter the network settings shown at the beginning of this example.
4. Select OK.
5. Select SEND project to **C-more** panel.

### Configure Your SE-SL3011 Router

1. Create your StrideLinX account at [www.StrideLinX.com](http://www.StrideLinX.com), as discussed in Chapter 2. *Steps 2 through 14 are outlined in detail in Chapter 2. If you have already completed router activation, please proceed to step 15.*
2. Once you're logged in, Select "Tools > Start Configuration" and select the appropriate company, then click NEXT.
3. Select "Wired Network using Ethernet cable".
4. Select the appropriate company if applicable, then click NEXT.
5. On the WAN information screen, click SHOW MORE if DHCP is not appropriate for your installation; otherwise, continue to step 6.
  - 5.1. Configure the network settings for the **C-more** location.
  - 5.2. Configure a static DNS server.
  - 5.3. Configure the Digital Input VPN router access control.
  - 5.4. Configure a proxy server and the login credentials, if necessary.
6. Click NEXT when finished.
7. On the LAN information screen, enter the router port IP address, which must match the default gateway entered in the **C-more** HMI setup (192.168.140.1 in this example).
8. Download the configuration file. Rename it ixrouter.conf if it has been saved with a suffix.
9. Copy ixrouter.conf to the root directory of your USB stick.
10. Install the VPN Client on your PC. (This step must be repeated for any new PC where you will use your StrideLinX account.)
11. Mount and wire your SE-SL3011 router, and connect Ethernet cables.
12. Insert the USB stick into the router.
13. Power your router. Wait while the router writes the configuration and then registers itself to the StrideLinX Server. After the router is successfully registered and connected to the StrideLinX platform, the Status LED will be on steady blue.




---

**NOTE:** *It's best practice to remove the config file from the USB after the router has been registered so that on power up the router boots from the current configuration rather than the initial configuration.*

---

14. Activate the router.
15. Now, your router will appear in the Devices list in your StrideLinX account.
16. Select the router from the list of devices, then click the CONNECT icon.

### *Configure the C-more Programming Software to Access the C-more Panel via VPN*

1. Open the **C-more** software on your PC and select “Read From Panel”.
2. Select the Ethernet radio button and click Browse.
3. Click the Remote Link List tab, then the Add... button.
4. Enter a Link Name (for identifying the panel in this list only) and the **C-more** IP address defined previously (192.168.140.19 in this example), then click OK.
5. Highlight your target **C-more** panel in the devices list, then click the CONNECT button.

You should now be successfully connected to the **C-more** HMI panel from a remote PC through the VPN.

# DATA LOGGING

---



## In this Chapter...

<b>Cloud Data Logging .....</b>	<b>4-3</b>
Why Cloud Data Logging? .....	4-3
How Does the Cloud Data Logger Work? .....	4-3
Configure Cloud Data Logging On Your Device .....	4-3
Set Up Datalogging Subscription .....	4-4
Set Up Data Sources for a Device Using Modbus Protocol.....	4-5
<b>Cloud Logging Web App.....</b>	<b>4-11</b>
Dashboards .....	4-11
Download Logged Data .....	4-17
Status Info .....	4-18
Tag Configuration .....	4-19
Trigger Configuration.....	4-21
Test Utility .....	4-23
<b>Pausing, Deactivating, &amp; Terminating Your Datalogging Subscription .....</b>	<b>4-24</b>
Activate / Deactivate Datalogging .....	4-24
Pause / Resume Datalogging.....	4-24
Terminating a Subscription .....	4-24

This manual covers the StrideLinx platform available from 2017 through 2021.

For details covering the StrideLinx Cloud 2.0 platform available after April 2021, please [click here](#) to link to that manual.

The StrideLinx Cloud 2.0 manual includes details describing the [Activation Code](#) model of Data Logging, Cloud Notify and other add-on features.

For information on the migration wizard from the original platform to StrideLinx Cloud 2.0, [click here](#).

## Cloud Data Logging



**NOTE:** Model SE-SL3001 does not support data logging.

### Why Cloud Data Logging?

Cloud data logging gathers remote data from your control components. The data is transmitted in the StrideLinX platform for administrative, monitoring and analytical purposes. Our goal is to give you an insight in the performance of your machine and/or installation.

### How Does the Cloud Data Logger Work?

The Cloud data logger is a completely cloud-based solution. All the values you have programmed in the PLC can be logged by the StrideLinX logger, easily and securely.

Once the data tags are added to the StrideLinX platform, you are prompted to push the configuration changes to the router. The router then transfers the data to our server where it will be stored in our database.

The PLC is not used by using cloud data logging; the router is doing all the work.

The StrideLinX platform has a crucial role in the functioning of the Cloud data logger. All settings and data points to be logged are set via the StrideLinX platform.

Refer to the following subsection or the video to the right (<https://www.AutomationDirect.com/VID-CM-0032>) for details to set up Data Reports and Live Monitors for datalogging.



**NOTE:** This chapter uses Modbus protocol to illustrate data logging configuration. Refer to Appendix G, H, I, J and K for Siemens S7, OPC UA, EtherNet/IP, BACnet, and MELSEC protocols, respectively.

### Configure Cloud Data Logging On Your Device

Cloud datalogging setup requires:

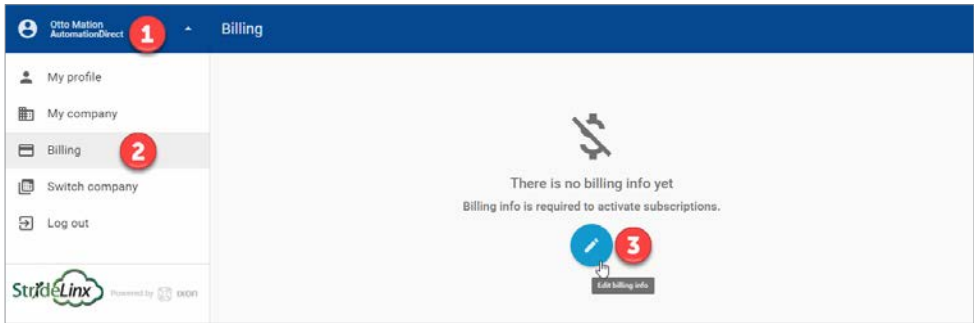
1. Set up datalogging subscription.
  - 1a. Enter credit card information and subscribe to the Cloud datalogging add-on service sized to suit your needs.
2. Set up data sources for a specific protocol (Modbus, Siemens S7, OPC UA, etc.)
  - 2a. Configure the address and protocol for the PLC (where the data is located).
  - 2b. Configure the data tags.
3. Test data tags to verify correct configuration
4. Design the data dashboard to display your data.

Each of these steps are detailed as follows.

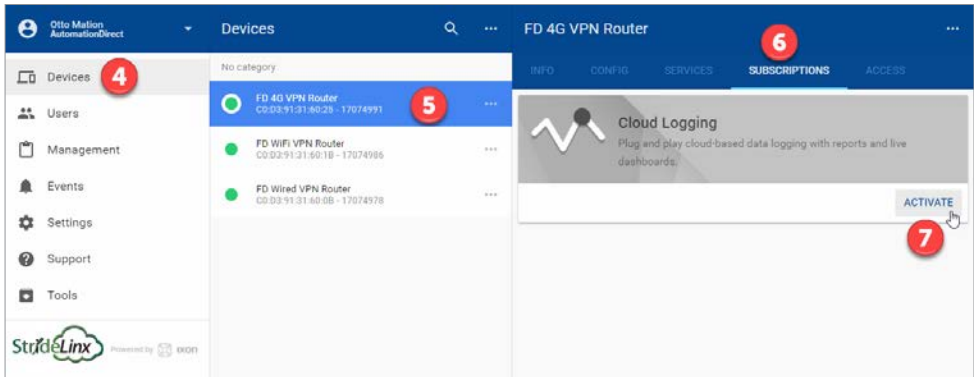
## Set Up Datalogging Subscription

*Enter credit card information and subscribe to the Cloud datalogging add-on service sized to suit your needs*

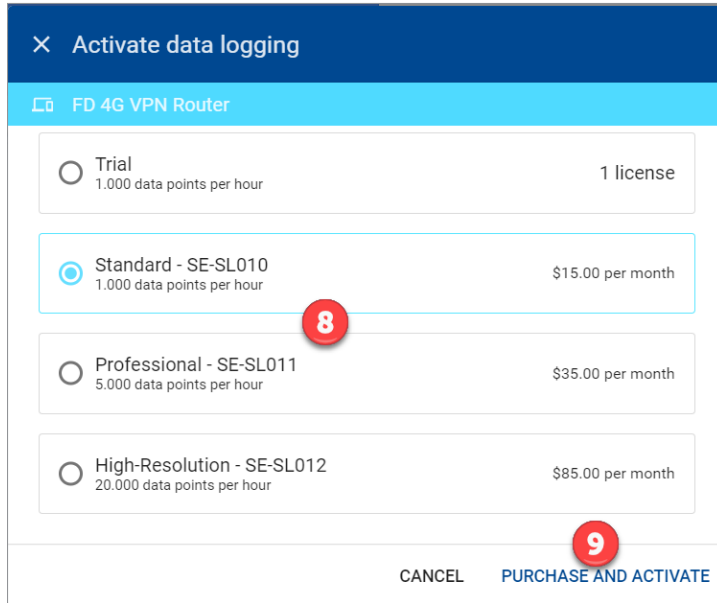
Click the account name (1) to toggle the menu list and show the Billing option (2). Click Billing and click the Edit Billing Info icon (3) to enter credit card information.



Click on Devices (4), click the desired router (5), click the SUBSCRIPTIONS tab (6), then click ACTIVATE.



Select the subscription that will suit your data recording requirements (8). Click PURCHASE AND ACTIVATE (9).



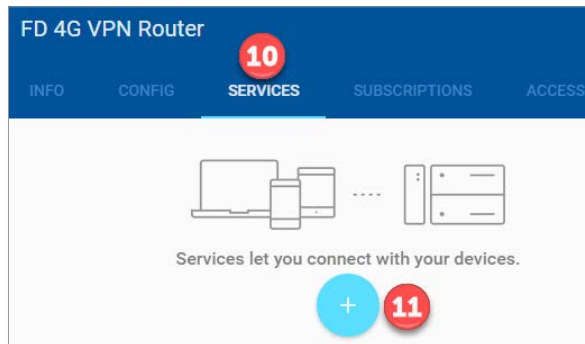
### Set Up Data Sources for a Device Using Modbus Protocol



**NOTE:** Refer to Appendix G, H, I, J and K for Siemens S7, OPC UA, EtherNet/IP, BACnet, and MELSEC protocols, respectively.

*Configure the address and protocol for the PLC from which data will be read*

Click on the SERVICES tab (10). Click the +(Add) button (11).



Add a Name and the IP Address of the PLC where the data resides. Click NEXT.

4

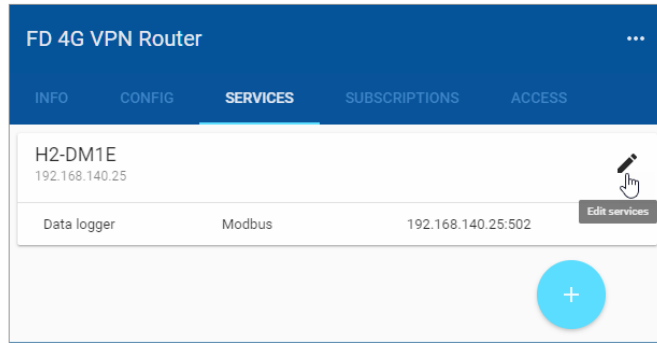
Select DATA SOURCE.

Select the Modbus protocol. If the Port must be changed, or a Slave ID must be entered for the device from which data will be logged, enter those values, then click ADD to continue.

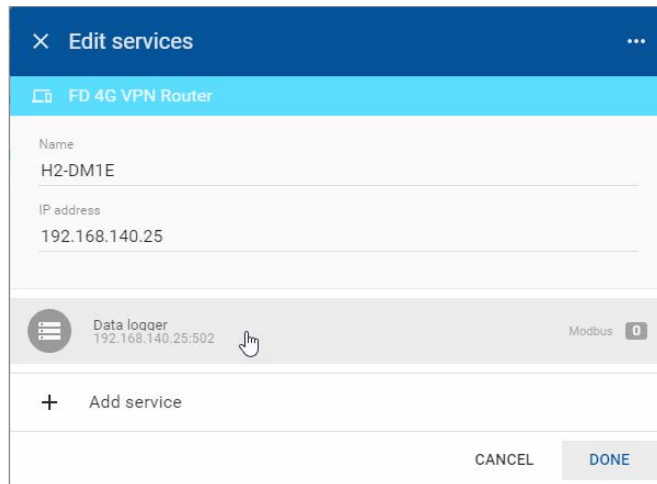


### Configure the data tags

To add a data tag, go to the SERVICES tab for the router, and click the Edit services (pencil) icon next to the device for which you want to add the data tag.

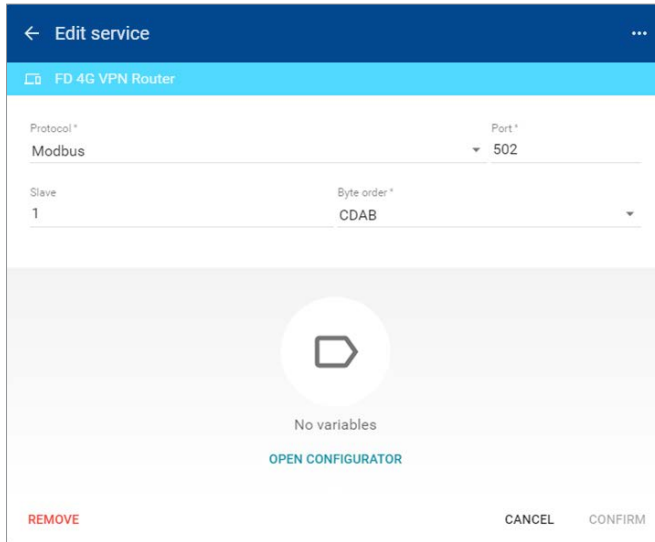


This opens the Edit services dialog. Click the name of the existing device for which you would like to add a data tag.

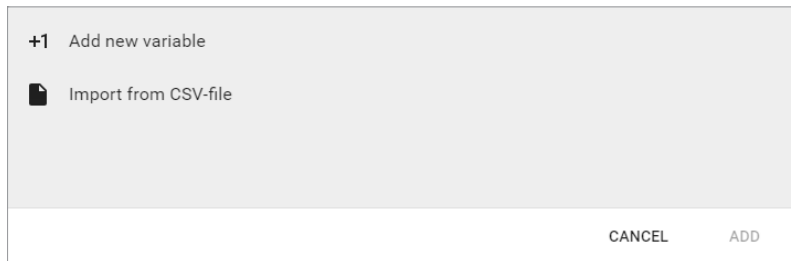


**NOTE:** It is advisable to enter data tags in small batches, and test the variables periodically to verify the entries. The entries can be tested by clicking “RUN TEST” in the Configurator, or from the Cloud Logging Web App as described in the [Data Logger Test Utility](#) section. Please refresh your browser if the information on screen appears to not be updated properly at any time.

The resulting “Edit service” screen displays the parameters for the data source, plus a count of existing data tags. Click OPEN CONFIGURATOR to add or edit tags.



Data tags can be entered interactively, or a set of tags can be imported from a previously-exported CSV file. Export of sets of data tags is discussed later in the “Export Data Tags” subsection. For this example, select “Add new variable” to manually enter tags.



A data entry screen opens, with one new data tag ready to be entered. Set the relevant parameters for the new data tag. Additional data tags can be entered in this round by clicking “+1” in the lower left corner of the screen. When all the desired tags have been entered click ADD.

The screenshot shows a data entry form with the following fields and controls:

- Name \***: A text input field.
- Function code \***: A dropdown menu currently showing "3 - Holding registers".
- Select a data type \***: A dropdown menu.
- Address \***: A text input field.
- Factor**: A text input field.
- Unit**: A text input field.
- Bottom right: Copy and delete icons.
- Bottom left: "+1" button.
- Bottom right: "CANCEL" and "ADD" buttons.

Data tag input fields are described in the following two tables. Also see the Modbus address translation chart in [Appendix D](#) for the key to enter addresses for AutomationDirect products. Refer to Appendix G, H, I, J and K for details on setting up Siemens S7, OPC UA, EtherNet/IP, BACnet and MELSEC protocols, respectively.

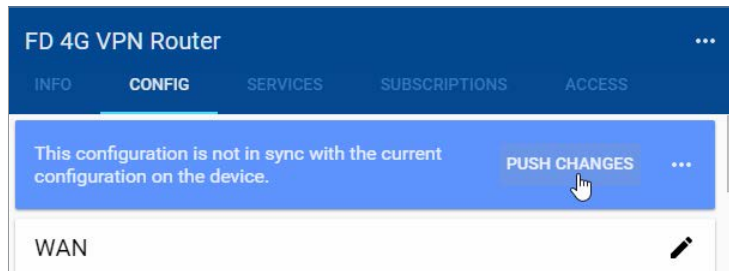
Data Tag Input Fields	
Field	Description
Name	Give the data tag a logical name.
Address	For Modbus protocol, the data tag address is the Modbus address (e.g., 412). Please see <a href="#">Appendix D</a> for address mapping for AutomationDirect PLCs.
Select a data type	See next table for the available data types.
Unit (optional)	Here you can assign a value to a unit, for example, gallons or psi.
Factor (optional)	This allows you to multiply by a value. For example, factor 0.01 divides the data value by 100. If a Factor is set for a widget in a dashboard, that Factor will override the global Factor configured here in the Data Configurator for the data as displayed in that widget only.



**NOTE:** Additional data tag parameters related specifically to data logging (i.e., sampling interval, data retention policy, and logging only when changed) can be set from the Cloud Logging web app discussed later in this chapter.

Data Types Supported
Bool
Float32
Float64
Int8
Int16
Int32
Int64
UInt8
UInt16
UInt32
UInt64

Once you have added all the data tags you want to log, you will be prompted to push the configuration to the router.



The Cloud Logging web app can now be used to set up data dashboards and to adjust additional data tag parameters related specifically to data logging.

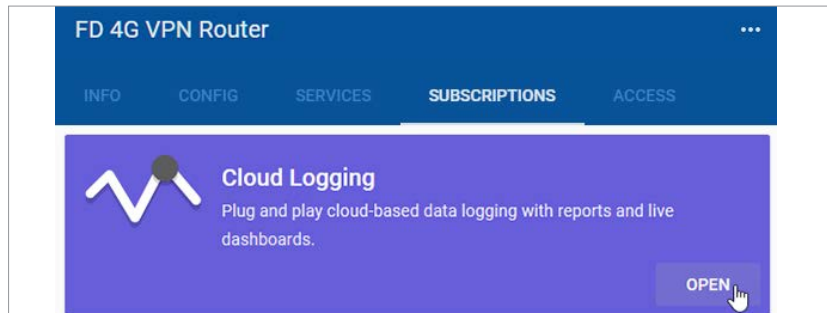
### *Export data tags*

Data tag configurations can be exported in CSV format. The CSV file is downloaded to your local PC, and can later be imported to set up another StrideLinx router.

Select data tags to be exported by clicking the icon for each data tag, or select all data tags at once from the More Options (⋮) menu in the upper right corner of the screen. The selected data tags can then be deleted, duplicated, or exported from the pop up menu at the bottom of the screen.

## Cloud Logging Web App

The Cloud Logging web app is found under the SUBSCRIPTIONS tab after selecting a StrideLinx device. Note that model SE-SL3001 does not support Cloud Logging.



The web app provides a central location to manage your data logging subscription, data tags, and data dashboards.

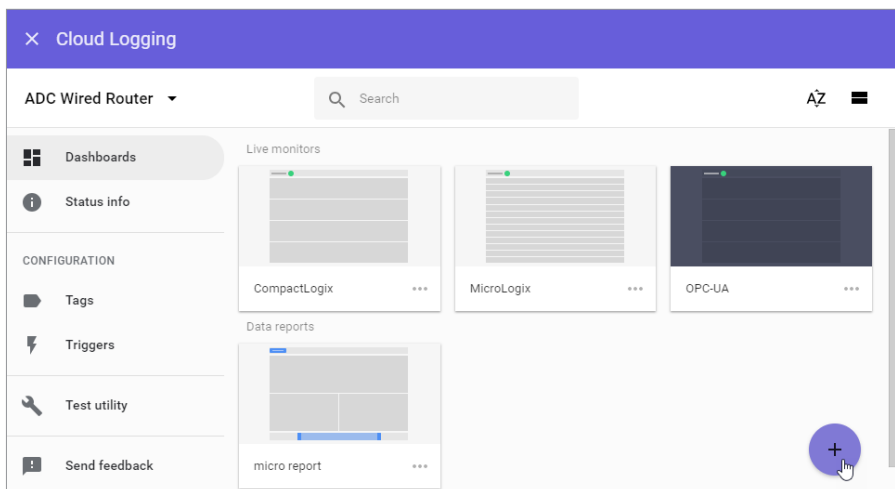
### Dashboards

The dashboards tab provides access to add, remove, edit and view both live monitors and data reports.

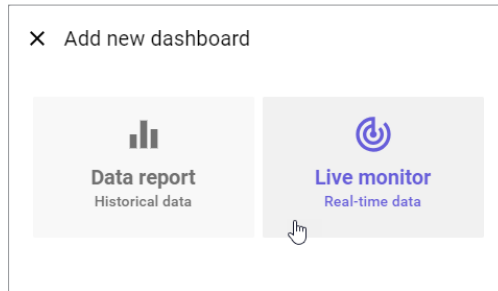
If a Factor is set for a widget in a dashboard, that Factor will override the Factor set for that data point in the Data Configurator for the data as displayed in that widget only. That is, the configuration of the widget changed the display of the data there but any other widget will use the default of the Configurator setting or the setting within each other widget.

### *Add a Live Monitor or Historical Data Report*

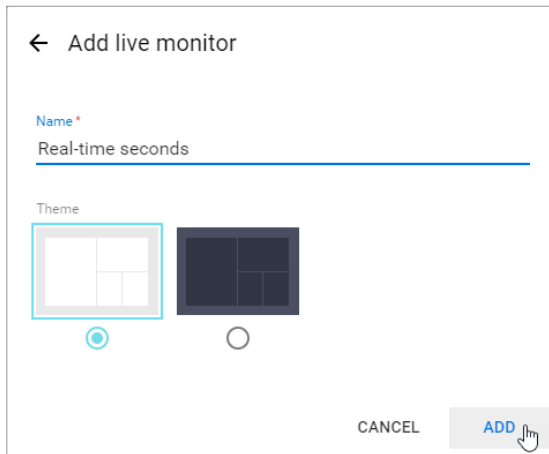
Click the “+” symbol in the lower right corner of the dashboard screen to begin creating a new Live Monitor or Data Report.



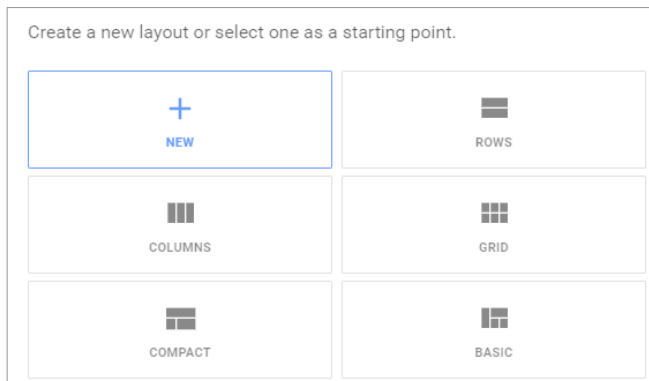
Select “Live Monitor” or “Data Report” to continue. The differences between the two are explained later in this chapter.



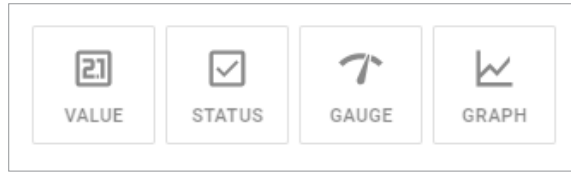
Give your dashboard a name and pick the black or white background then click ADD.



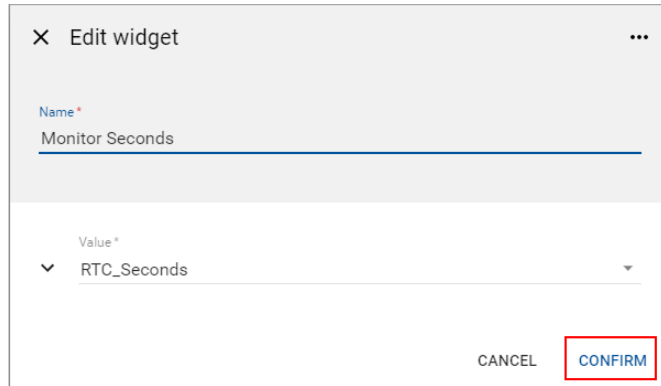
Pick a layout template as a starting point.



Click on a widget option to display the data.

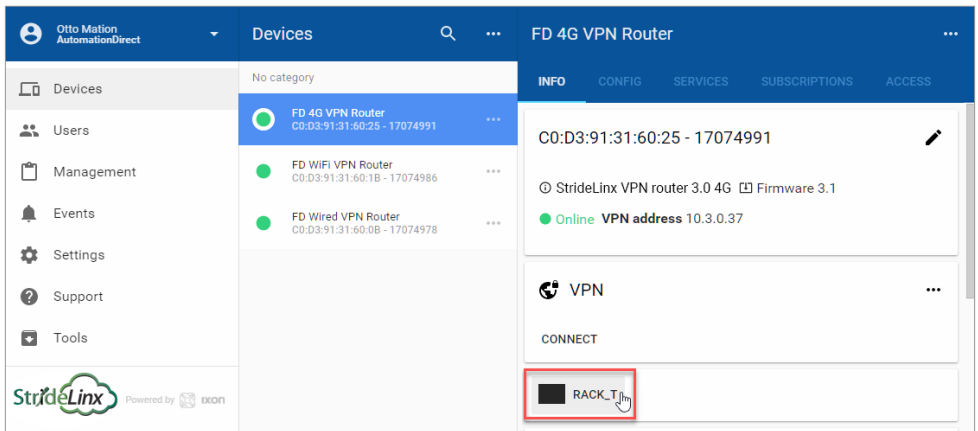


Enter the information requested for the widget type you've selected and click CONFIRM.



4

Add more widgets if you would like. When finished, click the VIEW button to display the Live Monitor or Data Report, or click the X to return to the main Cloud Logging page. The new dashboard is available on the router INFO tab as well as within the Cloud Logging web app.



## Live Monitor

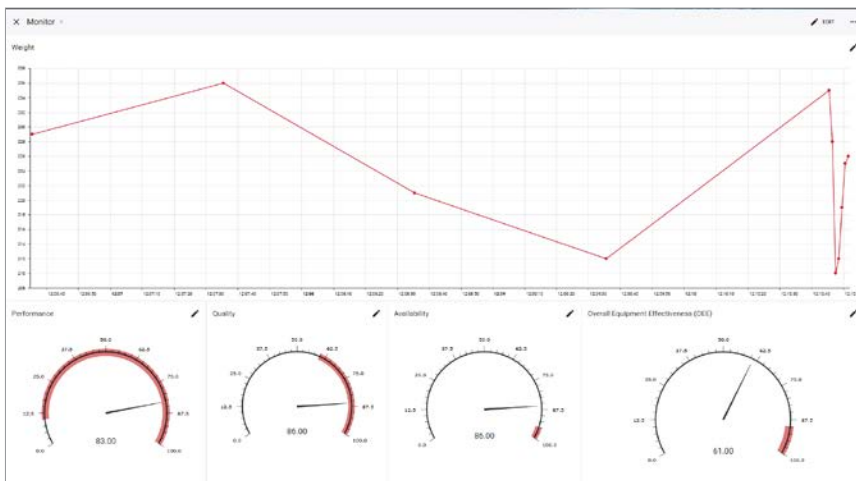
The live monitor displays real-time data. It gives you an insight into how the machine is operating at the moment.

### Widgets

We use widgets to display the data. In our live monitor we have four widget options:

Data Visualization Widgets		
Widget	Description	Setup
Value	Shows the current value of the data tag.	When you select the "Value" widget you give the widget a name and choose the data tag you want to be shown. Click CONFIRM.
Status	Relevant only to Boolean data, shows true or false.	When you select the "Status" widget you give the widget a name, label and choose the data tag you want to be shown. You may customize the display (for example True and False). Click CONFIRM.
Gauge	Relevant only to numeric data types. Select a range between numbers "X" and "Y". The gauge (meter) shows you the current value of the data tag in comparison to the numbers X and Y.	When you select the "Gauge" widget you name the widget and select the data tag you want to be shown. Enter the numbers for the bottom and top values of the gauge and drag the red bar to the left or the right. Click CONFIRM.
Graph	Shows the current value of the data tag(s) on a graph.	When you select the "Graph" widget you name the graph and select the data tags you want to be shown. Click on the color dot to customize the display. You can add as many data tags as you wish. Click CONFIRM.

A selection of templates is available to make creating your data dashboard more convenient. Example of a live monitor:



**NOTE:** The little dot next to the monitor's name shows the status of the monitor. When the dot is blinking grey/green the monitor is working (you can hover over the dot and see the date and time when the monitor checks the status). When the dot is grey, the monitor cannot connect to the PLC or the data tags are not configured properly. If you have configured a dashboard but no data is displaying, please refresh your browser. If that doesn't solve the issue, check your tags using the Data Logger Test utility. If one or more tags are configured incorrectly, no data will display.



## Data Reports

Historical data reports show the data that is logged over a period of time selected by you. The following is a step-by-step guide on how to configure a data report.

### Widgets

We use widgets to display the data. In our data report we have five widget options:

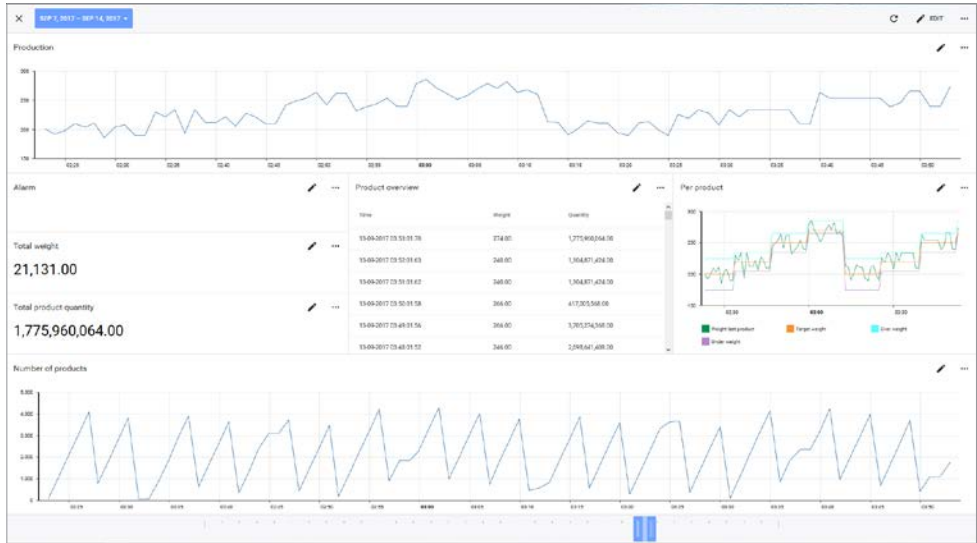
Data Visualization Widgets		
Widget	Description	Setup
Value	Shows the value of the data tag logged, depending on the configured formula.	When you choose the Value widget you can give a name to the value, select the data tag and enter the formula. More information about available formulas can be found in the next table.
Status	Shows a bar indicating status of a single data tag over time	Indicates status by color. Can be used with a boolean (i.e. true/false) or a threshold can be set on an integer or float (i.e. if value $\geq$ 5.4).
Period	Shows an advanced bar chart in which the data period is classified in fixed time intervals	Multiple variables can be stacked or displayed in separate bars. A formula can be set. More information about available formulas can be found in the next table.
Table	Shows a table of data tags and the logged value.	When you choose the table widget you can give a name to the widget and select data tags that the table should contain. Press CONFIRM to add the table to the data report.
Graph	Shows a bar of the data tags and the logged value.	The graph widget shows a chart where all the data points logged will be shown over the selected period of time. Enter a name for the chart and select which data tags you want to show in the chart. Chose a color for the data tags and click CONFIRM.

### Formula

You can select one of the following formulas:

Data Report Formulas	
Formula	Description
Average	Shows the average value over the time period selected
Min	Shows the minimum logged value in the time period selected
Max	Shows the maximum logged value in the time period selected
Median	The middle number of the logged numbers in the time period selected
Mode	Most common value in the time period selected
Range	Shows the difference between the minimum and the maximum logged value in the time period selected
Sum	Adds all the logged values in the time period selected
First	Shows the first logged value of the time period selected
Last	Shows the last logged value of the time period selected

Example of a data report:



As you can see in the image above, there are three dots located in the top-right of every widget. If you click on these three dots, you can export the raw data (i.e., the data directly logged from your PLC into the database, without any scaling factor applied).



**NOTE:** If you have configured a dashboard but no data is displaying, please refresh your browser. If that doesn't solve the issue, check your tags using the Data Logger Test utility. If one or more tags are configured incorrectly, no data will display.

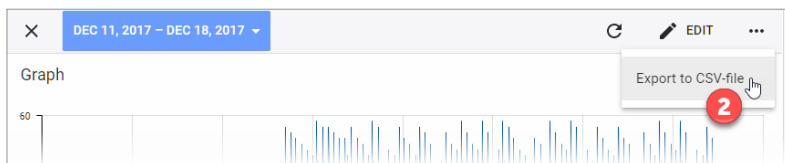
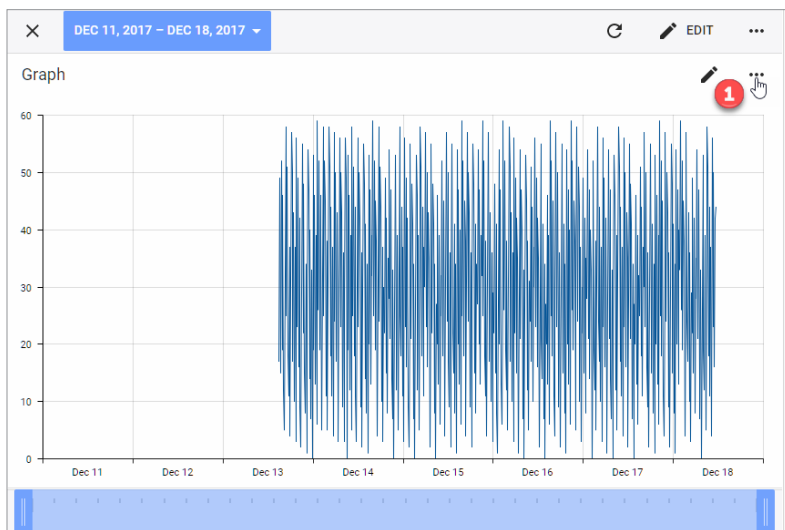
## Download Logged Data

Data that has been stored as a Data Report may be downloaded and saved locally.

Data is downloaded from the WIDGET configured in a data report. For this reason, a TABLE widget may be a good choice to log data that you expect to download. Configure the table with all tags that you expect to save. This may make downloading data more efficient since tags will be collected together in a single widget, allowing a single download.

While your subscription is active, view the Data Report that records the data you wish to save locally. Then (1) click on the ellipsis in the Widget that is configured with the desired tags.

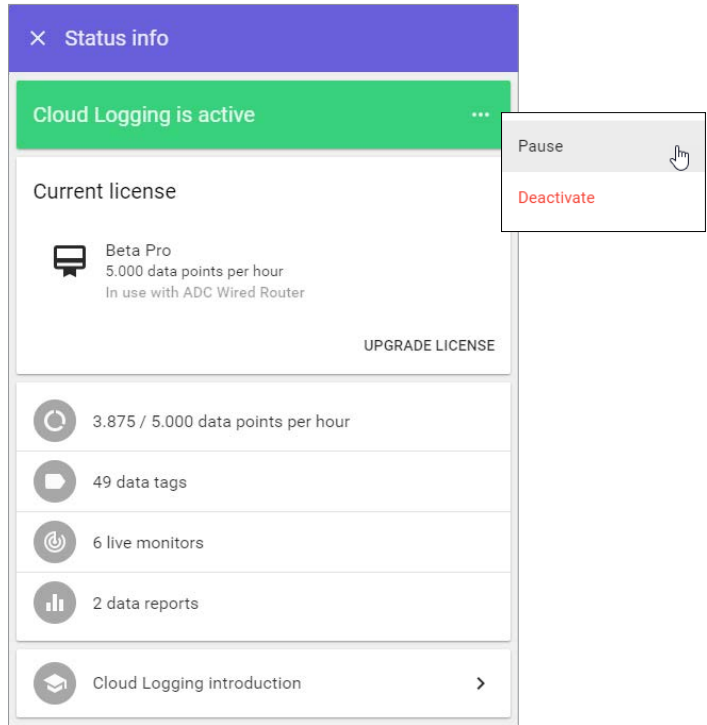
Click on the (2) Export to CSV option. The data file will save to the local path where Windows ordinarily downloads files. The file will be named (3) export.csv.



