Industrial VPN Router
with
StrideLinx Cloud 2.0
USER MANUAL

Manual Number: SE-SLVPN2-USER-M

⚡ WARNING ⚡

Thank you for purchasing automation equipment from AutomationDirect.com®, 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.

⚡ ADVERTENCIA ⚡

Gracias por comprar equipo de automatización de **AutomationDirect.com**®. 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 varian 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.

⚡ AVERTISSEMENT ⚡

Nous vous remercions d'avoir acheté l'équipement d'automatisation de **AutomationDirect.com®**, 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.

Industrial VPN Routers with StrideLinx Platform 2 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-SLVPN2-USER-M**
Issue:	**1st Edition Rev. E**
Issue Date:	**12/24**

Publication History		
Issue	**Date**	**Description of Changes**
1st Edition	04/21	Original Issue for StrideLinx Cloud 2.0. Based on User Manual SE-SLVPN-USER-M for StrideLinx Cloud 1.0.
1st Edition Rev. A	09/21	Corrected error in video references.
1st Edition Rev. B	02/22	Updated Mobile App Branding Add-on License descriptions.
1st Edition Rev. C	01/23	Corrected monthly data limit to 10GB. Removed Type 1 fonts.
1st Edition Rev. D	12/23	Updated subscription options, SIM Kits, Cloud Reporting features
1st Edition Rev. E	12/24	Added unsecure local browser interface to general specifications

Table of Contents

Chapter 1: Hardware

Chapter 2: StrideLinx Cloud 2.0

Chapter 3: Controller Connection Examples

Chapter 4: Cloud Reporting

Chapter 5: Cloud Notify

Appendix A: Accessories & Add-on Licenses

Appendix B: Troubleshooting

Appendix C: Safety and Security Considerations

Appendix D: Data Logging Address Notation – AutomationDirect Devices

Appendix E: StrideLinx Network Security

Appendix F: Capabilities of Connected AutomationDirect Devices

CHAPTER
1

HARDWARE

In this Chapter...

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

The StrideLinx series of industrial VPN routers is the hardware component for the StrideLinx Cloud. 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 Cloud to send alarms & notifications, log data locally or to the cloud, and brand the StrideLinx Cloud 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. The file is generated from a configuration wizard in the Tools menu of the Fleet Manager app in your StrideLinx Cloud 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[1]	✓		
SE-SL3011			
SE-SL3011-WF	✓	✓	
SE-SL3011-4GG (global)[2,3,4,5]	✓		✓

1. ***SE-SL3001 does not support data logging or notifications.***
2. ***Certified for AT&T and Verizon; compatible with T-Mobile and other carriers using the same cellular bands.***
3. ***Verizon support requires router firmware version 3.20 or later.***
4. ***AT&T support requires router firmware version 3.23.1 or later.***
5. ***Refer to specifications tables for supported cellular bands.***

What's in the Box?

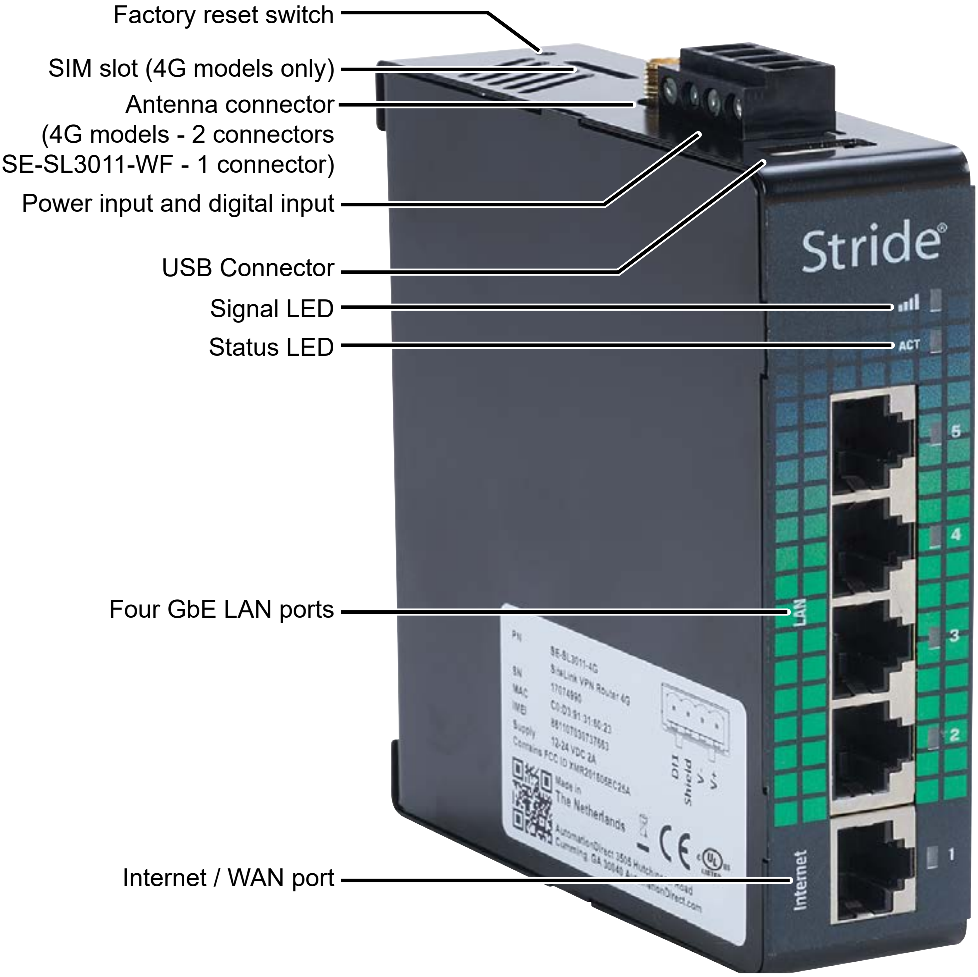
In the package you will find the following contents:

- 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
- 4G cellular routers include a SIM kit from Enabling Elements, Inc.

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

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

General Specifications	
USB	USB 2.0
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, FCC
Interface	Browser (Unsecure)
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

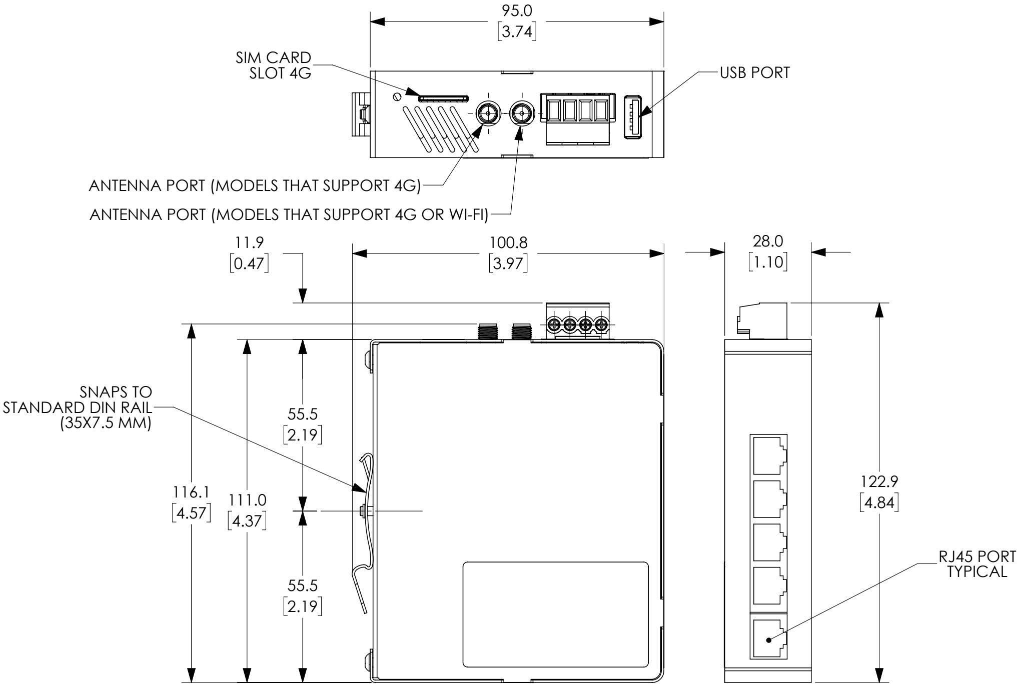
4G LTE Specifications for SE-SL3011-4G Only	
Cellular Bands (AT&T)	LTE-FDD: B2, B4, B12 WCDMA: B2, B4, B5
Speed	LTE-FDD: Max. 150 Mbps (DL)/Max. 50 Mbps (UL) WCDMA: Max. 384 kbps (DL)/Max. 384 kbps (UL)
Antenna Connection	Two (2) SMA plugs (male)
Antenna Connector Torque	3–5 lb·in [0.3–0.6 N·m]
SIM size	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-SL3011-4GG 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.

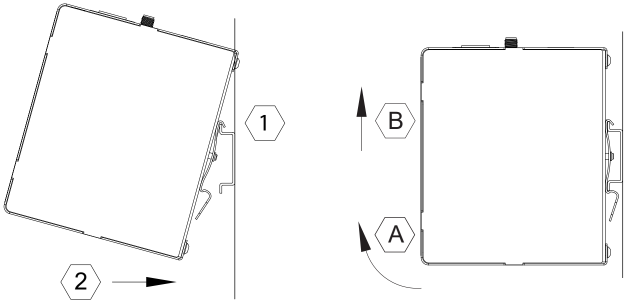
Installation

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-SL3011-4GG)

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.

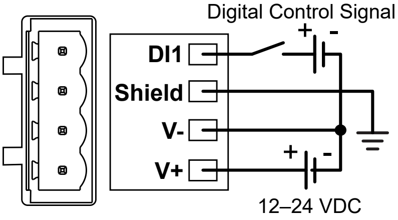
If you have any questions concerning the installation or operation of this equipment, or if you need additional information, please call technical support at 1-800-633-0405 or 770-844-4200.

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. The input uses the V- connection from the power supply as common ground, as shown in the wiring diagram above. Specifications for the input signal are given in the table below.

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)

Local control of remote access via the digital input must be configured using a configuration file. The settings cannot be remotely changed through the StrideLinx Cloud. For instructions on configuring the input, see the support article at https://support.stridelinx.com/hc/en-us/articles/360019029717-Switch-VPN-on-off#h_51214682651525330522824.

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.

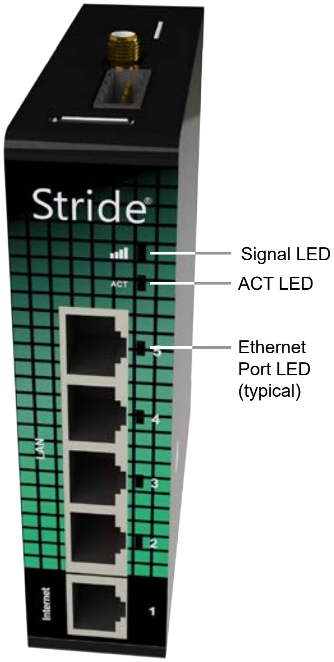
Shield

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

Operation

LED Status Indicators

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



Signal LED (SE-SL3011-4GG & -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 [1]
Red	Blinking 4 pulses	The router was removed from the StrideLinx Cloud [2]
Red	Blinking 5 pulses	The router was already registered to the StrideLinx Cloud [3]
Blue	Blinking 1 pulse	Connecting to StrideLinx Cloud
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

Online Help

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

Factory resetting a router will return all settings on the device to their factory default value. You cannot undo a factory reset! After doing a factory reset you'll have to register the device again.

NOTE: Remove USB and use stable power
Make sure the power supply is stable, as losing power during a factory reset will result in a defective unit. Also make sure to remove the USB flash drive from the device, if one is present.

Carefully follow the steps below to factory reset your device.

1. If you want to preserve the access related to an activation code applied to the router, deactivate that code before resetting the router, then re-activate it after the router is back online.
2. On top of the device, near the back, you'll see a small round opening. Using a paperclip or other small object, **gently press and hold** the factory reset button inside the opening.
3. After a few seconds, the LEDs on the device should start flashing, indicating that it is busy performing the factory reset.
4. **Keep holding the button** until the LEDs stop flashing and then **let go**.
5. The ACT LED should now be constant red.
6. **Wait** 2 minutes.

The device will now boot up. If after 2 minutes the ACT LED is still constant red, that means the factory reset was executed correctly. If it is not constant red, that means you likely let go of the factory reset button too early and you'll need to repeat the steps above.

NOTE: After a factory reset
If the device is still listed in StrideLinx Cloud 2.0 and you want to re-use those settings, make sure to turn on "Recover upon next registration" before registering again. If you want to start from scratch, make sure to remove the device from StrideLinx Cloud 2.0 before registering again.

Cellular Data Service and 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 offer technical support for AT&T or Verizon connections activated through Enabling Elements, Inc., as described in the following sections.

AT&T Cellular Data Service and SIM Card Registration

AutomationDirect has partnered with Enabling Elements, Inc., to assist customers with setting up AT&T M2M cellular service for StrideLinx 4G routers.

An AT&T SIM card is packaged with each new AT&T-compatible StrideLinx 4G router. To get started, email Enabling Elements at stridelinx@enablingelements.com or visit their website at https://enablingelements.com/stridelinx/ to sign up online. Pricing and terms are available on their website.

After you contact Enabling Elements, they will set up your AT&T service and provide you with the configuration information you will need to finish setting up the cellular data connection on your StrideLinx router.

Configuration of the 4G router to use the AT&T APN and provided SIM card is covered in the "Getting Started" section of Chapter 2.

***NOTE:** AutomationDirect recommends that users set up AT&T M2M cellular service through Enabling Elements. If you choose to set up the service on your own, we recommend an AT&T M2M SIM card intended for data applications. AutomationDirect can only offer support for AT&T 4G connections using an AT&T M2M SIM card activated through Enabling Elements.*

T-Mobile Cellular Data Service and SIM Card Registration

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,

1. Visit a T-Mobile store and purchase an LTE data plan and SIM card for a hotspot device.
2. Activate the T-Mobile SIM card by calling T-Mobile before use in the StrideLinx 4G router.
3. Power off the StrideLinx 4G router.
4. Insert the SIM card into the router.
5. Attach the primary antenna to the MAIN antenna connector. Optionally attach a secondary antenna to the DIV antenna connector.

Configuration of the 4G router to use the T-Mobile APN is covered in the "Getting Started" section of Chapter 2.

Verizon Cellular Data Service and SIM Card Registration

The global 4G cellular router (SE-SL3011-4GG) is compatible with cellular data service from Verizon Wireless. AutomationDirect has partnered with Enabling Elements, Inc., to assist customers with setting up Verizon cellular service for StrideLinx 4G routers.

To get started, email Enabling Elements at stridelinx@enablingelements.com or visit their website at https://enablingelements.com/stridelinx/ to sign up online. Pricing and terms are available on their website.

After you contact Enabling Elements, they will set up your Verizon service and provide you with the configuration information you will need to finish setting up the cellular data connection on your StrideLinx router.

Configuration of the 4G router to use the Verizon APN is covered in the "Getting Started" section of Chapter 2.

***NOTE:** Connection on Verizon network requires router firmware version 3.20 or later.*

***NOTE:** AutomationDirect recommends that users set up Verizon cellular service through Enabling Elements. If you choose to set up the service on your own, we recommend a Verizon M2M SIM card intended for data applications. AutomationDirect can only offer support for Verizon 4G connections using a SIM card activated through Enabling Elements.*

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 Cloud. 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[1]
Outbound	8443[2]	TCP	HTTPS
Outbound	53[3]	TCP & UDP	DNS[1]

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	
Directive	***Description***
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	
Standards	***Description***
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
- **Verizon** certification

c UL us
LISTED
ITE
E495151

CE

FC

AT&T Network
Ready Device

verizon

CHAPTER

2

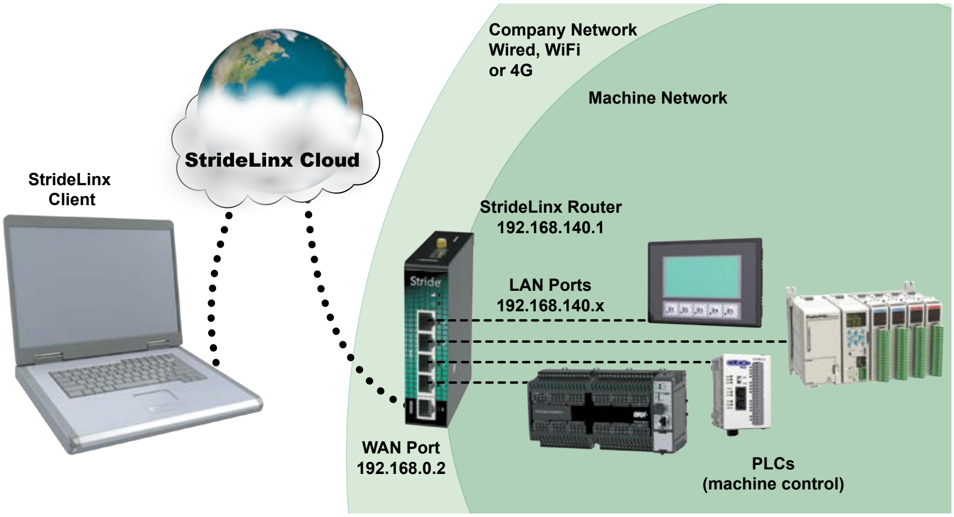
STRIDELINX CLOUD 2.0

In this Chapter...

