

Edge Intelligence Tunnel Manager Reference Manual

2024 April 11
Revision: 1.1.0.16

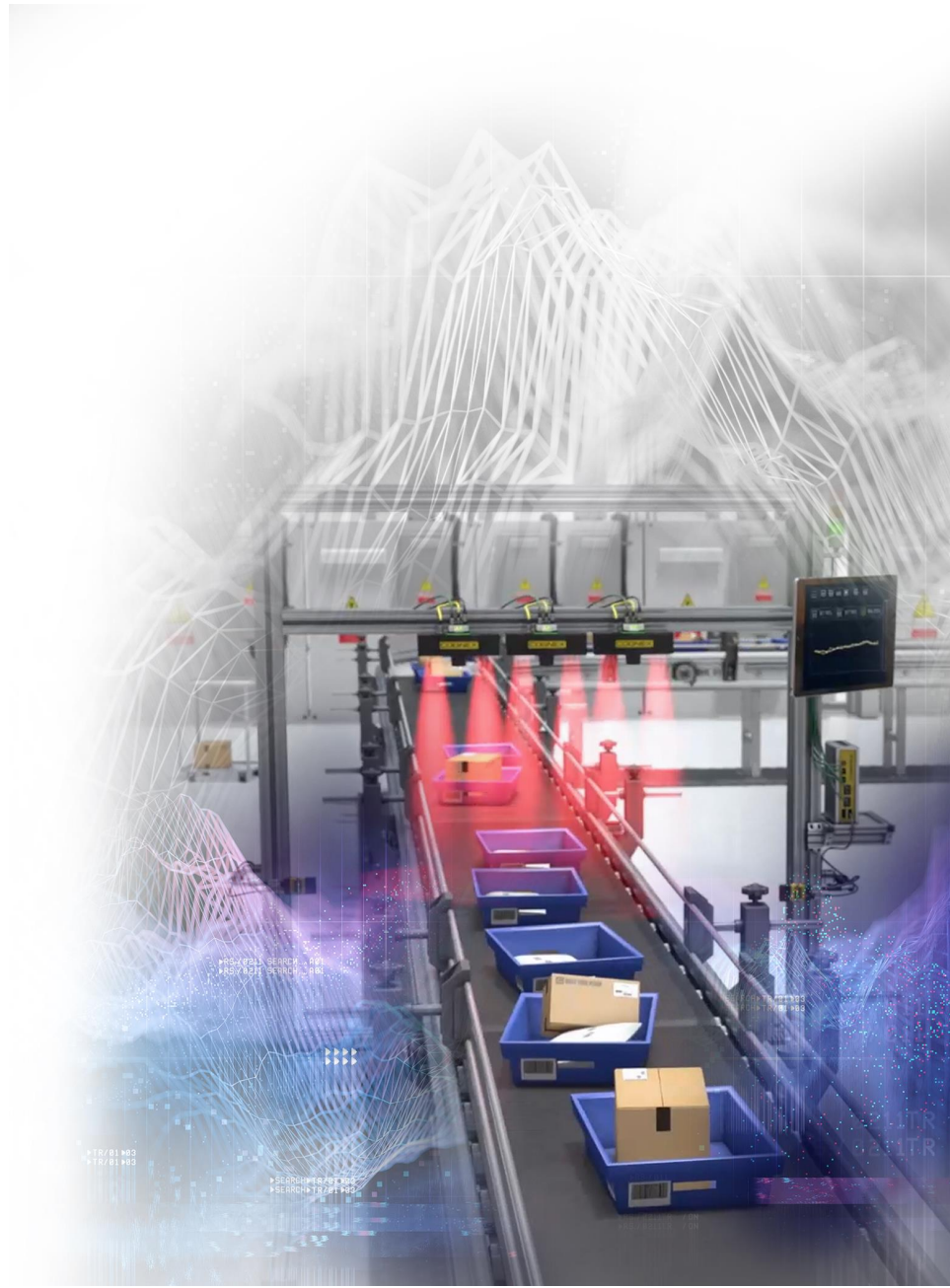


Table of Contents

Table of Contents	2
Legal Notices	4
Precautions	5
Symbols	6
Getting started	7
About Edge Intelligence Tunnel Manager	7
Edge Intelligence Tunnel Manager Features	8
Default User Credentials	9
Installation	10
Discovering Devices on the Network	10
Discover Devices	10
Network Settings	10
Remote Connection Troubleshooting	10
EI Tunnel Manager User Interface	12
Tunnel Analytics	12
Performance Dashboard	12
Edit the Dashboard	13
Live Dashboard	15
Result Browser	16
Filter Query	19
Multi Read Filter Query	21
Real Time Monitoring (RTM)	22
Configuration Change History	22
Configuration Changes	24
Provisioning	27
DataMan	27
Device Actions	28
Provisioning Devices	28
Provision Device by IP	29
Data Collection Settings	29
Remote Subnets	30
Multi-Reader Configuration (MRC)	31
DataMan	31
Individual Device Actions	32
Device Group Actions	32
DataMan WebHMI	34
Feature Keys	39
EI Tunnel Manager Setup Apps	41
Dynamic Test	41

3D Field Calibration	47
Archiver	52
Download Center	52
Extract a Single Archive File	54
Extract a Multi-Archive File	55
Settings	56
Edge Device	56
Setting up the NAT	58
NTP Server Function	59
MQTT Forwarding	59
MQTT Connection Parameters	62
SSL/TLS	62
Sparkplug Settings	63
AWS IOT Settings	63
DataMan WebHMI	64
Firmware Upgrade	65
User Management	66
Users	66
Roles	68
Single Sign-On	69
Identity Provider Configuration	69
Role Mapping	69
Certificates	71
Cloud Forwarding	72
Connections	73
Connection Manager	75
Licensing	76
Update	76
Main Elements of the User Interface	77
Notification Center	80
Notification Center Features	82
Notification Levels	85
Notification List	85
Cleaning and Maintenance	89
Open Source Licenses	90

Legal Notices

The software described in this document is furnished under license, and may be used or copied only in accordance with the terms of such license and with the inclusion of the copyright notice shown on this page. Neither the software, this document, nor any copies thereof may be provided to, or otherwise made available to, anyone other than the licensee. Title to, and ownership of, this software remains with Cognex Corporation or its licensor. Cognex Corporation assumes no responsibility for the use or reliability of its software on equipment that is not supplied by Cognex Corporation. Cognex Corporation makes no warranties, either express or implied, regarding the described software, its merchantability, non-infringement or its fitness for any particular purpose.

The information in this document is subject to change without notice and should not be construed as a commitment by Cognex Corporation. Cognex Corporation is not responsible for any errors that may be present in either this document or the associated software.

Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, nor transferred to any other media or language without the written permission of Cognex Corporation.

Copyright © 2023. Cognex Corporation. All Rights Reserved.

Portions of the hardware and software provided by Cognex may be covered by one or more U.S. and foreign patents, as well as pending U.S. and foreign patents listed on the Cognex web site at: cognex.com/patents.

The following are registered trademarks of Cognex Corporation:

Cognex, 2DMAX, Advantage, AlignPlus, Assemblyplus, Check it with Checker, Checker, Cognex Vision for Industry, Cognex VSOC, CVL, DataMan, DisplayInspect, DVT, EasyBuilder, Hotbars, IDMax, In-Sight, Laser Killer, MVS-8000, OmniView, PatFind, PatFlex, PatInspect, PatMax, PatQuick, SensorView, SmartView, SmartAdvisor, SmartLearn, UltraLight, Vision Solutions, VisionPro, VisionView

The following are trademarks of Cognex Corporation:

The Cognex logo, 1DMax, 3D-Locate, 3DMax, BGAll, CheckPoint, Cognex VSoC, CVC-1000, FFD, iLearn, In-Sight (design insignia with cross-hairs), In-Sight 2000, InspectEdge, Inspection Designer, MVS, NotchMax, OCRMax, PatMax RedLine, ProofRead, SmartSync, ProfilePlus, SmartDisplay, SmartSystem, SMD4, VisiFlex, Xpand

Portions copyright © Microsoft Corporation. All rights reserved.

Portions copyright © MadCap Software, Inc. All rights reserved.

Other product and company trademarks identified herein are the trademarks of their respective owners.


Precautions


To reduce the risk of injury or equipment damage, observe the following precautions when you install the Cognex product:


- This product is intended for industrial use in automated manufacturing or similar applications.
- The safety of any system incorporating this product is the responsibility of the assembler of the system.
- Do not install Cognex products where they are exposed to environmental hazards such as excessive heat, dust, moisture, humidity, impact, vibration, corrosive substances, flammable substances, or static electricity.
- Route cables and wires away from high-current wiring or high-voltage power sources to reduce the risk of damage or malfunction from the following causes: over-voltage, line noise, electrostatic discharge (ESD), power surges, or other irregularities in the power supply.
- This product does not contain user-serviceable parts. Do not make electrical or mechanical modifications to product components. Unauthorized modifications can void your warranty.
- Changes or modifications not expressly approved by the party responsible for regulatory compliance could void the user's authority to operate the equipment.
- Include service loops with cable connections.
- Ensure that the cable bend radius begins at least six inches from the connector. Cable shielding can be degraded or cables can be damaged or wear out faster if a service loop or bend radius is tighter than 10X the cable diameter.
- This device should be used in accordance with the instructions in this manual.
- All specifications are for reference purposes only and can change without notice.


Symbols

The following symbols indicate safety precautions and supplemental information:

 **WARNING:** This symbol indicates a hazard that could cause death, serious personal injury or electrical shock.

 **CAUTION:** This symbol indicates a hazard that could result in property damage.

 **Note:** This symbol indicates additional information about a subject.

 **Tip:** This symbol indicates suggestions and shortcuts that might not otherwise be apparent.

Getting started

About Edge Intelligence Tunnel Manager

El Tunnel Manager is a performance monitoring tool that collects and analyzes data generated by Cognex tunnel standards. El Tunnel Manager provides reader statistics, no read images, trigger details, and configuration changes for all connected devices.

The El Tunnel Manager software consists of a browser-based user interface that allows you to access to the El Tunnel Manager functions and provides the following features through the UI:

- **Tunnel Analytics**
 - Performance Dashboard
 - Live Dashboard
 - Result Browser
- **RTM**
 - Configuration Change History
- **Provisioning**
 - DataMan
 - Remote Subnets
- **Multi-Reader Configuration**
 - DataMan
 - Feature Keys
- **Tunnel Setup**
 - Tunnel Commissioning
 - Dynamic Test
 - 3D Field Calibration
- **Archiver**
 - Download Center
- **Settings**
 - Edge Device
 - MQTT Forwarding
 - DataMan WebHMI
 - Firmware Upgrade
- **User Management**
 - Users
 - Roles

- **Single Sign-On**
 - Identity Provider Configuration
 - Role Mapping
 - Certificates
- **Cloud Forwarding**
 - Connections
 - Connection Manager
- **Notification Center**
- **Licensing**
 - Update

Edge Intelligence Tunnel Manager Features

ET Tunnel Manager collects tunnel data and tracks reader configuration changes in real time, monitors performance, and provides data analysis to help identify root causes and facilitate quick action. The entire functionality of ET Tunnel Manager is accessible from a browser. ET Tunnel Manager has an intuitive user interface, no coding knowledge is required to use.

Main Features	Key elements
Device Management	Large storage for multi-day images/results
	Network, NAT
	Time Synchronization
Compatibility with DataMan Readers	Configurations, Firmware, Feature Keys
	Multi-Reader Sync group setup
	DataMan WebHMI to configure readers
Flexible and scalable solution: Integration with Industrial Analytics	Device results, and metadata
	Built-in MQTT/Sparkplug protocol (Ignition, Cloud providers) and analytics
Powerful Performance Monitoring tools	Real time performance with live dashboard
	Custom performance dashboards
	View and automatic categorization of Good Reads, No Reads, and Failed Validations
	Real time Device Configuration changes

Default User Credentials

The following predefined users are available by default:

User	Password	Default Permissions
admin	BnthWWSD	Has access to all apps and features.
engineer	TaRDpKVx	Has access to all apps and features.
operator	SxtXGmxs	User with read-only rights. The operator does not have access to the Multi-Reader Configuration app and the Settings.

Note: After creating the user profiles, changing the default password of each user profile is necessary to avoid security risks.

Note: Admin users can enable access permissions for other user roles.

Installation

This section describes the installation process.

Discovering Devices on the Network

The default IP address for the Internal Ethernet port of EI Tunnel Manager is set to 192.168.1.100. All devices on the network are discovered automatically, regardless of the network settings. However, discovered devices are labeled as misconfigured if they are not in the local subnet.

Discover Devices

Upon successfully logging in, the web UI launches, and EI Tunnel Manager auto-discovers the devices on your network, which appear listed on your home screen.

Click on the **Discover Devices** button in the header of the web interface to force a rediscovery if you have connected a new device after the initial auto-discovery.

Note:

If you need to change your EI Tunnel Manager's network settings, open the menu and go to the Settings > Edge Device. From there, you can set the network settings.



Network Configuration

Device Name

Network Interface: eth3

Enable DHCP

IP Address

Subnet Mask

Gateway

DNS Server

Network Settings

It is recommended that all Cognex devices be on the same network as EI Tunnel Manager. In order to make this happen, change the IP address of all readers on the network to be in the same network as 192.168.1.xxx, or change the IP address of the Ethernet port to match those of the readers.



Note: The devices found on the network are listed on the first page of the Multi-reader Configuration Application.

Home > Multi-Reader Configuration > DataMan

Add selected to group Upload configuration Upload firmware Download as CSV Discover devices

Test

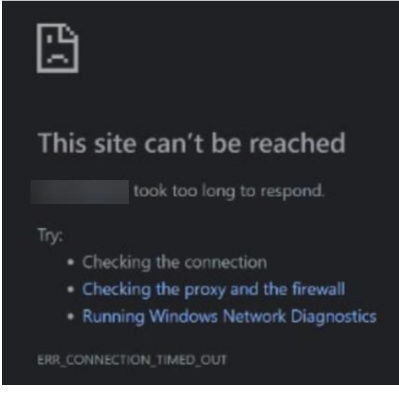
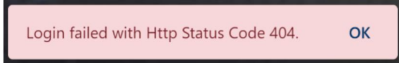
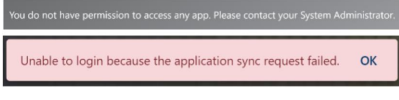

Actions	Primary	Name	Type	MAC Address	Firmware Version	Address Type	IP Address	Subnet Mask	Gateway	Source Network Interface	State	Task Status
<input checked="" type="checkbox"/>						Static					In Local Subnet	
<input type="checkbox"/>						DHCP					In Local Subnet	

Standalone Devices

Actions	Primary	Name	Type	MAC Address	Firmware Version	Address Type	IP Address	Subnet Mask	Gateway	Source Network Interface	State	Task Status
<input type="checkbox"/>						Static					In Local Subnet	
<input type="checkbox"/>						Static					In Local Subnet	

Remote Connection Troubleshooting

This section lists the most common errors and their solutions.

Error	Illustration	Solution
EI Tunnel Manager is not visible in the Setup Tool or in the browser		Check wire connectons, secure them if necessary.
Failed login error message		Check the credentials and re-enter username and/or password.
Component load error message		Reboot device and wait for services to start.
No data/images available		Check reader availability and setup.

Note: An Ethernet connection to your network is recommended, as Wi-Fi may not allow the connection depending on your network settings.

Note: The IP address of your device is listed on the login page.



About EI-DemoUnit

Documentation

[Click here to open documentation.](#)

Network Interfaces

Name	Operational	MAC Address	Address Type	IP Address	Subnet Mask	Gateway	DNS Server	Domain
	✓		DHCP					(none)
	✓		DHCP					(none)
	✓		Static					(none)

EI Tunnel Manager User Interface

The EI Tunnel Manager user interface provides the following applications:

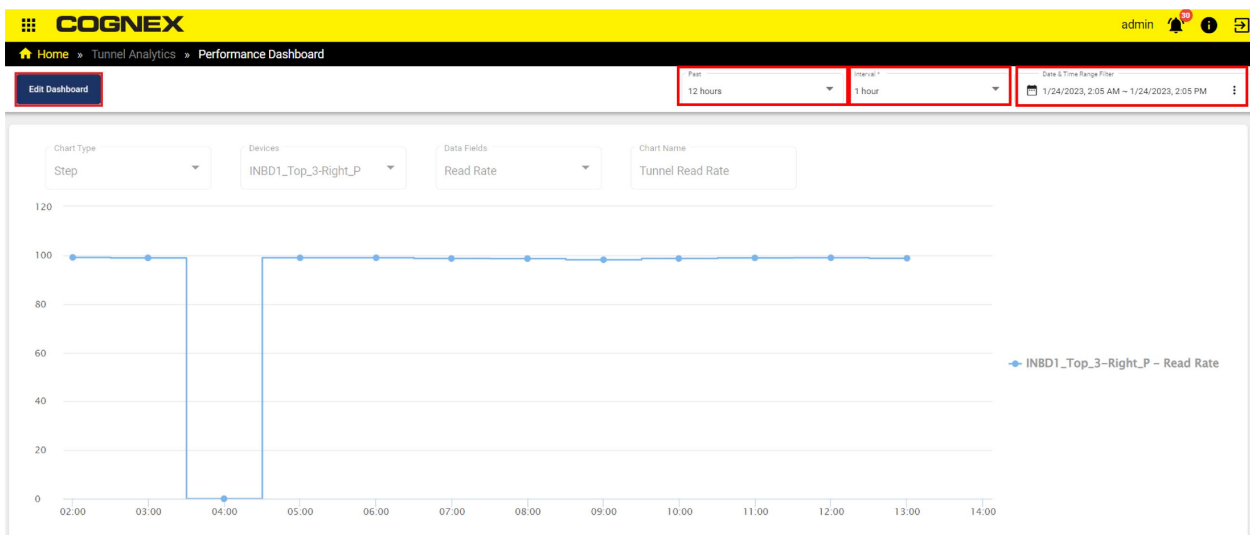
- Provisioning
- Real Time Monitoring (RTM)
- Tunnel Analytics
- Multi-Reader Configuration (MRC)
- User Management
- Settings
- Archiver
- Cloud Forwarding

Tunnel Analytics

The **Tunnel Analytics** application of the EI Tunnel Manager user interface provides additional analytics options over the Performance Monitoring page in the RTM application.

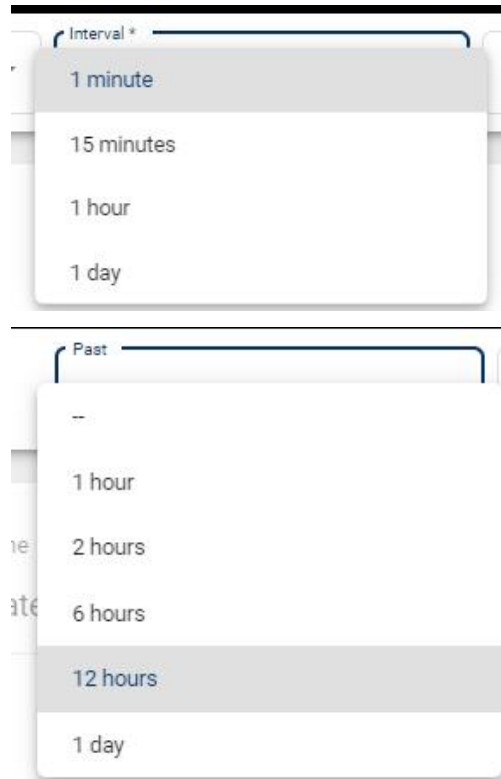
Performance Dashboard

The **Performance Dashboard** page of the Tunnel Analytics application provides a configurable set of saved charts that visualize the performance data of connected devices.



Setting a value you want for **Past**, **Interval***, **Date & Time Range Filter** fields helps you to see the visualization of the performance data for that specific time interval and date.

You can adjust the data point granularity using **Interval***.



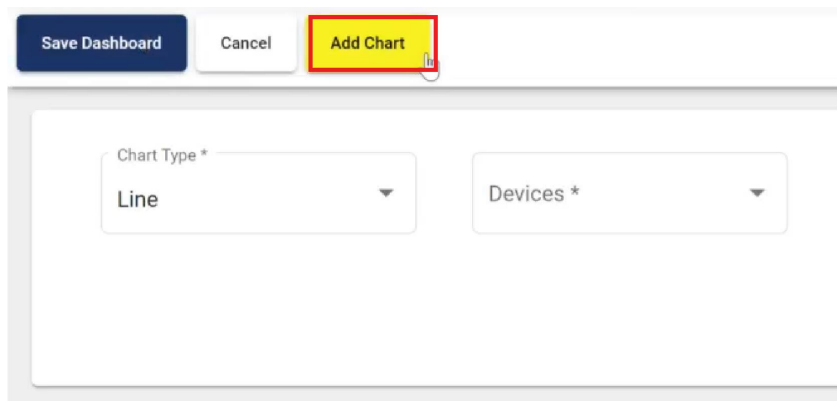
To look at a smaller time intervals, choose a smaller value for **Interval***.

For example, to see a data point for every hour in the past one day, set **Past** to *1 day*, **Interval*** to *1 hour*.

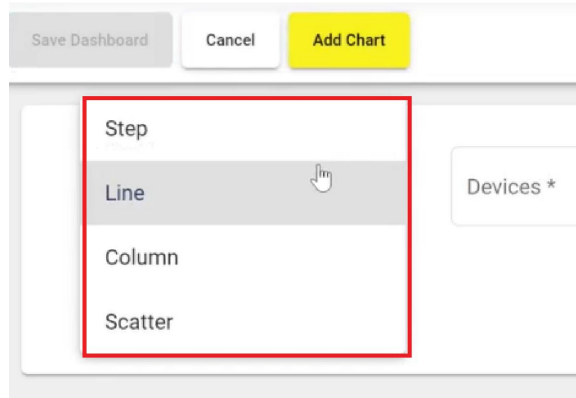
Edit the Dashboard

The **Edit Dashboard** function allows you to add, edit, delete, and sort charts.

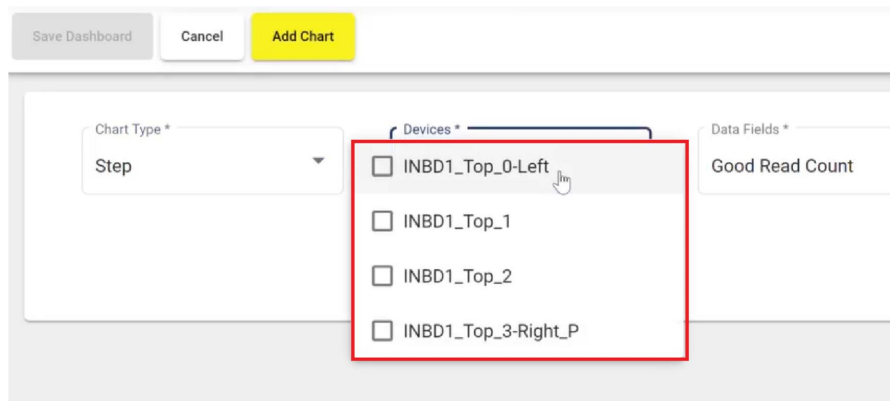
1. Click **Add Chart**.



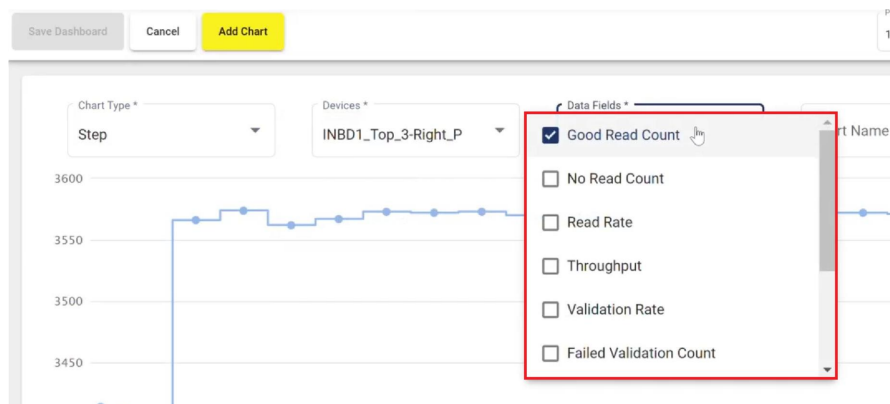
2. Select the chart type from the dropdown list.



