

ET Tunnel Manager Reference Manual

2025 June 05
Revision: 2.2.0.50

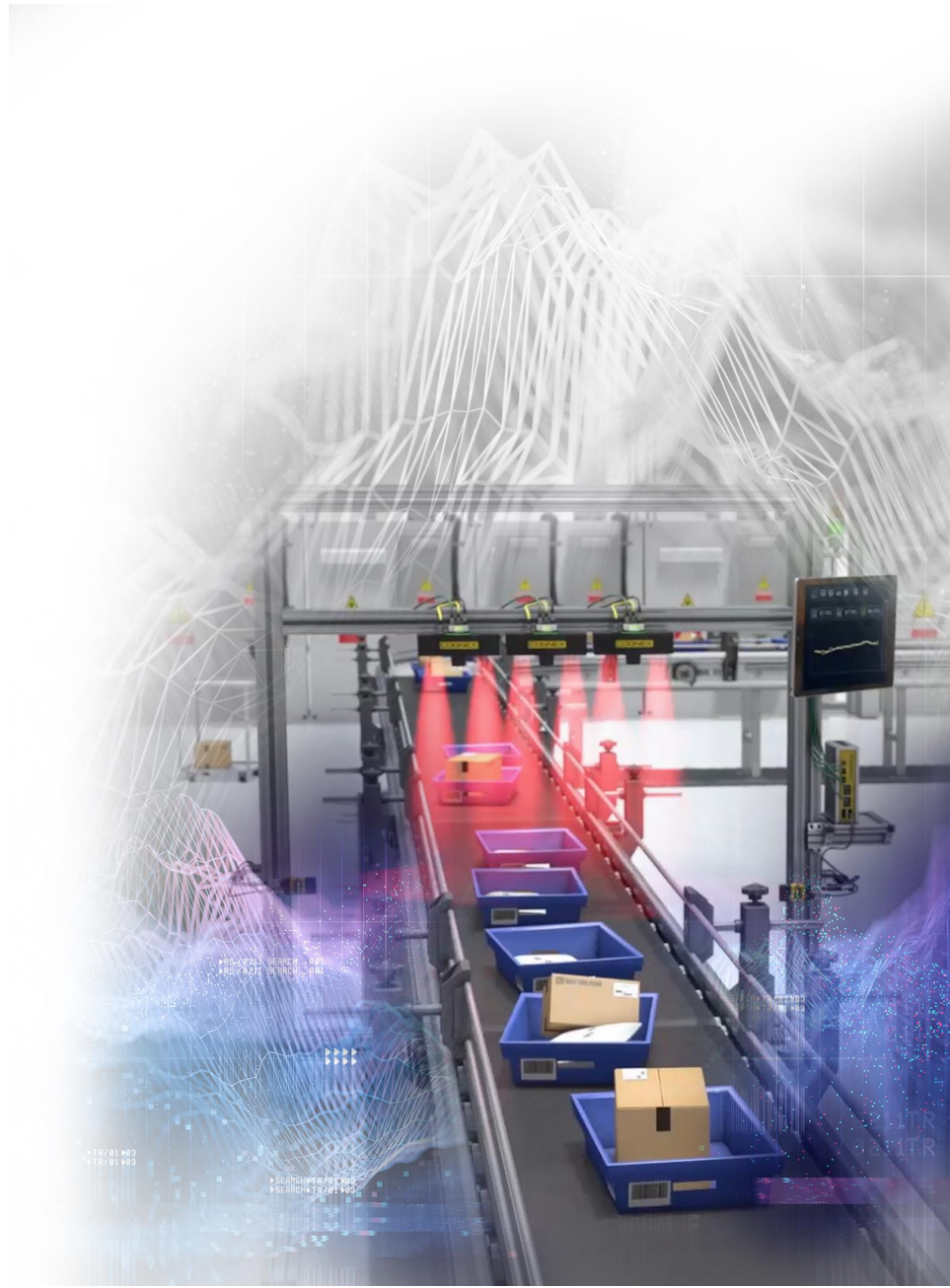


Table of Contents

Table of Contents	2
Legal Notices	4
Getting Started	5
About this Release	5
New features in Tunnel Manager 2.2	5
Enhancements and Changes	5
Logging In	7
EI Tunnel Manager Login Page	7
Default User Credentials	8
Discovering Devices on the Network	8
EI Tunnel Manager User Interface	10
About Pop-Up	10
Tunnel Analytics	11
Performance Dashboard	11
Live Dashboard	14
Result Browser	15
Events	32
Configuration Change History	32
Provisioning	35
DataMan	35
Remote Subnets	37
Device Management	38
DataMan	38
Other Devices	48
Feature Keys	51
Tunnel Setup	52
Dynamic Test	52
3D Field Calibration	64
Archiver	69
Download Center	69
Settings	73
Edge Intelligence	73
DataMan WebHMI	77
Firmware Upgrade	78
HTTPS	79
User Management	80
Users	80
Roles	82
Single Sign-On	83
Identity Provider Configuration	83
Role Mapping	84
Data Transfer	86
Data Forwarding	86
Notification Center	98

Notification Center Features	99
Notification Levels	102
Licensing	102
Update	102
Stitcher Settings	103
Troubleshooting	106
Remote Connection Troubleshooting	106
Enable Remote Access for Cognex Technical Support	107
Open Source Licenses	110

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 © 2025. 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.

Getting Started

EI Tunnel Manager, built upon the Cognex Edge Intelligence software platform, gathers data and analytics from vision tunnels for real-time insights into logistics operations. It provides tunnel analytics, setup and commissioning apps, and easy integration with on-premise and cloud-based data systems.

The EI Tunnel Manager is a web-based software that allows you to manage your tunnel assets with some key features as below:

Main Features	Key elements
Device Management	Large storage for multi-day images and results
	Network Address Translation (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	Reader results and metadata
	Built-in MQTT protocol (Ignition, cloud providers) and analytics
	Turnkey data connectivity to cloud-based systems (AWS, Azure)
Powerful Performance Monitoring tools	Real time performance with live dashboard
	Custom performance dashboards
	Browse tunnel trigger results and images with powerful queries and tagging
	Real time device configuration changes

About this Release

EI Tunnel Manager 2.2 includes updates to many existing applications and adds new features. This version also adds support for a new generation of Edge Intelligence hardware.

New features in Tunnel Manager 2.2

EI Tunnel Manager 2.2 adds the following new features:

- Support for the new EI-A3-TUNMGR- and EI-A9-TUNMGR-series devices.
- Image stitching across devices to allow single-image per side output on premium systems (add-on license).
- Pass-through access to web HMIs, including:
 - DataMan readers
 - 3D-A1000 dimensioning units
 - Mettler-Toledo TLD-950 dimensioning units
 - Remote Desktop

Enhancements and Changes

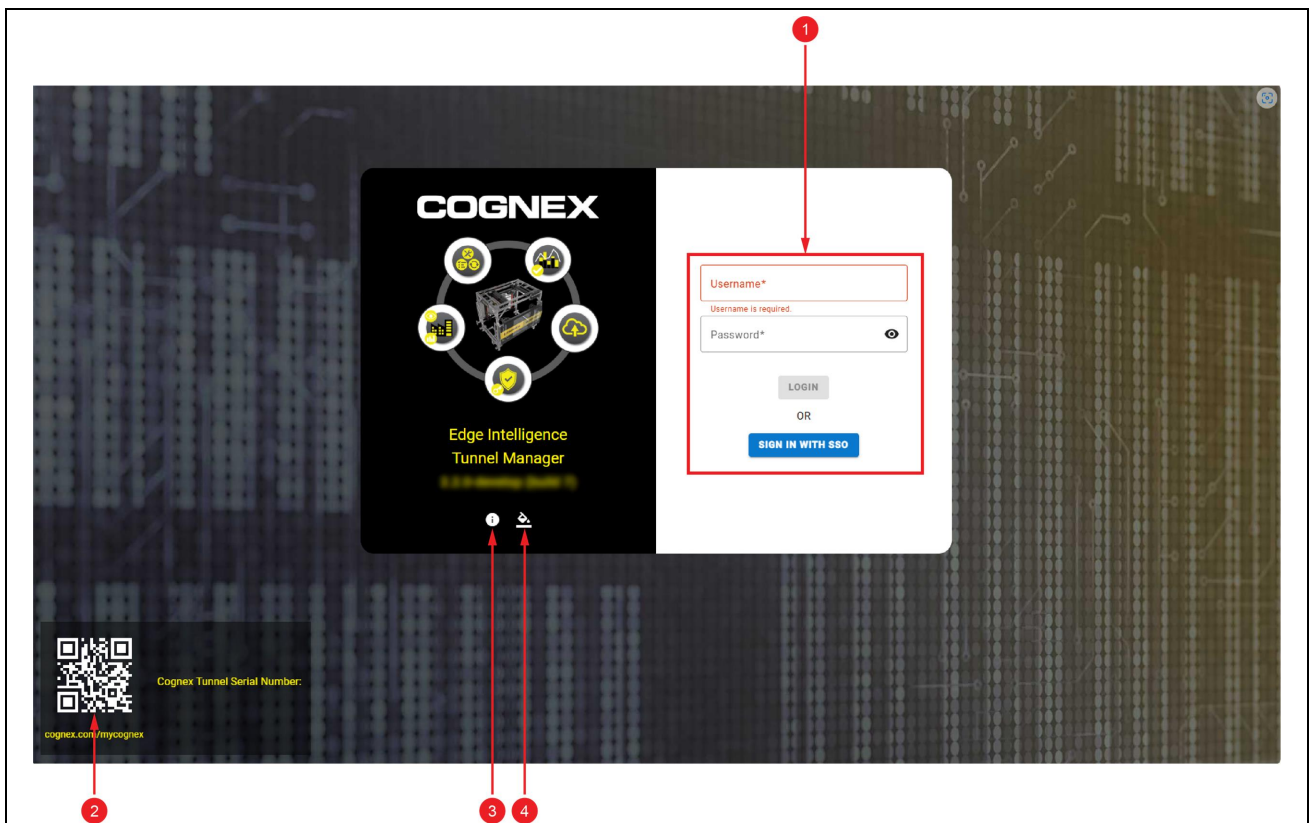
EI Tunnel Manager 2.2 adds the following enhancements and changes:

- Adds the following additional protocols supported by Data Forwarding:
 - Amazon S3
 - Amazon SNS
 - Azure IoT Hub
 - FTP
 - MQTT
 - SFTP
- Adds a photoeye testing step to the Dynamic Test Tunnel Setup app.
- You can now switch between a light mode theme and dark mode theme.
- General fixes and enhancements to the workflow of Tunnel Setup and commissioning apps.

Logging In

To access the EI Tunnel Manager web interface, simply log in using your credentials or single sign-on (SSO). If this is your first time logging in, use the default credentials. Once logged in, you can modify your settings and explore the apps available to you.

EI Tunnel Manager Login Page



Number	Element
1	Sign in using your credentials or SSO. Note: The Sign in with SSO button only appears in the login page if SSO is configured for the EI Tunnel Manager unit. For more information, see Single Sign-On on page 83 .
2	Scan the QR code to register your EI Tunnel Manager unit on the cognex.com/mycognex website.

3	<p>The information button opens the About Pop-Up on page 10 window that provides the following options and information:</p> <ul style="list-style-type: none"> • Information about the EI Tunnel Manager unit, such as serial numbers, software version, and license expiration date. • The documentation link opens the reference manual stored on the device. • The System Diagnostics Data section allows you to collect, download, and delete device logs that you can send to Cognex support engineers for troubleshooting support. • The Network Interfaces section lists the available and connected network ports with their configurations. • The Components section lists the different features that run on the device.
4	<p>The paint bucket icon allows you to change the website color theme.</p>

Default User Credentials

The following users credentials are available by default:

User	Password	Default Permissions
admin	BnthWWSD	Has access to all apps and features. Admin users can modify the default user profiles, enable access permissions for the other user roles, or create new profiles.
engineer	TaRDpKVx	Has access to all apps and features.
operator	SxtXGmxs	User with read-only rights. The operator does not have access to the Device Management app and the Settings.

Note: Change the default credentials to avoid security risks. For more information, see [User Management on page 80](#).

Discovering Devices on the Network

The default IP address for the Ethernet 2 port of Cognex product name uppercase is 192.168.1.100. The Cognex product name uppercase device discovers every reader automatically if the Cognex product name uppercase is connected to the corresponding network.

The readers found on the network appear on the [DataMan on page 38](#) page of the Device Management app.

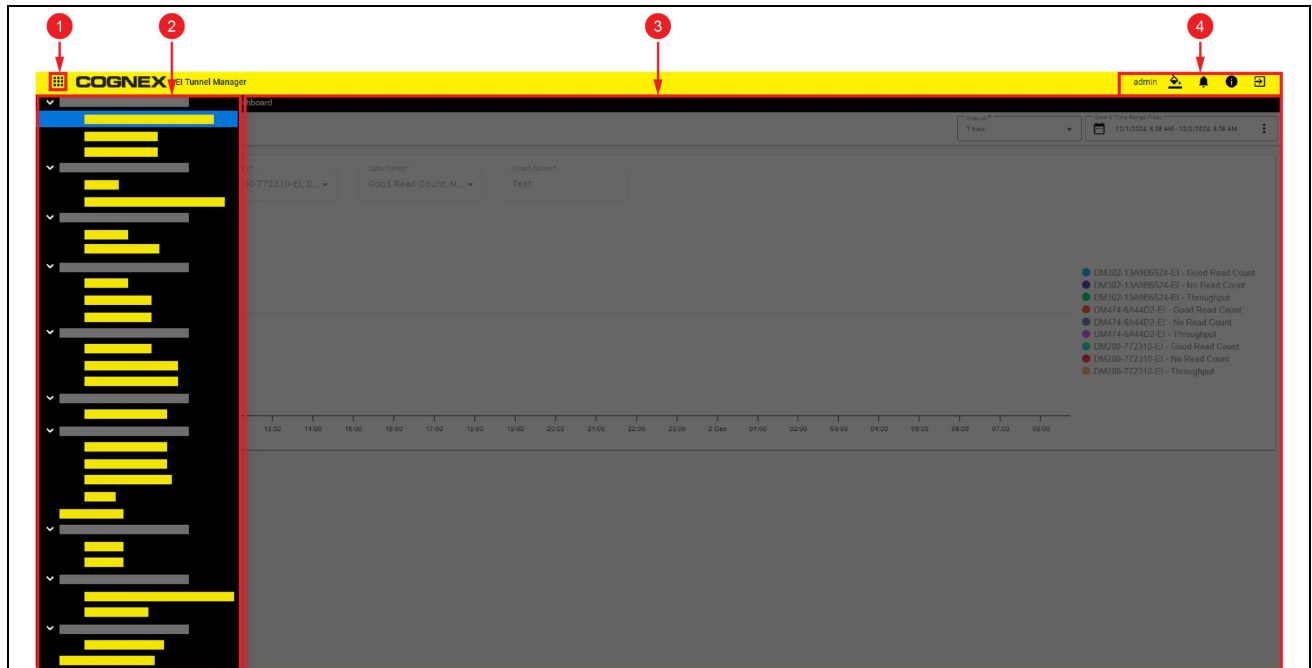
Actions	Password Protected	Primary	Name	Type	MAC Address	Firmware Version	Address Type	IP Address
<input type="checkbox"/>								
<input type="checkbox"/>								
<input type="checkbox"/>								
<input type="checkbox"/>								
<input type="checkbox"/>								
<input type="checkbox"/>								
<input 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"/>								

Note: The readers that are not on the same 192.168.1.x local subnet have the Misconfigured state.

Cognex recommends that all readers be on the same network as Cognex product name uppercase device. Either change the IP address of every reader on the network to be on the same network as 192.168.1.x, or change the IP address of the Ethernet port of the Cognex product name uppercase device to match those of the readers.

To change the network settings of your Cognex product name uppercase device, go to the [Edge Intelligence on page 73](#) page.

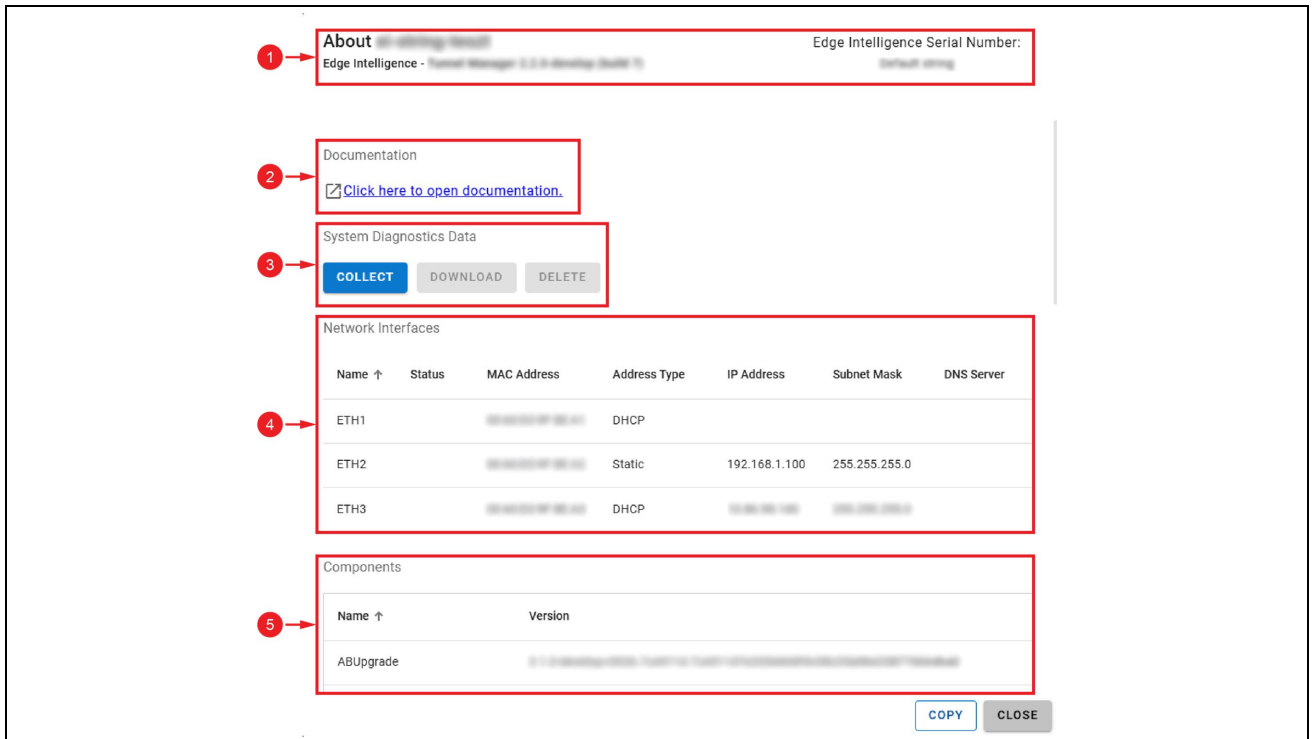
EI Tunnel Manager User Interface



Number	Element	Description
1	App menu	Click the Menu icon in the upper left corner to open the navigation pane.
2	Navigation pane	Use the navigation pane to open a page under an app.
3	App window	Use the app window to access the functions of the open page.
4	Ribbon elements	<ul style="list-style-type: none"> The ribbon displays the user that is signed in. Click the Theme icon to switch between dark and light themes. Click the Bell icon to view the notifications. Click on a notification to open it in the Notification Center on page 98. Click the Info icon to open the About Pop-Up on page 10 Click the Logout icon to log out.

About Pop-Up

The **About** pop-up window allows you to access documentation, collect diagnostics for troubleshooting support, and view network and component information for your EI Tunnel Manager unit.



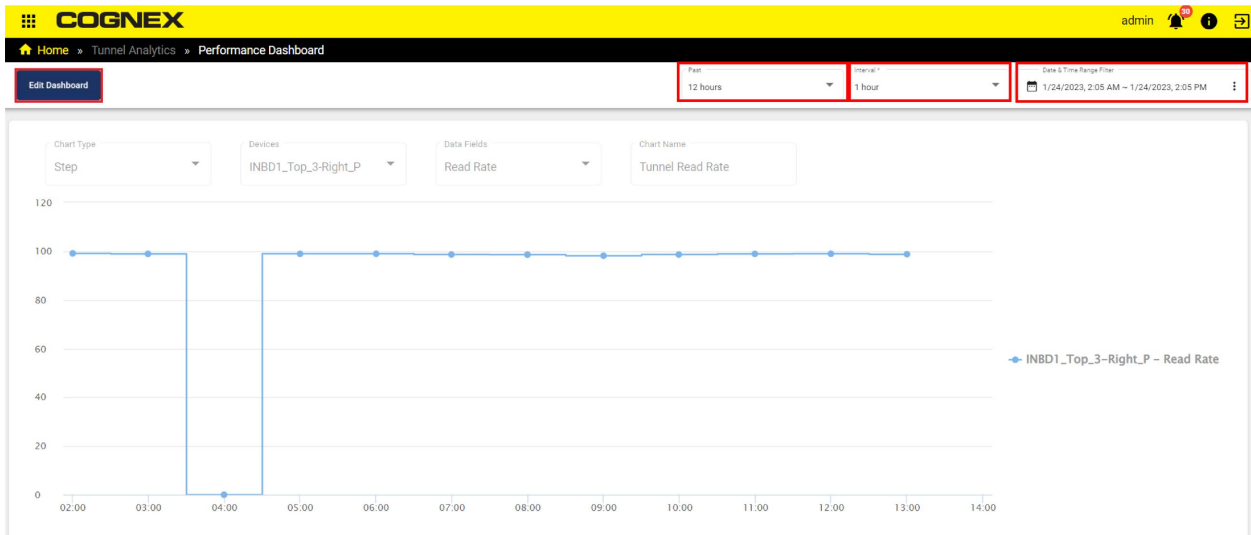
Number	Description
1	Information about the EI Tunnel Manager unit, such as serial numbers, software version, and license expiration date.
2	The documentation link opens the reference manual stored on the device.
3	The System Diagnostics Data section allows you to collect, download, and delete device logs that you can send to Cognex support engineers for troubleshooting support. Note: The log files in the downloaded .zip file are password-protected. Only Cognex support engineers can access them.
4	The Network Interfaces section lists the available and connected network ports with their configurations.
5	The Components section lists the different features that run on the device.

Tunnel Analytics

The Tunnel Analytics app provides analytics options.

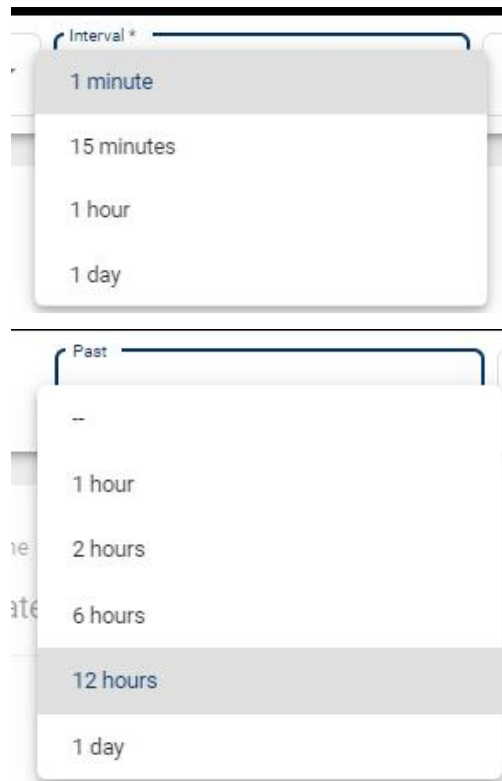
Performance Dashboard

The Performance Dashboard page 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***.



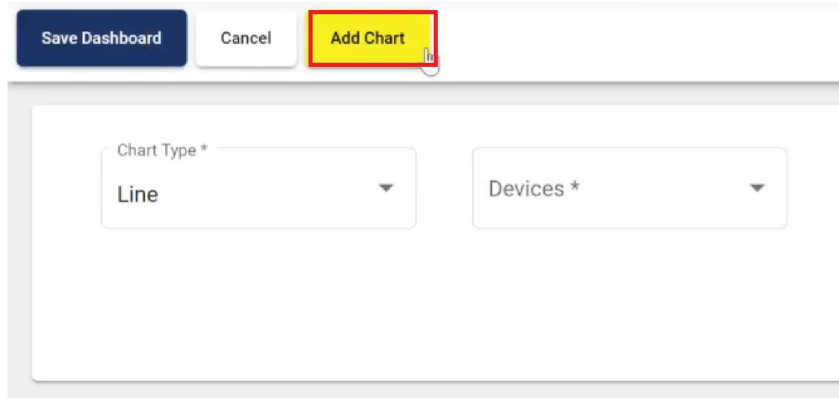
To look at a smaller time intervals, choose a smaller value for **Interval***.

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

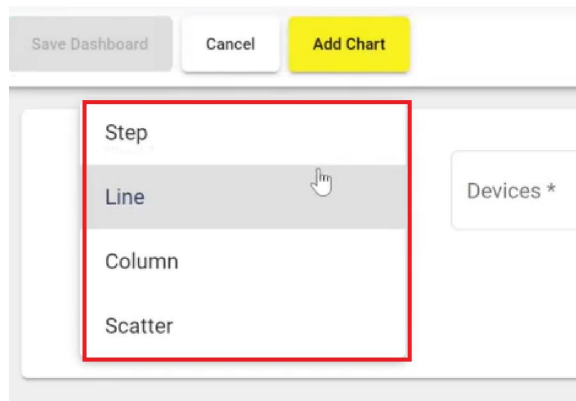
Edit the Dashboard

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

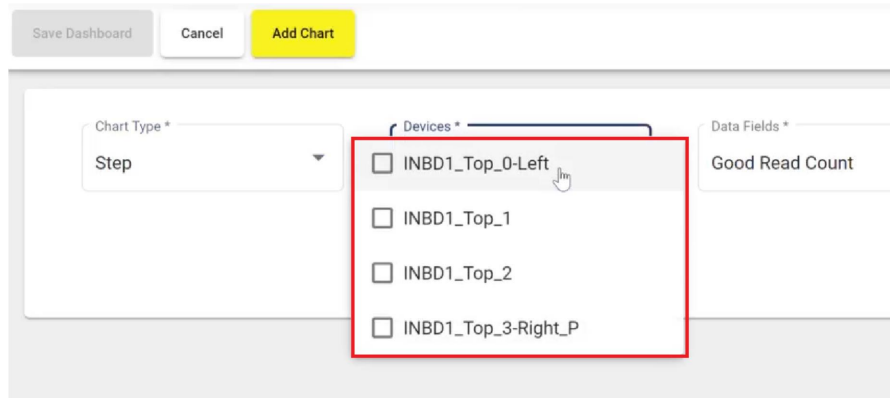
1. Click **Add Chart**.



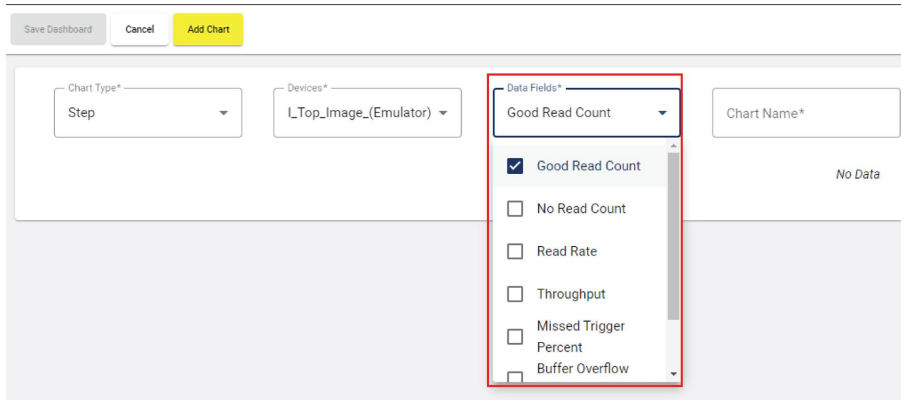
2. Select the chart type from the dropdown list.



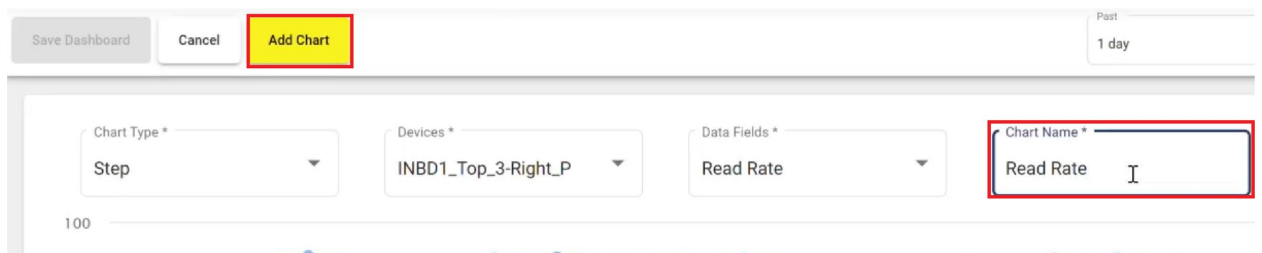
3. Select the device type from the dropdown list.



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

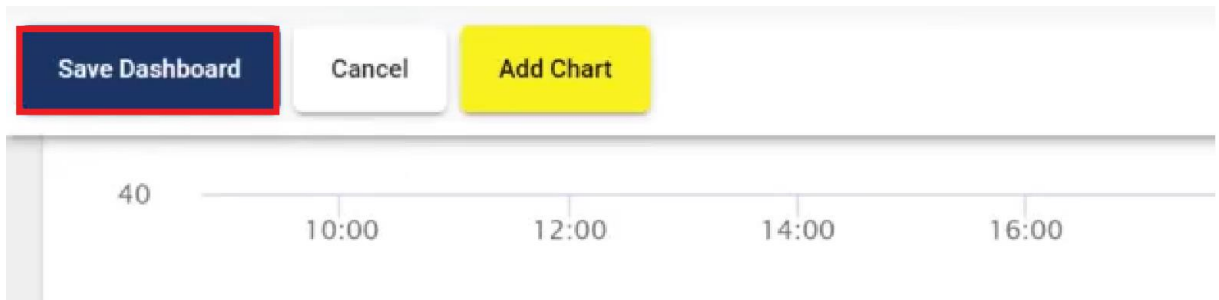


5. Name the new chart. Click **Add Chart**.



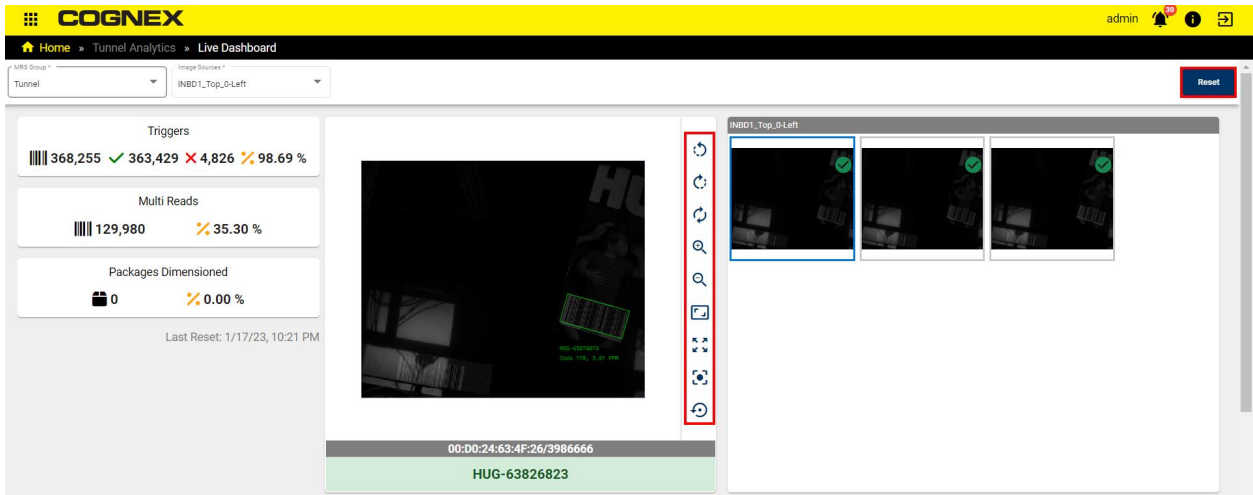
6. Repeat the procedure to add more charts to the Dashboard. You can sort, edit, and delete the charts from the Dashboard.

