

Corvina Basic Training

May 2025





Corvina Basic Training

Learn the fundamentals of Corvina, connect a device to the VPN and IOT while completing interactive examples. This training covers the following:

- Introduction to Corvina (4)
- Getting Started (18)
- VPN (38)
- IOT (60)
- CEM (90)
- Other Applications (102)

Corvina Basic Training Exercises

1. Sign in to Corvina (31)
2. Activate the Device for VPN (46)
3. Configuring Applications and Profiles (53)
4. Adding an Endpoint (55)
5. Install Corvina Cloud App Lite (57)
6. Test the Device (59)
7. Activate the Device for IOT (68)
8. Building a Dashboard (87)
9. Execute a Campaign with OTA (101)
10. Sending an email Notification (109)

Introduction to Corvina

Terminology (5)

Introduction (9)

Commercial Model (12)



Terminology

- PaaS – Platform as a Service. Allows for the holder to generate their own resources.
 - Dealer PaaS – The PaaS holder can generate an unlimited number of resources to distribute to customers.
 - Dedicated PaaS – Dealer Pass with additional features including first level domain name.
- SaaS – Software as a Service. A suborganization of a PaaS. The holder must receive resources from its parent organization or PaaS.
 - SaaS Owner – User with an organization that receives resources from the PaaS. It manages and distributes resources to its suborganizations (customers) or uses the resources for itself.
 - SaaS Reseller – Distributor of Corvina who will not have an organization above their customers. SaaS Reseller customers will be placed as Exor America suborganizations

Terminology

- IOT – Internet of Things. Corvina IOT receives data from field level devices (sent through MQTT) and stores it in the cloud. The data can be viewed, exported, displayed or written in a dashboard and integrated with other applications and platforms by using the API
 - MQTT – (Message Queuing Telemetry Transport) A lightweight, publish/subscribe protocol that is often used in IOT applications for transferring data between devices and the cloud
 - Model – (Data Model) A profile of tags and tag properties that is defined in Corvina and can be applied to any number of Corvina devices. The data model properties define the association between the device tags and the tags to be stored in Corvina
 - Mapping – Contains the send (push) policies for updating the tag's value in the cloud. This includes rules for when or how often to send data to the cloud, history policy, and read/write permission
 - Dashboard – User defined interface where IOT data (from any number of devices) can be read and/or written

Terminology

- VPN – Virtual Private Network. Corvina VPN provides an interface where devices can be accessed remotely
 - Corvina Cloud App – Application that is called by Corvina and runs in the background to establish the VPN connection
 - Gateway – Edge device (usually Exor HMI) that is connected to the internet to reach Corvina
 - Endpoint – Device that is connected to Corvina through the gateway
 - Application – Access to device or endpoint functions through web or third party applications installed on the client side , launched from Corvina
- Notification – email message sent as an indicator that a JMobile alarm (which was sent to Corvina) has been triggered.
- Rest API – Set of functions that allow other applications to access and interface with Corvina

Terminology

- CEM – Corvina Edge Management. An industrial fleet management solution that allows for update files to be deployed to many devices at the same time on a schedule.
- OTA – over the air. The fleet management application in Corvina that helps make CEM possible.
- Artifact Registry – the file storage/management application in Corvina that helps make CEM possible.

Terminology

- IAM – Identity Access Management. Interface where administrative level users can monitor and manage organizations and users
 - Organization – (Domain) Collection of users and devices, can be arranged in a hierarchy with child/suborganizations
 - User – Account used to access Corvina. Must belong to a particular organization.
 - Role – Policy used to define user permissions
- Dealer
 - Resources – Items generated by a PaaS that can be used or distributed to a SaaS (suborganization). This refers to Organizations, Users, Devices, IoT Messages, and VPN Credits.
 - Device (Activation) – Resource that allows for a device to be activated on Corvina.
 - IoT Message (Credit) – Resource that allows for 4KB of data to be sent to/from Corvina.
 - VPN Credit (Month) – Resource that allows for one device to be used with Corvina VPN for one month

What is the Corvina Platform?

- Corvina Platform is an Industrial IoT Platform for Smart Manufacturing and Smart Machine Solutions.
- Corvina Platform is the cloud-based, all-in-one data management platform that provides the technology you need for the industrial world.
- It is an administration shell for distributed edge systems, integrating data collection, monitoring and control, configuration management, integrated web tools and programming environments to support the machinery and applications throughout its whole lifecycle providing productivity increase and new Business Model based on Services.

What does the Corvina Platform do?

- Corvina Platform connects any products, plants, systems, and machines, new or legacy. It allows the data generated by the Internet of Things to be processed simply and intuitively with advanced analysis.
- It bridges layers between IT and OT architecture, providing effective tools to access all the Industry 4.0 benefits, such as asset performance management, artificial intelligence, cloud edge computing, predictive maintenance, data modeling and OT remote monitoring.

What does the Corvina Platform do?

- VPN for remote access.
 - Connect gateway devices to the platform. Establish a VPN connection to perform a project download/upload. Monitor or control the JMobile project using VNC or JMobile web pages.
 - Connect endpoint devices to the platform by extension of the gateway. Manage and monitor the endpoint through the VPN connection.
- IoT for data storage and management.
 - Send data from JMobile to Corvina for storage.
 - Create dashboards using a drag and drop interface to view data from any devices.
 - Use dashboards to write data back to JMobile or to manipulate it in the cloud.
 - Utilize the API to interface between Corvina and other applications and platforms.
- Development platform for other applications.
 - Corvina includes a marketplace where applications developed by Corvina or other developers can be distributed or sold.
 - Predictive maintenance, fleet management, ERP

Dealer PaaS

- Available for a monthly cost.
- “Top level” organization.
- Allows the owner to infinitely generate resources:
 - Unlimited device activations for no cost.
 - Generate VPN Credits for low cost, billed monthly based on consumption.
 - Generate IOT Messages for low cost, billed monthly based on consumption.
- Designed for distribution, system integrators, and OEMs who would like to offer their own IoT products to their customers.
- Generate resources and sell them to customers on the PaaS (SaaS Owners) with the freedom to determine custom business model and pricing.
- Includes access to the dealer dashboard to create and distribute resources in the form of license codes.



Dedicated PaaS

- Includes all features of Dealer PaaS.
- “Top level organization” with the option to have a 1st level domain name.
- Designed for large OEMs.
- On premises installation available as an option.
- Adds the ability to create SaaS owners who have access to the dealer dashboard.

SaaS Owner

- A suborganization of a PaaS.
- Receives resources from the PaaS they reside on, either manually from the PaaS owner or by adding product licenses.
- Designed for distributors or system integrators who need to manage their customers but do not have enough business to support a Dealer PaaS.
- OEMs or end users who do not resell Corvina ("SaaS Consumers") are also technically SaaS Owners.
- Cost per device activation and additional cost for resources.
- Sell resources to their suborganizations (their customers who are SaaS Owners beneath their organization).

VPN Price Model

- All devices must be activated on Corvina with a device activation code.
- In addition to the device activation, Corvina VPN must be purchased in one of two ways:
 1. Paid up front: the device activation code comes with 3 years, 5 years, or lifetime VPN included for the device.
 2. Pay as you go: the device activation code does not include VPN access. Individual months of VPN can be purchased. Once applied to a device, the VPN can be used for one month.
- VPN usage is always unlimited during the time that the service is active.
- Lifetime VPN can be retroactively applied to an existing device activation code that was purchased without VPN.
- Any device that was migrated from Corvina Cloud 1 includes 3 years of VPN (until January 2027).

IoT Price Model

- All devices must be activated on Corvina with a device activation code.
- IoT Messages are purchased and used to allow for data to be sent between JMobile and Corvina.
- An IoT Update occurs any time any of the following are processed:
 - A tag is sent from JMobile to Corvina.
 - A tag is sent from Corvina to JMobile.
 - An alarm is sent from JMobile to Corvina.
 - Data stored in Corvina is manipulated from within Corvina.
- 1 IoT Message is consumed after 160 IoT Updates are processed.
- IoT Messages will be applied to any device that uses them, they do not need to be assigned to a device.

Getting Started

Hardware and Software Compatibility (19)

Network Requirements (22)

Onboarding and Autoregistration (25)

Accessing Corvina (28)

Updates (36)





Software Compatibility

- Corvina VPN requires either BSP version 1.3 or higher or BSP 1.0 800 or higher
- Corvina IoT requires either JMobile version 4.5 or higher for use with BSP 1.3+ or JMobile version 4.2 for use with BSP 1.0



Hardware Compatibility

- Corvina is compatible with all Linux based Exor hardware:
 - All versions of eX700, eX700M, and eX700M-Web
 - All versions of eXWare
 - eSmart107 and all other versions of eSmart with limitations*
 - All versions of JSmart700, JSmart700M, and JSmart700M-Web with limitations*
 - All versions of eX200
 - All versions of MicroEdge

*See Network Recommendations (21)

Network Recommendations

- Corvina VPN is best used on devices with multiple ethernet ports.
 - Port eth0 should always be used as the WAN, ideally with DHCP enabled to easily connect to the network at any site.
 - Ports eth1 and eth2 should be reserved for connection to endpoint devices such as PLCs.
- The above configuration will allow for a system to be deployed at a new site without changing endpoint IP addresses to accommodate the network. eth0 will receive a valid IP address via the DHCP server which will allow endpoint devices to reach the internet.
- Since most eSmart have only one ethernet port, the above configuration is not possible. eSmart can still be used with Corvina VPN and IoT but it cannot be recommended because endpoints would need to be reconfigured to reach the internet and utilize the device's firewall.
- JSmart can only achieve this desired configuration when using the Wifi (because JSmart have only one ethernet port). eSmart can also achieve this configuration by using a USB Wifi dongle.



VPN Network Requirements

The following ports must be open to allow for the Exor device to use Corvina VPN services:

URLs	Service Name	Port	Direction
pairing.corvina.io	Corvina pairing services	443/TCP	Outgoing
remote2.pairing.corvina.io	Corvina VPN services	443/TCP	Outgoing
vpn2.corvina.io	Corvina VPN services	1194/UDP, 443/TCP	Outgoing
vpn2bck.corvina.io	Corvina VPN backup	1194/UDP, 443/TCP	Outgoing
corvinacloud.com	Migrated devices	443/TCP	Outgoing
vpn2wce.corvina.io	WCE devices	1194/UDP	Outgoing
47.106.172.82	Corvina China services	1194/UDP	Outgoing



IoT Network Requirements

The following ports must be open to allow for the Exor device to use Corvina IoT services:

URLs	Service Name	Port	Direction
pairing.corvina.io	Corvina pairing services	443/TCP	Outgoing
api.platform.corvina.io	Corvina IoT services	443/TCP	Outgoing
broker.corvina.io	Corvina IoT services	8883/TCP, 443/TCP	Outgoing

PC Network Requirements

The following ports must be open to allow for the PC to connect to Corvina VPN services:

URLs	Service Name	Port
*.corvina.io	Corvina website and services	443/TCP
*.remote2.corvina.io	Corvina Cloud App Lite	443/TCP
vpn2.corvina.io	Corvina VPN services	1194/UDP, 443/TCP
vpn2bck.corvina.io	Corvina VPN services	1194/UDP, 443/TCP



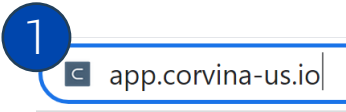
Onboarding

- Typically, the PaaS Administrator will create an organization for a new company that is using Corvina.
- The new organization must also have at least one user who will be able to access it.
- The user accounts can be created by the PaaS Administrator. The account will always be associated with an email address and a welcome message will be sent to the address with instructions for activating the new user account.
 - The welcome message may go to the spam/junk folder.
 - The account must be activated within 12 hours of the welcome message being sent.
- Exor America offers to host a 1-2 hour onboarding session to help new users access Corvina and activate their first device.

Autoregistration

- All versions of the MicroEdge include a special activation code that has been pre-entered into the device system settings (saving steps in the VPN device activation process).
- This code can be used to initiate organization and user autoregistration. This allows a new user to create their own organization and user account.
- Autoregistration should only be done by users with no existing organization or user account. Existing users should add their device normally to their organization.

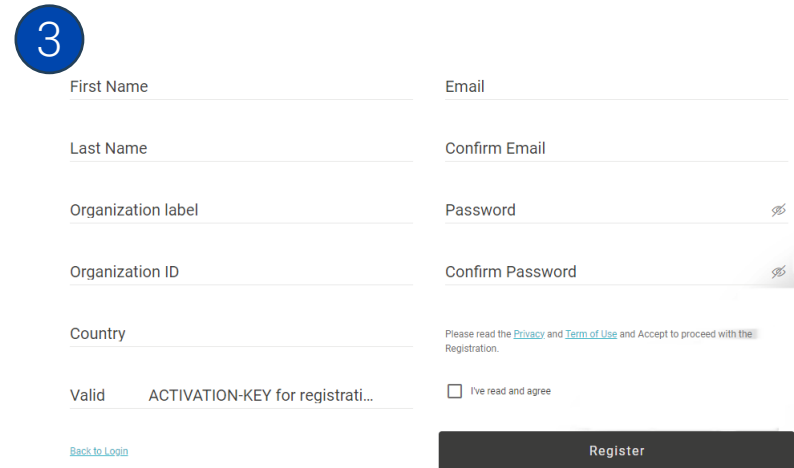
Autoregistration



Use the link to open the Corvina Platform page in your preferred browser: <https://app.corvina-us.io>



Click “Register” to begin the autoregistration process to create a new organization to add the MicroEdge to.



Enter the account information, agree to the terms, and register the new organization and account.



Sign In to Corvina Platform

1

 app.corvina-us.io

Use the link to open the Corvina Platform page in your preferred browser: <https://app.corvina-us.io>

2

CORVINA
CLOUD

Username

your.email@address.com

Password

.....

[Forgot Password?](#)

Log In

Enter your username (email address) and password to sign in. If the account is a member of multiple organizations, there will be an option to select the organization to access.

Forgot Password

- When the password is not known or if the email to activate the account has not been received, use “Forgot Password?” at the login screen to recover the account.
- A new email will be sent to the address associated with the account to set a new password.
- Passwords are not known to the PaaS Administrator and cannot be recovered in any other way.

Organization Access

- If the account that is being accessed exists as an account on more than one organization, a selection screen will show after logging in. Select the organization to sign in to Corvina from.
- Use this link to change the organization without signing out of Corvina:
<https://app.corvina-us.io/#/organization>
- Keep in mind that the organization that Corvina is being viewed from can be changed

CORVINA
CLOUD

Hi matt.durbin@exorint.com,
Select the organization to access

Brian's Playground



Laserax



exor



exor america demo



exortesting3



Exercise 1.1: Sign in to Corvina

The goal of this exercise is to log in to Corvina using an organization and account created specifically for this training. Feel free to refer back to the previous slides (noted in the parenthesis for help).

1. Open the automated email sent by Corvina. (25)
2. Activate the new Corvina account by clicking the link and setting a password (25) or by opening Corvina at <https://app.corvina-us.io> and using "Forgot Password". (29)
3. Sign in to Corvina. (28)
4. If the account belongs to multiple Corvina organizations, select "Corvina Training" when presented with the option. (30)

Navigating Corvina Platform

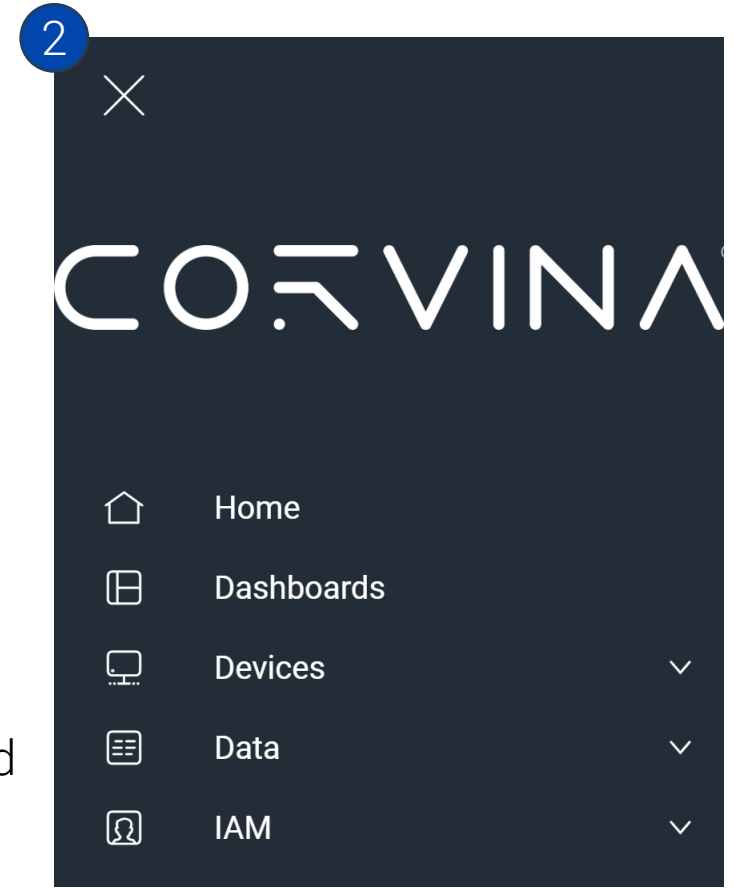


Click the menu icon to show the navigational options that are available to your user account.

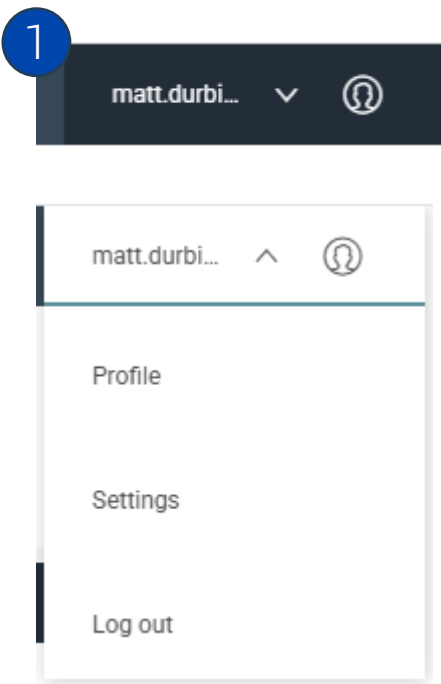
Expand Devices and Select VPN to open the VPN interface for remotely accessing the devices.

Expand Data and select Explore to view the stored IOT data. Alarms and Notifications can also be accessed from here.

