

# **Ignition 8.3 User Manual — Welcome, Getting Started and Other Editions**

Generated 2026-10-12 from  
<https://www.docs.inductiveautomation.com/docs/8.3/>

# Welcome



## About this Manual

This Welcome section provides a **broad overview** and information relating to **modules**, **architectures**, **installation**, and an **Upgrade Guide**. The sidebar on the left is a table of contents organized so you can navigate easily and quickly through Ignition's features, modules, functions, and so forth.

In the **Appendix** you'll find an exhaustive list of all the **Components**, **Expressions**, and **Scripting Functions** in Ignition.

Take a look at the navigation section on the left and poke around.

## Ignition 8.3

This User Manual is specifically for Ignition 8.3. Other major versions of the software have separate User Manuals. The manual version you are viewing can be adjusted by selecting a different version in the top navigation bar version dropdown.

## Security Portal

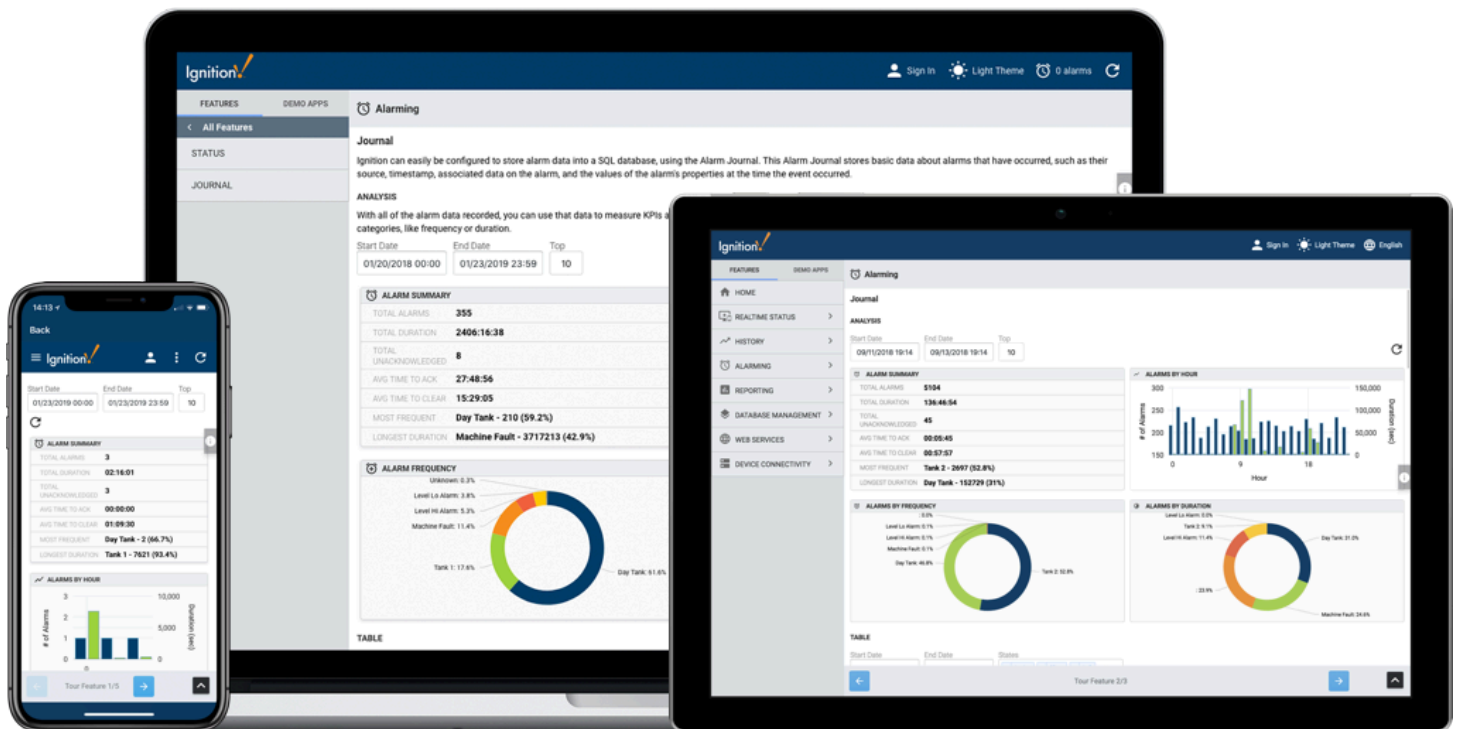
Stay up-to-date on all Ignition security news by subscribing to our **Trust Center** updates.

## Vulnerability Reporting

If you'd like to report a vulnerability, let us know through our **security@inductiveautomation.com** address. Additionally, Inductive Automation provides a **public PGP key** if encrypted communication is needed.

# Inductive University

**Inductive University** is a free online learning platform designed to help you master Ignition. You can watch hundreds of training videos and participate in our credential program to test your knowledge. It's the first step to joining our ranks of Certified Integrators.



## Ignition Basics

Learn what Ignition is, the basics of what it can do, and how it can work for you.

### Introducing Ignition

## Startup Guide

New to Ignition? Get Ignition running on your computer in minutes with our Startup Guide. Download Ignition and evaluate the full version right away.

### Startup Guide

## Installing and Upgrading

You can install Ignition in under 3 minutes; staying current is just as easy. No hassles, no secret handshakes, only one lightweight install and you can have clients running everywhere.

# System Architectures

Ignition can support many different types of architectures from single standalone systems to vast enterprise level structures. Learn about the types of architectures and how they work.

## System Architectures

# New in this Version

Are you looking for something that has changed? Or maybe you want to see the things we have been adding to Ignition? Check out the New in this Version page for a list of improvements for each version.

## New in this Version

# Partner Programs

Inductive Automation is proud to have a Partner Program that allows others to create modules to enhance Ignition's functionality. You can learn more about [Sepasoft's MES modules](#) and [Cirrus Link's MQTT modules](#) here.

# SDK Documentation

Documentation for the [Ignition Module SDK](#). Anyone looking to create a new module should start here.

### ! INFO

Custom module development is intended for use with Standard Ignition. If custom modules are needed for other editions of Ignition, such as Ignition Cloud Edition, Ignition Edge, or Ignition Maker Edition, customers can reach out to [Inductive Automation](#) to discuss exceptions on a case-by-case basis.

*Ignition™, Ignition Edge™, and Inductive Automation® are trademarks of Inductive Automation.*

*All other product or company names that may be mentioned in this publication are tradenames, trademarks, or registered trademarks of their respective owners.*

*Ignition User Manual © 2015-2026 Inductive Automation, Inc*

*All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording,*



*taping, or information storage and retrieval systems - without the written permission of the publisher.*

*All Inductive Automation products are trademarks or registered trademarks of Inductive Automation. Other brand and product names are trademarks or registered trademarks of their respective holders.*

*Every effort has been made to make this user manual as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. Inductive Automation shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this manual.*

# Getting Started

## **Introducing Ignition**

Ignition by Inductive Automation® combines an unlimited licensing model with instant web-based deployment an...

## **Modules Overview**

## **Startup Guide**

## **Installing and Upgrading Ignition**

## **Perspective and Vision - Which Visualization System is Best for Me?**

Ignition's Perspective module and the Vision module each enable you to rapidly develop industrial applications fo...

# Introducing Ignition

## What is Ignition?



INDUCTIVE  
UNIVERSITY

**What is Ignition?**

[Watch the video](#)

Ignition by Inductive Automation® combines an unlimited licensing model with instant web-based deployment and the industry-leading toolset for supervisory control and data acquisition (SCADA), all on one open and scalable universal platform. Ignition is "The New SCADA" because it solves all the major pain points of old SCADA. Ignition empowers your business to easily control your processes to track, display, and analyze data, without limits. Ignition is designed to be approachable and easy to get started with, while being flexible and capable of scaling up to the largest projects. Ignition is unlimited; for the low cost of one server license, you can connect all your data, design any kind of industrial application, and instantly deploy web-based unlimited Clients and Sessions to anyone or anywhere, all from one universal platform.

The features below are core to Ignition.



**Server-Based:** One computer controls everything in Ignition. You install a server in one place and connect everything else to that server. With this feature, you can have as many **Client** runtimes, **Sessions**, and **Designers** as you want.



**Simple Licensing:** Only one **license** for your server is required. This gives you unlimited access to various features such as unlimited Clients, Sessions, **tags**, and **projects**. Without limits on these resources, you can exchange important data and analytics with your entire team, and across your whole company. Ignition allows you to create and use as many tags as you need for different purposes like **devices**, **OPC servers**, and runtimes.



**Web-Based Deployment:** Ignition is installed, deployed, and managed using standard web technologies. You can connect from any computer on the network to perform actions like managing settings, updating projects, creating new tags, and launching new runtimes.



**Access to the Designer, Clients, and Sessions:** You can download the **Designer Launcher** to make changes to your projects, the **Vision Client Launcher** to launch Clients, and **Perspective Workstation** to launch Sessions. Alternatively, you can create deep links for each type of launcher pointing towards specified projects. Any of these options can be set up on any system in your network, giving you and your users access to Ignition from anywhere your network extends. In initial benchmark testing, Ignition Perspective can simultaneously and easily launch 200 Sessions.



**Built-in Security:** Security is built into every aspect of Ignition. You can **manage users**, edit screen permissions at the individual **tag** or component level for both **Vision** and **Perspective**, and even secure certain assets in your projects.



**Scalable Modular Architecture:** You can create a scalable and centrally managed SCADA system using Ignition's web-based server architecture. Configure unlimited connections to PLCs, databases, and web-launched runtimes, along with web-based deployment, and different types of **System Architectures** to suit your needs. Projects can initially be created small and expanded out indefinitely as your business grows, or you can have smaller installations connected to and interacting with other larger systems.



**Cross-Platform:** Ignition is built on Java and works with any major operating system, including Windows, MacOS, Linux, iOS, and Android. **Backups** of your system are also cross-platform, allowing you to load a backup from any system.

## New in This Release

Ignition 8.3 contains new features that are not available in previous versions. Some of these features include:

- New Core Historian, powered by QuestDB. This provides several advantages over the previous Internal Historian (Legacy), like downsampling, archiving, and optimization for time-series data. The previous Internal Historian (Legacy) will still be available to use.
- Robust Secrets Management system, providing better support and security for secrets such as credentials, API tokens, and private keys.
- Platform-wide event streams, allowing users to easily send and receive data across Ignition and external systems like Kafka.
- Deep link and File Association support, letting users launch an application using a simple URL and without needing to open a launcher.
- More user-friendly Store & Forward engine, using Google Protobuf instead of Java Serialization.
- New Drawing component in Perspective, letting users draw their own vector graphics, similar to Vision's drawing tools.
- New Form component for Perspective, with customizability and versatility for creating dynamic forms accepting user input.
- Gateway Deployment Modes, allowing users to override Gateway resources and assign them to custom-created deployment modes, which provides multiple Gateway runtime options.
- Scripting functions, including new system functions for new and existing features. Some system functions from 8.1 have also been overhauled, making them more efficient and easier to use.

For a full list of new features, see the [New in this Version](#) page. More features will also be released with every minor Ignition release version (8.3.X).



**Web-Based  
Deployment**



**Unlimited  
Licensing**



**Security &  
Scalability**



**Real-Time Control  
& Monitoring**



**Rapid  
Development**



**Expandability  
& Scalability**

## What Can Ignition Do?

Because of its modular nature, Ignition can be customized to your needs. A lot of the basic functionality is shared between modules and stored in the Gateway to make everything smooth and seamless. Some of these basic functionalities include database connections, device connections, tags, security profiles, and alarming. Because these are all shared resources, you don't have to manage multiple connections for the different modules in Ignition. Ignition's modular platform also supports your requirements by allowing you to select the modules you need and build processes suited for your business. You do not need to pay for any modules you do not want.

Using Ignition, you can build projects like **database** applications, point of sale (POS) systems, customer relationship management (CRM) tools, and inventory tracking software. Additionally, you can bring in data from any SQL database in your plant and interact with other existing enterprise resource planning (ERP) software and Access systems.

See the sections below to learn more about how Ignition utilizes all of these available tools for some inspiration of what's possible.

## Web-Based HMI and SCADA Applications Deployment

Using web technologies, you can access programmable logic controllers (PLCs) and connect to SQL databases on any platform. Ignition provides common HMI/SCADA capabilities easily and efficiently, by allowing you to:

- Create Clients and Sessions that show current or past data
- Interact with your other systems and devices
- Create displays and controls for anything wired into your system
- See and manage your entire system from one place



## Historian Capabilities

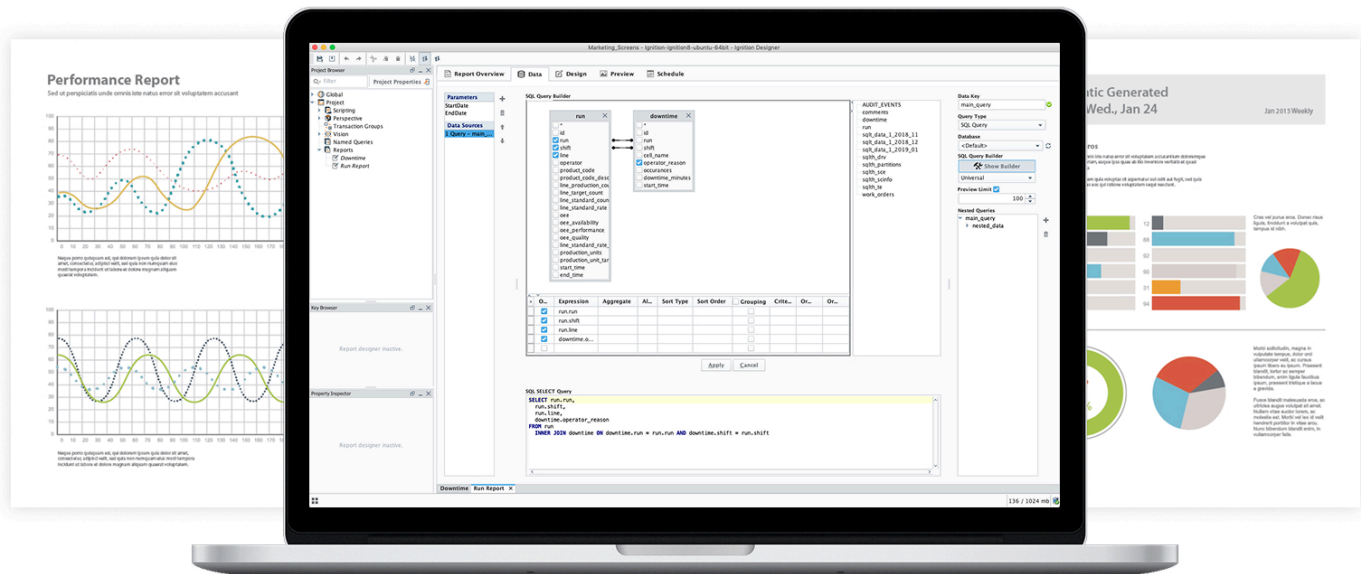
You can use any SQL database with Ignition's **tag historian** module. In addition to being simple to set up, Ignition will monitor and control the data for you. The historian includes partitioning and uses compression algorithms for fast data storage and retrieval.



## Reporting Engine

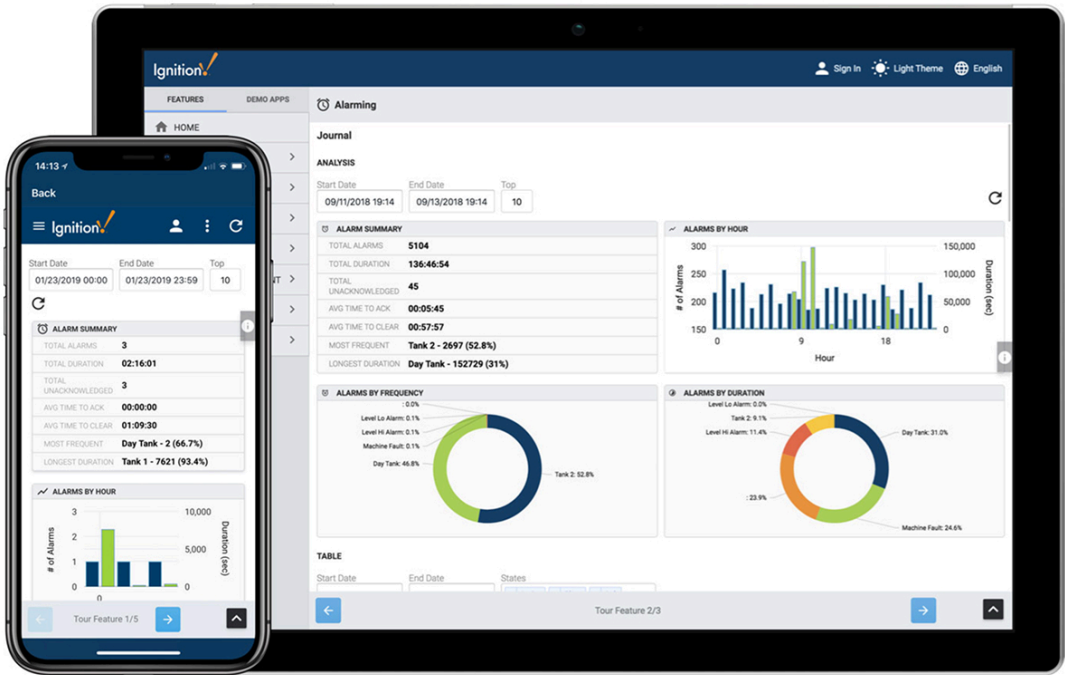
You can **create dynamic PDF reports** that users can see and change anytime. This can be automated by creating a schedule during which documents such as analytical data or compliance

reports can be generated or emailed out. Your users can change date ranges on any reports you create or select past reports without any changes to the system.



# Alarming

You can use Ignition's alarming engine to **create alarms** for any conditions. Alarms can be shelved, recorded, acknowledged, or handled through notifications and messaging. Email, standard text messages (SMS), and voice messages can be sent to individuals or lists of users based on any logic you need.

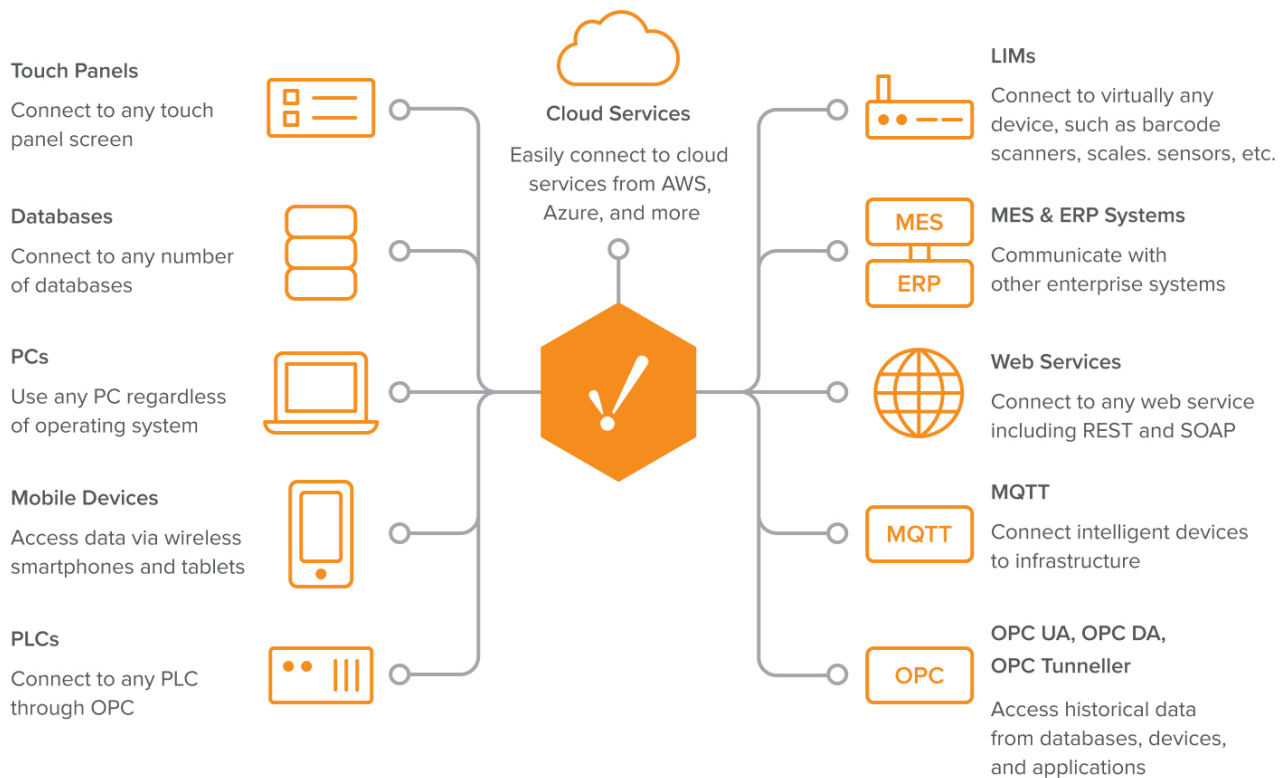




# Communications Hub

You can use Ignition as an effective communication hub in your network. You can use some or all of the features below to make Ignition move data throughout your facility. Ignition can function as the nexus of your system by using:

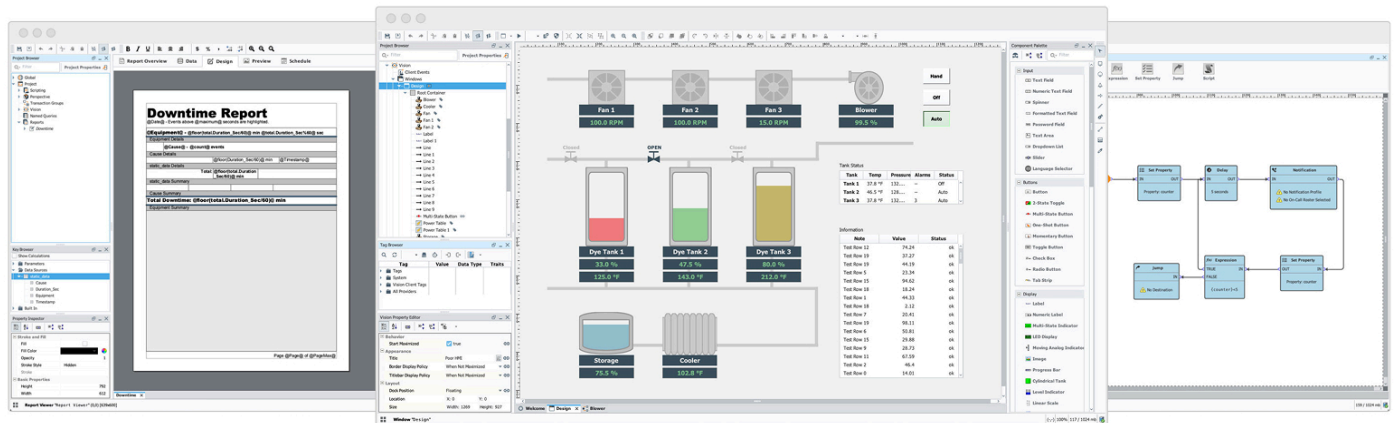
- OPC-based communication to interact with almost **any OPC server**
- **SQL-based** JDBC drivers to connect to any number of databases
- Built-in **PLC drivers** to connect to any PLC (such as Allen-Bradley, Siemens, Modbus) through OPC
- Web services to support launching anywhere
- System compatibility with **other enterprise systems** (ERP)
- **Connections to devices**, such as barcode scanners, scales, and sensors
- Connections to any mobile device, such as wireless smartphones and tablets
- Connections to any touch panel screen or human machine interface (HMI)



## Design Projects and Resources

By using different components and linking them to tags, each other, and different parts of your project, you can create any type of application you need. You can also directly interact with any projects you create or modify in the Designer as if you were an operator using the Designer's Preview Mode. This helps users test their projects before deploying any changes across your architecture.

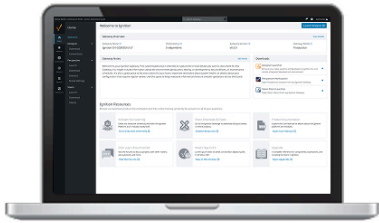
Using the features available in Ignition, you can create projects such as the one pictured below.



## Understanding Ignition's Flow

Ignition is easy to install and designed to be straightforward to use, from project creation to production deployment and beyond. Once Ignition is installed, you can use the steps below to assist in setting up and launching a project:

- **Launch the Gateway Webpage:** The Gateway Webpage is where you store all of your information, and configure all of your general settings, like device connections, database connections, security, Gateway backups, and redundancy.
- **Launch the Designer:** Once your connections are in place, you can use them when developing a project. Download the Designer Launcher or set up a deep link on any system that can connect to your Gateway, and then launch the Designer to begin creating your project. Add resources such as tags, query databases, status metrics, history trends, and alarms to your project.
- **Save your Project:** When you save, Ignition sends all your data and changes back to the Gateway. Everything is centrally stored in the Gateway, so you never have to worry about managing several versions or trying to combine multiple changes into one. You can even launch Designers concurrently to allow multiple people to work on the same project at the same time. Projects are not limited in scope, allowing you to create them for anything you can think of, such as HMIs, general SCADA software, reporting, history, and alarming.
- **Launch Client and Session Runtimes:** You can launch one runtime or multiple at the same time. Download the Vision Client Launcher, Perspective Workstation, or create a deep link on any system within your network to launch Clients and Sessions the same way as the Designer. All of your runtimes talk directly to the Gateway to get new information, eliminating any worry about sync issues or individual runtime loading changes.



Launch Gateway  
Webpage



Web-Launched  
Designer



Save  
Project



# Modules Overview



INDUCTIVE  
UNIVERSITY

About Ignition's Modules

[Watch the video](#)

Ignition's modular architecture allows you to customize and expand your system according to your needs. Modules enhance Ignition's functionality, enabling you to start with essential features and add more as required.

## What are Modules?



Modules extend Ignition's capabilities. They introduce specific features or functionalities, such as new Designer workspaces, Gateway settings, and drivers. Core modules include the **Perspective**, **Vision**, and **SQL Bridge** modules.

Modules integrate directly with Ignition, offering new features with minimal configuration. Once installed, modules work seamlessly with existing components.

## Benefits of Modules

- **Flexible Licensing:** License only the modules you need, reducing costs and simplifying system setup.
- **Dynamic Management:** **Enable or disable** modules as needed, with changes taking effect after a Gateway restart.
- **Increased Stability:** Modules built on a common platform benefit from improved reliability and isolation.
- **Plugable Architecture:** Easily add new features with new or third party modules.

# Capabilities of Modules

Modules provide a range of functionalities:

- **Screen Creation:** Design dashboards, detail windows, and historical displays using the **Vision** module. Integrate real-time data from **OPC UA** servers and create interactive user forms.
- **Mobile Access:** The **Perspective App** allows viewing and interacting with Ignition applications from mobile devices, including tablets and smartphones.
- **Alarm Management:** Configure alarms to detect system issues and notify users. Alarms can be displayed with pre-built components and logged into SQL databases. Notification modules can send alerts via **email**, **SMS**, or **phone calls**.
- **Data Collection:** Use the **SQL Bridge**, **Historian Core**, and **SQL Historian** modules for data logging. Historical data can be used in charts, tables, and reports, with storage in SQL databases for easy access by third party software.
- **Reporting:** Generate on-demand reports using data from various sources. The **Reporting** module allows for the creation, scheduling, and delivery of reports through email or network drives.

## Solution Suites

Building on how modules work together to expand functionality, the Ignition Solution Suites group modules as pre-packaged collections to address specific operational challenges. Modules within each suite cannot be removed, but you can add individual modules on top of a suite for further customization of your system. The modules included in each suite are listed in the table below.

| Name                         | Description                                                                                             | Included Modules                                                              |
|------------------------------|---------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Application Building Suite   | Build powerful mobile-responsive industrial applications like SCADA, HMI, Reporting, and more.          | Perspective and Reporting                                                     |
| Industrial Historian Suite   | Optimize time-series data management with powerful, high-performance Historians.                        | Historian Core and SQL Historian                                              |
| Enterprise Integration Suite | Integrate your industrial systems with your enterprise data for smarter decisions and sustained growth. | MongoDB, Kafka, MQTT Transmission, and MQTT Engine                            |
| Alarm Management Suite       | Ensure timely and effective responses to critical events with advanced alarm notifications.             | Alarm Notification, Voice Notification, SMS Notification, Twilio Notification |
| DataOps Suite                | Streamline data operations with event-driven management and custom web development tools.               | SQL Bridge, Web Development, and Event Streams                                |

## Third Party Modules

In addition to Inductive Automation’s modules, third party companies offer modules developed with Ignition’s Module Software Development Kit (SDK). Examples include:

- **MES Modules:** [Sepasoft](#) provides **Manufacturing Execution Systems (MES) modules** for tracking OEE, implementing SPC systems, and managing resources.
- **MQTT Modules:** [Cirrus Link’s](#) modules integrate **MQTT** with Ignition, expanding data access by exposing numerous data points as tags. Additional third party modules are available on our [downloads](#) page.

## Creating Custom Modules

To develop custom modules, refer to the [SDK documentation](#). This resource provides guidelines and tools for creating modules.

# Core Modules

Build any kind of human machine interface (HMI) or supervisory control and data acquisition (SCADA) system using Ignition's powerful offering of HMI/SCADA modules.

## What Are Core Modules?

Core modules are commonly used modules included in a typical installation. Most systems have at least one of these modules installed. Each core module encapsulates a core SCADA or HMI principle such as data-logging or process visualization. These modules are the foundation upon which great projects are built.

### SQL Bridge



Bridge the gap between OPC data and SQL databases and get a highly efficient SQL-based tag historian and transaction manager. Easily log data, call stored procedures, and synchronize data bi-directionally.

### Perspective



Create beautiful, mobile-responsive industrial applications that run natively on any device type such as smartphones, tablets, touchscreens, laptops, and desktop computers. It automatically adapts to fit screens of any size and orientation.

## Vision



Use this module to launch an unlimited number of powerful Ignition Vision clients anywhere on the network. Display charts, graphs, trends, HMI screens, and more.

## Historian Core



Use this module to create powerful time-series historians in Ignition.

## SQL Historian



Add the SQL Historian, which turns a SQL database into a high-performance time-series tag historian, to the list of historian options already available through the Historian module.



## Reporting



Create dynamic, database-driven PDF reports with ease.

## OPC-UA



Connect to most major PLCs (Programmable Logic Controllers) with the Ignition OPC-UA Module. This module serves as a totally cross-platform OPC-UA server with an open, plugable driver system.

## Alarm Notification



Configure the logic for how, why and when alarm notifications are delivered, manage alarm notification for groups of users, and send notifications via email.

## Event Streams



This module provides source and handler combination to receive, filter, and transform event-driven data.

## SMS Notification



Add text alerts with the SMS Notification Module for even more options.

## Sequential Function Charts



Streamline the creation, organization, and visualization of robust logic systems.

## Web Dev



Create webpages that are hosted on Ignition's web server.

## Enterprise Administration



The EAM provides a secure and intuitive way to manage many Ignition installations from one location.

## JDBC Drivers

JDBC Driver modules enable database connections by providing the MariaDB JDBC Driver (version 3.3.3), MSSQL JDBC Driver (version 9.4.0.jre11), and PostgreSQL JDBC Driver (version 42.7.2).

# Vision Module

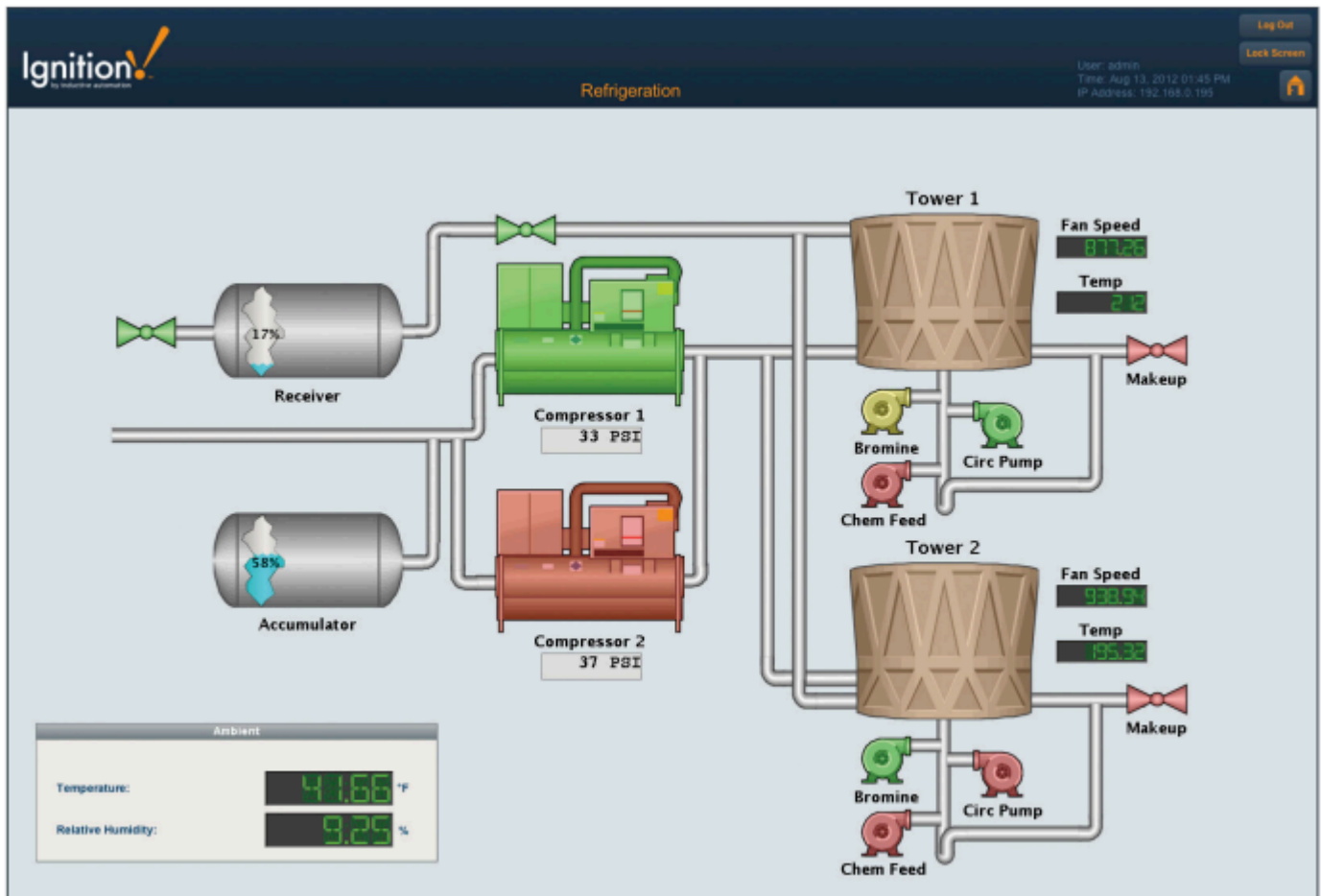


## HMI/SCADA Visualization

### Get Realtime and Historical Data on Control Screens

The Vision module delivers a dynamic, powerful, and beautiful HMI experience unlike any other. Display realtime and historical data on everything from status and control screens to interactive charts and tables so you can analyze data at a glance and quickly act on it. Since all clients are connected to a central server, everyone in your company will stay up to date and can easily access the realtime data they need.

You'll never be limited by how many Clients (runtimes) or screens you can use because the Ignition Vision module includes unlimited clients per central server. Every member of your company can have insight into operations at no additional cost.



## Realtime Status and Control

Ignition's realtime status and control functionality, coupled with advanced analytic capabilities provided by Ignition's SQL database integration, gives you the power to quickly analyze and easily display the status of your facility.

## Alarming

Set up screens to display realtime alarms from Ignition's [Alarming](#) system, so your operations team can respond quickly to resolve the issue.

## Analyze Realtime and Historical Data

Included customizable charts, tables and graphs display your real-time and historical data, making at a glance analysis easy. You'll be able to quickly set up executive dashboards, track key performance indicators (KPIs), and view trends.

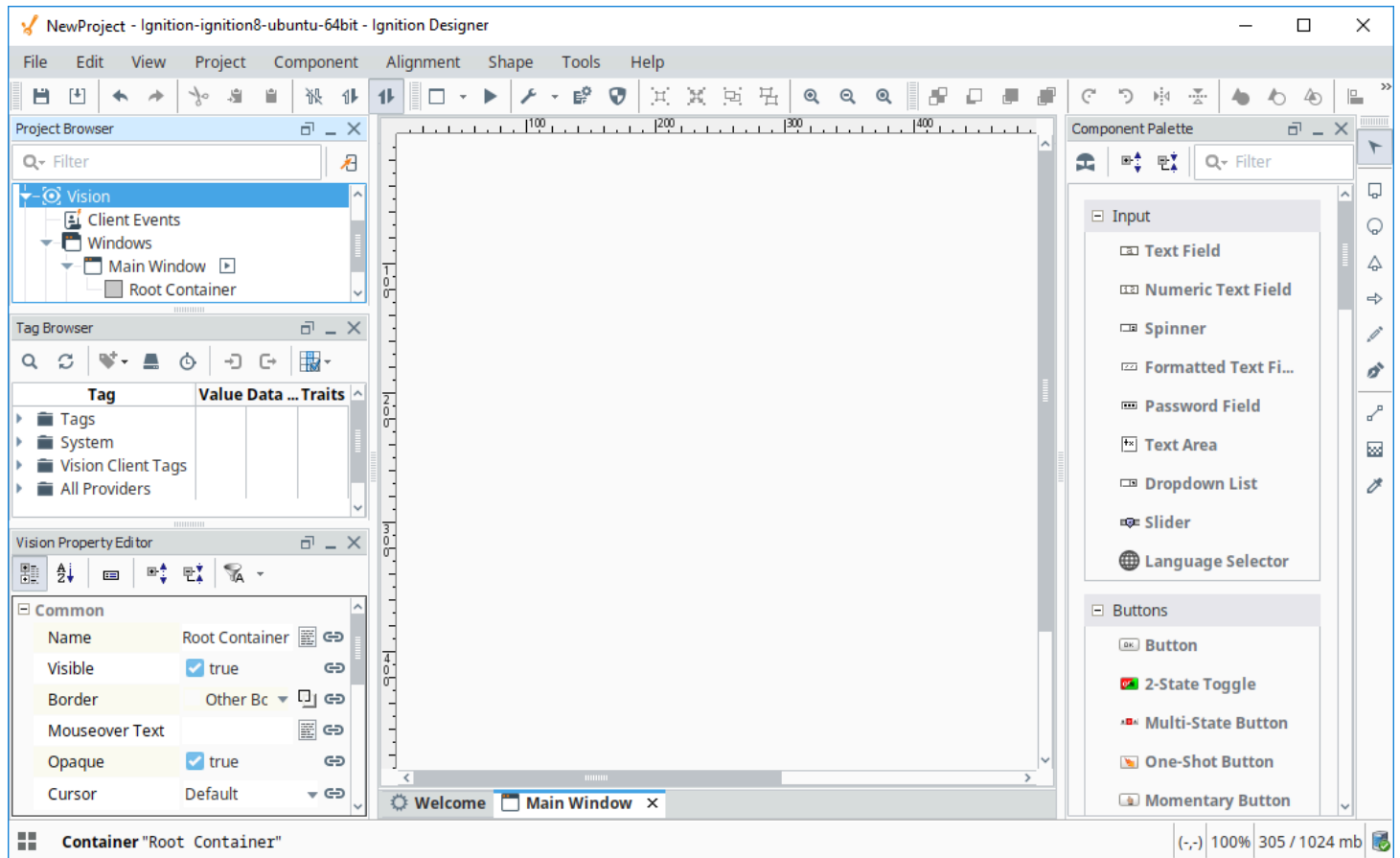
## Database Front-End

Easily integrate data from SQL databases with your SCADA system. Data entered by operators can be written directly to any database. The powerful property binding system makes it easy to display

information from databases on any screen.

## Designer Included

Clients are configured through the included Ignition Designer. Drag-and-drop configuration makes screen development intuitive; simply drag Tags and drop them onto components to instantly bind data to inputs, displays, tables, charts, and more.



## Vector-Based 2D Drawing Tools

Create distinctive screen designs and layouts with shape-building tools for lines, polygons, rectangles, arrows, and circles. Vector graphics let you create precision shapes and Bézier curves that look great on any size monitor; shapes scale to any size without losing image quality.

## Image Library

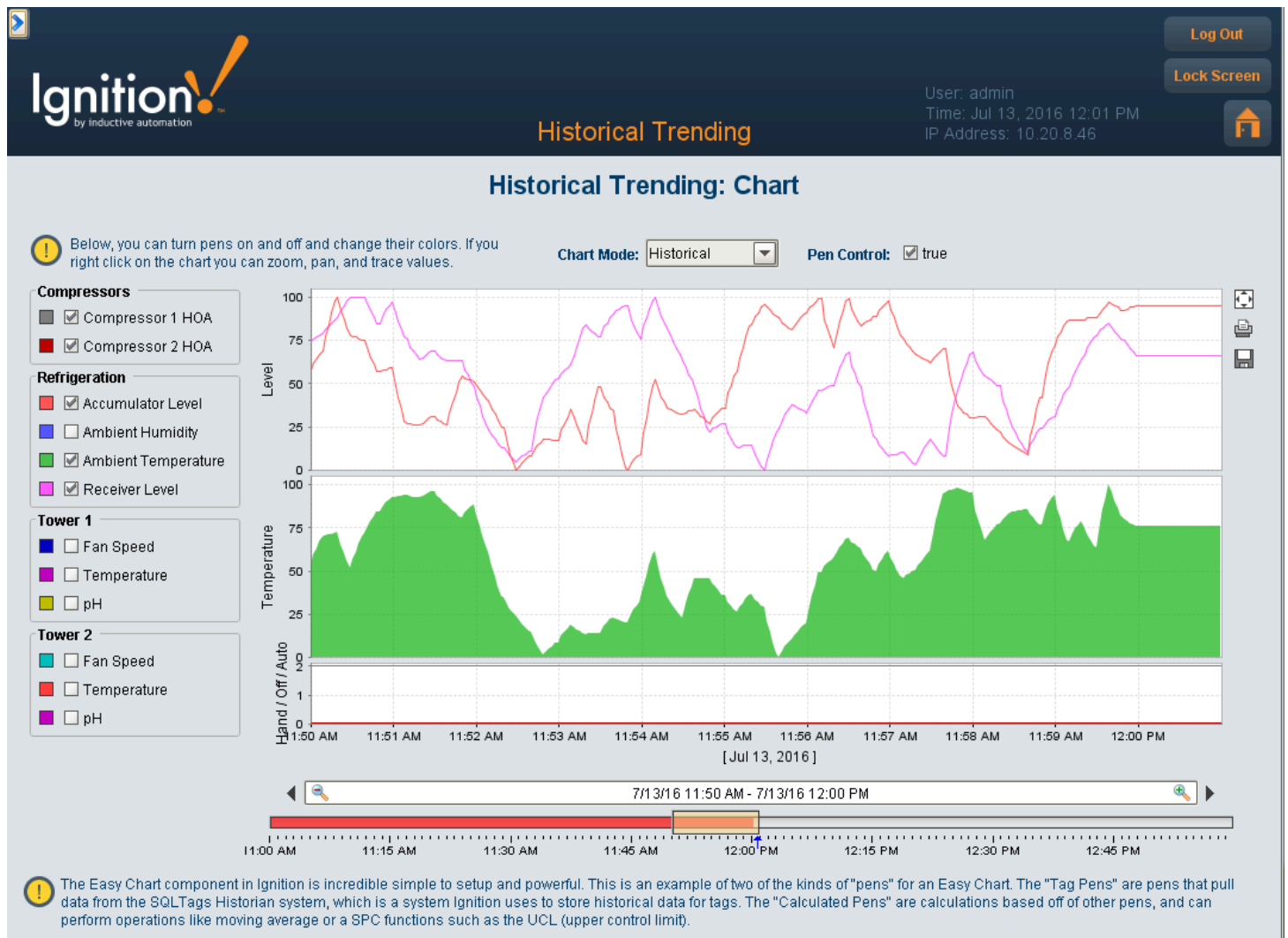
The designer integrates Symbol Factory 2.5 from Software Toolbox. The intuitive interface allows you to browse and search through nearly 4,000 high quality vector graphics symbols. Once you find the symbol you're looking for, simply drag-and-drop it onto your design window to use it right away.

# Easily Create Animations

State dependant settings and dynamic positioning lets you bind shape properties to data values so you can easily create animations.

## Speed Development With Templates

Develop large projects at record speeds by using component templates. Instances of each template can be placed on as many screens as you want. Any changes made to the template are automatically updated to any instance of that component, saving a huge amount of tedious development time.



## Python Scripting

Advanced functionality can be achieved using the built-in Python scripting engine. Python is an extremely popular, powerful, and easy to learn scripting language. Python is highly regarded for its readability, making your projects easy to maintain.

## Secured Via SSL

Every client you launch from the Vision module is secured using SSL protocols. In order to keep your data secure, authentication groups can be used to strictly limit access to certain areas of a project to only the users with appropriate access levels.

## Unlimited Clients and Instant Deployment

With the Ignition Vision module installed on your server, you can launch as many clients as you want, instantly. No individual client install required.

## Update All Screens With One Click

With Ignition, managing five clients is just as easy as managing 50. All clients can be updated instantly by making changes to the master project screen on your server, and then clicking the save button.

## View Anywhere, Any Time

View your HMI/SCADA system from anywhere, any time, on any machine. Ignition uses your computer's web browser to launch rich Java applications – not thin web pages – which are fast and cross-platform, making accessibility easy for anyone on your network. For more information on accessing Vision projects remotely, refer to the [Accessing Projects Remotely](#) section.

## Looking for Less?

Some systems only require a handful of clients at any given time. In cases like these the **limited version** of Vision is a perfect fit. It contains all the functionality of the full version, but at a greatly reduced cost. Contact our Sales department for more details.

## Want to Learn More?

For more information on the Vision module, please see the [Vision](#) section of this user manual.



# Perspective Module



## PUBLIC DEMO HOME PAGE

The Demo Project uses the Perspective Module to show many key features of Ignition. [Go to the Demo Page](#)



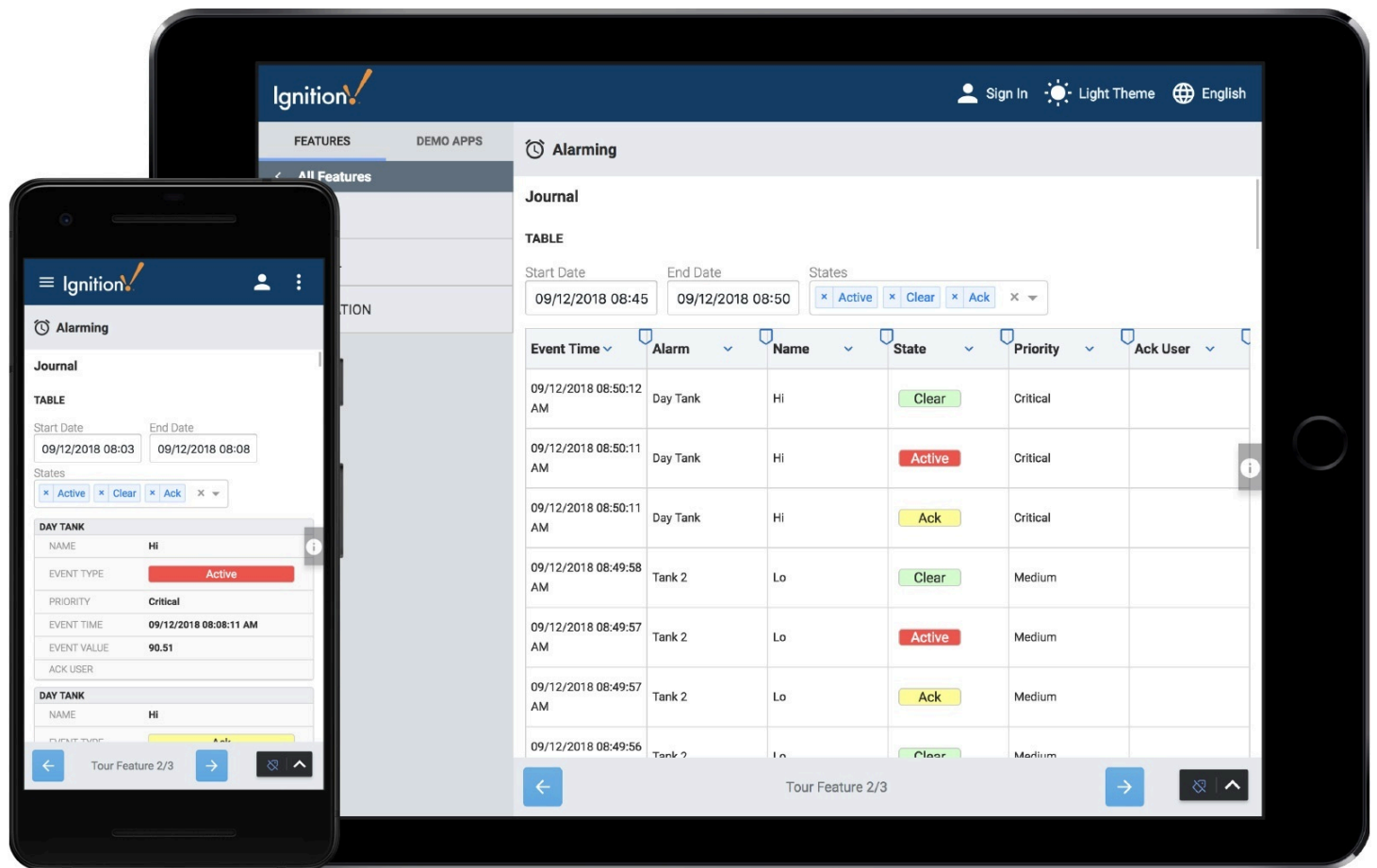
INDUCTIVE  
UNIVERSITY

**What is Ignition?**

[Watch the video](#)

## Mobile Responsive Design

The Perspective module raises the bar for visualizing your control applications in Ignition. Not only does it leverage the popular standard HTML5/CSS3 technology for its UI layer, but it also allows users to see and control their application on any device, from a small smartphone to an oversized desktop, in an optimized format. HTML5/CSS3 allows screens to display gracefully on any device, regardless of size or scale. Multi-touch responsiveness allows for greater flexibility of use than ever before. The Perspective module marks the beginning of truly mobile-optimized, touch-responsive, easily accessible applications for monitoring, control, analysis and data gathering in industrial systems.



## Device Compatibility

The Perspective module creates applications that are compatible with any device, including all mobile touchscreen devices like smartphones and tablets, and any desktop running any current web browser, on any major operating system: Windows, macOS, and Linux, iOS, and Android.

For more information on accessing Perspective projects remotely, refer to the [Accessing Projects Remotely](#) section.

## Run as a Native App

Run your Perspective Sessions in a web browser or in a native App on your device. Apps can be downloaded on Android or iOS devices and allow you to natively run a Perspective session on your phone or tablet. This gives you the ability to use more of your device, like using the camera to scan barcodes or the built-in GPS to verify a location.

## Responsive Design

Applications designed with the Perspective module respond to changes in screen size and orientation, and scale elegantly when launched on any size mobile multi-touch device. Perspective provides several container types for maximum design flexibility, each of which employs a different layout

technique. Designers can compose these container types together, providing a very flexible system that can handle any kind of responsive design.

## Designed for Touch

Perspective employs multi-touch technology, making it possible to work with TouchPad and touch-screen interfaces found on smartphones, tablets, laptops, and desktops. This allows users to work with familiar tools for panning, zooming, scrolling and more.

## CSS and Themes

The Perspective module takes advantage of its roots in web technology to give you easy to configure themes and styles using familiar CSS settings. Configure a few themes, use them throughout your projects, and swap between them however you'd like. It's easy to let your users change text, and colors whenever they like.

## Security via SSL

Clients launched from the Perspective module are secured using cutting-edge encrypting technologies and communications protocols to provide the most secure web-based data transfer. It also has strongly enforced “guest mode” access to prevent against unauthorized writes on the Gateway.

## Offline Mode Functionality

Perspective sessions can be run in **Offline Mode**, allowing for limited capabilities. This is useful in cases where network availability is spotty or nonexistent. Once a network connection is established, locally collected data is then synced to a central location, where it will then be available throughout the Gateway or Gateway Network.

# OPC UA Module



## Cross-Platform OPC UA Functionality

The Ignition OPC UA module offers OPC UA server functionality with a variety of device drivers and a robust, open driver API.



## OPC UA Server Functionality

This module turns Ignition into an OPC UA server, capable of handling connections from any OPC UA compatible client. Outgoing connections can also be made to third party OPC UA servers. In this way Ignition functions as both an OPC UA server and an OPC UA client.

## Built-in Device Drivers

The OPC UA module provides a suite of standard device drivers for common industrial protocols and is easily expandable thanks to Ignition's modular architecture. New drivers can be downloaded and installed in minutes without affecting other parts of the platform. However, changes to a module's status, such as Active, Inactive, or any Pending Restart state, only take effect when the Gateway restarts. If a restart is required, a banner will appear at the bottom of the Gateway, allowing you to apply the changes immediately.

### CAUTION

Restarting the Gateway may temporarily interrupt running services.

Drivers for the OPC UA module are deployed as modules themselves. While they don't add a visible element to the system, they are loaded and upgraded in the same manner as other Ignition modules. A list of the included drivers on install can be found on the [Driver Modules](#) page.

## Redundancy Support

The OPC UA module ties into the Ignition redundancy in order to provide efficient access to device data along with failover redundancy, with no additional configuration.

## Public Driver API

Ignition provides a public driver API that allows developers to create custom device drivers for the OPC UA module. These drivers can be installed like any other module and used to support proprietary or specialized protocols. Developers can also share drivers with others or integrate them into third party solutions. For more information about developing custom drivers, visit the [Inductive Automation](#) website.

## Ready to Get Started?

Documentation on the OPC UA module can be found on the [OPC UA and Device Connections](#) page.

# Driver Modules

The following drivers are available for Ignition's OPC UA module.

## Allen-Bradley

Ignition includes several drivers for connecting to Allen-Bradley PLCs over EtherNet/IP.

### Allen-Bradley Driver

The Allen-Bradley driver supports the following connections:

| PLC          | Capability                                                                    |
|--------------|-------------------------------------------------------------------------------|
| CompactLogix | Connect to Allen-Bradley CompactLogix firmware v20 and prior processors.      |
| ControlLogix | Connect to Allen-Bradley ControlLogix firmware v20 and prior processors.      |
| MicroLogix   | Connect to Allen-Bradley MicroLogix 1100, 1200, 1400 and 1500 series devices. |
| PLC5         | Connect to Allen-Bradley PLC5s via Ethernet.                                  |
| SLC          | Connect to Allen-Bradley SLC 5/05s via Ethernet.                              |

More information and detailed instructions can be found on the following pages:

- [Connecting to CompactLogix](#)
- [Connecting to ControlLogix](#)
- [Connecting to MicroLogix](#)
- [Connecting to PLC5](#)
- [Connecting to SLC](#)

### Logix Driver

The Logix driver supports connections to Allen-Bradley Logix series devices including devices with firmware v21+.

More information and detailed instructions on how to connect can be found on the [Connecting to Logix](#) page.

## Micro800 Driver

The Micro800 driver supports connections to Allen-Bradley Micro820, Micro850, and Micro870 series devices.

More information and detailed instructions on how to connect can be found on the [Connecting to Micro800](#) page.

## BACnet

### BACnet Driver

The BACnet driver allows the Ignition OPC UA server to communicate with devices over the BACnet/IP protocol.

More information and detailed instructions on how to connect can be found on the [BACnet driver](#) page.

## DNP3

### DNP3 Driver

The DNP3 driver enables communication with DNP3 outstations. It supports event-based polling, unsolicited messaging, and explicit reads for data acquisition.

More information and detailed instructions on how to connect can be found on the [DNP3 driver](#) page.

### Legacy DNP3 Driver

The legacy DNP3 driver also supports DNP3 outstations, but only provides unsolicited messaging and explicit reads. This driver is deprecated and no longer supported.

More information and detailed instructions on how to connect can be found on the [Legacy DNP3 driver](#) page.

# IEC 61850

## IEC 61850 Driver

The IEC 61850 driver supports IEC-enabled devices using the MMS protocol. It is built on the Triangle Microworks library and is available for Windows and Linux x64 operating systems.

More information and detailed instructions on how to connect can be found on the [IEC 61850 Driver](#) page.

# Mitsubishi

## Mitsubishi Driver

The Mitsubishi driver supports communication with devices that use the MELSEC protocol over TCP. Users can create, import, or export addresses to configure tag access.

More information and detailed instructions on how to connect can be found on the [Mitsubishi TCP driver](#) page.

# Modbus

## Modbus Driver

The Modbus driver supports devices that use the Modbus TCP or Modbus RTU over TCP protocols. Devices can be connected directly over Ethernet or through a Gateway device.

More information and detailed instructions can be found on the following pages:

- [Connecting to Modbus Device](#)
- [Modbus Addressing](#)
- [Modbus Address Mapping](#)



# Omron

## Omron Driver

The Omron driver supports communication with Omron NJ series controllers and devices using the FINS protocol.

More information and detailed instructions on how to connect can be found on the [Omron NJ driver](#) and [Omron FINS driver](#) pages.

# Siemens

## Siemens Drivers

The Siemens drivers provide support for connecting to select PLCs via TCP/IP using the S7 protocol with absolute addressing only:

- S7-300 Driver
- S7-400 Driver
- S7-1200 Driver
- S7-1500 Driver

More information and detailed instructions on how to connect can be found on the [Siemens Drivers](#) page.

## Siemens Enhanced Driver

The Siemens Enhanced driver provides support for connecting to select PLCs via TCP/IP using the S7 protocol with absolute addressing or symbolic tag access. It can connect to Siemens S7-300 and S7-400 with absolute addressing, or S7-1200 and S7-1500 with absolute or symbolic addressing.

More information and detailed instructions on how to connect can be found on the [Siemens Enhanced Driver](#) page.

# Generic Protocols

## UDP and TCP Drivers

The UDP driver passively listens for incoming data on one or more ports at a specified IP address. The TCP driver actively connects to one or more ports at a specified IP address and can also write data back to the connected ports. The configuration settings determine how the incoming data is parsed and interpreted.

More information and detailed instructions on how to connect can be found on the [UDP and TCP drivers](#) page.

# Historian Core Module



The Historian Core module records tag data to embedded or external time-series storage. With minimal configuration, you can start storing and querying tag history across your project. The module includes automatic table management, storage optimization, and built-in support for querying, aggregation, and charting.

The Historian Core module supports a pluggable API and multiple internal storage options, including the Core Historian and Internal Historian (Legacy).

## Store Tag History Easily

Enable history on a tag with a single click. No custom table design or SQL experience required.

## Automatic Table Management

The module manages all underlying tables automatically. Schema creation, indexing, partitioning, and retirement logic are built-in and fully optimized for time-series data.

## Query and Visualize

Query tag history through scripting or visual bindings in Perspective and Vision. Use built-in charts or build custom visualizations using raw history queries.

## Performance Features

The historian engine supports analog compression, interpolation, partitioning, and aggregation. These features work out of the box, helping you reduce storage and improve query performance.

## Accessible and Open

Data is stored in an open SQL database format, so it's available to other applications and reporting tools outside of Ignition. No vendor lock-in, and no proprietary formats.

## Integrated with Ignition

The Historian Core module works seamlessly with other modules. Use stored data in alarms, reports, dashboards, or any custom solution. The historian also supports distributed history, redundant storage, and hybrid cloud architectures.

## Learn More

To learn more about configuration, scripting, or architecture, refer to the [Historian Core](#) page.

# SQL Historian Module



The SQL Historian module expands the functionality of the **Historian Core** module by providing the SQL Historian as an additional option. The SQL Historian leverages a SQL database for the storage and retrieval of historical data.

## NOTE

The SQL Historian module requires the Historian Core module to be installed on the same Gateway.

## Connecting to the SQL Historian

When you have both the Historian Core module and SQL Historian module installed, you simply need to navigate to **Services > Historians > Historians** and select **Create Historian** to add a SQL Historian to your Gateway. From here you can choose where to store your tag history, and configure data partitioning and data pruning settings.

This historian type is well-suited for systems that require robust reporting, integration with external tools, or long-term historical data storage.

## Create Historian



### Create Historian

1. Select Type

2. Configure Historian



#### DB Table Historian

Adds historian style query support to standard wide database tables.



#### Internal Historian - QuestDB

A built-in local historian optimized for high-throughput, demanding workloads. Recommended choice for most use cases that require local timeseries data storage.



#### Internal Historian - SQLite

A built-in local historian for lightweight applications.



#### Remote Historian

Stores historical data to a remote historian using the Gateway Network.



#### Simulator Historian

Provides simulation data for testing without an external data source.



#### SQL Historian

A historian that leverages a SQL database for the storage and retrieval of historical data.

Cancel

Next

## Want to Learn More?

See the [SQL Historian](#) section on the History Providers page for more information.

# SQL Bridge Module



## High-Powered Data Acquisition

### Share Plant Floor Data With Any Database

The Ignition SQL Bridge Module brings the power of structured query language (SQL) databases to your industrial process. The module allows you to leverage Ignition's unlimited Tags and database connections at an astonishingly low price — even if you don't know much about SQL databases.

Think of the SQL Bridge module as a "Swiss Army Knife" for integrating programmable logic controllers (PLCs) and SQL databases in unlimited ways, such as the capability to move data bidirectionally, log huge amounts of data easily, synchronize PLCs with databases, create powerful recipe and batching systems, and sequence entire processes.

The screenshot displays the Ignition SQL Bridge Module interface. The main window is titled 'new historical' and is in a 'Running' state. It features a 'Project Browser' on the left, a 'Tag Browser' at the bottom left, and a 'Properties' panel on the right. The 'Properties' panel is divided into several sections:

- Basic OPC/Group Items (6)**: A table listing items and their properties.
- Run-Always Expression Items (ignore trigger) (0)**: An empty table.
- Triggered Expression Items (0)**: An empty table.
- Execution Scheduling**: Options for 'Timer' and 'Schedule'.
- Data source**: A dropdown menu set to '<Default>'. Below it, a 'Table name' field is set to 'group\_table'.
- Options**: Checkboxes for 'Automatically create table', 'Use custom index column: group\_table\_ndx', 'Store timestamp to: t\_stamp', 'Store quality code to: quality\_code', and 'Delete records older than: 1 day(s)'.

The 'Tag Browser' shows a hierarchy of tags under 'Sim\_Generic', including 'Ramp0 OPC' through 'Ramp8 OPC'. The 'Properties' panel also shows a 'Status' section with 'Running' and 'Events' tabs. The 'Status' section displays execution statistics:

- Last execution: Wed Apr 24 10:03:24 PDT 2019
- Last trigger: Wed Apr 24 10:03:24 PDT 2019
- Next execution: Wed Apr 24 10:03:25 PDT 2019
- Last duration: 0.0 second(s)
- Avg duration: 0.00020 second(s)
- Total executions: 44
- Failed executions: 0
- OPC/Tag writes: 0
- DB writes: 308
- OPC/Tag write failures: 0

The status bar at the bottom indicates 'Project saved. (215 ms)' and '222 / 1024 mb'.

## Move Data Bidirectionally

The module uses transaction groups that function as a bidirectional data bridge between an OPC server and a SQL database. Transaction groups can perform many data-centric tasks, such as event logging, vertical and horizontal data storage, inserting rows into a table, storing data to a specific row.

## Log Data Easily

The easiest, most powerful data logger on the market includes triggers, handshakes, expressions, and other items that help you store data in the exact way you need. Triggers offer endless data-storage possibilities, such as storing production summaries, logging the sequence of event information, and tracking downtime events. Simply map your process data to any table structure and let the module do the work of creating and managing new tables or writing to existing tables.



## Synchronize PLCs with Databases

Extend your PLC address space into your SQL database with bidirectional mirroring, which immediately reflects any value change in the PLC or database end in the opposite end. Bidirectional mirroring enables real-time control via common web technologies and other database-compatible front-ends. Set the update rate for rows/fields (down to sub-second rates), and create two-dimensional arrays by adding rows. The SQL Bridge Module is the first and only software in the industry to offer this functionality.

## Build Recipe & Batching Systems

By extending your process into the database, the full bidirectional access of the SQL Bridge Module enables you to create a robust, customized recipe and batching system. Use the database to store a virtually unlimited number of recipes, and modify recipes however and wherever you want, while tracking all changes historically. Set up reliable database-to-PLC transactions using triggers and handshakes. Leverage stored procedures to perform complex tasks or replace aging transaction systems.



## Sequence Your Processes

Flexible triggers and database tables enable you to easily sequence entire processes. Use dynamic references to step the index to a row of values that are then written to the PLC. Create complex triggers, which reference multiple process variables and expressions, by using a simple expression language. Use rows/fields as timers and counters by leveraging the unique built-in hour meter and event meter functionalities.

## Flexible and Easy to Use

Across the board, SQL Bridge is the clear winner for tying industrial systems into SQL databases. Online editing lets you make changes on the fly, without stopping your process or affecting other parts of Ignition. You can stop locking data away in proprietary boxes because all data is open and accessible in the database. Use flexible data modeling without a lot of work: the module automatically creates tables and columns in any format. The built-in table browser allows you to work entirely within the Ignition Designer, so there is no need for external programs.

## Powered by Ignition

The SQL Bridge Module is a SCADA module for Ignition, the powerful HMI, SCADA, MES and MQTT software from Inductive Automation. It integrates seamlessly with Ignition and all other modules in the Ignition SCADA suite. Because the module is built on the power of Ignition, it shares the same advantages, such as cross-platform compatibility, unlimited free clients, robust out-of-the-box SQL database support, and fast installation. Leveraging the full power of Ignition, it is a data management tool unlike any other in the SCADA software market.

## Looking for No-Frills Data Logging?

SQL Bridge Limited provides an affordable way to create [Historical Groups](#), and record history into any SQL database. Speak to our Sales department for more details.

## Want to Learn More?

For more information on the SQL Bridge Module, please see the [SQL Bridge \(Transaction Groups\)](#) section of the manual.