What is Stridelinx Cloud 2.0?

StrideLinx Cloud 2.0 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.

StrideLinx Cloud 2.0 is divided into four apps on the web site, as outlined below. Each app has a support page linked to the Online Help button and an overview video in the table. In this manual, we've organized by task, and will guide you to the appropriate app as needed.

	Portal	**Use your device's services and invite users:** This is where you'll normally interact with StrideLinx, including monitoring and connecting to your remote equipment. Video Overview: https://www.automationdirect.com/VID-CM-0054	Online Help
	Admin	**Manage your company:** Configure your companies, users, and roles. Manage access and audit changes. Video Overview: https://www.automationdirect.com/VID-CM-0052	Online Help
	Fleet Manager	**Manage your devices:** Add/remove devices, set up devices and services, manage licenses, download VPN client software. Video Overview: https://www.automationdirect.com/VID-CM-0053	Online Help
	Studio	**Create custom pages:** Design the pages you see when using the Portal app. Create one or more views to show you what you need when you need it. Video Overview: https://www.automationdirect.com/VID-CM-0055	Online Help

The Legalese

Terms of Use

The StrideLinx Cloud is powered by IXON, B.V., and use of the service requires acceptance of IXON's Terms of Use. The most recent version of the Terms of Use is always available by clicking your user avatar in the upper right corner of the StrideLinx Cloud 2.0 site.

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 Cloud is secure remote access to industrial control equipment for remote service. A monthly allowance of 10GB data traffic per company account is included, and is sufficient in most cases to accomplish remote service.

When the StrideLinx Cloud is used for other purposes, the data traffic may exceed the 10GB allowance. For unlimited data, the annual professional license can be purchased as an option. See "Add-on Licenses" in Appendix A for more details.

If the data traffic for a company reaches the monthly limit, further data traffic may 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 StrideLinx Cloud, we expect the most significant data usage to be from an IP camera connected on the service.

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

Getting Started With StrideLinx Cloud 2.0

We'll assume you have purchased a StrideLinx VPN Router, and have wired it up using the instructions in Chapter 1. Now you're ready to get started using the StrideLinx Cloud at https://www.StrideLinx.com.

We'll walk you through the basics here. At the end of this section, you should have simple and secure remote access to your equipment through the StrideLinx Cloud. We'll cover more advanced settings later in the chapter.

If you are new to the StrideLinx site, a "Getting Started" button will appear in the lower left corner of the screen, and will guide you through a tour of the site features and some common tasks. The button will go away when all its activities have been completed, or you can dismiss it at any time.

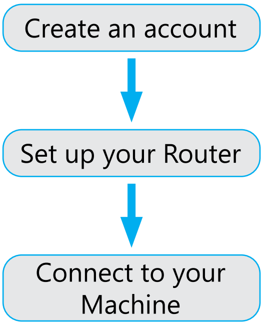
If you need help with any steps along the way, the StrideLinx Cloud 2.0 Support Portal is available at support.stridelinx.com. Click on the "Online Help" link to the right of some of the steps for direct access to that topic in the support portal.

Online Help

Additional help resources are available in the Resource Center, which is accessible by users with admin rights, as discussed further on page 2-47 of this chapter.

Overview of the Steps

To get started we need to go through the following steps:



Create an account

Set up your Router

Connect to your Machine

Create an Account

Each user on the StrideLinx Cloud must have a unique **User Account**, which can be connected to one or more **Companies**. Each StrideLinx VPN Router is a part of one **Company**. You can join the StrideLinx Cloud by joining an existing company or creating a new company.

Online Help

Join an existing company

An existing user can invite you to join a company, if they have permission to manage users.

Invite a user to an existing company

1. Open the Portal app on StrideLinx Cloud 2.0, which is accessible via the Apps menu in the top right corner if you are currently in a different StrideLinx Cloud 2.0 app.
2. Open the **main menu** ☰, go to **Users** 👥 in the left menu and click on **Invite users** +.
3. Enter the **email addresses** of the users to invite (separated by a comma or enter) and select their **roles** (more info at "Access and Permissions Management"). Add an **invitation message** and click **[Invite]** to send the invitation(s). An email will be sent to all recipients.

Accept an Invite to an existing company

- If you receive an Invite and don't yet have a personal StrideLinx account, you will be prompted to create one before you can accept the invitation. If you already have a personal account, you can immediately accept your invitation.

Create a new company

If you have no company account yet on the StrideLinx Cloud, you can easily register one.

- If you don't have a personal user account:
  1. Go to https://www.stridelinx.com and click **[Register]** to create both a user account and a company.
  2. Enter your user and company information, accept the terms of use, and click **[Register]**.
  3. You will receive a confirmation email. Open it and click on **[Complete registration]**.
- If you have a user account, you can add a new company from www.stridelinx.com.
  1. Open your account menu in the top right corner and click **[Switch Company]**.
  2. Click **Add company** +.
  3. Enter your **company name** and **[Register]** your company.

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

Set Up your StrideLinx VPN Router

Online Help

Now that you have your personal user account and it is associated with a company, you are ready to get your StrideLinx router connected.

To set up the StrideLinx VPN Router, we'll create a configuration file, then transfer it to the router using the USB flash drive.

***NOTE:** The router will be registered to the company you are logged into when creating the configuration file.*

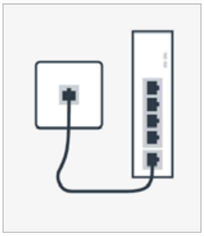
Before you Begin:

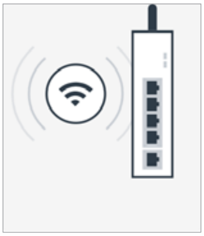
Here's what you'll need to get your StrideLinx VPN Router set up:

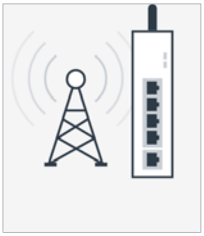
- a StrideLinx user account, set up in the previous step
- a StrideLinx VPN Router, with power
- a means to connect the router to the internet (wired, Wi-Fi, or cellular)
- physical access to the StrideLinx VPN Router for its initial setup
- a USB flash drive, formatted as FAT/FAT32
- a PC with internet access and a USB port

Choose a connection type

There are three possible ways to connect the router to StrideLinx Cloud 2.0, depending on which StrideLinx VPN router model you have: a **wired**, **wireless** or **cellular** connection. Choose one of the methods for now, but note that you can change the connection method later, and even add backup connections to use in case the primary method fails.

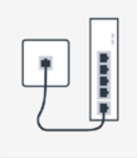

Wired


Wireless


Cellular

***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 Cloud 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.*

Using a wired connection (any model StrideLinx router)



The StrideLinx VPN Router will be connected to Stridelinx Cloud 2.0 using an Ethernet cable connected to a port on your company network.

Online Help

Create a configuration file

A configuration file wizard in StrideLinx Fleet Manager will guide you through creating the configuration file. The wizard is pre-populated with commonly used settings to simplify the process.

1. Go to the **Fleet Manager**, which is accessible via the **Apps menu** ⠿ in the top right corner when logged into your StrideLinx account.
2. Open the **main menu** ☰ , select **Tools** ⚙ in the left menu, and select **[Start configuration]** on the **Router config file** card.
3. Select the connection type "**Wired network**".
4. Enter the details for how your StrideLinx router will connect to the internet. In most cases, you can **obtain an IP address automatically**, **automatically assign your DNS server via DHCP**, and leave **HTTP Proxy disabled**. If you will be using port forwarding, though, we strongly advise you to configure a static IP address. Configuring a static IP address will also require that you set a custom DNS server. If you are unsure about what to configure or enter, please consult the local IT administrator.

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.

5. **Local control over remote accessibility**, if enabled, will allow you to enable/disable the VPN connection via a wired digital input on the router. Wiring details are in Chapter 1.
6. Enter a **unique IP address** for the LAN side of the router (machine network). Note that this IP address needs to be in the same range as the machine and that its last number needs to be different from the machine to prevent an IP conflict.

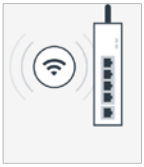
NOTE: *The LAN range (machine network, e.g. 192.168.140.x) needs to differ from the WAN range (company network). More information can be found in the online help.*

Online Help

7. Click **[Download file]** to download the generated file and save it to the root directory of a USB flash drive. Note that the filename on the USB drive must be exactly **router.conf** with no added characters, in case your browser added a suffix when saving the file.

You can now skip ahead to the Register your router step on page 2-12.

Using a wireless connection (Part # SE-SL3011-WF only)



The StrideLinx VPN Router will be connected to Stridelinx Cloud 2.0 using a 2.4 GHz wireless LAN connection to an access point on your company network.

Online Help

Create a configuration file

A configuration file wizard in StrideLinx Fleet Manager will guide you through creating the configuration file. The wizard is pre-populated with commonly used settings to simplify the process.

1. Go to the **Fleet Manager**, which is accessible via the **Apps menu** ⠿ in the top right corner when logged into your StrideLinx account.
2. Open the **main menu** ☰ , select **Tools** ⚙ in the left menu, and select **[Start configuration]** on the **Router config file** card.
3. Select the connection type "**Wireless network**".
4. Enter the **Network name (SSID)** and **Password** for your wireless network.

> ***NOTE:*** *The StrideLinx router can't connect to a Wi-Fi network if the network requires you to log in to a webpage or accept their terms of use first. Please use another Wi-Fi network.*
> *The StrideLinx router can only connect to 2.4GHz networks and only channels 1 - 11.*
> *The Network name (SSID) is case sensitive.*

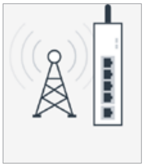
5. When using a wireless connection, the **IP address** and **DNS server** will be automatically assigned via DHCP, and **HTTP Proxy** will be disabled.
6. **Local control over remote accessibility**, if enabled, will allow you to enable/disable the VPN connection via a wired digital input on the router. Wiring details are in Chapter 1.
7. Enter a **unique IP address** for the LAN side of the router (machine network). Note that this IP address needs to be in the same range as the machine and that its last number needs to be different from the machine to prevent an IP conflict.

> ***NOTE:*** *The LAN range (machine network, e.g. 192.168.140.x) needs to differ from the WAN range (company network). More information can be found in the online help.*
>
> Online Help

8. Click **[Download file]** to download the generated file and save it to the root directory of a USB flash drive. Note that the filename on the USB drive must be exactly **router.conf** with no added characters, in case your browser added a suffix when saving the file.

You can now skip ahead to the Register your router step on page 2-12.

Using a cellular connection (Part # SE-SL3011-4GG only)



The StrideLinx VPN Router will be connected to Stridelinx Cloud 2.0 using a 4G LTE cellular connection.

Online Help

Before you begin this step

We recommend setting up your cellular service through Enabling Elements, Inc., using the SIM card included with your router. When you set up service through Enabling Elements, as described in Chapter 1, they will provide you with the settings and instructions to configure the cellular connection. If you choose to set up the cellular service independently, you will need the following:

- Your provider's APN (access point name) and SIM card's PIN code. The APN is established by your service provider.

Standard APNs*:	AT&T: m2m.com.attz	T-Mobile: fast.t-mobile.com	Verizon: vzwinternet

* See Chapter 1 for more information on setting up your SIM card and cellular service.

- An activated SIM card with sufficient internet credit

Create a configuration file

A configuration file wizard in StrideLinx Cloud 2.Fleet Manager will guide you through creating the configuration file. The wizard is pre-populated with commonly used settings to simplify the process.

1. Go to the **Fleet Manager**, which is accessible via the **Apps menu** ⠿ in the top right corner when logged into your StrideLinx account.
2. Open the **main menu** ☰ , select **Tools** ⚙ in the left menu, and select **[Start configuration]** on the **Router config file** card.
3. Select the connection type "**Cellular network**".
4. Enter the provider's **APN** and the SIM card's **PIN code** (if applicable).
5. When using a cellular connection, the **IP address** and **DNS server** will be automatically assigned via DHCP, and **HTTP Proxy** will be disabled.
6. **Local control over remote accessibility**, if enabled, will allow you to enable/disable the VPN connection via a wired digital input on the router. Wiring details are in Chapter 1.
7. Enter a **unique IP address** for the LAN side of the router (machine network). Only the router's IPv4 IP address needs to be entered now. After the router is connected to StrideLinx Cloud 2.0, additional settings can be configured.
8. Click **[Download file]** to download the generated file and save it to the root directory of a USB flash drive. Note that the filename on the USB drive must be exactly **router.conf** with no added characters, in case your browser added a suffix.

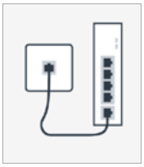
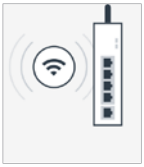
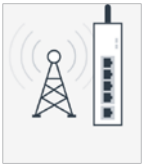
You can now skip ahead to the Register your router step on page 2-12.

Register your router on StrideLinx Cloud 2.0

Online Help

Once the configuration file is placed on a USB flash drive, you can start registering your StrideLinx router.

1. Prepare your network connection base on the selected connection type, as follows:

 Wired	 Wireless	 Cellular
Connect your router's WAN (internet) port to the company network via **Ethernet cable**.	**Connect** the antenna to the router's **Wi-Fi** RP-SMA connector.	**Connect** the antenna to the router's **4G** SMA connector, and **insert** the **SIM card** into the router before applying power.

NOTE: *Cellular antenna connector: The 4G models have 2 SMA connectors for your cellular antenna. The one closest to the power connector is the MAIN and the other connector is the DIV. Always connect an antenna to the MAIN. Connecting a second antenna to the DIV is optional.*

2. **Power on** your StrideLinx router. Please consult the Chapter 1 for details about the recommended power supply and wiring details.
3. **Insert** the **USB flash drive** into the StrideLinx router's USB port.
4. Wait about **2 minutes** for the StrideLinx router to configure and register itself.

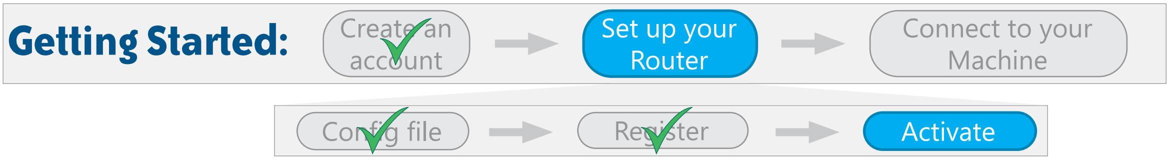
NOTE: ACT LED Status

*The router's ACT LED should **blink blue quickly** shortly after inserting the USB flash drive, indicating that the router is configuring itself.*

*If this hasn't happened after 1 minute, please check that the file is located in the **root directory** of the USB flash drive and that the file name is exactly "**router.conf**". Try a **different USB flash drive** if the problem persists.*

*After roughly 2 minutes, the router's ACT LED should be **solid blue**, indicating that it's registered in StrideLinx Cloud 2.0.*

NOTE: *Remove the USB flash drive after the setup is done. Otherwise, the router would read settings from the USB drive each time it powers up, overwriting any later changes you had made to the settings.*



Getting Started:

Create an account ✓ → Set up your Router → Connect to your Machine

Config file ✓ → Register ✓ → Activate

Activate your StrideLinx router

Online Help

After a successful registration of your router, you can activate your router, making it ready for use.

1. Go to the **Fleet Manager** app, which is accessible from the **Apps menu** ⠿ in the top right corner when logged into your StrideLinx account.
2. Open the **main menu** ☰ , select **Devices** ⎕.
3. You will find a yellow bar at the top of your devices list, saying “New device”. It also mentions your router’s serial number (e.g. 17055202), which you can verify with the serial number on the side of the router. This yellow bar also shows up in the StrideLinx Portal app.
4. Click the yellow bar, name your device as you see fit and select [**Activate**].

Your StrideLinx router is now set up and activated. It should appear in the Devices list, and have a green dot in its Status column. This indicates that it is online. You can now move on to connect to your machine.

Connect to Your Machine

Online Help

You will first establish a VPN connection to your router, and then you can connect to your machine using your development software and any other software you would normally use if you were on-site.

In this Getting Started guide, we'll focus on using StrideLinx with a PC. You can also connect using an Android or iOS mobile device, which is covered later in this chapter.

Before you Begin:

- Make sure your device has a green dot in its Status column of the Devices list. This indicates that the router is online and connected to the StrideLinx cloud.

Install the VPN Client software on your PC

Online Help

The VPN client is a lightweight application that runs in the background on your computer. It creates a virtual Ethernet port on your PC and handles all communication between your PC, StrideLinx Cloud 2.0, and your remote machine.

