

CLOUD NOTIFY



In this Chapter...

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

5

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

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

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

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

Cloud Notify



NOTE: Model SE-SL3001 does not support notifications.

Why Cloud Notify?

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

How Does the Cloud Notify License Work?

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

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

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



Configure Cloud Notify On Your Device

Cloud Notify setup requires:

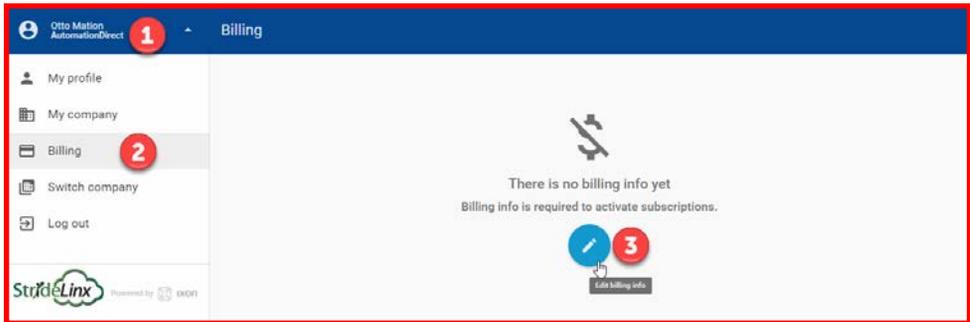
1. Set up Cloud Notify license.
2. Set up alarms for specific data variables in your connected equipment.
3. Select the priority level of alarm notifications to be sent to each user.

Each of these steps are detailed in this chapter.

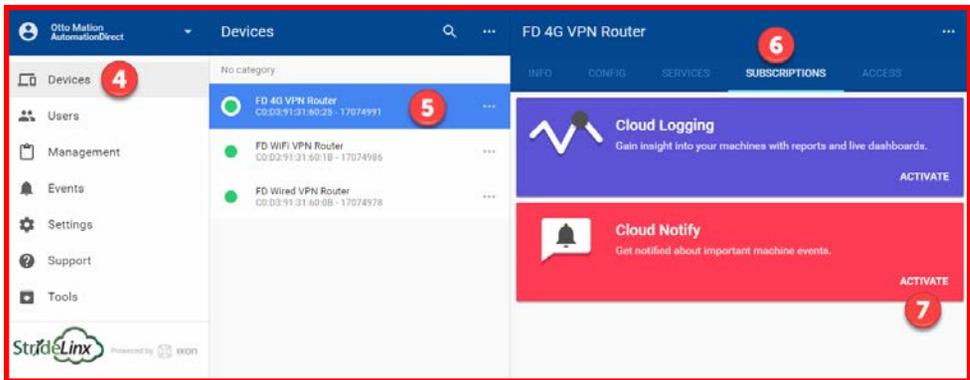
Set Up Cloud Notify License

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

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



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



Set Up Data Sources For Alarm Notifications

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

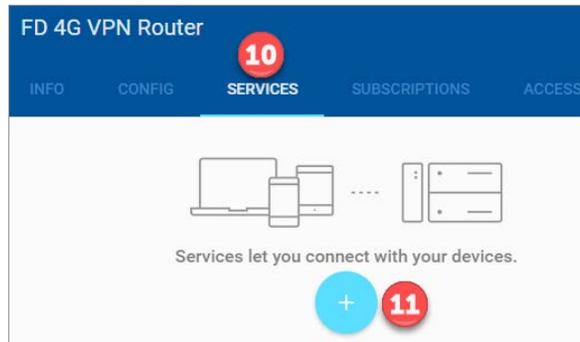


NOTE: This chapter uses Modbus protocol to illustrate data source configuration. Refer to Appendix G, H, I, J and K for Siemens S7, OPC UA, EtherNet/IP, BACnet, and MELSEC protocols, respectively.

5

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

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



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

×
Add service

🏠
FD 4G VPN Router

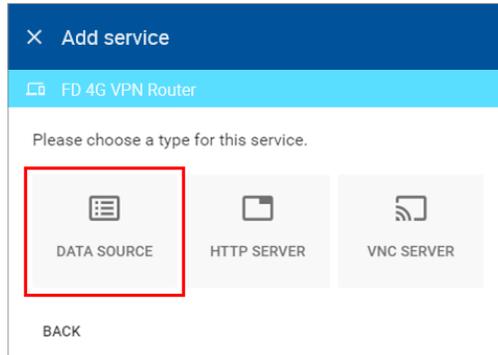
Please specify a target for this service.