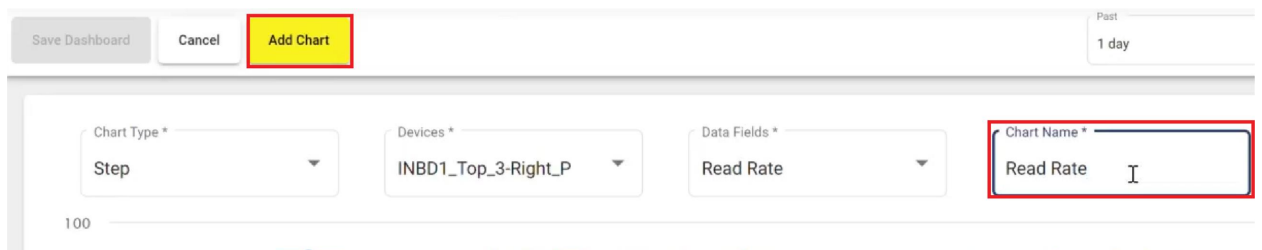
3. Select the device type from the dropdown list.



4. Select the data field type from the dropdown list.

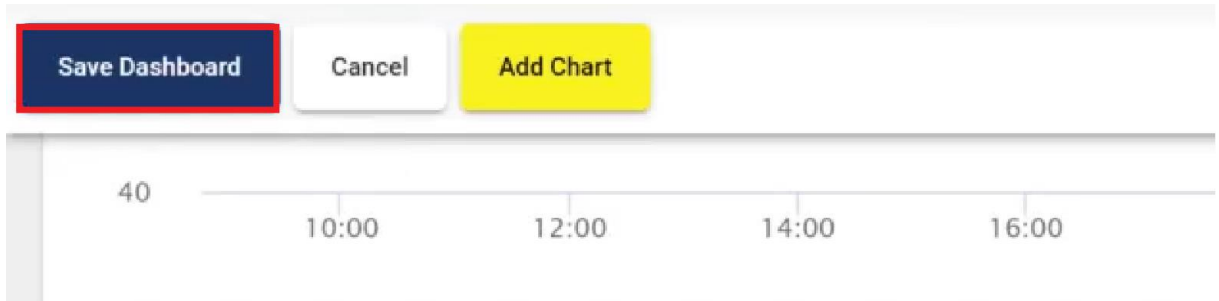


5. Name the new chart. Click **Add Chart**.



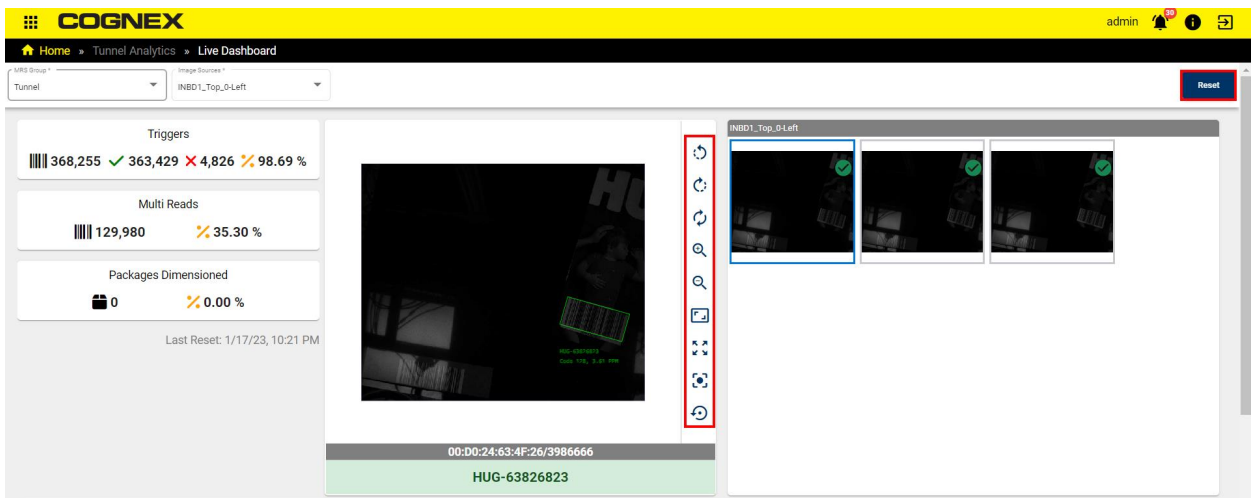
- Repeat the procedure to add more charts to the Dashboard. You can sort, edit, and delete the charts from the Dashboard.

Click **Save Dashboard** when you are done.



Live Dashboard

The **Live Dashboard** page of the Tunnel Analytics application allows you to configure the live dashboard and the triggers that visualize the performance data of connected devices.



Using the buttons on the right side of the live view, you can manipulate the image on the live feed.







To reset the live dashboard, click on **Reset** on the top right corner.

You can choose the image sources you want to work with on the top left corner under the **Image Sources*** field.

Note: **Image Sources*** corresponds to readers.



In the bottom of the **Live Dashboard** page you can find saved triggers that are available to download.

Download	Timestamp	Result	Trigger Index	Read String	Length (mm)	Width (mm)	Height (mm)	Object Gap (mm)
	2:47:29 PM	✓	3,987,528	HUG-10984288	873	768	905	2,381
	2:47:27 PM	✓	3,987,527	61109233810; BLU-95...	847	818	949	7,474
	2:47:25 PM	✓	3,987,526	COL-54801863; 74091...	901	761	947	740
	2:47:24 PM	✓	3,987,525	PUR-159455; 0971128...	1,056	854	934	1,462
	2:47:22 PM	✓	3,987,524	ARI-87748001; 99973...	839	760	918	7,484
	2:47:22 PM	✓	3,987,523	HILIC-46483632	800	767	926	2,783

Pause
Items per page: 10
1 - 10 of 300

You can also pause the saving of live triggers by clicking on **Pause**.

Set the number of items you want to see on each page in the **Items per page** field.

Result Browser

The **Result Browser** page of the Tunnel Analytics application allows you to filter the results that Cognex devices collect and to find the data that is the most important to you.

The screenshot shows the Cognex Result Browser interface. At the top, there is a navigation bar with the Cognex logo and user information. Below this, a breadcrumb trail indicates the current location: Home > Tunnel Analytics > Result Browser. The interface features a sidebar on the left with a list of tunnel names: INBD1_Top_0-Left, INBD1_Top_1, INBD1_Top_2, and INBD1_Top_3-Right_P. The main area contains a table of trigger data with columns for Timestamp, Result, Trigger Index, Read String, Length (mm), Width (mm), and Height (mm). Above the table, there are filter fields for Trigger Index, Result Type, Read String, and Date & Time Range Filter. A 'More Filters' button and a 'Download All' button are also present. At the bottom right, there is a pagination control showing 'Items per page: 10' and '1 - 10 of 34457'.

To download all triggers, click on **Download All**.

To filter out the data, you can use default filter fields, such as **Trigger Index**, **Result Type**, **Read String**, and **Date & Time Range Filter**.

The **Trigger Index** means that the El Tunnel Manager assigns an index number to every trigger as an identifier. You can search for multiple triggers by typing in the index numbers of those triggers. You can search for:

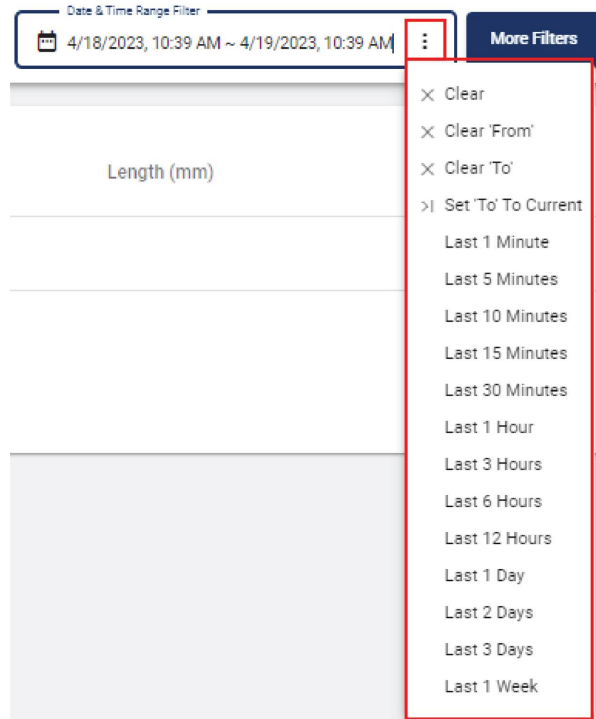
- Simple index number, for example 1010.
- Several index numbers separated them by pressing **ENTER**, for example, 1010, 1013, 1014.
- Range of index numbers using a hyphen, for example 1010-1016. You can also add another range by pressing **ENTER** and add the new value.

The **Result Type** is the classification of the trigger. The result type can be the following:

- Good Read: the EI Tunnel Manager successfully decoded the correct codes.
- No Read: the EI Tunnel Manager did not read any codes, or read the wrong codes.
- Failed Validation: the EI Tunnel Manager read an invalid code because the code is improperly formatted, or does not meet specific requirements.

The **Read String** is the string the EI Tunnel Manager reads.

The **Date & Time Range Filter** has quick relative time options. Use the options to set the range. Use the **clear** functions to delete all or a part of the range.



You can find more filter options by clicking on **More Filters** on the top right corner of the page:

Filters

Trigger Information ^

Multi Read True False

Trigger Index
e.g. 101 or 105-107 or >101 or <107 or >=101

Result Type ▼

Decode Results ▼

Dimensioner Results ▼

Scale Results ▼

Sorter Information ▼

To use more filters, click on the **down arrow** next to the name of a filter group.

Decode Results

Read String

Symbology Name ▼

Assignment Result ▼

Assigned Surface ▼

Dimensioner Results

Legal For Trade True False

Angle

e.g. 101 or 105-107 or >101 or <107 or >=101

Length

e.g. 101 or 105-107 or >101 or <107 or >=101

Width

e.g. 101 or 105-107 or >101 or <107 or >=101

Height

e.g. 101 or 105-107 or >101 or <107 or >=101

Object Gap

e.g. 101 or 105-107 or >101 or <107 or >=101

Side By Side True False

Scale Results

Legal For Trade True False

Weight

e.g. 101 or 105-107 or >101 or <107 or >=101

Sorter Information

Vendor Token

Filter Query

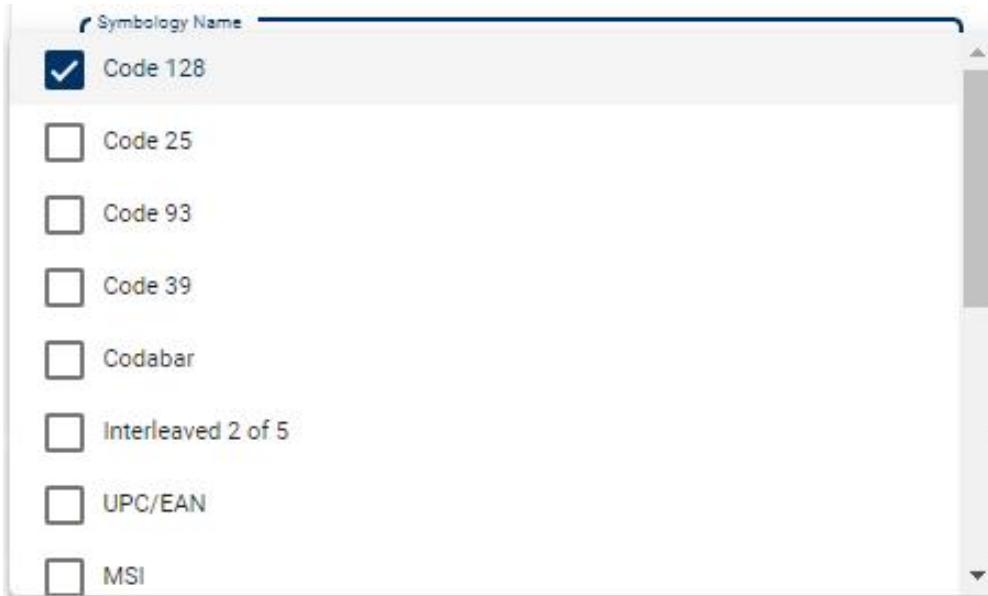
You can create a filter query by entering input into the filter fields. When you add an input into one of the fields, you create a search condition that limits your trigger results to those that meet the set condition.

For boolean values, you can set the value to:

- True: Search for results where this condition is true.
- False: Search for results where this condition is false.
- Neither: Do not filter the results by this field.

For fields that can have multiple string values, use the dropdown to select one or more values.

If you select a value, you are searching for results that match that value. For example, you can search for any results that contain a Code 128 code:



If you select more than one value, you are searching for results that match either of those values. For example, you can search for results that contain a Code 128 code, *OR* an I2of5, *OR* a UPC/EAN code:







Use the input fields for data that have a numerical value. The numerical input field supports the following input formats:

Condition	Example
Single value	Packages that have a reported length of 533 (length = 533).

Less than condition	Packages that have a reported length less than 533 (length < 533).
Less than or equal to	Packages that have a reported length that is less than or equal to 533 (length <= 533).
Greater than condition	Packages that have a reported length greater than 533 (length > 533).
Greater than or equal to	Packages that have a reported length that is greater than or equal to 533 (length >= 533).
Range	Packages that have a reported length between 500 and 550 (500 <= length <= 550).

You can add multiple inputs of the various format listed above. To add an additional input, press **ENTER** and begin typing the next input. Each input appears with a remove icon next to it. To remove any of the inputs, click on the remove icon next to the input you want to remove.

Height





100-150  <80  >=500  -1  Press ENTER to add new value...

e.g. 101 or 105-107 or >101 or <107 or >=101

Note: Any input field that has a text input field, or a dropdown that allows you to enter, or select multiple values are joined together with an *OR* function. This means that the results appear if any of the criteria meets any of the provided inputs.

For example, you can type in the following four inputs into the height filter field. This search filters the results by packages that have a reported height between 100 and 150, *OR* a height less than 80, *OR* a height greater than or equal to 500, *OR* a height that is -1.

Height

100-150  <80  >=500  -1  Press ENTER to add new value...

e.g. 101 or 105-107 or >101 or <107 or >=101

Multi Read Filter Query

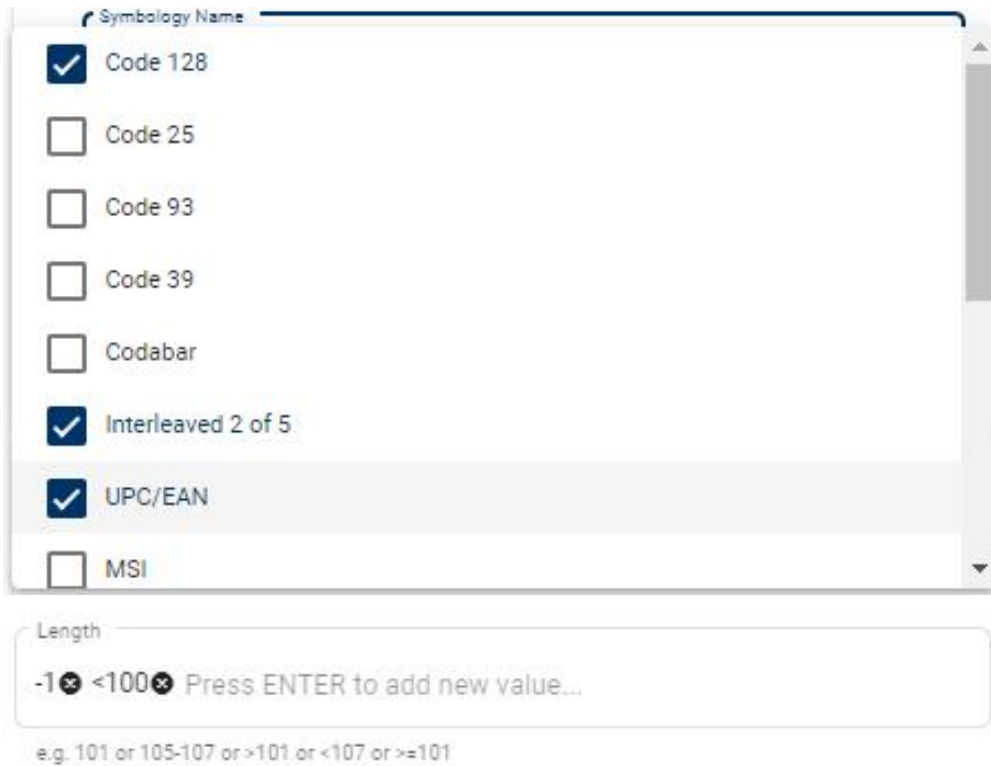
When you enter input to more than one of the filter fields, you create multi-conditional queries. The conditions from different filter fields are evaluated with an *AND* function.

For example, if you select True for the Multi Read filter, and add the following values:

- Code 128
- Interleaved 2 of 5
- UPC/EAN
- -1 and <100 values for the length filter

Then you created the following filter query:

Multi Read = TRUE AND (Symbology Name = Code 128 OR Symbology Name = Interleaved 2 of 5 OR Symbology Name = UPC/EAN) AND (Length = -1 OR Length < 100)



This means the filter shows results that are tagged as multi-reads *AND* contain a code that is either a code 128 *OR* Interleaved 2 of 5, *OR* UPC/EAN *AND* the reported length of the package is either -1 *OR* less than 100.

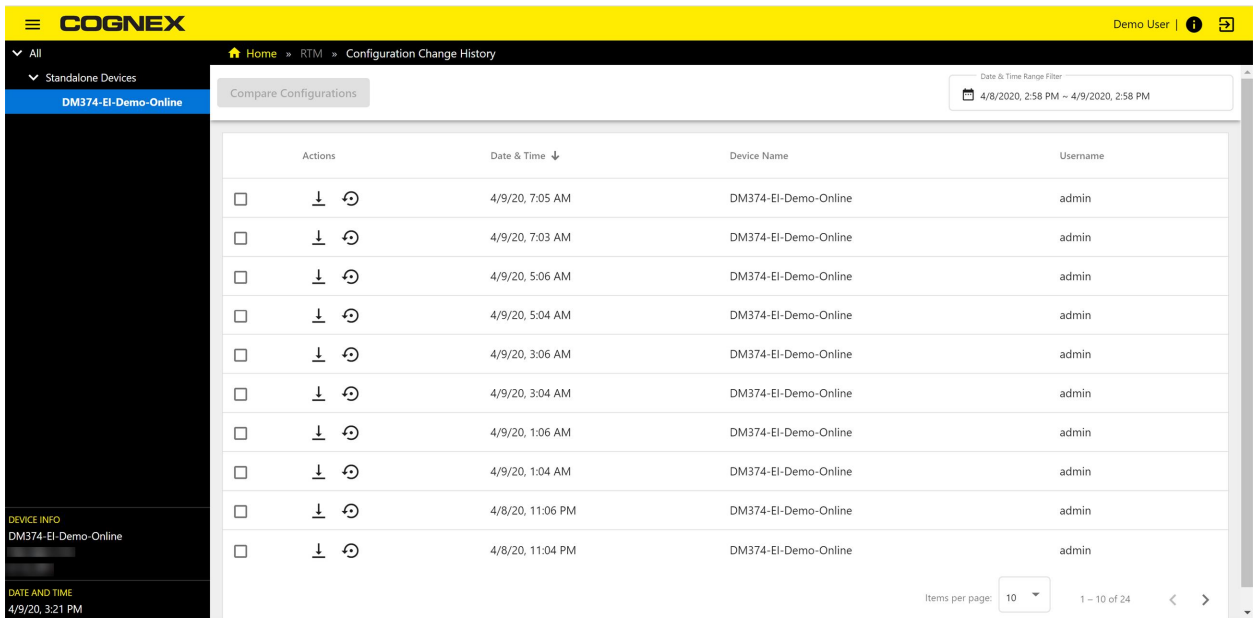
Real Time Monitoring (RTM)

Real Time Monitoring (RTM) is a software application that collects configuration change events from readers on the network and records that data into a configuration change history for each device.




- Configuration Change History - lists past configuration for a given group or reader, allows the user to compare configurations in a time frame

Configuration Change History

The Configuration Change History page tracks changes made to the configuration of all connected readers and shows changes in a customized fashion. The window displays the Device tree with available grouped and standalone readers. The page automatically links configurations with the respective usernames.

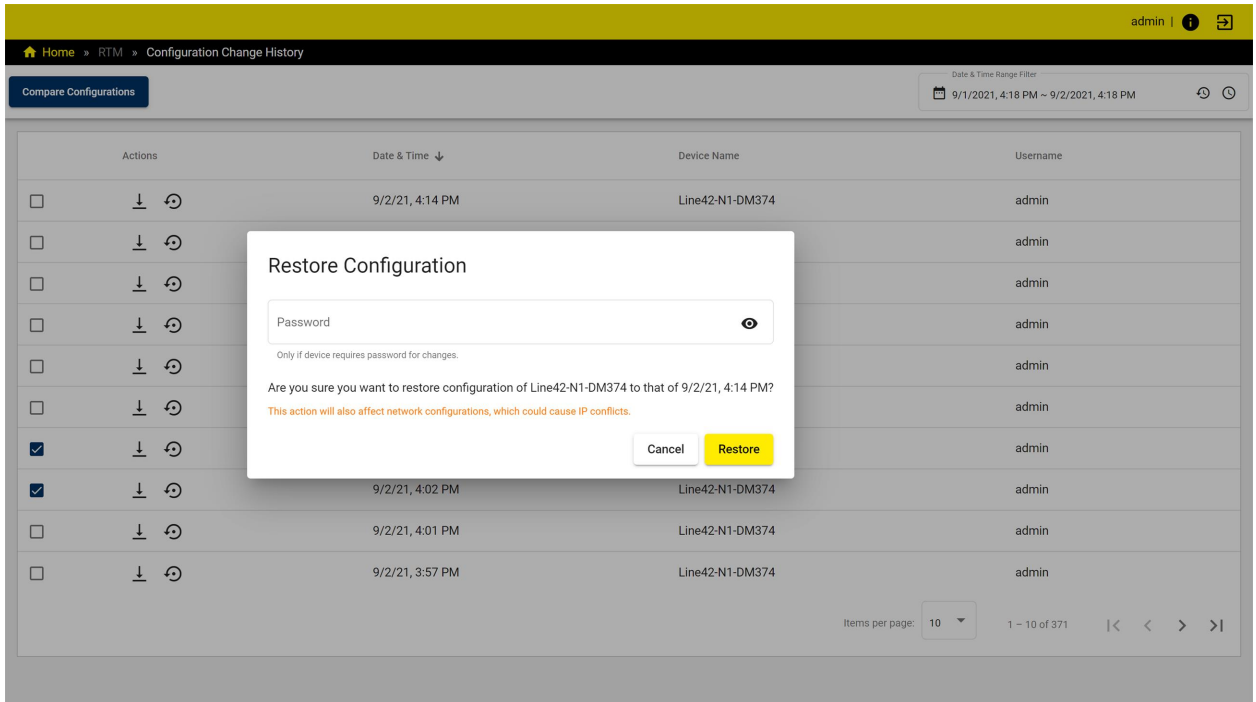


Configuration Change Actions

Icon	Action
	Selected checkbox
	Download Configuration File
	Restore Configuration

- Click the **checkbox** from the list in the left side of the rows to select a configuration.
- Click the **Download Configuration File** to download the selected Configuration files.

- Click **Restore Configuration** to revert to a previous configuration.
 - After clicking **Restore Configuration** enter your password and click **Restore** to revert configuration. Click **Cancel** to leave the popup window without restoring the selected configuration.



Dashboard overview:

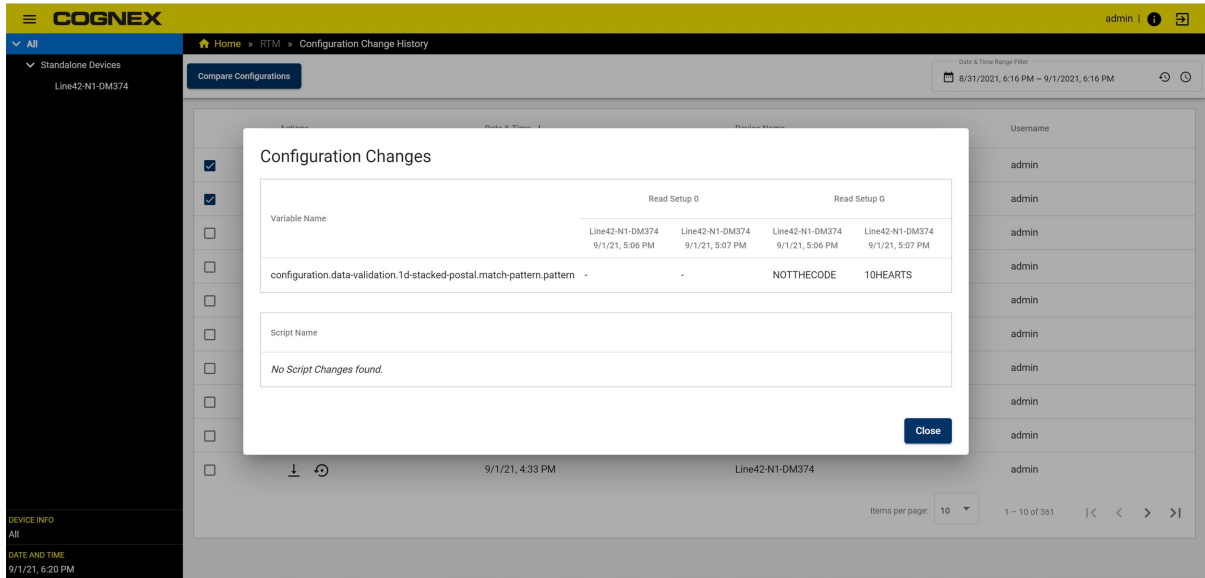
Item	Description
Compare Configurations button	Select 2 checkbox to enable the button. Click the button to see configuration changes in a pop-up window. For more information see
Date & Time Range Filter	Use the time range to define a period of time from which performance data is collected for the charts. For more information see Date & Time Range Filter on page 1
Configuration tables	List of readers and groups available for comparison.