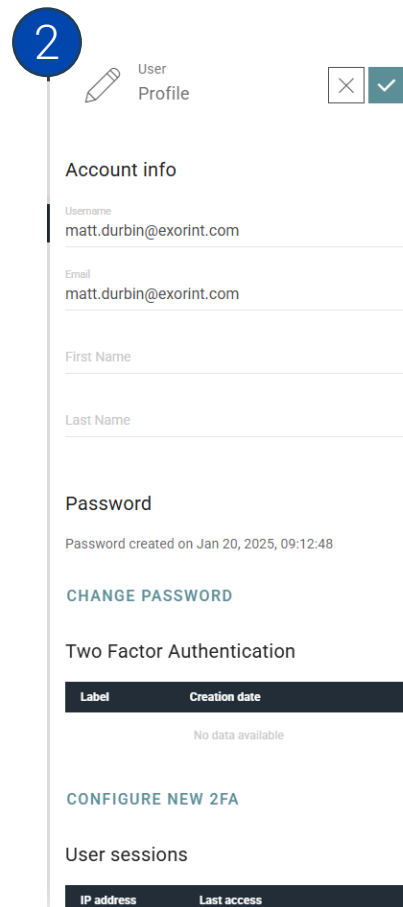
Click Home or Dashboards to view the Dashboards that can be accessed from your account.



User Profile



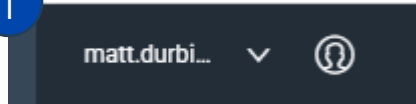
Click the account name in the upper right of Corvina to view the user menu. Click “Profile” to edit the profile.



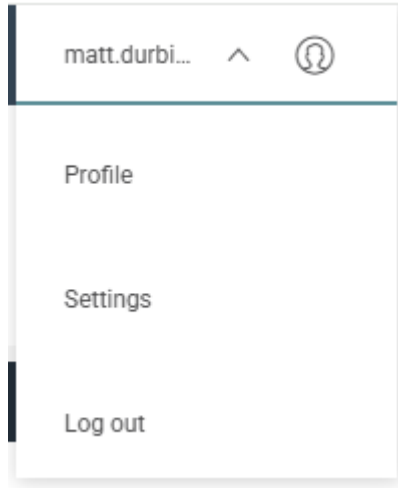
From here, it is possible to edit user information, change the password, configure two factor authentication, and view recent user sessions.

Logging Out

1



Click the account name in the upper right of Corvina to view the user menu. Click “Log out” to end the session.



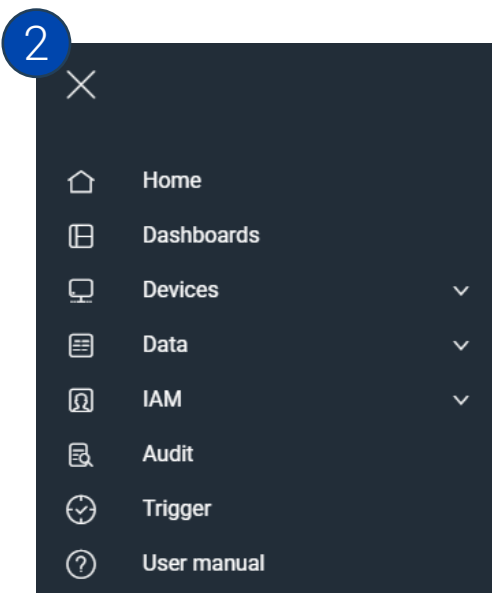
2

This will end the session and return to the login screen.

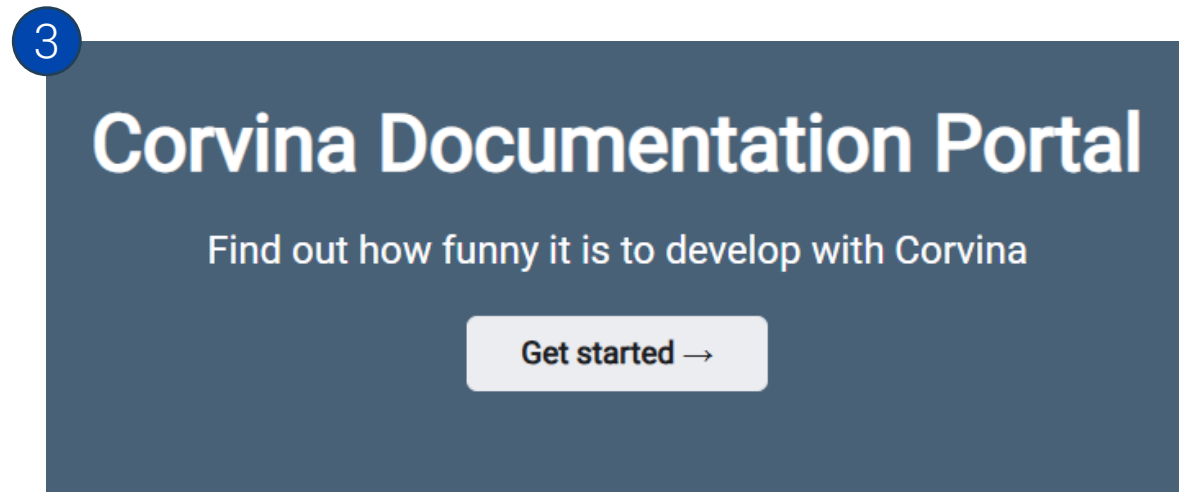
Help



Click the menu icon to show the navigational options that are available to your user account.



Click “User manual” to open the user manual in a new tab.



User Documentation

Discover all the services and cool features that our flexible and rich platform offers

Click “Get started” to view the documentation.

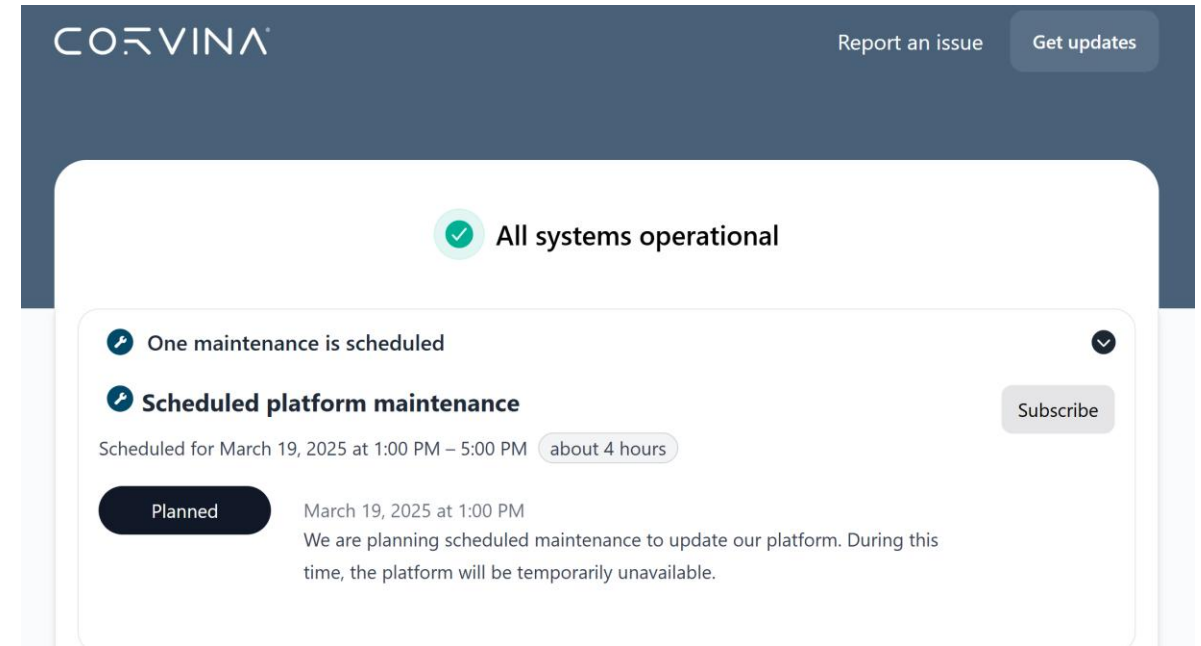


Changelog

- A complete log of all updates and changes made to Corvina can be found here:
<https://app.corvina-us.io/changelog/>

Updates and Maintenance

- Scheduled maintenance is communicated to users upon signing in to Corvina.
- Current status of Corvina as well as planned maintenance can be viewed at <https://corvina-us.instatus.com/>
- Use “Get updates” to subscribe to email notifications for scheduled maintenance.



VPN

Device Activation (39)

Applications and Profiles (48)

Endpoints (54)

Corvina Cloud App Lite (56)

VPN Connection (58)



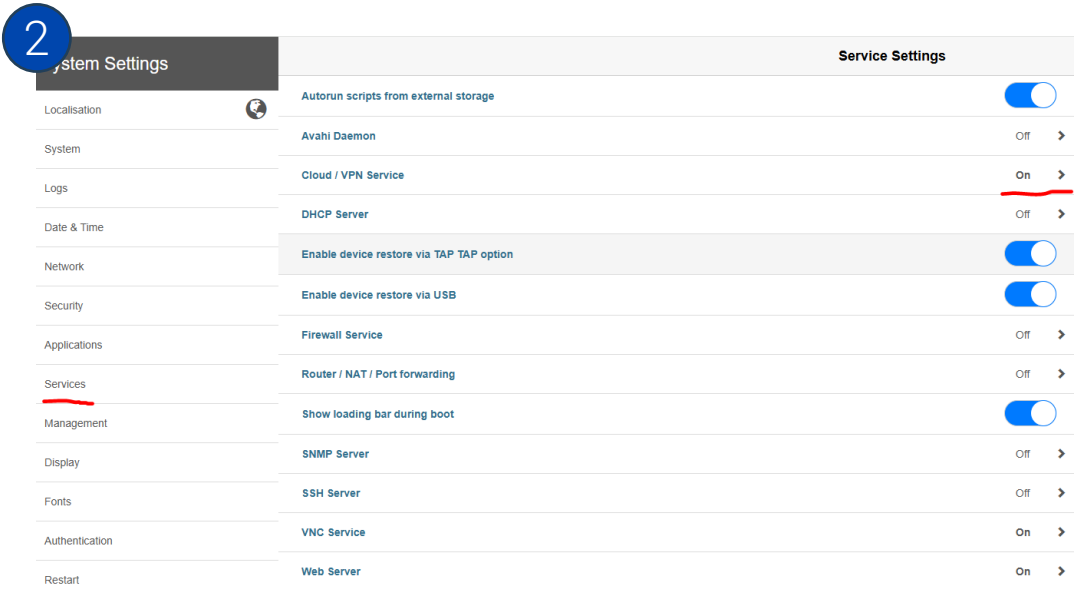


VPN Setup

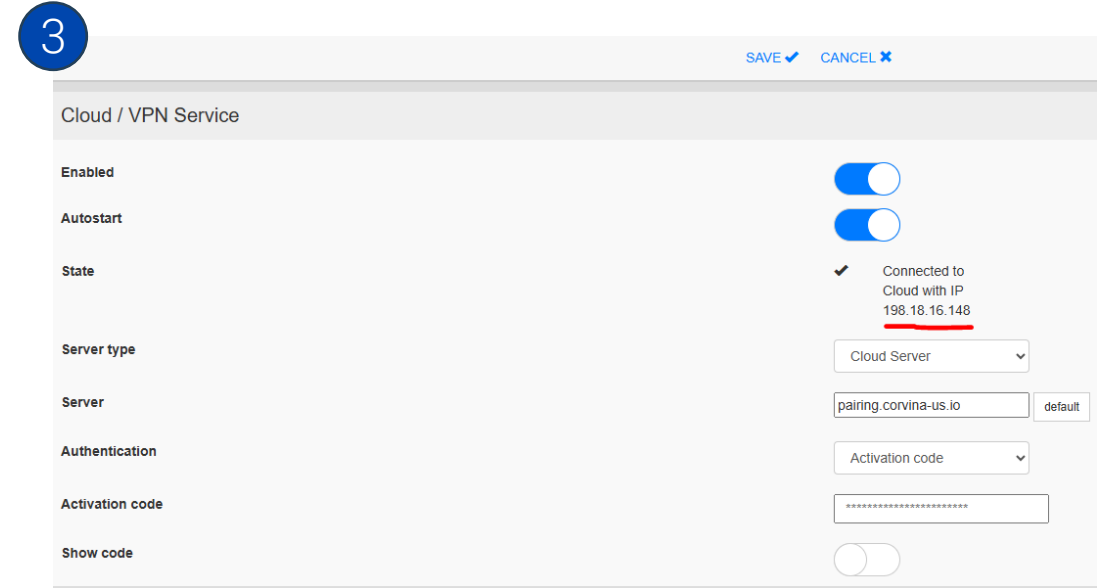
- The physical Exor device must be paired to the device in Corvina in order to activate it and establish a VPN connection.
- To pair the device, the same activation code needs to be entered:
 - On the device in the System Settings.
 - In the Corvina device activation interface.
- The above steps may be done in either order, the device will come online once both are completed and the service has been activated.
- For device activation codes that do not include 3 year, 5 year, or lifetime VPN, a VPN month must be applied to the device to activate the service.

System Settings VPN Configuration

1 Access the system settings from either startup, the context menu, or through a browser on a connected device at [https://\[IP_ADDRESS\]/machine_config](https://[IP_ADDRESS]/machine_config) Log in using the correct user credentials.

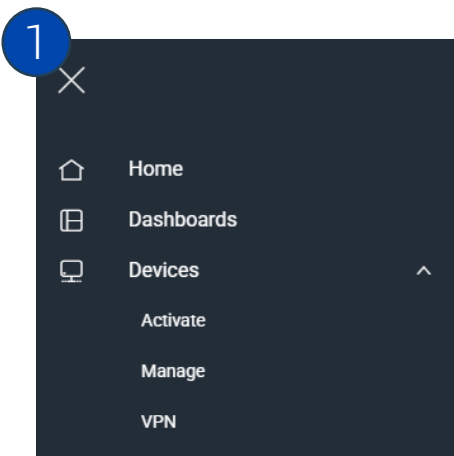


Navigate to “Services” and view the “Cloud/VPN Service”.



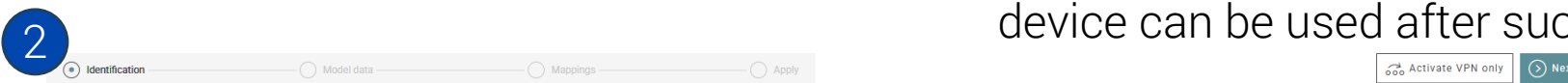
Enable the service and turn the autostart on. Make sure that server type is set to “Cloud Server’ add “pairing.corvina-us.io” as the server, set the authentication type to “Activation code” and enter the activation code. Save when finished. An IP address will show if the connection is successful. Keep in mind that the device needs to be activated in Corvina with the service enabled before it can successfully connect, otherwise an error here is to be expected.

Device Activation (VPN only)



From the menu, select Devices -> Activate to begin the device activation process.

Enter a name for the device, select a location on the map, enter the activation code, and add a description (optional). Click “Activate VPN only” when finished, this will create the device in Corvina to be used with VPN. A VPN credit may still need to be applied to enable the service if the activation code does not include VPN already. The system will automatically navigate to Devices -> VPN where the device can be used after successful pairing.



Device Label

Training_Test

Latitude

39.34383571572077

Longitude

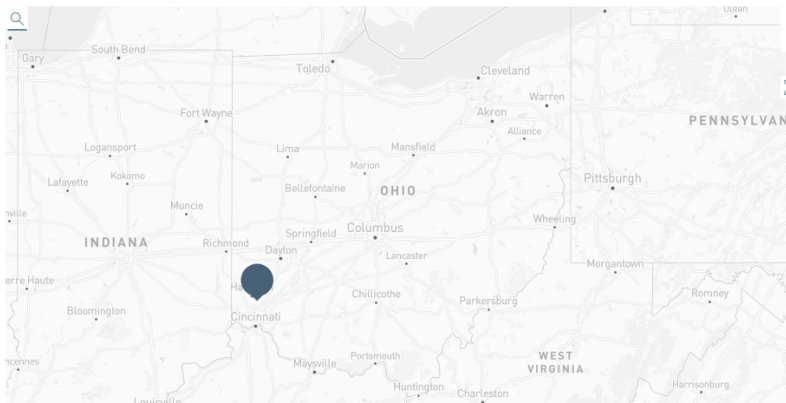
-84.49878931045532

Activation Code

5057J-Q0Si2-QX20U-8B61C

Description

Training demq



VPN Service

- In Devices -> VPN, a device with no service will show an empty circle as the “Enabled” icon and a gray status icon.

Device	Serial No.	Description	Groups	Enabled	Renew	Status
Training_Test		Training demo				

- Click the 3 dots icon and then click “Assign VPN months” to apply a VPN month to the device, enabling the service for 1 month. Check “Autorenew” to automatically apply another month when the month ends. Roll the mouse over the “Enabled” icon to view the service’s duration.

eXware_demo_01		eXwares				
eXware_demo_02		eXware...				

Will renew on Mar 27, 2025, 10:15:35

- A device with lifetime VPN will show service enabled until December 31, 2049.

TestDevice		Talk to Rockwell etc.				
						

Valid until Dec 31, 2049, 18:00:00

Debugging VPN Connectivity Problems

- If a configured device is not showing an online status in Corvina VPN, then this is an indication that the Device is failing to connect to Corvina VPN. Follow the steps to debug.
 1. Check to make sure that the service is enabled on the device in Devices -> VPN. If it is not enabled, apply a VPN Month. (42)
 2. Check to make sure that the device has a connection to the internet. In the System Settings, enable NTP in the Date and Time interface. If NTP does not work then this is indicative of there being no internet connection. (45)
 3. Check the VPN settings in the System Settings to see if there is an error message and to make sure that the settings are configured correctly.
 1. Is there an error message? (44)
 2. Is the activation code entered correctly? Does it match the code entered into Corvina?
 3. Is the server entered correctly? (40)

Cloud/VPN Service Error Messages

- The following errors may appear in the “Cloud/VPN Service” configuration screen of the HMI System Settings:

Error Message	Solution
VPN Client Failure	Refresh the “Cloud/VPN Service” configuration or cycle power. (40)
Server unreachable, Content not found, or Server Authentication Failure – please check the credentials	Make sure the server is entered correctly in the “Cloud/VPN service” configuration. (40)
Failed verifying Server – check CA certificate	Make sure date, time, and time zone are set correctly on the HMI. Make sure ports are not blocked by a network firewall. (22)
Server Authentication Failure – please check the credentials	Make sure the server is entered correctly in the “Cloud/VPN service” configuration. (40) Make sure the activation key is entered correctly in the “Cloud/VPN service” configuration and that it matches the one entered into Corvina. (40, 41)
Activation code not registered	Make sure the activation key is entered correctly in the “Cloud/VPN service” configuration and that it matches the one entered into Corvina. (40, 41)
Configuration download failed – please check logs	Make sure ports are not blocked by a network firewall. (22)

Debugging Internet Connectivity Problems

- In the System Settings, enable NTP in the Date and Time interface. If NTP does not work then this is indicative of there being no internet connection. Check the following:
 1. Is the device connected to a network where it can reach the internet through port eth0? Or via the Wifi on JSmart devices?
 2. Does port eth0 have either DHCP enabled, or a static IP address that can connect to the network?
 3. Could the connection be blocked by the IT department of the installation site? (22)
 4. Try restoring the network settings from System Settings -> Network and selecting "Restore".