## Status Info

The Status Info tab provides an overview of the usage of the data logging subscription, and allows the subscription to be upgraded, paused, or deactivated. The Cloud Logging Introduction button will open a brief slideshow outlining the top-level steps needed to set up data logging.

4



## Tag Configuration

The Tag Configuration tab provides an easy method to add, edit, copy, or export data tags from all defined data sources.



**NOTE:** The purpose of the tags export feature is to clone the set of tags in another router.

The Tag Configuration section displays all the data sources defined for the presently selected StrideLinx router in the left-hand column. Selecting a data source will display all defined data tags for that data source, sorted by data type by default. The display can also be switched to a table view showing a concise overview of the data logging parameters for each tag.

The screenshot displays the 'Cloud Logging' configuration page for an 'ADC Wired Router'. On the left, a sidebar lists various data sources under the 'CONFIGURATION' section, including 'Tags', 'SLC 5/05', 'CompactLogix L35E', 'CompactLogix 5380', 'Siemens S7-1200', 'CompactLogix', 'MicroLogix', 'Triggers', 'Test utility', and 'Send feedback'. The 'CompactLogix' source is selected. The main area shows a list of tags for this source, categorized by data type: Integer, Boolean, and myBoolArray. The 'Integer' category is expanded, showing a tag named 'MYN7\_DATA[0]' with a configuration form. The form includes a 'Variable' field with 'MYN7\_DATA[0]', a 'Tag name' dropdown with 'MYN7\_DATA[0]', a 'Log on Interval' dropdown set to 'Interval', an 'Interval' field set to 'Every 30 seconds', a 'Formula' dropdown set to 'LAST (default)', and a 'Retention policy' dropdown set to '5 years'. There are 'CANCEL' and 'UPDATE' buttons at the bottom right of the form. A '+ ' icon is visible in the bottom right corner of the tag list.

New tags can be added by clicking the “+” icon in the lower right of the screen, which presents the choice to add a new data tag or import tags from a CSV file. Selecting “Add new data tag” will open a blank new tag dialog as discussed previously in this chapter. Importing from a CSV file is discussed in the following subsection.

The configuration of any data tag can be edited by clicking the downward chevron at the right of the tag. Clicking the ellipsis at the right of a tag will allow the tag to be duplicated, removed or selected for group operations.

Tags can be logged on a time interval, when the value changes, or when a trigger condition is met.

### *Logging on Time Interval*

When Log on Interval is selected, a time interval must be selected. At least one value must be logged per hour and a maximum of 10 values per second may be logged. The logging formula can be selected to log the last value received, or the minimum, maximum or mean value over the time interval.

The Retention Policy for the logged data must be set. Valid options are 6 months, 2 years, 5 years, or 7 years.

### *Logging on Change*

When Log on Change is selected, the maximum number of logged values per hour must be selected. Options range from 5 values per hour to 20,000 values per hour. Select a limit appropriate for your application and data subscription. Logging only when the value changes or on value change plus once each hour of unchanged value can be selected.

The Retention Policy for the logged data must be set. Valid options are 6 months, 2 years, 5 years, or 7 years.

### *Logging on Trigger*

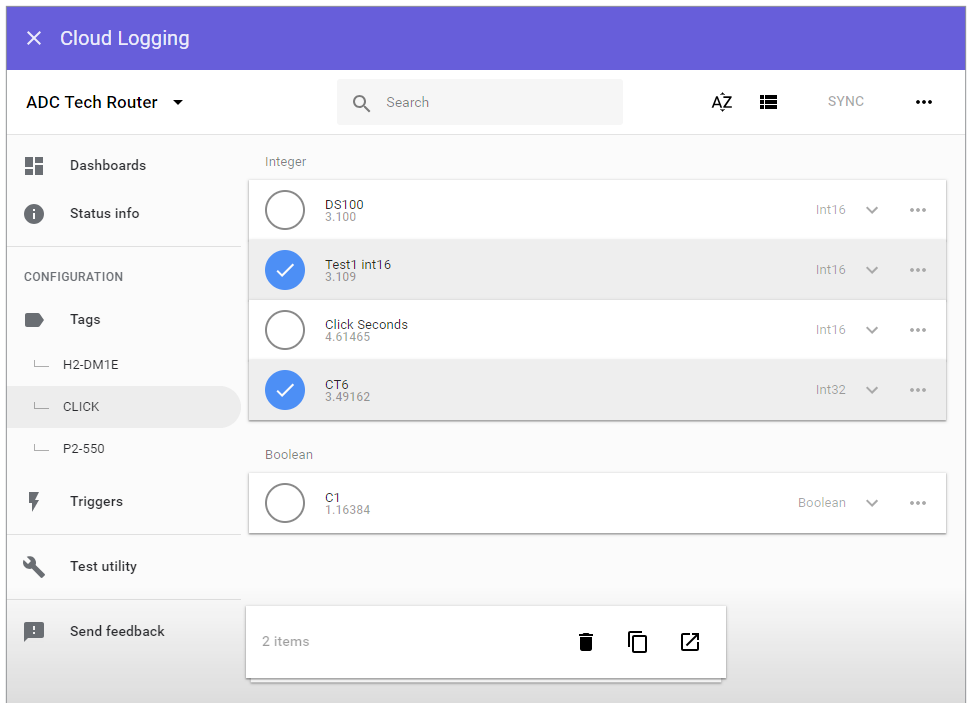
To log a batch of variables at the same time, ‘log on change’ is not sufficient. With the Log on Trigger system you can select a variable to act as a trigger (one-shot). You then associate other variables to this trigger variable. When that trigger variable changes, all attached variables are logged once.

When Log on Trigger is selected, the value is logged each time a custom trigger condition is met. The value will not be logged again until the trigger condition is false and then true again. The maximum number of logged values per hour must also be selected. Options range from 5 values per hour to 20,000 values per hour. Select a limit appropriate for your application and data subscription.

Trigger conditions can be created using any variable, and you can use the same trigger in multiple data tags. Creation of triggers is discussed under “Trigger Configuration” on page 4-21.

The Retention Policy for the logged data must be set. Valid options are 6 months, 2 years, 5 years, or 7 years.

Tags can also be selected for further operations by clicking the icon at the left side of the tag. The selected set of tags can then be deleted, duplicated, or exported. Tags are exported as a comma-delimited text file.



### *Importing Data Tags From CSV File*

After clicking “Import from CSV File,” a file open dialog is presented. Select a previously exported data tag file, which by default is named “export.csv.”

The CSV file will be opened, displaying the configuration data for all data tags in the file.

When ready to import the data tags, click the ADD button in the lower right.

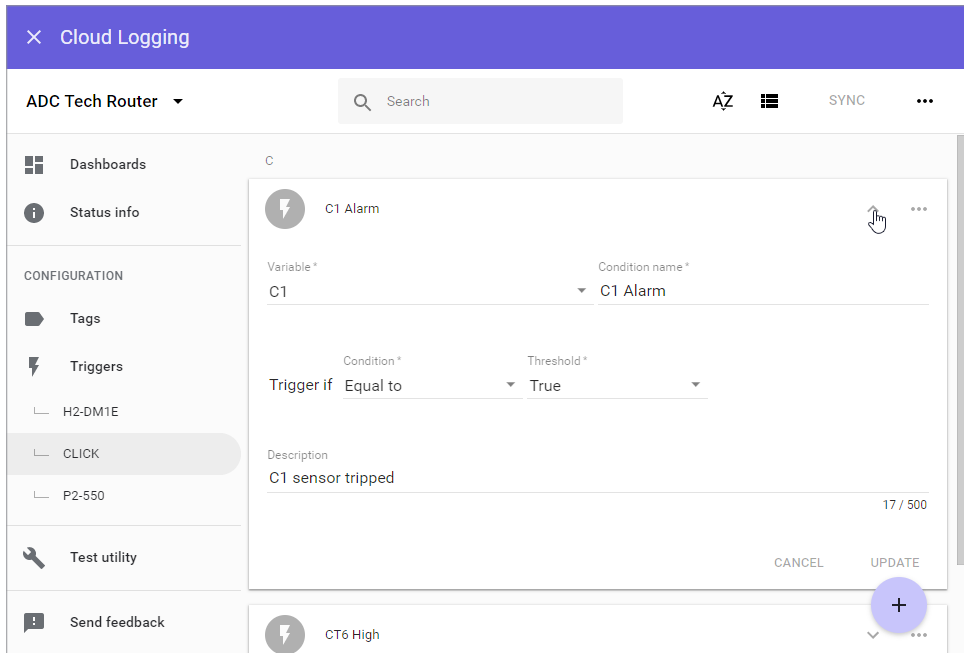
If any data tags conflict with tags already configured on the device, the conflicting tag will be highlighted on the screen and the import will not be completed. Delete any conflicting data tag from the import list and click ADD. The new data tags are then added to any existing data tags.

### **Trigger Configuration**

A Trigger allows logging of one or more data tags when a specified condition of another variable is met.

The Trigger Configuration tab provides an easy method to add, edit, copy, or export trigger conditions from all defined data sources. To begin, click Triggers

The Trigger Configuration section displays all the data sources defined for the presently selected StrideLinx router in the left-hand column. Selecting a data source will display all defined triggers for that data source. The display can also be switched to a table view showing a concise overview of the triggers for each data source.



New triggers can be added by clicking the “+” icon in the lower right of the screen, which presents the choice to add a new trigger or import triggers from a CSV file. Selecting “Add new trigger” will open a blank new trigger dialog. Importing from a CSV file is discussed in the following subsection.

The configuration of any trigger can be edited by clicking the downward chevron at the right of the trigger. Clicking the ellipsis at the right of a trigger will allow the trigger to be duplicated, removed or selected for group operations.

For each trigger, select a variable from the list of configured variables in the current data source, give the trigger a name, and select the condition to be met and threshold value. Optionally, a description of up to 500 characters can be added.

### *Importing Data Triggers From CSV File*

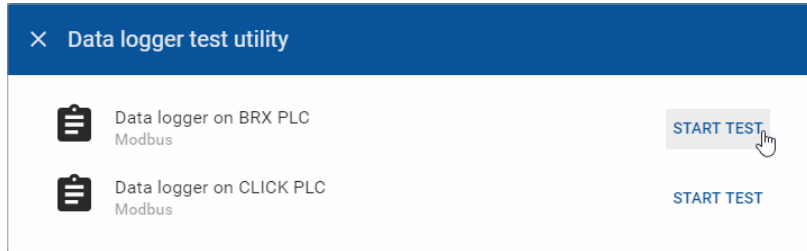
After clicking “Import from CSV File,” a file open dialog is presented. Select a previously exported trigger file. The CSV file will be opened, displaying the configuration data for all triggers in the file. When ready to import the triggers, click the ADD button in the lower right.



## Test Utility

The Data Logger Test Utility will test the configuration of each tag on a selected data source device and communication with the device. If you have configured a dashboard but no data is displaying, refresh/reload your browser. If data still does not display, one or more tags may be configured incorrectly. Please use this utility to verify your tags.

Click START TEST beside the data logger you wish to test.



If an error exists in any of the data tags, the first error encountered by the utility is displayed.

Address	Tag name	Type	Latest value	Status
3.0	MHR1	Int16		?
4.0	MIR1	Int16		?
4.65500	MIR65500	Int16		?

If the set of data tags passes the tests, “No errors” is displayed, as shown below. Tags which were successfully retrieved show a green check mark in the status column, and display the latest value.

Address	Tag name	Type	Latest value	Status
3.0	MHR1	Int16	17	✓
4.0	MIR1	Int16	17	✓



**NOTE:** To ensure Data Logger Test Utility provides accurate results, please update/refresh your browser prior to running the test, and make sure you have pushed the latest configuration to your router. The Test Utility displays raw data; Factor doesn't affect the data shown.

## Pausing, Deactivating, & Terminating Your Datalogging Subscription

Explanation of the Pause/Resume, Activate/Deactivate and Terminate Options for the Datalogging Subscriptions.

### Activate / Deactivate Datalogging

To begin a datalogging subscription, it must first be activated on the router. Go to Devices – SUBSCRIPTIONS – Activate. You will be given a choice of datalogging options including Trial (one free 30-day trial per company account), Standard (1K points per hour), Professional (5K points per hour), and High-Resolution (20K points per hour). Once you activate your subscription you may follow the instructions in this chapter to begin datalogging.

To Deactivate datalogging, you return to the same menu and select Deactivate. This will end your datalogging subscription on this router and permanently delete your data. It is recommended that you first save the data to your local machine before Deactivating. Once you have deactivated a router, the datalogging subscription will still be active and available to activate on another router. You will continue to be charged for its monthly use. If you wish to terminate the subscription from your company account, please refer to the Terminate Datalogging section below.

### Pause / Resume Datalogging

Once the data logger is configured and you are logging data, you may pause if you temporarily don't need to collect data (i.e. during periods of maintenance or scheduled downtime). To Pause data gathering, click on the ellipses in the Devices – SUBSCRIPTIONS page and select "Pause". If you plan to pause the data logging for a long period of time you may wish to push the changes to the router from the CONFIG tab so that the router will stop collecting data.

Once you are ready to resume data logging, simply select "Resume". If you had pushed the pause changes to the router, then you should proceed with pushing these changes as well.

### Terminating a Subscription

To terminate a subscription, navigate to the Billing – Subscriptions and "Edit Subscriptions". It is important to note that even though you may Deactivate a cloud data logging subscription, you must still terminate it or you will continue to be billed. You cannot terminate an activated data logging subscription. It must first be deactivated at the router and then can be terminated in the Billing – Subscriptions settings. You may want to continue the data logging subscription if you have data stored in the platform that you wish to remain active and available. Terminating your subscription will permanently erase the stored data. Be sure to save any data before permanently deleting it.



---

**WARNING: Data is only stored for as long as you maintain your paid subscription. ALL data will be lost if your subscription lapses or is terminated. Data for a specific device will be lost if a subscription is removed from that device. Data is also only stored for a maximum of 7 years. If data older than 7 years is important, please archive your data locally before the 7-year limit is reached.**

---

# CLOUD NOTIFY

---



## In this Chapter...

<b>Cloud Notify</b> .....	<b>5-3</b>
Why Cloud Notify?.....	5-3
How Does the Cloud Notify License Work? .....	5-3
Configure Cloud Notify On Your Device .....	5-3
Set Up Cloud Notify License.....	5-4
Set Up Data Sources For Alarm Notifications .....	5-5
Router Conditions for Alarm Notifications .....	5-10
Formatting the Alarm Notification Email .....	5-11
<b>Cloud Notify Web App</b> .....	<b>5-12</b>
Main Screen .....	5-12
Adding Alarms.....	5-13
Export Alarm Configurations .....	5-14
Managing Alarm Recipients.....	5-15
What Happens When an Alarm is Triggered? .....	5-16
Message Center.....	5-17
Configuring Your Mobile Device to Receive Push Notifications.....	5-19

**5**

This manual covers the StrideLinx platform available from 2017 through 2021.

For details covering the StrideLinx Cloud 2.0 platform available after April 2021, please [click here](#) to link to that manual.

The StrideLinx Cloud 2.0 manual includes details describing the [Activation Code](#) model of Data Logging, Cloud Notify and other add-on features.

For information on the migration wizard from the original platform to StrideLinx Cloud 2.0, [click here](#).

# Cloud Notify



**NOTE:** Model SE-SL3001 does not support notifications.

## Why Cloud Notify?

Cloud Notify allows you to receive notification of conditions occurring in your equipment. For instance, you can set alarms to be notified when your machine breaks down, needs maintenance or when a temperature runs too high. You can categorize notifications as low, medium or high priority, and receive only those notifications that are of importance to you.

## How Does the Cloud Notify License Work?

Cloud Notify is fully managed on the StrideLinX platform. There is no need to program or manually set up a PLC, router or any other device for notifications. This means you no longer have to worry about missing a notification due to an expired SIM card, problems with the internet connection, or SMTP servers.

Cloud Notify and the StrideLinX router work together seamlessly. Simply add a Cloud Notify license to your router on the StrideLinX platform, configure your triggers and the router will start monitoring your machine immediately.

Each Cloud Notify license is assignable to one router, and cannot be reassigned except that the license will still be active for that router if the router is transferred to another company. All Cloud Notify settings will be retained. A thirty day free trial is available prior to purchasing a license.



## Configure Cloud Notify On Your Device

Cloud Notify setup requires:

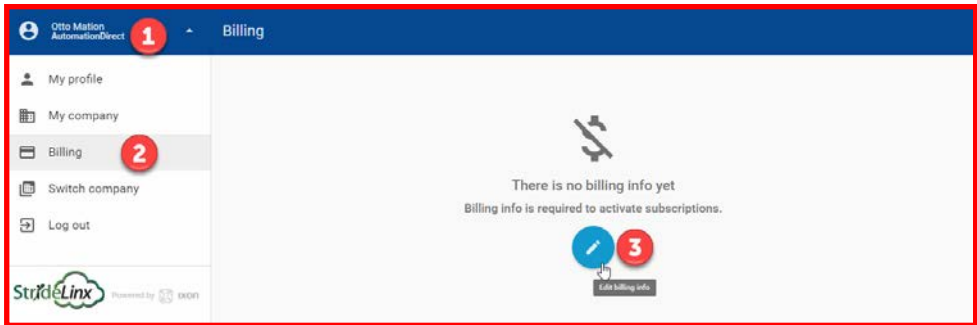
1. Set up Cloud Notify license.
2. Set up alarms for specific data variables in your connected equipment.
3. Select the priority level of alarm notifications to be sent to each user.

Each of these steps are detailed in this chapter.

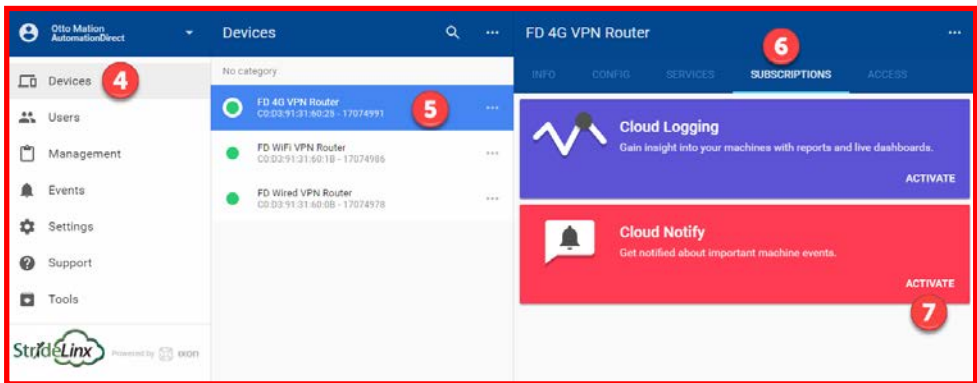
## Set Up Cloud Notify License

*Enter credit card information and subscribe to the Cloud Notify add-on service.*

Click the account name (1) to toggle the menu list and show the Billing option (2). Click Billing and click the Edit Billing Info icon (3) to enter credit card information.



Click on Devices (4), click the desired router (5), click the SUBSCRIPTIONS tab (6), then click ACTIVATE in the Cloud Notify section (7).



## Set Up Data Sources For Alarm Notifications

Both Data Logging and Cloud Notify use the same data source configuration tool. If data sources for Data Logging are already set up they can be used for Cloud Notify as well. If the data source and specific variables to be used to trigger alarms are not yet set up, then follow these steps. Otherwise, skip to the Cloud Notify Web App subsection later in this chapter.

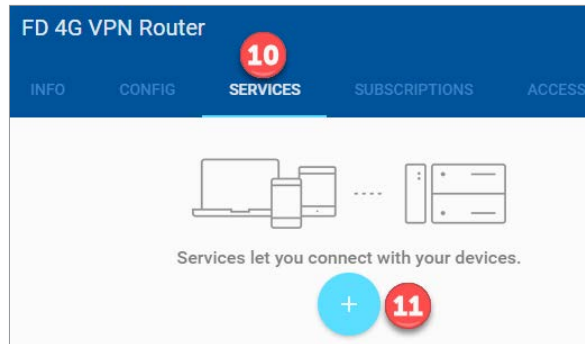


**NOTE:** This chapter uses Modbus protocol to illustrate data source configuration. Refer to Appendix G, H, I, J and K for Siemens S7, OPC UA, EtherNet/IP, BACnet, and MELSEC protocols, respectively.

5

### Configure the address and protocol for the PLC from which data will be read

Click on the SERVICES tab (10). Click the +(Add) button (11).



Add a Name and the IP Address of the PLC where the data resides. Click NEXT.

×
Add service

🏠
FD 4G VPN Router

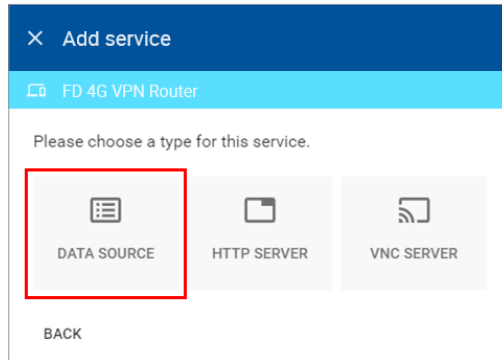
Please specify a target for this service.

Name

IP address   
e.g. 192.168.140.100

NEXT

Select DATA SOURCE.



×

 Add service

FD 4G VPN Router

Please choose a type for this service.



DATA SOURCE



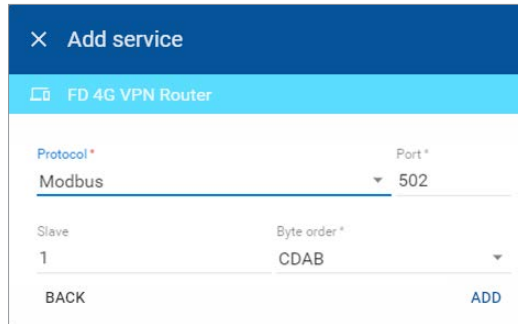
HTTP SERVER



VNC SERVER

BACK

Select the Modbus protocol. If the Port must be changed, or a Slave ID must be entered for the device from which data will be logged, enter those values, then click ADD to continue.



×

 Add service

FD 4G VPN Router

Protocol \*

Modbus

Port \*

502

Slave

1

Byte order \*

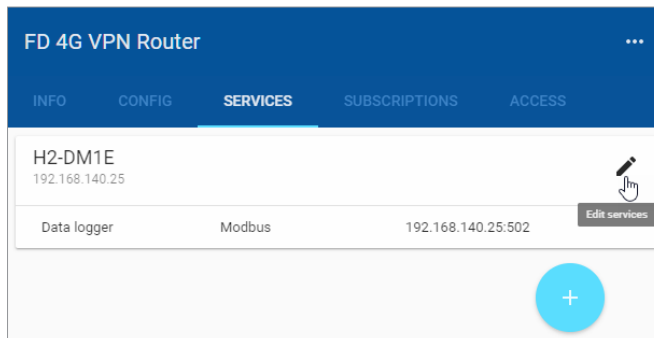
CDAB

BACK

ADD

### Configure the data tags

To add a data tag after steps 1 and 2 have been completed, go to the SERVICES tab for the router, and click the Edit services (pencil) icon next to the device for which you want to add the data tag.



FD 4G VPN Router

INFO CONFIG SERVICES SUBSCRIPTIONS ACCESS

H2-DM1E 192.168.140.25				
Data logger	Modbus	192.168.140.25:502		Edit services

+



This opens the Edit services dialog. Click the name of the existing device for which you would like to add a data tag.

× Edit services

FD 4G VPN Router

Name  
H2-DM1E

IP address  
192.168.140.25

Data logger  
192.168.140.25:502 Modbus 0

+ Add service

CANCEL DONE



**NOTE:** It is advisable to enter data tags in small batches, and test the variables periodically to verify the entries. The entries can be tested by clicking “RUN TEST” in the Configurator. Please refresh your browser if the information on screen appears to not be updated properly at any time.

The resulting “Edit service” screen displays the parameters for the data source, plus a count of existing data tags. Click OPEN CONFIGURATOR to add or edit tags.

← Edit service

FD 4G VPN Router

Protocol\* Port\*  
Modbus 502

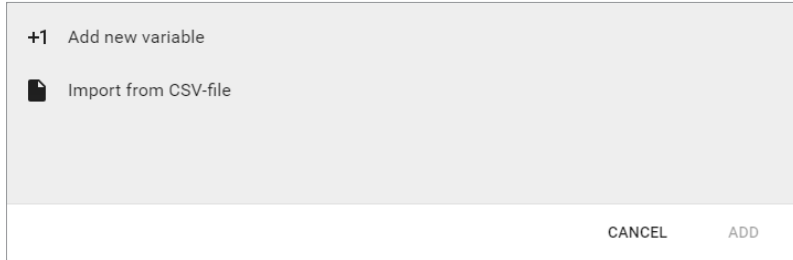
Slave Byte order\*  
1 CDAB

No variables

OPEN CONFIGURATOR

REMOVE CANCEL CONFIRM

Data tags can be entered interactively, or a set of tags can be imported from a previously-exported CSV file. Export of sets of data tags is discussed later in the “Export Data Tags” subsection. For this example, select “Add new variable” to manually enter tags.



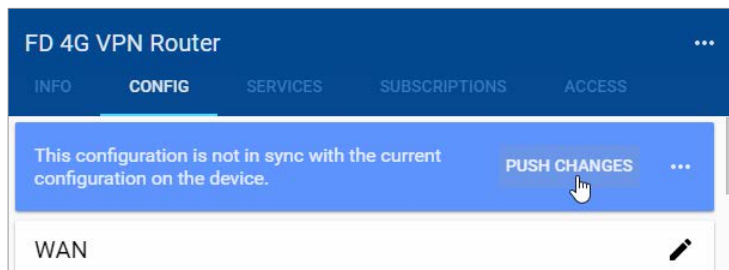
A data entry screen opens, with one new data tag ready to be entered. Set the relevant parameters for the new data tag. Additional data tags can be entered in this round by clicking “+1” in the lower left corner of the screen. When all the desired tags have been entered click ADD.

Data tag input fields are described in the following two tables. Also see the Modbus address translation chart in [Appendix D](#) for the key to enter addresses for AutomationDirect products. Refer to Appendix G, H, I, J and K for details on setting up Siemens S7, OPC UA, EtherNet/IP, BACnet and MELSEC protocols, respectively.

Data Tag Input Fields	
Field	Description
Name	Give the data tag a logical name.
Address	For Modbus protocol, the data tag address is the Modbus address (e.g., 412). Please see <a href="#">Appendix D</a> for address mapping for AutomationDirect PLCs.
Select a data type	See next table for the available data types.
Unit (optional)	Here you can assign a value to a unit, for example, gallons or psi.
Factor (optional)	This allows you to multiply by a value. For example, factor 0.01 divides the data value by 100.

Data Types Supported
Bool
Float32
Float64
Int8
Int16
Int32
Int64
UInt8
UInt16
UInt32
UInt64

Once you have added all the data tags you want to monitor, you will be prompted to push the configuration to the router.



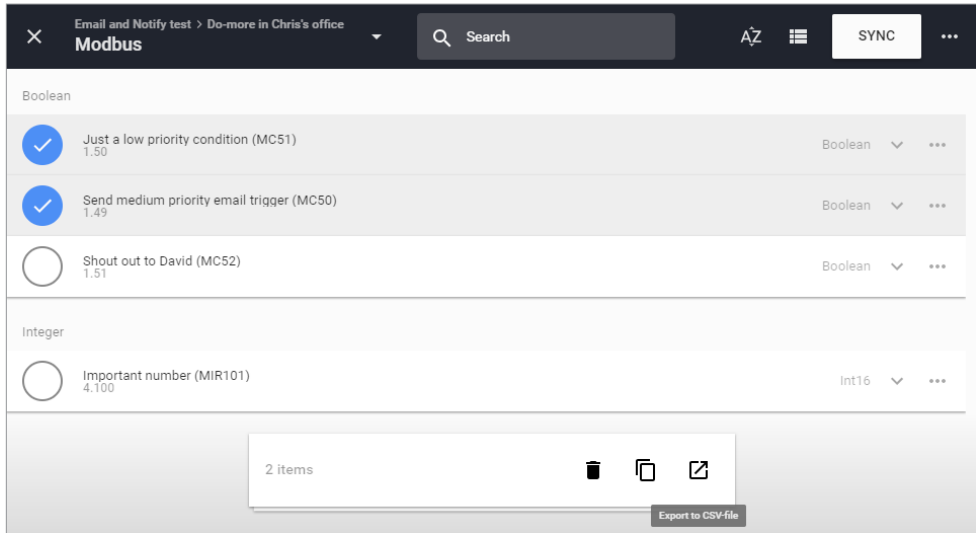
The Cloud Notify web app can now be used to set up alarm notifications using these data tags.

## Export data tags

Data tag configurations can be exported in CSV format. The CSV file is downloaded to your local PC, and can later be imported to set up another StrideLinX router.

Select data tags to be exported by clicking the icon for each data tag, or select all data tags at once from the More Options (⋮) menu in the upper right corner of the screen. The selected data tags can then be deleted, duplicated, or exported from the pop up menu at the bottom of the screen.

5



## Router Conditions for Alarm Notifications

The router itself may be a data source for events initiating notifications. The router appears on the Subscriptions > Cloud Notify device list as “Localhost.”

The conditions available to initiate a notification are:

- MQTT Connected (router online, connected to the cloud server)
- MQTT logger connected (data logging and/or cloud notify from the router to the cloud server is active)
- VPN connected (the router is connected via VPN to the cloud server)

Notifications based on these conditions may be configured to alert the receiver to activity by users or data usage on a cellular connection (typically when one of these conditions become TRUE), or perhaps when a router has lost internet service (when these conditions become FALSE).

## Formatting the Alarm Notification Email

The format of the timestamp in the heading of the email or message notifications is configured in My Profile > My localization settings, for each recipient of a message. The Localization setting controls the format of the time stamp (e.g., MM-DD-YY, DD-MM-YY, etc), and the timezone sets the offset from UTC. The alarm notification email will display time in the selected time zone, regardless of the time zone of the recipient email. Leaving timezone set as “Automatically” will display the time stamp as UTC.

The image shows two screenshots from a user interface. The top screenshot is the 'My profile' page for 'Otto Mation AutomationDirect'. It has a left sidebar with 'My profile', 'My company', 'Billing', 'Licences', 'Switch company', and 'Log out'. The main content area shows 'My info' (Full name: Otto Mation, E-mail address: otto@automationdirect.com) and 'My localization' (Language: English, Localization: English (United States), Timezone: (GMT-04:00) Eastern Time (US & Canada)). A 'My companies' section is at the bottom. Red circles highlight the user name, 'My profile', 'My localization', and an edit icon. Red arrows point from these circles to the 'Edit localization' dialog in the bottom screenshot.

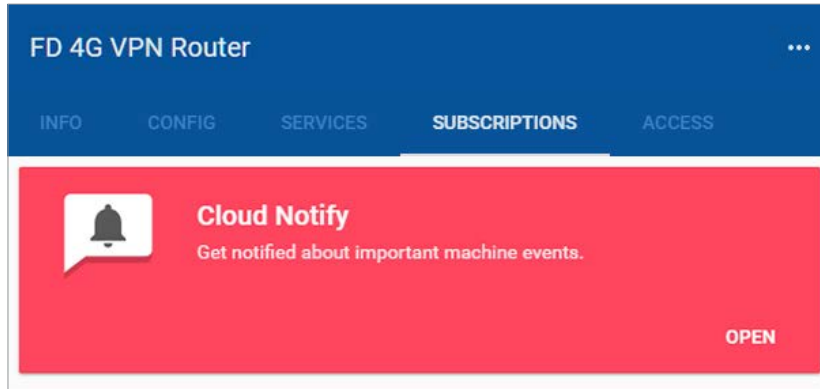
The bottom screenshot is the 'Edit localization' dialog for 'Otto Mation'. It has three dropdown menus: 'Select a language' (English), 'Select a localization' (Automatically), and 'Select a timezone' (Automatically). Red circles highlight the 'Automatically' options in the localization and timezone dropdowns. Red arrows point from these circles to the corresponding options in the list of localization and language options on the right.

The list of localization options includes: (GMT-05:00) Central Time (US & Canada), (GMT-05:00) Bogota, (GMT-05:00) Lima, (GMT-05:00) Quito, and (GMT-04:00) Eastern Time (US & Canada). The list of language options includes: English (United States), English (Zimbabwe), Afrikaans, Bahasa Indonesia, and Bahasa Melayu (Malaysia). At the bottom of the dialog are 'CANCEL' and 'CONFIRM' buttons.

## Cloud Notify Web App

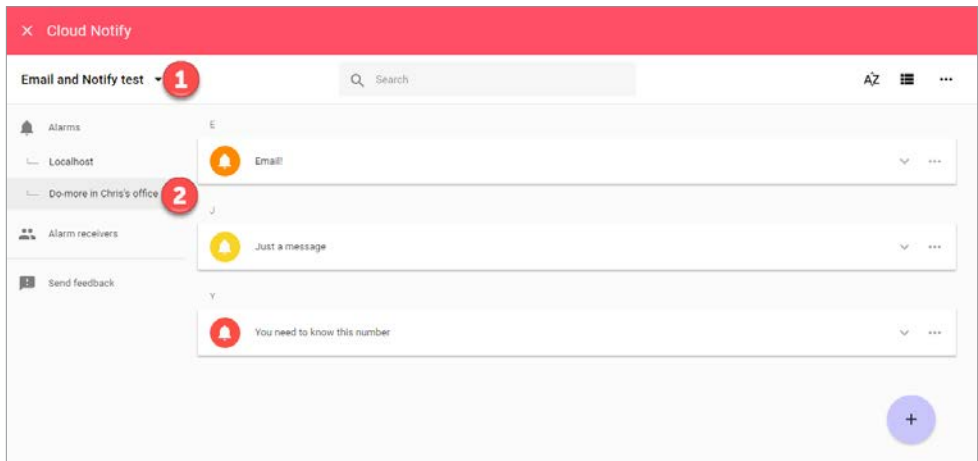
The Cloud Notify web app is found under the SUBSCRIPTIONS tab after selecting a StrideLinx device. Note that model SE-SL3001 does not support notifications.

5



### Main Screen

The web app provides a central location to manage your Cloud Notify alarm notifications and alarm recipients. To view or change the alarm notifications, (1) select a StrideLinx device with an active Cloud Notify license, then (2) select a data source on that device. The screen will then display the current list of configured alarm notifications.

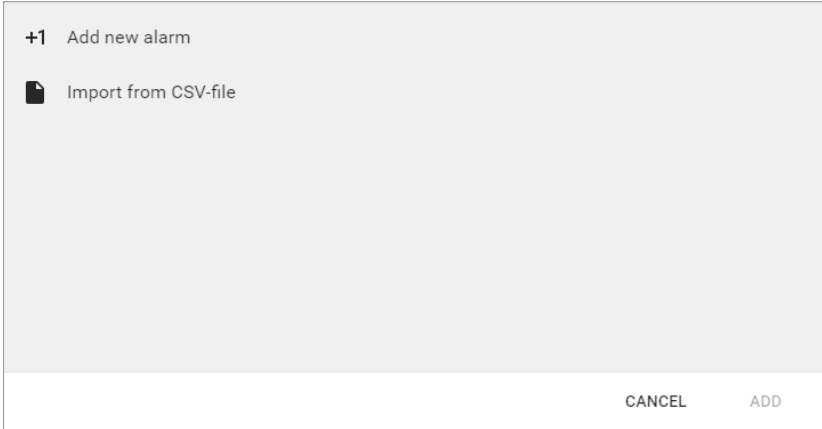


Click the downward chevron to the right of an alarm to display its details, or click the three dots to copy, delete, or select the alarm for export.

## Adding Alarms

To add a new alarm, click the “+” icon in the lower right corner.

Alarms can be entered interactively, or can be imported from a previously-exported CSV file. Export of sets of alarms is discussed later in this subsection. Importing a file will load the alarms to this screen, as if they had been manually entered. For this example, select “Add new alarm” to manually enter alarms.

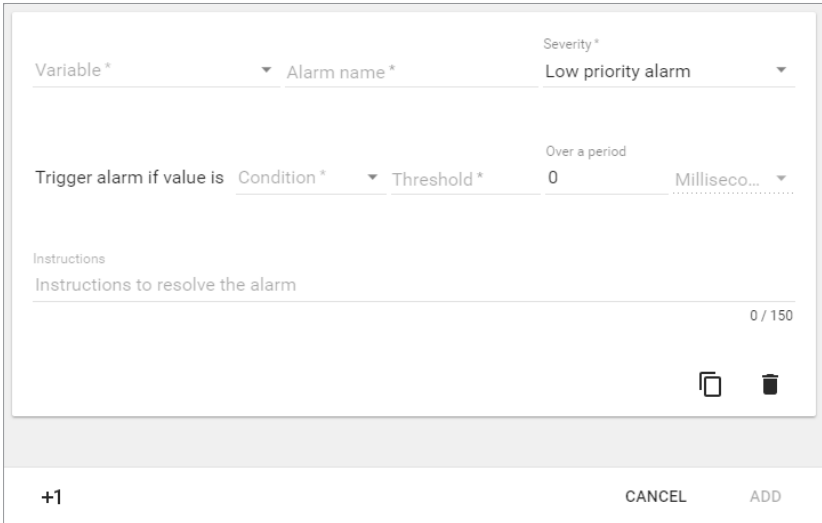


+1 Add new alarm

Import from CSV-file

CANCEL ADD

A new alarm dialog will be created, as shown below.