# Reporting Module

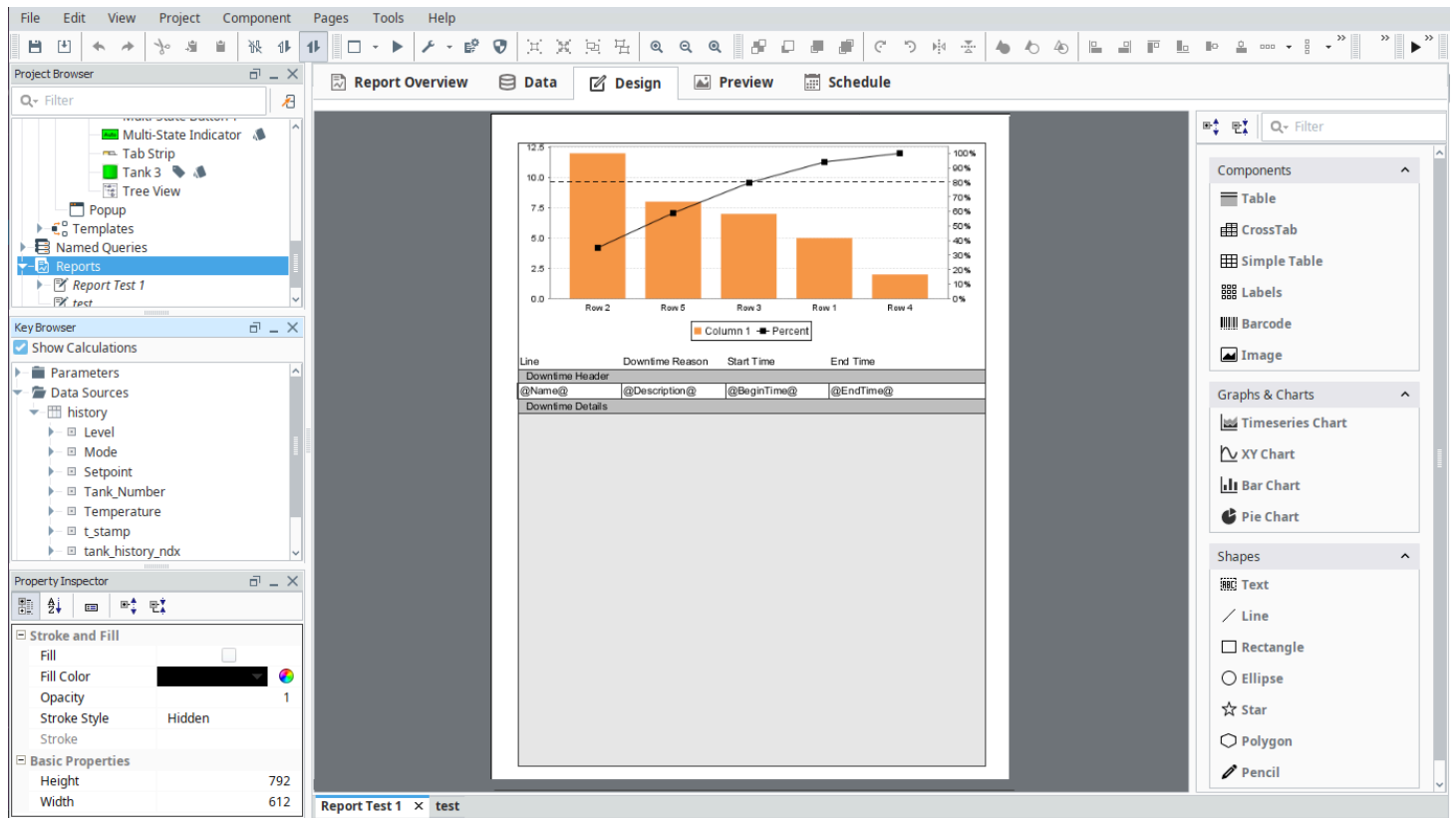


## Dynamic Report Generation

### Quickly and Easily Create Rich, Dynamic PDF Reports

Now it's easier than ever to make and distribute dynamic, professional reports in Ignition. The Ignition Reporting Module is a standalone reporting solution that simplifies and enhances the reporting process from beginning to end. Generate reports from existing files or create them from scratch. Pull data from a variety of sources, and design reports with a simple to use interface. Add charts, graphs, tables, crosstabs, shapes, and other components for visual impact. Save your reports in PDF, HTML, CSV, and RTF file formats, and set up automatic scheduling and delivery.

Use all of these powerful capabilities to quickly create many common types of reports such as production management, efficiency monitoring, downtime tracking, SPC, QA, OEE management, and historical data analysis.



## Select Data from Multiple Sources

The Reporting Module makes it easy to define the data behind your reports. Specify any number of report parameters and data sources in your reports.

Access information from any SQL database. Also, you can also easily query data from Ignition's Tag Historian and event data from the alarm journal.

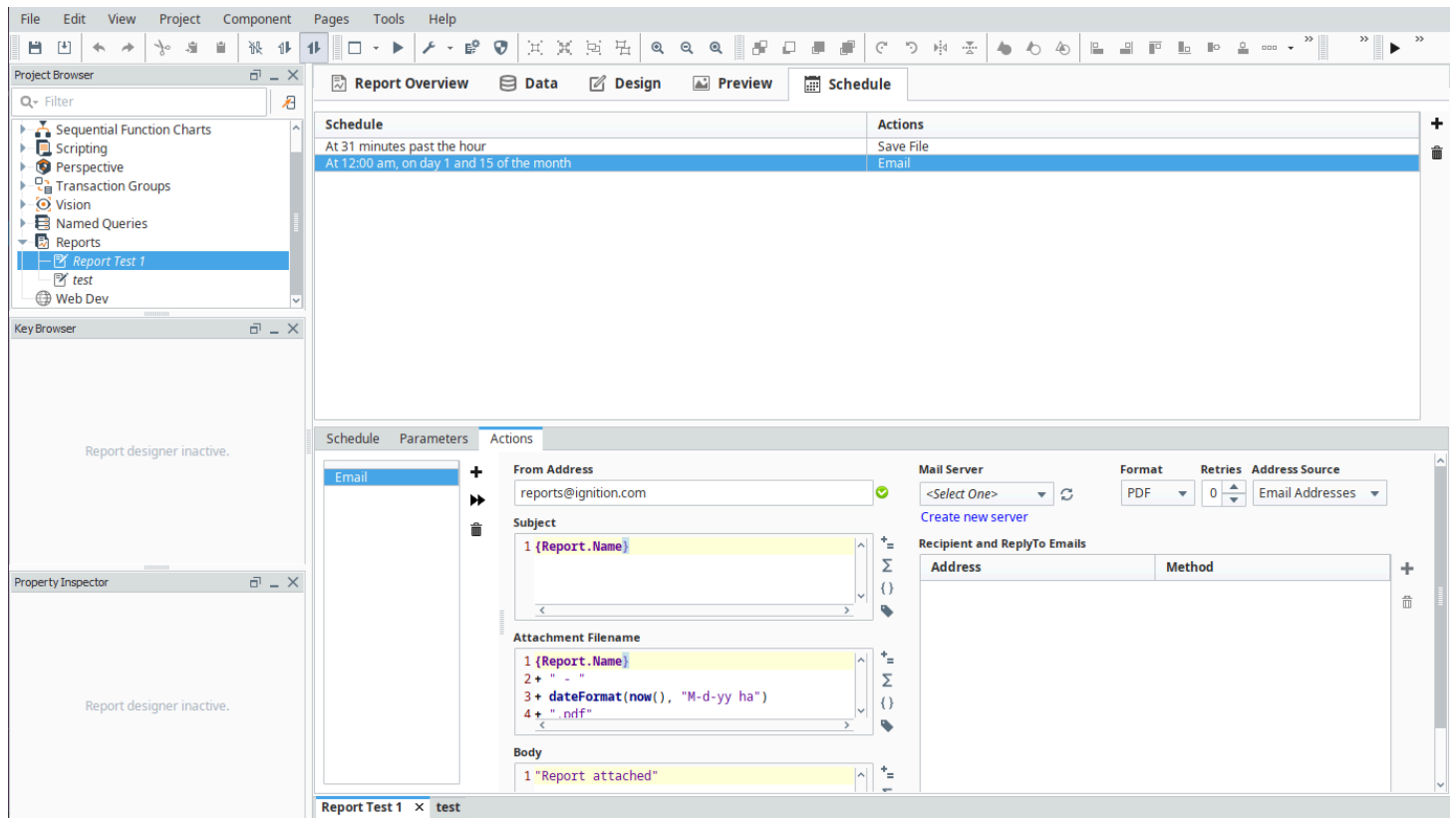
## Design Reports with an Easy-to-Use Interface

Design your reports easily inside Ignition's Designer application. The interface so user friendly because it enables you to design reports with the same intuitive feel and rapid application development tools that you get when designing applications in Ignition. This allows you to design your reports using the drag-and-drop method.

## Schedule Reports to Run Automatically

The Reporting module allows you to schedule reports within the Ignition Gateway. You can schedule a report to run on a regular basis; for example, on every Monday at 5:00 p.m. Then, your report will run as scheduled whether or not any Ignition clients are open.

You also have the option to set up triggered execution, which means that reports run on-demand when triggered by an event such as a tag change, a shift change, the finish of a production run, etc.

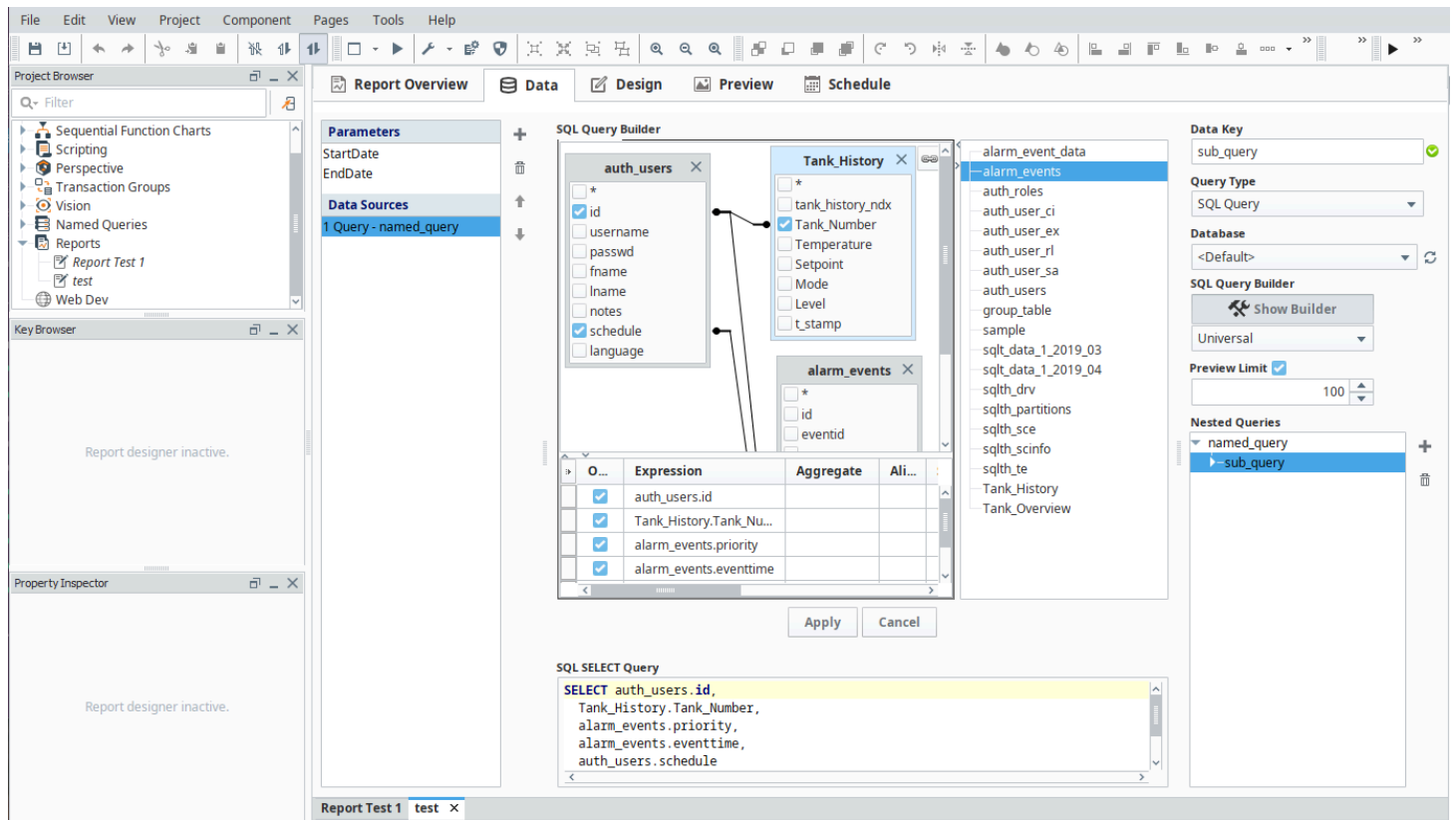


## Print, Send, or Save Automatically

Scheduled reports can be automatically delivered in many ways: print, email, save to a file server, upload to an FTP server, or use scripting to customize the method of delivery. Have your reports distributed in the way you want, every time, automatically.

## Powerful Query Tools

The Reporting Module has a powerful drag-and-drop query interface that allows you to build complex SQL queries easily. The new query structure allows you to create complex nesting which can correlate relational data and process historian data in a seamless fashion.



## Powered by Ignition

The Reporting module is a SCADA module for Ignition, the powerful software from Inductive Automation. The Reporting Module integrates seamlessly with Ignition and with all other Ignition modules. Because the module is built upon the power of Ignition, it shares the same advantages, such as cross-platform compatibility, unlimited free clients, robust SQL-database support, and fast installation. Leveraging the full power of Ignition, the Reporting Module is unmatched by any other SCADA reporting product on the market.

## Unlimited Options, Limited Price

The limited version of the Report module provides an affordable way to create and schedule just a few reports. Speak to our sales department for more details.

## Want to Learn More?

For more documentation on the Reporting module, please see the [Reporting](#) section.

# Alarm Notification Module



## Alarm Notification

### Manage SCADA Alarm Notifications Any Way You Choose

The Ignition Alarm Notification module enables you to configure the logic for how, why and when alarm notifications are delivered, manage alarm notification for groups of users, and send notifications via email. Notifications can be easily be acknowledged by the recipient via email.

### Control Your Alarm Notification Logic

Ignition's alarm notification pipeline feature is an innovative tool that lets you easily chart out the routing of your alarms. Make your alarm notification logic as simple or as multifaceted as you want. Prevent alarm flooding by directing the right alarms to the right people at the right time.

With Ignition and the Alarm Notification module, you'll have greater control of what happens between when an alarm or alert goes active and when it is sent out to personnel, and of who gets alarm notifications and when.

By using a simple drag-and-drop interface, you can build various types of alarm notification logic, including:

- **Delay:** Hold off on sending notifications until nearby operators are given time to deal with the problem first.
- **Escalation:** Elevate alarm notification when operators are not handling alarms.
- **Consolidation:** Combine multiple alarms into a digested message.
- **Selection:** Distribute different alarms to different groups of contacts.

### Escalation:

Send higher priority alarms to a different contact or group.

### Consolidation:

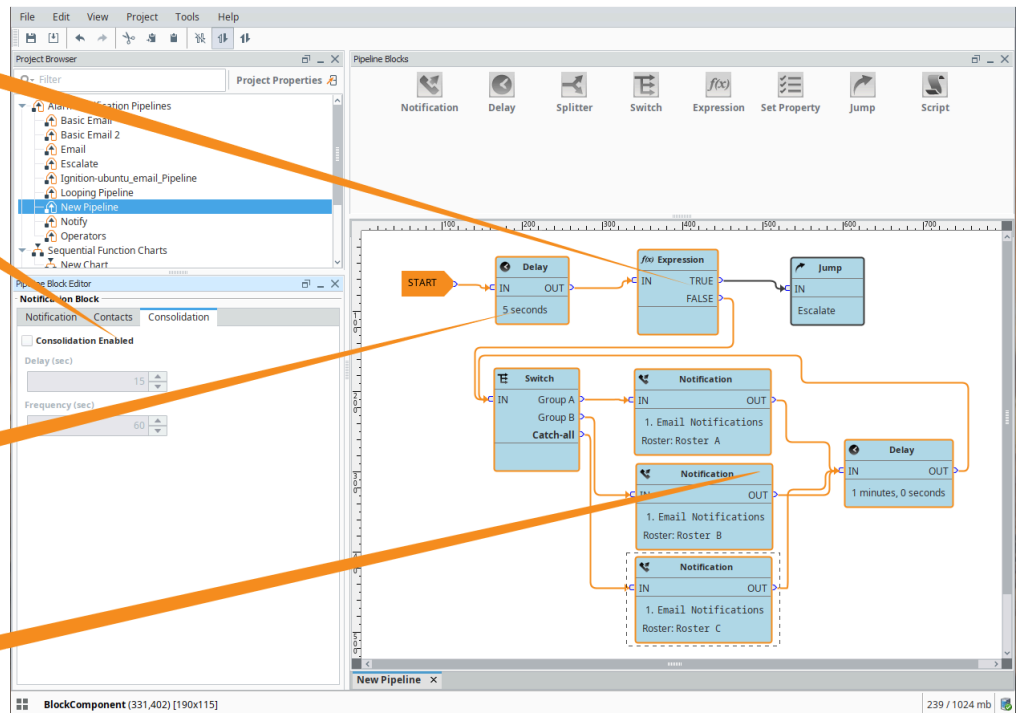
Combine multiple alarms into a digested message.

### Delay:

Hold off on sending notifications until nearby operators are given time to deal with the problem.

### Selection:

Distribute different alarms to different groups of contacts.



## Manage Users & Schedules to Ensure Timely Delivery

Make sure the right people – and especially those on shift – get notified quickly. The Alarm Notification Module lets you organize individuals into groups based on their roles with the On-Call Roster feature.

Config > Alarming > On-Call Rosters

💡 Click the right arrow on each user in the user source column (left) to move them to the on-call list (right). Re-order the users on the on-call list using the up and down arrows to control who gets called first.

All Users from

manage

|                                                                                                    |   |
|----------------------------------------------------------------------------------------------------|---|
|  bonnie lund    | → |
|  jessica lane   | → |
|  Karlin Trejo   | → |
|  millan douglas | → |
|  opcuauser      | → |

[Add All >](#)

On-Call Roster

|          |   |   |
|----------|---|---|
| ✕ admin  | ↓ | ↑ |
| ✕ arthur | ↓ | ↑ |
| ✕ susan  | ↓ | ↑ |
| ✕ wade   | ↓ | ↑ |

Save

When an alarm notification needs to be sent, it goes to a designated call roster and then the system evaluates individual schedules so that only those currently on shift will be notified. You can easily change schedules, assign roles and specify who should be notified when alarms pass through different notification blocks in the pipelines.

The Alarm Notification module lets you edit rosters in the client in real time and to edit individual schedules right in the authentication profile. With permission roles, you can let individuals edit their own information on-the-fly to account for irregular time away from work so that alarms will skip over them and be sent quickly to an available person.

## 2-Way Email Notification

With the Alarm Notification Module, users in your organization can receive and acknowledge alarm notifications by email.

## Let's Get Started!

Learn more about alarm notifications in the [Alarm Notification](#) section.



# SMS Notification Module



## SMS Alarm Notification

### Add SMS Functionality to Your Alarming System

Quickly let key people know about any alarm by sending a text message to any cell phone. The Ignition SMS Alarm Notification module enables both alarm notification and acknowledgment via text messages. You can enable phone-call alerts by adding the Voice Notification Module to your Ignition system.

### Notify Users Quickly with a Text Message

By adding the SMS Notification module to Ignition, you can send and acknowledge alarm notifications via text messaging. SMS notification is an efficient and immediate method that makes it easier for users to respond to alarms no matter where they are.

This module requires the [Alarm Notification module](#) and a cellular modem.



## Get Started

Read more about this module on the [SMS Notification Profile](#) page.



# Web Dev Module



## Use Web Services in Ignition

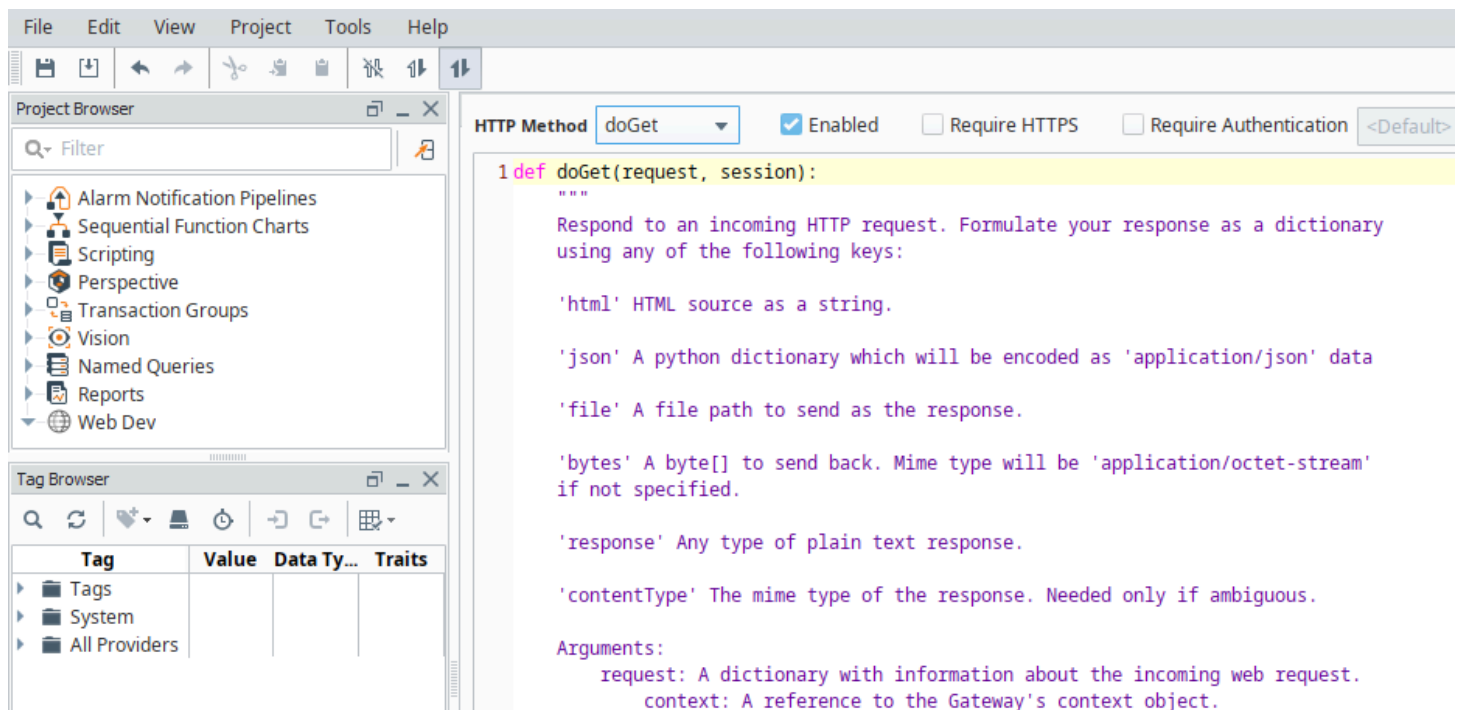
### Host a Web Page on an Ignition Gateway

This module enables you to directly program against the web server inside the Ignition Gateway. Webpages can be built by hand using a combination of Python programming and static web resources such as images, CSS files, javascript files, and html files. You can design and host custom web pages directly against the Ignition service.

### Configure Custom Web Service Calls

External systems can interact with the Ignition service through web service calls using the Web Dev module. Allow SAP and ERP systems to request data directly from Ignition by developing a custom, full-fledged, API.

More Information on the Web Dev module can be found on the [Web Dev](#) page.



## Barcode Scanners and Web Enabled Devices

Many newer barcode scanners are web-enabled and don't use serial ports to connect. For these types of scanners you can use the Web Dev module to write whatever connect functions that you need. This opens up a whole new world of possibilities for connecting to various mobile devices.

# Enterprise Administration Module



## Enterprise Administration

### Enhance the Reach of Ignition

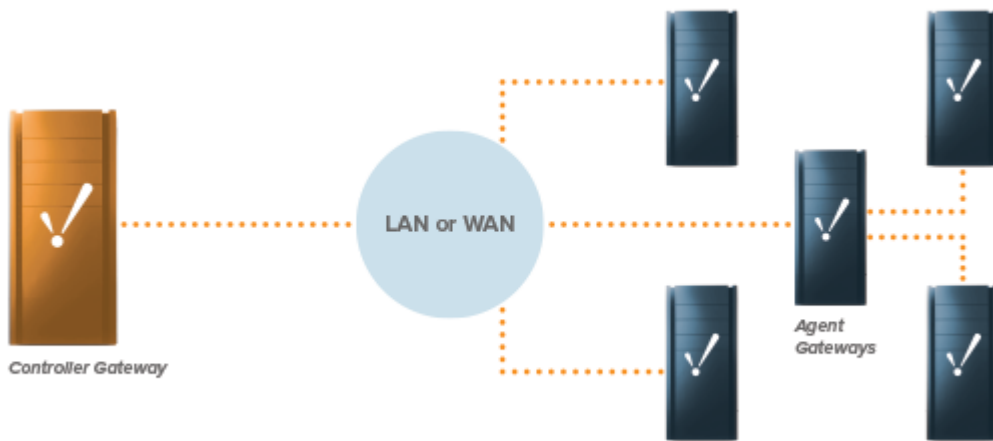
The Enterprise Administration module (EAM) provides a secure and intuitive way to manage many Ignition installations from one location. It is ideal for large enterprises that deploy multiple Gateways across vast geographical distances, but even companies with a few Ignition Gateways on a single plant floor can benefit from its ability to synchronize projects, monitor performance, and automate backup and recovery from a central location.

### Manage Multiple Gateways from One Gateway

With the EAM module installed, an Ignition Gateway can function as the central Controller Gateway that connects with, monitors, and manages any number of remote Agent Gateways. Use the Controller Gateway to coordinate and automate many administrative tasks for Agent Gateways, including:

- Assigning, updating, activating, and unactivating licenses
- Deploying new and updated modules
- Disaster Recovery
- Remote Backups

All of these actions can be executed immediately or scheduled for later.



## Synchronize Projects and Resources

The EAM gives you the ability to design resources and projects centrally in the Controller Gateway and send them out to the Agent Gateways.

## Communicate Over a Secure Network

The EAM is built on a high-performance, high-security communication network that facilitates simultaneous access to multiple Gateways. Connect multiple Ignition Gateways using the Gateway Network and all copies of Ignition will be able to communicate freely.

## Monitor Agent Health and Performance

In the Controller Gateway, the EAM provides health indicators for Agent Gateways and alarms for impending lifecycle events such as Agent Gateway failure. Memory usage notifications, warnings, and error events are also provided.

## Automate Gateway Backup and Recovery

The EAM enables automated backup and quick recovery for all Gateways through a Gateway backup archive.

## Powered by Ignition

The EAM is a SCADA module for Ignition, the powerful HMI / SCADA software from Inductive Automation. The EAM integrates seamlessly with Ignition and all other modules in the Ignition SCADA suite. Because the module is built on the power of Ignition, it shares the same advantages, such as cross-platform compatibility, unlimited free clients, robust out-of-the-box SQL database support, and

fast installation. Leveraging the full power of Ignition, it is an enterprise management tool unlike any other in the SCADA software market.

# Get Started

Read more about EAM in the [Enterprise Administration](#) section.

# SFC Module



## Sequential Function Charts

**Streamline the creation, organization, and visualization of robust logic systems.**

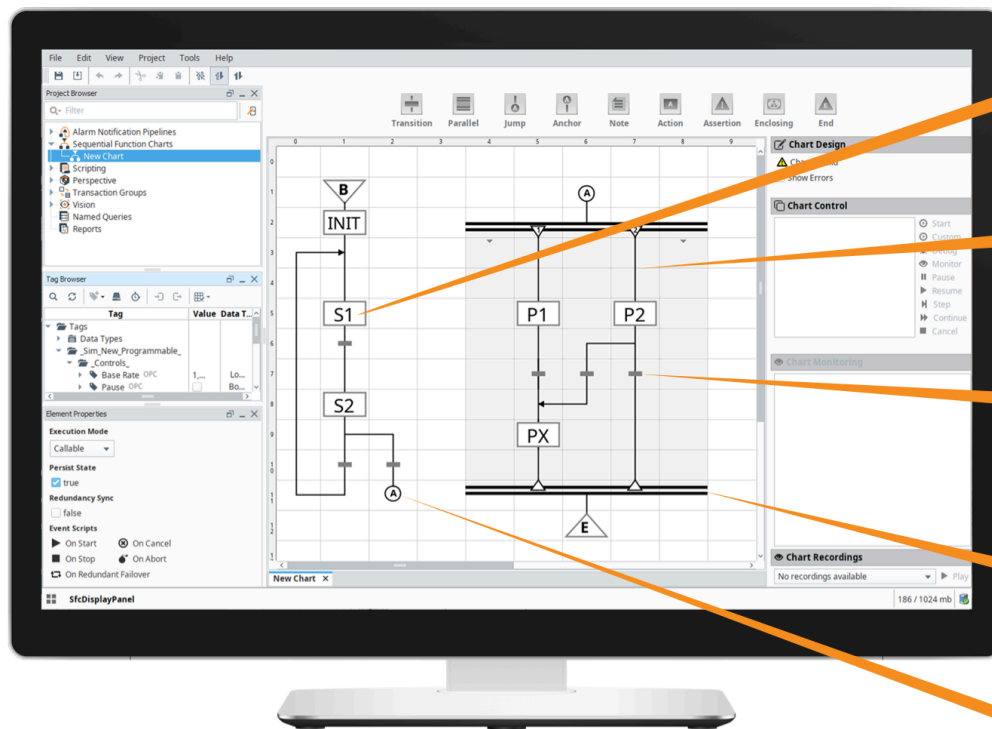
The Ignition SFC module's powerful visual programming language allows you to write complex logic in a simpler, more intuitive way. The SFC Module works seamlessly with Ignition, and represents a leap forward in the capabilities of the software.

## Visual Logic Programming

The SFC module's visual, drag-and-drop programming tool makes the process of writing complex logic much smoother than using the basic Python scripts included in Ignition. Its standardized programming method, part of the IEC 61131-3 specification, will be familiar to many users who have experience in programming PLCs. With a simple visual interface, you can use steps, transitions, parallel blocks and other drag-and-drop elements to create complex charts. SFCs within Ignition can make use of scripts, Tags, and other elements already available in the Ignition platform.

- **Steps:** These elements perform a variety of useful functions.
- **Directed Links:** Use these to connect steps and other transitions to each other.
- **Transitions:** Conditions that evaluate to true or false, either allowing the flow to proceed or blocking it.
- **Parallel Branches/Syncs:** Use these to set up parallel actions.
- **Jumps:** Set up connections without crossing links.





#### Steps:

These elements perform a variety of useful functions.

#### Directed Links:

Use these to connect steps and other transitions to each other.

#### Transitions:

Conditions that evaluate to true or false, either allowing the flow to proceed or blocking it.

#### Parallel Branches/Syncs:

Use these to set up parallel actions.

#### Jumps:

Set up connections without crossing links.

Drag and drop powerful components to create robust logic systems.

## Chart Monitoring

You can monitor charts visually in the Ignition designer and clients, watching each chart execute its logic, down to which specific step is currently running. You can even inspect the chart's internal variables as it runs. The visual nature of SFCs make them much easier to troubleshoot than Python scripts.

## Build Robust Logic

Now it takes far less time to build any type of robust logic your enterprise may need: long-running tasks, parallel tasks, tasks that pause for certain conditions before proceeding, loops, and sub-charts.

## Multiple Chart Instances

The module allows you to instantiate multiple instances of any chart. Each instance can be configured with different starting parameters, allowing the instances to be independent from each other.

## Long-Running Charts

Charts may be designed to run for a very long time. They can even keep running if a Gateway is restarted by pausing on shutdown and resuming on startup. SFCs also support redundant Ignition setups to ensure the chart keeps running even if the primary Gateway fails.

## Powered by Ignition

The SFC module is a SCADA module for Ignition, the powerful, award-winning, HMI / SCADA software from Inductive Automation. The SFC Module integrates seamlessly with Ignition and with all other modules in the Ignition SCADA suite. Because the module is built upon the power of Ignition, it shares the same advantages, such as cross-platform compatibility, unlimited free clients, robust out-of-the-box SQL database support, and fast installation. Leveraging the full power of Ignition, it is a SCADA logic engine unlike any other on the market.

## Learn More

Documentation on the SFC module is available in the [Sequential Function Charts](#) section.

# JDBC Driver Modules

JDBC drivers are leveraged by Ignition to offer a standardized set of functionality on a wide range of different systems and databases. Although you can always [add JDBC drivers](#) based on your database needs, three separate JDBC Driver modules are included out of the box with an Ignition installation:

- MariaDB JDBC Driver (version 3.3.3)
- MSSQL JDBC Driver (version 9.4.0.jre11)
- PostgreSQL JDBC Driver (version 42.7.2)

## Connecting to Supported Databases

Once the module is installed, the JDBC driver configurations are automatically created and added to the **Connections > Database > Settings** page. This allows you to immediately connect to various databases, such as MySQL and Microsoft SQL. Further configuration changes are available on the Gateway's Settings page as needed for your connection.

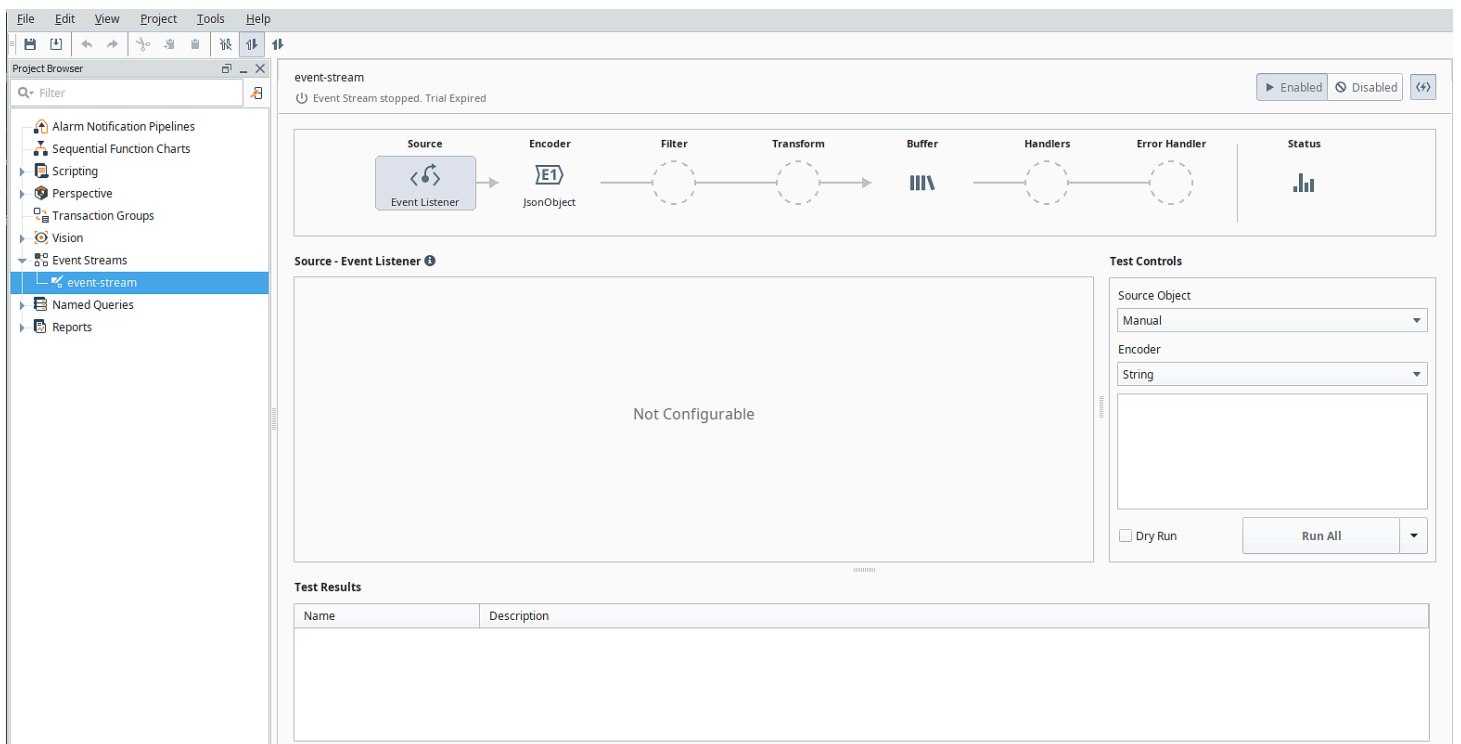
Read more about these modules on the [JDBC Drivers](#) page to get started.

# Event Streams Module



The Event Streams module reduces the complexity of handling data by providing the event streams resource, which streamlines data manipulation into stages. Unlike other mechanisms that handle data such as SQL databases, event streams are primarily event-driven or subscription-based, meaning no active solicitation of data is needed.

With this module, users are able to filter, transform, and react to those events in various ways from the Designer.



The screenshot displays the Event Streams module interface within a software designer. The main workspace shows a workflow diagram with the following stages: Source (Event Listener), Encoder (JsonObject), Filter, Transform, Buffer, Handlers, Error Handler, and Status. The Source stage is expanded, showing a large area labeled "Not Configurable". The Test Controls panel on the right includes a "Source Object" dropdown set to "Manual", an "Encoder" dropdown set to "String", and a "Run All" button. The Test Results table at the bottom is empty.

| Name | Description |
|------|-------------|
|------|-------------|

## Want to Learn More?

For more information on the event streams, see the [Event Streams](#) section.

# Additional Modules

Enhance Ignition's capabilities beyond traditional SCADA and HMI limits. These additional modules provide Ignition with even more functionality. Take your project to the next level with these powerful modules.

## Voice Notification



Enable both alarm notification and acknowledgement via a phone call.

## OPC COM



Integrate Ignition with Classic COM-based OPC Servers.

## OPC COM Tunneller



Exposes OPC servers accessed through the OPC-COM module to Ignition's OPC-UA server, allowing you to easily expose tags from a DA server to any UA server.

## Twilio Notification



Adds integration with Twilio via SMS, Voice, and WhatsApp Alarm Notification Profiles and their related scripting functions.

## SECS/GEM



Communicates with semiconductor fab equipment.

# Voice Notification Module



## Text to Speech Alarm Notification

### Send Notifications Via a Phone Call

Ensure no serious issue is overlooked by speeding alarm notification delivery to the right people as soon as possible. The Ignition Voice Notification Module uses state of the art text-to-speech technology to add phone-call notification to your alarming/alerting process.

Set up voice notification for alarms in Ignition with the Voice Notification module. Use text-to-speech (TTS) technology to notify users of an alarm via a phone call and to allow users to acknowledge it with a simple key press. The VoIP-over-SIP voice notification system can be tied in with a VoIP phone system or online VoIP service, or bridged to a standard phone line using an existing phone gateway.

The Voice Notification module adds the ability to deliver alarm notifications to users via telephone, using any SIP compatible phone system. Messages are constructed in text, and are delivered through a high quality text-to-speech engine.

#### NOTE

The Voice Notification module requires that the Alarm Notification module is also installed on the same Gateway.

### Two-Way Acknowledgement

The Voice Notification module can be configured to allow users to quickly acknowledge alarms. With the Two-Way property enabled, the notification is sent out a response code in the message. The user simply replies with the response code and the alarm will be acknowledged.

# Custom Notification Messages

The high quality Text-to-Speech Engine allows you to customize the alarm message the user hears, so you are not limited to a number of pre-recorded messages.

## Audit Log Integration

The Voice Notification module can be configured to log successful message delivery and user acknowledgement into any connected database. Once recorded, a simple query will return all notification activity.

## Multi-Language Support

Write your messages in any of the provided languages. A list of the available languages can be found on the [Voice Languages](#) page.

### NOTE

This module requires the Alarm Notification module and some SIP-compatible VoIP service, such as your office VoIP server, Skype Connect or an IP Telephony Gateway appliance to bridge to a standard phone line (not included).

Examples of an IP Telephony Gateway appliance include:

- Atcom IP02/IP04 (the number indicates the phone lines. Ignition can only use 1 line at a time)
- Grandstream HT-503
- GXW410x (It is the FXO port that connects to the phone line)



# OPC COM Module



## Connect to Legacy Devices

The OPC COM module offers Ignition the ability to connect to legacy ("classic") COM-based OPC DA servers. It supports OPC DA 2.0 and 3.0.

### NOTE

The [OPC Com Tunneller module](#) simplifies connecting to remote OPC-COM servers.

## Connecting to Classic OPC Servers

With the OPC-COM module installed, there will be a new option for COM-based OPC servers when creating a server connection in the Gateway. The OPC-COM module is primarily intended for use with local OPC servers, although it also provides basic support for remote connections.

Even when connecting locally, the application may run into the traditional difficulties of connecting to Windows based OPC servers. DCOM security settings on the machine can interfere with connections, and the OPC Core Components package (from the [OPC Foundation](#)) must be properly installed before connections can be established.

## Using Data from Classic OPC Servers

After a connection to a server has been defined, the server will appear along side of other OPC servers (both COM and UA based) in the OPC Tag Browser. You can use these tags like any others - bring them into Ignition's Tag Browser, use them in Transaction Groups, and so on.

# OPC COM Tunneller Module



## Create Remote Connections through OPC-UA



Knowledge  
Base

### OPC Com Tunneller

Learn how to configure the OPC Com Tunneller module.

[Link to Knowledge Base Article](#)

## Simplify COM Connections

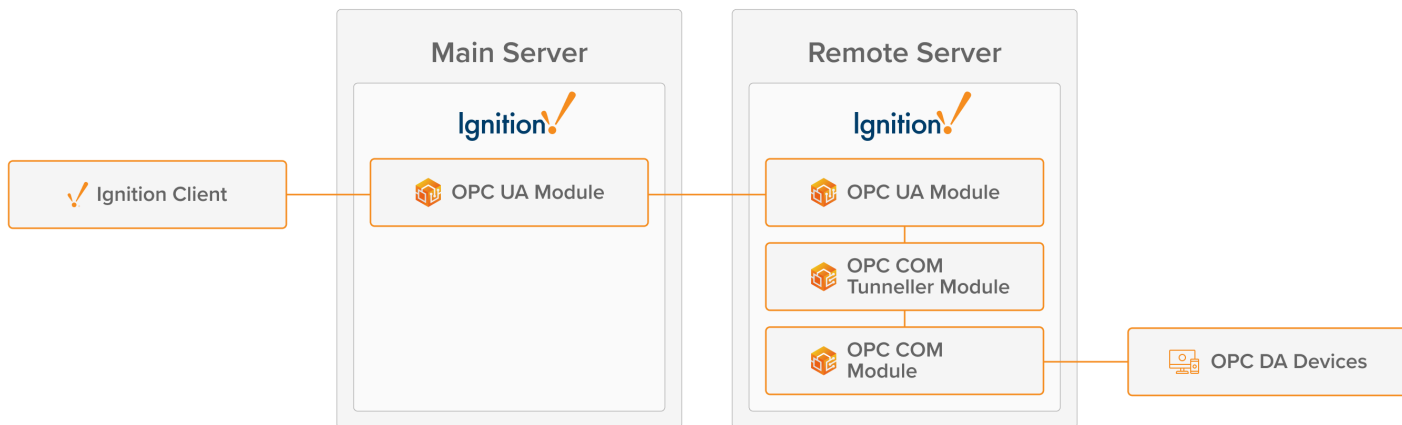
The OPC COM Tunneller module allows you to access remote OPC COM servers over the network without using Remote DCOM. It exposes local COM connections to Ignition's OPC UA server, so OPC UA clients can access them using modern protocols.

### NOTE

The OPC COM Tunneller module requires the OPC COM module to be installed and licensed.

## Modernize COM Servers

The module manages the COM connection internally and translates it into the OPC UA protocol. This enables secure communication using TCP, with support for encryption and authentication, and simplifies access to legacy COM servers.



# Twilio Notification



The Twilio Integration and Alarm Notification module enables SMS and voice alarm notification and acknowledgement capabilities with Twilio using the following notification profiles:

- [Twilio SMS Notification](#)
- [Twilio Voice Notification](#)
- [Twilio WhatsApp Notification](#)

Additionally, this module unlocks the `system.twilio` functions. See the [system.twilio](#) section of the appendix for more details.

## NOTE

The Twilio Notification module requires that the Alarm Notification module is also installed on the same Gateway.

No additional hardware is required, so there is no need to worry about firmware updates or hardware failure. More information on using the Twilio Integration and Alarm Notification module can be found on the [Twilio Notification Profiles](#) page.

## Send SMS Messages through Scripts

Integration with Twilio via an [Twilio SMS Notification Profile](#) sends SMS alarm notifications without a physical device.

# Send Voice Notifications with a Phone Call

Creating a [Twilio Voice Alarm Notification Profile](#) allows you to configure a custom message delivered as an automated phone call when an alarm is triggered. The alarm can then be acknowledged through the phone call.

## Send WhatsApp Notifications

A [Twilio WhatsApp Notification](#) profile allows WhatsApp notifications to be sent. Template and free-form messages can be configured.

# SECS/GEM Module



## Communicating with Semiconductor Fab Equipment

Ignition's SECS/GEM module is a highly specialized module that provides the ability to communicate with semiconductor fab equipment using the SECS-II, GEM, and HSMS standards. The SECS/GEM module is implemented as a host that can talk to one or more fab tools via equipment connections configured within the Ignition Gateway. It also provides the capability to create and configure equipment simulators that can be used for testing applications which is a big plus when getting started with the SECS/GEM module. Connections are made over Ethernet using TCP/IP (HSMS protocol) or over a direct serial connection (SECS-I protocol) using a RS-232 cable. Once installed, the SECS/GEM functionality is fully integrated into the Connections section of the Gateway Webpage where you can configure connections to the equipment, and set up equipment simulators.

The SECS/GEM module provides the framework to create and configure a common set of scripting functions to control equipment behavior and communication capabilities that monitor and support semiconductor manufacturing equipment. Through scripting, it provides the flexibility to start and stop equipment processing, set equipment configuration parameter values, collect data, send alarms to the host, and select recipes, as long as the host and OEM adhere to SECS/GEM standards.

Communication between Ignition and the equipment is in the form of SECS messages defined by the SECS-II standard. SECS messages are typically sent and received using scripting functions within Ignition using the SECS/GEM defined messages, SECS Definition Language (SDL), that are loaded into the equipment. SECS messages that contain data can also be written to tags, updating the tag's values as new messages come in. This functionality is used to capture data coming back from equipment, such as tool traces within S6F1 messages. The default SDL file that is included with the SECS/GEM module is already configured to create tags for S6F1 messages sent to the module from the tool. For other messages, the SECS/GEM module can be configured to update tags by adding some additional parameters to the equipment's SDL file.

To learn more, refer to the [SECS/GEM](#) section.

# Connector Modules

Connector modules expand Ignition's functionality, allowing users to connect to NoSQL databases such as MongoDB.

## MongoDB



Allows you to connect Ignition to a NoSQL MongoDB instance.

## Kafka



Allows you to receive and send Kafka events and records through Ignition.



# MongoDB Connector



## Easy and Responsive NoSQL Option

The MongoDB Connector allows you to connect Ignition to MongoDB, which is a scalable, document-oriented NoSQL database. Many existing features in Ignition, such as the Tag system, Python scripting system, and Perspective data are compatible with document-style data, making MongoDB integration into Ignition seamless and easy.

This connector is a part of a series of modules called Cloud Connectors. Cloud Connectors are bundled with Ignition Cloud Edition, as they leverage technology frequently associated with cloud-based architectures. Additionally, standard versions of Ignition will also be able to take advantage of the MongoDB Connector's features as a module add-on. This add-on can be found on [Inductive Automation's downloads page](#), under **Cloud Connectors**. The MongoDB Connector is not available for Ignition Edge or Ignition Maker Edition.

## MongoDB Connection Management

[Connect to specific collections hosted on MongoDB](#) by specifying connection schemes, hosts, and properties, along with a username and password for authentication. Enabling and disabling connections is possible and simple with just a toggle. You can also view connectivity status and obtain diagnostic information through the Gateway webpage's Status UI.

## Write and Query Data

Modify and view data with easy-to-use system functions that allow you to perform a range of actions, such as inserting data, updating data, deleting data, and more. The [system.mongodb](#) functions also

utilize Ignition's scripting autocomplete feature, making these functions simple and straight-forward to use.

## Enhance Your Perspective Experience

The MongoDB Connector adds a new **binding type** to Perspective components. Aptly named MongoDB, this binding type makes it easier to query data from your collections and integrate the results into your Perspective project. Users can choose between Find, FindOne, or Aggregate query types, making MongoDB bindings versatile and adaptable to many situations.

Edit Binding: Table.props.data

Binding Type

Tag

Property

Expression

Expression Structure

Query

Tag History

HTTP

MongoDB

Remove Binding

Configure MongoDB Binding

Connector

MongoDB Atlas

Collection

data

Query Type

Find

Query

filter {0}

+ Add Object Member...

project {0}

+ Add Object Member...

sort {0}

+ Add Object Member...

collation {0}

+ Add Object Member...

limit : 10 fx

skip : 0 fx

Options

☒ Enabled

☐ Overlay Opt-Out

☒ Cache & Share

☐ Polling

fx

sec

Add Transform +

☒ Binding Preview

MongoDB

info

 [{"\_id": "5553a998e4b02cf715...}

OK

Cancel

Apply

# Want to Learn More?

For more information on the MongoDB Cloud Connector, see the [MongoDB](#) page.

# Kafka Connector

## Convenient and Efficient Event Data Streaming

The Kafka Connector allows you to process event stream data received from a Kafka source, or publish event stream data to a Kafka topic. Kafka source data can also be sent to both internal subsystems, such as Gateway Events, or external applications, such as a database. Users can also receive non-Kafka source data and send it to Kafka topics.

This connector is a part of a series of modules called Cloud Connectors. Cloud Connectors are bundled with Ignition Cloud Edition, as they leverage technology frequently associated with cloud-based architectures. Additionally, standard versions of Ignition will also be able to take advantage of the Kafka Connector's features as a module add-on. This add-on can be found on [Inductive Automation's downloads page](#), under **Cloud Connectors**. The Kafka Connector is not available for Ignition Edge.

## Kafka Connection Management

[Create Kafka connections](#) from the Ignition Gateway by specifying settings such as bootstrap server hosts and ports, clients, consumer and producer configurations, and more. Kafka connections can also be enabled and disabled with a simple toggle.

## Produce and Consume Records

Receive and publish records from topics using the system functions that allow you to poll data, send records, list information, and more. The [system.kafka](#) functions can also be used with Ignition's scripting autocomplete feature, making the functions easy to understand and use.

## Want to Learn More?

For more information on the Kafka Cloud Connector, see the [Kafka](#) page.

# Startup Guide

Ignition can seem like an overwhelming system of connections and data. This section outlines how to install Ignition, demonstrates some of the most common tasks in Ignition, and provides a guide on creating a basic project using those tasks.

## **Downloading and Installing Ignition**

This document explains how to download and install Ignition.

## **Designing a Project**

This document follows the Downloading and Installing Ignition guide from the previous section and assumes you...

# Downloading and Installing Ignition

This document explains how to download and install Ignition.

## Downloading and Installing Ignition

This section is a simple guide on how to install Ignition using the installer from the Inductive Automation website. To see more information and other ways of installing Ignition, see the [Installing and Upgrading](#) page.

** BEFORE YOU INSTALL IGNITION, MAKE SURE YOU MEET THE MINIMUM SYSTEM REQUIREMENTS:**

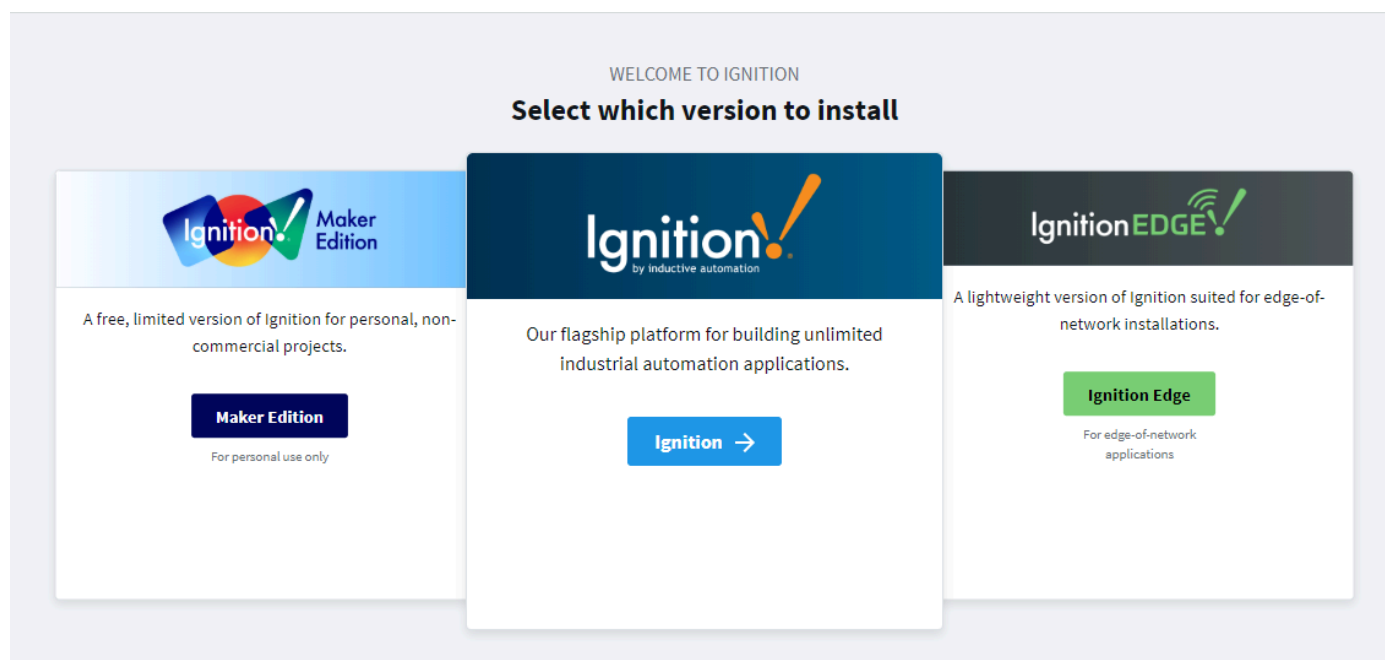
- Dual-Core Processor (32 or 64 bit)
- 4GB RAM
- 10GB free HD space

Also, ensure you have Administrator privileges to run the Ignition installer.

## Commissioning the Gateway

1. Go to the Inductive Automation website at [www.inductiveautomation.com](http://www.inductiveautomation.com), then click **Download Ignition** in the upper right corner of the page. Your web browser automatically detect which operating system you're running. Since this guide uses Windows, we will use the Windows installer.
2. Run the downloaded Ignition install wizard. Click **Next** on the Welcome page to proceed with the installation.
3. You will be prompted to specify the installation directory and Gateway Service Name. In this example, we will use the default options. Click **Next**.
4. Select the installation option you want to use. This example will use **Typical** to get the default modules Ignition comes with. Click **Next**.
5. The wizard is now ready to install Ignition. Click **Install** to start the installation process.
6. Once Ignition has successfully been installed, click **Finish** to launch the Ignition Gateway.

7. You will be presented with three versions of Ignition to choose from. In this example, we will use the **Standard Edition**.



**i NOTE**

Ignition Maker Edition is for personal, non-commercial use. See the [Ignition Maker Edition](#) page for more details.

Ignition Edge is a light version of Ignition intended for on field and edge-of-network use. See the [Ignition Edge](#) page for more details.

8. The **End User License Agreement (EULA)** window will be displayed. Click the button acknowledging you read and agree with the terms and conditions, then press **Next**.
9. You will then need to create your first user. Keep in mind that this first user will be the administrator account with full privileges in Ignition. Enter a **username** and **password**, confirm the **password**, and then click **Next**.
10. You will be prompted to select which ports the Ignition Gateway will use. During the commissioning process, the Gateway will check the specified ports for availability, and increment the port number until the next available port is found. In most cases, leaving the default port values on this page is recommended. Once you have specified which ports to use, click **Finish Setup**.

**i NOTE**

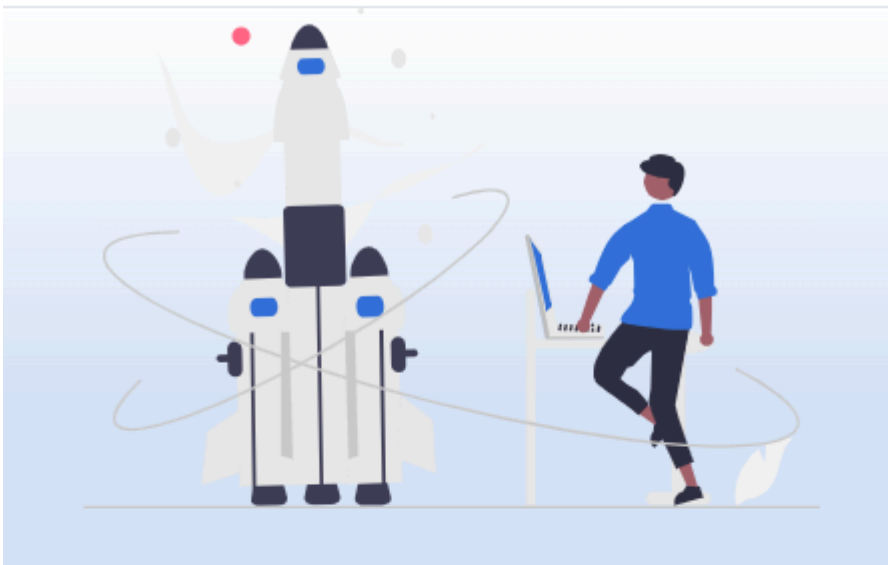
The default port values are:

- HTTP: 8088

- HTTPS: 8043
- Gateway Network: 8060

11. Click **Start Gateway** to begin the commissioning process.
12. Once the Gateway finishes commissioning, you will be prompted to enable Quick Start. Quick Start contains different preconfigured resources and connections. For this example, we will select **Yes, Enable Quick Start**.

## Enable Quick Start



Get your Ignition installation up and running with example applications, device connections, sample tags, and a configured Gateway. Recommended for new users.

### Quick Start Includes

- ◆ Sample application
- ◆ Device simulator
- ◆ Tags and Tag historian
- ◆ Internal alarm journal

No thanks, I'd like to start from scratch

**Yes, Enable Quick Start**

**i NOTE**



You cannot enable Quick Start past this point if you selected the option to start from scratch. If you decide that you would rather like to have the preconfigured resources Quick Start provides, [restore](#) the Gateway backup located [here](#).

13. You will be prompted to log in. Use the credentials you set in step nine to log in.
14. After logging in, Quick Start will automatically begin initializing resources, including a **Device Simulator**, **tags**, a **Historian**, and an **Internal Alarm Journal**. We will be using these resources in the **Designing a Project** section of this guide.
15. Once the Quick Start process is complete, your Gateway will be ready to use. If you are accessing the Gateway on the machine it is installed on, you can get to the Gateway by going to <http://localhost:8088> and signing in with the credentials created in step nine.

Home

Welcome

Designer

Perspective

Vision

Platform

Connections

Network

Services

Diagnostics

## Welcome to Ignition

[Launch Designer](#)

| Gateway Overview |             |                         |              | <a href="#">View Details</a> |
|------------------|-------------|-------------------------|--------------|------------------------------|
| Gateway Name     | Redundancy  | Gateway Version         | Gateway Mode |                              |
| My Gateway       | Independent | 8.3.0-rc1 (b2025082609) | N/A          |                              |

### Gateway Notes

[Edit Notes](#)

Welcome to your Ignition Gateway. This customizable area is intended to capture the critical details you want to document for this Gateway. You might include information about the environment (production, testing, or development), key workflows, or maintenance schedules. It's also a great place to list instructions for your team, important reminders about system health, or details about your configuration that require regular review. Use this space to keep everyone informed and ensure smooth operations across the board.

### Downloads

**Designer Launcher**  
Bring all your data, systems and developers together into one simple, integrated development environment. [→](#)

**Perspective Workstation**  
Open Perspective Sessions from any [→](#)

### Ignition Resources

Browse our extensive product documentation and free online training university for answers to all of your questions.

#### Kickstart Your Learning

Check out Inductive University and learn the Ignition Platform at an industry-ready level.

[Go to Inductive University](#)

#### Share, Download, & Create

Go to the Ignition Exchange to download and post assets or entire projects.

[Browse Resources](#)

#### NOTE

The 8088 port may be different if you chose to use different ports than the default in step 10. If it is, you can access the Gateway using the port you configured instead of 8088.

# Downloading and Installing the Designer Launcher

To begin designing a project, you will first need the **Designer Launcher**, which is found on the Gateway Webpage.

The Designer Launcher is simply a location to consolidate the different Gateways you can connect to and create projects for within your network, including remote Gateways. It is convenient to have if you want to connect to multiple Gateways.

**NOTE**

Alternatively, you can use the **Launch Designer** button on the top right of the Gateway Webpage to launch the Designer directly. Go to step **x** if you want to skip using the Designer Launcher.

1. On the Gateway Webpage, click on **Designer Launcher** in the Downloads category. This will bring you to the **Download** page for the Designer.

Welcome to Ignition

Launch Designer

Gateway Overview

View Details

| Gateway Name | Redundancy  | Gateway Version         | Gateway Mode |
|--------------|-------------|-------------------------|--------------|
| My Gateway   | Independent | 8.3.0-rc1 (b2025082609) | N/A          |

Gateway Notes

Edit Notes

Welcome to your Ignition Gateway. This customizable area is intended to capture the critical details you want to document for this Gateway. You might include information about the environment (production, testing, or development), key workflows, or maintenance schedules. It's also a great place to list instructions for your team, important reminders about system health, or details about your configuration that require regular review. Use this space to keep everyone informed and ensure smooth operations across the board.

Downloads

Designer Launcher

Bring all your data, systems and developers together into one simple, integrated development environment.

Perspective Workstation

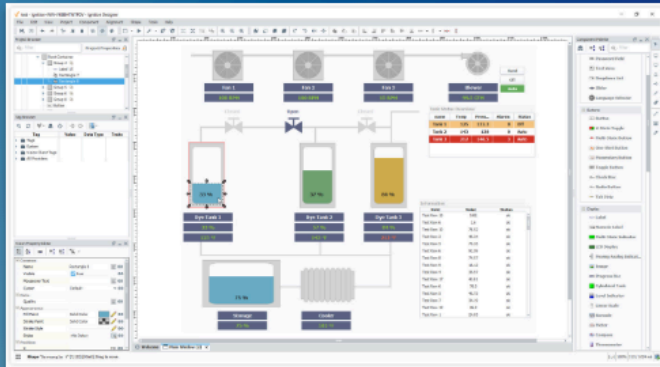
Open Perspective Sessions from any Ignition Gateway.

Vision Client Launcher

Open Vision Clients from any Ignition Gateway.

2. Click the **Download** button to download the launcher. The Gateway will automatically detect which operating system to download the launcher for.

## Download the Designer Launcher



### Designer Launcher

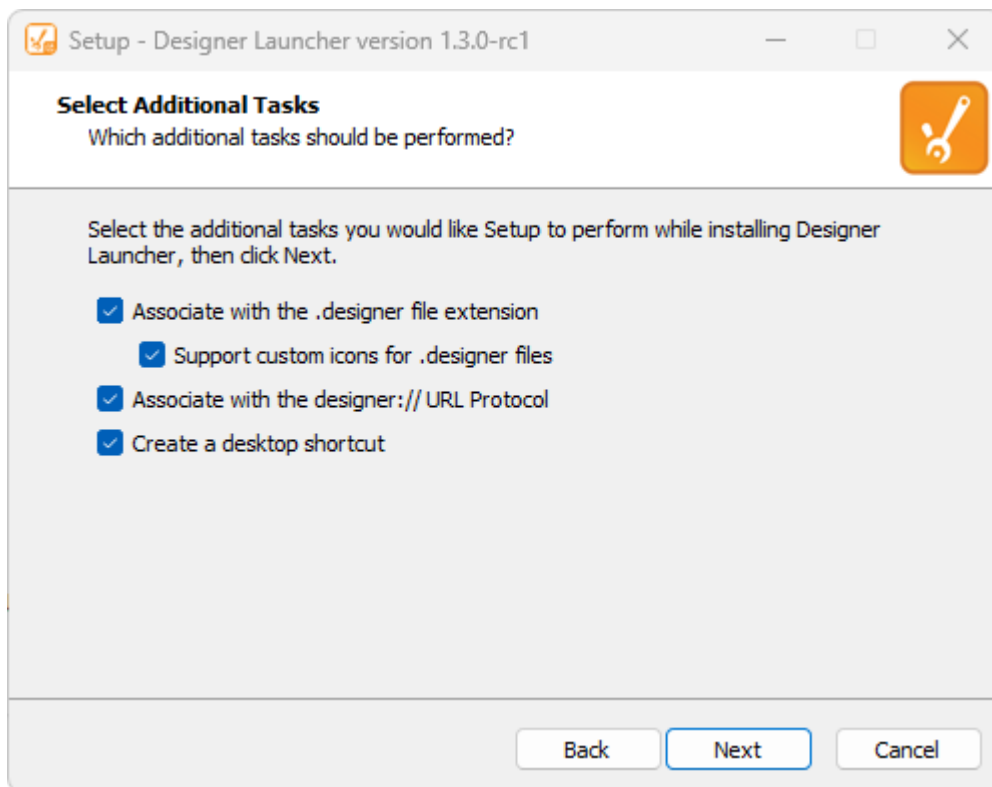
The Designer brings all your data, systems, and developers together into one beautifully simple, integrated development environment.