1. Go to the **Fleet Manager**, which is accessible via the **Apps menu** ⠿ in the top right corner when logged into your StrideLinx account.
2. Open the **main menu** ☰ , select **Tools** ⚙ in the left menu, and select **[Download installer]** on the **VPN Client** card.
3. Select and **download the installer** for your PC. VPN client versions are available for Windows, MacOS, and Linux. The instructions here will focus on the Windows installer.

> ***NOTE:*** *If you are using **Mozilla Firefox**, please close your browser during the installation.*

4. Run the downloaded installer and **follow the steps in the installation wizard**.
5. Once the installation has completed, **refresh the StrideLinx web page**.
6. The VPN client will be launched automatically as a Windows Service. Now that you've installed the VPN client, you are ready to make a VPN connection.

> ***NOTE:*** *If your computer's internet connection uses a **proxy server**, or your country or network **doesn't allow standard VPN connections**, please see the online help article to the right for additional instructions.*

Online Help

Establish a VPN connection

1. Open the StrideLinx **Portal**, which is accessible via the **Apps menu** ⠿ in the top right corner when logged into your StrideLinx account.
2. Open the **main menu** ☰ , select **Devices** ▭ in the left menu, select the router, and press **[Connect]** in the VPN section.
3. The router's status will change from "online" to "connected", and its indicator turns blue.

> ***NOTE: Unable to connect?*** *If you see an error at the bottom of your screen, please refer to Troubleshooting in Appendix B of this manual or the online troubleshooting article at the link to the right.*
>
> Online Help

Success!

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

Here are a few things to keep in mind regarding VPN connections:

- If your software allows you to select a specific network adapter to connect to your machine, you may have to select the **TAP Windows Adapter**.
- Your **PC** can only make **one VPN connection at a time**, but you can connect to all the machines attached to that VPN router.
- Each **user account** can connect **to one router** and **from one PC or mobile device** at a time.
- **Multiple users**, on **different devices**, can connect to the **same VPN router** at once, but your machine or software may restrict connections to a single user.

Where to go from here?

- The rest of this chapter covers managing your devices, companies, users, and access permissions, and remote access to your equipment.
- See Chapter 4 for the optional Cloud Reporting and Data Logging features
- See Chapter 5 for the optional Notification features

Update Router Settings

Most router settings are managed in the **Fleet Manager** app. To open it, log in to StrideLinx and select Fleet Manager from the **Apps menu** ⠿ in the top right corner of the screen.

Throughout this section, we'll assume you already have the Fleet Manager app open. The features in this section are accessed from the Fleet Manager menu on the left side of the screen. If the menu is not visible on your device, open it with the **main menu** ☰ icon.

Router Name, Description, Location and Groups

Online Help

Individual device information can help in providing a clear overview of all your devices. This includes a device name, description, location, and groups. The next steps show you where to change this device information.

1. In the **Fleet Manager** menu, select **Devices** ▭, then click the name of your StrideLinx router.
2. Go to **Info** ⓘ and **[Edit]** what you'd like to change (details below).

Router Info Settings	
Information	**Description**
Name	The name of the device. Usually includes the name of the project or machine for easy identification.
Description	A description of the device. You can include any details that are relevant to the device, project, or machine.
Location	The location of your device is used to determine the nearest VPN server and thus provide the best possible connection. If no location is manually entered, its rough location is automatically determined based on its WAN IP address (GeoIP).
Groups	You can assign a device to one group for every group type that you have created.

Firmware Upgrade/Downgrade

Online Help

Firmware upgrades are needed to **fix bugs**, **improve security**, and **add new features**. You can easily upgrade the router's firmware from your StrideLinx account when the router is online.

⚠ ***CAUTION: We strongly recommend reading the full Online Help article linked above before starting a firmware upgrade. In particular, make sure that:***

- ***There is no USB flash drive in the router.***
- ***You have someone available near the router to reboot it if necessary.***

1. In the **Fleet Manager** menu, select **Devices** ▭, then click the name of your router.
2. Go to **Info** ⓘ and click **[Manage]** next to firmware version.
3. Select a firmware version and click **[Start Upgrade]**.
4. The upgrade will start, and usually takes about 5 minutes.

Update Router Settings (cont'd)

WAN (Internet) Settings, Wired Network

Online Help

The router's WAN configuration determines how the router connects to StrideLinx Cloud 2.0. Depending on your router model, you can configure it to connect via a wired, wireless, or cellular network.

If the router has more than one connection available (e.g., wired and wireless), you can set up multiple connection types for redundancy. To do so, see Fallback WAN Connections (Failover) on page 2-20.

If your router is currently offline

1. Follow the steps on pages 2-8 through 2-12 to create a config file and register your router. These steps will not register your router again, as it is already registered, but this will apply the configuration file settings to the router.
2. In the **Fleet Manager** menu, select **Devices**, then click the name of your router.
3. Click the dropdown arrow beside **[Push config to device]** in the upper right of the screen, and select **[Import config from device]**.

If your router is currently online

1. In the **Fleet Manager** menu, select **Devices**, then click the name of your router.
2. Expand the **Network** options and go to **[WAN]**.
3. Enter the details for how your StrideLinx router will connect to the internet (IPv4 only). In most cases, you can **obtain an IP address automatically**, **automatically assign your DNS server via DHCP**, and leave **HTTP Proxy disabled**. If you will be using port forwarding, though, we strongly advise you to configure a static IP address. Configuring a static IP address will also require that you set a custom DNS server. If you are unsure about what to configure or enter, please consult the local IT administrator.

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.

4. You have now made the changes in StrideLinx Cloud, but these are not yet active in your device. Click **[Push config to device]** in the top right corner for them to take effect.

Update Router Settings (cont'd)

WAN (Internet) Settings, Wireless Network

Online Help

The router's WAN configuration determines how the router connects to StrideLinx Cloud. Depending on your router model, you can configure it to connect via a wired, wireless, or cellular network.

If the router has more than one connection available (e.g., wired and wireless), you can set up multiple connection types for redundancy. To do so, see Fallback WAN Connections (Failover) on page 2-20.

If your router is currently offline

1. Follow the steps on pages 2-8 through 2-12 to create a config file and register your router. These steps will not register your router again, as it is already registered, but this will apply the configuration file settings to the router.
2. In the **Fleet Manager** menu, select **Devices**, then click the name of your router.
3. Click the dropdown arrow beside **[Push config to device]** in the upper right of the screen, and select **[Import config from device]**.

If your router is currently online

1. In the **Fleet Manager** menu, select **Devices**, then click the name of your router.
2. Expand the **Network** options and go to **[WAN]**.
3. Enter the **Network name (SSID)** and **Password** for your wireless network.

NOTE: *The StrideLinx router can't connect to a Wi-Fi network if the network requires you to log in to a webpage or accept their terms of use first. Please use another Wi-Fi network.*
The StrideLinx router can only connect to 2.4GHz networks and only channels 1 - 11.
The Network name (SSID) is case sensitive.

4. When using a wireless connection, the **IP address** and **DNS server** will be automatically assigned via DHCP, and **HTTP Proxy** will be disabled.
5. You have now made the changes in StrideLinx Cloud, but these are not yet active in your device. Click **[Push config to device]** in the top right corner for them to take effect.

Update Router Settings (cont'd)

WAN (Internet) Settings, Cellular Network

Online Help

The router's WAN configuration determines how the router connects to StrideLinx Cloud. Depending on your router model, you can configure it to connect via a wired, wireless, or cellular network.

If the router has more than one connection available (e.g., wired and wireless), you can set up multiple connection types for redundancy. To do so, see Fallback WAN Connections (Failover) on page 2-20.

If your router is currently offline

1. Follow the steps on pages 2-8 through 2-12 to create a config file and register your router. These steps will not register your router again, as it is already registered, but this will apply the configuration file settings to the router.
2. In the **Fleet Manager** menu, select **Devices** ▭▯, then click the name of your router.
3. Click the dropdown arrow beside **[Push config to device]** in the upper right of the screen, and select **[Import config from device]**.

If your router is currently online

1. In the **Fleet Manager** menu, select **Devices** ▭▯, then click the name of your router.
2. Expand the **Network** ⚙ options and go to **[WAN]**.
3. Enter the provider's **APN** and the SIM card's **PIN code** (if applicable). The APN is established by your service provider.
   - If you set up your cellular service through Enabling Elements, Inc., they sent you an email with the necessary settings for your AT&T or Verizon connection. Please contact them at https://enablingelements.com/stridelinx/ if you need the information again.
   - If you set up the service independently, the standard APN settings listed on page 2-11 in the Getting Started section may work. Otherwise, please contact your provider for the settings.
4. You have now made the changes in StrideLinx Cloud, but these are not yet active in your device. Click **[Push config to device]** in the top right corner for them to take effect.

Update Router Settings (cont'd)

Fallback WAN Connections (Failover)

Online Help

If your router model supports different connection types then you can configure multiple connections (max. one of each type) which will then be used as backup connections when the primary connection is unavailable, thus increasing the availability of your machine. The fallback connection must be on a different network than the primary connection.

How does it work?

The router constantly checks each configured connection to determine whether the connection is available or not. This is done by sending a keep alive message to a public IP address every couple of seconds. This keep alive message needs to fail several consecutive times for the connection to be considered unavailable. The same goes for it to be considered available again.

When the preferred connection is unavailable, the router will automatically switch to its fallback connection. When the higher priority connection is back up, the router will automatically switch back to that connection.

To set it up

1. In the **Fleet Manager** menu, select **Devices** ▭, then click the name of your router.
2. Expand the **Network** ⚙ options and go to **[WAN]**.
3. Set up multiple WAN connections, following the steps on pages 2-17 through 2-19.
4. When multiple WAN connection types are configured, the router will automatically use one as the preferred connection and others as fallback connections.
5. To change the priority of the connections, you can **drag and drop** ⠿ the connections to arrange their priority.
6. You can edit each connection's tracking settings ⚙ to change the IP addresses and interval used to check if the connection is available or not. We recommend leaving the default values untouched for the best results. If you do need to change the settings, 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.
7. You have now made the changes in StrideLinx Cloud, but these are not yet active in your device. Click **[Push config to device]** in the top right corner for them to take effect.

Update Router Settings (cont'd)

LAN (Machine Network) Settings

DHCP Server

Online Help

The StrideLinx router has its own DHCP server that automatically assigns an IP address, and other necessary network parameters, to clients connected to the router's LAN ports if they do not have a static IP address configured.

The DHCP server is enabled by default, but can be disabled if necessary. It also automatically changes along with other changes you make. If you change the IP range of the router's LAN IP address, then the IP range of the DHCP server will automatically change as well.

Follow these steps if you want to manually change the DHCP server settings:

1. In the **Fleet Manager** menu, select **Devices** ◫, then click the name of your router.
2. If your machines are all assigned static IP addresses, you can uncheck [**Assign IP addresses automatically**].
3. Otherwise, enter a range of IP addresses to be assigned by the router. The range must be within the local subnet as defined by the router LAN IP and network mask.
4. Click the dropdown arrow beside **[Push config to device]** in the upper right of the screen, and select [**Import config from device**].
5. **Address Reservations**: To reserve specific IP addresses for certain machines, add the **MAC address** and **reserved IP address** for each machine.
6. You have now made the changes in StrideLinx Cloud, but these are not yet active in your device. Click **[Push config to device]** in the top right corner for them to take effect.

Source NAT

Source NAT is the translation of the source IP address of a packet leaving the router. It should generally be left enabled. When disabled, each machine that is connected to the router must have a default gateway set up.

Update Router Settings (cont'd)

Wi-Fi Hotspot

Online Help

The SE-SL3011-WF StrideLinx VPN Router can serve as a **Wi-Fi hotspot** for LAN devices, either with a wired WAN connection or simultaneously with a wireless WAN connection. The Wi-Fi hotspot can be used to:

- Wirelessly access your machine while you are on-site.
- Wirelessly access the internet, if allowed.
- Wirelessly connect machine components.

The Wi-Fi hotspot can be remotely enabled/disabled from your StrideLinx account, as follows.

1. In the **Fleet Manager** menu, select **Devices**, then click the name of your router.
2. Expand the **Network** options and go to **[LAN]**.
3. Check the **[Enable wifi hotspot]** box in the "Wi-Fi hotspot" section.
4. Enter the **Network name (SSID)**, set a **Password** , and select a **channel** for your hotspot.

***NOTE:** The StrideLinx router can only use the 2.4GHz band and only channels 1 - 11. The Network name (SSID) is case sensitive.*

5. You have now made the changes in StrideLinx Cloud, but these are not yet active in your device. Click **[Push config to device]** in the top right corner for them to take effect.

Network Time (NTP) Server

Online Help

The router runs a **Network Time Protocol** (NTP) server, which automatically and periodically syncs its own time with StrideLinx Cloud.

The **Real Time Clock** and NTP server built into the router allows the entire machine line connected to the router to sync their time, preventing time drift. This guarantees identical internal clocks.

***NOTE:** NTP does not acknowledge time zones. Instead, it manages all time information **based on UTC**. To convert UTC to **local time**, you'll need to apply the local time zone in the machine itself.*

To have your machine utilize the router's NTP server, enter the router's **LAN IP address** in the NTP settings of your machine. If possible, apply the **correct time zone** in the machine's time settings.

Update Router Settings (cont'd)

Additional Subnets Behind External Gateway

Online Help

Usually, you can only access one IP range (subnet) remotely, based on the LAN IP and network mask set for your router (e.g., 192.168.140.x).

If you have a device on the LAN (machine side) of your router that has **multiple Ethernet ports** and can serve as a **gateway** between subnets, then you can add those extra subnets to your router to allow remote access to them over StrideLinx Cloud, as follows.

1. In the **Fleet Manager** menu, select **Devices**, then click the name of your router.
2. Expand the **Network** options and go to **[LAN]**.
3. Check the **[Add additional subnet]** in the "Additional subnet" section.
4. Enter the information below and click **[Add]**.

Additional Subnet Settings	
Information	***Description***
Network Address	The additional subnet's IP range with a 0 as final number (e.g. 192.168.200.0)
Network Mask	The additional subnet's network mask (usually 255.255.255.0)
Gateway Address	The machine's IP address, which is functioning as gateway, that's in the same IP range as the router

5. To remove a subnet entry, click the trash can icon to the right of the entry.
6. You have now made the changes in StrideLinx Cloud, but these are not yet active in your device. Click **[Push config to device]** in the top right corner for them to take effect.

Update Router Settings (cont'd)

Router Firewall Settings

Online Help

The StrideLinx router's advanced built-in firewall completely separates its WAN network (company network) from its LAN network (machine network). It blocks all communication except for authorized and encrypted data verified by a valid identity certificate. This means that only authorized users can access the machine network via StrideLinx Cloud. Please see the linked Online Help article for a more detailed explanation of how it works.

To change the firewall permissions, do the following.

1. In the **Fleet Manager** menu, select **Devices**, then click the name of your router.
2. Expand the **Network** options and go to **[Firewall]**.
3. The table below outlines the firewall settings.

Router Firewall Settings	
Setting	***Description***
LAN>WAN Corporate Network	**Allow access to corporate network**: Enable to allow your equipment on the machine side of the StrideLinx router to access devices on the local network outside the router.
LAN>WAN Internet	**Allow access to internet**: Enable to allow your equipment on the machine side of the StrideLinx router to access the internet through the router.
WAN>LAN	Allow devices on your local network to access equipment on the machine side of the router by setting up port forwarding. For each machine to be accessed, you will need to set up the following. External port: All incoming network traffic at this port (at router's WAN address) will be forwarded. Target IP address: The IP address to which the traffic needs to be forwarded. Target port: The port number to which the traffic needs to be forwarded. Often the same as the "External port", unless you are setting up multiple machines with the same type of connection.
VPN>LAN	Traffic coming in via the VPN connection, going to the LAN network of the router, is allowed. Remotely you can access all devices that are connected to the LAN (machine side) network of the router as if you were directly connected to the LAN.

4. You have now made the changes in StrideLinx Cloud, but these are not yet active in your device. Click **[Push config to device]** in the top right corner for them to take effect.

Update Router Settings (cont'd)

Switch VPN Off Remotely to Reduce Data Usage

Online Help

Your device's VPN connection (StrideLinx router to StrideLinx Cloud) is, by default, always enabled. However, you can disable it for moments you don't need it and then enable it again for moments you do need it. This will reduce the monthly bandwidth to about 5MB/mo. In order to access the router (by VPN or through the webserver/VNC server shortcuts), you will have to turn this back on. This is a simple method to minimize data if data consumption is of concern.

To remotely enable or disable the router's VPN connection, do the following:

1. In the **Fleet Manager** menu, select **Devices**, then click the name of your router.
2. Expand the **Network** options and go to **[VPN]**.
3. Toggle **[Use VPN]** in the **VPN access** section
4. This setting is applied immediately, and does not require pushing the configuration change to the router.

Connect via a censored network (stealth mode)

Stealth mode routes the VPN traffic over port 8443, which is normally used for secure websites (HTTPS). This may allow your VPN to function in a country that restricts VPN usage, or when connecting to the internet across a network with restrictive firewall rules.

This may decrease performance, and should only be used when necessary.

The steps below will set up stealth mode for the StrideLinx router's VPN connection. For more information, including steps to enable stealth mode for your PC's VPN connection, please see the Online Help article linked at the right.