Name

IP address
e.g. 192.168.140.100

NEXT

Select DATA SOURCE.

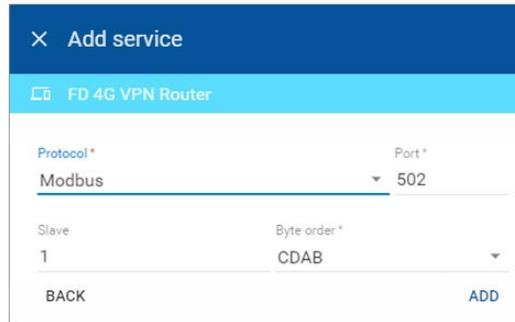


5

×

 Add service

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

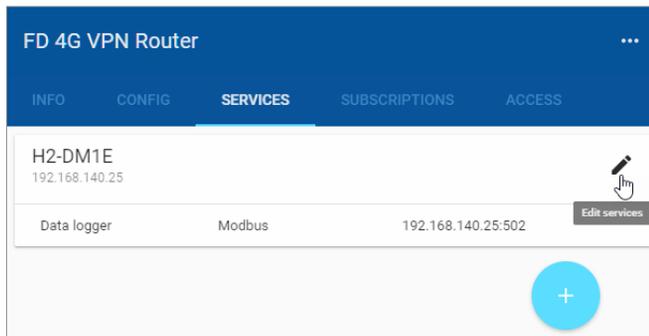


×

 Add service

Configure the data tags

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



FD 4G VPN Router

INFO CONFIG SERVICES SUBSCRIPTIONS ACCESS

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

+

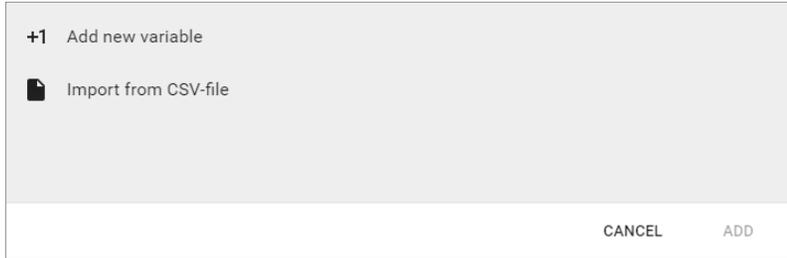
This opens the Edit services dialog. Click the name of the existing device for which you would like to add a data tag.



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

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

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



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

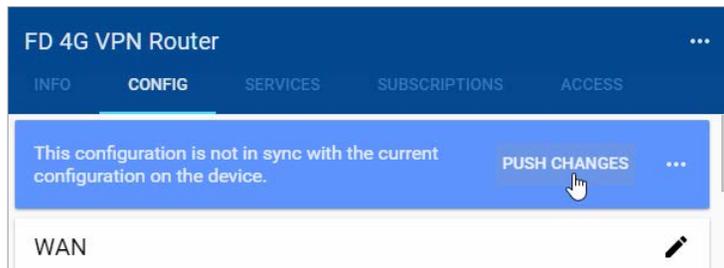
Data tag input fields are described in the following two tables. Also see the Modbus address translation chart in [Appendix D](#) for the key to enter addresses for AutomationDirect products. Refer to Appendix G, H, I, J and K for details on setting up Siemens S7, OPC UA, EtherNet/IP, BACnet and MELSEC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