[Download for Windows](#)

Windows: 58.81 MB

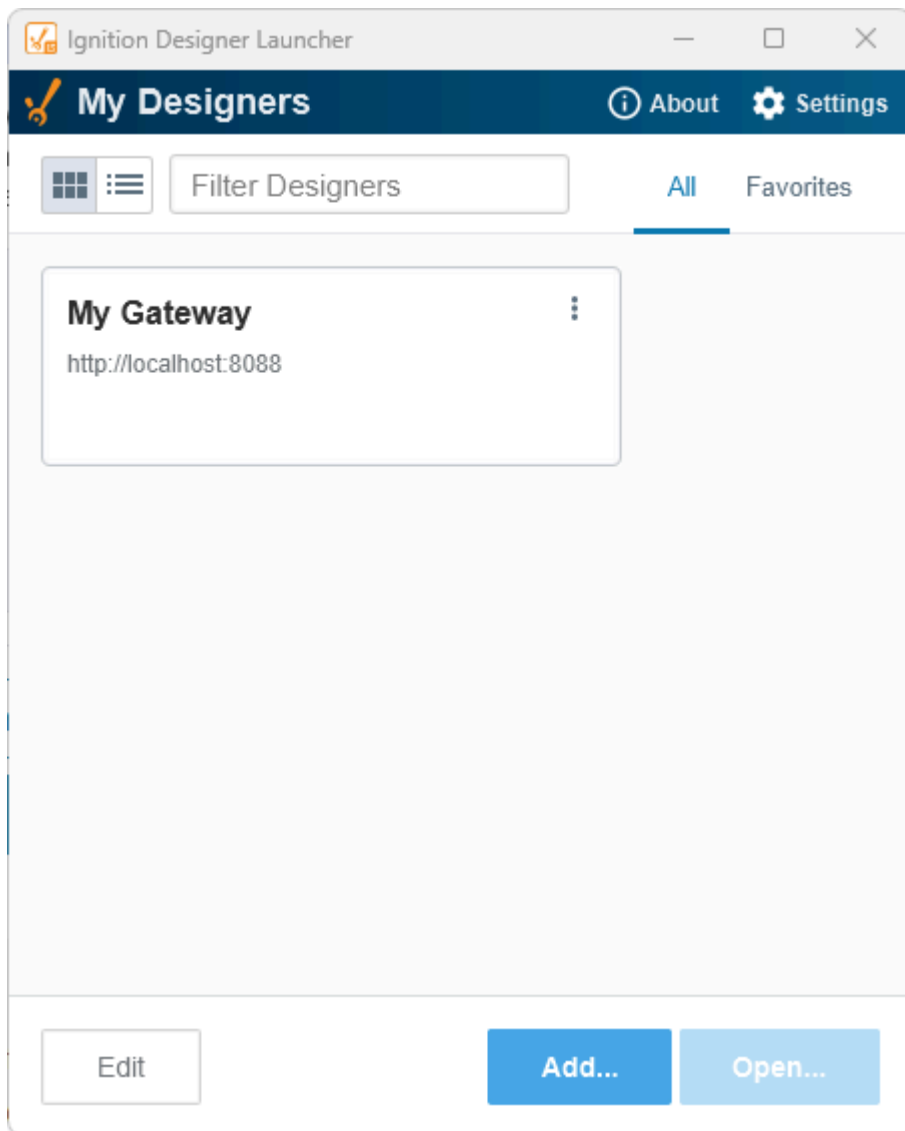
Download for: [Mac](#) | [Linux](#)

3. Open the downloaded file. You may be prompted to install for either all users or only the current user, depending on your administrative privileges. We will install the Designer Launcher for all users.
4. The Designer Launcher Setup Wizard will open and display the file location to install the launcher in. We will use the default directory. Once you have specified a location, click **Next**.
5. You will be prompted to select any additional tasks to perform, such as associating the .designer file extension or creating a desktop shortcut. We will leave the default settings here and click **Next**.



6. The Ready to Install page will provide a summary of your choices. If you are satisfied, click **Install**.

7. Once the Designer Launcher finishes installing, click **Finish**. The setup wizard will close and open the newly installed launcher, and your Gateway should be selectable in the Designer Launcher.



## Downloading and Installing Perspective Workstation

Since this guide focuses on using Perspective, this section will demonstrate how to download and install Perspective Workstation.

Similar to the Designer Launcher, Perspective Workstation will allow you to quickly launch any Perspective-based project regardless of whether the Perspective project is locally hosted or on a remote system. This will allow us to open and test our Perspective project when it is done as an operator would.

1. On the Gateway Webpage, click on **Perspective Workstation** in the Downloads category. This will bring you to the **Download** page for Perspective Workstation.

Welcome to IgnitionLaunch Designer

Gateway OverviewView Details

| Gateway Name | Redundancy  | Gateway Version         | Gateway Mode |
|--------------|-------------|-------------------------|--------------|
| My Gateway   | Independent | 8.3.0-rc1 (b2025082609) | N/A          |

Gateway NotesEdit Notes

Welcome to your Ignition Gateway. This customizable area is intended to capture the critical details you want to document for this Gateway. You might include information about the environment (production, testing, or development), key workflows, or maintenance schedules. It's also a great place to list instructions for your team, important reminders about system health, or details about your configuration that require regular review. Use this space to keep everyone informed and ensure smooth operations across the board.

Downloads

Designer Launcher

Bring all your data, systems and developers together into one simple, integrated development environment.

→

Perspective Workstation

Open Perspective Sessions from any Ignition Gateway.

→

Vision Client Launcher

Open Vision Clients from any Ignition Gateway.

→

- Click the **Download** button to download the launcher. The Gateway will automatically detect which operating system to download the launcher for.

### Download Perspective Workstation

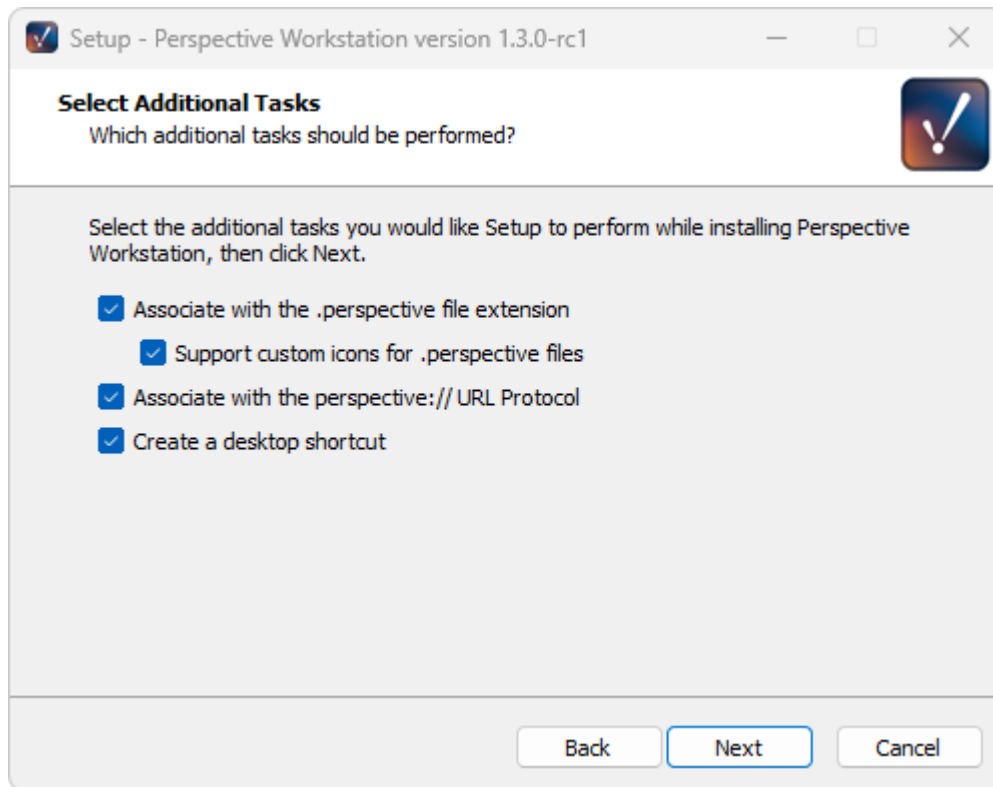
### Perspective Workstation

Perspective Workstation is an application that acts as both a launcher and a desktop wrapper for Perspective Sessions. Download the application to open Sessions from any Ignition Gateway.

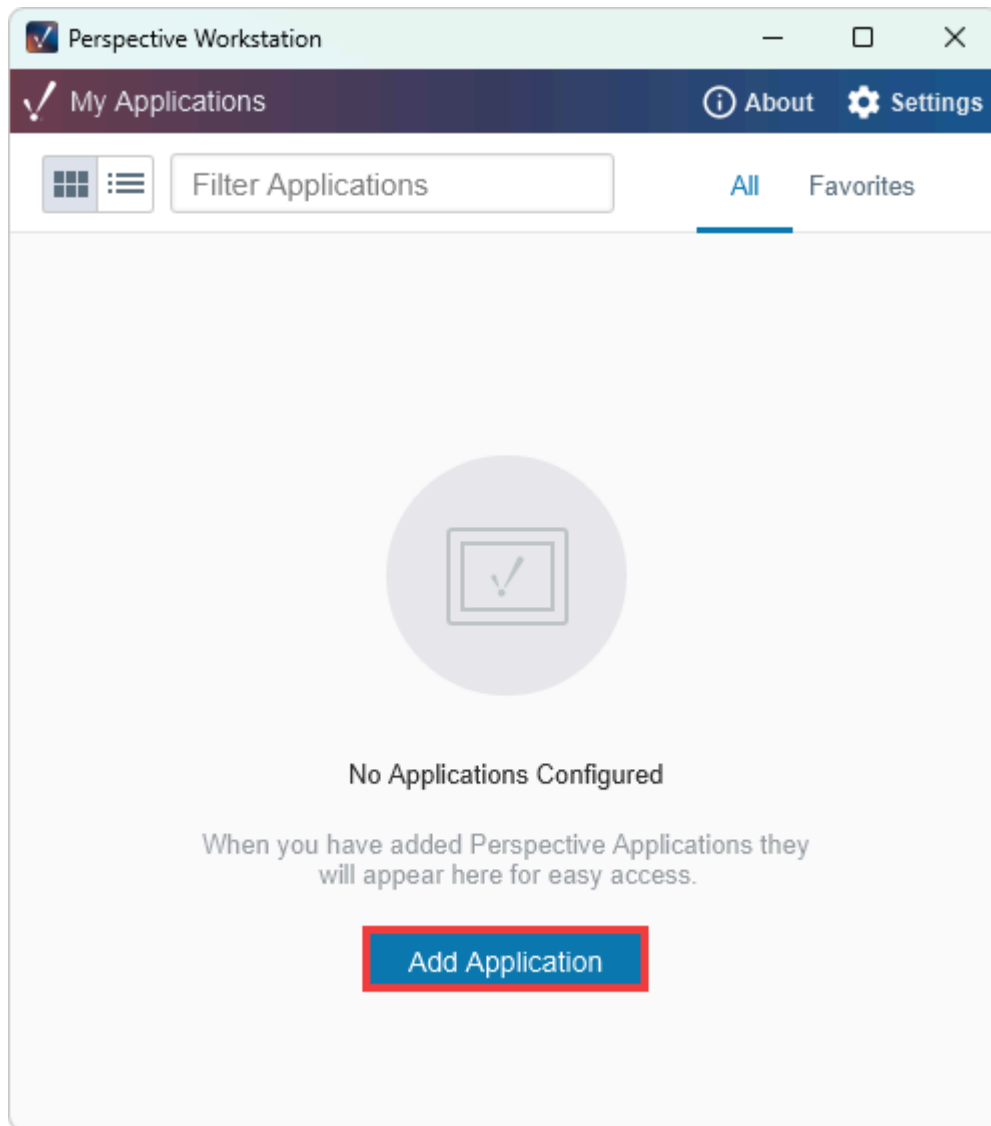
Download for Windows

Windows: 183.01 MB    Download for: [Mac](#) | [Linux](#)

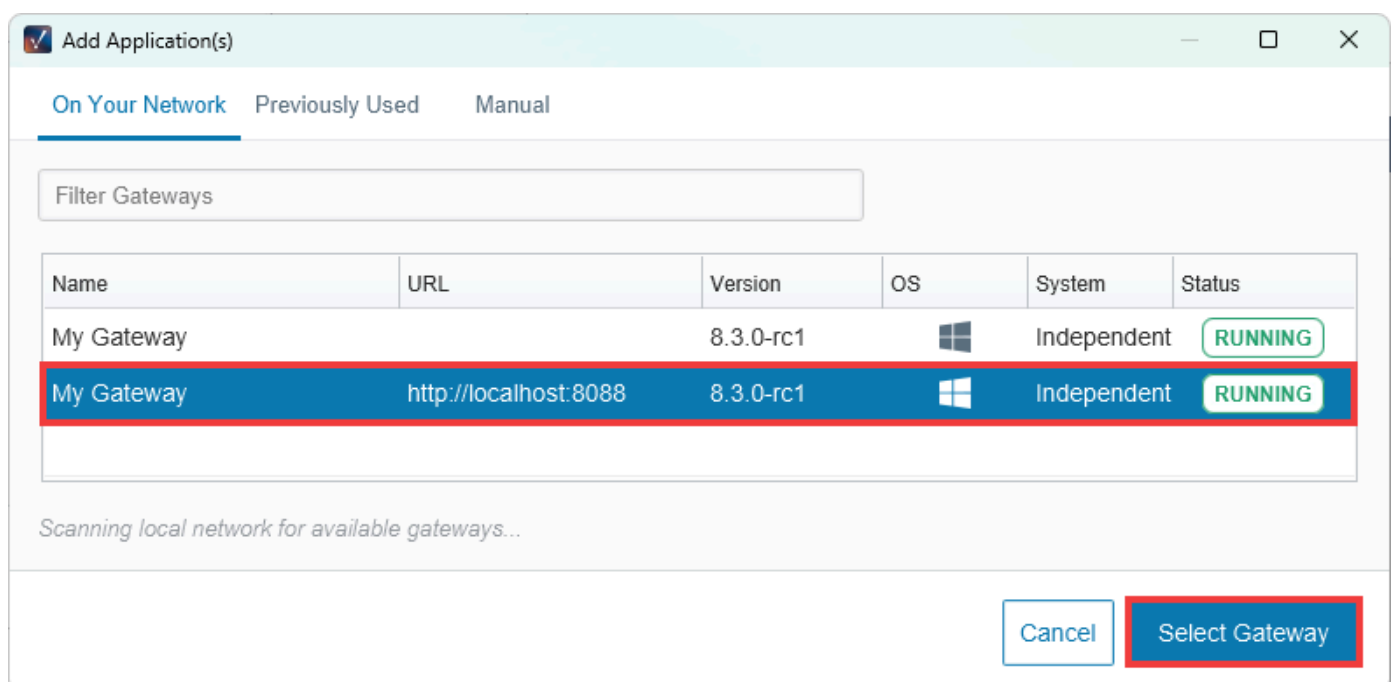
- Open the downloaded file. You may be prompted to install for either all users or only the current user, depending on your administrative privileges. We will install Perspective Workstation for all users.
- The Perspective Workstation Setup Wizard will open and display the file location to install the launcher in. We will use the default directory. Once you have specified a location, click **Next**.
- You will be prompted to select any additional tasks to perform, such as associating the .perspective file extension or creating a desktop shortcut. We will leave the default settings here and click **Next**.



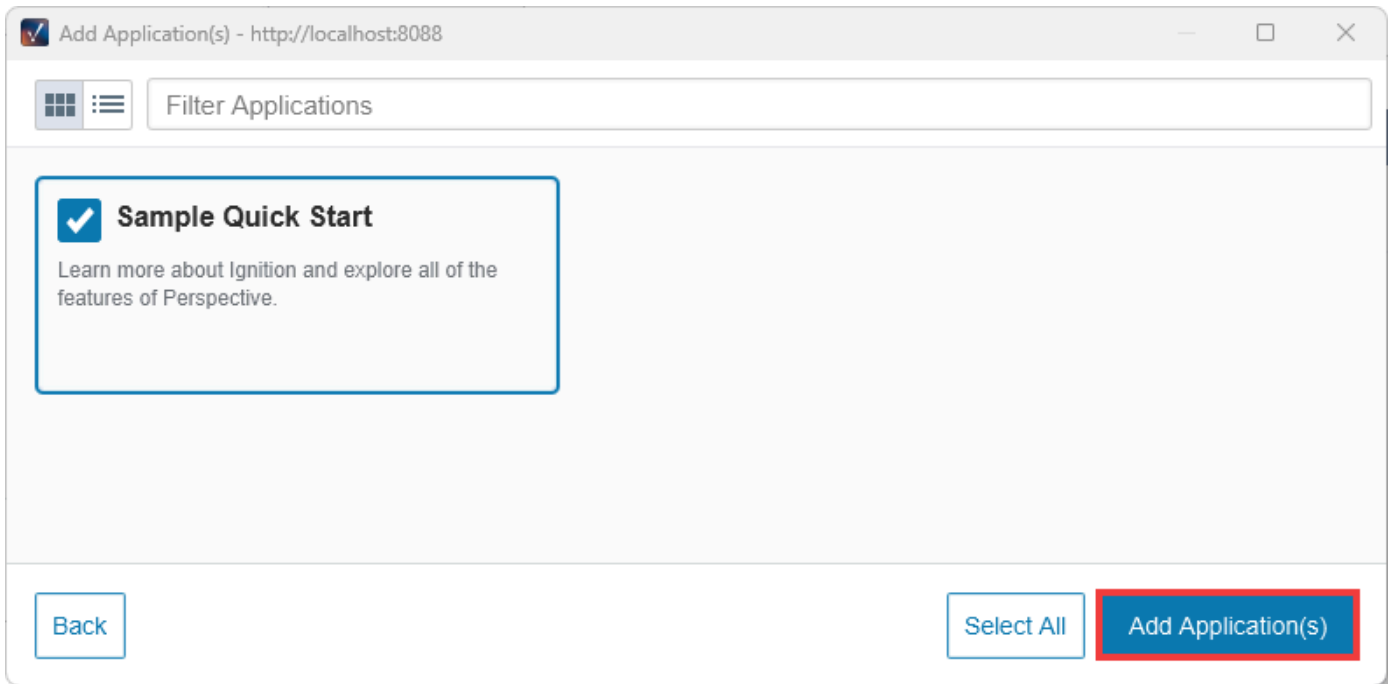
6. The Ready to Install page will provide a summary of your choices. If you are satisfied, click **Install**.
7. Once Perspective Workstation finishes installing, click **Finish**. The setup wizard will close and open the newly installed launcher.
8. You may need to add your Gateway if you are receiving a **No Applications Configured** message. To do this, click on **Add Application** in Perspective Workstation.



9. The Add Application(s) window will appear and display all the available Gateways to select. Since our project is going to be on our locally hosted Gateway, we can select the Gateway located at <http://localhost:8088>, then click **Select Gateway**.



10. You will be prompted to select which projects to add. Since we enabled Quick Start when first commissioning our Gateway, we already have a project called **Sample Quick Start**, which we will add by clicking **Add Application(s)**.



Your Perspective project should now be launchable within Perspective Workstation.

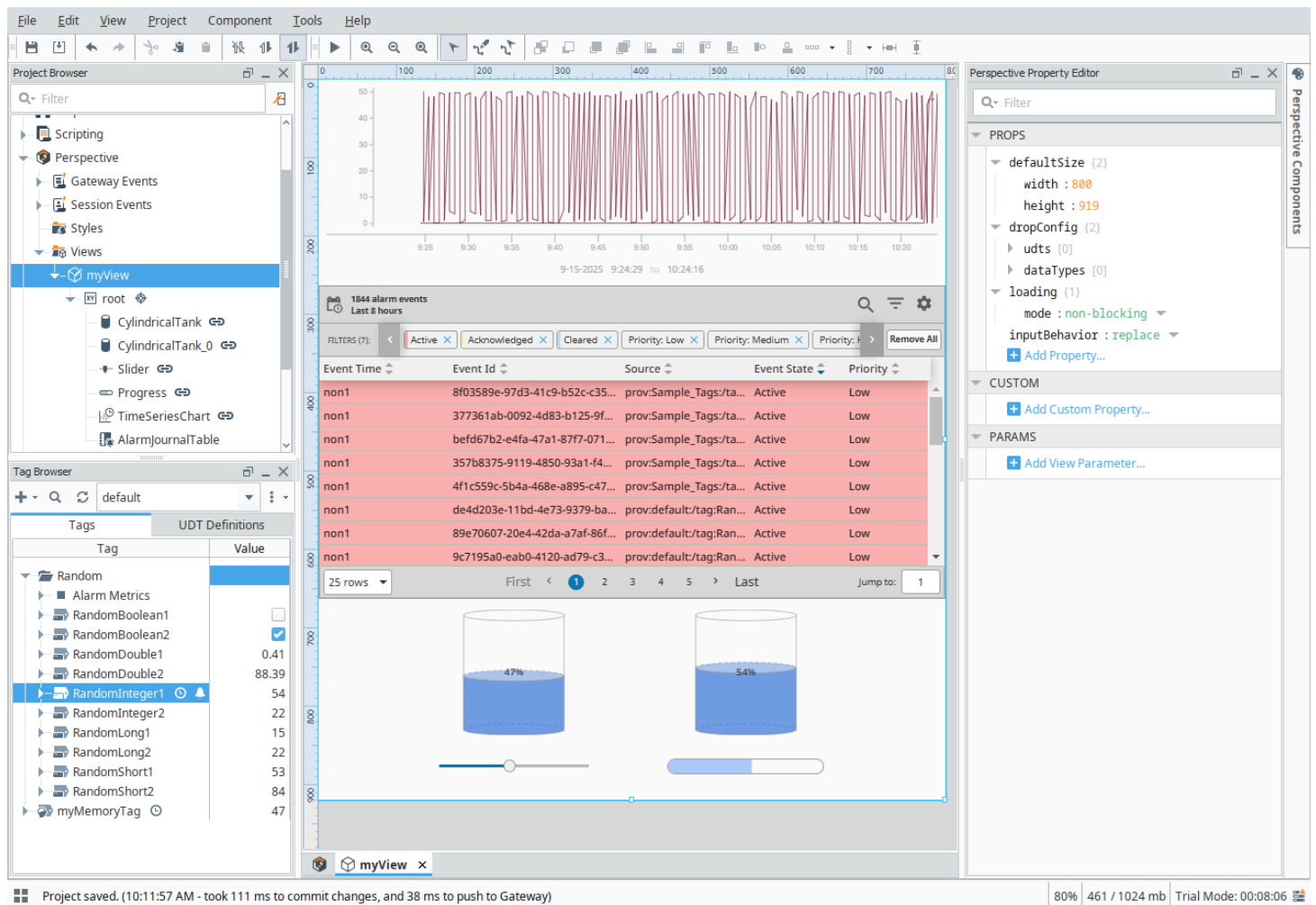


# Designing a Project

This document follows the [Downloading and Installing Ignition](#) guide from the previous section and assumes you have enabled the Quick Start feature on the Gateway. See the [Commissioning the Gateway](#) section for more details.

Additionally, this guide will use the [Perspective](#) module to visualize our data and project. The resources configured within the Gateway's Quick Start, including the [Device Simulator](#), [tags](#), [Tag Historian](#), and [Internal Alarm Journal](#), will also be used for this project.

The project this guide creates will start from a blank Perspective project and end with several components with [bindings](#) that interact, as well as visualizing [historical tag data](#), and creating an [alarms system](#) that alerts users if a tag reaches a certain threshold. By the end of this guide, we will have a simple project that looks similar to this:



## Creating the Project

To begin working on a project, we will first need to create one.

1. In the Designer Launcher, select the Gateway to create the project on and then click **Open....** We will be using our locally installed Gateway in this guide.
2. The Designer will initialize and then prompt you for login credentials. Use the credentials you set up when first commissioning the Gateway.
3. After logging in, a list of projects on the Gateway will be displayed. Click on **+ New Project** on the top left. This will bring you to the New Project Setup page.

**i NOTE**

Since we enabled Quick Start on the Gateway, we will already have a project titled **Sample Quick Start**. This project is a good example of what your own project can eventually look like, but for the purposes of this guide, we will create a new project.

4. Give your project a name and title, then click **Create New Project**. Your new project will initialize and open the Designer. We will call our project **myProject** and give it a title of **My Project**.

My Gateway — Open/Create Project

Ignition designer  
by inductive automation

← Back

New Project Setup

Project Settings

Project Name

myProject

Project Title

My Project

Description

Project Template

Parent Project

☐ Inheritable Project

Connection Settings

User Source

default

Default Database

Sample\_SQLite\_Database

Default Tag Provider

default

Identity Provider

default

Cancel

Create New Project

Your project should now be ready to build in.

## Working in Perspective

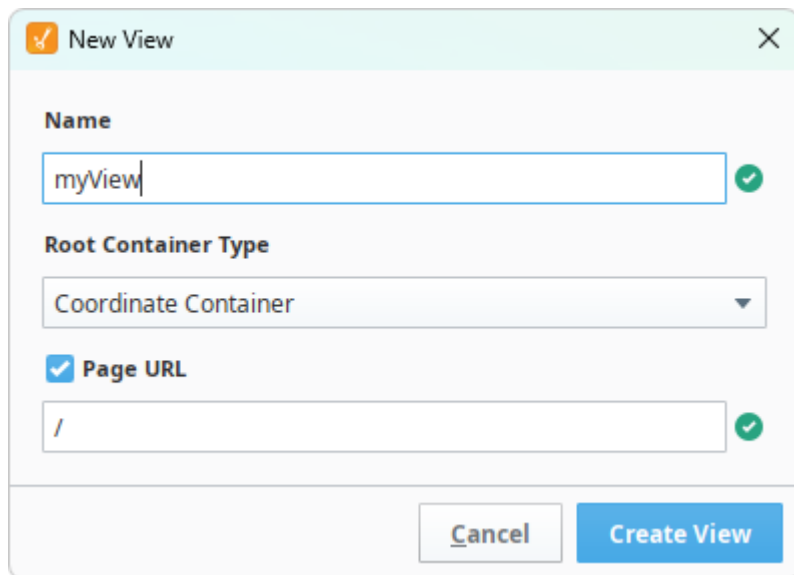
This section will encompass all the steps taken within the Designer's Perspective workspace.

### Creating a View

Since we are using Perspective, we will need to first create a **view**.

1. In the **Project Browser** on the top left of the Designer, expand the Perspective Module.

2. Right-click on the **Views** folder and select **New View....** A New View configuration window will pop up.
3. Give your new view a name and choose a **Root Container** type, then click **Create View**. We will name our view **myView** and keep the default **Coordinate Container** selection.



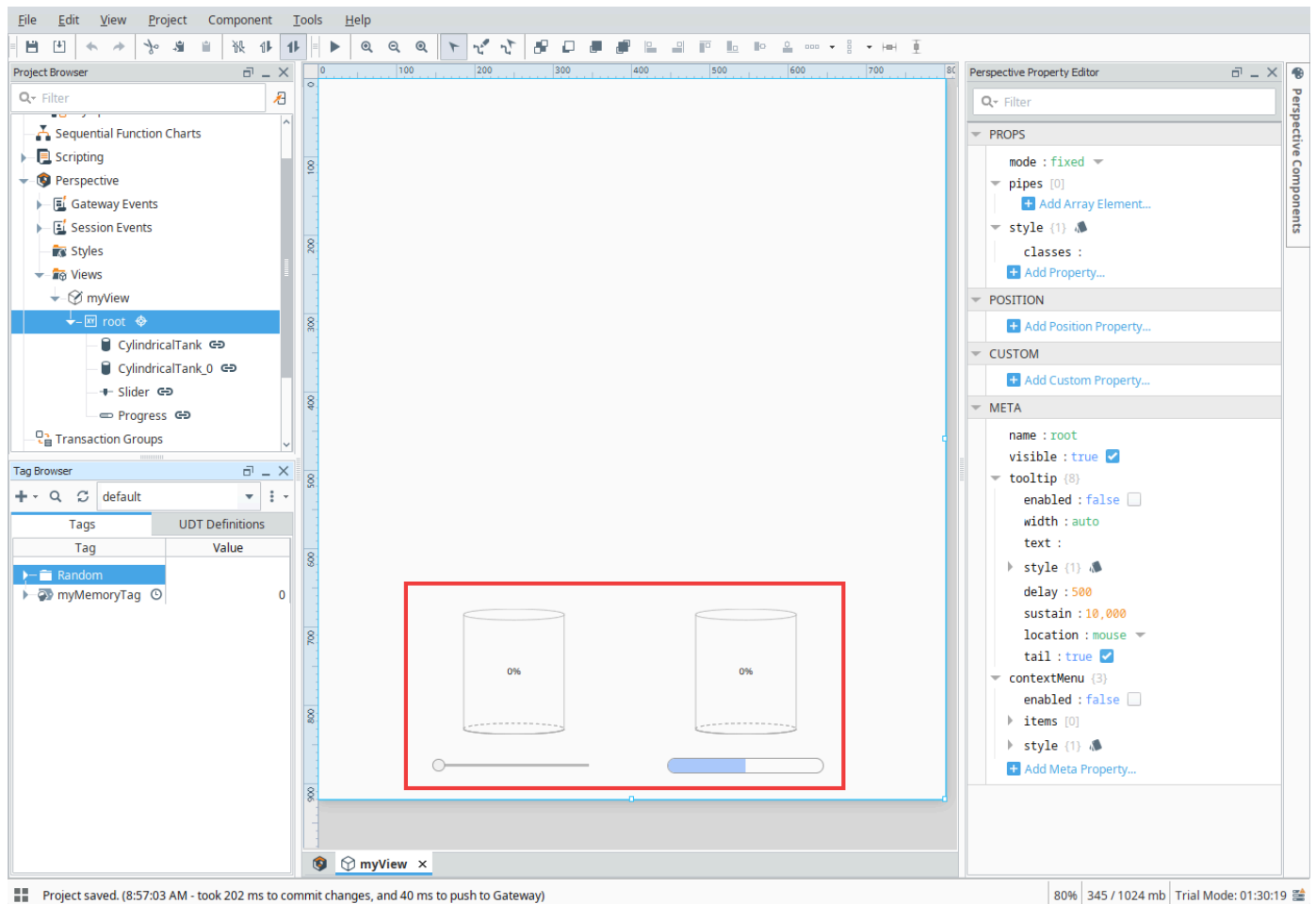
The 'New View' configuration window is shown. It has a title bar with a checkmark icon and the text 'New View'. The window contains three input fields: 'Name' with the value 'myView', 'Root Container Type' with a dropdown menu showing 'Coordinate Container', and 'Page URL' with a checked checkbox and a text field containing '/'. Each input field has a green checkmark icon to its right. At the bottom, there are two buttons: 'Cancel' and 'Create View'.

Your view is now created and has a blank workspace to begin designing your project.

## Preparing Perspective Components

Let's start putting components into our view. Components are the main features an operator interacts with within a project and includes things like **charts**, **input** components, and **display** components.

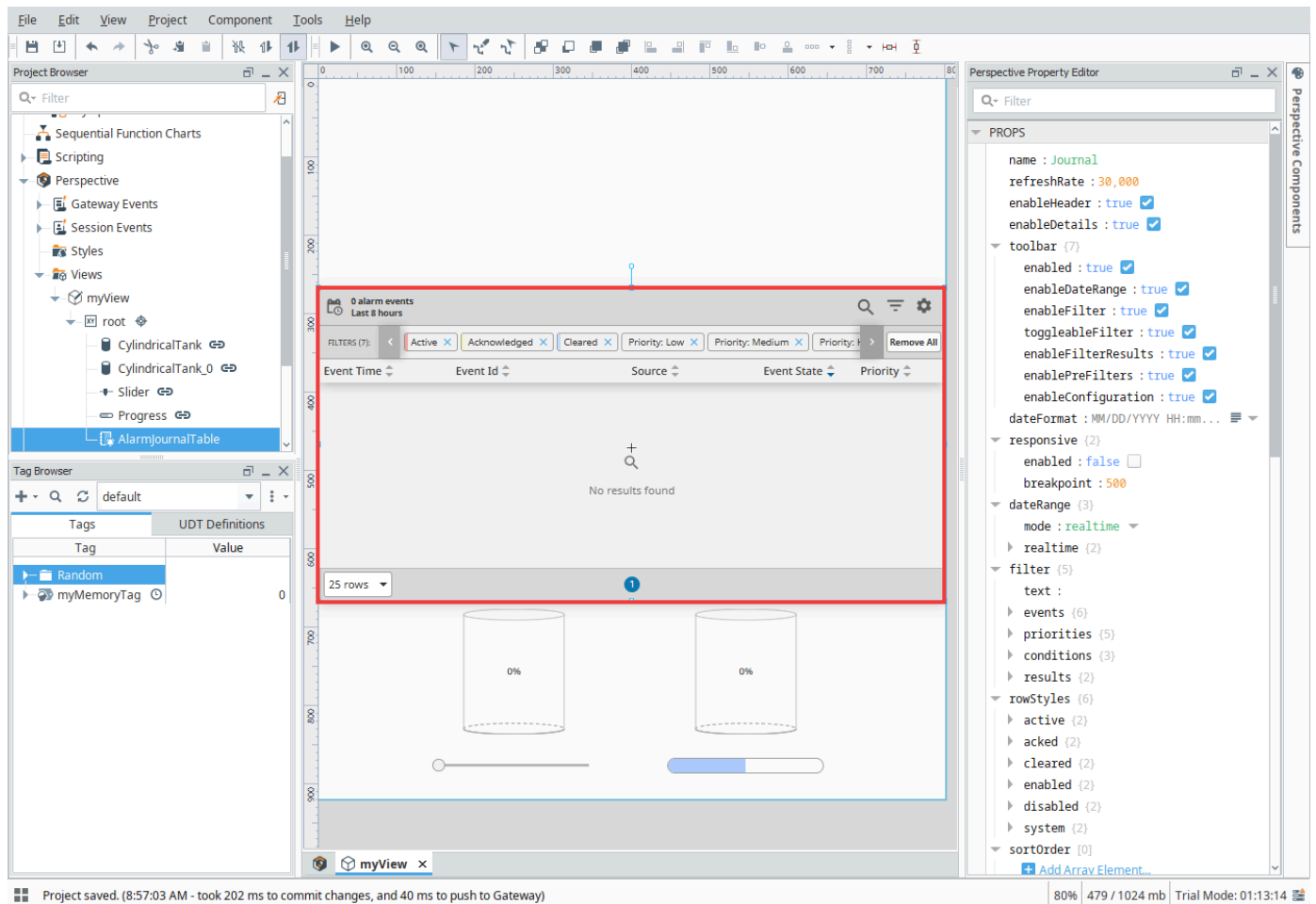
1. Begin by dragging two **Cylindrical Tanks**, a **Slider**, and a **Progress Bar** from the **Perspective Component Palette** onto your workspace and orient them on the bottom as shown in the image below. We will bind these together using tag data in a **later section**.



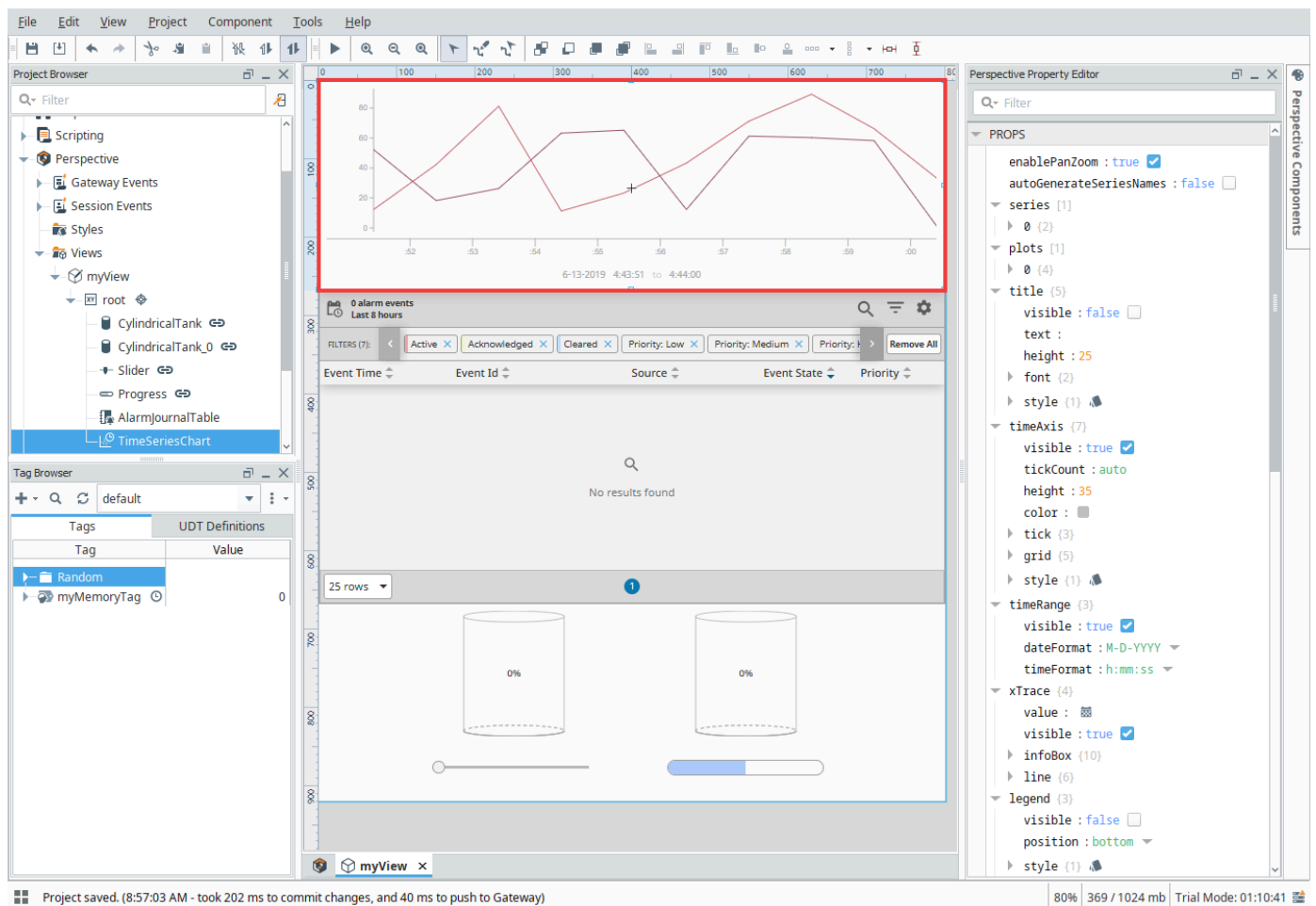
### TIP

You can use the Designer's red dotted guiding lines to help line up components so that they are on the same axis.

- Next, drag an **Alarm Journal Table** to the space above the components from the previous step. We will use this table to display our alarm history in a **later section**.



3. Drag a **Time Series Chart** from the Component Palette onto the top of your workspace. Use the handles to resize the component so that it sits flush with the top of the view and the top of the Alarm Journal Table. We will use this to visualize your tag's historical data in a **later section**.



#### 4. Save your project.

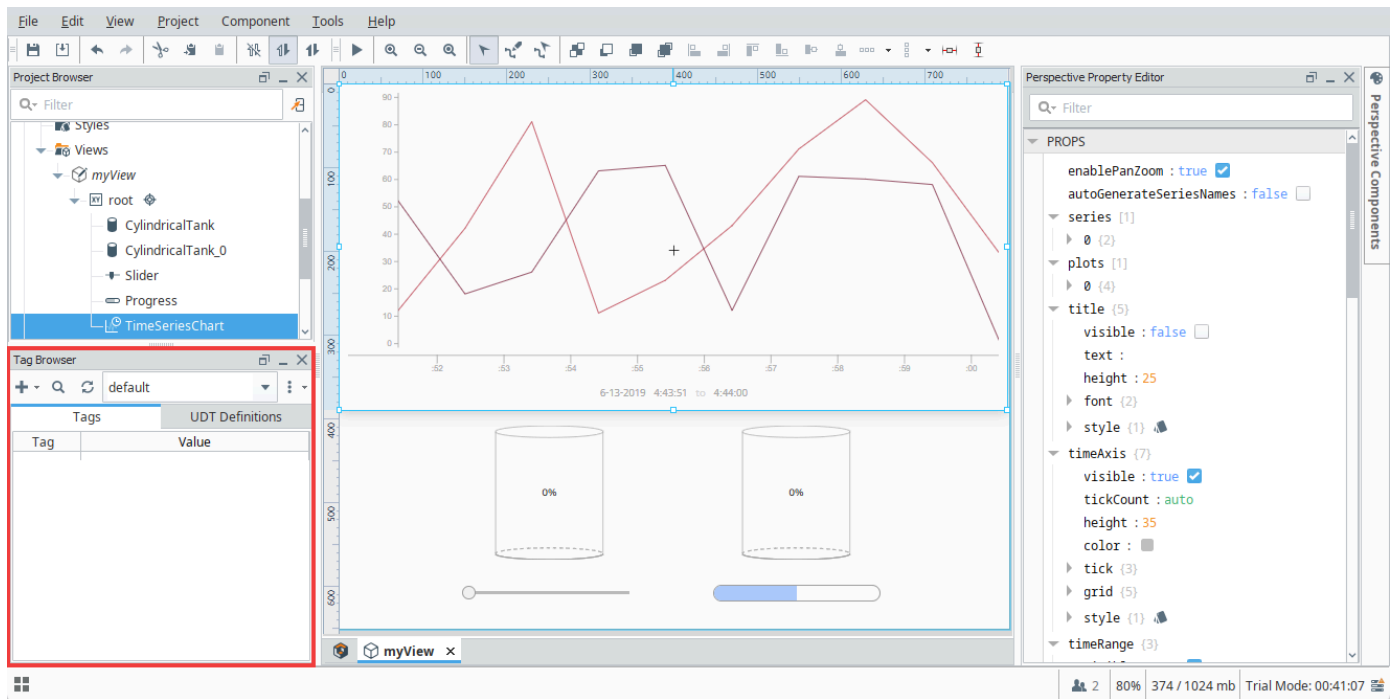
Your components are now ready to have tags bound to them to display data.

## Adding Tags from a Device

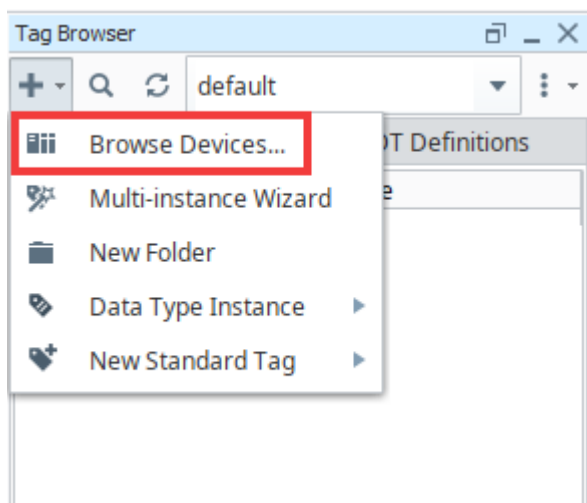
Since components visualize and interact with data, they do not do anything if no tags or data is bound. This section will go over the most common way a component gets data to display, typically from PLCs or external devices through an **OPC UA** connection using **OPC tags**.

In this example, we will use the Gateway Quick Start's preconfigured Device Simulator, as this mimics an external device that tags pull data from. The steps below assume you already have a Device Simulator configured from Quick Start. See the **Connecting with OPC UA** section for details on creating a connection to a physical device or **Device Simulator** if you did not enable Quick Start.

1. Go to the **Tag Browser** on the bottom left of your Designer.

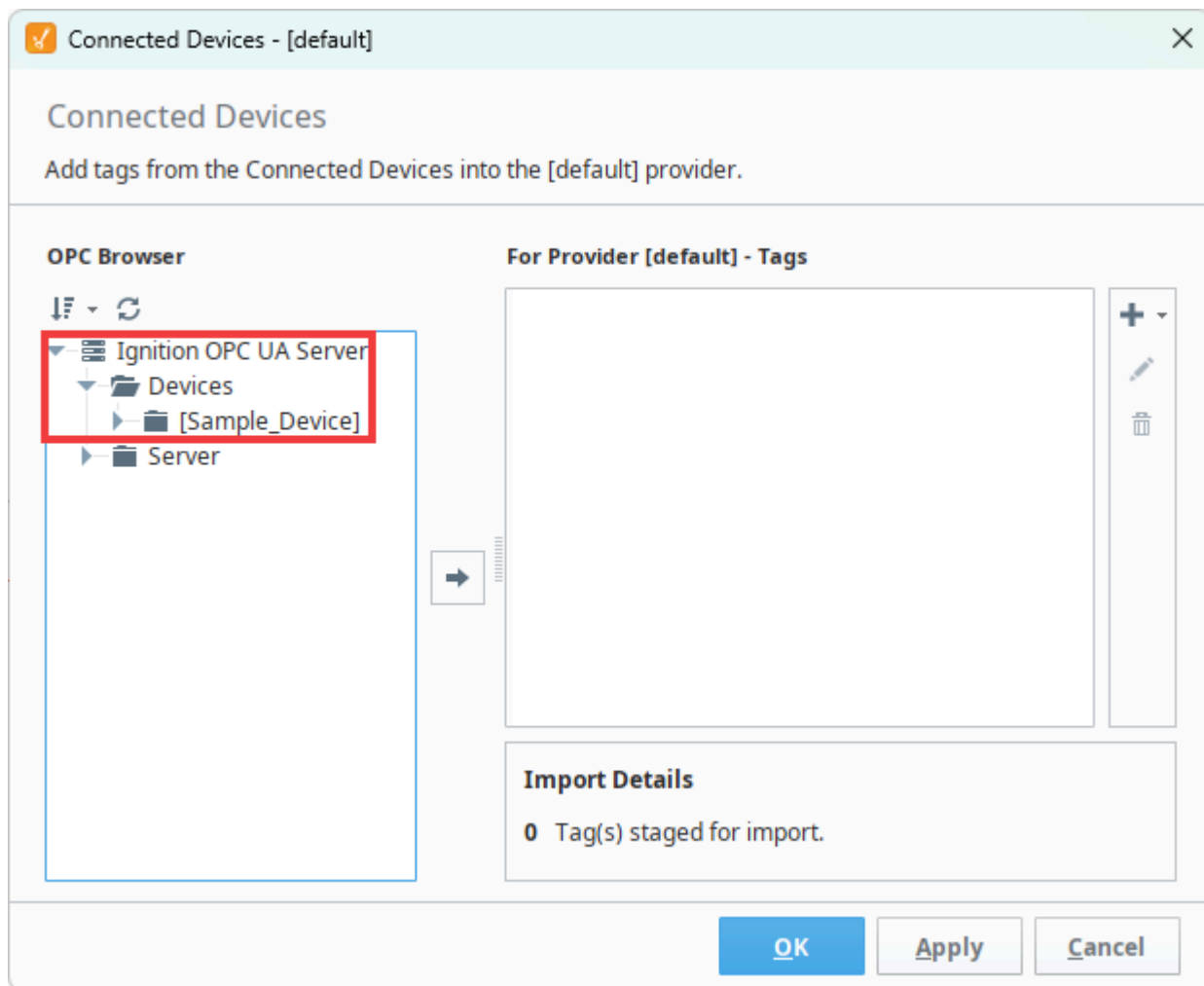


2. Click on the **Add**  icon, then select **Browse Devices**. This will bring up the Connected Devices popup.



3. The **Ignition OPC UA Server** will populate under the OPC Browser column. Go to the Device Simulator by expanding **Ignition OPC UA Server > Devices**. The preconfigured simulator will be called **[Sample\_Device]**.





- Expand the **[Sample\_Device]** folder and click on the **Random** folder. This folder contains all the tags we need for this basic project.

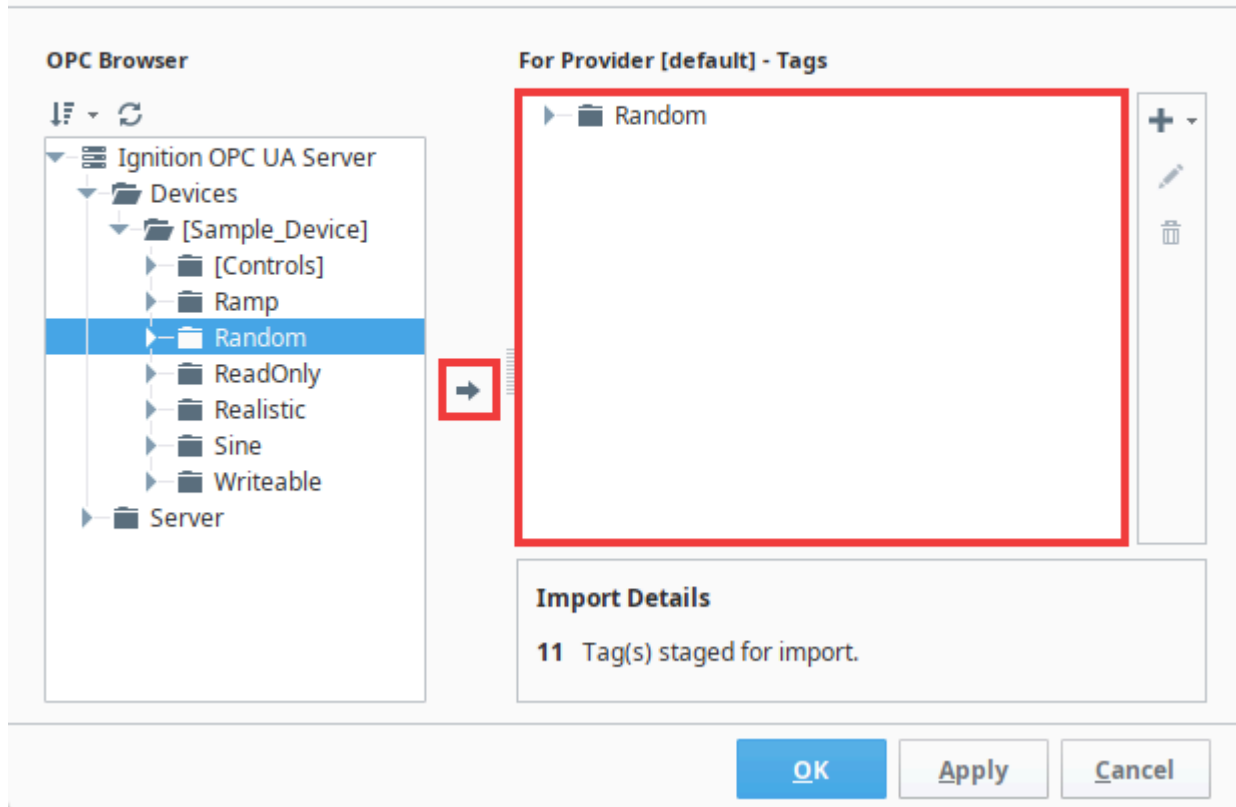
**NOTE**

You can choose to import all the tags from your device. However, since we don't need the other tags on the Device Simulator, we will just import the **Random** folder.

- With the **Random** folder selected, click on the **Add** ➔ icon in the middle of the Connected Devices popup. This will add the **Random** folder and its tags to the staging area for import.

## Connected Devices

Add tags from the Connected Devices into the [default] provider.



### TIP

You can add tags to a different [Tag Provider](#) than the default provider by changing the provider in the Tag Browser before importing any tags.

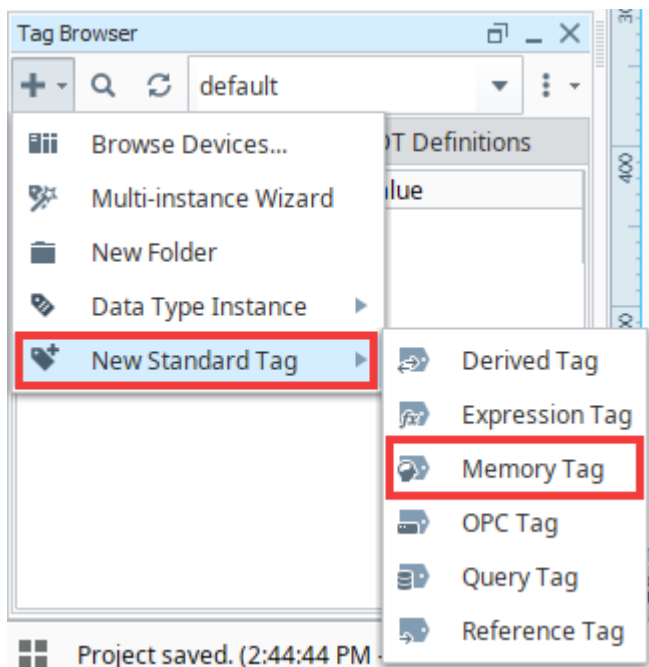
6. Click **OK** to add the **Random** folder.

The folder and tags within will now appear in the Tag Browser.

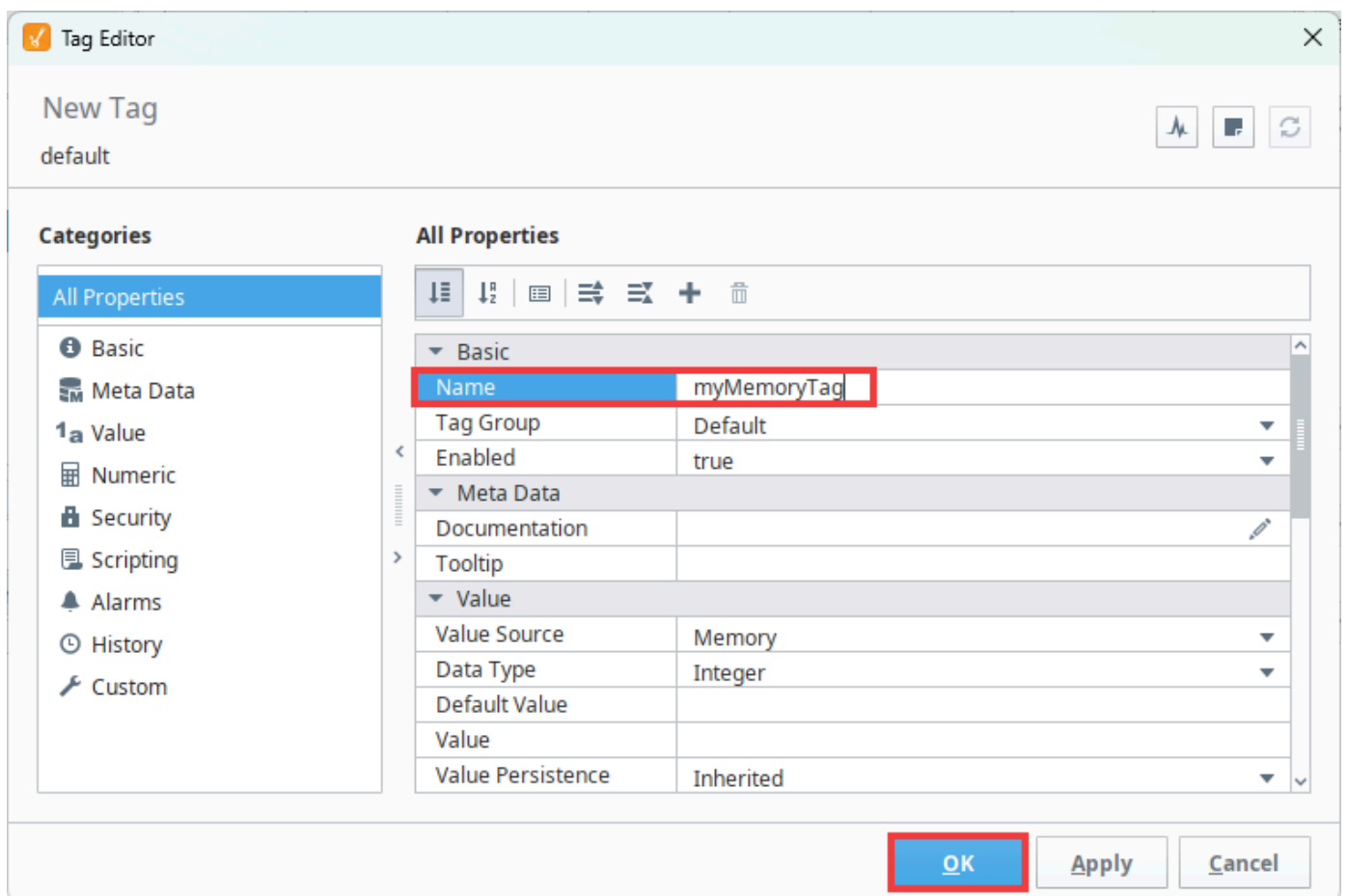
## Creating Tags Within the Tag Browser

Besides pulling tags from a device over OPC UA, you can also create your own tag. This section will demonstrate how to create a **Memory tag**, which will be used in a **later section**.

1. In the Tag Browser, click on the **Add**  icon, then select **New Standard Tag > Memory Tag**. This will open the **Tag Editor**.



2. Give your tag a name. We will name our tag **myMemoryTag**. Since we are making a simple binding to a component, we do not need to configure any other properties at this time. After you have named your tag, click **OK**.



Your Memory tag is now created and ready to use.

# Setting Up Tag History

Now that your tags have been created, we can set up history on the tags we will be using. This lets us record historical tag values and display them to see trends and past data.

Storing historical data typically requires setting up a [database connection](#) and a [history provider](#).

We will be storing history to the SQLite SQL Historian resource configured by the Gateway's Quick Start when first commissioning the Gateway.

## ⚠ CAUTION

Even though we are using the SQLite database connection for this example, it is **NOT** recommended to store history using SQLite. A dedicated external database, such as [Microsoft SQL Server](#) or [MySQL](#), should be used instead, as they will handle the potential amount of writes and reads needed for development and production data much better.

1. In the Tag Browser, right-click on the Memory tag you created, then select **Edit tag(s)**. This will open the Tag Editor.
2. Click on the **History** category of the Categories section.

myMemoryTag  
default

**Categories**

- All Properties
- Basic
- Meta Data
- Value
- Numeric
- Security
- Scripting
- Alarms
- History**
- Custom

**History**

|                          |          |
|--------------------------|----------|
| History Enabled          | false    |
| Storage Provider         |          |
| Include Metadata         | false    |
| Deadband Style           | Auto     |
| Deadband Mode            | Absolute |
| Historical Deadband      | 0.01     |
| Sample Mode              | OnChange |
| Min Time Between Samples | 1        |
| Min Time Units           | SEC      |
| Max Time Between Samples | 0        |
| Max Time Units           | HOURL    |

OK Apply Cancel

3. Under the **History Enabled** property, change the field from false to **true**. This will enable the rest of the history fields.

4. Under the **Storage Provider** property, change the field to the history provider you set up previously. In this example, we will be using the **Sample\_SQLite\_Database** configured from Quick Start.
5. Click **OK** to save these settings.

We will now do the same thing with the tag in the **Random** folder that we will be binding later.

1. In the Tag Browser, expand the **Random** folder, right-click on **RandomInteger1**, and then select **Edit tag(s)**. This will open the Tag Editor.
2. Click on the **History** category of the Categories section.
3. Under the **History Enabled** property, change the field from false to **true**. This will enable the rest of the history fields.
4. Under the **Storage Provider** property, change the field to the history provider you set up previously. In this example, we will be using the **Sample\_SQLite\_Database** configured from Quick Start.
5. Click **OK** to save these settings.

## Binding Tags to Components

Now that we have added our Perspective components, configured our tags, and enabled history on them, we can start binding them to our Perspective components to visualize our data.

### Binding the Memory Tag

We'll first bind our Memory tag to the Slider and left Cylindrical Tank. This will allow us to control our Memory tag using our Slider and easily see the tag's value through the Cylindrical Tank.

1. In the Perspective Workspace, click on the Slider component. Selecting the Slider will populate the **Perspective Property Editor** with the Slider's configurable settings.

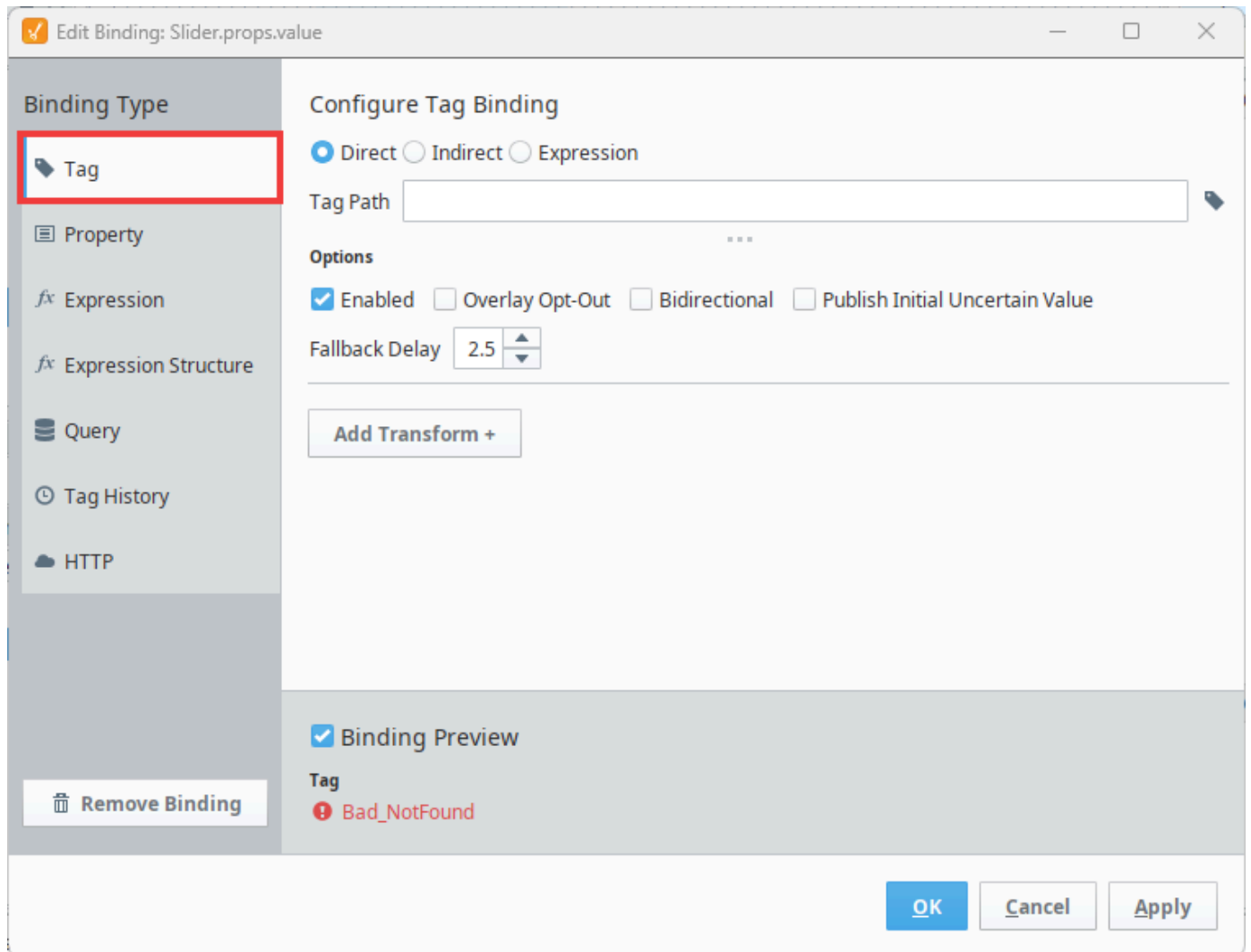


**TIP**

You can also select the Slider in the Project Browser by navigating through **Perspective > Views > myView > root > Slider**. Other components are also selectable through the Project Browser.

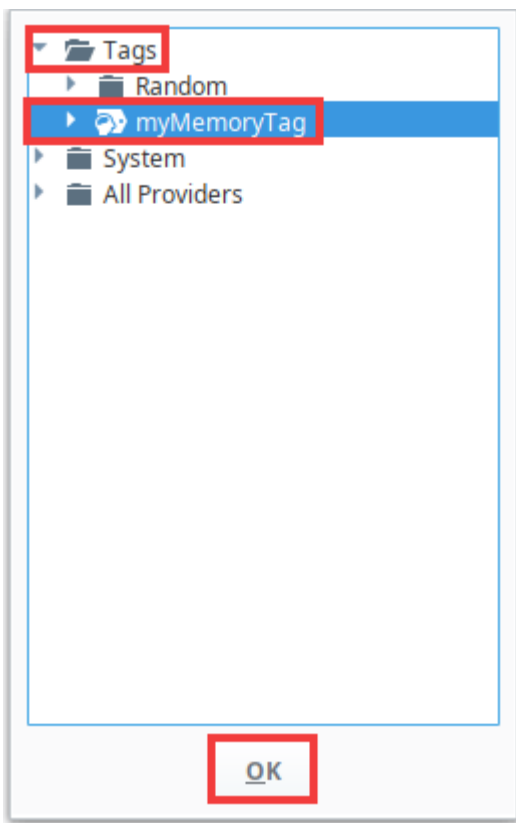
2. Go to the **value** property. You'll notice that hovering over this property will cause a light gray **Add Binding**  icon to appear. Click on the icon to open the **Edit Binding** window.

3. Click on the **Tag** Binding Type. This will open the **Configure Tag Binding** section.



4. Click on the **Browse Tags**  icon to the right of the **Tag Path** field. This will open a navigatable tree.

5. Within the tree, expand the **Tags** folder and select the Memory tag you **created previously**, then click **OK**. This will populate the **Tag Path** field with your Memory tag.



**NOTE**

If you do not have a value for your Memory tag by the end of the Slider Tag binding process, the Tag binding will still work, but an error will be shown.

6. Toggle the **Bidirectional property** to enable it. This will allow our Slider to control our Memory tag.
7. Click **OK**.

You'll notice that changing the Slider will now also update your Memory tag. Next, we'll bind the Cylindrical Tank to display the Memory tag's value.

1. Click on the left Cylindrical Tank.
2. Click on the **Add Binding**  icon for the Cylindrical Tank's **value** property.
3. In the **Edit Binding** window, click on the **Tag** Binding Type.
4. Click on the **Browse Tags**  icon.
5. Expand the **Tags** folder, select your Memory tag, then click **OK**.

**NOTE**

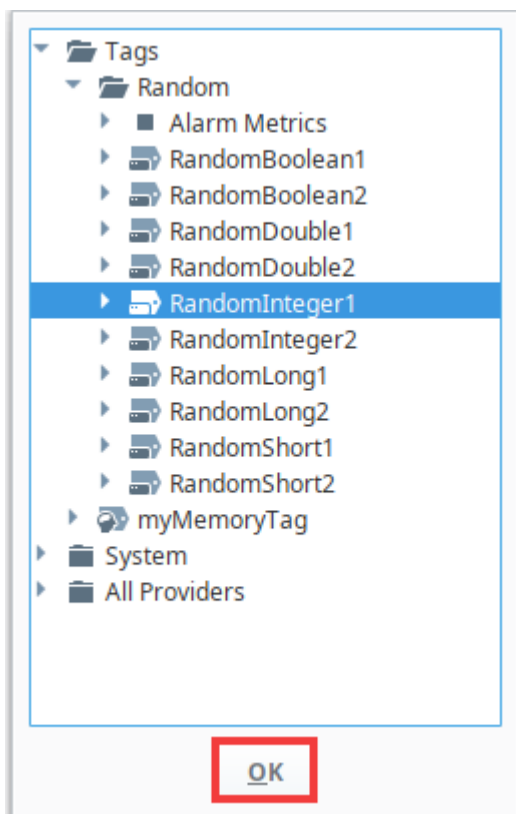
We did not enable the **Bidirectional** property for the Cylindrical Tank. This is because we are only using the Cylindrical Tank to read the tag's value without writing to it.