Variable \*    Alarm name \*    Severity \*  
Low priority alarm

Trigger alarm if value is    Condition \*    Threshold \*    Over a period  
0    Milliseco...

Instructions  
Instructions to resolve the alarm    0 / 150

+1    CANCEL    ADD

Enter the details for the new alarm. Each field is described in the following table.

Alarm Input Fields	
<i>Field</i>	<i>Description</i>
Variable	Select a variable from the current data source.
Alarm Name	Give the alarm a logical name.
Severity	Select Low, Medium or High priority. Used to filter which alarms notify each user.
Condition	Select a comparison condition (e.g., Equal to, Greater than, etc.). Available conditions are based on variable data type. The current value of the variable is compared to the value set in Threshold using the selected Condition.
Threshold	Enter the threshold value to which the current variable value will be compared.
Period	A time value and unit may be entered to require the variable to meet the trigger condition for the given time before the alarm is triggered.
Instructions	Enter a message that will be sent when the alarm is triggered. Maximum 150 characters.

The router status can also be used to trigger an alarm. The router status variables are included in the automatically generated “localhost” data source, as described below.

Localhost Data Source	
<i>Variable</i>	<i>Description</i>
MQTT connected	Router is online and connected to the cloud server
MQTT logger connected	Data logging and/or cloud notify from the router to the cloud server is active
VPN connected)	Router is connected via VPN to the cloud server

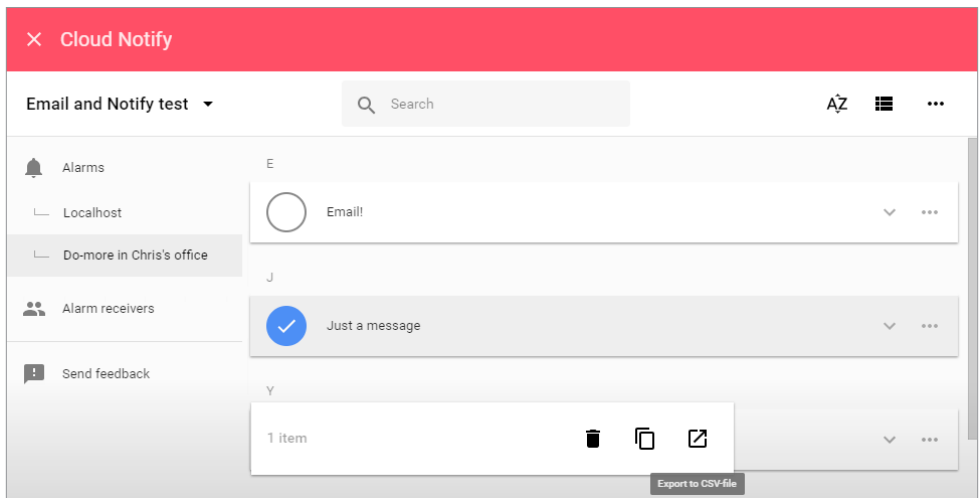
Additional alarms can be created by clicking “+1” or copying the existing entry. When all alarms have been entered click “ADD” in the lower right of the screen. The web app will return to its main screen, with the alarms displayed Each alarm’s icon is color coded to indicate its priority.

### Export Alarm Configurations

Alarm configurations can be exported in CSV format. The CSV file is downloaded to your local PC, and can later be imported to set up another device.

Select alarms to be exported by clicking the icon for each alarm, or select all alarms at once from the More Options (•••) menu in the upper right corner of the web app. The selected alarms can then be deleted, duplicated, or exported from the pop up menu at the bottom of the screen.

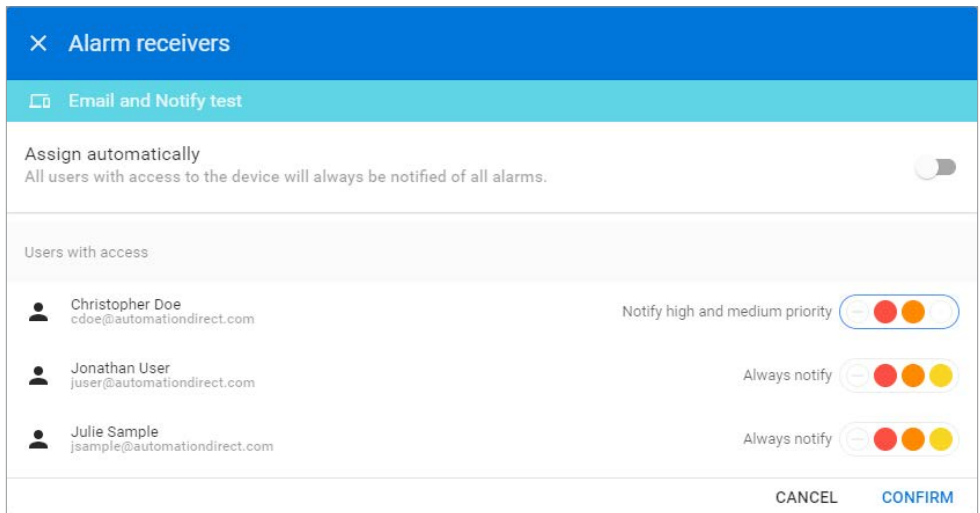




5

## Managing Alarm Recipients

Each user that is a member of this company within the StrideLinx platform can receive alarm notifications at or above a selected priority. To edit the notification levels for each user, click Alarm Receivers on the main web app screen.



By default all users are set to receive all alarm notifications. To assign notification levels to individual users, turn off “Assign automatically,” which will then initially set all users to

receive no notifications. Select the lowest priority alarm to be received by each user, and click CONFIRM. The users will receive all alarms at the selected priority or higher.

Each user can fine tune email notifications for specific alarms by creating filters in the Message Center, as discussed in the “Message Center” subsection later in this chapter.

### What Happens When an Alarm is Triggered?

When the trigger condition for an alarm is met, a notification is sent to the relevant group of users and the alarm is archived in the Message Center on the main StrideLinx platform page.



**NOTE:** A maximum of 10 notifications will be sent within a 5 minute period for each alarm. Subsequent notifications will be dropped until the 5 minute window has expired. Notifications will continue for other alarms occurring within the 5 minute period.

The alarm notification will be sent to the user’s email address as configured on the Users tab of the StrideLinx platform, and a push notification will be sent to the user’s mobile device if the iOS or Android mobile app is installed and configured to accept notifications. Email and push notifications can each be disabled for individual alarms using Message Filtering. The notification includes:

- the Alarm Name
- the date and time the alarm was triggered
- the name and Device ID of the StrideLinx router
- the alarm’s Instructions message

as well as custom branding elements and the subscribed email address. A sample notification email is shown below.

The image shows a sample notification email with various parts highlighted by red boxes and lines pointing to labels on the right. The email content includes:

- Company Logo (Custom Branding):** Automation Direct logo.
- VPN Router Name:** Email and Notify test
- Date and Time of Alarm:** 8/1/18, 7:26 PM UTC
- Alarm Name:** Just a message of [VPN Router Name] went off on [Date and Time of Alarm]
- Alarm Instructions:** Instructions: This is a low priority alarm. It will go to Jonathan and Julie, but not Chris. this is so easy to enter, I'll send a million notifications.
- VPN Router Name & Device ID:** Device ID: FkPFSYqqaW07; Device name: Email and Notify test
- Company Name:** ADC
- Custom URL (Premium Branding):** You are signed up for [Custom URL]
- Subscribed Email Address:** [Subscribed Email Address]

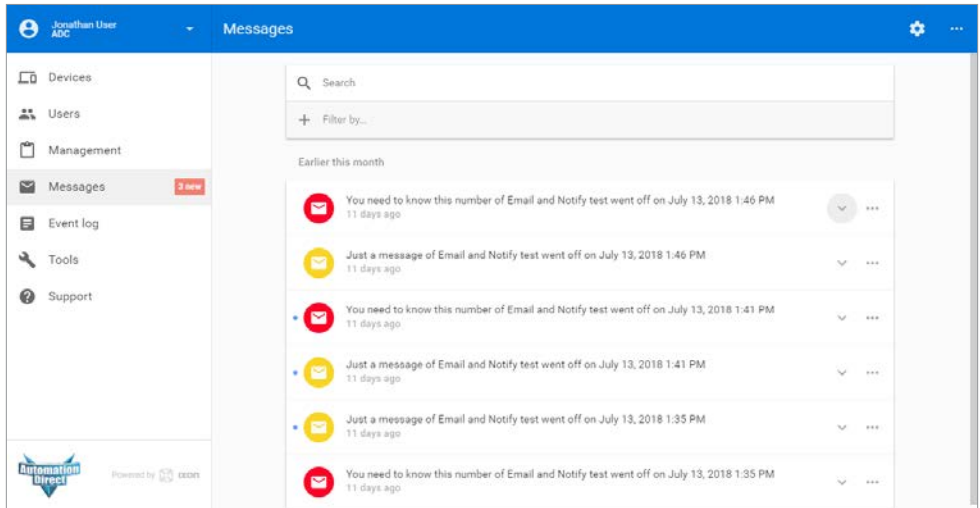
At the bottom, it says "Powered by ixon".

## Message Center




### *Message Archive*

The Message Center collects messages from all companies of which the user is a member, and can be viewed and searched from the Messages tab on the main StrideLinX platform page. All messages are viewable regardless of which company is currently connected.

Messages are stored on the StrideLinX platform for six months.



The archived messages contain the same information as the email notification and remain available for six months.

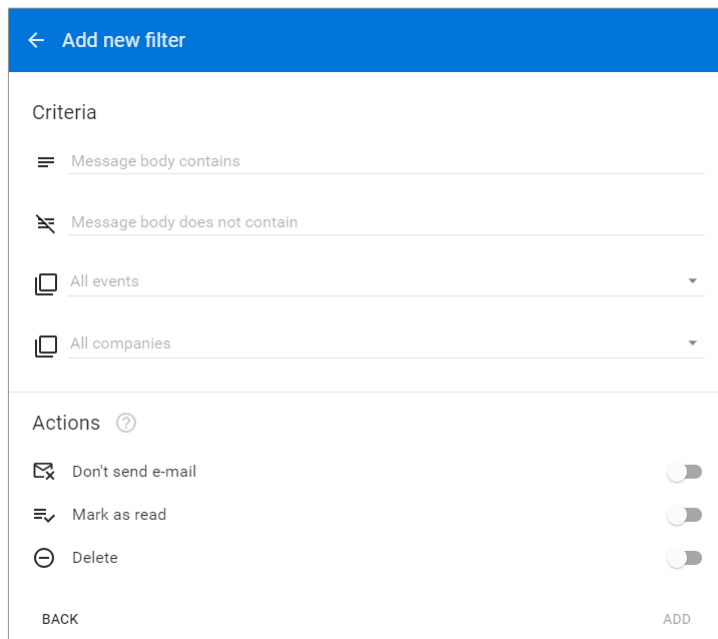
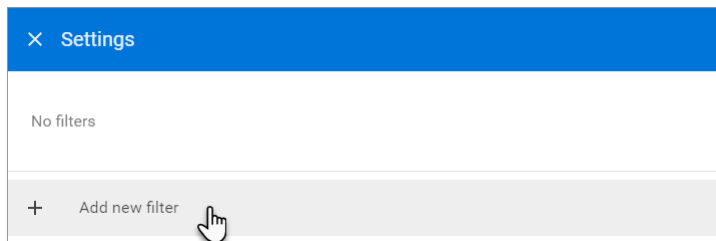
	You need to know this number of Email and Notify test went off on July 13, 2018 1:46 PM 11 days ago	 
Received on	07/13/2018 1:46:29 PM	
Message	Instructions: This number has lasted more than a second!	
Device ID	FkPFSYqoaW07	
Device name	Email and Notify test	
Company	<span>ADC</span>	
Event	<span>High priority alarm</span>	

To search for specific messages, enter any text in the search box. The entire message is searched, including all fields, and the results update dynamically as you type. The results may also be filtered by company name or message priority.

### Message Filtering

Message filters can be created to perform actions on messages meeting preset criteria. To create a filter, click the Settings (gear) icon in the upper right of the Message Center, then click “Add new filter.” After entering the filter details, click ADD to save the filter.

5



*Criteria*

- **Message body contains** – Matching messages must contain this text. All text from all fields of the message is used in this criteria, as formatted in the message.
- **Message body does not contain** – Matching messages must not contain this text. All text from all fields of the message is used in this criteria, as formatted in the message.
- **Events** – Any combination of Low, Medium or High Priority alarms, or Device Transfer, can be selected to match.
- **Companies** – A subset of companies in which the user is a member can be selected.

*Actions*

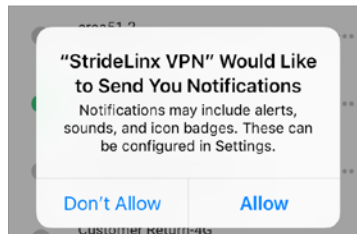
- **Don't send e-mail** – Allows a user to receive the alarm in the Message Center without receiving e-mails.
- **Don't send push notification** – Allows a user to receive the alarm in the Message Center without receiving push notifications to a mobile device.
- **Mark as read** – Mark matching messages as read on arrival in the Message Center.
- **Delete** – Matching messages are deleted from the Message Center on arrival.

**Configuring Your Mobile Device to Receive Push Notifications**

The method for configuring push notifications on your device may vary by device manufacturer and operating system version. We provide here examples for iOS and Android devices, but please consult the documentation on your device if the following procedures do not match your device.

*Push Notification on iOS*

When the StrideLinx app is first installed on your iOS device, you may be asked to allow notifications from the app. If you select “Allow” at this step, your device will be added to the list of push devices on your StrideLinx account once you log into the app.



If you didn't allow notifications initially and want to enable them later, tap Settings on your device, tap Notifications, select StrideLinx VPN, then toggle “Allow Notifications.” This settings dialog may also allow you to fine tune how notifications appear on your device.

Your device will now appear in the “My push devices” section of the “My profile” screen in the StrideLinx platform and will receive push notifications by default.

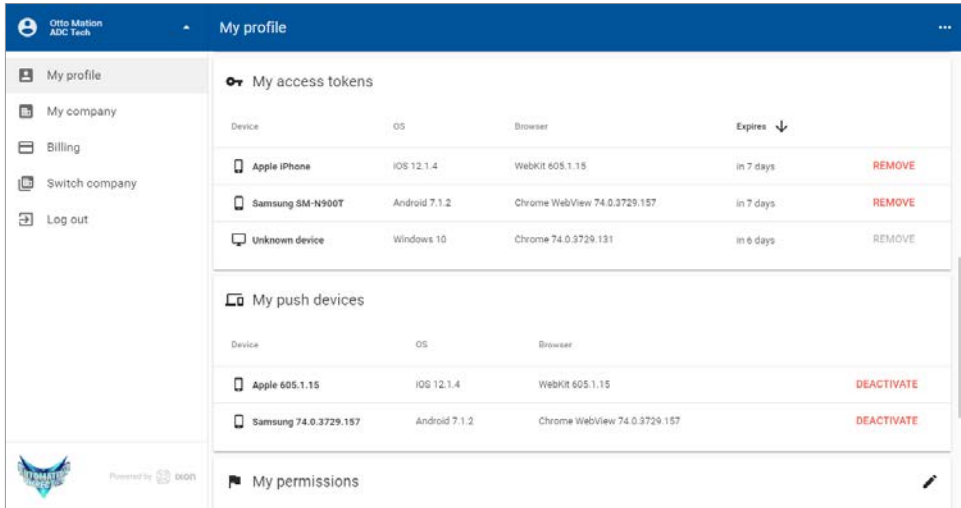
## Push Notification on Android

When the StrideLinx app is first installed on your Android device, the device may apply your default settings for app notifications. To check or change these settings, you will typically open Settings, tap Notifications, then select StrideLinx VPN. From the subsequent screen, you can allow notifications and set the details of how the StrideLinx app notifications will appear on your device. The specifics of this screen will be device and OS version dependent.

Your device will now appear in the “My push devices” section of the “My profile” screen in the StrideLinx platform and will receive push notifications by default.

## View the List of Configured Push Devices on the StrideLinx Platform

You can verify that a device is set to receive push notifications by checking the “My push devices” list on the StrideLinx platform, found by clicking your user name in the upper left, then clicking “My profile.” A device can be deactivated from receiving any push notifications by selecting DEACTIVATE on this screen.



# ACCESSORIES & ADD-ON SUBSCRIPTIONS

---



## In this Appendix...

<b>Antennas</b> .....	<b>A-3</b>
4G LTE Antennas (for P/N SE-SL3011-4G and SE-SL3011-4GG) .....	A-3
WiFi Antennas, IEEE 802.11 b/g/n 2.4 GHz (for P/N SE-SL3011-WF).....	A-4
<b>Add-on Subscriptions &amp; Licenses</b> .....	<b>A-5</b>
Service Level Agreement .....	A-6
Cloud Logging .....	A-6
Cloud Notify .....	A-7
Data Top-up.....	A-7
Premium Branding .....	A-7

This manual covers the StrideLinx platform available from 2017 through 2021.

For details covering the StrideLinx Cloud 2.0 platform available after April 2021, please [click here](#) to link to that manual.

The StrideLinx Cloud 2.0 manual includes details describing the [Activation Code](#) model of Data Logging, Cloud Notify and other add-on features.

For information on the migration wizard from the original platform to StrideLinx Cloud 2.0, [click here](#).



## Antennas

The WiFi and 4G LTE variants of the StrideLinx VPN Router require external antennas to improve signal strength. The 4G LTE antennas use a standard SMA screw antenna connector, and the WiFi antennas use an RP-SMA screw antenna connector.

Several antenna options are available, as follows.

### 4G LTE Antennas (for P/N SE-SL3011-4G and SE-SL3011-4GG)

STRIDE 4G LTE antennas are available in three versions, providing direct connection, magnetic mount, and panel mount options.

Note: Two antennas will provide best performance, including improved and more predictable throughput and improved resistance to interference. If only one antenna is connected to the router, it must be connected to the MAIN antenna connector, closer to the front of the router.



STRIDE whip/tilt LTE antenna, connector mount.



STRIDE whip/straight LTE antenna, magnetic base mount, 9.8ft/3m cable length.



STRIDE dome LTE antenna, IP67, panel mount, 9.8ft/3m cable length.

4G LTE Antenna Specifications			
	SE-ANT110	SE-ANT130*	SE-ANT150
Fits	SE-SL3011-4G and SE-SL3011-4GG		
Antenna Connector	SMA (M)		
Application	LTE, CDMA, GSM, HSPA, UMTS		
Impedance	50Ω		
Antenna Type	whip, tilt	whip, straight	dome
Cable Length	N/A	3m [9.8 ft]	3m [9.8 ft]
Frequency Range	700–960MHz / 1.71–3.8 GHz	700–960MHz / 1.71–3.5 GHz	700–960MHz / 1.71–2.7 GHz
Gain	-3.0 dBi / 0.9 dBi	-2.5dBi / 0.1dBi	1.2 dBi / 3.2 dBi
Height	2.84 in	13 in	1.89 in
IP Rating	–	–	IP67
Maximum Power	10W	50W	5W
Mounting Screw Torque	NA	NA	2.94 N·m

\* Gains listed are based on the antenna being mounted on a suitable ground plane.



## WiFi Antennas, IEEE 802.11 b/g/n 2.4 GHz (for P/N SE-SL3011-WF)

STRIDE WiFi antennas are available in two versions, providing direct connection and panel mount options.



STRIDE whip/straight 2.4 GHz WiFi antenna, IP65, connector mount.



STRIDE dome 2.4 GHz WiFi antenna, IP67, panel mount, 9.8ft/3m cable length.

802.11 b/g/n 2.4 GHz WiFi Antenna Specifications		
	SE-ANT210	SE-ANT250
Fits	SE-SL3011-WF	
Antenna Connector	RP-SMA (M)	
Application	802.11 b/g/n	
Impedance	50Ω	
Antenna Type	whip, straight	dome
Cable Length	NA	3m [9.8 ft]
Frequency Range	2.4–2.5 GHz	2.4–2.5 GHz
Gain	1.8 dBi	1.5 dBi
Height	1.2 in	1.89 in
IP Rating	IP65	IP67
Maximum Power	1W	5W
Mounting Screw Torque	NA	2.94 N·m

**A**

## Add-on Subscriptions & Licenses

These subscriptions and licenses provide added services to your StrideLinX remote access. These are not needed for the basic function of the VPN remote access, but can be added to enhance the value of the platform to you and your customers.



**NOTE:** Model SE-SL3001 does not support Cloud Logging subscriptions or Cloud Notify license.

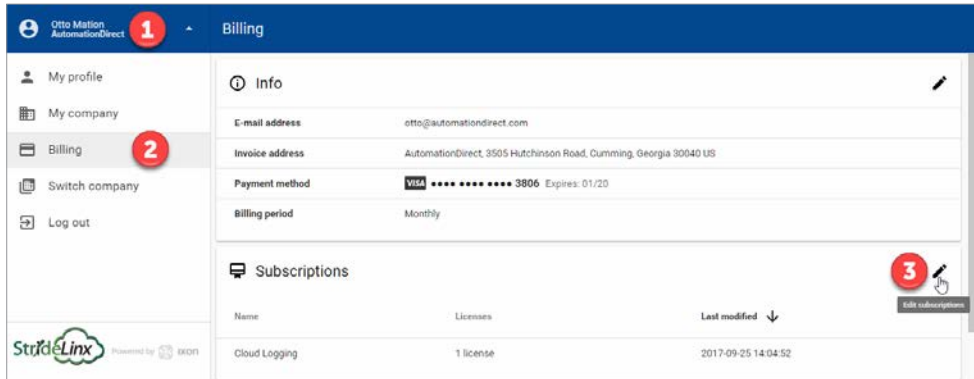
StrideLinX Add-on Subscriptions & Licenses		
Part #	Description	Features
<b>SE-SL001</b>	Service Level Agreement (SLA)	99.6% availability, 4-hour max consecutive downtime. For use with one StrideLinX company.
<b>SE-SL010*</b>	Cloud Logging, Standard Data logging enabled at 1,000 data samples per hour	Unlimited cloud storage for up to 7 years with active subscription, unlimited real time and user configurable dashboards, unlimited data reports, unlimited data tags, Modbus, EtherNet/IP, Siemens S7 and OPC UA protocol support  For use with one StrideLinX company.  Data logging traffic does not affect monthly data usage (5 GB free or Data Top-up subscriptions).
<b>SE-SL011*</b>	Cloud Logging, Professional Data logging enabled at 5,000 data samples per hour	
<b>SE-SL012*</b>	Cloud Logging, High Resolution Data logging enabled at 20,000 data samples per hour	
<b>SE-SL020*</b>	Cloud Notify License	Prioritized push and email notifications for lost device connections and customized trigger conditions. Supports Modbus, EtherNet/IP, Siemens S7 and OPC-UA protocols. For use with one StrideLinX router.
<b>SE-SL030</b>	Data Top-up, 5GB	Additional monthly data traffic. For use with one StrideLinX company.
<b>SE-SL031</b>	Data Top-up, 15GB	
<b>SE-SL032</b>	Data Top-up, 50GB	
<b>SE-SL040</b>	Premium Branding License	Includes rebranded StrideLinX platform with custom company domain and contact/support information. For use with one StrideLinX company.

\* Model SE-SL3001 does not support Cloud Logging subscriptions or Cloud Notify License.

All add-on subscriptions and licenses are available at [www.StrideLinX.com](http://www.StrideLinX.com). Log into your account for all subscription purchases, upgrades, and cancellations.



To order a subscription, credit card information must be added to your account on the Billing page. Subscriptions can be purchased from the Billing page by (1) clicking your user name, (2) clicking Billing, and (3) clicking the “Edit subscription” (pencil) icon under “Subscriptions”. Cloud data logging subscriptions (and 30-day free trials) may also be added by clicking on a device and selecting SUBSCRIPTIONS on the third-tier menu.



To terminate a subscription, navigate to Billing–Subscriptions and “Edit Subscriptions”. It is important to note that even though you may Deactivate a cloud data logging subscription, you must still terminate it or you will continue to be billed. You cannot terminate an activated data logging subscription. It must first be deactivated at the router and then can be terminated in the Billing–Subscriptions settings. You may want to continue the data logging subscription to easily transfer the datalogging license to other routers in your company. Deactivating or terminating your subscription will permanently erase the stored data. Be sure to save any data before permanently deleting it.

All subscriptions can be purchased on a recurring monthly or annual basis. Annual purchases receive a free month of subscription. Subscriptions are automatically renewed until they are canceled. There is no prorating or refunds on subscription services.

Add Data top-up and SLA subscriptions from the Subscription Edit link (3) shown in the previous screenshot.

## Service Level Agreement

Our services are normally provided as is and on a best-effort basis. However, for customers who prefer a specific level of service a Service Level Agreement (SLA) is available for an additional fee. The SLA provides guarantees of 99.6% availability and 4-hour maximum consecutive downtime per router. Full terms of the agreement are available for download from the Subscription Edit link discussed previously.

## Cloud Logging

The Cloud Logging subscription is a completely cloud-based solution for gathering remote data from your control components. All the values you have programmed in the PLC can be logged by the StrideLinx logger, easily and securely. All Cloud Logging subscriptions offer unlimited

live monitoring and historical data reporting dashboards, with unlimited number of data tags and unlimited storage for up to 7 years.

### Cloud Notify

Cloud Notify allows you to receive notification of conditions occurring in your equipment. For instance, you can set alarms to be notified when your machine breaks down, needs maintenance or when a temperature runs too high. You can categorize notifications as low, medium or high priority, and receive only those notifications that are of importance to you.

Cloud Notify and the StrideLinx router work together seamlessly. Simply add a Cloud Notify license to a router on the StrideLinx platform, configure your triggers and the router will start monitoring your machine immediately.

Each Cloud Notify license is assignable to one router, and cannot be reassigned except that the license will still be active for that router if the router is transferred to another company. All Cloud Notify settings will be retained.

### Data Top-up

The intended use of the StrideLinx platform is secure remote access to industrial control equipment for remote service. A monthly allowance of 5GB data traffic per company account is included, and is sufficient in most cases to accomplish remote service.

When the platform is used for other purposes, the data traffic may exceed the 5GB allowance. The StrideLinx platform includes optional Data Top-up subscriptions to increase the monthly limit by an additional 5GB (SE-SL030), an additional 15GB (SE-SL031) or an additional 50GB (SE-SL032)

If the data traffic for a company reaches the monthly limit, further data traffic will be throttled to 50kbit/sec. This is adequate to access and program a PLC.

Although data usage is affected by the number of users accessing the platform, we expect the most significant data usage to be from an IP camera connected on the platform.

Any Cloud Logging subscription data does not count toward the data traffic allowance and is not subject to throttling.

### Premium Branding

The StrideLinx premium branding license extends the level of customization available on the StrideLinx platform. The license includes rebranding of the StrideLinx platform with a custom company domain and contact/support information.

Premium branding can be purchased and activated from the My Company page.

See Appendix L for more detail on Premium Branding features.

# TROUBLESHOOTING

---



## In this Appendix...

Troubleshooting Overview .....	B-3
<b>My StrideLinx Router Doesn't Come Online .....</b>	<b>B-3</b>
Internet Connection .....	B-3
Connectivity .....	B-3
Network Settings.....	B-3
Configuration.....	B-3
StrideLinx Router Log File.....	B-5
<b>I Can't Connect to the StrideLinx Router .....</b>	<b>B-5</b>
VPN Client .....	B-5
TAP Adapter .....	B-5
VPN Client Log File .....	B-6
<b>I Can't Connect to My Device(s) Behind the StrideLinx Router .....</b>	<b>B-6</b>
VPN Connection.....	B-6
IP Range.....	B-6
Default Gateway.....	B-6
Timeout Setting .....	B-6
Programming Software Does Not Allow Multiple Programming Connections .....	B-6
I Don't Know How to Configure My Device .....	B-6
I Am Unable to Configure My Device.....	B-7
Check Your Settings .....	B-7
I Still Can't Connect to My Device .....	B-7
<b>I Can't Connect to My HTTP/VNC Server.....</b>	<b>B-7</b>
Accessibility .....	B-7
HTTP/VNC Server.....	B-7
Password .....	B-7
StrideLinx Router Settings .....	B-7
Specific Service and Server Settings.....	B-8
<b>Wireless Connectivity .....</b>	<b>B-8</b>

This manual covers the StrideLinx platform available from 2017 through 2021.

For details covering the StrideLinx Cloud 2.0 platform available after April 2021, please [click here](#) to link to that manual.

The StrideLinx Cloud 2.0 manual includes details describing the [Activation Code](#) model of Data Logging, Cloud Notify and other add-on features.

For information on the migration wizard from the original platform to StrideLinx Cloud 2.0, [click here](#).

## Troubleshooting Overview

A video providing a troubleshooting overview is accessible by clicking the thumbnail at the right, or by copying the following URL to your browser:

<https://www.AutomationDirect.com/VID-CM-0029>



## My StrideLinx Router Doesn't Come Online



**NOTE:** The ACT and SIGNAL LEDs always display the active status of the router. See the [LED Status Indicators](#) section in Chapter 1 to review the status descriptions and help identify the problem.

### Internet Connection

Make sure that the StrideLinx router is connected to the internet, via an Ethernet cable, WiFi signal or 4G cellular signal.

Make sure your cellular 4G SIM card is activated by the carrier.

### Connectivity

Make sure that the router can connect to our servers. The [connectivity requirements](#) section in Chapter 1 explains how the StrideLinx router connects to our servers.

### Network Settings

Make sure that the router's LAN and WAN IP addresses are in different subnets. This isn't typically a problem if the default WAN DHCP settings are used.

### Configuration

Make sure that the StrideLinx router has been configured properly. The name of the configuration file must be `ixrouter.conf` and it needs to be placed in the root directory of a USB stick. Once placed in the router, the ACT light should blink fast (blue) for 20–30 seconds, indicating that it's running the registration procedure. If this doesn't happen and you've followed the instructions, you may try a different USB stick.



**NOTE:** It's best practice to remove the config file from the USB after the router has been registered so that on power up the router boots from the current configuration rather than the initial configuration.

### Proxy

If the internet connection uses a proxy, you'll have to configure the StrideLinx router accordingly. You do this during the creation of your WAN configuration file by clicking SHOW MORE in the top right of the "WAN" page, as is described in the ["Registering your Device"](#) section of Chapter 2. Contact the local IT department for details on the proxy server.

### Configuring the SE-SL3011-4G or SE-SL3011-4GG Router for a New SIM Card

If you're reconfiguring your router with a different SIM card than before, make sure that:

1. The router is powered OFF when switching the SIM cards, as removing a SIM card from a powered device may cause problems.
2. The new SIM card was inserted before starting the router, otherwise it doesn't recognize the new SIM card.



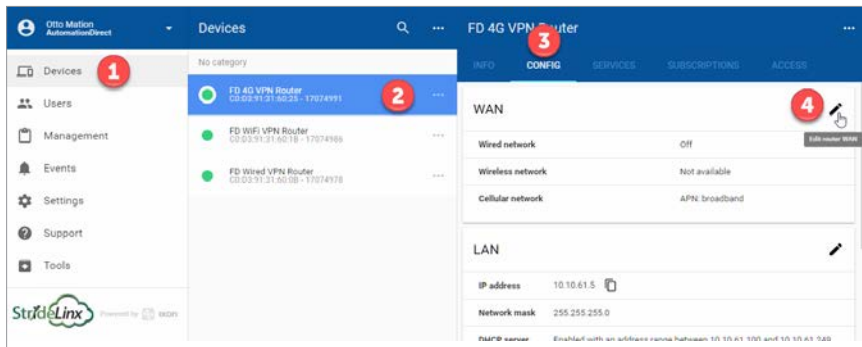
## Switching Your WAN Configuration from Wired to WiFi/4G and Vice Versa

The internet connection method can be changed for a WiFi or 4G StrideLinX router from the StrideLinX platform. Before changing the connection method, make sure the new connection method is available to the router (e.g., Ethernet cable is connected, WiFi network is available, SIM card is inserted, antennas are connected). Remember that if the new connection method to the router is not available, access to the router will be lost and the router will need to be defaulted and reconfigured.

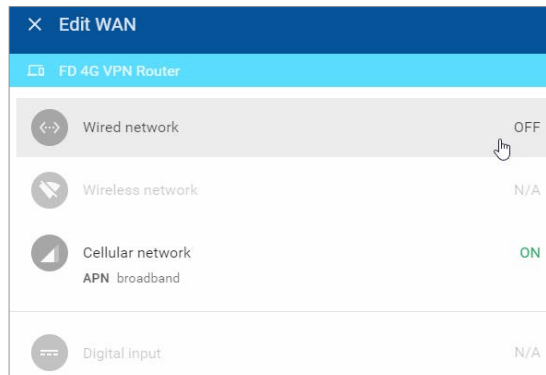


**WARNING: DO NOT insert or remove the SIM card when power is applied to the router.**

To begin, select Devices from the first-tier menu (1), select the router to be configured in the second-tier menu (2), select the CONFIG tab in the third-tier menu (3), and then click the pencil icon in the “WAN” (4).



An “Edit WAN” dialog opens, as shown below.

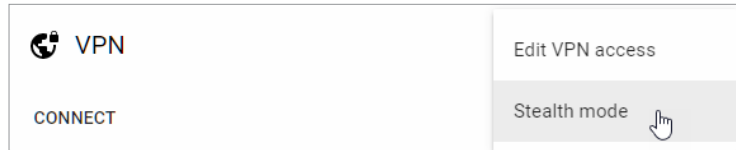


Click the desired WAN connection method to turn it on. A configuration dialog for the selected WAN connection method will open. Enter the relevant configuration parameters as discussed in the “[Configure the Internet Settings](#)” subsection of Chapter 2.

Finally, from the CONFIG tab push the changes to the router.

### *Country-wide Censored Internet Accessibility?*

If your StrideLinx router is located in China or another country with censored internet accessibility, you need to turn on the “censoring” option to have your router be able to set up a VPN connection to our StrideLinx servers. You can find this setting on the respective StrideLinx router’s info page by clicking the ellipsis in the VPN section and selecting “Stealth mode”, as is depicted below. The configuration change will be automatically pushed to the router if it is online, or the next time it connects to the StrideLinx Platform.



### **StrideLinx Router Log File**

The log file can be obtained by placing a USB stick (without a config file) in the StrideLinx router and removing it after 10 seconds. If you just rebooted the router it is best to wait at least 3 minutes before removing the USB stick to be sure that the router has gone through all the necessary steps. With this log file we can further investigate your issue.

## **I Can't Connect to the StrideLinx Router**

### **VPN Client**

Make sure you have installed the VPN Client. The [Installing the VPN Client](#) section of Chapter 2 explains the installation.

Once you've installed the VPN Client, refresh the StrideLinx Platform page to have it re-check for the VPN Client to see if it's installed.

### *Proxy*

If you're behind a proxy the VPN Client will try to automatically detect the necessary settings. In case the VPN Client is unable to do so, you may have to manually enter the address, port, login and password in your VPN Client's settings. Contact your local IT department for this information.

### **TAP Adapter**

Make sure that the TAP adapter (installed with the VPN Client) isn't disabled and that an older version (< version 9) has not been installed after installing the VPN Client. You can check this in Windows at: Control Panel\Network and Internet\Network Connections.

### *VPN Connection*

In Windows you can only have one active VPN connection at a time. If you get disconnected shortly after connecting to your StrideLinx router it is possible you already have a VPN connection active.

Simplify the connection. For example, connect directly to the internet rather than connecting through an office VPN, and connect to the internet using a Windows PC rather than a virtual Windows machine on a Mac.

### **VPN Client Log File**

On a Windows PC you can find the VPN Client log files at “C:\ProgramData\StrideLinx\VPN Client\Logs”. Usually, the most recent log file is the most relevant. With this log file we can further investigate your issue.

## **I Can't Connect to My Device(s) Behind the StrideLinx Router**

### **VPN Connection**

Make sure that you are connected to the StrideLinx router. As a check you can try to ping the router's VPN address or LAN-side IP address. If you don't get a reply, but the website says you're connected, close and restart the VPN Client and attempt to connect again.

Simplify the connection. Connect directly to the internet rather than connecting through an office VPN, for example. Connect to the internet using a Windows PC rather than a virtual Windows machine on a Mac, for example.

### **IP Range**

Make sure that your device's IP address is in the same range as the StrideLinx router and that the subnet mask is the same as the router, which is usually 255.255.255.0.

### **Default Gateway**

Make sure that your device is configured with a default gateway. This setting can also just be named “gateway” or something along the lines of “use router”. The default gateway needs to be set to the IP address of the StrideLinx router.

### **Timeout Setting**

Increase the timeout setting to allow sufficient time for the internet connection. For testing, set this to the maximum timeout. If the problem is not the timeout, a maximum setting will cause the failure response to take a very long time (over a minute).

### **Programming Software Does Not Allow Multiple Programming Connections**

Most programming software will only allow a single user to be connected to and programming a device at a time. Make sure no other users are programming the device.

### **I Don't Know How to Configure My Device**

If you don't know how to configure your device for connection through the StrideLinx VPN, you can consult our connection examples in Chapter 3.

## I Am Unable to Configure My Device

If you are unable to configure your device, you can set “no gateway configured” in the LAN configuration of your StrideLinX router. Go to the StrideLinX Platform, select your router, go to the CONFIG tab, click on the pencil icon in the top right corner of the LAN settings, and click SHOW MORE in the newly opened window to change the advanced LAN settings.