To enable stealth mode for your router:

1. In the **Fleet Manager** menu, select **Devices**, then click the name of your router.
2. Expand the **Network** options and go to **[VPN]**.
3. Toggle **[Use stealth mode]** in the **Stealth mode** section
4. This setting is applied the **next time your device connects**, and does not require pushing the configuration change to the router.
5. If the VPN connection is active when changing this setting, then turn the VPN connection **OFF** and back **ON** again as explained at the top of this page to use the new setting.

Local Router Configuration Through LAN Port

All the router network configuration parameters available through Fleet Manager can also be changed locally.

1. In a web browser, navigate to the router's LAN IP address to see the current settings.
2. Select **[Configuration]** and enter the router's password, found on the side of the router, to change any of the network settings.

Device Management

Transfer a Router to Another Company

Online Help

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 you can easily transfer a device from one company (source) to another (destination) in StrideLinx Cloud without the need to remove or re-register the device. The device will then no longer be available in the source company and will become immediately available in the destination company.

To transfer a device, you are going to need the **device ID** and a **device key**.

1. Go to the **Fleet Manager**, which is accessible via the **Apps menu** ⠿ in the top right corner of your StrideLinx account.
2. Open the **main menu** ☰, select **Devices** ◫, then click the name of your router.
3. Go to **More** •••, click on [**→Request device key**], and copy the **device ID** and **device key**.
4. Click [**Done**].

Now that you have obtained the required information, you can easily transfer the device to a different company. Please follow the steps described below to transfer your device.

1. You now have to switch to the destination company. Open the **account menu** in the top right corner and select [**Switch company**], then select the company to which you want to transfer your device.
2. In the **Fleet Manager** menu, select **Tools** ⊘ , and select [**→Transfer device**].
3. Enter the **device ID** and **device key** you obtained earlier and click [**Transfer device**].

The device should now be successfully transferred to the new company.

Device Management (cont'd)

Recover device settings after factory reset (recovery mode)

Online Help

After doing a factory reset, the device may no longer automatically connect to StrideLinx Cloud, as its network has been reset.

If the device is still listed in StrideLinx and you want to re-use those settings, follow the steps below and then register your device again.

1. Go to the **Fleet Manager**, which is accessible via the **Apps menu** ⠿ in the top right corner of the StrideLinx site if you are currently in a different StrideLinx Cloud app.
2. Open the **main menu** ☰, select **Devices** ▭, then click the name of your router.
3. Go to **More** ••• and set **[Recover upon next registration]** to one of the following options:
    - **Restore** - After a factory reset, registering the device again will make it come up as the same device.
    - **Replace** - Replace the router hardware with a new unit. Upon registering a new unit, it will come up as this device. All settings, licenses, and data remain but must be pushed to the new device. You have to enter the **MAC address** of the new device. This can be found on the new router's label.
4. Click **[Confirm changes]**.

You can now register your device again, and it will retain its previous network settings.

NOTE: *Cloud Notify and Cloud Reporting licenses will be restored following a recovery of a router that previously had those licenses.*

Remove a device from your company

Online Help

To clean up your company you may decide to remove a router. After removing a device from your company, it is no longer remotely accessible and you'll need to register the device again in order to use it again.

To remove a device from your company, please follow the steps described below.

1. Go to the **Fleet Manager**, which is accessible via the **Apps menu** ⠿ in the top right corner of your StrideLinx account.
2. Open the **main menu** ☰, select **Devices** ▭, then click the name of your router.
3. Go to **More** ••• and select **[Remove device]**.
4. A confirmation dialog will display the router name and id, and ask you to verify the action.

You can now register the device with another company.

Device Management (cont'd)

Save/Load Router Configuration Templates

Online Help

A device template can help you copy router network settings and efficiently set up multiple routers. The template can include most of the network parameters used to configure a new device. A few settings, such as router hardware info, WAN connection parameters and data details for the devices behind the router, are specific to each router and can't be included in a template.

To create a device template from an existing router

1. Go to the **Fleet Manager**, which is accessible via the **Apps menu** ⠿ in the top right corner of your StrideLinx account.
2. Open the **main menu** ☰, select **Device templates** 🗎, then click **Add template**.
3. **Select the existing router**, give the template a **name**, and click **[Add]**.

To create a device template from scratch

1. Go to the **Fleet Manager**, which is accessible via the **Apps menu** ⠿ in the top right corner of your StrideLinx account.
2. Open the **main menu** ☰, select **Device templates** 🗎, then click **Add template**.
3. Select **Create new**, give the template a **name** and **device type**, and click **[Add]**.
4. Enter the parameters you wish to include in the template. The template can include most of the parameters used to configure a new device. A few settings, such as router hardware info and WAN connection parameters, are specific to each router and can't be included in a template.

To apply a device template to a router

1. The router must be registered to your company and online. First go through the initial setup in the Getting Started section if necessary.
2. Go to the **Fleet Manager**, which is accessible via the **Apps menu** ⠿ in the top right corner of your StrideLinx account.
3. Open the **main menu** ☰, select **Devices** ▭▯, then click the name of your router.
4. Go to **More** ••• and select **[→Load device template]**.
5. Select a template, then select which types of settings you want to apply, and **load settings**.
6. You have now made the changes in StrideLinx Cloud, but these are not yet active in your device. Click **[Push config to device]** in the top right corner for them to take effect.

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 StrideLinx without requiring a VPN connection. In this section, we'll cover how to set up and use the following types of services through your StrideLinx router:

- VPN Service (remote access to your machines as if you are on the same network)
- VNC Service (remote screen sharing)
- HTTP Service (access web pages served from your machine)
- WebSocket Service (connect a WebSocket client on your PC to a WebSocket server on your machine)

Please refer to Chapter 3 to configure the many device options from AutomationDirect.com.

Setting up access to services on your equipment is managed in the **Fleet Manager** app. To open it, log in to your StrideLinx account and select Fleet Manager from the **Apps menu** ⠿ in the top right corner of the screen.

Using these services is managed in the **Portal** app. To open it, log in to your StrideLinx account and select Portal from the **Apps menu** ⠿ in the top right corner of the screen.

The features in this section are accessed from the menu on the left side of each app. If the menu is not visible on your device, open it with the **main menu** ☰ icon.

Device Status

The current status of a device is indicated by the status icon in the **Fleet Manager** and **Portal** apps.

Device Status		
Icon	***Label***	***Description***
⚪	Offline	The router is offline. You can't set up any kind of connection to the router.
🟢	Online	The router is online. You can now set up a connection to the router.
🔵	Connected	The router is connected through the VPN. Your PC now has access to the router's machine network.

Connect to Devices Behind the StrideLinx Router (cont'd)

VPN Service

Online Help

The VPN service, which enables you to establish a VPN connection to your device, is added to each router by default and cannot be removed. You can, however, configure who may use this VPN service by assigning an **access category**, as explained below, or you can disable the VPN service entirely by switching off the device's VPN connection.

Set an access category

The access category determines who can use this VPN service. More information about access categories and how you can create one can be found in this online help article, or in the "Access and Permissions Management" section of this chapter.

1. In the **Fleet Manager** menu, select **Devices**, then click the name of your router.
2. Open the **VPN connect** service in the Services section.
3. Select the appropriate **access category** and press **[Confirm changes]**.

Connect to your machine over VPN

Steps to connect your PC to the VPN and access your machine through it are explained in "Connect to Your Machine" on page 2-14.

NOTE: *Can't click the connect button? Refer to Troubleshooting in Appendix B of the manual.*

NOTE: *Configuring the other service types (VNC, HTTP, WebSocket) allow access to the respective service through a web browser without a VPN connection. You can also access any of these services on your machines directly over the VPN connection without setting them up separately in StrideLinx Cloud.*

Connect to Devices Behind the StrideLinx Router (cont'd)

VNC Service

Online Help

VNC is a remote screensharing protocol. If you can connect your PC to your machine's local subnet and share its screen via VNC, the StrideLinx Cloud 2.0 VNC service will allow you to access the shared screen remotely from a web browser. You can also use VNC over VPN without setting it up as a separate service.

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.

Add a VNC service

1. In the **Fleet Manager** menu, select **Devices**, then click the name of your router.
2. Click the **Add a service** + icon in the left menu and select **[VNC server]**.
3. **Enter** the requested information (details below) and click **[Add]**.

VNC Settings	
Setting	***Description***
Name	Name your VNC service for easy distinction from other services.
IP address	The IP address of your machine.
Port	The port number where the VNC server can be reached. By default it's 5900 (for VNC).
Password	If your machine's VNC server is password protected, enter its password here.
Access category	The access category determines who can use this VNC service. More information about access categories and how you can create one can be found can be found in this online help article, or in the User Management section of this chapter.
Read-only mode	Enabling read-only mode will ignore any user input for this VNC service.
Encoding	Leave "automatic" for compatibility with most systems. Set encoding to match your machine if necessary.
Color depth	Leave "automatic" for compatibility with most systems. Set color depth to match your machine if necessary.

4. You have now made the changes in StrideLinx Cloud, but these are not yet active in your device. Click **[Push config to device]** in the top right corner for them to take effect.

NOTE: *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.*

Use a VNC service

1. In the **Portal** menu, select **Devices**, then click the name of your router.
2. Make sure the StrideLinx router is **online**, (has a **green dot** beside it in the Portal.
3. Click on the **name** of your VNC service in the **remote access** section.

Connect to Devices Behind the StrideLinx Router (cont'd)

HTTP Service

Online Help

If your machine runs an HTTP server, you can access it over the VPN connection, or you can access it without needing to establish a VPN connection to your device by setting it up as a service.

Add an HTTP service

1. In the **Fleet Manager** menu, select **Devices**, then click the name of your router.
2. Click the **Add a service** + icon in the left menu and select **[HTTP server]**.
3. **Enter** the requested information (details below) and click **[Add]**.

VNC Settings	
Setting	***Description***
Name	Name your HTTP service for easy distinction from other services.
IP address	The IP address of your machine. Leave empty if you want to access the HTTP server of the router.
Protocol	The protocol supported by the machine's server: HTTP or HTTPS.
Port	The port number where the HTTP server can be reached. By default it's 80 (for HTTP) or 443 (for HTTPS).
Default landing page	If your machine has a specific page that you want to open by default, you can enter the page name here. You can find the page name in the address bar after opening it. Leave "/" if you are unsure.
Access category	The access category determines who can use this HTTP service. More information about access categories and how you can create one can be found can be found in this online help article, or in the User Management section of this chapter.

4. You have now made the changes in StrideLinx Cloud, but these are not yet active in your device. Click **[Push config to device]** in the top right corner for them to take effect.

Use an HTTP service

1. In the **Portal** menu, select **Devices**, then click the name of your router.
2. Make sure the StrideLinx router is **online** (has a **green dot** beside it in the Portal).
3. Click on the **name** of your HTTP service 🌐 in the **remote access** section.

Connect to Devices Behind the StrideLinx Router (cont'd)

WebSocket Service

Online Help

If your machine runs a WebSocket server, you can access it over the VPN connection, or you can access it without you first needing to establish a VPN connection to your device by setting it up as a service.

StrideLinx Cloud will act as a proxy for the WebSocket connection between your computer, that is running a WebSocket client, and the machine that is running the WebSocket server.

Add a WebSocket service

1. In the **Fleet Manager** menu, select **Devices** ▭▯, then click the name of your router.
2. Click the **Add a service** + icon in the left menu and select **[WebSocket server]**.
3. **Enter** the requested information (details below) and click **[Add]**.

VNC Settings	
Setting	***Description***
Name	Name your WebSocket service for easy distinction from other services.
Protocol	The protocol supported by the machine's server: WebSocket (WS) or WebSocket Secure (WSS).
IP address	The IP address of your machine.
Port	The port number where the WebSocket server can be reached. By default it's 80 (for WS) or 443 (for WSS).
Access category	The access category determines who can use this WebSocket service. More information about access categories and how you can create one can be found can be found in this online help article, or in the User Management section of this chapter.

4. You have now made the changes in StrideLinx Cloud, but these are not yet active in your device. Click **[Push config to device]** in the top right corner for them to take effect.

Use a WebSocket service

You can connect to your WebSocket server using an app that includes a WebSocket client. This app also needs to **support** the option for you to **login** to your StrideLinx account and select a **company**, **agent** (device), and **agent's service** (WebSocket). StrideLinx Cloud will act as a **proxy** for the WebSocket connection.

Installing VPN Client Software on Your PC

Online Help

The VPN client is a lightweight application that runs in the background on your computer. It creates a virtual Ethernet port on your PC and handles all communication between your PC, StrideLinx Cloud, and your remote machine.

1. Go to the **Fleet Manager**, which is accessible via the **Apps menu** ⠿ in the top right corner of your StrideLinx account.
2. Open the **main menu** ≡ , select **Tools** ⊘ in the left menu, and select **[Download installer]** on the **VPN Client** card.
3. Select and **download the installer** for your PC. VPN client versions are available for Windows, MacOS, and Linux. The instructions here will focus on the Windows installer.

NOTE: *If you are using* ***Mozilla Firefox****, please close your browser during the installation.*

4. Run the downloaded installer and **follow the steps in the installation wizard**.
5. Once the installation has completed, **refresh the StrideLinx web page**.
6. The VPN client will be launched automatically as a Windows Service. Now that you've installed the VPN client, you are ready to make a VPN connection.

NOTE: *If your computer's internet connection uses a* ***proxy server****, or your country or network* ***doesn't allow standard VPN connections****, please see the online help article to the right for additional instructions.*

Online Help

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.

Using StrideLinx on Your Mobile Device

Online Help

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 Cloud, or may establish a direct VPN connection through the StrideLinx router. Mobile VPN access requires router firmware versions v3.14 or newer. The apps provide mobile access to the StrideLinx Cloud Portal, including the following:

- Connect to devices behind the router, for example, using the ***C-more*** Remote Access app.
- Invite users
- Router status
- Read messages
- Monitor data dashboards
  (Note that model SE-SL3001 does not support Cloud Reporting or Cloud Notify.)
- 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.*

Connecting to the VPN on your mobile device

1. **Start** the StrideLinx Portal mobile app and **login**.
2. Open the StrideLinx **Portal**, which is opened by default but also accessible via the **More menu** ••• in the bottom right corner if you are currently in a different cloud app.
3. Go to **Devices** ▭ in the bottom menu, **select** your router, and press **[Connect]** in the VPN section.

You now have a VPN connection and can switch to another app on your smartphone to connect to the machine. The VPN connection stays active in the background.

iOS Client

The VPN client for iOS devices is available in the iTunes App Store at https://apps.apple.com/us/app/stridelinx-portal/id1561323550, or by scanning the QR code to the right.

Using StrideLinx on Your Mobile Device (cont'd)

Android Client

The VPN client for Android devices is available in the Google Play Store at https://play.google.com/store/apps/details?id=com.stridelinx.portal, or by scanning the QR code to the right.

Access via Web

Alternatively, mobile devices not connected through a StrideLinx app can access services set up for connection through the StrideLinx Cloud via the web at 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

1. Open the Safari browser
2. Navigate to www.StrideLinx.com
3. Tap the menu-icon
4. In the menu, tap on the "Add to Home Screen" option
5. Choose "Add"
6. The StrideLinx WebApp will now be accessible from your home screen

On Android Devices

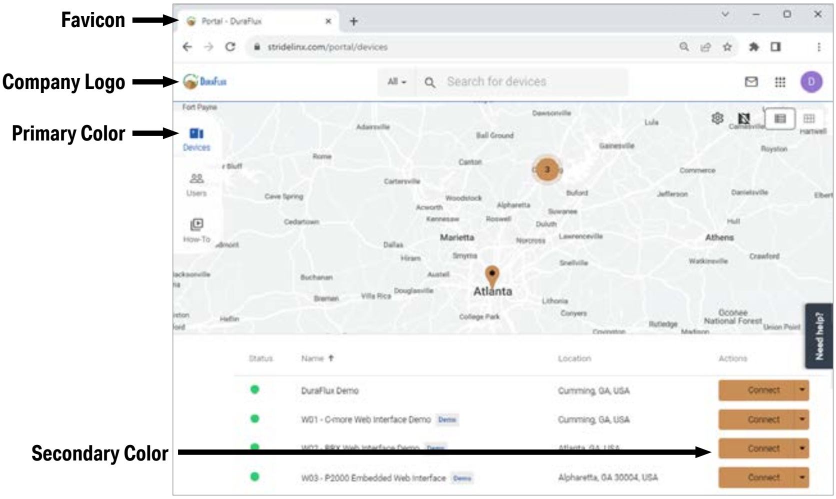
1. Open the Chrome browser
2. Navigate to www.StrideLinx.com
3. Tap the menu-icon (three dots)
4. In the menu, tap on the "Add to Home Screen" option
5. Choose "Ok"
6. The StrideLinx WebApp will now be accessible from your home screen

Branding

Online Help

StrideLinx Professional License

Branding is available as part of the StrideLinx Professional license. Branding enables you to set your own company name, logo, favicon and color scheme.