Your Cylindrical Tank should now be displaying your Memory tag's value. To test your binding, set the Designer to **Preview Mode** and enable both **read and write** functionality. Notice that when adjusting the Slider, the Cylindrical Tank's value will also adjust.

## Binding the OPC Tag

Now we'll bind our OPC tag **RandomInteger1** to our Progress Bar and right Cylindrical Tank. This will allow users to see the values coming in from our **RandomInteger1** tag.

1. In the Perspective Workspace, click on the Progress Bar component. Selecting the Progress Bar will populate the Perspective Property Editor with the Progress Bar's configurable settings.
2. Go to the **value** property and click on the **Add Binding**  icon. This will open the **Edit Binding** window.
3. Select the **Tag** Binding Type. This will open the **Configure Tag Binding** section.
4. Click on the **Browse Tags**  icon to the right of the **Tag Path** field.
5. In the tag tree, navigate to **Tags > Random**, select **RandomInteger1**, and press **OK**.



6. Click **OK** on the **Edit Binding** window. Note that we don't have to enable the **Bidirectional** option since the Progress Bar will only read the tag value and not write.



Your Progress Bar is now displaying your **RandomInteger1** tag value. We'll now do the same for our second Cylindrical Tank.

1. Click on the right Cylindrical Tank.
2. Click on the **Add Binding**  icon for the Cylindrical Tank's **value** property.
3. In the **Edit Binding** window, click on the **Tag** Binding Type.
4. Click on the **Browse Tags**  icon.
5. In the tag tree, navigate to **Tags > Random**, select **RandomInteger1**, and press **OK**.
6. Click **OK** on the **Edit Binding** window. Similar to the Progress Bar, we don't have to enable the **Bidirectional** option since the Cylindrical Tank will only read the tag value and not write.

Your second Cylindrical Tank should now be displaying the same value as your Progress Bar.

## Displaying Tag History

Now that we have our tags' live values displayed in our project, let's focus on displaying our tags' history. To do this, we will bind our historical data to the Time Series Chart we created in the [Preparing Perspective Components](#) section.

1. Click on The Time Series Chart to bring up its properties in the Perspective Property Editor. The property we will want to utilize is **series**.
2. Expand the **series** property, and then the **0** property if they aren't expanded already. You'll notice that unlike the previous component properties, there are additional subproperties beneath **series**. This is because unlike **value**, **series** is an array that contains multiple sources of data.
3. Click on the **Add Binding**  icon for the Chart's **series > 0 > data** property.
4. Select the **Tag History** Binding Type.
5. Change the **Time Range** property to **Historical**.

Binding Type

Tag

Property

fx Expression

fx Expression Structure

Query

Tag History

HTTP

Remove Binding

Configure Tag History Binding

Return Format

☒ Wide
☐ Tall
☐ Calculations

Query Mode

Point Count

PointCount

100

fx

Time Range

Start Date

End Date

Historical

thmetic(now(0), -1, 'hour') fx

now(0) fx

Select Tags

☒ Direct
☐ Expression

| Tag Path | Alias | Aggregation Mode |
|----------|-------|------------------|
|          |       |                  |

Default Aggregation Mode

MinMax

Options

☒ Enabled
☐ Overlay Opt-Out
☐ Ignore Bad Quality
☐ Prevent Interpolation
☒ Cache & Share

Value Format

DATASET

Add Transform +

☒ Binding Preview

Tag History

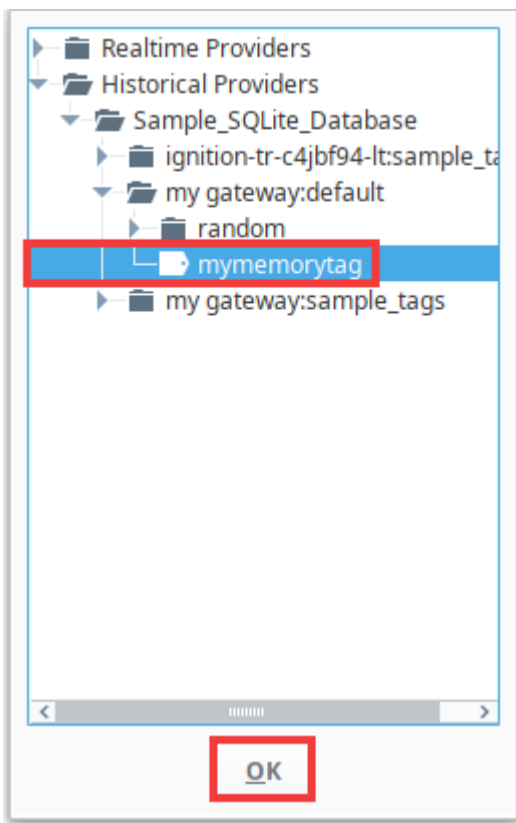
Dataset[0 rows, 0 cols]

OK

Cancel

Apply

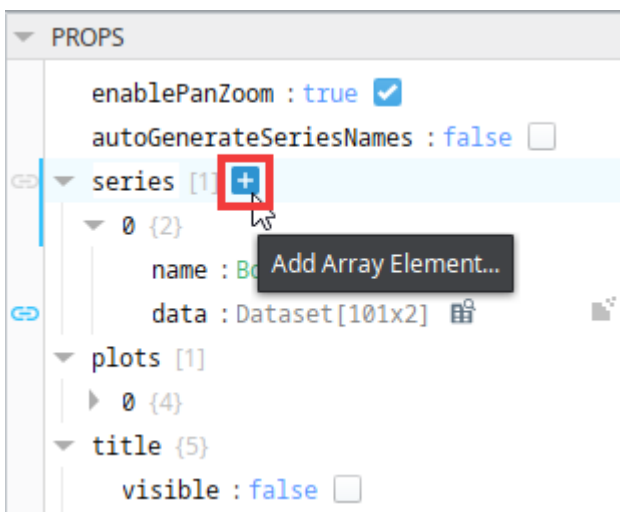
- Click on the **Browse Tags**  icon.
- In the tag tree, navigate to **Historical Providers > Sample\_SQLite\_Database > myGateway:default**. Select your Memory tag, and then press **OK**.



8. Press **OK** on the **Edit Binding** window.

Your Memory tag's history should now be displayed on the Time Series Chart. We'll now add the historical data from **RandomInteger1**.

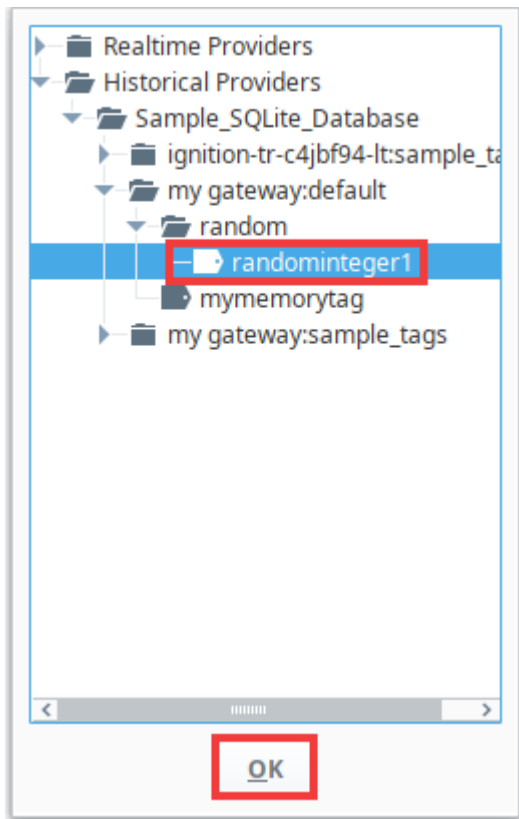
1. Click on The Time Series Chart to bring up its properties in the Perspective Property Editor.
2. Since **series** is an array, we can add additional properties to it. Hovering over the **series** property will bring up an **Add Array Element...**  icon. Click on this icon to add an element to the array. This will add a new **1** property under **series**.



3. Click on the **Add Binding**  icon for the Chart's **series > 1 > data** property.

4. Select the **Tag History** Binding Type.

5. Change the **Time Range** property to **Historical**.
6. Click on the **Browse Tags**  icon.
7. In the tag tree, navigate to **Historical Providers > Sample\_SQLite\_Database > myGateway:default > random**. Select **RandomInteger1**, and then press **OK**.



8. Press **OK** on the **Edit Binding** window.

Your **RandomInteger1** OPC tag should now also be displayed on the Time Series Chart.

## Configuring Alarms

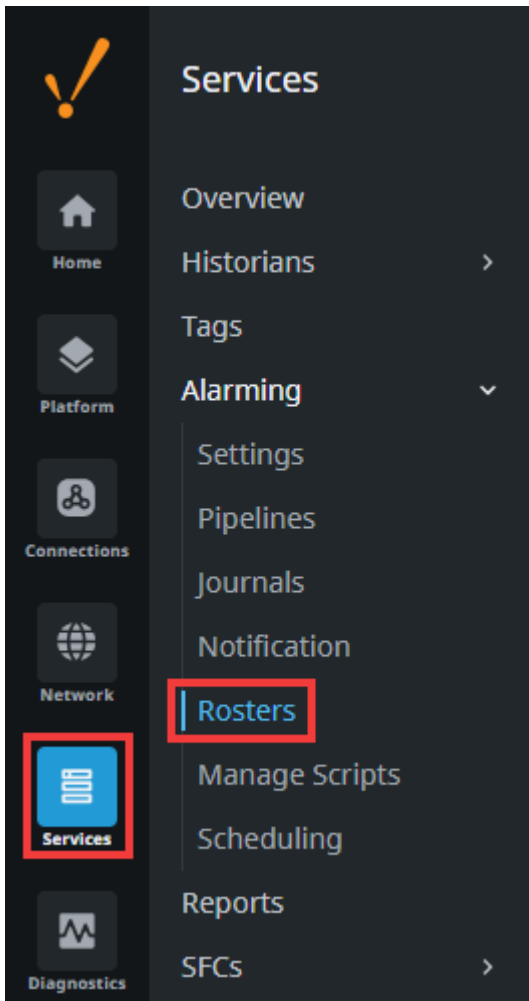
Another common task is to set up alarms on your tags. This section will demonstrate how to navigate through the various Gateway and Designer sections set up an alarm on a tag and notify a user.

Setting up an alarm and corresponding notifications consists of three parts: an **On-Call Roster**, a **Notification Profile**, and an **Alarm Notification Pipeline**. The On-Call Roster determines who receives notifications, while the Notification Profile determines how they are delivered. Then, the Alarm Notification Pipeline incorporates both of these to control alarm notifications for designated tag alarms.

## Creating an On-Call Roster

We'll first set up an On-Call Roster on the Gateway. If your Gateway is installed locally, you can access your Gateway at <http://localhost:8088/>.

1. Navigate to **Services > Alarming > Rosters**.



2. Click on **Create Alarm Roster +**.
3. Give your roster a name, then click **Create Alarm Roster**. We will name ours **myRoster**.
4. Click on the three dots menu on the right of the new roster, and click **Manage Users**.

| <input type="checkbox"/> | NAME     | DESCRIPTION | # OF USERS |                                                                                     |
|--------------------------|----------|-------------|------------|-------------------------------------------------------------------------------------|
| <input type="checkbox"/> | myRoster |             | 0          |  |

Showing 1 of 1 items

Edit

Rename

Duplicate

**Manage Users**

Disable

RESOURCE DEFINITIONS

+ Create Override

➡ Move Definition

Delete

5. Select **default** from the Select User Source dropdown. The default **User Source** contains the admin user you created when first commissioning the Gateway.
6. With the admin user displayed, click on the **Add to Roster** ➡ icon and then **Save Changes** on the bottom right.

Select User Source

default

**Users**

Filter users...

Add All ➡

| USERNAME | CONTACT INFO                                                                        |
|----------|-------------------------------------------------------------------------------------|
| admin    |  |

Showing 1 of 1 items

**On-Call Roster**

Remove All

| USERNAME | CONTACT INFO |
|----------|--------------|
| admin    | ⬆ ⬇ ⬇        |

Showing 1 of 1 items

Cancel

**Save Changes**

Your admin user is now part of the roster.

## Creating an Alarm Notification Profile

Next, we'll set up an Email Notification Profile for our Notification Profile. All Notification Profile options and their settings are described on the [Notification Profile Types](#) page.

1. Navigate to **Services > Alarming > Notification**.
2. Click on **Create Profile +**.

3. Select the **Email Notification** option. Click **Next**.

4. Fill in the required fields. Take note of the **Username** field, as you will need this value **later**. Once you have filled out the form, click **Create Alarm Notification Profile**. In this example, we used the following values:

- Name: **Email Profile**
- Hostname: [mail@inductiveautomation.com](mailto:mail@inductiveautomation.com)
- Username: [user@inductiveautomation.com](mailto:user@inductiveautomation.com)

**Create Alarm Notification Profile**

**Create Alarm Notification Profile**

1. Profile Selection

2. Profile Setup

**Hostname**

mail@inductiveautomation.com

Hostname of the SMTP server to send email through. Only used when Use SMTP Profile is false.

**Port \***

25

Port SMTP service is running on. Only used when Use SMTP Profile is false.

**Enable SSL/TLS**

☐ Connect using SSL/TLS. Only used when Use SMTP Profile is false.

**Username**

user@inductiveautomation.com

Only used when Use SMTP Profile is false.

**Password**

☒ None

☐ Embedded

☐ Referenced

**TWO-WAY SETTINGS**

Back

Create Alarm Notification Profile

Your Email Notification Profile has been created and now needs contact information to be set up before it is ready to use.

## Adding Contact Information

The Email Notification Profile requires matching contact information to be added to our On-Call Roster user in order to send out alarm alerts.

1. Navigate to **Platform > Security > User Sources**.

2. Click on the three dots menu on the default user source, and select **Manage Users**.

## User Sources

View 20

Verify User Source

Create User Source

Edit

Rename

Duplicate

Manage Users

Disable

RESOURCE DEFINITIONS

Create Override

Move Definition

Delete

3. Click on the three dots menu on the admin user, and select **Edit**.

default Manage Users

Users Roles

Create User

| USERNAME | ROLES         | SCHEDULE |  |
|----------|---------------|----------|--|
| admin    | Administrator | Always   |  |

Edit

Assign Roles

Delete

4. Under the Contact section, click **Add +** to add a new row.

5. Change the Type to **E-Mail**, and enter the Email Notification Profile Username in the Value field.

6. Click the **Save** icon, then click **Save Changes**.

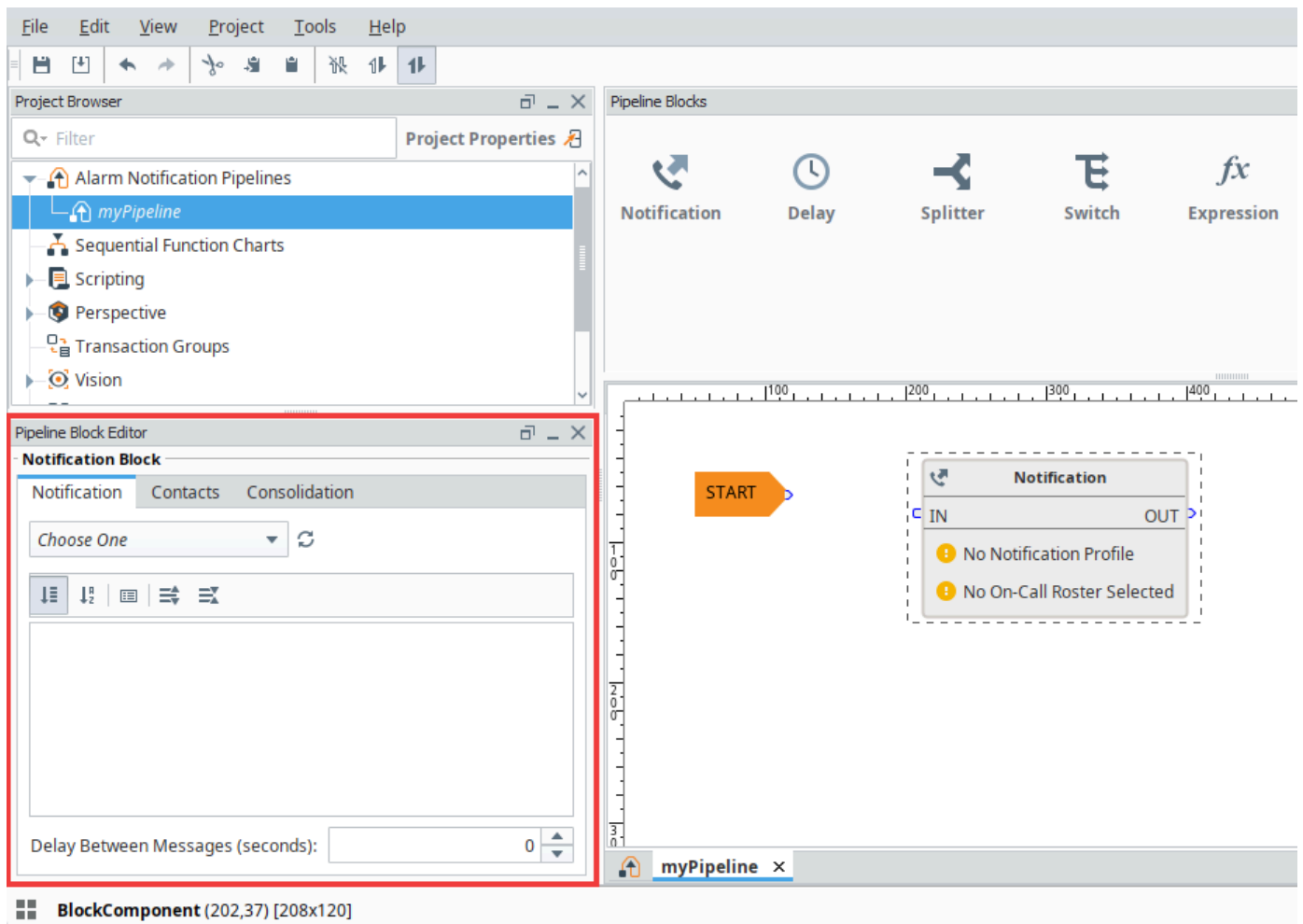
Your admin user is now ready to begin receiving alarm notifications.



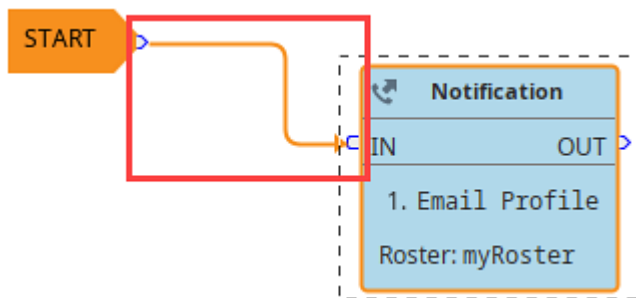
## Creating an Alarm Pipeline

Now, we'll access the Designer to set up an alarm pipeline and configure how and when alarm notifications are sent out.

1. In the Project Browser, right-click on **Alarm Notification Pipelines** and then select **New Alarm Pipeline**. We will name our pipeline **myPipeline**.
2. Drag a **Notification block** from the top bar down to the Alarm Pipeline workspace.
3. Click on the Notification block to display the Notification Block properties in the **Pipeline Block Editor**.



4. In the Notification tab, click on the dropdown menu and select your Notification Profile. Ours is called **Email Profile**.
5. Click on the **Contacts** tab and select the On-Call Roster we **created**. Ours is called **myRoster**.
6. On the Alarm Pipeline workspace, connect the **START** node to the **IN** node of your Notification block, then save your project.



Now that we've created an Alarm Notification Pipeline, we can use it on the tags we want to keep an eye on. In this example, we'll configure an alarm on the **RandomInteger1** tag that's available from the Gateway's Quick Start resources.

1. In the Tag Browser, expand the Random folder, right-click on **RandomInteger1**, and then select **Edit tag(s)**. If your Tag Browser isn't currently displayed, navigate back to the view you created in your Perspective project. The Designer interface will change and show the Tag Browser again.
2. Select the **Alarms** category, then click the **Add +** icon.
3. Under Alarm Mode Settings, change the Mode to **Above Setpoint** and the Setpoint to **85**. This will cause the alarm to trip if the tag value reaches 85 or above.
4. Under **Notification > Active Pipeline**, select the pipeline we created and then click **OK**.

Your alarm will now send an email notification to the admin user's contact information whenever the **RandomInteger1** tag value exceeds setpoint. You can test this out by changing the tag's value, and even add an Alarm Journal Table component to a view to display alarm history. This component works with the Gateway's Alarm Journal from Quick Start.

## Displaying Alarm History

We'll now utilize the Alarm Journal component we put on our project in step 2 of [Preparing Perspective Components](#).

1. Go to your Alarm Journal Table component.
2. Change the **name** property to the actual name of the Alarm Journal configured in your Gateway. If you are using the Quick Start, the name should be `Sample_Alarm_Journal_Profile`.

Your Alarm Journal Table will now populate with the data from the Gateway's Alarm Journal. Further details on the Gateway Alarming settings can be found in the [Alarm Notification](#) section, while more information about alarm states, schedules, and usage with tags can be found in the [Alarming](#) section.

# Accessing Your Project

Now that you have finished your project, you can launch the application to see what it looks like to an operator. You can view your project through the Designer's **Preview Mode**, launch the application through the Designer's **Tools Menu**, or use Perspective Workstation.

## View Your Project in Preview Mode

Preview Mode will allow you to interact with your project as if you were an operator without needing to leave the Designer.

1. Click on the **Project** menu item at the top of the Designer.
2. Toggle **Preview Mode** to enable it.

## View Your Project Through the Tools Menu

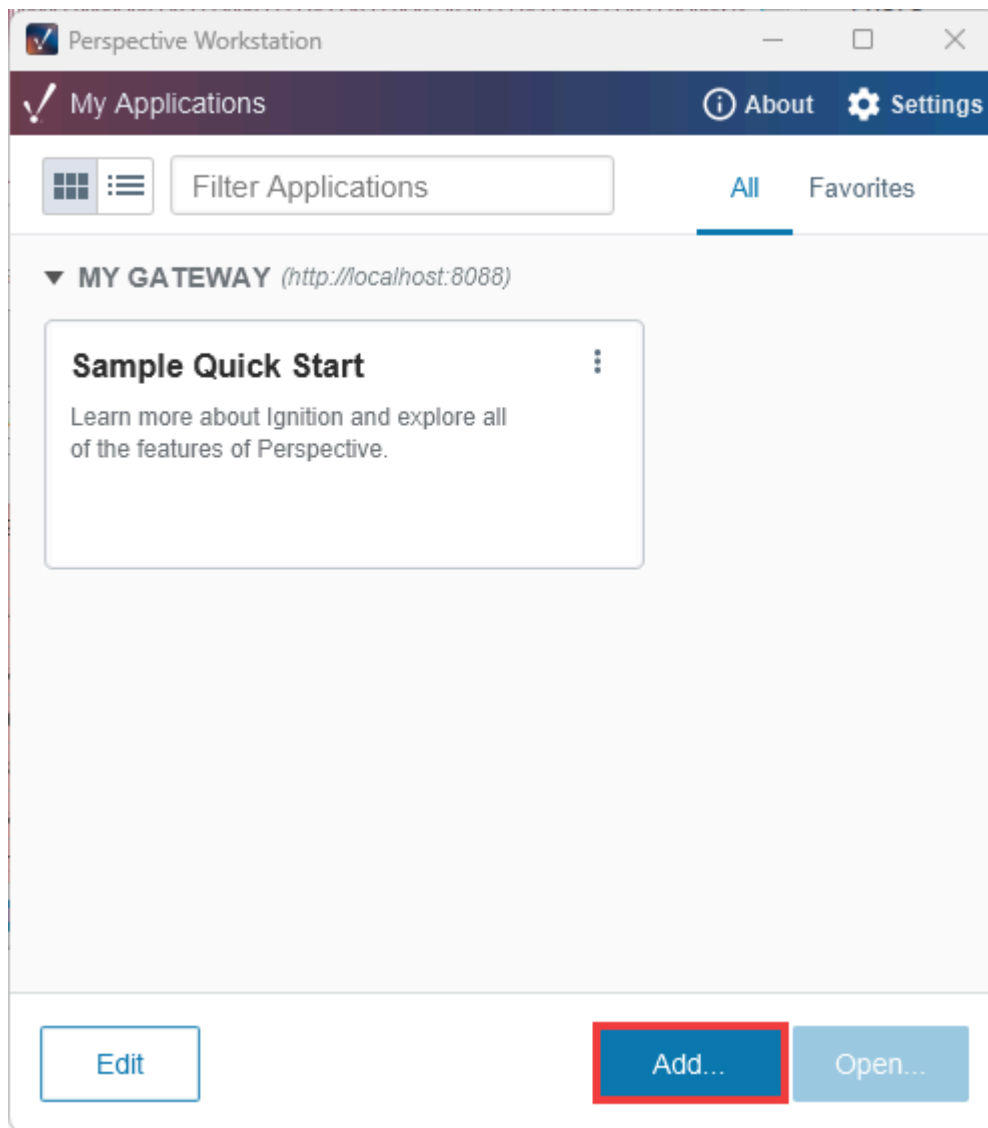
Using the Designer's Tools Menu will allow you to launch your project without using a launcher.

1. Click on the **Tools** menu item at the top of the Designer.
2. Navigate to the **Launch Perspective...** option, then click **Launch Session**.

## View Your Project Using Perspective Workstation

Perspective Workstation is usually how operators would launch your Perspective project. Because of this, it is recommended to ensure your project launches correctly through the Perspective Workstation launcher.

1. Open the Perspective Workstation launcher we installed in the **Downloading and Installing Ignition** section.
2. Click **Add...** on the bottom of the launcher.



3. Select the local Gateway, then click **Select Gateway**.

Filter Gateways

| Name       | URL                       | Version   | OS                                                                                  | System      | Status               |
|------------|---------------------------|-----------|-------------------------------------------------------------------------------------|-------------|----------------------|
| My Gateway | http://192.168.179.1:8088 | 8.3.0-rc1 |  | Independent | <span>RUNNING</span> |
| My Gateway | http://localhost:8088     | 8.3.0-rc1 |  | Independent | <span>RUNNING</span> |
|            |                           |           |                                                                                     |             |                      |
|            |                           |           |                                                                                     |             |                      |
|            |                           |           |                                                                                     |             |                      |
|            |                           |           |                                                                                     |             |                      |
|            |                           |           |                                                                                     |             |                      |
|            |                           |           |                                                                                     |             |                      |
|            |                           |           |                                                                                     |             |                      |
|            |                           |           |                                                                                     |             |                      |

Scanning local network for available gateways...

Cancel

Select Gateway

4. Select the project we just created, then click **Add Application(s)**. Your project will be added to the **My Applications** window.

Filter Applications

☐

**Sample Quick Start**  
Learn more about Ignition and explore all of the features of Perspective.

☒

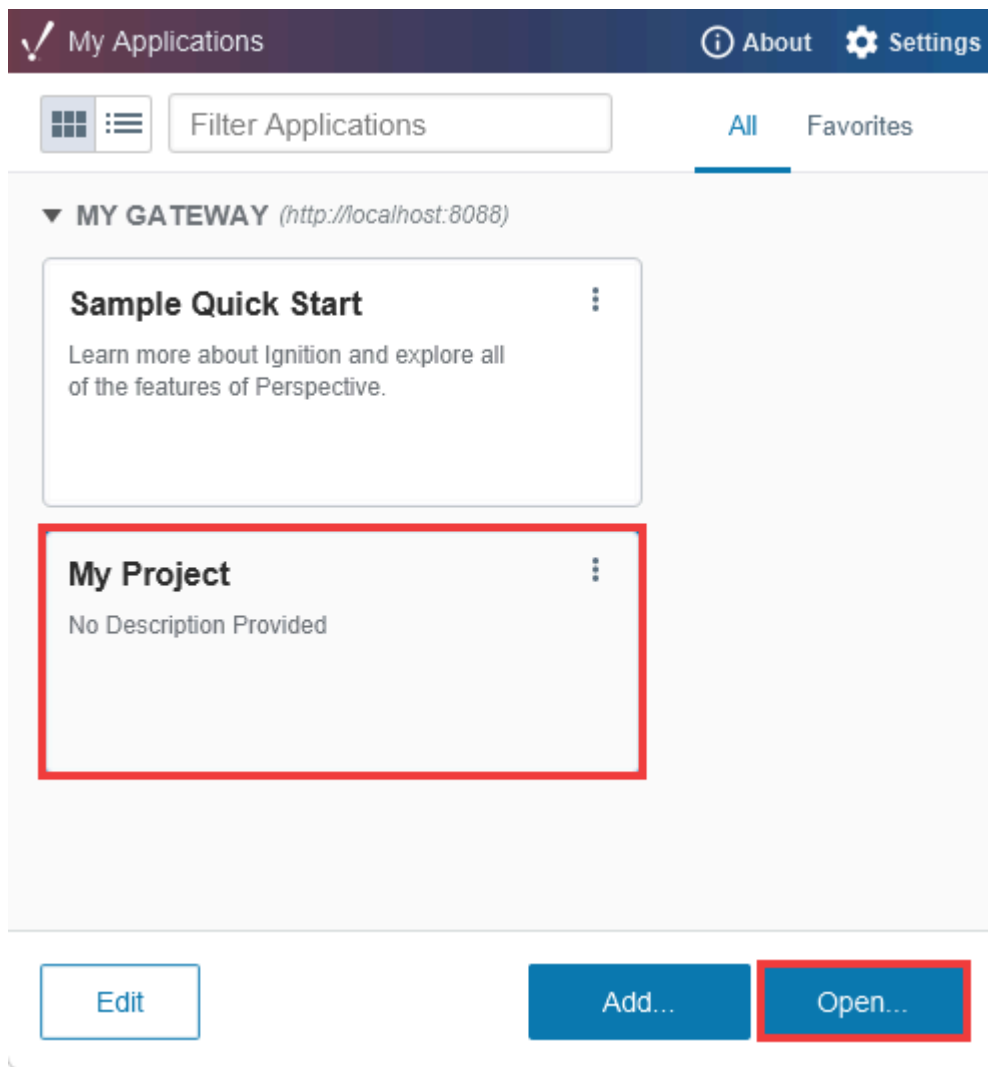
**My Project**  
No Description Provided

Back

Select All

Add Application(s)

5. Click on your project, then click **Open....**



Perspective Workstation will launch your project and you can now interact with it as if you were an operator.

# Installing and Upgrading Ignition

The installation process for Ignition is designed to be as simple as possible. You can find installers on our Downloads page: <https://inductiveautomation.com/downloads/ignition/>.

The Downloads page has the dedicated Installers (called "installer" for all major operating systems) and ZIP files. Both options install Ignition, but the installers are generally easier to use. Download an installer and head to the appropriate section below. For information on ZIP file installation instead, refer to the [ZIP File Installations](#) page.

Make sure your system meets our minimum system requirements, which are also listed on our Downloads page.

The installer will provide timestamped logs for installs and upgrades in the logs directory. Timestamped uninstall logs are stored in the root install directory.



**TIP**

Learn how to [verify that your installation of Ignition is genuine](#) at the bottom of this page.

## Software Bill of Materials

A Software Bill of Materials in SPDX 2.2 (JSON) format is included when installing Ignition. The SBOM can be found in the installation directory at SBOM.txt. Third Party Licenses and Copyright Notices can be found at Notice.txt, also located in the installation directory.

## Install Ignition

The process described below demonstrates a basic Ignition installation. If you are looking for more advanced installation information, such as with Docker, refer to the [Advanced Deployment](#) section.

1. Download an installer from our [Downloads](#) page.
2. Run the installer.

**Windows Installations**

---

**Linux Installations**

**macOS Installations**





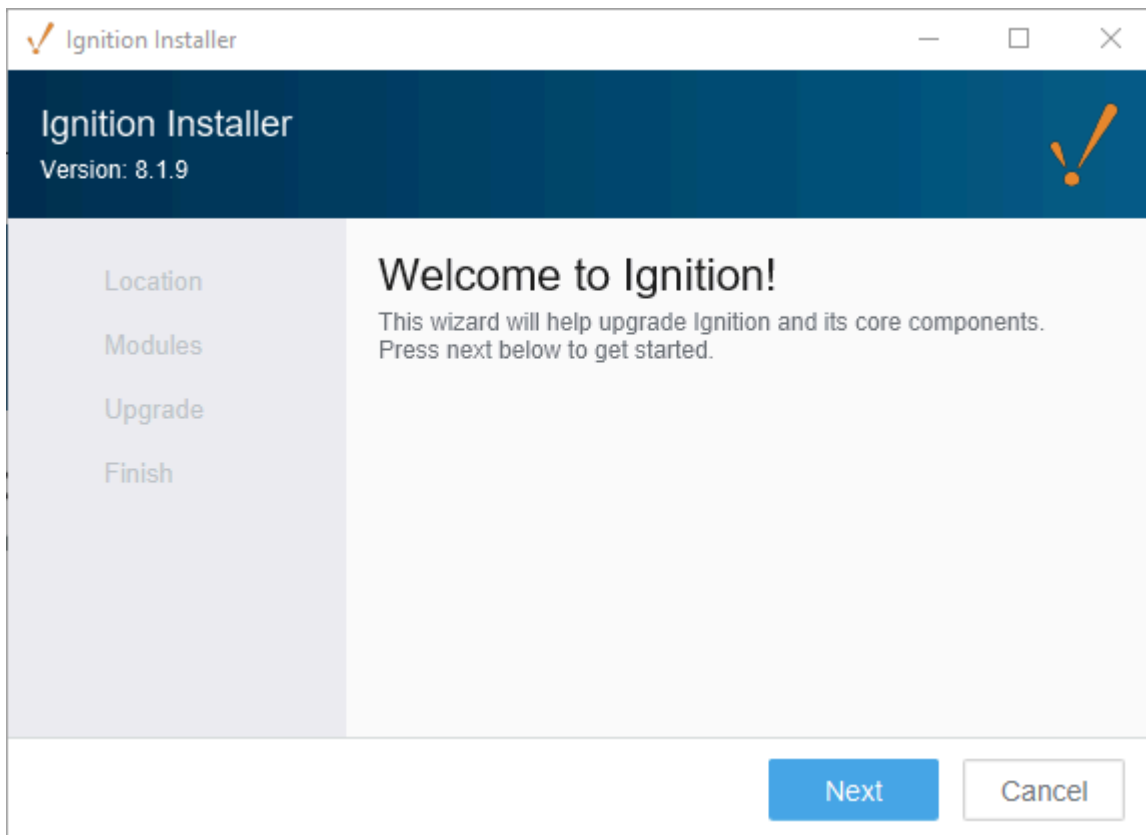
INDUCTIVE  
UNIVERSITY

## Installing Ignition on Windows

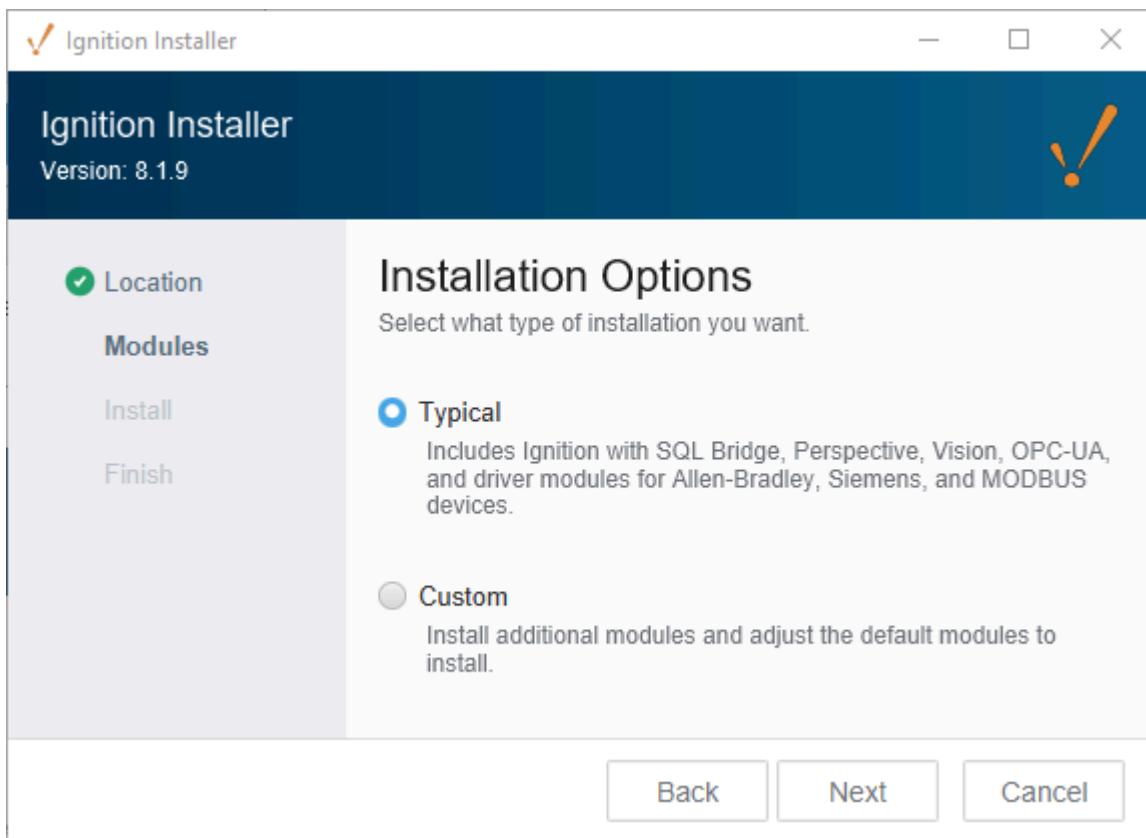
[Watch the video](#)

### CAUTION

Windows has a 255 character limitation that may cause issues when copying over file paths or creating backups due to Ignition's file storage configuration. See the [Working with Long File Paths](#) page for more information on how your system may be impacted.



3. Select the installation type and follow the steps in the installation wizard. The **Typical** option includes a selection of many popular modules. Additional modules can be added after the installation, so we will use the **Typical** option for now.



## INSTALLER SETTINGS BREAKDOWN

In most cases you can use the default settings in the installer. This section describes what each setting does.

- **Default Installation Directories** This determines the installation directory. You're free to pick the directory you wish. See the [Ignition Default Installation Directories](#) section below for the default paths.
- **Gateway Service Name (Windows Only)** This field allows you to choose the service name of Ignition, as it appears in the operating system's service listing.
- **Restore from Backup (Optional)**

**New in 8.3.8** Lets you select a Gateway backup (`.gwbk`) file to restore on the first Gateway startup. Leave the field blank to skip and configure a new Gateway instead. See the [Gateway Backup and Restore](#) page for more details on how to restore a Gateway backup after installation.

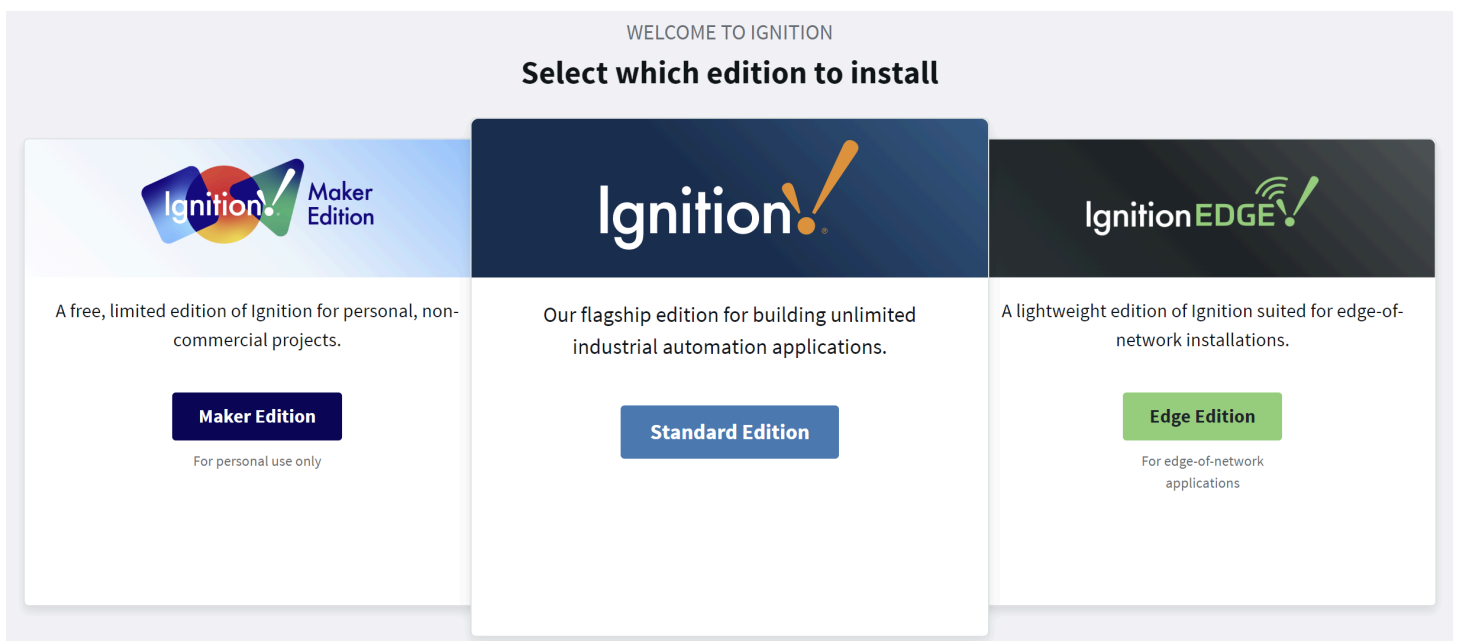
- **Installation Options** Allows which modules are included in your base installation. Your choices are Typical and Custom. The Typical option will use a select list of commonly used modules. The Custom option allows you to install specific modules. In most installations the Standard option will suffice, and you can always add and remove modules after the installation process.

- **Start Ignition Now** Once the installer finishes, you'll be provided with an option to start the Gateway immediately. In most cases this is the desired option. You would only opt out of this choice if you didn't want the Gateway to start once the installer finishes.

Once finished, a web browser will open, and start off the System Commissioning process.

- **Install As a Service (Linux and MacOS only)** Allows you to install Ignition as a service, allowing you to manage certain actions via command line. It is recommended to opt into this setting. For Windows systems Ignition is installed as a service by default as it is a requirement for Ignition to run.

4. After the installation wizard finishes, a web browser will open and start the commissioning process. At this point you'll need to select your edition.



- **Standard Edition** - Unlimited edition of our flagship platform. Designed for commercial use.
  - **Edge Edition** - A lightweight edition of Ignition suited for edge-of-network installations.
  - **Maker Edition** - A free, limited edition of Ignition for personal, non-commercial projects.
5. Follow the steps in the commissioning process to complete installation. The System Commissioning process is a series of steps that further configure your Gateway. This process begins after installation or upgrading. In addition, it can be re-triggered via a password reset with the **Gateway Command-Line Utility**.
- **Set the Gateway Network Port:** Commissioning can set the Gateway Network port in addition to the HTTP and HTTPS port. Clean installs of Ignition will check the default ports for their availability. If no ports are available, the Gateway will iterate that port number until

one is found that is available. These ports can be modified during the commissioning process.

Existing or upgraded Gateways will not search for available ports, and will result in a faulted Gateway.

**i NOTE**

By default, Linux will not allow you to run on port 1024 and below. If you need to run on one of these ports, such as port 80, you can add the `CAP_NET_BIND_SERVICE` capability to your systemd service configuration override file.

- **Activate License (Maker Edition Only):** When installing Maker Edition, you'll be asked to provide a License Key (an 8 digit string) and an Activation Token (a considerably longer string). Both of these can be acquired for free from your Inductive Automation account: <https://account.inductiveautomation.com/>.
- **Create a User:** This step asks you to create an initial user. This user will have full access to Ignition, although you're free to modify this user later. You'll need this user account to make any changes to Ignition, so make sure you remember these credentials. Otherwise you'll need to perform a password reset. See the [Gateway Command-Line Utility](#) page for this process.
- **HTTP Configuration:** Allows you to specify the ports Ignition uses. By default, HTTP is **8088**, and HTTPS is **8043**.

Once you finish the commissioning process, your service will start.

SETUP COMPLETED

# Start and Launch the Gateway Now?

Start Gateway

## Ignition Default Installation Directories

The default directories for each operating system are listed below.

Windows

C:\Program Files\Inductive Automation\Ignition

MacOS

/usr/local/ignition

Linux

/usr/local/bin/ignition

## MacOS and Linux Installation Directory

Mac and Linux installations contain a `ignition.sh` file and `ignition-util.sh` file, which both contain some configuration parameters for the installation. Modifying these files is not advised, unless directed to by a member of our support team. Instead, an `ignition.conf` file, which is also located in

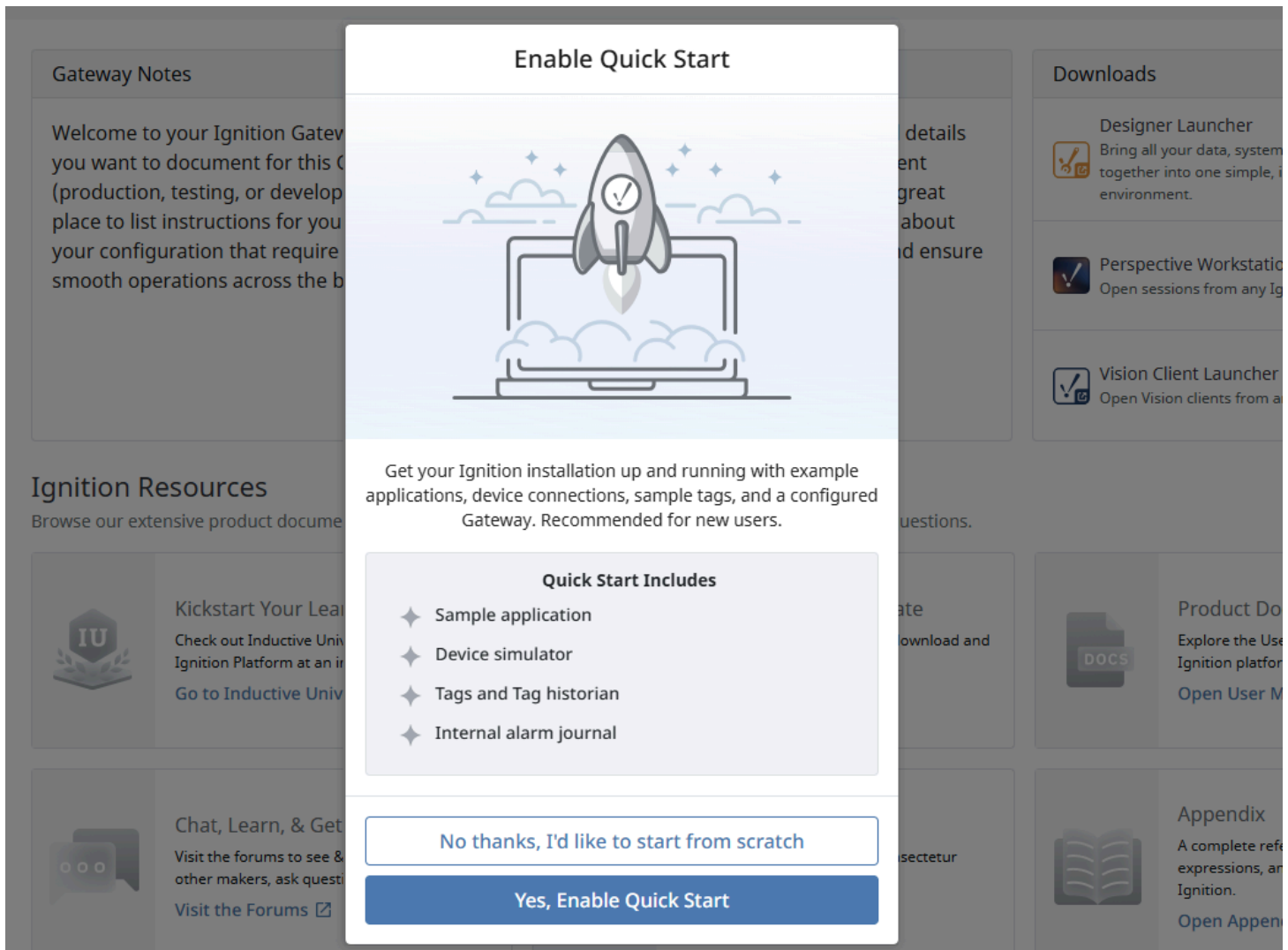
the installation directory, should be used instead. Additionally, during installation on Mac and Linux, the installer will create a sudoer file at `/etc/sudoers.d/99-<serviceName>`, with the service name being Ignition-Gateway by default. This ensures the Gateway can be restarted without an interactive login. In most cases, the sudoer file does not need to be modified or maintained. However, more information can be found in the `ignition-util.sh` file in the installation directory.

## Quick Start Configuration

Once the installation process has finished, you'll be redirected to the Gateway Webpage. From there you'll be asked to opt into the Quick Start configuration, which makes several configuration changes to the system. Quick Start can only be enabled upon a new installation.

The following changes are made once Quick Start is enabled:

- Creates an internal SQLite database connection.
- Configures a device connection to a **Programmable Device Simulator** instance, and adds Tags from the simulator into a Tag provider.
- Configures an internal alarm journal.
- Creates a sample project.



## Start or Stop Ignition

After installing with the Installer, Ignition will have a service representing it on the operating system. By default Ignition will start when the system starts, but you can manually start and stop the system with the following terminal commands:

### Windows

```
## The examples below assume "Ignition" is the service named used during
installation
## (which also happens to be the default service name).
## You may need to modify the examples below using your system's service name.

net start Ignition
net stop Ignition
```

### Mac

```
/usr/local/ignition/ignition.sh start
/usr/local/ignition/ignition.sh stop
/usr/local/ignition/ignition.sh restart
```

Linux

*## The examples below use the default installation directory*

```
/usr/local/bin/ignition/ignition.sh start
/usr/local/bin/ignition/ignition.sh stop
/usr/local/bin/ignition/ignition.sh restart
```

## Upgrade Ignition

Upgrading Ignition is as easy as running the installer. When you run the installer from the same directory as a previous install, our installers are able to detect that Ignition is already installed. If Ignition is already installed, the installer will ask if you would like to proceed with the upgrade. A wizard takes you through the upgrade in a similar workflow as installation workflow.

Before starting the upgrade process, it is **strongly advised** to take a [Gateway backup](#) of your system. You should also set aside time to upgrade your Launcher. When a Gateway version is ahead of the Launcher, the Launcher will notify you that an update is available. See the [Upgrading Launchers](#) section for more information.

Ignition installers can be used to upgrade any edition of Ignition (Edge, Maker, or Standard) with the exception of ARM, as it will require a [ZIP installer for upgrading](#).

### JDBC DRIVERS AND UPGRADING

Sometimes new versions of Ignition will incorporate new JDBC drivers, which are used to connect to SQL databases. When upgrading Ignition, the JDBC drivers will **not** be upgraded. The reason being, is that you should only need to change the JDBC driver if you upgrade your database. See the [JDBC Drivers and Translators](#) page for more details.

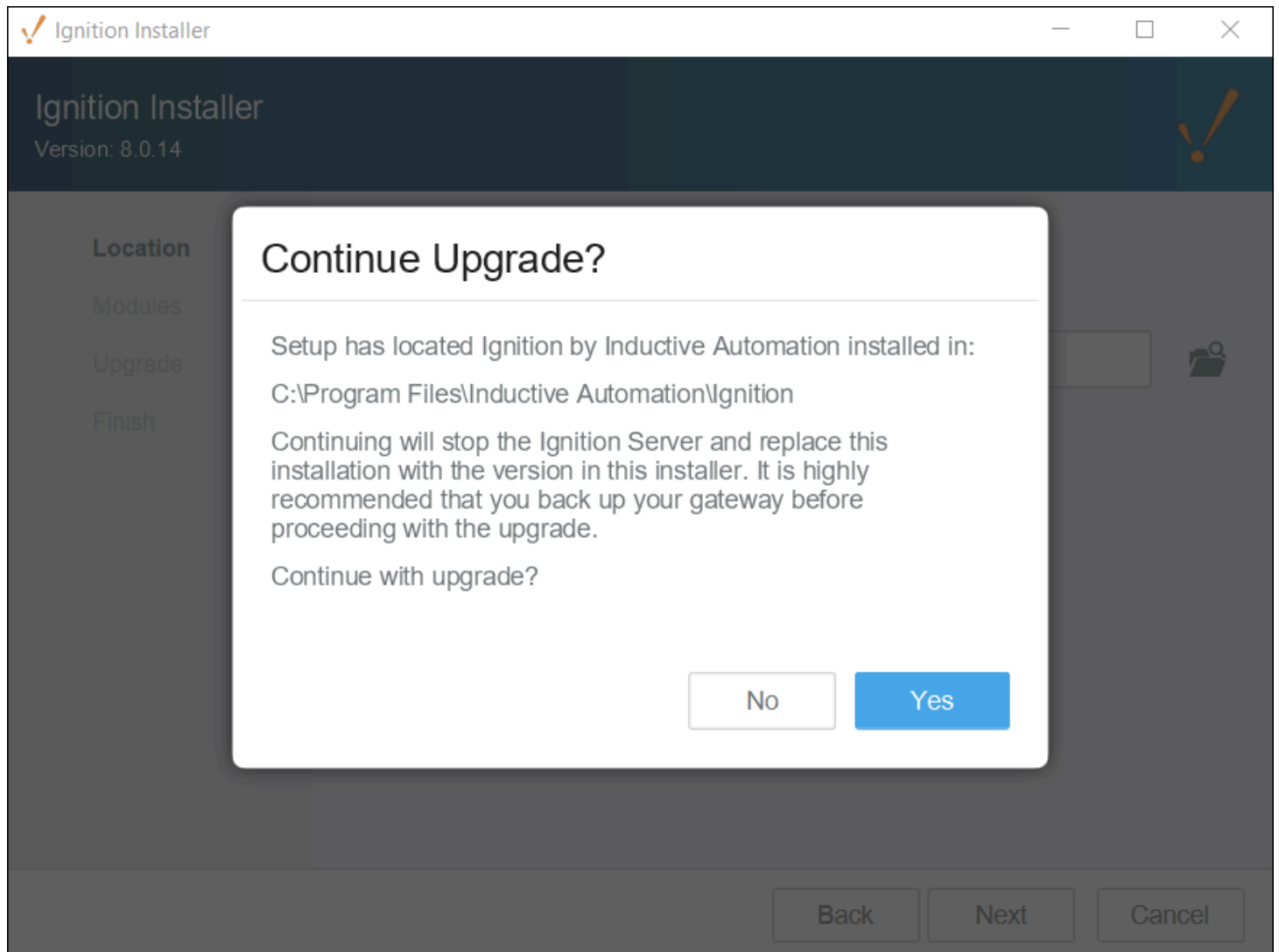
### IMPORTING LEGACY GATEWAY BACKUPS

Gateways running on Ignition versions earlier than 8.1 cannot be directly upgraded to 8.3. They must first be upgraded to 8.1, and then upgraded to 8.3. This limitation also applies to restoring

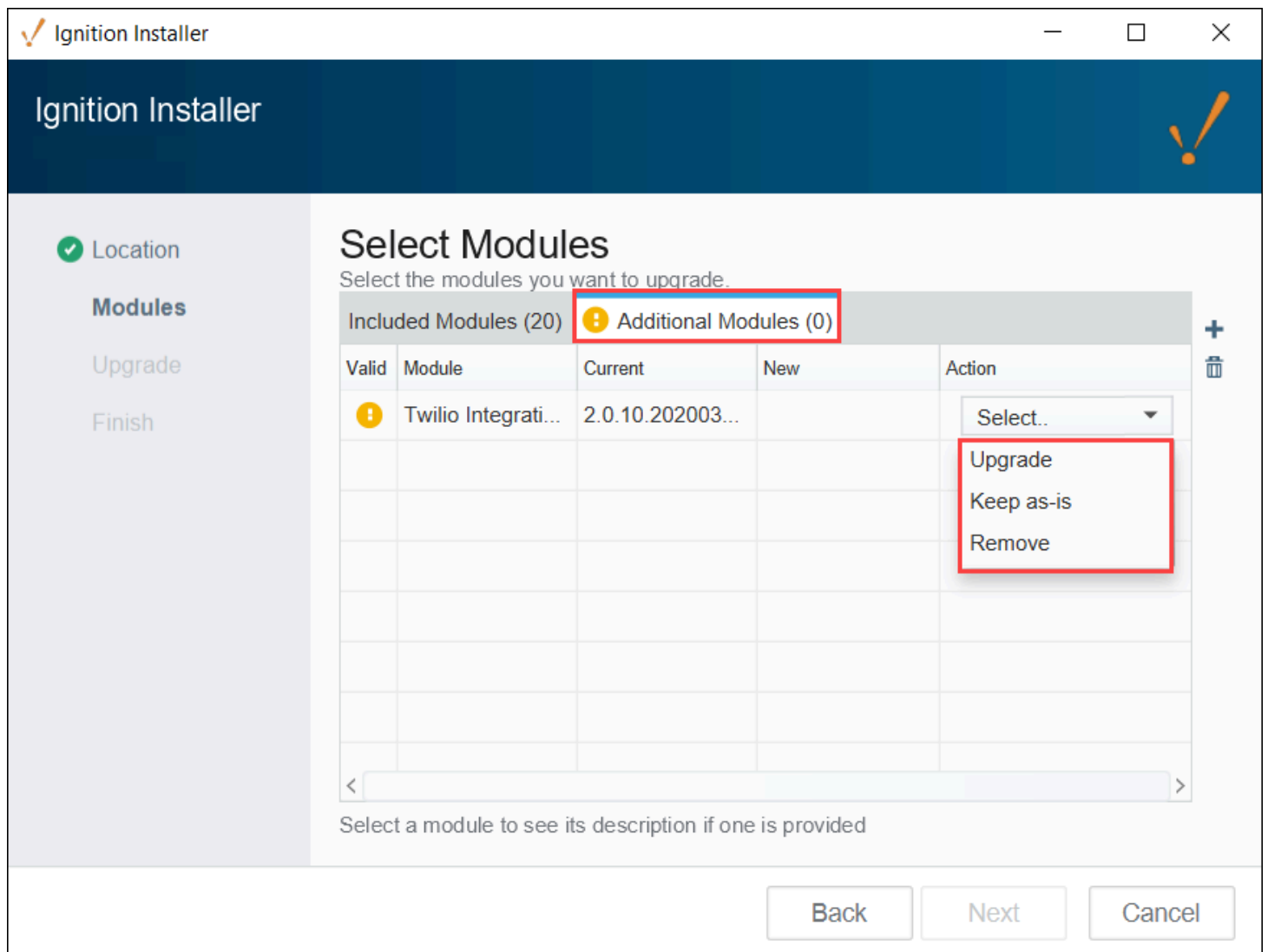


Gateway backups, where you will first need to upgrade the Gateway backup to version 8.1, then restore the 8.1 Gateway backup onto your 8.3 Gateway.

During the upgrade process, the Gateway will have to restart, so make sure to account for downtime when upgrading.



When you upgrade Ignition, you'll also be given the option to update any additional modules you currently have installed, including third party modules. On the Select Modules screen, there is a tab for the modules included in your version of Ignition, and a tab for Additional Modules you may be using. Under the Action column, you can choose to upgrade or remove the module, or leave it unchanged.



## Updating License for an Upgrade

If you are updating from one major version to the next, you will need an updated license. You can do this before upgrading so there is no unlicensed time after the upgrade.

1. Let us know. You can reach Inductive Automation by phone at **(800) 266-7798**. Some major upgrades include new modules or have modified the functionality of pre-existing modules. If your license needs to be updated, call us and we can guide you through it. If you are updating from one version to the next, we can talk you through what is different and what new functionality is available. See the [New in this Version](#) page for more specifics about what was updated in the various versions.

### NOTE

If your license is covered by a support plan, you have Upgrade Protection which automatically keeps your platform and module versions up to date in our system. Refreshing your license on your Gateway will synchronize the license on your server with the updated license on our activation servers.

2. Reload your license. Once your license is updated in our system, go to your Gateway and navigate to **Platform > System > Licensing**. Expand the three dots menu and select Reactivate for the license that was changed. For a detailed guide on reloading a license, see [Updating a License](#).

## Upgrading a Redundant Pair

When performing the upgrade locally, we recommend upgrading the Backup first. The Master will be unaffected and remain active during this process. After the upgraded Backup comes online, the Master can fail over to the Backup. It's also recommended to use Manual recovery mode to control when the Master takes over again. The active Backup can collect redundancy sync info, while the Master goes down for upgrade. Then, once both Gateways are on the same version again, the redundancy sync data can be passed from the Backup to the Master.

### NOTE

This procedure applies to both upgrades between minor versions and upgrades between major versions, such as 8.1 to 8.3. If you are upgrading between major versions, be sure to review the [8.3 Upgrade Guide](#) before making any changes.

The following procedure details this process:

1. Navigate to **Platform > System > Redundancy** on your Master Gateway.
2. Click **Configure Redundancy** to open the Redundancy Settings panel.
3. Under Master Node Settings, change the Recovery Mode to **Manual**. This keeps the Master Gateway inactive after it has been upgraded and allows you to decide when the Master Gateway can take over.
4. Click **Save Changes** and click **Confirm**.
5. Upgrade and start your Backup Gateway.
6. After the Backup Gateway has started again, navigate to **Platform > System > Redundancy** on your Master Gateway.
7. Select **Force Failover** to set your Backup as your active Gateway.
8. Upgrade and start your Master Gateway.
9. Navigate back to **Platform > System > Redundancy** on your Master Gateway.
10. Confirm that the Master Gateway and Backup Gateway are connected.
11. Select **Assume Control** to set your Master Gateway as your active Gateway.

# Reset the Password

To reset the main password for the user with full privileges, use the Gateway Command-line Utility (gwcmd) utility. The `gwcmd` utility triggers system commissioning, and prompts the user to reset the username and password for the main user (with full privileges) after the Gateway restarts. For more information, see the [Gateway Command-line Utility - gwcmd](#) page.

## Uninstall Ignition

### NOTE

Uninstalling Ignition will remove any projects or Gateway level configurations you made. If you wish to preserve anything, make sure to take a [Gateway backup](#) first.

To uninstall Ignition, run the uninstaller file. This file can be found in the main Ignition installation directory, for example:

Windows

```
C:\Program Files\Inductive Automation\Ignition\Uninstall.exe
```

Mac

```
/usr/local/ignition/Uninstall.app
```

Linux

```
/usr/local/bin/ignition/Uninstall.run
```

## Verify that Ignition Software is Genuine

Code signing is applied to installers to help the OS prevent the installer from being run if it has been tampered with. Notarization is an additional step on macOS that works with Apple's systems to validate that the software has undergone their malicious code scanning.

### EXPECTED CERTIFICATE:

Name of signer: Inductive Automation, LLC

CN = DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1

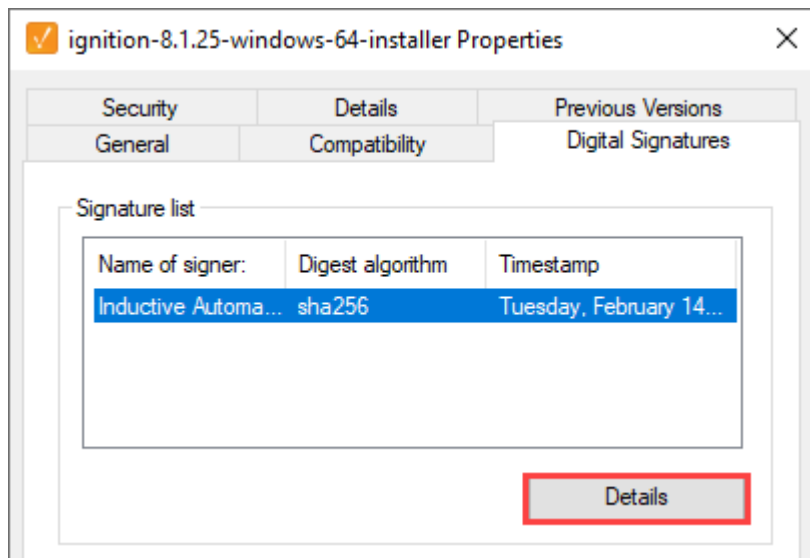
## Windows

## macOS Installations

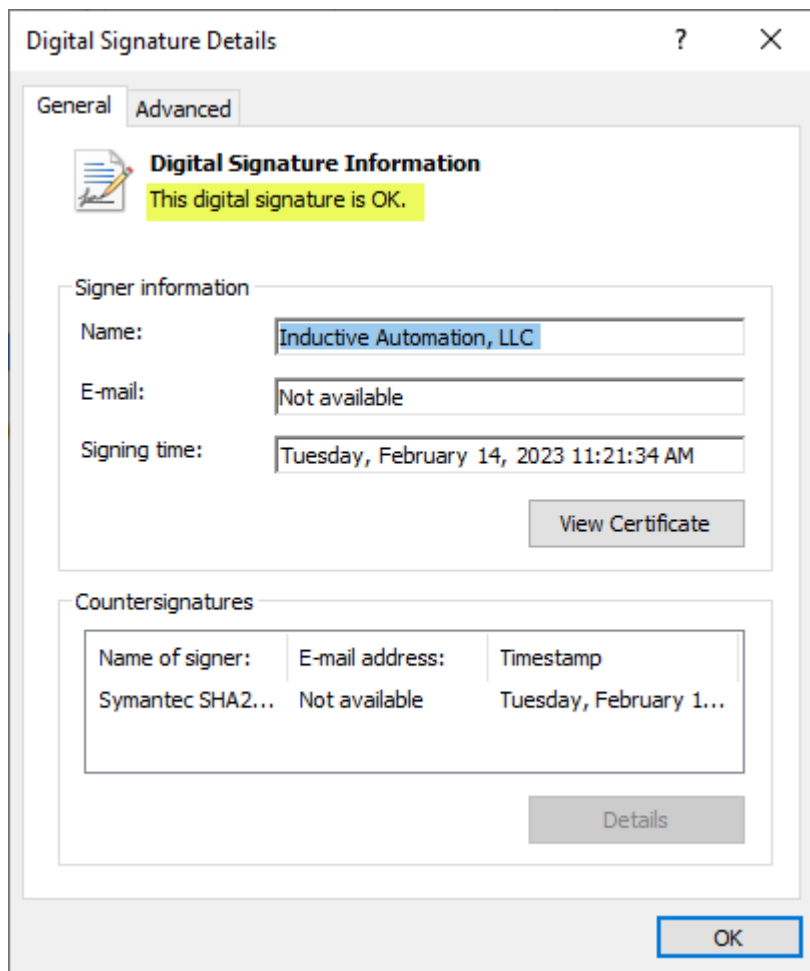
## Linux Installations

View verification of the digital signature on Ignition's installer on Windows in the User Account Control popup when running the installer. It can also be viewed in the Digital Signatures section of the file Properties dialog.