**NOTE:** The “No gateway configured” setting should only be used as a last resort. In some cases it may cause unexpected behavior. We recommend to always properly configure your device with a default gateway if you want to access it remotely.

## Check Your Settings

You can check if your device is properly configured by pinging its IP address once you’ve set up a VPN connection to your StrideLinX router.



**NOTE:** Pinging a PC? A PC may have firewall rules that block your inbound ping request. Resulting in you not receiving a reply and thus not being able to check if you can access the PC remotely. If possible, you could enable the following inbound firewall rules on that PC:

- All ICMP V4
- File and Printer Sharing (Echo Request - ICMPv4-In).

## I Still Can’t Connect to My Device

If you receive a reply in the ping check above, but are still unable to connect to your device, the issue may reside in the (development) software that you are using to connect. In this case you can consult our connection examples in Chapter 3 or contact the manufacturer.

## I Can’t Connect to My HTTP/VNC Server

### Accessibility

Make sure you can reach your device. You can check this by pinging its IP address once you’ve set up a VPN connection to your StrideLinX router. If you do not receive a reply, please follow the steps explained above under “I can’t connect to my device(s) behind the StrideLinX router.”

### HTTP/VNC Server

Make sure there is an HTTP or VNC server running on your device. You can check this by establishing a VPN connection to your StrideLinX router and:

- In case of an HTTP server, type the IP address of your device in your browser.
- In case of a VNC server, connect using a 3rd party VNC viewer (e.g. RealVNC).

### Password

There may be a password set on the device. This can usually be checked on the device itself.

### StrideLinX Router Settings

Make sure the router settings are properly configured, including a password if applicable, if you’re trying to access the HTTP/VNC server directly via [www.StrideLinX.com](http://www.StrideLinX.com). The “[HTTP/VNC/Data Logging services and shortcuts](#)” section of Chapter 2 explains how you can add or manage these services.

## Specific Service and Server Settings

A VNC server running on certain devices may require advanced settings, such as encoding type or color depth. You can configure these settings by clicking SHOW MORE in the top right corner when configuring a service.

If you have a VNC server running on a computer, make sure you configure your VNC server's encryption setting, if available, to also accept unencrypted connections.

## Wireless Connectivity

Troubleshooting a StrideLinx router with 4G or WiFi is best accomplished as follows.

1. The WiFi connection SSID must be alphanumeric; it cannot include special characters, such as hyphen, apostrophe, etc.
2. Be sure the issue is WAN connectivity - The ACT LED will be blinking red 1 time for no internet connectivity. If the ACT LED is anything other than blinking red 1 time, then the issue is not wireless connectivity.
3. Check the Signal LED to determine if the router has a good signal. If not, check to make sure the antenna connectors are properly screwed on to the router and that the cable is not twisted, pinched, or damaged.
  - a. Observe the area around the antenna installation. The magnetic and screw mount antennas work best when connected to a metal ground plane at least 30 cm<sup>2</sup>. In addition, metal located above or on the sides of the antenna will decrease the range.
  - b. Clear line of sight between the router antenna and the wireless access point will provide a better connection.
  - c. (4G) If a single antenna is used, ensure the antenna is connected to the MAIN antenna connector, nearer to the front of the router. If a single antenna is connected properly to the MAIN connector, add a second antenna to the DIV connector.
4. If a good signal is shown (purple or blue) on the Signal LED, then
  - a. (WiFi) check to make sure the SSID and password are correct.
  - b. (4G) check to make sure the SIM card is properly inserted into the router and that the APN and PIN code have been correctly entered.
  - c. (4G) Make sure your cellular 4G SIM card is activated by the carrier.
5. As a double check, use a smartphone at the router location to check the signal strength.
  - a. (WiFi) Open WiFi settings and confirm wireless access point signal strength and SSID, password.
  - b. (4G) On an AT&T smartphone, look in the upper left hand corner to determine network signal strength.

If your smartphone shows a signal the wireless connection to the router should also be adequate.

6. For the 4G router, diagnose issues with the data plan or SIM card using AT&T's web site at <https://marketplace.att.com/data-plans>.
  - a. Verify that the monthly 4G data limit has not been exceeded.
  - b. Verify that the correct certified device type (i.e., IXON StrideLinx VPN Router 4G) has been selected for use with the SIM card.
  - c. Use AT&T's diagnostics feature to check for other issues with the data plan.

# **SAFETY AND SECURITY CONSIDERATIONS**

---



**In this Appendix...**

<b>Security Considerations for Control Systems Networks.....</b>	<b>C-3</b>
<b>Safety Guidelines.....</b>	<b>C-4</b>
Plan for Safety .....	C-4
Digital Input Safety Lockout.....	C-5

This manual covers the StrideLinx platform available from 2017 through 2021.

For details covering the StrideLinx Cloud 2.0 platform available after April 2021, please [click here](#) to link to that manual.

The StrideLinx Cloud 2.0 manual includes details describing the [Activation Code](#) model of Data Logging, Cloud Notify and other add-on features.

For information on the migration wizard from the original platform to StrideLinx Cloud 2.0, [click here](#).

## Security Considerations for Control Systems Networks

A video providing an overview of security considerations is accessible by clicking the thumbnail at the right, or by copying the following URL to your browser:

<https://www.AutomationDirect.com/VID-CM-0028>



Manufacturers are realizing that to stay competitive, their Automation and Control Systems need to be more integrated within their plant. The systems often need to be integrated with upstream Enterprise Data Systems, and even further integrated to allow information to be accessible across multiple plants, or even through the Internet. This convergence of the IT world with the Automation World creates challenges in maintaining secure systems and protecting your investments in processes, personnel, data and intellectual property.

While Automation Networks and Systems have built-in password protection schemes, this is only one very small step in securing your systems. Automation Control System Networks need to incorporate data protection and security measures that are at least as robust as a typical business computer system. We recommend that users of PLCs, HMI products and SCADA systems perform your own network security analysis to determine the proper level of security required for you application. However, the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has provided direction related to network security and safety under an approach described as "Defense in Depth", which is published at [https://www.us-cert.gov/sites/default/files/recommended\\_practices/NCCIC ICS-CERT Defense in Depth 2016 S508C.pdf](https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC%20ICS-CERT%20Defense%20in%20Depth%202016%20S508C.pdf).

This comprehensive security strategy involves physical protection methods, as well as process and policy methods. This approach creates multiple layers and levels of security for industrial automation systems. Such safeguards include the location of control system networks behind firewalls, their isolation from business networks, the use of intrusion detection systems, and the use of secure methods for remote access such as Virtual Private Networks (VPNs). Further, users should minimize network exposure for all control system devices and such control systems and these systems should not directly face the internet. Following these procedures should significantly reduce your risks both from external sources as well as internal sources, and provide a more secure system.

It is the user's responsibility to protect such systems, just as you would protect your computer and business systems. AutomationDirect recommends using one or more of these resources in putting together a secure system:

- US-CERT's Control Systems Security Program at the following web address: <https://ics-cert.us-cert.gov/Recommended-Practices>
- Special Publication 800-82 of the National Institute of Standards and Technology – Guide to Industrial Control Systems (ICS) Security <https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final>
- ISA99, Industrial Automation and Control Systems Security <http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821> (please note this is a summary and these standards have to be purchased from ISA)



This set of resources provides a comprehensive approach to securing a control system network and reducing risk and exposure from security breaches. Given the nature of any system that accesses the internet, it is incumbent upon each user to assess the needs and requirements of their application, and take steps to mitigate the particular security risks inherent in their control system

## Safety Guidelines



---

**NOTE:** Products with CE marks perform their required functions safely and adhere to relevant standards as specified by CE directives provided they are used according to their intended purpose and that the instructions in this manual are adhered to. The protection provided by the equipment may be impaired if this equipment is used in a manner not specified in this manual. A listing of our international affiliates is available on our Web site: <https://www.AutomationDirect.com>

---



**WARNING:** Providing a safe operating environment for personnel and equipment is your responsibility and should be your primary goal during system planning and installation. Automation systems can fail and may result in situations that can cause serious injury to personnel or damage to equipment. Do not rely on the automation system alone to provide a safe operating environment. You should use external electromechanical devices, such as relays or limit switches, that are independent of the PLC application to provide protection for any part of the system that may cause personal injury or damage. Every automation application is different, so there may be special requirements for your particular application. Make sure you follow all national, state, and local government requirements for the proper installation and use of your equipment.

---

### Plan for Safety

The best way to provide a safe operating environment is to make personnel and equipment safety part of the planning process. You should examine every aspect of the system to determine which areas are critical to operator or machine safety. If you are not familiar with control system installation practices, or your company does not have established installation guidelines, you should obtain additional information from the following sources.

- NEMA — The National Electrical Manufacturers Association, located in Washington, D.C. publishes many different documents that discuss standards for industrial control systems. You can order these publications directly from NEMA. Some of these include:
  - ICS 1, General Standards for Industrial Control and Systems*
  - ICS 3, Industrial Systems*
  - ICS 6, Enclosures for Industrial Control Systems*
- NEC — The National Electrical Code provides regulations concerning the installation and use of various types of electrical equipment. Copies of the NEC Handbook can often be obtained from your local electrical equipment distributor or your local library.
- Local and State Agencies — many local governments and state governments have additional requirements above and beyond those described in the NEC Handbook. Check with your local Electrical Inspector or Fire Marshall office for information.

### Digital Input Safety Lockout

A video providing an overview of using the StrideLinx router's Digital Input as a part of your safety lockout procedures is accessible by clicking the thumbnail at the right, or by copying the following URL to your browser:

<https://www.AutomationDirect.com/VID-CM-0034>





# **DATA LOGGING ADDRESS NOTATION – AUTOMATIONDIRECT DEVICES**

# **APPENDIX D**

**In this Appendix...**

<b>StrideLinx Modbus to AutomationDirect PLC Address Maps .....</b>	<b>D-3</b>
CLICK PLCs .....	D-3
DirectLogic PLCs .....	D-6
Do-more PLCs .....	D-8
Productivity Series PLCs.....	D-10

This manual covers the StrideLinx platform available from 2017 through 2021.

For details covering the StrideLinx Cloud 2.0 platform available after April 2021, please [click here](#) to link to that manual.

The StrideLinx Cloud 2.0 manual includes details describing the [Activation Code](#) model of Data Logging, Cloud Notify and other add-on features.

For information on the migration wizard from the original platform to StrideLinx Cloud 2.0, [click here](#).

## StrideLinx Modbus to AutomationDirect PLC Address Maps

The following tables provide mapping between StrideLinx Modbus addresses and specific AutomationDirect PLC product line addresses.

### CLICK PLCs

Reading Coils (Function Code 1)			
<i>Function Code</i>	<i>StrideLinx Modbus Address</i>	<i>Data Type</i>	<i>CLICK Address</i>
1	8192	BOOL	Y1
1	8207		Y16
1	8224		Y101
1	8239		Y116
1	8256		Y201
1	8273		Y216
1	8287		Y301
1	8302		Y316
1	8320		Y401
1	8335		Y416
1	8352		Y501
1	8367		Y516
1	8384		Y601
1	8399		Y616
1	8416		Y701
1	8431		Y716
1	8448		Y801
1	8463		Y816
1	16384		C1
1	18383		C2000

Reading Input Bits (Function Code 2)			
Function Code	StrideLinx Modbus Address	Data Type	CLICK Address
2	0	BOOL	X1
2	15		X16
2	32		X101
2	47		X116
2	64		X201
2	79		X216
2	96		X301
2	111		X316
2	128		X401
2	143		X416
2	160		X501
2	175		X516
2	192		X601
2	207		X616
2	224		X701
2	239		X716
2	256		X801
2	271		X816
2	45056		T1
2	45555		T500
2	49152		CT1
2	49401		CT250
2	61440		SC1
2	62439		SC1000

Reading Input Registers (Function Code 4)			
Function Code	StrideLinx Modbus Address	Data Type	CLICK Address
4	61440	INT16, UINT16 or BOOL*	SD0
4	62439		SD1000
4	57344/57345	INT32 or UINT32	XD0
4	57360/57361		XD8

\* *BOOL*: When using *BOOL* with Input and Holding Registers, a zero value in the register indicates False in the data logger. Any non-zero value indicates True in the data logger.

Reading Holding Registers (Function Code 3)			
Function Code	StrideLinx Modbus Address	Data Type	CLICK Address
3	0	INT16, UINT16 or BOOL**	DS1
3	4499		DS4500
3	24576		DH1
3	25075		DH500
3	45056		TD1
3	45555		TD500
3	16384/16385	INT32 or UINT32	DD1
3	18382/18383		DD1000
3	49152/49153		CTD1
3	49650/49651		CTD250
3	57856/57857		YD0
3	57872/87873		YD8
3	28672/28673	FLOAT32	DF1
3	29670/29671		DF500

\* **BOOL**: When using **BOOL** with Input and Holding Registers, a zero value in the register indicates False in the data logger. Any non-zero value indicates True in the data logger.

## DirectLogic PLCs

Reading Coils (Function Code 1)			
<i>Function Code</i>	<i>StrideLinx Modbus Address</i>	<i>Data Type</i>	<i>DirectLogic Address</i>
1	0	BOOL	GY0
1	2047		GY3777
1	2048		Y0
1	3071		Y1777
1	3072		C0
1	5119		C3777
1	5120		S0
1	6143		S1777
1	6144		T0
1	6399		T377
1	6400		CT0
1	6655		CT377

Reading Input Bits (Function Code 2)			
<i>Function Code</i>	<i>StrideLinx Modbus Address</i>	<i>Data Type</i>	<i>DirectLogic Address</i>
2	0	BOOL	GX0
2	2047		GX3777
2	2048		X0
2	3071		X1777
2	3072		SP0
2	3583		SP777



Reading Input Registers (Function Code 4)			
Function Code	StrideLinx Modbus Address	Data Type	DirectLogic Address
4	0	INT16, UINT16 or BOOL*	V0
4	17055		V41237
4	0/1	INT32 or UINT32	V0/V1
4	1/2		V1/V2
4	17054/17055		V41236/V41237
4	0/1	FLOAT32	V0/V1
4	1/2		V1/V2
4	17054/17055		V41236/V41237

\* *BOOL*: When using *BOOL* with Input and Holding Registers, a zero value in the register indicates False in the data logger. Any non-zero value indicates True in the data logger.

Reading Holding Registers (Function Code 3)			
Function Code	StrideLinx Modbus Address	Data Type	DirectLogic Address
3	0	INT16, UINT16 or BOOL*	V0
3	17055		V41237
3	0/1	INT32 or UINT32	V0/V1
3	1/2		V1/V2
3	17054/17055		V41236/V41237
3	0/1	FLOAT32	V0/V1
3	1/2		V1/V2
3	17054/17055		V41236/V41237

\* *BOOL*: When using *BOOL* with Input and Holding Registers, a zero value in the register indicates False in the data logger. Any non-zero value indicates True in the data logger.

**Do-more PLCs**

Reading Coils (Function Code 1)			
Function Code	StrideLinx Modbus Address	Data Type	Do-more! Address
1	0	BOOL	MC1
1	1		MC2
1	65534		MC65535

Reading Input Bits (Function Code 2)			
Function Code	StrideLinx Modbus Address	Data Type	Do-more! Address
2	0	BOOL	MI1
2	1		MI2
2	65534		MI65535

Reading Input Registers (Function Code 4)			
Function Code	StrideLinx Modbus Address	Data Type	Do-more! Address**
4	0	INT16, UINT16 or BOOL*	MIR1
4	1		MIR2
4	65534		MIR65535
4	0	INT32 or UINT32	-
4	1/2		MIR2:D
4	65533/65534		MIR65534:D
4	0	FLOAT32	-
4	1		MIR2:RD
4	65533/65534		MIR65534:RD

\* *BOOL*: When using *BOOL* with Input and Holding Registers, a zero value in the register indicates *False* in the data logger. Any non-zero value indicates *True* in the data logger.

\*\* *Double integers (32 bit) can only be used on even number addresses in Do-more! (MIR2, MIR4, etc...).*

Reading Holding Registers (Function Code 3)			
Function Code	StrideLinx Modbus Address	Data Type	Do-more! Address**
3	0	INT16, UINT16 or BOOL*	MHR1
3	1		MHR2
3	65534		MHR65535
3	0	INT32 or UINT32	-
3	1/2		MHR2:D
3	65533/65534		MHR65534:D
3	0	FLOAT32	-
3	1/2		MHR2:RD
3	65533/65534		MHR65534:RD

\* *BOOL*: When using *BOOL* with Input and Holding Registers, a zero value in the register indicates False in the data logger. Any non-zero value indicates True in the data logger.

\*\* *Double integers (32 bit)* can only be used on even number addresses in Do-more! (*MIR2, MIR4, etc...*).

## Productivity Series PLCs

Reading Coils (Function Code 1)			
Function Code	StrideLinx Modbus Address	Data Type	Productivity Address*
1	0	BOOL	000001
1	1		000002
1	65534		065535

\* Modbus addresses must be assigned to the tags in the "Tag Database" area of the Productivity Suite Programming Software.

Reading Input Bits (Function Code 2)			
Function Code	StrideLinx Modbus Address	Data Type	Productivity Address*
2	0	BOOL	100001
2	1		100002
2	65534		165535

\* Modbus addresses must be assigned to the tags in the "Tag Database" area of the Productivity Suite Programming Software.

Reading Input Registers (Function Code 4)			
Function Code	StrideLinx Modbus Address	Data Type	Productivity Address**
4	0	INT16, UINT16 or BOOL*	300001
4	1		300002
4	65534		365535
4	0	INT32 or UINT32	30001/300002
4	1		30002/300003
4	65534		365535/365536
4	0	FLOAT32	30001/300002
4	1		30002/300003
4	65534		365535/365536

\* **BOOL**: When using **BOOL** with Input and Holding Registers, a zero value in the register indicates False in the data logger. Any non-zero value indicates True in the data logger.

\*\* Modbus addresses must be assigned to the tags in the "Tag Database" area of the Productivity Suite Programming Software.

Reading Holding Registers (Function Code 3)			
Function Code	StrideLinx Modbus Address	Data Type	Productivity Address**
3	0	INT16, UINT16 or BOOL*	400001
3	1		400002
3	65534		465535
3	0	INT32 or UINT32	400001/400002
3	1		400002/400003
3	65534		465535/465536
3	0	FLOAT32	400001/400002
3	1		400002/400003
3	65534		465535/465536

\* *BOOL*: When using *BOOL* with Input and Holding Registers, a zero value in the register indicates False in the data logger. Any non-zero value indicates True in the data logger.

\*\* *Modbus addresses must be assigned to the tags in the "Tag Database" area of the Productivity Suite Programming Software*

# STRIDELINX NETWORK SECURITY

---



## In this Appendix...

<b>Introduction: Intended Audience.....</b>	<b>E-3</b>
<b>Solution explained.....</b>	<b>E-3</b>
StrideLinx Router.....	E-3
StrideLinx Platform.....	E-3
StrideLinx Client.....	E-3
Overview.....	E-3
<b>Controls Network Security .....</b>	<b>E-5</b>
Remote access.....	E-5
Local access.....	E-5
<b>Company Network Security .....</b>	<b>E-6</b>
Connectivity.....	E-6
Remote access.....	E-7
Local access.....	E-7
<b>StrideLinx Platform Security.....</b>	<b>E-7</b>
Servers .....	E-7
StrideLinx platform.....	E-7
<b>VPN Client Security .....</b>	<b>E-8</b>

This manual covers the StrideLinx platform available from 2017 through 2021.

For details covering the StrideLinx Cloud 2.0 platform available after April 2021, please [click here](#) to link to that manual.

The StrideLinx Cloud 2.0 manual includes details describing the [Activation Code](#) model of Data Logging, Cloud Notify and other add-on features.

For information on the migration wizard from the original platform to StrideLinx Cloud 2.0, [click here](#).

## Introduction: Intended Audience

The StrideLinx Remote Access Solution is designed to offer safe and secure remote access to industrial equipment worldwide for efficient remote troubleshooting, programming and monitoring. As a result, it significantly reduces service costs and machine downtime. The intended audience of this document is personnel responsible for the administration and security of the network environment in which the StrideLinx product will reside (i.e., IT dept., network admins, etc.). The router will generate outbound traffic to create an internet connection; therefore, the network administrator of your network should be consulted.

The StrideLinx platform and router provide a secure method to access your control devices remotely, but it is important to note that it is just one part of an overall security strategy. It is important to evaluate and re-evaluate over time, the conditions of your particular network. A list of helpful resources is available in Appendix C, “Safety and Security Considerations” or at <http://support.automationdirect.com/docs/securityconsiderations.pdf>.

## Solution explained

The StrideLinx Remote Access Solution comprises the StrideLinx router, web-based platform, and VPN client.

### StrideLinx Router

The StrideLinx router can easily be connected to the hardware on your machine, allowing you to access your machine remotely for monitoring, troubleshooting and service purposes. ADC will offer the router in 3 variants: Ethernet wired, 4G LTE (America – AT&T) and WiFi (802.11b/g/n). The 4G LTE & WiFi models can also be configured as wired by using the RJ45 WAN port.

### StrideLinx Platform

The StrideLinx platform is a secure web-based platform made up of a worldwide network of scalable servers. It is focused on delivering and enhancing innovative secure remote access. The StrideLinx router connects your hardware to the StrideLinx platform via a secure VPN connection.

### StrideLinx Client

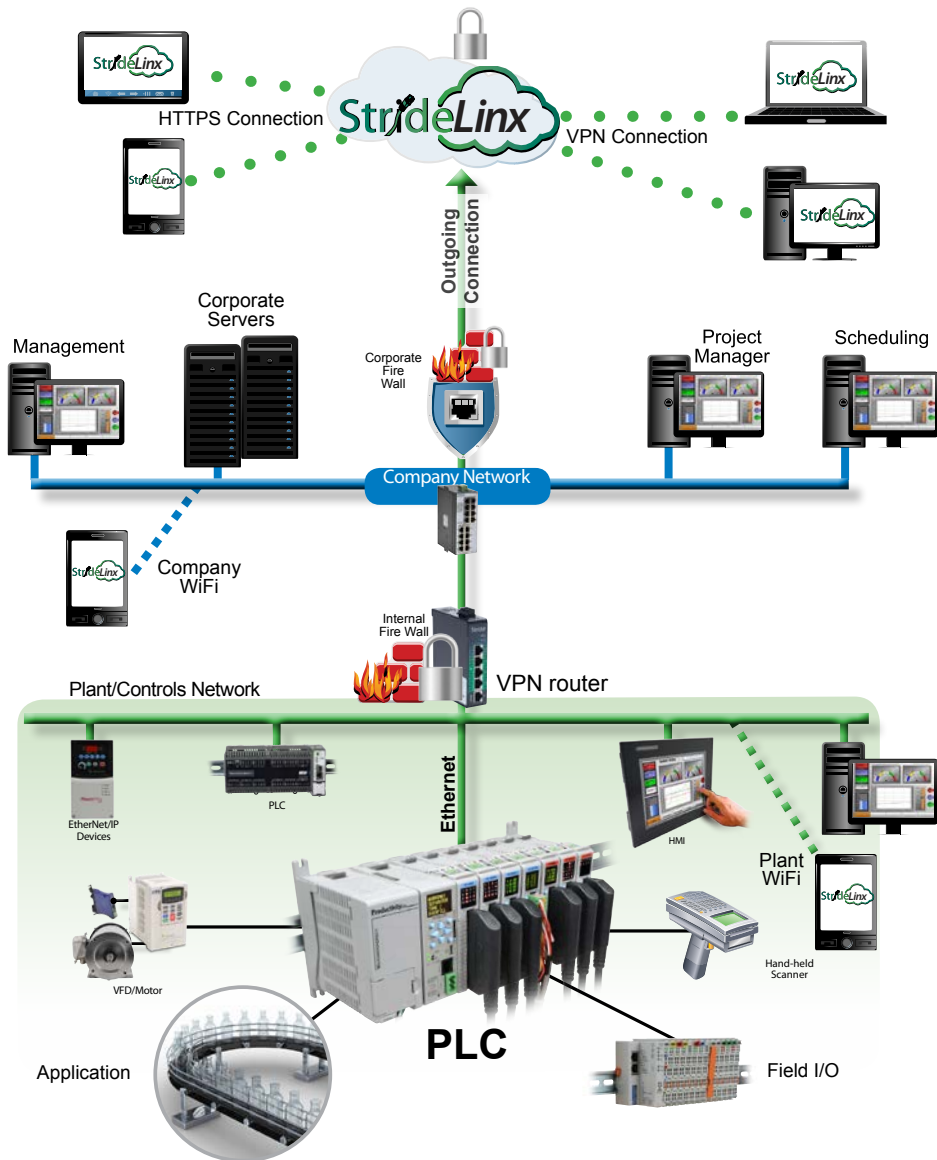
The VPN client is a light-weight application that runs in the background on your laptop or PC. A VPN connection is established when you use the StrideLinx platform to remotely connect to your devices.

### Overview

The remote access solution is made up of two connections – the client to platform (cloud servers) and the platform (cloud servers) to the router. This first connection is made when the local VPN router makes a VPN connection to the cloud server immediately upon startup. This ensures that all traffic between the router and platform is securely encrypted through the VPN tunnel. Communication for this link is initiated by the local router to the cloud-based server via an outbound connection through standard ports that are typically open, such as HTTPS. This usually requires no changes to the corporate IT firewall, thus satisfying IT security concerns.



E



With the router and server connected, the remote user is given two options for the second connection between them and the cloud servers. The first option is to connect by HTTPS by simply connecting the mobile device or PC/laptop to the platform using a web browser (clientless access). No VPN client is required for this mode and allows the user flexibility in connecting to the platform from any mobile device or PC with a web browser. Capabilities in

this mode include all standard platform functionality except VPN connection. The user has access to the router, but not to the LAN devices behind the router. So, programming software and other tools that require being on the local area network will not work in this mode. Two features that are supported in clientless access mode are VNC server & web server access by creating a shortcut on the Info tab of the router. This shortcut creates a secure port forward from the LAN port to the VPN tunnel. The shortcut allows users to access all of the features included on the LAN devices' VNC or web servers in a secure manner. Clientless access mode is protected by TLS1.2, but does not pass through the VPN tunnel from the cloud server to the remote user.

The second option for users to connect is by PC/laptop to the platform by VPN, allowing full local area network access. This method requires users log in to the platform through a web browser and have the VPN client installed on their PC. Upon a verified request from the remote user, the VPN client connects to the cloud server, providing a full VPN connection from remote user (PC) to the router. Once both connections have been made, all data passing through this VPN tunnel is secure.

## Controls Network Security

### Remote access

The StrideLinx router is equipped with a built-in firewall that completely separates the WAN port (company network) from the LAN ports (controls network). The firewall blocks all communication except for authorized and encrypted data verified by a valid certificate. This means that only authorized users can access the controls network via our StrideLinx platform.

### Local access

Default settings allow for zero communication from the company network to the controls network (and vice versa). The StrideLinx router is configurable to allow communication from the controls network to the company network, to the internet, or both. Authorization under this scenario is by means of the firewall section of the Configuration in the StrideLinx platform. There are three types of port forwarding supported in the StrideLinx router: LAN→WAN, WAN→LAN, VPN→LAN.

- LAN→WAN options allow access from the LAN to the corporate network or the internet. This option is needed if you are accessing an FTP or mail server on the corporate network or cloud. This option maintains good security practice if the corporate router is in place with strong security measures.
- WAN→LAN options allow access by port forwarding to incoming traffic.



***WARNING: This is usually not recommended as it opens specific ports to anyone on the internet and could make the control network insecure.***

- VPN→LAN port forwarding provides a secure port forward inside the encrypted VPN tunnel so that StrideLinx users can access the HTTP server or VNC server of their control network devices by shortcut services in the StrideLinx platform. This feature allows the clientless access mode for mobile & PC users as described in the “Solutions Explained” section above.

## Company Network Security

### Connectivity

The StrideLinx router uses an outgoing port to establish a secure connection to our StrideLinx platform. This means there is no need to open any incoming ports in your firewall. Via this outgoing port, the StrideLinx router connects to different servers: REST API, MQTT and OpenVPN servers. The IP addresses of these servers, as well as the number of servers, may change over time and are thus not pre-defined. What is pre-defined is the domain of these servers. This is why the StrideLinx router needs to be able to perform DNS requests; otherwise, the StrideLinx router can't connect to our servers.

Below is an overview of the outgoing ports and protocols that the StrideLinx router utilizes.

Outgoing Ports and Protocols		
Port	Protocol	Application
443	TCP	HTTPS, MQTT/TSL, OpenVPN
53	TCP & UDP	DNS

Port 443 is a port that is normally open and also used by other services to set up a secure connection (i.e. internet banking).

If necessary, the local (plant) IT department can choose to allow internet access based on the MAC address or IP address of the StrideLinx router. The router WAN IP address can be set to a static IP address on the wired router configuration; the WiFi router is set to default. However, by default the WAN IP address is set to be obtained automatically via DHCP.

To communicate with the StrideLinx platform, the StrideLinx router firmware uses the proven encryption standard SSL / TLS. The required TLS key exchange, crucial for security, is done in accordance with the industry standard 2048-bit RSA with SHA-256. During the RSA handshake the public server keys are shared and with built-in Certificate Authorities the server's identity is verified. The StrideLinx agent does not use 3rd party Certificate Authorities which guarantees an up-to-date security for embedded devices. When setting up a VPN tunnel, the necessary security licenses are downloaded and the Blowfish/AES encrypted VPN tunnel is set up. Attacks like Man-in-the-middle, spoofing ARP and DNS hijacking will be detected immediately.

The StrideLinx router remains permanently connected to the platform and sends out 'keep-alive heartbeats' on a regular interval. The remote connection between the StrideLinx router and StrideLinx platform can be managed by the local operator. A digital input allows the user to enable/disable the VPN connection at the flick of a switch, literally. For instance, this input can be used by plant personnel to manage access to the router by outside personnel on an as-needed basis. Alternatively, the connection can be terminated by powering off the StrideLinx router. Once it is powered again, the StrideLinx router automatically re-establishes the connection with the StrideLinx platform.

If the local (plant) IT department does not allow any form of internet connection to third party hardware, the StrideLinx router with 4G LTE may be used to isolate the controls network from the corporate IT network. LTE 4G access requires a standard SIM card (standard size, 2FF) for cellular internet access.

### Remote access

The StrideLinx router is equipped with a built-in firewall that completely separates the WAN port (company network) from the LAN ports (controls network). The firewall blocks all communication except for authorized and encrypted data verified by a valid certificate. This means that only authorized users can access the controls network via our StrideLinx platform.

### Local access

Default settings allow for zero communication from the company network to the controls network (and vice versa). The StrideLinx router is configurable to allow communication from the controls network to the company network, to the internet, or both. Authorization under this scenario is by means of the firewall section of the Configuration in the StrideLinx platform. There are three types of port forwarding supported in the StrideLinx router: LAN→WAN, WAN→LAN, VPN→LAN.

- LAN→WAN options allow access from the LAN to the corporate network or the internet. This option is needed if you are accessing a FTP or mail server on the corporate network or cloud. This option maintains good security practice if the corporate router is in place with strong security measures.
- WAN→LAN options allow access by port forwarding to incoming traffic.



**WARNING:** This is usually not recommended as it opens specific ports to anyone on the internet and could make the control network insecure.

- VPN→LAN port forwarding provides a secure port forward inside the encrypted VPN tunnel so that StrideLinx users can access the HTTP server or VNC server of their controls network devices by shortcut services in the StrideLinx platform. This feature allows the clientless access mode for mobile & PC users as described in the “Solution Explained” section above.

## StrideLinx Platform Security

### Servers

Our servers are hosted at one of the world’s largest cloud providers. All servers are certified by national and international safety standards.

### StrideLinx platform

A crucial link within the complete StrideLinx solution is the StrideLinx platform, which acts as a secure proxy for the data between the StrideLinx router and StrideLinx client. The browser always checks for the valid SSL certificate on the StrideLinx platform. As a result, the StrideLinx platform is protected against so called man-in-the-middle attacks.

**E** Only authorized users can access the controls network via our StrideLinx platform. This requires you to have an account (login information) as well as having received an invite to the particular company and being granted access and permission to the registered StrideLinx router(s).

The StrideLinx platform checks for login attempts forced by software to identify a username and password combination (so called Brute Force Attacks). Such attempts are detected and blocked by the StrideLinx platform. As an additional safety measure it is possible to set up 2-factor authentication for your account.

All login sessions, connections with the StrideLinx router, changes made to the details or configuration and reboots of the StrideLinx router are being logged with a timestamp and designated user (if applicable). All these logs can be viewed on the StrideLinx platform under “Latest events”: when navigating to “Devices” and selecting a specific StrideLinx router, or when navigating to “Users” and selecting a specific user.

The StrideLinx platform is the only component in the complete StrideLinx solution in which ports are exposed to the Internet. However, only VPN connections which carry a valid x.509 certificate receive access. The certificate is downloaded automatically once the user is successfully logged in and presses “connect” to connect to a specific StrideLinx router.

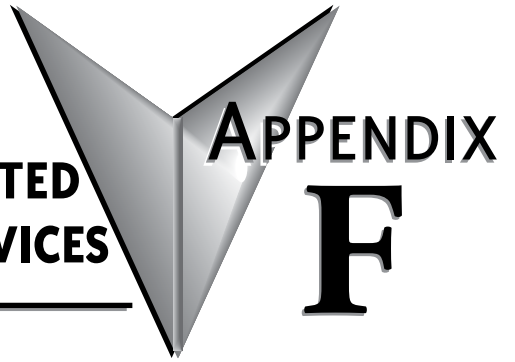
## VPN Client Security

StrideLinx client is a light-weight application that runs in the background on your PC. It creates a virtual Ethernet port on your PC and handles all communication between your PC and the StrideLinx platform.

The StrideLinx client uses the proven encryption standard SSL / TLS. The required TLS key exchange, crucial for security, is done in accordance with the industry standard 2048-bit RSA with SHA-256. During the RSA handshake the public server keys are shared, with built-in Certificate Authorities the server’s identity is verified. The StrideLinx client does not use 3rd party Certificate Authorities which guarantees an up-to-date security. When setting up a VPN tunnel, the necessary security licenses are downloaded and the Blowfish/AES encrypted VPN tunnel is set up. Attacks like man-in-the-middle, spoofing ARP and DNS hijacking will be detected immediately.

# **CAPABILITIES OF CONNECTED AUTOMATION DIRECT DEVICES**

---



**In this Appendix...**

<b>Network Topology</b> .....	<b>F-3</b>
Network with StrideLinx VPN router using wired or WiFi network connectivity .....	F-4
Network with StrideLinx VPN router using 4G cellular network connectivity .....	F-5
<b>Device Capabilities</b> .....	<b>F-6</b>

This manual covers the StrideLinx platform available from 2017 through 2021.

For details covering the StrideLinx Cloud 2.0 platform available after April 2021, please [click here](#) to link to that manual.

The StrideLinx Cloud 2.0 manual includes details describing the [Activation Code](#) model of Data Logging, Cloud Notify and other add-on features.

For information on the migration wizard from the original platform to StrideLinx Cloud 2.0, [click here](#).

### Network Topology

To facilitate description of the capabilities of various AutomationDirect product lines when connected to a StrideLinx VPN router, the overall topology of a network connecting plant devices to the StrideLinx platform can be divided into three zones, as illustrated in the two figures later in this appendix.

The zones are defined as follows.

- Zone 1 is outside the company network, and includes the StrideLinx platform and secure connections to it from various devices.
- Zone 2 is the company network, which exists behind a corporate firewall. This zone may include various computer systems, but is isolated from the plant/controls network by the internal firewall of the VPN router.
- Zone 3 comprises the devices connected to the VPN router, and thus potentially capable of secure remote connection.