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

5

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

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



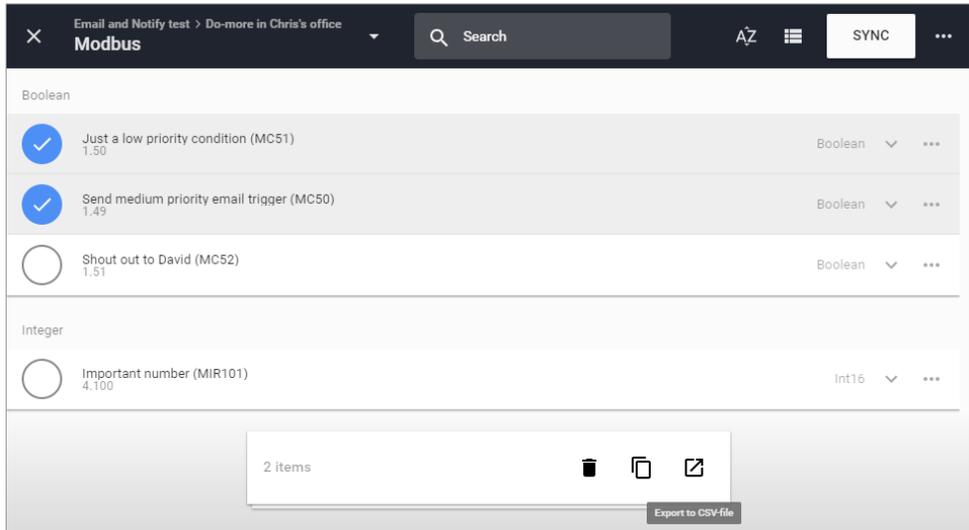
The Cloud Notify web app can now be used to set up alarm notifications using these data tags.

Export data tags

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

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

5



Router Conditions for Alarm Notifications

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

The conditions available to initiate a notification are:

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

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

Formatting the Alarm Notification Email

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

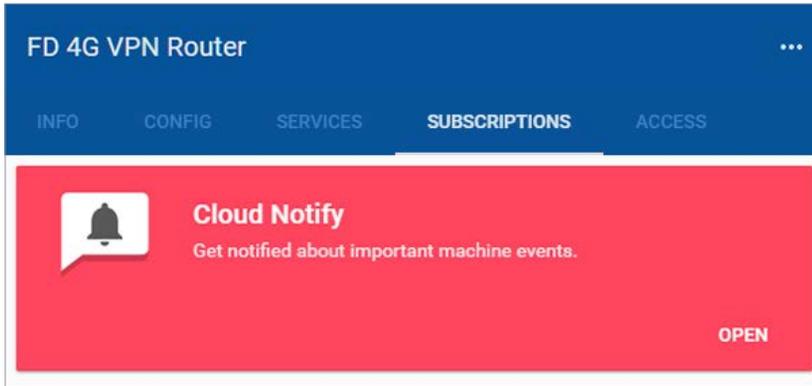
The image shows two screenshots from a user interface. The top screenshot is the 'My profile' page for 'Otto Mation AutomationDirect'. It has a left sidebar with options: My profile, My company, Billing, Licences, Switch company, and Log out. The main content area shows 'My info' (Full name: Otto Mation,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

The bottom screenshot is the 'Edit localization' dialog for 'Otto Mation'. It has three dropdown menus: 'Select a language' (English), 'Select a localization' (Automatically), and 'Select a timezone' (Automatically). Red circles highlight the 'Automatically' options in the localization and timezone dropdowns. Red arrows point from these circles to the corresponding lists in the right-hand panels. The right-hand panels show two scrollable lists: the top one contains time zones like '(GMT-05:00) Central Time (US & Canada)', '(GMT-05:00) Bogota', '(GMT-05:00) Lima', '(GMT-05:00) Quito', and '(GMT-04:00) Eastern Time (US & Canada)'; the bottom one contains languages like 'English (United States)', 'English (Zimbabwe)', 'Afrikaans', 'Bahasa Indonesia', and 'Bahasa Melayu (Malaysia)'. At the bottom of the dialog are 'CANCEL' and 'CONFIRM' buttons.