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



Live Dashboard

The Live Dashboard page 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	HUG-46483632	900	767	926	2,783

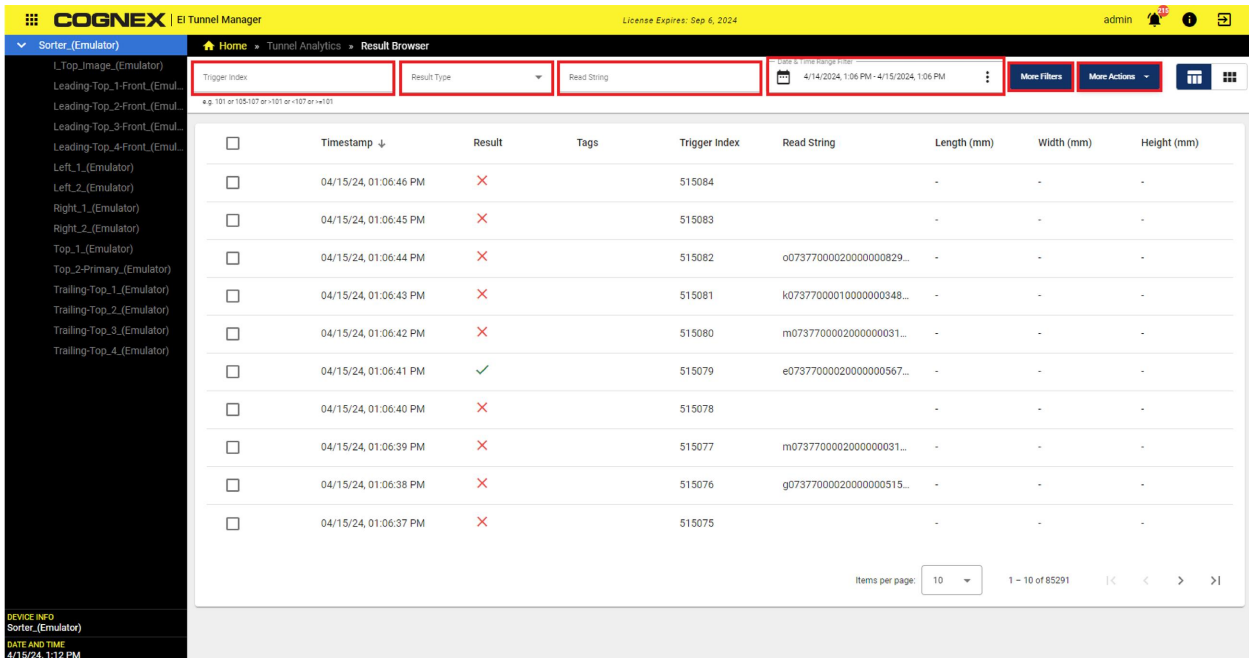
At the bottom left of the table is a yellow **Pause** button. At the bottom right, there is a dropdown menu for 'Items per page' set to 10, and a pagination indicator '1 - 10 of 300'.

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 allows you to filter the results that Cognex devices collect and to find the data that is the most important to you. By default, the page is in Table View. You can also switch to [Gallery View on page 21](#).



To download all triggers, select **Download All** in the **More Actions** menu. To avoid exceeding the trigger count, select the triggers you want to download before clicking **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** is an index number that the DataMan reader assigns 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:

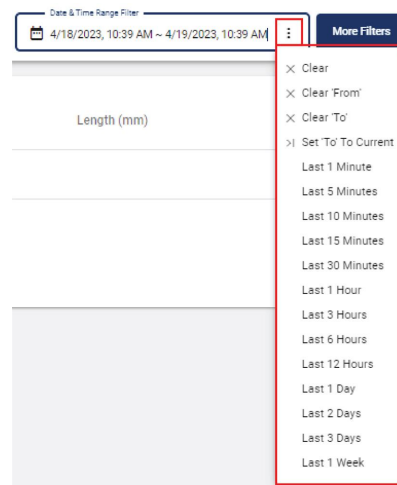
- Good Read: the reader successfully decoded the correct codes.
- No Read: the reader did not read any codes, or read the wrong codes.
- Failed Validation: the reader read an invalid code because the code is improperly formatted, or does not meet specific requirements.

The **Read String** is the string the unit reads.

The **Date & Time Range Filter** provides options to type a time range directly into the input field, select a time range using the menu, or select from a list of relative time options. Use the options to set the range. Use the **clear** functions to delete all or a part of the range.



Date and Time Range Picker



Quick Relative Time Options

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 ▼

Cancel

Search

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

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

Sorter Information

Filter Query

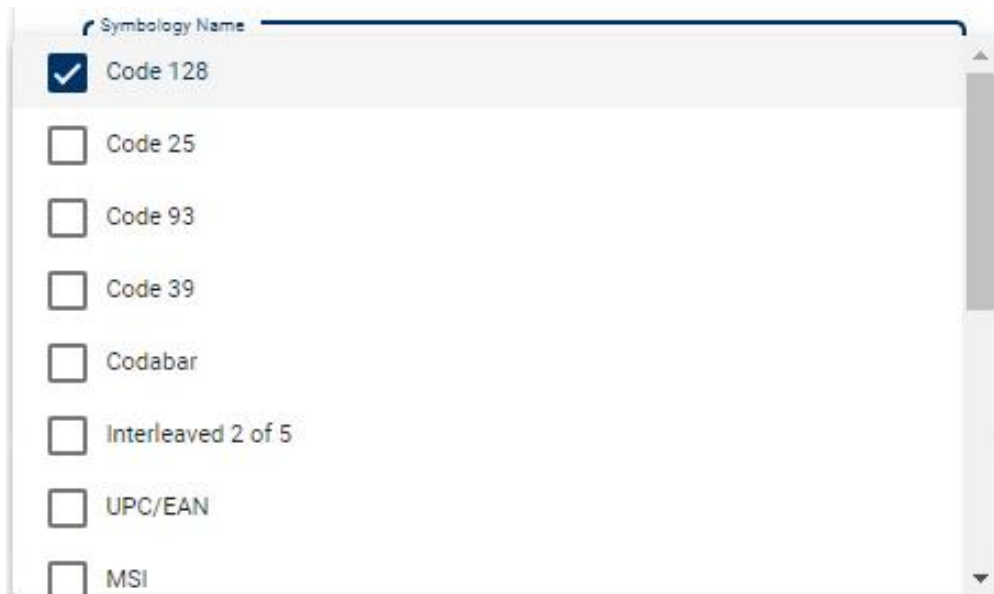
You can create a filter query by entering input into the filter fields. When you add an input into one of the fields, you create a search condition that limits your trigger results to those that meet the set condition.

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:



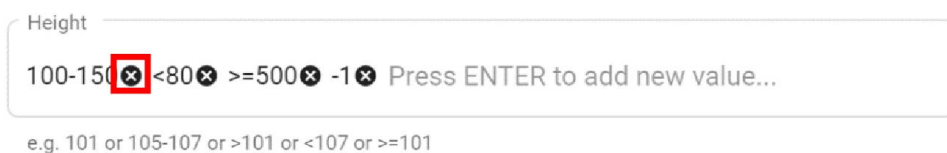
If you select more than one value, you are searching for results that match either of those values. For example, you can search for results that contain a Code 128 code, OR an I2of5, OR a UPC/EAN code:



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

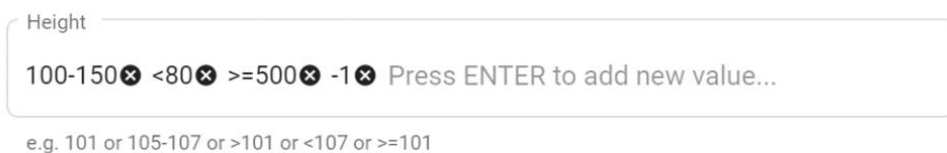
Condition	Example
Single value	Packages that have a reported length of 533 (length = 533).
Less than condition	Packages that have a reported length less than 533 (length < 533).
Less than or equal to	Packages that have a reported length that is less than or equal to 533 (length <= 533).
Greater than 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.



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.



Combining Filter Queries

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)

The screenshot shows a filter configuration interface. At the top, a dropdown menu titled "Symbology Name" is open, displaying a list of options with checkboxes: Code 128 (checked), Code 25 (unchecked), Code 93 (unchecked), Code 39 (unchecked), Codabar (unchecked), Interleaved 2 of 5 (checked), UPC/EAN (checked), and MSI (unchecked). Below this, there is a "Length" input field containing the text "-1 <100" followed by a prompt "Press ENTER to add new value...". Below the input field, there is a small example text: "e.g. 101 or 105-107 or >101 or <107 or >=101".

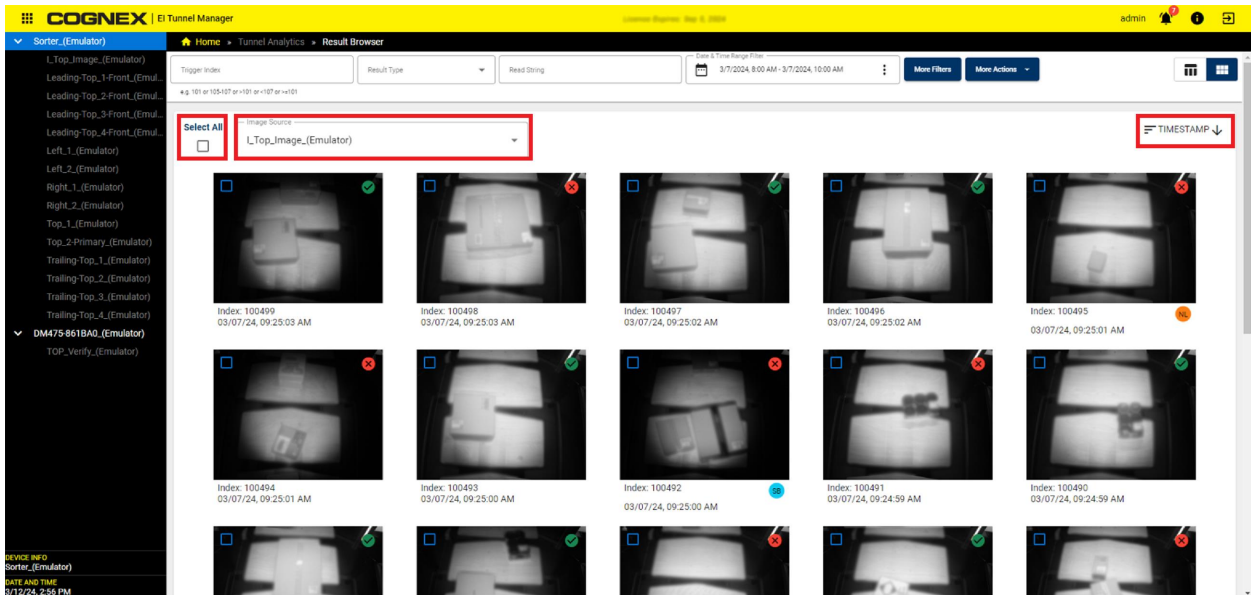
This means the filter shows results that are tagged as multi-reads *AND* contain a code that is either a code 128 *OR* Interleaved 2 of 5, *OR* UPC/EAN *AND* the reported length of the package is either -1 *OR* less than 100.

Gallery View

By default, the Result Browser page is in Table View. Switch the page from Table View to Gallery View using the view controls at the top of the page. Toggle between the two views by clicking on the representative icon.



In Gallery View, the table is replaced by a grid of thumbnail images. All other components remain the same. Similar to the Table View, the Gallery View shows all the triggers within the filtered time range.



Click the **Select All** checkbox to select all the items displayed on the current page.

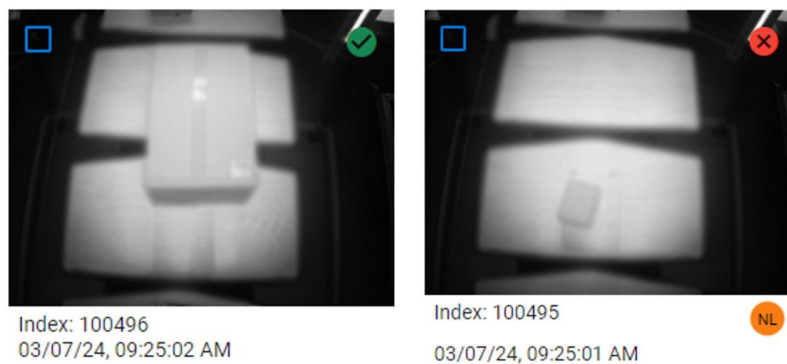
The **Image Source** dropdown lists all the devices. You can change the device source of the images displayed by selecting a different device name from the list.

The **Timestamp** sort option allows you to sort the triggers by timestamp in ascending or descending order.

Instead of trigger data shown in the columns of the table, the Gallery View shows a cell for each trigger.

Each cell contains:

- A single image from the selected device source.
- A Good Read or No-Read icon (top-right corner).
- The trigger index.
- The date and timestamp of the trigger (bottom-left).
- The data tags assigned to the trigger (bottom-right).



Click on a trigger cell to navigate to the [Trigger Review](#) page, which displays the rest of the images and the specific data for that trigger.

Trigger Review

The Trigger Review page shows all the images and data associated with a selected trigger. Navigate to the Trigger Review page by clicking on a table row in Table View or by clicking on a cell in the Gallery View. The Trigger Review page is either in

Data View or Image View. To switch between the views, click on the **Settings** icon in the upper right-hand corner. In the **General** section of the **View Settings** menu, select the Data View or Image View icon.



Data View provides expanded data cards which display more of the result data and condense the main image viewer. From Table View, the Trigger Review page is in Data View by default.

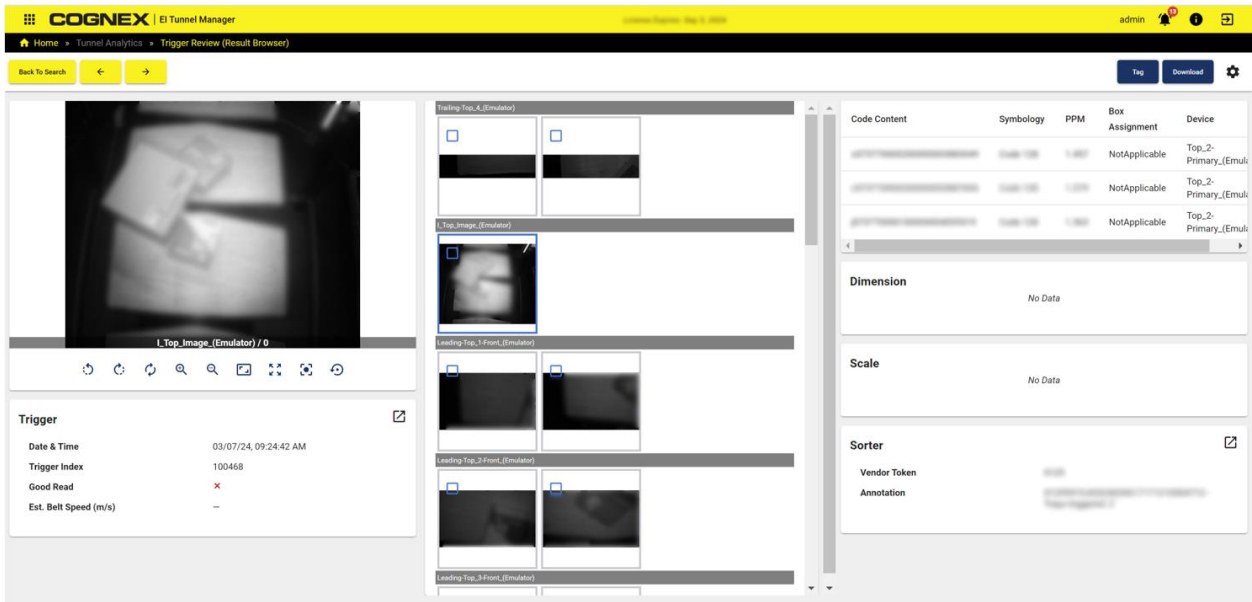
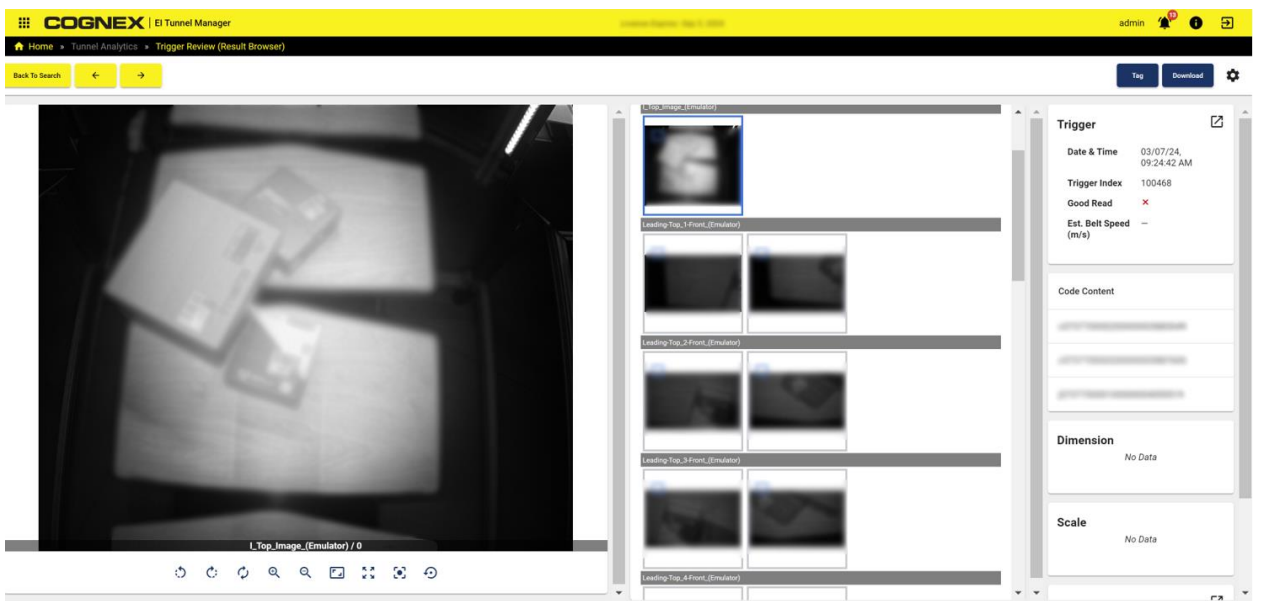


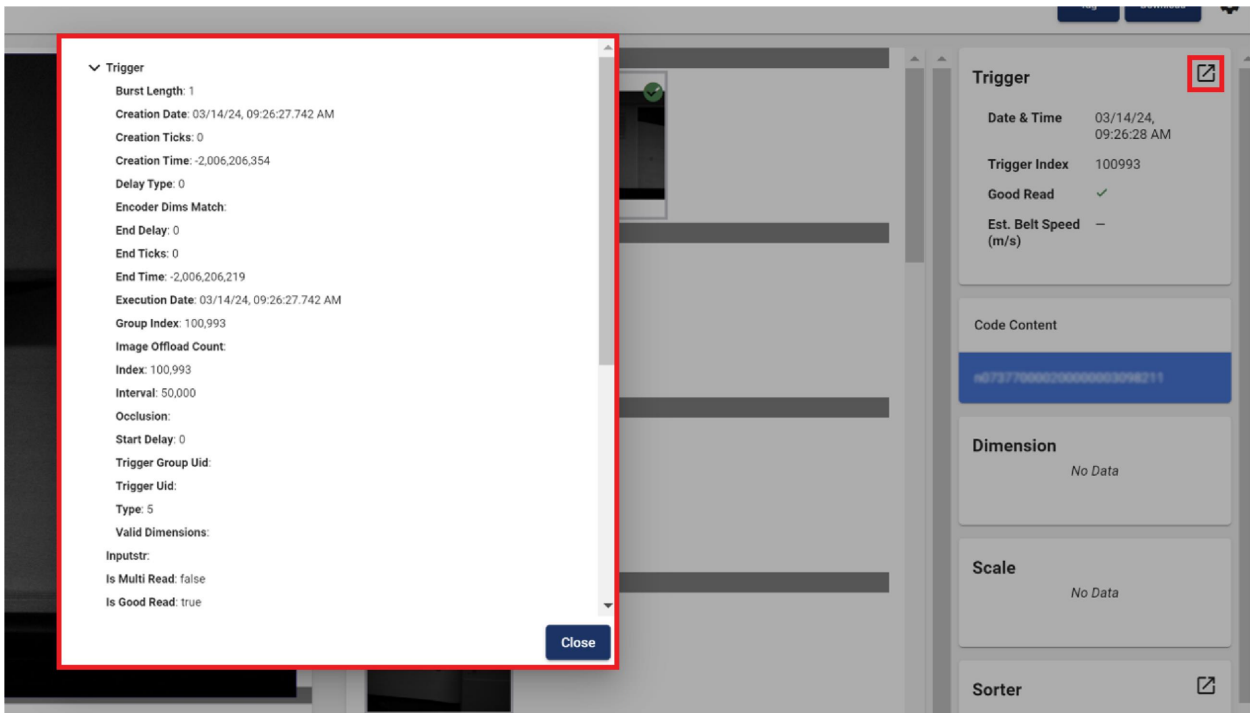
Image View collapses the data cards to the right side of the page and expands the main image viewer, so you can focus on the images rather than the result data. From Gallery View, the Trigger Review page is in Image View by default.

Note: Image View is useful for browsing No-Read results, where result data is minimal and most insights come from the image data.

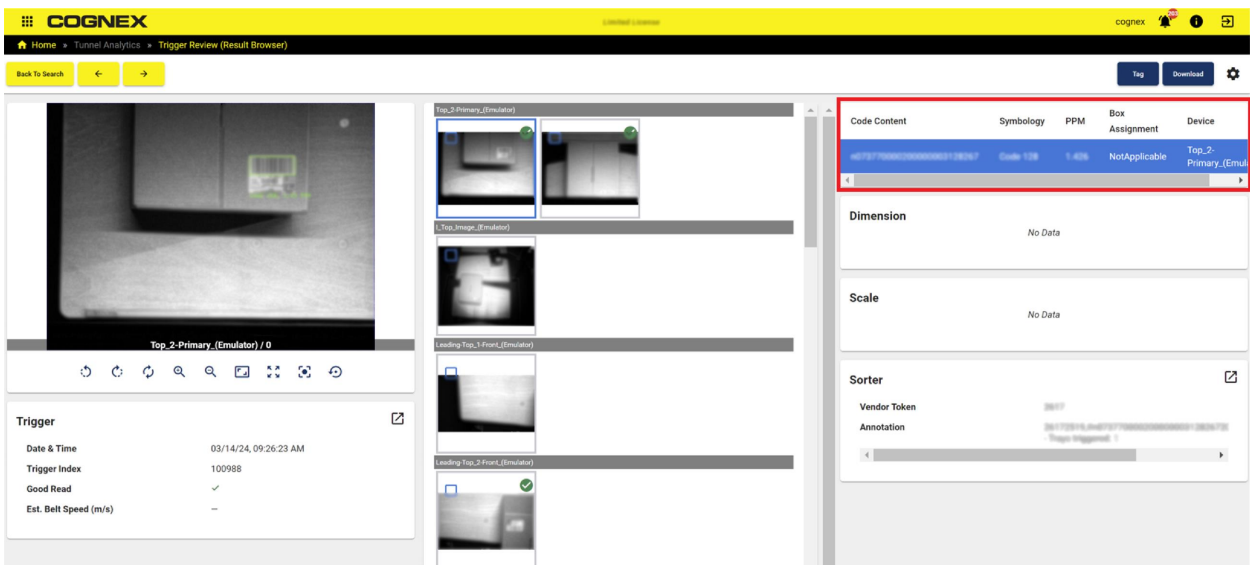


Click on the pop-out icon to open a dialog with all the details of the trigger. The icon is available in both the Image and Data Views.

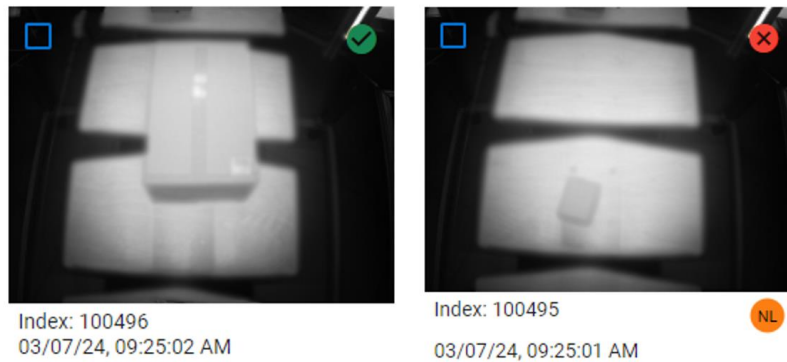
Note: The pop-out icon does not appear on cards that have no data. Instead, the card shows **No Data** indicating that no data was collected. This can happen if the system does not have a dimension or scale.



In both views, the **Code Content** table is populated with read codes. Click on a row to populate the main image viewer with an image of the read code.

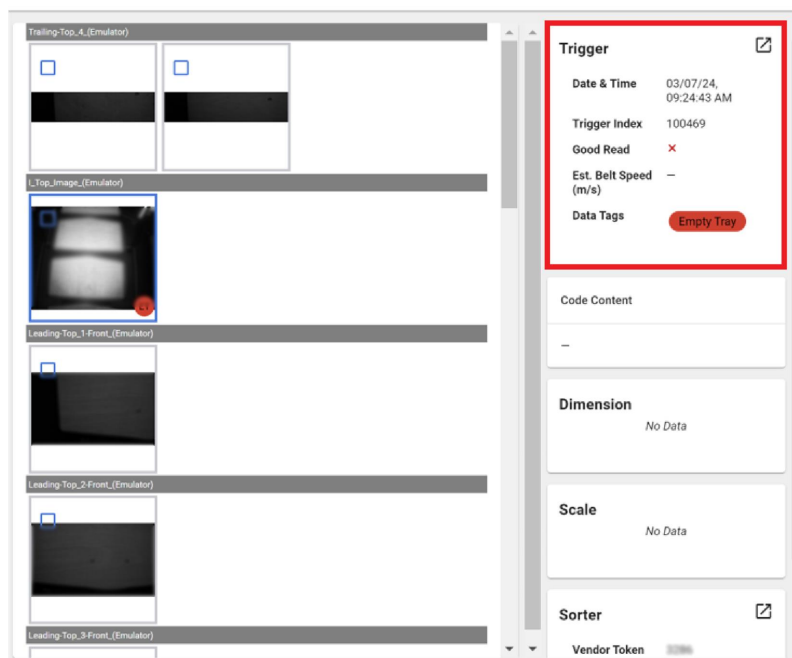


Click on the **Settings** icon in the upper right-hand corner. In the **All Images** section, select to display the SVG overlays or hide them. By default, the SVGs are shown.



The tags appear as abbreviated versions. The letters from the first two words in the tag are displayed in a circular chip. For example, if the tag is "Flagged Label", the chip displays "FL" as the abbreviation. If the tag is "Side by Side", the chip displays the letters "SB". You can hover over the tags to see the full name.

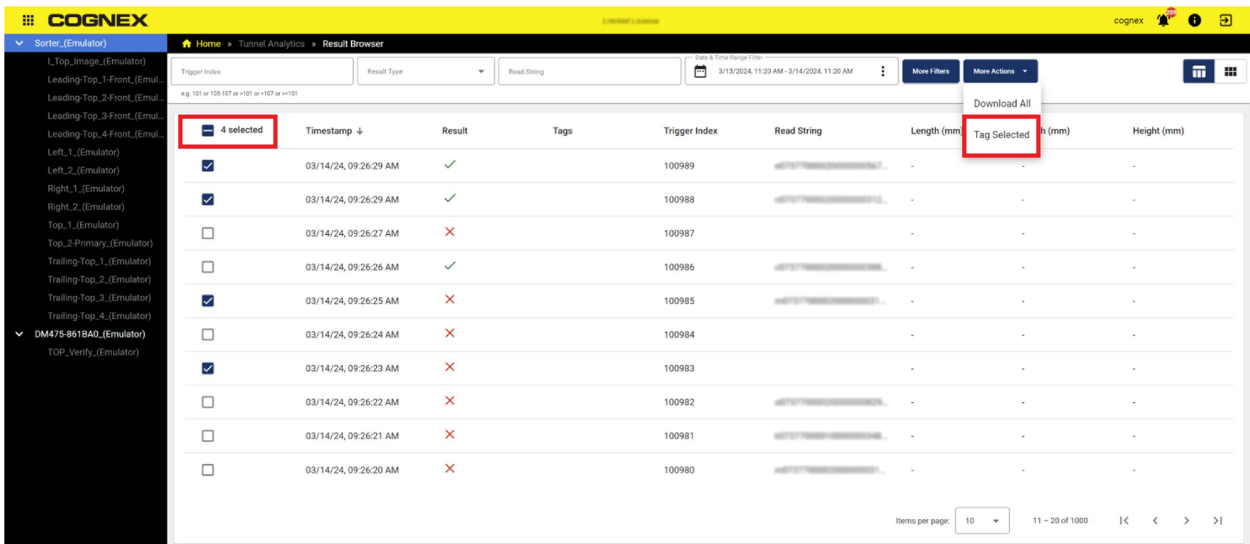
In the [Trigger Review](#) page, the tags applied to the entire trigger result are shown in the **Trigger** section under **Data Tags**. The tags are displayed in the non-abbreviated form. Tags applied to specific images appear in the thumbnail image in the abbreviated form.