1. Right-click on the installer and select **Properties**.
2. Under the Digital Signatures tab, select the signature from the Signature list and click **Details**.



3. If the text **This digital signature is OK** appears under the General tab, the installer is genuine and has not been manipulated.



## Verify the Download is Authentic by Hash Comparison

The Ignition automated build process writes a precalculated fingerprint (hash) to the download site allowing users to verify the authenticity of the download file. On the [Downloads](#) page, click **sha-256** to view the hash for your selected installer file. You may also copy this hash to your clipboard for comparison.

### System Installers (includes all modules)

|  Microsoft Windows | Version |                         |
|-------------------------------------------------------------------------------------------------------|---------|-------------------------|
| <a href="#">Ignition - Windows Installer 64-bit (1.4 GB)</a>                                          | 8.1.25  | <a href="#">sha-256</a> |
| <a href="#">Ignition - Windows 64-bit zip (1.4 GB)</a>                                                | 8.1.25  | <a href="#">sha-256</a> |
| <a href="#">Ignition Edge - Windows 64-bit zip (1.4 GB)</a>                                           | 8.1.25  | <a href="#">sha-256</a> |

c7124792a0e9e54c0c3df2647bc8a4b7ea32  
bb27d881b6e3fd43e0e72c20e1  
[Copy to clipboard](#)

A SHA256 hash of the downloaded installer package can be compared to the values on the website with terminal commands such as:

```
PowerShell
```

```
Get-FileHash path\to\installer
```

macOS/Linux

```
sha256sum /path/to/installer
```

## Verify an Ignition Module Download is Authentic - Advanced

Ignition modules are collections of files and resources that are loaded and run by the Ignition Platform. Inductive Automation publishes a number of modules and third-party authors can also create modules through the Ignition Module SDK. In order to help verify file integrity of these modules, code signing is applied to ensure that the contained files and resources within the module package have not been tampered with.

Verification of a given Ignition module's code signatures is handled automatically by the platform. The following manual verification steps (requires **openssl**) are listed below to provide a fuller understanding of the mechanisms at play:

1. Extract the **.modl** file as a zip file into a working directory.
2. Observe the contained **certificates.p7b** file which is a PKCS#7 package containing the certificate chain used for generating the signatures for each of the files within the **.modl** package.
3. Observe the contained **signatures.properties** file. Each line contains a path to a file within the **.modl** package and a base64-encoded signature for the file.
4. Extract the public key **signingPublicKey.pem** from the **certificates.p7b** file with the following steps:
  - **openssl pkcs7 -outform PEM -in certificates.p7b -print\_certs > certificates.cer**
  - **openssl x509 -pubkey -noout -in certificates.cer > signingPublicKey.pem**
5. Decode the base64 content for a given file (from **signatures.properties**) into a signature file, e.g. **signature.sign**.
6. Verify the signature of the file with the following:
  - **openssl dgst -sha256 -verify signingPublicKey.pem -signature signature.sign <file from .modl>**
7. Observe a **Verified OK** message indicating that the signature from **signatures.properties** for the respective file is correct.

# System Rollback

Downgrading Ignition is not a supported use case of the Ignition upgrade, and can lead to unexpected problems. If you need to roll back to a previous version of Ignition, it is recommended to instead perform a clean reinstallation and restore a Gateway backup from the same version or older. When reinstalling Ignition, the Ignition service should first be uninstalled, and the Ignition installation directory itself should be deleted.



# Command Line Installations

Command line argument keys can be used to modify the installation process. Each operating system supports launching with arguments that contain some small modifications to ensure they are passed through to the installer:

- Windows: a `--%` arg should go before installer args
- Mac: requires `open -a` command with `--args` before the args to pass to the installer
- Linux: a `--` arg should go before installer args

Note that all arguments should be quoted.

## Arguments Table

The table below lists the supported arguments.

| Command Line Argument Key | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Possible Values                                                                                                                                                                                                                                                                                                                                                                                    | Example             |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| unattended                | <p>The unattended install mode to run the installer in. It runs with all default values unless otherwise specified.</p> <p>The unattended upgrades remove known IA modules that are deprecated, leaves third party as they are, and upgrades currently installed bundled modules. Additionally, unattended upgrades do not trigger the Ignition service to start automatically. The Ignition service <i>must</i> be started by a user.</p> <p>The argument also works with the uninstaller, allowing for unattended uninstalls.</p> | <ul style="list-style-type: none"> <li>• <b>graphical</b>: run with full size installer window but no interaction</li> <li>• <b>minimal</b>: shows a progress bar only unless errors occur</li> <li>• <b>text</b>: feedback on the command line only, no GUI</li> <li>• <b>none</b>: completely silent, no feedback except for the log file when complete regardless of success or fail</li> </ul> | "unattended=minir   |
| textMode                  | Whether to run this installer in <i>interactive</i> text mode regardless of graphical support. Note that <i>unattended</i> supersedes this value.                                                                                                                                                                                                                                                                                                                                                                                   | true - run in text mode                                                                                                                                                                                                                                                                                                                                                                            | "textMode=true"     |
| location                  | Overrides the default installation directory, allowing you to specify where Ignition should be installed.                                                                                                                                                                                                                                                                                                                                                                                                                           | A fully qualified file path                                                                                                                                                                                                                                                                                                                                                                        | "location=/usr/locæ |
| logLevel                  | The logging level for the installer. The default is                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Options are (from most granular to least                                                                                                                                                                                                                                                                                                                                                           | "logLevel=trace"    |

| Command Line Argument Key | Description                                                                                                                                                                                                                                                                                                                                                          | Possible Values                                                                                                                                                                                                                   | Example                  |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
|                           | INFO, however more detail can be provided, revealing more information about the install process, as wells as the installer's internal operations.                                                                                                                                                                                                                    | granular): <ul style="list-style-type: none"> <li>• trace</li> <li>• debug</li> <li>• info</li> <li>• warn</li> <li>• error</li> </ul>                                                                                            |                          |
| user                      | Sets the ownership of the install to this user.                                                                                                                                                                                                                                                                                                                      | The username (as recognized by the operating system) that should be the owner of the installation.                                                                                                                                | "user=myUser"            |
| serviceName               | <p>Sets the service name for the Gateway. Defaults to "Ignition". When running the graphical installer, the service is installed immediately on Windows and set for optional future installs on Linux/Mac.</p> <p>When using this key with the unattended key during an upgrade, the existing service on windows will be removed, and replaced by a new service.</p> | my-gateway                                                                                                                                                                                                                        | "serviceName=my gateway" |
| autoStart                 | Boolean that specifies whether or not to automatically start the Gateway after installing or upgrading is complete. By default, clean installs will automatically start the Gateway, but upgrades will                                                                                                                                                               | <ul style="list-style-type: none"> <li>• <b>true</b>: starts the Gateway without any user input after installing/upgrading.</li> <li>• <b>false</b>: forces the install/upgrade to not automatically start the Gateway</li> </ul> | "autoStart=true"         |

| Command Line Argument Key | Description                                                             | Possible Values                    | Example |
|---------------------------|-------------------------------------------------------------------------|------------------------------------|---------|
|                           | not. Will revert to default behavior if this argument is not specified. | after install/upgrade is complete. |         |

## Example Commands

The following examples demonstrate how arguments can be used when running the installer. For the purposes of these examples, any mention of a user directory will use **yourUser**, and the Ignition version number in the installer name will be **8.1.14**. These should be replaced by appropriate values when attempting to run the installer on your system. Additionally, depending on the Ignition version you are installing you may also need to remove the **x** from **x64** text.

### Windows

```
# Runs the installer on command line only and requires user interaction.
C:\Users\yourUser\Downloads\ignition-8.1.14-windows-x64-installer.exe --%
"textMode=true"

# Runs the installer on command line, changes the default install directory, and
uses the "text" unattended mode.
C:\Users\yourUser\Downloads\ignition-8.1.14-windows-x64-installer.exe --%
"unattended=text" "location=C:\Ignition"
```

### Mac

```
# Runs the installer on command line only and requires user interaction.
open -a /Volumes/IgnitionInstaller/ignition-8.1.14-osx-installer.app --args
"textMode=true"

# Runs the installer on command line, changes the default install directory, and
uses the "text" unattended mode.
open -a /Volumes/IgnitionInstaller/ignition-8.1.14-osx-installer.app --args
"unattended=text" "location=/Users/yourUser/Desktop/test"
```

### Linux

*# Runs the installer on command line only and requires user interaction.*

```
"/home/yourUser/Downloads/ignition-8.1.14-linux-x64-installer.run" --  
"textMode=true"
```

*# Runs the installer on command line, changes the default install directory, and uses the "text" unattended mode.*

```
"/home/yourUser/Downloads/ignition-8.1.14-linux-x64-installer.run" --  
"unattended=text" "location=/home/yourUser/Desktop/test"
```

# ZIP File Installations

Aside from the graphical installers, our downloads page features ZIP files that can be used to install and run Ignition. The ZIP file installation process differs from the graphical installation process. Using the ZIP files to install involves following the included README file, which contains instructions on how to use the content of the ZIP.

## CAUTION

If you are performing an upgrade, it is important to **not** overwrite the **Ignition Configuration File (ignition.conf)**, as overwriting the ignition.conf file can cause the upgrade to fail.

## Upgrading Ignition Service on Linux

If you installed Ignition as a service on Linux, you will need to first remove the service before upgrading to a new edition and reinstalling the service.

```
./ignition.sh remove
```

## Deploying Ignition to Another System

Some users are interested in "preconfiguring" an Ignition Gateway. That is, configuring an instance of an installation, and then moving the installation files to a new server. This can be useful in cases where you're attempting to push out new Ignition installations via command-line interface to multiple separate systems. Normally, you need to install Ignition manually on each of these systems and walkthrough the commissioning process to create an initial user and select an Ignition edition, which defeats the purpose of this whole deployment strategy. Thus, the following example will demonstrate how to deploy a preconfigured Ignition Gateway that has already been commissioned and is ready to start up.

## Requirements

### NOTE

Although you can run the Ignition Gateway and Perspective Sessions on ARM-based Desktops (such as a Raspberry Pi), the Designer, Vision Client, and Perspective Workstation cannot be

run on ARM-based Linux machines. Instead, the Designer, Vision Client, or Perspective Workstation will need to be installed and run from an Intel-based machine.

You'll need the following:

- A ZIP installer for the OS and Ignition Version you're planning to deploy on. ZIP installers can be found on our [Downloads](#) page.
- An existing Ignition Gateway where you already accepted the End User License Agreement (EULA). This existing Gateway must match the Ignition version of the system you're going to deploy to. If you don't have an install available, simply run through the installation process once, agree to the terms in the EULA, and finish the rest of the commissioning process. Accepting the EULA is important because you'll need to manually do this once.
- An Ignition Gateway backup from an existing system. We'll use this to define the initial user, and carry over any other resources we want on the new system. This can be a backup from the Gateway you used in the previous requirement. We'll use this backup to inject a user account that only you have credentials for.

## Example

1. Locate the EULA hash from your existing Ignition Gateway. You will find the hash in the commissioning.json file in Gateway's installation directory:  
`%installDirectory%/data/commissioning.json`.

### NOTE

You'll only find this file on systems that have completed the commissioning process.

Part of the commissioning process involves accepting the EULA. The steps in this guide involve skipping the commissioning process, including the EULA. Thus, to be able to follow along with this guide you'll need to review the terms in the EULA and manually accept them on a separate system.

2. Open the file in a text editor, and copy the value for the `eulaSetup.eula` key, including the quotation marks. For example, assuming a file looked like the entry below, you would copy "XXXXX" (the actual hash will be much longer). Save this value for later, as we'll need to reference it in a future step.

```
{
  "isCommissioned": "COMMISSIONED",
  "connections.useSsl": "false",
  "eulaSetup.eula": "XXXXX"
}
```

3. Next, take the Ignition installer and unzip it into a directory that's easily accessible. This directory will be the **base directory** that we'll ultimately end up deploying to on one or more different servers.
4. In the base directory, edit the **Gateway's configuration file** (ignition.conf) using the text editor of your choice. The file is located at `%baseDirectory%/data/ignition.conf`.
5. Part of the installation process normally includes an edition selection, but we can bypass that by modifying the configuration file to explicitly state which edition the Gateway should be set to. Located the "Java Additional Parameters" line in the configuration file. The should have some entries like the following:

```
# Java Additional Parameters
wrapper.java.additional.1=-Ddata.dir=data
#wrapper.java.additional.2=-Xdebug
#wrapper.java.additional.3=-
Xrunjdpw:transport=dt_socket,server=y,suspend=n,address=:8000
```

at the end of that section, add the following:

```
wrapper.java.additional.2=-Dedition=%value%
```

Where %value% is the edition, you want the deployed system to use: "edge" for Ignition Edge, and "maker" for Ignition Maker. For "standard" edition, simply omit the "=%value%" portion. For example, the file should look something like the following when configuring for Standard edition:

```
# Java Additional Parameters
wrapper.java.additional.1=-Ddata.dir=data
#wrapper.java.additional.2=-Xdebug
#wrapper.java.additional.3=-
Xrunjdpw:transport=dt_socket,server=y,suspend=n,address=:8000
wrapper.java.additional.2=-Dedition
```

And the file would look like the following if deploying Edge edition:



```
# Java Additional Parameters
wrapper.java.additional.1=-Ddata.dir=data
#wrapper.java.additional.2=-Xdebug
#wrapper.java.additional.3=-
Xrunjdwp:transport=dt_socket,server=y,suspend=n,address=*:8000
wrapper.java.additional.2=-Dedition=edge
```

6. Save the changes you made to the configuration file.
7. Also in `%baseDirectory%/data/`, create a text file and call it `commissioning.json`.
8. Edit the newly created commissioning file, and set contents to the following:

```
{
  "isCommissioned": "COMMISSIONING",
  "connections.useSsl": "false",
  "eulaSetup.accepted": "true",
  "eulaSetup.eula": "xxxxxxxxxxxxxxxxxxxxxx",
  "authSetup.username": "admin",
  "authSetup.password": "[e811cfc7]fc3b28ad5f73331c94790129f0931437ac31d59376b0e4b15df580a8841ba165"
}
```

The JSON above does a couple of things, but notably defines an initial user on the new system. The user is **"admin"**, with a password of **"password"**. Later, we'll restore from our Gateway backup which will replace this initial user, but for now, we simply need to have a user to bypass commissioning.

9. In the same commissioning file, replace the value of the `eulaSetup.eula` key with the value you took from step 2.
10. Save the commissioning file.
11. At this point, you're ready to deploy. Take the contents of your base directory, move them to a new server, and perform a normal ZIP installation. When the Gateway starts, it will bypass the commissioning process and the Gateway will immediately startup.
12. Once the Gateway is running, you can use the **admin** user we configured earlier to access the newly deployed instance of Ignition. From here, you can restore from the Gateway Backup file mentioned in the requirements section of this guide. You can do this from **command-line** which would look something like the following:

```
gwcmd --restore /path/to/your/GWBK
```

# Installing or Upgrading a Module



INDUCTIVE  
UNIVERSITY

Installing or Upgrading a  
Module

[Watch the video](#)

## Module Configuration

All module configuration is done from Gateway Webpage in the **Platform > System > Modules** section. The Modules page shows a list of the currently installed modules, their current version, and if they are running properly with a license. The top of the page shows a quick count of the running and licensed modules, so you can easily tell if anything is not working. It is then easy to scroll down through the list to see which modules are having issues.

From here you can also add, remove, enable, and disable modules. Modules integrate their settings into the Gateway configuration tree, and therefore do not offer settings in this section.

✓

Platform

Overview

System

Gateway Settings

Projects

Modules

Licensing

Redundancy

Modes

Store & Forward

Ignition Exchange

Backup & Restore

Security

Modules

Install or Upgrade Module +

STATUS

RUNNING MODULES

32 / 32

LICENSED MODULES

0 / 32

Modules

Filter modules...

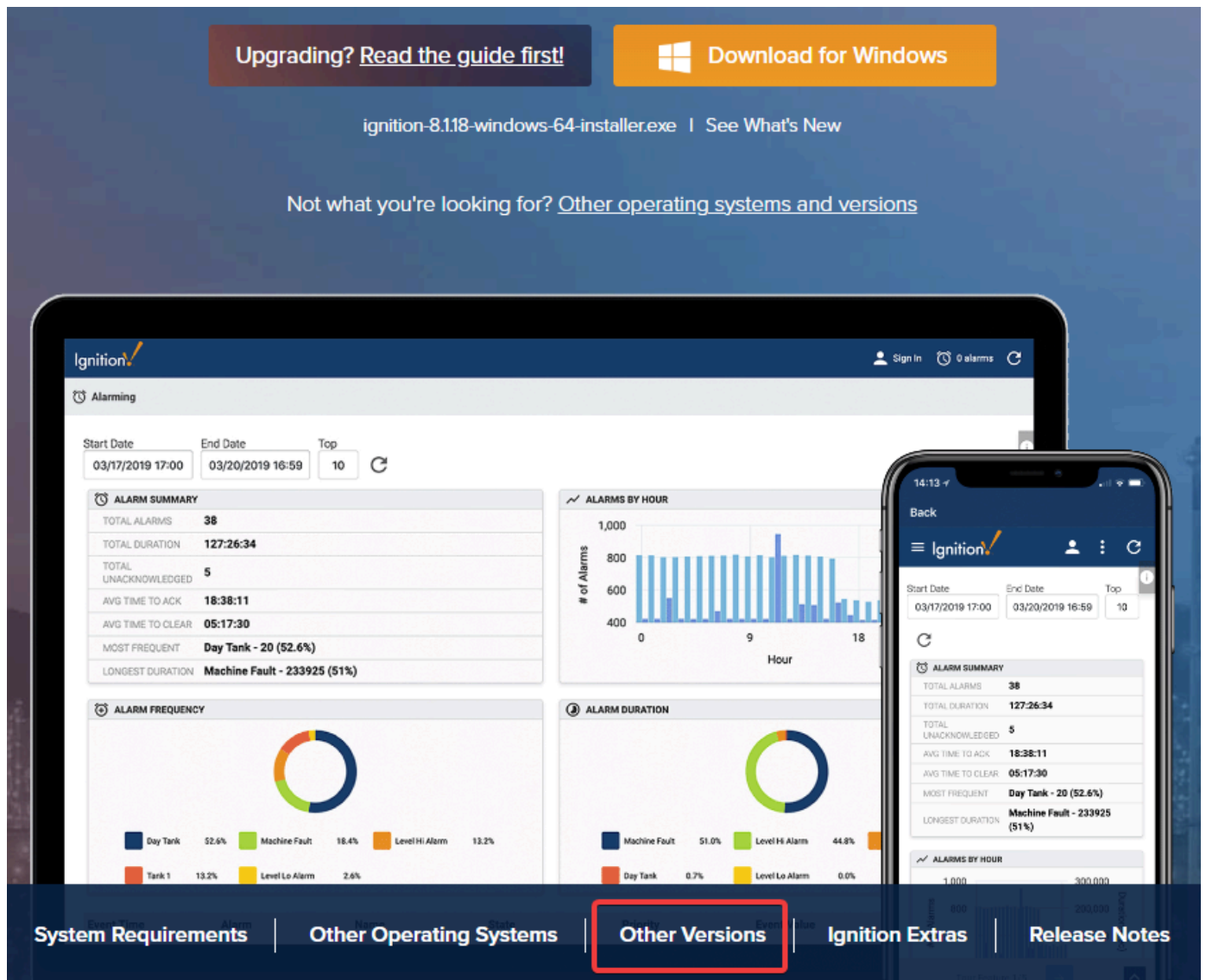
View 20

| <input type="checkbox"/> | VENDOR NAME               | NAME                     | VERSION                       | LICENSE | STATUS   |   |
|--------------------------|---------------------------|--------------------------|-------------------------------|---------|----------|---|
| <input type="checkbox"/> | Inductive Automation, LLC | UDP and TCP Drivers ⓘ    | 7.3.1-SNAPSHOT (b2025092517)  | Trial   | 🟢 ACTIVE | ⋮ |
| <input type="checkbox"/> | Inductive Automation, LLC | Omron Driver ⓘ           | 5.3.1-SNAPSHOT (b2025092517)  | Trial   | 🟢 ACTIVE | ⋮ |
| <input type="checkbox"/> | Inductive Automation, LLC | SFC ⓘ                    | 6.3.1-SNAPSHOT (b2025092517)  | Trial   | 🟢 ACTIVE | ⋮ |
| <input type="checkbox"/> | Inductive Automation, LLC | SQL Bridge ⓘ             | 11.3.1-SNAPSHOT (b2025092517) | Trial   | 🟢 ACTIVE | ⋮ |
| <input type="checkbox"/> | Inductive Automation, LLC | MariaDB JDBC Driver ⓘ    | 1.3.1-SNAPSHOT (b2025092517)  | Free    | 🟢 ACTIVE | ⋮ |
| <input type="checkbox"/> | Inductive Automation, LLC | BACnet Driver ⓘ          | 3.3.1-SNAPSHOT (b2025092517)  | Trial   | 🟢 ACTIVE | ⋮ |
| <input type="checkbox"/> | Inductive Automation, LLC | Event Streams ⓘ          | 1.3.1-SNAPSHOT (b2025092517)  | Trial   | 🟢 ACTIVE | ⋮ |
| <input type="checkbox"/> | Inductive Automation, LLC | PostgreSQL JDBC Driver ⓘ | 1.3.1-SNAPSHOT (b2025092517)  | Free    | 🟢 ACTIVE | ⋮ |
| <input type="checkbox"/> | Inductive Automation, LLC | Siemens Drivers ⓘ        | 7.3.1-SNAPSHOT (b2025092517)  | Trial   | 🟢 ACTIVE | ⋮ |
| <input type="checkbox"/> | Inductive Automation, LLC | SMS Notification ⓘ       | 7.3.1-SNAPSHOT (b2025092517)  | Trial   | 🟢 ACTIVE | ⋮ |

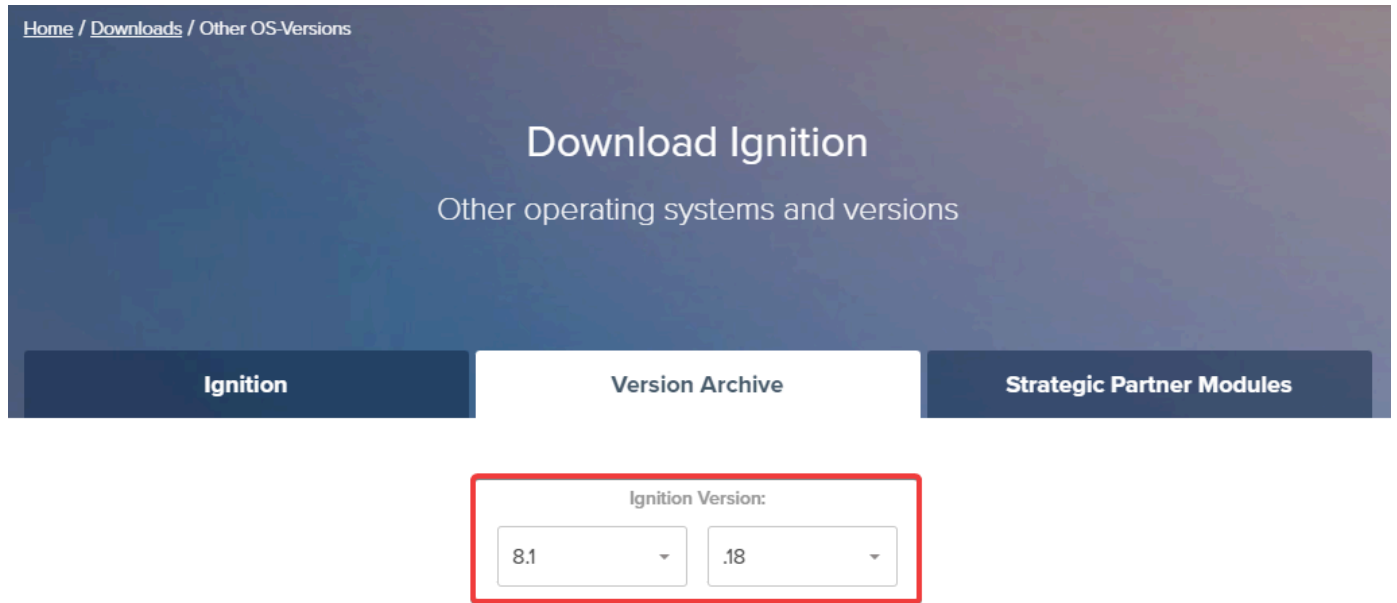
# Downloading a Module

Ignition comes with some default modules when installing the software. There may be a few modules you require that are not included when performing the initial installation, however. To find the module(s) you require, follow the instructions below.

1. Go to the [downloads page](#) on the Inductive Automation website.



2. Click on "Other Versions", located under the Ignition tablet and mobile device graphic. By default, this will take you to different installers and modules for the **latest** version of Ignition.



3. Select which version of Ignition you are currently running.
4. Scroll down the page until you see which module you are looking for. Once you click on the target module, it will start downloading the .modl file.

## Install or Update a Module

The following procedure assumes you have a .modl already downloaded in preparation for installing or upgrading a module, including for third party modules.

### NOTE

Installing a module will require connected Vision Clients and Designers to restart. Perspective Sessions will not require a restart. Production systems using either Clients or Designers should wait for downtime before installing a module.

1. On the Gateway Webpage, select **Platform > System > Modules** to open the **Modules** page.
2. Click the **Install or Upgrade Module +**.
3. Click **Choose File**, select a .modl file that you have previously downloaded.

Install or Upgrade Module

To **install** a module, choose its \*.modl file and press "Install Module".

To **upgrade** a module, install the new version on top of the existing version.

Import from file

Choose File...

No file selected.

Modules can be downloaded from [our website](#)

Cancel

Install Module

- Click **Install**. When the page reloads you can now see the module you installed in the list of modules.

## Manual Module Installation

Alternatively, you can add module files directly to your Gateway File System by following the steps below. This example will add the MongoDB Connector module.

- Navigate to the `%IgnitionInstallationDirectory%/user-lib/modules` folder.
- Add your .modl file to your modules folder.
- After adding your new module, we will need to create an entry in our modules.json file to bring the MongoDB module into our Gateway. Go to `%IgnitionInstallationDirectory%/data` and open the **modules.json** file.
- We will use the same format as the existing entries, and the **onStartup** and **certFingerprint** properties will use the same values. However, we will change the **module name** and **filename** (file path) properties to reflect using the MongoDB Connector module:
  - Module Name: `com.inductiveautomation.connectors.mongodb`
  - Filename: `C:\\Program Files\\Inductive Automation\\Ignition\\user-lib\\modules\\MongoDB Connector-module.modl`

```
"com.inductiveautomation.connectors.mongodb": {  
  "filename": "C:\\Program Files\\Inductive Automation\\Ignition\\user-lib\\modules\\MongoDB Connector-module.modl",  
  "onStartup": "enabled",  
  "certFingerprint": "0299d53c38bdbe7ca79bd6c778a5bab884e4c813"  
},
```

5. Once you have added your entry, save the modules.json file.

6. Restart your Gateway service.

Your new module will now be ready to use.

## Uninstall a Module

### NOTE

Uninstalling a module will require connected Vision Clients and Designers to restart. Perspective Sessions will not require a restart. Production systems using either Clients or Designers should wait for downtime before uninstalling a module.

1. On the Gateway Webpage, select **Platform > System > Modules** to open the **Modules** page.
2. Locate the module you want to uninstall.
3. To the right of module name, click the three dot menu and select **Uninstall**.

| <input type="checkbox"/> | VENDOR NAME                   | NAME                                                                                                    | VERSION                          | LICENSE | STATUS                                                                                       |            |
|--------------------------|-------------------------------|---------------------------------------------------------------------------------------------------------|----------------------------------|---------|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | Inductive Automation, L<br>LC | UDP and TCP Drivers  | 7.3.0-SNAPSHOT (b2025<br>010715) | Trial   |  ACTIVE |            |
| <input type="checkbox"/> | Inductive Automation, L<br>LC | Omron Driver         | 5.3.0-SNAPSHOT (b2025<br>010715) | Trial   |  ACTIVE |  Disable   |
| <input type="checkbox"/> | Inductive Automation, L<br>LC | SFC                  | 6.3.0-SNAPSHOT (b2025<br>010715) | Trial   |  ACTIVE |  Uninstall |

4. Click **Uninstall**. The module is no longer installed and is removed from the list.

Uninstall Module?

×

ⓘ

Module Configuration changes will not take effect until the Gateway has been restarted.

Are you sure that you want to uninstall module "UDP and TCP Drivers"?

The file will be permanently deleted from the local file system.

Cancel

Uninstall

## Disable a Module

1. On the Gateway Webpage, select **Platform > System > Modules** to open the **Modules** page.
2. Locate the module you want to disable.
3. To the right of module name, click the three dot menu and select **Disable**. A confirmation message appears.

| <input type="checkbox"/> | VENDOR NAME               | NAME                  | VERSION                      | LICENSE | STATUS   |                                                       |
|--------------------------|---------------------------|-----------------------|------------------------------|---------|----------|-------------------------------------------------------|
| <input type="checkbox"/> | Inductive Automation, LLC | UDP and TCP Drivers ⓘ | 7.3.0-SNAPSHOT (b2025010715) | Trial   | ✔ ACTIVE | ⋮                                                     |
| <input type="checkbox"/> | Inductive Automation, LLC | Omron Driver ⓘ        | 5.3.0-SNAPSHOT (b2025010715) | Trial   | ✔ ACTIVE | <div><div>⏻ Disable</div><div>🗑 Uninstall</div></div> |
| <input type="checkbox"/> | Inductive Automation, LLC | SFC ⓘ                 | 6.3.0-SNAPSHOT (b2025010715) | Trial   | ✔ ACTIVE |                                                       |

4. Click **Disable**.

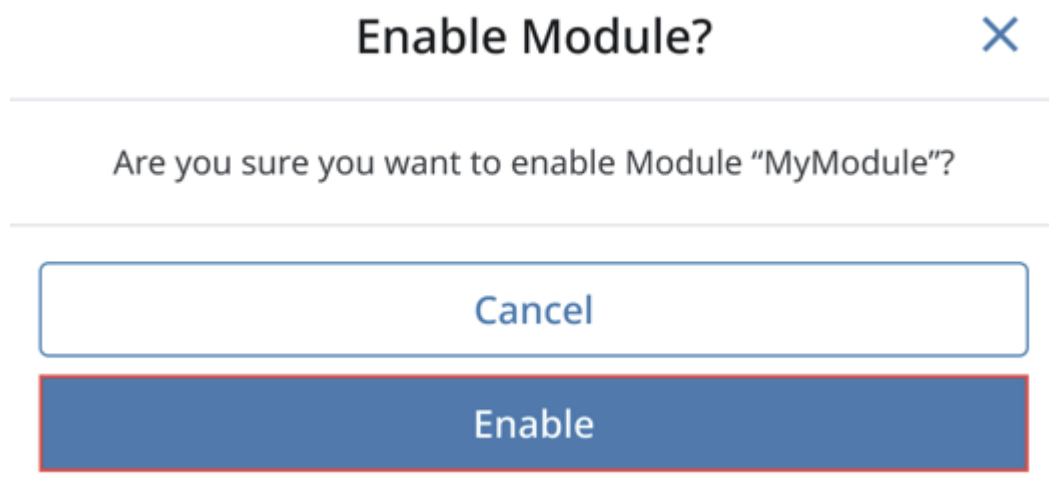
The module status will change to Active Pending Restart until the Gateway has been restarted, and the **Gateway Restart Required banner** will appear at the bottom of the page. After the Gateway has been restarted, the module will still be listed but will not be functional.

## Enable a Module

This option is only available for a currently disabled module.



1. On the Gateway Webpage, select **Platform > System > Modules** to open the **Modules** page.
2. Locate the module you want to enable.
3. To the right of module name, click the three dot menu and select **Enable**. A confirmation message appears.



4. Click **Enable**.

The **Gateway Restart Required banner** will appear at the bottom of the page for you to easily restart your Gateway. After the Gateway has been restarted, the module will be enabled.

## Module Status

The installed module list on the **Modules** page also provides some basic information about each module. The **Version**, **License**, and **Status** columns are all displayed in the list. **Module licensing** is performed centrally on the **Platform > System > Licensing** page, so the values on the Modules page are only for informational purposes.

## Module Shows as Faulted After Installation

In some cases, a module may appear to install successfully, but its functionality does not become available. A common cause of this behavior is a version mismatch between the installed module and the Ignition platform. For a module to load correctly, the middle digit of the module version must match the middle digit of the Ignition platform version. If a version mismatch is detected, the module will display a Status of **Faulted** on the Modules page.

## Status

RUNNING MODULES

31 / 32

LICENSED MODULES

28 / 32

## Modules



View

20



| <input type="checkbox"/> | VENDOR NAME               | NAME   | VERSION              | LICENSE | STATUS         |  |
|--------------------------|---------------------------|--------|----------------------|---------|----------------|--|
| <input type="checkbox"/> | Inductive Automation, LLC | WebDev | 5.1.51 (b2025121607) | n/a     | <b>FAULTED</b> |  |

To verify compatibility, navigate to **Diagnostics > Overview** and note the Ignition version currently running on your Gateway.

## Gateway Overview

Gateway Name

Ignition-

Gateway Version

8.3.3-SNAPSHOT (b2025122310)

License

licensed

Uptime

0 days, 0 hours, 15 minutes, 7 seconds

Because the WebDev module shown above has 1 as the middle digit and the Gateway has 3, there is a version mismatch and the module will remain in a faulted state. To resolve this, download the correct version of the module from the Inductive Automation [Downloads](#) page. Use the Ignition Version dropdown or Version Archive tab to select the Ignition version that matches your Gateway. From the list of available modules, locate the compatible version and download it.

# Download Ignition

Other operating systems and versions

Ignition

Version Archive

Strategic Partner Modules

Ignition Version:

8.3.3 - LTS

NIGHTLY ▾

## Ignition Modules

| Core Modules                             | Version                   | Checksum                |
|------------------------------------------|---------------------------|-------------------------|
| <a href="#">WebDev Module (135.8 KB)</a> | 6.3.3.2025122218-SNAPSHOT | <a href="#">sha-256</a> |

After installing the compatible version, the Gateway Restart Required banner will appear at the bottom of the Modules page. Click the **Restart Gateway** button to complete the installation.

### Modules

| <input type="text"/>     | View                      | 20 ▾     |                      |         |                  |   |
|--------------------------|---------------------------|----------|----------------------|---------|------------------|---|
| <input type="checkbox"/> | VENDOR NAME               | NAME     | VERSION              | LICENSE | STATUS           | ⚙ |
| <input type="checkbox"/> | Inductive Automation, LLC | WebDev ⓘ | 5.1.51 (b2025121607) | n/a     | <b>⚠ FAULTED</b> | ⋮ |

Showing 1 of 1 items

**Gateway Restart Required** There are 2 pending gateway updates. A gateway restart is required to complete.

**Restart Gateway**

Once the Gateway has been restarted, the module will show a Status of **Active**, and will become available for use.

Status

RUNNING MODULES

32 / 32

LICENSED MODULES

29 / 32

Modules

View 20

| <input type="checkbox"/> | VENDOR NAME               | NAME                     | VERSION                      | LICENSE                     | STATUS                   |                   |
|--------------------------|---------------------------|--------------------------|------------------------------|-----------------------------|--------------------------|-------------------|
| <input type="checkbox"/> | Inductive Automation, LLC | WebDev <a href="#">i</a> | 6.3.3-SNAPSHOT (b2025122218) | Activated <a href="#">i</a> | <a href="#">i</a> ACTIVE | <a href="#">⋮</a> |

# Verify Trusted Modules

Verify the authenticity of Ignition modules on the **Platform > System > Modules** page. Expand the three dot menu for your module and select **View Certificate** to see details about each certificate.

A warning message will appear if the module certificate is expired, however this will not have any impact on security or module behavior.

Module Certificate Information

×

✔

This certificate has been signed by a trusted Certificate Authority.

|                 |                                                                    |
|-----------------|--------------------------------------------------------------------|
| Not Valid       | 9/7/21, 5:00:00 PM                                                 |
| Not Valid After | 9/7/24, 4:59:59 PM                                                 |
| Subject Name    | Inductive Automation, LLC                                          |
| Issuer Name     | DigiCert Trusted G4 Code Signing<br>RSA4096 SHA384 2021 CA1        |
| Thumbprint      | [ B2 EA 7D 97 66 30 1D C7 A6 8D 3C D2<br>82 DF 01 B7 DC 3F 30 02 ] |

# Quarantined Modules

Near the bottom of the Modules page is the **Quarantined Modules** section. Modules can be quarantined for various reasons, such as a certificate being unsigned or needing review, or licensing issues. The Gateway will list the specific reason a module is quarantined, along with the module name and version.

**New in 8.3.2** If a module has been quarantined, you can still trust it and add it to your Gateway. To do this, click on the three dots menu next to the quarantined module you want to use. You will be presented with an option to either resolve the quarantine reason or delete the module.

### Quarantined Modules

View 20 ▾

| NAME         | VERSION    | QUARANTINE REASON                  | ⚙ |
|--------------|------------|------------------------------------|---|
| Test Project | 1.0.0 (b0) | Certificate has not been accepted. | ⋮ |

Showing 1 of 1 items

Trial Mode 1:54:00 We are glad to see you are test driving our software, have fun!

🔍 Review Certificate

🗑 Delete Module

# Third Party Modules

Third Party modules are not produced by Inductive Automation. Ensure that you know who produced the code and perform due diligence as you would with any other software vendor in accordance with organizational policy.

Strategic Partners, such as Cirrus Link, and Premier Technology Providers, such as 4IR and Sepasoft, are trusted parties by Inductive Automation. However, their modules or services are created by separate groups and may need to be vetted separately from the Ignition platform.

The **Module Showcase** hosts Ignition modules written by the community. Authors are required to request certificates from Inductive Automation (IA). IA will remove modules with known problems or risk, but hosting does not require a high level of vetting. Your account representative may be able to provide more information on known authors or organizations.

The bundled version of Java in Ignition uses Java 17.0.13, which may impact third party module compatibility. Refer to third party module documentation for further communication about any end-user modifications that may be required.

# Ignition 8 Upgrade Guide

This section contains guides for users that are considering upgrading to newer versions of Ignition.

## Should I Upgrade?

It may not be advisable for all users to immediately upgrade production systems to 8. It is highly recommended that all users who wish to upgrade should first install Ignition 8 on a separate server and validate all of the functionality required by their system before deploying it into production. Please read this guide in its entirety to understand the changes introduced in Ignition 8 and evaluate if they will impact your installation(s).

The bundled version of Java in Ignition has been upgraded from Java 11 to Java 17.0.8. Upgrading is recommended for Ignition versions running Vision Clients and Designers 8.1.2 or lower as they will fail to retarget to new clients running Java 17.

## Expected Downtime

If you are upgrading Ignition 8, there are some changes that may require a downtime window, even when using Ignition's Redundancy. These changes are covered on the the pages listed below.

- [7.9 to 8.1 Upgrade Guide](#)
- [8.0 to 8.1 Upgrade Guide](#)
- [8.1 to 8.3 Upgrade Guide](#)

# 7.9 to 8.1 Upgrade Guide

Ignition 8.1 is a major update across virtually all subsystems and modules. Inductive Automation strives to maintain its commitment to backwards compatibility and a straight-forward upgrade process. However, given the vast scope of changes in 8.1, there are inevitably special considerations that need to be evaluated and actions taken in order to successfully upgrade an existing system. This document seeks to identify those issues and provide guidance for users who are migrating from an Ignition 7 system. To discover the new features of Ignition 8.1, please see the [What's New](#) section.

## NOTE

In some cases, it is not advisable or possible to upgrade from Ignition 7 to 8.1 at this time. Please read this guide carefully before upgrading a production Gateway.

## Upgrade Process

When upgrading from Ignition 7 to Ignition 8.1, there are two general approaches.

### Using the Installer to Upgrade (Preferred Approach)

Using the Installer to upgrade is the easiest approach. Simply run an Ignition 8 installer on your existing server (similar to how upgrades normally work). As always, we highly advise taking a Gateway backup before upgrading.

### Importing Projects into a Fresh Install

We have found that some users prefer to completely uninstall their Ignition 7 Gateways, install a fresh copy of Ignition 8.1, and then manually import projects and Tags from the old Ignition 7 Gateway, one-by-one. We generally **discourage** this practice, as it results in unintended consequences. We recommend you take the "Using the Installer to Upgrade" approach instead. However, if you must import Ignition 7 resources into an Ignition 8.1 Gateway, then we recommend you use Gateway Backups instead (when possible).

The reason for this, is that a Gateway Backup triggers an upgrade check that looks over the Gateway Backup and makes modifications to the resources so they run as expected on an Ignition 8.1 system. The same check is triggered when running the installer. Project and Tag imports do **not** trigger this check. As a result, you may need to make manual modifications to the imported resources.

For example, the project system in Ignition 8.1 is drastically different, so running the installer directly on an Ignition 7 Gateway or importing an Ignition 7 Gateway Backup into an Ignition 8.1 Gateway will trigger all of the updates listed under the **Project Inheritance & “Global” Upgrade Logic** heading below. Individually importing projects one-by-one will not trigger the upgrade logic, so any legacy "shared" scripts may not work in Ignition 8 without user intervention.

The same could be said for Tag imports. Ignition's built-in OPC UA server connection on Ignition 7 used the name "Ignition OPC-UA Server", but Ignition 8.1 changed the name to "Ignition OPC UA Server", removing the hyphen "-" character. As a result, your Ignition 7 Tags are likely using the old name, where as a freshly installed Gateway is using the new name. Thus, OPC Tags imported from an Ignition 7 file will likely break upon import as the OPC Server name won't match, so you'll need to either A) rename the OPC UA server connection or B) find-and-replace the OPC UA server name on all of the Tags.

## Changes That Require User Action

These changes will require manual action on the part of the system administrator/project author. In other words, these are features or situations that have a direct corresponding solution, but for various reasons cannot be automatically upgraded.

### Look and Feel changes

The general look and feel of the Ignition Designer and Vision Client has been updated. This may result in subtle changes to the appearance of Vision Clients depending on the components used by a given project. It is not possible to revert to the old “look and feel” as it’s not compatible with new version of Java.

This means screens that have been developed in version 7 may look different after upgrade. Notably, the default font on many Vision components is larger. To preserve your pre-8.0 look, you will want to enable the **Use Condensed Font** Gateway setting (introduced with version 8.1.4).

Manual configurations to Vision resources, such as manually selecting a font or background color for a component, will be preserved upon upgrade. However, visual properties left with default values may appear differently after upgrade. You may also notice component properties like `antialias` and `background3D` no longer exist.

#### NOTE

It is highly advised to upgrade version 7 projects to version 8.1 on a test server and verify the look of the project, before upgrading the production servers.



## Redundancy Connection Configuration

Redundancy communication is now accomplished through a Gateway Network connection between the master Gateway and the backup. This mechanism provides greater security and performance than the previous communication channel, but will require the system administrator to re-establish the connection.

The settings for the communication channel are still configured in the Gateway under Configure>Redundancy, and are still established from the Backup to the Master, but must be modified before the backup will successfully connect to the master after upgrade.

## Replacement for the `system.tag.browseConfiguration` Function

The Tags system in Ignition changed dramatically in Ignition 8, which makes the Ignition 7 function `system.tag.browseConfiguration` obsolete. The function has been removed from the code base, so scripts using the old `browseConfiguration` function will break upon upgrade. The functionality has been replaced by `system.tag.getConfigurations`.

## OPC UA Certificate Management

Prior to Ignition 8, Ignition's built-in OPC UA client implicitly trusted the certificate of any server it connected to, and Ignition's built-in OPC UA server implicitly trusted the certificate of any client connecting to it. This is no longer true. New certificate management pages for the client and server have been added to the configuration section of the Gateway under "OPC UA > Security". From this UI, trusted certificates can be imported and quarantined certificates can be marked as trusted. Ensuring the remote certificate is trusted, is required for all secured inbound and outbound connections.

*On upgrade, all secured inbound and outbound connections other than the default "loopback" connection will be faulted until the remote certificate is explicitly marked as trusted.*

## Query Tags

Query Tags in Ignition 7.9 have a default behavior that allow Array and Dataset type Tags to ignore AutoDetect logic and execute queries as SELECT statements. Starting in 8.1.3, if a Query Tag does not start with SELECT, Ignition will execute the query as an UPDATE query. Manually selecting either SELECT or UPDATE will circumvent any issues that may arise from this change.

## Quality Codes

8.1 quality codes are different from the quality codes in 7.9. Existing values are adapted automatically so tag history quality results and bindings can still be trusted in your upgraded versions. However, it is important to check areas where manual entry may prevent adapted values from populating correctly such as scripts for live checks of tag quality.

## Discontinued Features

These are areas that have been removed or discontinued, as new methodologies have been adopted to replace the functionality.

### Vision Mobile Module Discontinued

The Vision Mobile Module is no longer supported in Ignition 8. The new Ignition Perspective Module provides a robust, modern solution for mobile visualization. Users should migrate their mobile visualization needs to be based on Perspective applications going forward.

A few important points:

- The Mobile Module will continue to be supported on Ignition 7.9 for the remainder of its respective Long Term Support (LTS) terms.
- All customers who own the Mobile Module and have current TotalCare Upgrade Protection contracts are entitled to a license of Perspective Mobile upon upgrade.

### External Database “SQLTags” Providers No Longer Supported

The “Database Provider” and “Database Driving Providers” are no longer supported in Ignition 8. These systems were very early ways to bridge outside data into Ignition’s Tag system and have been replaced over the years with much easier and faster methods of data integration.

### 32 bit Support

Support for 32-bit platforms other than ARM has been discontinued.

### Project Rollback

The Project Rollback feature has been discontinued in Ignition 8.

## OPC UA Server Stale Threshold

The Stale Threshold setting on Ignition's OPC UA server has been retired. The setting was originally used in earlier versions of Ignition as a means to help some of our drivers determine when values should be marked as stale. Our drivers have since gained their own methods to determine staleness. The setting has little use in Ignition 8, so it was removed.

## Staging and Publishing

Ignition 8 features a completely revamped project system. This new project system does not have different “staging” and “published” versions of each project. When you upgrade from Ignition 7, any projects that were split into separate staging and publish versions will have their staging versions imported into Ignition 8. This is to prevent any loss: the staging version is always at least as and usually more up-to-date than the published project.

Staging and publishing was not included in Ignition 8's project subsystem for two reasons:

1. Staging and Publishing was not consistently implemented across various modules, leading to confusion about which types of resources participated in it.
2. Projects are not self-contained; they rely on tags and external connections to devices, databases, etc. For this reason, the staging and publishing feature was only effective in limited circumstances.

You can emulate the old staging and publishing system by simply having a “staging” copy of your project and either move resources between projects or copy & overwrite them in order to “publish” your changes.

## OEM Lock

The “OEM Lock” feature that was used to encrypt project resources by authors is not currently supported in Ignition 8. Project authors that used this feature may migrate their projects to 8.0, as the owner license will decrypt Ignition 7 resources, but they should be aware that the resources will currently remain unencrypted.

End users who upgrade OEM-Locked systems to 8.0+ will not be able to view the project resources.

## OPC UA Server Exposed Tags Auditing

When a Tag made available via the “Exposed Tags” feature of Ignition's OPC UA server is written to by an OPC UA client, the write is not currently entered into the audit log.

## OPC UA Server “ReadOnly” Role

The undocumented “ReadOnly” role no longer has any effect.

## Changes to Be Aware Of

Ignition 8 has many additional changes and improvements that system administrators should be aware of. Although none of them present a significant issue, some may directly affect end users (for example, launching clients), and some can be leveraged to improve the security and performance of your system.

### Third-Party Modules

Please consult individual module authors concerning upgraded module availability. Modules built for Ignition 7 will not work in Ignition 8 without modification.

### Tag Historian Licensing

See the [Tag History Licensing](#) changes on the [Upgrading from 8.0 to 8.1] page.

### Default Security Certificate

Ignition installations no longer come with initial security certificates.

### Native Client Launchers Replaced

The Native Client Launcher has been replaced by the [Designer Launcher](#) and [Vision Client Launcher](#), which offer similar functionality. Due to the aforementioned "Default Security Certificate" change, secure connections between the launchers and Gateway will require valid certificates are in place.

### Java Web Start Discontinued

Support for Java Web Start has been discontinued by Oracle and the OpenJDK community as of Java 11. This technology has been used in Ignition since its original release to launch the Designer and Vision clients, though we have also offered alternative launching tools for years.

In anticipation of this change, the designer and client launching tools have been greatly improved in Ignition 8. In addition to a fresh and more functional UI, the launch tools now manage the Java runtime environment used by the client (see next point), and can help you track many projects and

Gateways. There are separate launchers for Vision Clients and the Designer, representing the natural distinction between the target users of these products, and the launchers can be downloaded for Windows, Mac, and Linux directly from the Gateway homepage.

Java Web Start is no longer supported, please use the Designer and Client launchers to launch those applications.

## Embedded Java

Ignition no longer requires Java to be installed on the Gateway or client machines. Native versions of the Ignition installer and launchers have been made available for 64-bit Windows, Mac, and Linux, as well as ARM, for use in edge devices. These distributions include embedded JREs (Java Runtime Environment) that are provided by Inductive Automation and managed by Ignition.

The native client launchers manage retrieving the current version of the JRE as necessary for the client and designer runtimes. Updates to the embedded JREs are managed by Inductive Automation and are made available through updates to Ignition. The client launchers will automatically update their local versions as necessary, ensuring that Vision Clients and the Designer are always running the latest version available on the Gateway.

Ignition no longer requires Java to be installed on server or client machines. System administrators should monitor Inductive Automation for important system and security updates, and can sign up for important notifications at <http://support.inductiveautomation.com>

## Project Inheritance & “Global” Upgrade Logic

The project system in Ignition 8 has been improved and now features a more flexible inheritance model. Each project may have a “parent” project, and will inherit all of the resources of that parent project. That project may in turn have its own parent project, and so in this way complex hierarchies of re-usable resources may be designed. Within each project, inherited resources may be used by other, “local” resources. For example, an inherited Vision template could be embedded in a window, or an inherited script could be executed by a button. Inherited resources may also be overridden, allowing them to be re-defined when needed. Conversely, resources in parent projects may be marked as “not overridable” to ensure that children cannot alter them, when appropriate.

This new inheritance system makes Ignition 7’s “global” project concept obsolete. In order to maintain backwards compatibility, the following will happen when an Ignition 7 Gateway is upgraded to Ignition 8:

- The resources from the Ignition 7 special “[global]” project will be copied into an Ignition 8 standard, inheritable project called “global”.
- All other projects will have their parent project set to this new “global” project.

- All “shared” scripts are now simply project-level scripts in a top-level script package called “shared”, stored in the new “global” project. This allows all existing scripts to function without edits.
- All “project” scripts are now simply project-level scripts in a top-level script package called “project”.
- All Vision templates stored in the old global area are moved into a folder called “SharedTemplates/” in the new global project. The Vision module will automatically convert a template path like “[shared]MyTemplate” as “SharedTemplates/MyTemplate” so that no further action is needed.
- If any run-always sequential function charts are present in the global area, a new project called “run-always-charts” will automatically be created upon upgrade, and these charts will be moved into this project. This is because resource types that execute automatically like run always SFCs and Transaction Groups do not run in inheritable projects.
- If any alarm pipelines exist, a project called “alarm-pipelines” will be created and all alarm pipelines will be moved into this project. Tags can target pipelines in any project, but in the absence of a specific project, the pipeline is assumed to be in this special upgrade project.
- There is a new Gateway-wide setting called “Gateway Scripting Project”. This setting lets you specify one project which all scripts that are outside the scope of a project will execute against. For example: Tag Change Scripts and Tag expressions using the runScript expression. On upgrade, this will be set to the new “global” project so that Tag scripts can continue to access shared.\* scripting functions.
  - In addition to Tag scripts, this can potentially impact other features, such as expression items in a Transaction Group using the runScript function.

## Deprecated system.tag Functions

- The system.tag.read and system.tag.readAll functions were deprecated. They has been replaced by [system.tag.readBlocking](#).
- The system.tag.write and system.tag.writeAll functions were deprecated. They have been replaced by [system.tag.writeAsync](#).
- The system.tag.writeSynchronous and system.tag.writeAllSynchronous functions were deprecated. They have been replaced by [system.tag.writeBlocking](#).

## Tag System Changes

The Tag system has undergone significant changes in Ignition 8. The majority of these changes should go unnoticed upon upgrade (apart from obvious UI changes), and most systems should immediately benefit from improved performance, faster edits, and expanded functionality. To summarize:

- "Scan Classes" have been renamed to "Tag Groups". Functionally they're identical. Scan Classes on Ignition 7 systems will gracefully migrate to Tag Groups upon upgrade.
- "LastChanged" has been renamed to "Timestamp". Like Scan Classes, LastChanged values will migrate to Timestamp upon upgrade.
- The Tag Editor has been gone through a major UI rework, but remains as easy-to-use as ever.
- Tags are fundamentally defined via JSON structure now. A new right-click menu has been added to the Tag Browser, allowing you to edit the raw JSON of a given Tag. Additionally, Tag exports/import files now support a JSON format.

The upgrade process will attempt to convert older tags to the new system. Should this process fail, log files will be generated in the installation directory: `/logs/legacy-tag-conversion` (as of 8.1.11+).

You can also leverage [Tag Report Tool](#) to identify broken tags.

## UDT Performance

The Tag system has been redesigned to optimize for UDT oriented design. In Ignition 7, certain aspects of UDT performance led some system designers to favor standard Tags over UDTs for some applications. Such systems should be re-evaluated in Ignition 8, as use of User Defined Types will lead to more efficient memory usage and lighter weight change processing.

## UDT Parameter Usage

The way that Parameter references are applied to Tags has changed. Instead of being replaced in a “pre-compilation” stage of Tag execution, they are now treated as true property references. This means that they can be modified, and those modifications propagate dynamically to referencing properties, causing those to be updated in turn.

An important consequence of these changes is that syntax for parameter references in Expressions has changed in a subtle, but crucial way. In Ignition 7, due to the replacement strategy, the following would have been a valid expression:

```
“The value of the parameter is: {ParamRef}”
```

In Ignition 8, this value would no longer be a valid reference. It is counter-intuitive to all other uses of reference in Ignition, and has been replaced with a more familiar syntax:

```
concat(“The value of the parameter is: “, {ParamRef})
```

All existing references will be upgraded automatically to the new syntax upon system upgrade. Designers should be aware of this change when creating new Tags.

## UDT Parameter Formatting

OPC tags using **+00** in parameter bindings on their OPC Item Paths will return an `Error_Configuration` message as 8.0+ no longer allows **+0#** in parameter bindings when 7.9 allowed an arbitrary amount of zeroes. Changing this to **+0** in the path will fix any broken tags.

### NOTE

Due to a change in 8.0.3 that "Improved mathematical operator support for UDT parameters", using operators such as `+` or `-` in your UDT Parameter is not recommended, as this can lead to Ignition executing a mathematical equation instead.

## Quotes Taken Literally in String UDT Parameters

In addition, string UDT parameters that contained quotation marks in 7.9 will now be represented literally. In 7.9 the quotation marks were omitted. After upgrading, the quotation marks will be included in the UDT parameter value.

## The `instanceName` UDT Parameter

The built-in `instanceName` UDT parameter works differently in nested UDTs. Referencing the parameter in a nested UDT will return the name of the nested UDT. In 7.9 the parameter would always return the name of the root UDT.

## The `UDTParentType` Property

The UDT property `UDTParentType` has been renamed in Ignition 8 to `TypeId`.

## Script Based Tag Editing

The various scripting functions for editing Tags (`system.tag.editTag`, `system.tag.addTag`, etc.) have been deprecated and replaced by **`system.tag.configure`**. The previous functions will continue to work, but designers should learn the new function, which is far more intuitive and powerful than the previous functions.

Tags are now defined as JSON objects, which consist of properties, arrays, and sub-objects. The `system.tag.configure` function can take either a String document definition, or a JSON object that



defines one or more Tags. Overrides for UDTs are created by simple redefinition of properties, and complex structures like Event Scripts and Alarm configurations will be merged with inherited definitions.

## OPC UA Default Configuration Changes

New installations have some new OPC UA related defaults:

- The server binds only to localhost (i.e. no remote connections allowed)
- The server uses port 62541 instead of 4096
- The server only allows secured connections (SecurityPolicy Basic256Sha256)
- The default “loopback” connection is called “Ignition OPC UA Server” (there is no longer a “-” between “OPC” and “UA”)

Upgrades are not affected by these changes; they retain their existing configuration.

## OPC UA Discovery with Third-Party Clients

Ignition's OPC UA server disallows anonymous access on new installations, which can make the server endpoint difficult to discover by UA clients. To help with this, Ignition's UA server runs a separate unsecured endpoint to allow discovery. The discovery endpoint is accessible by appending /discovery to the end of the URL:

```
opc.tcp://1.2.3.4:62541/discovery
```

## OPC UA Exposed Tags NodeIds

When using the OPC UA Exposed Tags feature, the NodeId returned by the browse has changed slightly. In prior versions the NodeId would follow a pattern like: `[prov]Path/To/Tag`

As of 8.0+ the pattern now includes a slash after the provider: `[prov]/Path/To/Tag`.

Both patterns still function as expected for the purposes of Reads, Writes, and Subscriptions. However a NodeId returned by a browse will always use the newer pattern.

## Changes to `system.alarm.listPipelines`

The `listPipelines` function was changed to search a single project for pipelines. Upgrading from Ignition 7 to Ignition 8 will migrate all alarm pipelines into a project named "alarm-pipelines". To maintain backwards comparability, `system.alarm.listPipelines()` will check for a project named "alarm-

pipelines", but now accepts a project name as a parameter, allowing the function to check for pipelines in any project.

## SQLite Storage

Gateways can now create SQLite databases, or "Internal databases" for many of the storage subsystems (Database Connections, Historian, Alarm Journal, and Auditing), allowing your gateway to store and retrieve data without needing to connect to a remote SQL database, which is useful for development systems and demonstrations.

### NOTE

We still recommend external SQL databases are used in production systems, as they generally offer a level of performance and redundancy not available to SQLite databases.

## TLSv1.0 and TLSv1.1 No Longer Supported

Ignition version 8.1.6 started embedding Java version 11.0.11 and Ignition version 8.1.33 started embedding Java version 17.0.8. These versions of Java do not offer support for TLS v1.0 and v1.1. This could impact connections the gateway makes to external systems and applications, especially so if those external systems cannot support a more recent version of TLS. The following items could be effected:

- Database connections: This can generally be resolved by simply updating the JDBC driver that the gateway uses. Check your database vendor's JDBC driver recommendations.
- HTTP calls from Ignition (such as those generated by scripting): This is highly unlikely since modern browsers and services already deprecated older versions of TLS. If this is an issue then you'd need to update the service (if the endpoint is an internally hosted service) or check the documentation for the service.

## JDBC Drivers May Need Updating

Due to updated Java versions, JDBC drivers for existing installations may need to be updated for compatibility. See the [JDBC Drivers and Translators](#) page for more details.

## SFCs

Due to the tag system changes, SFC parameters are no longer able to store entire QualifiedValue objects, such as those returned by the [system.tag.readBlocking](#) function. However fields of a QualifiedValue, such as the value, can still be stored in parameter.

```
# No longer supported
chart.new_param = system.tag.readBlocking(["[default]myTag"])

# Supported
chart.new_param = system.tag.readBlocking(["[default]myTag"]).value
```

## Web Dev Endpoints

In 7.9, Web Dev resource endpoints resembled the following:

Legacy Endpoint

```
host:port/main/system/webdev/projectname
```

In 8.1, Web Dev endpoints no longer contain "main":

8.1 Endpoint

```
host:port/system/webdev/projectname
```

Note that requests using the legacy endpoint will simply be redirected to the 8.1 endpoint, so endpoints created in 7.9 will still function after upgrading.

## Tag Paths in Expressions

Expressions that make use of a tag path will need to be updated to include either a tag provider or "[~]".

```
{Path/To/Tag}           // paths that look like this...

{[~]Path/To/Tag}         // ...should be changed to this.
{[MyProvider]Path/To/Tag} // You could always explicitly state the provider too.
```

# New Features

## Introducing Ignition Perspective

Ignition Perspective is an entirely new visualization system, built from the ground up to allow you to create modern, high performance, and highly functional pure-web applications that can be viewed anywhere. Learn more about Perspective by visiting the [Perspective pages](#) in the User Manual, or the [Inductive University](#).

## Using Perspective without Upgrading

The Ignition Perspective module is one of the most exciting new features of Ignition 8, offering an entirely new and innovative way to visualize data and deploy applications to mobile devices. Many users will want to begin leveraging this module right away, and will feel compelled to upgrade for that purpose.

It is important to understand how various Ignition features, in particular the Gateway network and remote services, can be leveraged to allow immediate usage of Ignition Perspective without the potential risk or disruption necessary to upgrade a running production Gateway.

As part of the base platform, the Gateway Network allows you to create connections between Gateways, including between 8 and 7. The Remote Tag Provider allows you to use Tags from one Gateway on another, including both realtime and historical values. Remote Tag Providers created in Ignition 8 targeting Ignition 7 Gateways will support reading, writing, real-time subscriptions, and Tag history queries. For more information, see the [Tag Providers](#) page.

Therefore, to develop and deploy Perspective applications with minimum impact on your production system you can:

1. Install Ignition 8 onto a different computer or VM instance.
2. Limit the installation to the Perspective module (though, of course, other modules can be used).
3. Create a Gateway network connection between the Ignition 8 Gateway and the Ignition 7 Gateway.
4. Create a Remote Tag Provider on the Ignition 8 system for each provider you'd like to access.

Unless previously changed, remember that the Ignition 7 Gateway will employ the default “service security” settings for the remote Tag Gateway network service. This will allow read only data, but if you want to support writes, you'll need to change the policy by going to `Configure>Security/Service Security` in the Gateway.

# Introducing Identity Providers

Ignition 8 adds support for connecting to SAML and OpenID Connect Identity Providers. In addition, Ignition can act as an Identity Provider, using a User Source as a backing source of users. On upgrade, a new Ignition Identity Provider will be created that points to a single user source, allowing users in that user source to authenticate against the Identity Provider. You can learn more about this on the [Configuring Identity Providers](#) page.

For more information, see the [Gateway Authentication with Identity Providers](#) section in the 8.0 to 8.1 Upgrade Guide.

Introducing Identity Providers also introduced the option to log in with RFID and badges starting in Ignition 8.0.5. This, in turn, required a new column called "badge" to be added to the \*users table. When upgrading Ignition while your User Sources are set to "Automatic" Mode, this column will be created by default. If you are running into an issue with your User Sources, check to see if the "badge" column has been created.

## System Commissioning

Upon installing Ignition, the user is now presented with a “system commissioning” web based walkthrough. This process must be completed for new installations, and requires that an initial user is created for the newly commissioned Gateway.

As of Ignition 8.0, there is no longer a pre-defined default “admin” user. System administrators should choose a secure root username and password for optimal system security.

## Security Levels

Ignition 8 introduces the concept of [Security Levels](#), which are abstracted attributes that can be given to users, and used as a means to restrict access to different parts of the system. Security Levels can be assigned to users based on User Roles, Security Zones, a combination of both, or neither, as the Expression Language can be used to determine which level any given user falls under.

Many subsystems in Ignition will automatically migrate over to security levels upon upgrade, such as Tag read and write permissions.

## Expanded Auditing Scope

Ignition's built-in auditing system was very limited in version 7, recording only a handful of events. Most events that registered in the system had to originate from a project, so changes made at the Gateway level were largely ignored, save for Tag writes.

In Ignition 8, the auditing system's reach has broadened greatly. The system now accounts for configuration changes made at the Gateway level. Check out the [Auditing Actions Reference](#) page for a full listing of actions that are audited.

## Project Resource Storage

The new project subsystem in Ignition 8 uses a new file-based storage strategy, instead of the internal-database strategy used in Ignition 7. This has several significant benefits over the previous methodology:

1. All resources can now be tracked with industry standard source control tools, such as Git. Resources can be tracked individually, and changes to disk caused by source control operations (checkout, pull, etc.) will be applied automatically to the running system.
2. Project resources can be transferred between systems with simple file system operations. System administrators can use a wide range of tools to synchronize all types of resources between Gateways.
3. Project backups are simply standard zip files organized in the same way as the file system.

## Designer Concurrent Editing and Conflict Resolution

Ignition 8's Designer uses a new lock-free strategy for handling concurrent editing. We believe that this strategy is significantly more robust and will allow for more designers to work together on projects.

The Ignition 7 locking strategy is incompatible with the new file system storage strategy. Since changes can occur in the file system at any time, it isn't possible to maintain exclusive edit locks in the Designer.

In Ignition 8, you may open and modify any resource in your project. You will be notified if the system detects that you and another user are both editing the same resource, or if the resource you're editing has already been modified remotely. If you modify the resource anyway, and someone else has modified it first, this is called a conflict. The system automatically detects conflicts when you try to save. If any are detected, you are given the opportunity to resolve these conflicts by choosing whether to use your changes, accept the changes that happened elsewhere, or cancel your save and figure out what to do in another way.

## Changes to Gateway Command Utility (GCU)

As of Ignition 8.0, the Gateway Command Utility is deprecated. Functions similar to the ones found in the Gateway Command Utility are now run through the command line. You can find a list of available commands on the [Gateway Command-line Utility - gwcmd](#) page.

# 8.0 to 8.1 Upgrade Guide

This section details notes and advisories for users planning on upgrading from 8.0 to 8.1.