Note: Changes made from Dataman Setup Tool are labeled as admin changes.

Column Name	Description	Display
Date and time	Date and time of the configuration change.	3/3/20, 9:10 AM
Device name	Name of the reader on the network.	
Username	Name and type of the user who made the configuration change.	

Configuration Changes

To compare two configurations, select the readers to compare. Click on the Compare Configurations button. A pop up window appears with a table containing the comparison results.



Item	Description
Configuration Changes	Lists variables which have different values in the compared versions
Variable Name	Name of the variable which has different values in the compared versions
Script Name	Name of the recently modified script
Read Setup	Name of the read setup

Variable changes:

Configuration Changes

Read Setup 0		
Variable Name		
	DM374-EI-Demo-Online 4/9/20, 7:03 AM	DM374-EI-Demo-Online 4/9/20, 7:05 AM
configuration.imager.gain-factor	15.00	5.00

Script Name
<i>No Script Changes found.</i>

Close

Column Name	Description
Variable Name	List of variables that have different values in the compared configuration versions
Read Setups	Display the name of the readers compared, and the difference in values pertaining to the row of the configuration scripts

Script changes:

Configuration Changes

Variable Name
No Variable Changes found.

Script Name	DM474-628156 4/15/20, 1:02 PM	DM474-628156 4/15/20, 2:08 PM
communication.script	<pre>// Comms script that triggers the reader twice/second var timerHandler = null; var trigger_delay = 0.5; // trigger twice/second function CommHandler() { return { onConnect: function (peerName) { // Disable the handler for this connection: if (peerName.indexOf("COM") >= 0) { timerHandler = this; timerHandler.setTimer(trigger_delay); return true; } return false; }, onDisconnect: function () {}, onError: function (errorMsg) {}}, onExpectedData: function (inputString) { return true; }, onUnexpectedData: function (inputString) { return true; }, onTimer: function () { dmccCommand("TRIGGER", "ON"); if (timerHandler != null) timerHandler.setTimer(trigger_delay); }, onEncoder: function () {} }; }</pre>	<pre>// Comms script that triggers the reader twice/second function CommHandler() { return { onConnect: function (peerName) { // Disable the handler for this connection: return false; }, onDisconnect: function () {}, onError: function (errorMsg) {}, onExpectedData: function (inputString) { return true; }, onUnexpectedData: function (inputString) { return true; }, onTimer: function () {}, onEncoder: function () {} }; }</pre>
format.script	<pre>// Default script for data formatting function onResult (decodeResults, readerProperties, output) { if (decodeResults[0].decoded) { output.content = decodeResults[0].content; }</pre>	<pre>// Default script for data formatting function onResult (decodeResults, readerProperties, output) { if (decodeResults[0].decoded) { output.content = decodeResults[0].content; } else { output.content = "Not able to decode candidates"; }</pre>

Close

Column Name	Description
Variable Name	List of variables that have different values in the compared configuration versions
Read Setups	Display the name of the readers compared, and the difference in values pertaining to the row of the configuration scripts

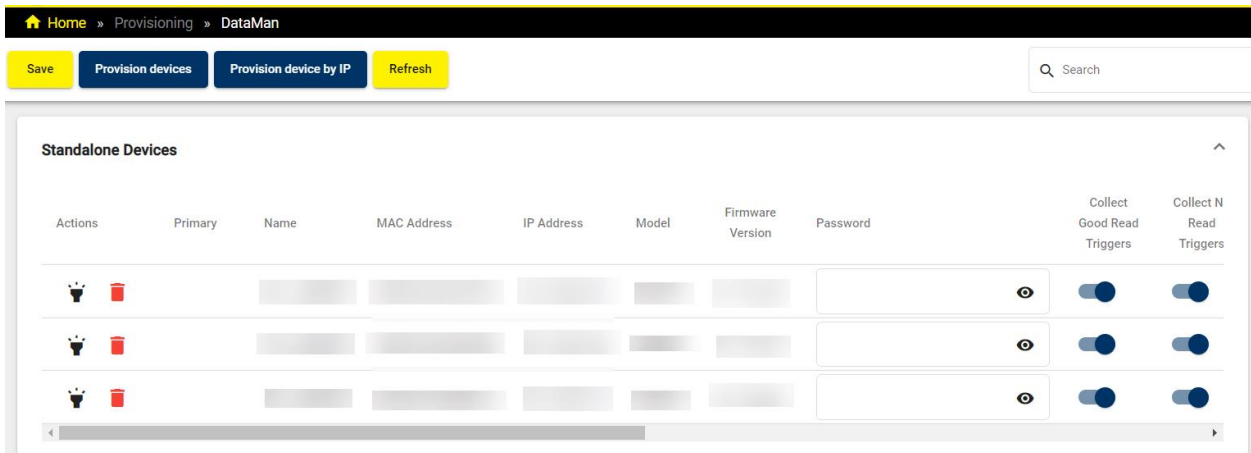
Provisioning

The Provisioning application of the EI Tunnel Manager user interface allows you to provision your connected devices and device groups, configure what data to collect from your devices, and manage your remote subnets.

DataMan

The DataMan page of the Provisioning application provides a list of standalone devices, as well as device groups, and allows you configure what data you want to collect from each of your devices. You can also provision one or more of your devices at the same time, or individually by IP address.

The DataMan page:



To refresh the list of connected devices, click **Refresh** in the header.

To provision devices, click **Provision devices** and use the pop-up dialog to select the devices. To provision a device by IP address, click **Provision device by IP** and enter the device IP address.

Click **Save** to apply any changes you make to device data collection settings.

Device Actions

You can perform actions on an individual device by clicking on the icons in the **Actions** column of the row for the selected device:

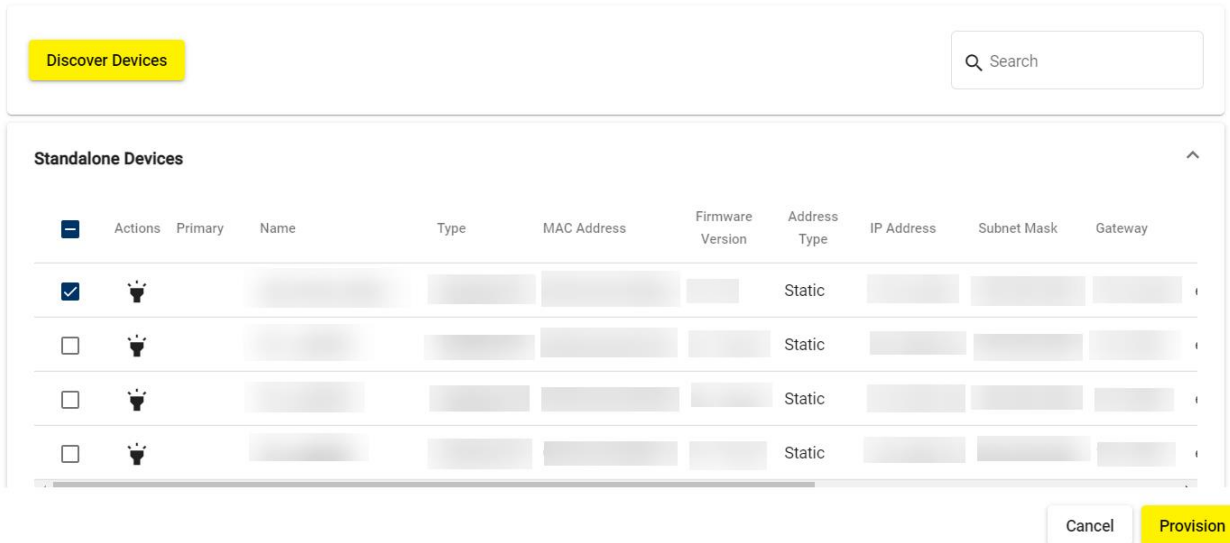
Actions	
Icon	Action
	Flash LED
	Delete

- Click the **Flash LED** button to remotely trigger the LED of the device for easy identification.
- Click the **Delete** button to remove the device from the list.

Provisioning Devices

Click on **Provision devices** in the header to open the **Provision devices** pop-up dialog:

Provision devices



The **Provision devices** dialog provides a list of connected devices. To provision one or more devices, check the checkbox for the selected devices, and click **Provision**.

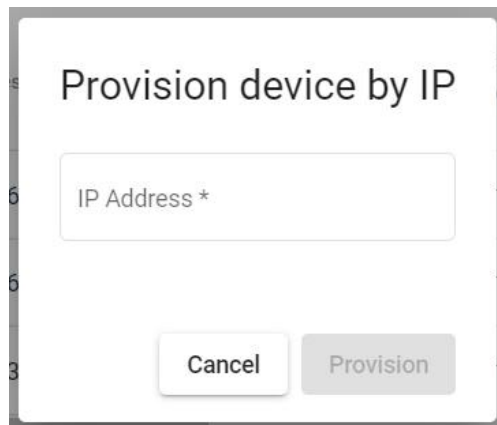
To flash the LED on a device for easier identification, click the **Flash LED** icon in the **Action** column of the row for the selected device.

To refresh the list of connected devices, click **Discover Devices**.

To search for a specific device in the list, enter the name or IP address in the **Search** bar.

Provision Device by IP

Click on **Provision device by IP** in the header to open the **Provision device by IP** pop-up dialog:



Enter the IP address of the selected device, and click **Provision**.

Data Collection Settings

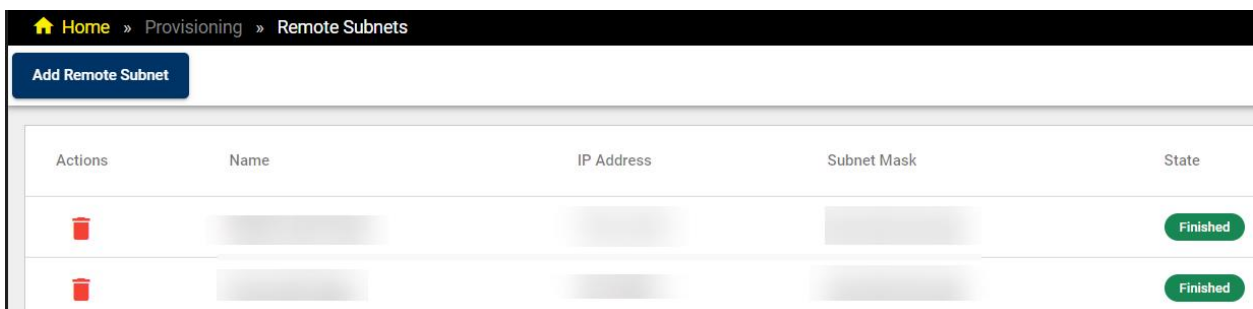
You can modify collection settings for different types of device data by switching the toggles on or off in each data collection column of the row for the selected device:

Column	Description																																								
<table border="1"> <thead> <tr> <th>Password</th> <th>Collect Good Read Triggers</th> <th>Collect No Read Triggers</th> <th>Collect Validation Failure Triggers</th> <th>Collect Good Read Images</th> <th>Collect No Read Images</th> <th>Collect Validation Failure Images</th> <th>Collect Device Configuration Changes</th> <th>Collect Statistics</th> <th>Collect Tunnel Trigger Result</th> </tr> </thead> <tbody> <tr> <td><input type="password"/></td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td><input type="password"/></td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td><input type="password"/></td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Password	Collect Good Read Triggers	Collect No Read Triggers	Collect Validation Failure Triggers	Collect Good Read Images	Collect No Read Images	Collect Validation Failure Images	Collect Device Configuration Changes	Collect Statistics	Collect Tunnel Trigger Result	<input type="password"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="password"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="password"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>Provide the password for the device to make any changes.</p> <p>Enable this setting to collect good read trigger data from the device.</p> <p>Enable this setting to collect no read trigger data from the device.</p> <p>Enable this setting to collect validation failure trigger data from the device.</p> <p>Enable this setting to collect good read image data from the device.</p> <p>Note: When you enable good read image data collection, the device image format is set to 1/4 size JPEG.</p> <p>Enable this setting to collect no read image data from the device.</p> <p>Enable this setting to collect validation failure image data from the device.</p> <p>Enable this setting to collect device configuration change data from the device.</p> <p>Enable this setting to collect statistics from the device.</p> <p>Enable this setting to collect tunnel trigger results from the device.</p>
Password	Collect Good Read Triggers	Collect No Read Triggers	Collect Validation Failure Triggers	Collect Good Read Images	Collect No Read Images	Collect Validation Failure Images	Collect Device Configuration Changes	Collect Statistics	Collect Tunnel Trigger Result																																
<input type="password"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																
<input type="password"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																
<input type="password"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																

To order the list of devices by type of data collection enabled, click on a data collection column header.

Remote Subnets

The Remote Subnets page of the Provisioning application provides a list of remote subnets, and allows you to add additional subnets.



To remove a remote subnet from the list, click on the **Bin** icon in the **Actions** column of the row for the selected subnet.

Click on **Add Remote Subnet** to open the **Add Remote Subnet** pop-up dialog:

Enter the name, IP address, and subnet mask for the remote subnet you want to add, and then click **Add**.

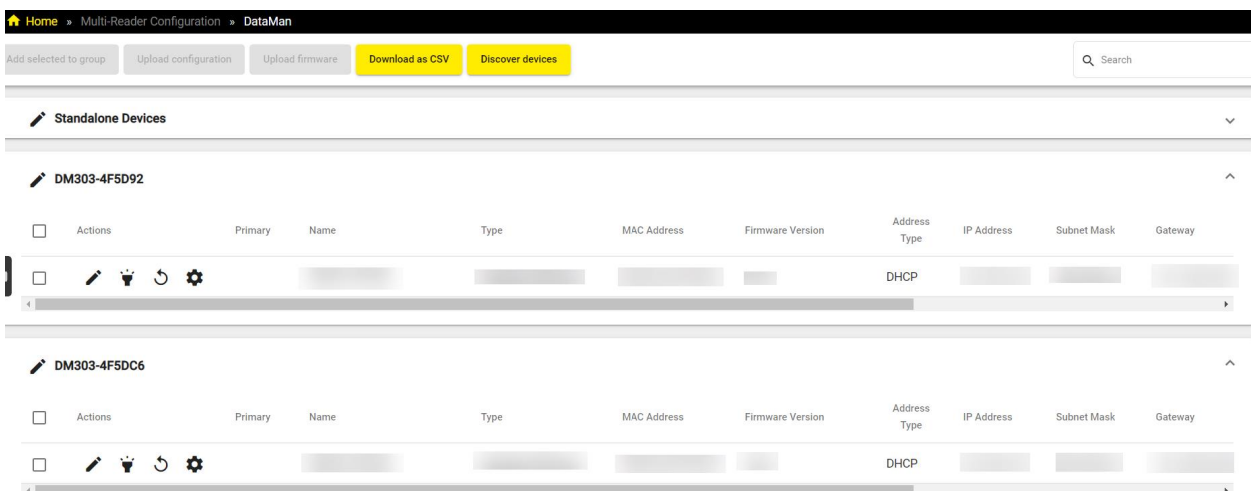
Multi-Reader Configuration (MRC)

The Multi-Reader Configuration application of the EI Tunnel Manager user interface provides a list of standalone devices and device groups, shows device information, and allows you to modify settings on individual devices as well as multiple devices simultaneously. You can also save entire tables of device configuration data to your local machine.

DataMan

The DataMan page of the Multi-Reader Configuration application provides a list of standalone devices, as well as device groups, including device data. You can edit the configuration, flash the LED, reboot, or access the DataMan WebHMI of individual devices from the DataMan page. You can perform mass configuration or firmware updates for device groups.

The DataMan page:











To refresh the list of connected devices, click **Discover devices** in the header.

To save the device information for the connected devices in CSV format, click **Download as CSV** in the header .

Individual Device Actions

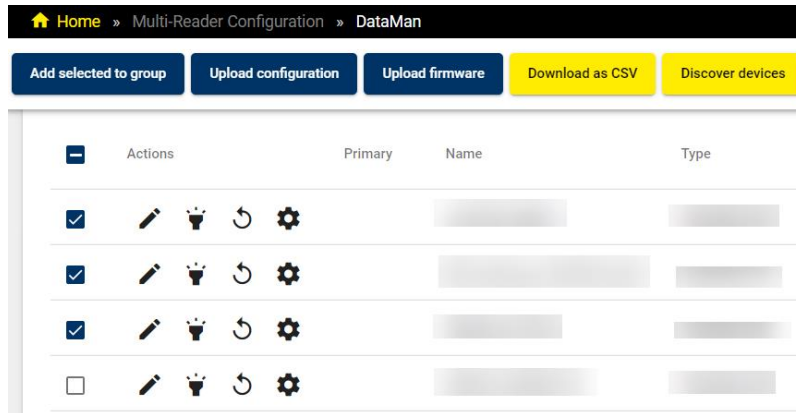
You can perform actions on an individual device by clicking on the icons in the **Actions** column of the row for the selected device:

Actions	
   	
Icon	Action
	Single Device Edit
	Flash LED
	Reboot
	Open DataMan WebHMI

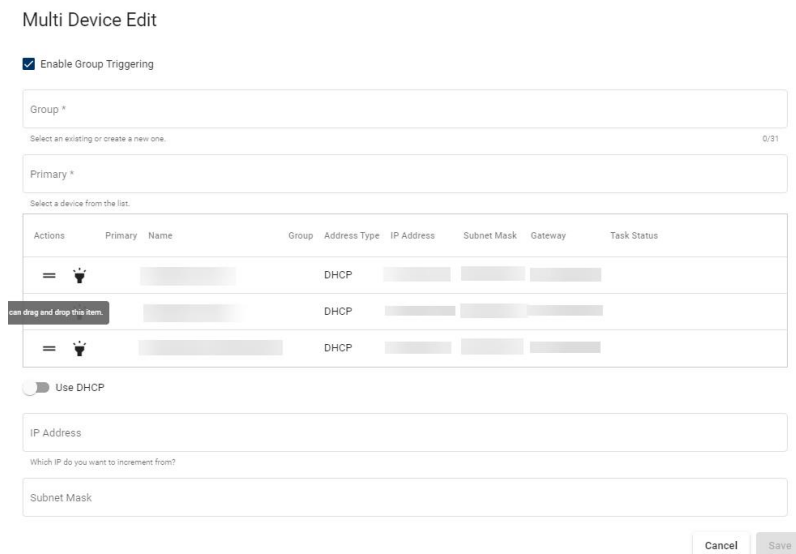
- Click the **Single Device Edit** button to modify the name, IP address, Subnet Mask, and Default Gateway of the device. Enter the device password if required.
- Click the **Flash LED** button to remotely trigger the LED of the device for easy identification.
- Click the **Reboot** button to initiate a reboot on the device.
- Click the **Open DataMan WebHMI** button to open the DataMan WebHMI in a new tab. For more information on the DataMan WebHMI, see [DataMan WebHMI on page 34](#).

Device Group Actions

To perform group actions, check the checkbox of the selected devices, enabling the group action buttons in the header:



Click the **Add to selected group** button to open the **Multi Device Edit** window:

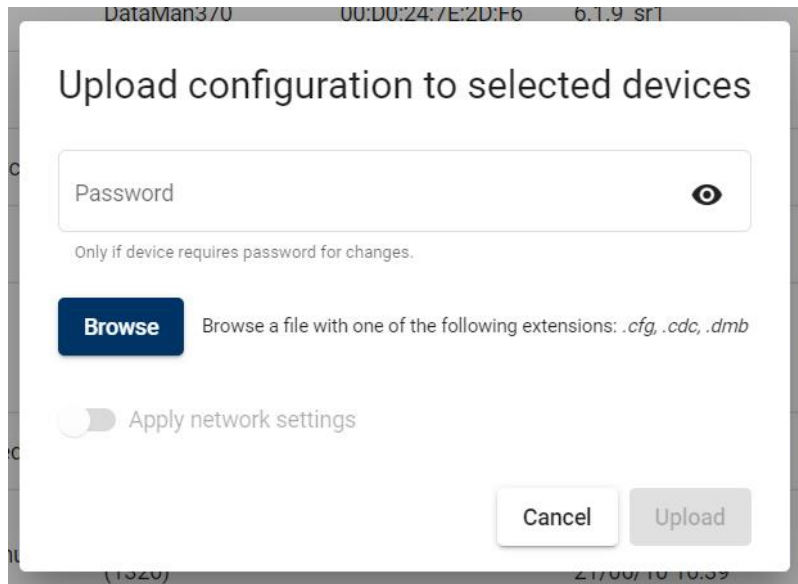


In the **Multi Device Edit** window, you can:

- add the selected devices to an existing group
- create a new group with the selected devices
- define a primary device in the group
- reorder the devices
- flash the LEDs of the individual devices for easy identification
- manually configure the IP Address, Subnet Mask, and Default Gateway

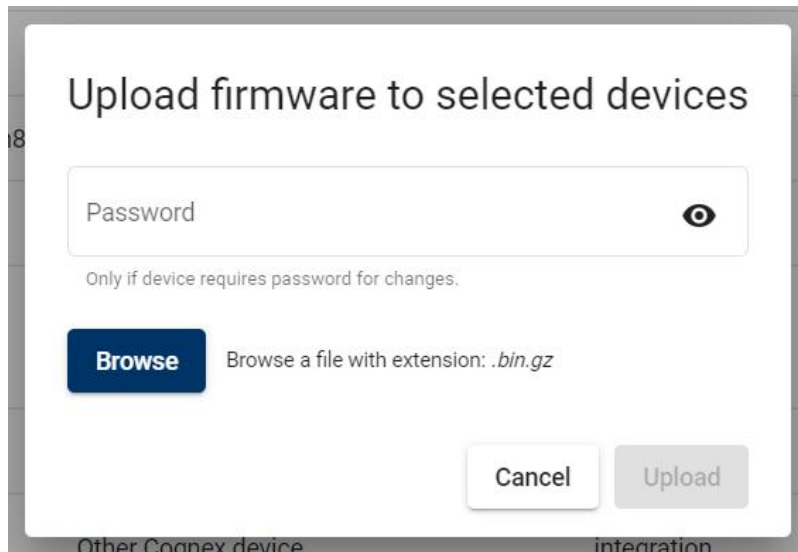
Enter the device password if the device is set up to require it. Click **Save** to apply any changes.

To upload a saved configuration file to selected devices, click the **Upload configuration** button, opening the **Upload configuration to selected devices** window:



Click **Browse** to select the configuration file for upload. Enable **Apply network settings** to apply network settings. Enter the device password if the device is set up to require it, and click **Upload**.

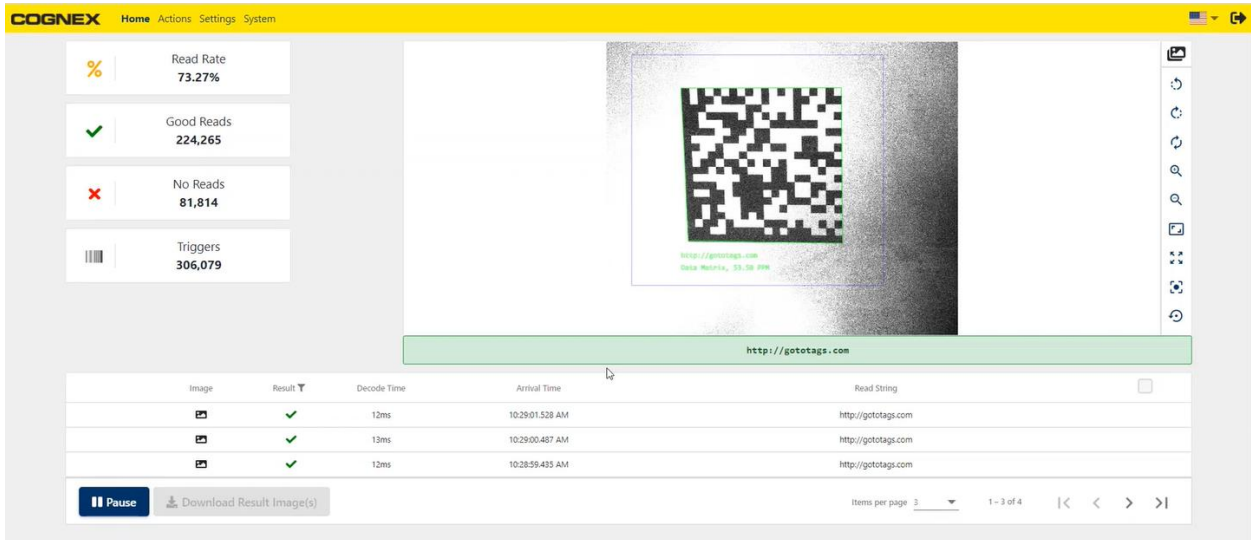
To update the firmware on selected devices, click the **Upload firmware** button, opening the **Upload firmware to selected devices** window:



Click **Browse** to select the firmware file for upload. Enable **Apply network settings** to apply network settings. Enter the device password if required, and click **Upload**.