Exercise 1.2: Activate the Device for VPN

The goal of this exercise is to successfully connect a device to Corvina VPN with the service enabled for one month. Feel free to refer back to the previous slides (noted in the parenthesis for help).

1. Configure the “Cloud/VPN Settings” on the HMI so using a device activation code from the training folder. The folder contains a spreadsheet called “Device Activation Codes”, use the code corresponding to the training kit number. (40)
2. Activate the device on Corvina. (41)
3. Enable the service for one month. (42)

A device that is properly connected will show a blue “Status” icon. Refer to slides 42-44 to debug a failed connection.

Device Management

- Devices -> Manage allows for the device to be:
 - Edited
 - Change device name or description
 - Change device location
 - View the last 5 digits of the device activation code
 - Add the device to a device group
 - Change IoT Model and Mapping
 - Deleted
 - Moved to a different organization
- Devices can be added to a device group to easily organize them and collectively assign permissions to all devices in the group simultaneously

Applications and Profiles

- Applications can be used to access a gateway or endpoint device via a third party service.
 - HTTP and HTTPS
 - VNC
 - SSH
 - RDP
 - Custom (launch an application on the PC such as JMobile Studio, Codesys, or other PLC programming software)
- A profile is a defined group of applications. The profile is meant to be applied to the gateway or endpoint, this designates which applications may be used with that device.
- The applications that are applied to the device via the profile can be launched with a single click.

Creating Applications

1



Click the "+" icon from the "Applications" tab to begin creating a new application.

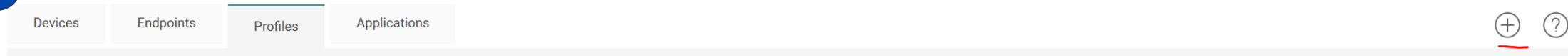
2



Name the application and select the application type. Configure any additional parameters and then save the completed application.

Creating and Assigning a Profile

1



Click the "+" icon from the "Profiles" tab to begin creating a new profile.

2

Name the profile and select the applications to be applied to the profile, then save the completed profile.

3

Assign the profile to the device either from the "Devices" tab or from the "Endpoints" tab by editing the device.

Launching Applications

1

^

eXware_demo_01

✓

✓

⋮

Endpoint	Application	Status
gateway connected - Disconnect Gateway VPN IP: 100.64.0.65 Real IP: 127.0.0.1 Connected users: matt.durbin@exorint.com	JM4Web	
	JMobile_4.5	Native
	System_Settings	
	VNC	

Click the application that you would like to launch.

JM4Web will open the web page for the JMobile project in a new tab.

VNC will open a VNC client to remotely view and control the JMobile project in a new tab.

JMobile 4.5 will attempt to launch JMobile Studio (which will only be possible if it is installed on your PC). Once there, the VPN IP address can be used to upload the JMobile project.

2

View the JM4Web or VNC application in the new tab. Use it to demo the project and close when finished.

Application Direct Access

- Direct access can be assigned to a user account. This will make it so that a selected application will immediately load after logging in to a user account where this feature is enabled.
- To assign direct access, edit the user account and configure a "Favorite App" with the "+" icon. Select a device and an application (which the device has access to) to launch with direct access.

Favourite Apps



× Matt_707M/gateway/VNC

Exercise 1.3: Configuring Applications and Profiles

The goal of this exercise is to successfully create applications, apply them to a profile, and assign the profile to the device. Feel free to refer back to the previous slides (noted in the parenthesis for help).

1. Create 3 applications: (49)
 - HTTPS to open the JM4Web page
 - VNC
 - HTTPS to open the system settings
2. Create a new profile and apply the 3 applications to it. (50)
3. Assign the new profile to the VPN device. (50)

Endpoints

1

Device	Endpoint	Description	IP Address/CIDR	Application profile	Enabled	Actions
▼ Brian_JSmart		Brian's JSmart710 demo				

Click the "+" icon from the "Endpoints" tab, corresponding to the device that the endpoint is connected to.

2

Create Endpoint

Name

PLC

Description

IP Address/CIDR

192.168.1.20

Application profile

Default

×

Enabled

☒

Name the endpoint. Enter its IP address. Assign the profile If any applications are to be used with it, then save the completed endpoint.

Edit the device to increase the maximum number of endpoints or to use real IPs instead of virtual. There is a default maximum of 14 endpoints but this may be expanded.

Exercise 1.4: Adding and Endpoint

The goal of this exercise is to add two endpoints to the device. Feel free to refer back to the previous slides (noted in the parenthesis for help).

1. Edit the device and change the maximum number of endpoints from 2 to 6. (54)
2. Add two endpoints that are placeholders for PLCs. (54)

Corvina Cloud App Lite

Before the VPN can be used for the first time on your PC, the Corvina Cloud App must be installed. The Corvina Cloud App is a service, managed by the Corvina Platform web portal, that is used to establish a VPN connection. After installing this, it will not need to be installed or even opened manually again on the PC, it will be managed by Corvina.



On the VPN page, click the arrow to download Corvina Cloud App.

2

Locate the installer in the downloads folder and run it to install Corvina Cloud App.

Exercise 1.5: Install Corvina Cloud App Lite

The goal of this exercise is to install Corvina Cloud App Lite to allow for a point to point VPN connection to be initiated from the PC. Feel free to refer back to the previous slides (noted in the parenthesis for help).

1. Open the Devices -> VPN page and locate the red bar at the bottom of the screen, which indicates that Corvina Cloud App Lite has not yet been installed on this PC. (56)
2. Click the red arrow to download Corvina Cloud App Lite. (56)
3. Locate the installation file in the downloads folder and install Corvina Cloud App Lite. (56)

VPN Connection

1

☒ Corvina Cloud App
ON-LINE - Open Corvina Cloud App interface

LOGIN

☒ Corvina Cloud App
ON-LINE - Open Corvina Cloud App interface

IP : 198.18.0.32
matt.durbin@exorint.com

On the VPN page, click Login to launch the Corvina Cloud App service and open the possibility to establish a connection to the devices.

2

☒ eXware_demo_01

Locate the device that you would like to connect to and click the arrow to expand it.

3

☒ eXware_demo_01

Endpoint	Application	Status
gateway not connected - Connect Gateway	JM4Web	
	JMobile_4.5 Native	
	System_Settings	
	VNC	

Click Connect to establish the connection. A successful connection will show the connected user and the VPN IP address. This IP address can be used to interface with the device. Disconnect when finished.

☒ eXware_demo_01

Endpoint	Application	Status
gateway connected - Disconnect Gateway VPN IP: 100.64.0.65 Real IP: 127.0.0.1 Connected users: matt.durbin@exorint.com	JM4Web	
	JMobile_4.5 Native	
	System_Settings	
	VNC	

Exercise 1.6: Test the Device

The goal of this exercise is to establish a VPN connection to the HMI and download a JMobile project. Feel free to refer back to the previous slides (noted in the parenthesis for help).

1. Log in to the Corvina Cloud App Lite application. (58)
2. Locate the device and connect to it. (58)
3. Once connected, use the virtual IP address to download a project from JMobile. Open a JMobile project, enter the virtual IP address into the Run -> Manage Target interface, and download the project. (58)

IoT

Device Activation, Models, and Mapping (61)

Stored Data (69)

Editing Models and Mapping (70)

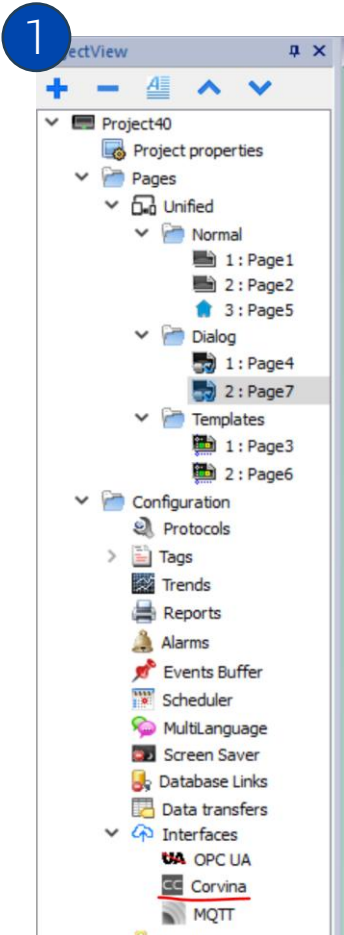
Dashboards (72)



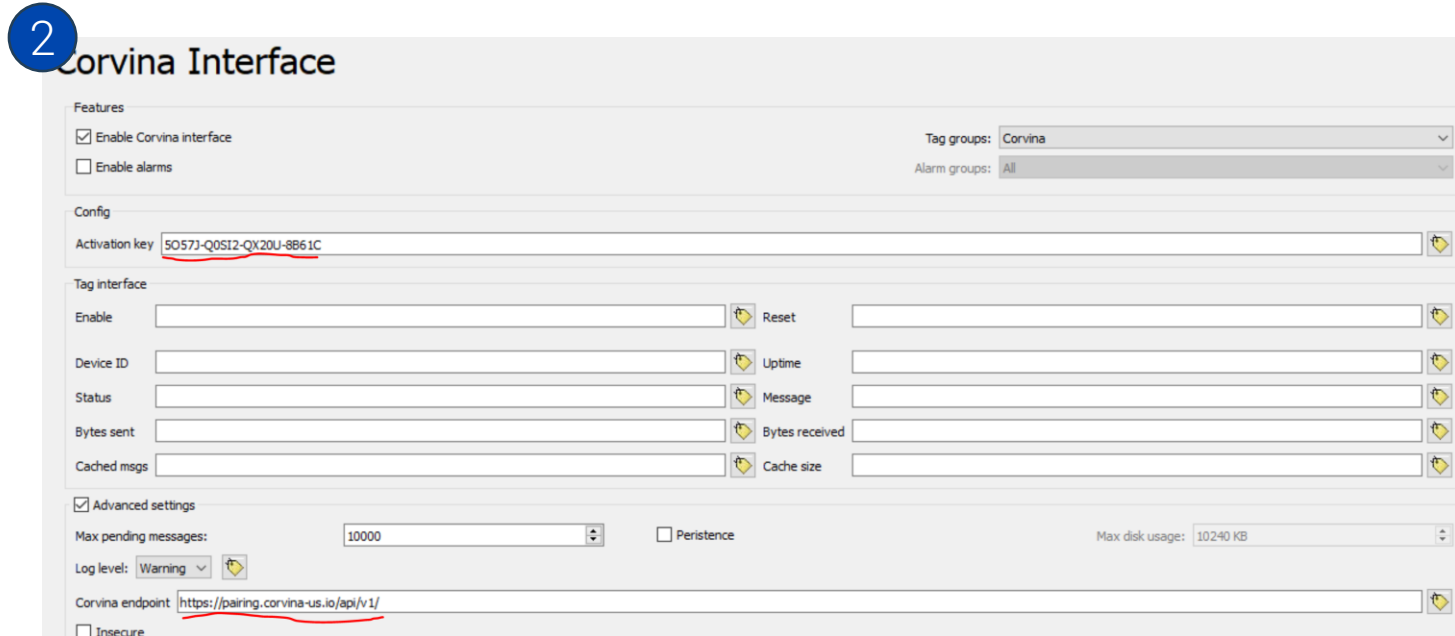
IoT Setup

- The physical Exor device must be paired to the device in Corvina in order to activate it and establish an IoT connection.
- To pair the device, the same activation code needs to be entered:
 - On the device in the JMobile Corvina Interface.
 - In the Corvina device activation interface.
- Unlike with the VPN, the activation process is best done in order, with the JMobile Corvina interface being configured first before adding the device in Corvina.

JMobile Corvina Configuration

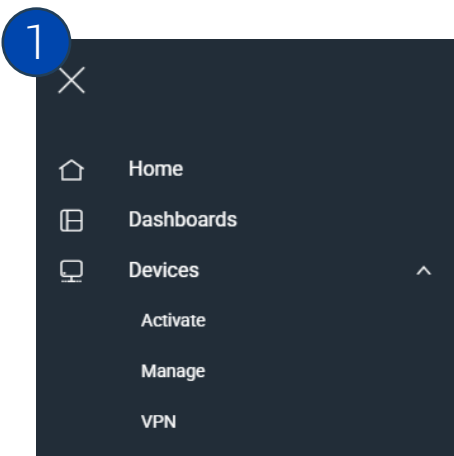


Open the JMobile project that will be used with Corvina. Expand "Interfaces" and double click "Corvina" to open the JMobile Corvina interface.



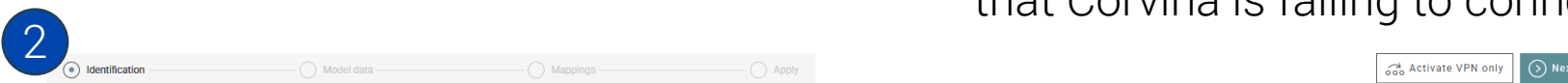
Enable the interface. Select the tag group(s) that should be used with Corvina, or select "All" to use all tags in the project with Corvina. Enter the activation code; if using both IoT and VPN, the same activation code will be used for both. Enter "<https://pairing.corvina-us.io/api/v1/>" as the Corvina endpoint. Download the JMobile project to the HMI after the configuration is complete.

Device Activation



From the menu, select Devices -> Activate to begin the device activation process.

Enter a name for the device, select a location on the map, enter the activation code, and add a description (optional). Click "Next" when finished to initiate the device pairing process for IoT. Corvina will attempt to communicate with the HMI and read the tags that are being used with Corvina. If the connection is successful, a message will appear about models and mapping. Click "Continue" to proceed with creating the model and mapping. If the interface permanently stalls with an option to "Continue with device offline", this indicates that Corvina is failing to connect to the device.



Device Label

Training_Test

Latitude

39.34383571572077

Longitude

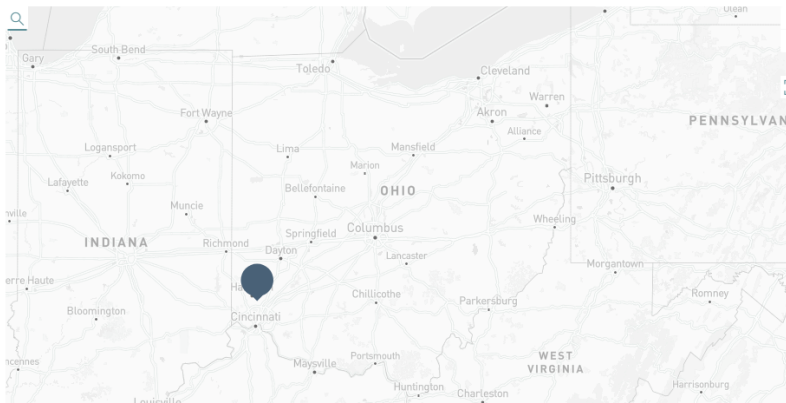
-84.49878931045532

Activation Code

5057J-Q0Si2-QX20U-8B61C

Description

Training demq



Debugging IoT Connectivity Problems

- After clicking Next and attempting to activate and pair the device on the Devices -> Activate page in Corvina, Corvina will automatically proceed from the Identification Page to the Model Data Page if the connection is successful.
- If Corvina becomes stuck on the Device Activation screen (showing that the device is attempting to connect, with the option to proceed with device offline) then this is an indication that the Device is failing to connect to Corvina IOT. Follow the steps to debug.
 1. Check to make sure that the device has a connection to the internet. In the System Settings, enable NTP in the Date and Time interface. If NTP does not work then this is indicative of there being no internet connection.
 2. Check to make sure that the Corvina IOT interface in JMobile has been configured correctly.
 1. Is the interface enabled?
 2. Is the activation code entered correctly? Does it match the code entered into Corvina?
 3. Is the Corvina endpoint entered correctly?

Model and Mapping

- A model is a collection of the tags and tag properties to be used by a device.
- The same models can be used by multiple devices.
- A mapping defines the send policies (or push policies) for how and when the tag data will be sent from JMobile to Corvina.
- A mapping must be applied to a model, and a device will need to have both a model and a mapping.
- Mappings can also be reused by multiple devices if they also use the same model.

Create the Data Model

1

Back Next



- Empty
- Device
- Device (hierarchical)

After pairing the device, click the "+" icon to scan the device for its tags.

2

Create New Model

Model name
Test_Model

Tags panel

- Tag1
- Tag2
- Tag3
- Tag4
- Tag5
- Tag6



Discard model

Mappings

...ag2, Tag3, Tag4, Tag5, Tag6

Assign properties:

Labels

Unit

Select the tags to add to the model.
Properties can be assigned at this point. Click "Mappings" to proceed to set up the mapping.

Configure the Mapping and Send Policies

Select the tags to edit, then assign the send policies. Here, it can be defined whether to send the tags to Corvina on change, on interval, or on level. Enable the History policy to save the tag values in the database. Set the tags to RW to allow for them to be written from Corvina. Click "Review" to finalize the mapping.



Name
Test_Mapping

Tags panel



Tag1

Tag2

Tag3

Tag4

Tag5

Tag6

Back to model

Review

...Tag2, Tag3, Tag4, Tag5, Tag6

Assign properties:

Send policy

On change

Deadband (%)

0

%

ABS

Insert min interval(s):

1

☒ Value ☐ Quality ☐ Timestamp

Set N first changes to skip:

0

History policy: Mode:



R



RW

Exercise 1.7: Activate the Device for IoT

The goal of this exercise is activate the device for Corvina IoT and send data from JMobile to Corvina. Feel free to refer back to the previous slides (noted in the parenthesis for help).