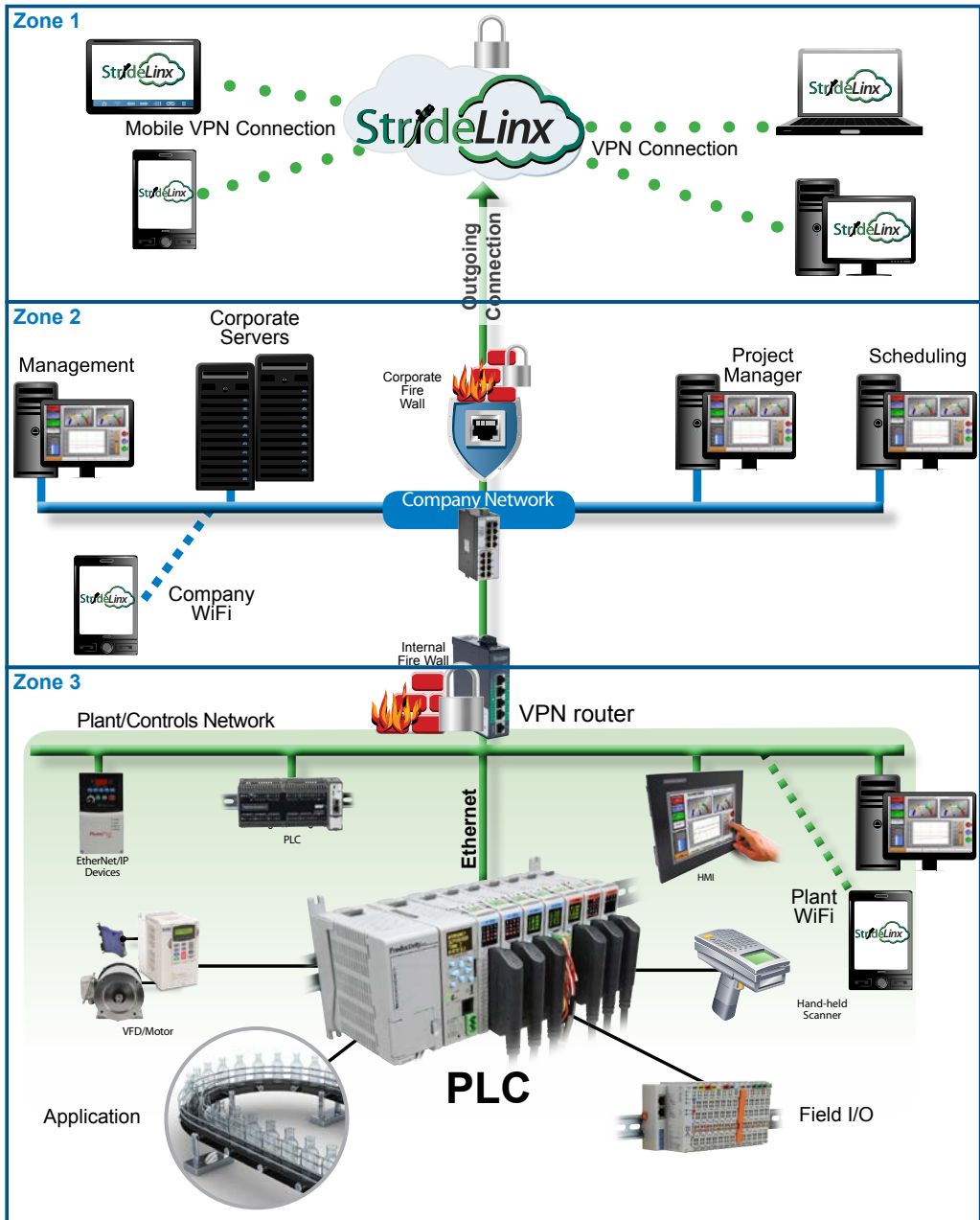
---

**NOTE:** Zone 2 does not participate at all in StrideLinx communications when a 4G cellular connection is used on the VPN router, since the 4G connection does not traverse the company network.

---

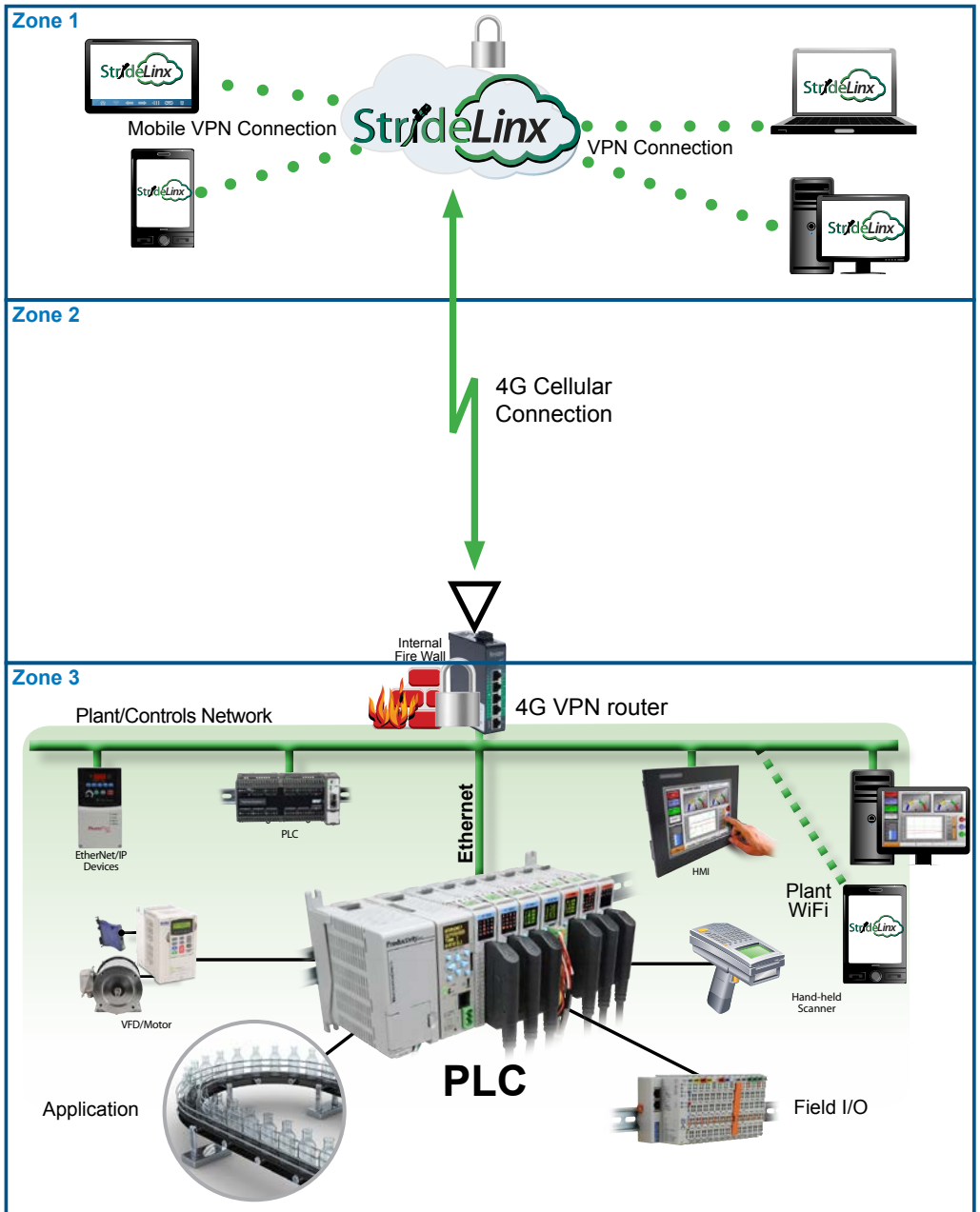


Network with StrideLinx VPN router using wired or WiFi network connectivity



F

Network with StrideLinx VPN router using 4G cellular network connectivity



F

## Device Capabilities

The following table describes the capabilities of devices to establish communications connections across various network zones, as defined earlier.

**F**

Communications Capabilities of Devices Connected to StrideLinX Router						
Functionality	Zone 1->3 (StrideLinX App or Browser w/o VPN)	Zone 1->3 (VPN)	Zone 2->3 <sup>1,6</sup>	Zone 3->2 <sup>6</sup>	Zone 3->1	Zone 3->3
Generic PLC programming SW (Windows)	N	Y	Y	NA	NA	Y
Productivity programming SW	N	Y	Y	NA	NA	Y
BRX programming SW	N	Y	Y	NA	NA	Y
<b>C-more</b> programming SW	N	Y	Y	NA	NA	Y
<b>C-more</b> Remote Access (PC)	N	Y	Y	NA	NA	Y
PxK/ <b>C-more</b> web server	Y <sup>4</sup>	Y	Y	NA	NA	Y
PxK/ <b>C-more</b> FTP access (into PxK/ <b>C-more</b> )	N	Y	Y	NA	NA	Y
BRX/PxK/ <b>C-more</b> Email to Server (sent from BRX/PxK/ <b>C-more</b> )	NA	NA	NA	Y <sup>2</sup>	Y <sup>2</sup>	NA
PxK/ <b>C-more</b> FTP to PC (sent from PxK/ <b>C-more</b> )	NA	NA	NA	Y <sup>2</sup>	Y <sup>2</sup>	NA
PxK/ <b>C-more</b> mobile app (connect by WiFi)	N	Y <sup>8</sup>	Y <sup>3</sup>	NA	NA	Y
3rd party PLC or HMI web/VNC server	Y <sup>5</sup>	Y	Y	NA	NA	Y
Windows-based machine control	N	Y	Y	NA	NA	Y
2nd StrideLinX Router (M2M or site-to-site)	NA	NA	NA	NA	N	NA

1. Connections from Zone 2 to 3 can be made through VPN on a PC but require firewall adjustments (port forwarding) for other devices. Consideration for security should be made before making firewall adjustments.
2. StrideLinX router firewall must be configured to allow internet access from the LAN side or allow access to corporate network. This data does not pass through the VPN tunnel.
3. StrideLinX router firewall must be configured to allow access to corporate network in order for the C-more Mobile App to connect.
4. PxK/C-more web server must be configured in StrideLinX platform (services tab) to provide the shortcut on the router dashboard page.
5. Web/VNC server capability depends on 3rd party device capability. Web/VNC server must be configured in StrideLinX platform (services tab) to provide the shortcut on the router dashboard page.
6. Connections to/from Zone 2 are not applicable when using a 4G cellular connection.
7. NA is used when the device is not located in the starting or ending zone.
8. Router firmware versions v3.13 and newer support connection from the C-more Mobile App across a mobile VPN tunnel (app versions 2.0.0 and newer).



**NOTE:** The StrideLinX router & platform should operate with any TCP/UDP Ethernet device designed with remote connectivity functions such as unicast messaging, default gateway support and retry timeout parameters. ADC tech support can assist with basic networking/connectivity troubleshooting for any device connected to a StrideLinX router, but only officially supports ADC hardware and programming software tools.

# **SET UP DATA SOURCE USING SIEMENS S7 PROTOCOL**

---



In this Appendix...

Set up data source for a device using Siemens S7 protocol.....G-3

**G**

This manual covers the StrideLinx platform available from 2017 through 2021.

For details covering the StrideLinx Cloud 2.0 platform available after April 2021, please [click here](#) to link to that manual.

The StrideLinx Cloud 2.0 manual includes details describing the [Activation Code](#) model of Data Logging, Cloud Notify and other add-on features.

For information on the migration wizard from the original platform to StrideLinx Cloud 2.0, [click here](#).

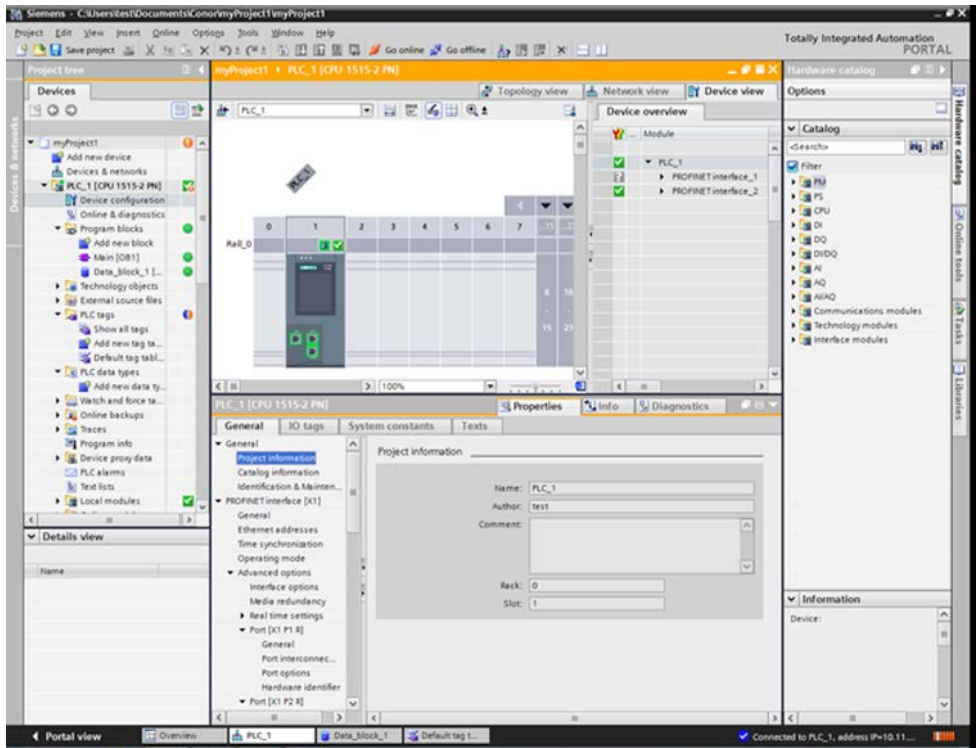
## Set up data source for a device using Siemens S7 protocol

In order to use the cloud data logging or cloud notification functionality with a Siemens S7 PLC, the communication between the StrideLinx router and the PLC must be configured first. We will use Siemens TIA Portal software to collect information on the PLC and set required configuration options, then use the StrideLinx platform to set up data logging.

### *Prepare the Siemens PLC for remote data logging or notifications*

#### *Find the rack and slot numbers*

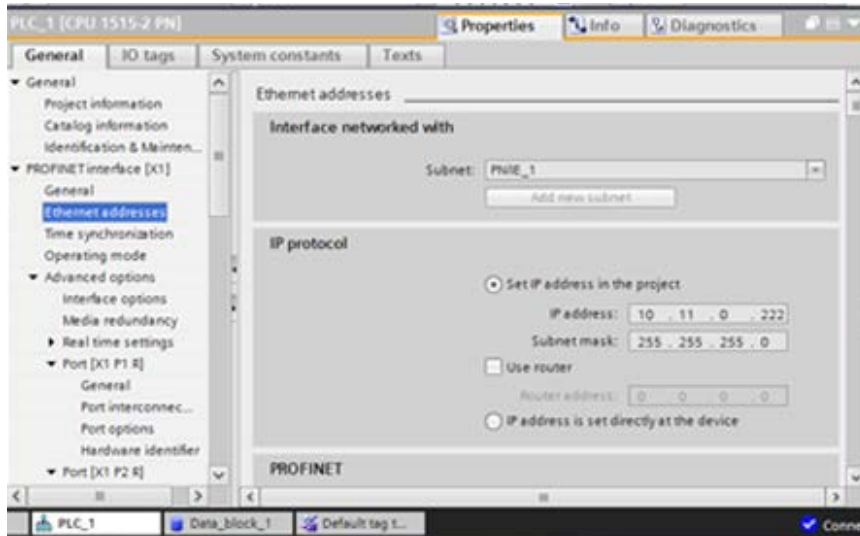
In TIA Portal, click on the CPU and select “Project Information” in the center panel. Make note of the rack number and slot number to enter into the StrideLinx platform later.



#### *Find the static IP address*

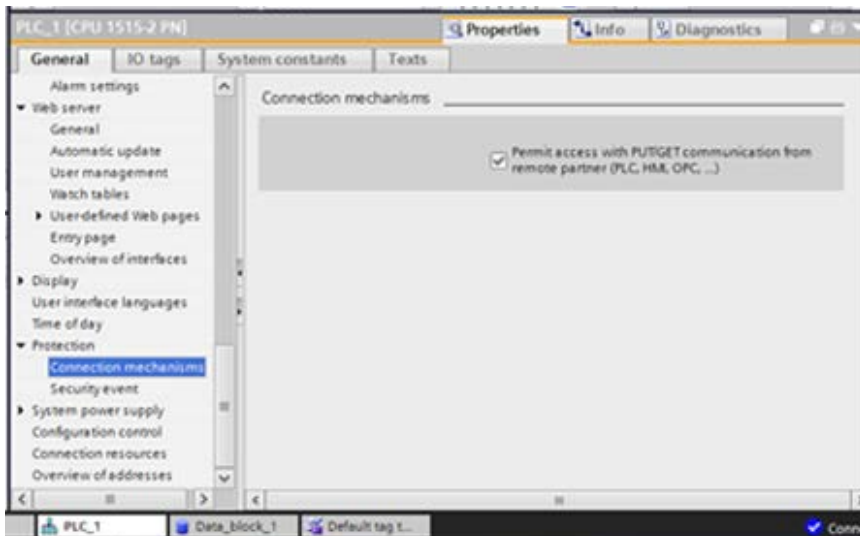
The PLC must have a static IP address in order to be accessed through the VPN. To find or set the IP address, select “Ethernet addresses” in the center panel. Make note of the IP address

and subnet mask. Be sure the subnet mask shown matches the subnet mask of the VPN router.



### *Enable external access*

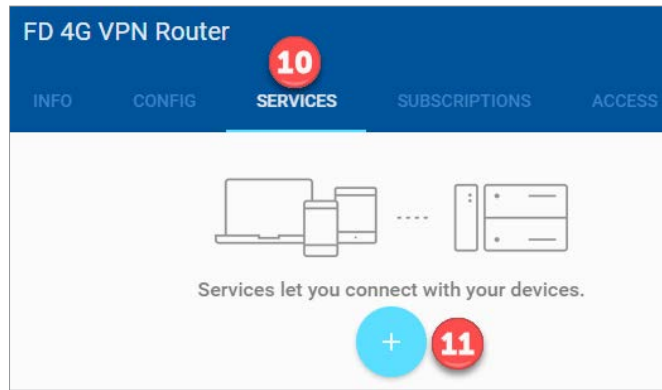
In the PLC, make sure you enable the “Permit access with PUT/GET communication from remote partner (PLC, HMI, OPC, …)” option.



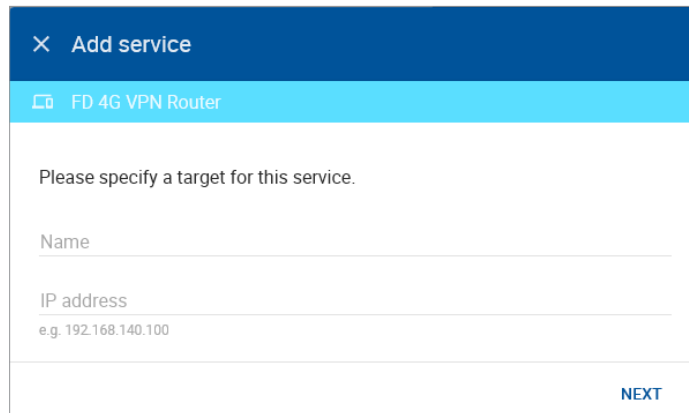
The Siemens S7 PLC is now ready to set up data logging or notifications on the StrideLinX platform.

*Configure the address and protocol for the PLC from which data will be read*

On the StrideLinX platform, click on the SERVICES tab (10). Click the +(Add) button (11).

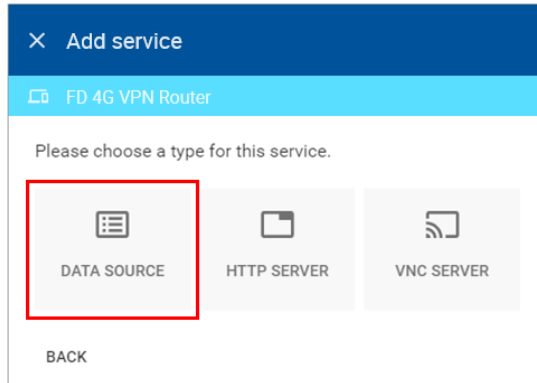


Add a Name and the IP Address of the PLC where the data resides. Click NEXT.

The screenshot shows a dialog box titled 'Add service' with a close button (X) in the top left. Below the title bar, the selected device 'FD 4G VPN Router' is shown. The main content area contains the instruction 'Please specify a target for this service.' followed by two input fields: 'Name' and 'IP address'. Below the 'IP address' field, there is a small example text 'e.g. 192.168.140.100'. At the bottom right of the dialog box, there is a blue 'NEXT' button.



Select DATA SOURCE.



×

Add service

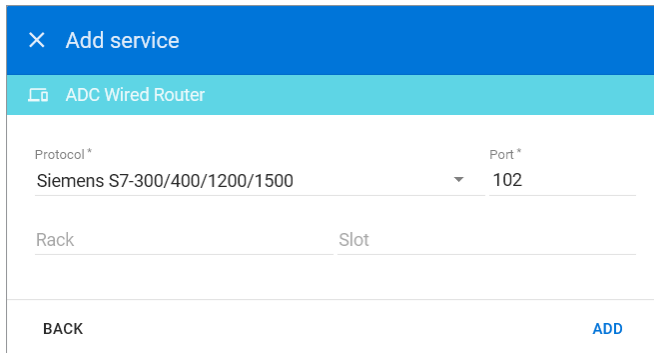
FD 4G VPN Router

Please choose a type for this service.

DATA SOURCE HTTP SERVER VNC SERVER

BACK

Select the Siemens S7 protocol. Fill in the rack and slot that were previously recorded for the PLC. Then click ADD to continue.



×

Add service

ADC Wired Router

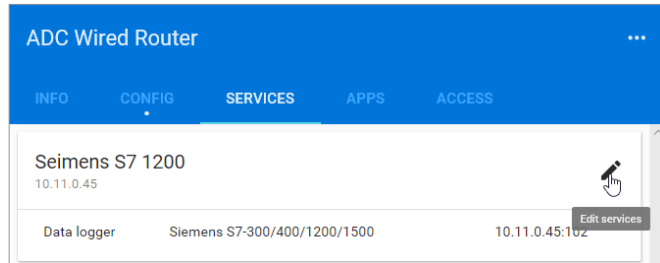
Protocol\* Siemens S7-300/400/1200/1500 Port\* 102

Rack Slot

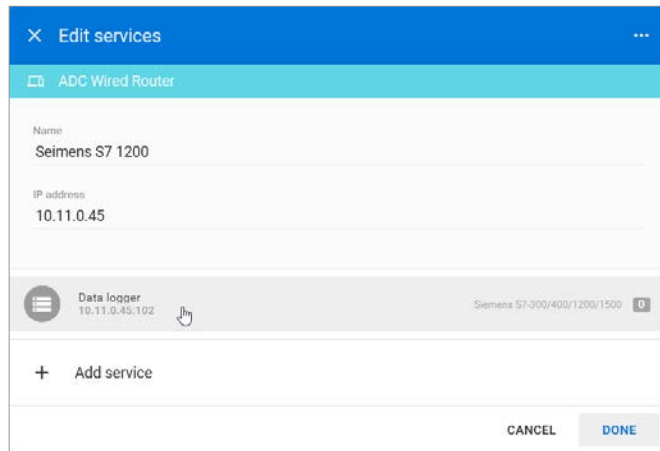
BACK ADD

### Configure the data tags

To add a data tag, go to the SERVICES tab for the router and click the Edit services (pencil) icon next to the device for which you want to add the data tag.

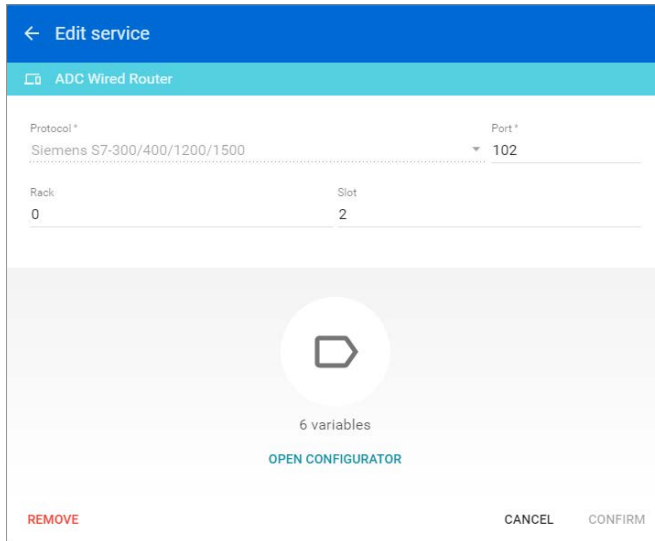


This opens the Edit services dialog. Click the name of the existing device for which you would like to add a data tag.



**NOTE:** It is advisable to enter data tags in small batches, and test the variables periodically to verify the entries. The entries can be tested by clicking “RUN TEST” in the Configurator, or from the Cloud Logging Web App as described in the [Data Logger Test Utility](#) section. Please refresh your browser if the information on screen appears to not be updated properly at any time.

The resulting “Edit service” screen displays the parameters for the data source, plus a count of existing data tags. Click OPEN CONFIGURATOR to add or edit tags.



← Edit service

ADC Wired Router

Protocol\* Siemens S7-300/400/1200/1500 Port\* 102

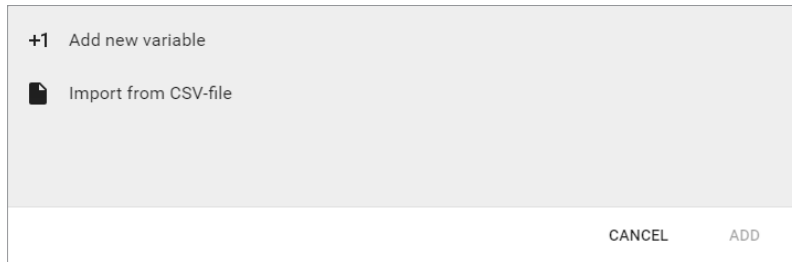
Rack: 0 Slot: 2

6 variables

OPEN CONFIGURATOR

REMOVE CANCEL CONFIRM

Data tags can be entered interactively, or a set of tags can be imported from a previously-exported CSV file. Export of sets of data tags is discussed later in the “Export Data Tags” subsection. For this example, select “Add new variable” to manually enter tags.



+1 Add new variable

Import from CSV-file

CANCEL ADD

A data entry screen opens, with one new data tag ready to be entered. Set the relevant parameters for the new data tag. The data tag input fields and supported data types are described in the next two tables, respectively. Subsequent figures illustrate the correct syntax for entering Siemens S7 addresses. Additional data tags can be entered in this round by clicking “+1” in the lower left corner of the screen. When all the desired tags have been entered click ADD.

Name \*

---

Select a data type \*      Region \*      Data block \*      Address \*

---

Factor      Unit

---

+1

CANCEL      ADD

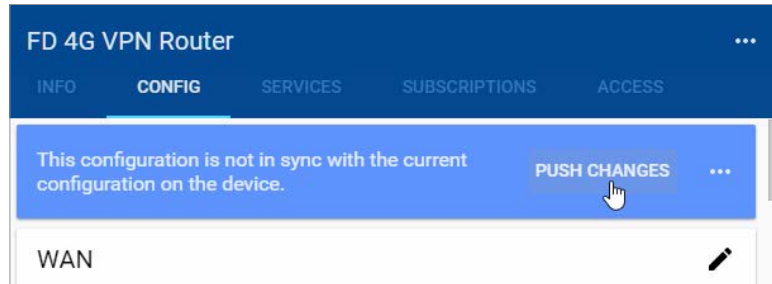
Data Tag Input Fields	
Field	Description
Name	Give the data tag a logical name.
Select a data type	See next table for the available data types.
Region	Select the type of value that needs to be logged. Values are Output Byte (AB), Input Byte (EB), Data Block (DB) and Markers (MB)
Data Block	Define in which data block the data tag is located.
Address	Define at which address in the data block the tag is located.
Unit (optional)	Here you can assign a value to a unit, for example, gallons or psi.
Factor (optional)	This allows you to multiply by a value. For example, factor 0.01 divides the data value by 100.

Data Types Supported		
StrideLinx	Siemens S7 Elementary Types	Siemens S7 Memory Types
Bool	BOOL	I/Q/M/DBX
Float32	REAL	ID/QD/MD/DBD
Float64		
Int8	BYTE	IB/QB/WB/DBB
Int16	INT	IW/QW/MW/DBW
Int32	DINT	ID/QD/MD/DBD
Int64		
String	CHAR	DBB String/DBB Char
UInt8		
UInt16	WORD	IW/QW/MW/DBW
UInt32	DWORD	ID/QD/MD/DBD
UInt64		

The following subsection, “Siemens S7 address notation and lookup,” presents the recommended method to determine the correct address and syntax for your data tag. After all data is entered, click ADD to continue.

Once you have added all the data tags you want to log, you will be prompted to push the configuration to the router.

G



The data tag entries should now be verified using the procedure described in the “Test Utility” subsections of Chapter 4 and Chapter 5.



**NOTE:** Additional data tag parameters related specifically to data logging (i.e., sampling interval, data retention policy, and logging only when changed) can be set from the Cloud Logging web app discussed in Chapter 4.

The Cloud Logging web app can now be used to set up data dashboards and to adjust additional data tag parameters related specifically to data logging, and the Cloud Notify web app can be used to set up alarm notifications.

### *Export data tags*

Data tag configurations can be exported in CSV format. The CSV file is downloaded to your local PC, and can later be imported to set up another StrideLinx router.

Select data tags to be exported by clicking the icon for each data tag, or select all data tags at once from the More Options (⋮) menu in the upper right corner of the screen. The selected data tags can then be deleted, duplicated, or exported from the pop up menu at the bottom of the screen.

### Siemens S7 address notation and lookup

The following data within Siemens S7 PLC is addressable for remote access.

Siemens S7 Memory Addressing					
Memory Type	Range	Description	Read/Write	Data Type	
I	I *	0.00–65535.7	Input Memory	R/W	Bit
	IB *	0–65535			Byte
	IW *	0–65535			Word
	ID *	0–65535			Double Word
Q	Q *	0.00–65535.7	Output Memory	R/W	Bit
	QB *	0–65535			Byte
	QW *	0–65535			Word
	QD *	0–65535			Double Word
M	M *	0.00–65535.7	Internal Memory	R/W	Bit
	MB *	0–65535			Byte
	MW *	0–65535			Word
	MD *	0–65535			Double Word
DB	DBX *	1.0–65535.65535	Data Block Memory	R/W	Bit
	DBB *				Byte
	DBW *				Word
	DBD *				Double Word

*\* Does not need to be entered. Only displayed.*

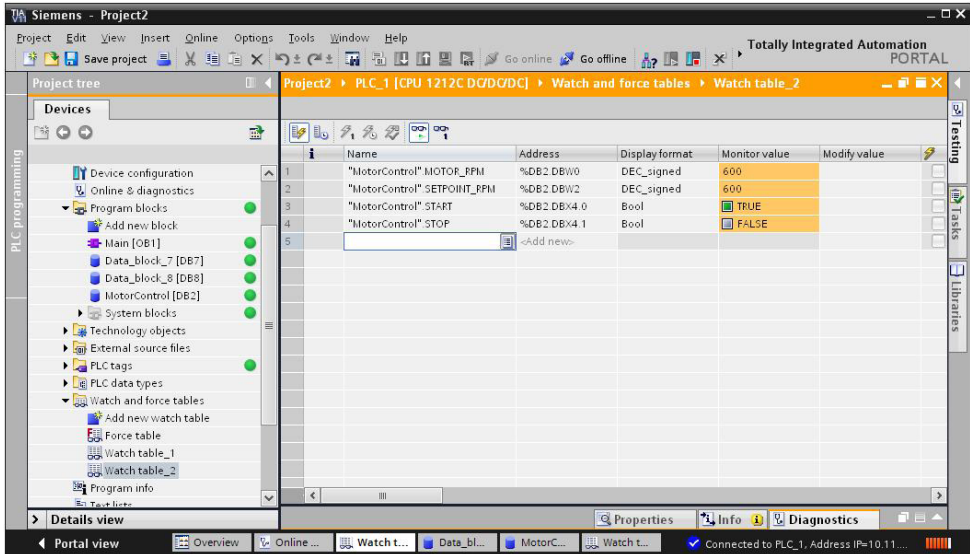
**NOTE:** Timers and Counters are System Blocks that are not addressable.

**NOTE:** Data Blocks must have “Optimized Block Access” DISABLED in SIMATIC STEP 7 software in order to be accessed remotely.

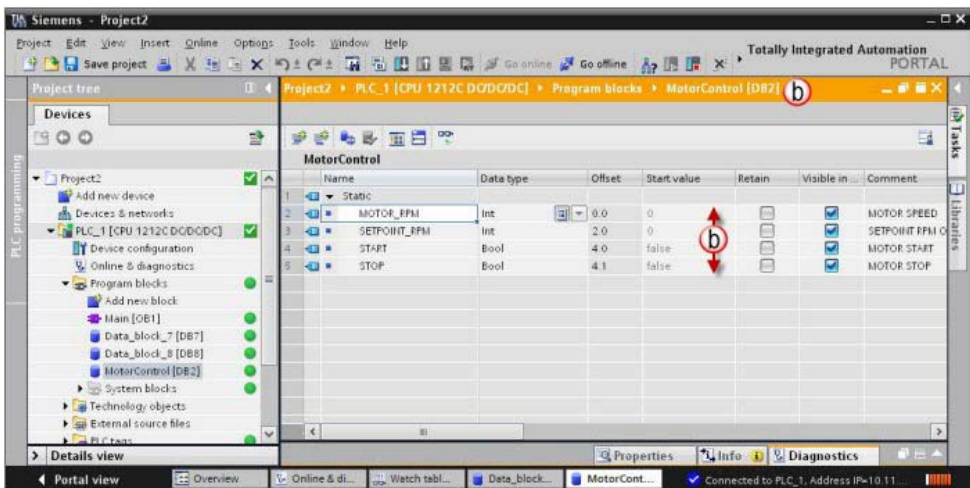


Use the Offset column of the Data Block as the byte address for StrideLinx. Even though the DB is defined as “Int” the offset is still byte not word.

To view the status of the variables in the PLC, connect to the PLC within SIMATIC STEP 7 and add or open an existing Watch Table from the Devices Tree as shown below.



Data Block Addressing syntax differs some between what is seen in SIMATIC STEP 7 and in StrideLinx. To view the Data Block, double click on the specific Data Block you wish to view. When a specific Data Block is selected, a window like the one shown below will open.



The previous image shows DB2. Inside DB2, there are four variables:

- MOTOR\_RPM is addressed at byte0 and is a 16-bit Integer.
- SETPOINT\_RPM is addressed at byte2 and is also a 16-bit Integer.
- START is addressed at byte 4, bit 0 and is a Boolean.
- STOP is addressed at byte 4, bit 1 and is a Boolean.

If the “Offset” column is not displayed, right-click any column header to Show / Hide Columns.

These four variables would be addressed as follows in StrideLinx:

- MOTOR\_RPM: Type = Int16, Region = DB, Data block = 2, Address = 0
- SETPOINT\_RPM: Type = Int16, Region = DB, Data block = 2, Address = 2
- START: Type = Boolean, Region = DB, Data block = 2, Address = 4, Bit = 0
- STOP: Type = Boolean, Region = DB, Data block = 2, Address = 4, Bit = 1



# **SET UP DATA SOURCE USING OPC UA PROTOCOL**

---



In this Appendix...

Set up data source for a device using OPC UA protocol ..... H-3

# H

This manual covers the StrideLinx platform available from 2017 through 2021.

For details covering the StrideLinx Cloud 2.0 platform available after April 2021, please [click here](#) to link to that manual.

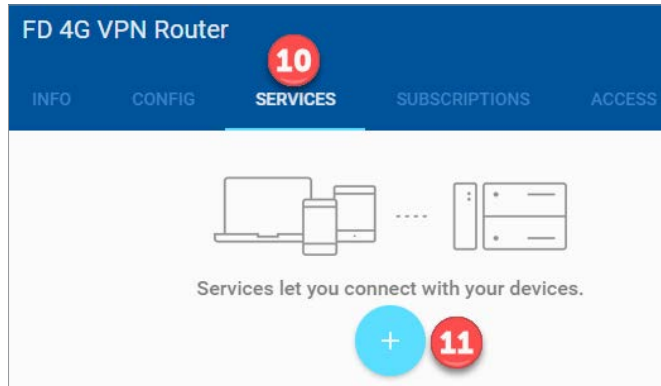
The StrideLinx Cloud 2.0 manual includes details describing the [Activation Code](#) model of Data Logging, Cloud Notify and other add-on features.

For information on the migration wizard from the original platform to StrideLinx Cloud 2.0, [click here](#).

## Set up data source for a device using OPC UA protocol

*Configure the address and protocol for the PLC from which data will be read*

Click on the SERVICES tab (10). Click the +(Add) button (11).



Add a Name and the IP Address of the PLC where the data resides. Click NEXT.

×
Add service

☰
FD 4G VPN Router

Please specify a target for this service.

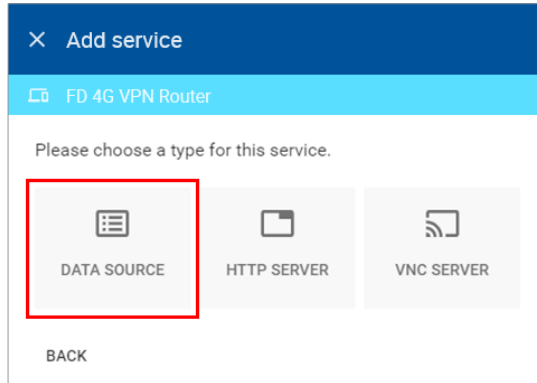
Name

IP address   
e.g. 192.168.140.100

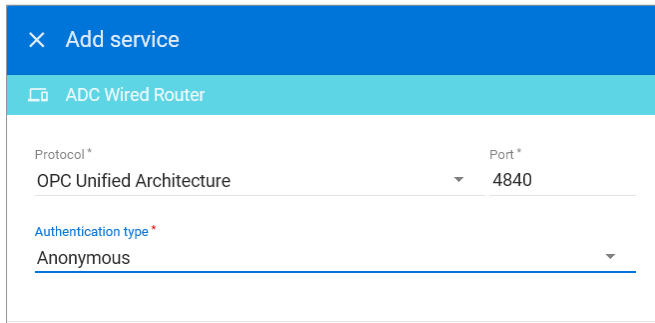
NEXT



Select DATA SOURCE.