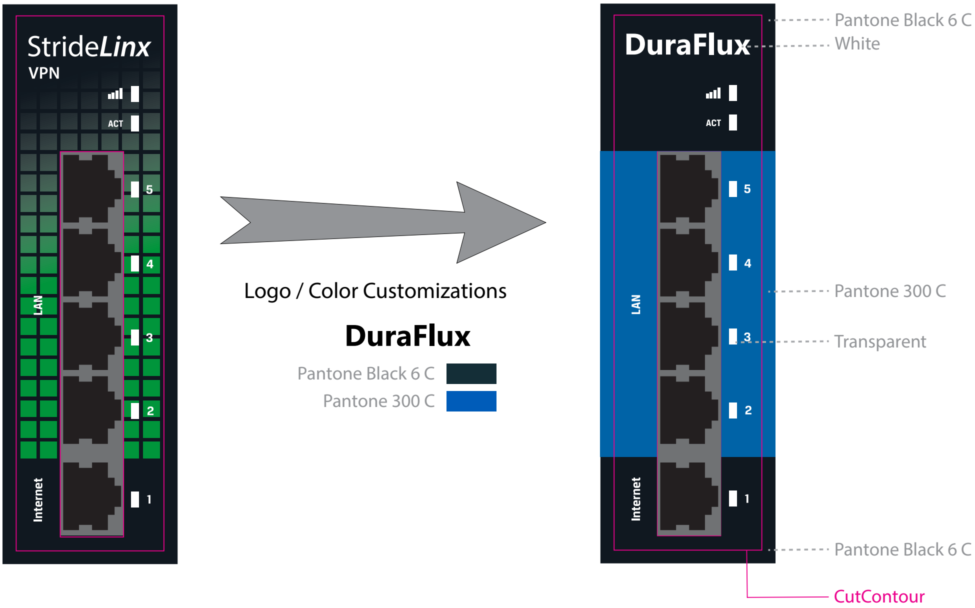
With the StrideLinx Professional license you can make changes to the company branding by selecting **Identity** from the **Admin menu** ☰, then selecting the branding entity to customize.

Branding Parameters	
Field	***Details***
Company ID	The unique identifier of your company. This can't be changed. You might need this for certain actions.
Company name	The name your own company environment in StrideLinx Cloud 2.0.
Country	The country where you want your company to be based.
Company branding	You can choose the colors and logo's displayed in the Cloud in this menu. Your options are:
Company logo	Upload your own logo. Images up to 10MB can be uploaded. The following formats are supported: .jpg, .jpeg, .png, .bmp, .tiff, .ico.
Detect logo colors	Automatically add the colors of your logo.
Primary	The primary color. You can also choose the text color.
Secondary	The secondary color. You can also choose the text color.
Header style	Choose the way you want to apply the primary and secondary colors.
Logo style	Choose the background color behind your logo.
Site title	the title of the site that will be displayed in your browser.
Favicon	The image that will be displayed in your browser.

Branding (cont'd)

Custom Faceplates

A template and instructions for creating a custom faceplate label are available on the item page for each router at www.automationdirect.com. You can change the appearance of the router by adding your colors and logo/name to the router faceplate template and getting a custom label printed at the printer of your choice.



Company Administration

Online Help

Switch companies or create a new company

1. If you have a user account, you can add a new company from www.stridelinx.com
2. Open your **account menu** in the top right corner and click **[Switch Company]**.
3. Select an existing company, or click **Add company** +.
4. If adding a new company, enter your **company name** and **[Register]** your company.

Remove a Company

1. Open the **account menu** in the top right corner and select **[switch company]**.
2. Select **More options** ⋮ on the right side of the company you would like to remove.
3. Select **[Leave company]**, then check the **I'm sure** box.
4. Finally press **[Leave and remove company]**.

NOTE: Action cannot be undone.
You cannot regain access to a company after you have removed that company.

Licenses

From the **Admin menu** ☰, select **Licenses** 🎫 to view or add licenses for any add-on services associated with the company.

Licenses for add-on services can be purchased from www.automationdirect.com. You'll receive an activation code to add here.

NOTE: *The license will be activated immediately and the expiration date will be set. If you are activating a Cloud Logging or Cloud Notify license it will still need to be linked to a router.*

Data Usage

From the **Admin menu** ☰, select **Usage** ○ to view an interactive log of VPN data usage for the company. You can track monthly data usage, or drill down to daily or hourly details.

Company Administration (cont'd)

Audit Trail

Online Help

The audit trail contains a detailed event log for all changes that have been made within the StrideLinx Cloud company. It can be used to see what has changed within the company. In the audit trail you can also see which person, server or device triggered a certain change, and when the change occurred.

NOTE: Requirements
You need to have a role with audit trail viewing rights to access the audit trail in your company.

Please follow the steps described below to view a log of activities and details of specific events.

1. From the **Admin menu** ≡, select **Audit Trail** ▤, then select **[Details]** for the event. The event details contain the following information.

Audit Trail Details	
Field	**Details**
Date and Time	The date and time when the event occurred in the configured timezone
Timestamp (UTC)	The UTC timestamp of the date and time
Action	The kind of action that occurred with the event (e.g. CREATE, UPDATE and DELETE)
Target	The object to which the action applies (e.g. a router or user)
Actor	The person, server or device that caused the event
Topic	Detailed information about the target and the object of which the target is part
Before	The configuration as it was before the event occurred
After	The configuration as it was after the event occurred

NOTE: *The Audit trail retains events for 6 months.*

Access and Permissions Management

Online Help

A standard company account allows for basic user management only. The Professional subscription allows for user management as outlined here.

User management is a system you can use to determine what permissions a user will get and for which devices this user will get to execute these permitted actions. The user management system consists of three core elements, as defined below.

User Management Elements	
Element	**Definition**
Roles	A role is a selection of permissions. The role of a user will determine what a user can do. This is partly regulated through permissions for our apps, and partly through permissions to use the pages and services in an access category. There are admin and device permissions, and you can add access categories.
Access categories	An access category is a selection of pages and services.
Groups	A group is a selection of devices and users. Groups put users and devices together. This determines the devices for which a user can execute his or her permissions. You can divide groups in different group types.

How do I use user management?

For an overview of StrideLinx user management, please see our User Management video at https://www.automationdirect.com/VID-CM-0056.

StrideLinx user management allows you to:

- Create your own roles or use our default roles to set-up user management.
- Create your own access categories or use our defaults to set-up user management.
- Create groups or use our default groups.
- Assign new users to roles and groups and manage access of existing users.
- Assign devices to groups and assign services to access categories.

Roles

Online Help

Every user has to get assigned a role in your company. This role determines what permissions that user will have in StrideLinx Cloud. You can configure as many roles as you like yourself, or you can use our default roles. Our default roles are: platform administrator, engineer and customer. They are the most common roles for users of StrideLinx Cloud. It is always possible to change or remove a role later.

Edit an existing role

Please follow the steps described below to edit an existing role.

1. Go to the **Admin**, which is accessible via the **Apps menu** ⠿ in the top right corner of your StrideLinx account.
2. Open the **main menu** ☰, select **Roles** ▦, then click on **[Edit ✎]**.
3. Change the role name, if you want.
4. Edit all the permissions you want to give users with this role. The table on the previous page contains a list of your options. Then click **[confirm]**.

Access and Permissions Management (cont'd)

Add a new role

Please follow the steps described below to add a new role.

1. From the **Admin menu** ☰, select **Roles**, then click [→ **add role**].
2. If you want to give users access to all devices, groups and templates, select **company-wide role**. This is required for some of the permissions, as indicated in the table below. A company-wide role doesn't belong to a group.
3. Select all the permissions you want to give users with this role. The table below contains a list of your options. Then click [**add**].

Permissions Assignable to Roles

Permission	***Details***	***Company-wide role required***
Configure company identity	Make changes to the branding and company info.	Yes
View audit trail	You can see a log of all changes that have been made in your company.	Yes
View licenses	You can see whether Cloud Logging and Cloud Notify licenses are active.	Yes
Manage roles, access categories and group types	Make changes to user management.	Yes
Manage groups	Make changes to the groups in your company.	Yes
Can manage pages and cards	You can create, edit and remove all dashboards in your company.	Yes
Manage users	You can add or remove new users within your group and edit the roles and groups that apply to them.	No
Manage devices	You can manage all existing devices in your group and add new devices.	No
Manage device templates	You can create, edit and remove all device templates.	Yes
Access categories	You can give every role permission to all your access categories.	No
Enforce two-factor authentication	You can enforce 2FA for all users with a certain role. You need to turn on 2FA yourself to apply this permission.	No

Remove a role

Please follow the steps described below to remove an existing role.

NOTE: *When a user is assigned to a role you can't remove that role. You first have to assign that user to a different role to remove that role. There has to be a platform administrator. This means you can't remove the platform administrator role.*

1. From the **Admin menu** ☰, select **Roles**.
2. Choose the role you would like to remove, then click [**Remove** 🗑].
3. Confirm by clicking [**remove**].

Access and Permissions Management (cont'd)

Access Categories

Online Help

The **role** of every user determines what permissions that user has. **Access categories** are a selection of **pages and services** that can be added to a role. All users with that role will then have permission to view and use those pages and services.

Create a new access category

Please follow the steps described below to add a new access category.

1. In the **Admin menu** ☰, select **Roles**, then click [→ **add access category**].
2. Fill in the desired name, then click [**add**].

Edit or remove an access category

Please follow the steps described below to edit or remove an access category.

1. In the **Admin menu** ☰, select **Roles**, then click [**Edit** ✎] or [**Remove** 🗑] beside an access category.

NOTE: *When an access category is still in use with a service, you can't remove that access category. Please move all services to another access category first.*

Link an access category to a service (VPN, VNC, HTTP and/or WebSocket)

Please follow the steps described below to link an access category to a service.

1. In the **Fleet Manager menu** ☰, select **Devices**, then select the device to link services.
2. Select the service to link to an access category, then click [**Access category**] and select the access category to link to the service.

Link an access category to a page

Please follow the steps described below to link an access category to a page.

1. In the **Fleet Manager menu** ☰, select **Devices**, then select the device to which you would like to link a page.
2. Go to **View** ⊞, then go on the page you would like to link. The default page provides basic information on your router and services. If you use our optional Data Logging feature, you can add key parameters from your equipment to be monitored from the router page. Customizing these pages is covered in Chapter 4, Data Logging.
3. Click on [**Access category**] and select the access category to link to the page.

Access and Permissions Management (cont'd)

Groups

Online Help

You can make as many groups as you need, organized any way you like, such as customers, regions and machine types. Every user with a non company-wide role must be assigned to a group. Each user can be assigned to multiple groups.

If you have many groups or groups in different categories, you can **create group types** in order to keep your groups structured. You can add every device to **one group of every group type**. This way **a device can be part of multiple groups**.

We have two **default groups** to get you started: **Customer A** and **Customer B**. Both fall under group type **Customer**. This is the most common way to divide users and routers into groups on StrideLinx Cloud. It is always possible to change or remove a group or group type later.

When you want to add a device-specific role, you don't have to create a group, since that group would consist of only one device.

Create a new group type

1. In the **Admin menu** ☰, select 👥 **Groups**, **More options** ⋮ menu, **Manage**.
2. Select [→ **Add new group type**].
3. Fill in the desired name, then click [**add**].

Edit, remove or rearrange group types

1. In the **Admin menu** ☰, select 👥 **Groups**, **More options** ⋮ menu, **Manage**.
2. Drag a group type to rearrange the display order, or select ✎ **Edit** or 🗑 **Remove**.

Create a new group

1. In the **Admin menu** ☰, select 👥 **Groups** and choose your group type.
2. Select [+ **add new group**]., then fill in the desired name and click [**add**].

Edit or remove a group

1. In the **Admin menu** ☰, select 👥 **Groups** and choose your group type.
2. Open the **More options** ⋮ menu beside a group, then choose [**Edit**] or [**Delete**].

NOTE: *You can't remove a group that contains a device. Please move all devices to another group first.*

Add devices to your groups

To make devices visible for users with a non company-wide role, add your devices to groups.

1. In the **Fleet Manager menu** ☰, select **Devices** ▭, then select your router.
2. Go to [**Info** ⓘ] and click [**Edit** ✎] on the right of a group type.
3. Select the group you would like assigned to this device from that group type.

Two-factor Authentication (2FA)

Online Help

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 Cloud and a time-based encryption algorithm. Thus, access to the enrolled phone device provides a second authentication of your identity.

Enable two-factor authentication

A mobile device is required for enabling two-factor authentication. Every time you log in to StrideLinx Cloud you will need to have access to your mobile device. These next steps will show you how to enable two-factor authentication.

1. On StrideLinx Cloud, open the **account menu** in the top right corner, and select [👤 **My profile**].
2. Go to **Login and security** 🔒 and click [**Two-factor authentication**].
3. Install an **authenticator app** on your mobile phone (e.g. Google Authenticator, Authy, or Duo Mobile).

> ***NOTE: Authentication app***
> *Open the Google Play Store (Android phones), Apple Store (iOS phones), or the Windows Store (Windows phones), search for the application, and follow the steps described there to correctly install the app.*

4. In the authenticator app you'll be able to scan a QR code which will generate a one-time password, which changes every 30s. Enter this one-time **password**, **name** the mobile device, and click [**Turn on**].

> ***NOTE: "I can't scan a QR Code"***
> *If you can't scan a QR code on your device you can also manually enter a code needed to register your device. Click on "I can't scan a QR code" to display a 16-character long code.*

> ***NOTE: Backup codes***
> *You will receive an email containing backup codes after setting up two-factor authentication. We recommend you print or save these codes in a secure location.*

Disable two-factor authentication

1. On StrideLinx Cloud, open the **account menu** in the top right corner, and select [👤 **My profile**].
2. Go to **Login and security** 🔒 and click [**Two-factor authentication**].
3. Click [**Turn off**] to receive a confirmation by email. Open the email and click on the [**Disable two-factor authentication**] link.
4. A webpage will be opened where you have to complete one **final confirmation** step to effectively disable two-factor authentication.

Two-factor Authentication (2FA) (cont'd)

Backup Codes

Once your two-factor authentication setup is completed, you will receive an email which contains five one-time-use backup codes. If your authentication device becomes unavailable for any reason, for example if you replace your phone, you can still use a backup code to enter your account. You can choose to enter a backup code instead of generating a one-time password. You will be notified by email 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 email.

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.

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 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 Cloud may be removed to prevent automatic login, as follows.

1. On StrideLinx Cloud, open the **account menu** in the top right corner, and select [👤 **My profile**].
2. Go to **Login and security** 🔒 and **remove** any devices other than your current connection. Note that you cannot remove the access token for the device you are currently using to access StrideLinx Cloud.

Loss of mobile phone or backup codes

If you lost access to your mobile device, e.g. stolen, broken, or lost, you will need the backup codes that you received per email when you enabled two-factor authentication.

NOTE: Lost backup codes

*If you have lost your backup codes, we urge you strongly to **disable two-factor authentication**. If you re-enable two-factor authentication, new backup codes will be sent to your email address.*

NOTE: Lost device and backup codes

If you lose both your device and your backup codes, you will have no way of logging in to your account!

Resource Center

The Resource Center is available to all users within your StrideLinx company with admin rights, and offers several additional avenues of help.

To open the Resource Center, click the floating **Need help?** tab on the right edge of the Portal or Admin apps, and on the Device page for each router in the Fleet Manager app.

Migration tool

The **Migration Wizard** guides you through migrating devices and users from one company to another. When devices are migrated, they are removed from the original company. When users are migrated, you can choose to remove them from the original company, or keep them a part of both companies. The wizard allows you to remove a company as well once it contains no devices or users.

Support portal

The **Support Portal** is the online help system linked throughout this manual chapter. The link in Resource Center will open the Support portal and allow you to search or browse the help articles.

ADC Community

The **ADC Community** is a place for all AutomationDirect community members to connect, share, and learn from others. You'll find forums for our various product categories, as well as our library of technical articles.

Still have a question?

If your self-service resources don't answer your question, please use our **contact support** page to submit a question directly to our technical support staff.

Install the mobile app

This link gives you quick access to the **install the StrideLinx Portal mobile app** from either the Apple App store or the Google Play store.

AutomationDirect.com Store

All **StrideLinx Licenses** are available on the AutomationDirect webstore. This link will take you to the StrideLinx section of our store.

Chapter 3

Controller Connection Examples

In this Chapter...

CLICK PLC Connection via Cellular Router SE-SL3011-4GG

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-SL3011-4GG 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-SL3011-4GG

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. Locate the Enabling Elements SIM kit provided with the router.
2. Know your CLICK network settings.
3. Have your SE-SL3011-4GG router, LTE antennas and USB stick available.