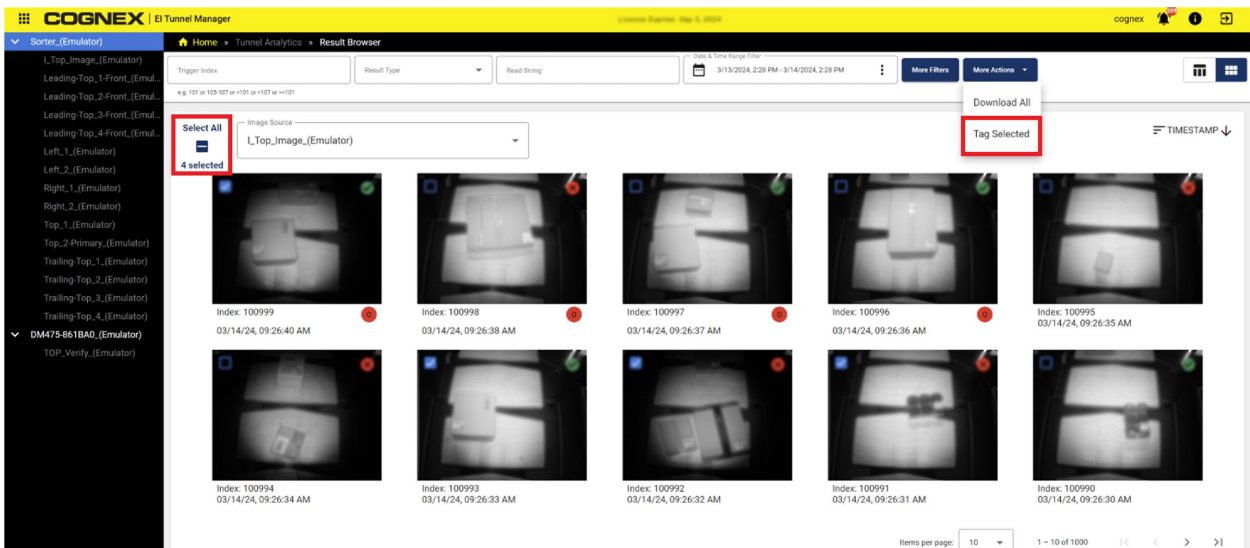
Tagging in the Result Browser

You can apply tags in bulk to multiple triggers or images in the Result Browser page.

To apply a tag in Table View, use the corresponding checkboxes in each row to select multiple triggers. Use the global checkbox to select all the triggers on a single page. The count next to the global checkbox shows the number of triggers selected.

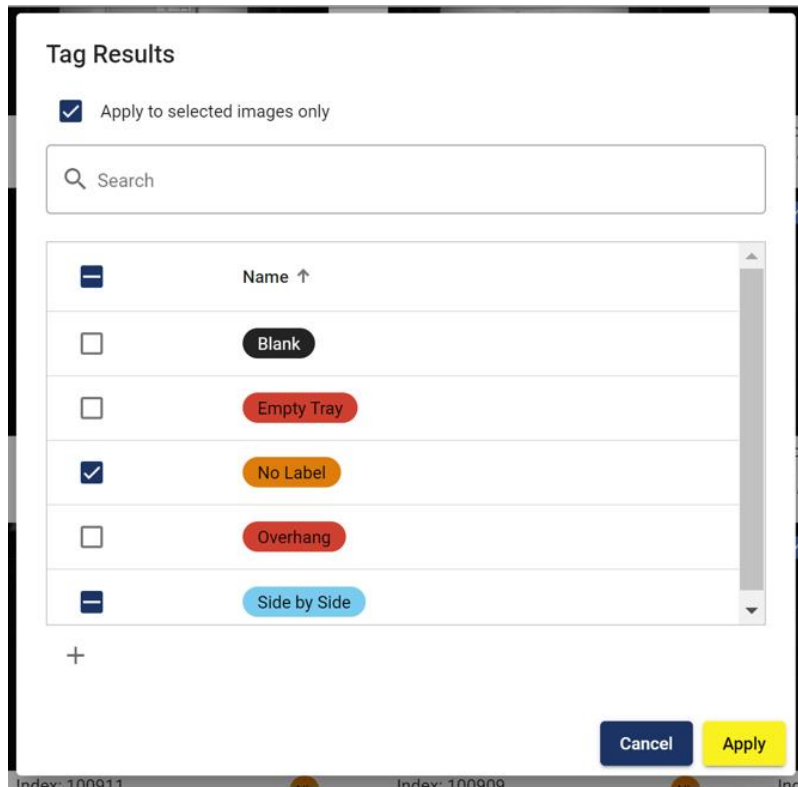


To apply a tag in Gallery View, select the checkboxes located in the top left corner of the thumbnail in each trigger cell. Click the **Select All** global checkbox to select all the items on the current page. The count below the global checkbox shows the number of triggers selected.



Note: In Gallery View, you apply the tag to the specific image shown. When you click on the trigger to navigate to the Trigger Review page, the tag is on the thumbnail image in the gallery. Tagging specific images also gives you the option to only download an image from the trigger rather than the entire set of images.

Click **More Actions**. Click the **Tag Selected** option to open the **Tag Results** dialog.



Previously-created tags appear in the table list. You can search for a specific tag using the search field above the list.

If the triggers selected do not have any existing tags, all the tag selections show an empty checkbox. If all the selected triggers have one or more of the same tags, those tags have a checked checkbox. If only some of the selected triggers have one or more of the tags, those tags have a partial checkbox.



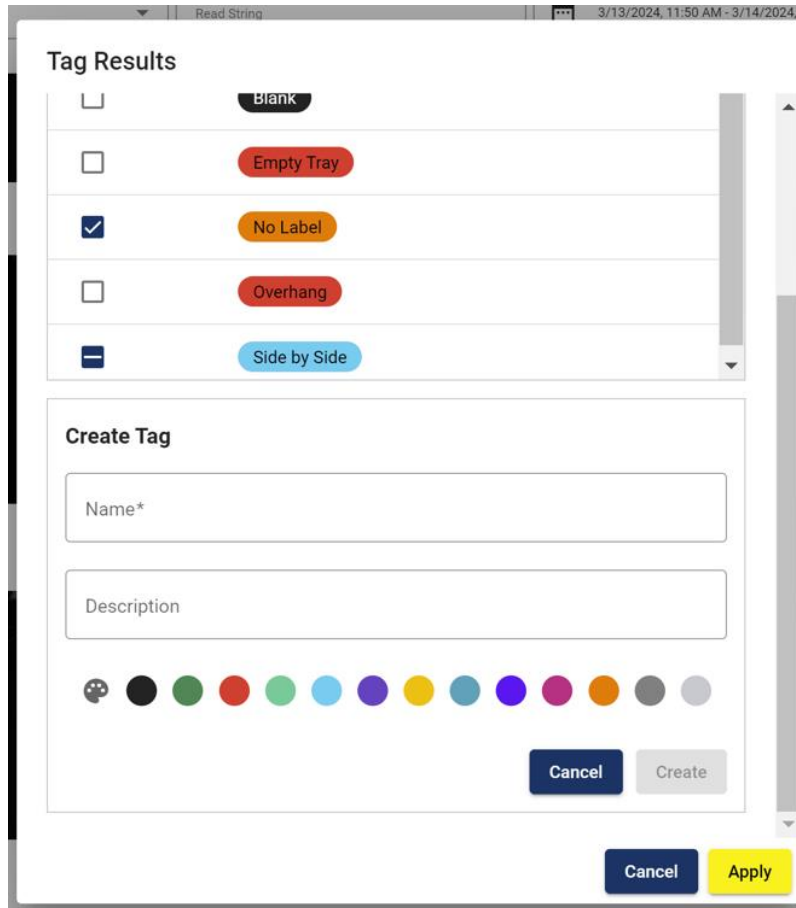
You can remove tags from the selected triggers by unchecking the checkbox. To add a tag that exists on some of the triggers but not all, click once to clear the checkbox and then click again so the checkbox is checked. This applies the tag to the rest of the triggers which do not already contain the tag.

Note: Duplicate tags are not created for a single trigger.

Click **Apply** to add tags to the selected triggers. Click **Cancel** to discard changes or close the **Tag Results** dialog.

Create a New Tag

Click on the plus icon below the tag list in the **Tag Results** dialog. The **Create Tag** section appears within the dialog.



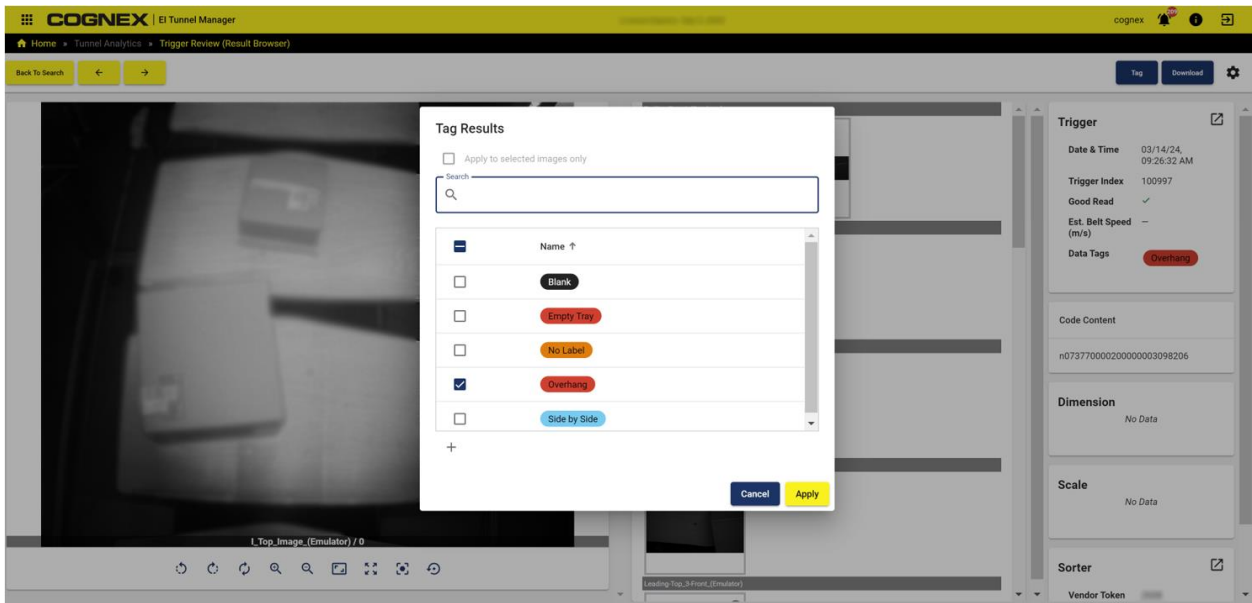
Provide a name for the tag and select a color. Choose from the default colors available or create a custom color by clicking on the palette icon. You can also provide a short description for the tag. Click **Create**, and the tag appears in the list above.

Note: Tags applied in the Table View are automatically applied generally to the entire trigger rather than to specific images.

Tagging in Trigger Review

You can tag triggers one at a time in the Trigger Review page. This is useful when sorting through no-reads and classifying the root cause one at a time.

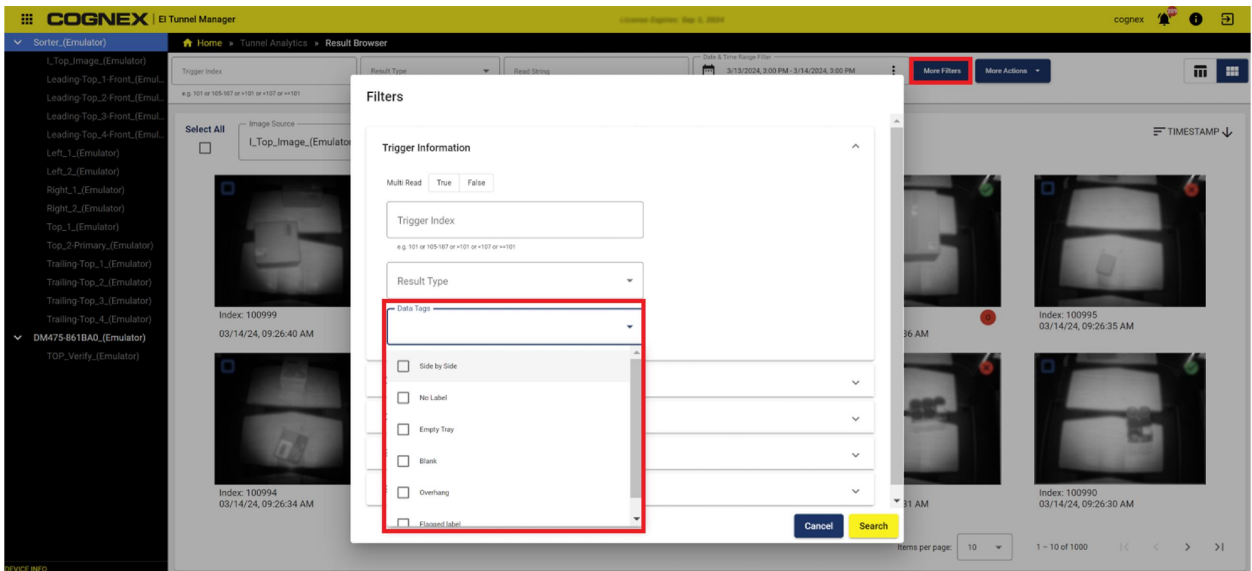
To tag in the Trigger Review page, select images and click the **Tag** button. The **Tag Results** dialog appears. You can select, deselect, and add tags to the selected images.



Filtering by Tags

You can filter results by tag in the Result Browser page. Select **More Filters**. The **Filters** dialog appears. In the **Trigger Information** section, use the **Data Tags** dropdown to select one or more data tags to filter the results by.

Note: If you select more than one data tag from the list, the filter includes triggers that contain any one of the tags selected.



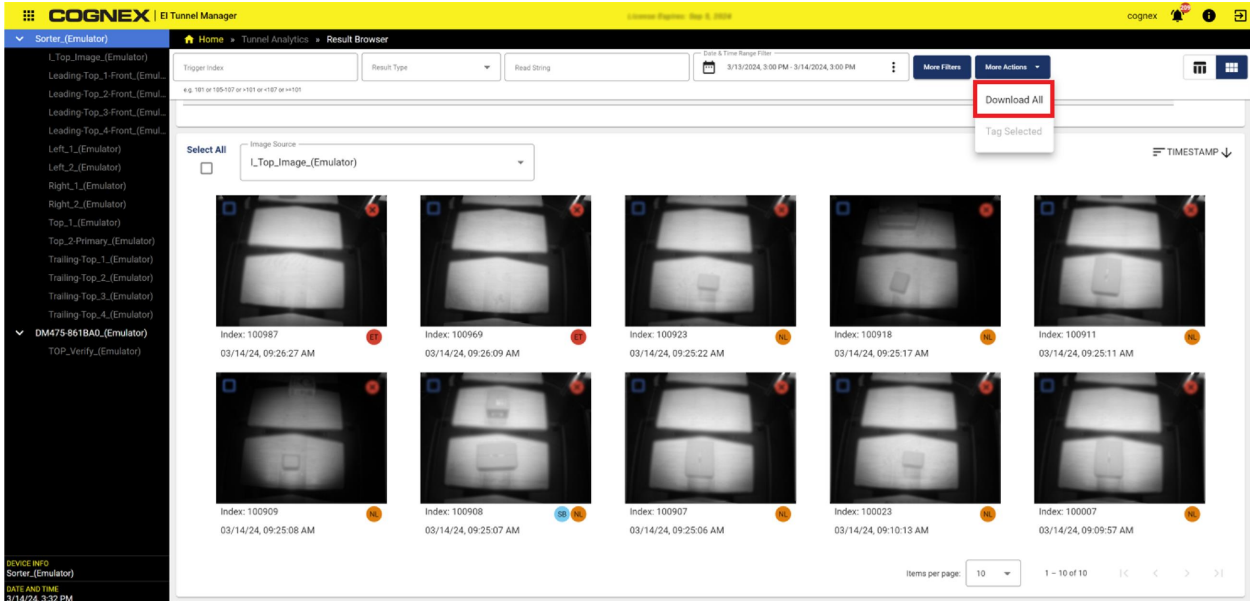
Click **Search**. The Result Browser now only shows the results within the filtered dataset. The **Active Filters** section shows the filters.



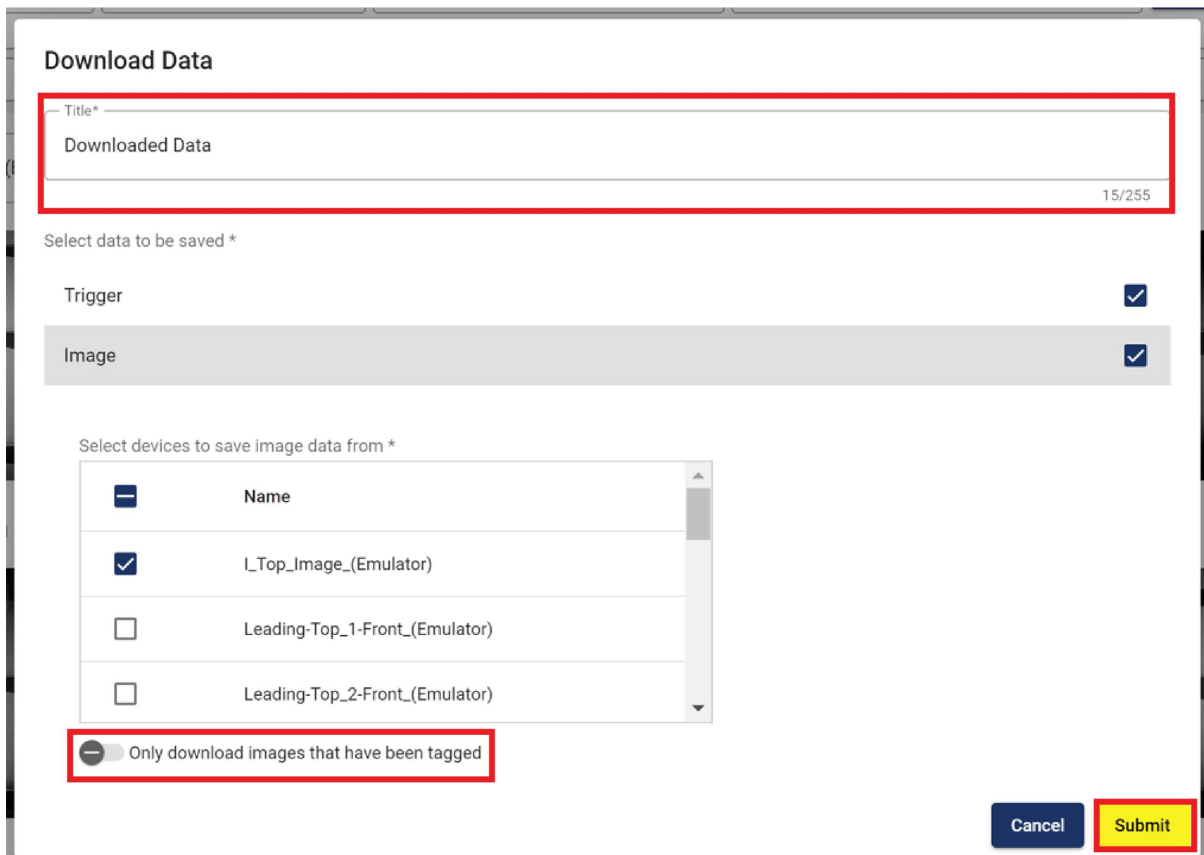
Downloading Tagged Images

You can download images in bulk from the Result Browser or individually from the Trigger Review page.

In the Result Browser, download the set of filtered data by selecting **More Options** and clicking **Download All**.



The **Download Data** dialog appears.



Provide a title for the download. Select Trigger and Image data to include in the download. The Trigger data is all the result data, such as trigger index, read code string, and dimensions, downloaded into a .csv file. The Image data is the .jpg for each trigger.

In the Image data section, you can choose to download the image data for all devices or only from select devices. You can select all devices by clicking the global checkbox.

Note: From Gallery View, the device you were already viewing is selected by default. From Table View, all devices are selected by default.

You can choose to only download tagged images by switching the **Only download images that have been tagged** toggle. Click **Submit** to start the download.

Note: After filtering the triggers or images to specific tags, you can also download the tagged triggers or images specifically by the filter applied. For example, if you select "empty tray" as the filter for the data tags, when you click **Download All**, it downloads the triggers or images with just the "empty tray" tag, not the entire timeframe of data.

Events




The Events app allows you to track changes to the connected readers.

Configuration Change History

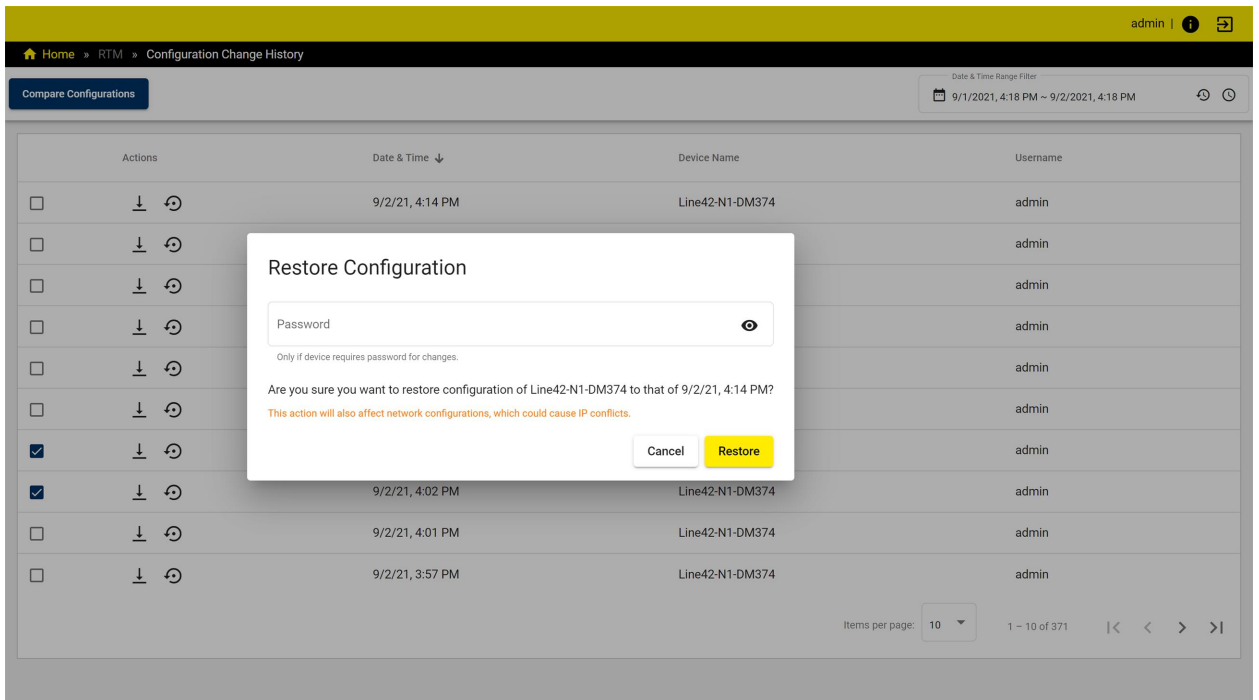
The Configuration Change History page tracks changes made to the configuration of all connected readers and shows changes in a customized fashion. The window displays the Device tree with available grouped and standalone readers. The page automatically links configurations with the respective usernames.

Actions	Date & Time ↓	Device Name	Username
<input type="checkbox"/> ↓ ↻	4/9/20, 7:05 AM	DM374-El-Demo-Online	admin
<input type="checkbox"/> ↓ ↻	4/9/20, 7:03 AM	DM374-El-Demo-Online	admin
<input type="checkbox"/> ↓ ↻	4/9/20, 5:06 AM	DM374-El-Demo-Online	admin
<input type="checkbox"/> ↓ ↻	4/9/20, 5:04 AM	DM374-El-Demo-Online	admin
<input type="checkbox"/> ↓ ↻	4/9/20, 3:06 AM	DM374-El-Demo-Online	admin
<input type="checkbox"/> ↓ ↻	4/9/20, 3:04 AM	DM374-El-Demo-Online	admin
<input type="checkbox"/> ↓ ↻	4/9/20, 1:06 AM	DM374-El-Demo-Online	admin
<input type="checkbox"/> ↓ ↻	4/9/20, 1:04 AM	DM374-El-Demo-Online	admin
<input type="checkbox"/> ↓ ↻	4/8/20, 11:06 PM	DM374-El-Demo-Online	admin
<input type="checkbox"/> ↓ ↻	4/8/20, 11:04 PM	DM374-El-Demo-Online	admin

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.



The screenshot shows the 'Configuration Change History' page in the EI Tunnel Manager. A modal dialog titled 'Restore Configuration' is displayed over a table of configuration changes. The dialog prompts the user to enter a password and confirms the restoration of configuration for device 'Line42-N1-DM374' to the state of '9/2/21, 4:14 PM'. A warning message states: 'This action will also affect network configurations, which could cause IP conflicts.' The dialog has 'Cancel' and 'Restore' buttons. The background table lists configuration changes with columns for 'Actions', 'Date & Time', 'Device Name', and 'Username'.

Dashboard overview:

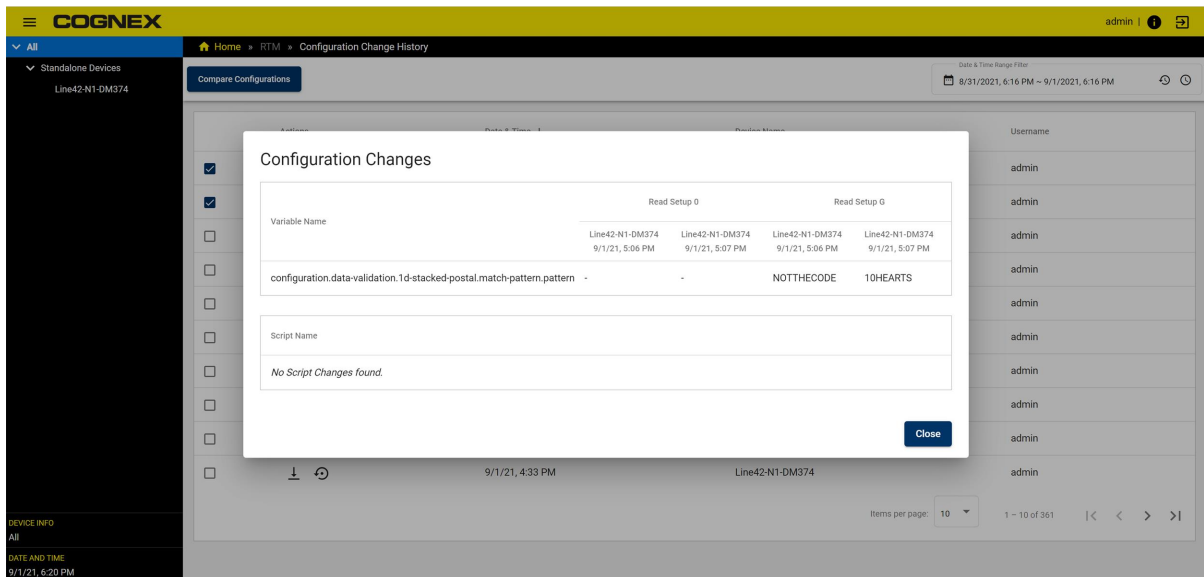
Item	Description
Compare Configurations button	Select 2 checkbox to enable the button. Click the button to see configuration changes in a pop-up window. For more information see
Date & Time Range Filter	Use the time range to define a period of time from which performance data is collected for the charts. 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 the **Compare Configurations** button. A pop up window appears with a table that shows the compared configurations.



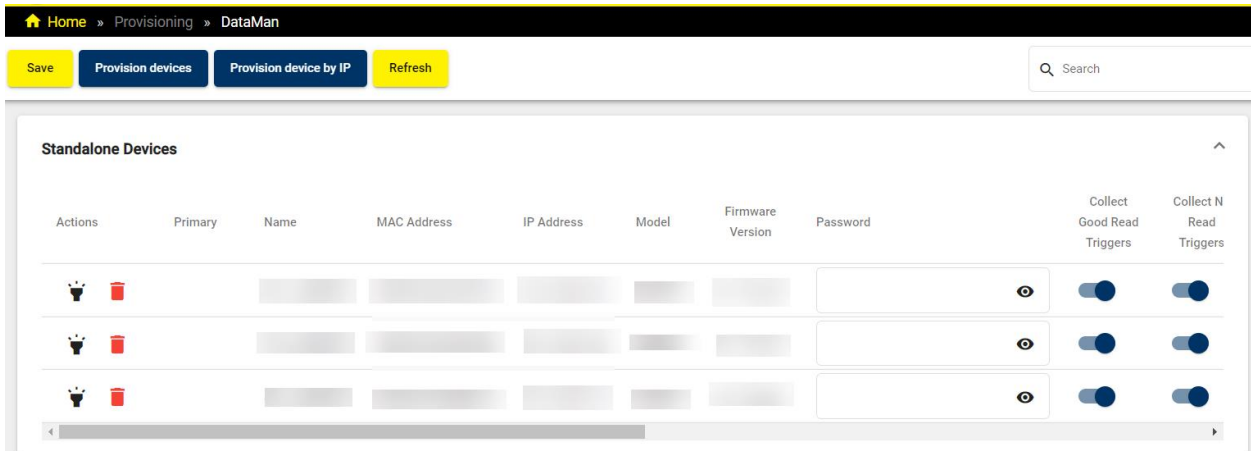
Item	Description
Configuration Changes	Lists variables that have different values in the compared versions
Read Setups	Display the name of the readers compared, and the difference in values pertaining to the row of the configuration scripts
Variable Name	Name of the variable which has different values in the compared versions
Script Name	Name of the recently modified script
Read Setup	Name of the read setup

Provisioning

The Provisioning app allows you to provision your connected devices and device groups, and allows you configure what data you want to collect from each of your devices, and manage your remote subnets.

DataMan

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




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

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

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

Actions

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

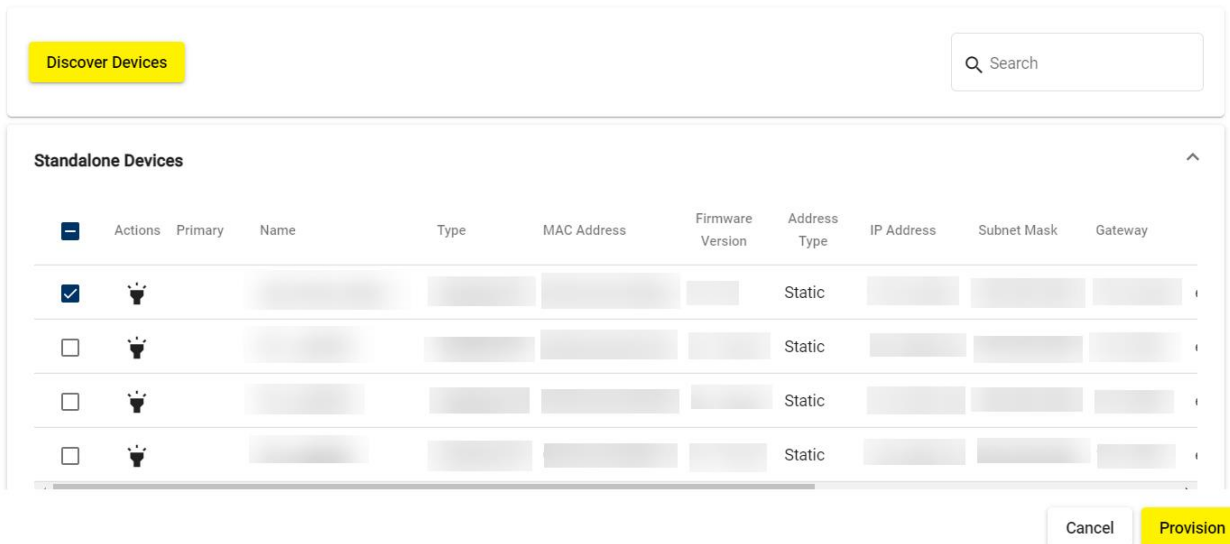
Actions	
Icon	Action
	Flash LED
	Delete

- Click the **Flash LED** button to remotely trigger the LED of the reader for easy identification.
- Click the **Delete** button to remove the reader 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 readers. To provision one or more readers, check the checkbox for the selected readers, and click **Provision**.

