

STRIDELINUX CLOUD 2.0



In this Chapter...

What is Stridelinx Cloud 2.0?	2-4
The Legalese	2-5
Terms of Use	2-5
Data Fair Use Policy	2-5
Getting Started With StrideLinx Cloud 2.0	2-6
Overview of the Steps	2-6
Create an Account	2-7
Set Up your StrideLinx VPN Router	2-8
Connect to Your Machine.....	2-14
Update Router Settings	2-16
Router Name, Description, Location and Groups	2-16
Firmware Upgrade/Downgrade.....	2-16
WAN (Internet) Settings, Wired Network	2-17
WAN (Internet) Settings, Wireless Network.....	2-18
WAN (Internet) Settings, Cellular Network.....	2-19
Fallback WAN Connections (Failover).....	2-20
LAN (Machine Network) Settings.....	2-21
Wi-Fi Hotspot	2-22
Network Time (NTP) Server	2-22
Additional Subnets Behind External Gateway	2-23
Router Firewall Settings	2-24
Switch VPN Off Remotely to Reduce Data Usage	2-25
Connect via a censored network (stealth mode)	2-25
Local Router Configuration Through LAN Port.....	2-25

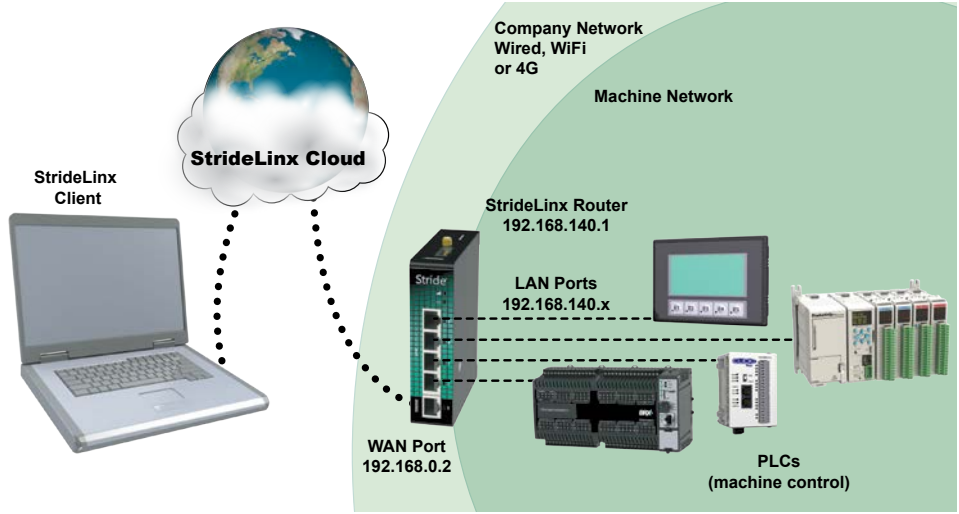
Device Management	2-26
Transfer a Router to Another Company	2-26
Recover device settings after factory reset (recovery mode).....	2-27
Remove a device from your company.....	2-27
Save/Load Router Configuration Templates	2-28
Connect to Devices Behind the StrideLinx Router	2-29
Device Status	2-29
VPN Service	2-30
VNC Service.....	2-31
HTTP Service.....	2-32
WebSocket Service	2-33
Installing VPN Client Software on Your PC	2-34
Support.....	2-34
Using StrideLinx on Your Mobile Device.....	2-35
Connecting to the VPN on your mobile device.....	2-35
iOS Client	2-35
Android Client	2-36
Access via Web.....	2-36
Branding	2-37
StrideLinx Professional License	2-37
Custom Faceplates	2-38
Company Administration.....	2-39
Switch companies or create a new company	2-39
Remove a Company.....	2-39
Licenses	2-39
Data Usage.....	2-39
Audit Trail.....	2-40
Access and Permissions Management	2-41
How do I use user management?	2-41
Roles	2-41
Access Categories.....	2-43
Groups	2-44

Two-factor Authentication (2FA)	2-45
Enable two-factor authentication.....	2-45
Disable two-factor authentication	2-45
Backup Codes.....	2-46
Logging In	2-46
User Access Token.....	2-46
Loss of mobile phone or backup codes.....	2-46
Resource Center	2-47
Migration tool	2-47
Support portal.....	2-47
ADC Community.....	2-47
Still have a question?.....	2-47
Install the mobile app	2-47
AutomationDirect.com Store	2-47

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.