Setup

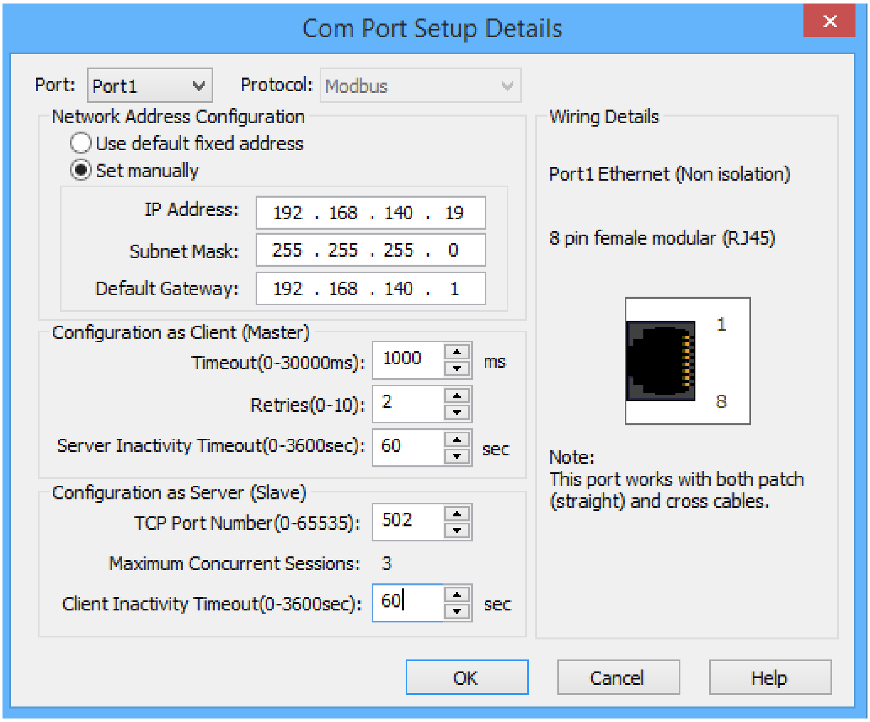
Remember that you can't browse across the VPN to the router's LAN network, so the CLICK must be configured and the network settings known before you configure your router.

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.



Com Port Setup Details

Port: Port1 Protocol: Modbus

Network Address Configuration

○ Use default fixed address

● Set manually

IP Address: 192 . 168 . 140 . 19

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 192 . 168 . 140 . 1

Configuration as Client (Master)

Timeout(0-30000ms): 1000 ms

Retries(0-10): 2

Server Inactivity Timeout(0-3600sec): 60 sec

Configuration as Server (Slave)

TCP Port Number(0-65535): 502

Maximum Concurrent Sessions: 3

Client Inactivity Timeout(0-3600sec): 60 sec

Wiring Details

Port1 Ethernet (Non isolation)

8 pin female modular (RJ45)

Note:
This port works with both patch (straight) and cross cables.

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

Configure Your SE-SL3011-4GG Router

1. Activate the Enabling Elements SIM kit provided with the router through https://enablingelements.com/stridelinx/.

   Steps 2 through 16 are outlined in detail in Chapter 2. If you have already completed router activation, please proceed to step 17.

2. Create your StrideLinx account at www.StrideLinx.com, as discussed in Chapter 2.
3. From **Fleet Manager**, select **Tools** in the left menu, and select **[Start configuration]** on the **Router config file** card.
4. Select the connection type "**Cellular network**".
5. Enter the provider's **APN** and the SIM card's **PIN code** (if applicable).

6. When using a cellular connection, the **IP address** and **DNS server** will be automatically assigned via DHCP, and **HTTP Proxy** will be disabled.
7. **Local control over remote accessibility**, if enabled, will allow you to enable/disable the VPN connection via a wired digital input on the router. Wiring details are in Chapter 1.
8. Enter a **unique IP address** for the LAN side of the router (machine network). This must match the default gateway entered in the CLICK PLC setup (192.168.140.1 in this example).
9. Click **[Download file]** to download the generated file and save it to the root directory of a USB flash drive. Note that the filename on the USB drive must be exactly **router.conf** with no added characters, in case your browser added a suffix.
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-SL3011-4GG router, and **connect** the LTE antenna.
12. **Power on** your StrideLinx router.
13. **Insert** the **USB flash drive** into the StrideLinx router's USB port.
14. Wait around **2 minutes** for the StrideLinx router to configure and register itself. After the router is successfully registered and connected to the StrideLinx Cloud, 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. From **Fleet Manager**, select **Devices** ▭, and look for a yellow bar at the top of your devices list, saying "New device". It also mentions your router's serial number (e.g. 17055202), which you can verify with the serial number on the side of the router. This yellow bar also shows up in the StrideLinx Portal app.
16. Click the yellow bar, name your device as you see fit and select **[Activate]**.
17. Now, your router will appear in the Devices list in your StrideLinx account.
18. 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 option 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 StrideLinx Cloud 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

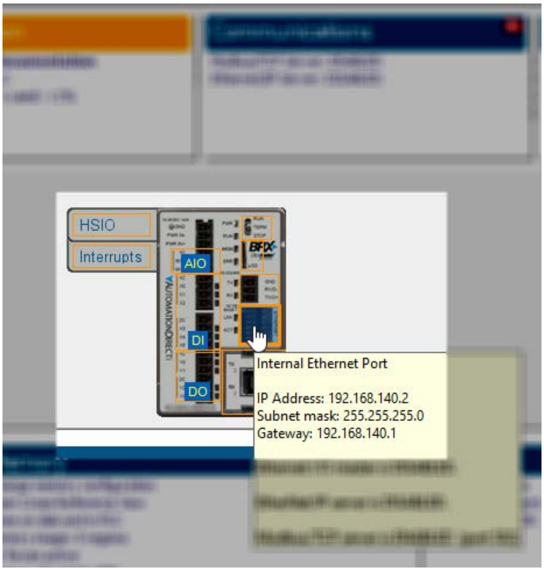
Remember that you can't browse across the VPN to the router's LAN network, so the BRX PLC must be configured and the network settings known before you configure your router.

Configure the BRX PLC Network Settings

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

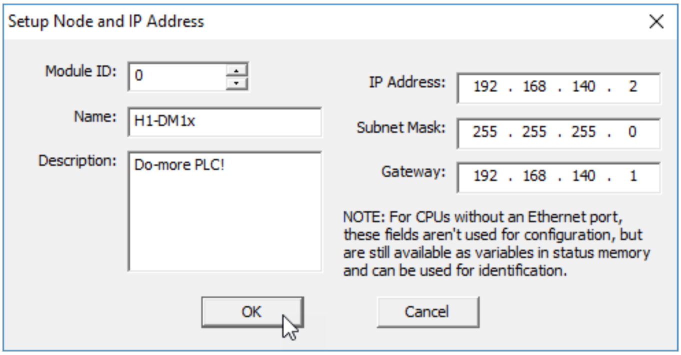
IP Address:	192.168.140.19
Subnet mask:	255.255.255.0
Default Gateway:	192.168.140.1 (the router's LAN IP address) This must be on the same subnet as the BRX PLC

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.



Internal Ethernet Port

IP Address: 192.168.140.2
Subnet mask: 255.255.255.0
Gateway: 192.168.140.1


Setup Node and IP Address

Module ID: 0

Name: H1-DM1x

Description: Do-more PLC!

IP Address: 192 . 168 . 140 . 2

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 140 . 1

NOTE: For CPUs without an Ethernet port, these fields aren't used for configuration, but are still available as variables in status memory and can be used for identification.

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, as discussed in Chapter 2.

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

2. From **Fleet Manager**, select **Tools** in the left menu, and select **[Start configuration]** on the **Router config file** card.
3. Select the connection type "**Wireless network**".
4. Enter the **Network name (SSID)** and **Password** for your wireless network.
5. When using a wireless connection, the **IP address** and **DNS server** will be automatically assigned via DHCP, and **HTTP Proxy** will be disabled.
6. **Local control over remote accessibility**, if enabled, will allow you to enable/disable the VPN connection via a wired digital input on the router. Wiring details are in Chapter 1.
7. Enter a **unique IP address** for the LAN side of the router (machine network). This must match the default gateway entered in the BRX PLC setup (192.168.140.1 in this example).
8. Click **[Download file]** to download the generated file and save it to the root directory of a USB flash drive. Note that the filename on the USB drive must be exactly **router.conf** with no added characters, in case your browser added a suffix when saving the file.
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. **Power on** your StrideLinx router.
12. **Insert** the **USB flash drive** into the StrideLinx router's USB port.
13. Wait around **2 minutes** for the StrideLinx router to configure and register itself. After the router is successfully registered and connected to the StrideLinx Cloud, 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. From **Fleet Manager**, select **Devices**, and look for a yellow bar at the top of your devices list, saying "New device". It also mentions your router's serial number (e.g. 17055202), which you can verify with the serial number on the side of the router. This yellow bar also shows up in the StrideLinx Portal app.
15. Click the yellow bar, name your device as you see fit and select **[Activate]**.
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 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 Cloud 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, and select OK.
4. Select SEND project to ***C-more*** panel.

Configure Your SE-SL3011 Router

1. Create your StrideLinx account at 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.

1. From **Fleet Manager**, select **Tools** ⚙ in the left menu, and select **[Start configuration]** on the **Router config file** card.
2. Select the connection type "**Wired network**".
3. Enter the details for how your StrideLinx router will connect to the internet. In most cases, you can **obtain an IP address automatically**, **automatically assign your DNS server via DHCP**, and leave **HTTP Proxy disabled**. If you will be using port forwarding, though, we strongly advise you to configure a static IP address. Configuring a static IP address will also require that you set a custom DNS server. If you are unsure about what to configure or enter, please consult the local IT administrator.
4. **Local control over remote accessibility**, if enabled, will allow you to enable/disable the VPN connection via a wired digital input on the router. Wiring details are in Chapter 1.
5. Enter a **unique IP address** for the LAN side of the router (machine network). This must match the default gateway entered in the ***C-more*** HMI setup (192.168.140.1 in this example).
6. Click **[Download file]** to download the generated file and save it to the root directory of a USB flash drive. Note that the filename on the USB drive must be exactly **router.conf** with no added characters, in case your browser added a suffix when saving the file.
7. **Install** the VPN Client on your PC. (This step must be repeated for any new PC where you will use your StrideLinx account.)
8. **Mount** and **wire** your SE-SL3011 router, and **connect** Ethernet cables.
9. **Power on** your StrideLinx router.
10. **Insert** the **USB flash drive** into the StrideLinx router's USB port.
11. Wait around **2 minutes** for the StrideLinx router to configure and register itself. After the router is successfully registered and connected to the StrideLinx Cloud, 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.*

12. Activate the router.
13. Now, your router will appear in the Devices list in your StrideLinx account.
14. 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.

Chapter 4

Cloud Reporting

In this Chapter...

Cloud Reporting

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

Why Cloud Reporting?

Cloud Reporting gathers remote data from your control components. The data is transmitted in the StrideLinx Cloud 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 Cloud Reporting Work?

Cloud Reporting (previously called Cloud Logging) enables you to log data from your machine and view it in the StrideLinx Cloud. The data can be visualized in various components, like a graph, that can be viewed in the Portal. It can also be exported as CSV or periodically e-mailed to you in the form of a PDF report.

Cloud Reporting 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. Cloud Reporting does not use your PLC for processing or data storage; the router retrieves the data and stores it on the StrideLinx Cloud.

If there is no internet connection available for the StrideLinx router, your data is not lost. The StrideLinx router will then continue logging data and can store it locally for months at a time, depending on how much data you log. This data is locally not accessible. Once the internet connection has been restored, the logged data will be sent to the cloud (requires StrideLinx router firmware 3.12 or higher).

The StrideLinx Cloud has a crucial role in the functioning of Cloud Reporting. All settings and data points to be logged are set via the StrideLinx Fleet Manager. The StrideLinx Studio allows you to create multiple custom views of your processes, including real-time data and historical trending. Once everything is set up, the StrideLinx Portal is your central location for monitoring your equipment, connecting to it, and exporting data.

The support pages at the Online Help link to the right will answer questions about Cloud Reporting, and guide you through setting up the service.

Online Help

Configure Cloud Reporting On Your Device

To use Cloud Reporting, you'll need:

- a StrideLinx account with a router configured and online
- a Cloud Reporting activation code, purchasable at AutomationDirect.com

The rest of this chapter gives an overview of setting up and using Cloud Reporting. Details are available in the Online Help pages, and linked throughout the chapter.

Activate Cloud Reporting in the Admin App

Online Help

You can purchase a Cloud Reporting license from automationdirect.com and activate it in the Admin App.

1. Go to the **Admin** app, which is accessible via the **Apps menu** ⠿ in the top right corner when logged into your StrideLinx account.
2. Open the **main menu** ☰, select **Licenses** ★ and click [+ Add new license].
3. Enter your activation code and click [Activate].
4. If the license you're activating should apply to a specific router, select a device from the list of available devices and click [Activate]. The newly assigned license will be added to the selected device, and will deactivate any incompatible existing license from the device.
5. Any deactivated license goes into the pool of unassigned licenses and becomes available to activate on a different device.

NOTE: *To see StrideLinx Cloud Reporting in action, please scan the QR code or visit https://go2adc.com/vpn-cloud and click the StrideLinx demo site link to sign up for an interactive product tour.*

Now that you've activated your license, you're ready to set up a data source.

More options for managing your Cloud Reporting license are covered later in this chapter, or at the Online Help link above.

Set Up a Data Source

Online Help

The second step in Cloud Reporting is setting up a data source. This is done by selecting a communication protocol and defining the variables.
The specific steps will vary slightly depending on the selected communication protocol. The table below lists the supported protocols, with a link to the Online Help page with details for setting up each protocol.

Data Source Types	
Protocol	***Online Help Link***
Modbus TCP/IP	https://support.stridelinx.com/hc/en-us/articles/360019030157-Modbus-TCP-IP
Siemens S7	https://support.stridelinx.com/hc/en-us/articles/360019145098-Siemens-S7
Ethernet/IP	https://support.stridelinx.com/hc/en-us/articles/360019029957-Ethernet-IP
OPC-UA	https://support.stridelinx.com/hc/en-us/articles/360019030337-OPC-UA
MELSEC Communication Protocol	https://support.stridelinx.com/hc/en-us/articles/360019146238-MELSEC-Communication-Protocol
BACnet/IP	https://support.stridelinx.com/hc/en-us/articles/360019146318-BACnet-IP
Universal Robots	https://support.stridelinx.com/hc/en-us/articles/360019146398-Universal-Robots
Digital Input	https://support.stridelinx.com/hc/en-us/articles/360019146138-Digital-Input
SMTP	https://support.stridelinx.com/hc/en-us/articles/360019146438-SMTP
Plain-text TCP	https://support.stridelinx.com/hc/en-us/articles/360019030697-PlainTextAPI

Log your Data

The third step in Cloud Reporting is to set up logging your data. To do so, you'll configure data tags, and define custom log triggers if desired.

Configure the data tags

Online Help

Data tags describe how you wish to log your variables. You can choose to log them at a static interval (100ms to 1hr), when their values change, or on a custom trigger. Additionally, you define how long the data should be stored (retention policy).

The Online Help link above will walk you through adding data tags, either manually or by importing from another router or a .csv file, and testing them.

Configure the log triggers

Online Help

Log triggers allow you to log data based on the state of any variable. They allow you to record the value of any number of data tags at the moment that the trigger condition is met There is no limit to the number of triggers you can define, and you can use the same trigger for different data tags.

The Online Help link above will walk you through creating and managing log triggers.

Visualize or Export your Data

Finally, once your data is being logged you'll need a way to use it. StrideLinx lets you export your data to a .csv file, or visualize it on the StrideLinx Cloud.

Visualize your data

Online Help

Visualization does not affect your Cloud Reporting credit (data points per hour). However, the configuration of your data tags, i.e. the effectively logged data, does. There are two ways to visualize your data: Through data reports and through live monitoring. The data is displayed on detailed pages for each router. These views are created in StrideLinx Studio, and viewed online in StrideLinx Portal.

Visualize production counters

Online Help

Machines often contain production counters that count the total number of operations completed. The help article linked to the right gives specific tips on how you can best visualize these to gain insight into how well the machine is doing and whether it's reaching its desired production rates.

Export your data

Online Help

You can easily export your Cloud Reporting data in a .csv format, which you can then use in Microsoft Excel, 3rd party business intelligence tools, or other programs for more advanced analytics. Log triggers allow you to log data based on the state of any variable. They allow you to record the value of any number of data tags at the moment that the trigger condition is met There is no limit to the number of triggers you can define, and you can use the same trigger for different data tags.

The Online Help link above will walk you through exporting your data.

Email your data as PDF reports

Online Help

Machine data that is logged using Cloud Reporting can be periodically e-mailed to you in the form of a PDF report.

With Report Generator you can:

- Create multi-page report templates of your machine data.
- Schedule a report to be sent to you periodically, in PDF format.
- Manually send a report to yourself or other users, in PDF format.

The Online Help link above will walk you through emailing a PDF report.

Test Utility

The test utility is used to check if all the variables are set correctly, and is normally run during the creation of data tags. It shows the communication status with the PLC and displays each variable's current value if everything is configured correctly. If not, the values will stay empty. The test utility will attempt to update values every 0.5 seconds. Please follow the steps below to test your variables.

1. Go to the **Fleet Manager**, which is accessible via the **Apps menu** ⠿ in the top right corner when logged into your StrideLinx account.
2. Open the **main menu** ≡, select **Devices** ▭ in the left menu, and select your router.
3. Expand the **Data source** ▤ service, go to **[Variables]**, and click **[Run test]** at the top.

A connection will now be set up to stream the data directly to your computer, using:

Port: 443

Transport protocol: TCP

Application protocol: WebSocket

You will see live values of all variables, if the configuration is set up correctly.