## CAUTION

If upgrading to 8.1.33 or newer, be aware the bundled Java version for Ignition has been upgraded from Java 11 to Java 17. For most users, this upgrade will be seamless. However, users should check Java 17 compatibility with installed JDBC drivers and third party modules in case modifications are needed.

## Changes to Be Aware Of

### Tag Historian Licensing

In 8.1, the Tag Historian module licensing has been adjusted.

1. Licensing for the full Tag History works identically to before. If you have a normal Tag Historian license, and are using the standard Tag Historian functionality, there are no changes.
2. For customers with a Scale-Out architecture, the Tag Historian could be used on the front-end Gateways unlicensed. This would provide a message of "Partially licensed" on those Gateways, even though the configuration was an acceptable architecture with no need for additional licensing. In 8.1, we added the ability for the Tag Historian to be licensed for read-only operations, to eliminate that message. This is available for free for users upgrading from existing licenses 7.9 and 8.0 licenses that have Upgrade Protection by contacting your sales representative at Inductive Automation.
3. A small set of customers use third-party modules that act as a storage engine for Ignition's Tag Historian. Previously, Inductive Automation did not require a Tag Historian license for a module to act as an engine for our Tag Historian (i.e. to use our API for storage and retrieval). Starting in 8.1, a Tag Historian license is needed in order for these modules to function. If you are using one of these modules in 7.9 or 8.0 and you have Upgrade Protection on your license, Inductive Automation will provide a free addition to your license, so no additional cost is required upon upgrade. If you have Upgrade Protection, Inductive Automation will attempt to auto detect if you're running one of these modules to update your license in our system automatically, so you would only need to click the refresh license button in your Ignition Gateway to pull in the change. Some third party modules cannot be auto detected, so call your sales representative if a third

party historian module does not work on upgrade and you have an existing 7.9 or 8.0 license with Upgrade Protection, and we will add the necessary parameters to your license.

If your system is one of the few that uses third-party historian engine modules, it is highly advised that you review the system after upgrading to 8.1 and ensure the historian system is working as expected. If there are any issues with historian system after upgrade, and clicking refresh on your license hasn't resolved the issue, please contact your sales representative for assistance.

## Gateway Scan of Project Directory

As of 8.1, the Gateway scans the project directory every **five** minutes for changes. This is an important change for users that have a Version Control System with their Gateway. Previously in 8.0, the scan time was every **10 seconds**, which proved to be resource intensive.

Users who want to change this scan rate back to the 10 second frequency can do so by placing the following system flag in the ignition.conf file:

```
-Dignition.projects.scanFrequency=10
```

## JxBrowser Library Update

We updated our bundled JxBrowser library from version 6 to version 7. For most users, this has no ramifications at all.

For users that have intentionally written scripts against the JxBrowser library, those scripts may have broken as a result of the update. Take a look at the [JxBrowser migration guide](#) for more details.

## Gateway Authentication with Identity Providers

In Ignition 8.1, Identity Providers are used to authenticate users on the gateway, whereas version 8.0 and prior used User Sources. To make the upgrade process seamless, your newly upgraded 8.1 gateway will create a new Ignition Identity Provider, and point it to the System User Source (under Gateway Settings prior to upgrade). For this to work, the Ignition Identity Provider needs to be able to view the list of users from the backing User Source.

In cases where Active Directory or Hybrid User Sources were set as the System User Source, you'll want to make sure that the list of users from the underlying user source is available. Otherwise, some users may not be able to log into the gateway after upgrading. You can validate this before upgrading by viewing the [Manage Users](#) page. If one or more users are missing from the resulting list, then you'll want to refine how the user source builds that list. Based on the system's user source, you may need to check some settings:



- For Active Directory User Sources, it's a good idea to verify the **User Search** and **User List filter** settings on the User Source, making sure they're filtering on the criteria you expect.
- For Hybrid User Sources, the **List Users from Active Directory** will determine where the list of users is generated from. If the resulting user list is missing users, you may need to toggle this setting.
- For Database User Sources using the "Manual" Mode, make sure the **List Users Query** is able to return the users you'd expect. If, after upgrading, you're unable to log into the Gateway you can always perform a [gateway password reset](#) to troubleshoot any authentication issues.

## Perspective Script Transforms

Arrays in script transforms will now automatically be returned as valid JSON. This change technically modifies the value returned by the transform (i.e., potentially adding quotation marks around string elements), which may impact some existing bindings. If you're making use of Script Transforms that interact with arrays, then you may want to reexamine their configuration after upgrade.

## Changes That Require User Action

These changes will require manual action on the part of the system administrator/project author. In other words, these are features or situations that have a direct corresponding solution, but for various reasons cannot be automatically upgraded.

### Redundancy Connection Configuration

Redundancy communication is now accomplished through a Gateway Network connection between the master Gateway and the backup. This mechanism provides greater security and performance than the previous communication channel, but will require the system administrator to re-establish the connection.

The settings for the communication channel are still configured in the Gateway under **Configure>Redundancy**, and are still established from the Backup to the Master, but must be modified before the backup will successfully connect to the master after upgrade.

### Replacement for the `system.tag.browseConfiguration` Function

The Tags system in Ignition changed dramatically in Ignition 8, which makes the Ignition 7 function `system.tag.browseConfiguration` obsolete. The function has been removed from the code base, so scripts using the old `browseConfiguration` function will break upon upgrade. The functionality has been replaced by [system.tag.getConfigurations](#).

# OPC UA Certificate Management

Prior to Ignition 8, Ignition's built-in OPC UA client implicitly trusted the certificate of any server it connected to, and Ignition's built-in OPC UA server implicitly trusted the certificate of any client connecting to it. This is no longer true. New certificate management pages for the client and server have been added to the configuration section of the Gateway under "OPC UA > Security". From this UI, trusted certificates can be imported and quarantined certificates can be marked as trusted. Ensuring the remote certificate is trusted, is required for all secured inbound and outbound connections.

*On upgrade, all secured inbound and outbound connections other than the default "loopback" connection will be faulted until the remote certificate is explicitly marked as trusted.*

# 8.1 to 8.3 Upgrade Guide

## Overview

Ignition 8.3 is a **major** update across all subsystems and modules. Inductive Automation strives to maintain its commitment to backwards compatibility and a straight-forward upgrade process. However, given the vast scope of changes in 8.3, there are inevitably special considerations that need to be evaluated and actions taken in order to successfully upgrade an existing system. This document seeks to identify those issues and provide guidance for users who are migrating from an Ignition 8.1 system. To discover the new features of Ignition 8.3, please see the [What's New](#) section.

**Please read this guide carefully before upgrading a production Gateway.**

### UPGRADING REDUNDANT PAIRS?

If you are looking to upgrade redundant pairs, refer to the [Upgrading a Redundant Pair](#) procedure on the Installing and Upgrading page for a step-by-step description of the process. Be sure to review this guide before getting started.

## Important Considerations

Before upgrading, check your license to ensure it is compatible with 8.3. If your license is not 8.3 ready, contact your Sales Representative.

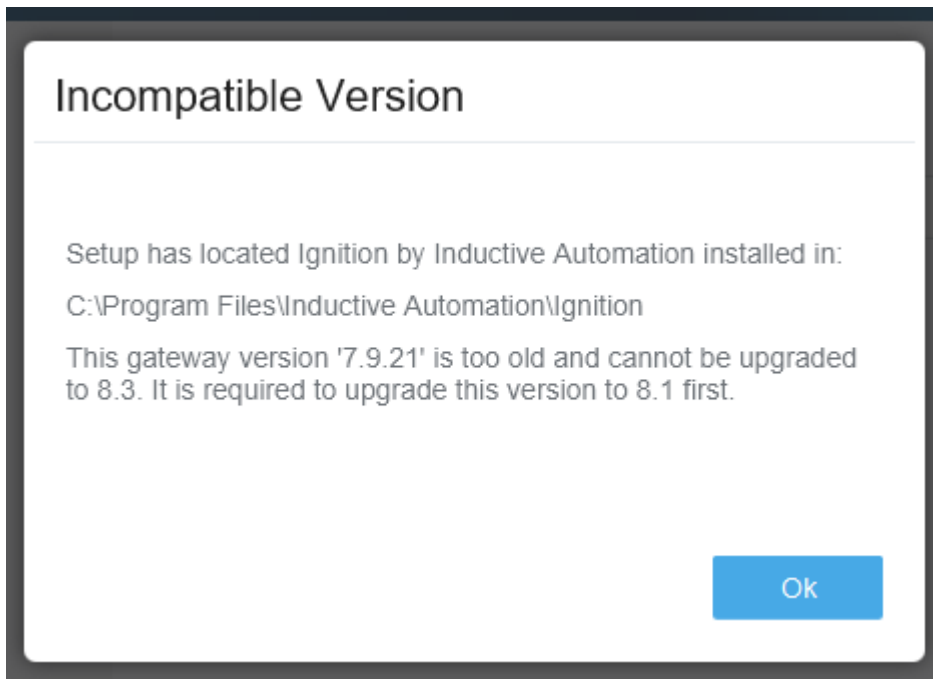
Since Ignition 8.3 is a major version update with many new features such as Store and Forward multi-threading, you may notice some performance impacts after upgrading.

Prior to performing any kind of upgrade, it is good practice to first take a [Gateway Backup](#) of your system. In case something goes wrong during the upgrade process, you will still have a configuration of your system to restore available.

It is **strongly advised** to first upgrade your Gateway to the latest version of 8.1, if you have not already. There **will** be compatibility issues if upgrading directly from 7.9 to 8.3, including changes to:

- Gateway Network
- Serialization

- Data syncing, communication, and storage



### 7.9 END OF LIFE (EOL)

Ignition's Long-Term Support (LTS) for version 7.9 ends on June 30th, 2025. This means that 7.9 Gateways will not be supported by neither the development nor support teams past this date. Due to this, it is recommended to upgrade to Ignition 8.1 to continue receiving support, bug fixes, and security updates.

Additionally, it is **strongly advised** to upgrade either your development or test environment before production. This will help you foresee and eliminate any potentially issues when upgrading, without affecting production. To further reduce any potential issues, your development environment should have similar hardware to your production environment. Upgrading your development environment first will also allow you to see exactly what changes have been made, and how they affect your system.

## Upgrade Process

There are two general approaches when upgrading from Ignition 8.1 to Ignition 8.3. The recommended approach is to use the installer to upgrade, but some users may prefer to uninstall their current Gateways and install a fresh copy of Ignition 8.3. Both options are described below.

### Using the Installer

Using the Installer to upgrade is the easiest approach. Simply run an Ignition 8.3 installer on your existing server, similar to how [minor version upgrades](#) work. As always, we highly advise taking a Gateway backup before upgrading.

# Importing Projects into a Fresh Install

When installing a fresh copy of Ignition, you'll need to manually import projects and tags from the Ignition 8.1 Gateway. We generally **discourage** this practice, as it results in unintended consequences. However, if you must import 8.1 resources into an 8.3 Gateway, then we recommend you use Gateway Backups when possible.

The reason for this is that a Gateway Backup triggers an upgrade check that makes modifications to the resources so they run as expected on the Ignition 8.3 system. The same check is triggered when running the installer. Project and tag imports do **not** trigger this check. As a result, you may need to make manual modifications to the imported resources.

For example, the file system in Ignition 8.3 is drastically different, so without the updates and checks, legacy resources may not work without user intervention. This same consideration applies to other differences, like product name changes. Your 8.1 tags are likely using an old name, where a freshly installed Gateway is using the new name. Therefore, tags imported from an Ignition 8.1 file will likely break upon import due to name mismatches.

## Changes That Require User Action

The following sections detail changes made from 8.1 to 8.3 that require user action, and are organized by subsystem.

### Audit Profile Schemas

Audit Profile table and column names differ in capitalization between 8.1 and 8.3, which can cause SQL queries to fail when new 8.3 installs connect to 8.1 databases with existing Audit Profiles. For example, `AUDIT_EVENTS` and `AUDIT_EVENTS_ID` in 8.1 are now `audit_events` and `audit_events_id` in 8.3, respectively. However, when upgrading a Gateway from 8.1 to 8.3, the Audit Profiles will maintain formatting and work as expected.

## Architecture Considerations

### Data Management

Ignition systems that rely on any Gateway Network services for remote storage will need to follow a specific process when upgrading. Because of serialization changes using Protobuf instead of Java serialization, 8.3 Gateways are not able to store data to 8.1 Gateways over the Gateway Network. This includes storing data using:

- Edge Sync Services

- Remote History Providers
- Remote Alarm Journals
- Remote Audit Profiles

To prevent data loss, the central Gateway hosting the data **must** be upgraded to 8.3 first. This includes Gateways where the main Alarm Journal, audit profile, and history provider are configured. After taking your Gateway offline and upgrading it, ensure that the Gateway is running correctly.

Once the primary Gateway has been successfully upgraded to 8.3, you can proceed to upgrade each of your remote and Edge Gateways that utilize data storing services.

## Tag Editing

Editing tag configurations originating from a different major Ignition version is not supported. If you attempt to edit a tag hosted on an 8.3 remote provider within an 8.1 Designer, this action will fail and cause the Gateway to throw an error, such as a `GatewayException` or `UndeclaredThrowableException`.

## Gateway Network

Ignition 8.3 Gateways can only communicate with other 8.3 or 8.1 Gateways, even if you are using proxies.

The **Require Two-Way Authentication** property now also defaults to `True`. This change enhances your Gateway Network's security, but requires that both ends of a Gateway Network connection **explicitly trust each other**.

To have two Gateways trust each other using **Require Two-Way Authentication**, you will need to approve the certificates on each end of the Gateway Network. On the outgoing Gateway, accept the certificate on the Outgoing Connections page. You can then accept the certificate and connection on the Gateway expecting the incoming connection on the **Incoming Connections** page.

If you are upgrading a redundant pair and the backup node is a new installation, you **must** adjust the backup node's **Require Two-Way Authentication** property to mirror the master Gateway's configuration in order to establish a connection.

## Protobuf and Java Serialization Within the Gateway Network

Due to security and configuration persistence updates, Ignition 8.3 no longer uses Java serialization to convert your data to a saveable state, but instead relies on Protobuf. When upgrading or restoring an 8.3 Gateway, the webserver settings will enable the **Allow Java Serialization property**

automatically. In the Gateway Network, there will be a banner on the Gateway expecting an incoming connection warning you that this property is enabled.

Keep in mind that **Allow Java Serialization** must be enabled if you add 8.3 Gateways to your architecture containing 8.1 Gateways.

## JDBC Driver Modules

Since the MariaDB, MSSQL, and PostgreSQL **JDBC drivers** are now added as modules, containers that used the `GATEWAY_MODULES_ENABLED` flag in 8.1 will need to have the drivers added to the enabled modules list using their new **module identifiers** after upgrading. Once added, the JDBC drivers will startup and their database connections will work as expected.

## OPC UA

If you have the **OPC UA** module, new client and server application instance certificates will be generated when you upgrade. The new client certificate will need to be trusted on the server for any **outbound** connections to third party OPC UA servers. Additionally, the new server certificate will need to be trusted on the client side for any **inbound** connections from third party OPC UA clients.

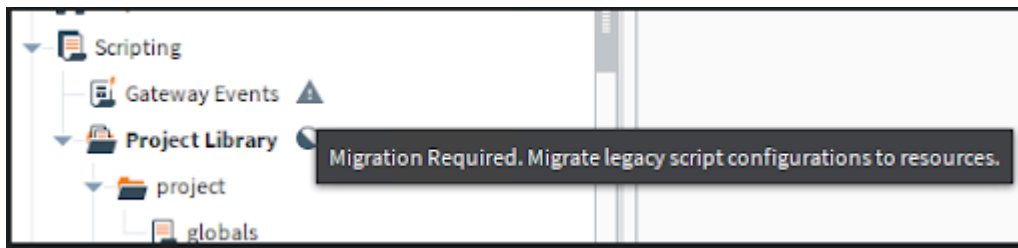
Ignition now uses OPC UA 1.05. Version 1.05 includes better security with role-based access control for your Ignition OPC UA Server, devices, and tag providers. However, this update results in some changes regarding OPC UA access. Namely, anonymous (not logged in) OPC UA clients will no longer have write and call access to devices and Tag Providers by default. Instead, anonymous users will be granted browse and read permissions, while browse, read, write, and call access will be granted to authenticated users.

This change also applies to any device or Tag Provider without explicit role mappings defined. After upgrading, if write and call permissions for anonymous users is necessary, you **must** configure custom permission mappings on the desired devices and Tag Providers to restore that functionality.

Make sure you thoroughly test both anonymous and authenticated OPC UA clients to confirm expected browse, read, write, and call behaviors, especially if they are impacted by the changes detailed above. You can review your **Gateway logs** for any OPC UA access errors.

## Projects

After you successfully upgrade to 8.3, you may see an icon in your Designer next to projects that use **Gateway** or **Client Event Scripts**. This indicates that one final step is needed to finish migrating your scripts.



The scripts that have this warning are still fully functional and will continue to work without needing any immediate action. The warning will also disappear when you select the resource in the Designer, as the platform will finish migrating that specific resource.

#### **(i) NOTE**

Migrated Gateway Event Scripts are located at

`%IgnitionInstallationDirectory%/data/projects/%ProjectName%/Ignition/%GatewayEvent%/` as .py files, while migrated Client Event Scripts are located at

`%IgnitionInstallationDirectory%/data/projects/%ProjectName%/Ignition/script-python/%ScriptName%/` as .py files.

During this migration, some resources may need to be renamed to comply with our [naming validation schema](#). Keep in mind that changing a script's name can break existing references within your project. You will need to manually update these references to the new script names and ensure your scripts are organized and up-to-date with Ignition 8.3's file structure.

## Third Party Modules

Due to major changes between 8.1 and 8.3, any third party modules will need to be checked to ensure they are compatible with 8.3. Check the official documentation and release notes from the developers of your third party modules for explicit statements of compatibility with Ignition 8.3. If compatibility information is not readily available, contact the support or development teams of your third party modules to inquire about their compatibility with Ignition 8.3.

## User Sources

Ignition 8.3 Gateways do not allow users in Internal or AD/Internal Hybrid User Sources to have the same username. An 8.1 Gateway with Internal or AD/Internal Hybrid User Sources must have duplicate users removed before upgrading. Any duplicate users will be displayed on an 8.1 Gateway User Source's Manage User page, and can also be deleted from there. If an upgrade is attempted before removing duplicates, you will need to restore your 8.1 Gateway, remove the duplicate users and upgrade again. Contact our [Support](#) team for more assistance.

**Changed in 8.3.4**



The migration process now detects User Sources with duplicate users, logs information on the duplicate users, and skips migrating the User Sources, instead of incorrectly migrating and breaking User Sources. It is still recommended to remove all duplicate users before an upgrade is attempted.

# Changes To Be Aware Of

The following sections detail the different changes made in Ignition 8.3.

## Call Scripts

The VOIP Notification call script serialization method has been switched from the Apache Commons library's Locale serialization to Java's built-in language tags, which are deterministic and used elsewhere in Ignition. When upgrading, note that certain locales may now resolve to the same language tag. If you have two different call scripts with these respective locales, it will cause a name collision and one of the records will fail to migrate.

For instance, the following locales are technically different, but share a language tag.

| Locale   | Display Name                | Language Tag |
|----------|-----------------------------|--------------|
| nn_NO_NY | Norwegian (Norway, Nynorsk) | nn-NO        |
| nn_NO    | Norwegian Nynorsk (Norway)  | nn-NO        |

## Licensing Considerations

The Tag Historian license item has been replaced by the Historian Core and SQL Historian license items. Some modules, such as Serial Support Client, Serial Support Gateway, and Web Browser, have also either been bundled into other modules, bundled into the Ignition platform, or replaced by newer modules. In particular:

- Serial Support Client and Serial Support Gateway have been bundled into the Ignition platform.
- The Web Browser module has been bundled into Vision. Due to this, the Web Browser component can now be found under the Misc category in the Designer's Vision components.

These items will no longer show up as individual modules, but may still be shown as separate license items. Due to the changes to the Historian, individual JDBC drivers will now show up on the Modules page. The license parameter for JDBC drivers will be marked as "Free" rather than "Activated".

# Gateway Security

8.3 Gateway webpages now operate on a required role basis. Certain pages and actions will not be available if a user is not signed in, or does not have the correct **roles or permissions**. Additionally, permissions granted in 8.1 will not automatically roll over into 8.3, and must be reassigned. Note that some setting names have also been updated.

## Identity Providers

The shape of an exported JSON file for an Identity Provider on the Gateway has changed from 8.1 to 8.3, which means importing Identity Providers from 8.1 Gateways onto 8.3 Gateways is currently not supported.

## Service Security and Security Zones

Service security settings are now part of Security Zone configurations. To modify **service security settings for a policy** in 8.3, you can click on the three dots menu on the right of the zone you want to modify on the Security Zones Gateway page and select **Manage Policy**.

If you have a policy defined on the `default` security zone, it will be brought in as part of the Gateway Deployment Mode's core collection for that zone.

## Enterprise Administration

The Agent Recovery EAM task has been removed from Ignition 8.3. You can still use other agent tasks to perform a similar operation.

The 8.3 **License Management** page on the controller Gateway can now display and manage leased licenses (eight-character licenses). Additional information, such as the last renewal timestamp and result, will be displayed. The Activate License, Update License, and Unactivate license tasks will also work with leased licenses.

The EAM Remote Upgrade task cannot upgrade Ignition agents from version 8.1.x to 8.3.x on Apple M-series Macs. This is because Ignition 8.3.0 introduced native builds for M-series architecture, whereas version 8.1.x only supported the x86 architecture. The EAM task doesn't handle the architecture change that occurs during this specific upgrade. To upgrade these agents, you must perform an in-place upgrade instead of using EAM. Once the agent is successfully upgraded to version 8.3.0 using this method, subsequent EAM Remote Upgrades task (e.g., to 8.3.1) will work.

When using the **Send Project** or **Send Project Resources** task, some resources, such as Gateway Event Scripts and Perspective Event Scripts, cannot be sent from an 8.3 EAM controller to an 8.1 agent.

## Store and Forward

When upgrading your historians, the **Store and Forward Primary Store Maintenance Value** property (known in 8.1 as Max Records) will be set to zero by default. This means that the local disk cache is configured to store an unlimited number of data points before forwarding them to the historian.

This is possible due to the Store and Forward engine now utilizing multi-threading, allowing different data types to be stored and forwarded at the same time without blocking another, namely:

- Alarming
- Auditing
- Scripting
- SECS/GEM
- Tag history
- Transaction Group

Quarantine exports have also been changed to use JSON rather than XML. This means that quarantine exports from 8.1 Gateways cannot be imported into 8.3 Gateways.

When upgrading the Gateway, the Store and Forward system will begin converting your old serialized data. Any leftover data will remain as an HSQL file, and should be moved to

`%IgnitionInstallationDirectory%/data/local/store-forward/quarantined-databases/`.

## Tags

The **Alarms** folder in the **Tag Browser** for tags with alarms has been replaced with a new **Alarm Metrics** folder, providing a new set of metrics for scripting and monitoring issues. This change also makes it easier to find the **Alarm Metrics** folder, and improves performance related to tag alarm metrics. Existing scripts and bindings will still work with the deprecated **Alarms** folder.

Additionally, due to the Gateway file system changes, tag JSON files are now stored with the path that's shown in the Tag Browser following

`C:\Ignition\8.3.0\data\config\resources\core\ignition>tag-definition`. This change can result in long filepaths, and may impact Windows users since the Windows API has a filepath limit of 255 characters. See the **Working with Long File Paths** page for more information on how your system may be impacted.

Note that the names of files and directories are still bound by names less than 255 characters long, and this change is focused on the filepaths themselves.

## OPC UA

Ignition will not migrate any data within the `Iec61850ReportEntryIds` table, which uses reports that are subscribed to IEC61850 devices to help Ignition keep track of the latest ID it has received. In certain scenarios, migrating this data would cause Ignition to attempt to store duplicate data, resulting in the data being quarantined in the Store and Forward system.

## Perspective

### File Upload Component

The File Upload component will now only accept files smaller than 20 MB, regardless of the `fileSizeLimit` property. This can be increased using the `max-file-size` property within the `web.xml` file.

### Browser Requirements

The Ignition 8.3 minimum browser versions required to run Perspective Sessions have changed from 8.1. See the [Browser Version Requirements](#) page for the current list to make sure you meet the new minimums before upgrading.

## Launcher Considerations

Application launchers and Perspective Workstation running 8.3 are backwards compatible with 8.1. However, 8.1 launchers and Perspective Workstation are not forward compatible with 8.3. Because of this, you can use [DeepLinks and File Associations](#) to open projects hosted on 8.1 Gateways.

## Hot Swapping Modules

Hot swapping modules is no longer supported in Ignition 8.3. You will need to restart your Gateway if you want to install or upgrade a module.

## System Function Changes and Deprecations

Ignition 8.3 introduces two new sets of system functions, prefixed by `system.vision` and `system.historian`.

The `system.vision` namespace replaces many system functions from different subsystems, including:

- `system.file`
- `system.gui`
- `system.nav`
- `system.net`
- `system.print`
- `system.security`
- `system.util`

Many of the replaced system functions are still functional, but it is recommended to utilize the `system.vision` namespace instead.

The `system.historian` namespace both introduces new system functions and replaces others. The following table of system functions have been deprecated, replaced with various `system.historian` functions:

| System Function                              | Replacement System Function                         |
|----------------------------------------------|-----------------------------------------------------|
| <code>system.tag.browseHistoricalTags</code> | <code>system.historian.browse</code>                |
| <code>system.tag.queryTagHistory</code>      | <code>system.historian.queryRawPoints</code>        |
| <code>system.tag.queryTagCalculations</code> | <code>system.historian.queryAggregatedPoints</code> |
| <code>system.tag.queryTagDensity</code>      | No Replacement Function                             |
| <code>system.tag.queryAnnotations</code>     | <code>system.historian.queryAnnotations</code>      |
| <code>system.tag.storeTagHistory</code>      | <code>system.historian.storeDataPoints</code>       |
| <code>system.tag.storeAnnotations</code>     | <code>system.historian.storeAnnotations</code>      |
| <code>system.tag.deleteAnnotations</code>    | <code>system.historian.deleteAnnotations</code>     |

In addition to the new system function namespaces, the `system.db` namespace has been overhauled with the following deprecated and replacement functions listed in the table below.

| Deprecated System Function                      | Replacement System Function                                                        |
|-------------------------------------------------|------------------------------------------------------------------------------------|
| <code>system.db.clearAllNamedQueryCaches</code> | <code>system.db.clearCache</code>                                                  |
| <code>system.db.clearNamedQueryCache</code>     | <code>system.db.clearCache</code>                                                  |
| <code>system.db.dateFormat</code>               | <code>system.date.format</code>                                                    |
| <code>system.db.refresh</code>                  | <code>system.vision.refreshBinding</code>                                          |
| <code>system.db.runNamedQuery</code>            | <code>system.db.execQuery</code> , <code>system.db.execUpdate</code>               |
| <code>system.db.runQuery</code>                 | <code>system.db.execQuery</code> , <code>system.db.runPrepQuery</code>             |
| <code>system.db.runScalarQuery</code>           | <code>system.db.execScalar</code> ,<br><code>system.db.runScalarPrepQuery</code>   |
| <code>system.db.runSFNamedQuery</code>          | <code>system.db.execQuery</code>                                                   |
| <code>system.db.runSFUpdateQuery</code>         | <code>system.db.execUpdateAsync</code> ,<br><code>system.db.runSFPrepUpdate</code> |
| <code>system.db.runUpdateQuery</code>           | <code>system.db.execUpdate</code> , <code>system.db.runPrepUpdate</code>           |

Other functions that have been deprecated include the various `system.net.http*` functions, which can now be performed using the `system.net.httpClient` function.

The following system functions have been deprecated, with no new system function replacements:

- `system.gui.convertPointToScreen`
- `system.gui.getQuality`
- `system.dataset.toPyDataSet`
  - Note that this function has been deprecated because datasets no longer need to be manually wrapped as PyDatasets. This change also impacts `system.dataset.toDataSet` from 8.1, which now has only a single syntax and should be written as `system.dataset.toDataset` in 8.3.

## Custom Themes

In 8.1, theme authorship relied solely on the filesystem. In 8.3, the new config and resource collection model required the existing theme structure to conform to this new model. The old entry point files that

existed at the root of the themes folder have been removed. Instead, each respective theme gets a `config.json`.

Within this config file is an `isPrivate` property that when set to true will prevent this theme from being listed as an available theme. This is useful in instances where you may have a common or shared set of theme resources that other themes might import or extend. Also within this config file is an `entrypoint` property that lets Ignition know where to start processing your theme. This is generally an `index.css` file that exists within your theme folder. See the [Creating and Using Custom Perspective Themes](#) page for more information on how the new file structure works.

If you followed the structure and format Ignition used for the built-in themes (light, dark, light-cool, dark-warm, etc.) in 8.1, then your themes will migrate successfully. If not, you will likely need to update some of your imports, and in some situations create a new theme. For example, if your old `custom-theme.css` entry file had an import like `@import "../light.css"`, you will need to add `@import "../light/index.css"` to your theme's entrypoint file. Additionally, all external imports or declarations you might have had in the old entry file will need to be moved into the new entrypoint file for your theme. You can find all of the original migrated files in the `.migrated-themes-TIMESTAMP` directory within `data/modules/com.inductiveautomation.perspective` for reference when resolving your imports and into this new structure.

In circumstances where you had an old entry file (i.e., `themes/test-theme.css`), but no peer directory of the same name (i.e., `themes/test-theme`), one will be created as part of the migration process. Within this migrated directory will be an `index.css` entrypoint. You will need to update this `index.css` to include any imports you might have included in the old entry file as Ignition will not attempt to resolve, modify, or move any imports during the migration.

## Discontinued Features

### Deprecated Expression Functions

The `forceQuality` expression function has been deprecated. Users should instead utilize the `qualifiedValue` [expression function](#).

### Designer

The Identity Provider property within the Designer's **Project Properties > Perspective > General** has been deprecated. The [Identity Provider setting](#) under **Project Properties > Project > General** will be used instead.

## Perspective

The `pager.initialOption` property for Perspective **Tables** has been deprecated and replaced with a new `option` property. This new property improves on the deprecated property by honoring external writes even after the table initializes upon loading.

## Tag Historian

**Custom Tag History Aggregates** have been deprecated, as this was originally intended to be a workaround to older SQL historian schema limitations. This feature is only supported when used with the legacy `system.tag.queryTagHistory` and `system.tag.queryTagCalculations` functions, which are also deprecated. While still functional, these features are no longer recommended for new development.

## New Features

The following sections details new major features added in Ignition 8.3. See the [New in this Version](#) page for information on all new features.

## Modules

The following is a list of modules introduced in Ignition 8.3:

- Event Streams
- Kafka Connector
- MariaDB JDBC Driver
- MSSQL JDBC Driver
- PostgreSQL JDBC Driver
- Siemens Enhanced
- SQL Historian

## Drivers

A new **Siemens Enhanced driver** is available through the Siemens Enhanced Driver module. This new driver supports browsing and symbolic access when connected to S7-1200 and S7-1500 devices.



# Event Streams

**Event streams** have been added to Ignition 8.3 as project resources, and allow users to pull data from a specified source, perform different actions on the data, and send it to a defined handler.

Event streams operate in stages, with each stage performing a different action. Some stages, such as filtering and transforming, are optional. Each stage and their function is displayed below:

| Stage         | Description                                                                                                                                                                                                         |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Source        | The origin of the data to send through the event stream.                                                                                                                                                            |
| Encoder       | Encodes the data in the event stream into a specified format.                                                                                                                                                       |
| Filter        | Filters out any unwanted or unnecessary data using a script.                                                                                                                                                        |
| Transform     | Transforms the data from one type of object to another, with the new object being sent down the event stream.                                                                                                       |
| Buffer        | The staging area for event data, batched together based off a set of defined parameters. Batches of data will be sent once the parameters are met.                                                                  |
| Handler       | Takes the data from the event stream and performs a user-defined action with them. Multiple handlers can be utilized at the same time, allowing your data to be sent to different places or used in different ways. |
| Error Handler | Acts as a final catch-all for any missed errors during the event stream.                                                                                                                                            |

## Gateway Deployment Modes

**Gateway deployment modes** allow you to create different configurations of your Gateway. These configurations can be preset with different values for Gateway resources and properties, creating a separate environment.

Deployment modes are created in the Gateway, but utilize the **Gateway Configuration File** when you want to switch the deployment mode your Gateway is running in.

You can also modify deployment modes through Ignition's file system. If modified this way however, the Gateway will not recognize any changes until the file system is scanned and updates are brought in.

Deployment modes follow **Gateway security** logic, meaning any unauthorized users will not be able to view Gateway configuration pages or resources unless permissions and access roles are defined.

## Historians

A new **Core Historian** was introduced in 8.3. This new Historian, initially referred to as the Power Historian, is powered by QuestDB and optimized for storing time-series data. The Core Historian will automatically partition data by tables, using specified intervals set within the Historian's configuration. Additionally, the Core Historian will only use the Store and Forward system if there are pending writes to the database. If there are no pending writes, the Core Historian will skip the Store and Forward system entirely.

The historian changes additionally introduced a change in formatting for qualified historical paths. The path still relies on key-values pairs, but instead of using `drv` to include both the Gateway and Tag Providers names, `sys` and `prov` need to be used to identify the Gateway name and Tag Provider name, respectively.

### Syntax Examples

```
# 8.1 Historical Path Syntax
```

```
histprov:Sample_DB:/drv:myGateway:My_Provider:/tag:My_Folder/Another_Folder
```

```
# 8.3 Historical Path Syntax
```

```
histprov:Sample_DB:/sys:myGateway:/prov:My_Provider:/tag:My_Folder/Another_Folder
```

Note that the SQL Historian still requires the `drv` key-value pair syntax, and any `drv` syntax used in Ignition 8.1 will still work in 8.3.

### ! INFO

The Internal Historian (Legacy), powered by SQLite, is still available to use.

Ignition 8.3 also introduces new `system.historian` **functions**, allowing users to interact with Ignition's Historian system. Some of these new functions have replaced deprecated functions. See the **System Function Changes** section for more information on which functions have been deprecated.

## Launchers and Workstation

You can now set **deep links and file associations** to launch your application without needing to open the launcher. Keep in mind that the file extension and URL protocol associations options must be enabled when installing the launcher.

Deep links will allow you to open a project or Designer with a URL. These URLs use the following format: `%LauncherType%://%GatewayAddress%/%ProjectName%`. For example, if you wanted to launch a local Perspective project through Workstation, the URL would be:

```
perspective://localhost:8088/MyPerspectiveProject.
```

File Associations allow you to customize how to launch projects by using JSON files based off the launcher type. Each launcher will use a different file extension:

- Perspective Workstation: `.perspective`
- Vision Client Launcher: `.vision`
- Designer Launcher: `.designer`

## Perspective

Perspective has several new features in 8.3, including the **Drawing** component, **Form** component, and **Offline Mode**.

The Perspective Drawing component allows you to create custom drawings and images, similar to Vision's **Drawing Tools**. You can also import vector graphics (SVGs) and images that use `.gif`, `.jpeg`, and `.png` file extensions.

The Perspective Form component makes inputting data much easier for your users. Different aspects of the form can be customized, such as dynamically displaying fields depending on user input and creating validation rules. You can use bindings to further tailor the form to behave exactly how you need.

Finally, Offline Mode allows users to continue using a Perspective project, even if the project loses network access to the Gateway. This is useful in scenarios like when you are using a mobile device, remote locations, and unstable network connectivity. Some features will not be available if a project is running in Offline Mode, including:

- Realtime values from tags, alarms, and queries
- Gateway Event or database scripts
- Previously unloaded views

Any data inputted by a user running in Offline Mode will be cached until network connectivity is restored, after which the data will be sent to the appropriate location.

## Reporting

The following **components** can be used as either raster or vector images:

- Barcode
- Bar Chart
- Pie Chart
- Radar Chart
- Timeseries Chart
- XY Chart

A new **Radar Chart** component is also available to use on reports.

## Scripting

When using a scripting window, the **autocomplete and hints** feature will also list system library constants and identify deprecated functions.

## Security

You can encrypt secrets such as credentials, API tokens, and private keys using the 8.3 **Secrets Management** system and customize different aspects of it using Secret Providers. You can also use the **Secrets Management Key CLI Tool** to manage keys and run scripts from the command line.

## Tags

A new System Tags folder called **ModuleVersions** has been added to help EAM controllers monitor module versions on connected agents.

# Post Upgrade Actions

The following sections detail different actions to take after upgrading to 8.3.

## Verifying System Health

It is good practice to ensure everything is working correctly after upgrading. The following list of tips is not exhaustive, but can help ensure your system is working properly.

- Check the Diagnostics Overview page for a quick top-level view of your system. This page is found on the **Gateway Webpage > Diagnostics > Overview**.
- Check your Gateway and wrapper logs for any repeated warnings or errors. See the **Logs** section for more details.
- Verify that historical data is still being stored.

- Verify your projects are still functioning correctly.
- Make sure that all behavior after upgrading is expected, and that there are no unintended actions or consequences.

### **MODULES RUNNING IN TRIAL MODE?**

If your modules show a Trial license status after upgrading when Activated is expected, you may need to reactivate your license. Once your license has been reactivated, the modules will display an Activated status.

## Troubleshooting Issues

If you run into any problems while upgrading or after upgrading, we recommend reaching out to our [Support](#) team. When creating a ticket, please provide a detailed explanation and any relevant resources, including any photos or screenshots that help illustrate the problem.

The section below details the various logs and locations that pertain to an upgrade that you can provide our Support team. If you are able to reliably reproduce the issue, please document the exact steps and include any necessary resources used during your replication attempts. For instructions on how to roll back to a previous version, refer to the [System Rollback](#) section of Installing and Upgrading page.

### **NOTE**

During the upgrade process, Ignition migrates resources from the internal database (IDB) to the new file system. The deprecated IDB is not removed after upgrading, but will not affect your system as it is no longer used.

## Logs

The following table displays different types of logs that can help troubleshoot errors from upgrading and the log locations.

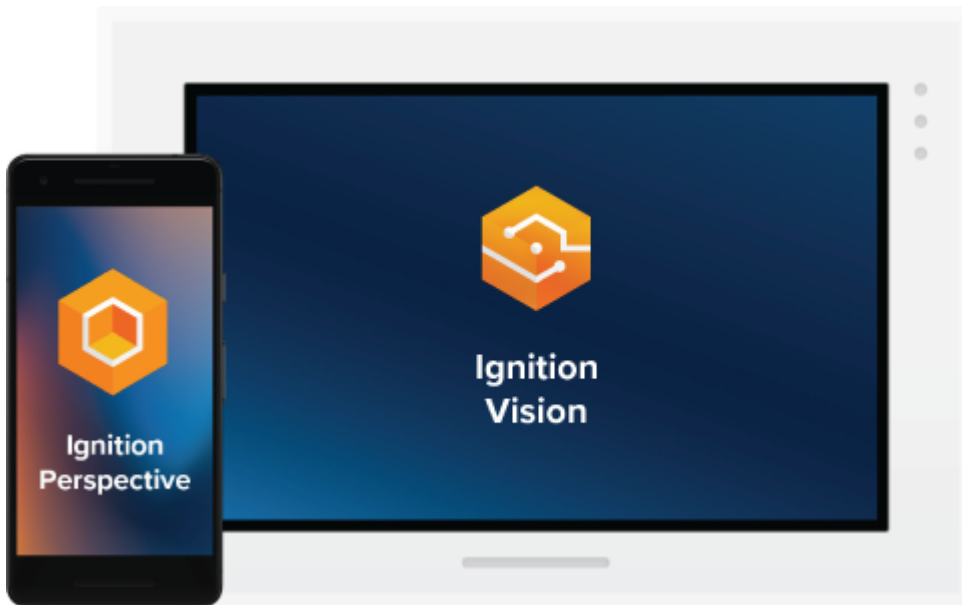
| Log Directory                                      | Type of Log                           | Description                                                                                                                                                                                                   |
|----------------------------------------------------|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>%IgnitionInstallationDirectory%/logs/</code> | Wrapper                               | Provides information about the Gateway, subsystems and errors from Gateway-scoped resources.                                                                                                                  |
| <code>%IgnitionInstallationDirectory%/logs/</code> | Tag-migration                         | Provides information about the migration status of different Tag Providers. Each Tag Provider will have its own JSON migration file, with a summary metrics for different issues, and the affected tag paths. |
| <code>%IgnitionInstallationDirectory%/logs/</code> | <code>install_{YYYYMMDD-HH:mm}</code> | Provides information about the installer for the extraction and                                                                                                                                               |

| Log Directory                                                       | Type of Log       | Description                                                                                                                                                               |
|---------------------------------------------------------------------|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                     |                   | replacement of the configuration files in the Ignition 8.3 file system after which the Ignition service is started.                                                       |
| <code>%IgnitionInstallationDirectory%/data/config/resources/</code> | migration-log     | Provides a summary of migrated IDB resources to the Ignition 8.3 file system, along with information about tabs that either failed to migrate or have yet to be migrated. |
| <code>%IgnitionInstallationDirectory%/data/projects/</code>         | Conversion-report | Provides information about the conversion of project resources to the Ignition 8.3 file system.                                                                           |

# Perspective and Vision - Which Visualization System is Best for Me?

Ignition's Perspective module and the Vision module each enable you to rapidly develop industrial applications for your site. Perspective is Ignition's visualization solution that covers both desktop and mobile devices, taking advantage of the latest technologies, and is recommended for almost all new projects. If your application needs to run on a desktop, in an HMI, in a web browser, or on a mobile OS like iOS or Android, then Perspective is a great choice. Desktop PCs, iPCs, big screen displays, phones, tablets, and other devices can easily run Perspective Sessions.

When you start a new project, there are many things to consider, such as who the users will be, how much data you need, and what kind of time and resources you have to work with. Deciding whether to use Perspective or Vision (or both) really comes down to which options best fit your project at the visualization level. Note that Vision and Perspective both support security with Two-Factor Authentication (2FA) or federated identities for the application you're building.



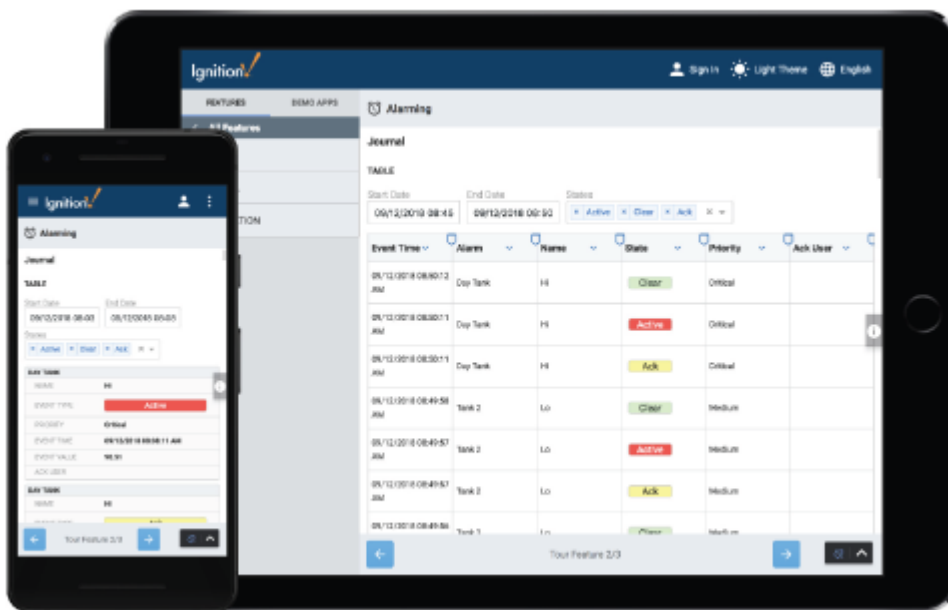
## When to Use Perspective

If you need to build mobile-responsive applications, then Perspective is the recommended way to go. If your application needs to run on a mobile OS, namely iOS or Android, then choose Perspective. Phones, tablets, and other mobile devices can easily run Perspective Session. New in Ignition 8.1, **Perspective Workstation** runs in Windowed mode and also has built-in features to run in full screen



Kiosk mode eliminating any distractions from the underlying operating system. Perspective also runs in web browsers on desktop PCs. If you're building an application that needs to run on phones, browsers, and desktop applications that don't have a strong need for OS resource access, Perspective is a great choice.

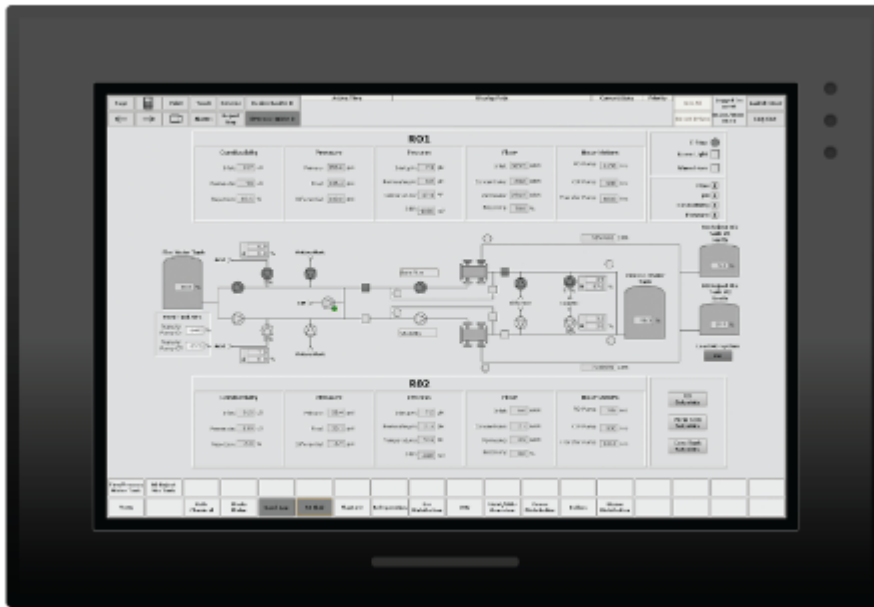
With Perspective, you can automatically adapt to fit any screen size using mobile-optimized container types. It provides the ability to use your device's sensors and intuitive touch commands, as well as message handling, flexible property bindings, and CSS3 styles. For example, with an application built in Perspective, you could augment alarm information by taking a picture of the faulty machine. You could scan a QR code by a machine and have the SCADA system tell you what to do, or take readings or photos in the field and tag them with GPS and other sensor data. There are so many possibilities.



## When to Use Vision

Vision is and has been for many years a top-class desktop application. Vision is a great choice for traditional industrial plant-floor and desktop screens, standalone HMIs, and the like. If you need OS resources, file access, serial port access, or custom Java code running directly in the client, and you're looking for visualization through a desktop application, choose Vision.

In Ignition 8, the Vision Module got one of its biggest updates since it was first released in 2010, allowing you to make your HMIs and plant-floor dashboards faster, easier to deploy, and more beautiful than ever.



## Should I Upgrade?

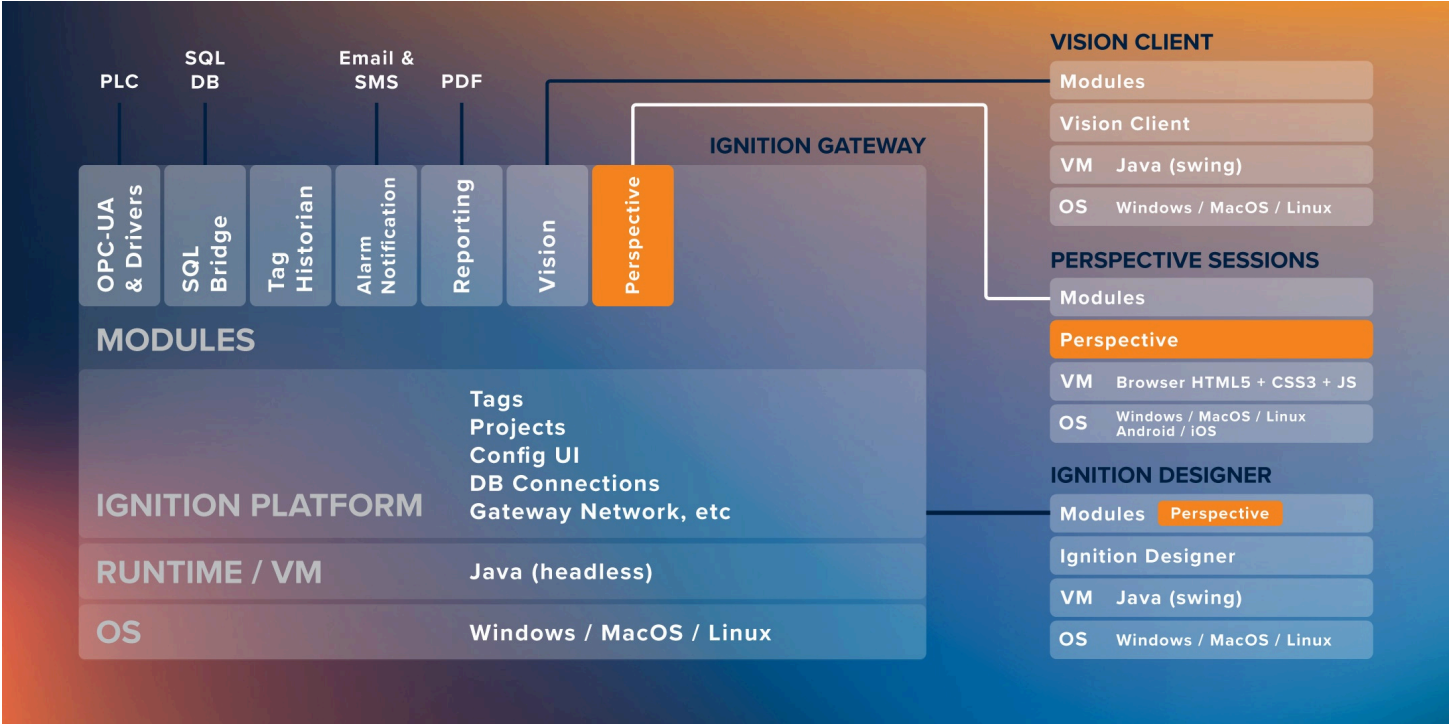
There are many considerations for using Perspective or Vision. Perspective contains familiar elements like the drag-and-drop Designer, property binding system, and scripting engine. Refer to the [7.9 to 8.1 Upgrade Guide](#) for complete information. See also [A Vision-Oriented Guide to Perspective](#).

## Behind the Scenes

A “**Client**” in Vision is called a “**Session**” in Perspective, and the two actually have very similar tech stacks. At the bottom of the stack is the OS. In addition to supporting Windows, macOS, and Linux, Perspective also supports Android and iOS. The next part of the stack is the web browser, which is very similar to the runtime/VM layer in the other stacks because it provides an environment to execute code, generate user interfaces, and communicate back to the Gateway. On top of that runs the Perspective session application itself, and then modules can augment the features of Perspective.

In the topology of a typical Ignition installation, there’s the Ignition Gateway, the Ignition Designer, and Vision clients. At the base of the Gateway is the operating system, which can be Windows, Mac, or Linux. Above the OS is the Java runtime/VM layer, which is what Ignition runs on. Above the runtime/VM layer is the Ignition platform, which provides many features and services like Tags, projects, database connections, the Gateway Network, and so on. At the top of the tech stack are modules, which let you do a number of useful things like connect to devices, use databases effectively, send alarm notifications, generate reports, and, in the case of the Vision Module, create applications which run as Vision clients.

As you can see, Perspective is just another module. It installs into the Gateway and provides a design experience in the Designer just like other Ignition modules do.



# System Architectures

## Overview



INDUCTIVE  
UNIVERSITY

**Ignition System Architecture**

[Watch the video](#)

Ignition is flexible enough to meet the demands of any enterprise infrastructure large, small, or somewhere in-between. You can deploy Ignition at one site, multiple sites, or host it in the Cloud. This section displays several common architecture examples. Many are simply examples, but they are a great starting point. Additionally, these example architectures can be modified or scaled out to accommodate a number of different requirements.

Click on each architecture to learn more about it.

### SECURITY ARCHITECTURE

Learn some best practices for how to secure the following architectures by reviewing [Ignition Security Architecture](#).

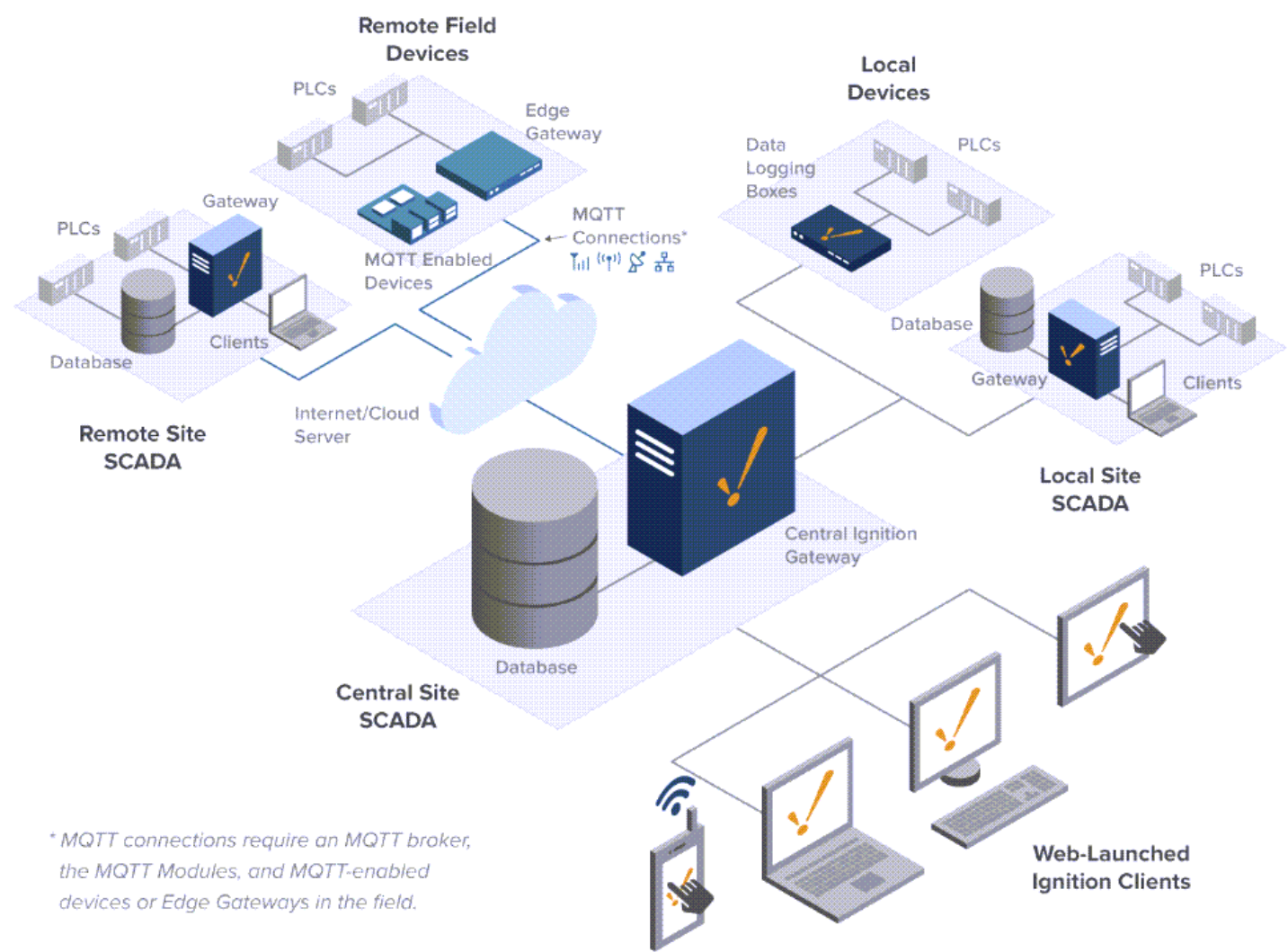
# Basic Architecture



# Scale Out Architecture

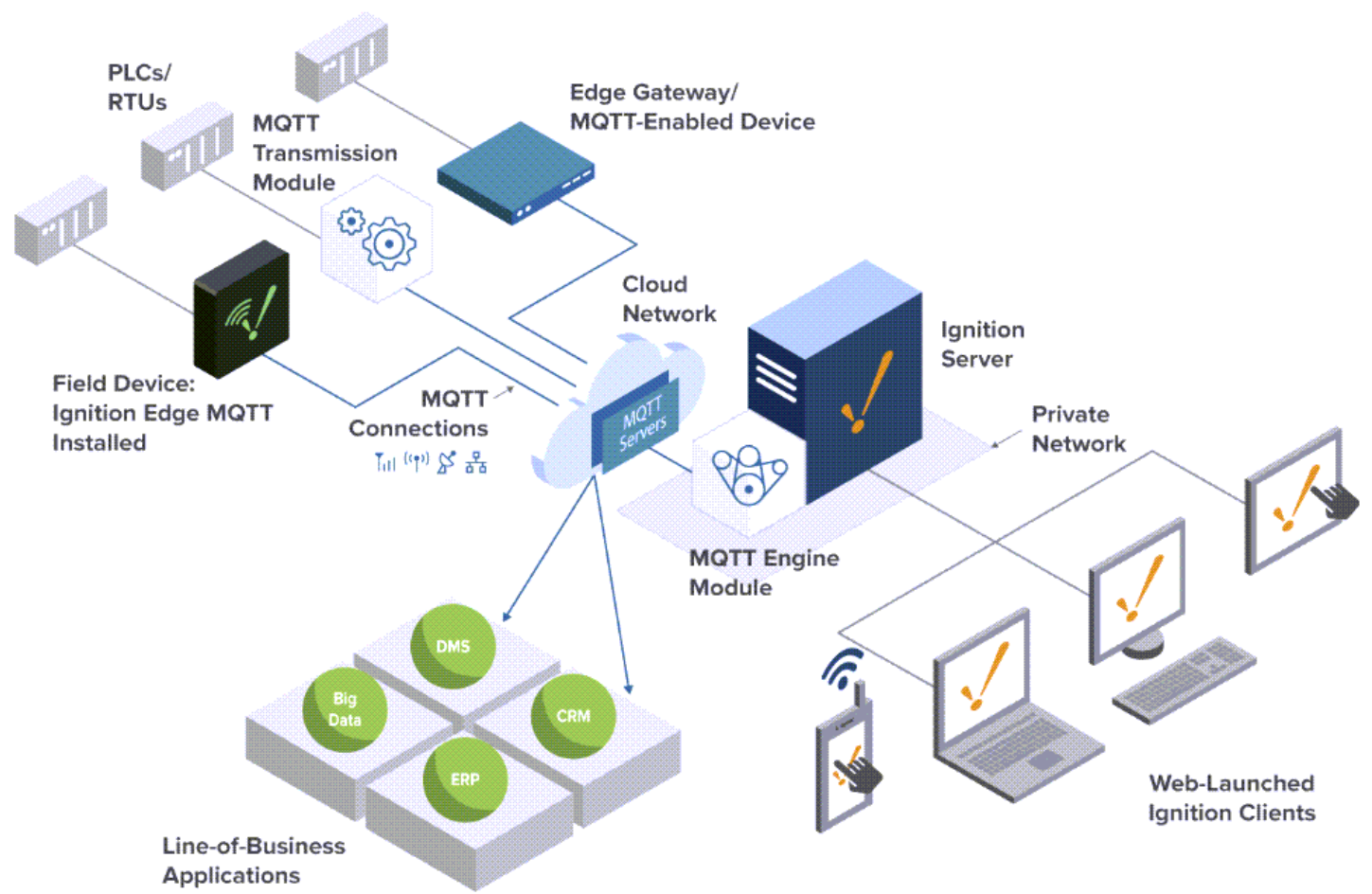


# Hub and Spoke Architecture



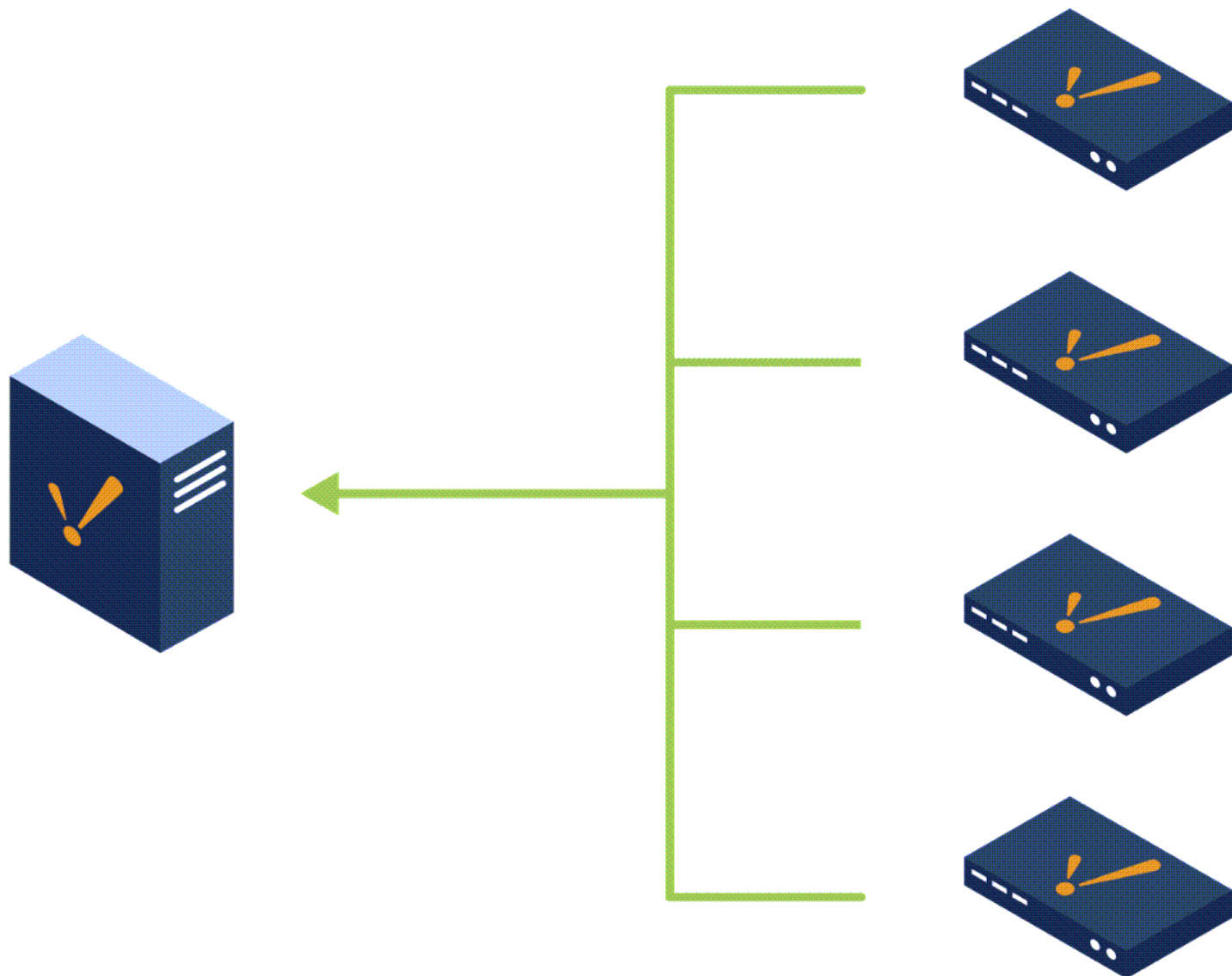


# IIoT Architecture





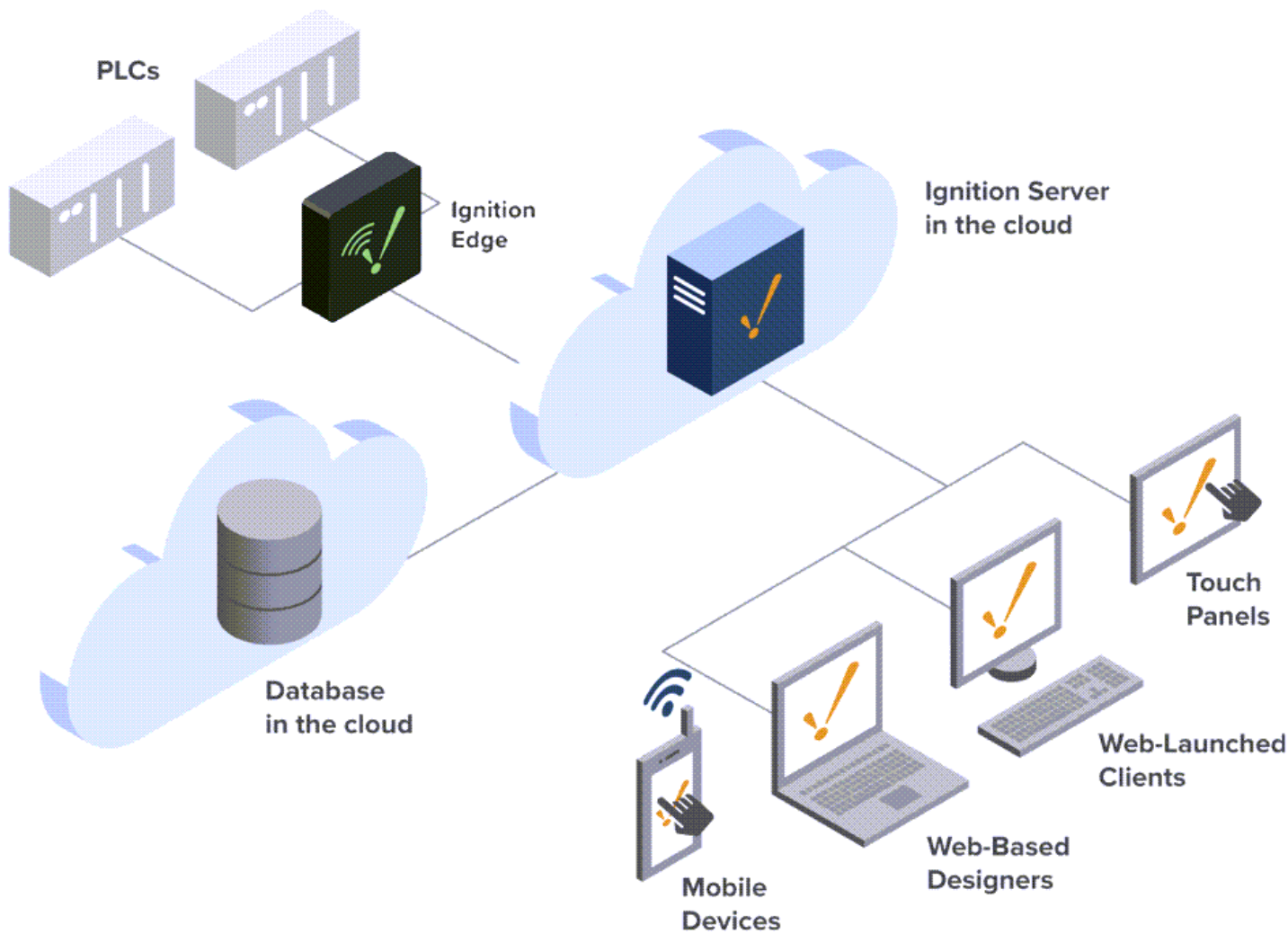
Enterprise Architecture



# Redundancy Architecture



# Cloud Based Architecture



# AWS Outposts Architecture

# Basic Architecture

## Single Server Install

Ignition's most typical architecture is a basic single installation. This is very simple to set up and it provides the powerful functionality of the Ignition Gateway and it can serve as a starting point for more complicated architectures.