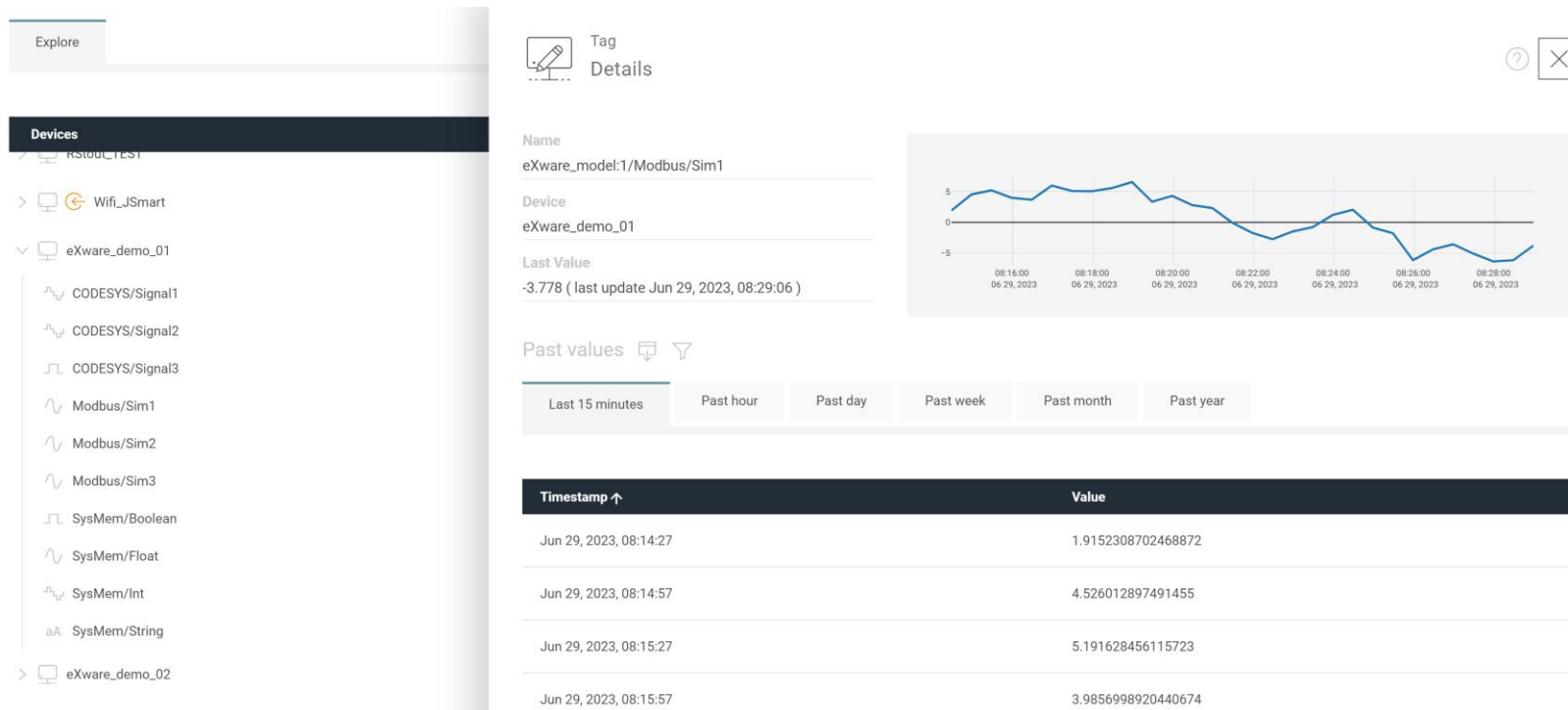
1. Create a JMobile project with a few numeric tags. Add them to a tag group called "Corvina".
2. Configure the Corvina interface in JMobile. Use a device activation code from the training folder. The folder contains a spreadsheet called "Device Activation Codes", use the code corresponding to the training kit number. (62)
3. Activate the device on Corvina. (63)
4. Add all of the tags to the model. Configure the mapping to send the data to Corvina only when the tag values change. Set the access type to RW and enable the history policy. (66, 67)

Viewing the Stored Data

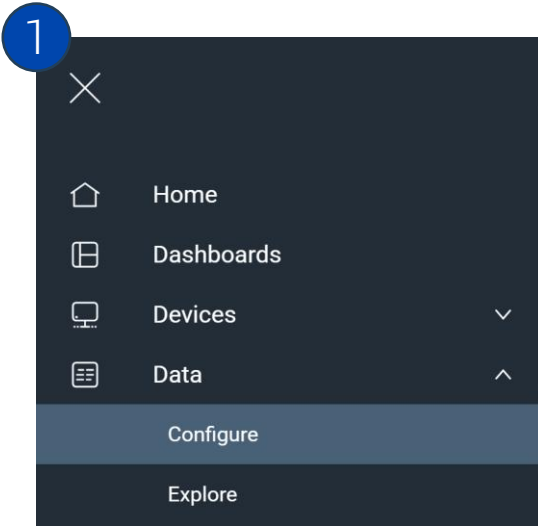
1 View the stored IOT data on the Data Explore page.

2 Click the arrow to expand a device and view its stored data.

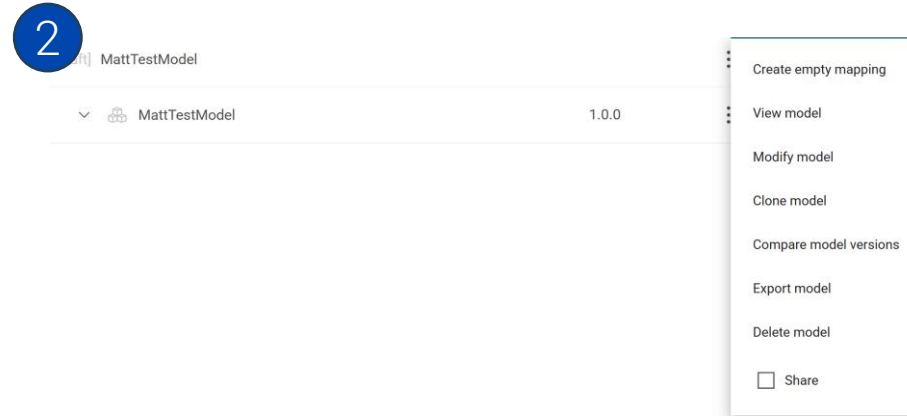
3 Browse the data over the given intervals of time or view it in the chart. The icons to the right of “Past values” can be used to export and filter the data.



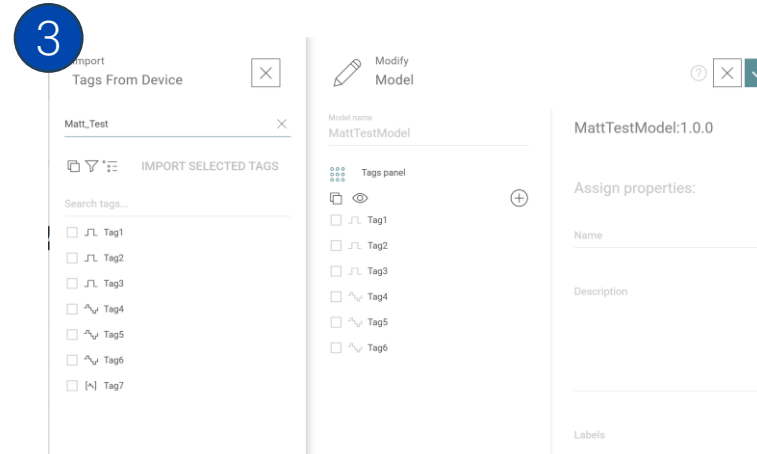
Modifying the Model



If new tags need to be added to the model, or if the model needs to be modified, it can be changed from Data -> Configure.

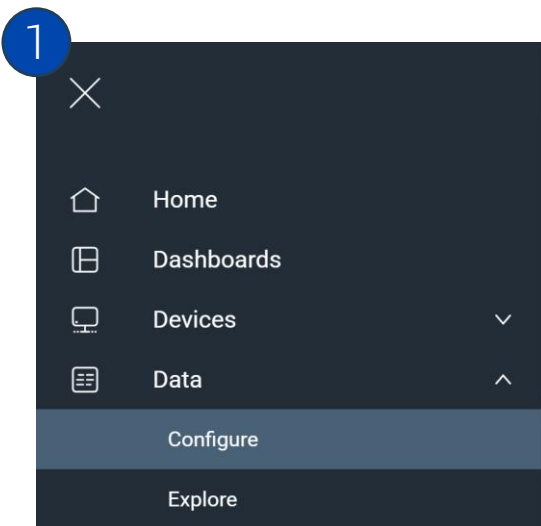


Click the icon with 3 dots corresponding to the model and select "Modify model".

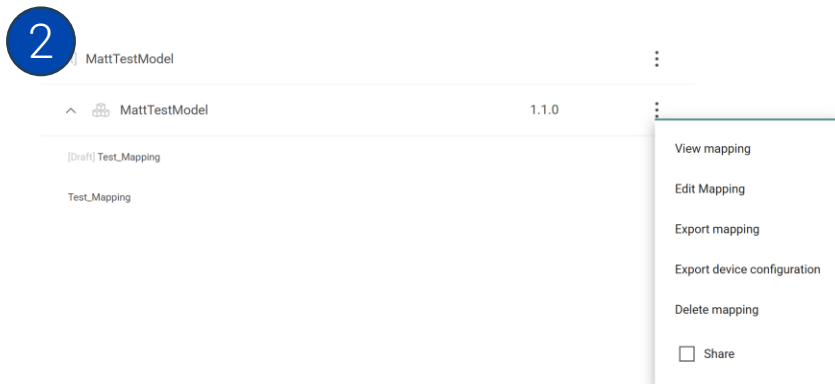


Click the "Tags panel" icon to view the tags. Then select the device to discover the updated tags. Select the tags to add to the updated model.

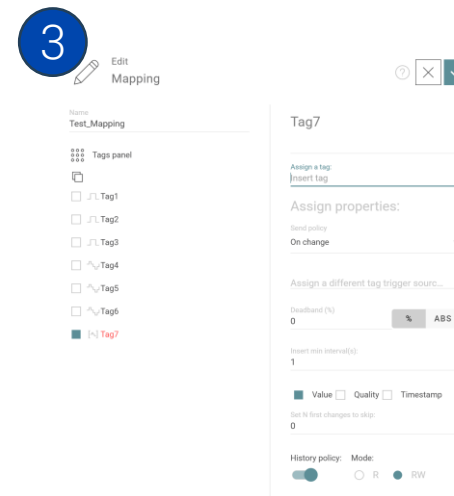
Modifying the Mapping



If new tags have been added to the model and their send policies need to be changed, or if the mapping simply needs to be modified, it can be changed from Data -> Configure.

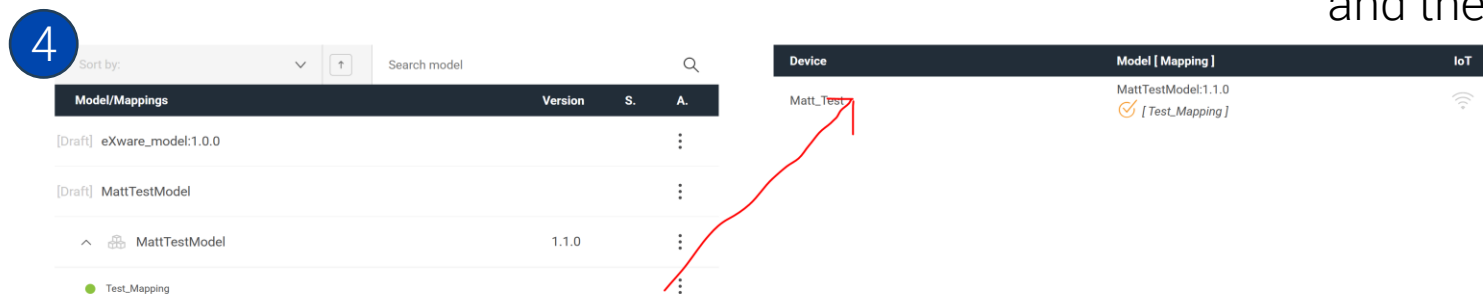


Click the icon with 3 dots corresponding to the mapping and select "Edit Mapping".



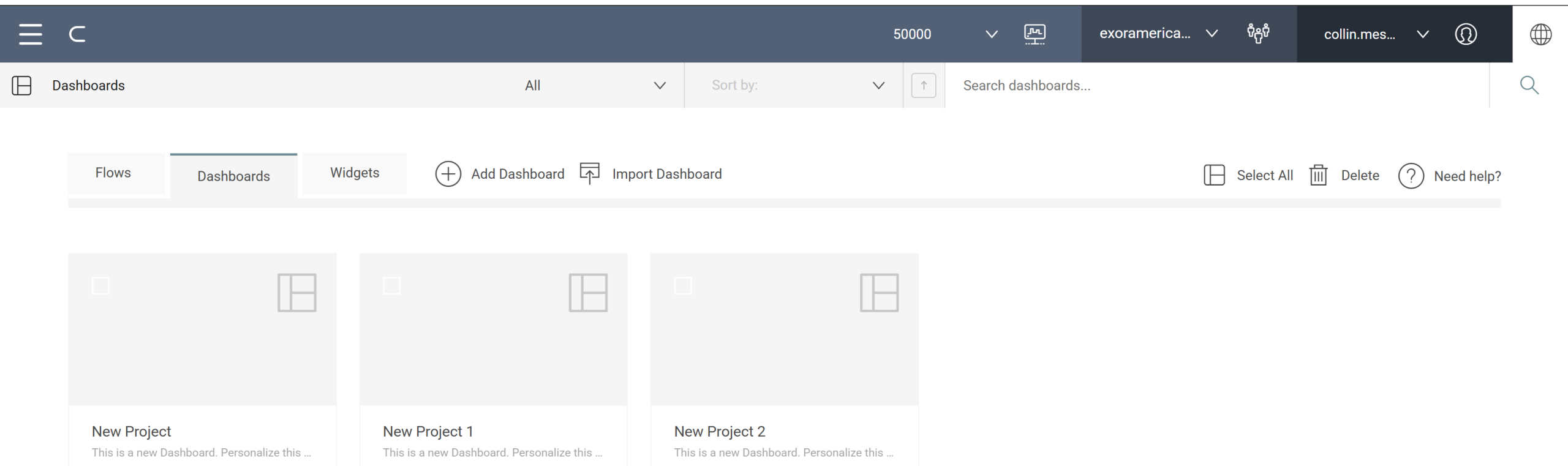
Select the tags that need to be edited and assign the new send policies.

Click and drag the updated mapping to the device to apply it and the model.



Dashboards

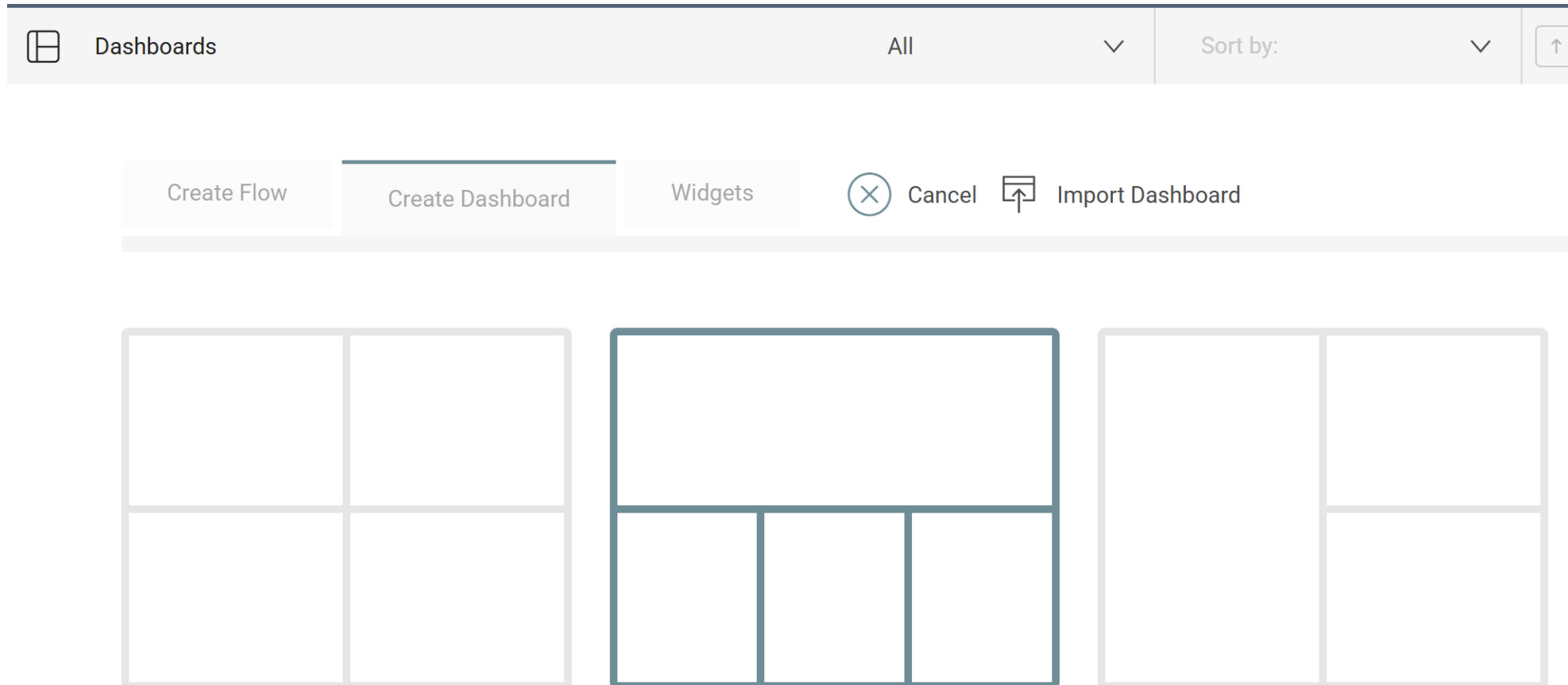
- Corvina Dashboards fetch and display data collected through the IoT service.
- Like JMobile pages, Corvina dashboards are widget-based and require no code.
- Dashboard widgets link to data model properties, meaning one dashboard can dynamically display data from any device with that model, or several devices at once.



The screenshot shows the Corvina Dashboards web application interface. At the top is a dark blue header bar with a hamburger menu icon, a 'C' logo, a value of '50000' with a dropdown arrow, a monitor icon, a user profile dropdown labeled 'exoramerica...', and another user profile dropdown labeled 'collin.mes...'. Below the header is a light gray navigation bar with a 'Dashboards' tab selected, followed by 'All' with a dropdown arrow, 'Sort by:' with a dropdown arrow, and a search bar labeled 'Search dashboards...'. Below this is a secondary navigation bar with tabs for 'Flows', 'Dashboards' (selected), and 'Widgets'. To the right of these tabs are buttons for '+ Add Dashboard' and 'Import Dashboard'. Further right are icons for 'Select All', 'Delete', and 'Need help?'. The main content area displays three dashboard cards, each with a placeholder icon and the text 'New Project', 'New Project 1', and 'New Project 2' respectively, followed by the subtitle 'This is a new Dashboard. Personalize this ...'.