DataMan WebHMI

The DataMan WebHMI application provides a live view of device reads, results and statistics, and allows you to pause the feed and scroll back to analyze or download individual result images. You can manually trigger or tune devices and adjust device settings from the DataMan WebHMI.



You can access the DataMan WebHMI for a connected DataMan device from the DataMan page of the EI Tunnel Manager user interface by clicking on the gear icon labeled **Open DataMan WebHMI** in the **Actions** column of the selected device.

Home







The DataMan WebHMI **Home** page displays a live feed of the device with statistics and result logs.

On the left side, the DataMan WebHMI home page shows statistics for:

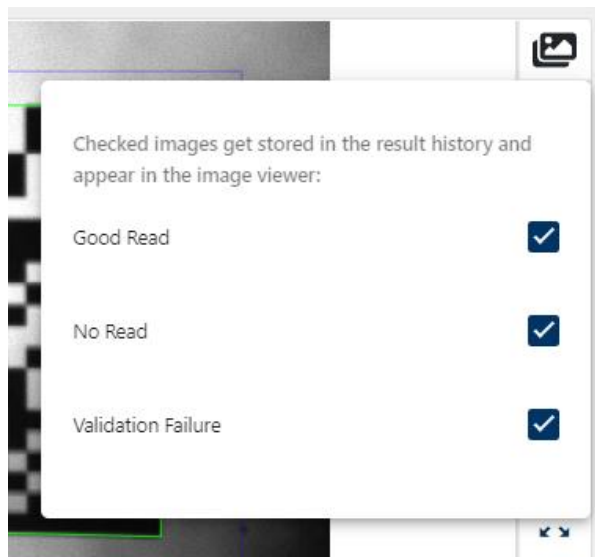
- **Read Rate** percentage
- Number of **Good Reads**
- Number of **No Reads**
- Number of **Triggers**

The display on the right side of the page provides a live feed of the device view with additional controls on the right side of the display for changing orientation and zoom:




Icon	Action
	Rotate Left 90°
	Rotate Right 90°
	Reset Rotation
	Zoom In

	
Icon	Action
	Zoom Out
	Zoom To Original Size
	Reset Zoom
	Move Center
	Reset All Settings

You can also filter the feed to display only **Good Read**, **No Read**, or **Validation Failure** results by clicking on the **Images** icon in the top right corner of the display.



The result logs of the last 50 captures are listed on the bottom of the page. You can browse the list using the navigation buttons in the bottom right corner of the pane.

Image	Result	Decode Time	Arrival Time	Read String
	✓	13ms	12:03:18.947 PM	12
	✓	12ms	12:03:17.783 PM	http://www.google.com
	✗	13ms	12:03:16.586 PM	

Items per page 3
 1 – 3 of 50

Click on the **Pause** button in the bottom left corner to pause the live feed. Pausing the feed allows you to select and download result images. Click on a log to put the result image on the display.

To download the image currently on the display, click on the **Download Result Image(s)** button without selecting any images from the result logs.

Check the checkboxes in the rightmost column of the result logs to select images for download, or check the checkbox in the table header to select all images. Click on **Download Result Image(s)** while multiple images are selected to download a ZIP file containing the selected result images.

Actions

The **Actions** page of the DataMan WebHMI allows you to manually trigger, start or stop, tune, or untrain the device.



Click **Trigger** to trigger the device manually.

Click **Live** to show the live feed of the device camera.

Click **Tune** to initiate an automatic recalibration. Open the Tune dropdown to optimize brightness or focus individually.

Note: When you tune a device, the device stops triggering.

Click **Untrain** to untrain the device.

Settings

The **Settings** page of the DataMan WebHMI allows you to manually change the device configuration, upload, download, or save the current configuration, or reset the device to a previously saved configuration.

Variable Name	Setup 0
Read Setup	
Name	Setup 0
Enabled	<input checked="" type="checkbox"/>
Enable Distance Check	<input type="checkbox"/>
Min Distance (mm)	0
Max Distance (mm)	10000
Starting Setup	0
Last Successful Decode	<input type="checkbox"/>
Tuning	
Train Code	<input checked="" type="checkbox"/>

- Click **Expand All** or **Collapse All** at the top of the page to expand or collapse the setting categories in the settings table.
- Click **Add New Read Setup** to create a new setup using default settings or an existing setup as a template.

- Click **Upload** to upload a local configuration file to the device.
- Click **Download** to save the device configuration locally.
- Click **Save** to save the configuration on the device flash memory.
- Click **Reset** to reset the device configuration to default or a saved configuration.

The settings table provides you with detailed and in-depth configuration options for all device functionality. Each setting corresponds to a control command for the reader. For a detailed description of the available settings for the reader you are configuring, see the corresponding control commands for the reader in the *DataMan Control Commands Documentation*.

System

The **System** page of the DataMan WebHMI displays detailed device information, reader statistics, feature keys, and device time.

COGNEX Home Actions Settings System

Device Information

Device Model:	Firmware Version:
Serial Number:	Installed Hardware: LiquidLens, Custom
Device Name:	Bootloader Version:
MAC Address:	OS Version:
IP Address:	

Feature Keys

1DCodeQuality, 1DDataStitching, 1DExtendedRes, 2DCode, 2DCodeQuality, BarCode, DotCode, IDMax, FullSpeed, IDQuick, ImageDownload, ImageFiltering, ImageFoV_Full, IntImageBuffer, LadderAndPicket, MST, Omnidirectional, PostalCode, PowerGrid, Scripting, SignopticSig, Validation

Device Time

Local Time:
Jan 26, 2019, 2:36:11 AM

Uptime:
601h 36m 13s

Reader Statistics

[Clear](#)

Total Triggers: 1,376,159	Missed Triggers: 0
Total Reads: 1,225,743	Passed Validations: 0
Read Rate: 89.07%	Failed Validations: 0
Total No-Reads: 150,416	Buffer Overflows: 0
No-Read Rate: 10.93%	Trigger Overruns: 0
	Item Count: 0

Feature Keys

The Feature Keys page shows the feature keys applied on each discovered reader.

Home > Multi Reader Configuration > Feature Keys

Upload feature keys Download as CSV Discover devices

Search

Standalone Devices

Unlocked

Actions	Name	Type	Firmware Version	Serial Number	Feature Keys	Task Status
👤					1DCodeQuality, 1DDataStitching, 1DExtendedRes, 2DCode, 2DCodeQuality, BarCode, DPM_IDMax, DotCode, FullSpeed, HDRPlus, IDQuick, ImageDownload, ImageFiltering, IntImageBuffer, LadderAndPicket, Omnidirectional, PostalCode, PowerGrid, Scripting, Validation	
👤					1DCodeQuality, 1DDataStitching, 1DExtendedRes, 2DCode, 2DCodeQuality, BarCode, DPM_IDMax, DotCode, FullSpeed, HDRPlus, IDQuick, ImageDownload, ImageFiltering, IntImageBuffer, LadderAndPicket, Omnidirectional, PostalCode, PowerGrid, Scripting, Validation, MST, PFP, SymbolDiagnostics	
👤					1DCodeQuality, 1DDataStitching, 1DExtendedRes, 2DCode, 2DCodeQuality, BarCode, DPM_IDMax, DotCode, FullSpeed, HDRPlus, IDQuick, ImageDownload, ImageFiltering, IntImageBuffer, LadderAndPicket, Omnidirectional, PostalCode, PowerGrid, Scripting, Validation, MST, PFP, SymbolDiagnostics	
👤					1DCodeQuality, 1DDataStitching, 1DExtendedRes, 2DCode, 2DCodeQuality, BarCode, DPM_IDMax, DotCode, FullSpeed, HDRPlus, IDQuick, ImageDownload, ImageFiltering, IntImageBuffer, LadderAndPicket, Omnidirectional, PostalCode, PowerGrid, Scripting, Validation, SymbolDiagnostics	
👤					1DCodeQuality, 1DDataStitching, 1DExtendedRes, 2DCode, 2DCodeQuality, BarCode, DPM_IDMax, DotCode, FullSpeed, HDRPlus, IDQuick, ImageDownload, ImageFiltering, IntImageBuffer, LadderAndPicket, Omnidirectional, PostalCode, PowerGrid, Scripting, Validation	
👤					1DCodeQuality, 1DDataStitching, 1DExtendedRes, 2DCode, 2DCodeQuality, BarCode, DPM_IDMax, DotCode, FullSpeed, HDRPlus, IDQuick, ImageDownload, ImageFiltering, IntImageBuffer, LadderAndPicket, Omnidirectional, PostalCode, PowerGrid, Scripting, Validation, SymbolDiagnostics	

Test

All

Actions	Name	Type	Firmware Version	Serial Number	Feature Keys	Task Status
👤					1DCodeQuality, 1DDataStitching, 1DExtendedRes, 2DCode, 2DCodeQuality, BarCode, DPM_IDMax, DotCode, FullSpeed, HDRPlus, IDQuick, ImageDownload, ImageFiltering, IntImageBuffer, LadderAndPicket, MST, Omnidirectional, PostalCode, PowerGrid, Scripting, SymbolDiagnostics, Validation, PFP	
👤					1DCodeQuality, 1DDataStitching, 1DExtendedRes, 2DCode, 2DCodeQuality, BarCode, DPM_IDMax, DotCode, FullSpeed, HDRPlus, IDQuick, ImageDownload, ImageFiltering, IntImageBuffer, LadderAndPicket, MST, Omnidirectional, PostalCode, PowerGrid, Scripting, SymbolDiagnostics, Validation, PFP	

The following actions are available:

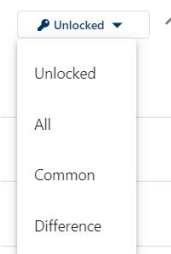
- Uploading feature key files
- Downloading Feature Keys page information in CSV
- Discovering devices

Upload feature keys Download as CSV Discover devices	
Button	Description
Upload feature keys	Upload feature key files.
Download as CSV	Download device list with all data in CSV format.
Discover devices	Discover connected devices.

The Feature Keys page also allows comparing uploaded feature keys between readers in a group:

Feature Key Color	Description
BLUE	The feature is unlocked for the device.
RED	The feature is unlocked for some devices in the group, but not for the respective device.

Click the **Difference** dropdown menu to select the following menu items for comparison:



Item	Description
Unlocked	Show unlocked feature keys for all devices.
All	Show unlocked and locked feature keys for all devices.
Common	Show feature keys which are unlocked for all devices.
Difference	Show feature keys which have a different status among the devices.

Click the **Upload feature keys** button to upload a feature key file from your computer:

Upload feature key files

Only if device requires password for changes.

Browse Browse files with extension: .xml

Verification	File Name	Device Name	Serial Number	Feature Keys in File
✓				PTP MST

Cancel
Upload

Item	Description
Password	Password is only needed if the device requires a password.
Browse	Browse files with .xml extension on your computer.
Verification	Shows verified status.
File Name	Name of the feature key files.

Upload feature key files

👁

Only if device requires password for changes.

Browse
Browse files with extension: .uml

Verification	File Name	Device Name	Serial Number	Feature Keys in File
✓				PTP MST

Cancel
Upload

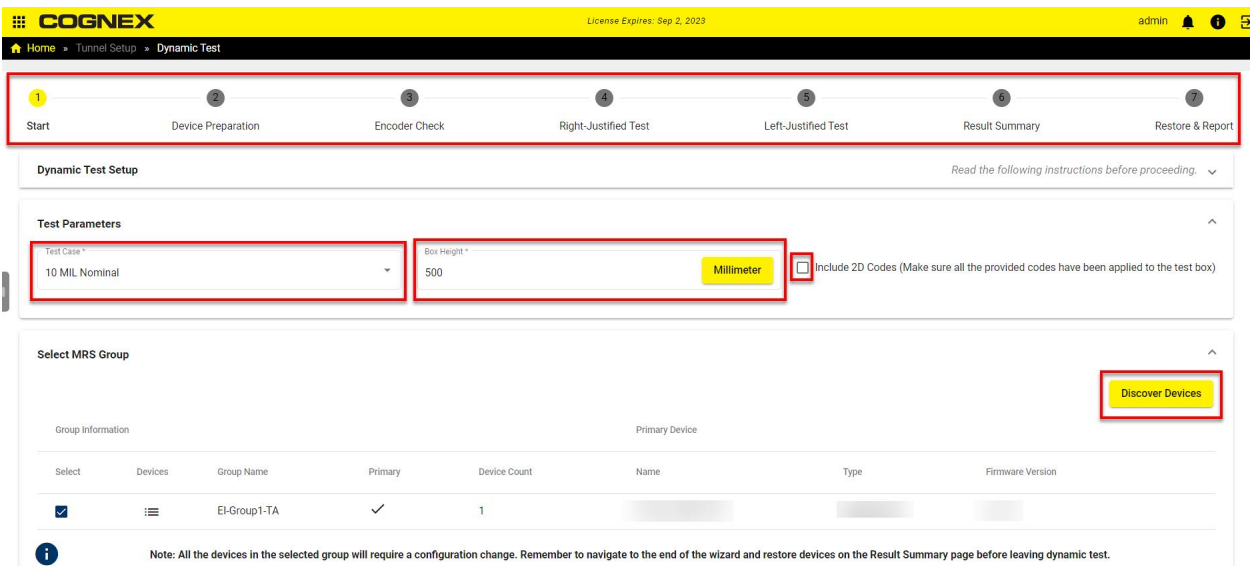
Item	Description
Device Name	Name of the device which gets the new feature key file.
Serial Number	Serial number of the device.
Feature Keys in File	Feature keys contained in the file.

El Tunnel Manager Setup Apps

El Tunnel Manager Setup Apps allow you to perform dynamic tests and 3D calibration on your device.

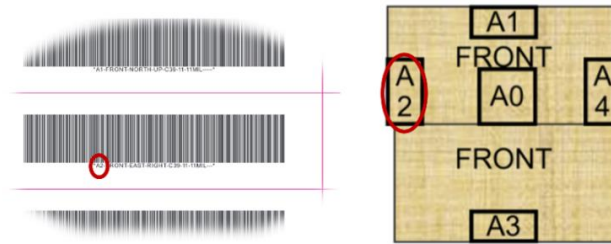
Dynamic Test

The **Dynamic Test** page of the **El Tunnel Manager Setup** allows you to perform a dynamic test of the tunnel in seven steps.

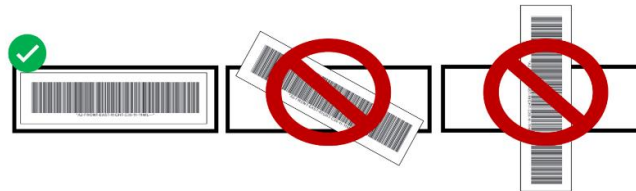


To set Set up the target box and perform dynamic tests:

1. Locate the box and the sheet of adhesive 1D and 2D code labels.
 Build the box and adjust the height to the maximum height supported by the tunnel.
 If 2D codes are in the dynamic test, apply the 2D codes from the label sheet to the box.
 Select the **Include 2D Codes checkbox**. This step is optional.
 Apply each code label within the corresponding rectangular outline printed on the target box by matching the first two characters of the code content and the two characters printed within the rectangle.

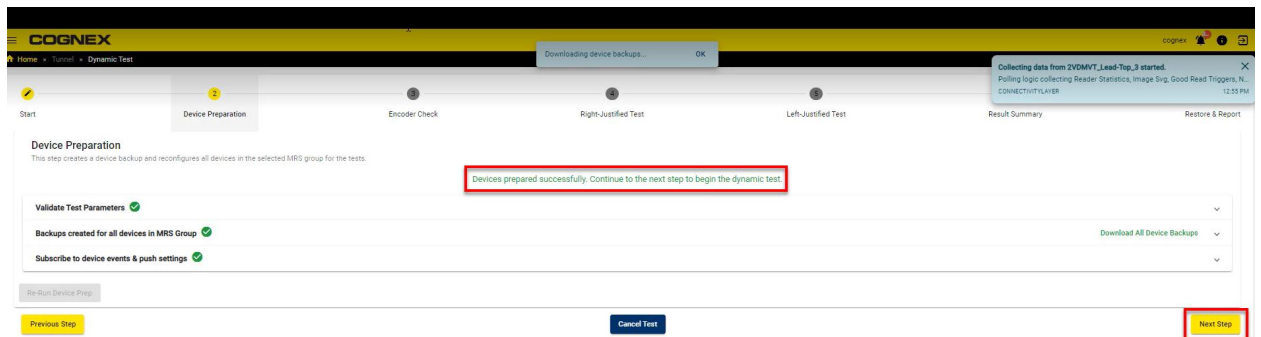


Make sure you apply the label within the rectangle printed on the box as demonstrated below:

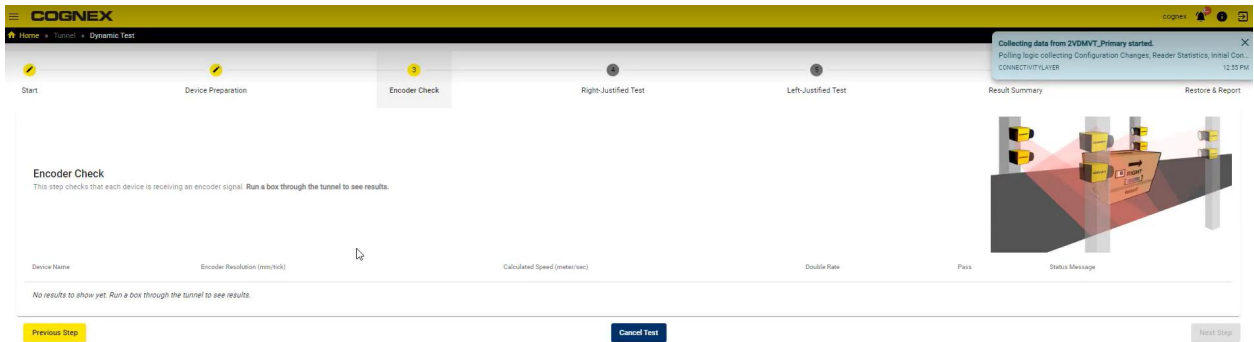


Fill in the **Test Parameters** fields such as **Test Case*** and **Box Height*** and select an *MRS group* from the **Primary Device** list discovered by clicking on **Discover Devices**.

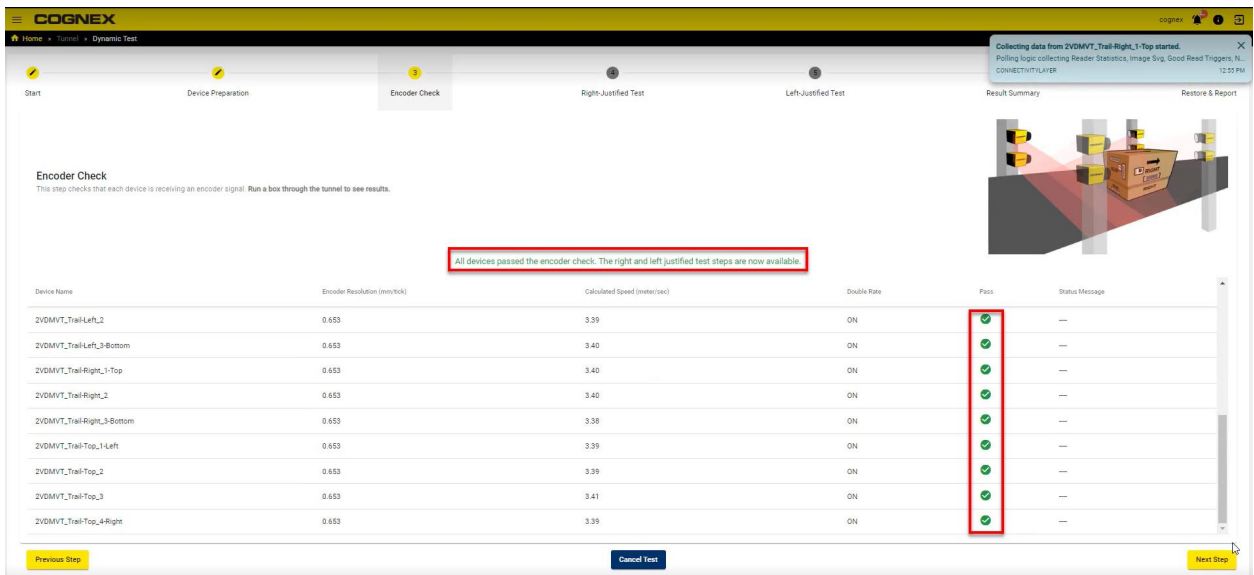
2. After seeing the message *Device prepared successfully. Continue to the next step to begin the dynamic test.*, to create device backups and reconfigure all devices in the selected MRS group for the tests in the **Device Preparation** step, click on **Next Step**.



- The **Encoder Check** step is the third one, allowing you to check if each device is receiving an encoder signal. To see the results, bring the conveyor belt up to full production speed and run a box through the tunnel. Any orientation is acceptable.

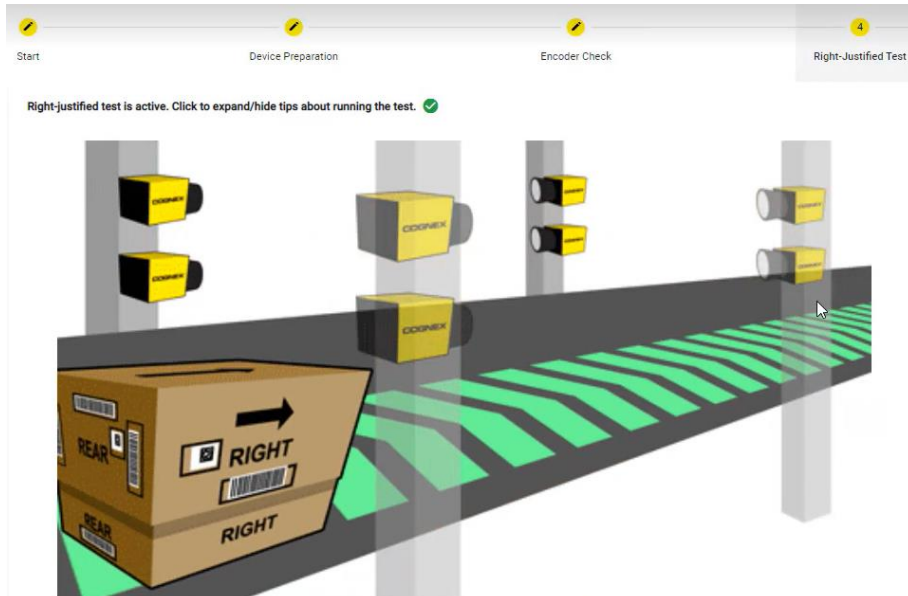


After the encoder check is complete, you see the message *All devices passed the encoder check. The right and left justified test steps are now available.* and pass icons under the **Pass** column.