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

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

To search for a specific reader 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 reader, and click **Provision**.

Data Collection Settings

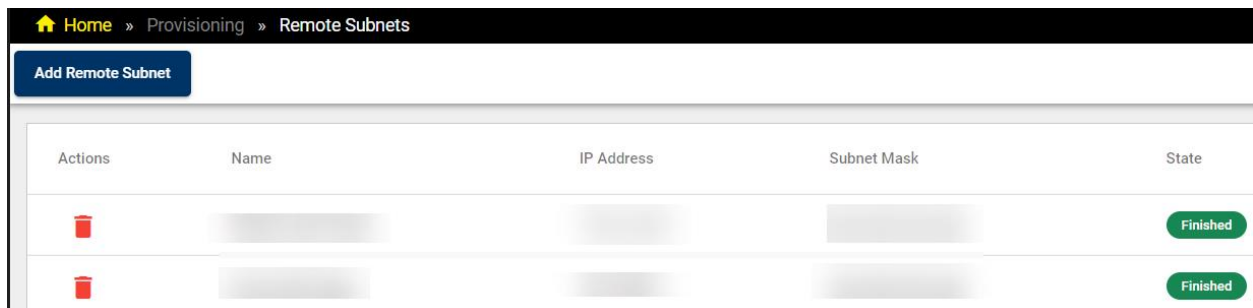
You can modify collection settings for different types of data using the toggles in each column of the row for the selected reader:

Column	Description
Password	Provide the password for the reader to make any changes.
Collect Good Read Triggers	Enable this setting to collect good read trigger data from the reader.
Collect No Read Triggers	Enable this setting to collect no read trigger data from the reader.
Collect Validation Failure Triggers	Enable this setting to collect validation failure trigger data from the reader.
Collect Good Read Images	Enable this setting to collect good read image data from the reader.
Collect No Read Images	Enable this setting to collect no read image data from the reader.
Collect Validation Failure Images	Enable this setting to collect validation failure image data from the reader.
Collect Device Configuration Changes	Enable this setting to collect reader configuration change data from the reader.
Collect Statistics	Enable this setting to collect statistics from the reader.
Collect Tunnel Trigger Result	Enable this setting to collect tunnel trigger results from the reader.

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

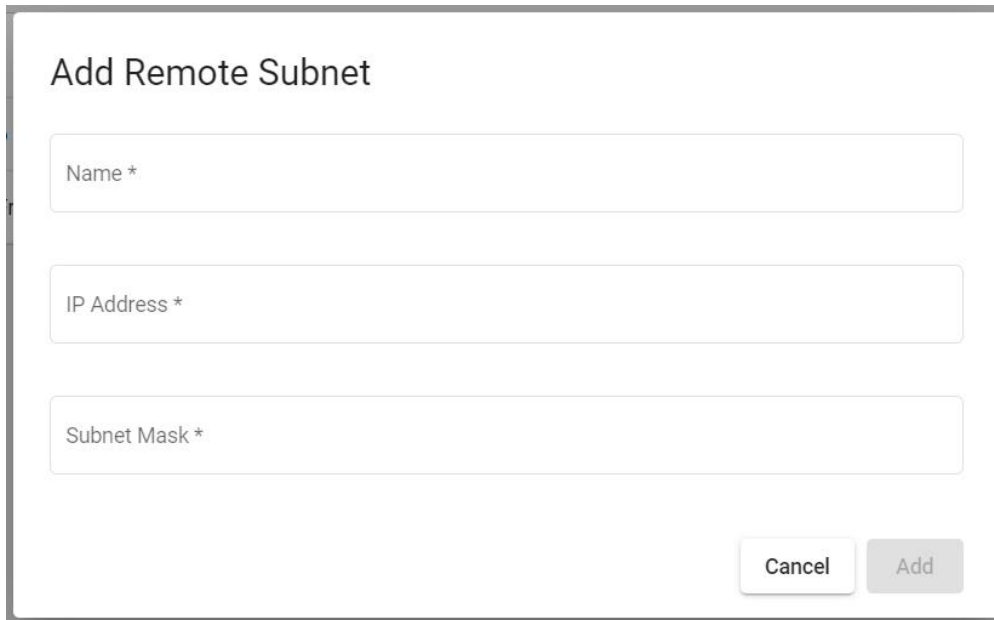
Remote Subnets

The Remote Subnets page 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:



The screenshot shows a dialog box titled "Add Remote Subnet". It contains three text input fields, each with an asterisk indicating it is required: "Name *", "IP Address *", and "Subnet Mask *". At the bottom right of the dialog, there are two buttons: "Cancel" and "Add".

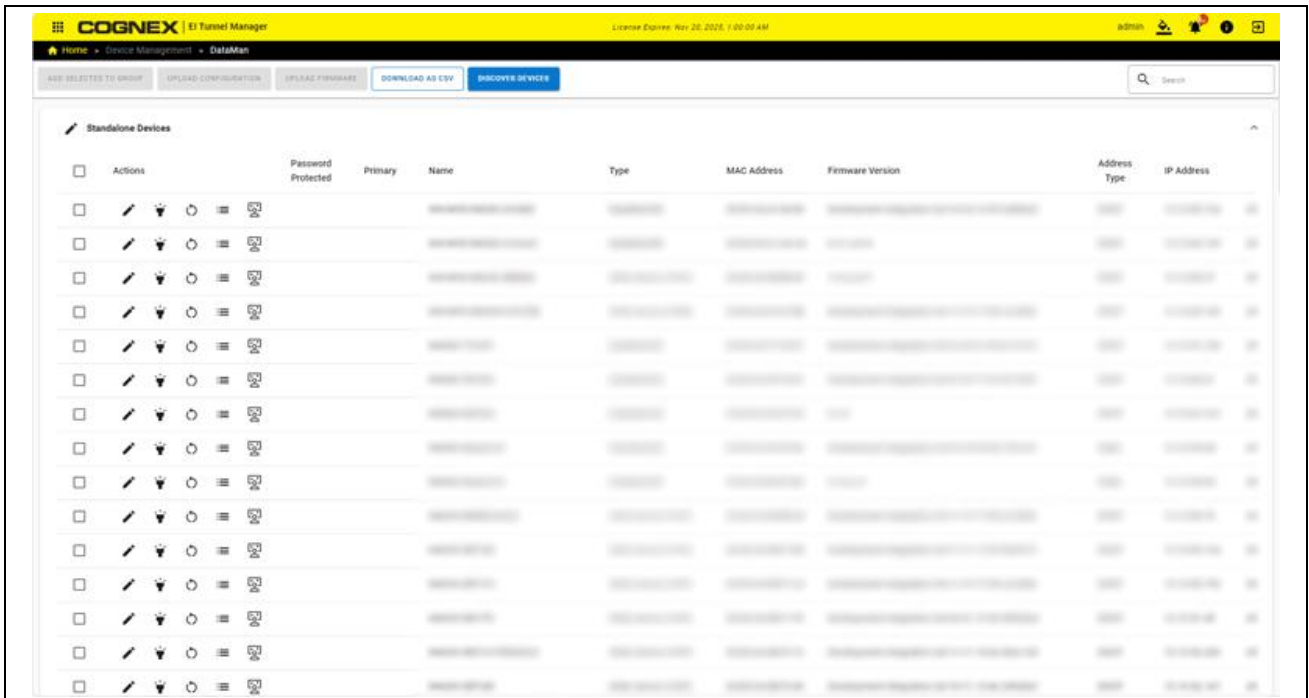
Enter the name, IP address, and subnet mask for the remote subnet you want to add, and then click **Add**.

Device Management

The Device Management app 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 Device Management app provides a list of standalone readers and reader groups, including reader data. You can edit the configuration, flash the LED, reboot, or access the DataMan WebHMI of individual readers. You can perform mass configuration or firmware updates for reader groups.








Item	Description												
Action ribbon	Provides quick access to actions you can perform on the selected readers.												
	<table border="1"> <thead> <tr> <th>Button</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Add Selected to Group</td> <td>Add selected readers to MRS group.</td> </tr> <tr> <td>Upload Configuration</td> <td>Upload a configuration file to the selected readers.</td> </tr> <tr> <td>Upload Firmware</td> <td>Upgrade firmware on selected readers.</td> </tr> <tr> <td>Download as CSV</td> <td>Download a list of readers as a CSV file.</td> </tr> <tr> <td>Discover devices</td> <td>Find readers on the local and remote networks, depending on the configuration on the Remote Subnets on page 37 page.</td> </tr> </tbody> </table>	Button	Description	Add Selected to Group	Add selected readers to MRS group.	Upload Configuration	Upload a configuration file to the selected readers.	Upload Firmware	Upgrade firmware on selected readers.	Download as CSV	Download a list of readers as a CSV file.	Discover devices	Find readers on the local and remote networks, depending on the configuration on the Remote Subnets on page 37 page.
	Button	Description											
	Add Selected to Group	Add selected readers to MRS group.											
	Upload Configuration	Upload a configuration file to the selected readers.											
	Upload Firmware	Upgrade firmware on selected readers.											
Download as CSV	Download a list of readers as a CSV file.												
Discover devices	Find readers on the local and remote networks, depending on the configuration on the Remote Subnets on page 37 page.												
Search Field	Allows for searching for a reader by any characteristic, such as name, model or firmware version.												
Standalone reader list	A table view of the settings of the standalone readers that are discovered on the network with options that can be enabled or disabled for the reader.												
Grouped reader list	Table views of the readers in a group sorted alphabetically by group name with options that can be enabled or disabled for the individual reader.												

Columns of the Table View

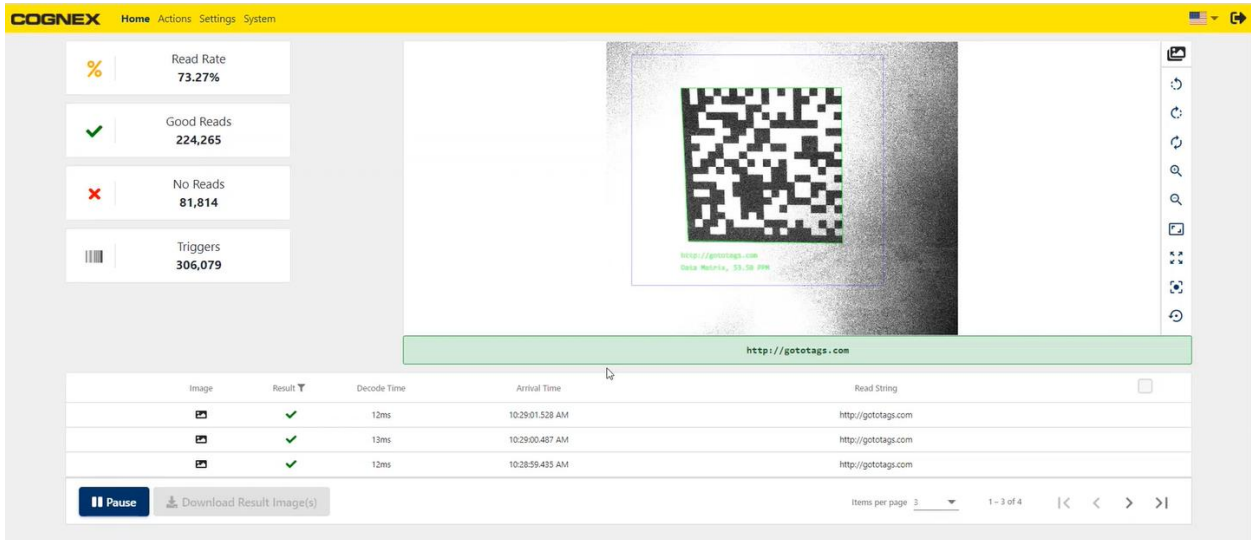
The table view of the standalone or group readers displays information and allows setting changes to the individual readers.

Column Title	Description
--------------	-------------

<p>Actions</p>	<p>Click on the icons to perform actions on an individual reader.</p> <div style="text-align: center; margin-bottom: 10px;">      </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #f2f2f2;"> <th style="text-align: center;">Button</th> <th style="text-align: center;">Description</th> </tr> </thead> <tbody> <tr> <td>Edit Device Network Settings</td> <td>Modify the name, IP address, Subnet Mask, and Default Gateway of the reader. Enter the reader password if required.</td> </tr> <tr> <td>Flash LED</td> <td>Remotely trigger the LED of the reader for easy identification.</td> </tr> <tr> <td>Reboot</td> <td>Reboot the reader.</td> </tr> <tr> <td>Show Device Logs</td> <td>Opens a window that shows the reader logs. In this window, you can reload to pull the latest logs or download them as <code>.log</code> file.</td> </tr> <tr> <td>Open DataMan WebHMI</td> <td>Open the DataMan WebHMI in a new tab. For more information, see DataMan WebHMI on page 40.</td> </tr> </tbody> </table>	Button	Description	Edit Device Network Settings	Modify the name, IP address, Subnet Mask, and Default Gateway of the reader. Enter the reader password if required.	Flash LED	Remotely trigger the LED of the reader for easy identification.	Reboot	Reboot the reader.	Show Device Logs	Opens a window that shows the reader logs. In this window, you can reload to pull the latest logs or download them as <code>.log</code> file.	Open DataMan WebHMI	Open the DataMan WebHMI in a new tab. For more information, see DataMan WebHMI on page 40 .
Button	Description												
Edit Device Network Settings	Modify the name, IP address, Subnet Mask, and Default Gateway of the reader. Enter the reader password if required.												
Flash LED	Remotely trigger the LED of the reader for easy identification.												
Reboot	Reboot the reader.												
Show Device Logs	Opens a window that shows the reader logs. In this window, you can reload to pull the latest logs or download them as <code>.log</code> file.												
Open DataMan WebHMI	Open the DataMan WebHMI in a new tab. For more information, see DataMan WebHMI on page 40 .												
<p>Password Protected</p>	<p>Indicates whether the reader is password protected.</p>												
<p>Primary</p>	<p>A check mark signifies the primary reader.</p>												
<p>Name</p>	<p>A customizable name of the reader.</p>												
<p>Type</p>	<p>The model of the reader.</p>												
<p>MAC Address</p>	<p>The MAC address of the reader.</p>												
<p>Firmware Version</p>	<p>The version of firmware installed on the reader.</p>												
<p>Address Type</p>	<p>Indicates network address type (DHCP or static) for the reader.</p>												
<p>IP Address</p>	<p>The IP address of the reader.</p>												
<p>Subnet Mask</p>	<p>The subnet mask of the reader.</p>												
<p>Gateway</p>	<p>The gateway of the reader.</p>												
<p>Source Network Interface</p>	<p>The Ethernet port the reader uses for connection.</p>												
<p>State</p>	<p>Displays the state of the reader, which can be:</p> <ul style="list-style-type: none"> • In Local Subnet • In Remote Subnet • In Remote Subnet Behind NAT • Waiting For DHCP • Misconfigured • Unknown 												
<p>Task Status</p>	<p>Displays the status of the task, such as rebooting, applying network settings, and name changes.</p>												

DataMan WebHMI

The DataMan WebHMI provides a live view of 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 readers and adjust reader settings from the DataMan WebHMI.



You can access the DataMan WebHMI for a connected reader from the DataMan page by clicking the icon labeled **Open DataMan WebHMI** in the **Actions** column of the selected reader.

Home







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

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

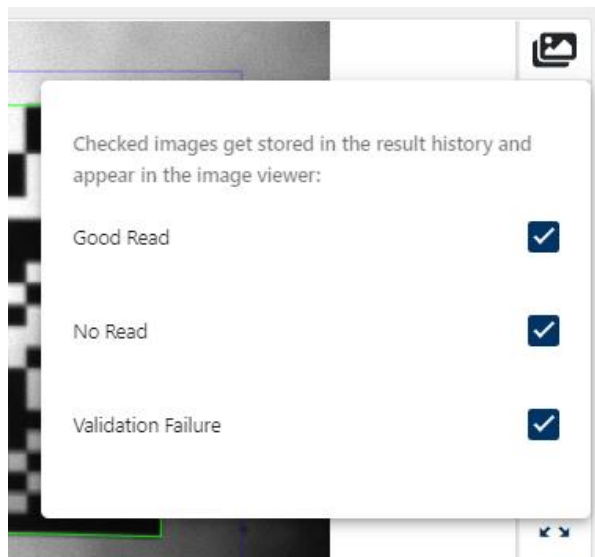
- **Read Rate** percentage
- Number of **Good Reads**
- Number of **No Reads**
- Number of **Triggers**

The display on the right side of the page provides a live feed of the reader 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 reader.



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

Click **Live** to show the live feed of the reader.

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

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

Click **Untrain** to untrain the reader.

Settings

The **Settings** page of the DataMan WebHMI allows you to manually change the reader configuration, upload, download, or save the current configuration, or reset the reader 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 reader.
- Click **Download** to save the reader configuration locally.
- Click **Save** to save the configuration on the reader flash memory.
- Click **Reset** to reset the reader configuration to default or a saved configuration.

The settings table provides you with detailed and in-depth configuration options for all reader 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 reader information, reader statistics, feature keys, and reader time.

The screenshot displays the COGNEX EI Tunnel Manager interface. At the top, there is a yellow navigation bar with 'COGNEX' and 'Home Actions Settings System'. Below this, the interface is divided into several sections:

- Device Information:** A grid of fields including Device Model, Serial Number, Device Name, MAC Address, IP Address, Firmware Version, Installed Hardware (LiquidLens, Custom), Bootloader Version, and OS Version.
- Reader Statistics:** A section with a 'Clear' button, containing metrics for Total Triggers (1,376,159), Total Reads (1,225,743), Read Rate (89.07%), Total No-Reads (150,416), No-Read Rate (10.93%), Missed Triggers (0), Passed Validations (0), Failed Validations (0), Buffer Overflows (0), Trigger Overruns (0), and Item Count (0).
- Feature Keys:** A list of supported features: 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:** Shows Local Time as Jan 26, 2019, 2:36:11 AM and Uptime as 601h 36m 13s.

Add DataMan Readers to Groups

Create device groups to organize and manage the configuration of your readers collectively.

Procedure

1. Click the **Menu** icon and go to the **DataMan** page of the Device Management app.
2. Select one or more readers or reader groups using the checkboxes.
3. Click the **Add Selected to Group** button.

The screenshot shows the 'DataMan' page in the COGNEX EI Tunnel Manager. The top navigation bar includes 'COGNEX | EI Tunnel Manager' and a breadcrumb trail 'Home > Device Management > DataMan'. Below the navigation are several action buttons: 'ADD SELECTED TO GROUP' (highlighted with a red box and an arrow), 'UPLOAD CONFIGURATION', 'UPLOAD FIRMWARE', 'DOWNLOAD AS CSV', and 'DISCOVER DEVICES'.

The main content area is titled 'Standalone Devices' and contains a table with the following columns: 'Actions', 'Password Protected', 'Primary', and 'Name'. The table lists five devices. The first three rows have their checkboxes checked (highlighted with a red box), indicating they are selected. Each row also contains icons for edit, refresh, menu, and delete.

4. In the window that pops up:

Multi Device Edit

Enable Group Triggering

Group* Primary Device*
Select an existing group or type a new group name. 4/31 Select the primary device from the list.

Actions	Primary	Name	Group	Address Type	IP Address	Subnet Mask	Gateway	Task Status
	<input checked="" type="checkbox"/>	10.86.98.100	10.86.98.100	Static	10.86.98.100	255.255.255.0	10.86.98.1	
	<input type="checkbox"/>	10.86.98.101	10.86.98.100	Static	10.86.98.101	255.255.255.0	10.86.98.1	
	<input type="checkbox"/>	10.86.98.102	10.86.98.100	Static	10.86.98.102	255.255.255.0	10.86.98.1	

Use DHCP

Mass Network Settings Generator Change network settings at once

- a. Type in the name of an existing group, or type a new group name.
- b. Select the primary reader in the group.
- c. Optionally, you can:
 - Reorder the readers in the group.
 - Flash the LEDs of the individual readers for easy identification.
 - Manually edit the network settings of each reader, or edit the network settings for every reader in the group with the **Use DHCP** toggle and the **Mass Network Settings Generator** option.

Note: When editing the IP address of readers in a group, the readers get sequential IP addresses. For example, if you enter 10.86.98.100 in the **IP Address** field, the first reader in the group gets the 10.86.98.100 address, and the other readers get 10.86.98.101, 10.86.98.102, and the subsequent addresses.

5. If editing a password-protected reader, enter the password.
6. Click **Submit**.

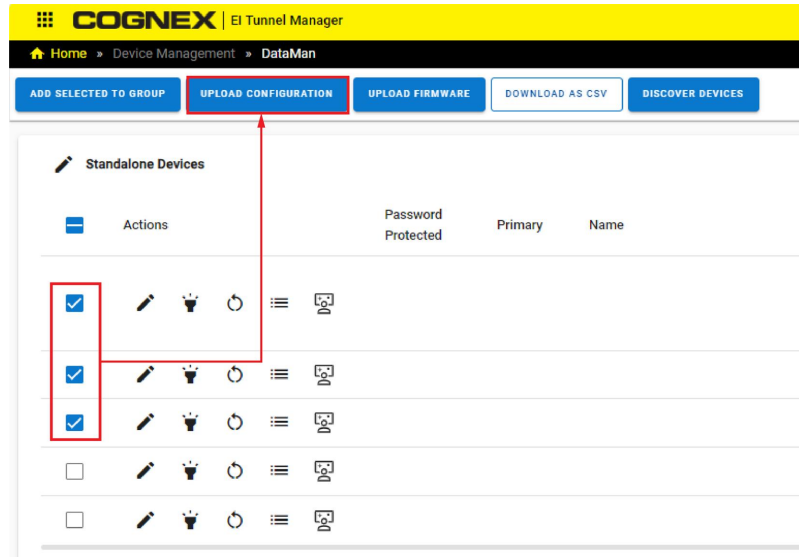
Upload Configuration to DataMan Readers

Upload a configuration file to one or more readers to apply the same configuration to multiple readers in one batch.

Procedure

1. Click the **Menu** icon and go to the **DataMan** page of the Device Management app.
2. Select one or more readers or reader groups using the checkboxes.

3. Click the **Upload Configuration** button.



4. Click **Browse** in the window that pops up.
5. Select the configuration file for upload.
6. If you want to apply network settings, enable the **Apply Network Settings** toggle.

Note: When uploading configuration to multiple readers, this option is disabled.

7. If editing a password-protected reader, enter the password.
8. Click **Submit**.

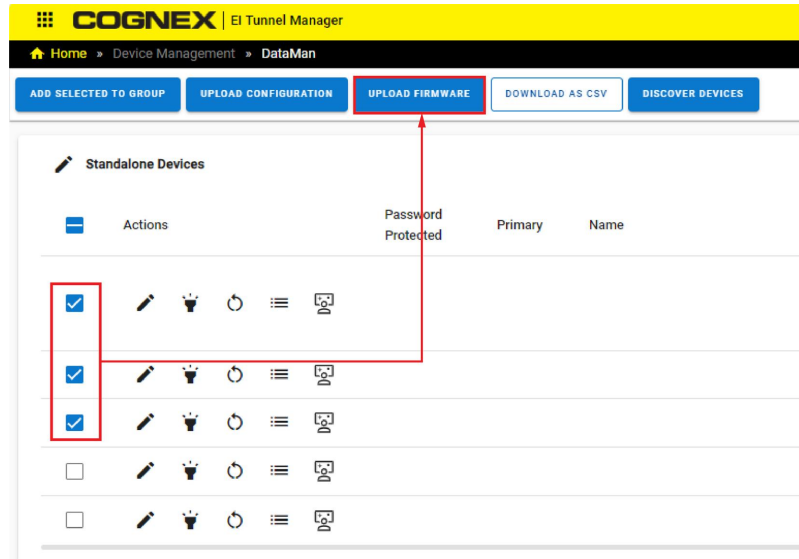
Upload Firmware to DataMan Readers

Upload a firmware file to one or more readers to update the firmware of multiple readers in one batch.

Procedure

1. Click the **Menu** icon and go to the **DataMan** page of the Device Management app.
2. Select one or more readers or reader groups using the checkboxes.

3. Click the **Upload firmware** button.



4. Click **Browse** in the window that pops up.
5. Select the firmware file for upload.
6. If editing a password-protected reader, enter the password.
7. Click **Submit**.

Other Devices

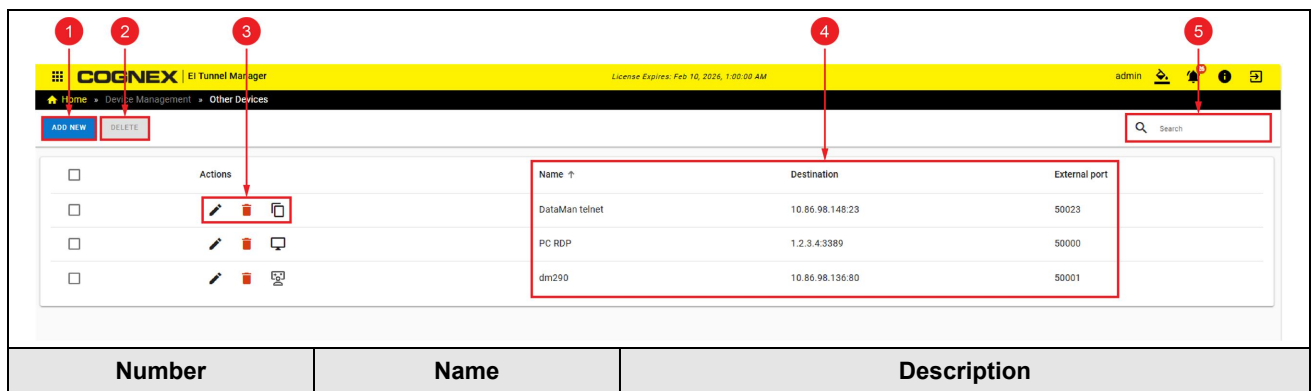
The Other Devices page allows you to create a connection between the production network and devices on the subnet of an El Tunnel Manager unit. The connection uses port forwarding to access the device through the IP address of the El Tunnel Manager unit. Using this method, you can connect to devices such as a reader, dimensioner, network switch, or computer.

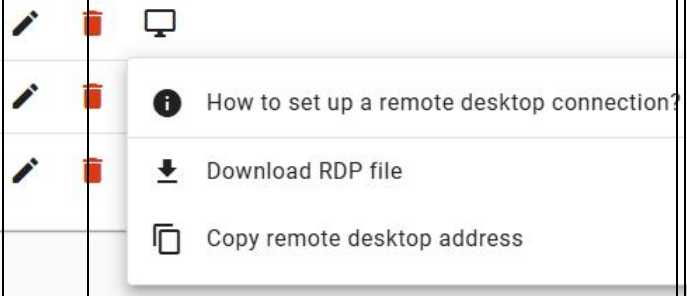
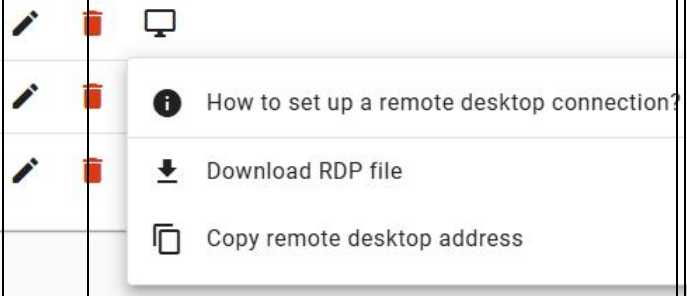
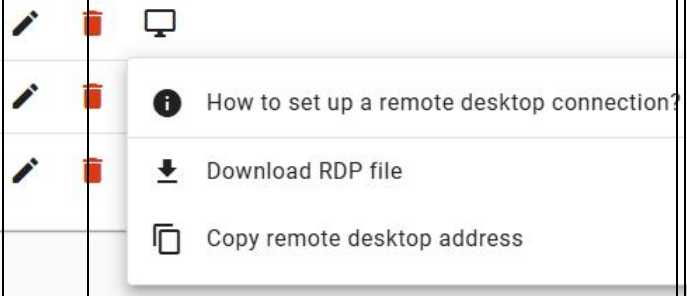
The following examples are typical use cases for port forwarding:

- Accessing the WebHMI of a DataMan reader or a 3D-A1000 dimensioner
- Connecting to a laptop through remote desktop

Features of the Other Devices User Interface

At first, the Other Devices page only provides an option to create a new connection. The connections you create appear in a list along with their name and network details. The list provides options to edit, delete, access, or filter your connections.



1	Add New button	Opens the form where you can create a connection for a device.												
2	Delete button	Deletes the selected connections. This button only becomes active after you select one or more connections from the list.												
3	Actions	<p>Several actions are available for each connection in the list.</p> <table border="1" data-bbox="736 331 1412 1499"> <thead> <tr> <th data-bbox="736 331 822 415">Action</th> <th data-bbox="822 331 1412 415">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="736 415 822 527">Edit</td> <td data-bbox="822 415 1412 527">Allows you to edit the connection. This action opens the same form used when creating the port forwarding configuration.</td> </tr> <tr> <td data-bbox="736 527 822 573">Delete</td> <td data-bbox="822 527 1412 573">Deletes a connection.</td> </tr> <tr> <td data-bbox="736 573 822 751">Copy Device Address</td> <td data-bbox="822 573 1412 751">Copies the IP address and port number of the device to the clipboard. This action is available only if you select the Other Destination Type when creating the configuration.</td> </tr> <tr> <td data-bbox="736 751 822 1388">Remote Desktop</td> <td data-bbox="822 751 1412 1388"> <p>Downloads an <i>.rdp</i> file for connecting remotely or copies the remote desktop address to the clipboard, depending on the sub-option you select.</p>  <p>This action is available only if you select the Remote Desktop Destination Type when creating the configuration.</p> <p>Note: For more information about using an <i>.rdp</i> file, see the in-app help.</p> </td> </tr> <tr> <td data-bbox="736 1388 822 1499">Open WebHMI</td> <td data-bbox="822 1388 1412 1499">Opens the WebHMI of the device. This action is available only if you select the WebHMI Destination Type when creating the configuration.</td> </tr> </tbody> </table>	Action	Description	Edit	Allows you to edit the connection. This action opens the same form used when creating the port forwarding configuration.	Delete	Deletes a connection.	Copy Device Address	Copies the IP address and port number of the device to the clipboard. This action is available only if you select the Other Destination Type when creating the configuration.	Remote Desktop	<p>Downloads an <i>.rdp</i> file for connecting remotely or copies the remote desktop address to the clipboard, depending on the sub-option you select.</p>  <p>This action is available only if you select the Remote Desktop Destination Type when creating the configuration.</p> <p>Note: For more information about using an <i>.rdp</i> file, see the in-app help.</p>	Open WebHMI	Opens the WebHMI of the device. This action is available only if you select the WebHMI Destination Type when creating the configuration.
Action	Description													
Edit	Allows you to edit the connection. This action opens the same form used when creating the port forwarding configuration.													
Delete	Deletes a connection.													
Copy Device Address	Copies the IP address and port number of the device to the clipboard. This action is available only if you select the Other Destination Type when creating the configuration.													
Remote Desktop	<p>Downloads an <i>.rdp</i> file for connecting remotely or copies the remote desktop address to the clipboard, depending on the sub-option you select.</p>  <p>This action is available only if you select the Remote Desktop Destination Type when creating the configuration.</p> <p>Note: For more information about using an <i>.rdp</i> file, see the in-app help.</p>													
Open WebHMI	Opens the WebHMI of the device. This action is available only if you select the WebHMI Destination Type when creating the configuration.													
4	Connection details	<p>The connection list shows details for each connection.</p> <ul style="list-style-type: none"> • Name: The unique name given when adding a new connection. • Destination: The IP address and port of the device. • External Port: The port by which you can access the device through the EI Tunnel Manager unit. 												
5	Search field	Filters the connection list. Enter any detail (name, destination, external port) to quickly find a specific connection.												