Creating a Dashboard

- 1 Create a new dashboard by clicking the + icon.
- 2 Choose from a standard layout or start with a blank dashboard to build your own from scratch.



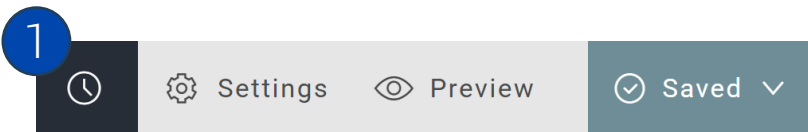
Dashboards – Edit Mode

The screenshot displays the EXOR dashboard in edit mode. The interface is divided into several key sections:

- Dashboard Name:** Located at the top left, showing "My Dashboard".
- Global Clocks:** A clock icon in the top navigation bar, circled in blue, with a label "Global Clocks" pointing to it.
- Dashboard Properties:** A settings gear icon in the top navigation bar, circled in blue, with a label "Dashboard Properties" pointing to it.
- Device/Data Sources:** A dropdown menu in the top navigation bar, circled in blue, with a label "Device/Data Sources" pointing to it.
- Version Control:** A "Saved" button with a dropdown arrow in the top right, with a label "Version Control" pointing to it.
- Widget Properties:** A "Properties" tab in the right sidebar, with a label "Widget Properties" pointing to it.
- Widget Gallery:** A "General" tab in the right sidebar, showing a grid of widget icons, with a label "Widget Gallery" pointing to it.
- Breakpoints (For Mobile Devices):** A "Breakpoints" section at the bottom right with an "ENABLE" button, with a label "Breakpoints (For Mobile Devices)" pointing to it.

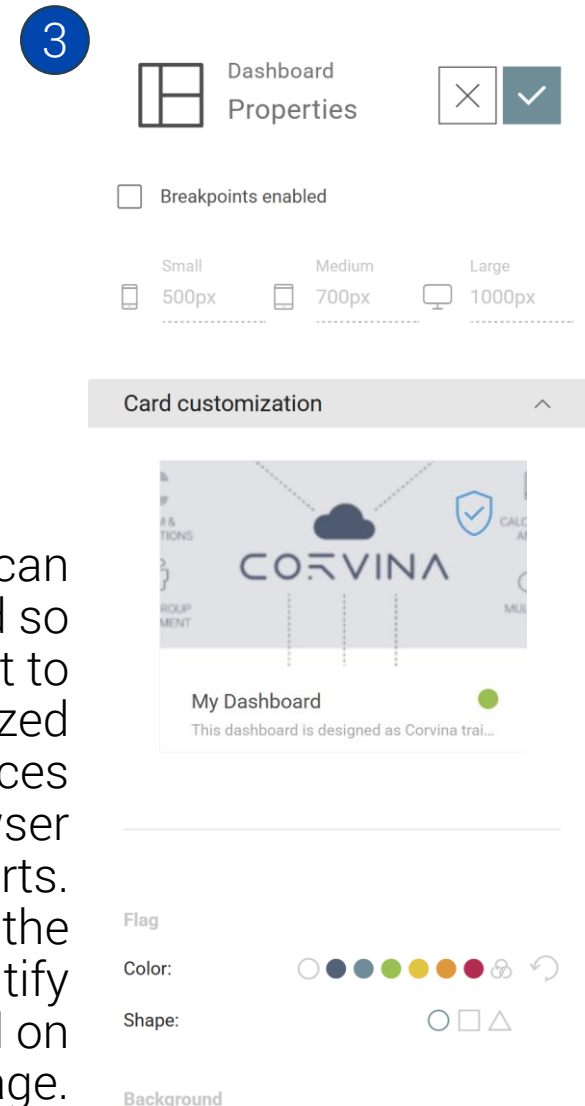
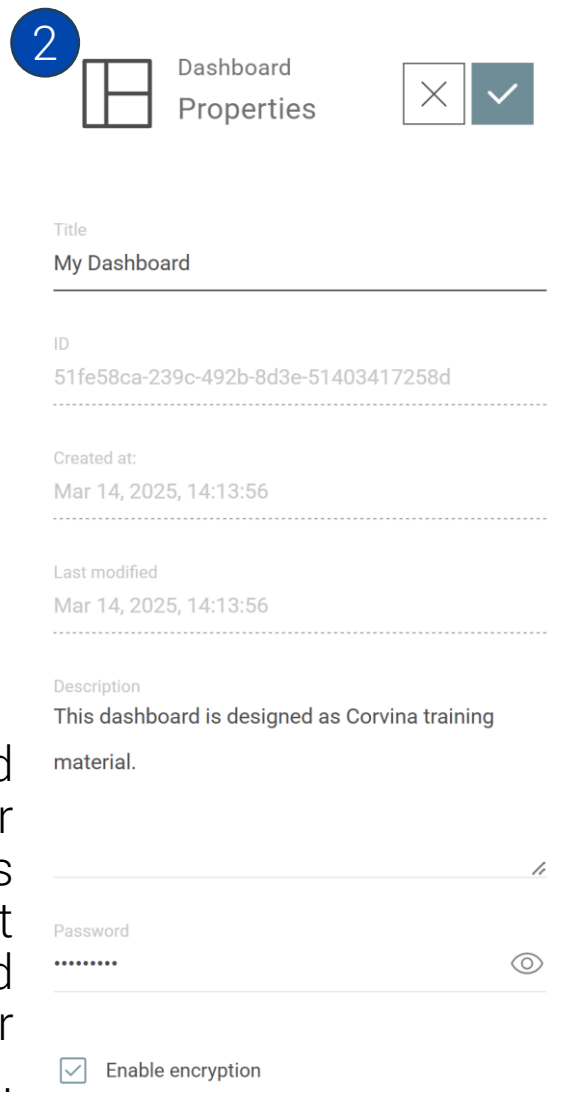
The main dashboard area contains a large card titled "Card Title" with a "Drop Here" placeholder, and three smaller cards below it, each also titled "Card Title" and containing a "Drop Here" placeholder.

Dashboard Properties



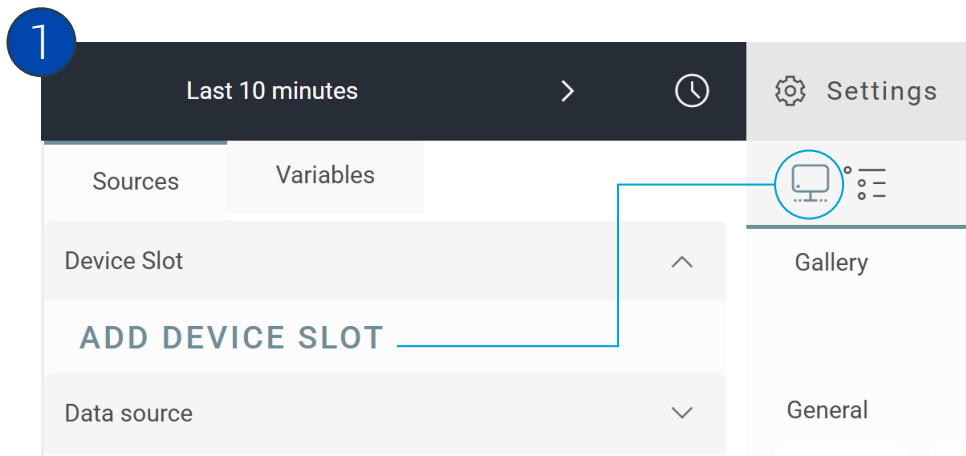
Press Settings from the toolbar to view dashboard properties.

Edit the title and description of your dashboard. It is possible to encrypt and password protect your dashboard.

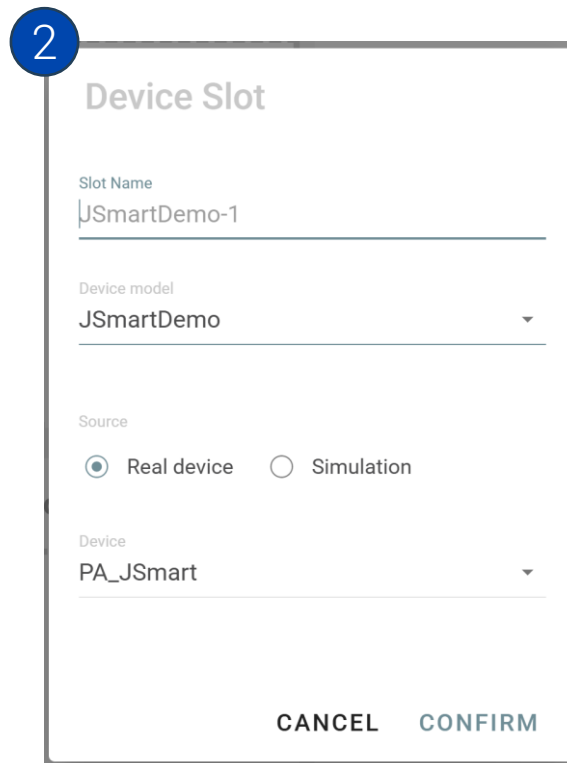


Breakpoints can be enabled so layouts adapt to differently sized browsing devices and browser viewports. Customize the card to identify this dashboard on the home page.

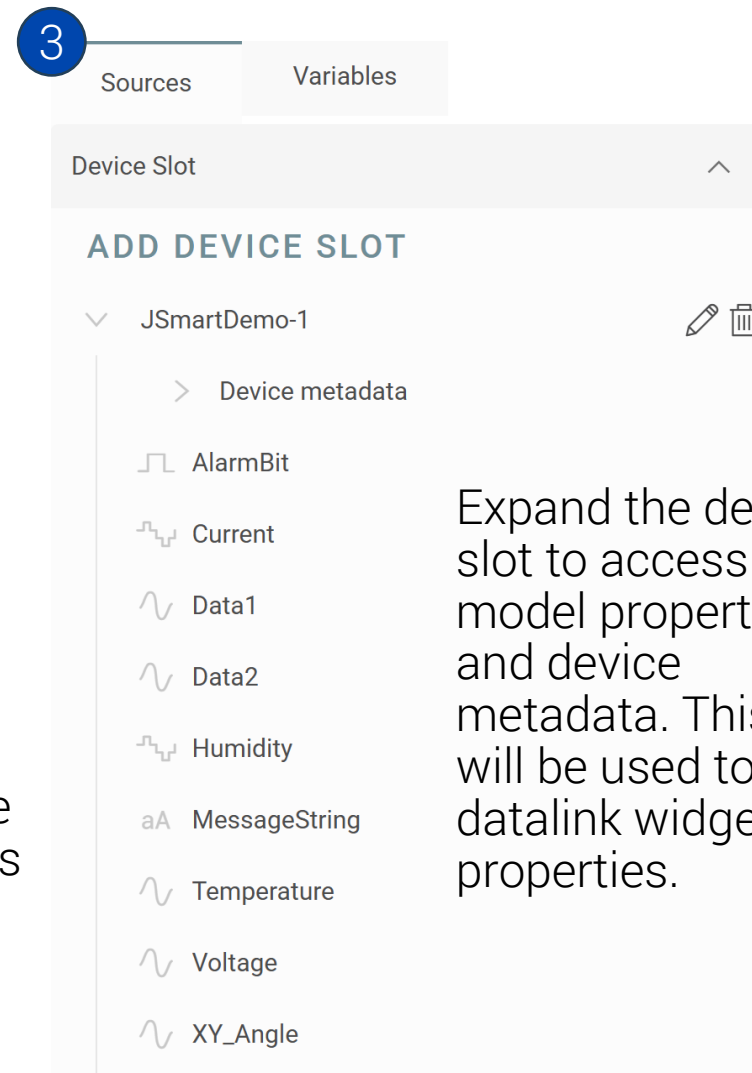
Importing Data Sources



Press the device icon to open the data source pane. Press Add Device Slot to create a link to a device.

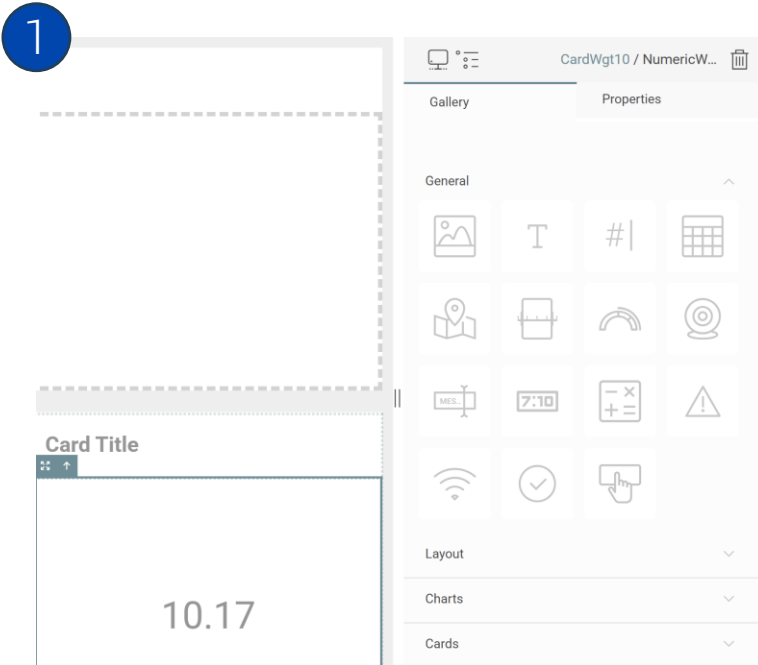


Select the device model to inherit the slot. A particular device that uses this model can be set as the default, although any device that shares the model can populate the dashboard.

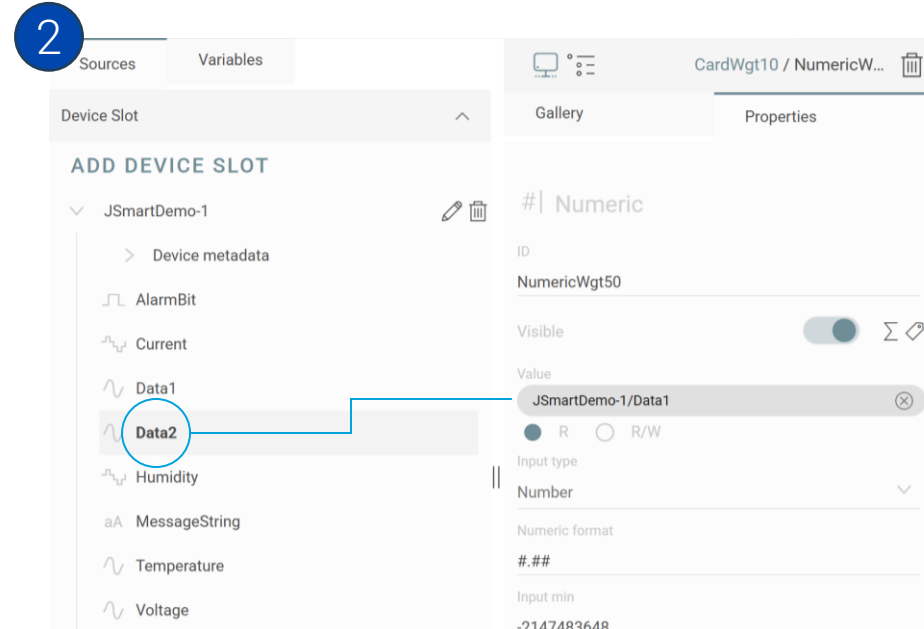


Expand the device slot to access the model properties and device metadata. This list will be used to datalink widget properties.

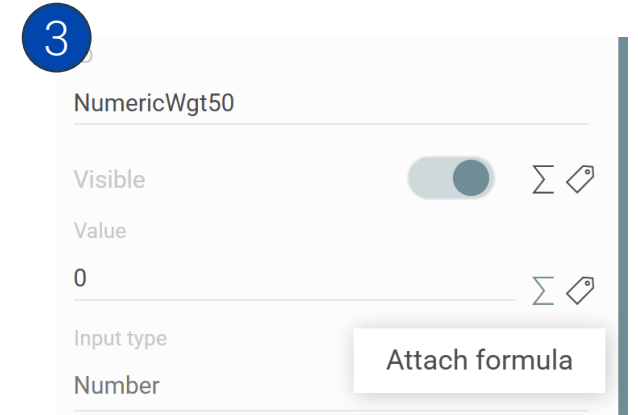
Dashboard Widgets



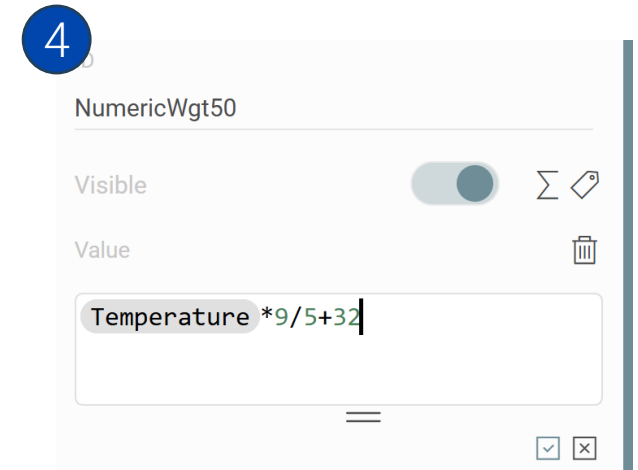
Click and drag a widget from the gallery onto an open card in your dashboard.



Select a widget to view its properties. Drag and drop a data source onto a property to create a datalink.



Press the Σ icon to create a formula instead of a direct datalink.



Enter the formula in the text box, clicking and dragging data sources in as needed. Press the check box to accept the formula.

Dashboard Widgets

1

Card Title

Drop Here

Data1

SourcesVariables

Device Slot

ADD DEVICE SLOT

JSmartDemo-1

Device metadata

AlarmBit

Current

Data1

Data2

Humidity

2

Label

Numeric

Data Table

Data time window

Pie Chart

Timeseries Chart

Discrete Chart

Pareto Chart

Bar Chart

Gauge

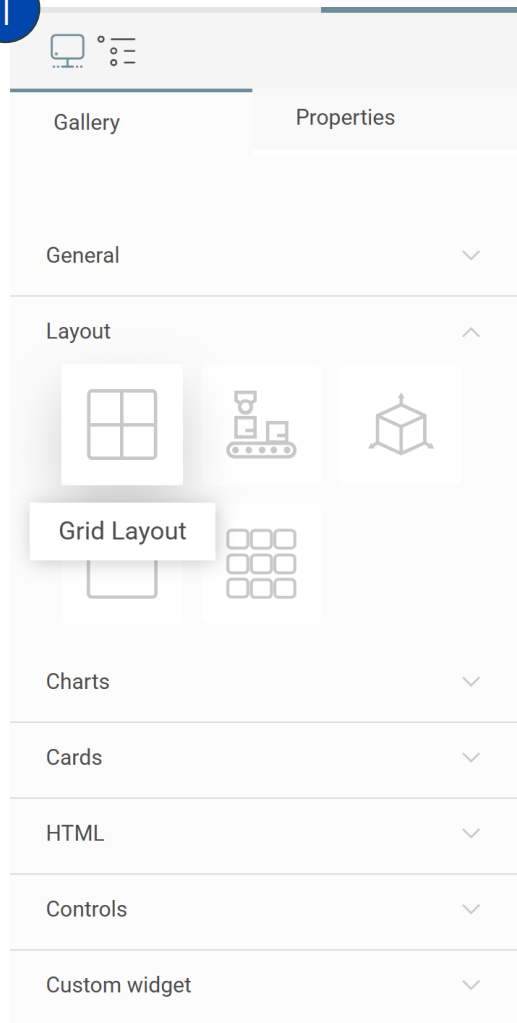
Gauge Card

Another way to add content to a dashboard is by clicking and dragging directly from a data source onto an open card.