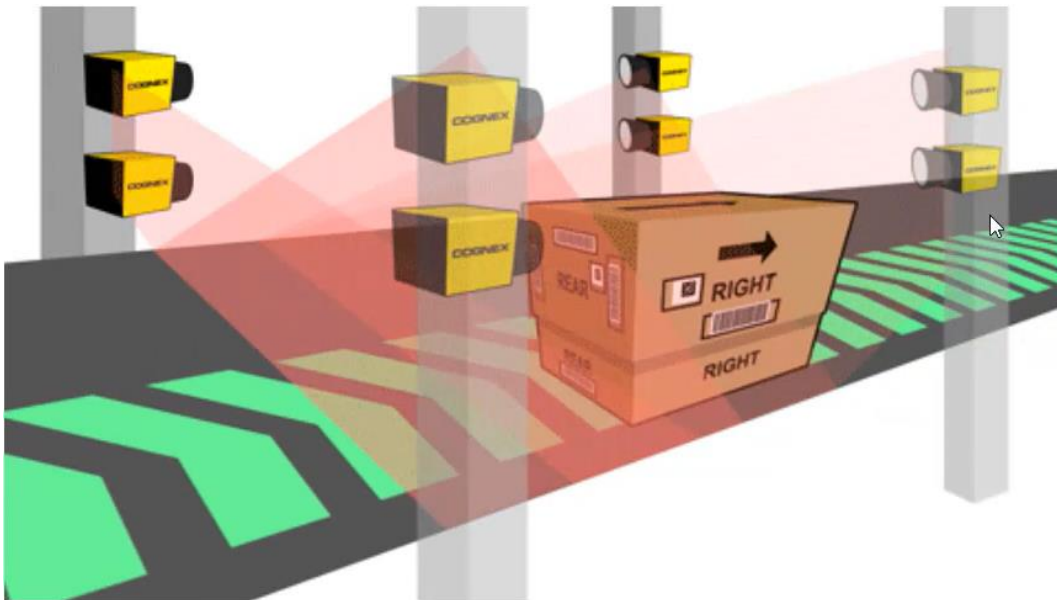
To complete this step and switch to the **Right-Justified Test** step, click on **Next Step**.

- In the **Right-Justified Test** step the right-justified test becomes active. For this test, run the test box right justified on the belt. Place the box on the belt with the front side facing downstream. Make sure to use the dynamic test box.

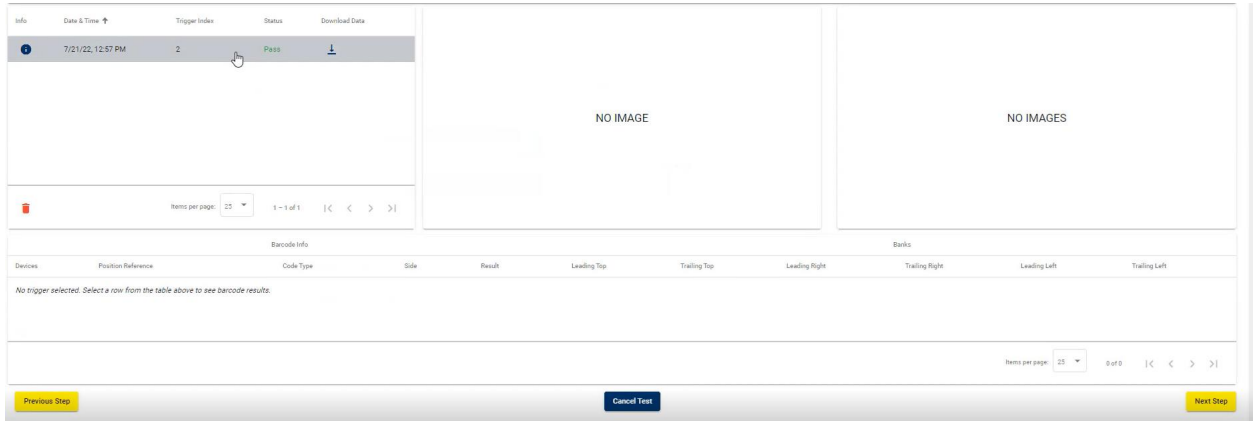


Wherever possible, include box that runs at both slower (less than or equal to 300 ft/min or 1.52 m/s) and faster belt speed (greater than 300 ft/min or 1.52 m/s) before completing the test and generating the report.

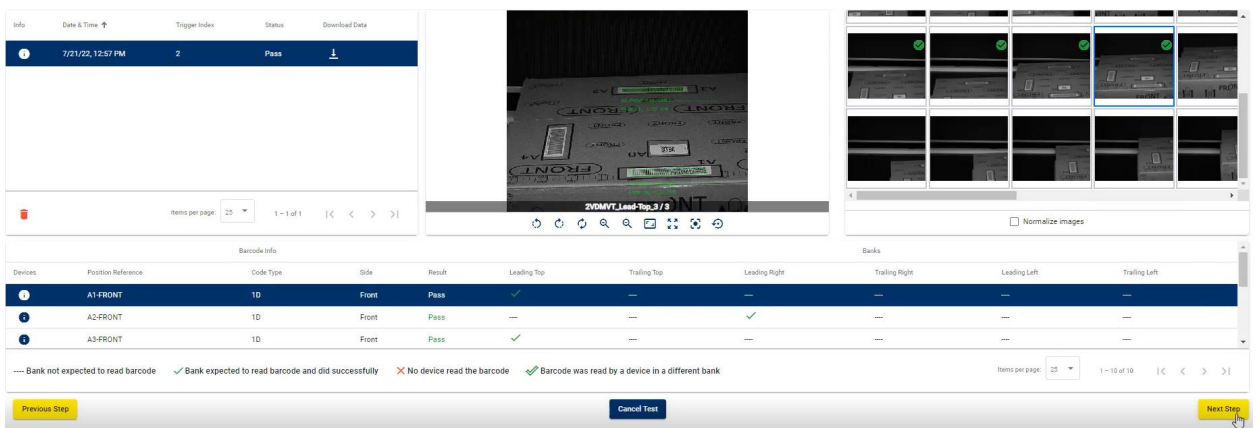
To make sure the box stays level to the belt, add weight to the box. Give the box enough distance before the tunnel, so it moves through at full speed.



5. To see the passed test details, click on the test row.



More detailed test results open up.



Review the table and verify there are no codes with an **X**. The **X** indicates that the code must be read but it was not read.

The barcodes with the green check mark indicate that they must be read and were read successfully.

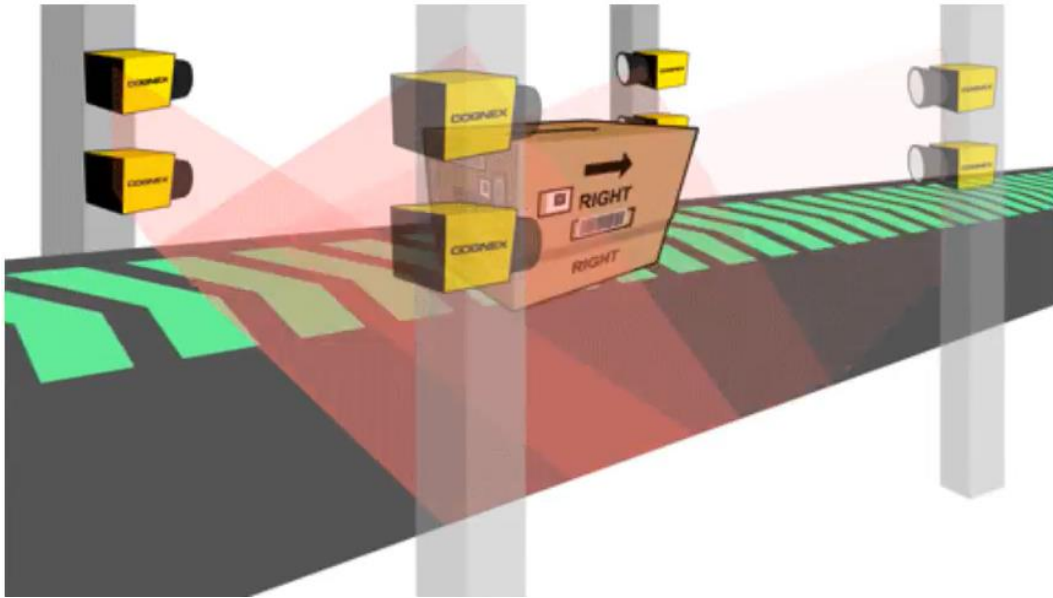
- At belt speeds of less than 300 fpm we need every code to be read at least once.
- At faster belt speeds each code needs to be read by the specific banks.

It is possible that you have to run the box through multiple times to pass. Once you pass on all barcodes, you can move on to the **Left-Justified Test** step by clicking on **Next Step**.

- In the **Left-Justified Test** step the left-justified test becomes active. For this test, run the test box right justified on the belt. Place the box on the belt with the front side facing downstream. Make sure to use the dynamic test box.

Wherever possible, include box that runs at both slower (less than or equal to 300 ft/min or 1.52 m/s) and faster belt speed (greater than 300 ft/min or 1.52 m/s) before completing the test and generating the report.

To make sure the box stays level to the belt, add weight to the box. Give the box enough distance before the tunnel, so it moves through at full speed.



To see the passed test details, follow the same steps as in **Right-Justified Test**.

To proceed to the **Result Summary** step, click on **Next Step**.

- In the **Result Summary** step you can review the summary of the dynamic tests.

Test Mode	Status	Total Attempts	Successful Attempts	Unsuccessful Attempts	Device Summary
Right	Pass	1	1	0	☰
Left	Pass	1	1	0	☰
Encoder	Pass	1	1	0	☰

Buttons: Previous Step, Cancel Test, Next Step

When you click on **Next Step**, the **Complete Dynamic Test** pop-up appears.

Complete Dynamic Test

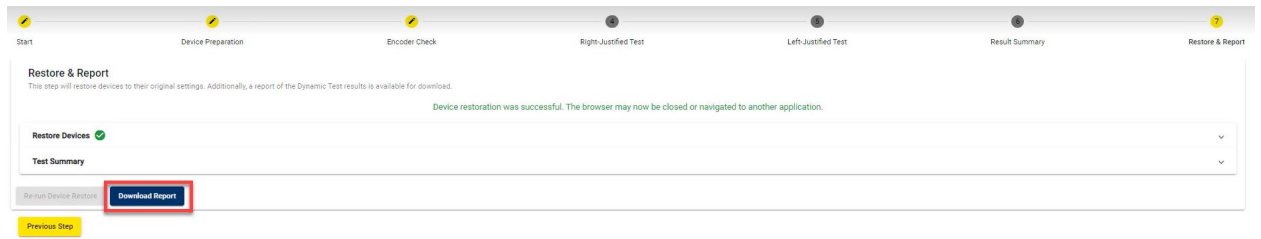
Navigating to the final step will end the dynamic test, and your devices will be restored to their original settings. Do you wish to continue?



To complete the dynamic test and switch to the next step, click on **Confirm**.

Note: If you have to abort the test at any time, you can click on the **Cancel** button at the bottom of the page.

- The **Restore & Report** step restores devices to their original settings. Additionally, a report of the dynamic test results is also available for downloading.



To download the test report, click on **Download Report**. Fill in the details in **Generate Dynamic Test Report** pop-up, and click on **Generate Report**.

Generate Dynamic Test Report

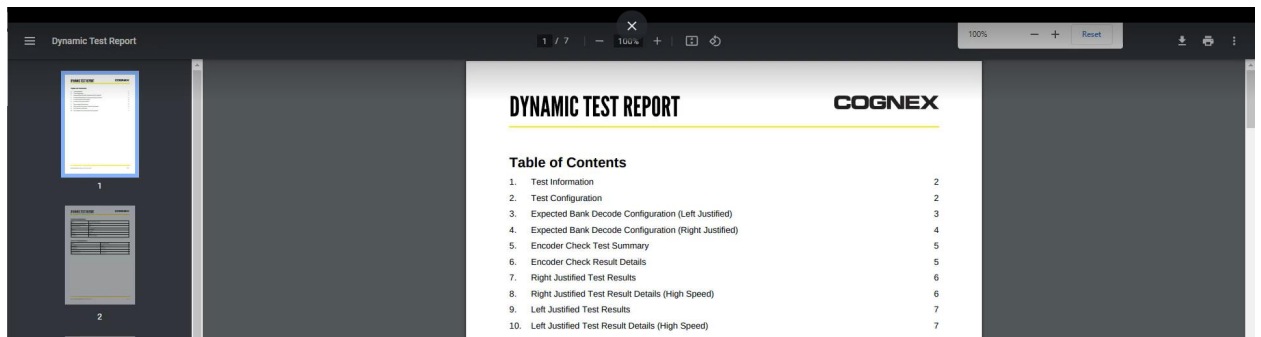
Test Executed By Project Name

Site Station

Comment

Cancel

The report generation is complete and the file opens up.



3D Field Calibration

The **3D Field Calibration** page of the **EI Tunnel Manager Setup Apps** application allows you to calibrate devices which consists of five different steps allowing for features such as barcode assignment.

Before getting started:

- Complete the **Dynamic Test** page steps.
- Make sure that the dimensioner collects the data.
- Disconnect DataMan Bottom Side Line Scan and Image-Only readers.

Home » Tunnel Setup » 3D Field Calibration

1 Setup 2 Pre-Calibration Validation 3 Data Collection 4 Calibration 5 Restore & Push Calibrations

Calibration Parameters All parameters are required. ^

Static Calibration Mode

Setting the calibration interval

- When running a calibration, the app will update the intervals for all selected devices and revert them in the final step of this app
- The calibration interval will be automatically calculated based on the production and calibration belt speeds
- For best results, perform the calibration at a belt speed that does not exceed **250 feet/minute (1.25 meter/second)**
- The calibration belt speed should not exceed the production belt speed
- To set the calibration interval manually, check the **Set Calibration Interval Manually** box below and enter the desired camera interval

Set Calibration Interval Manually

Production Belt Speed *	feet/minute	Calibration Belt Speed *	feet/minute
<small>The speed of the belt when run normally.</small>		<small>The speed of the belt when performing a calibration.</small>	

Vision Service Hostname

This EI Box ()

Tunnel RTM PC ()

Other Server

This EI Box for the Vision Service Hostname and LGM-CALIBBOX-556 for the Calibration Box Type are by default selected values.

1. In the first step, start with setting the calibration interval. Enter conveyor parameters which are **Production Belt Speed** and **Calibration Belt Speed** and select readers:

Note: Consider the following aspects when setting the calibration interval:

- When running a calibration, the app updates the intervals for all selected devices and reverts them in the final step.
- The calibration interval is automatically calculated based on the production and calibration belt speeds.
- For best results, perform the calibration at a belt speed that does not exceed 250 feet/minute (1.25 meter/second).
- The calibration belt speed must not exceed the production belt speed.
- To set the calibration interval manually, check the **Set Calibration Interval Manually** box below and enter the desired camera interval.

Select devices to calibrate:

<input checked="" type="checkbox"/>	Primary	Name	Type	MAC Address	Firmware Version	IP Address	Group
<input checked="" type="checkbox"/>							2VDMVT580
<input checked="" type="checkbox"/>							2VDMVT580
<input checked="" type="checkbox"/>							2VDMVT580
<input checked="" type="checkbox"/>							2VDMVT580
<input checked="" type="checkbox"/>							2VDMVT580
<input checked="" type="checkbox"/>							2VDMVT580
<input type="checkbox"/>	<input checked="" type="checkbox"/>						2VDMVT580
<input checked="" type="checkbox"/>							2VDMVT580
<input checked="" type="checkbox"/>							2VDMVT580
<input checked="" type="checkbox"/>							2VDMVT580
<input checked="" type="checkbox"/>							2VDMVT580
<input checked="" type="checkbox"/>							2VDMVT580
<input checked="" type="checkbox"/>							2VDMVT580
<input checked="" type="checkbox"/>							2VDMVT580

Next Step

Click on **Next Step** to switch to the **Pre-Calibration Validation** step.

2. In the **Pre-Calibration Validation** step, validate the test parameters. After the validation is complete, the *All validations successful.* message appears. Click on **Next Step**.

Pre-Calibration Validation
 These validations will help determine if there are any issues with the tunnel/devices before data collection occurs.

All validations successful.

- Validate entered parameters
- New Camera Interval Calculated Expand here to review all devices and their new camera interval that will be set during data collection.
- Calibration Vision Service Set
- Factory Calibrations available for all selected devices Download All Factory Calibrations
- Backups created for all selected devices Download All Device Backups

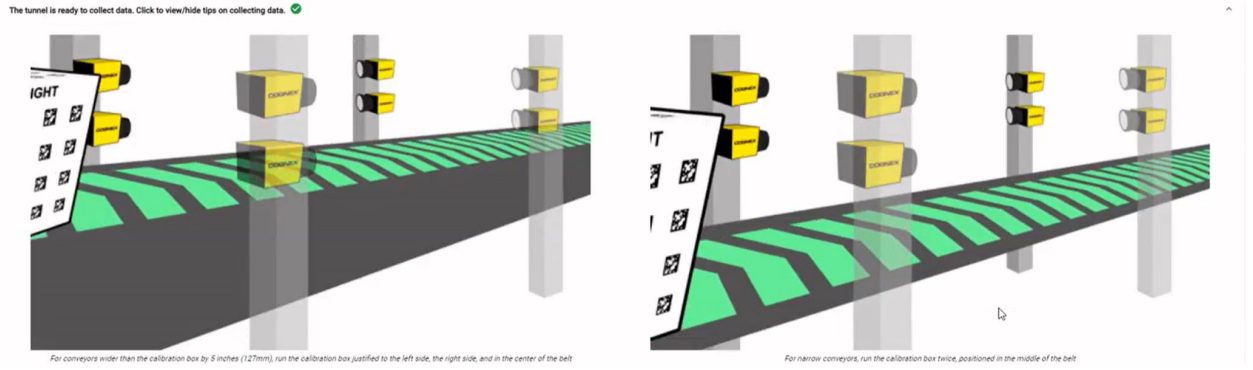
Re-Run All Validations

Note: All the devices being calibrated will require a configuration change. Remember to navigate to the end of the wizard and restore devices on the restore & push calibrations page before leaving this app.

Previous Step Next Step

Note: If you receive an error that you cannot take backups and expanding the drop down shows an error about dirty configurations, either reload the backups taken from a previous run or re-run *Tunnel Commissioning* wizard.

3. In the **Data Collection** step, the calibration triggers are captured.



- Make sure that the calibration box is oriented correctly with the front side facing downstream on the conveyor and run the box through the tunnel at the calibration speed you set in the previous step.

Note: If the conveyor is wider than the calibration box by 5 inches, you have to run the box through at different positions on the belt:

- The left side of the belt.
- The right side of the belt.
- The center of the belt.

i

If the conveyor is narrow, place the box at the center of the belt and run it through twice.

- Select the best triggers from the triggers list and click on **Next Step** to calibrate.

<input type="checkbox"/>	<input type="checkbox"/>	Date & Time	Trigger index	Length	Width	Height	Angle	Image Count	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Jul 21, 2022, 1:13:42 PM	26					214	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	Jul 21, 2022, 1:14:05 PM	27	515	514	611	-1	167	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Jul 21, 2022, 1:14:28 PM	28	514	510	611	-4	174	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	Jul 21, 2022, 1:14:51 PM	29	516	511	612	1	167	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	Jul 21, 2022, 1:17:55 PM	30	514	513	611	-5	174	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Jul 21, 2022, 1:18:18 PM	31	513	513	611	2	174	<input type="checkbox"/>
Total images for selected triggers								348	

2VDMVT_LeadLeft_1-Top	9
2VDMVT_LeadLeft_2	9
2VDMVT_LeadLeft_3-Bottom	9
2VDMVT_LeadRight_1-Top	8
2VDMVT_LeadRight_2	8
2VDMVT_LeadRight_3-Bottom	8
2VDMVT_LeadTop_1-Left	9
2VDMVT_LeadTop_2	9
2VDMVT_LeadTop_3	9
2VDMVT_LeadTop_4-Right	9
2VDMVT_TrailLeft_1-Top	9
2VDMVT_TrailLeft_2	9
2VDMVT_TrailLeft_3-Bottom	9
2VDMVT_TrailRight_1-Top	8
2VDMVT_TrailRight_2	8
2VDMVT_TrailRight_3-Bottom	8
2VDMVT_TrailTop_1-Left	9
2VDMVT_TrailTop_2	9
2VDMVT_TrailTop_3	9
2VDMVT_TrailTop_4-Right	9

- The **Calibration** step appears. Click on **Re-run Failed Devices** to re-run the the failed device calibrations where the calibration process begins automatically and the calibration for each device takes place.

Name	Status	Trigger Used	Image Used	Arrival Time	Max. Error (mm)	Side	Max. Error (mm)	Side
2VDMVT_Lead-Left_3-Bottom	Complete	28	3	7/21/22, 1:16 PM	13.784	Left	16.618	Front
2VDMVT_Lead-Left_1-Top	Complete	28	3	7/21/22, 1:16 PM	9.95	Left	12.946	Front
2VDMVT_Lead-Left_2	Complete	28	3	7/21/22, 1:16 PM	11.612	Left	15.436	Front
2VDMVT_Lead-Right_2	Complete	28	4	7/21/22, 1:16 PM	7.864	Right	---	---
2VDMVT_Lead-Right_1-Top	Complete	28	4	7/21/22, 1:16 PM	7.835	Right	---	---
2VDMVT_Lead-Right_3-Bottom	Complete	28	4	7/21/22, 1:16 PM	7.369	Right	---	---
2VDMVT_Lead-Top_1-Left	Code validation failure	0	0	7/21/22, 1:16 PM	---	---	---	---
2VDMVT_Lead-Top_2	Complete	28	1	7/21/22, 1:16 PM	8.259	Top	12.507	Front
2VDMVT_Lead-Top_3	Complete	28	1	7/21/22, 1:16 PM	8.914	Top	12.25	Front
2VDMVT_Lead-Top_4-Right	Complete	28	1	7/21/22, 1:16 PM	9.277	Top	12.067	Front
2VDMVT_Tail-Left_1-Top	Complete	28	3	7/21/22, 1:16 PM	5.356	Left	---	---
2VDMVT_Tail-Left_2	Complete	28	3	7/21/22, 1:16 PM	5.665	Left	---	---
2VDMVT_Tail-Left_3-Bottom	Complete	28	3	7/21/22, 1:16 PM	5.103	Left	---	---
2VDMVT_Tail-Right_1-Top	Complete	28	6	7/21/22, 1:16 PM	9.056	Right	11.298	Back
2VDMVT_Tail-Right_2	Complete	28	4	7/21/22, 1:17 PM	7.571	Right	14.667	Back

If necessary, after all the calibration is successfully complete, click on **Next Step**.

Trigger Info						Plane 1		Plane 2	
Name	Status	Trigger Used	Image Used	Arrival Time	Max. Error (mm)	Side	Max. Error (mm)	Side	
2VDMVT_Lead-Left_3-Bottom	Complete	28	3	7/21/22, 1:16 PM	13.784	Left	16.618	Front	
2VDMVT_Lead-Left_1-Top	Complete	28	3	7/21/22, 1:16 PM	9.95	Left	12.946	Front	
2VDMVT_Lead-Left_2	Complete	28	3	7/21/22, 1:16 PM	11.612	Left	15.436	Front	
2VDMVT_Lead-Top_2	Complete	28	1	7/21/22, 1:16 PM	8.259	Top	12.507	Front	
2VDMVT_Lead-Top_3	Complete	28	1	7/21/22, 1:16 PM	8.914	Top	12.25	Front	
2VDMVT_Lead-Top_4-Right	Complete	28	1	7/21/22, 1:16 PM	9.277	Top	12.067	Front	
2VDMVT_Tail-Right_1-Top	Complete	28	6	7/21/22, 1:16 PM	9.056	Right	11.298	Back	
2VDMVT_Tail-Right_2	Complete	28	4	7/21/22, 1:17 PM	7.571	Right	14.667	Back	
2VDMVT_Tail-Right_3-Bottom	Complete	28	5	7/21/22, 1:17 PM	10.095	Right	10.859	Back	
2VDMVT_Tail-Top_2	Complete	28	8	7/21/22, 1:17 PM	6.635	Top	4.663	Back	
2VDMVT_Tail-Top_3	Complete	28	8	7/21/22, 1:17 PM	4.799	Top	9.083	Back	
2VDMVT_Tail-Top_4-Right	Complete	28	7	7/21/22, 1:17 PM	4.01	Top	10.043	Back	

The error value columns determine if the test result is pass or fail. It is expected that error values to be higher in the right column due to higher perspective on those faces:

- An optimal error value is less than 25 mm.
- An acceptable error value is between 25 and 50 mm.
- Any values over 50 mm are not accepted.

If you receive unacceptable values, you can return to the previous step and run another box for the area that failed by clicking on **Re-run Failed Devices** or **Re-run All Devices**.

The **Complete Calibration** pop-up appears. To complete the calibration, click on **Confirm**.

- The final step of **Restore & Push Calibrations** restores the devices to their original settings and automatically load calibration data to all devices. Once this process is complete, you can close the page.

Archiver

The **Archiver** application of EI Tunnel Manager provides a method of storing and organizing data obtained from your readers, such as downloaded images and trigger sequences.