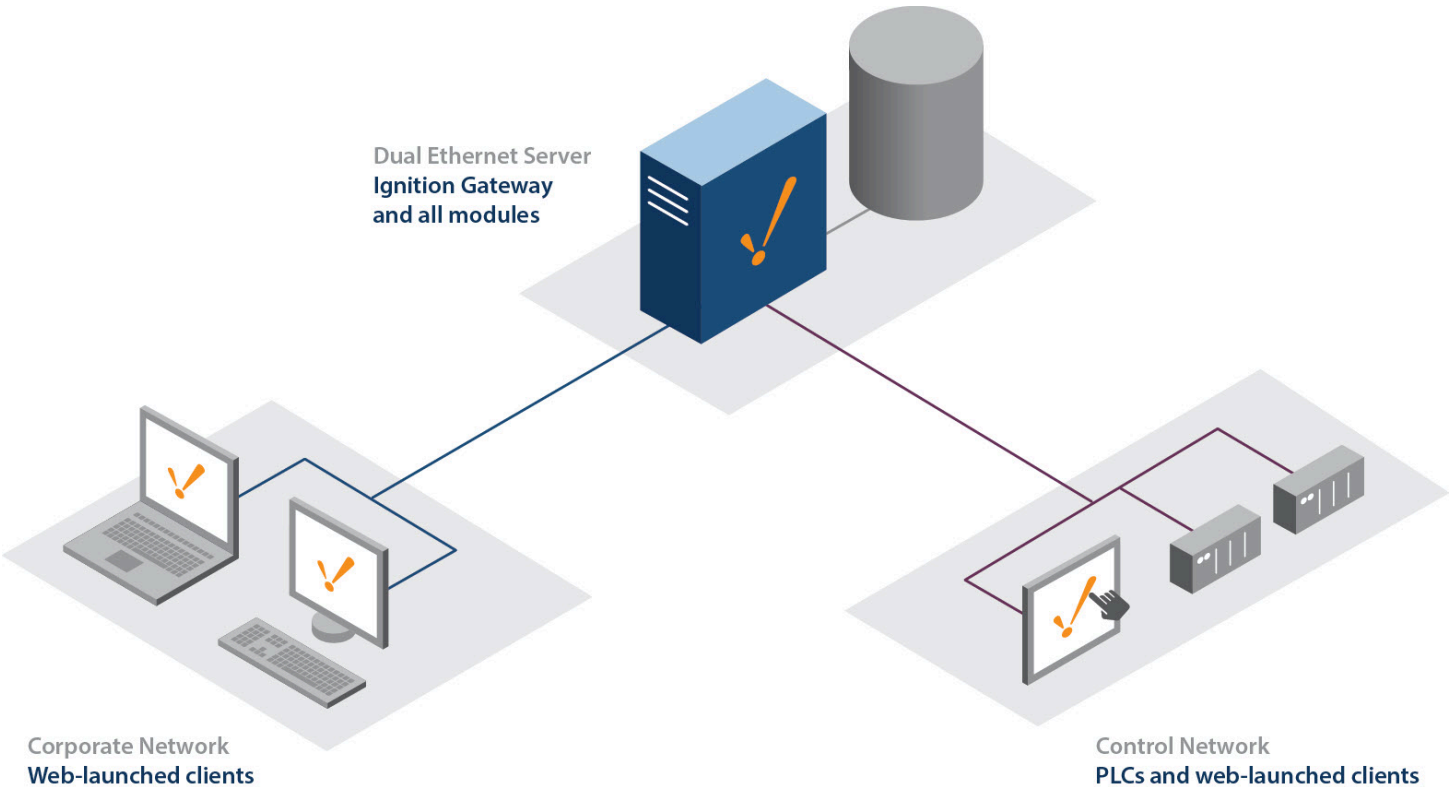
The Basic Architecture consists of a single Gateway that can connect to multiple PLCs, databases, and other devices, all with a single licensed install. With the Ignition licensing system, it's easy to add new devices, databases, and clients. Simply connect them to the Ignition Gateway, no licensing changes required. The Ignition Gateway can launch multiple clients on everything from touch panels to workstations and even mobile devices, all from one Ignition installation.



## One Server, Multiple Networks

The Ignition Gateway supports dual-NIC servers, and can act as a bridge between multiple networks, or communicate with multiple sites over a corporate WAN. Since clients talk to databases and PLCs

through the Gateway, clients can be launched from both a corporate network and an isolated control network, and provide full access to both. Built-in **security settings** can restrict project access to users on different networks, either by restricting certain things in a project, or denying access to a whole project based on user role and network location.



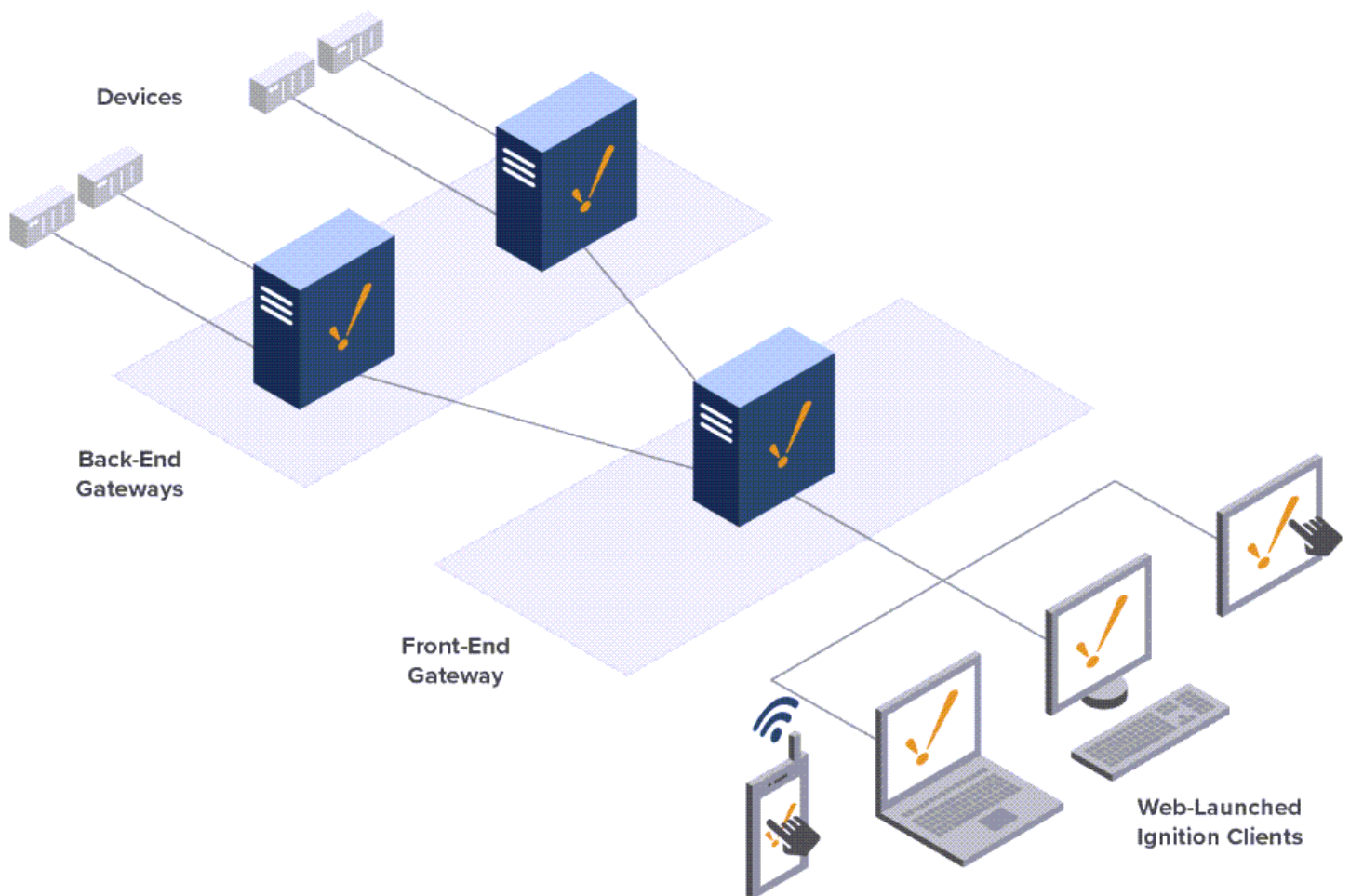
# Scale Out Architecture

## Scaling Out Ignition for Larger Systems

In larger systems, it is often easier to have multiple Ignition installations to help split the load between the front-end tasks and the back-end tasks. This is perfect for single large systems that aren't split up into different sites. In those cases, the [Hub and Spoke Architecture](#) is usually a better fit.

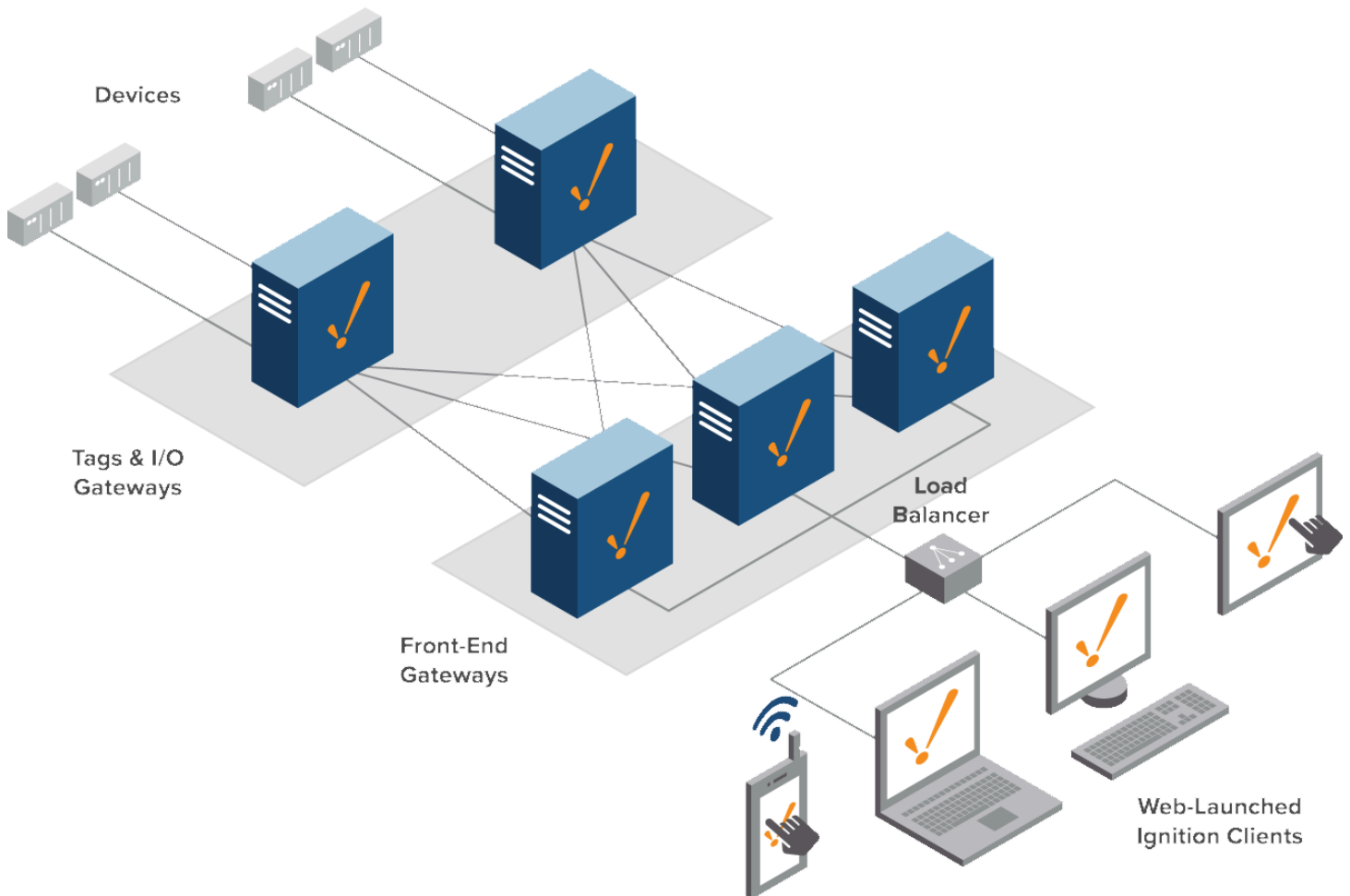
In the Scale Out Architecture, we have at least one Gateway that handles back-end communications. The back-end Gateway deals with all PLC and device communications. The front-end Gateway handles all of the Clients, serving up the data pulled from the back-end Gateway. This is made possible through the [Gateway Network](#), connecting Gateways to each other, and allowing tags to be shared through remote Tag Providers.

For more information on migrating to a scaled out architecture, see the [Scale-Out Architecture Guide](#) page.



# Load Balancing

The best thing about the Scale Out Architecture is that it is easy to scale up Ignition as your system grows. In the image below, we added more front-end Gateways to help handle an increase in clients, and a Load Balancer to automatically distribute the clients between them.



## Gateway Types

When utilizing Scale Out, an Ignition Gateway is given focus due to its placement. There are two possible types:

- **Back-End Gateway:** This gateway is responsible for communicating with the PLCs, and executing Tags. They share their local Tags with the Front-End Gateways via a Remote Tag Provider, and are generally responsible for recording history. Additionally, alarms can be added to Tags locally, and exposed elsewhere in the system.
- **Front-End Gateway:** This Gateway is responsible for hosting the clients, allowing the Back-End Gateways to focus solely on PLC communication and history.



## Database Placement

With this type of architecture, both types of Gateways will need database access: the Back-End Gateways need to be able to store data, while the Front-End Gateways need to query the data out.

## Scaling Out the Databases

Multiple on-site databases may also be utilized with this architecture. This typically involves configuring a database cluster.

## Why Use the Scale Out Architecture?

Scale Out is utilized in large systems to distribute the workload across multiple servers. This is in contrast to a 'Scale Up' ideology where you have a single powerful server manage the whole system.

## Decentralized Servers

In this architecture, each server only deals with a small part of the overall system. Should a server fault, only that part of the system is hindered, allowing other parts in organization to continue uninterrupted. Applying Redundancy to the Back-End servers is ideal to maximize uptime.

## Pooled Resource Usage

Since multiple servers are working together, bottlenecks are reduced. A massive amount of work can be performed in this system without slowing down other servers.

## Easy Growth

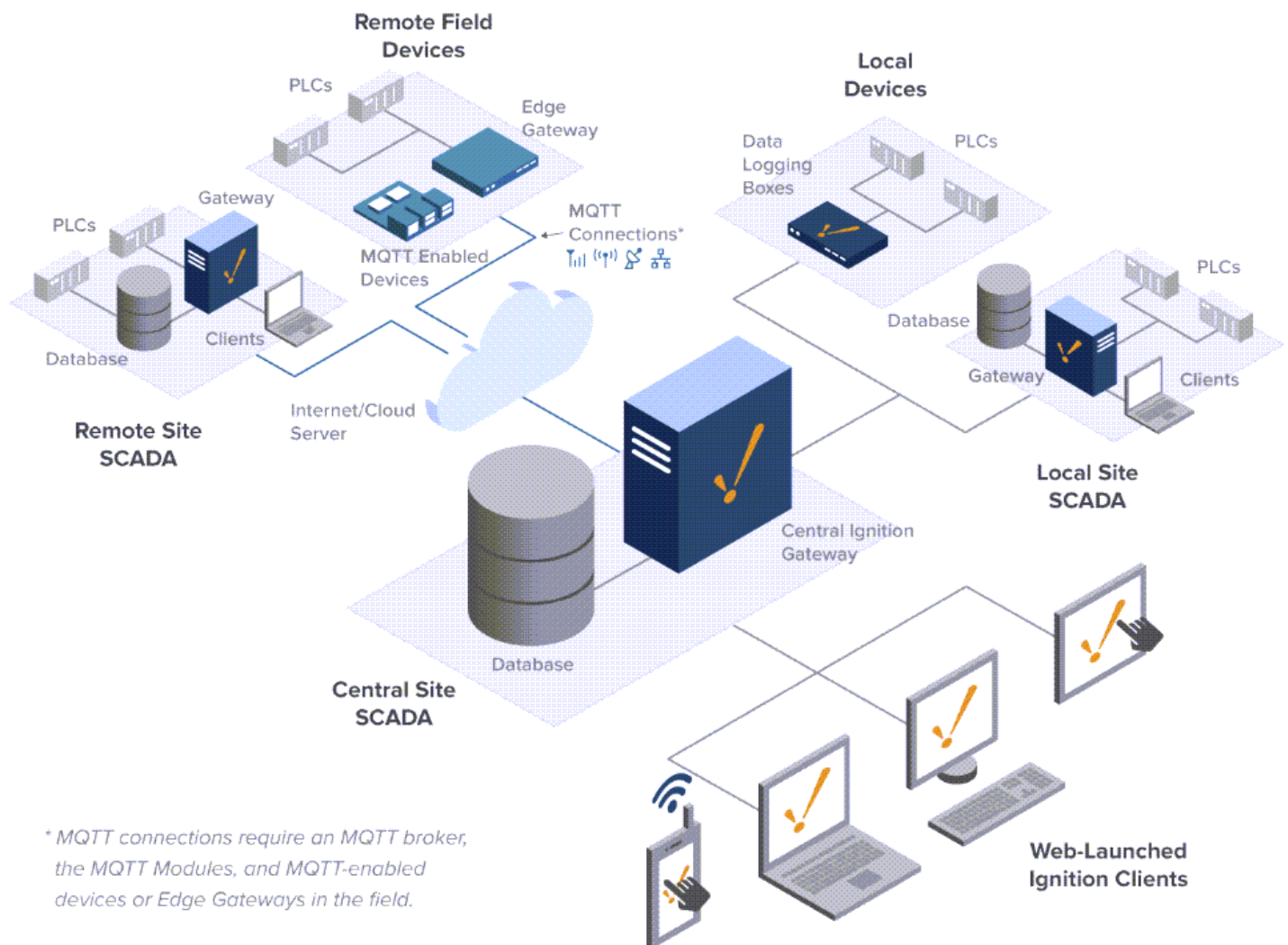
Improving performance in this architecture is simple: add another Gateway where appropriate. Because the system is spread out on purpose, it's easy to determine which kind of Gateway to add. A Back-End Gateway would help if you're adding new PLCs, and a Front-End Gateway will help when more clients need to be active at a time.



# Hub and Spoke Architecture

## Centrally Managed Systems

The Hub and Spoke Architecture involves multiple Ignition installations (the spokes) communicating and forwarding data points to a centralized Ignition installation (the Hub). The Hub and Spoke Architecture is unique in that you start with a single Ignition install at a central site. Ignition can then be installed at as many other remote or local sites as needed. These sites can then be customized or configured to suit that specific site's needs.



### **CAUTION**

Due to serialization updates, 8.3 Gateways will not be able to store data to a remote 8.1 Gateway. This includes remote history providers, remote audit logs, remote Alarm Journals, and data sent using Edge Sync Services. It is recommended to first upgrade the central server hosting data to 8.3 before upgrading any remote 8.1 Gateways. See the [8.3 Upgrade Guide](#) for more information.

# Reliable Remote Data Logging

Because connections between a database and remote PLCs can be unreliable, we can install either the **SQL Bridge** module or **Historian Core** module. The **Store and Forward** system then ensures that data is never lost. The system may still be accessed through the OPC-UA server built into Ignition, or database-based tags may be used to communicate current status.

The Hub and Spoke Architecture is ideal for centralizing historical data from multiple remote sites, and allows access to locally collected data via Ignition's **Gateway Network**.

## Local and Remote Logging

The Hub and Spoke Architecture can be modified to store data at each spoke, in addition to the hub by splitting the tag history. Redundant data is stored at each site, as well as the hub database to protect against hard drive failure.

## Local Client Fallback

Typically, the Hub and Spoke Architecture does not include the **Vision** module at the remote sites. You can add the Vision module at each spoke to take advantage of local client fallback. This way, each site can continue to operate at full efficiency in the event communication with the hub Gateway drops. Users at each spoke will never lost visibility of the system. **Vision Limited** licenses help lower costs on the spokes.

## Remote Site Alarming

By adding the **Alarming Notification** module to a remote site, you can notify users when a problem occurs at each spoke. It is best to handle alarms at each remote site rather than centrally, to avoid any problems in case the connection to the central location is lost.

# Edge Architectures

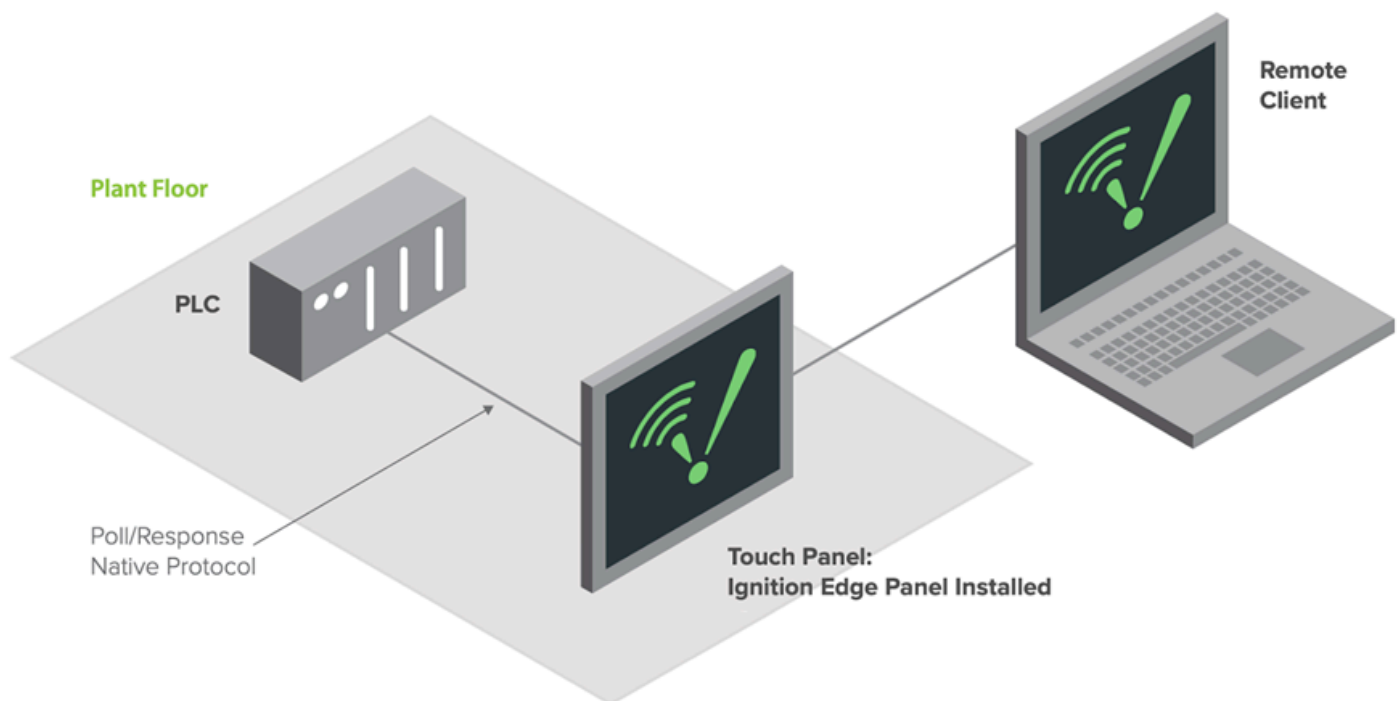
The Ignition Edge system is unique in that it can be very flexible and fill in the gaps in any system architecture. Ignition Edge is a smaller version of the standard Ignition install. Edge is deployed at the edge of a network to provide local visualization, data publishing, and centralized synchronization within a larger Ignition architecture.

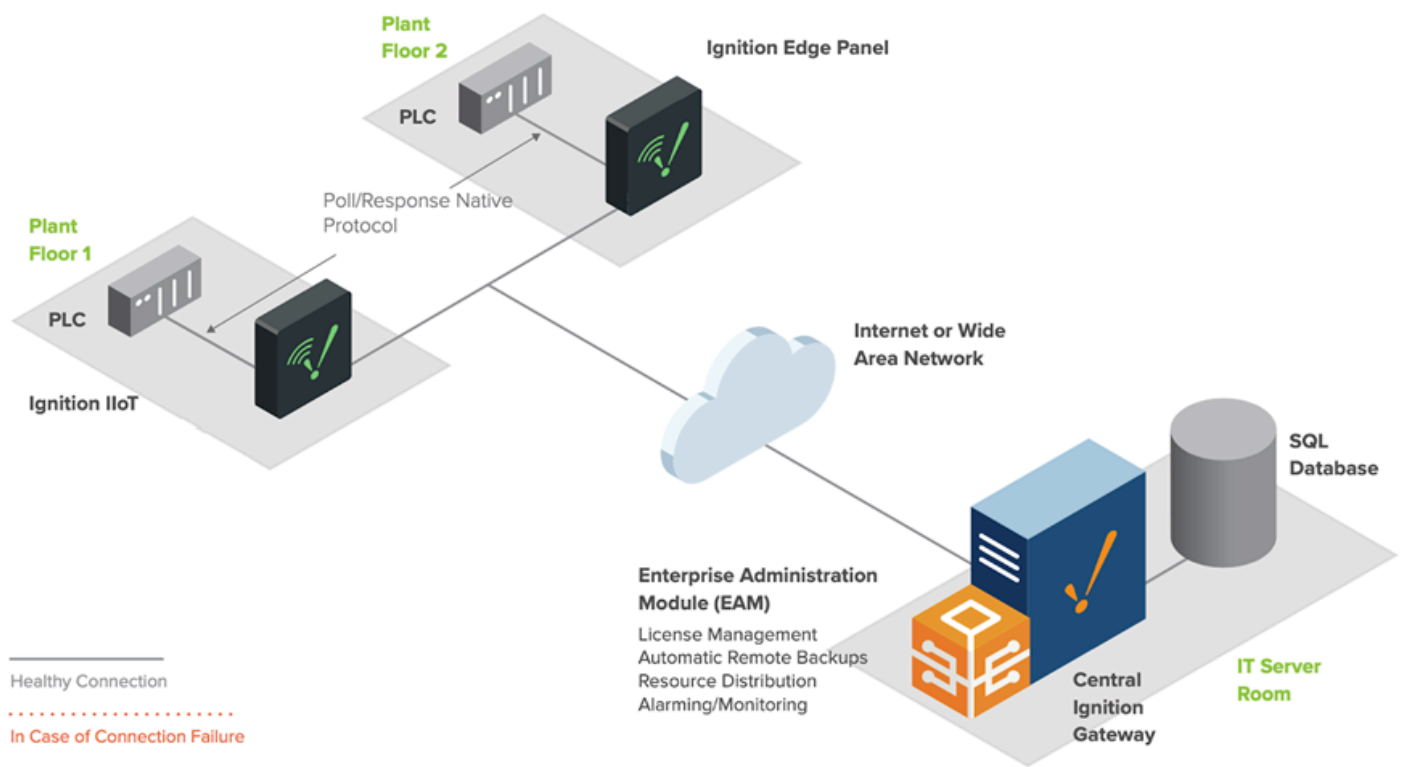
Up to 35 days or 10 million data points of tag history can be stored locally with an Edge installation. Additionally, Alarm Journal and audit log data is able to be stored locally for 7 days.

Each Edge product (Panel and IIoT) offers specific functionality that works best in certain scenarios. The diagrams show some architecture options using Edge. Additionally, these architecture diagrams show an Edge Gateway paired with an Ignition Gateway, which shows how an Edge system architecture can be added on to any of the other Ignition architectures.

## Panel

An Edge **Panel** Gateway can act as a stand-alone panel by simply connecting to a local PLC and building a basic screen. When paired with a central Ignition Gateway, the Edge can also act as a local Client fallback, providing control on site in the event of a lost network connection.

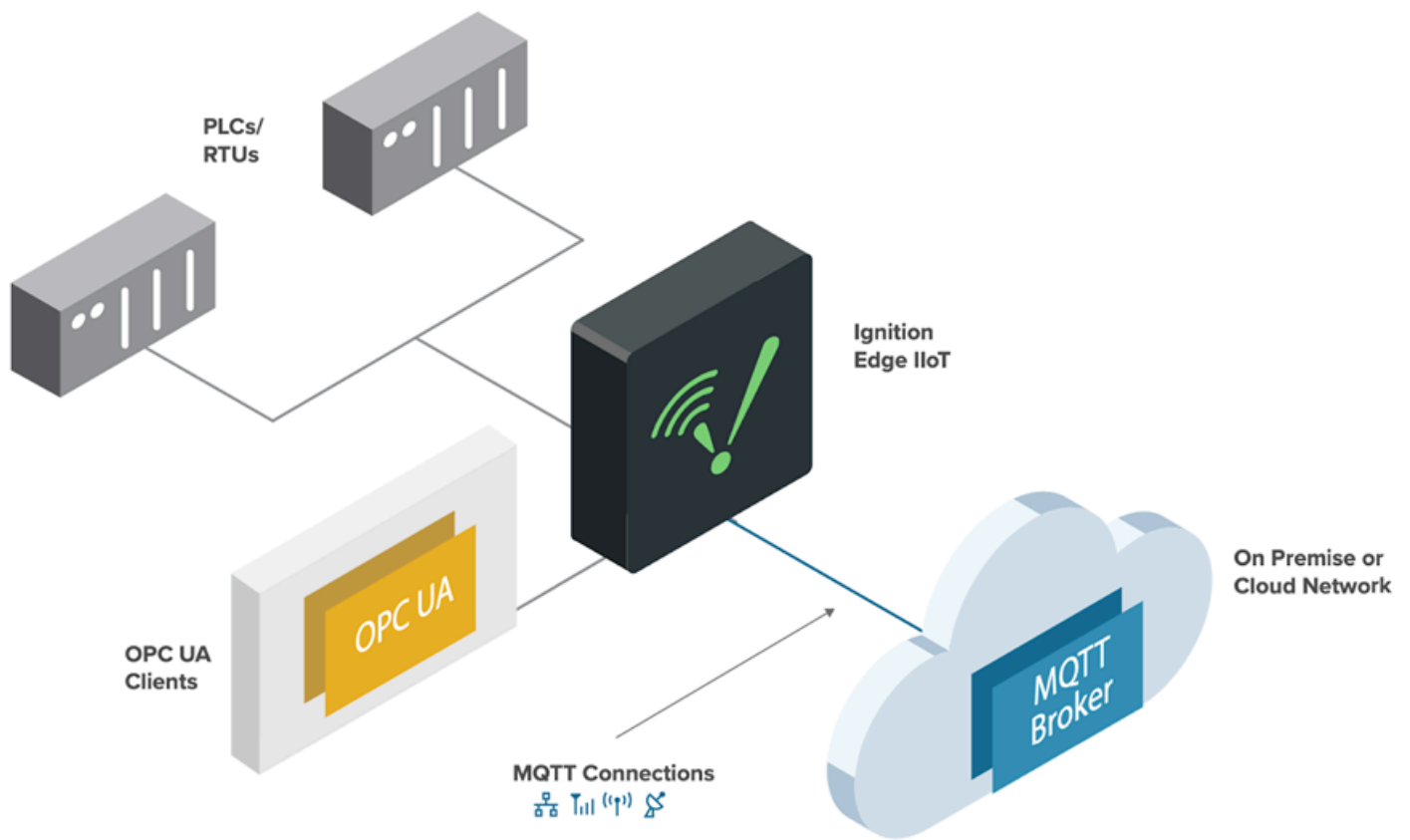




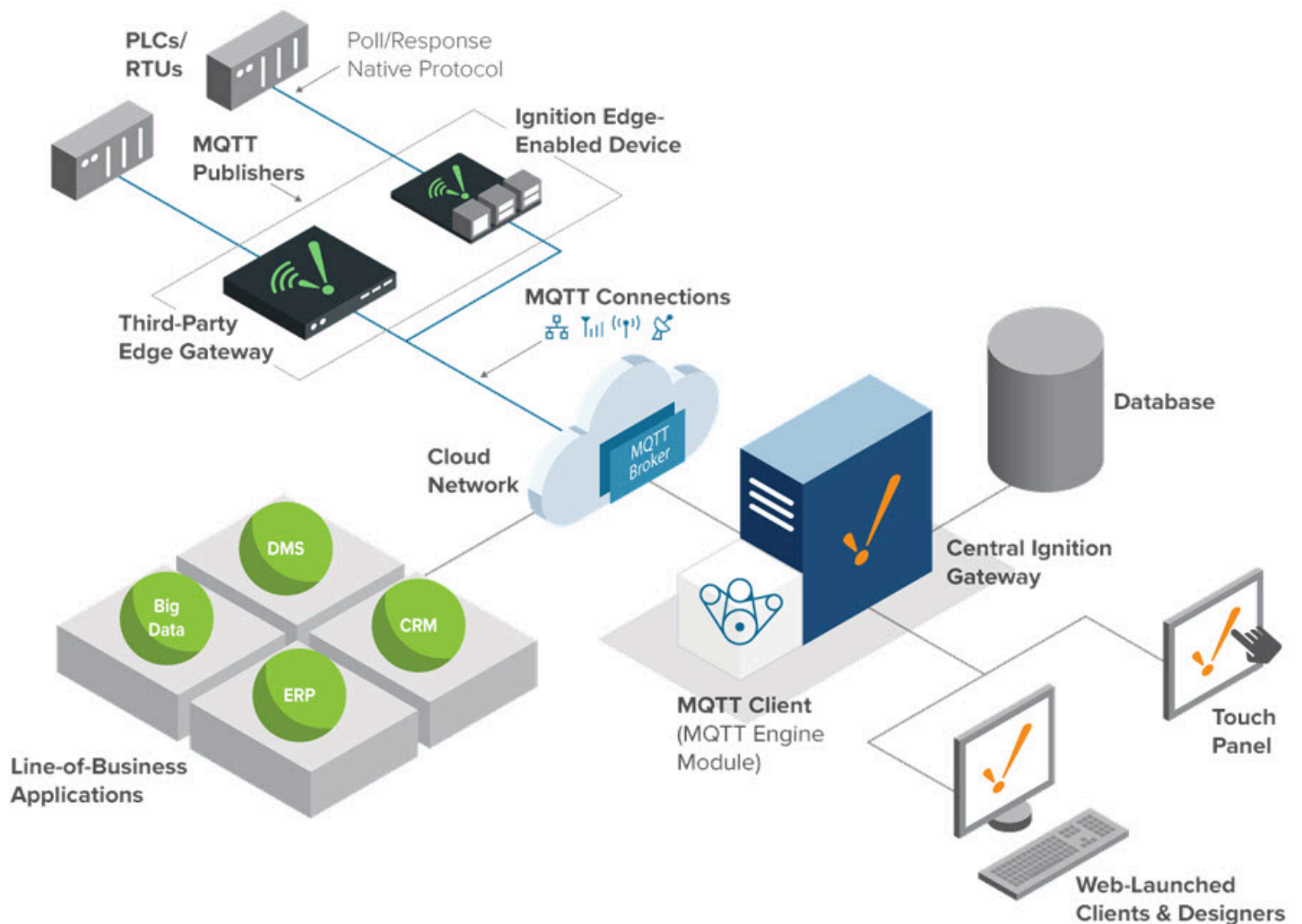
## Edge IIoT

An Edge **IIoT** (formerly MQTT) Gateway provides a simple way of setting up an MQTT Publisher next to a PLC, allowing it to connect to a greater IIoT architecture. Here, you can see multiple types of devices using Ignition Edge to connect in the network.

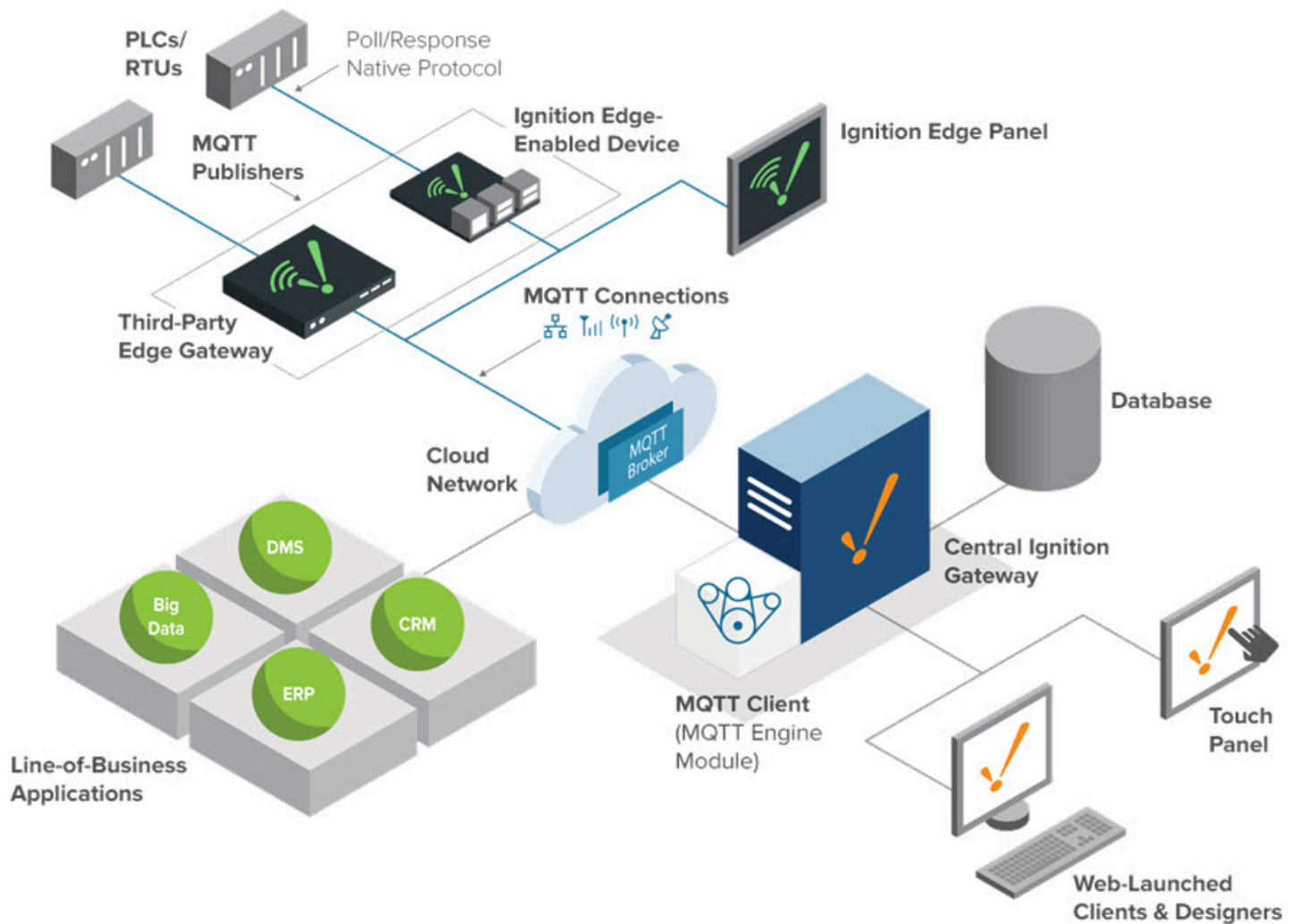
**Edge IIoT** as a standalone Edge Gateway to publish device data from the edge of the network to an MQTT broker:



**Edge IIoT** as an Edge Gateway to publish device data from the edge of the network to an MQTT broker:



**Edge IIoT** and **Edge Panel** together to add a local client at the edge of the network and to publish data to an MQTT broker:



## Synchronization and Central Management

### Data Synchronization

Both Ignition Edge IIoT and Ignition Edge Panel can synchronize data from the edge of the network to a central Ignition Gateway over the Gateway Network. This includes tag history, Alarm Journal entries, and audit log data.

Edge stores data locally (up to 35 days or 10 million records) and uses Store and Forward to buffer data during network interruptions. When the connection is restored, buffered data is automatically forwarded to the central Gateway for long-term storage and enterprise-wide visibility. This architecture allows Edge to operate independently at the network boundary while maintaining centralized reporting and long-term data retention.

# Enterprise Administration (EAM) Agent Mode

Both Ignition Edge IIoT and Ignition Edge Panel can function as remote EAM agent Gateways when connected to a central Ignition Gateway with the Enterprise Administration module installed.

In this architecture, the central Gateway acts as the EAM Controller and the Edge Gateway acts as an agent. This allows centralized management of Edge Gateways, including project updates, configuration synchronization, backup coordination, and licensing management.



# IIoT Architecture

## Overview

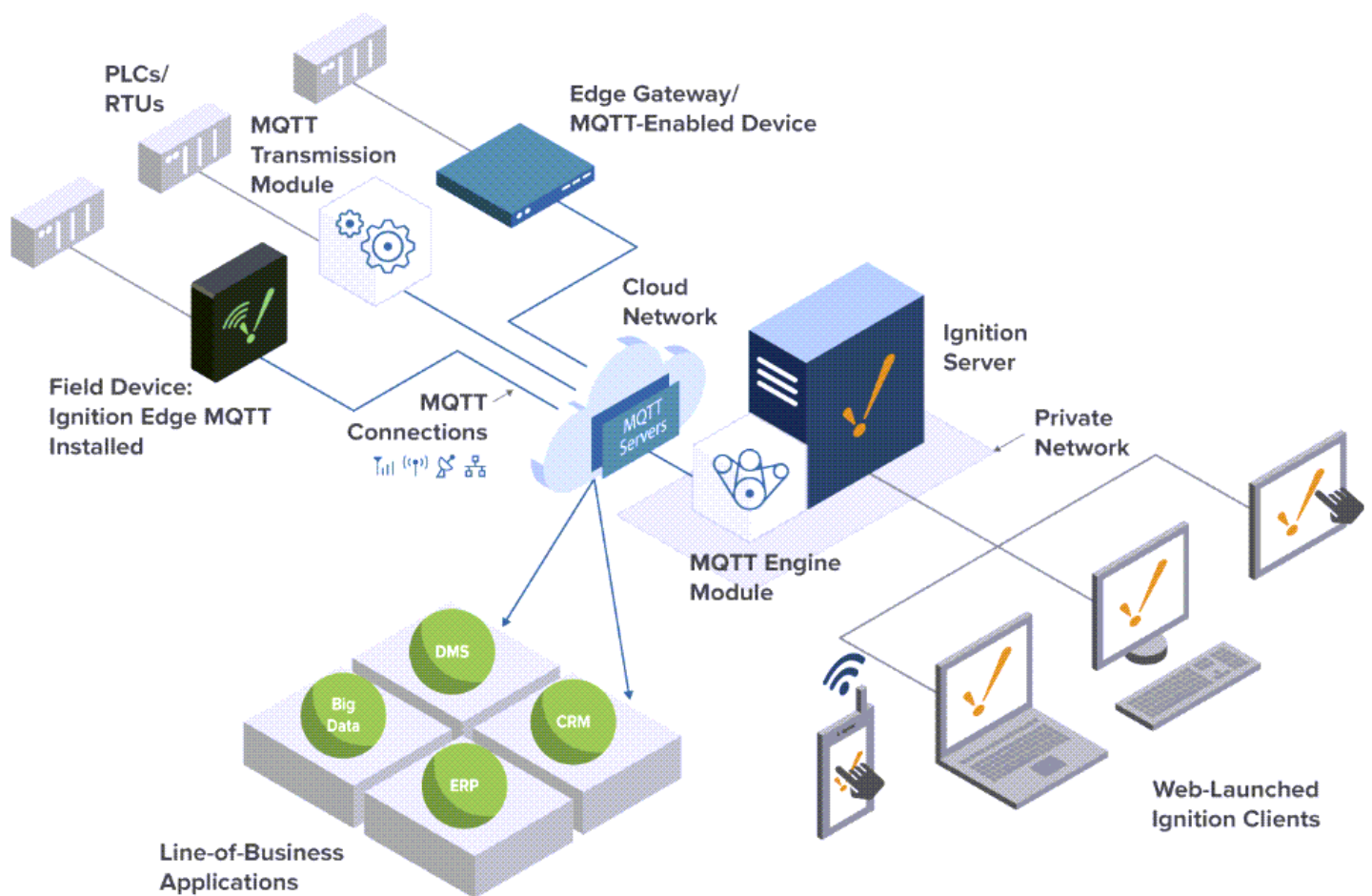
Ignition can collect data from any devices at the edge of the network, publish that data to a central broker, and push that data to subscribed industrial and line-of-business applications. Ignition IIoT can connect to PLCs in the field through the use of the MQTT Transmission module, field devices with Ignition Edge MQTT installed, and/or MQTT-enabled edge gateways and field devices that use the Cirrus Link Sparkplug MQTT specification. This data is published to an MQTT broker, this broker can be located on-premise, in the cloud, or a hybrid of the two. The MQTT Engine module located on an Ignition Gateway can subscribe to any data published from the broker. This data can be used in any Ignition application.

## IIoT Architecture Example

IIoT architecture typically involves the use of the MQTT protocol to communicate with a large number of devices. MQTT is a lightweight and secure protocol that makes use of a unique publish/subscribe transportation method. Additional information on the MQTT protocol and modules can be found in the [Cirrus Link documentation](#).

The [Basic Architecture](#) can easily be expanded with the MQTT modules to collect data from numerous Edge of Network devices. Data collected by the MQTT Engine can be historized and presented in a client with the Vision module, or via reports with the Reporting module.





## IIoT Architecture Objects

The following are key pieces in the IIoT Architecture.

### Field Device

A Field Device of some sort can be used to connect to a PLC. This device also needs to be able to publish Tag values to an MQTT server. Any of the following hardware can act as a Field Device:

- Ignition Edge with the MQTT product
- Ignition server with the MQTT Transmitter Module
- Third-party MQTT enabled device

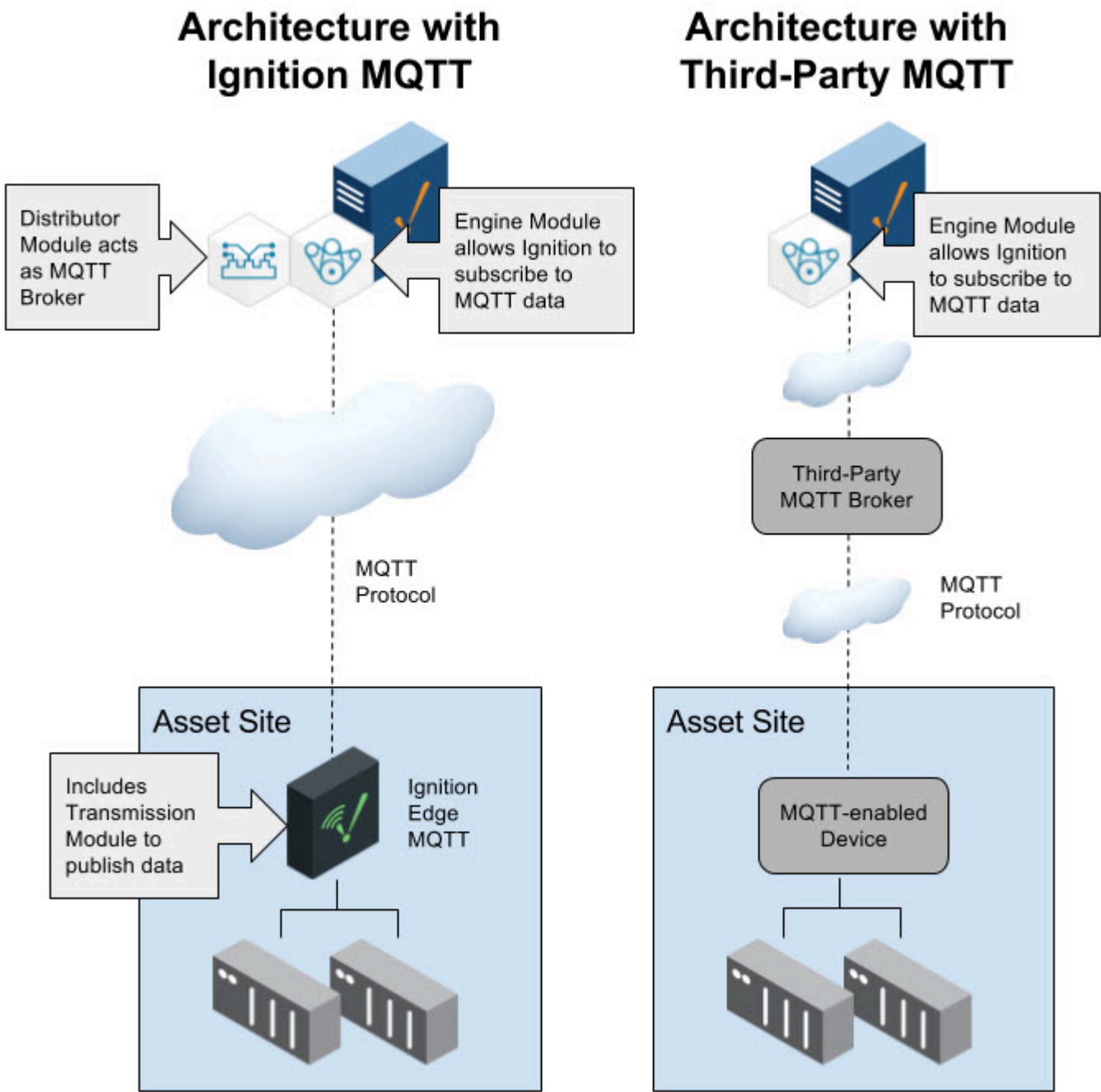
### MQTT Server (Broker)

An MQTT Broker is a server that can communicate with your Field Devices via MQTT. This can be an Ignition Gateway with the MQTT Distributor Module installed, or a third-party server, such as a [Chariot MQTT Server](#).

# Subscriber

A subscriber is some application that subscribes to topics in the Broker. In regards to Ignition, this is the Gateway with the the MQTT Engine Module installed.

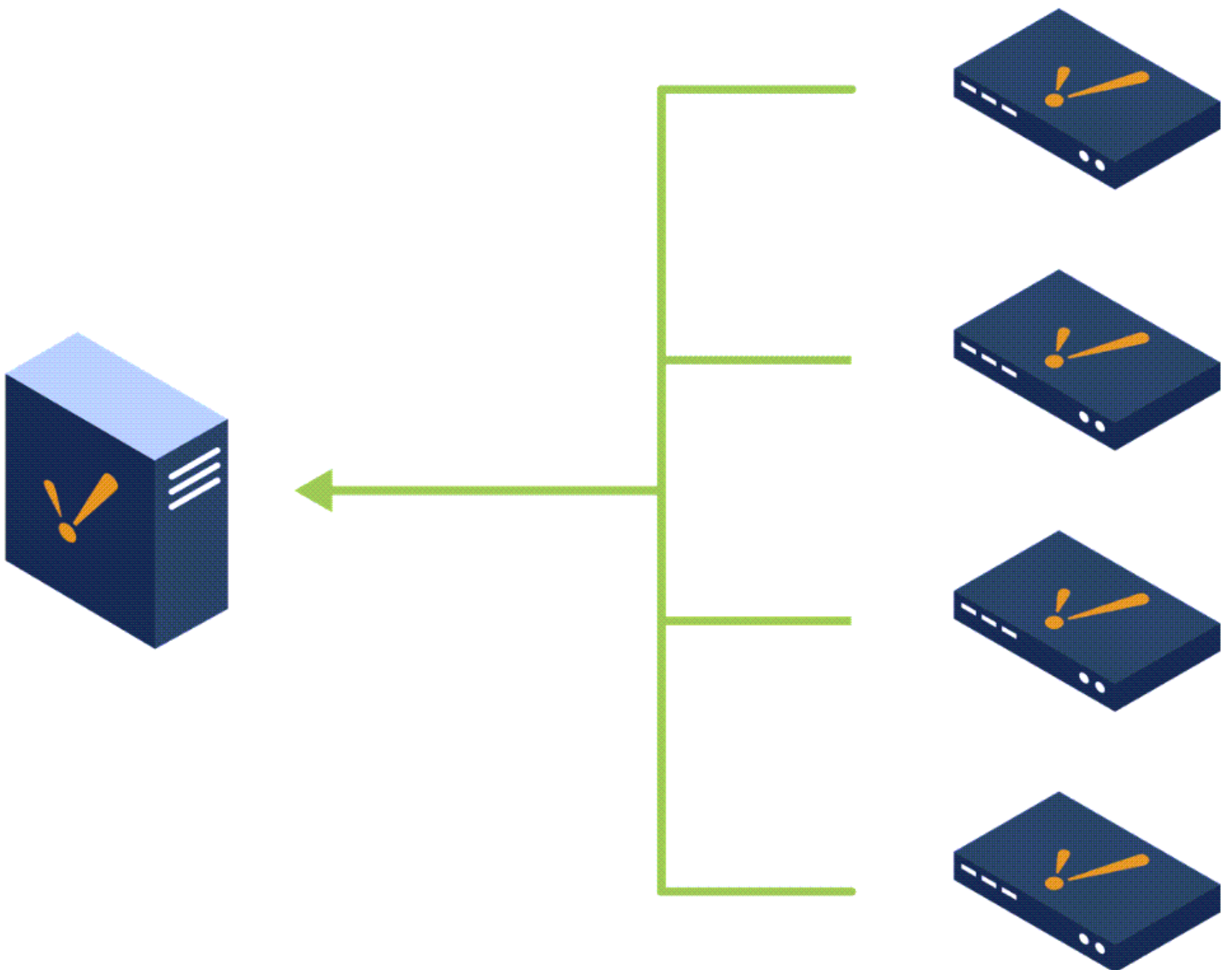
More details on the MQTT modules can be found in the [Cirrus Link documentation](#).



# Enterprise Architecture

Many types of architecture involve multiple Ignition servers. Eventually, some assistance overseeing each server can be helpful. Enterprise Architecture typically involves having a mechanism to monitor and manage multiple Ignition Gateways. This involves utilizing the [Enterprise Administration Module \(EAM\)](#).

EAM specifies one Gateway as the Controller, and the others as Agents. Connections between these Gateways take advantage of the [Gateway Network](#), which is a secure method multiple Gateways can use to share information.



# Why Use Enterprise Architecture

## System Management

Monitoring the health of several systems can be time consuming. EAM streamlines system management by having each Gateway report to a single Controller Gateway. This Controller can then generate alarms when problems occur, or assist in recovering from a hardware failure. Agent events can be stored in a SQL database, and easily incorporated into an Ignition Report. The best part is that the EAM can easily be incorporated into any architecture where multiple Gateways are present.

## Project Synchronization

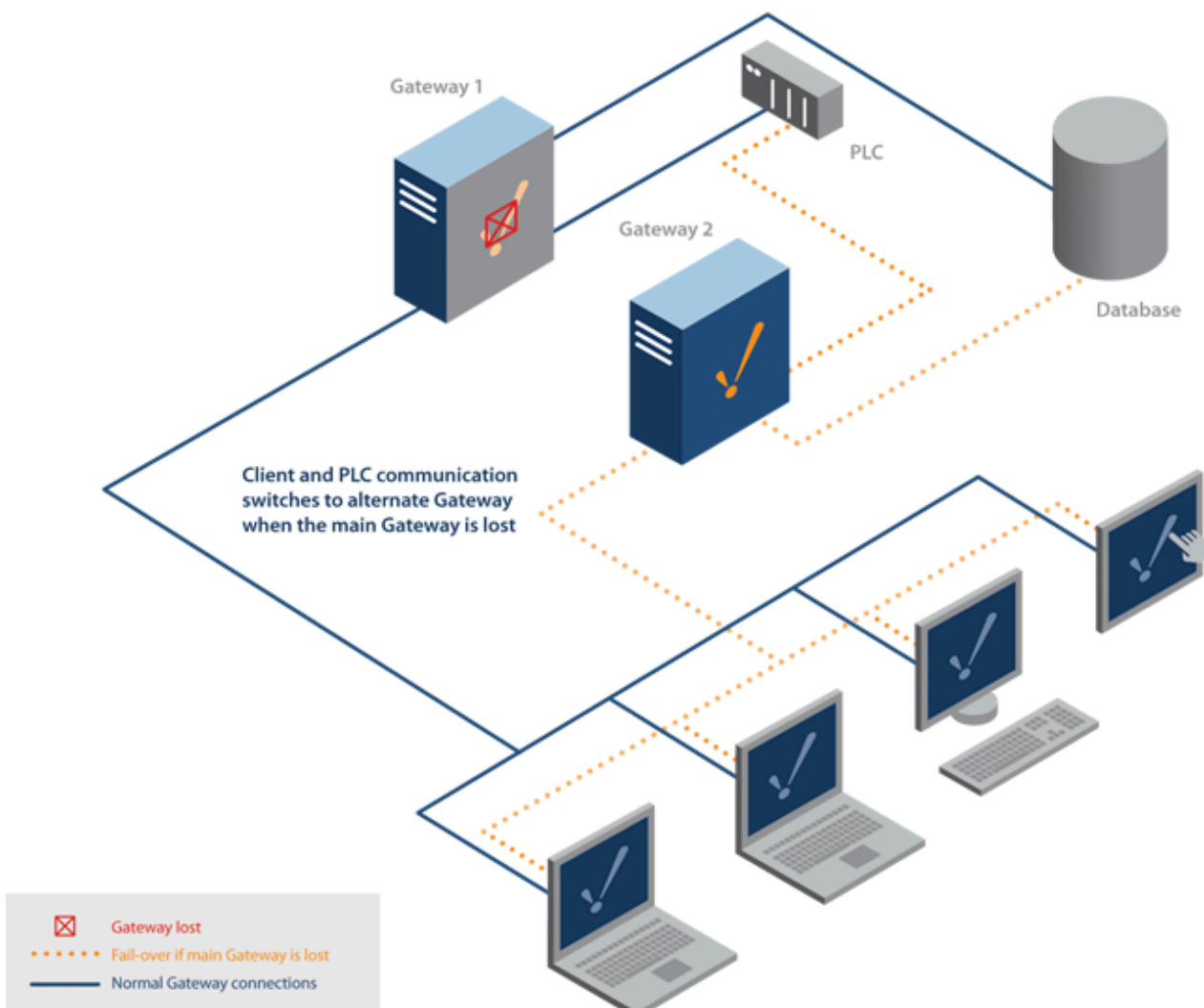
When multiple Gateways are used to launch clients, such as in the [Hub and Spoke Architecture](#), standardizing the look and feel of projects across both Gateways is important for a consistent organization. With EAM, the Controller can synchronize resources across multiple Agents, allowing development to occur on one Gateway, and updates pushed out to other Agent automatically.

# Redundancy Architecture

## Mission Critical - Gateway Redundancy

Using **Redundancy**, two Ignition installations can be linked together, so if one server fails, the other takes over and continues executing. All of the clients connected will be redirected to the backup machine, and historical data will continue to be logged. The transition is seamless, meaning processes will never be prevented from executing due to one server going down.

Any single installation in the System Architectures can be replaced with a redundant pair of Ignition Gateways. If you have a dedicated backup computer, Inductive Automation offers a cheaper Backup-specific license.



## Redundancy Architecture Examples

In this section, we will take a look at several other types of architectures that have been enhanced by redundancy.

# Standard Architecture

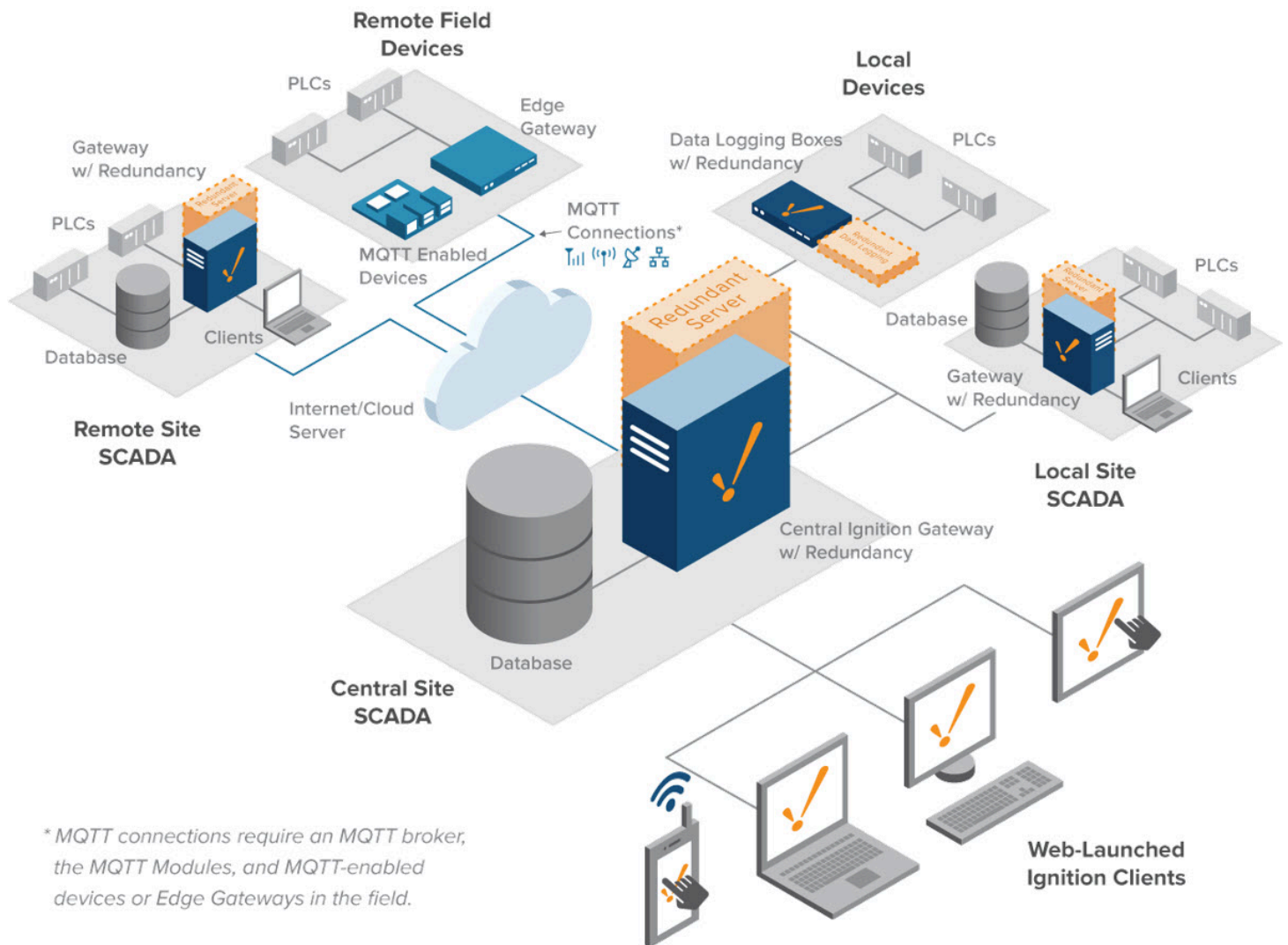
Reliability in the **Basic Architecture** can dramatically be improved by adding a redundant server. Should the primary server fail, the redundant server can seamlessly take over, allowing production to continue while the primary is brought back online.



## Hub and Spoke

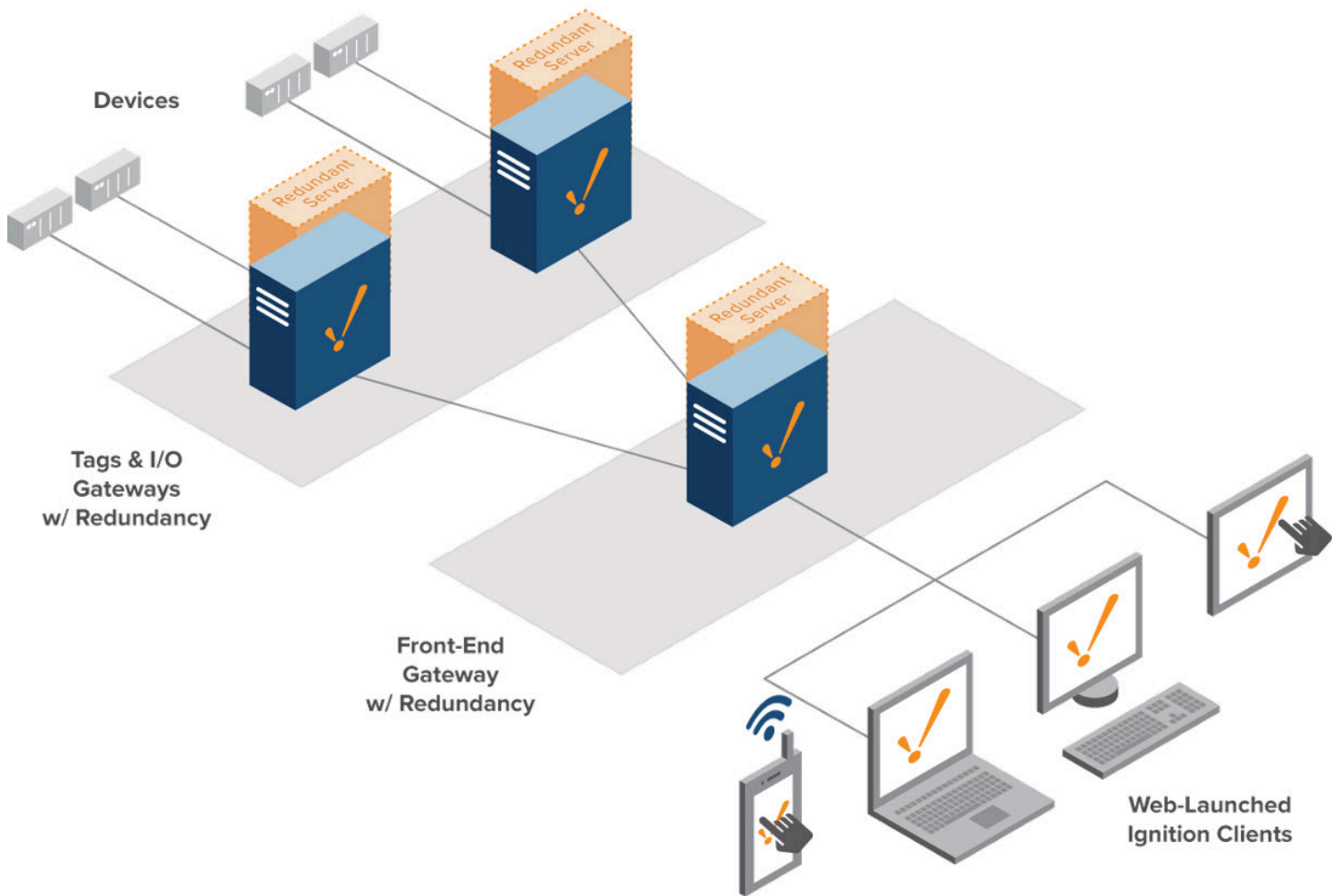
The **Spokes** that contain an Ignition Gateway can be thought of as individual instances of the Basic Architecture. Incorporating a backup server at each of these Spokes will ensure uptime is maintained locally. The **Hub** can also utilize a backup server, which is especially useful if clients are also launched from it.