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.

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.*

Managing your Cloud Reporting License

Online Help

You can **activate** a new Cloud Reporting license, or **extend**, **change** or **transfer** an existing Cloud Reporting license. Further details are provided at the Online Help link at the right.

Activate Cloud Reporting

You can purchase a Cloud Reporting license from AutomationDirect.com and activate it in the Admin App.

1. Go to the **Admin** app, which is accessible via the **Apps menu** ⠿ in the top right corner when logged into your StrideLinx account.
2. Open the **main menu** ≡, select **Licenses** ⭐ and click [+ Add new license].
3. Enter your activation code and click [Activate].
4. If the license you're activating should apply to a specific router, select a device from the list of available devices and click [Activate]. The newly assigned license will be added to the selected device, and will deactivate any incompatible existing license from the device.
5. Any deactivated license goes into the pool of unassigned licenses and becomes available to activate on a different device.

Extend Cloud Reporting

To maintain uninterrupted logging, activate a new license on the router before the current license expires. If the current license expires without a replacement, new logging will stop, but the existing data logs will be kept for up to two weeks. To retain the old logs and begin logging again, simply activate a new license on the router within that two-week period.

To extend a license:

1. Go to the **Admin** app, which is accessible via the **Apps menu** ⠿ in the top right corner when logged into your StrideLinx account.
2. Open the **main menu** ≡, select **Licenses** ⭐.
3. Select **More options** ⋮, then select [**Extend license**].
4. Enter an activation code or select an available unassigned license.

NOTE: *You should only activate one data logging license per router at a time as they will not queue up. Activating a second license on a router will cause the clock to start ticking on activation, not after the first license has expired.*

Transfer a Cloud Reporting license to another device

You can transfer any previously activated Cloud Reporting license to another device by first **deactivating** Cloud Reporting on the current device and then **activating** Cloud Reporting on the new device using the license you just made available. Note that the time period for a previously activated license continues to count down while it is deactivated.

1. Go to the **Admin** app, which is accessible via the **Apps menu** ⠿ in the top right corner when logged into your StrideLinx account.
2. Go to **Licenses**, select **More options** ⋮ on the licenses you want to deactivate and select [**deactivate license for device**].
3. Select the Cloud Reporting license you just made available, select **More options** ⋮ and select [**activate license for device**].
4. Select a device and click [**Activate**].

WARNING: Data is only stored for as long as you maintain an activated Datalogging plan. Activation Codes are purchased at AutomationDirect.com. Data is only stored for the data retention duration of your license. If data older than that duration is important, please archive your data locally before the retention limit is reached.

Chapter
5

Cloud Notify

In this Chapter...

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 Cloud. 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 activate a Cloud Notify code purchased at AutomationDirect.com to your router on the StrideLinx Cloud, configure your triggers and the router will start monitoring your machine immediately.

Each Cloud Notify activation code is tied to a company as an annual subscription, and can be assigned or reassigned to one router at a time.

You can configure any variable as trigger, and set its alarm condition. When the alarm condition is met, all users (configurable) will receive a message, e-mail, and push notification, once. For this to happen again, the alarm condition will have to be removed first.

The support pages at the Online Help link to the right will answer questions about Cloud Notify, and guide you through setting up the service. The rest of this chapter gives an overview of setting up and using Cloud Notify. Details are available in the Online Help pages, and linked throughout the chapter.

Online Help

Configure Cloud Notify On Your Device

To use Cloud Notify, you'll need:

- a StrideLinx account with a router configured and online
- a Cloud Notify activation code, purchasable at AutomationDirect.com

Activate Cloud Notify in the Admin App

Online Help

You can purchase a Cloud Notify license from automationdirect.com and activate it as follows.

1. Go to the **Admin** app, which is accessible via the **Apps menu** ⠿ in the top right corner when logged into your StrideLinx account.
2. Open the **main menu** ☰, select **Licenses** 🎫 and click [+ Add new license].

3. Enter your activation code and click [Activate].
4. If the license you're activating should apply to a specific router, select a device from the list of available devices and click [Activate]. The newly assigned license will be added to the selected device, and will deactivate any incompatible existing license from the device.
5. Any deactivated license goes into the pool of unassigned licenses and becomes available to activate on a different device.

NOTE: *To see StrideLinx Cloud Notify in action, please scan the QR code or visit https://go2adc.com/vpn-cloud and click the StrideLinx demo site link to sign up for an interactive product tour.*

Now that you've activated your license, you're ready to set up a data source.

More options for managing your Cloud Notify license are covered later in this chapter, or at the Online Help link above.

Set Up a Data Source

Online Help

The second step in Cloud Notify is setting up a data source. This is done by selecting a communication protocol and defining the variables. The specific steps will vary slightly depending on the selected communication protocol. The table below lists the supported protocols, with a link to the Online Help page with details for setting up each protocol.

Data Source Types	
Protocol	**Online Help Link**
Modbus TCP/IP	https://support.stridelinx.com/hc/en-us/articles/360019145738-Modbus-TCP-IP
Siemens S7	https://support.stridelinx.com/hc/en-us/articles/360019145078-Siemens-S7
Ethernet/IP	https://support.stridelinx.com/hc/en-us/articles/360019029917-Ethernet-IP
OPC-UA	https://support.stridelinx.com/hc/en-us/articles/360019145978-OPC-UA
MELSEC Communication Protocol	https://support.stridelinx.com/hc/en-us/articles/360019146218-MELSEC-Communication-Protocol
BACnet/IP	https://support.stridelinx.com/hc/en-us/articles/360019030577-BACnet-IP
Universal Robots	https://support.stridelinx.com/hc/en-us/articles/360019146378-Universal-Robots
Digital Input	https://support.stridelinx.com/hc/en-us/articles/360019030477-Digital-Input
SMTP	https://support.stridelinx.com/hc/en-us/articles/360019030657-SMTP
Plain-text TCP	https://support.stridelinx.com/hc/en-us/articles/360019146458-PlainTextAPI

Set up alarms

Online Help

The third step in Cloud Notify is to set up alarms. Alarms describe what trigger event should be notified and to whom, based on priority. Alarms include an on-delay option and you can personalize the event message.

Add connection monitoring alarms

If the router isn't connected, you can't be alerted about machine events. You can add alarms that notify you when the router itself has been offline for at least 15 minutes or comes back online.

1. In the **Fleet Manager** menu, select **Devices**, then click the name of your router.
2. Go to **More** ••• and select **[→Add notification]**.
3. Select the **connection**, enter the **alarm details**, as shown below, and press **[Add]**.

Alarm Details	
Field	**Description**
Connection	Select the connection you want to be notified about. More information: VPN, Configuration, and Data logging connections
Alarm name	The alarm name will be shown in the title of the notification.
Severity	The severity indicates how important the alarm is and will be shown in the notification as well.
Event and Duration	The event and duration determine when the notification will be sent.
Access Category	The access category determines which users receive the notification. More information: How to use access categories
Instructions	Add instructions to the notification to make sure appropriate action is taken. The instructions will be shown in the notification as well.

Manually add alarms

You can add as many alarms as you like, and can use the same variable for different alarms.

1. In the **Fleet Manager** menu, select **Devices**, then click the name of your router.
2. Click **Data source** ☰, **[Alarm triggers]**, then click **[+Add trigger]**.
3. Select a **variable**, enter the **alarm details** as shown below, and press **[Add]**.

Alarm Details	
Field	**Description**
Variable	Choose the variable for which you want to set an alarm.
Name	Enter a name for the alarm.
Severity	Choose the level of severity of the alarm (high, medium or low).
Condition	Choose the condition that will set off the alarm.
Threshold	Choose the value that will set the alarm off together with the condition.
Period	Enter the period for which the alarm event is to be valid to set off the alarm.
Instructions	(optional) Enter instructions on how to resolve the alarm.
Access Category	Choose the access category that will receive the alarms.

4. You have now made the changes in StrideLinx Cloud, but these are not yet active in your device. Click **[Push config to device]** in the top right corner for them to take effect. The router will disconnect temporarily. This may take a minute.

Import alarms from a file

You can easily and effortlessly copy alarms from one device to another by exporting the concerning alarms (see “Manage alarms” below) and then importing them in your new device. Alternatively, you can manually prepare your alarms in the required CSV format to load them all at once into your device. The file structure for manually editing the alarms CSV file is explained in the the Online Help link at the right.

Online Help

You can add as many alarms as you like; there’s no limit. It is possible to use the same variable for different alarms. To manually add an alarm, please follow the steps described below:

1. In the **Fleet Manager** menu, select **Devices** ▭, then click the name of your router.
2. Click **Data source** ☰, **[Alarm triggers]**, then click **[+Add trigger]**.
3. Press **[Import from CSV-file]**, and **select** a CSV file to import.
4. You have now made the changes in StrideLinx Cloud, but these are not yet active in your device. Click **[Push config to device]** in the top right corner for them to take effect. The router will disconnect temporarily. This may take a minute.

Set alarm triggers

You can assign alarm triggers to users with a role that need it using **access categories**. Every alarm has to be added to a certain access category. All users with access to that access category will receive notifications for that alarm. Users can individually opt-out of notifications in the **message center** ✉ located on the StrideLinx home page.

Manage alarms

You can view all defined variables in table form on the **alarm triggers** screen. Variables can be selected by checking the box on the left, or you can select all by checking the box at the top. You can remove selected variables by clicking **[remove selection]** at the top right corner of the screen. You can also choose to download the set alarms by clicking **[Export to CSV-file]**.

Notifications

Online Help

Notifications will appear in the StrideLinx Cloud **message center** ✉ , accessible from the top of the main menu in any of the four StrideLinx web apps. You will receive a message in the message center when any Cloud Notify alarm has been triggered, and also when a device from your company is transferred to another company.

Additionally, you will receive an e-mail and push notification on your phone (requires the StrideLinx mobile app to be installed), unless a filter is set up in the message center to prevent these additional delivery methods.

Details for setting up notification filters are explained in the Online Help link above.

Formatting the Alarm Notification Email

The format of the timestamp in the heading of the email or message notifications is configured in each user's localization preferences, found by clicking your user icon in the upper right of the StrideLinx Cloud, then **[My profile]** > **[Preferences]**.

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.

What Happens When an Alarm is Triggered?

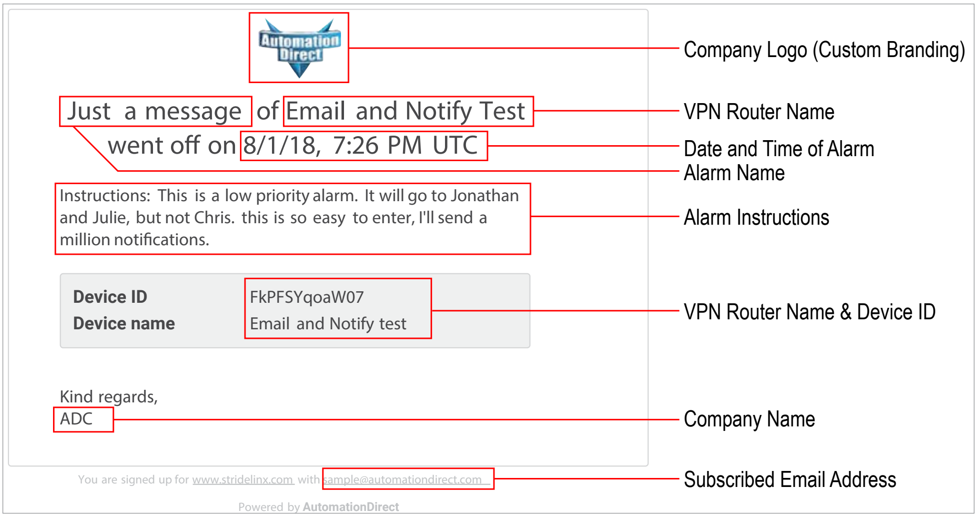
When the trigger condition for an alarm is met, a notification is sent to the relevant group of users and the alarm is archived in the Message Center on the main StrideLinx page.

***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 each user based on the selected Access Category. Each user will receive email and push notifications based on their individual notification filters. Push notification will be sent to the user's mobile device only if the iOS or Android mobile app is installed and configured to accept notifications. 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.



Just a message of Email and Notify Test went off on 8/1/18, 7:26 PM UTC

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.

Device ID	FkPFSYqoaW07
Device name	Email and Notify test

Kind regards,
ADC

You are signed up for www.stridelinx.com with sample@automationdirect.com

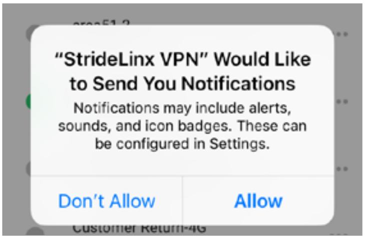
Powered by AutomationDirect

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.



"StrideLinx VPN" Would Like to Send You Notifications

Notifications may include alerts, sounds, and icon badges. These can be configured in Settings.

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 Cloud 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 Cloud and will receive push notifications by default.

View the List of Configured Push Devices on the StrideLinx Cloud

You can verify that a device is set to receive push notifications by checking the "My push devices" list on the StrideLinx Cloud, found by clicking your user icon in the upper right of the StrideLinx Cloud, then **[My profile]** > **[Preferences]**. A device can be deactivated from receiving any push notifications by selecting DEACTIVATE on this screen.

Appendix A

Accessories & Add-on Licenses

In this Appendix...

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

Add-on Licenses

These optional features 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 StrideLinx Cloud to you and your customers.

After you purchase these optional features, you will receive an email with an Activation Code. This code is applied to your router in the StrideLinx Cloud. Activation codes can only be used once. So if a device is removed the license will also be removed. This is prevented by deactivating the code and then re-activating it on the same or another router. In the event of accidental removal, a router can also be put into “recovery mode” which will enable it to automatically reacquire a lost license when the device is registered in the cloud again.

NOTE: *Model SE-SL3001 does not support Cloud Reporting or Cloud Notify.*

Cloud Reporting

The Cloud Reporting license 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 Reporting licenses offer unlimited live monitoring and historical data reporting dashboards, with unlimited number of data tags.

StrideLinx Cloud Reporting Options

Part #	Description	Term	Data Logging Points/Hour	Data Retention	Features
SE-SLR010-1	StrideLinx Basic Reporting and Logging License	1 year	1,000	6 months	License includes data logging enabled at 1,000 data samples per hour with schedule reporting. For use with (1) StrideLinx router.
SE-SLR011-1	StrideLinx Professional Reporting and Logging License	1 year	10,000	7 years	License includes data logging enabled at 10,000 data samples per hour with schedule reporting. For use with (1) StrideLinx router.

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 Cloud, configure your triggers and the router will start monitoring your machine immediately.

Cloud Notify license offers unlimited live monitoring dashboards

StrideLinx Add-on Licenses			
Part #	**Description**	**Term**	**Features**
SE-SL021-1	StrideLinx Notify License	1 year	License includes alarm, trigger, recipient, and priority management with push and email notifications. For use with (1) StrideLinx router.
SE-SLR001-1	StrideLinx Professional License	1 year	License includes white label StrideLinx platform, unlimited VPN data traffic and advanced user and device access management. For use with (1) StrideLinx company. Throttling may occur after 1 TB.
SE-SL051	StrideLinx Mobile App Sustained Service License	1 year	License includes sustained service of white label StrideLinx iOS/Android mobile app with branding. For use with (1) existing white label StrideLinx iOS/Android mobile app.

Appendix B

Troubleshooting

In this Appendix...

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 router.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, enable **HTTP Proxy** and enter your proxy's information during the WAN settings step of creating your configuration file. The settings can also be changed directly in your router's local web interface, as explained in the Online Help link to the right.

Online Help

Configuring the 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 isn't recognized.

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 Cloud. 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.***

1. In the **Fleet Manager** menu, select **Devices** ▭▯, then click the name of your router.
2. Expand the **Network** ⚙ options and go to **[WAN]**.
3. Set up the new WAN connection, following the steps on pages 2-17 through 2-19.
4. When multiple WAN connection types are configured, the router will automatically use one as the preferred connection and others as fallback connections.
5. To change the priority of the connections, you can **drag and drop** ⠿ the connections to arrange their priority.
6. To remove the old WAN connection method instead of using it as a backup, simply click **[Configure]** on the connection type, then **[Remove]**.
7. You have now made the changes in StrideLinx Cloud, but these are not yet active in your device. Click **[Push config to device]** in the top right corner for them to take effect.

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 "stealth" option to have your router be able to set up a VPN connection to our StrideLinx servers.

1. In the **Fleet Manager** menu, select **Devices** ▭▯, then click the name of your router.
2. Expand the **Network** ⚙ options and go to **[VPN]**.
3. Toggle **[Use stealth mode]** in the **Stealth mode** section
4. This setting is applied the **next time your device connects**, and does not require pushing the configuration change to the router.
5. If the VPN connection is active when changing this setting, then turn the VPN connection **OFF** and back **ON** again as explained at the top of this page to use the new setting.

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 VPN Client Software on Your PC” section of Chapter 2 explains the installation, as well as the Online Help link to the right.

Online Help

Once you’ve installed the VPN Client, refresh the StrideLinx Cloud 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 áfter 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.