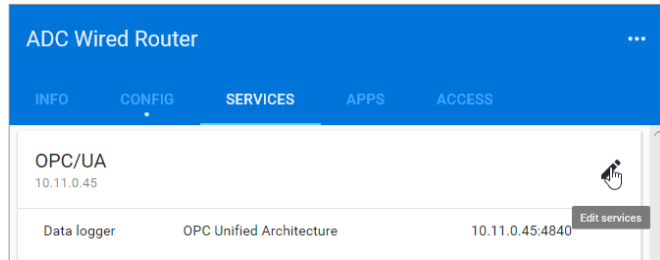


Select the OPC UA protocol and enter the port number of the OPC Server you are using. If your PLC is protected with a password, select “Username and password” as the authentication type and enter the credentials. Then click ADD to continue.

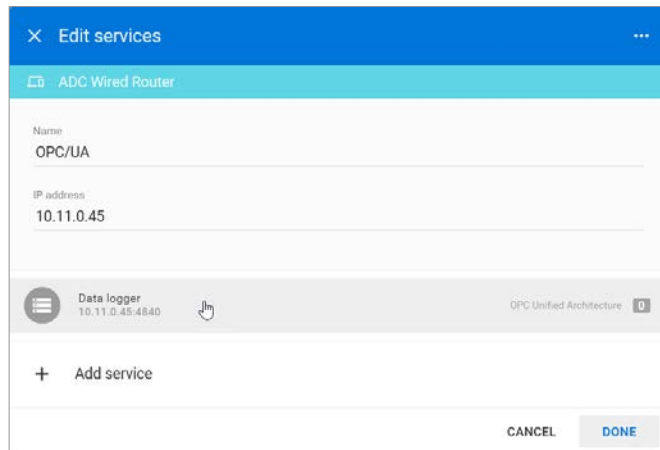


### Configure the data tags

To add a data tag, go to the SERVICES tab for the router and click the Edit services (pencil) icon next to the device for which you want to add the data tag.



This opens the Edit services dialog. Click the name of the existing device for which you would like to add a data tag.



**NOTE:** It is advisable to enter data tags in small batches, and test the variables periodically to verify the entries. The entries can be tested by clicking “RUN TEST” in the Configurator, or from the Cloud Logging Web App as described in the [Data Logger Test Utility](#) section. Please refresh your browser if the information on screen appears to not be updated properly at any time.

The resulting “Edit service” screen displays the parameters for the data source, plus a count of existing data tags. Click OPEN CONFIGURATOR to add or edit tags.

← Edit service

ADC Wired Router

Protocol\* OPC Unified Architecture Port\* 4840

Authentication type\* Anonymous

1 variable

OPEN CONFIGURATOR

REMOVE CANCEL CONFIRM

Data tags can be entered interactively, or a set of tags can be imported from a previously-exported CSV file. Export of sets of data tags is discussed later in the “Export Data Tags” subsection. For this example, select “Add new variable” to manually enter tags.

+1 Add new variable

Import from CSV-file

CANCEL ADD

A data entry screen opens, with one new data tag ready to be entered. Set the relevant parameters for the new data tag. The data tag input fields and supported data types are described in the next two tables, respectively. Subsequent figures illustrate the correct syntax for entering OPC UA addresses. Additional data tags can be entered in this round by clicking “+1” in the lower left corner of the screen. When all the desired tags have been entered click ADD.

Name \*

---

Select a data type \* ▼ Address \*

---

Factor Unit

---

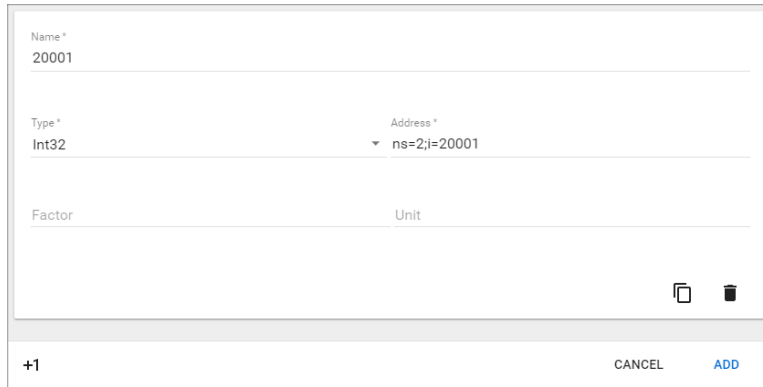
+1
CANCEL
ADD

Data Tag Input Fields	
Field	Description
Name	Give the data tag a logical name.
Select a data type	See next table for the available data types.
Address	See the next subsection, <i>OPC UA Address notation and lookup</i> .
Unit (optional)	Here you can assign a value to a unit, for example, gallons or psi.
Factor (optional)	This allows you to multiply by a value. For example, factor 0.01 divides the data value by 100.

Data Types Supported
Bool
Float32
Float64
Int8
Int16
Int32
Int64
UInt8
UInt16
UInt32
UInt64
String

There are two types of identifiers: string and numeric value. Both require a different data tag address with cloud data logging or notification.

Addressing a data tag when the identifier type is “Numeric” is as follows: ns=(id);i=(identifier). For example, a piece of integer numeric data with a numeric identifier of “20001” would be set up in StrideLinx as shown below.

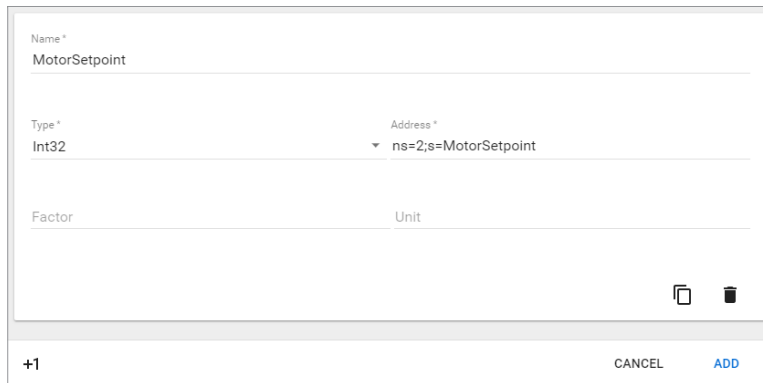


The screenshot shows a configuration form for a data tag. The fields are as follows:

Field	Value
Name*	20001
Type*	Int32
Address*	ns=2;i=20001
Factor	
Unit	

At the bottom of the form, there is a '+1' indicator, a 'CANCEL' button, and an 'ADD' button.

Addressing a data tag when the identifier type is “String” is as follows: ns=(id);s=(identifier). Thus, the same piece of numeric data with a string identifier of “MotorSetpoint” would be set up in StrideLinx as shown below.



The screenshot shows a configuration form for a data tag. The fields are as follows:

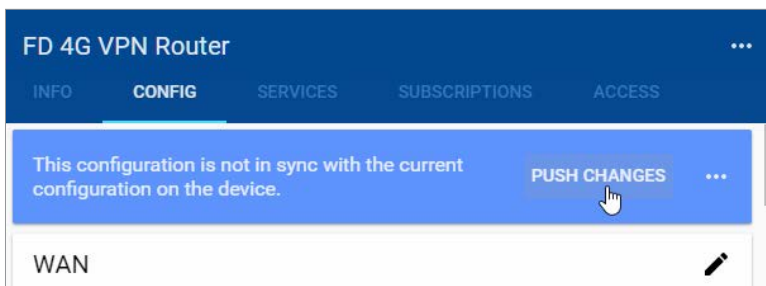
Field	Value
Name*	MotorSetpoint
Type*	Int32
Address*	ns=2;s=MotorSetpoint
Factor	
Unit	

At the bottom of the form, there is a '+1' indicator, a 'CANCEL' button, and an 'ADD' button.

The following subsection, “OPC UA Address notation and lookup,” presents the recommended method to determine the correct address and syntax for your data tag. After all data is entered, click ADD to continue.

Once you have added all the data tags you want to log, you will be prompted to push the configuration to the router.





The data tag entries should now be verified using the procedure described in the “Test Utility” subsection of Chapter 4.



**NOTE:** Additional data tag parameters related specifically to data logging (i.e., sampling interval, data retention policy, and logging only when changed) can be set from the Cloud Logging web app discussed in Chapter 4.

The Cloud Logging web app can now be used to set up data dashboards and to adjust additional data tag parameters related specifically to data logging, and the Cloud Notify web app can be used to set up alarm notifications.

### *Export data tags*

Data tag configurations can be exported in CSV format. The CSV file is downloaded to your local PC, and can later be imported to set up another StrideLinx router.

Select data tags to be exported by clicking the icon for each data tag, or select all data tags at once from the More Options (•••) menu in the upper right corner of the screen. The selected data tags can then be deleted, duplicated, or exported from the pop up menu at the bottom of the screen.

### OPC UA address notation and lookup

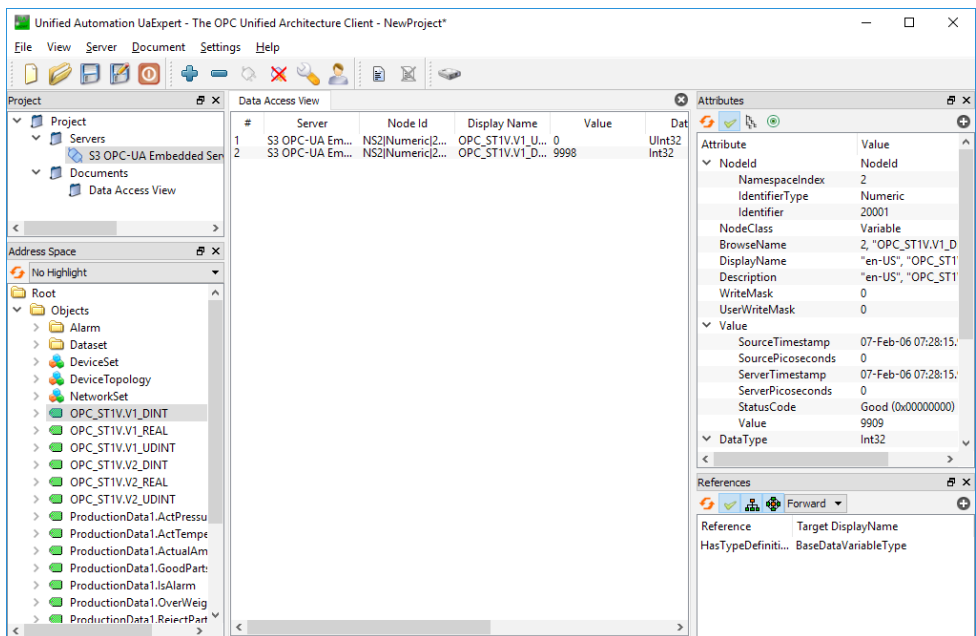
We recommend the UaExpert client software (available from United Automation) to search for tags.

After installing and opening the UaExpert software, complete the following actions to set up a connection with the OPC UA server:

1. Click the right mouse button on “Servers” at the top left.
2. Click “Add Server”.
3. Click “Advanced”.
4. Enter the IP-address and the port of the server and click “Ok”.

After the connection is made with the server, complete the following actions:

5. Find the tag in the “address space” in the bottom left.
6. Select the tag so its details are shown in the attribute window.



The namespace and identifier are the important attributes here. In this example, the namespace and identifier are “2” and “20001”, respectively.

Thus, in this example the addressing of the data tag would look like this: ns=2;i=20001.

# SET UP DATA SOURCE USING ETHERNET/IP PROTOCOL

---



## APPENDIX

# I

In this Appendix...

Set up data source for a device using EtherNet/IP protocol.....	I-3
Error Messages .....	I-13

This manual covers the StrideLinx platform available from 2017 through 2021.

For details covering the StrideLinx Cloud 2.0 platform available after April 2021, please [click here](#) to link to that manual.

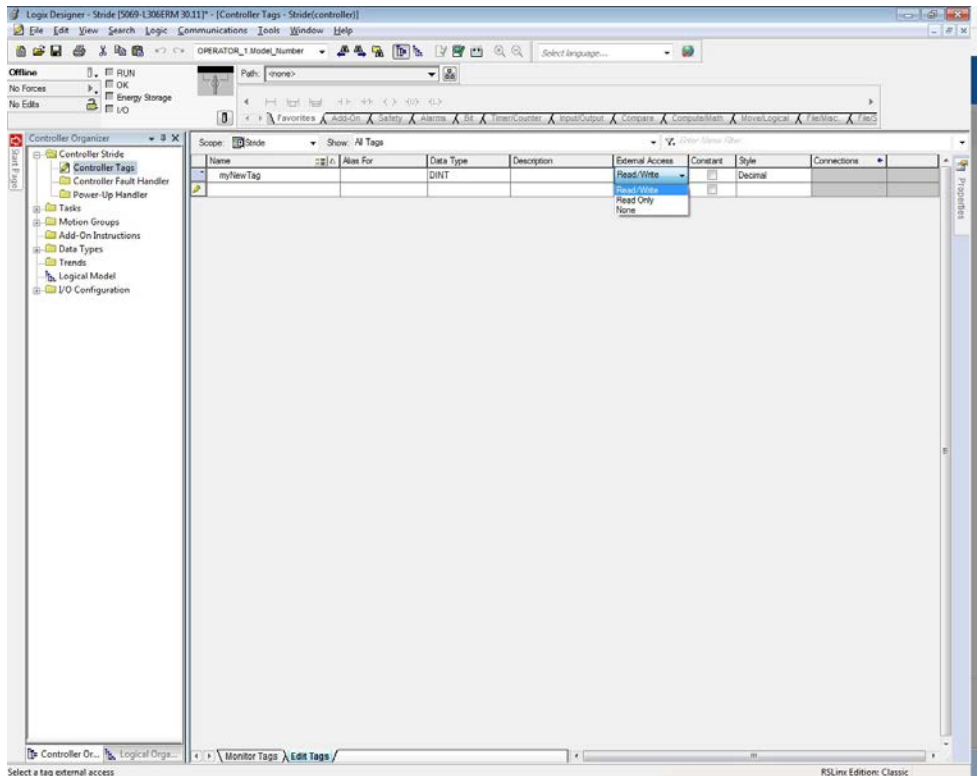
The StrideLinx Cloud 2.0 manual includes details describing the [Activation Code](#) model of Data Logging, Cloud Notify and other add-on features.

For information on the migration wizard from the original platform to StrideLinx Cloud 2.0, [click here](#).

## Set up data source for a device using EtherNet/IP protocol

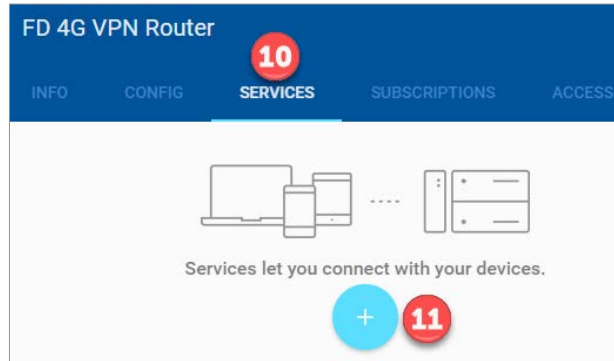
### *Considerations when defining tags to be read using EtherNet/IP*

- The StrideLinx EtherNet/IP data source driver supports the MicroLogix, ControlLogix, CompactLogix and Micro800 families. Explicit and Implicit messaging are not supported.
- StrideLinx EtherNet/IP data sources can communicate to CompactLogix, ControlLogix and FlexLogix Ethernet modules and CPU Ethernet port back to version 15.
- StrideLinx MicroLogix EtherNet/IP driver will communicate to the onboard ethernet ports of the Micrologix 1100, 1200 and 1400. It will also communicate to the onboard ethernet port of the SLC 5/05 CPU (Series A, FW Rev OS501, FRN5 and Series B and C) as well as the ENI Adapter (Series B or newer).
- The file number must always be specified in the Address definition for the Micrologix driver.
- Each StrideLinx data source service consumes 1 TCP connection but no CIP connection (Unconnected Messaging is used).
- To access the tags in the Logix PLCs, the tag attribute “External Access” needs to be set to Read/Write or Read Only, as shown below.



*Configure the address and protocol for the PLC from which data will be read*

Click on the SERVICES tab (10). Click the +(Add) button (11).



Add a Name and the IP Address of the PLC where the data resides. Click NEXT.

×
Add service

🏠
FD 4G VPN Router

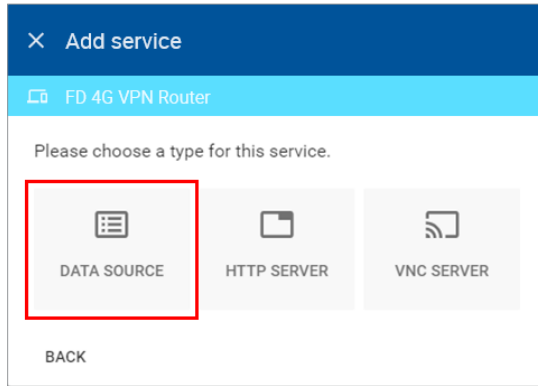
Please specify a target for this service.

Name

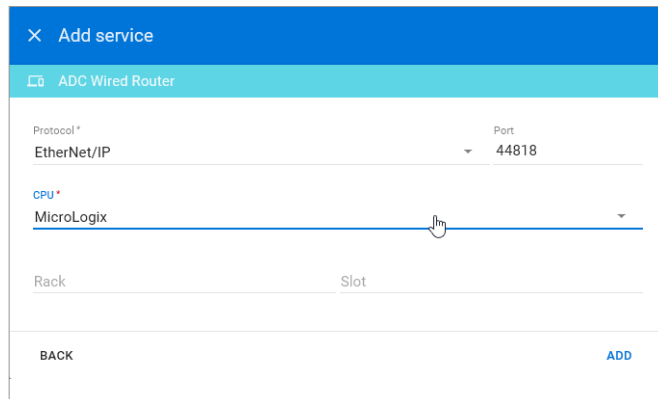
IP address   
e.g. 192.168.140.100

[NEXT](#)

Select DATA SOURCE.

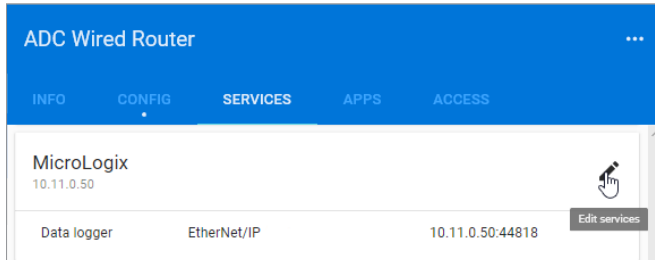


Select the EtherNet/IP protocol. The CPU type (MicroLogix, CompactLogix/ControlLogix/FlexLogix or Micro800) must be selected. If CompactLogix/ControlLogix/FlexLogix or Micro800 is selected, then the Rack number and Slot number must be entered. Click ADD to continue.

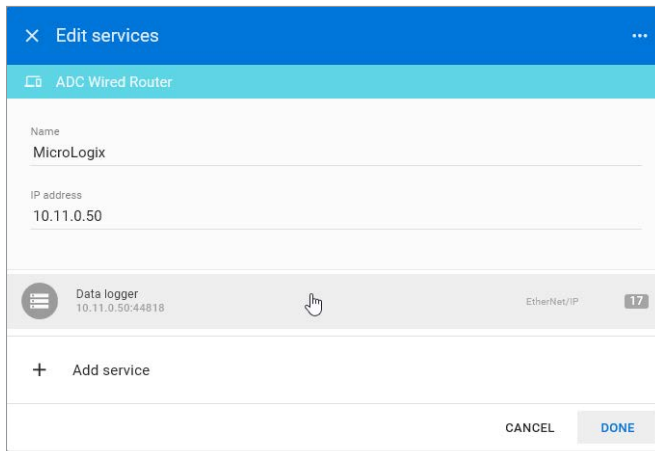


### Configure the data tags

To add a data tag, go to the SERVICES tab for the router and click the Edit services (pencil) icon next to the device for which you want to add the data tag.



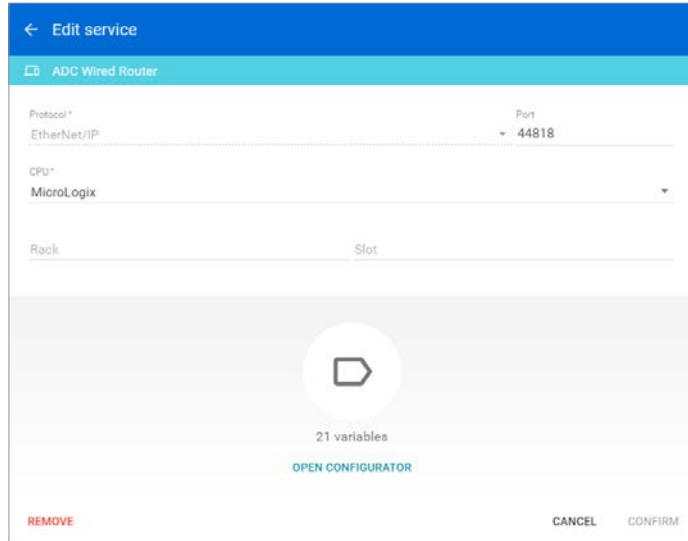
This opens the Edit services dialog. Click the name of the existing device for which you would like to add a data tag.



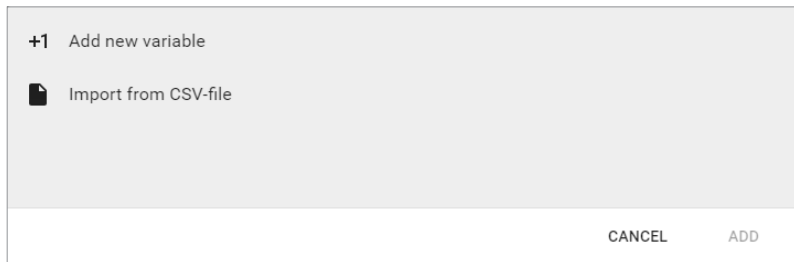
**NOTE:** It is advisable to enter data tags in small batches, and test the variables periodically to verify the entries. The entries can be tested by clicking “RUN TEST” in the Configurator, or from the Cloud Logging Web App as described in the [Data Logger Test Utility](#) section. Please refresh your browser if the information on screen appears to not be updated properly at any time. Possible EtherNet/IP errors and their potential resolutions are listed in the Error Messages subsection at the end of this appendix.



The resulting “Edit service” screen displays the parameters for the data source, plus a count of existing data tags. Click OPEN CONFIGURATOR to add or edit tags.



Data tags can be entered interactively, or a set of tags can be imported from a previously-exported CSV file. Export of sets of data tags is discussed later in the “Export Data Tags” subsection. For this example, select “Add new variable” to manually enter tags.



A data entry screen opens, with one new data tag ready to be entered. Set the relevant parameters for the new data tag. The data tag input fields are described in the next table. Details for data tag addressing with CompactLogix/ControlLogix/FlexLogix, MicroLogix and Micro800 are presented in the next subsections. Additional data tags can be entered in this round by clicking “+1” in the lower left corner of the screen. When all the desired tags have been entered click ADD.

Name \*

---

Select a data type \* Address \*

---

Factor Unit

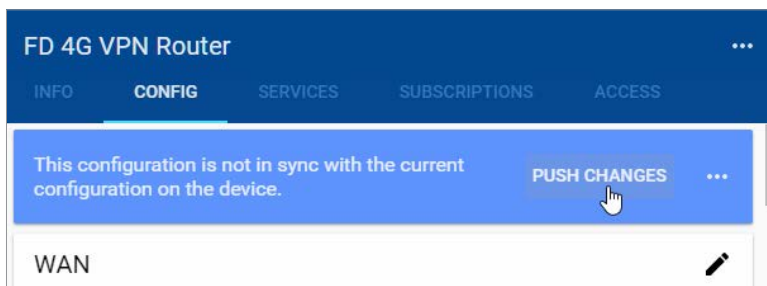
---

+1
CANCEL
ADD

Data Tag Input Fields	
<i><b>Field</b></i>	<i><b>Description</b></i>
Name	Give the data tag a logical name.
Select a data type	See next two subsections for the available data types.
Address	Define at which address in the data block the tag is located. See next three subsections for specific addressing considerations for CompactLogix/ControlLogix/FlexLogix, MicroLogix and Micro800.
Unit (optional)	Here you can assign a value to a unit, for example, gallons or psi.
Factor (optional)	This allows you to multiply by a value. For example, factor 0.01 divides the data value by 100.

After all data is entered, click ADD to continue.

Once you have added all the data tags you want to log, you will be prompted to push the configuration to the router.



The data tag entries should now be verified using the procedure described in the “Test Utility” subsections of Chapter 4 and Chapter 5.



**NOTE:** Additional data tag parameters related specifically to data logging (i.e., sampling interval, data retention policy, and logging only when changed) can be set from the Cloud Logging web app discussed in Chapter 4.

The Cloud Logging web app can now be used to set up data dashboards and to adjust additional data tag parameters related specifically to data logging, and the Cloud Notify web app can be used to set up alarm notifications.

### *Export data tags*

Data tag configurations can be exported in CSV format. The CSV file is downloaded to your local PC, and can later be imported to set up another StrideLinx router.

Select data tags to be exported by clicking the icon for each data tag, or select all data tags at once from the More Options (⋮) menu in the upper right corner of the screen. The selected data tags can then be deleted, duplicated, or exported from the pop up menu at the bottom of the screen.

## CompactLogix/ControlLogix/FlexLogix addressing

This driver uses symbolic name addressing for access to the PLC tags. Enter the tag name (up to 60 characters) in the Address field. This needs to be the base Atomic address of the tag. StrideLinx CANNOT access the full structure, only the structure members and simple Atomic tags.

Data Types Supported		
StrideLinx	EtherNet/IP Data Type	EtherNet/IP Tag Types
Bool	BOOL	Atomic (Base) tags Pre-defined Structure tags* User-defined Structure tags* AOI tags* Program Scope tags**
Float32	REAL	
Int8	SINT	
Int16	INT	
Int32	DINT	
String	STRING	

\* Only the base tag members of any of these type of tags. See next two screenshots.

\*\* Program scope tags require the following prefix syntax: Program: AAAA.BBBB where AAAA is the Program name and BBBB is the tag name.

Name	Alias For	Data Type	Value	Force Mask	Style	Desc
myNewTag		DINT	0		Decimal	
Line 1		Fan_Motor	{...}	{...}		
Line 1.Speed		DINT	0		Decimal	
Line 1.Start		BOOL	0		Decimal	
Line 1.Stop		BOOL	0		Decimal	
Line 1.RunTime		TIMER	{...}	{...}		
Line 1.RunTime.PRE		DINT	0		Decimal	
<b>Line 1.RunTime.ACC</b>		DINT	0		Decimal	
Line 1.RunTime.EN		BOOL	0		Decimal	
Line 1.RunTime.TT		BOOL	0		Decimal	
Line 1.RunTime.DN		BOOL	0		Decimal	
Line 1.Temp		REAL	0.0		Float	

Name\*  
Line1 Motor Run Time

Type\*  
Int32

Address\*  
Line1.RunTime.ACC

Factor \_\_\_\_\_ Unit \_\_\_\_\_

+1 CANCEL ADD

### *MicroLogix addressing*

There are a few different formats of addressing that StrideLinx supports when connecting to the MicroLogix and SLC 500 PLCs.

Addressing syntax is: **Mf:w/b**

Where M = Memory Type  
       f = File Number  
       w = Word Number  
       b = Bit Number

Specific memory types supported for StrideLinx datalogging of MicroLogix and SLC 500 PLCs are listed in the following table.

Data Types Supported							
<i>Memory Type</i>	<i>File Number</i>	<i>Word Number</i>	<i>Bit Number</i>	<i>Description</i>	<i>Flag</i>	<i>Read/Write Type</i>	<i>StrideLinx Data Type</i>
S	2:	0-255		Status		R	Int16
S	2:	0-255	0-15	Status		R	Boolean
B	3, 9: TO 255:	0-255		Binary		R/W	Int16
B	3, 9: TO 255:	0-255	0-15	Binary		R/W	Boolean
T	4, 9: TO 255:	0-255		Timer	.ACC	R/W	Int16
C	5, 9: TO 255:	0-255		Counter	.ACC	R/W	Int16
N	7, 9: TO 255:	0-255		Integer		R/W	Int16
N	7, 9: TO 255:	0-255	0-15	Integer		R/W	Boolean
F	8: to 255:	0-255		Float		R/W	Float32
L	9: to 255:	0-255		Long		R/W	Int32
ST	9: to 255:	0-255		String		R/W	String

## Micro800 addressing

This driver uses symbolic name addressing for access to the PLC tags. Enter the tag name (up to 60 characters) in the Address field. This needs to be the base Atomic address of the tag. StrideLinx can only access Global Variables, and only Atomic data types.

Data Types Supported		
<i>StrideLinx</i>	<i>Micro800 Data Type*</i>	<i>Description</i>
Boolean	BOOLEAN	Single discrete bit
Int8	SINT	Signed integer 8 bit
Int16	INT	Signed integer 16 bit
UInt16	UINT	Unsigned integer 16 bit
	WORD	
Int32	DINT	Signed integer 32 bit
UInt32	UDINT	Unsigned integer 32 bit
	DWORD	
Float32	REAL	Floating point 32 bit
String	STRING	String (up to 254 characters)
All of the above	Single Dimension Arrays	Single dimension arrays of the data types above

**\* Global Variables only (No Program Local Variables or Function Block Local Variables), Atomic Data types and single dimension elements of Atomic Data types only**

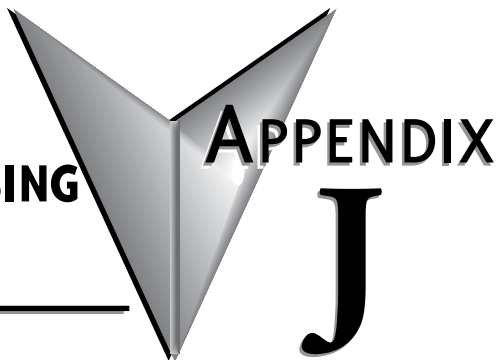
### Error Messages

The following error message may arise during testing of the data source configuration. Possible causes and remedies are shown for each error.

<b>EtherNet/IP Error List</b>	
<b><i>CompactLogix / ControlLogix / FlexLogix and Micro800</i></b>	
<b><i>Error Text</i></b>	<b><i>Cause / Remediation Steps</i></b>
PLC Timeout	No reply of any type from device. Device not existing, powered down or IP address incorrect.
TCP connection denied	Device exists but does not appear to be an EtherNet/IP device. Wrong IP address or EtherNet/IP not enabled on product.
Too much data received. Ensure Structure element is requested.	Full structure requested. Tagname should be ELEMENT of structure.
Error 0x01, EXT STS 0x0311: <Bad rack #>	Rack number does not exist for device. Default is typically 1.
Error 0x01, EXT STS 0x0312: <Bad slot #>	Slot number incorrect for device. Default is typically 0.
Error 0x04, EXT STS 0x00: <Bad tagname>	Tagname entered incorrectly or does not exist in device.
Error xxx, EXT STS xxx	Manufacturer's error code. Consult documentation of manufacturer for cause and resolution.
<b><i>MicroLogix</i></b>	
<b><i>Error Text</i></b>	<b><i>Cause / Remediation Steps</i></b>
PLC Timeout	No reply of any type from device. Device not existing, powered down or IP address incorrect.
TCP connection denied	Device exists but does not appear to be an EtherNet/IP device. Wrong IP address or EtherNet/IP not enabled on product.
Error 0x10, EXT STS 0x00: <Bad tagname>	Address entered incorrectly or not in project. Correct or add to project.
Error xxx, EXT STS xxx	Manufacturer's error code. Consult documentation of manufacturer for cause and resolution.

# **SET UP DATA SOURCE USING BACNET/IP PROTOCOL**

---



In this Appendix...

Set up data source for a device using BACnet/IP protocol ..... J-3



### J

This manual covers the StrideLinx platform available from 2017 through 2021.

For details covering the StrideLinx Cloud 2.0 platform available after April 2021, please [click here](#) to link to that manual.

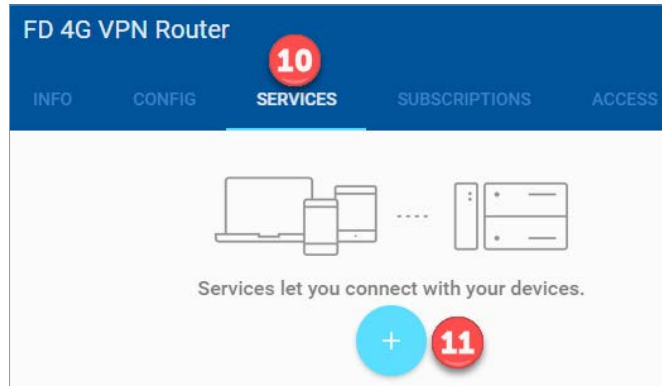
The StrideLinx Cloud 2.0 manual includes details describing the [Activation Code](#) model of Data Logging, Cloud Notify and other add-on features.

For information on the migration wizard from the original platform to StrideLinx Cloud 2.0, [click here](#).

## Set up data source for a device using BACnet/IP protocol

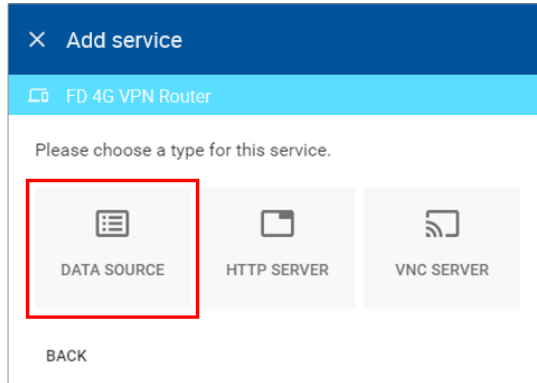
*Configure the address and protocol for the PLC from which data will be read*

Click on the SERVICES tab (10). Click the +(Add) button (11).

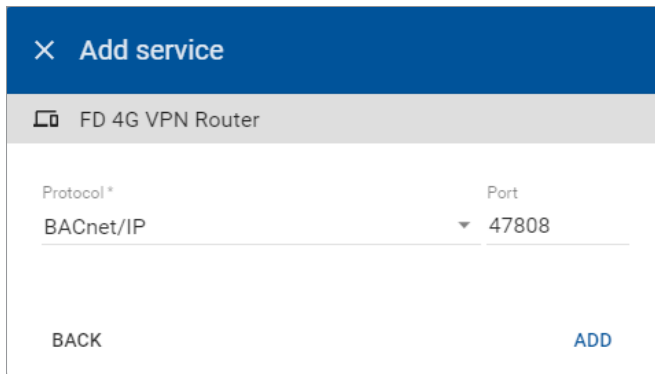


Add a Name and the IP Address of the PLC where the data resides. Click NEXT.

Select DATA SOURCE.

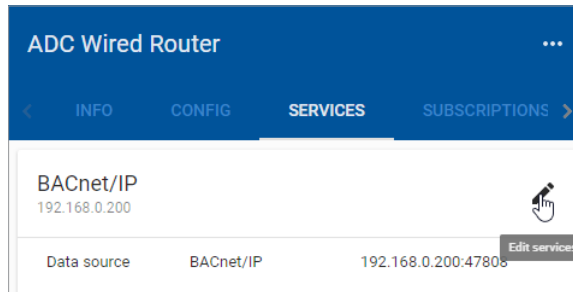


Select the BACnet/IP protocol and enter the port number of the BACnet device (47808 by default). Click ADD to continue.

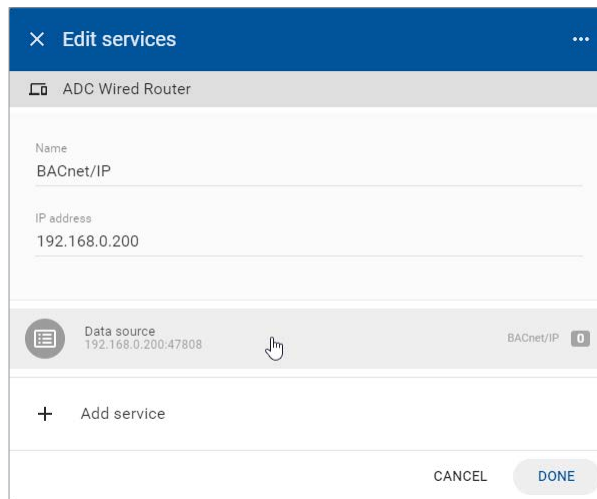


### Configure the data tags

To add a data tag, go to the SERVICES tab for the router and click the Edit services (pencil) icon next to the device for which you want to add the data tag.

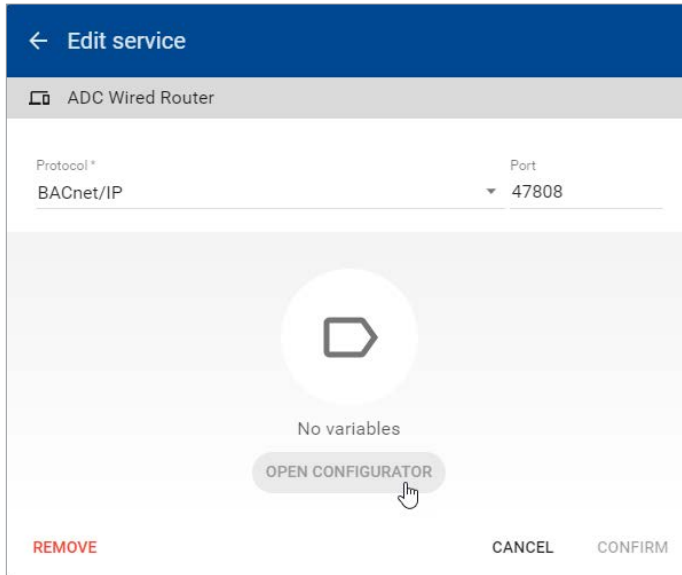


This opens the Edit services dialog. Click the name of the existing device for which you would like to add a data tag.