Cloud Notify Web App

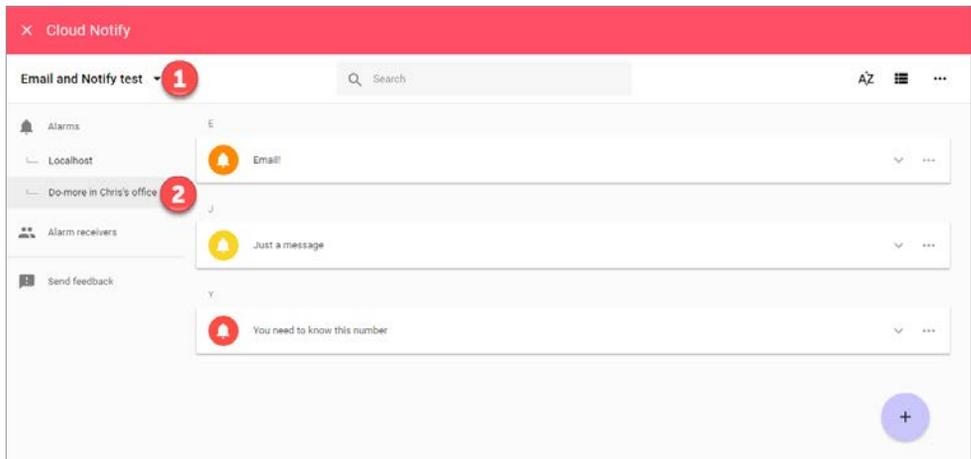
The Cloud Notify web app is found under the SUBSCRIPTIONS tab after selecting a StrideLinx device. Note that model SE-SL3001 does not support notifications.

5



Main Screen

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

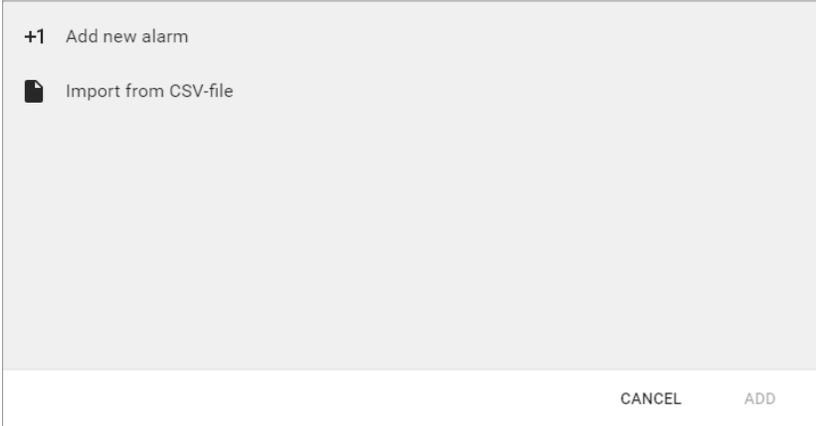


Click the downward chevron to the right of an alarm to display its details, or click the three dots to copy, delete, or select the alarm for export.