1. In the **Fleet Manager** menu, select **Devices** ▭, then click the name of your router.
2. Expand the **Network** ⚙ options and go to **[LAN]**.
3. Change the advanced LAN settings.
4. You have now made the changes in StrideLinx Cloud, but these are not yet active in your device. Click **[Push config to device]** in the top right corner for them to take effect.

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. The "Connect to Devices Behind the StrideLinx Router" section of Chapter 2 and the Online Help link at the right explain how you can add or manage these services.

Online Help

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 as follows:

1. In the **Fleet Manager** menu, select **Devices**, then click the name of your router.
2. Select the VNC service in **[Services]**, and edit the advanced settings to match your application.

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^2. 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. Check the wireless signal strength at the router location.
   a. (WiFi) On a smartphone, open WiFi settings and confirm wireless access point signal strength and SSID, password. If your smartphone shows a signal the wireless connection to the router should also be adequate.
   b. (4G) Check the 4G LTE signal strength in the Overview section of the router's local web server page at it's LAN IP address (default 192.168.27.1).
6. For the 4G router, contact Enabling Elements, Inc. (https://enablingelements.com/stridelinx/) to troubleshoot cellular issues on AT&T and Verizon networks.

Appendix C

Safety and Security Considerations

In this Appendix...

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.

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/pubs/sp/800/82/r3/final
- ISA99, Industrial Automation and Control Systems Security https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99 (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

The StrideLinx router's Digital Input should be used as a part of your safety lockout procedures for any device accessible remotely via the StrideLinx VPN.

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.

Local control of remote access via the digital input must be configured using a configuration file. The settings cannot be remotely changed through the StrideLinx Cloud. For instructions on wiring and configuring the input, see the support article at https://support.stridelinx.com/hc/en-us/articles/360019029717-Switch-VPN-on-off#h_5121468265152533O522824.

Appendix D

Data Logging Address Notation — AutomationDirect Devices

In this Appendix...

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)			
Function Code	***StrideLinx Modbus Address***	***Data Type***	***CLICK Address***
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)			
Function Code	***StrideLinx Modbus Address***	***Data Type***	***DirectLogic Address***
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)			
Function Code	***StrideLinx Modbus Address***	***Data Type***	***DirectLogic Address***
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	300001/300002
4	1		300002/300003
4	65534		365535/365536
4	0	FLOAT32	300001/300002
4	1		300002/300003
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*

Appendix

E

StrideLinx Network Security

In this Appendix...

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 Cloud 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. This appendix discusses how StrideLinx complements your network security. For an in-depth look at StrideLinx Platform security, please see the white paper at https://library.automationdirect.com/wp-content/uploads/2020/10/StrideLinx-Security-white-paper.pdf.

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 Cloud

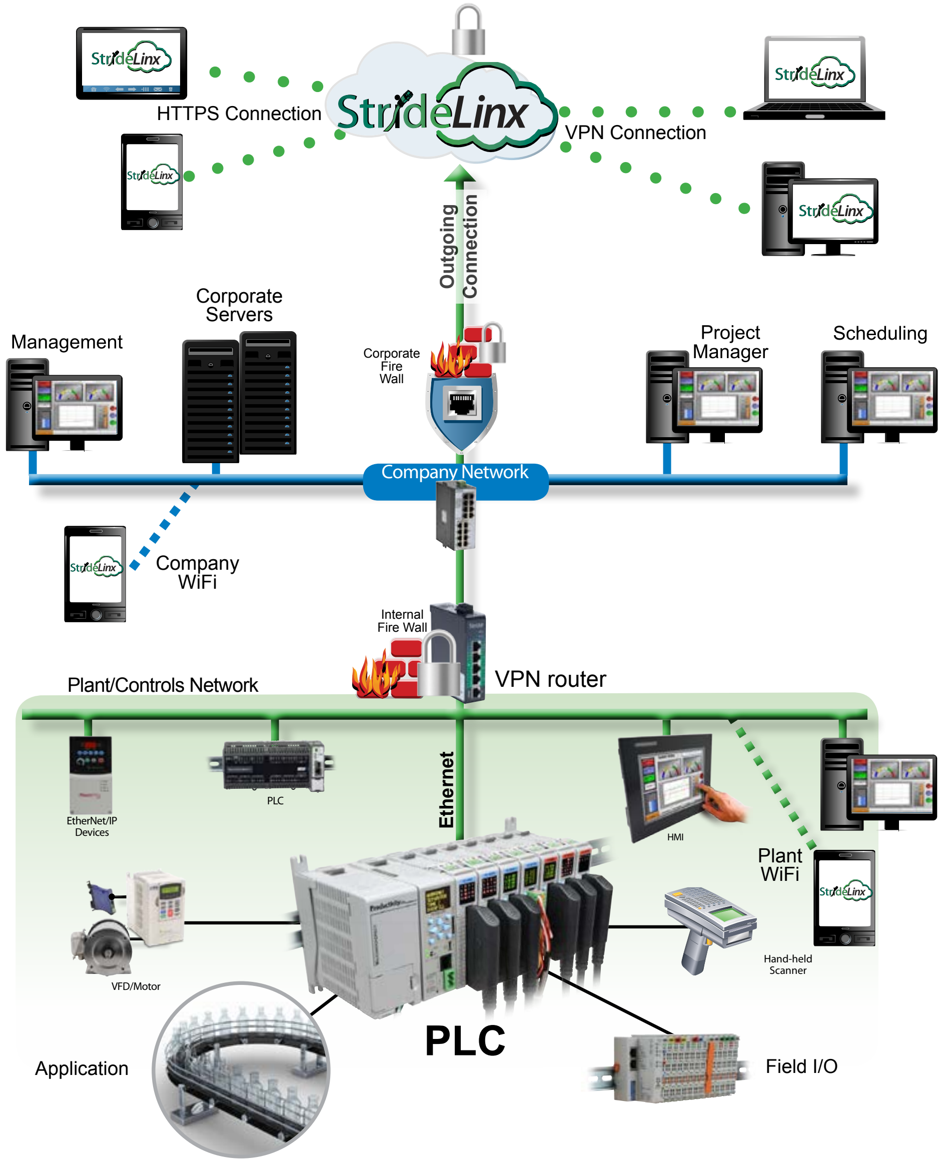
The StrideLinx Cloud is a secure web-based platform made up of a worldwide network of scalable servers. It is focused on delivering and enhancing innovative secure remote access. The StrideLinx router connects your hardware to the StrideLinx Cloud via a secure VPN connection.

StrideLinx Client

The VPN client is a light-weight application that runs in the background on your PC. A VPN connection is established when you use the StrideLinx Cloud to remotely connect to your devices.

Overview

The remote access solution is made up of two connections – the client to cloud servers and the 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 Cloud 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.



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 Cloud using a web browser (clientless access). No VPN client is required for this mode and allows the user flexibility in connecting to the Cloud from any mobile device or PC with a web browser. Capabilities in this mode include all standard Cloud 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 Cloud by VPN, allowing full local area network access. This method requires users log in to the Cloud 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 Cloud.

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 Cloud. 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 unsecure.

- VPN→LAN port forwarding provides a secure port forward inside the encrypted VPN tunnel so that S trideLinx users can access the HTTP server or VNC server of their control network devices by shortcut services in the StrideLinx Cloud. 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 Cloud. 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 Cloud, 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 Cloud and sends out 'keep-alive heartbeats' on a regular interval. The remote connection between the StrideLinx router and StrideLinx Cloud 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 Cloud.

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 Cloud.

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 Cloud. 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 unsecure.***

- 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 Cloud. This feature allows the clientless access mode for mobile & PC users as described in the “Solution Explained” section above.

StrideLinx Cloud 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 Cloud

A crucial link within the complete StrideLinx solution is the StrideLinx Cloud, 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 Cloud. As a result, the StrideLinx Cloud is protected against so called man-in-the-middle attacks.

Only authorized users can access the controls network via our StrideLinx Cloud. 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 Cloud 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 Cloud. 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 Cloud 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 Cloud 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 Cloud.

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.

Appendix F

Capabilities of Connected AutomationDirect Devices

In this Appendix...

Network Topology

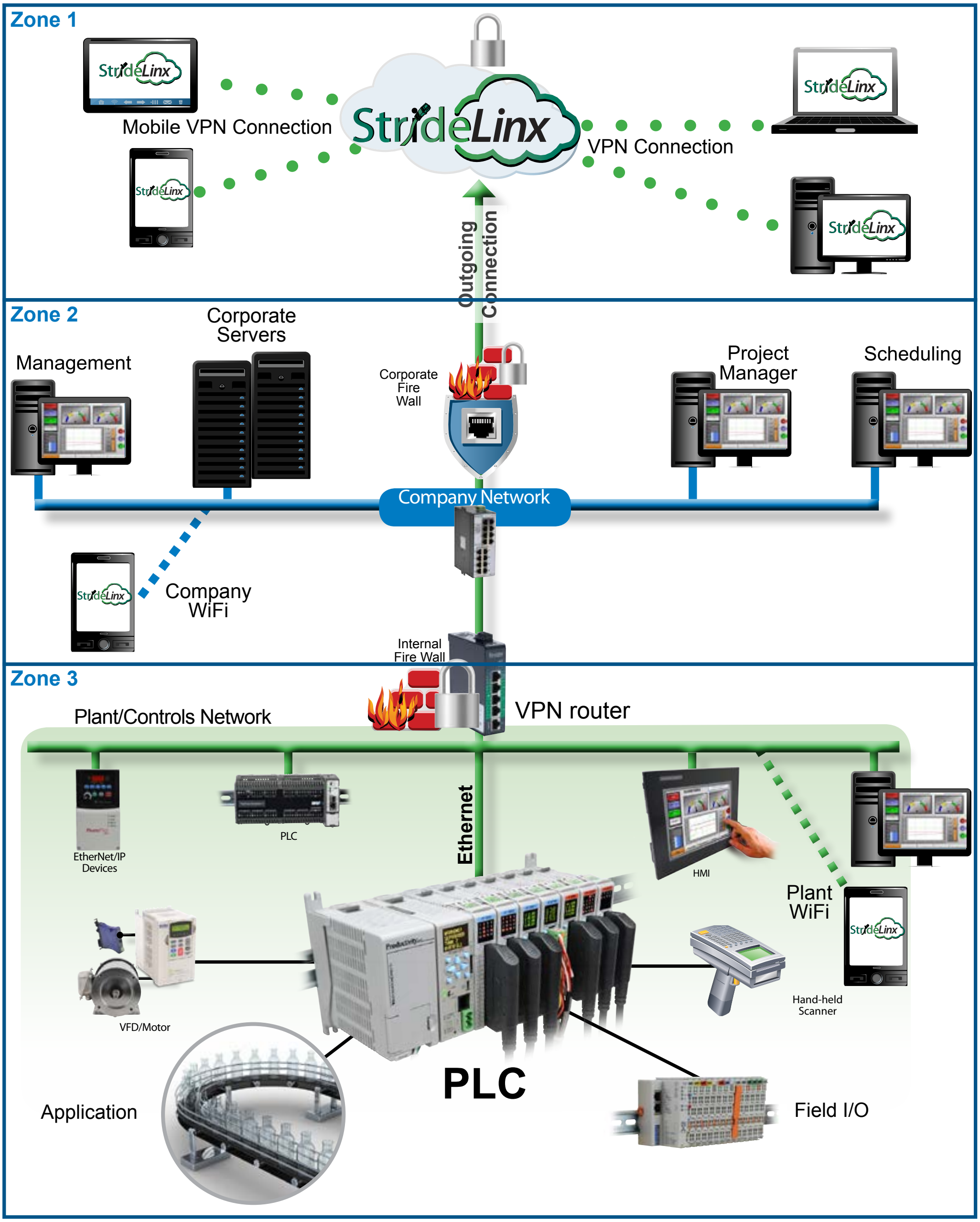
To facilitate description of the capabilities of various AutomationDirect product lines when connected to a StrideLinx VPN router, the overall topology of a network connecting plant devices to the StrideLinx Cloud can be divided into three zones, as illustrated in the two figures later in this appendix.

The zones are defined as follows.

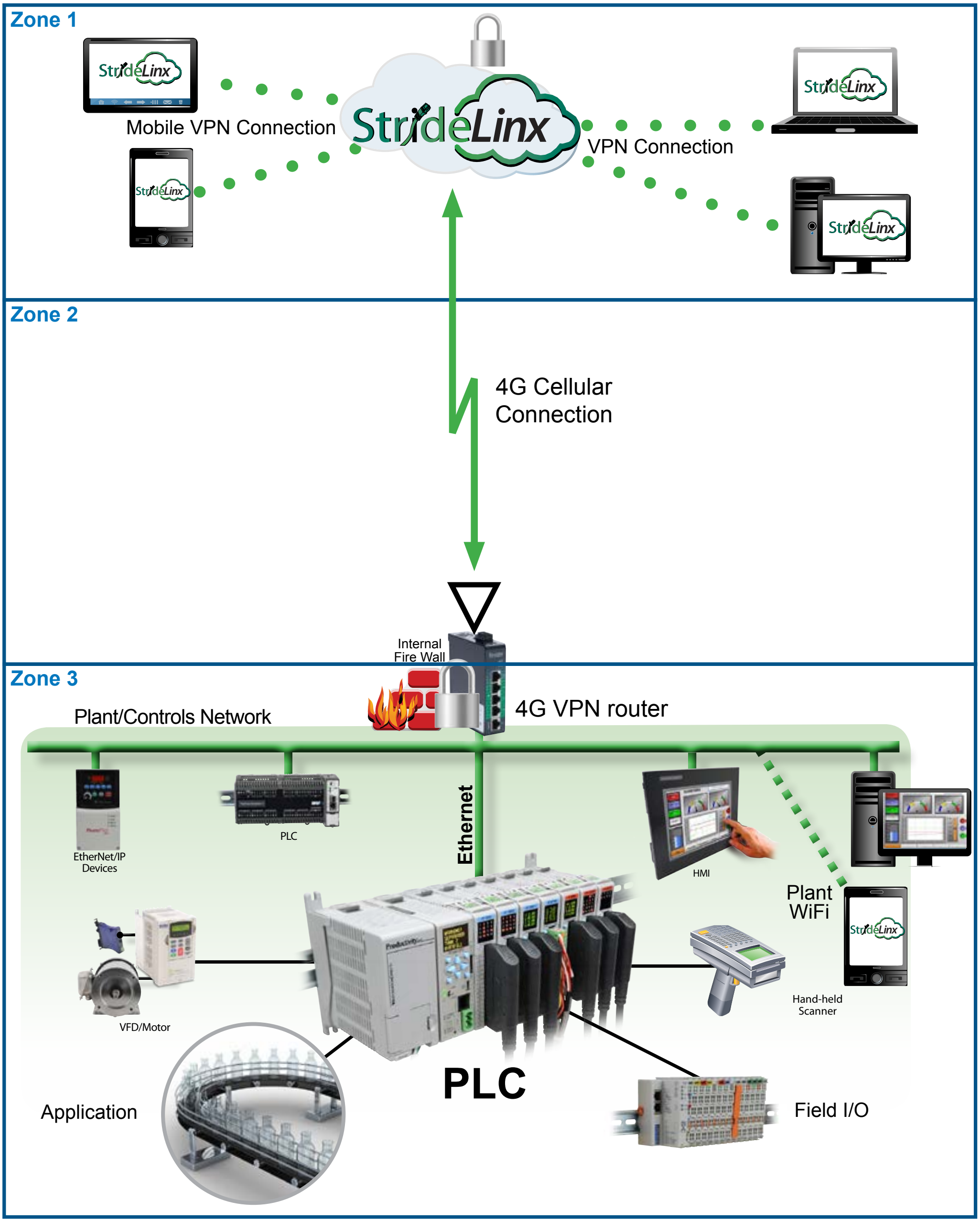
- Zone 1 is outside the company network, and includes the StrideLinx Cloud and secure connections to it from various devices.
- Zone 2 is the company network, which exists behind a corporate firewall. This zone may include various computer systems, but is isolated from the plant/controls network by the 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



Network with StrideLinx VPN router using 4G cellular network connectivity



Device Capabilities

The following table describes the capabilities of devices to establish communications connections across various network zones, as defined earlier.

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*** [1,6]	***Zone 3->2*** [6]	***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
CLICK programming SW	N	Y	Y	NA	NA	Y
C-more programming SW	N	Y	Y	NA	NA	Y
C-more Remote Access (PC)	N	Y	Y	NA	NA	Y
PxK/***C-more*** web server	Y[4]	Y	Y	NA	NA	Y
PxK/***C-more*** FTP access (into PxK/***C-more***)	N	Y	Y	NA	NA	Y
BRX/PxK/***C-more*** Email to Server (sent from BRX/PxK/***C-more***)	NA	NA	NA	Y[2]	Y[2]	NA
PxK/***C-more*** FTP to PC (sent from PxK/***C-more***)	NA	NA	NA	Y[2]	Y[2]	NA
PxK/***C-more*** mobile app (connect by WiFi)	N	Y[8]	Y[3]	NA	NA	Y
3rd party PLC or HMI web/VNC server	Y[5]	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 Cloud (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 Cloud (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 & cloud 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.*

Automation
Direct®