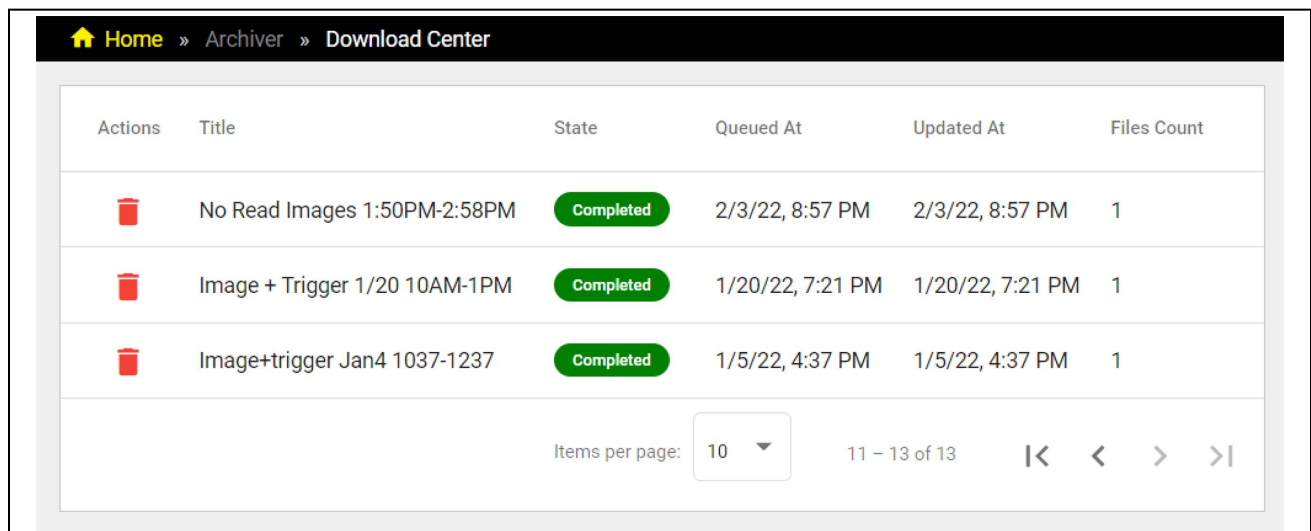
Download Center




The **Download Center** page of the Archiver application allows you to manage your current and historical archives.

When you download image or trigger data from the Results Explorer page of the Performance Analytics application, EI Tunnel Manager stores it in an archive file. Downloaded archives reside on the hard drive of the EI Tunnel Manager unit. The time it takes to create the archive depends on the size and the number of images that needs processing, and can take from around one minute to up to two hours. Depending on the amount of data, EI Tunnel Manager generates one or more archives. The size limit for a single archive is 1 GB. When the remaining disk space approaches approximately 50 GB, EI Tunnel Manager automatically starts to delete older images.

Note: Archives always have storage priority over the images stored in Results Explorer.

The Download Center page:



Column	Description
Actions	The possible actions for an archive. The following actions are available when clicking in the appropriate icon: <ul style="list-style-type: none">  deletes an archive  cancels the request to create the archive  resubmits the request to create the archive
Title	The user-specified name of the archive.

Home » Archiver » Download Center

Actions	Title	State	Queued At	Updated At	Files Count
	No Read Images 1:50PM-2:58PM	Completed	2/3/22, 8:57 PM	2/3/22, 8:57 PM	1
	Image + Trigger 1/20 10AM-1PM	Completed	1/20/22, 7:21 PM	1/20/22, 7:21 PM	1
	Image+trigger Jan4 1037-1237	Completed	1/5/22, 4:37 PM	1/5/22, 4:37 PM	1

Items per page: 10 11 - 13 of 13 << < > >>

Column	Description
State	The status of the archive. Displays one of the following states: <ul style="list-style-type: none"> Idle Collecting Data Running Completed Canceled
Queued At	The time when download starts.
Updated At	The time of the last status update or when the download finishes.
Files Count	The total number of ZIP files in the archive.

The archive file has the following contents:

- One or more folders that contain the images. El Tunnel Manager organizes the folders by date, and each folder name has the format of YYYYMMDD.

The images in each folder follow a naming convention based on whether they originate from a standalone reader or from an MRS group:



- For standalone readers, the image name contains the device name, the trigger index, the image index, and the time stamp, in this order and separated by underscores. For example, *ST_1_DM470_566898_0_20211221T190905.jpg*.
- For readers in an MRS group, the image name contains the group name, the device name, the trigger index, the image index, the time stamp, and four random characters to prevent name collision, in this order and separated by underscores. For example, *Tunnel1_ST_3_DM470_1126_0_20220204T141531_6802.jpg*.

- One CSV file that contains trigger data. The name of the file contains the MRS group name when applicable, and the name of the primary device, for example, *Tunnel_1_ST1_DM470.csv*. The file organizes data into the following columns:
 - time: The time stamp of the image.
 - deviceMacAddress: The MAC address of the device.
 - group: The MRS group name.
 - type: The trigger type
 - triggerIndex: The index of the trigger.
 - goodRead: TRUE indicates a Good-read, FALSE indicates a No-read.
 - readString: The read string. For an MRS group, this column contains the overall result string.



Note: For an MRS group, the image folder(s) contain images from all readers, and the CSV file contains trigger data from the primary reader.

Extract a Single Archive File

1. In the **Download Center**, click on the row of the archive you want to download to see its contents.

Actions	Title	State	Queued At	Updated At	Files Count
	4/8 10:47-10:50	Completed	4/8/22, 4:52 PM	4/8/22, 4:52 PM	1
<p><i>Download only one file at a time. Simultaneous downloads severely impact device performance. Download all partial zip archives (if created) before opening the '.zip' file. You may need a third-party utility to automatically combine partial archives.</i></p> <p> ei-data-export-20220408_1452-f61cd806-3697-4d56-a9c8-1686cc5feec2.zip</p>					

2. Click on the download icon to download the ZIP file.

Actions	Title	State	Queued At	Updated At	Files Count
	4/8 10:47-10:50	Completed	4/8/22, 4:52 PM	4/8/22, 4:52 PM	1
<p><i>Download only one file at a time. Simultaneous downloads severely impact device performance. Download all partial zip archives (if created) before opening the '.zip' file. You may need a third-party utility to automatically combine partial archives.</i></p> <p> ei-data-export-20220408_1452-f61cd806-3697-4d56-a9c8-1686cc5feec2.zip</p>					

The default download location depends on the browser you are using.


3. Navigate to the folder on your computer that contains your downloaded file, and extract the contents of the file.

Extract a Multi-Archive File


When the size of the archive exceeds 1 GB, EI Tunnel Manager creates multiple partial ZIP files from that archive.

Note: As the built-in Windows file extractor cannot handle partial ZIP files, you need to install 7Zip or a similar program to manage them.

1. In the **Download Center**, click on the row of the archive that you want to download to see its contents.

Actions	Title	State	Queued At	Updated At	Files Count
	2/13-2/14 Images + Triggers	Completed	2/14/22, 6:16 PM	2/14/22, 6:21 PM	6
<p><i>Download only one file at a time. Simultaneous downloads severely impact device performance. Download all partial zip archives (if created) before opening the '.zip' file. You may need a third-party utility to automatically combine partial archives.</i></p> <p> ↓ ei-data-export-20220214_1716-4e4d06cf-c77f-4054-baff-e2940a9c920f.z01 ↓ ei-data-export-20220214_1716-4e4d06cf-c77f-4054-baff-e2940a9c920f.z02 ↓ ei-data-export-20220214_1716-4e4d06cf-c77f-4054-baff-e2940a9c920f.z03 ↓ ei-data-export-20220214_1716-4e4d06cf-c77f-4054-baff-e2940a9c920f.z04 ↓ ei-data-export-20220214_1716-4e4d06cf-c77f-4054-baff-e2940a9c920f.z05 ↓ ei-data-export-20220214_1716-4e4d06cf-c77f-4054-baff-e2940a9c920f.zip </p>					

- Download each ZIP one at the time file by clicking on the download icon, and store them in the same location.

Actions	Title	State	Queued At	Updated At	Files Count
	2/13-2/14 Images + Triggers	Completed	2/14/22, 6:16 PM	2/14/22, 6:21 PM	6

Download only one file at a time. Simultaneous downloads severely impact device performance. Download all partial zip archives (if created) before opening the '.zip' file. You may need a third-party utility to automatically combine partial archives.

- [↓ ei-data-export-20220214_1716-4e4d06cf-c77f-4054-baff-e2940a9c920f.z01](#)
- [↓ ei-data-export-20220214_1716-4e4d06cf-c77f-4054-baff-e2940a9c920f.z02](#)
- [↓ ei-data-export-20220214_1716-4e4d06cf-c77f-4054-baff-e2940a9c920f.z03](#)
- [↓ ei-data-export-20220214_1716-4e4d06cf-c77f-4054-baff-e2940a9c920f.z04](#)
- [↓ ei-data-export-20220214_1716-4e4d06cf-c77f-4054-baff-e2940a9c920f.z05](#)
- [↓ ei-data-export-20220214_1716-4e4d06cf-c77f-4054-baff-e2940a9c920f.zip](#)

The default download location depends on the browser you are using.

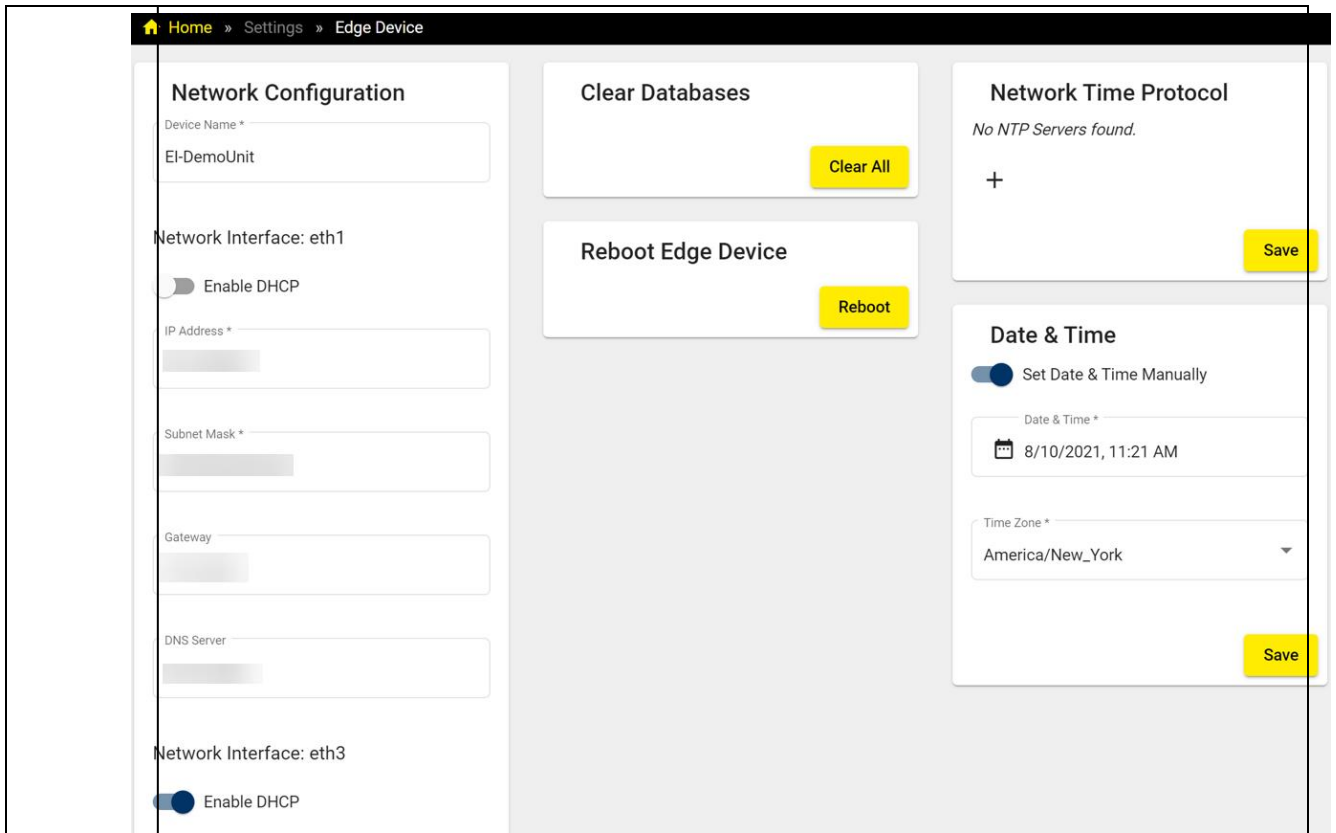
- Navigate to the folder on your computer that contains all the downloaded partial ZIP files.
- Right-click on the file with ZIP extension.
- Click on the ZIP file extractor.
- Click on **Extract to** to merge all partial files.

Settings

The Settings application allows you to configure your Edge Device, set up MQTT and other IoT connections, enable or disable the DataMan WebHMI pages of your connected devices, and upgrade your device firmware.

Edge Device

The Edge Device page shows the network configuration and allows editing and saving the network settings of the EI Tunnel Manager device.



Section	Item	Description
Network configuration	Device Name	The name of the EI Tunnel Manager device.
	Enable DHCP	To enable using DHCP protocols instead of static protocols toggle the switch.
	IP Address	The IP Address of the EI Tunnel Manager device.
	Subnet Mask	The Subnet Mask of the EI Tunnel Manager device. Note: Do not set more than one network port to the same subnet mask.
	Gateway	The Gateway of the EI Tunnel Manager device.
Clear databases	You can clear the device lists, data, and images from the EI Tunnel Manager device, and create a new state. Note: Clear database option is only available with Admin level clearance.	
Reboot Edge device	You can reboot the Edge device with the Reboot Edge device option.	

The screenshot displays the 'Edge Device' settings page. On the left, there are two network configuration sections: 'Network Interface: eth1' and 'Network Interface: eth3'. Each section includes a toggle for 'Enable DHCP', an 'IP Address *' field, a 'Subnet Mask *' field, a 'Gateway' field, and a 'DNS Server' field. In the center, there are two action buttons: 'Clear Databases' with a 'Clear All' button and 'Reboot Edge Device' with a 'Reboot' button. On the right, there are two more sections: 'Network Time Protocol' showing 'No NTP Servers found.' with a '+' button and a 'Save' button; and 'Date & Time' with a 'Set Date & Time Manually' toggle, a 'Date & Time *' field showing '8/10/2021, 11:21 AM', a 'Time Zone *' dropdown menu set to 'America/New_York', and a 'Save' button.

Section	Item	Description
Network time protocol		<p>You can sync the time between the EI Tunnel Manager device and an NTP server. To Add New Address enter IP address of the NTP Server then click Save.</p>
Date and time		<p>Toggle Set Date and Time manually to specify the date, time and the time zone. For more information see Date & Time Range Filter on page 1.</p>

Setting up the NAT

Network address translation (NAT) remaps IP address spaces into other IP address spaces by modifying network address information in the IP header of information packets. Scroll down for the NAT option.

To set up the NAT:

1. Make sure that the Default Gateway of the DataMan readers is the IP address of the TM network port they are connected to.

- Set the switch to enable NAT Settings.

Network Address Translation (NAT)

Enable

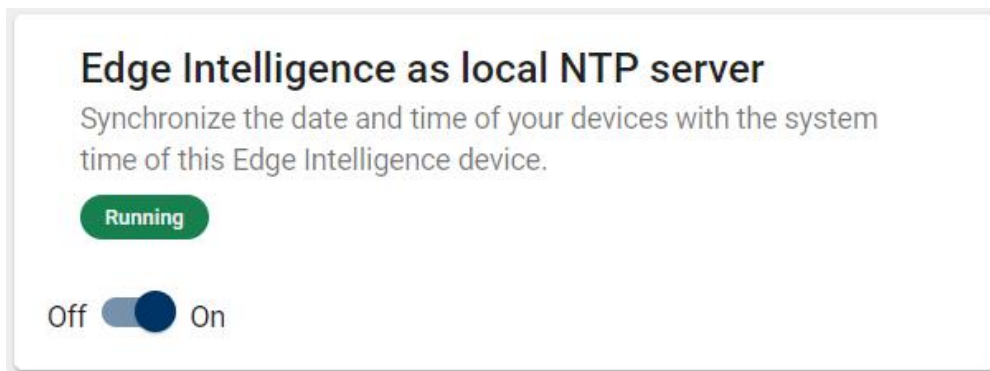
+

- Click the + symbol to Add New Mapping.
- Set the reader IP address as the Internal IP.
- For the External IP, enter an available IP address you want to map to the reader.
- Click Save.

NTP Server Function

The EI Tunnel Manager device can act as a Network Time Protocol (NTP) server. NTP is an internet protocol for synchronizing clocks on a network to within a few milliseconds of universal coordinated time (UTC).

In the **Settings** menu, click on the **Edge Device** tab. Set the switch to **On** to enable NTP server and synchronize the date and time of your devices with the system time of EI Tunnel Manager.



MQTT Forwarding

The **MQTT Forwarding** page of the **Settings** application allows you to set up network connections for forwarding to the IoT devices. You can configure MQTT, SSL/TLS, Sparkplug, and AWS settings on the **MQTT Forwarding** page.

[Home](#) » [Settings](#) » [MQTT Forwarding](#)

[Upload Certificate](#) [Upload Private Key](#) [Upload Bundle](#) [Save](#)

MQTT Connection Parameters

Enable MQTT Forwarding

Enabled Disabled

Broker IP Address or URL

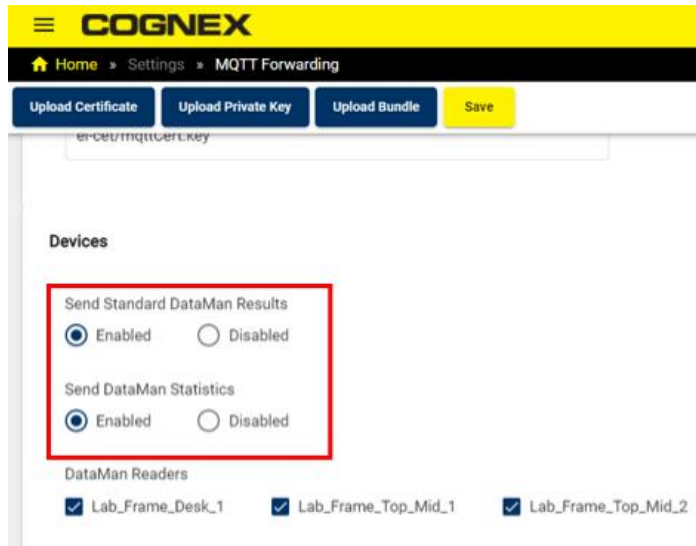
Broker Port

Topic

MQTT_Test

You can also upload certificates, private keys, or bundles using the buttons at the top. It is possible to upload a *.crt*, *.csr*, *.pem*, or *.key* file.

By enabling **Send Standard DataMan Results** and **Send DataMan Statistics**, you send results and statistics from the DataMan devices.



You can select readers to forward data from under **DataMan Readers**.

To implement any changes you make, click **Save**.

See below about the forwarded data for **Standard DataMan Results** and **DataMan Statistics**:

Standard DataMan Results		DataMan Statistics
Decode Results <ul style="list-style-type: none"> • Decode Time • Image Index • Is Good Read • Module Size 	Read Setup Index Read String Result Index Source Device Mac Address Source Device Name Device Mac Address Encoder End Tick Encoder Start Tick	Good Read Count No read Count Passed Validation Count Failed Validation Count Buffer Overflow Count Missed Trigger Count Trigger Overrun Count Timestamp Device Mac Address
Symbology <ul style="list-style-type: none"> • Angle • Center • Id • Name • Size 	Group Timestamp Trigger End Time Trigger Index Trigger Start Time Trigger Time Unique Id	
Process Control Metrics <ul style="list-style-type: none"> • Standard 		
Validation <ul style="list-style-type: none"> • Error Code • Error Position • Error Text • Is Read String Valid 		

MQTT Connection Parameters

The **MQTT Connection Parameters** section of the page allows you to configure MQTT forwarding.

MQTT Connection Parameters

Enable MQTT Forwarding

Enabled Disabled

Broker IP Address or URL

Broker Port

Topic

MQTT_Test

Username

Cognex

Password (Optional)

Keepalive Interval (s)

10

QoS Level

0 - at most once 1 - at least once 2 - exactly once

To enable MQTT forwarding, click **Enable**.

Provide the

- **Broker IP Address or URL,**
- **Broker Port,**
- **Topic name,**
- **Username,**
- the optional **Password,**
- **Keepalive Interval (s)**

Define the QoS Level you want, then click on **Save** at the top of the page to apply your changes.

SSL/TLS

The **SSL/TLS** section of the page allows you to configure SSL/TLS connections.

SSL/TLS

Enable SSL/TLS

 Enabled Disabled

Certificate Authority (CA) Endpoint

www.ssl.com

Certificate File Path

ei-cet/mqttCert.pem

Private Key File Path

ei-cet/mqttCert.key

To enable SSL/TLS forwarding, click **Enable**.

Provide the **Certificate Authority (CA) Endpoint**, **Certificate File Path**, and **Private Key File Path**, then click on **Save** at the top of the page to apply your changes.

Sparkplug Settings

The **Sparkplug Settings** section of the page allows you to configure Sparkplug formatting.

Sparkplug Settings

Enable Sparkplug Formatting

 Enabled Disabled

Group ID

Cognex

Custom Node ID (Optional)

To enable Sparkplug formatting, click **Enable**.

Provide the **Group ID** and **Custom Node ID**, then click on **Save** at the top of the page to apply your changes.

AWS IOT Settings

The **AWS IOT Settings** section of the page allows you to configure AWS forwarding.

AWS IOT Settings

Enable AWS Forwarding

 Enabled Disabled

AWS Client ID

EI-AWS-MQTT-Client

To enable AWS formatting, click **Enable**.

Provide the **AWS Client ID**, then click on **Save** at the top of the page to apply your changes.

The **Devices** section of the page allows you to select the **Result Input Source** and the readers you want to apply your changes to.

Devices

Result Input Source

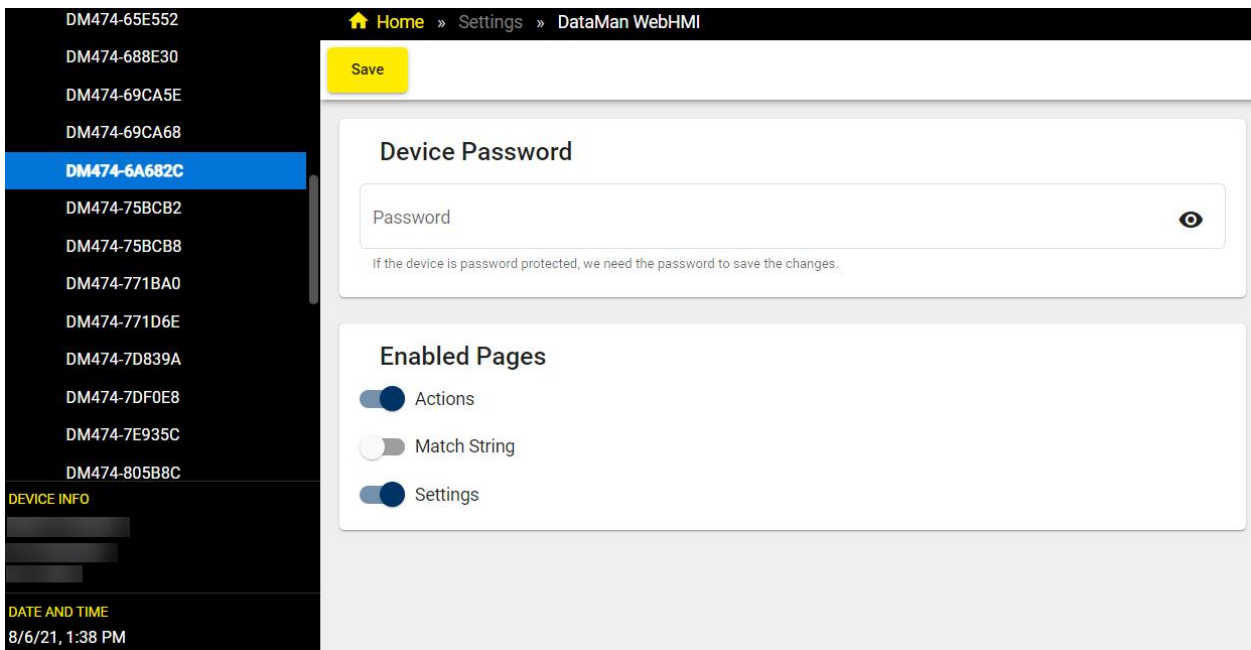
- Standard DataMan result
- Scripted DataMan result (requires JSON format v2.1)

DataMan Readers

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

DataMan WebHMI

The **DataMan WebHMI** page of the **Settings** application allows you to enable or disable the pages displayed on the individual device DataMan WebHMI interfaces that are accessible through the **DataMan** page of the **Multi-Reader Configuration** application.



Select the device for which you want to change the displayed DataMan WebHMI pages from the device list on the left side of the page. The device information for the selected device appears under the list.

If the selected device is password protected, provide the password in the **Device Password** section of the page, otherwise you will not be able to save your changes.