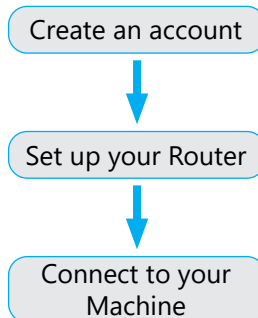
If you need help with any steps along the way, the StrideLinx Cloud 2.0 Support Portal is available at support.stridelinx.com. Click on the "Online Help" link to the right of some of the steps for direct access to that topic in the support portal.

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:



Getting Started:

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.

Getting Started:

Create an account



Set up your Router



Connect to your Machine

Set Up your StrideLinx VPN Router

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

[Online Help](#)

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.

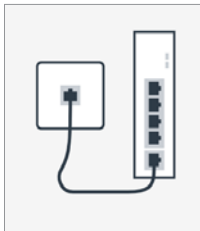
Before you Begin:

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

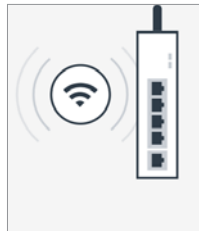
- a StrideLinx user account, set up in the previous step
- a StrideLinx VPN Router, with power
- a means to connect the router to the internet (wired, Wi-Fi, or cellular)
- physical access to the StrideLinx VPN Router for its initial setup
- a USB flash drive, formatted as FAT/FAT32
- a PC with internet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

Choose a connection type

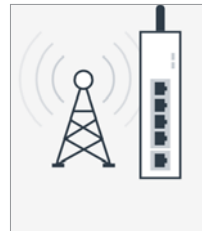
There are three possible ways to connect the router to StrideLinx Cloud 2.0, depending on which StrideLinx VPN router model you have: a **wired**, **wireless** or **cellular** connection. Choose one of the methods for now, but note that you can change the connection method later, and even add backup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

Getting Started:

Create an account



Set up your Router



Connect to your Machine

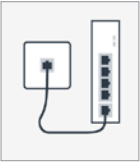
Config file



Register



Activate






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** , 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.

Getting Started:

Create an account



Set up your Router



Connect to your Machine

Config file



Register



Activate



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.

Getting Started:

Create an account



Set up your Router



Connect to your Machine

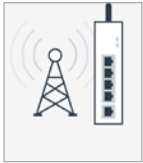
Config file



Register



Activate



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.

- Go to the **Fleet Manager**, which is accessible via the **Apps menu**  in the top right corner when logged into your StrideLinx account.
- Open the **main menu** , select **Tools** , and select **[Start configuration]** on the **Router config file** card.
- Select the connection type "**Cellular network**".
- Enter the provider's **APN** and the SIM card's **PIN code** (if applicable).
- When using a cellular connection, the **IP address** and **DNS server** will be automatically assigned via DHCP, and **HTTP Proxy** will be disabled.
- 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.
- 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.
- 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.

Getting Started:

Create an account



Set up your Router



Connect to your Machine

Config file



Register



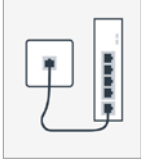

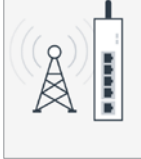
Activate

Register your router on StrideLinx Cloud 2.0

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

[Online Help](#)

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

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



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
RouterConnect to your
Machine

Config file ✓



Register ✓



Activate

Activate your StrideLinx router

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

[Online Help](#)

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.

Getting Started:

 Create an account Set up your Router

Connect to your Machine

Connect to Your Machine

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.

[Online Help](#)

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](#)

Getting Started:

Create an account






Set up your Router



Connect to your Machine

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

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.

[Online Help](#)

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

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.

[Online Help](#)


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 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 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 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

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.