Adding Alarms

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

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

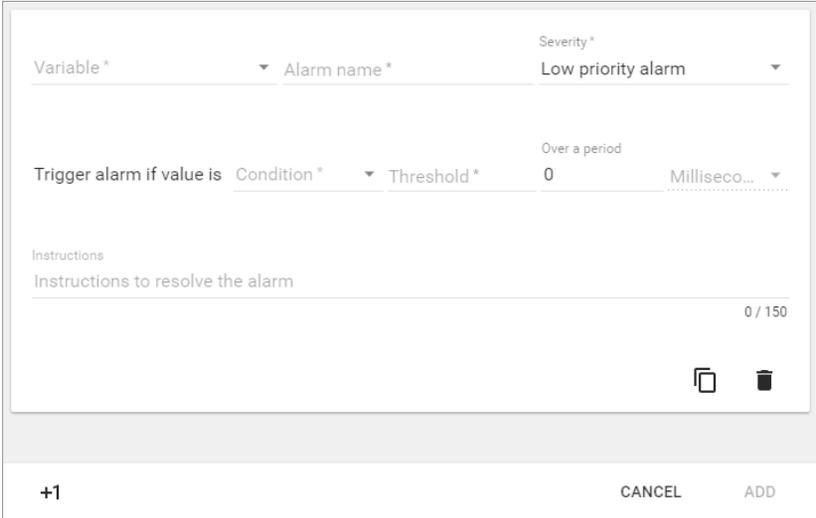


+1 Add new alarm

Import from CSV-file

CANCEL ADD

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



Variable * Alarm name * Severity *
 Low priority alarm

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

Instructions
 Instructions to resolve the alarm 0 / 150

+1 CANCEL ADD

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

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

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

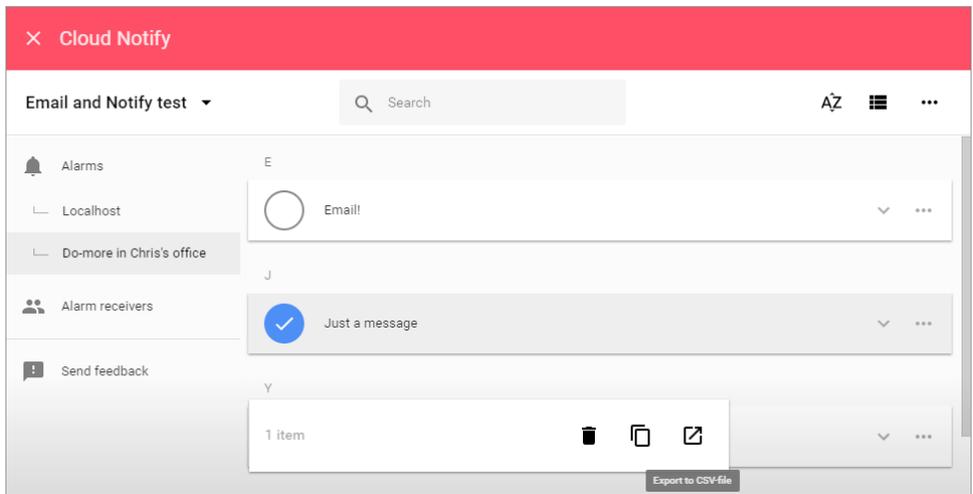
Localhost Data Source	
<i>Variable</i>	<i>Description</i>
MQTT connected	Router is online and connected to the cloud server
MQTT logger connected	Data logging and/or cloud notify from the router to the cloud server is active
VPN connected)	Router is connected via VPN to the cloud server

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

Export Alarm Configurations

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

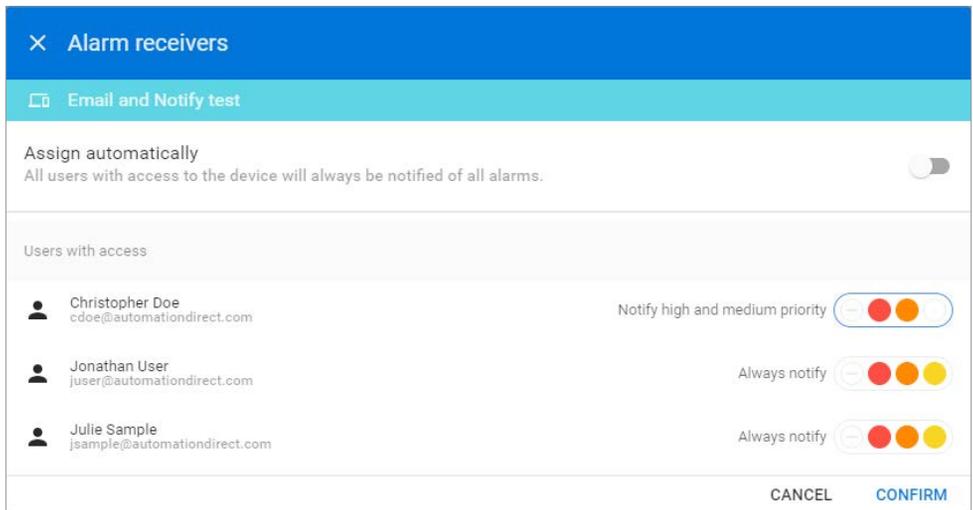
Select alarms to be exported by clicking the icon for each alarm, or select all alarms at once from the More Options (•••) menu in the upper right corner of the web app. The selected alarms can then be deleted, duplicated, or exported from the pop up menu at the bottom of the screen.



5

Managing Alarm Recipients

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



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

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

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

What Happens When an Alarm is Triggered?