You can enable or disable the following DataMan WebHMI pages for the selected device in the **Enabled Pages** section of the page:

- **Actions**
- **Match String**
- **Settings**

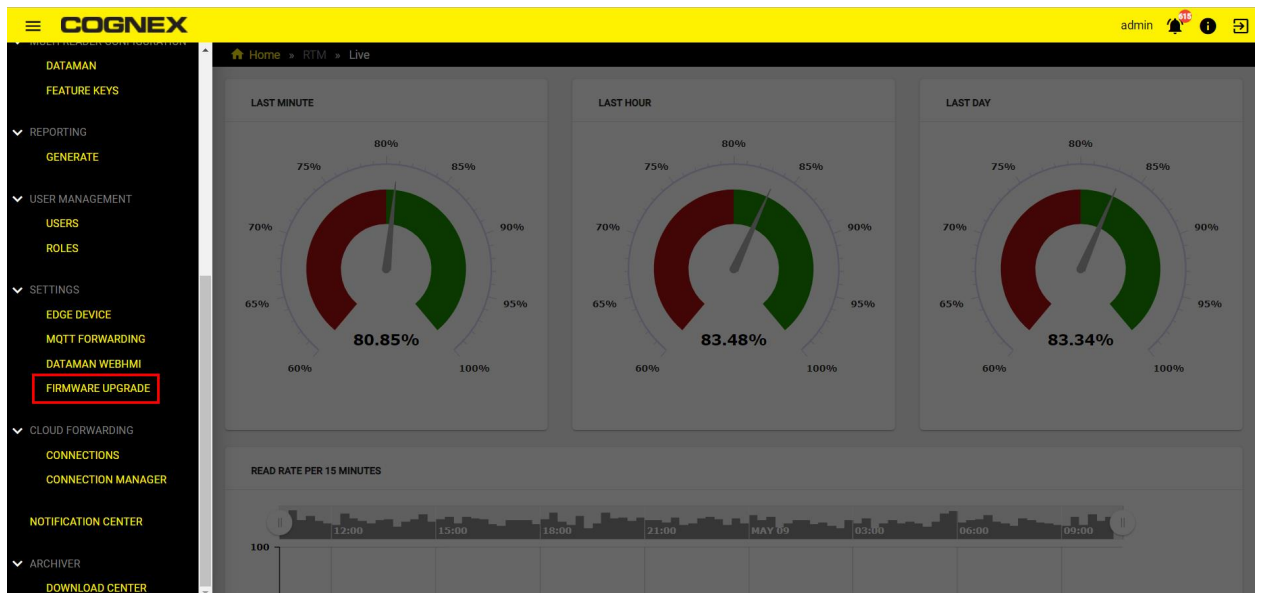
Click **Save** at the top of the page to apply your changes.

Firmware Upgrade

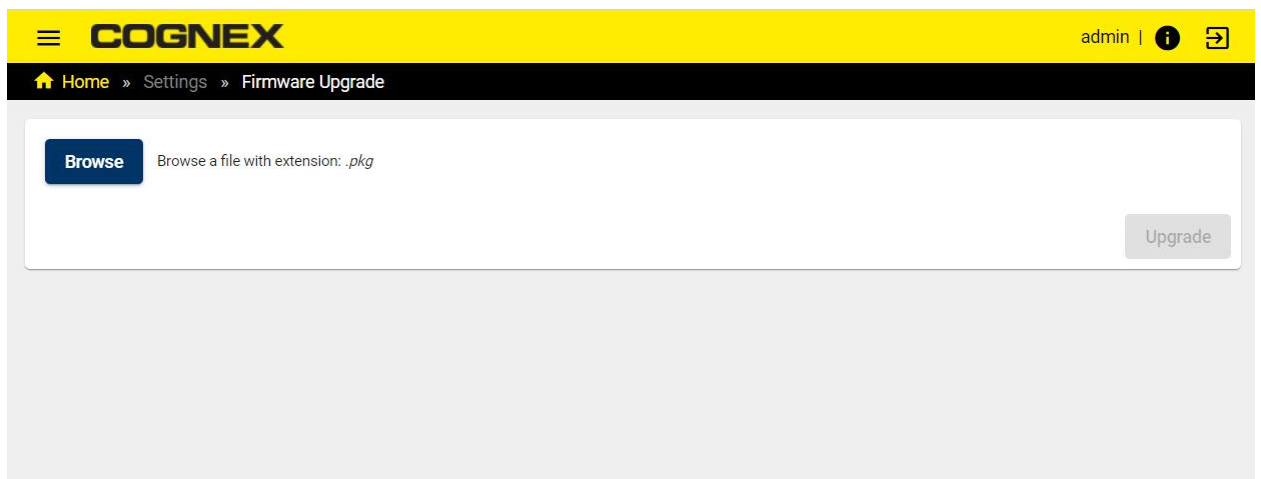
The **Firmware Upgrade** page of the **Settings** application step allows you to upload new firmware packages for upgrading device firmware.

If the EI Tunnel Manager unit is on version 1.2.1 or later, you can upgrade the EI Tunnel Manager firmware through the user interface by performing the following steps:

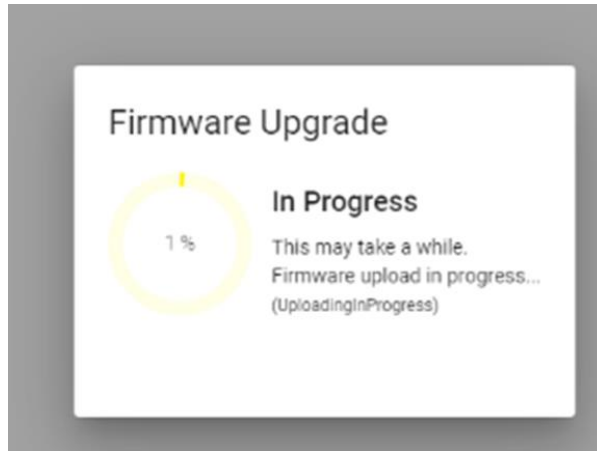
1. Make sure you are on the same network as EI Tunnel Manager Internal Ethernet port. The IP address of the Internal Ethernet port is in the form of 192.168.1.X.
2. Connect to the EI Tunnel Manager Internal Ethernet port. For more information, see [Connecting the EI Tunnel Manager](#).
3. Open a web browser and type the IP address of the EI Tunnel Manager unit into the address bar. The default static IP address is 191.168.1.100. The EI Tunnel Manager user interface opens up.
4. Navigate to **Settings > Firmware Upgrade** in the EI Tunnel Manager navigation pane.



5. Click on the **Browse** button and select the latest firmware version available for download on the Cognex website. The firmware is a *.pkg* format file.



6. Click on the **Upgrade** button and wait for upgrade to complete.



If the EI Tunnel Manager unit is on version 1.1.1, you can upgrade EI Tunnel Manager firmware through DataMan Setup Tool. For more information, see [Software Update](#).

User Management

The **Roles** page allows an admin level user to create roles and define which EI features those roles have access to. The **User** page allows an admin level user to create users and assign them roles.

Users

The Users page allows creating new users and assigning Roles to them.

☰ **COGNEX**
cognex | ⓘ 🗄️

🏠 Home » User Management » Users

Create User

Actions	Username ↑	Roles
✎ 🗑️	admin	Admin
✎ 🗑️	cognex	Admin
✎ 🗑️	engineer	Engineer
✎ 🗑️	operator	Operator

Items per page: 10 ▾
1 – 4 of 4
⏪ ⏩

Item	Description
Create User	Brings up the pop-up window to add a new user.
User management table	Table listing the existing users, the assigned Username and roles.

The Create user action is available on the top ribbon. Set the following options for each user:



Create User



Item	Description
Username	The username of the user for logging in.
Role	The role of the user: <ul style="list-style-type: none"> • Admin • Engineer • Operator
Password	The password of the user for logging in.
Confirm Password	Reenter the password.



Note: A user with admin rights can also edit the same options for each user by clicking the **Edit** button.



The Users page lists the existing users. Edit or delete an existing user by clicking the appropriate icon.

Actions







Icon	Description
	Click Edit to edit the settings of a user.
	Click Delete to delete a user.

Roles

This page allows admin level users to create new roles and grant access to certain applications.

Home » User Management » Roles

- Admin 
- Engineer 
- Operator 
- +

Role Name *

All application claims

- Access to ADWS app
The user has access to the ADWS application.
- > Access to Customer Acceptance Test App
The user has access to the Customer Acceptance Test application.
- Access to Ignore Codes app
The user has access to the Ignore Codes application.
- > Access to Multi-Reader Configuration App
The user has access to the Multi-Reader Configuration application.
- > Access to Reporting app
The user has access to the Reporting application.
- > Access to RTM App
The user has access to the Real-Time Monitoring application.

Item	Description
Roles	List of roles.
Accesses	List of accesses for the specified role.

The following predefined users are available by default:

Note: After creating the user profiles, always change the default password to avoid security risks.

User	Password	Permission
admin	BnthWWSD	Has access to all apps and features.
engineer	TaRDpKVx	Has access to all apps and features.
operator	SxtXGmxs	User with read-only rights. The operator does not have access to the Multi-Reader Configuration app and the Settings.

Single Sign-On

EI Tunnel Manager supports Single Sign-On (SSO). Single Sign-On is a session and user authentication service that permits you to use a single set of login credentials. For example, you can set up a username and password that allows you to access multiple applications.

When choosing SSO on the EI Tunnel Manager login page, you are directed to the authentication service login page where you provide your credentials. Once your credentials are validated, you are redirected back with the security token to EI Tunnel Manager and logged in.

To configure this process on EI Tunnel Manager, you have to configure roles and map these roles to an existing one in the customer identity provider. Then, you have to setup EI Tunnel Manager as a client and configure return URLs. For more information, see [Role Mapping on page 69](#).

The Single Sign-On application of the EI Tunnel Manager provides additional analytics options over the Performance Monitoring page in the RTM application.

Identity Provider Configuration

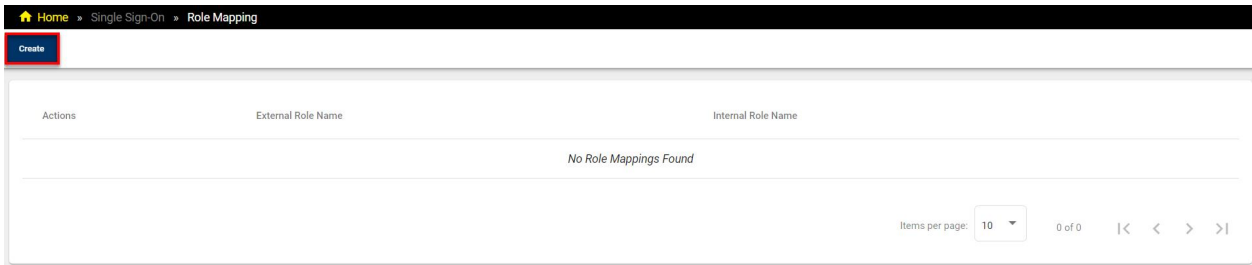
To set up SSO in EI Tunnel Manager, you log in to EI Tunnel Manager using the admin credentials. The **Identity Provider Configuration** page of the **Single Sing-On** application allows you to enter the details of your configuration to setup the login with the existing environment.

The screenshot shows the 'Identity Provider Configuration' page. At the top, there is a breadcrumb trail: Home > Single Sign-On > Identity Provider Configuration. Below this, there are five text input fields, each with an asterisk indicating it is mandatory: 'Authority *', 'Client ID *', 'Client Secret *', 'Role Claim Type *', and 'User Name Claim Type *'. A 'Save' button is located at the bottom right of the form area.

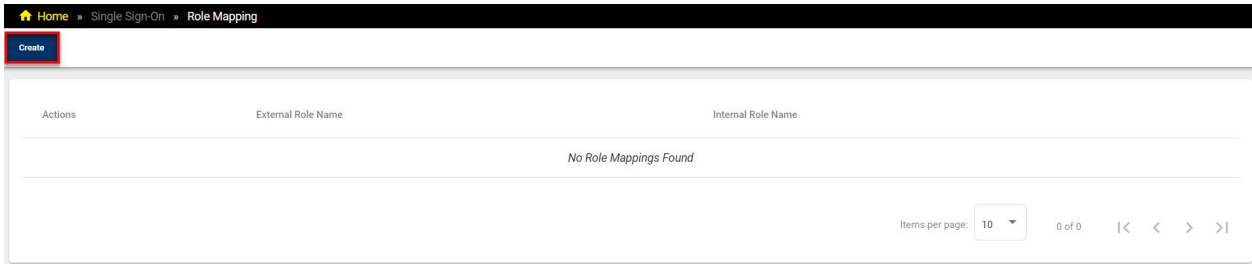
After filling in the **Authority**, **Client ID**, **Client Secret**, **Role Claim Type**, and **User Name Claim Type** mandatory fields, click on **Save** to proceed.

Role Mapping

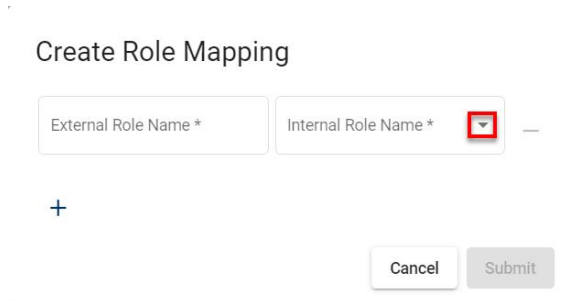
The **Role Mapping** page of the **Single Sign-On** application allows you to create external roles and map them to the internal roles that are system-provided default roles.



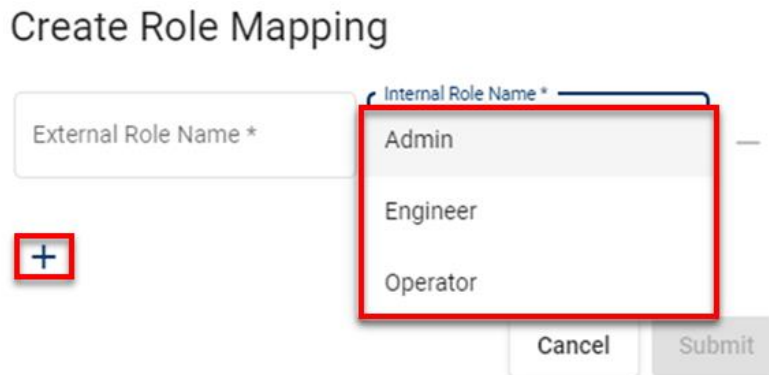
Click on **Create** on the top left corner of the **Role Mapping** page to create a role mapping.



The **Create Role Mapping** pop-up appears.



Fill in any external role name in the **External Role Name** field and select an **Internal Role Name** from the default options.



Click on the **+** to add more role mappings.

Create Role Mapping

External Role Name * Internal Role Name * —

External Role Name * Internal Role Name * —

+

After filling in the given fields you can click **Submit** to create the role mappings. The role mappings, now, appear.

Home » Single Sign-On » Role Mapping

Create

Actions	External Role Name	Internal Role Name
<input style="border: 2px solid red;" type="button" value="✎"/> <input style="border: 2px solid red;" type="button" value="🗑️"/>	Admin	Admin
<input type="button" value="✎"/> <input type="button" value="🗑️"/>	Someone	Engineer

Items per page: 10 | 1 - 2 of 2 | < >

You can edit or delete any role mapping from the list by clicking on the corresponding button icons.

If you click on the **Pencil** icon, the **Edit Role Mapping** pop-up appears.

Edit Role Mapping

External Role Name * Internal Role Name *

To save your changes after editing, click on **Submit**.

Certificates

The **Certificates** page of the **Single Sign-On** application allows you to upload a self-signed certificate to use to establish the https connection. The **Certificates** page lets you ensure a secure authentication when using EI Tunnel Manager.

Home » Single Sign-On » Certificates

Upload

Friendly Name	File Name	Password Protected	Valid From	Valid To	Issuer	Self Signed
	AutoGeneratedSelfSigned.pfx	✓	Nov 2, 2022, 1:33:51 PM	Nov 3, 2023, 1:33:51 PM	CN=Cognex-EI-SelfSigned	✓

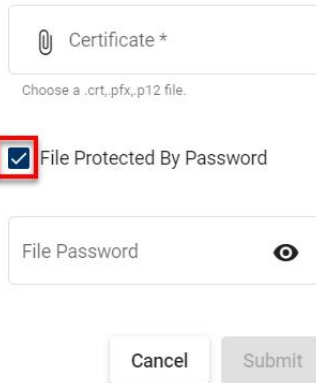
Items per page: 10 | 1 - 1 of 1 | < >

If you do not already have a certificate, EI Tunnel Manager automatically creates one for you.

To add a certificate, click on **Upload** on the top left corner of the **Certificates** page.

The **Upload Certificate** pop-up appears.

Upload Certificate



Certificate *

Choose a .crt, .pfx, .p12 file.

File Protected By Password

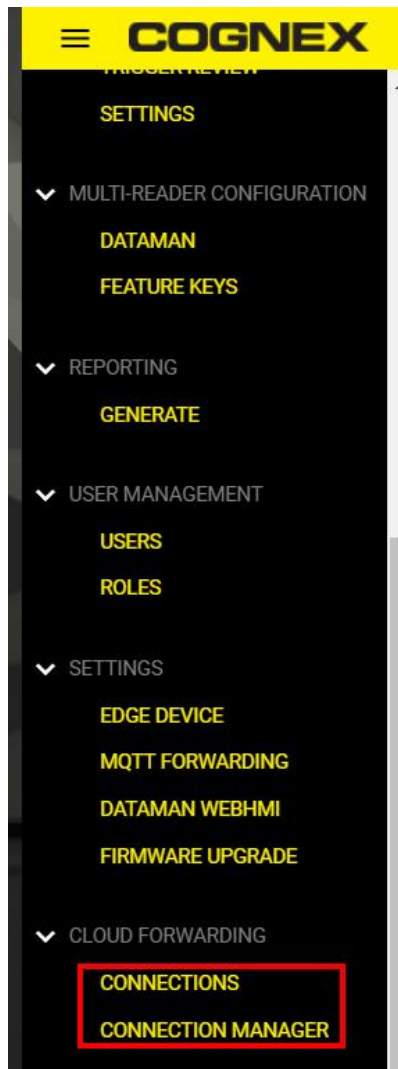
File Password

Cancel Submit

You can also check the **File Protected By Password** checkbox to create a password for the uploaded file.

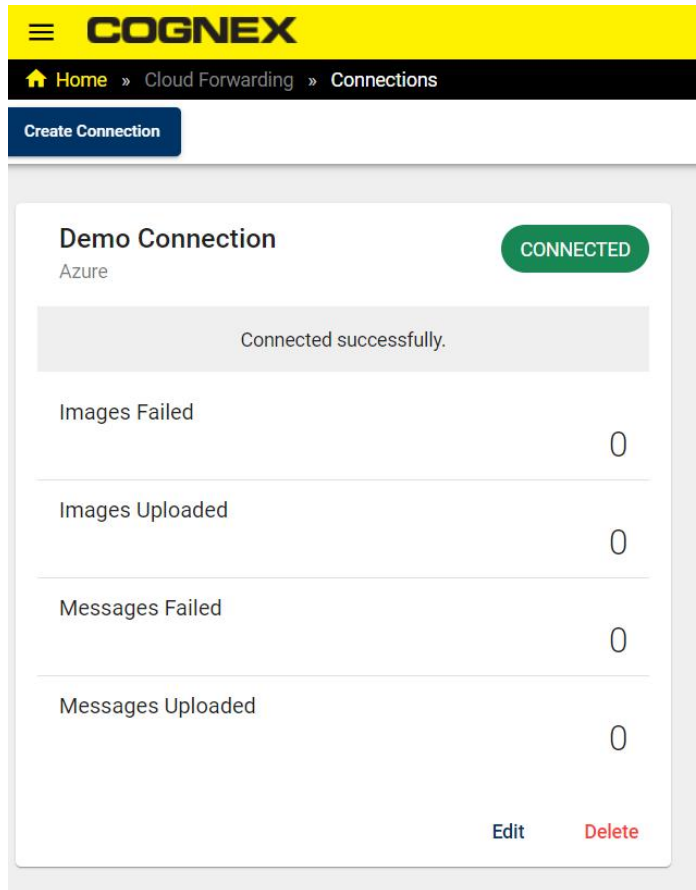
Cloud Forwarding

The Cloud Forwarding application allows you to configure your cloud connections and manage the forwarded data. The Cloud Forwarding application contains two pages: Connections and Connection Manager.



Connections

The **Connections** page of the **Cloud Forwarding** application displays the current status of the cloud connection and total number of images and messages uploaded or failed.



To edit the connection, click on **Edit**. The **Edit Connection** pane opens up:

Edit Connection

Connection Name *
Demo Connection

Destination Type *
Azure

Connection Type *
Connection String

Connection Settings

Azure Connection String *
HostName=EI-Demo-IOTHub.azure-devices.net;DeviceId

Cancel Save

- The **Connection Name** field shows the name of the connection.
- The **Destination Type** dropdown shows where the data is forwarded to.
- The **Connection Type** dropdown shows the connection type, such as Connection String, SAS Token, x509 Certificate.
- In the **Azure Connection String** field you have to enter details for the specific connection type and destination.

Connection Manager

The **Connection Manager** page of the **Cloud Forwarding** application is for specifying the data to forward from each device.

Primary	Name	IP Address	Model	Firmware Version	Password	Forward Good Read Trigger	Forward Good Read Images	Forward No Read Triggers	Forward No Read Images	Forward Validation Failure Triggers	Forward Validation Failure Images	State
						<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	In Local Subnet
						<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	In Local Subnet
						<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	In Local Subnet

To select the data to forward from each device, switch on the toggle. In this example, **Good Read Trigger, No Read Triggers, No Read Images, Validation Failure Triggers, Validation Failure Images** are chosen to forward for the first device in the list.

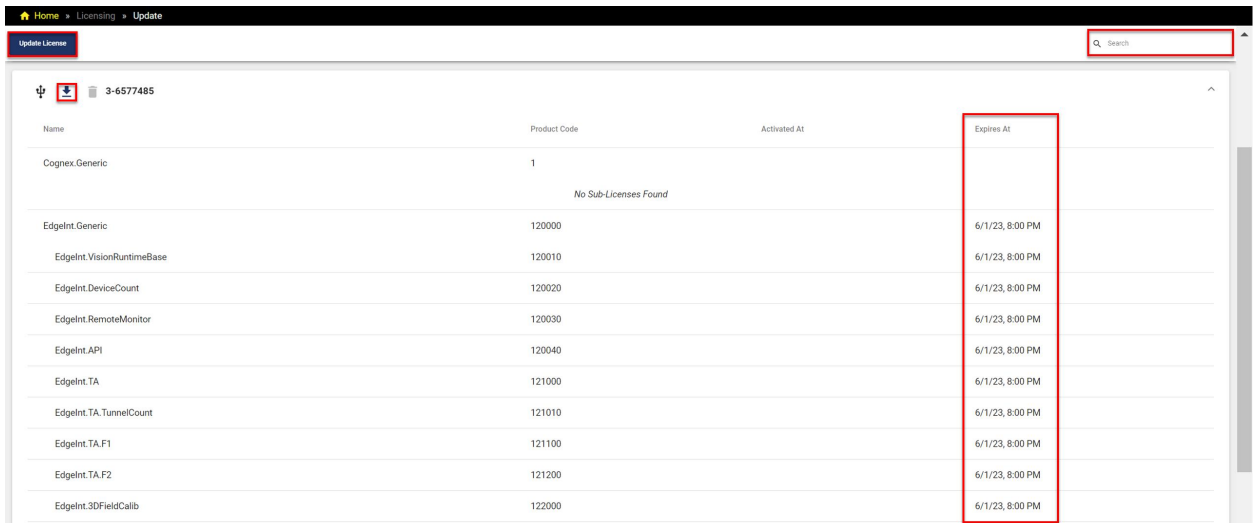
Licensing

The **Licensing** application of the EI Tunnel Manager user interface allows you to update your licenses using the **Update** page.

Update

The **Update** page of the **Licensing** application allows you to update your licenses.

1. Download the license request file by clicking on the **Download License Request File** icon from the license table.



2. Email the generated license request file with the *.WibuCmRaC* extension to Cognex Support: TSupport@cognex.com.
3. Cognex Support emails the license file with the *.WibuCmRaU* extension back to you.

- Click on **Update License**. Select the file you have received with the *.WibuCmRaU* extension and click on **Submit**.

Update License

Select license update file (.WibuCmRaU)

License *



Required field.

Cancel

Submit

- Check if the **Expires At** column updates automatically to the new license expiration date, to verify successful license update.