As soon as the source is dropped on the card, Corvina will present a list of possible widgets depending on its data type. Press one to generate a widget with the data already linked.

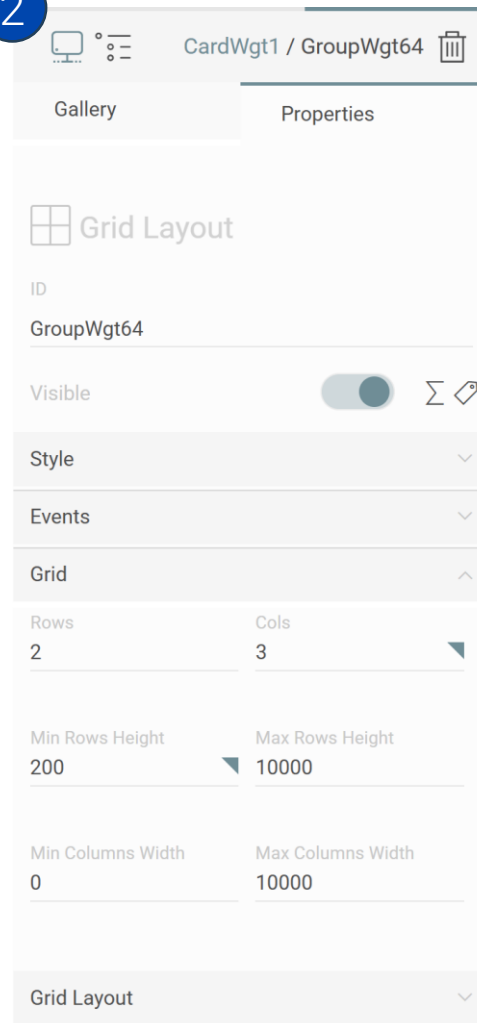
Grid Layout Widget

1



The grid layout widget can be used to arrange widgets in your dashboard and expand the content capacity of a card. It can be found in the gallery under Layout.

2



Once added to your dashboard, inspect the widget's properties to modify the grid dimensions. The Grid category also contains min and max properties for row height and column width. Scrolling automatically activates if the cells overflow.

Grid Layout Widget

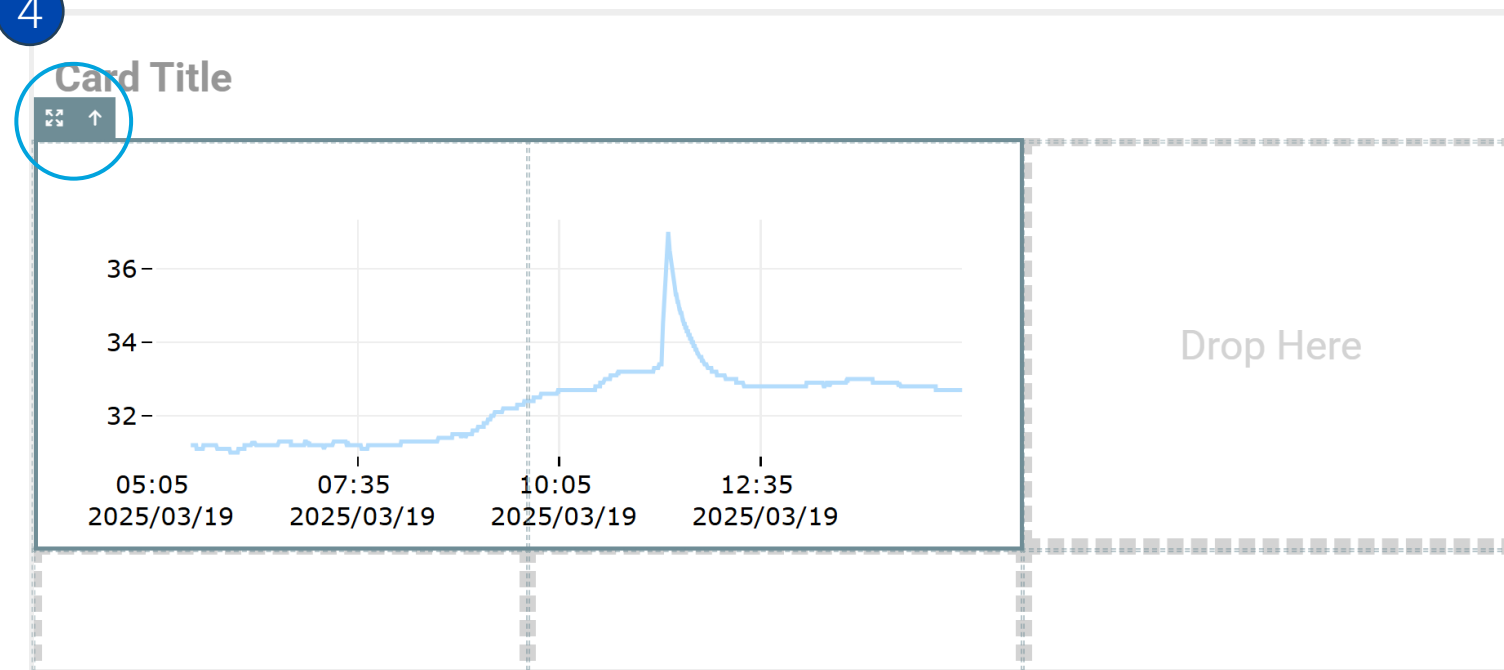
3

Grid Layout

Row Span	Col Span
1	2
Max Width	Max Height
100000	100000
Top Margin	Bottom Margin
0	0
Left Margin	Right Margin
0	0
Preserve Aspect Ratio ☐	
Vertical Align	Horizontal Align
Inherit	Inherit

Add widgets to the grid. The Grid Layout section of each widget's properties determine how it behaves with respect to the grid. Row Span and Col Span can be modified to expand the widget beyond one cell.

4



When a widget is selected, two icons appear in the top left. Press and hold the icon to pick up and move the selected widget to another available location. Click the icon to move the selection up one level in the hierarchy. In the example above, moves the selection from the chart to the grid layout.

VPN Application Widget

1

2

Click the + icon to set an application.

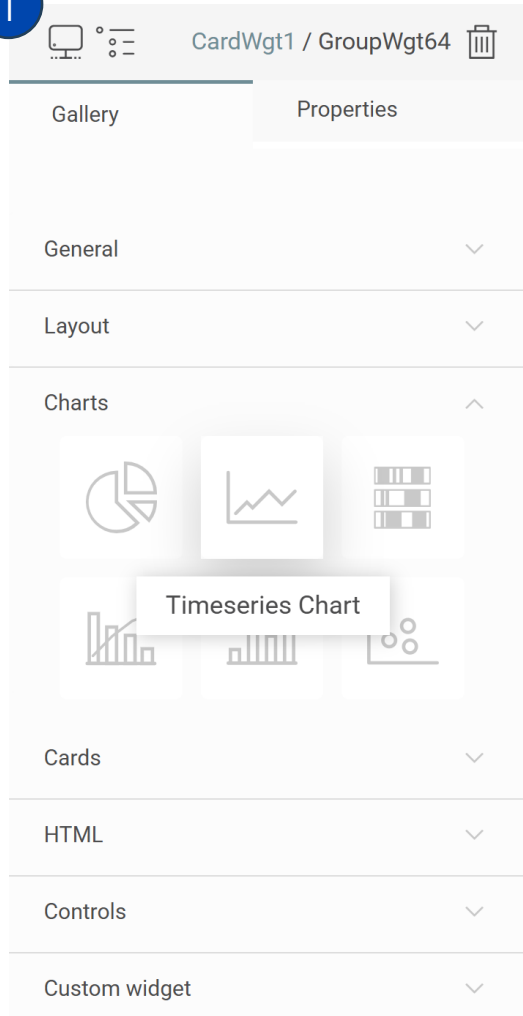
The VPN Application widget embeds an app from one of your VPN endpoints in your dashboard. It can be found in the gallery under HTML.

3

Select the device, then the endpoint, then the application to attach it to the widget.

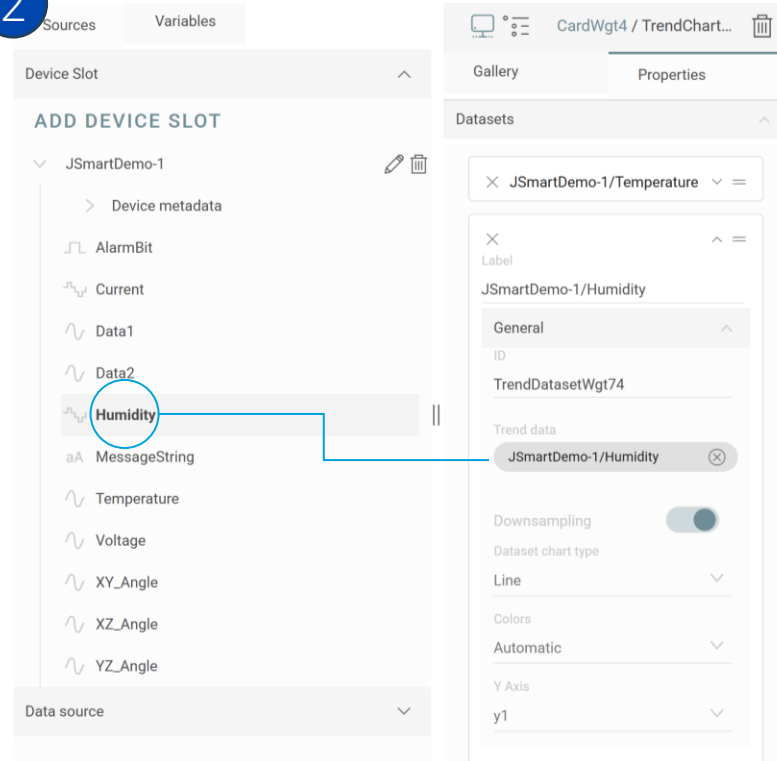
Time Series Chart Widget

1



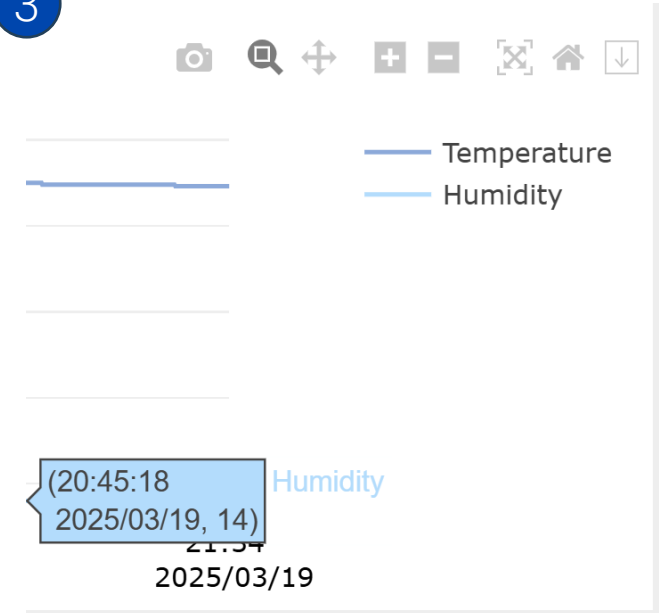
The time series chart widget is a convenient way to display data over time. It can be found in the gallery under Charts.

2



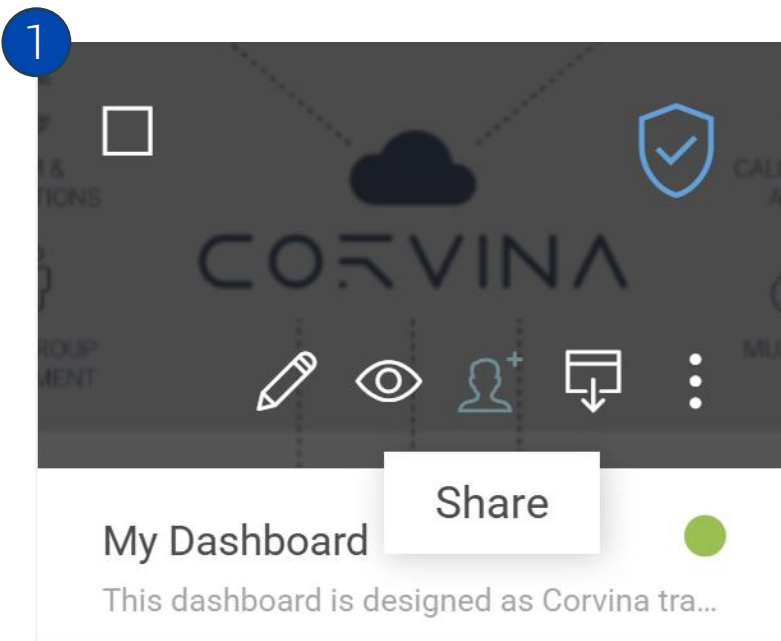
Add curves to the chart under the Datasets category. Drag and drop data sources into the Trend data property to populate each dataset/curve.

3

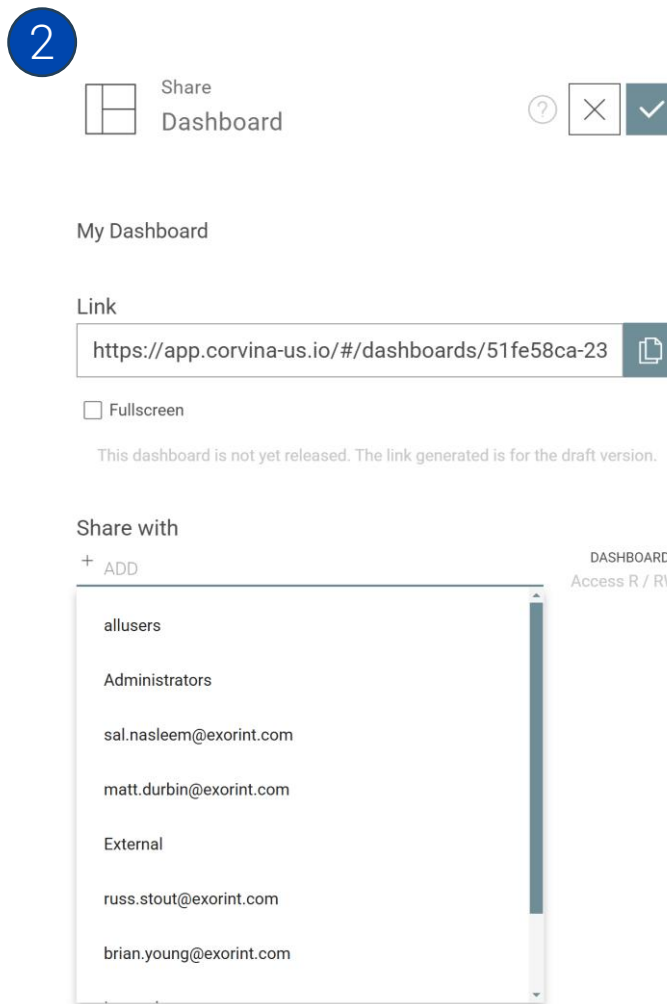


When viewed, the chart has a toolbar for easy navigation. The entries on the legend can be clicked to toggle visibility, and a built in cursor will display the value closest to the mouse location.

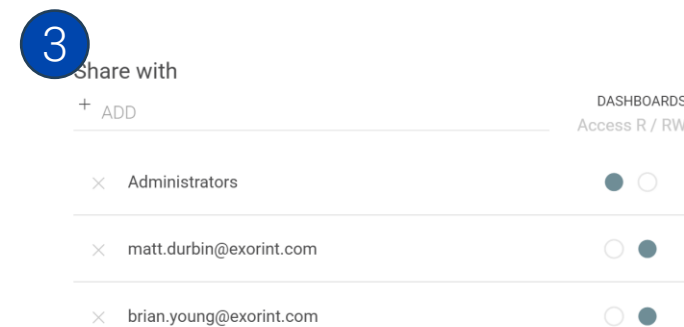
Sharing a Dashboard



From the dashboard home page, click the icon on the card to share your dashboard.

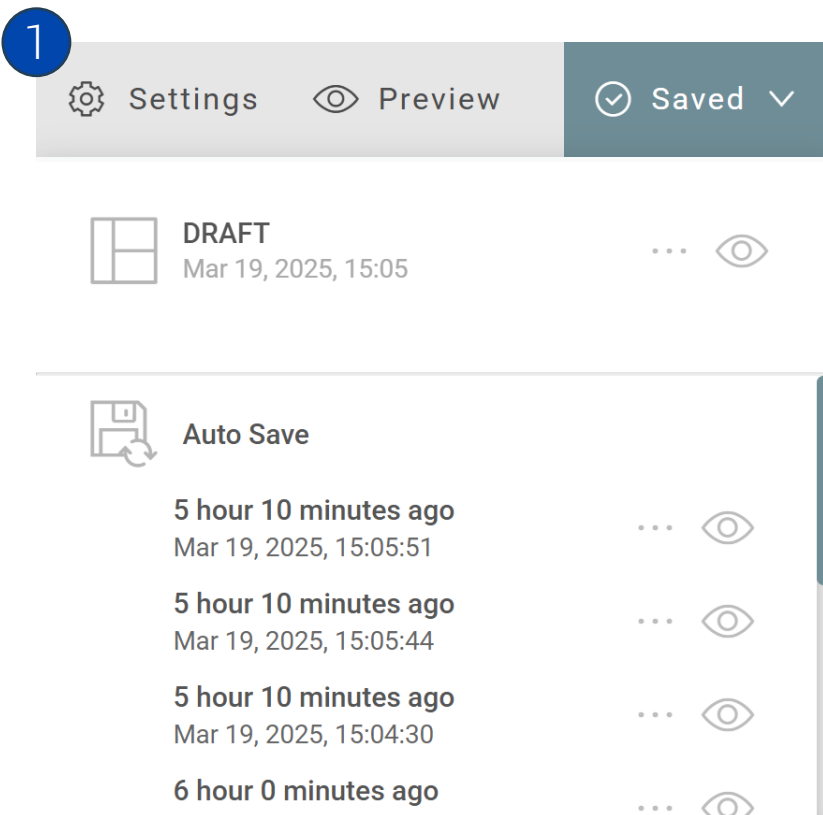


A link to the dashboard can be copied to your clipboard. Give access to Corvina users or groups by adding them in the Share with section. When you are finished, click the check to apply the new permissions.