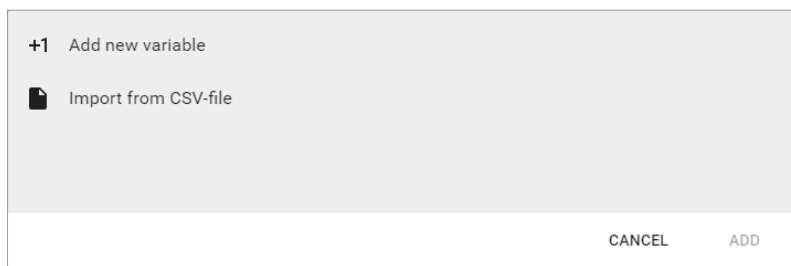


**NOTE:** It is advisable to enter data tags in small batches, and test the variables periodically to verify the entries. The entries can be tested by clicking "RUN TEST" in the Configurator, or from the Cloud Logging Web App as described in the [Data Logger Test Utility](#) section. Please refresh your browser if the information on screen appears to not be updated properly at any time. Possible EtherNet/IP errors and their potential resolutions are listed in the Error Messages subsection at the end of this appendix.

The resulting “Edit service” screen displays the parameters for the data source, plus a count of existing data tags. Click OPEN CONFIGURATOR to add or edit tags.



Data tags can be entered interactively, or a set of tags can be imported from a previously-exported CSV file. Export of sets of data tags is discussed later in the “Export Data Tags” subsection. For this example, select “Add new variable” to manually enter tags.



A data entry screen opens, with one new data tag ready to be entered. Set the relevant parameters for the new data tag. The data tag input fields are described in the next table. Details for determining data tag addressing with BACnet/IP is presented in the next subsection. Additional data tags can be entered in this round by clicking “+1” in the lower left corner of the screen. When all the desired tags have been entered click ADD.

Name \*

---

Select a data type \*

Object Type \*

Property \*

Search...

Object Instance \* Search...

---

Factor

Unit

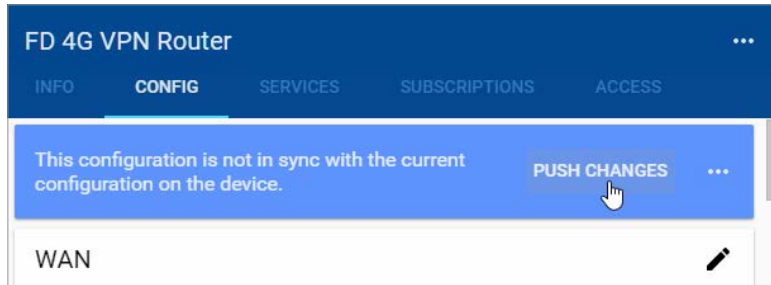
---

+1
CANCEL
ADD

Data Tag Input Fields	
<i>Field</i>	<i>Description</i>
Name	Give the data tag a logical name.
Select a data type	See next two subsections for the available data types.
Object Type	BACnet addressing parameters. See "Find BACnet addresses using BACnet Explorer" on page J-9 for help determining parameters.
Object Instance	
Property	
Unit (optional)	Here you can assign a value to a unit, for example, gallons or psi.
Factor (optional)	This allows you to multiply by a value. For example, factor 0.01 divides the data value by 100.

After all data is entered, click ADD to continue.

Once you have added all the data tags you want to log, you will be prompted to push the configuration to the router.



The data tag entries should now be verified using the procedure described in the “Test Utility” subsections of Chapter 4 and Chapter 5.



---

**NOTE:** Additional data tag parameters related specifically to data logging (i.e., sampling interval, data retention policy, and logging only when changed) can be set from the Cloud Logging web app discussed in Chapter 4.

---

The Cloud Logging web app can now be used to set up data dashboards and to adjust additional data tag parameters related specifically to data logging, and the Cloud Notify web app can be used to set up alarm notifications.

### *Export data tags*

Data tag configurations can be exported in CSV format. The CSV file is downloaded to your local PC, and can later be imported to set up another StrideLinx router.

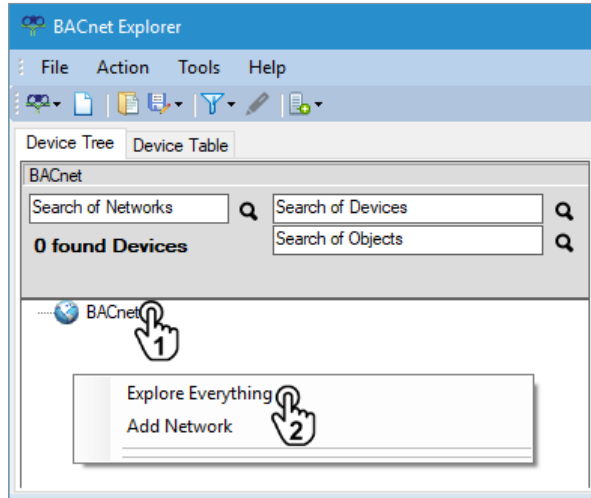
Select data tags to be exported by clicking the icon for each data tag, or select all data tags at once from the More Options (⋮) menu in the upper right corner of the screen. The selected data tags can then be deleted, duplicated, or exported from the pop up menu at the bottom of the screen.

### *Find BACnet addresses using BACnet Explorer*

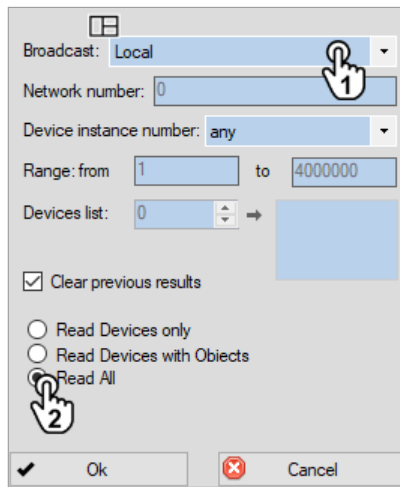
The address of a BACnet variable consists of an object type, object instance and object property. The BACnet Explorer software from Cimetrics, Inc. (<https://www.cimetrics.com/products/bacnet-explorer>) is one convenient method to determine the addressing for your variables.

To retrieve BACnet addresses using BACnet Explorer:

- Connect your PC to the BACnet device, or its network, and open BACnet Explorer
- Right-click 'BACnet' in the device tree (1) and select 'Explore Everything' (2).

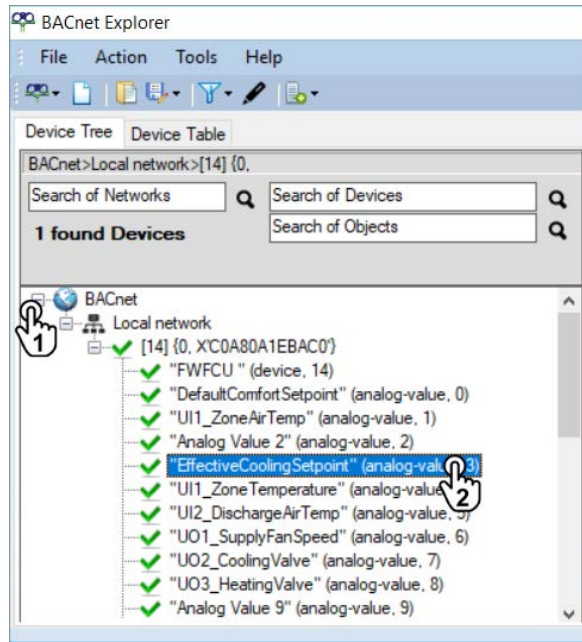


- Select 'Local' as broadcast type (1), select 'Read All' (2) and press OK.



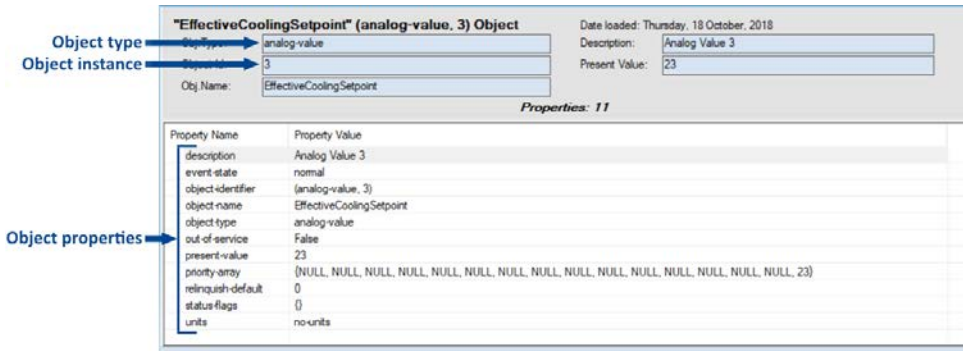


- Expand the device tree (1) and select an object from the list (2).



**NOTE:** If your device is not listed, connect your PC to the BACnet device, or its network, before you open BACnet Explorer.

- After selecting an object, you'll see its details to the right. Record the Object Type, Object Instance and Object Property of all variables that you would like to log. These values can now be used to define data tags in your StrideLinX data source.



**NOTE:** If the object property is an array, you can choose an index number to read a specific element of the array. Be aware that the first index in an array is often 0, not 1.

# SET UP DATA SOURCE USING MELSEC PROTOCOL

---



## In this Appendix...

Set up data source for a device using MELSEC protocol .....	K-3
PLC settings .....	K-4
Select a communication protocol .....	K-9
<b>Add variables (new, import) .....</b>	<b>K-11</b>
Manually add new variables .....	K-11
Import variables from a file (or device) .....	K-12
<b>Test variables .....</b>	<b>K-13</b>
<b>Connecting StrideLinx to Q series Ethernet module QJ71E71-100 with MELSEC Protocol.....</b>	<b>K-14</b>

This manual covers the StrideLinx platform available from 2017 through 2021.

For details covering the StrideLinx Cloud 2.0 platform available after April 2021, please [click here](#) to link to that manual.

The StrideLinx Cloud 2.0 manual includes details describing the [Activation Code](#) model of Data Logging, Cloud Notify and other add-on features.

For information on the migration wizard from the original platform to StrideLinx Cloud 2.0, [click here](#).

**K**

## Set up data source for a device using MELSEC protocol

### *Supported hardware and firmware*

StrideLinX routers support Cloud Logging via MELSEC Communication in firmware 3.17 and newer, for the following Mitsubishi PLCs:

- MELSEC-L Series: LO2CPU-P\*
- MELSEC-Q Series
- MELSEC iQ-R Series: R08CPU\*
- MELSEC iQ-F Series

\* Other CPUs in this series may also be supported, but are unconfirmed.



---

**NOTE:** Please first activate Cloud Logging or start the 30 day free trial if you haven't already.

---

**K**

The first step in Cloud Logging is setting up a data source. This is done by selecting a communication protocol and defining the variables. This appendix shows you how to do this for a Mitsubishi PLC in both MELSOFT GX Works2 and GX Works3.

## PLC settings

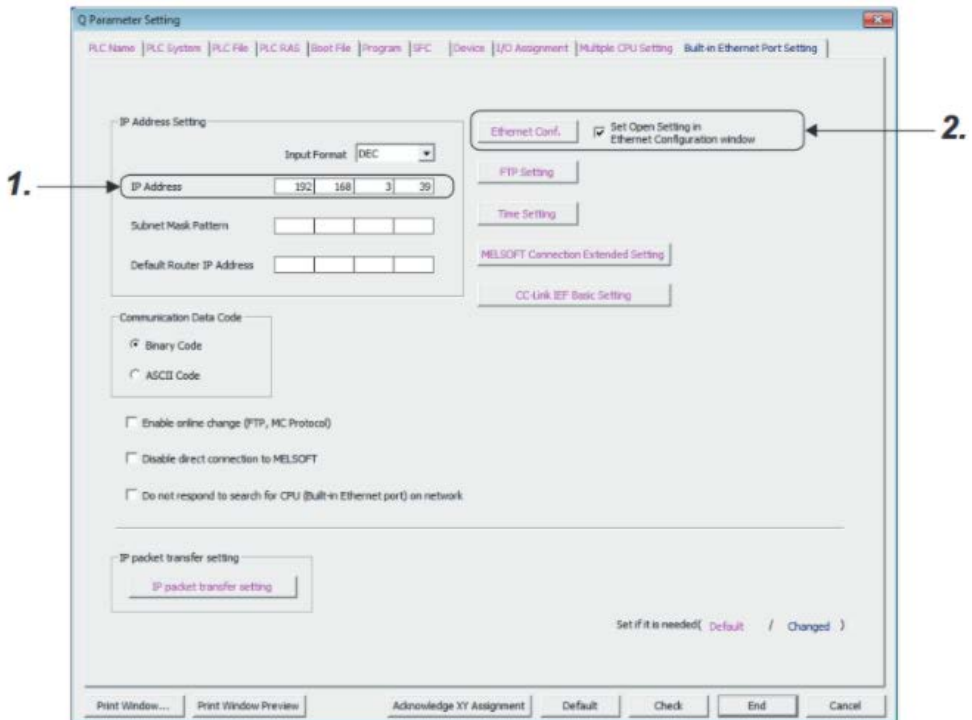
Depending on the type of Mitsubishi PLC you're using, the setup of the PLC has to be performed in either GX Works2 or GX Works3:

- L and Q series are set up using GX Works2.
- iQ-F and iQ-R series are set up using GX Works3.

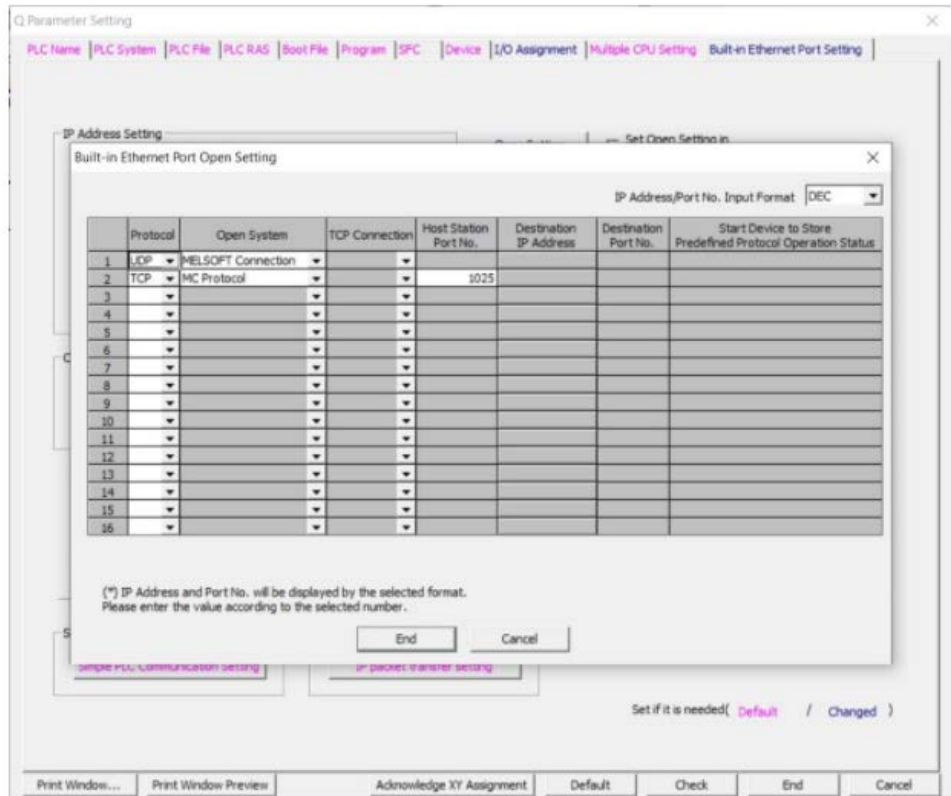
## GX Works2

Setting up the CPU Module enables the PLC to communicate with an external device (i.e., your StrideLinX router). This can be done by following the next steps:

- In the Project Window, open **Parameter > PLC Parameter** and go to the tab **Built-in Ethernet Port Setting**.
- If you haven't already, enter an **IP address** for the CPU Module (1) and a **Subnet Mask Pattern** (usually 255.255.255.0).
- Check the option "**Set Open Setting in Ethernet Configuration window**" and press **Ethernet Conf** (2).



- On a new row, select protocol “TCP”, select open system “MC Protocol” and choose a Host Station Port Number between 1025-4999 or 5010-65534.



K



**NOTE: TCP or UDP?**

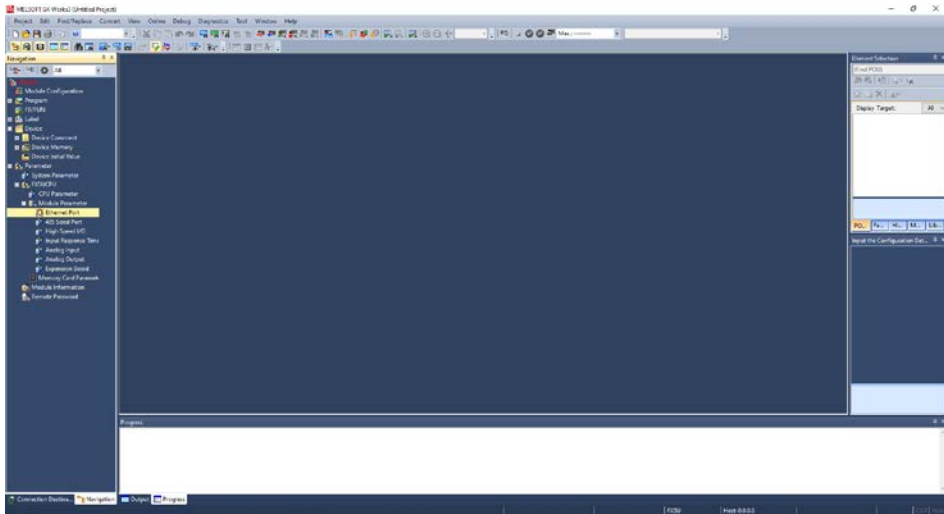
*We support both the TCP and UDP protocols but recommend using TCP as this protocol is less error-prone.*

Your PLC is now ready and you can continue setting up your StrideLinX router by selecting a communication protocol.

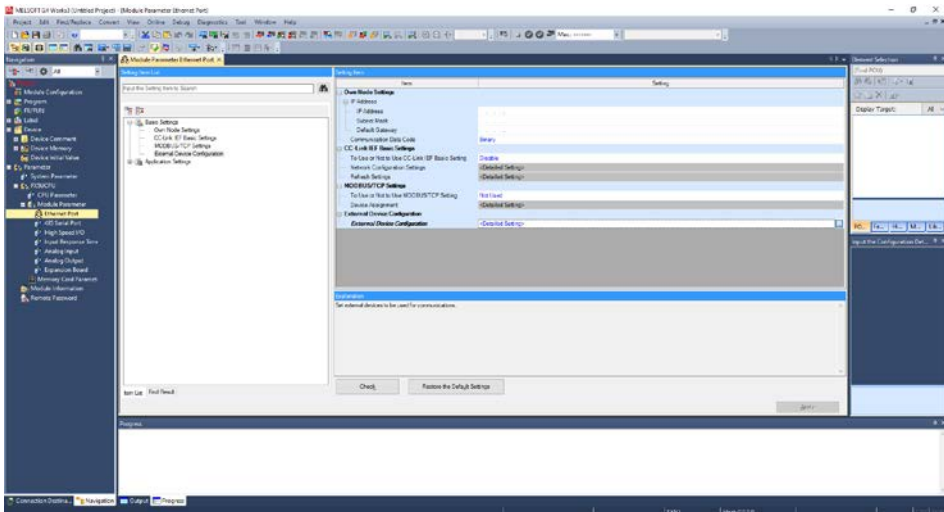
## GX Works3

Setting up the CPU Module enables the PLC to communicate with an external device (i.e., your StrideLinX router). This can be done by following the next steps:

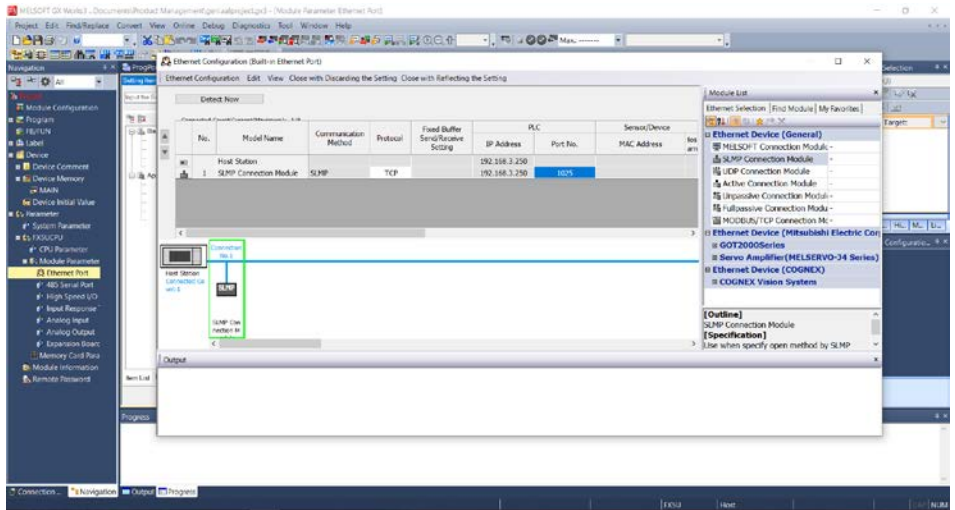
- In the Navigation pane, go to **Parameter > CPU (FX5UCPU in the example below) > Module parameter**.
- Open the **Ethernet Port** parameters.



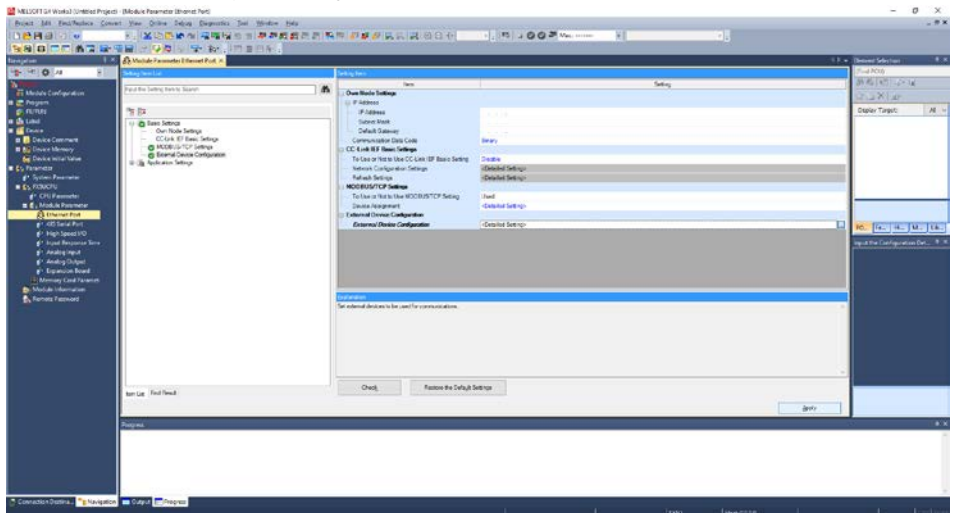
- Expand **Basic Settings** in the Item List and double click **External Device Configuration**.
- Expand Setting Item **External Device Configuration** and open the External Device Configuration window by double clicking “<Detailed Setting>”.



- Expand **Ethernet Device (General)** in the Module List.
- Drag and drop **SLMP Connection** into the grey area. This is the MELSEC Communication Protocol.
- Select protocol “TCP” and choose a Port No. between 1025-4999 or 5010-65534.
- Save the setting by pressing **Close with Reflecting the Setting** at the top.



- **Apply** the new project setting.



Now all that's left is to write these settings to the PLC.



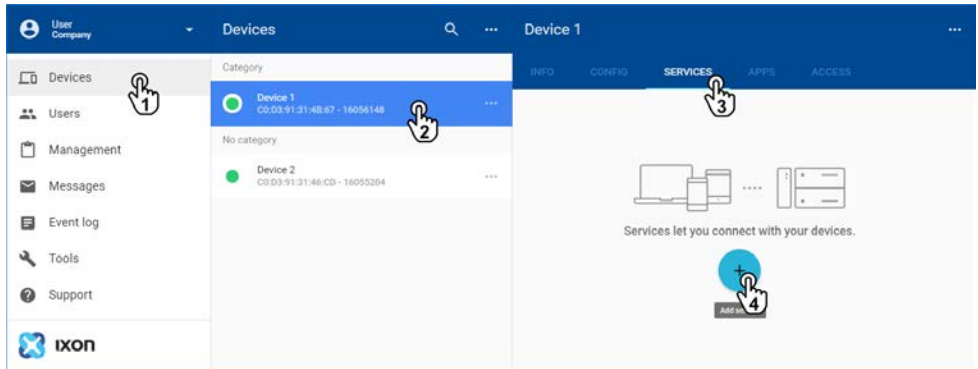




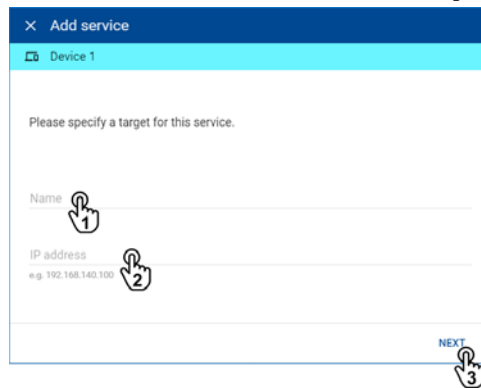
## Select a communication protocol

First, select a communication protocol. This is the protocol that your StrideLinX router uses to communicate with the PLC.

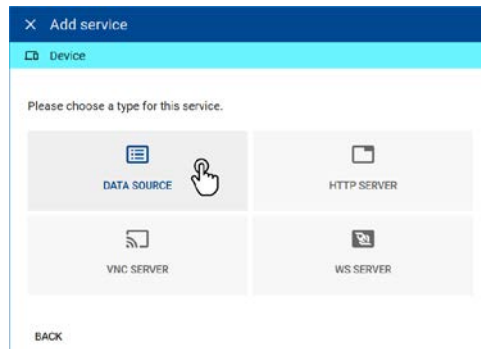
- Go to **Devices** (1) in the main menu, select your StrideLinX router (2) open its **Services** tab (3), and press **Add service** (4).



- Name the PLC (1), enter the PLC's **IP address** (2), and press **Next** (3).



- Select the **Data source** service type.



- Select “MELSEC Communication Protocol” from the drop down list and enter the following details:

Data Source Settings	
Field	Description
Port	Enter the Port No. that you configured in your PLC.  <i>This is named “Host Station Port Number” in GX Works2.</i>
MELSEC Series	The Mitsubishi MELSEC PLC series to which your PLC belongs.  <i>If you’re unsure, please consult the Mitsubishi website. “QnUCPU” is Mitsubishi’s notation for every MELSEC-Q Series PLC with CPU type Q..U..CPU, for example Q04UDVCP or Q26UDEHCP.</i>
Transport protocol	Select the same protocol that you configured in your PLC.
Network No. and PC No.	If configured in the PLC, enter the correct settings here. If not, leave the default settings.  <i>Applicable when using a custom MELSEC PLC network.</i>
Request destination module I/O No. and Request destination module station No.	If configured in the PLC, enter the correct settings here. If not, leave the default settings.  <i>Applicable when using a specific I/O module for communication.</i>
Authentication Type	The Ethernet connection in the PLC may be password protected. Enter the password or leave it empty if no password is configured on the PLC.

- Press **Add** to create the data source.

## Add variables (new, import)

Once you've added a Data Source and selected a communication protocol, you can start adding variables. This is done in the configurator tool, specifically designed to quickly **add**, **duplicate**, **import**, **export**, and **remove** variables.

- Go to **Devices** in the main menu, select your StrideLinx router, open its **Services** tab, and edit the PLC's services.
- Select **Data source** and press **Open configurator**.
- To add a variable press **Add variable**.


You can choose to:

- **Manually** add new variables
- **Import** variables from a file (or device)

### Manually add new variables

- Press **Add new variable**.
- Enter your variable's **name**, **type**, additional information, and press **Add**. The table below contains explanatory text for each text field. Use GX Works to find these values for each variable that you want to log.

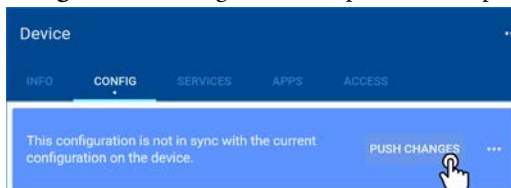
Data Tag Input Fields		
Field	Description	Example
Name	Enter a name for the variables.	Temperature
Type	The variable's data type	Unsigned word
Device Type	The variable's device type	D - Data register
Device No.	Address in the PLC memory	100
Factor (optional)	Multiplies the value (leave empty if boolean)	0.1
Unit (optional)	Displayed text behind the value	Celsuis

You can easily duplicate  this variable if you're adding variables that are only slightly different. This way you only have to make small adjustments.



**NOTE:** After this next step, the config push, the device will temporarily disconnect to reconfigure its network settings and will automatically reconnect. This may take a minute.

- Press **Push changes** in the config tab to complete the setup.



## Import variables from a file (or device)

You can easily **copy variables from one device to another** by exporting the variables and then importing them in your new device.

When you press **Import from CSV-file**, you'll see a browse window.

- Select a CSV file to import and press **Open**.
- When the file has been read, press **Add** to add all variables to your data source.

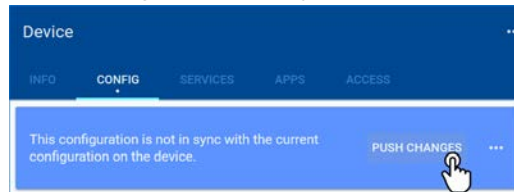


---

**NOTE:** After this next step, the config push, the device will temporarily disconnect to reconfigure its network settings and will automatically reconnect. This may take a minute.

---

- Finally, press **Push changes** in the config tab to complete the setup.

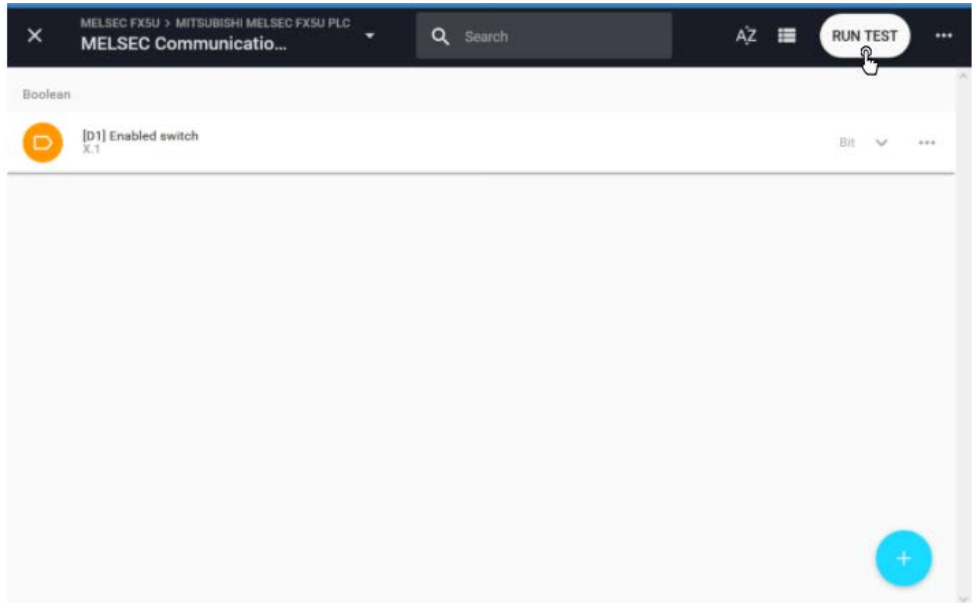


Now that you've added the variables, you can test if they're configured properly.

## Test variables

The test utility is used to **check if all the added variables are set correctly**. It shows the **status** of every variable and displays the variables' **latest values** if everything is configured correctly. If not, it will show an error message.

- In the configurator, press **Run test**.



A connection will now be set up to stream the data directly to your computer, using:

- Port: 443
- Transport Protocol: TCP
- Application Protocol: WebSocket

### *Unexpected result?*

If the test utility shows unexpected values, please check if the addresses and data types of all variables are entered correctly.

If you get no data at all, please also check that the above listed port and protocols are not being blocked by your computer's or company's firewall.

## Connecting StrideLinx to Q series Ethernet module QJ71E71-100 with MELSEC Protocol

← Edit service

Chris ADC Router2

Protocol \* **a**  
MELSEC Communication Protocol

Port \* **b**  
2050

CPU \* **c**  
Q (other CPU types)

Transport protocol \* **d**  
TCP

Network No. \* **e**  
0

PC No. \* **f**  
FF

Request destination module I/O No. \* **g**  
03FF

Request destination module station No. \* **h**  
0

Authentication type \*  
None

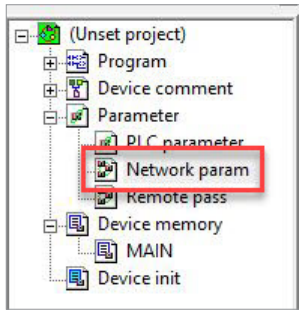
5 variables

[OPEN CONFIGURATOR](#)

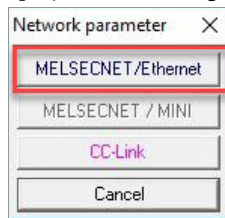
REMOVE CANCEL CONFIRM

- Choose the MELSEC Communication Protocol
- The port number needs to match the “Host station Port No.” field in the “Open settings” dialog described later in this document. NOTE: the value configured in StrideLinx platform is in decimal format but the value in the Mitsubishi programming software is in Hex format. So in the example above, using a value of 2050 here should be 0802 in the Mitsubishi programming software.
- Choose the “Q (other CPU types)” option.
- Choose TCP transport protocol.
- Use a value of 0 for the “Network Number”.
- Leave the default value of FF for the “PC number”.
- Leave the default value of 03FF for the “Request destination module I/O No”.
- Use a value of 0 for the “Request destination module station No”.

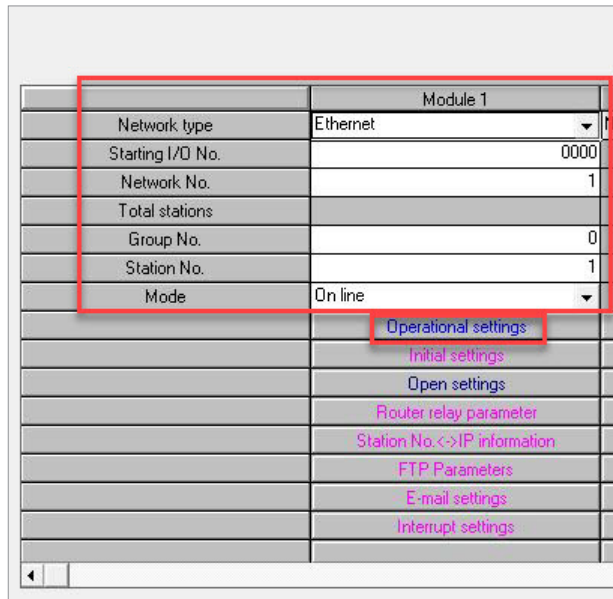
Module setup in the Mitsubishi programming software:



- Double click on the “Network param” option on the left-hand side tree under the “Parameter” section of the project. This will generate a new dialog box.



- Select the “MELSECNET/Ethernet” option in the “Network parameter” dialog.



- Configure the settings as shown in the dialog above.



- Next, click on the “Operational settings” button to open a new dialog.

- Configure the options as shown above.
- IP address: choose a unique IP address that is compatible with the subnet of the LAN side of your StrideLinX router.
- Click on the “End” button after setting up this dialog.

	Protocol	Open system	Fixed buffer	Fixed buffer communication procedure	Pairing open	Existence confirmation	Host station Port No.	Transmission target device IP address	Transmission target device Port No.
1	TCP	Unpassive	Receive	Procedure exist	Disable	No confirm	0802		
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									
16									

End      Cancel

- Now click on the “Open settings” button in the “MELSECNET/Ethernet” dialog to display the settings above.

- Configure your ethernet module to match the settings above. NOTE: the “Host station Port No.” must match the setup in the StrideLinx router. The value shown here is in hex format while the value in the StrideLinx router is in decimal format.
- Click on the “End” button and write these values to your PLC. A power cycle may be required on the PLC for these settings to take effect.

# CUSTOM BRANDING

---



## In this Appendix...

Custom branding.....	L-3
Basic branding .....	L-3
Premium branding .....	L-6

This manual covers the StrideLinx platform available from 2017 through 2021.

For details covering the StrideLinx Cloud 2.0 platform available after April 2021, please [click here](#) to link to that manual.

The StrideLinx Cloud 2.0 manual includes details describing the [Activation Code](#) model of Data Logging, Cloud Notify and other add-on features.

For information on the migration wizard from the original platform to StrideLinx Cloud 2.0, [click here](#).