[Online Help](#)

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.

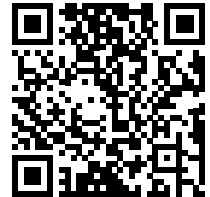
Connecting to the VPN on your mobile device

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

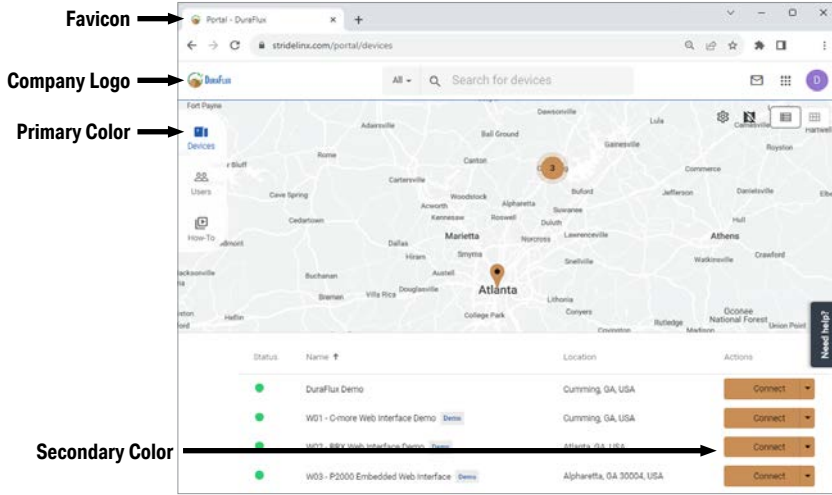
1. Open the Chrome browser
2. Navigate to www.StrideLinx.com
3. Tap the menu-icon (three dots)
4. In the menu, tap on the “Add to Home Screen” option
5. Choose “Ok”
6. The StrideLinx WebApp will now be accessible from your home screen

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.



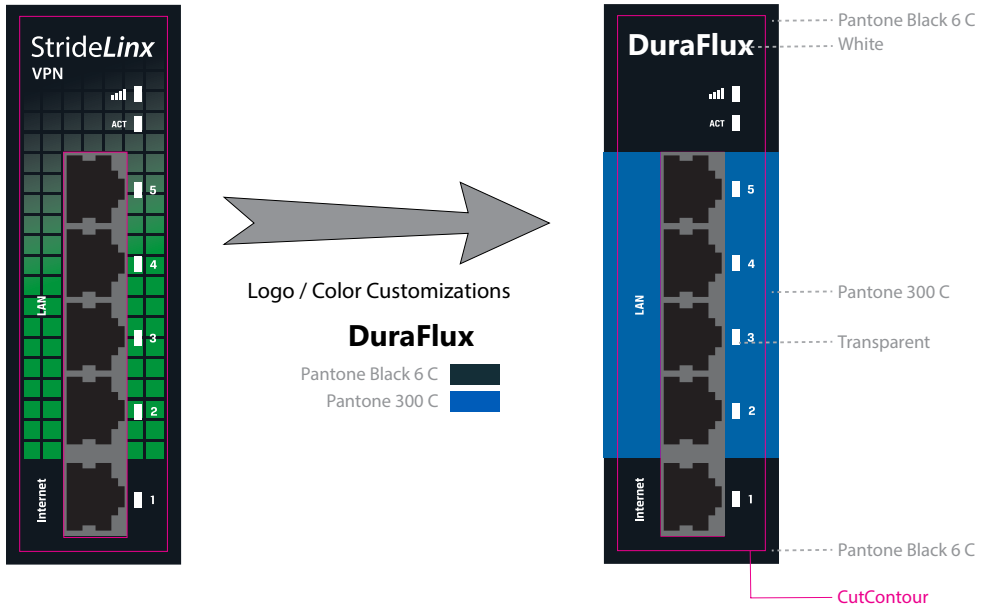
With the StrideLinX Professional license you can make changes to the company branding by selecting **Identity** from the **Admin menu**, then selecting the branding entity to customize.

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, .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

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

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

[Online Help](#)

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)

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.