Connect to Other Devices

You can connect from the production network to devices on the subnet of an EI Tunnel Manager unit by creating a port-forwarding configuration.

Prerequisites

Obtain the IP address and the port of the device you want to access.

Procedure

To create a new connection:

1. Open the **Apps** menu and select the [Other Devices on page 48](#) page of the Device Management app.
2. Click **Add New**, which opens the form where you can configure port forwarding for a device.

3. Fill in the required fields:

Required Fields	Description
Name	The unique name of the connection. The name can only contain lowercase and uppercase letters, numbers, spaces, periods, hyphens, and underscores.
Destination Type	The type of access you want to configure for the device. Select an option from the dropdown menu: <ul style="list-style-type: none"> • WebHMI: Adds a button on the Other Devices page that opens the WebHMI of the device. • Remote Desktop: Adds a button on the Other Devices page that downloads an <i>.rdp</i> file for connecting remotely or copies the remote desktop address to the clipboard. • Other: Adds a button to the Other Devices page that copies the IP address and port number of the device to the clipboard.
Destination IP	The IP address of the device that you want to access. Ensure that each Destination IP and Destination Port combination is unique among your connections. <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> Note: The Destination IP cannot be the IP address of the EI Tunnel Manager unit. </div>
Destination port	The port of the device that you want to access. You can use any of the valid ports of the device. If you do not know which port to use, consider the following examples: <ul style="list-style-type: none"> • Port 80 for HTTP • Port 443 for HTTPs • Port 3389 for a remote desktop connection

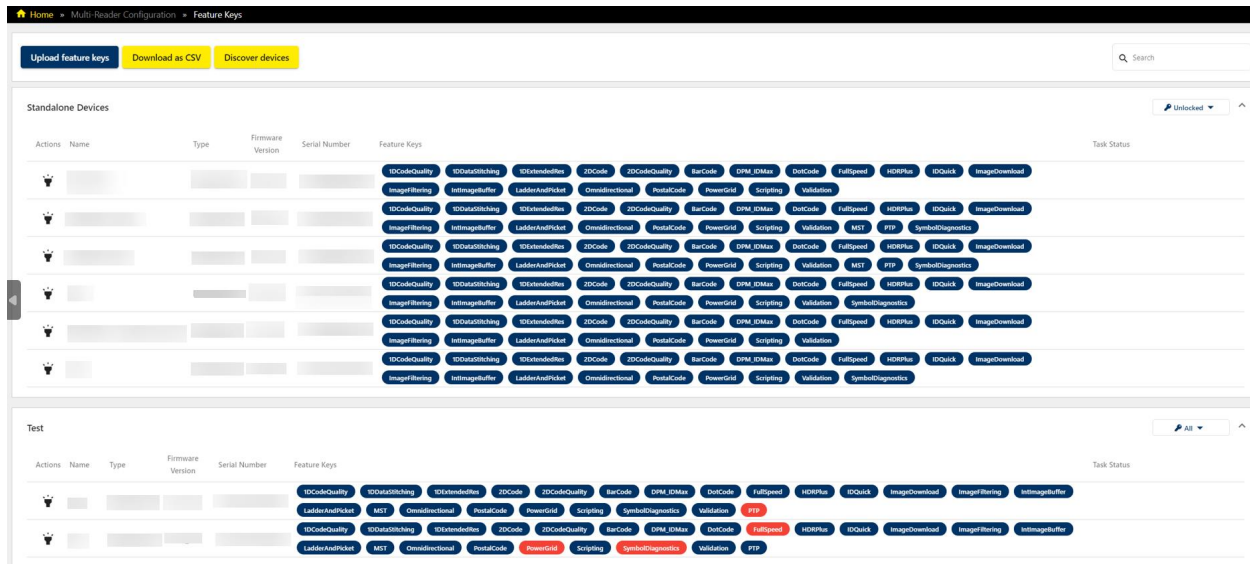
- Option: To configure a specific open port of the EI Tunnel Manager unit for port forwarding, fill out the **External port** field. You have to use a unique external port for each connection. The available range is 50000-59999.

Note: If you leave the **External port** field empty, the EI Tunnel Manager unit automatically assigns a suitable port.

- Click **Save**.

Feature Keys

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



The following actions are available:

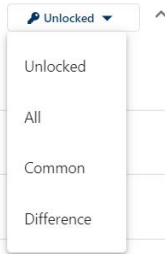
- Uploading feature key files
- Downloading Feature Keys page information in CSV
- Discovering devices

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:

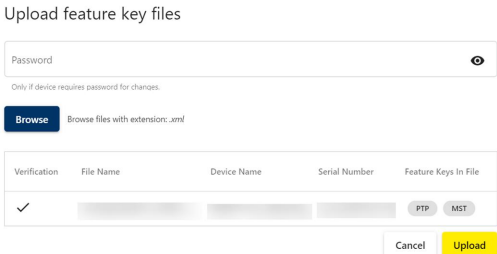
Feature Key Color	Description
BLUE	The feature is unlocked for the device.
RED	The feature is unlocked for some devices in the group, but not for the respective device.

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:



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.
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.

Tunnel Setup

The Tunnel Setup app allows you to perform dynamic tests and 3D calibration on your device.

Dynamic Test

Dynamic Test is a diagnostic tool in the Tunnel Setup app. The test allows you to validate the proper functioning of your vision tunnel. During the initial commissioning of the vision tunnel, Cognex engineers use this test to validate that the vision tunnel functions properly. The engineers ensure that the test is run correctly, and they address all issues. It is a standard procedure for new installations.

While the test is typically part of the installation process, you can rerun the test any time to validate that the vision tunnel still functions correctly. If you run into an error during the test, refreshing the page can likely solve the error. If the error persists, contact Cognex technical support for further assistance.

Note: The Dynamic Test can have variations to fit various vision tunnel designs. This document describes one common type of Dynamic Test but you might have a different variation. Despite this, most of the guidance here is still relevant.

- In some variations, the test includes only a center position, without the left- and right-justified tests.
- Certain variations allow you to skip the encoder check or do not include it at all. This is more common when using a non-belted conveyor, such as a tilt tray, crossbelt, or bomb-bay system.

Prepare the Target Box for the Test

The Dynamic Test uses a special target box that you have to build specifically for the purpose of the test. The box and a sheet of adhesive 1D and 2D code labels comes with the tunnel delivery.

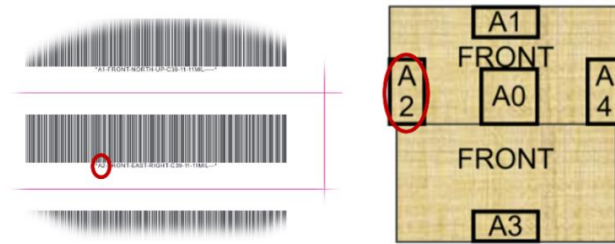
Prerequisites

Locate the box and the sheet of adhesive 1D and 2D code labels.

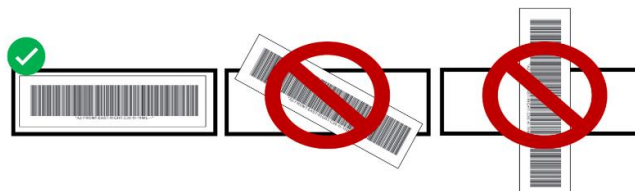
Procedure

To prepare the box for the test:

1. Build the box.
2. Adjust the height of the box to the maximum height supported by the vision tunnel.
3. Apply each code label within the corresponding rectangular outline on the box.
 - a. Match the first two characters of the code content and the two characters printed within the rectangle.



- b. Apply the label within the rectangle printed on the box.

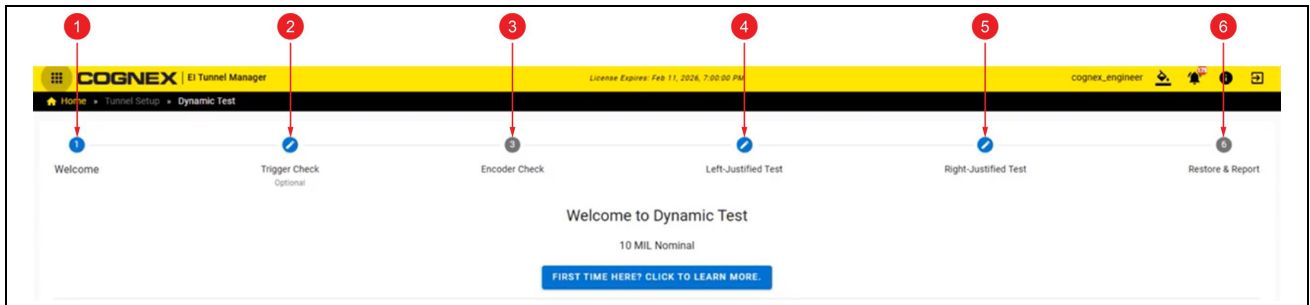


Steps of the Dynamic Test

During the Dynamic Test, you physically run a target box, specifically built for the test, through the vision tunnel multiple times. The readers take images of the box as it runs through the vision tunnel on the conveyor belt. While the box runs on the conveyor belt, you navigate through the steps of the test in the user interface of your El Tunnel Manager unit. The test validates the proper functioning of the vision tunnel and gives you visual feedback and detailed test results in the user interface for each step.

The test consists of six steps, which you can access through the Dynamic Test page of the Tunnel Setup app. The user interface guides you through the steps. The test is mostly automatic and it requires little user input.

The following image shows the steps of the test in order.



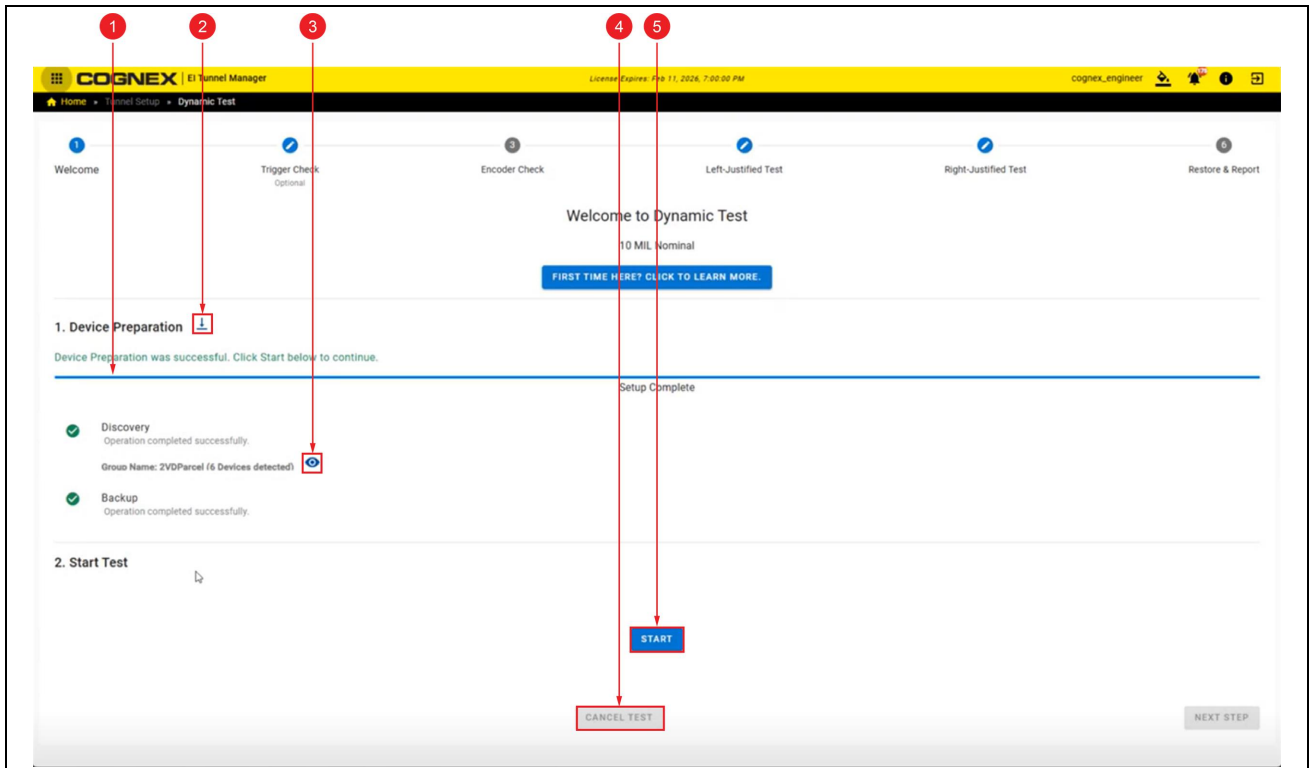
Step	Description
1	The Welcome on page 54 step prepares the readers on the vision tunnel for the test.
2	Trigger Check on page 55 is an optional step, which validates whether the box passing through the vision tunnel correctly triggers the readers.
3	The Encoder Check on page 56 step validates whether each reader is receiving an encoder signal.
4	The Left-Justified Test on page 57 step validates that the readers properly read barcodes if the box is running on the left side of the conveyor belt.
5	The Right-Justified Test step is similar to the Left-Justified Test , but the box is running on the right side of the conveyor belt.
6	The Restore & Report on page 60 step restores the readers to their original settings and allows you to generate and download a report of the test results.

Welcome

This step prepares the readers on the vision tunnel for the test as follows:

1. Runs device discovery to discover the Multi-Reader Sync (MRS) group of the vision tunnel.
2. Makes backups of the reader settings.
3. Modifies the reader settings for the purposes of the test.

Note: At the end of the test, the app restores the original settings of your readers and reboots them. You can manually download the backups, but it is not necessary.

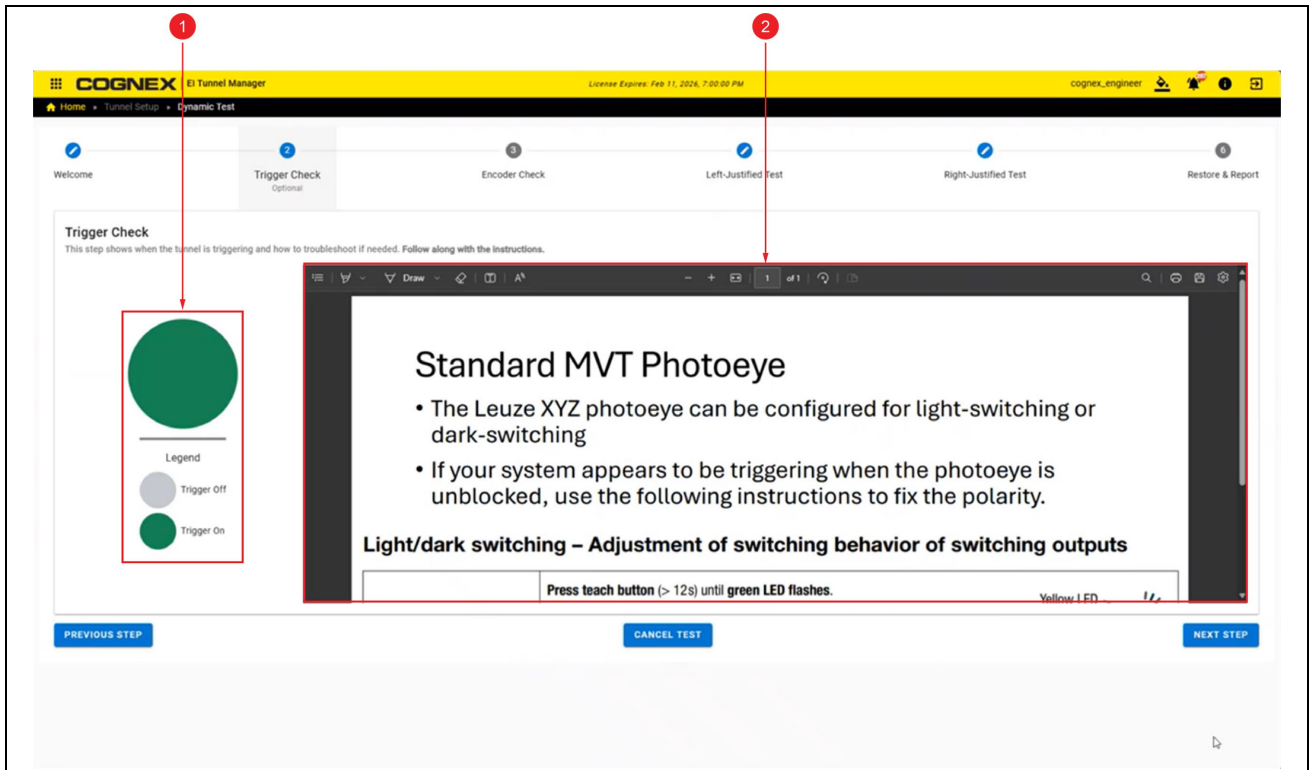


Number	Description
1	The progress bar gives you information about the status of the current step of the test.
2	Click the download button to manually download the backups.
3	Click the eye icon to access detailed information about the readers in the MRS group.
4	Click Cancel Test if you want to cancel the test for any reason. If you cancel the test, the app automatically restores the original settings of your reader.
5	Click Start to proceed to the next step.

Trigger Check

The **Trigger Check** step helps you to validate whether the box passing through the vision tunnel correctly triggers the readers. This is an optional step, which means that you can skip this step and still complete the test. If there is a problem with triggering, however, the test might fail because of it.

Vision tunnels typically use a photoeye to control the triggering. The photoeye, also known as a photoelectric sensor, detects the presence or absence of boxes using a light beam. When a box interrupts the light beam, the photoeye senses this change and sends out a signal that turns the trigger on. The test validates whether the trigger signal and the trigger delay settings are correct.

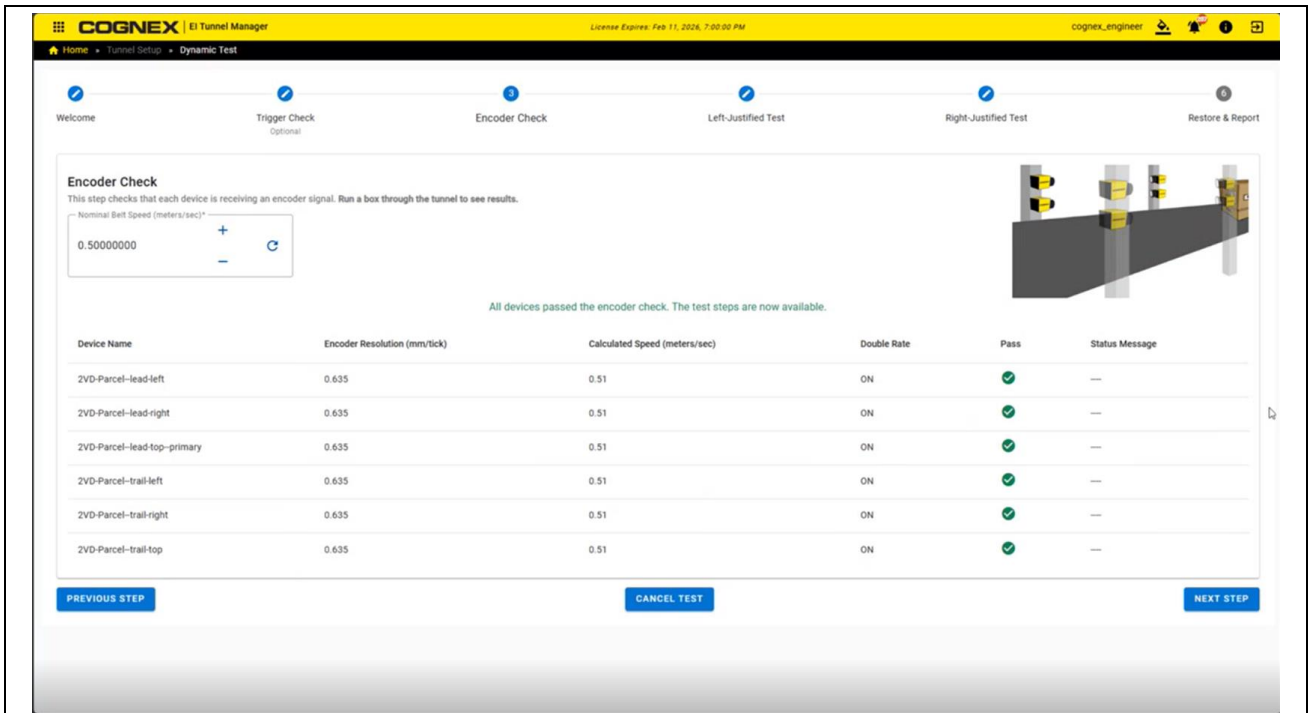


Number	Description
1	The green circle on the left side of the user interface shows that the trigger is currently on. If the circle is grey, the trigger is currently off. As the box passes through the vision tunnel, validate that the trigger turns on and off at the correct time.
2	The Trigger Check step shows instructions for fixing common problems with the photoeye. The instructions appear on the right side of the user interface.

Encoder Check

In the **Encoder Check** step, first specify the normal speed of your conveyor belt using the input field. Then run the target box through the vision tunnel to validate that each reader is receiving an encoder signal.

After the box passes through the vision tunnel, the results appear in the user interface. Each line represents a reader and provides the following details:



Element	Description
Device Name	The name of the reader.
Encoder Resolution	This is a setting of the reader.
Calculated Belt Speed	The calculated belt speed is computed based on encoder pulses received by the reader, the encoder resolution, and the trigger time. Note: Inconsistent calculated speed results can indicate physical (electrical wiring, mechanical coupling) problems or configuration errors.
Double Rate	This is a setting of the reader.
Pass	A green check mark or a red X, indicating whether the test passed or failed.
Status Message	Provides additional information about the reason why the test failed.

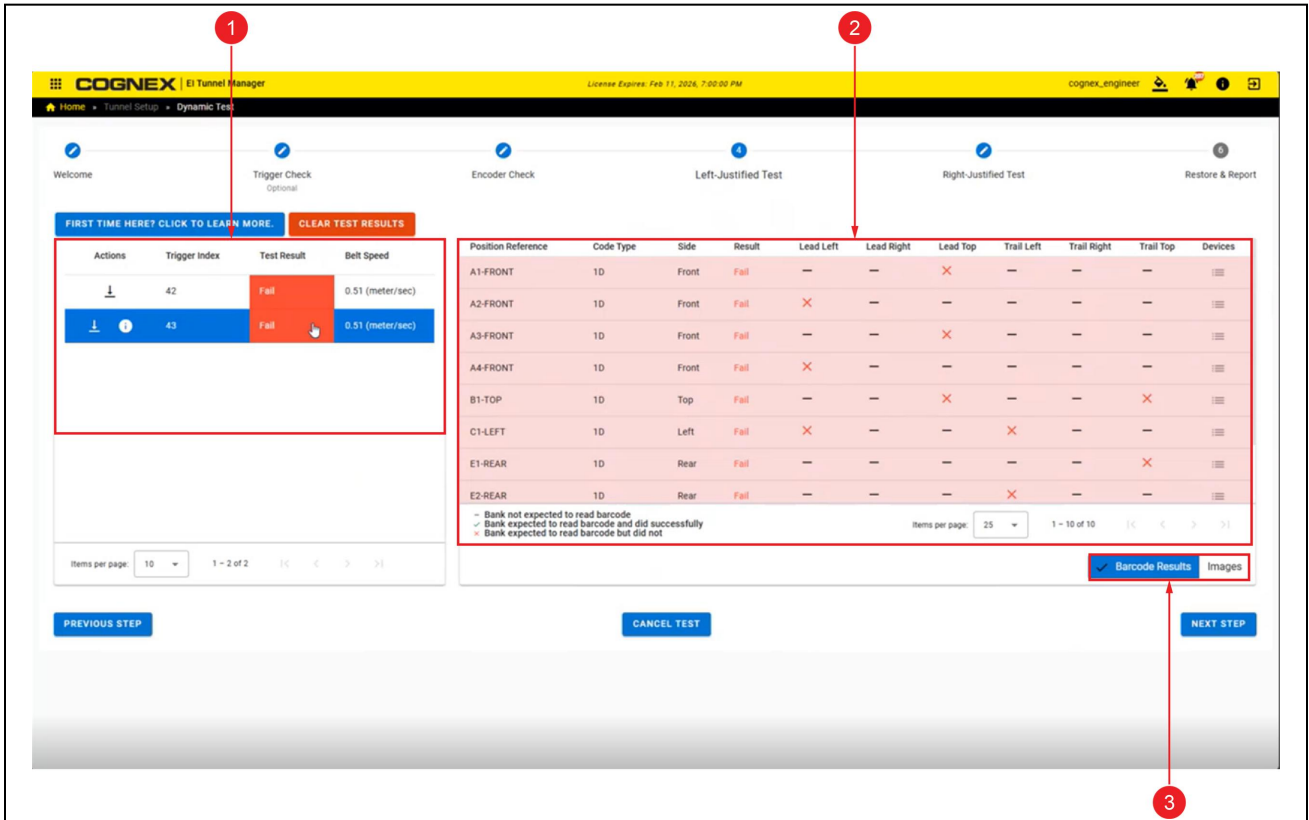
Left-Justified Test

The **Left-Justified Test** step involves running the target box through the vision tunnel. You place the box on the left side of the conveyor belt with the front of the box facing downstream. The test validates whether the readers can read the various codes on the target box in this position.

After the target box passes through the vision tunnel, the test results appear in the left side of the user interface, with one row for each test run. If you select a row, more detailed test results appear in the right side of the user interface. A green check mark indicates that the test passed, while a red X indicates that the test failed.

- At belt speeds of less than 300 fpm, every code needs to be read at least once.
- At faster belt speeds, each code needs to be read by the specific banks (group of readers on the vision tunnel).

Note: The **Right-Justified Test** step is similar to the **Left-Justified Test**, but the box is placed on the right side of the conveyor belt instead of the left side.



Number	Description
1	<p>In this section, the results of each test run appear after the box passes through the vision tunnel.</p> <ul style="list-style-type: none"> Actions column: <ul style="list-style-type: none"> Click the download icon to download detailed information about the barcodes read by the readers. Click the information button to see the same details in a pop-up window. Trigger Index: The index number assigned by the reader associated with the test run. Test Result: Can be Pass or Fail. Belt Speed: The speed of the conveyor belt at the time of the read. <p>To get more details about a test run in the right side of the user interface, click one of the rows.</p> <p>To clear the results in this section, click the Clear Test Results button.</p>

2

This section provides more detailed information about the selected test result. Using this information, you can determine which specific tests passed or failed. The details only appear in this section after you have selected one of the tests in the previous section.

The image shows the **Barcode Results** tab, which displays a table of the barcodes used in the test and the readers expected to read them.

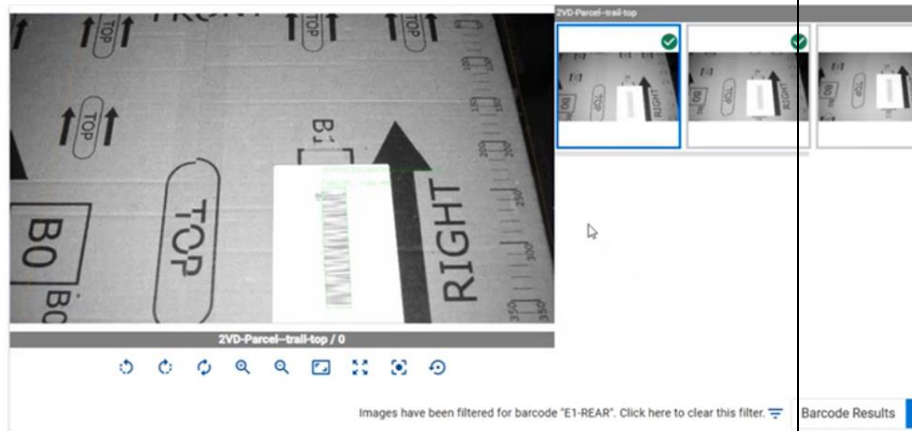
The **Barcode Results** tab provides the following information:

- **Position Reference:** The area on the box where the specific barcode is applied.
- **Code Type:** The type of the barcode, such as 1D or 2D.
- **Side:** The side of the target box where the specific barcode is applied.
- **Result:** Can be **Pass** or **Fail**. This indicates whether the bank was able to read the barcode as expected.
- From **Lead Left** to **Trail Top:** These refer to the banks of your vision tunnel. Each bank is expected to read a specific barcode on the target box.
- **Devices:** Click the icons in this column to access more details about your readers in a pop-up window.

Not all banks are expected to read every barcode on the box.

- A blank (-) appears in the table if a bank was not supposed to read a specific barcode.
- A green check mark indicates that the bank was expected to read the barcode and it was a good read.
- A red **X** indicates that the bank was expected to read the barcode but it was a no-read.

If you click on a specific test in the **Barcode Results** tab, you are taken to the corresponding image in the **Images** tab.