## Custom branding

We understand how important branding and customer loyalty is. This is why you have the option to white label the StrideLinx platform, applying your custom brand, and essentially making it your very own IoT platform.

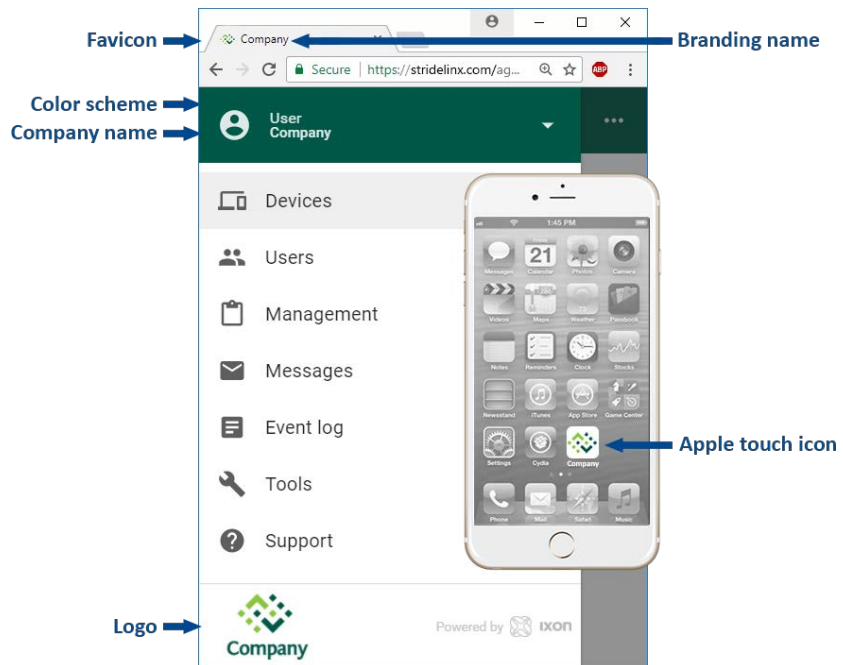
We distinguish between two levels of custom branding: basic and premium branding. Basic branding enables you to apply your corporate identity (company logo, color scheme, etc.) to the StrideLinx platform. Additionally, premium branding enables you to customize the login page, set a custom URL and support/contact information, making it possible for you to market our service as your own.

There are a variety of emails sent from the platform to users: invitation, link to change password, alert that password has changed, status of subscriptions, and other emails. With the basic service, all emails will come from “StrideLinx@AutomationDirect.com”. Invite emails will all come from the company name you have entered, as an alias. That is, the email will be from “YourCompany <StrideLinx@AutomationDirect.com>”.

When you have purchased the Premium Branding license, **all** emails will come from the company name you have configured as an alias.

### Basic branding

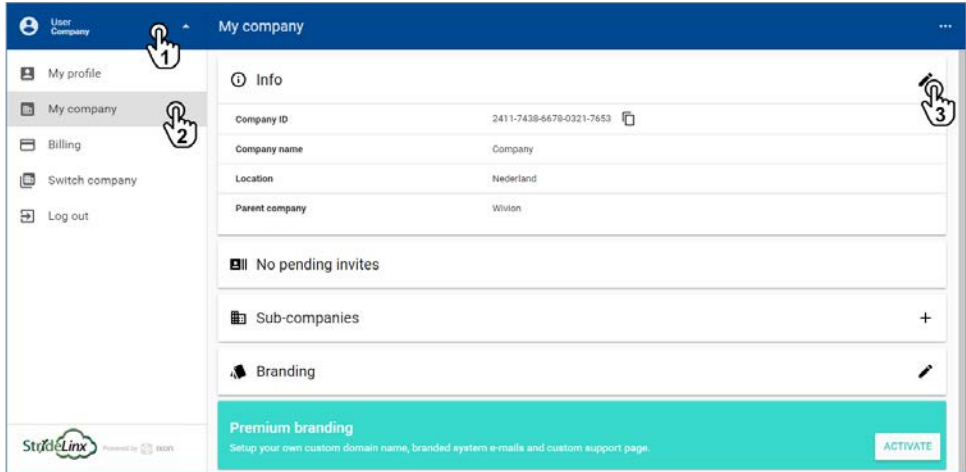
Basic branding is by default included in your company account and enables you to set your own company name, branding name, logo, favicon, Apple touch icon, and color scheme. These changes apply to all pages of the StrideLinx platform as well as e-mails sent from the platform.



## Set up your branding

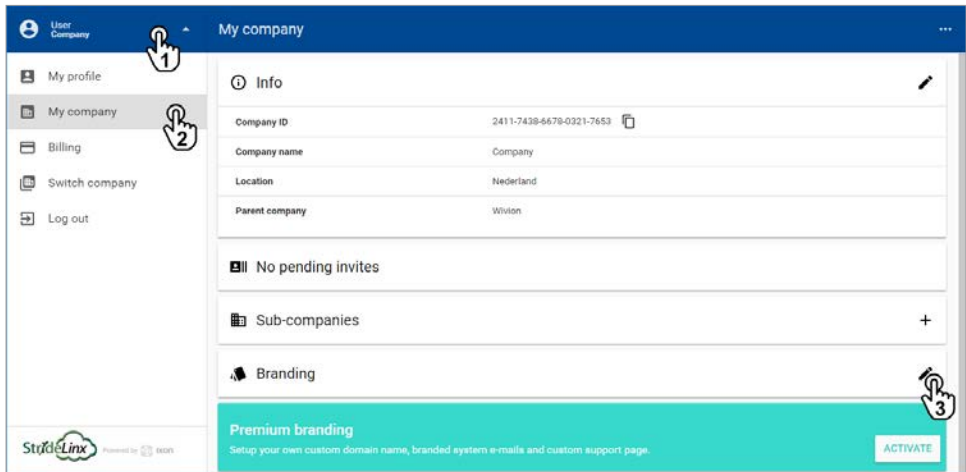
The company name is first set when a company account is created. If necessary, it can be changed as follows:

Go to the account menu (1), select “My company” (2) and click the pencil icon (3) in the “Info” section to edit the company name.



Setting up your own branding name, logo, favicon, Apple touch icon, and color scheme can be done as follows:

Go to the account menu (1), select “My company” (2) and click the pencil icon (3) in the “Branding” section.



Here you can edit the branding name, primary/accent color, and upload a logo, favicon, and Apple touch icon. The Apple touch icon is the icon you see on your Apple device when you bookmark a web page to your home screen, as depicted in the image at the beginning of this section.



**NOTE:** Images up to 10MB can be uploaded. The following formats are supported: .jpg, .jpeg, .png, .bmp, .tiff, .ico.

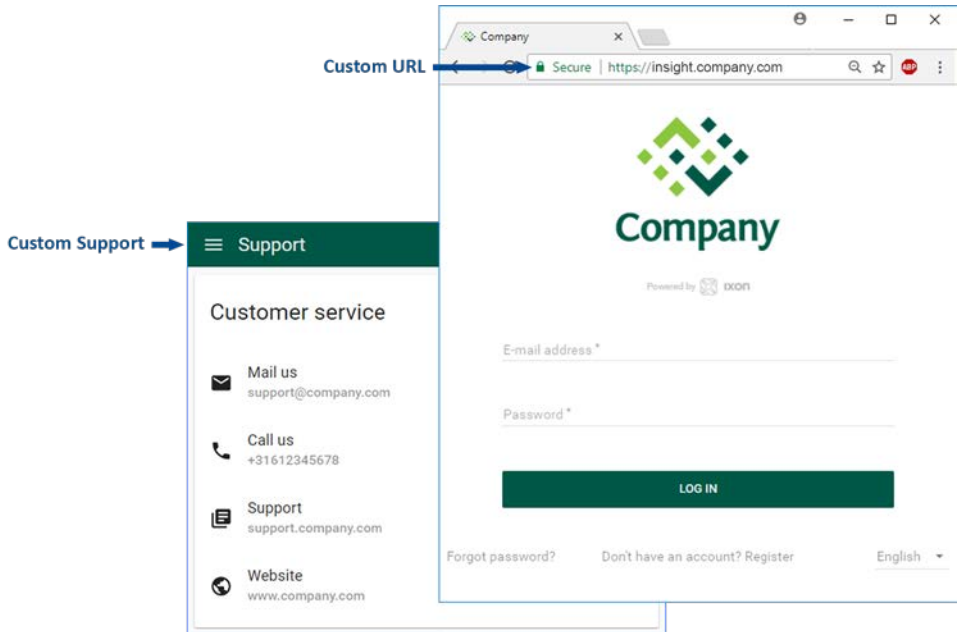
The screenshot shows a dialog box titled "Edit branding" with a close button (X) in the top left corner. The dialog contains the following fields and controls:

- Name:** A text input field with the placeholder text "Name" and a sub-note "Also used as the title of your browser tab". A blue arrow labeled "Enter name" points to this field.
- Logo:** An upload icon (a circle with an upward arrow) and the label "Logo". A blue arrow labeled "Upload icon" points to this icon.
- Favicon:** An upload icon and the label "Favicon".
- Apple touch icon:** An upload icon and the label "Apple touch icon".
- Primary color:** A color selection control (a black circle) and the label "Primary color". Below it is the text "Only hexadecimal color codes".
- Accent color:** A color selection control (a black circle) and the label "Accent color". Below it is the text "Only hexadecimal color codes". A blue arrow labeled "Set color" points to this control.
- Buttons:** "CANCEL" and "CONFIRM" buttons at the bottom right. A hand cursor icon with the number "1" is pointing to the "CONFIRM" button.

Changes will be applied when you click “Confirm” (1).

## Premium branding

Premium branding enables additional branding options, essentially making it your very own IoT platform. You can set your own custom StrideLinx platform URL, for which we'll automatically generate the necessary SSL certificate. Additionally, you'll also be able to set your own contact or support information, making it easier for your customers to contact you.

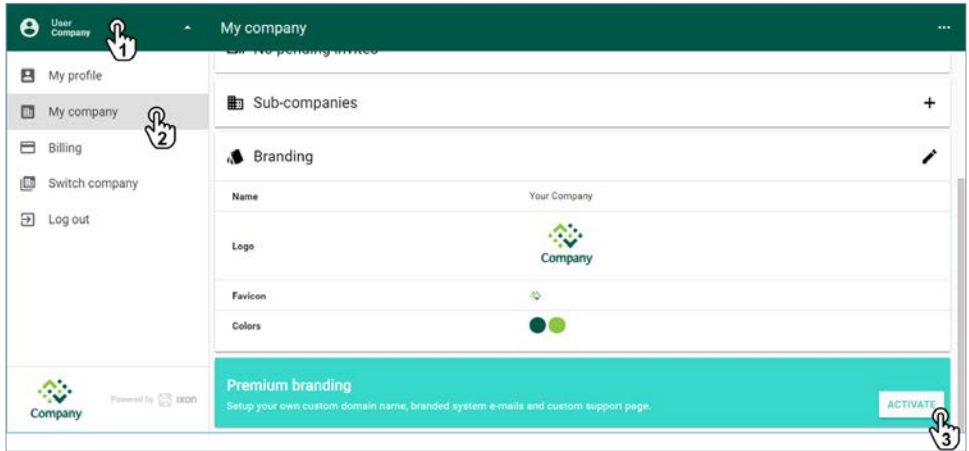


L



### Activation

First, purchase and activate the premium branding feature . Go to the account menu (1), click “My company” (2) and click “Activate” (3) in the “Premium branding” section.

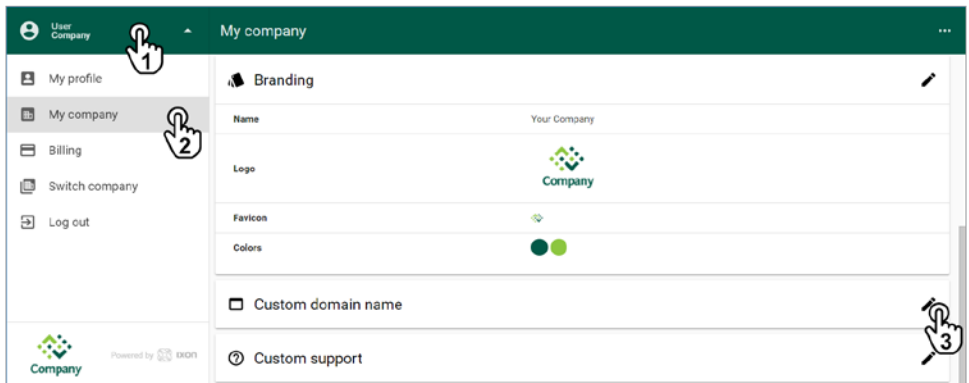


A popup appears with additional information regarding premium branding. Click “Purchase and activate” and then “Confirm” to activate premium branding for your company.

### Custom domain name

After you’ve purchased and activated premium branding, a new section “Custom domain name” will appear. Here you can set your own custom StrideLinx platform URL, or “domain”, for which we’ll automatically generate the necessary SSL certificate.

Go to the account menu (1), click “My company” (2) and click the pencil icon (3) in the “Custom domain name” section.



Enter your desired domain name (1). This needs to be a subdomain (i.e. insight.yourcompany.com, not just yourcompany.com).

You or your hosting provider will have to add a CNAME record to your DNS. Exact details about this record will be provided in the pop-up screen.

Wait 24 hours, then click “Validate” (2) to check if the CNAME record is added properly (3).



**NOTE:** After you enter the CNAME request with your hosting provider it will take some time for the change to propagate through the DNS network. It may take up to 24 hours for the Validate button here to confirm the entry.



**WARNING:** Validation response “Domain has no CNAME specified” means that the CNAME record has not yet been created. Check the CNAME record for typing errors or contact your hosting provider.

Click “Confirm” (4) to finish the setup.

Custom domain name

Company

Domain name \*  
insight.yourcompany.com  
The custom domain name you want to use for your company

**Setting up a CNAME**

Before you can continue, you must set up a CNAME record for the domain entered above. You or your hosting provider can set up a CNAME record to our webserver using the following information.

Type	Host	Answer	TTL
CNAME	insight.yourcompany.com	am01.cdn.trox.net	300

**Validate CNAME**

Come back to this dialog after you add the CNAME record to your DNS. Use the Validate button and our system will automatically validate your domain's DNS settings. If the DNS record is added successfully, complete this step by pressing the Confirm button.

Note that after you enter the CNAME request with your hosting provider it will take some time for the change to propagate through the DNS network. It may take up to 24 hours for the Validate button here to confirm the entry.

VALIDATE

For a secure HTTPS connection, we will automatically generate an SSL certificate using Let's Encrypt. We reserve the right to switch to another certificate authority in the future.

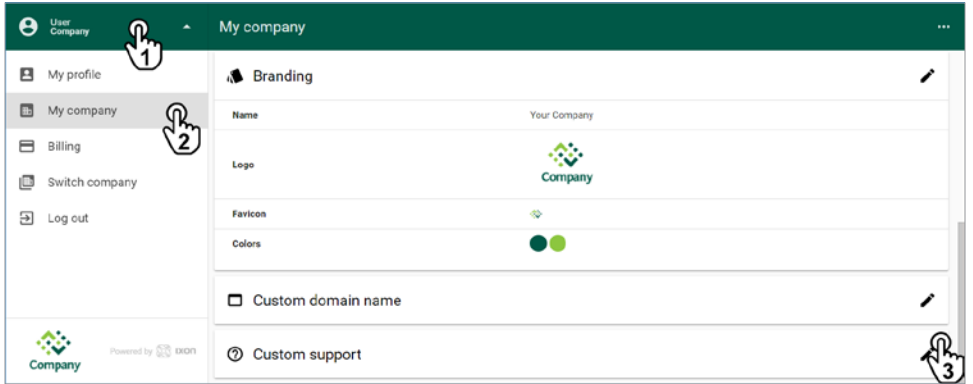
Domain is correctly CNAME'd to am01.cdn.trox.net.

CANCEL CONFIRM

### Custom contact details

The support page, accessible via “Support” from the main menu, displays StrideLinx’s contact information by default. After you’ve purchased and activated premium branding, you can set your own contact or support information, making it easier for your customers to contact you.

Go to the account menu (1), click “My company” (2) and click the pencil icon (3) in the “Custom support” section.



You can add as many links as you prefer. You can edit the icon, link text, link subtext, and URL.

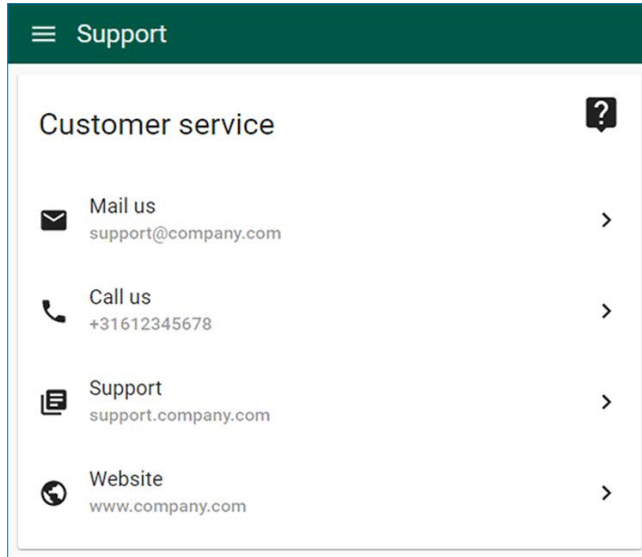


**NOTE:** Telephone numbers should be prefaced with “tel:”, e-mails with “mailto:”, and webpages with “http://”, “https://”, or “//” to resolve http/https automatically.



Click “Confirm” to save your changes.

You can view your custom contact information by clicking “Support” in the main menu.





# TERMS OF USE

---

## In this Appendix...

IXON B.V. Terms of Use .....	M-3
Annex I .....	M-11

This manual covers the StrideLinx platform available from 2017 through 2021.

For details covering the StrideLinx Cloud 2.0 platform available after April 2021, please [click here](#) to link to that manual.

The StrideLinx Cloud 2.0 manual includes details describing the [Activation Code](#) model of Data Logging, Cloud Notify and other add-on features.

For information on the migration wizard from the original platform to StrideLinx Cloud 2.0, [click here](#).

**M**

## IXON B.V. Terms of Use

These terms of use regulate the use of the services provided by IXON B.V., a Dutch limited liability company with its principal place of business in Overloon, the Netherlands, and registered with the Dutch Chamber of Commerce under file number 62729918, hereinafter referred to as “IXON”.

IXON engages in and has experience, know-how and expertise in design and development of cloud based virtual private networks (VPN) solutions for industries, including programmable hardware. IXON’s services typically comprise of three main components, specifically: a hardware component, a software component and a cloud based component. IXON’s current services are described in detail on IXON’s website.

### 1. Definitions

1. **User:** the legal entity to which IXON has made available the use of its services or the end user, who has been granted a right of use by the aforementioned legal entity and who uses or wishes to use the Service.
2. **Agreement:** any agreement between IXON and User concerning (the purchase of) a Service.
3. **Service:** service(s) and/or hardware provided by IXON, such as IXplatform, IXrouter, IXclient, IXagent or any related services and the future services that have not been brought into fruition at the inception of These Terms.
4. **These Terms:** this document containing the terms of use.
5. **Website:** The websites of IXON or its reseller, where User is able to make use of the Service (for example: [www.ixon.co](http://www.ixon.co) and/or any subdomains and extensions).
6. **Personal Data:** any information relating to an identified or identifiable natural person, as stated in the Dutch Personal Data Protection Act.

2. Applicability and order of precedence
  1. These Terms shall be considered accepted by User either by signing These Terms as part of a separate Agreement, accepting an offer to which These Terms have been attached, by agreeing to These Terms when creating an account for the Service or by making use of the Service.
  2. These Terms, including any other terms and conditions made available on the Website or through other channels, apply to every offer of IXON and to every use made of the Service and form an integral part of every Agreement.
  3. Terms and conditions applied by User that deviate from or that are not included in These Terms are only binding for IXON if and in so far as they have been explicitly accepted in writing by IXON.
3. Service and restrictions
  1. IXON hereby grants User a non-exclusive, non-transferable, limited right to access and use its Service, under the conditions of These Terms and for the duration of the Agreement. Use of the Service is subject to a fair use policy. This fair use policy is available on the Website and can be provided on request.
  2. The use of the Service is at User's own expense and risk. User is responsible for meeting the technical and functional requirements of the Service and using the electronic communication facilities that are necessary to be able to access and use the Service.
  3. Any use of the Service, including the transmission, distribution and making available thereof, and any other (legal) act relating to the Service, by or on behalf of User is for User's own risk and responsibility. IXON is not liable and/or responsible for the use of the Service by User.
  4. User is at all times obliged to ensure that its use of the Service corresponds to These Terms and does not violate applicable law and/or the Agreement or infringe upon third party rights. User shall indemnify and hold IXON and its resellers harmless for any and all damages resulting from not complying with the aforementioned restrictions.



5. Notwithstanding any other provisions of These Terms, and any of the User's legal obligations, the use of the Service may not, at IXON's sole discretion:
    1. include software such as viruses or trojans that can damage or erase, make unavailable or make inaccessible any computers or data of IXON, (other) Users or third parties;
    2. bypass technical security measures of the computer systems of IXON, (other) Users or third parties;
    3. involve unreasonable or disproportionate use of the infrastructure of IXON's or third parties' computer systems (the Website contains more information about specific bandwidth usage and increased bandwidth subscriptions);
  6. In addition to the restrictions stated in the previous paragraph, the User is not allowed to make any other changes to the Service or to remove, alter or destroy any form of copyright notice, proprietary markings, trademarks or confidential legends placed upon or contained within the Service.
  7. Furthermore, the User will not translate, disassemble, reverse engineer, decompile or otherwise attempt to reconstruct or discover any source code or underlying ideas or algorithms of, or embodied in, the Service. Excluded from the restrictions in this article are the rights that are explicitly granted to the User by IXON or applicable law.
4. Installation and configuration
    1. Any Service is installed and configured by the User. Any installation and use of the Service is contingent upon the User (at its own costs and effort) providing or having the necessary requirements for use of the Service, such as: (i) adequate internet access, (ii) a personal computer, (iii) adequate user rights on its personal computer, (iv) sufficient knowledge of its own industrial equipment.
  5. User data (privacy and Personal Data)
    1. If the User processes Personal Data using the Service, the User will be subject to the applicable privacy and data protection legislation, such

as the General Data Protection Regulation. In respect thereof, the User guarantees that it will only process Personal Data in a manner that is fully compliant with applicable law.

2. The User, upon using the Service, agrees to the data processing agreement as specified in Annex I of these Terms.
3. The User indemnifies IXON and its resellers against claims of third parties whose Personal Data is processed by the User in any way that does not correspond with applicable law.
4. IXON will use its best efforts to provide an appropriate level of security concerning the risks involved in the usage of the Service in processing Personal Data and the nature thereof.

## 6. Payment

1. Any prices communicated by IXON are exclusive of turnover tax (VAT) and other levies imposed by the government. User must make all payments in the currency stated by IXON or its resellers.
2. IXON may require immediate payment via credit card or bank transfer. IXON may send any invoices electronically, including through email.
3. If User doesn't pay an invoice within the stated or agreed upon payment term then IXON is entitled to limit or block access to the Service until all outstanding invoices (including interest etc.) have been paid in full. IXON is not liable for any damage resulting from such limitation or blocking of access.
4. If User fails to pay the amount due after a demand for payment or a notice of default has been issued, IXON shall be entitled to refer the debt for collection, in which case User must pay all judicial and extrajudicial costs, including all costs charged by external experts. The foregoing shall be without prejudice to the other legal and contractual rights of IXON.
5. IXON is entitled to suspend its obligations in part if invoices are not paid within the agreed upon period or period that is stated on an invoice. If User doesn't fully pay the amounts owed within a reasonable time after IXON has suspended its obligations in part, then IXON is entitled to fully suspend all its obligations.

## 7. Availability, maintenance and support

1. IXON will use its best efforts to provide User with a reasonable level of support. If User purchases Services to be used by its employees or certain end users, then User will provide these employees or end users with primary support. In such case IXON will use its best efforts to provide a reasonable level of secondary support.
2. IXON will use its best efforts to realize uninterrupted availability of the Service and its servers, but offers no guarantees in this respect unless explicitly agreed upon, for example: in a service level agreement.
3. IXON may choose to change its hosting providers in order to optimize the balance between cost and quality. IXON will use its best efforts to make such changes without requiring the User to perform any reconfiguration of equipment.
4. IXON is entitled to stop its Service temporarily for maintenance, modification or improvement of the Service. IXON will use its best efforts to manage this period of inactivity in a manner which will result in the least possible inconvenience to its clients (according to IXON's statistics). IXON will use its best efforts to notify User of any unavailability of the Service in advance.

## 8. Employees and end users

1. If User purchases Services to be used by its employees or certain end users, the User will make sure that such employees or end user will accept These Terms and comply with These Terms fully.
2. Aforementioned User will be fully liable towards IXON for any acts or omissions of such employees or end users.

## 9. Intellectual property

1. Nothing in These Terms shall be interpreted or construed so as to transfer any right, title, or interest in any intellectual property of IXON to User.
2. IXON or its licensors retain all rights, titles and interests to the intellectual property developed by IXON, including: copyrights, patents, know-how, trade secrets and other information or proprietary rights

3. All rights pertaining to the data that User processes through the Service, remain vested in User.

## 10. Liability

1. Unless explicitly agreed upon otherwise in writing by IXON, the liability of IXON for direct damages sustained by User on any ground whatsoever will not exceed the purchase price that the User paid to IXON or its resellers.
2. Direct damages only include:
  1. reasonable costs for determining the cause and extent of the damages;
  2. reasonable costs to repair any shortcomings in the Service;
  3. reasonable costs for the prevention or restriction of damages.
3. Liability on the part of IXON and its resellers for any other damages is explicitly excluded.
4. Any limitations of liability will not be applicable:
  1. in the event that the damages are a result of deliberate recklessness or fraud on the side of IXON;
  2. insofar the liability cannot be limited or excluded by applicable law.
5. IXON shall only be liable due to an attributable failure in the performance of an Agreement if User declares IXON to be in default in writing without delay and grants IXON a reasonable term to remedy the failure, and IXON culpably fails to remedy the failure within the reasonable term. The notice of default must describe the breach as comprehensively and in as much detail as possible in order to give IXON the opportunity to respond adequately.
6. For there to be any right to compensation, User must always report the damages to IXON in writing as soon as possible after the loss has occurred. Each claim for compensation from User to IXON shall be barred by the mere expiry of a period of 12 months following the inception of the claim.

## 11. Force majeure

1. IXON shall not be liable whatsoever if IXON is prevented from or delayed in performing its obligations under an Agreement, or from carrying on its business, by acts, events, omissions or accidents beyond its reasonable control, i.e. by force majeure. On the part of IXON, this can include, among other things: (i) force majeure on the part of suppliers of IXON, (ii) the failure to properly fulfill obligations on the part of suppliers that were prescribed to IXON by User, (iii) defects in items, equipment, software or materials of third parties, (iv) government measures, (v) power failures, (vi) internet, data network or telecommunication facilities failures, (vii) network attacks, and (viii) war.

## 12. Term and amendments

1. These Terms will remain in force for as long as User uses a Service.
2. IXON reserves the right to amend or supplement These Terms.
3. Amendments will also apply to Agreements concluded prior to the amendment. An amendment will not take effect until 30 days after IXON has informed User about the amendment. Among other ways, IXON may inform User about the amendment: through email (newsletter), by traditional mail or by disclosing the amendment on its Website.
4. If User refuses to accept an amendment to These Terms, it may terminate the Agreement and stop using the Service by the date on which the amendment would take effect. Use of the Service after the date of effect, shall constitute acceptance of the amendments to These Terms.

## 13. Miscellaneous

1. These Terms and Agreements with IXON are governed by Dutch law.
2. Insofar as the rules of mandatory law do not prescribe otherwise, any disagreements between the parties concerning the fulfilment, the interpretation or the judicial implication of an Agreement will be submitted to the competent Dutch court for the district where IXON has its registered office.

3. If any provision in These Terms is null and void or is declared void, the remainder of These Terms will remain in full effect. This does not absolve the User from abiding by These Terms. IXON and User shall in this case consult each other for the purpose of agreeing to new provisions to replace the null and void or voided provisions. These provisions shall be as similar to the null and void or voided provisions as is legally possible.
4. Information from IXON's records shall count as conclusive evidence with respect to the performance delivered by IXON and the amounts owed by User for delivery of this performance, without prejudice to the Users right to produce evidence to the contrary.
5. Changes to management or legal form will not affect an Agreement. IXON may transfer an Agreement or any rights and obligations resulting from an Agreement or These Terms to third parties.

## Annex I

- THE PARTIES
  - IXON B.V., a Dutch company registered with the Dutch Chamber of Commerce under number 17128312, having its registered place of business at Vlieringsbeekseweg 52a, 5825AV in Overloon (The Netherlands), in this matter duly represented by W. Hofmans, hereinafter called: “Processor”;
  - The User of the Service, hereinafter called: the “Controller”

hereinafter collectively referred to as ‘Parties’ and individually as ‘Party’,

### HAVING REGARD TO THE FACT THAT

- Processor provides an industrial ‘Internet of Things’ platform, that enables users (often machine builders) to provide remote services for their industrial machines;
- Controller wishes to use the aforementioned platform and has concluded an agreement with Processor on this date;
- by using the platform, Processor will process certain personal information of Controller, its employees or its customers;
- Parties must comply with the relevant privacy legislation, such as: the Dutch Personal Data Protection Act (Dutch translation: Wet bescherming persoonsgegevens, hereinafter: ‘Wbp’), and from the 25th of May 2018 the General Data Protection Regulation (hereinafter: ‘GDPR’);
- Parties therefore conclude this data processing agreement (hereinafter: ‘Data Processing Agreement’);
- With personal data, data within the meaning of article 1 (a) of the Wbp is being meant;
- Controller is hereby deemed to be the responsible party within the meaning of article 1 (d) of the Wbp;
- Processor is hereby deemed to be the Processor within the meaning of article 1 (e) of the Wbp;

**M**

- Parties, having regard also to the provisions of article 14 (5) of the Wbp, wish to lay down their rights and duties in writing in this Data Processing Agreement;
- where, within the meaning of this Data Processing Agreement, the Wbp is referred to, from the 25th of May 2018 onwards, the corresponding provisions of the GDPR are meant.

HAVE AGREED AS FOLLOWS,

1. Processing objectives

1. Processor undertakes to process personal data on behalf of Controller in accordance with the conditions laid down in this Data Processing Agreement. The processing will be executed within the framework of the Agreement, and for all such purposes related thereto and as may be agreed to subsequently.
2. The personal data processed by Processor, and the categories of data subjects to whom the personal data relates, are specified in Annex 1. Processor shall refrain from making use of the personal data for any other purpose than as specified by Controller. Controller will inform Processor of any such purposes which are not contemplated in this Data Processing Agreement.
3. Processor will not take any independent decisions about the processing of personal data for other purposes, including but not limited to the provision of personal data to third parties and the retention periods of the data. The control over the personal data processed under this Data Processing Agreement and/or other agreements between the Parties rests with Controller.
4. All personal data processed on behalf of Controller shall remain the property of Controller and/or the relevant data subjects.

2. Processor's obligations

1. With regard to the processing mentioned in the previous article, Processor shall use its best efforts to ensure compliance with applicable laws and



- regulations governing the protection of personal data, under which the Wbp and the GDPR.
2. Processor shall inform Controller, at its request, about the measures Processor has taken in relation to its obligations under the Data Processing Agreement.
  3. The obligations of Processor arising from the Data Processing Agreement also apply to those processing personal data under the authority of Processor, including but not limited to employees.
3. Transfer of personal data
1. Processor may process the relevant personal data in countries within the European Union. Transfer of personal data to countries outside the European Union is only allowed in accordance with applicable laws.
  2. On request, Processor will inform Controller about the countries in which the relevant personal data is processed.
4. Allocation of responsibility
1. The authorized processing shall be carried out within a(semi-)automated environment under control of Processor. Processor is only responsible for the processing of personal data under the Data Processing Agreement, with due consideration of the instructions provided by Controller and carried out under the responsibility of Controller.
  2. For any other processing of personal data, which does not fall within the scope of this Data Processing Agreement, including but not limited to the collecting of personal data by Controller, processing for purposes that have not been disclosed by Controller, Processor cannot be held responsible. The responsibility of these types of processing lies with Controller.
5. Engaging of third parties or subcontractors
1. Controller hereby permits Processor to engage third parties in the processing of personal data under the Agreement. On request, Processor

will inform Controller of any third parties it engages in the performance of the Data Processing Agreement.

2. Data Processor will use its best efforts to make sure that any such third party is bound by similar obligations as agreed upon between Controller and Processor.

## 6. Security

1. Processor will use its best efforts to take appropriate technical and organizational measures with respect to the processing of the personal data against loss or against any form of unlawful processing (such as unauthorized disclosure, damage, alteration or transfer of personal data). These measures should, taking into account the state of technology and the costs of implementation, provide a suitable protection level, taking into account the risks associated with the processing and the nature of the information to be protected.
2. Controller will only make personal data available to the Processor for processing if it is assured that the necessary security measures have been taken.

## 7. Data breaches

1. For the purpose of this Data Processing Agreement, a “Data Breach” shall mean: a security incident that leads to a considerable likelihood of serious adverse effects or that has serious adverse effects on the protection of personal data as meant in article 34a of the Wbp.
2. In the event of a Data Breach, Processor shall, to the best of its ability, notify Controller thereof without undue delay, no later than 48 hours after discovery of the Data Breach.
3. In the event of a Data Breach, Controller shall determine whether or not to inform the Autoriteit Persoonsgegevens and/or the data subjects. If there is any (legal) obligation or requirement for the Processor to assist Controller, Processor will assist Controller in informing the Autoriteit Persoonsgegevens and/or the data subjects.

4. The duty of Processor to report a Data Breach includes, in any event, the duty to report the fact that a Data Breach has occurred and the following details (if available):
  - information about the first point of contact regarding the notification;
  - the date at which the Data Breach has occurred (the period in which a Data Breach occurred suffices in case the Processor is unable to determine the exact date at which the breach occurred);
  - the date and time at which the breach has become known by the Processor or by the third party enabled by Processor;
  - the (suspected) cause of the breach;
  - the (currently known and or anticipated) consequences thereof;
  - whether the personal data has been encrypted, hashed or in any manner has been made incomprehensible or inaccessible to unauthorized individuals;
  - the proposed and or taken measures to end the breach and to limit its consequences.

#### 8. Handling requests from data subjects

1. Where a data subject submits a request to Processor to exercise one of its legal (privacy) rights, Processor will forward this request to Controller. Controller will then deal with this request. Processor may notify the data subject hereof.

#### 9. Non-disclosure and confidentiality

1. All personal data from Controller processed by Processor within the framework of this Data Processing Agreement is subject to a duty of confidentiality vis-à-vis third parties.
2. This duty of confidentiality will not apply in the event that Controller
  - has expressly authorized the furnishing of such information to third parties,

- where the furnishing of the information to third parties is reasonably necessary with a view on the nature of the instructions and the implementation of this Data Processing Agreement, or
- if there is a legal obligation to make the information available to a third party.

## 10. Audit

1. Controller has the right to perform an audit in order to determine to what extent Processor complies with the provisions of the Data Processing Agreement. This audit will be performed by an independent, professional third party, who will be bound by an obligation of confidentiality.
2. The audit may take place once per year and/or in the event Controller has legitimate reasons to doubt Processors compliance with the Data Processing Agreement. Controller provides Processor with at least two-weeks' notice before such audit may take place.
3. The results of the performed audit will be jointly evaluated by the Parties. If necessary, the Parties will implement measures to comply with the Data Processing Agreement.
4. In case Controller initiates a Privacy Impact Assessment (hereinafter: 'PIA'), Processor shall assist Controller where possible in fulfilling this PIA, by inter alia providing the required information to Controller that is available for Processor.
5. The costs of the audit and/or PIA, including the costs that Processor has to make to cooperate with the audit and/or PIA, shall be borne by Controller.

## 11. Liability

1. The Data Processing Agreement forms an integral part of the Agreement, including the general terms and conditions of IXON, which contain a liability regime. This liability regime is also applicable to this Data Processing Agreement.

## 12. Duration and termination

1. This Data Processing Agreement enters into force on the date of accepting these Terms.
2. This Data Processing Agreement is entered for the duration of use of the Service, and may not be terminated in the interim.
3. Upon termination of the Data Processing Agreement Processor shall end the processing of the personal data by deleting the data of Controller on its systems. If Controller wishes that its personal data is returned to Controller, then Controller must request this before the end of the Data Processing Agreement. Parties will then discuss if Processor can reasonably comply with the request of Controller.
4. Both Parties shall provide their full cooperation in amending and adjusting this Data Processing Agreement in the event of any new (privacy)legislation.

## 13. Miscellaneous

1. The Data Processing Agreement forms an integral part of the Agreement, including the general terms and conditions of IXON, which (amongst others) contain a liability regime and a provision with regards to jurisdiction.
2. Logs and measurements taken by Processor count as compelling proof, except where Controller is able to provide counterevidence.
3. If and to the extent that one or more of the provisions of this Data Processing Agreement are or are to be ineffective, the remaining terms of this Data Processing Agreement remain in full force. In that situation, the Parties shall replace the non-binding provisions with provisions that are binding and as close as possible to the purpose and intention of the non-binding provisions.