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



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

5

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

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

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

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

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

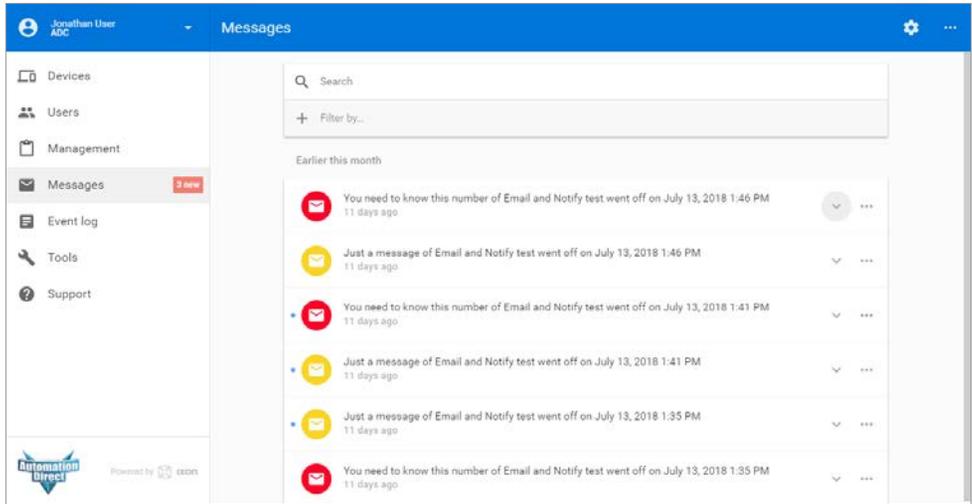
At the bottom, it says "Powered by ixon".

Message Center

Message Archive

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

Messages are stored on the StrideLinX platform for six months.



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

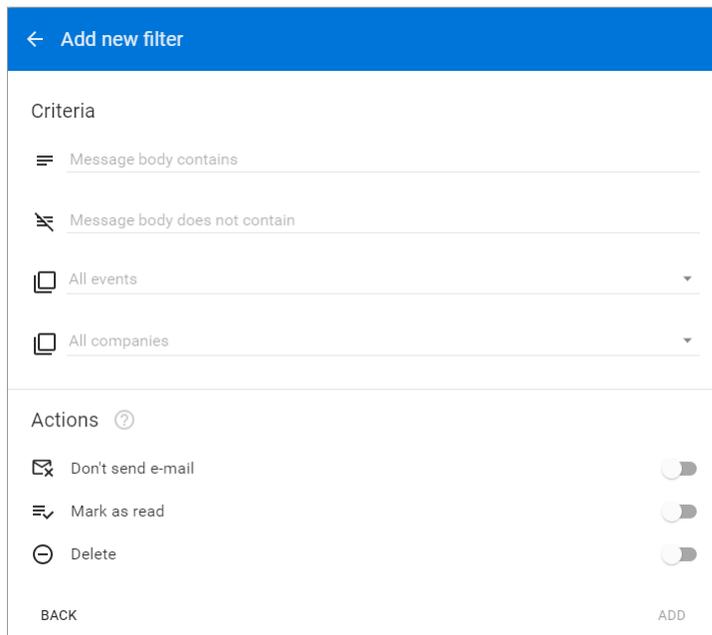
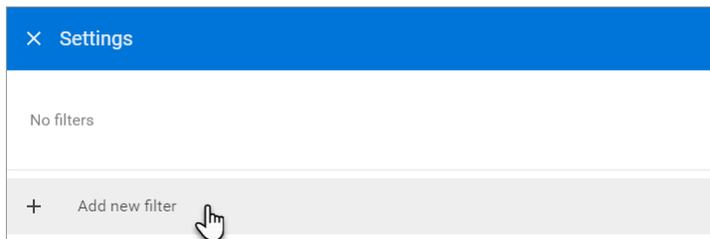
	You need to know this number of Email and Notify test went off on July 13, 2018 1:46 PM 11 days ago	 
Received on	07/13/2018 1:46:29 PM	
Message	Instructions: This number has lasted more than a second!	
Device ID	FkPFSYqoaW07	
Device name	Email and Notify test	
Company	ADC	
Event	High priority alarm	

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

Message Filtering

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

5



Criteria

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

Actions

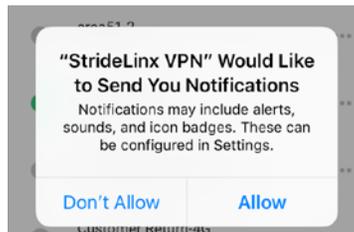
- **Don't send e-mail** – Allows a user to receive the alarm in the Message Center without receiving e-mails.
- **Don't send push notification** – Allows a user to receive the alarm in the Message Center without receiving push notifications to a mobile device.
- **Mark as read** – Mark matching messages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

Configuring Your Mobile Device to Receive Push Notifications

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

Push Notification on iOS

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



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

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

Push Notification on Android

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

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

View the List of Configured Push Devices on the StrideLinx Platform

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