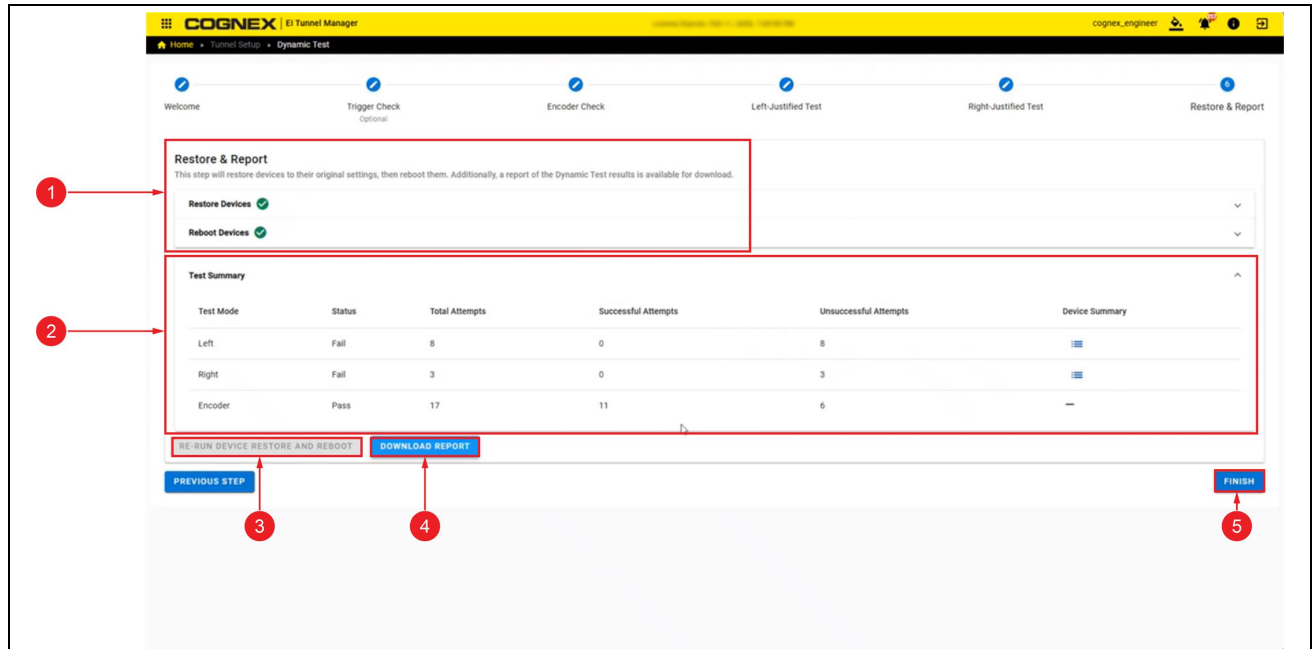
3

Click these buttons to switch between the **Barcode Results** view and the **Images** tabs.

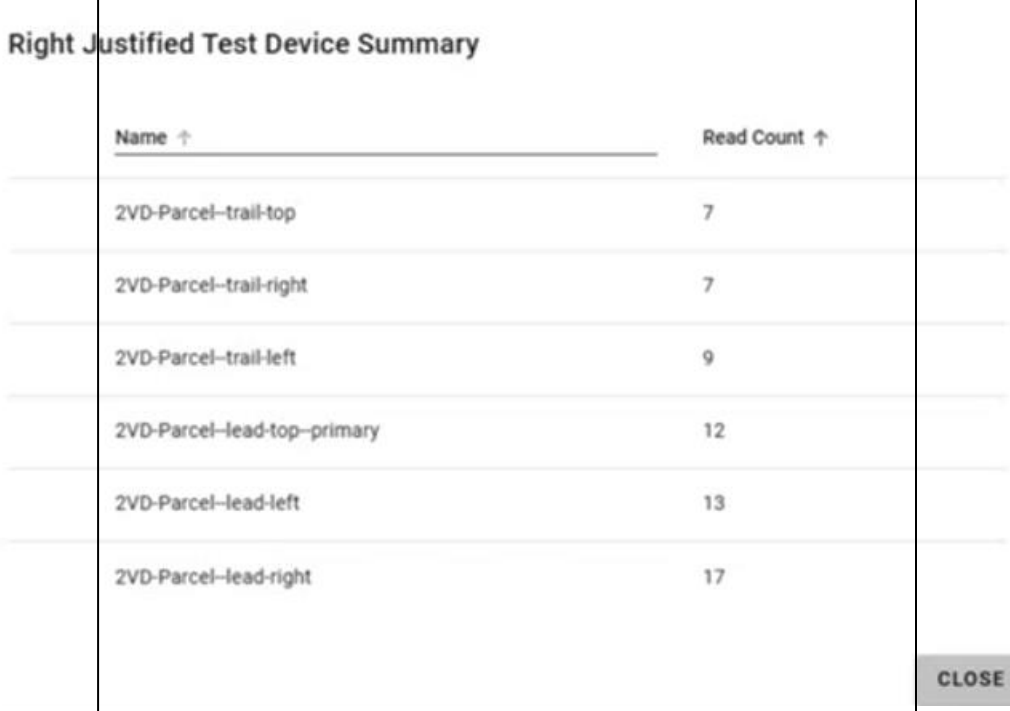
Restore & Report

The **Restore & Report** step automatically restores the readers to the original settings and reboots them to ensure that all settings are effective. After the reboot, the test summary appears in the user interface. You can download the report as a *.pdf*.

The summary includes the number of attempts, indicating how many times you ran the target box through the vision tunnel, and the number of failed attempts. Ideally, the summary should show that the box ran through the vision tunnel a few times and the test passes every time.



Number	Description
1	The Restore & Report section indicates the status of reader restoration and reboots. After the readers reboot, the results appear in the Test Summary section.

2	<p>The Test Summary section provides a quick overview of the mandatory tests and their results.</p> <ul style="list-style-type: none"> • Test Mode: Refers to the test, such as Left-Justified Test. • Status: Can be Pass or Fail. • Attempts: Refers to the number of times you ran the target box through the vision tunnel. The Test Summary lists the total number of attempts, and the number of successful and unsuccessful attempts. <p>Click the buttons in the Device Summary column to access additional information about how many codes the different readers read.</p>  <p>Right Justified Test Device Summary</p> <table border="1"> <thead> <tr> <th>Name ↑</th> <th>Read Count ↑</th> </tr> </thead> <tbody> <tr> <td>2VD-Parcel-trail-top</td> <td>7</td> </tr> <tr> <td>2VD-Parcel-trail-right</td> <td>7</td> </tr> <tr> <td>2VD-Parcel-trail-left</td> <td>9</td> </tr> <tr> <td>2VD-Parcel-lead-top-primary</td> <td>12</td> </tr> <tr> <td>2VD-Parcel-lead-left</td> <td>13</td> </tr> <tr> <td>2VD-Parcel-lead-right</td> <td>17</td> </tr> </tbody> </table> <p style="text-align: right;">CLOSE</p>	Name ↑	Read Count ↑	2VD-Parcel-trail-top	7	2VD-Parcel-trail-right	7	2VD-Parcel-trail-left	9	2VD-Parcel-lead-top-primary	12	2VD-Parcel-lead-left	13	2VD-Parcel-lead-right	17
Name ↑	Read Count ↑														
2VD-Parcel-trail-top	7														
2VD-Parcel-trail-right	7														
2VD-Parcel-trail-left	9														
2VD-Parcel-lead-top-primary	12														
2VD-Parcel-lead-left	13														
2VD-Parcel-lead-right	17														
3	<p>Click the Re-Run Device Restore and Reboot button to re-attempt failed reader restorations or reboots.</p>														
4	<p>Click the Generate Report button to download the test report as <i>.pdf</i>. For more information, see Generate Dynamic Test Report on page 64.</p>														
5	<p>Click the Finish button to return to the EI Tunnel Manager home page.</p>														

Run a Dynamic Test

The [Dynamic Test on page 52](#) involves running the target box through the vision tunnel multiple times, allowing the readers to take images and validate the proper functioning of the vision tunnel. The test consists of six steps, which are mostly automated and require minimal user input.

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

Prerequisites

Before you start, ensure that the following prerequisites are met:

- Learn about the test and its various steps by reading [Steps of the Dynamic Test on page 53](#)
- [Prepare the Target Box for the Test on page 53](#)
- Add weight to the box to ensure it stays on the conveyor belt. Always give the box enough distance before the vision tunnel, so it moves through at full speed.

Procedure

To run the dynamic test:

1. Open the **Apps** menu and select the Dynamic Test page of the Tunnel Setup app. You are now at the [Welcome on page 54](#) step.
 - a. Wait until the app finishes preparing your readers.
 - b. To continue to the [Trigger Check on page 55](#) step, click **Start**.
2. Option: In the **Trigger Check** step, validate that the readers are triggered correctly.
 - a. To validate the trigger settings, run the box through the vision tunnel, and validate that the trigger turns on and off at the correct time.
 - b. If the check fails, follow the instructions on the right side of the user interface to fix common problems with the photoeye.
 - c. To continue to the [Encoder Check on page 56](#) step, click **Next Step**.
3. In the **Encoder Check** step, first set the **Nominal Belt Speed** to the actual speed of your conveyor belt.
 - a. Place the box on the conveyor belt.
 - b. Bring your conveyor belt up to full production speed and run the box through the vision tunnel.
 - c. If any of the readers fail the check:
 - i. Review and note the messages in the status message column.
 - ii. If errors are returned on subsequent runs, click **Cancel Test**, which restores the readers to the original settings.
 - iii. Fix the encoder errors, for example using DataMan Setup Tool then restart the Dynamic Test.
 - d. If every reader passes the test, click **Next Step** to continue to the [Left-Justified Test on page 57](#) step.

4. In the **Left-Justified Test** step:

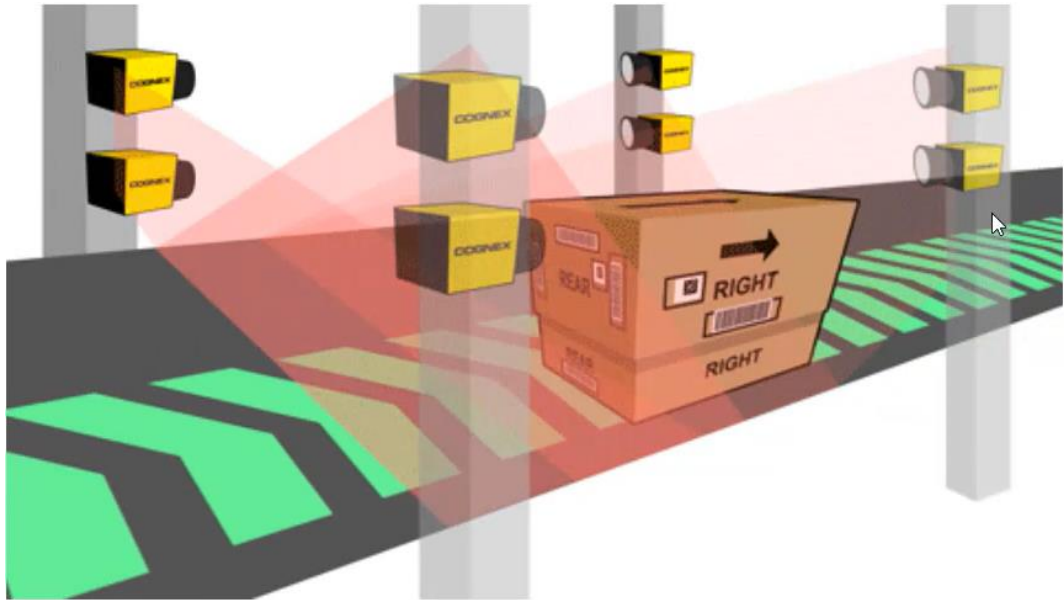
- a. Place the box on the left side of the conveyor belt with the front side of the box facing downstream.



- b. Run the box through the vision tunnel. If possible, run the box 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).
- c. As the box runs through the vision tunnel, the test results appear in the user interface.
 - If any **Xs** appear, it indicates that a test failed.
 - To review the no-read image, click on the row that has an **X**. Reviewing the image can tell you why the reader could not read the barcode.
 - You might have to run the box multiple times through the vision tunnel to pass.
 - If all of the rows have green check marks, it means that the readers can read the barcodes correctly.
- d. To continue to the **Right-Justified Test** step, click **Next Step**.

5. In the **Right-Justified Test** step:

- a. Place the box on the right side of the conveyor belt with the front side of the box facing downstream. Otherwise, this step has the same workflow as the previous step.



- b. Run the box through the vision tunnel the same as in the previous step, then review the results.
- c. If all of the rows have green check marks, click **Next Step** and the **Complete Dynamic Test** pop-up appears.

6. To complete the test and continue to the next step, click **Confirm**.

After the Procedure

- The [Restore & Report on page 60](#) step automatically restores your readers to their original settings.
- Option: Generate and download a report of the test results. For more information, see [Generate Dynamic Test Report on page 64](#).

Generate Dynamic Test Report

In the **Restore & Report** step of the [Dynamic Test on page 52](#), you can download the test report in *.pdf* format.

To generate and download the test report:

1. In the **Restore & Report** step of the Dynamic Test, click **Download Report**.
2. Fill in the details in the pop-up window.
3. Click **Generate Report**, which automatically downloads the file into the download directory on your computer.

3D Field Calibration

The 3D Field Calibration page 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

The speed of the belt when run normally.

Calibration Belt Speed * feet/minute

The speed of the belt when performing a calibration.

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

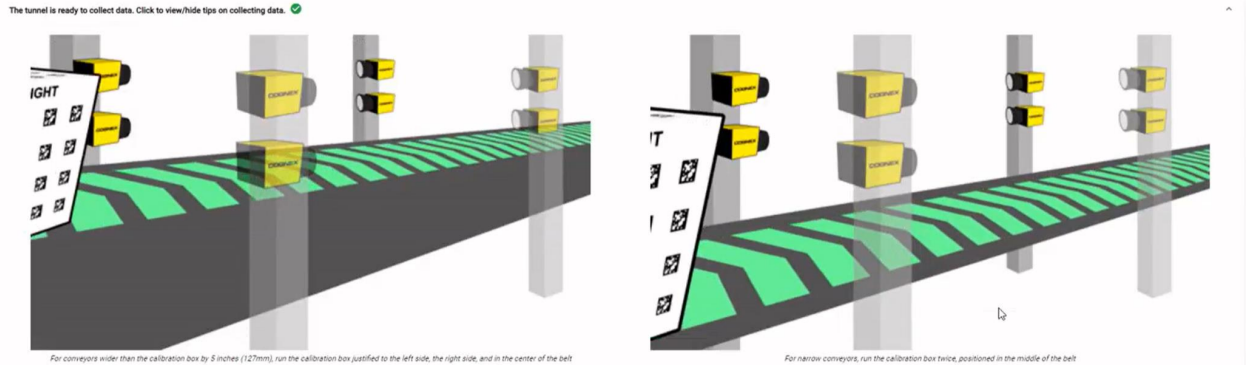
Re-Run All Validations

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

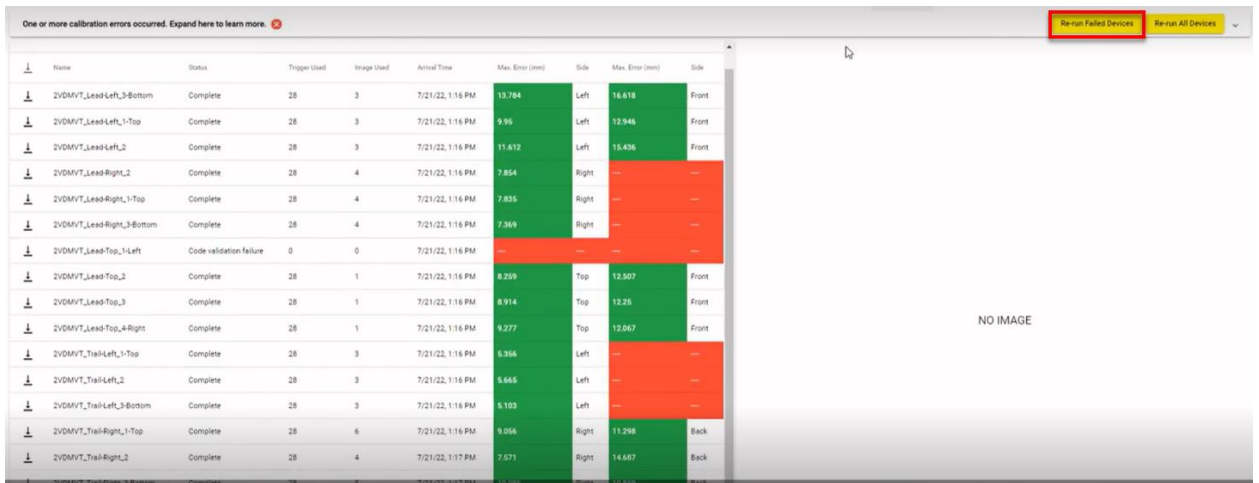
If the conveyor is narrow, place the box at the center of the belt and run it through twice.

- 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.



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_Trail-Right_1-Top	Complete	28	6	7/21/22, 1:16 PM	9.056	Right	11.298	Back	
2VDMVT_Trail-Right_2	Complete	28	4	7/21/22, 1:17 PM	7.571	Right	14.667	Back	
2VDMVT_Trail-Right_3-Bottom	Complete	28	5	7/21/22, 1:17 PM	10.095	Right	10.859	Back	
2VDMVT_Trail-Top_2	Complete	28	8	7/21/22, 1:17 PM	6.635	Top	4.663	Back	
2VDMVT_Trail-Top_3	Complete	28	8	7/21/22, 1:17 PM	4.799	Top	9.083	Back	
2VDMVT_Trail-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 app provides a method of storing and organizing data obtained from your readers, such as downloaded images and trigger sequences.

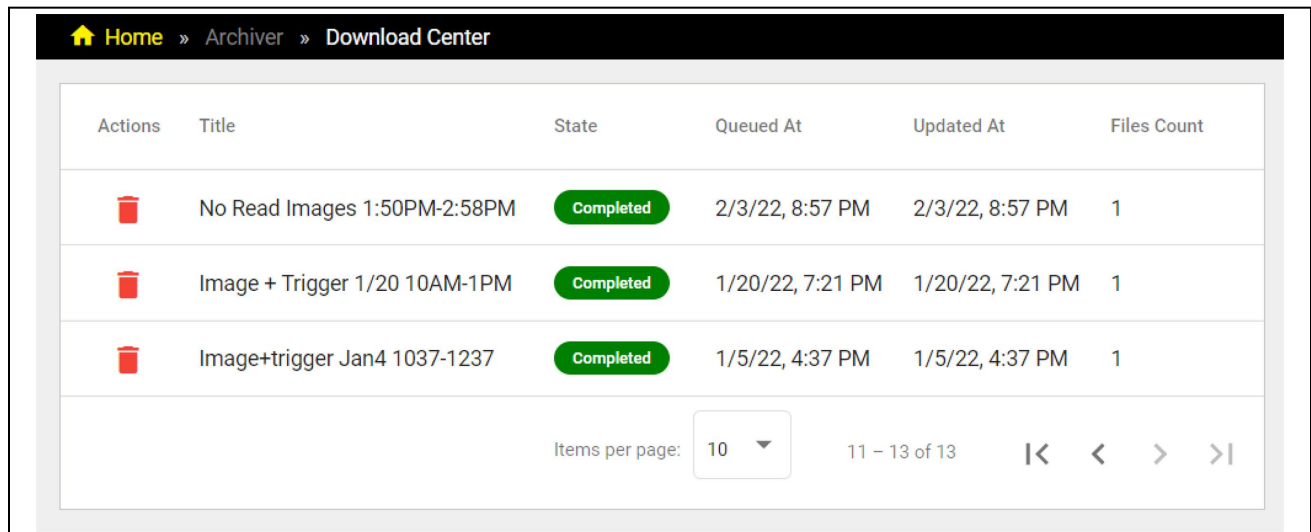
Download Center

The Download Center page allows you to manage your current and historical archives.

When you download image or trigger data from the Results Explorer page, Unit stores it in an archive file. Downloaded archives reside on the hard drive of the Unit 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, Unit generates one or more archives. The size limit for a single archive is 1 GB. When the remaining disk space approaches approximately 50 GB, Unit 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. Unit 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, Unit 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.

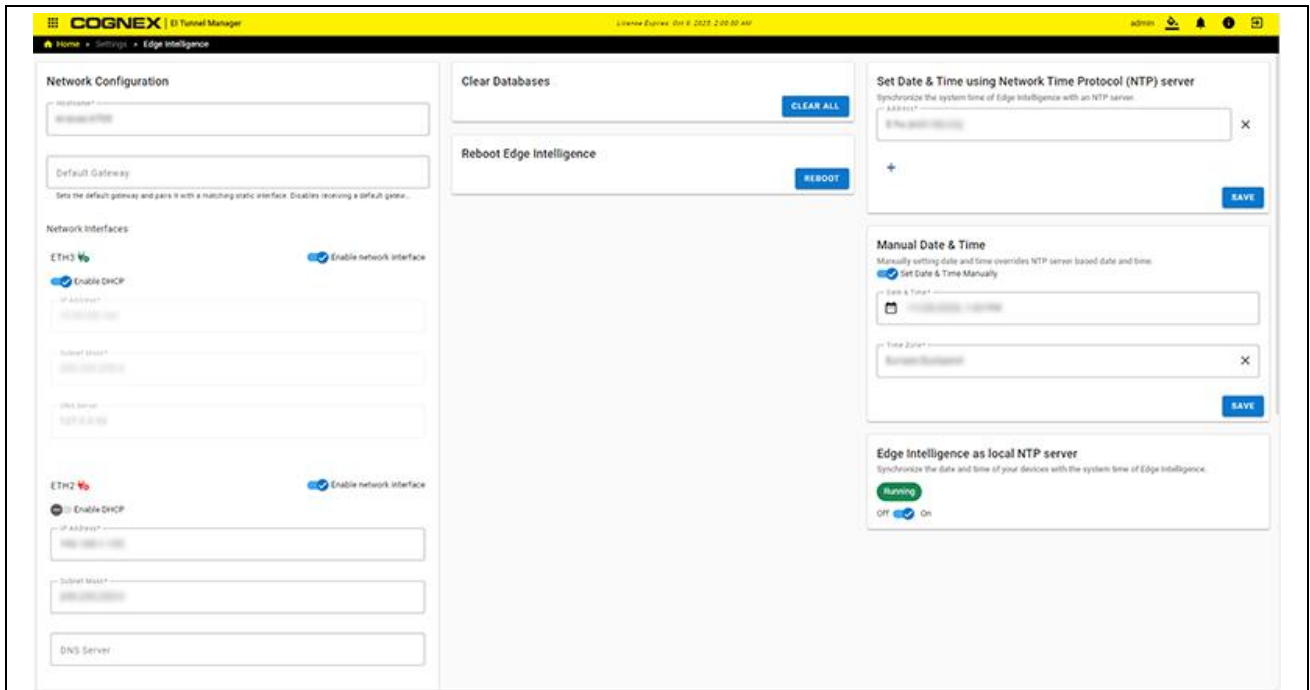
- Navigate to the folder on your computer that contains all the downloaded partial ZIP files.
- Right-click on the file with ZIP extension.
- Click on the ZIP file extractor.
- Click on **Extract to** to merge all partial files.

Settings

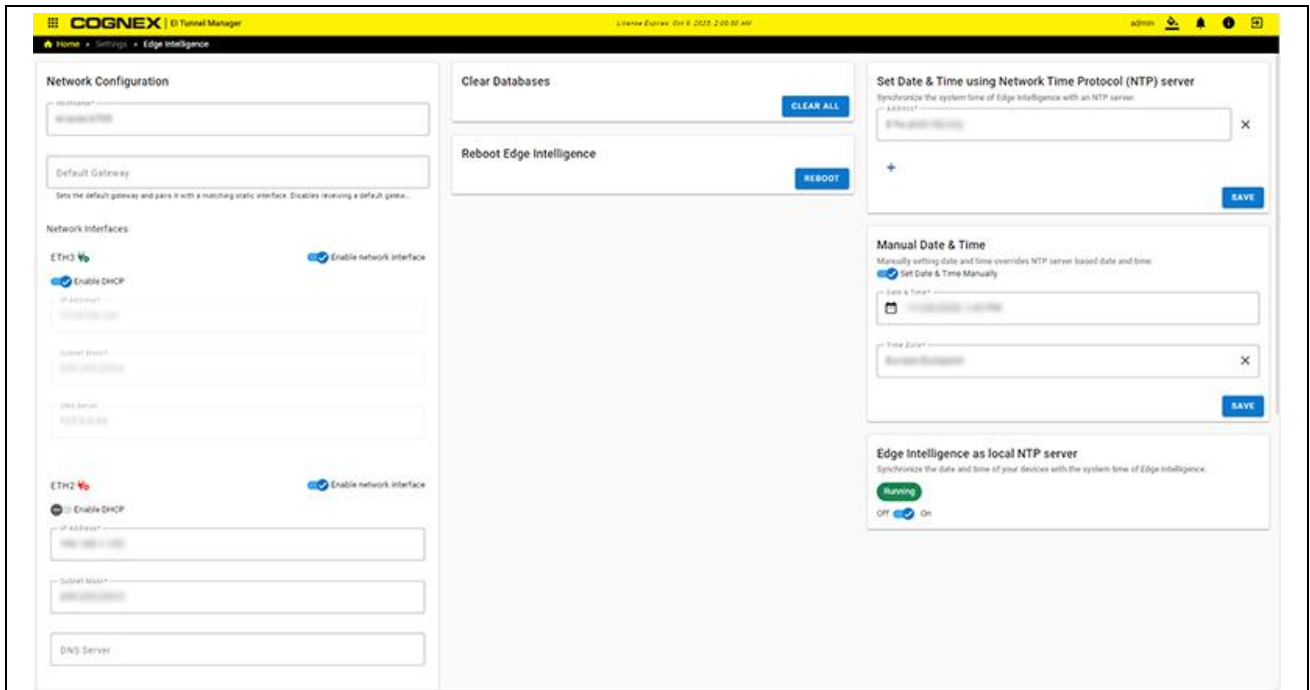
The Settings app allows you to configure your device, enable or disable the DataMan WebHMI pages of your connected devices, and upgrade your device firmware.

Edge Intelligence

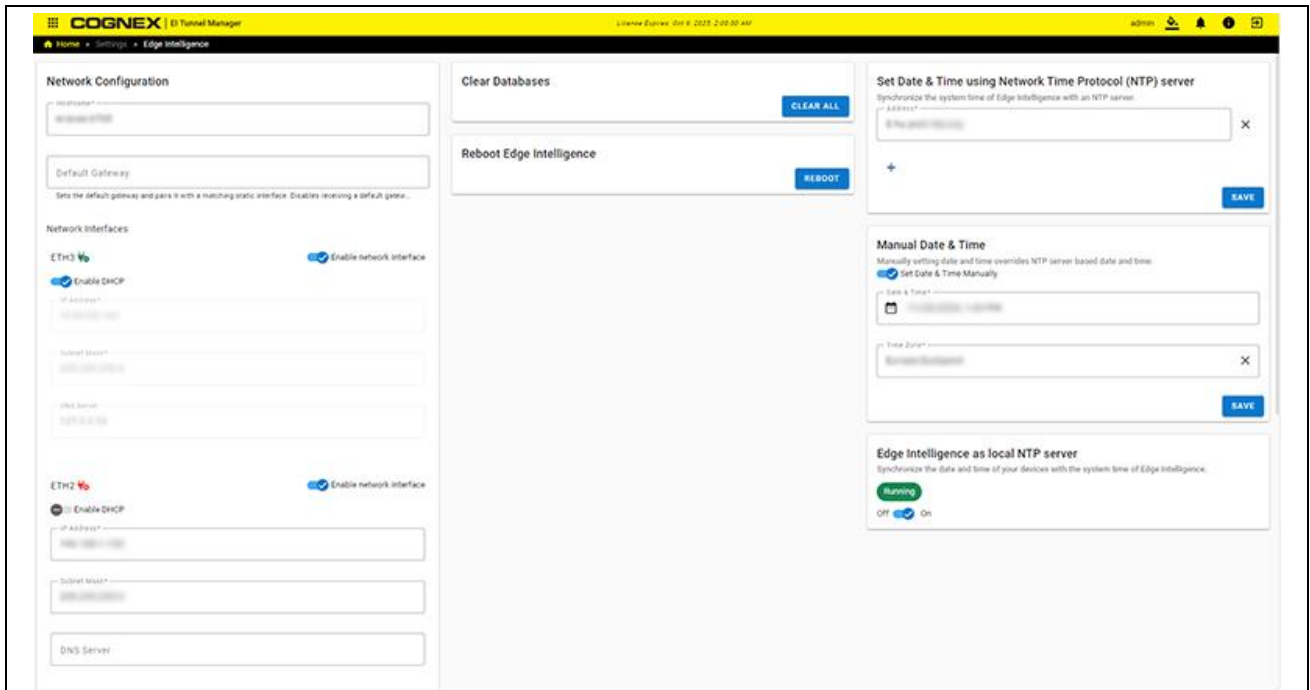
The Edge Intelligence page shows the network configuration, and allows you to edit and save the network settings of the EI Tunnel Manager device.



Section	Item	Description
Network Configuration	Hostname	The hostname of the EI Tunnel Manager.
	Default Gateway	The Gateway of the EI Tunnel Manager.
	Network Interfaces	Configuration options for each of the Ethernet ports (1-3). For each Ethernet port: <ul style="list-style-type: none"> • Enable or disable the interface. • Enable using the DHCP protocol instead of static protocols. • See if the Ethernet cable is connected by checking the green and red icons next to the name of the interfaces.
	IP Address	The IP Address of the EI Tunnel Manager.
	Subnet Mask	The Subnet Mask of the EI Tunnel Manager.
	DNS Server	The DNS server of the EI Tunnel Manager.
	Network Address Translation (NAT)	Toggle the switch to enable the NAT. See Setting up the NAT on page 76 .



Section	Item	Description
Clear Databases	<p>Clear the device lists, data, and images from the Unit, and create a new state.</p> <p>Note: The Clear database option is only available with Admin level clearance.</p>	
Reboot Edge Intelligence	Reboot the EI Tunnel Manager device.	
Set Date & Time using Network Time Protocol (NTP) server	<p>Add an NTP server to set the system time:</p> <ol style="list-style-type: none"> Click +. <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Set Date & Time using Network Time Protocol (NTP) server</p> <p>Synchronize the system time of Edge Intelligence with an NTP server.</p> <p>Address* <input style="width: 100%;" type="text"/></p> <p style="text-align: right;">X</p> <p style="text-align: center;">+</p> <p style="text-align: right; margin-top: 10px;">SAVE</p> </div> <ol style="list-style-type: none"> Enter the IP address of the NTP Server. Click Save. <p>Note: You need to log out and log back in after saving the system time.</p>	
Manual Date & Time	<p>Toggle Set Date & Time Manually to specify the date, time and the time zone.</p> <p>Note: You need to log out and log back in after saving the system time.</p>	



Section	Item	Description
Edge Intelligence as local NTP server		Toggle the switch to synchronize the date and time of your devices with the EI Tunnel Manager device.

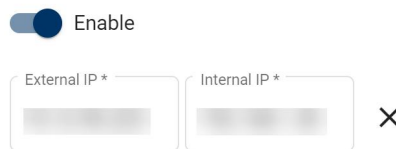
Setting up the NAT

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.
2. Set the switch to enable NAT Settings.