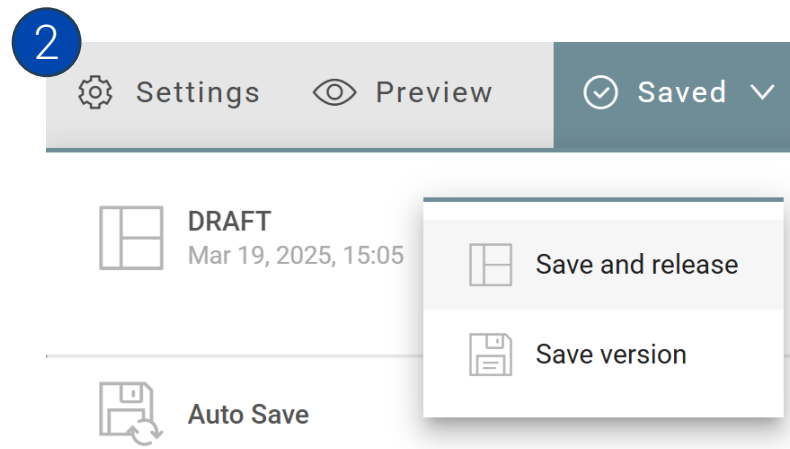


Change the access level to RW to add users as collaborators with edit permission.

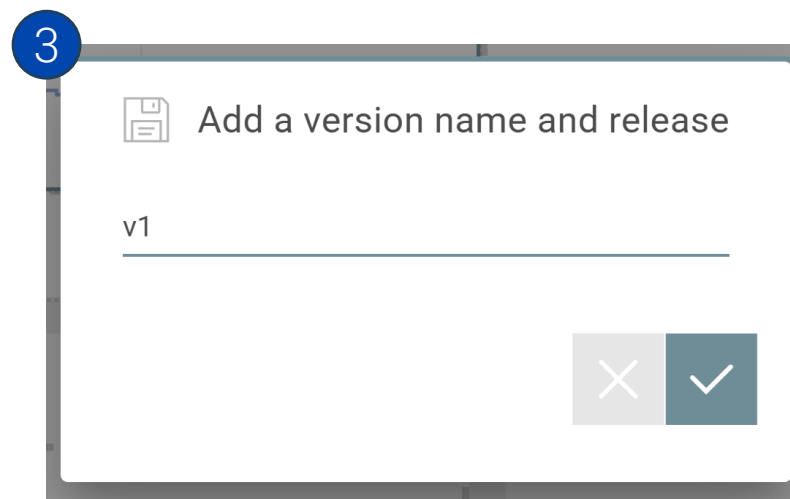
Dashboard Version Control



Click the “Saved” button in the top corner to view saved versions of the dashboard.

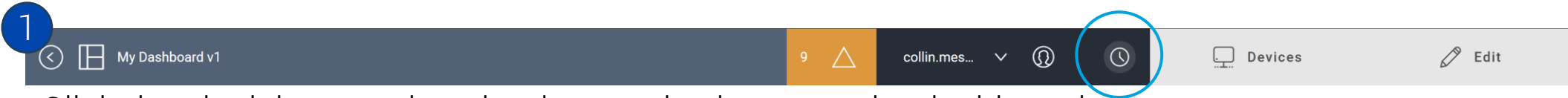


Click the three dots next to the working draft to save (and release) the current version.



Enter a name and click the check to save/release the dashboard. Each dashboard has one released version, which all users will see when they enter view mode. The most recent draft will be shown when entering edit mode.

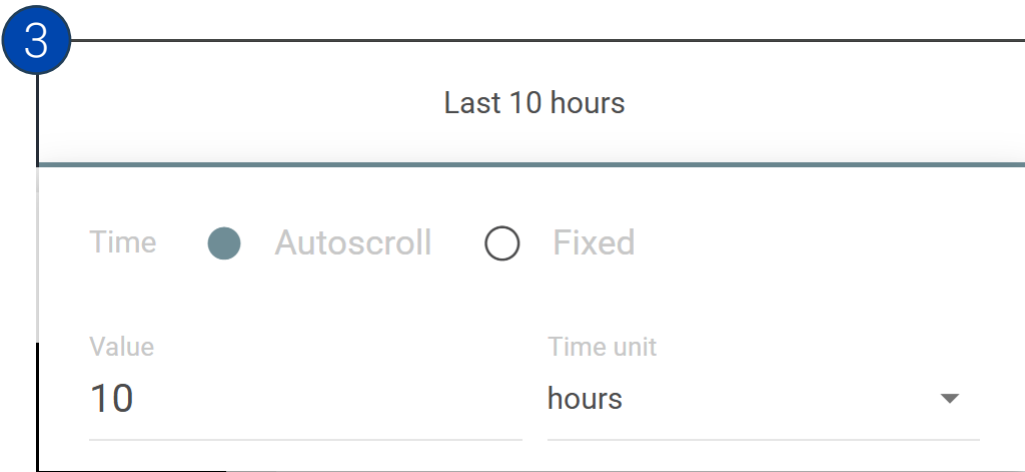
Dashboards – View Mode



Click the clock icon to view the time scale shown on the dashboard.



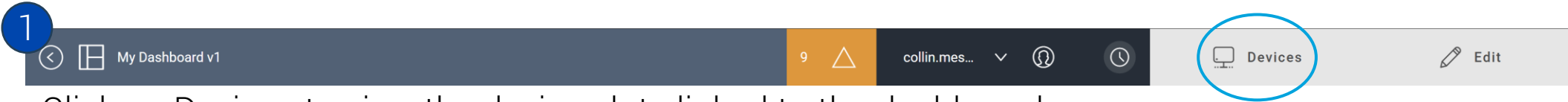
Click directly on the text shown to edit your clock(s).



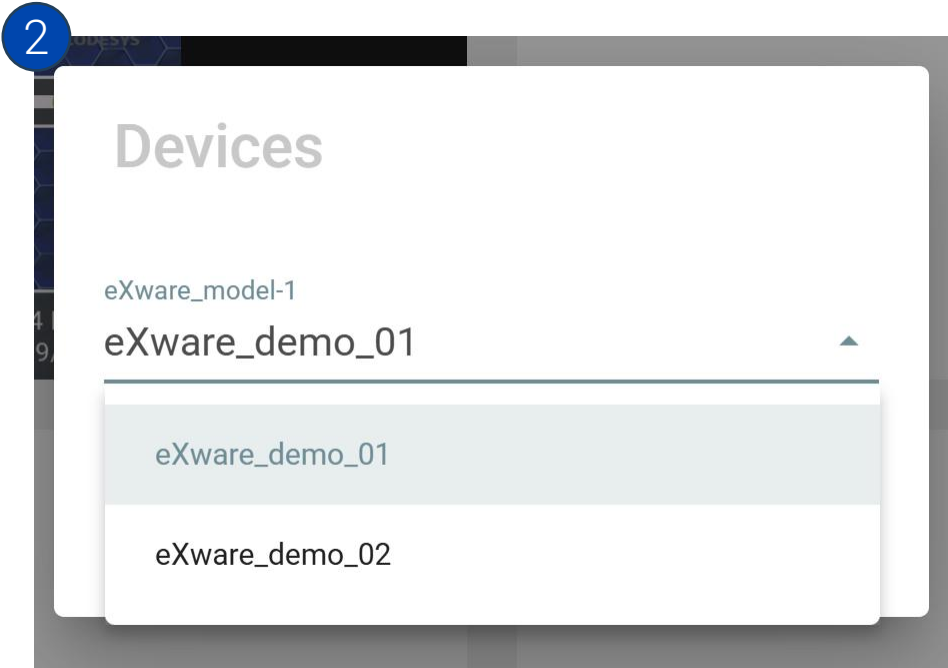
Set the time period over which to view any historized data. The global clock is used by widgets like time series charts, discrete charts, alarm tables, etc. Clocks can be set to autoscroll—fetching data from some amount of time into the past—or display a fixed period between two timestamps.

This can be done in edit mode also, which sets a default period for the dashboard whenever it is viewed in a new session.

Dashboards – View Mode



Click on Devices to view the device slots linked to the dashboard.



Click the dropdown and select a device to inhabit the slot. Click Confirm to proceed with any changes. The selected device's data will filter through the data model and display on the dashboard. This functionality allows you to add new devices and plug them into pre-existing dashboards with no edits required.

Exercise 1.8: Building a Dashboard

The goal of this exercise is to display data from an EXOR HMI on a Corvina dashboard in real time.

1. Add a dashboard and select a layout with at least 3 cards. (73)
2. Change the dashboard name to "Corvina Training". (74)
3. In one card, drop a numeric widget and link it to one of your numeric or string type properties. Change the access to R/W. Set the input type to Text if your tag is a string. (78, 76)
Optionally, place a grid layout first and add multiple numeric widgets to it. (79, 80)
4. In a second card, add a VPN application widget. Link it to [your device]/gateway/VNC. (81)
5. In a third card, insert a time series chart widget. Add two curves (datasets) to it and link them to two numeric tags from your device. (82)
tip – drag and drop data sources straight onto the chart to easily add new datasets

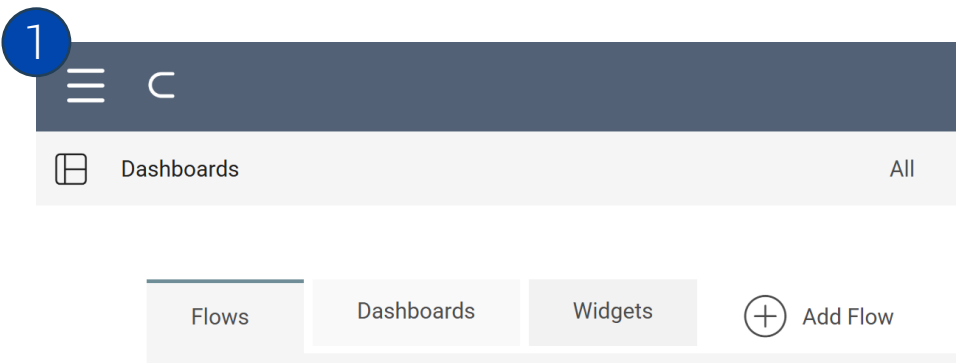
Flows

- A flow is a group of dashboards with a built-in navigation menu that allows users to move between them.
- Dashboards used in flows are still accessible individually.
- Like dashboards, flows have customizable cards and can be shared with other users.

The screenshot displays the EXOR Flows interface. At the top, a dark navigation bar contains the EXOR logo, a hamburger menu, a search bar, and user information (exoramerica... and collin.mes...). Below this, a light gray bar shows 'Dashboards' and 'Sort by:' options. The main content area features a tabbed interface with 'Flows', 'Dashboards', and 'Widgets' tabs, and an 'Add Flow' button. A 'Need help?' link is also present. The dashboard grid shows four items:

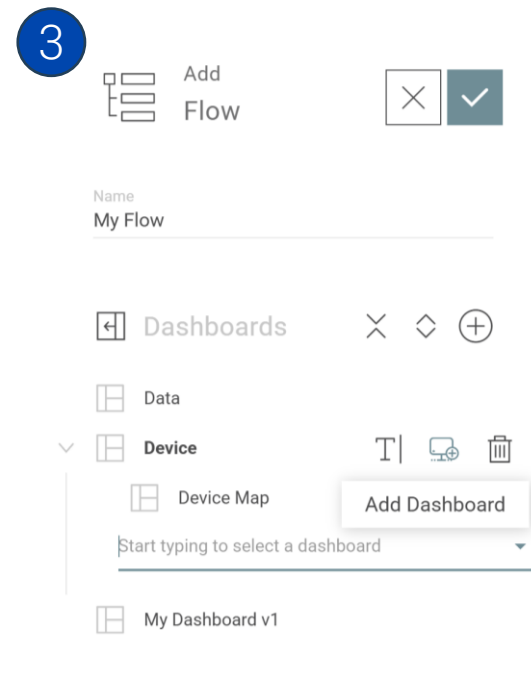
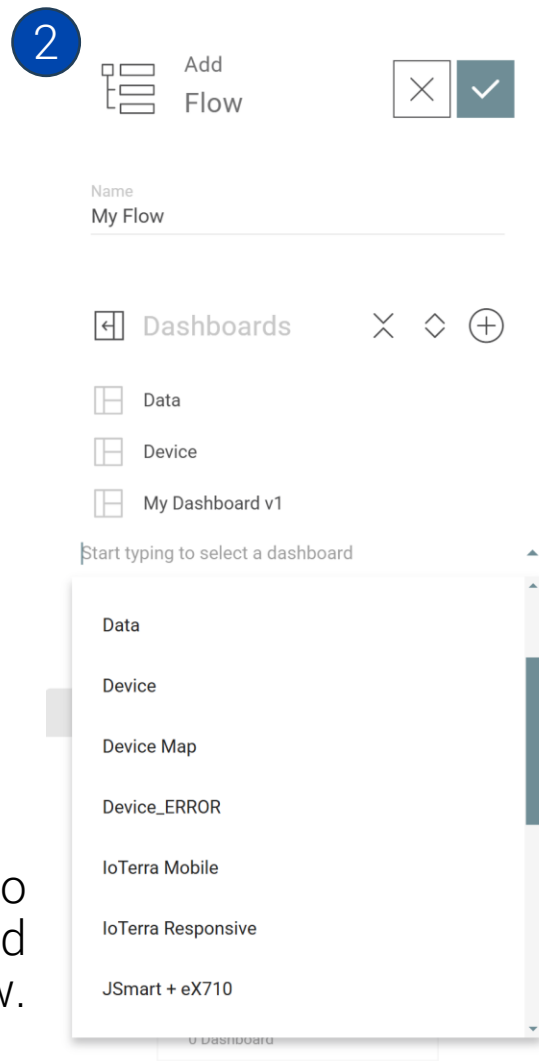
Flow Name	Icon	Count
JSmart710 x Cor...	Cloud with up arrow	2 Dashboards
Lumon Industrial	Water drop	3 Dashboards
XR Steel	Factory building	1 Dashboard
OEM-1 Machines Pla...	Tractor	2 Dashboards

Creating a Flow



Navigate to the Flows tab and click “+ Add Flow” to create a new flow.

Click the + icon next to “Dashboards” to add dashboards to your flow.



Once added select a dashboard to change its name or add more dashboards beneath it, creating a hierarchy of pages. When the flow is viewed, this list will become the navigation menu.

Application Store

Accessing the Store (91)

Installing an Application (93)



Application Store

- The store can be enabled for an organization to allow it to install and use additional applications in Corvina.
- Once enabled, it can be accessed from the menu.
- This interface allows for applications to be installed on the organization, once installed they will appear in the menu.

Accessing the Store

1

Add Organization

Label
test8

Name
test8

Has hostname ☐

Allow full privacy ☐

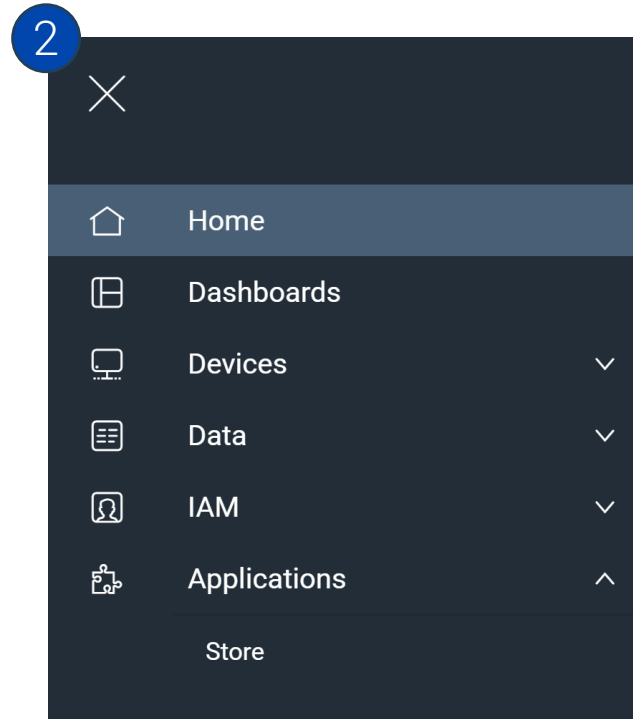
IoT Enabled ☒

VPN Enabled ☒

Lives on own resources ☒

Store Enabled ☒

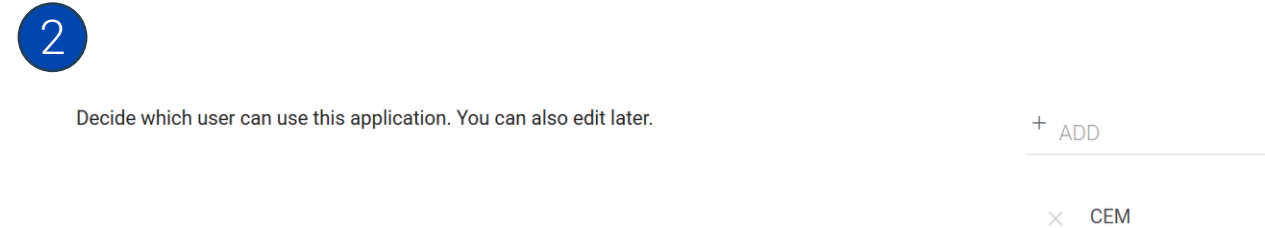
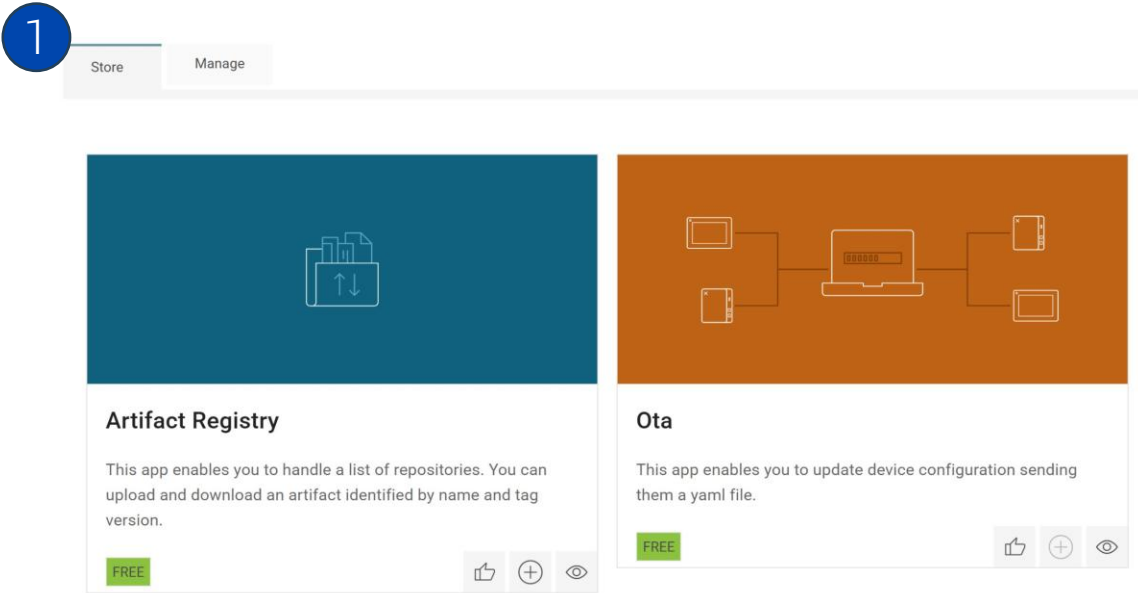
Create an organization with store enabled or edit an organization to enable the store.