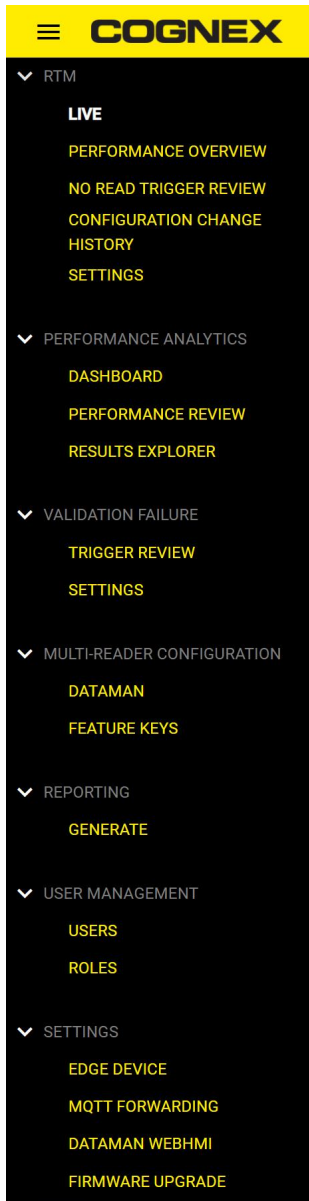
You can search for any information on the page by using the **Search** field.

Main Elements of the User Interface

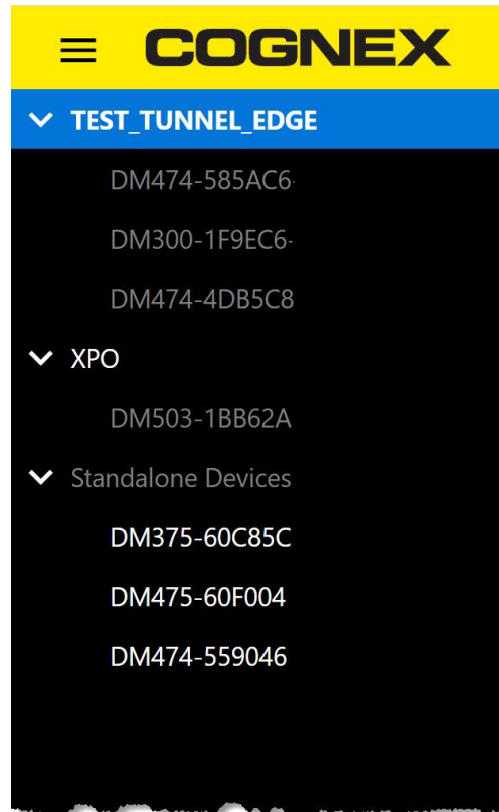
The yellow top ribbon appears on all pages, and provides the following features:

Main menu: Click on the **Menu icon** in the upper left corner to open the navigation pane. Use the tree to navigate between the available apps and their pages.





Device tree



The device tree shows you what devices, readers, and reader groups are on the network. Click on the group or standalone reader to view the live data collected from it. IDs of the individual readers within a group appear grey, but the individual readers can not collect data separately within a group. The bottom of the pane displays information about the selected group and the date and time.

The ribbon displays the type of the user signed in.



To reach the Documentation of EI Tunnel Manager, Network Interfaces, and Components, click the **i (info) icon** to open the **About section pop-up window**.

About El-DemoUnit

Documentation

[Click here to open documentation.](#)

Network Interfaces

Name	Operational	MAC Address	Address Type	IP Address	Subnet Mask	Gateway	DNS Server	Domain
	✓		Static					(none)
	✓		DHCP					(none)
	✓		Static					(none)

Components

Name	Version
Frontend	1.9.0

Close

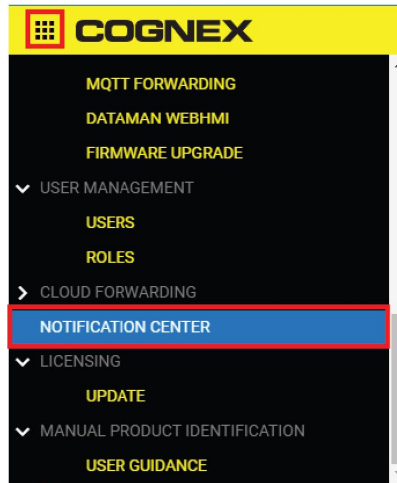
The **Log out button** is in the upper right corner:



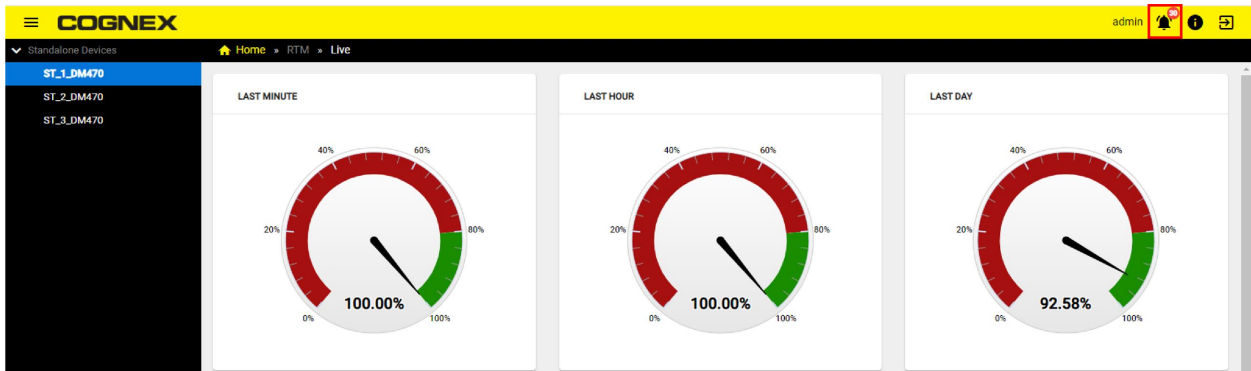
Notification Center

The Notification Center allows you to filter and sort the notifications that El Tunnel Manager sends you. You can access the Notification Center from the main menu or from the notification bell icon.

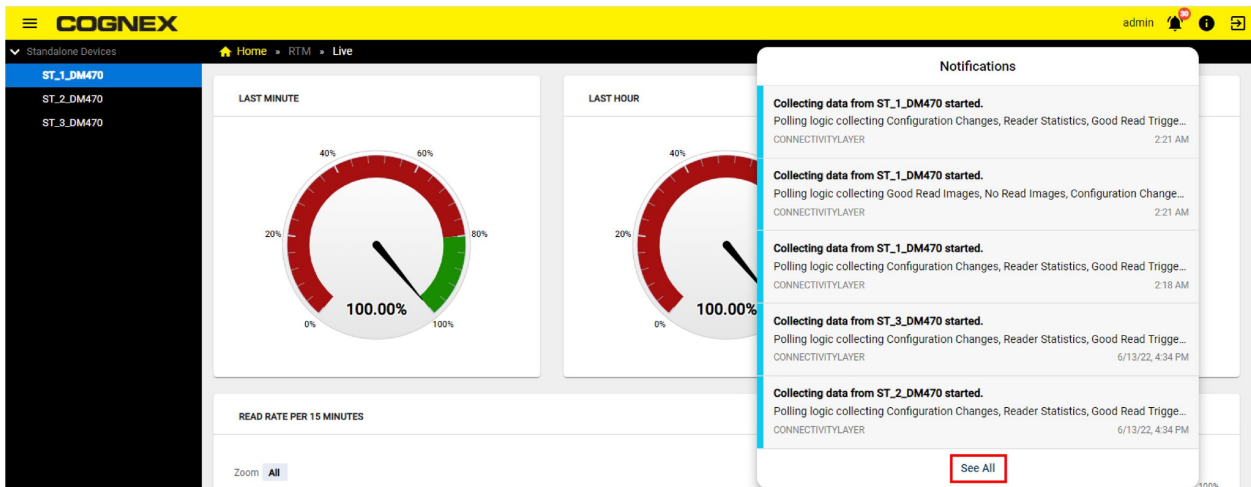
For access from the main menu, click on the **Menu** icon and select **Notification Center**.



For access from the notification bell, click on the bell icon in the upper right corner of the home page to see the latest notifications.



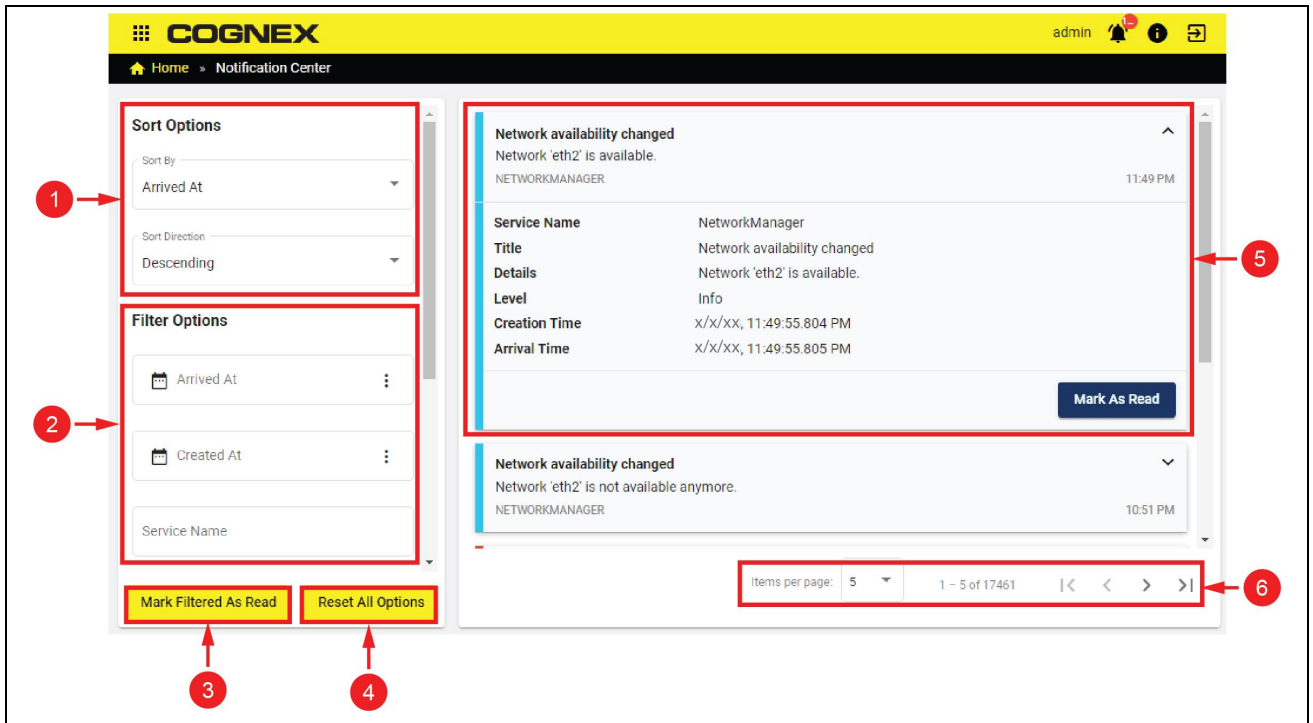
Click on the **See All** button to open the Notification Center.



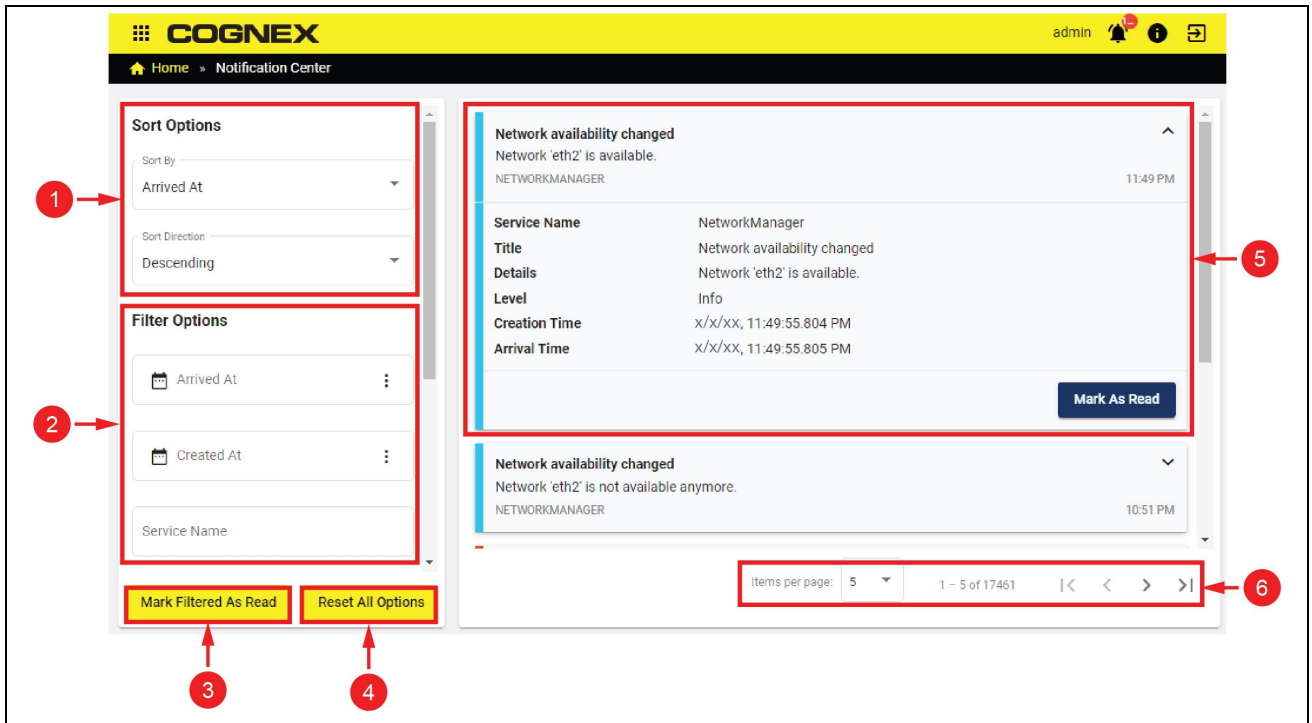
Notification Center Features

The screenshot shows the COGNEX Notification Center interface. It features a yellow header with the COGNEX logo and user information (admin). The main content area is divided into a left sidebar and a main notification list. The sidebar contains 'Sort Options' (Sort By: Arrived At, Sort Direction: Descending) and 'Filter Options' (Arrived At, Created At, Service Name). Below the sidebar are 'Mark Filtered As Read' and 'Reset All Options' buttons. The main area displays two notifications: 'Network availability changed' (Network 'eth2' is available) and 'Network availability changed' (Network 'eth2' is not available anymore). A 'Mark As Read' button is present for the first notification. At the bottom right, there is a pagination control showing 'Items per page: 5' and '1 - 5 of 17461'.

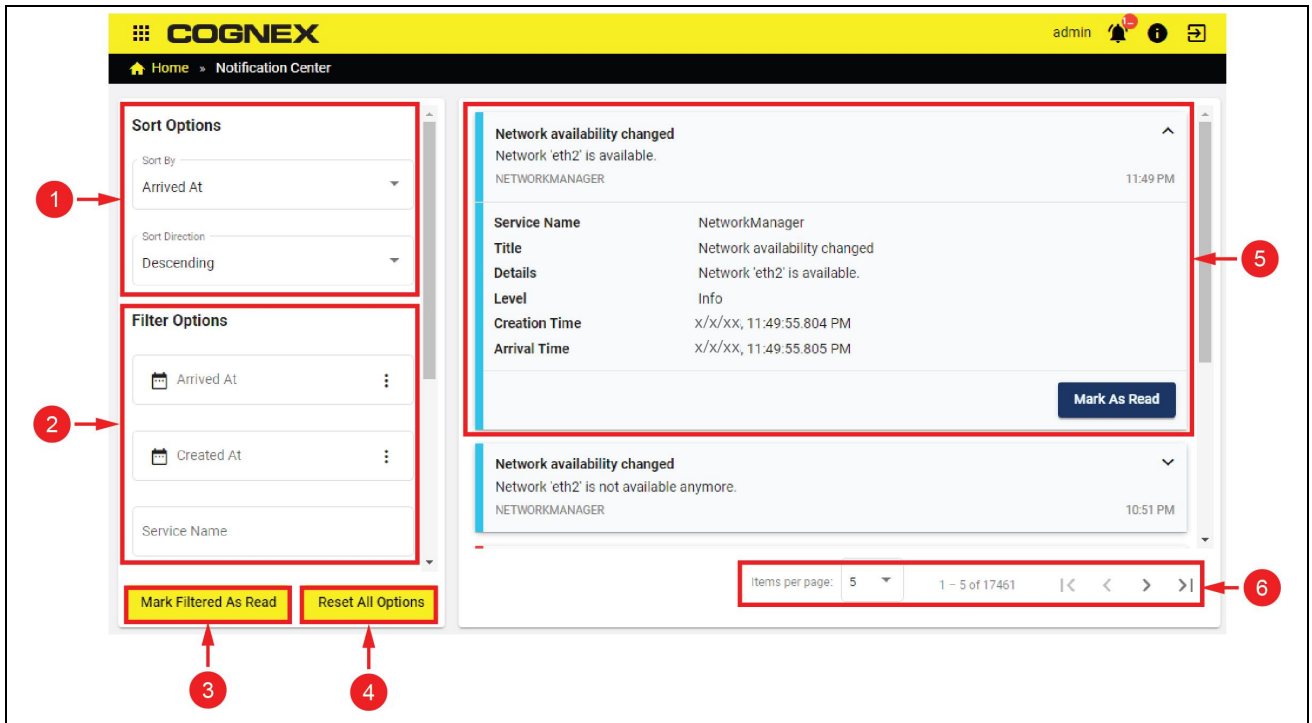
Number	Element	Description
1	Sort Options	Sort By: Arrived At, Sort Direction: Descending
2	Filter Options	Arrived At, Created At, Service Name
3	Mark Filtered As Read	Button to mark filtered items as read
4	Reset All Options	Button to reset all filter and sort options
5	Notification Card	Network availability changed: Network 'eth2' is available. Includes details like Service Name, Title, Level, Creation Time, and Arrival Time.
6	Pagination	Items per page: 5, 1 - 5 of 17461, navigation arrows



<p>1</p>	<p>Sort Options</p>	<p>Click on the Sort By dropdown to sort your notifications according to the following options:</p> <ul style="list-style-type: none"> • Service Name: Sorts the notifications according to service name of the notifications. • Created At: Sorts the notifications according to the date of creation. • Level: Sorts the notifications according to the level of the notification (Info, Warning, Error, or Critical). • Is Read: Sorts the notifications according to whether the notification is read. • Arrived At: Sorts the notifications according to the date of arrival. <p>Click on Sort Direction dropdown to determine the order of the notifications:</p> <ul style="list-style-type: none"> • Ascending • Descending
----------	---------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



2	Filter Options	<p>You can filter the notifications by using the following filter options:</p> <ul style="list-style-type: none"> • Arrived At: When the notification arrived in the Notification Center. • Created At: When the notification is created. • Service Name: Type in the Service Name of the notification. • Title: Type in the title of the notification. • Details: Type in the details of the notification. • Is Read: Filters your notifications according to the status of the notification (Read/Unread). • Notification Level: Filters according to level (Info, Warning, Error, or Critical).
3	Mark Filtered as Read	Mark the filtered notifications as read.
4	Reset All Options	Clears the selected Sort and Filter options.



5	Notification	Click on the notification to see the details. Click on the Mark as read button to mark the notification as read.
6	Paging buttons	Click on the Items per page dropdown to choose the number of notifications showed on the screen. Click on the arrows to turn pages between the notifications.

Notification Levels

The Notification Center displays four levels of notifications:

- **Info:** Updates about general processes. No action is required.
- **Warning:** Caution, your process can be halted. You have to resolve the issues in the notifications before continuing.
- **Error:** Blocks your process. You have to resolve the issues in the notifications before continuing.
- **Critical:** Your process is no longer working. You have to resolve the issues in the notifications before continuing.

Notification List

Service Name	Event	Notification Level	Title	Message
ALERT	When an alert gets triggered.	Info, Warning, Error	<Alert Name>	<Alert Description>


Service Name	Event	Notification Level	Title	Message
ARCHIVER	Archiving process started, collecting data.	Info	Collecting data for <existingProcess.Title>	Archiving process <existingProcess.Title> (ID: <processId>) has started collecting data.
	The zipping process started.	Info	Started <existingProcess.Title>	Archiving process <existingProcess.Title> (ID: <processId>) has been started.
	The zipping process finished.	Info	Finished <existingProcess.Title>	Archiving process <existingProcess.Title> (ID: <processId>) has been finished successfully.
	Archiving process cancelled.	Info	Cancelled <existingProcess.Title>	Archiving process <existingProcess.Title> (ID: <processId>) has been cancelled.
	Failed running the archiving process.	Error	Failed <existingProcess.Title>	Archiving process <existingProcess.Title> (ID: <processId>) has failed.
	Failed cancelling the archiving process.	Error	Failed to cancel <existingProcess.Title>	Archiving process <existingProcess.Title> (ID: <processId>) has been failed to cancel.
COGNAMER	CogNamer packet initiated reboot.	Warning	Packet initiated reboot	Reboot has been initiated on the EI Tunnel Manager box remotely via CogNamer. Wait until it boots up before applying any new modifications.
CONNECTIVITYLAYER	ConnectivityLayer started polling data from device.	Info	Collecting data from <_device.Name> started.	Polling logic collecting <requestedEvents> from the device.
	Could not log in to device to collect data.	Error	Could not login to device <_device.Name>	Polling logic failed to login to device.
	Could not connect to device to collect data.	Error	Collection stops for device <_device.Name>	Polling logic failed to connect to or get data from the device.


Service Name	Event	Notification Level	Title	Message
FILESTORAGE	FileStorage recovered from database errors.	Info	File save restored	Saving to the database has been recovered.
	Low free space is detected.	Error	Storage manager failure	Your SSD has reached critical storage limit. Please reboot the system to try and restore storage management. Call Cognex tech support if you see this error again.
FIRMWAREUPGRADE	Firmware upgrade started.	Info	Firmware upgrade	Firmware upgrade process has been started on the EI Tunnel Manager box.
	Firmware upgrade finished.	Info	Firmware upgrade	Firmware upgrade process has been finished. The EI Tunnel Manager box is going to be restarted soon. Wait until it boots up before applying any new modifications.
NETWORKMANAGER	The availability of one of network interfaces of the box changed.	Info	Network availability changed	Network <Network Name> is available.
	After network settings have been saved.	Warning	Reboot is initiated	Network setting changes were successfully saved. The system is going to be rebooted shortly.
	When someone reboots the box from the UI.	Warning	Manually initiated reboot	A reboot has been initiated on the EI Tunnel Manager box. Wait until it boots up before applying any new modifications.

Service Name	Event	Notification Level	Title	Message
MQTTFORWARDING	On updating MQTT settings.	Info	MQTT settings updated	Applying new MQTT connection settings. Failed connections will result in an error notification.
	On successful connection to MQTT server.	Info	Connection successful	Successfully connected to MQTT server.
	On unsuccessful connection to MQTT server.	Error	Failed to connect	<ul style="list-style-type: none"> • Connection accepted. • Attempted to connect with MQTT v3.1.1 but server rejected that protocol version. • Attempted to connect with Client ID 'EI00D0COGNEX' but server rejected that ID. • Network Connection made but the MQTT server is unavailable at <IP address>:<port>. • Server rejected username and password. Check user credentials on the MQTT Forwarding page. • Client is not authorized to connect to the MQTT server at <IP address>:<port>. • Failed to connect with MQTT Return Code 6.
	On disconnection with MQTT server.	Error	Unexpected MQTT disconnection	Unexpected disconnection from MQTT server. Attempting to reconnect.
	On failure to reconnect with MQTT server.	Error	Failed to connect	The connection attempt to the MQTT server at <IP address>:<port> failed due to a connection timeout. Automatically retrying.
TUNNELMANAGER	On license activation.	Info	License activated	The EI Tunnel Manager license has been activated.
	On license expiry.	Warning	License expired	The EI Tunnel Manager license has expired. Limited capabilities are available.

Cleaning and Maintenance

To clean the outside of the chassis, use a dry cleaning cloth.

 **CAUTION:** Do not clean EI Tunnel Manager products with liquids.

 **CAUTION:** Do not attempt to clean any EI Tunnel Manager product with harsh or corrosive solvents, including lye, methyl ethyl ketone (MEK) or gasoline.

Open Source Licenses

The table below shows the open source licenses used by EI Tunnel Manager:

angular-resize-event	MIT
angular2-moment	MIT
core-js	MIT
dateformat	MIT
daterangepicker	MIT
fullscreen	MIT
moment	MIT
ngx-daterangepicker-material	MIT
ngx-spinner	MIT
primeicons	MIT
rxjs	Apache-2.0
rxjs-compat	Apache-2.0
screenfull	MIT
socket.io	MIT
socket.io-client	MIT
zone.js	MIT
@amcharts/amcharts3-angular	Paid