Network Address Translation (NAT)



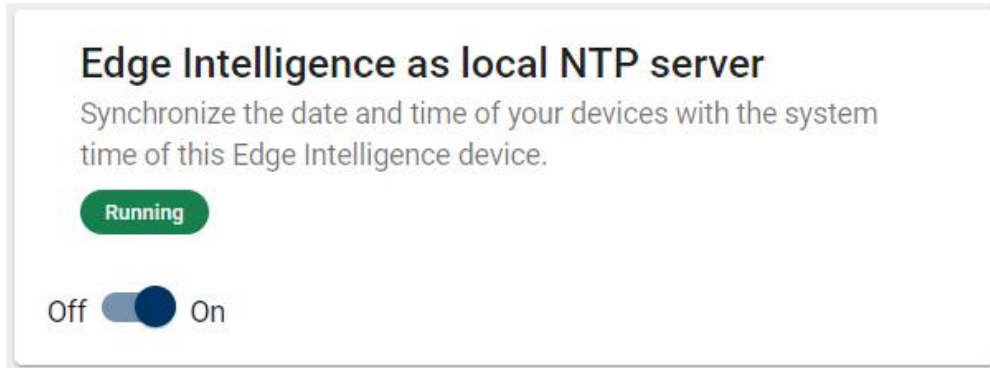
+

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

NTP Server Function

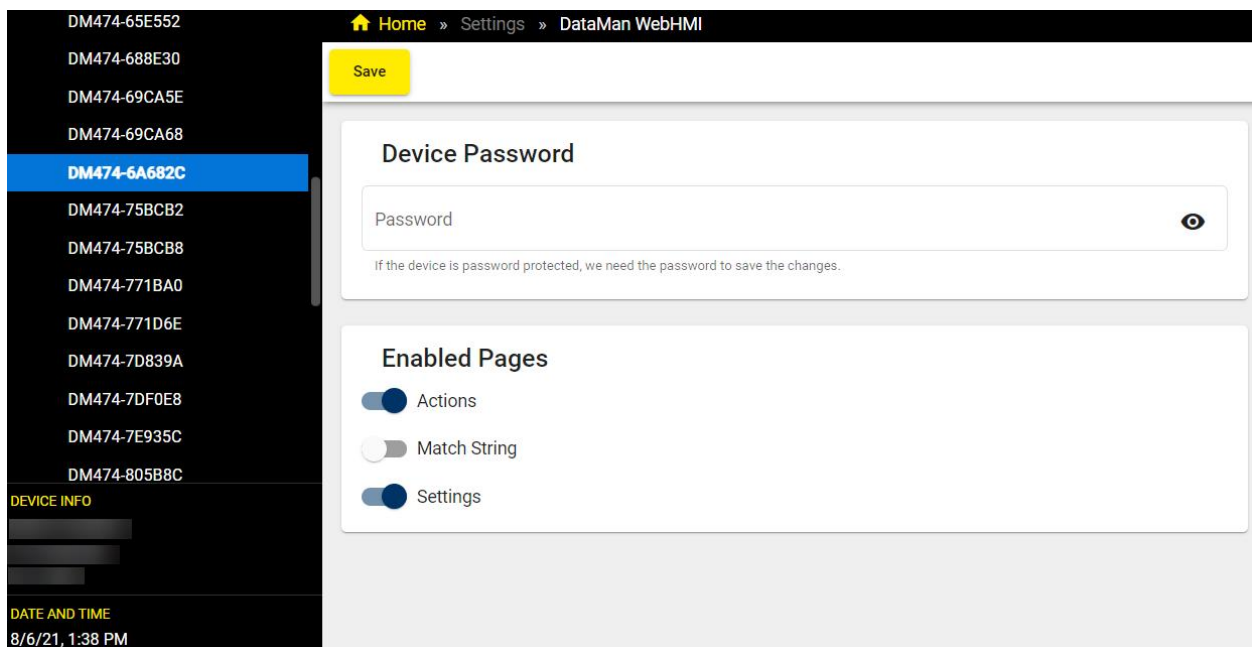
The Unit device can act as a Network Time Protocol (NTP) server. NTP is an internet protocol for synchronizing clocks on a network to within a few milliseconds of universal coordinated time (UTC).

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 Unit.



DataMan WebHMI

The DataMan WebHMI page 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 Device Management app.



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**

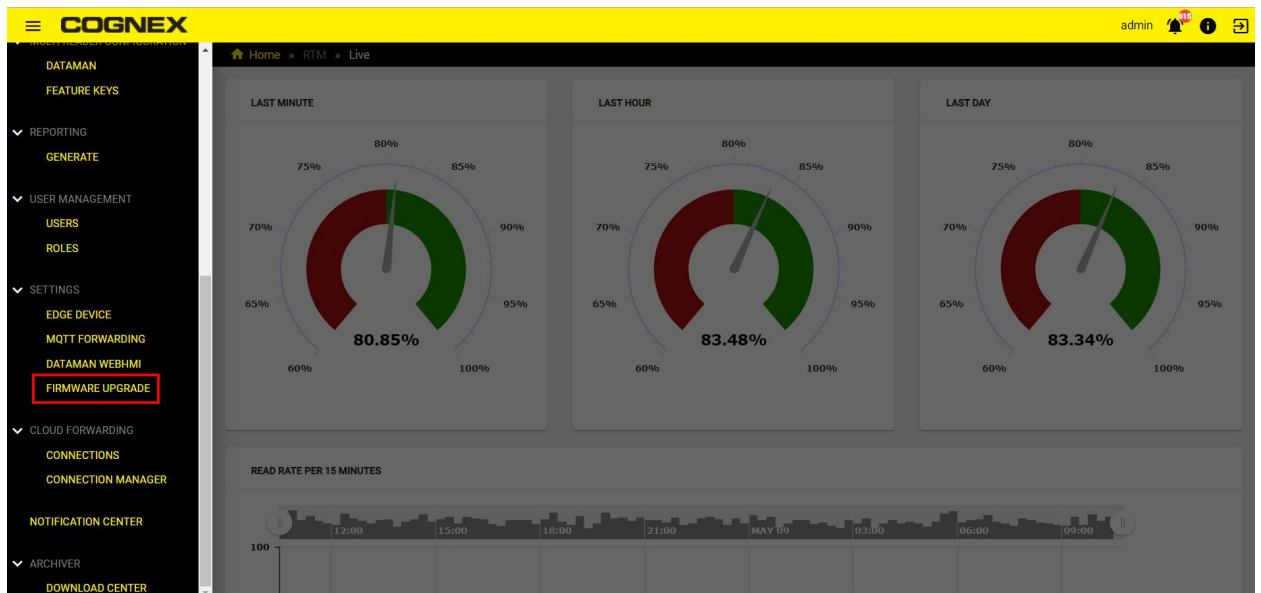
Click **Save** at the top of the page to apply your changes.

Firmware Upgrade

The Firmware Upgrade page 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..
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.



1. Click **Upload Certificate** to add a .pem file.
2. Click **Submit**.
3. Turn on the **Enable HTTPS** toggle. You are automatically logged out.
4. Log in again to the El Tunnel Manager, either with the normal login or with Single Sign-On.

Username*

Password* 

Login

OR

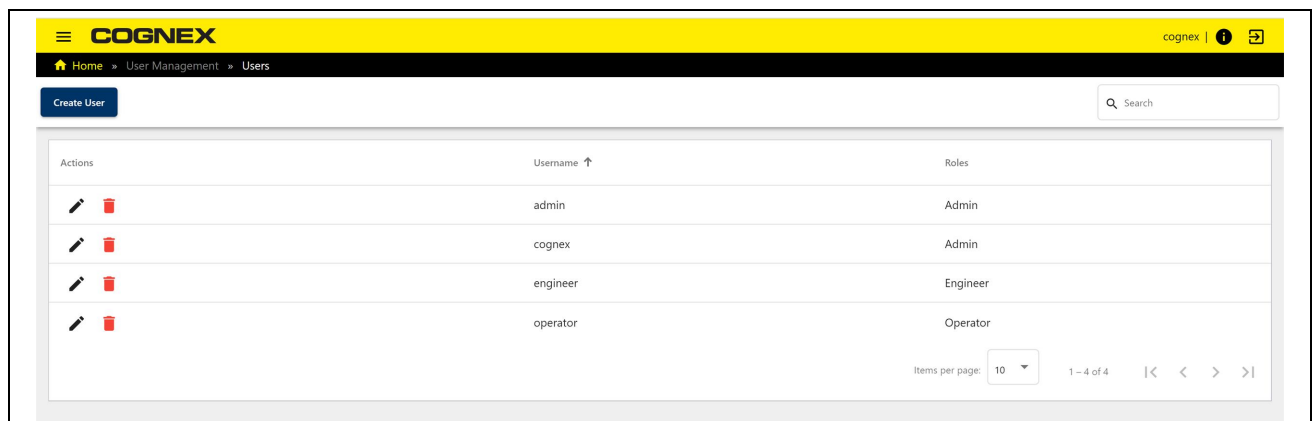
Sign in with SSO

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.



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** button 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 *
 Admin

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.

Reset
Save

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

Default User Credentials

The following users credentials are available by default:

User	Password	Default Permissions
admin	BnthWWSD	Has access to all apps and features. Admin users can modify the default user profiles, enable access permissions for the other user roles, or create new profiles.
engineer	TaRDpKVx	Has access to all apps and features.
operator	SxtXGmxs	User with read-only rights. The operator does not have access to the Device Management app and the Settings.

Note: Change the default credentials to avoid security risks. For more information, see [User Management on page 80](#).

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. You need to

To configure this process on EI Tunnel Manager, set up HTTPS with uploading certificates. From there, 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 84](#).

Note: Cognex product name uppercase only supports the OpenID Connect (OIDC) standard for Single Sign-On.

Identity Provider Configuration

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

After filling in the mandatory fields, click **Save** to proceed.

Input Field	Description
-------------	-------------

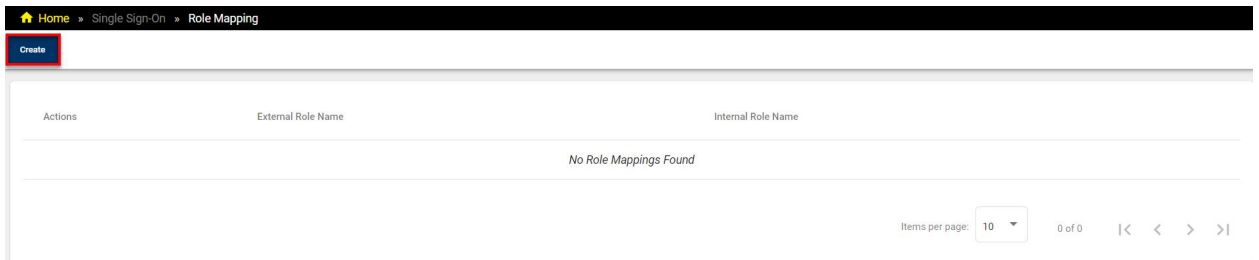
Authority	Your Identity Provider (IdP) Authority URL. This is the endpoint where EI Tunnel Manager redirects users to perform the login step with the IdP.
Client ID	Your EI Tunnel Manager fully qualified domain name and any variations.
Client Secret	You need to configure a client secret on your IdP and enter the EI Tunnel Manager domain entries as redirect URLs. Redirect URLs take the following form: <i>https://%3cEIhttps://<EI address>/identity-provider/api/v1/oidc-external/callback</i>
Role Claim Type	This field indicates the roles or groups of the user. If you do not use Role Based Access Control in your IdP, this might not be required.
User Name Claim Type	This field indicates the username of the individual.

Role Mapping

The Role Mapping page of the Single Sign-On app allows you to create external roles and map them to the internal roles.

To create role mapping:

1. Click on **Create** on the top left corner of the **Role Mapping** page.



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

Create Role Mapping

External Role Name *

Internal Role Name * ▼

+

Cancel

Submit

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

Create Role Mapping

Admin
 Engineer
 Operator

+
Cancel
Submit

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

Create Role Mapping

+

Cancel
Submit

- After filling in the given fields, click **Submit** to create the role mappings.

Home > Single Sign-On > Role Mapping

Create

Actions	External Role Name	Internal Role Name
<div style="display: flex; justify-content: space-around;"> ✎ 🗑 </div>	Admin	Admin
<div style="display: flex; justify-content: space-around;"> ✎ 🗑 </div>	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

Cancel
Submit

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

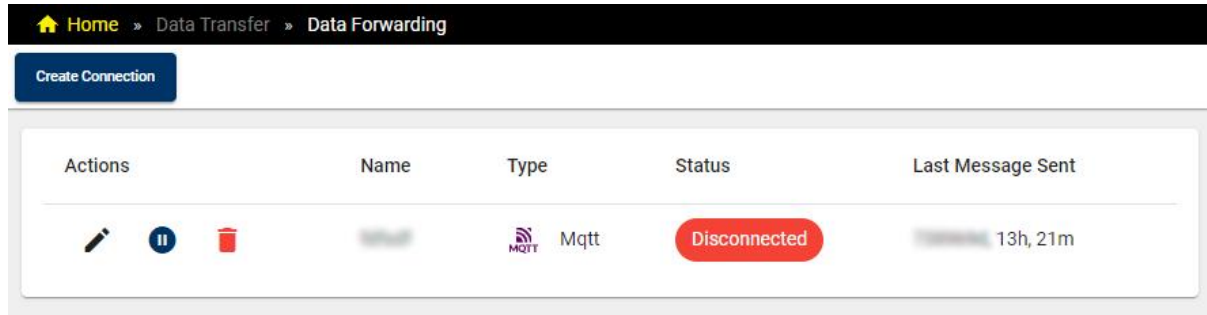
Data Transfer

Unit collects, parses, formats, and collates data from several readers.

Data Forwarding

The Data Forwarding page allows you to manage how the Unit sends your device data to different destinations. On this page, you can:

- Set up a data forwarding connection.
- Check, edit, pause, and delete connections.



Note: To enable data forwarding, you need a license from Cognex. See [Licensing on page 102](#).

Unit supports the following connection types:

- MQTT
- SFTP
- Amazon S3
- Amazon SNS
- Azure IoT Hub
- FTP

Set Up an MQTT Connection

You can set up data forwarding through an MQTT connection from the Data Forwarding page. Data forwarding through MQTT only supports transferring results data. To set up the connection, you need to provide the details of your MQTT broker.

Prerequisites

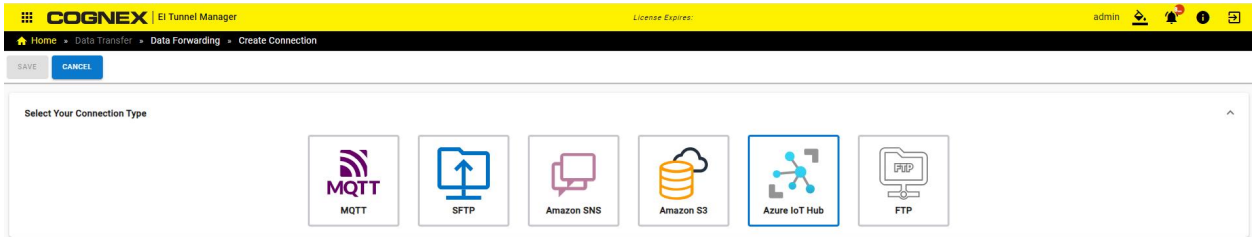
Before you start, ensure that the following prerequisites are met:

- The Unit is connected to the local network.
- You are subscribed to the devices from which you intend to forward data.
- The details of your MQTT broker are available.

Procedure

To set up an MQTT connection:

1. Click **Create Connection** on the Data Forwarding page.
2. Choose **MQTT**.



3. Choose either Standard, TLS, or mTLS from the **Authentication Method** drop-down menu. Once you have selected the authentication method, the **Connection Settings** section appears in the page.

Note: If you select TLS, you must upload a CA certificate. If you select mTLS, you must upload a **CA certificate** and a **Client pfx**.

Configure Your Connection

<input type="text" value="Connection Name*"/>	<input type="text" value="Client ID"/>
<input type="text" value="Authentication Method*"/> mTLS	<input type="text" value="CA Certificate"/> <small>Choose a.crt, .cert, .pem file.</small>
	<input type="text" value="Client pfx*"/> <small>Choose a.pfx, .pem, .p12 file.</small>

4. Enter the connection details, QoS, and Protocol Version for the MQTT broker.

Connection Settings

QoS Level

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

Protocol Version

- 3.1.1
 5

- Choose the application data you want to forward and from which device. Under **Device Data** and **Tunnel Data**, you can choose specific data from each device by checking the corresponding box.

Choose application data to forward ^

Device Data ^

Results Statistics

Summary Test	Device	<input type="checkbox"/> Good Read Trigger	<input type="checkbox"/> No Read Trigger	<input type="checkbox"/> Validation Failure Trigger
Tunnel (Simulation)	simulator-dragon-Primary	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Image Services	simulator-dragon-Prod-Tag 1,2...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- Click **Save**.

Your connection is now listed on the Data Forwarding page. You can edit, pause, and delete connections here.

Set Up an SFTP Connection

You can set up data forwarding through an SFTP connection from the Data Forwarding page. Data forwarding through SFTP supports both transferring results data and images. To set up the connection, you need to provide a custom file path.

Prerequisites

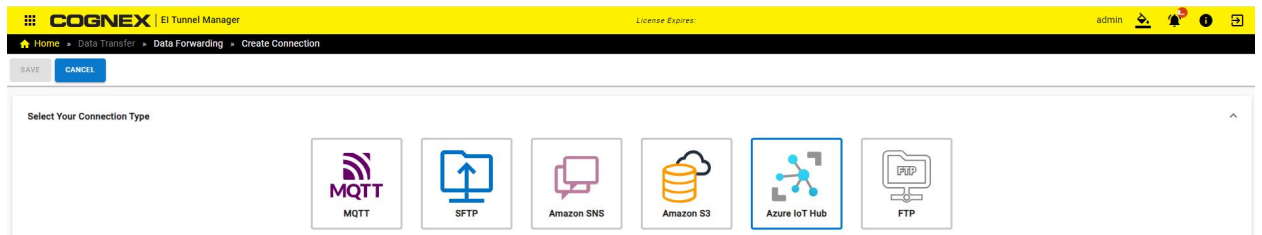
Before you start, ensure that the following prerequisites are met:

- The Unit is connected to the local network.
- You are subscribed to the devices from which you intend to forward data.

Procedure

To set up an SFTP connection:

- Click **Create Connection** on the Data Forwarding page.
- Choose **SFTP**.



3. Configure your connection.
 - a. Provide the **Connection Name**.
 - b. Optionally, to help differentiate between connections, provide a custom **Client ID**.
 - c. Choose the **Authentication Method** from the drop-down menu.

Configure Your Connection ^

Connection Name*

Client ID

Authentication Method* ▼

4. Define a custom file path.

Define Your Custom File Path ^

File Path*

Click a token below to add it to the file path.

<p>Event Information</p> <ul style="list-style-type: none"> + <EventTypes> Notifies if the result is an image event or data event. + <ID> Unique ID for each event. + <FileExtension> File extension of the incoming message. 	<p>Time Information</p> <ul style="list-style-type: none"> + <Timestamp> The timestamp recorded for the trigger result. + <Date> Date in format YYYYMMDD (e.g. 2020-10-31T01:02:03Z = 20201231) + <Time> Time in format HH:mm:ss (e.g. 2020-10-31T01:02:03Z = 010203) + <Day> Day from timestamp (e.g. 2020-10-31T01:02:03Z = 31) + <Month> Month from timestamp (e.g. 2020-10-31T01:02:03Z = 10) + <Year> Year from timestamp (e.g. 2020-10-31T01:02:03Z = 2020) + <Hours> Hour from timestamp (e.g. 2020-10-31T01:02:03Z = 01) + <Minutes> Minutes from timestamp (e.g. 2020-10-31T01:02:03Z = 02) + <Seconds> Seconds from timestamp (e.g. 2020-10-31T01:02:03Z = 03) + <Milliseconds> Milliseconds from timestamp (e.g. 2020-10-31T01:02:03.560Z = 560) 	<p>Image Information</p> <ul style="list-style-type: none"> + <ImageIndex> Image number for a trigger. + <Group> MIME group name the image is originating from. + <TriggerIndex> Trigger index for which image is for. + <DeviceMacAddress> MacAddress of the device which generated this image. + <SourceDeviceName> Name of the device which generated this image. + <ExtraInformation> Any extra information embedded in the image.
---	--	---

Note: You can use a mix of literals and tokens to set up the custom file path. Tokens are replaced object information at the time of forwarding (for example, triggerID, timestamp). Image information tokens are only available for forwarding images and are not replaced on other data types.

5. Choose the application data you want to forward and from which device. Under **Device Data** and **Tunnel Data**, you can choose specific data from each device by checking the corresponding box.

Choose application data to forward ^

Device Data ^

Results

Statistics

Summary Item	Device	<input type="checkbox"/> Good Read Trigger	<input type="checkbox"/> No Read Trigger	<input type="checkbox"/> Validation Failure Trigger
Tunnel_0(Instance)	localhost-00000-Primary	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ingress Device	localhost-00000-Prod-Top-1-L	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

6. Click **Save**.

Your connection is now listed on the Data Forwarding page. You can edit, pause, and delete connections here.

Set Up an Amazon SNS Connection

Set up data forwarding through an Amazon SNS connection from the Data Forwarding page. Data forwarding through Amazon SNS only supports transferring results data. To set up the connection, you need files and details that you can get

from your AWS account.

Prerequisites

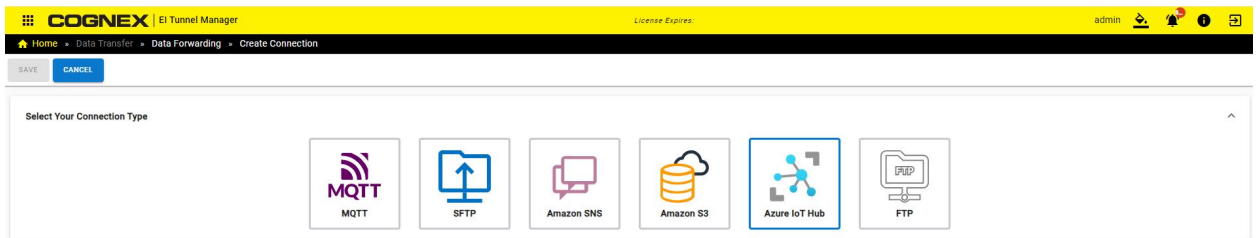
Before you start, ensure that the following prerequisites are met:

- The Unit is connected to the Internet.
- You are subscribed to the devices whose data you want to forward to an SNS topic.
- The certificate and private key files, generated from your AWS account, are available.

Procedure

To set up an Amazon SNS connection:

1. Click **Create Connection** on the Data Forwarding page.
2. Choose **Amazon SNS**.



3. Configure your connection.

- a. Provide the **Connection Name**.
- b. Optionally, to help differentiate between connections, provide a custom **Client ID**.
- c. Choose the **Authentication Method** from the drop-down menu.
- d. Upload the certificate and private key files generated from your AWS account.

Configure Your Connection

Connection Name*

Client ID

Authentication Method* X509 Certificate

Certificate* Choose a.crt, .cert, .pem file.

Private Key* Choose a.pfx, .pem, .p12, .key file.

4. Provide the details for the **Connection Settings**. You can find these details in your AWS account.

Connection Settings

Credentials Endpoint*

 Certificate Password



Role Alias Name*

Thing Name*

AWS Region*

SNS TopicArn*

Message Attributes



5. To choose the data you want to forward and the source devices, check the corresponding box.

Choose application data to forward ^

Device Data ^

Results Statistics

MarketingDEMO	Device	<input type="checkbox"/> Good Read Trigger	<input type="checkbox"/> No Read Trigger	<input type="checkbox"/> Validation Failure Trigger
	192.168.1.100	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	192.168.1.101	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	192.168.1.102	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	192.168.1.103	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Tunnel Data ^

Results

MarketingDEMO	Device	<input type="checkbox"/> Tunnel Trigger Result
	192.168.1.103	<input type="checkbox"/>

6. Click **Save**.

Your connection is now listed on the Data Forwarding page. You can edit, pause, and delete connections here.

Set Up an Amazon S3 Connection

Set up data forwarding through an Amazon S3 connection from the Data Forwarding page. Data forwarding through Amazon S3 supports both transferring results data and images. To set up the connection, you need to provide a custom file path, and files and details that you can get from your AWS account.

Prerequisites

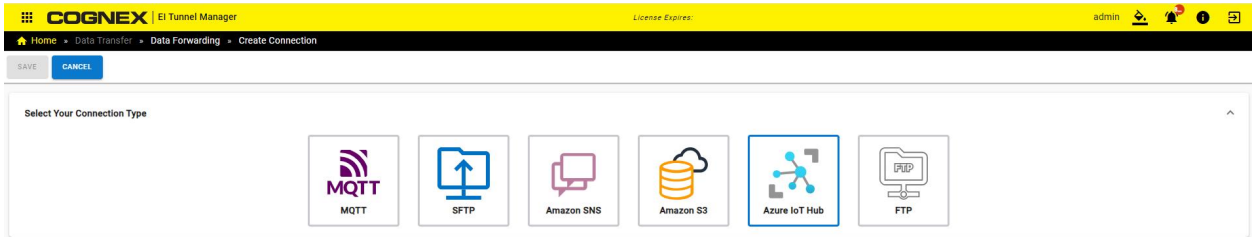
Before you start, ensure that the following prerequisites are met:

- The Unit is connected to the Internet.
- You are subscribed to the devices whose data you want to forward to an S3 bucket.
- The certificate and private key files, generated from your AWS account, are available.

Procedure

To set up an Amazon S3 connection:

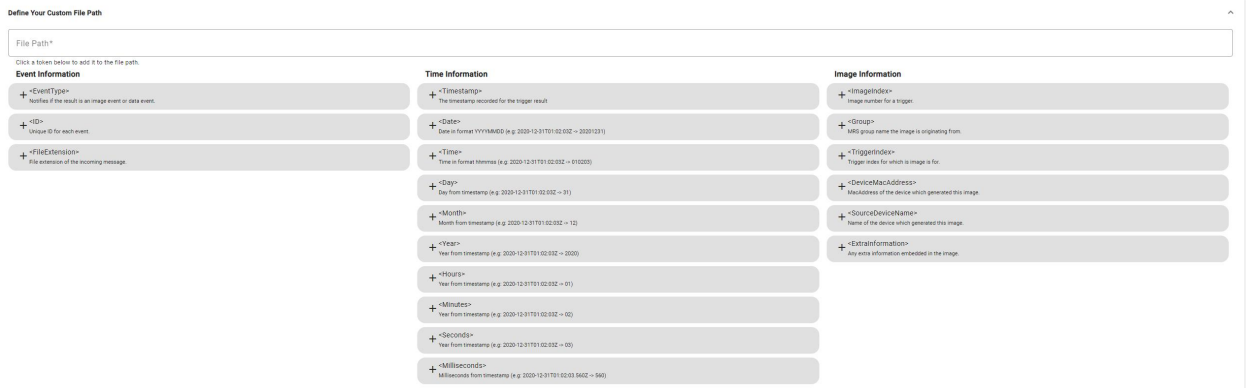
1. Click **Create Connection** on the Data Forwarding page.
2. Choose **Amazon S3**.



3. Configure your connection.
 - a. Provide the **Connection Name**.
 - b. Optionally, to help differentiate between connections, provide a custom **Client ID**.
 - c. Choose the **Authentication Method** from the drop-down menu.
 - d. Upload the certificate and private key files generated from your AWS account.



4. Define a custom file path.



Note: You can use a mix of literals and tokens to set up the custom file path. Tokens are replaced object information at the time of forwarding (for example, triggerID, timestamp). Image information tokens are only available for forwarding images and are not replaced on other data types.

5. Provide the details for the **Connection Settings**. You can find these details in your AWS account.

Connection Settings ^

Credentials Endpoint*

Certificate Password

Role Alias Name*

Thing Name*

S3 Region*

BucketName*

6. To choose the data you want to forward and the source devices, check the corresponding box.

Choose application data to forward ^

Device Data ^

Results Statistics

MarketingDEMO	Device	<input type="checkbox"/> Good Read Trigger	<input type="checkbox"/> No Read Trigger	<input type="checkbox"/> Validation Failure Trigger
	XXXXXXXXXXXX	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	XXXXXXXXXX	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	XXXXXXXXXX	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	XXXXXXXXXXXX	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Tunnel Data ^

Results

MarketingDEMO	Device	<input type="checkbox"/> Tunnel Trigger Result
	XXXXXXXXXXXX	<input type="checkbox"/>

7. Click **Save**.

Your connection is now listed on the Data Forwarding page. You can edit, pause, and delete connections here.

Set Up an Azure IoT Hub Connection

Set up data forwarding through an Azure IoT Hub connection from the Data Forwarding page. Data forwarding through Azure IoT Hub only supports transferring results data. To set up the connection, you need to provide a custom file path.

Prerequisites

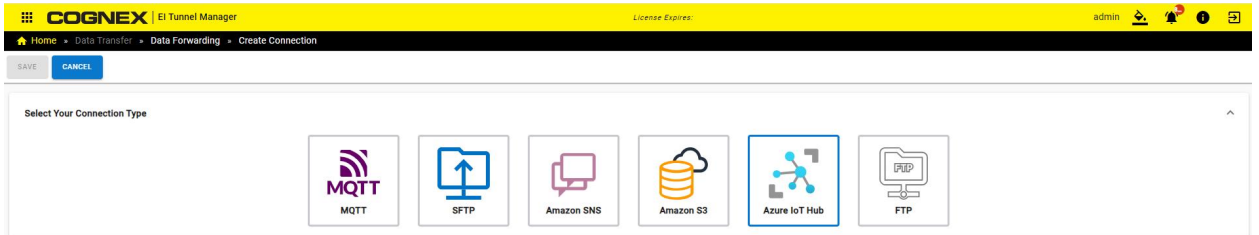
Before you start, ensure that the following prerequisites are met:

- The Unit is connected to the local network.
- You are subscribed to the devices from which you intend to forward data.

Procedure

To set up an Azure IoT Hub connection:

1. Click **Create Connection** on the Data Forwarding page.
2. Choose **Azure IoT Hub**.



3. Configure your connection:
 - a. Provide the **Connection Name**.
 - b. Optionally, to help differentiate between connections, provide a custom **Client ID**.
 - c. Choose the **Authentication Method** from the drop-down menu.

Configure Your Connection

Connection Name*

Client ID

Authentication Method*

4. Define a custom file path.

Define Your Custom File Path

File Path*

Click a token below to add it to the file path.

Event Information	Time Information	Image Information	Stitcher
+ <EventType> Notifies if the result is an image event or data event.	+ <Timestamp> The timestamp recorded for the trigger result	+ <ImageIndex> Image number for a trigger.	+ <StitchedSurface> Surface that is stitched
+ <ID> Unique ID for each event.	+ <Date> Date in format YYYY/MM/DD (e.g. 2020-12-31T01:02:03Z -> 20201231)	+ <Group> MRS group name the image is originating from.	
+ <FileExtension> File extension of the incoming message.	+ <Time> Time in format hh:mm:ss (e.g. 2020-12-31T01:02:03Z -> 010203)	+ <TriggerIndex> Trigger index for which image is for.	
	+ <Day> Day from timestamp (e.g. 2020-12-31T01:02:03Z -> 31)	+ <DeviceMacAddress> MacAddress of the device which generated this image.	
	+ <Month> Month from timestamp (e.g. 2020-12-31T01:02:03Z -> 12)	+ <SourceDeviceName> Name of the device which generated this image.	
	+ <Year> Year from timestamp (e.g. 2020-12-31T01:02:03Z -> 2020)	+ <Extrainformation> Any extra information embedded in the image.	
	+ <Hours> Year from timestamp (e.g. 2020-12-31T01:02:03Z -> 01)		
	+ <Minutes> Year from timestamp (e.g. 2020-12-31T01:02:03Z -> 02)		
	+ <Seconds> Year from timestamp (e.g. 2020-12-31T01:02:03Z -> 03)		
	+ <Milliseconds> Milliseconds from timestamp (e.g. 2020-12-31T01:02:03.560Z -> 560)		

- Choose the application data you want to forward and from which device. Under **Device Data** and **Tunnel Data**, you can choose specific data from each device by checking the corresponding box.