Open the menu and expand Applications to show the store. Click "Store" to open it.

If any other applications have been installed, they will appear on this list beneath "Applications".

Installing an Application



Give permission to the application to run and assign users or user groups to have access.

In the "Store" tab, click the plus icon corresponding to an application to install it.

Corvina Edge Management: OTA

Devices (96)

Modules (98)

Recipes (99)

Campaigns (100)



Corvina OTA

- Corvina OTA (over the air) will allow for software updates to be deployed to many devices at once, on a schedule.
- The OTA agent must be installed on any devices that will be used with OTA.
- Modules – files that can be uploaded to the Artifact Registry.
- Recipes – collections of modules that are to be deployed .
- Campaign – a scheduled deployment of a recipe to a given set of devices.

- In order to use Corvina OTA with a device, a service account must be created to grant access.
- Devices that will be used with Corvina OTA must also already be activated on Corvina VPN.

Create a Service Account to Enable use of OTA

1

Email	Groups	Application Roles	Device Roles
admin@exor.com	Administrators	Administrator	Device data Administrator
fabio.fiorio@corvina.io	Administrators	Administrator	Device data Administrator
matt.durbin@exorint.com	Administrators	Administrator	Device data Administrator
didier.sos@exorint.com	Administrators	Administrator	Device data Administrator

Add a service account by navigating to IAM -> Users and clicking the icon shown to create a service account.

2

Modify User

Device roles

ADD

Administrator

Apps

ADD

corvina-app-artifact-registry

corvina-app-ota

Associated devices

ADD

Matt-eX707M

Collin-eX707M

Add the OTA and Artifact Registry applications. Add the devices or device groups that will be used with the OTA.

Install the OTA Agent

1

Devices	Modules	Recipes	Campaigns							
										Need help?
☐	Device name	Agent	HW	SN	Modules		S	D	L	
☐	MEdge-CM	1.0.27	UN96	AA0001C83001564770AA	jmproject	appBootSequence				

From the OTA -> Devices tab, click the download button to download the OTA Agent. Use "Exor armv7" for 32 bit HMIs such as eX700 and JSmart700. Use "Exor arm64" for 64 bit HMIs such as eX700M, JSmart700M, and eX200.

2

Install the OTA Agent as an application in the HMI system settings. Once complete, the device should appear in the list as shown above.

Upload a Module

1

Devices

Modules

Recipes

Campaigns

NEW MODULE

Need help?

	Module	Type	Author	Version	A
	ota-test-jmproject	HMI project	collin.messics@exorint.com	1.0	

From the OTA -> Modules tab, click "New Module".

2

Upload New Module

Name

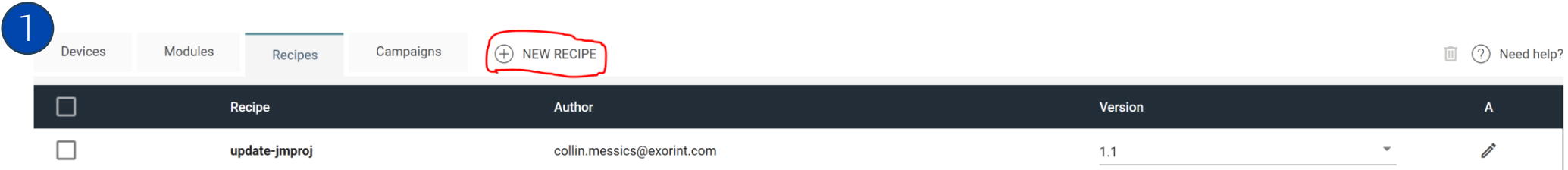
Version

File

Type

Assign the module a name and version number. Upload the file and select the correct file type.

Add a Recipe



From the OTA -> Recipes tab, click "New Recipe".

- 2
- Assign a name and a version number.
 - Select the modules to add to the recipe.
 - Select the desired confirmation options.

Import Module

Select

Search for modules

ota-test-jmproject (1.0)

New Recipe

Name

Recipe name must be at least 4 characters long

Version

Modules

OTA Agent:latest

Confirmation

Required

Discardable

Postpone

1

Day

Create a Campaign

1

Devices Modules Recipes Campaigns **+ NEW CAMPAIGN** Scheduler view Show only in progress ? Need help?

Name	State	Start At	Progress	A
test-campaign-jmproj-only	✓	Mar 20, 2025, 14:58:38	COMPLETED	

From the OTA -> Campaigns tab, click "New Campaign".

2

Create Campaign

Name

Recipe

No devices selected SELECT DEVICES

Assign a name and a recipe to the campaign. Select the devices to deploy it to.

3

Progress A

READY

Click the start icon to prepare to launch a campaign. Use the prompt to either deploy it immediately or on a schedule.

Exercise 1.9: Execute a Campaign with OTA

The goal of this exercise is to deploy an update to the JMobile project via Corvina OTA. The Artifact Registry and OTA applications as well as the service account are already added to the organization (93, 96).

1. Download the OTA Agent from Corvina and install it on the HMI. (97)
2. Create a JMobile project and save it as an update package. Upload the update package to Corvina as a module. (98)
3. Create a recipe containing the JMobile project module. (99)
4. Create a campaign to deploy the recipe to your device. (100)

Other Applications

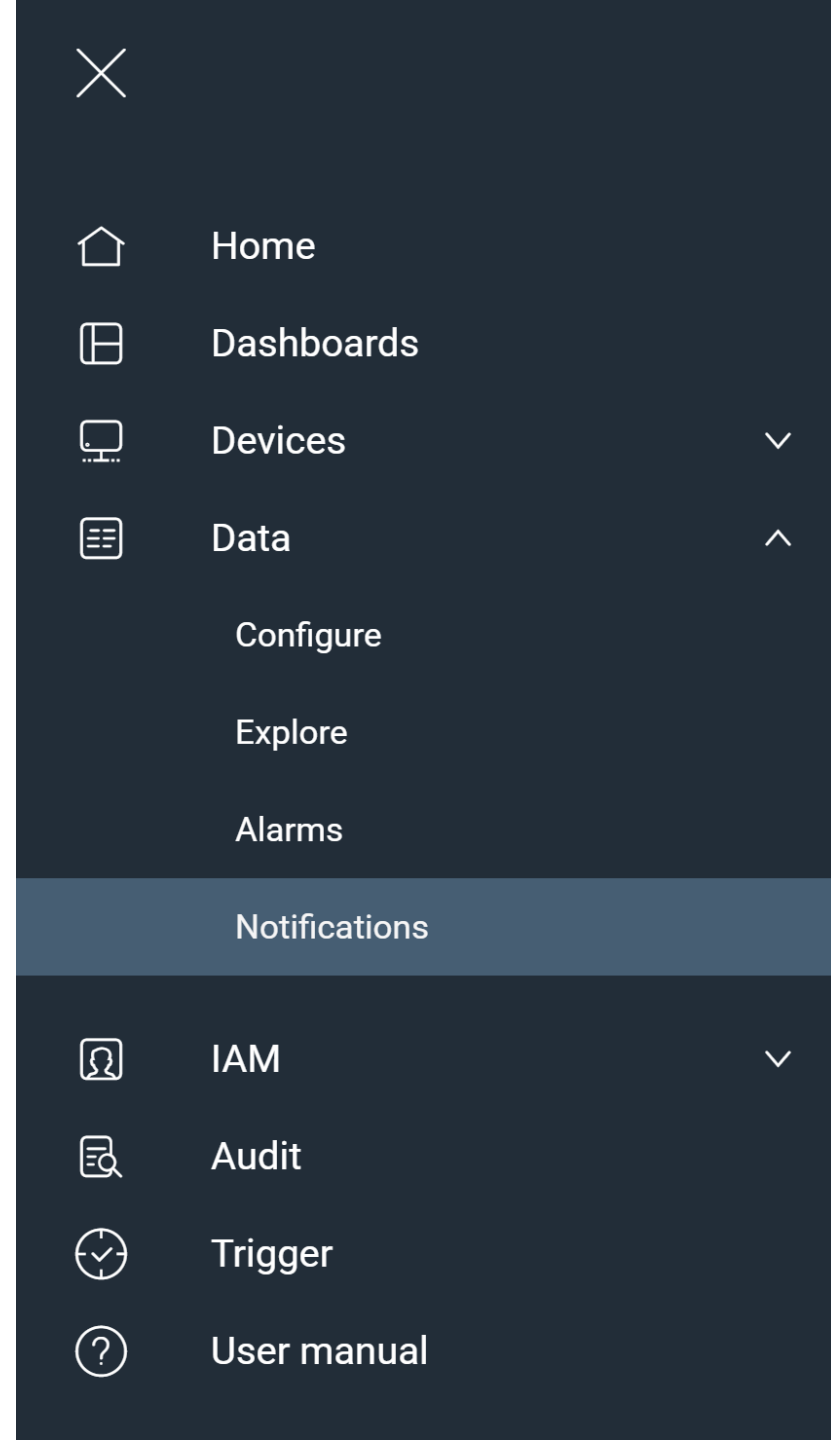
Notifications (103)

Triggers (107)



Notifications

- Notifications send email alerts when a Corvina alarm is triggered.
- These emails are sent by the Corvina platform—not the device—meaning they do not require machine owners to setup and manage their own email server architecture.
- Notifications can be easily edited through Corvina without any modification on the device side, making outgoing messaging adaptive.
- Notifications are a simple yet powerful tool that offer immediate benefits from the moment an IoT-enabled device is activated on Corvina.



Notifications

1 Add a new notification by clicking the + icon. Enter a name and optional description for this notification.

2 Check the enable box to turn the notification on. Select an Ack buffer and active time period to filter based on time.

+

Create Notification

?

×

✓

Name

Demo Notification 1

Description

Send email to Corvina trainees

Properties

Enabled

☒

Wait for ACK

Send immediately

▼

Active time period

Mon

Tue

Wed

Thu

Fri

Sat

Sun

☒
☒
☒
☒
☒
☐
☐

Recipients

Add Users

@

Type email and press enter

Add User Groups

Subject ?

Corvina Alarm Triggered

Body ?

Alarm from {{deviceLabel}} has been detect

3 From the right column, recipients can easily be added and removed. Notifications can be sent to Corvina users, entire user groups, or any generic email address.

4 Edit the subject and body of the email to be sent. Wildcards can be used to embed device and alarm information within the text. Type {{ to see a list of available wildcards.

Notifications

- 5 Scroll down and set device and alarm filters. Only alarms fitting these criteria will send the notification. *Severity* selects only alarms of that severity or higher. *Alarm name* allows you to specify specific alarms that trigger the notification. *Device groups* will select only alarms from the selected devices or groups. *Extra filters* are available to add more criteria for sending the notification.

Severity

Low ▼

Alarm name (OR)

Type alarm name and press enter



Extra filters (AND)

Select type ▼

Type value and press enter



Device groups

Add Device Group

TestDevice ×

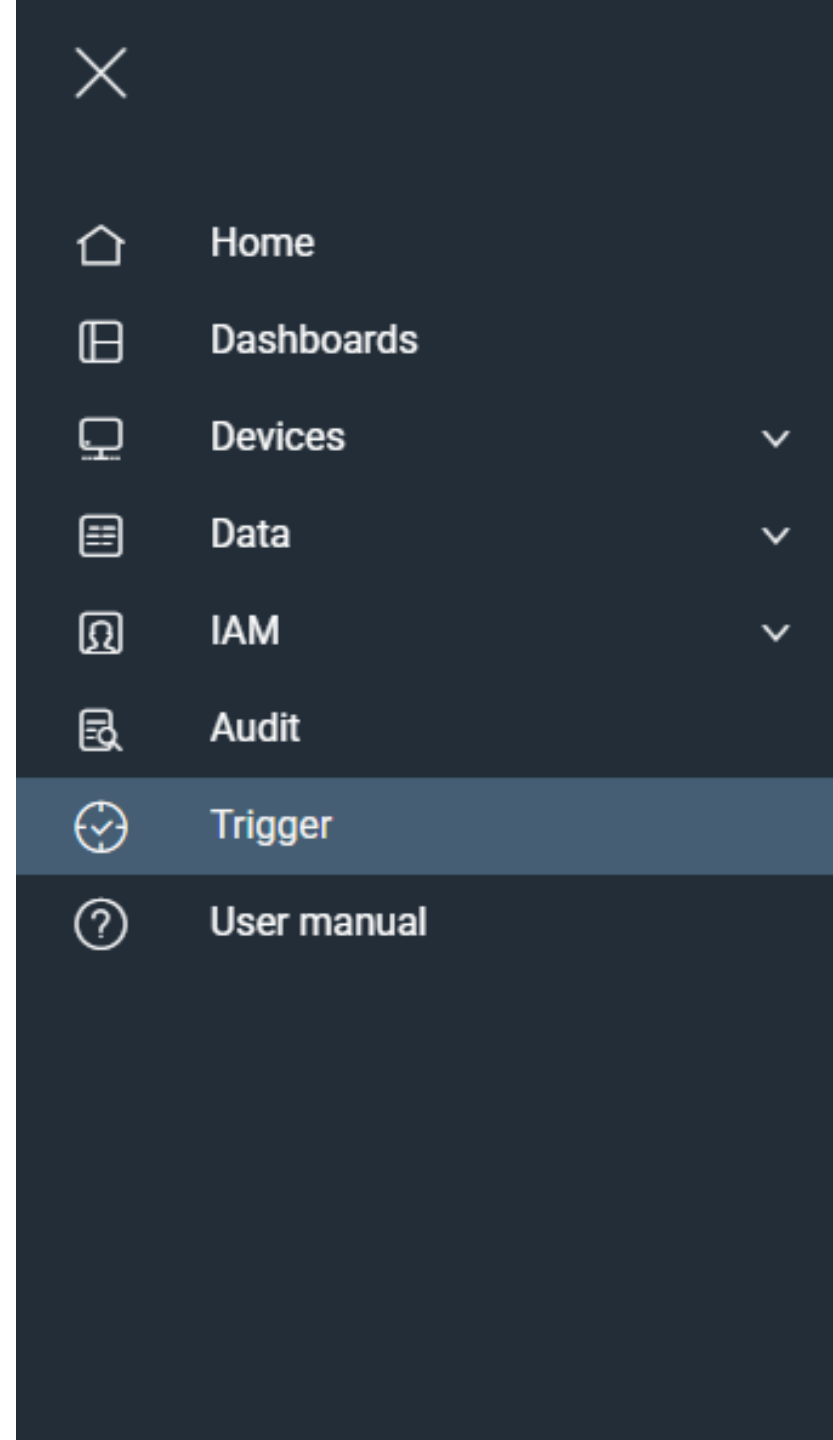
JSmarts ×

eXwares ×

Be sure to press Enter when entering new criteria. This will move your input from the entry field to its own box. Otherwise, the entry will not be saved.

Triggers

- Triggers respond to Corvina events by performing one or more actions.
- The conditions for a trigger are called “policies”. They include events like a tag’s value changing or a device losing its VPN connection to Corvina.
- Like notifications, triggers can send emails to specified users.
- Triggers can interface with third party services like Webhook, Telegram, and Microsoft Teams to execute commands and exchange information with other software’s APIs.



Triggers

1 Add a new trigger by clicking the + icon. Name the trigger and select the devices or device groups that the trigger will be applied to.

2 Add policies to determine when the trigger occurs. Multiple policies can be added, using either AND or OR logic to handle the various conditions.

Create Trigger

?

✕

✓

Name

Demo Trigger 1

Device groups

Add device group

TestDevice ✕

Policy

✕

◇

▼ And

Analog Band

Connection

Analog Band - Configure

?

🗑️

Model Path Matcher Mode

☒ Simple
 ☐ Advanced

Model

eXware_model:1.0.0

▼

Tag

CODESYS/Signal1

▼

Match interval

☒ Inside
 ☐ Outside

Min

20

Max

30

Interval policy validation [s]

0

Action

+

Add action

Triggers

3 Add the actions that Corvina will take when the policy conditions are met. Multiple actions can be added to the list and their order can be modified by clicking and dragging.

4 Configure each action individually. The example shown uses Webhooks to post to x.com (twitter API).

Policy

✕ ◇

▼ And

Analog Band

Connection

Action

⊕ Add action

≡	🔗	Teams Action	🗑
≡	🔗	Webhook Action	🗑
≡	🔗	Email Action	🗑

Webhook Action - Configure

🗑

Method

POST

▼

URL

https://api.twitter.com/2/tweets

Headers

Key	Value	↔
Authorization :	dfiSrt4Hrve2xcij	>
Content-Type :	application/json	>

Body ?

```
{
  "text": "tweeted by Corvina"
}
```

Exercise 1.10: Sending an Email Notification

The goal of this exercise is to send yourself an email when a JMobile alarm is triggered.

1. Create a new Corvina notification and add yourself as a recipient. (104)
2. Set the severity filter to high so only critical alarms are included. (105)
3. Select only your HMI in the device groups filter. (105)
4. Edit the subject and body of your email. Include at least the {{alarmName}} and {{deviceLabel}} wildcards in the email body to identify the source of the alarm. (105)
5. Test the notification by triggering a high severity alarm on your device. You should receive an email within 1-2 minutes.