Choose application data to forward

Device Data

Image Results Results Statistics

Device	<input type="checkbox"/> Good Read Image	<input type="checkbox"/> No Read Image	<input type="checkbox"/> Validation Failure Image	<input type="checkbox"/> Image SVGs
...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Tunnel Data

Results

Device	<input type="checkbox"/> Tunnel Trigger Result
...	<input type="checkbox"/>

- Click **Save**.

Your connection is now listed on the Data Forwarding page. You can edit, pause, and delete connections here.

Set Up an FTP Connection

Set up data forwarding through an FTP connection from the Data Forwarding page. Data forwarding through FTP only supports transferring results data. To set up the connection, you need to provide a custom file path.

Prerequisites

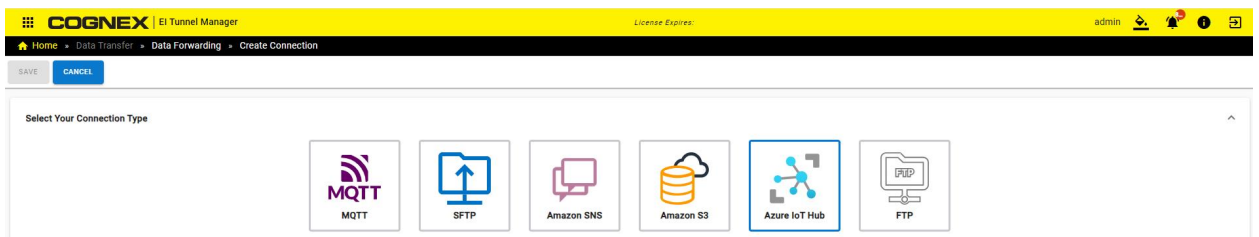
Before you start, ensure that the following prerequisites are met:

- The Unit is connected to the local network.
- You are subscribed to the devices from which you intend to forward data.

Procedure

To set up an FTP connection:

- Click **Create Connection** on the Data Forwarding page.
- Choose **FTP**.



3. Configure your connection:
 - a. Provide the **Connection Name**.
 - b. Optionally, provide an **FTP Port**.
 - c. Provide a **Username**.
 - d. Optionally, provide a **Password**.

Connection Settings



4. Define a custom file path.

Define Your Custom File Path

File Path*

Click a token below to add it to the file path.

Event information	Time information	Image information	Stitcher
+ <EventType> Notifies if the result is an image event or data event.	+ <Timestamp> The timestamp recorded for the trigger result	+ <ImageIndex> Image number for a trigger.	+ <StitchedSurface> Surface that is stitched
+ <ID> Unique ID for each event.	+ <Date> Date in format YYYYMMDD (e.g. 2020-12-31T01:02:03Z -> 20201231)	+ <Group> MSG group name the image is originating from.	
+ <FileExtension> File extension of the incoming message.	+ <Time> Time in format hhmmss (e.g. 2020-12-31T01:02:03Z -> 010203)	+ <TriggerIndex> Trigger index for which image is for.	
	+ <Day> Day from timestamp (e.g. 2020-12-31T01:02:03Z -> 31)	+ <DeviceMacAddress> MacAddress of the device which generated this image.	
	+ <Month> Month from timestamp (e.g. 2020-12-31T01:02:03Z -> 12)	+ <SourceDeviceName> Name of the device which generated this image.	
	+ <Year> Year from timestamp (e.g. 2020-12-31T01:02:03Z -> 2020)	+ <Extrainformation> Any extra information embedded in the image.	
	+ <Hour> Year from timestamp (e.g. 2020-12-31T01:02:03Z -> 01)		
	+ <Minutes> Year from timestamp (e.g. 2020-12-31T01:02:03Z -> 02)		
	+ <Seconds> Year from timestamp (e.g. 2020-12-31T01:02:03Z -> 03)		
	+ <Milliseconds> Milliseconds from timestamp (e.g. 2020-12-31T01:02:03.560Z -> 560)		

Note: You can use a mix of literals and tokens to set up the custom file path. Tokens are replaced object information at the time of forwarding (for example, triggerID, timestamp). Image information tokens are only available for forwarding images and are not replaced on other data types.

5. Choose the application data you want to forward and from which device. Under **Device Data** and **Tunnel Data**, you can choose specific data from each device by checking the corresponding box.

Choose application data to forward

Device Data

Image Results Results Statistics

Device	<input type="checkbox"/> Good Read Image	<input type="checkbox"/> No Read Image	<input type="checkbox"/> Validation Failure Image	<input type="checkbox"/> Image SVGs
[Device Name]	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Tunnel Data

Results

Device	<input type="checkbox"/> Tunnel Trigger Result
[Device Name]	<input type="checkbox"/>

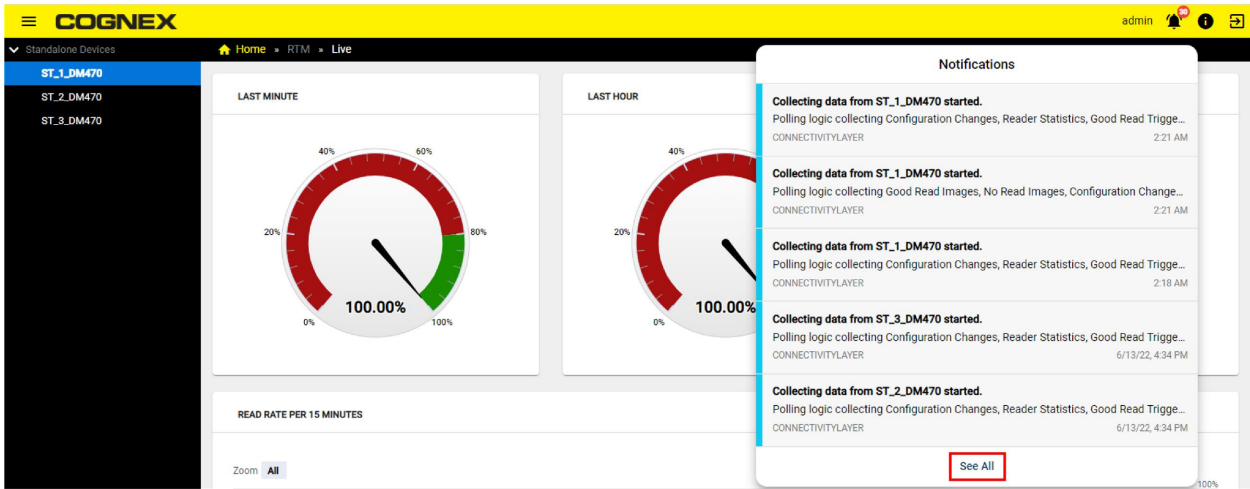
6. Click **Save**.

Your connection is now listed on the Data Forwarding page. You can edit, pause, and delete connections here.

Notification Center

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

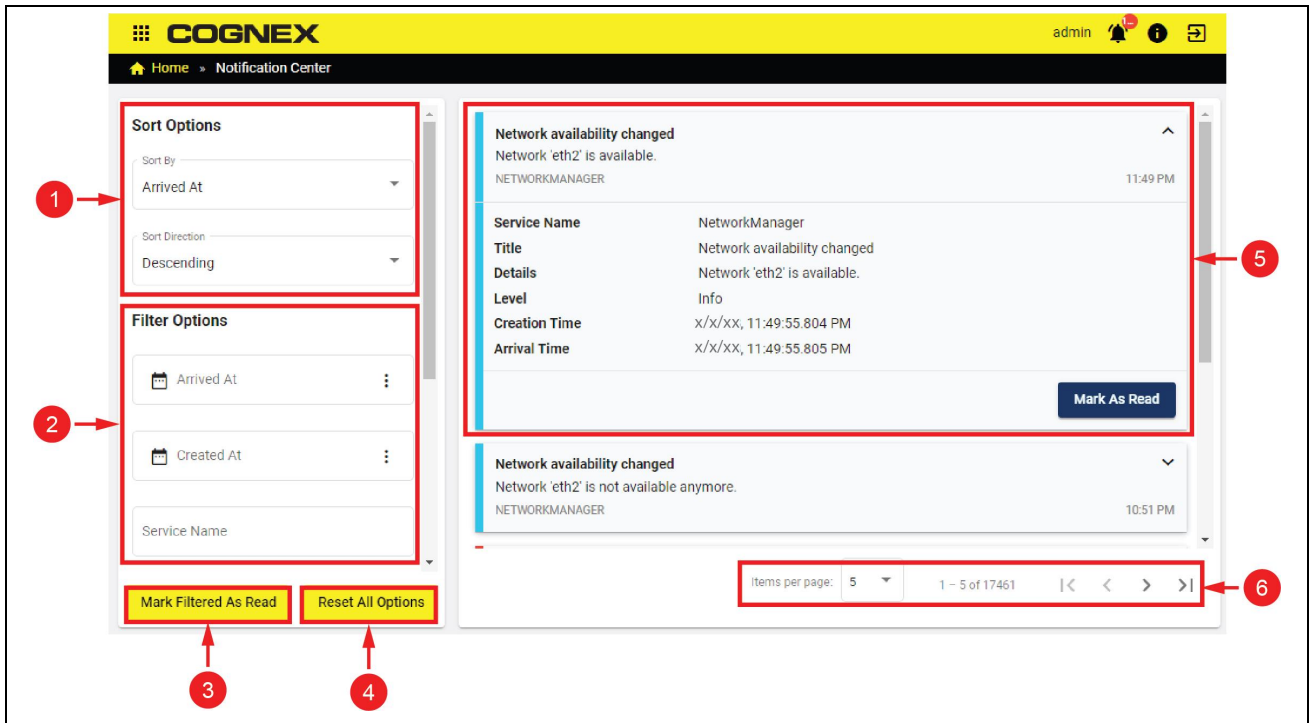
For access from the notification bell, click on the bell icon in the upper right corner of the home page to see the latest notifications. Click the **See All** button to open the Notification Center.



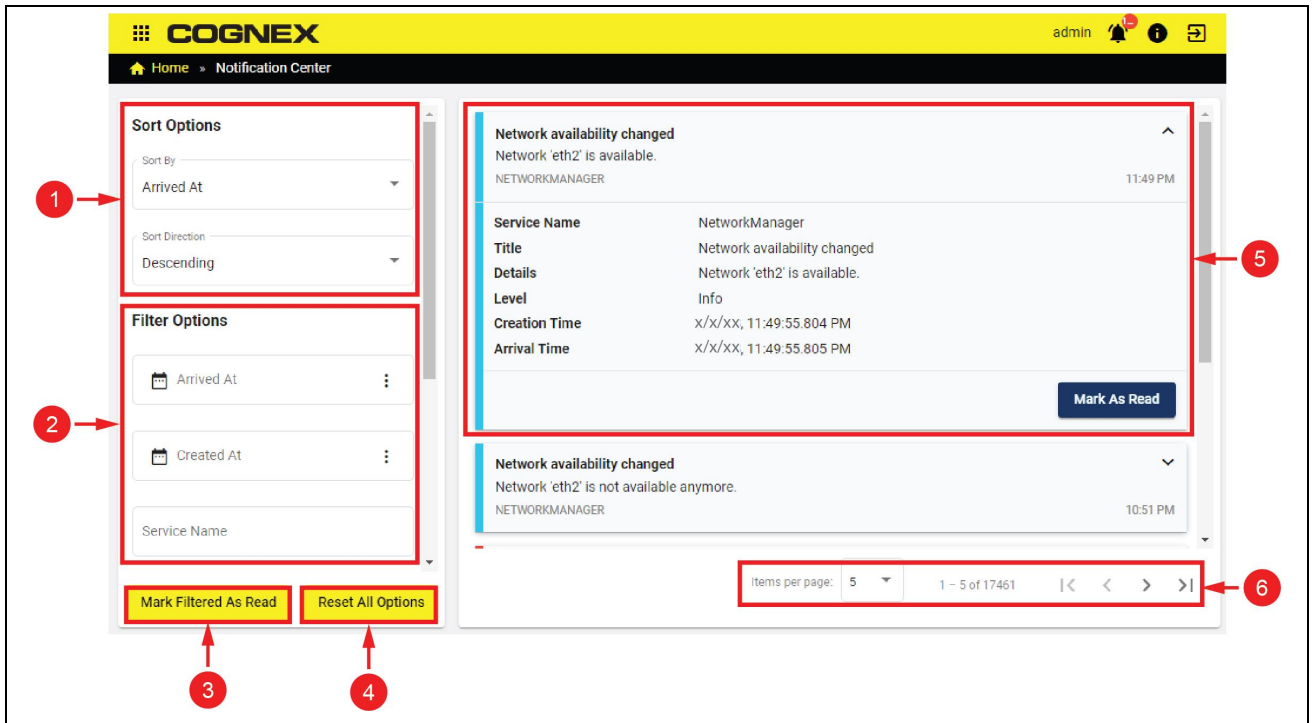
Notification Center Features

The screenshot shows the COGNEX Notification Center interface. The header includes the COGNEX logo and the user name 'admin'. The navigation bar shows 'Home' and 'Notification Center'. The main content area is divided into several sections. On the left, there is a 'Sort Options' section with a 'Sort By' dropdown set to 'Arrived At' and a 'Sort Direction' dropdown set to 'Descending'. Below this is a 'Filter Options' section with three filterable fields: 'Arrived At', 'Created At', and 'Service Name'. At the bottom of the filter options, there are two buttons: 'Mark Filtered As Read' and 'Reset All Options'. On the right, there is a list of notifications. The first notification is titled 'Network availability changed' and states 'Network 'eth2' is available.' It includes details such as 'Service Name: NetworkManager', 'Title: Network availability changed', 'Details: Network 'eth2' is available.', 'Level: Info', 'Creation Time: x/x/xx, 11:49:55.804 PM', and 'Arrival Time: x/x/xx, 11:49:55.805 PM'. A 'Mark As Read' button is located at the bottom right of this notification. The second notification is titled 'Network availability changed' and states 'Network 'eth2' is not available anymore.' At the bottom right of the notification list, there is a pagination control showing 'Items per page: 5' and '1 - 5 of 17461'. Red callouts with numbers 1 through 6 point to these specific features.

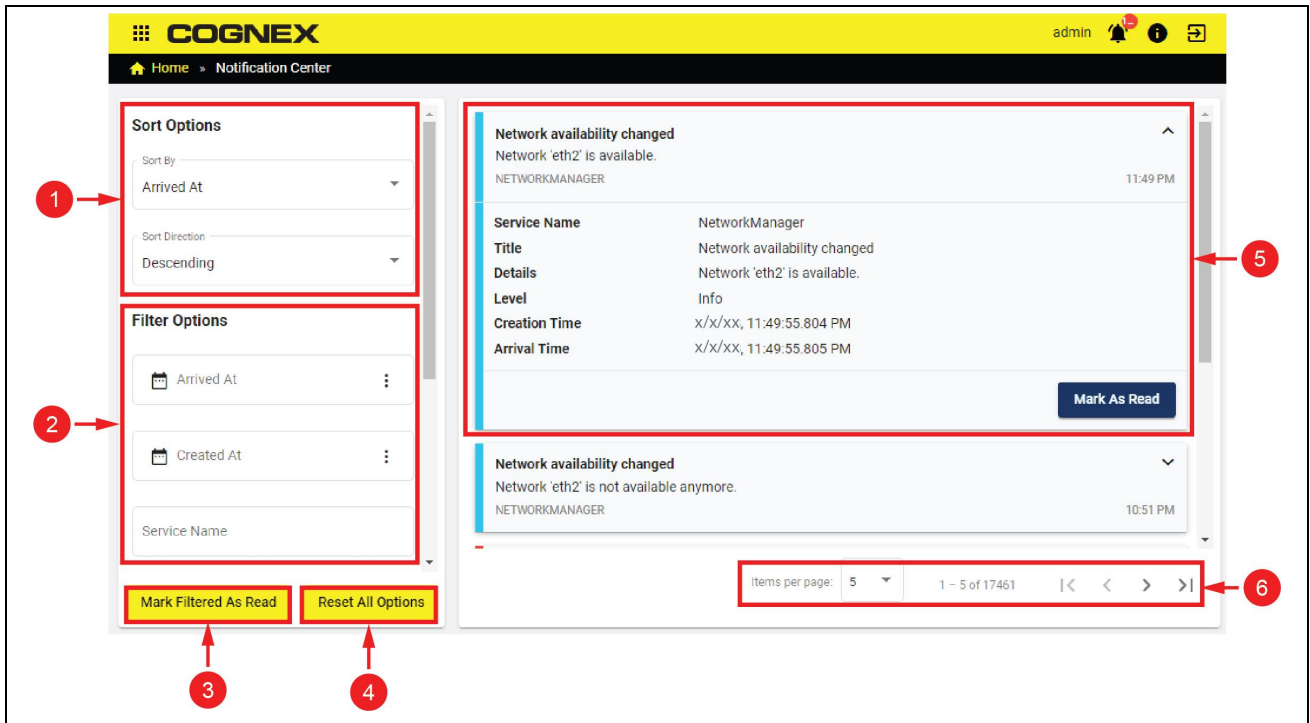
Number	Element	Description
1	Sort Options	Sort By: Arrived At, Sort Direction: Descending
2	Filter Options	Arrived At, Created At, Service Name
3	Mark Filtered As Read	Button to mark filtered items as read
4	Reset All Options	Button to reset all filter and sort options
5	Notification Card	Network availability changed: Network 'eth2' is available. Includes details like Service Name, Title, Details, 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.

Licensing

The Licensing app allows you to update your licenses using the Update page.

Update

The Update page 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.

The screenshot shows the 'Update License' page with a search bar and a table of licenses. The table has columns for Name, Product Code, Activated At, and Expires At. The 'Expires At' column is highlighted with a red box. Below the Cognex.Generic entry, it says 'No Sub-Licenses Found'.

Name	Product Code	Activated At	Expires At
Cognex.Generic	1		
No Sub-Licenses Found			
EdgeInt.Generic	120000		6/1/23, 8:00 PM
EdgeInt.VisionRuntimeBase	120010		6/1/23, 8:00 PM
EdgeInt.DeviceCount	120020		6/1/23, 8:00 PM
EdgeInt.RemoteMonitor	120030		6/1/23, 8:00 PM
EdgeInt.API	120040		6/1/23, 8:00 PM
EdgeInt.TA	121000		6/1/23, 8:00 PM
EdgeInt.TA.TunnelCount	121010		6/1/23, 8:00 PM
EdgeInt.TA.F1	121100		6/1/23, 8:00 PM
EdgeInt.TA.F2	121200		6/1/23, 8:00 PM
EdgeInt.3DFieldCallb	122000		6/1/23, 8:00 PM

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.
4. 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

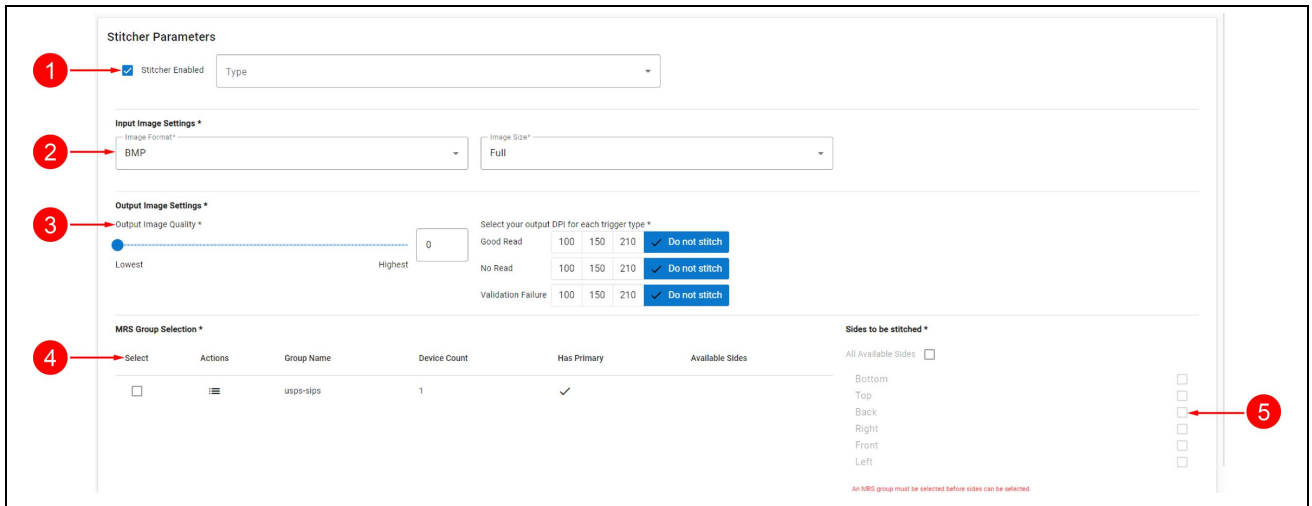
5. Check if the **Expires At** column updates automatically to the new license expiration date, to verify successful license update.

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

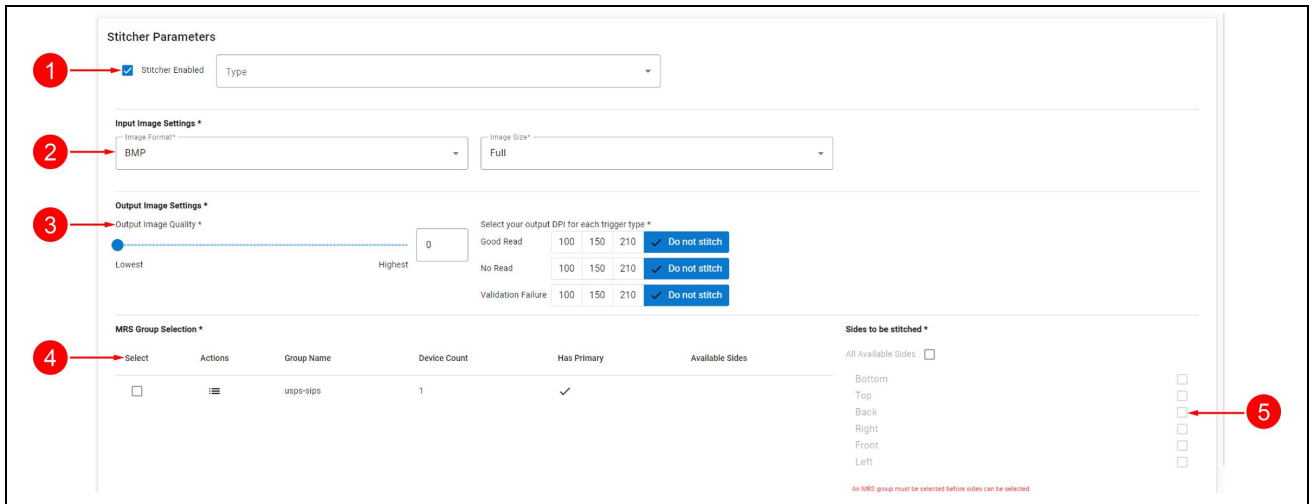
Stitcher Settings

The Stitcher feature stitches images together into one bigger image. The stitched images appear in the Results Browser as normal images.

Note: Only the EI-A9-TUNMGR-xxx hardware supports image stitching.



Number	Description
1	<p>Click the Stitcher Enabled checkbox to enable the type. You can choose the type of the Stitcher feature:</p> <ul style="list-style-type: none"> • Modular Vision Tunnel (MVT): A flexible scan tunnel in which the units can detect up to six sides of the boxes. Scalable for various speeds and gaps, without sacrificing accuracy. • Top Only No Perspective: For units that only aimed at the top of the boxes.
2	<p>Choose the image format from the dropdown:</p> <ul style="list-style-type: none"> • JPG • PNG • BMP <p>Choose the image size from the following:</p> <ul style="list-style-type: none"> • Full • Quarter • 1/16 • 1/64



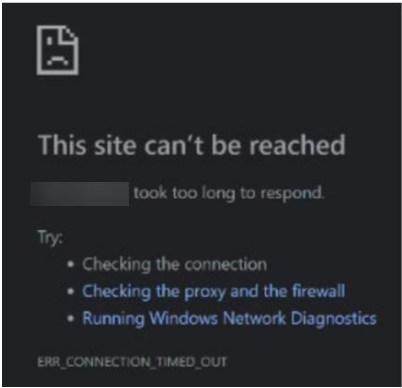
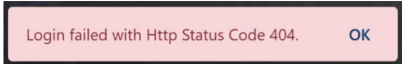
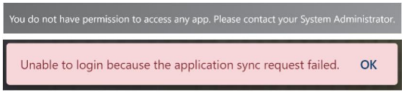

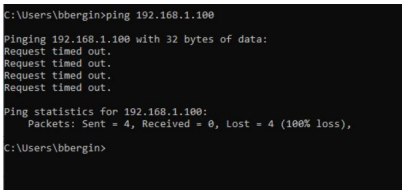
<p>3</p>	<p>Adjust the quality of the output image on the slider or write a number in the box.</p> <p>Select the Dots per Inch (DPI) value of the output images for each trigger type:</p> <ul style="list-style-type: none"> • 100 DPI: lower quality, suitable for long-term storage and basic analysis. • 150 DPI: sacrifice some quality to reduce storage size. • 210 DPI: suitable for post-processing, for example OCR. • Do not stitch: you can choose not stitching the images together for that particular trigger type.
<p>4</p>	<p>Select the Multi-Reader Sync (MRS) group. You can choose a group if there are multiple groups provisioned on the Edge Intelligence system.</p>
<p>5</p>	<p>Select which sides of the boxes you want to stitch into one image. For example, if you have a unit that detects the top and the front of a box, you can select only the top to be stitched into one image.</p>

Troubleshooting

This section provides solutions to common issues, helping you troubleshoot and resolve issues quickly and efficiently.

Remote Connection Troubleshooting

This section lists the most common errors and their solutions.

Error	Illustration	Solution
Unit is not visible in the browser		Check cable connections and secure them if necessary.
Failed login error message		Check the credentials and reenter username and/or password.
Component load error message		Reboot unit and wait for services to start.
No data/images available		Check unit availability and setup.
Cannot access Cognex product name uppercase URL		Check that subnets do not overlap. The network administrator must ensure that the IPs do not overlap.

Note: For the best results, use Ethernet connection to your network, because Wi-Fi might not allow the connection depending on your network settings.

Note:
The login page lists the IP address of your devices.

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
	✓		DHCP					(none)
	✓		DHCP					(none)
	✓		Static					(none)

Enable Remote Access for Cognex Technical Support

Select the appropriate remote access solution depending on the specific requirements and infrastructure of your organization.

Virtual Private Networking (VPN) and Virtual Desktop Infrastructure (VDI) allow Cognex Technical Support to connect with network-connected devices remotely. VPN and VDI access solutions provide secure, authorized remote support personnel with access to impacted equipment when resolving issues. Make sure you have support for HTTP, HTTPS, SSH, or SCP when using these solutions.

These solutions require engagement between the IT groups of both parties so that they can properly configure the remote access solution.

Contact Cognex Technical Support to get started.

Note: For further assistance or specific configuration guidance, contact the Cognex Technical Support department directly.

Access Solution	Requirements
VPN	<ul style="list-style-type: none"> • A VPN-compatible router or firewall at your site or a software VPN (such as Hamachi or TeamViewer). • Known accessible hostname for setup. • VPN software to provide the Cognex Technical Support team with. <p>Recommendations for Setup:</p> <ol style="list-style-type: none"> 1. Configure your VPN device (router/firewall) to enable VPN tunnels. For example: <ol style="list-style-type: none"> a. Set up a VPN server. b. Define user access controls. c. Select encryption protocols and specify permissions to ports. 2. Create user accounts for Cognex Technical Support personnel with unique credentials. <div style="border: 1px solid black; background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p>Note: At least 20 access accounts are required to ensure all support personnel have individual access.</p> </div> 3. Assign the necessary permissions for accessing the required systems. 4. Provide the Cognex Technical Support team with the VPN connection details, including the server address, login credentials, two-factor authentication, and any required VPN client software. 5. Continuously maintain accounts and provide the Cognex Technical Support team with relevant updates on policies.

<p>Virtual Desktop Infrastructure (VDI)</p>	<ul style="list-style-type: none"> • VDI solution (such as VMware Horizon or Citrix). • Sufficient bandwidth to support remote desktop sessions. • Software or web browser to provide the Cognex Technical Support team with. <p>Recommendations for Setup:</p> <ol style="list-style-type: none"> 1. Set up a VDI instance within your network. For example: <ol style="list-style-type: none"> a. Configure a virtual desktop. b. Set resource allocations (CPU, RAM, storage, and necessary software to access Cognex equipment). c. Define access controls. 2. Create dedicated VDI user accounts for the Cognex Technical Support personnel. <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>i Note: At least 20 access accounts are required to ensure all support personnel have individual access.</p> </div> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>i Note: Make sure that the support personnel only have access to the necessary applications and data.</p> </div> <ol style="list-style-type: none"> 3. Provide the Cognex Technical Support team with the connection details, including the VDI portal URL, login credentials, and two-factor authentication.
<p>TeamViewer</p>	<ul style="list-style-type: none"> • Latest TeamViewer software installed. • Internet connection for simultaneous connection between on-site equipment and Cognex Technical Support. <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>i Note: Make sure you have IT permission to change the Ethernet adapter settings on your laptop.</p> </div> <p>Recommendations for Setup:</p> <ol style="list-style-type: none"> 1. Make sure TeamViewer is installed and running on a Windows PC connected to the Unit box. 2. Open TeamViewer to obtain the session ID and password. 3. Share the session ID and password with the Cognex Technical Support team to enable a secure connection.

<p>Video Conferencing Software</p>	<ul style="list-style-type: none"> • Video conferencing software application installed, such as: <ul style="list-style-type: none"> ◦ Microsoft Teams ◦ Zoom ◦ Webex <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p>i Note: Run the video conferencing software on a Windows PC connected to the Unit box.</p> </div> <ul style="list-style-type: none"> • Internet connection for simultaneous connection between on-site equipment and Cognex Technical Support. <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p>i Note: Make sure that you have company permissions to share in a meeting and give remote control.</p> </div> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p>i Note: This access option is not recommended by the Cognex Technical Support team since it limits the ability of the support team to resolve problems.</p> </div> <p>Recommendations for Setup:</p> <ol style="list-style-type: none"> 1. Either party can schedule a meeting and share the meeting invitation link with the other party. 2. Use the provided meeting ID or link to join the meeting at the scheduled time. 3. Share your screen with the Cognex Technical Support.
------------------------------------	--

Open Source Licenses

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

@amcharts/amcharts3-angular	Paid
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
Timescaledb	Apache-2.0
Timescale toolkit	Timescale License
zone.js	MIT

Copyright © 2025
Cognex Corporation. All Rights Reserved.