## Scale Out Architecture

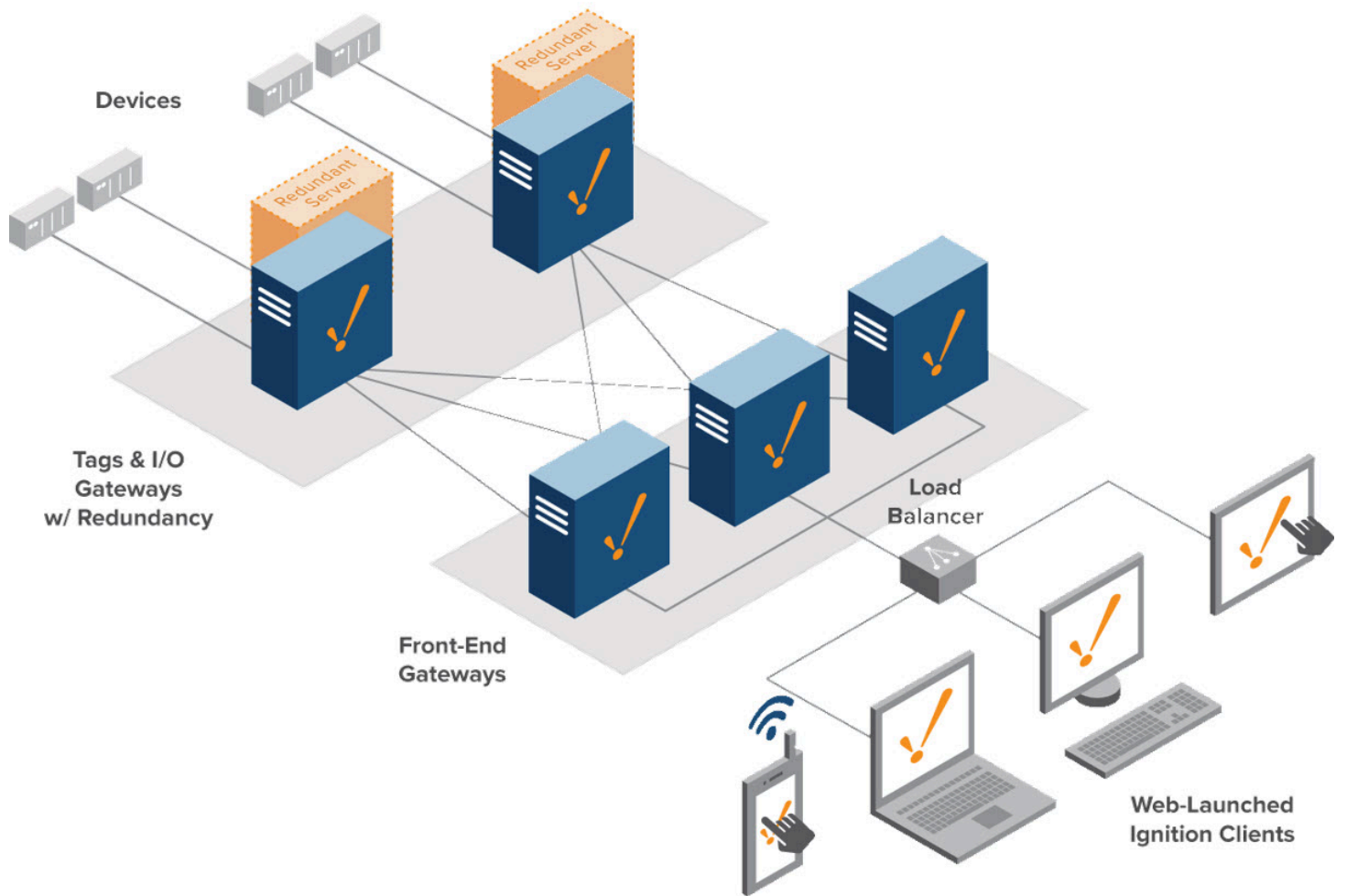
A server fault using the **Scale Out Architecture**, while not fatal to the whole system, can cripple the system. Without a Load Balancer, a Backup Gateway should be utilized at each Gateway. These means each Gateway has a failsafe ready to take over in the event of a failure.



## Scale Out Architecture with a Load Balancer

When utilizing a **Load Balancer**, redundancy should not be applied to the Front-End Gateways: the Load Balancer is responsible for distributing the workload amongst the front-end, so a backup Gateway is not required. However, an extra Front-End Gateway could be incorporated to act as a failover. If you plan on having three Front-End Gateways active at any time, then a fourth Gateway should be available in case one server faults.





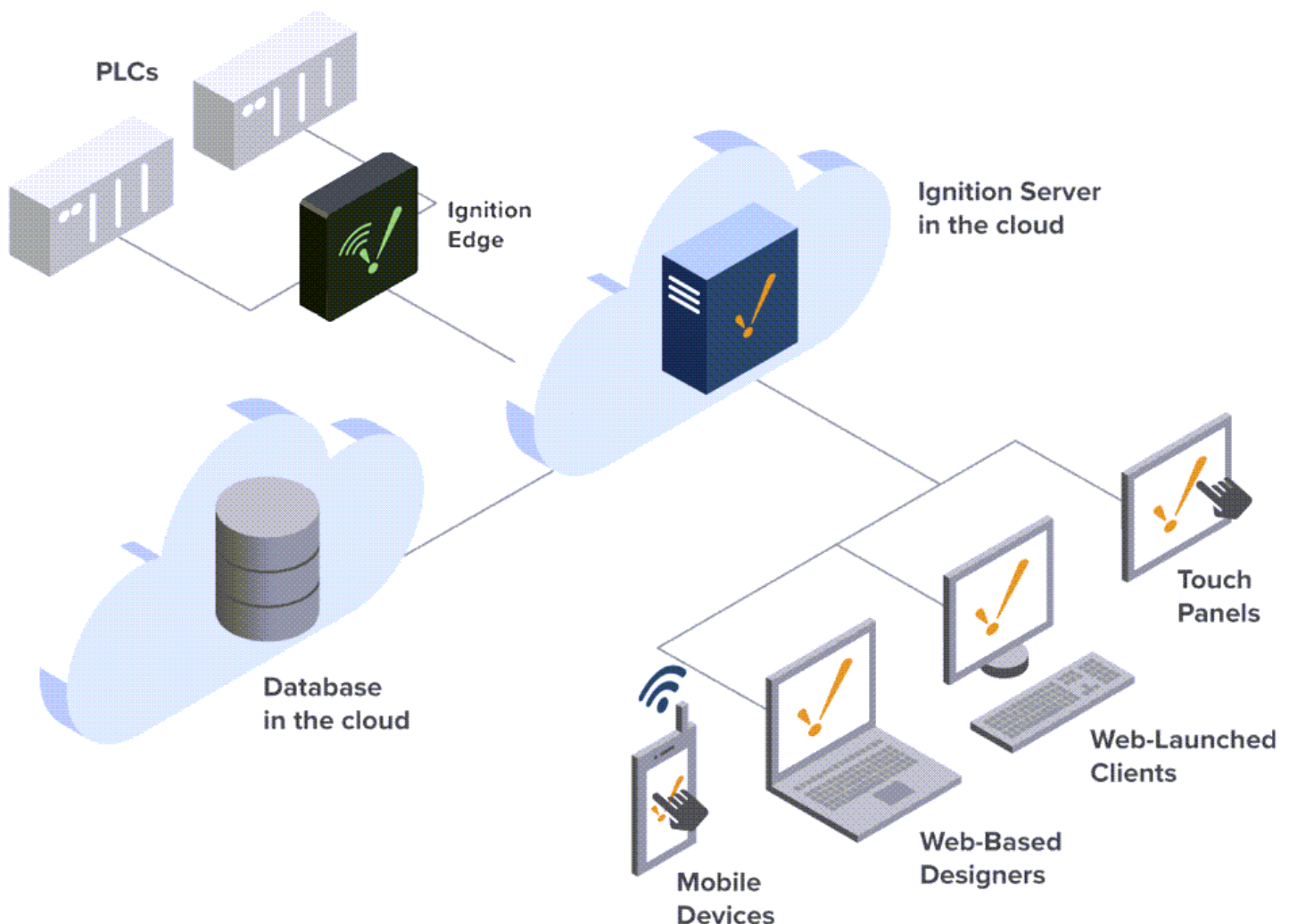
# Cloud Based Architecture

## Hosted Ignition Server

Ignition server can be hosted in the Cloud. Inductive Automation does not provide cloud services, but there are many great providers out there, such as Amazon EC2, or Windows Azure. The server can connect to the PLCs at the remote or customer sites via Round Robin Poll, Cell Tower, Satellite, or Secure VPN. The clients are connected to the Ignition server via Internet.

## Architecture Example

In this example, we see the **Basic Architecture**, but with the Ignition Server and Database both running on cloud servers. Note, that the Database and Ignition are on different cloud servers. This is because cloud service providers generally have specialized services that are designed explicitly for hosting SQL databases, as well as more general purpose services such as running Ignition. An installation of Ignition Edge is placed local to the PLCs, and is responsible for forwarding data to the cloud.



## Why Use a Cloud Based Architecture?

This type of architecture is ideal in smaller organizations since you don't have to worry about maintaining a server. Additionally, there is no on-site IT staff required to monitor the system.

## Does the Database Always Have to be in the Cloud?

If Ignition is hosted in the cloud, then it is very common to have your database also hosted in the cloud. However, many of our customers find that also having a controls database on-site to store temporary or in-progress data useful. This is great when you want to have data stored locally.

## Are Cloud Based Servers Secure?

Cloud based servers are increasingly common, but it is important to educate your organization on the risks associated with them. If your organization is interested in a cloud based solution, we recommend following the guidelines in the [Ignition Security Hardening Guide](#), as it addresses many potential security issues for both cloud and non-cloud based servers. Additionally, it offers recommendations on how to better protect your system.

## Should I have a Redundant Ignition Server in the Cloud?

If you are using redundancy or are concerned about uptime, you should be using Ignition redundancy regardless of whether your Ignition is in the cloud. While most cloud providers offer built-in redundancy, this is often much slower than Ignition's redundancy failover time. Typically Cloud Server redundancy has a new computer instance spun up (started) in the event the original fails. This will often take a couple minutes where Ignition's redundancy (with default settings) takes around 20 seconds to switch over. There are other options to make a Cloud Server start faster, but currently they all slow down the CPU substantially to make it possible.

## What if I Require an On-Site Server with Redundancy?

If you are using Ignition's Redundancy with a Cloud Server, then typically we recommend that both of the servers are run side-by-side. This means either both in the cloud or both on site. One warning: If you have both instances of Ignition in the cloud but if your connection to the internet goes down, then you lose access to both instances of Ignition.

## Cloud Service Suggestions

Many customers find the following cloud-based service suggestions helpful:

## Amazon Web Services

- Ignition Hosting: [AWS EC2 Instance types](#). The M3 and M4 instance types meet most customers needs in regards to hosting Ignition.
- Database Hosting: [AWS Relational Database Service](#).

## Microsoft Azure

- Ignition Hosting: [Azure for Discrete Manufacturing](#)
- Database Hosting: [Azure SQL Database](#)

# AWS Outposts Architecture

Amazon Web Services (AWS) Outposts is a fully managed service that offers the same AWS infrastructure, AWS services, APIs, and tools to virtually any datacenter, co-location space, or on-premises facility for a truly consistent hybrid experience. AWS Outposts is ideal for workloads that require low latency access to on-premises systems, local data processing, data residency, and migration of applications with local system interdependencies.

AWS compute, storage, database, and other services run locally on Outposts, and you can access the full range of AWS services available in the region to build, manage, and scale your on-premises applications using familiar AWS services and tools.

Inductive Automation is an AWS partner and Ignition can easily be deployed to AWS Outposts.

## Use Cases

Easily transition any architecture from an existing infrastructure to AWS Outposts.

## On-Premise Ignition or Ignition Edge with AWS Services and Tools

Customers often require ultra-low latency and high bandwidth between their local devices and the SCADA systems. Using the Inductive solution on Outposts, customers will have the benefit of a fully-managed infrastructure with native AWS APIs. Without Outposts, Inductive Automation's customers will need to procure, manage, support, secure, and maintain the hardware and software stack that the SCADA solution will run on.

## AWS Connected Factory Solution (Formerly IMC Kit)

The Industrial IoT Segment has used Ignition by incorporating it directly into Connected Factory Solution / IMC Kit (<https://aws.amazon.com/blogs/iot/connected-factory-offering-based-on-aws-iiot-for-industry-4-0-success/>). Customers can use AWS Outpost as mechanism to host the Edge component of IMC Kit workload.

## Available AWS Services on Outposts

You can take advantage of the majority of AWS Services on AWS Outposts.

- **VPC** - Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network Gateways. You can use both IPv4 and IPv6 in your VPC for secure and easy access to resources and applications.
- **EC2** - Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers. Amazon EC2's simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment.
- **EBS** - Amazon Elastic Block Store (EBS) is an easy to use, high performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction intensive workloads at any scale. A broad range of workloads are widely deployed on Amazon EBS, such as relational and non-relational databases, enterprise applications, containerized applications, big data analytics engines, file systems, and media workflows.
- **RDS** - Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups. It frees you to focus on your applications so you can give them the fast performance, high availability, security and compatibility they need. Limited to MySQL and PostgreSQL on AWS Outposts.

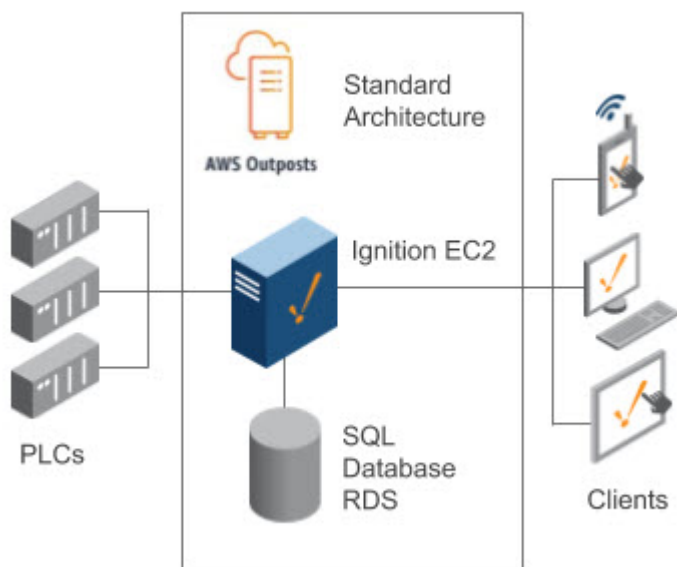
The most common use case is to deploy Ignition to an EC2 instance backed by an EBS volume and store historical data in a RDS database.

## Architectures

There are many architecture options available on AWS Outposts.

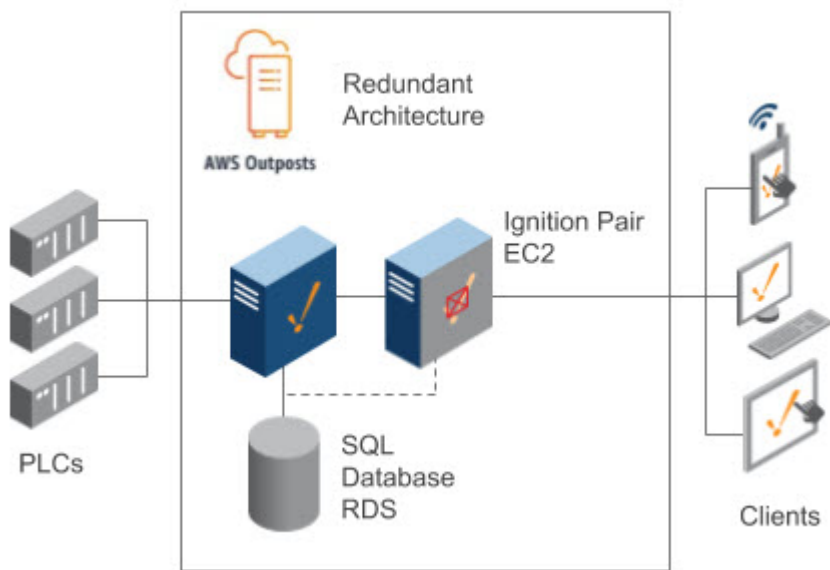
### Standard Architecture

Ignition's most common architecture consists of a single on-premise Ignition server connected to a SQL database (RDS), PLCs, and clients.



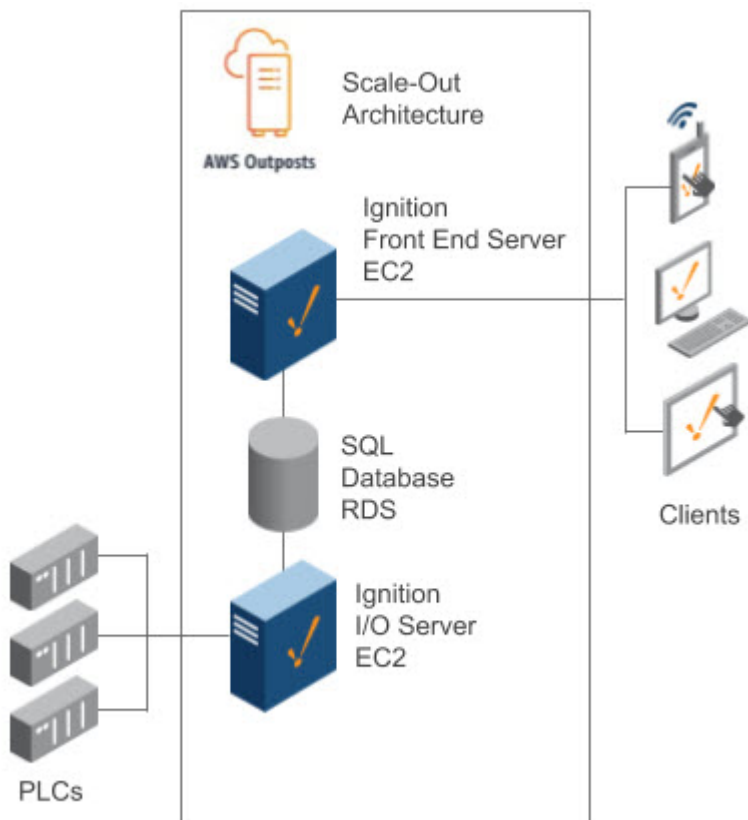
# Standard with Redundancy Architecture

Another common Ignition architecture consists of a single on-premise Ignition server (with a redundant server) connected to a SQL database (RDS), PLCs, and clients.



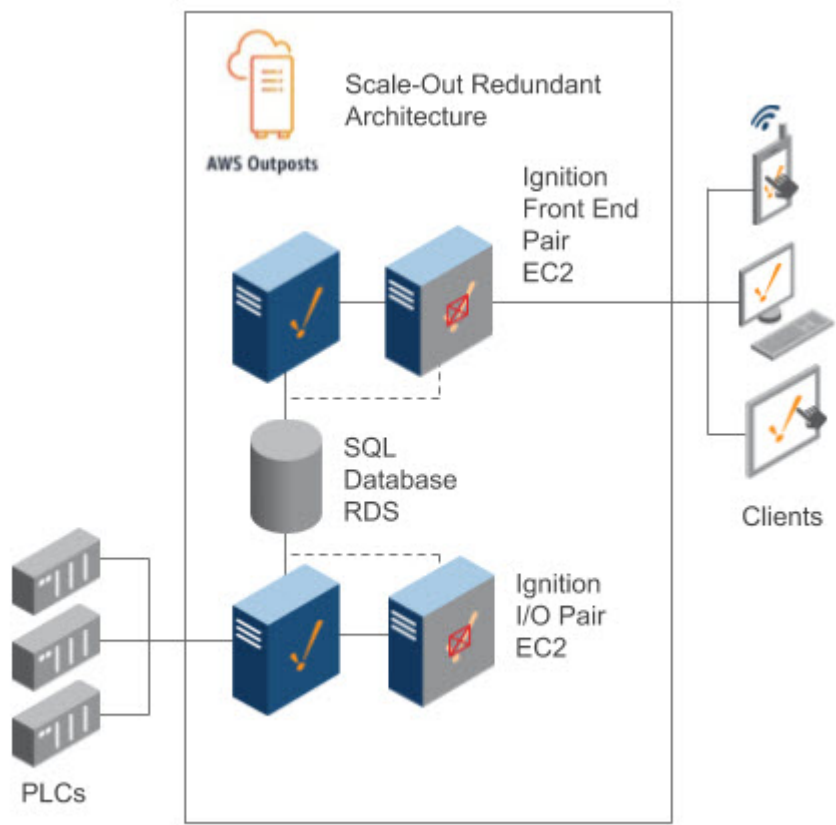
# Scale-Out Architecture

The scale-out architecture links together several Ignition Gateways to form a decentralized system. You can easily separate out Ignition's I/O from the front end and scale each independently.



## Scale-Out with Redundancy Architecture

The scale-out architecture with redundancy links together several Ignition Gateways (with redundant servers) to form a decentralized system. You can easily separate out Ignition's I/O from the front end and scale each independently.

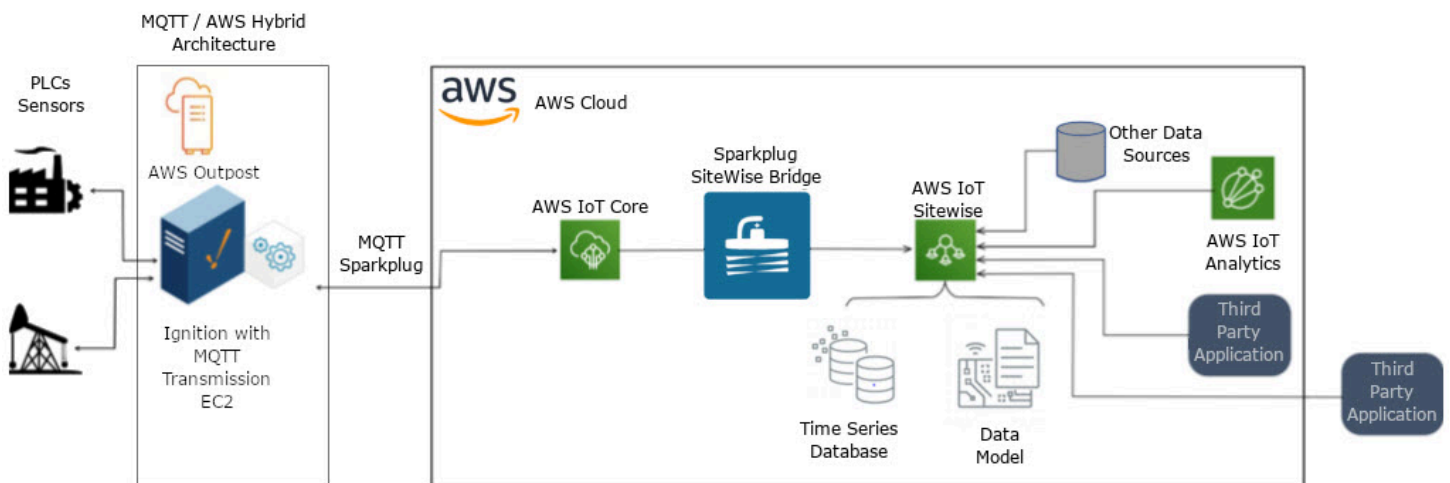




# AWS Connected Factory Architecture (MQTT and AWS SiteWise)

You CAN easily combine on-premise solutions running on AWS Outposts with AWS Cloud services. With the use of Inductive Automation's Ignition platform, and Cirrus Link MQTT modules and Sparkplug SiteWise Bridge, OT data from Industrial applications is delivered to AWS IoT SiteWise with minimal configuration and zero coding. Simply point the Cirrus Link module at the AWS IoT service. The asset model, properties, and hierarchy are 100% self-discovered by SiteWise. Then real-time data is securely and efficiently delivered directly to the SiteWise time series database for Big Data Analytics, ML and AI. This solution provides the simplest data ingest for AWS SiteWise delivering the Digital Transformation organizations are striving to achieve.

- Automatically Discovery of Assets
- Automatically Creates Asset model
- Automatically Defines Asset properties
- Automatically Defines Asset hierarchy
- Efficiently pushes Tag Data into SiteWise Time Series Database
- Requires No Coding, just a little Configuration



Learn more about [AWS SiteWise and Sparkplug SiteWise Bridge](#).

## Redundancy on AWS Outposts

It is possible to deploy Ignition in a redundant configuration on AWS Outposts. Using Redundancy, two Ignition installations can be linked together, so if one server fails, the other takes over and continues executing. All of the clients connected will be redirected to the backup machine, and historical data will continue to be logged. The transition is seamless, meaning processes will never be prevented from executing due to one server going down. Any single installation in the System Architectures can be replaced with a redundant pair of Ignition Gateways.

# High Availability on AWS Outposts

Ignition only supports high availability with the front end (Vision or Perspective) running behind a load balancer in a scale-out architecture. You can easily deploy one or more front end servers behind a standard load balancer such as nginx or HAProxy. You cannot use AWS Load Balancer since it doesn't support "sticky sessions" on AWS Outposts currently. The load balancer must support "sticky sessions" in order for the client to function properly. It is recommended to set the "sticky" duration to 1 hour.

## How to Deploy Ignition to AWS Outposts

Deploying Ignition to AWS Outposts is extremely easy.

1. Create a new VPC with private subnets and public subnets.
2. Set up a NAT Gateway if your EC2 instances need Internet access.
3. Spin up an EC2 instance on AWS Outposts. You can use a Windows or Linux OS. It is recommended to use Microsoft Windows Server 2019 Base or Ubuntu Server 20.04 LTS, as they are tested by Inductive Automation's Quality Assurance team. The recommended minimum specs of an EC2 instance is:
  - 4 vCPUs
  - 8 GiB Memory
4. Download and install Ignition on the EC2 instances.
5. Make sure to set up proper security groups to only allow ports 22 (SSH), 8088 (Ignition HTTP), 8043 (Ignition HTTPS), and 3306 or 5432 (database).
6. Spin up a MySQL or PostgreSQL database in RDS. You can also install a database in an EC2 instance and manage yourself. It is recommended to use RDS.
7. Connect Ignition to SQL database.
8. Build your project and have fun!

## Common EC2 Instance Types

You can deploy Ignition to virtually any EC2 instance type. Recommended to use EBS backed volumes. Most customers deploy Ignition to the following:

- m5.xlarge
- m5.2xlarge
- c5.xlarge
- c5.2xlarge

- r5.xlarge
- r5.2xlarge

## How Do I Get Support?

Inductive Automation is dedicated to providing our customers with high quality product support. There are 2 types of support options available: solution support and technical support. Inductive Automation has a partnership with AWS. The Sales Engineering team is certified as AWS Solution Architect Associate. The team can help figuring out the right architecture and configuring AWS services. Simply schedule a call with the team through your account representative.



Visit our [Support, Feedback, and Resources](#) page for complete information on technical support.

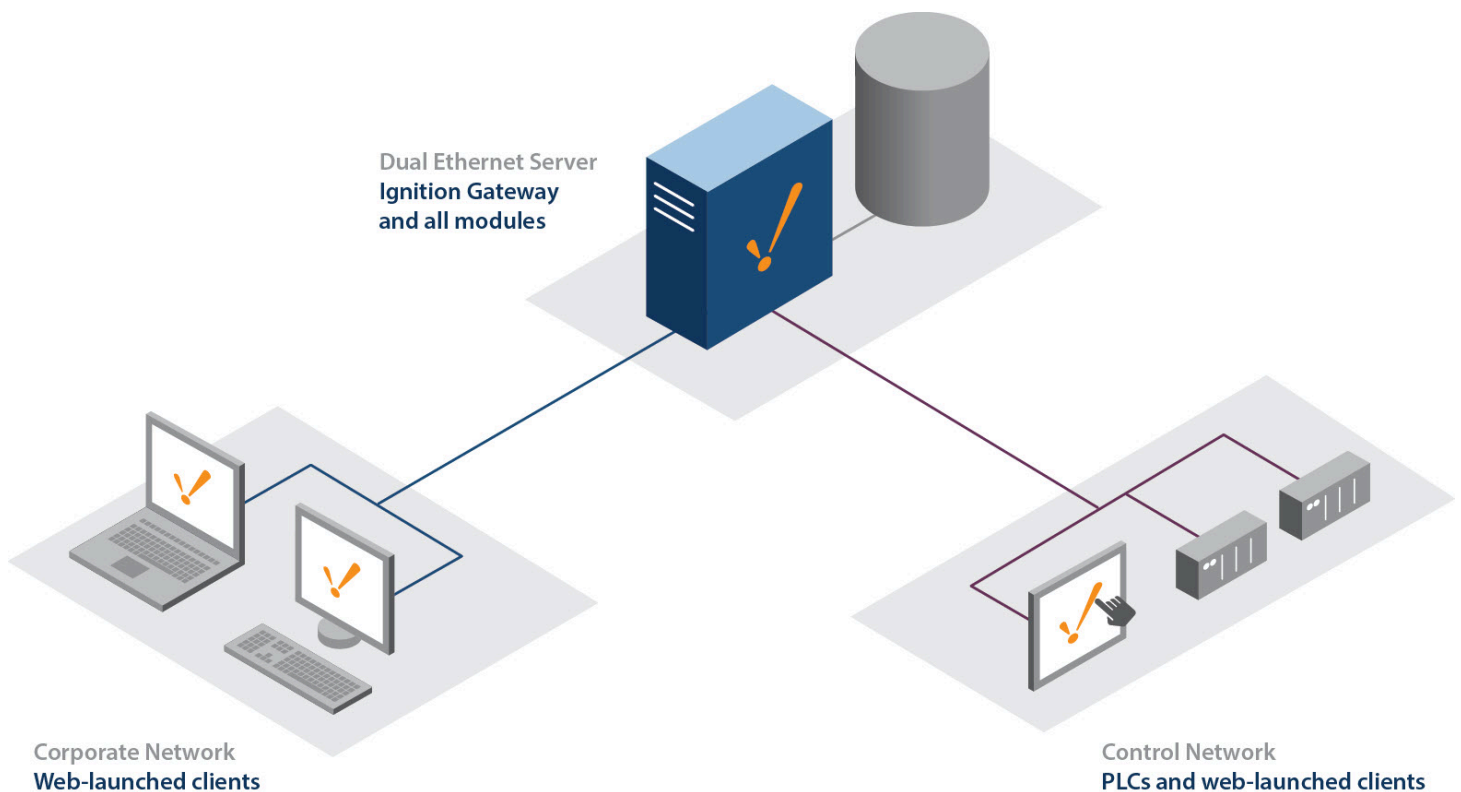
# Security Architecture

## Network Segmentation

Network segmentation is a powerful technique for securing an Ignition Architecture. Inductive Automation recommends adhering to proven strategies and standards such as ISA 62443 “zones and conduits”, “Zero Trust”, NIST or ISO standards, or other industry accepted approaches.

Consumers of each class of traffic should communicate with Ignition Gateways, but not with other types of consumers. For example, Ignition communicates with PLCs, Ignition communicates with databases, users communicate with Ignition, and Ignition gateways communicate with each other. The principle of least privilege suggests that users, PLCs, and databases should not be able to communicate with each other directly.

Network segmentation can be applied externally to Ignition using standard IT and OT technology such as routers, switches, firewalls, and load balancers. Ignition Gateways can communicate securely with each other using HTTPS with 2-way trust based on certificates over port 8060 (definable) via the **Gateway Network**. Secure communication is also possible using MQTT.



## One Server, Multiple Networks

The Ignition Gateway supports dual-NIC servers, and can act as a bridge between multiple networks, or communicate with multiple sites over a corporate WAN. Since clients talk to databases and PLCs

through the Gateway, clients can be launched from both a corporate network and an isolated control network, and provide full access to both. Built-in **security settings** can restrict project access to users on different networks, either by restricting certain things in a project, or denying access to a whole project based on user role and network location.

## Best Practices

Start with the **Ignition Security Hardening Guide** and the **Server Sizing and Architecture Guide** for an overview on how to implement Security Architecture.

## Security Engineering

Security Engineering is required for non-standard applications and Enterprise Integration. The **ISA 62443** series of standards is a great starting point to determine the level of security required to meet your risk needs. The **NIST Cybersecurity Framework (CSF)** is another option.

Be especially careful with high access or risk environments, such as Internet accessible Gateways, or Operational Technology (OT) environments with high safety requirements.

## Separate Architectures

Using a single Ignition system to perform distinct functions increases risk. Consider separating Ignition architectures and security providers (e.g. Identity Providers, databases, etc) when:

- Dealing with multiple different application types (“use cases”)
- Dealing with different types of sensitive data (e.g. Personally Identifiable Information, banking, versus organizational trade secrets)

## Stateless Services

Frontend Ignition Gateways host “stateless” services with visualization modules such as Perspective, Vision, and Reporting. Using application load balancers can protect Ignition, create redundancy, and scale performance. Any number of identically configured Gateways may be used to **scale out**. Configure the load balancer to favor persistent connections (“sticky sessions”).

Remote providers allow access to data. Consider “read only” Gateway Network connections if needed.

# Stateful Services

Ignition I/O Gateways are used for machine-to-machine communication and are usually segmented from Internet connections and user remote access. These Gateways host tag systems, PLC connections, database connections, historians, etc, which are considered to be “stateful”. Ignition I/O Gateways are best protected with **Ignition redundancy** or redundant systems implemented below Ignition. End users should not need to communicate directly with I/O Gateways.

Ignition I/O Gateways should be scaled out by adding additional Gateways. I/O gateways should host distinct content from each other. For example, “Gateway A” might connect to PLC 1 and PLC2, while “Gateway B” connects to PLC3. Both support Ignition redundancy.

Scaling is often separated by geographic location or process function. Consider using **Ignition Edge** Gateways close to the data source. Utilizing **Store and Forward** from Edge Gateways to a central Gateway or database mitigates the effects of a network outage.

# New in this Version

Over the course of development, naturally there are changes and additions to the Ignition software. This page highlights any new functionality or modified behavior, but is not meant as a complete resource for new features. You can find more about these items by following the links on this page.



INDUCTIVE  
UNIVERSITY

## What's New in 8.3

[Watch the video](#)

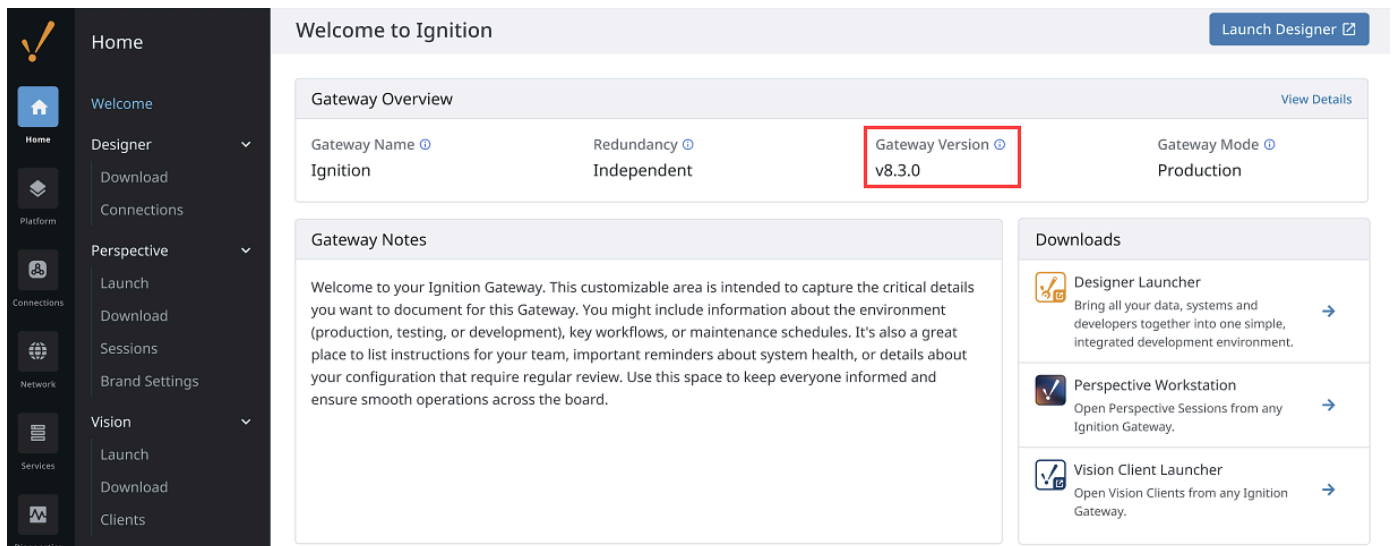
## Determining Your Current Version

The current version of Ignition can be viewed by visiting the Welcome page of the Gateway.

1. Navigate to your Gateway and select the Home tab to view the Welcome page.
2. Locate the Gateway Version under the Gateway Overview section on the Welcome page.

### NOTE

You must be logged in with [Read or Write Permissions](#) to see this section. If you aren't prompted to log in, you can select the **Log In** option in the upper right-hand corner of the screen.



The screenshot shows the Ignition Gateway Welcome page. On the left is a dark sidebar with navigation options: Home, Welcome, Designer, Download, Connections, Perspective, Launch, Download, Sessions, Brand Settings, Vision, Launch, Download, Clients, and Diagnostics. The main content area is titled 'Welcome to Ignition' and includes a 'Launch Designer' button in the top right. Below the title is a 'Gateway Overview' section with a table containing the following data:

| Gateway Name | Redundancy  | Gateway Version | Gateway Mode |
|--------------|-------------|-----------------|--------------|
| Ignition     | Independent | v8.3.0          | Production   |

The 'Gateway Version' cell is highlighted with a red border. Below this is a 'Gateway Notes' section with a text area for notes. To the right is a 'Downloads' section with three items: 'Designer Launcher', 'Perspective Workstation', and 'Vision Client Launcher', each with a description and a right-pointing arrow.

# Upgrading Ignition

Upgrading Ignition is easy, but there are a few things we recommend to ensure everything goes smoothly.

See the [Installing and Upgrading](#) page for a complete guide.

## New Ignition Perspective Mobile App Features

This section is devoted to new features introduced to the [Ignition Perspective Mobile App](#). New versions of the app are released separately from new Ignition versions, so notable changes to the app will be listed in this section.

## New Ignition Features

This section is devoted to new features introduced to Ignition. Any pages in this user manual that contain features that were added will be accompanied by a display like this:

**New in 8.3.X**

## New in 8.3.10

### Drivers

- Updated the Postgres JDBC driver to include [autosave and cleanupSavepoints](#) as new default [Extra Connection Properties](#).

### Gateway Network

- Added the [Data Channel Thread Pool Initial Size](#) and [HTTP Client Max Allowed Connections](#) Gateway Network settings.

### OPC UA

- Updated S7-1200 device behavior for the Siemens Enhanced driver to match other device types having a [100 item cap](#) per request.
- Updated the Eclipse Milo OPC UA library to version 1.1.7 to improve trusted certificate management and browsing behavior.



## Perspective

- Replaced the `initialOption` property with an `activeOption` property for both the **Alarm Journal** and **Alarm Status** Tables.

## Scripting

- Added an `extendedProperties` parameter for the `system.historian.queryAggregatedPoints` function.

## Store and Forward

- Updated the **Load Disk Cache** process to create a dedicated database connection for the archived data.

## New in 8.3.9

### BACnet

- Added a new **system property** that controls whether or not BACnet devices will perform concurrent manifest reads.

### Docker

- Added a new **runtime argument** to restore local-only configuration files from a Gateway backup.

### Embedded Java

- Updated the Java Service Wrapper from version 3.5.60 to version 3.6.5.

## Enterprise Administration Module (EAM)

- Users can now **upgrade** multiple remote agents simultaneously.

## Gateway

- The **Redundancy page** is now accessible to users with read permissions.
- Added a new **system property** that allows users to opt out of automatically gzipped remote procedure calls between the Designer, Vision Client, and Gateway.

- Added a new **system property** that allows users to choose whether the IEC 61850 driver will use the module-bundled OpenSSL libraries, or the host system's OpenSSL libraries.
- Updated the **max-file-size** property's default value from 20 MB to 128 MB to allow larger JDBC drivers to be uploaded.

## OPC UA

- Updated the Eclipse Milo OPC UA library to version 1.1.6, which now requires a **ConfigureAdmin** or **SecurityAdmin** role to enable server diagnostics.
- Added **Sampling tags** to track metrics for the Siemens Enhanced driver.
- Updated **IEC 61850** addressing so that attributes shared by multiple Functional Constraints (FCs) are exposed as separate OPC nodes with an **[FC]** suffix. Tags on affected addresses must be re-addressed after upgrading.

## Scripting

- Updated the parameter syntax for the **system.historian.queryAggregatedPoints**, **system.historian.queryRawPoints**, and **system.historian.browse** functions.

## Tag Browser

- Added an **Alarm Metrics folder** at the tag provider level to the Tag Browser.
- Added the **List of Names** Pattern Type that was removed in 8.3.0 back into the Multi-Instance Wizard.

## New in 8.3.8

### Event Streams

- Icons have been added in the Project Browser for **event streams** to indicate running, modified, disabled, and failed statuses.

## Gateway

- Added an optional **Restore from Backup** step to the Ignition installer, allowing a user to restore a Gateway backup on new installations.
- The active **deployment mode** will now be logged during Gateway startup.

- Disabled redundant **automatic backup** and **VACUUM** operations on the internal database to improve Gateway startup performance.
- Larger text boxes on the Gateway Webpage, such as description fields, can now be vertically resized.

## Historian

- Added a **Number of past partitions queried for seed values** setting to control how many partitions are searched when finding a seed value.

## Perspective

- The Form component's **Dropdown widget** now includes the same `search`, `showClearIcon`, and `allowCustomOptions` properties that the Dropdown component has.
- Added a **File Upload** widget to the Form component for selecting and uploading files.

## Scripting

- Updated Ignition's Jython version from 2.7.3 to 2.7.4.
- Added a new **system.config** namespace that allows users to copy, create, delete, move, rename, replace, and retrieve Gateway resource configurations.
- Added three new system.secrets functions that allow users to create configurations for secrets to use with relevant Gateway resources.
  - **system.secrets.createEmbeddedSecretConfig()**
  - **system.secrets.createReferencedSecretConfig()**
  - **system.secrets.readConfiguredSecretValue()**

## Sequential Function Charts (SFC)

- Added Insert Tag, Operators, and Functions buttons and support for Ignition's expression language to an SFC's **Parallel Element** Cancel Condition.

## New in 8.3.7

## Alarming

- Added a **Consolidation** section to Simple One-Way Email Notification Profiles to allow configuration for consolidating multiple alarms into single notifications.

- Reconnection attempts to **Twilio accounts** are now automatic if the connection fails immediately after being configured.

## Designer

- Updated the **-Dignition.designer.websocketMaxBinaryMessageSize** system property's default value to 4096 KB from 2048 KB.

## OPC UA

- Added the ability to **export PLC symbols** from Siemens Enhanced Driver connections that are using symbolic addressing.

## Perspective

- Added the ability to use expressions as dynamic **Query Binding** paths for Perspective components.

## Sequential Function Charts (SFC)

- Updated the SFC Element Properties panel when an **element is selected** to include a dedicated Notes tab for Transitions, Parallels, Actions, Assertions, and Enclosings.

## Security

- Deprecated the **Create Project Permission** setting from the Gateway **Platform > Security > General Settings** page.

## User Sources

- Added a Legacy Naming Enabled property to the **Active Directory**, **AD/Database Hybrid**, and **AD/Internal Hybrid** User Sources to improve migration during upgrades from 8.1.

## New in 8.3.6

Ignition version 8.3.6 only contains a patch for an issue found in 8.3.5.

# New in 8.3.5

## Cloud Edition

- Ignition Cloud Edition is now available as a **container product** on the AWS Marketplace, deployable through Amazon Elastic Kubernetes Service (EKS).

## Docker

- Added `jq` utility to the **Docker image** to parse and manipulate JSON configuration files.

## Event Streams

- Updated the test controls functionality and added a **Ready** state for event stream stages.
- Added a **previousValue** object to the Tag Event source metadata to display previous tag values.
- Added an **HTTP Version** property to specify whether HTTP/1.1 or HTTP/2 should be used for HTTP handler requests.

## Gateway Network

- Added the **Remote Gateways** tab on the Gateway Network Connections webpage.

## Leased Licensing

- Leased license **activation tokens** will now still be accepted even when the token is pasted into the Activation Token field wrapped in quotes.

## OPC UA

- Added a **GDS Push Enabled** property to Ignition's OPC UA Server to allow an external Global Discovery Server (GDS) to manage the server's certificate and trust list.

## Perspective

- Added an **enabled** parent property to the File Upload component. Corresponding **enabled** and **disabled** child properties have also been added to support functionality.
- Added an **onElementClicked** component event for the Perspective Drawing component.
- Added **enabled** and **style** properties under the **radios** property for the **Radio Group** component.

- Updated the XY Chart `series.line.appearance.bullets` child properties to replace `height` and `width` with `radius` and added `label.truncate`, `label.hideOversized`, and `tooltip.getFillFromObject` properties.

## Scripting

- Added a new parameter to `system.tag.getConfiguration` to return overridden properties from UDT members.
- Added `system.historian.types.annotationPoint`, `system.historian.types.dataPoint`, and `system.historian.types.metadataPoint` functions to support structured data creation for historian writes and accept type-based objects.

## Security

- Added a **File Secret Provider** that can access secrets from files on disk.

## New in 8.3.4

### Gateway

- Added a `route-actor` **Mapped Diagnostic Context (MDC) Key** to Gateway log messages that originates from route API code paths. Depending on the access strategy used, the Key will include the username of the user, the API token name, and Client IP address pair, or the Security Zone names and Client IP address.
- Improved filesystem resource collection management and added an `ignition.resources.digest.pruning` system property to enable further maintenance of the resource directories.

### Gateway Network

- Replaced the Gateway Network 60 second enumeration call with an **event-based system**.

### Historian

- Updated the Core Historian directory to include **server.conf and log.conf files**, which increase flexibility and customization for the server configuration.

## JxBrowser

- Upgraded JxBrowser to version 8.16.0 and added a new **ignition.jxBrowser.sandboxMode** system property to control the Chromium sandbox on Linux.

## OPC UA

- Replaced the Force Secure Connection property used by Siemens Enhanced drivers with **Secure Connection Mode** to allow for greater control when using TLS.

## Perspective

- Added **typeAttr** as an element property for the Drawing component.
- Added a read-only currentBreakpoint property for the **Breakpoint** and **Column** containers.
- The **Form component** number type widget now supports using a value of **any** for step validation.

## Tags

- Added Internal Indicator (IIN) **diagnostic tags** for the DNP3 and DNP3 (Legacy) drivers.
- Wildcards can now be used to specify tag paths at both the folder level tag level when using the **Tag Event source** and **Gateway Event Tag Change Scripts**.

## User Sources

- The upgrade process now detects **User Sources with duplicate users**, logs the issues, and skips migration.

## New in 8.3.3

## OPC UA

- Updated the **Authentication property** for OPC UA connections to include Anonymous and Certificate types.
- The OPC Quick Client is now available, allowing users to browse and test OPC UA items directly from the Gateway.
- S7-1200 G2 PLCs are now supported for **Siemens Enhanced driver** connections.

## Perspective

- Updated Perspective to use the **Intl.NumberFormat** object instead of the **Numeral.js** library for better locale support.
- Added **two new parameters** to the Perspective Table component scripting events: `canceledValue` for the `onEditCellCancel` event and `originalValue` for the `onEditCellCommit` event.
- Added a `color.disabled` property to the **Toggle Switch** component.

## Redundancy

- General Gateway Network settings can now be modified on a backup Gateway to allow **disabled connections to reconnect**.

## Reporting

- Holding the Shift key while right-clicking on a report in the Project Browser will now display **two additional options**: Copy XML To Clipboard and Set XML From Clipboard.

## Scripting

- Added `sizeCutoff` and `timeoutMs` parameters to the **system.kafka.pollPartition** and **system.kafka.pollTopic** system functions to control the amount of records returned when polling.

## SECS/GEM

- The **SECS/GEM** pages are now available on the Gateway when the SECS/GEM module is installed.

## Security

- Added the ability to **import 8.1 Gateway Identity Provider exports** to 8.3 Gateways.
- Added a **Remote Secret Provider** that can access Secret Providers from another Gateway over the Gateway Network.

## Tags

- Added a **deploymentMode** System Tag to display the Gateway's active deployment mode.



# New in 8.3.2

## Drivers

- Updated the Mitsubishi driver **Max Gap Size** default to -1 for improved request optimization.

## Enterprise Administration

- Updated the **Send Stats Interval** setting on agent Gateways from 30 seconds to 45 seconds.

## Event Streams

- Added support for numeric quality codes for event stream **tag handlers**.
- Users can now subscribe to Alarm Metrics in a **Tag Event source**.
- Added a Tag Browser  icon to the event stream **tag handler** form to make adding tag paths easier.

## Gateway

- Improved Gateway **System Name** validation so that invalid names, such as those containing a | character, will be rejected and fail to save. Non-ASCII Unicode and emoji characters are supported, but may cause rendering issues in certain areas.
- Quarantined Modules** now have actions allowing users to either resolve the quarantine reason or delete the module from the Gateway.
- Updated the 8.3 Gateway UI graphic assets and Quick Start menu to ensure contrast ratio and shape distinction accessibility standards are met.
- Added **two new properties** to the Gateway Network General Settings page to support the Gateway Network now using its own thread pool to process incoming messages. Users who have previously adjusted the `gateway.maxThreads` property found in the `gateway.xml` file, especially those using large Hub and Spoke Architectures, should now configure these settings instead.
- Added a **Manage JAR Files** option on the JDBC Drivers page to improve visibility and access to JAR files.
- Added an **Identity Provider** setting to configure the Identity Provider selection when creating a project. This addition matches the process already available when setting up projects in the Designer.

## Reporting

- Improved **vector settings and print quality** for Report components using vector graphics.

## Security

- A new Connect Timeout property has been added to **Active Directory**, **AD/Database Hybrid**, and **AD/Internal Hybrid** User Sources, allowing users to set a custom connection timeout for LDAP operations.

## Tags

- Added a **Qualified Value** option to Tag Event Scripts, allowing scripts to run when a tag receives a qualified value update.

## Vision

- Updated the **Resource Encoding** project property to also include Vision Client tags when applying binary or XML serialization format.

## New in 8.3.1

### Gateway

- Users can now edit endpoints for overridden **OPC UA Connections** that are within different Gateway Deployment Modes.

### Launchers

- Added support for JVM arguments in File Associations for Designers and Vision Clients.

### OPC UA

- Users can now utilize the `.getDescription()` method when using **system.opc.browseServer** to retrieve **Documentation** meta data from **exposed tags**.
- Added a new property allowing users to specify read and write **max holding register** values independently of each other.
- Added a **Timestamp Source** property for OPC UA Connections.

### Perspective

- Upgraded the Markdown library to v5.0.3 to address CVE-2020-7753 and improve the **Markdown component** functionality.

- Added **keyboard shortcuts (F1-F10)** to the Drawing component's Drawing Editor for quickly switching tools.
- Updated shortcut behavior to include the ⌘ (Command) key for macOS, and modified the ⌘ + Drag functionality to now pan instead of opening a right-click menu.

## Scripting

- The PyOPCTag return object for **system.opc.browseServer** has been updated to include functionality that was already included in the OPCBrowseElement return object.
- Added a new `PyPlaintext` class and **system.secrets** functions to interact with `SecretProviders` and the `SystemEncryptionService`.

## Security

- Added **User Attribute Mapping**, **User Grants**, and **Security Levels** to be configurable on overridden Identity Providers within mutable **collections**.
- Updated Netty library to version 4.1.127.

## Tags

- Added the **Preserve Source Timestamp** property to Derived tags.
- Added an option to hide **Alarm Metrics** within the Tag Browser.

## Vision

- Added an **Auto-Redirect** option for Vision Clients using the Identity Provider strategy to skip the login steps when launching.

# New in 8.3.0

## Alarming

- The **Runtime Alarm Metric** properties are now available at the folder level and for all UDT instances, along with an additional 15 aggregated alarm metric properties.
- Added two new **tag alarm modes**, When True and When False.
- Added Twilio **Voice** and **WhatsApp** Notification Profiles for the Twilio Notification module to allow more options for alarm acknowledgement.

## Designer

- Added a **-Dignition.designer.websocketMaxBinaryMessageSize** system property to adjust the maximum size of binary data that the websocket between the Designer and Gateway can handle.

## Docker

- Improved Docker image support for third party modules, especially during container upgrades with the following:
  - Updated **module identifiers** to be fully qualified IDs.
  - Added two new **environment variables** to automate third party module acceptance across container lifecycle events.
- Updated the **Docker image** to be compatible with OpenShift 4 **restricted** Security Context Constraints.

## Drivers

- Added a new **Siemens Enhanced driver** through the Siemens Enhanced Driver module that supports browsing and symbolic access when connected to S7-1200 and S7-1500 devices.
- The **MariaDB, MSSQL, and PostgreSQL JDBC drivers** are now bundled with Ignition.

## Enterprise Administration Module (EAM)

- Added the option to use **Leased Licenses (Eight-Character Keys)** for EAM license activation.

## Event Streams

- **Event Streams** are now available to use as project resources.

## Gateway

- Added a **-Dignition.gateway.externalModulesFolder** system property to allow to specify an install folder location for external or third party modules.
- Added two **system properties** that enable the ability to query the Core Historian directly using Postgres.
- Added a new **banner** state to indicate when Gateway Restarts are required.
- Added **Gateway Deployment Modes** to allow Gateways to have different running environments.
- Added a **reference page** for the Gateway's folder structure.

- Added a new **OpenAPI** documentation page at the `/openapi` endpoint, providing a dynamically generated specification of available HTTP API routes for external integration.
- Updated the **Gateway sidebar navigation**, along with other interface changes, for improved usability and layout.
- Added a `-Dignition.gateway.rpcErrorDetailSuppression` system property to filter error details from Clients and Designers as desired.
- Added a **Permissions tab** to the OPC UA Server Settings page to allow users to apply access levels to OPC UA devices and exposed Tag Providers.
- Added an **environment variable** and **Gateway Network setting** to allow Java serialization as needed for upgrading 8.1 Gateways to 8.3.
- Added a **Serialization Format** setting to allow Java Serialization for messaging between Clients, Designer and the Gateway during upgrade.
- Added a **Roles & Permissions** section to the Gateway **Platform > Security > General Settings** page. These settings enable access levels and permissions based on the current user role.

## Historian

- Added the **Core Historian** as an additional historical provider option for time-series data.

## JxBrowser

- Upgraded JxBrowser to 8.5.0.

## Launchers

- Added **deep link and File Association** support to the launchers to allow direct launching of targeted Gateways.
- Updated **Launcher** supported architecture for Mac to Apple Silicon, x86 Mac is no longer supported.
- Added a new **allow.uri.schemes** Launcher JSON setting to support direct access to applications from the operating system.

## OPC UA

- Added support for GDS Push in Ignition's OPC UA server with a `gdsPushEnabled` property now available in the **OpenAPI** under `IgnitionOpcUaServerConfig.Advanced`. When enabled, a user with the SecurityAdmin role is allowed to manage the server's certificates and trust lists via the `ServerConfigurationObject` and its associated methods. Note that the `SecurityAdmin` does not exist by default and will need to be created on the Gateway for this feature to function properly.

## Platform

- The **gwcmd utility** **-u** **command** now supports unactivating supplemental license keys in addition to the primary license key.
- Added the ability to **create Backup version configurations** that will override master Gateway configurations in redundant pair setups.

## Perspective

- Added a **Drawing** component to create and configure SVG-based vector graphics directly within the Designer.
- Added a **Form** component to create and manage interactive forms with dynamic validation, submission handling, and custom scripting capabilities.
- Added a **Form Submission** Session Event, allowing users to handle form submission, manage validation, and process form data within the Gateway.
- Upgraded minimum browser versions required for **Perspective Sessions**.
- Added a **Page Details** section to the Perspective Session Status Popup to display page counts, latency, and up time data.
- Updated Perspective themes to now use APIs for overriding built-in themes or **creating new themes** resources under the config-perspective-themes resource type.
- Added **Offline Mode** support in the Perspective App, allowing mobile users to continue interacting with cached project views and resources during periods of network disconnection. Offline Mode must be enabled in the Perspective Project Properties and is only available in the Perspective App.
- Upgraded the react-pdf library to version 7.7.3.
- The File Upload component will now only accept files smaller than 20 MB, regardless of the **fileSizeLimit** property. This can be increased using the max-file-size property within the **web.xml** file.

## Reporting

- Added a **Radar Chart** component to the Reporting module.
- Added a **hidden** property for the Page Object component to allow entire pages to be excluded from a report.
- Images can now be added through **copy and paste** in addition to the drag and drop method.
- The following components can now be used as either raster or vector images:
  - **Barcode**
  - **Bar Chart**

- [Pie Chart](#)
- [Radar Chart](#)
- [Timeseries Chart](#)
- [XY Chart](#)

## Redundancy

- Added a [-Dignition.redundancy.syncMaxAttempts](#) system property to set a limit on sync attempts for redundancy providers.

## Scripting

- Improved [scripting autocompletion and hint](#) details for system functions, including listing system library constants and identifying deprecated functions.
- Migrated the [system.serial](#) scripting functions into the Ignition platform, and removed the Serial modules as they are no longer needed.
- Added a [system.db.execScalar](#) scripting function to provide a way to execute scalar queries, compared to [system.db.execQuery](#), which only executes select queries.

## Security

- Extra LDAP attributes can now be defined for the [Active Directory](#), [AD/Database Hybrid](#), and [AD/Internal Hybrid](#) user sources.
- Two additional properties for nested group membership lookup and group role attributes are now available for the [Active Directory](#) user source.
- Three new properties are now available for [Ignition Internal Authentication](#):
  - Prohibit Password
  - Prohibit Username
  - Maximum Consecutive Repeated Characters
- The Administrator role is now automatically listed under the Authenticated/Roles [security level](#) when installing a fresh Gateway.
- Implemented a [Secrets Management system](#) that provides support for encrypting secrets like credentials, API tokens, and private keys. The Secrets Management system also includes opt-in functionality for establishing a more secure system setup.

## System Functions

- Updated syntax for system functions that are only scoped for the Vision Client to [system.vision](#). This affected functions under `system.dataset`, `system.db`, `system.file`, `system.gui`, `system.nav`,

system.net, system.print, system.security, system.tag, and system.util.

- Deprecated `system.gui.convertPointToScreen` and `system.gui.getQuality`.
- Reconfigured dataset scripting to automatically expose all datasets as PyDatasets. The function `system.dataset.toPyDataSet` has been deprecated with this change.
- Replaced `system.db.clearAllNamedQueryCaches` and `system.db.clearNamedQueryCache` system functions with **`system.db.clearQueryCache`**.

## Tags

- A new System tags folder called **ModuleVersions** has been added for EAM controllers to monitor module versions on agents.
- Two Memory tag **Value properties** have been added: **Default Value** and **Value Persistence** that determine Memory tag values on startup and storage behaviors.

## Vision

- Vision Client settings now propagate on **retargets** to preserve launch modes, screens, and more.
- The **Web Browser** component is now included within the Vision module, and can now be found under the Misc category in the Designer Vision Components panel.



# Mobile App Changelog

## Updates for version 1.0.10

### General

- Improved logging around DeepLinks.
- Improved backwards compatibility and error handling when interacting with the WebView.
- Improved memory leak notifications and tests.
- Updated barcode scanning to align with device orientation and ensure more accurate barcode captures.
- Updated the logs to maintain a 1MB file size between Sessions.
- Added support to automatically upgrade the Perspective Mobile Demo project to the current version.
- Fixed issues associated with SAML sign in for Offline mode.

### Android

- Added support for 16KB page size devices.
- Migrated builds from KAPT to KSP, and updated AndroidX Room from 2.4.3 to 2.7.2 and Dagger2 from 2.28.3 to 2.57.1.
- Improved offline submission processes by collating results into a single notification and displaying the submission queue filter on a new page instead of a popup.
- Fixed an issue where docked Perspective views would sometimes scroll after unlocking the device.
- Updated the minimum supported version of Android to version 8.
- Fixed an issue where the Identity Provider's Remember Me option did not behave as expected.
- Upgraded Firebase from 27.0.0 to 33.16.0 to eliminate a protobuf-javalite vulnerability.

### iOS

- Updated SSL certificate instructions to align with supported iOS versions.
- Fixed an issue where iOS camera previews could be opened in a windowed view.
- Added support for handling DeepLinks.
- Improved iBeacon filtering on iOS.

# Updates for version 1.0.9

## General

- Updated with build fixes, improvements, and modernizations.

## Android

- Added support for Offline projects and Offline form submission.

## iOS

- Upgraded minimum supported iOS version to iOS 16.
- Updated dependencies for iOS Privacy Manifest Inclusions.
- Added support for Offline projects and Offline form submission.

# Updates for version 1.0.8

## General

- Updated error handling for Gateway address fields and parsing.
- Fixed an issue preventing redundant Gateways with module mismatches from being added to the Perspective App.
- Added support for the following Eddystone formats: UID, EID, URL, Plain TLM, and Encrypted TLM. BLE Beacon UUID and MAC address are also now included at the new address key, if available.
- Added support for the insecure Boolean query arg: If set to true, HTTP will be preferred over HTTPS.

## iOS

- Added an additional iOS AppConfig Boolean restriction of `internal_webview_auth` to keep authentication flows within a webview for external IDPs. Note that this should not be used unless it is the only way to perform auth.

# Updates for version 1.0.7

## General

- Fixed an issue so that view permissions are now properly reflected upon login.

## Android

- Accelerometer actions now return values at the requested rate instead of only once.

## iOS

- Fixed a system.perspective.download issue to allow downloads regardless of the port a Gateway is using.
- Added a new iOS Restriction ephemeral\_auth\_sessions and relaxed the requirement of using Safari for authentication when using Single App mode or guided access on iOS.
- Added landscape orientation support for barcode scanning.

## Updates for version 1.0.6

### General

- DeepLinks will now always attempt connecting over HTTPS first when launching Perspective apps.

### Android

- Fixed an issue with Bluetooth scanning permission requests.

## iOS

- Fixed an issue with Accelerometer usage crashing the mobile app.
- Fixed an issue with Perspective barcode events not being processed while the Accelerometer is enabled. Simultaneous Accelerometer actions and barcode scanning now works as expected.

## Updates for version 1.0.5.1

### Android

- Fixed an issue with NFC scanning on Android versions 12 and 13

## Updates for version 1.0.5

### General

- Improved error handling from shared library code.

### Android

- Minor Library compatibility updated for Android 13

## iOS

- Updated back swipe gestures to behave like the Back navigation action.
- Improved handling of Gateway status discovery and app launches for Gateways over poor network connections.
- Included additional privacy info keys for compliance.

## Updates for version 1.0.4

### General

- Added third party dependency attribution.
- Added support for front camera barcode scanning. In addition, the Scan Barcode Action now supports specifying either the front or back camera as the default.
- Updated various third party dependencies.

## iOS

- Users can now click outside of the login panel on iPads.
- Added support for EMM, which conforms to the AppConfig standard. An AppConfig compatible specification document is available in under the [Extra Materials](#) page of the Inductive Automation website.

## Updates for version 1.0.3

### Android

- Geolocation tracking in the mobile apps has been improved and a new accuracy setting of 'HIGH' has been added which is accurate up to about 3 meters
- Pinch and zoom functionality for running perspective sessions fixed on Android

## iOS

- Geolocation tracking in the mobile apps has been improved and a new accuracy setting of 'HIGH' has been added which is accurate up to about 3 meters

## Updates for version 1.0.2

- The [system.perspective.download](#) function now prompts the app to save the target file locally (requires Ignition 8.1.14)

## Updates for version 1.0

- Fixed several issues that could cause the app to crash.
- Fixed an issue that caused views to resize when an onscreen keyboard is displayed.
- The mobile app will now prevents swipes from causing a refresh if `session.device.pullToRefresh` is disabled.

## Updates for version 0.98

- Added support for scanning inverse barcodes. Corresponds with Ignition 8.1.3, which added an option to the **Scan Barcode Action** that can limit light or dark background.
- In a Perspective **Barcode Scanned** event script, the scanned barcode type is now returned via the `barcodeType` property.

## Updates for version 0.97.2

- Fixed an issue with the app's login screen when using OpenId Connect or SAML authorization on Android.

## Updates for version 0.96:

- The app can now be **managed remotely** via Enterprise Mobile Management services.

# Other Editions

 **Ignition Edge**

 **Ignition Maker Edition**

A community version of Inductive Automation's Ignition SCADA application.

 **Ignition Cloud Edition**

# Ignition Edge

Ignition Edge is a lightweight version of Ignition designed for use on field devices and OEM hardware at the edge of the network. It allows industrial systems to collect data, run local automation logic, and communicate with central Ignition systems while operating on resource-constrained hardware. Ignition Edge supports multiple operating systems, including Linux, Windows, and macOS, and is compatible with ARM processors, making it suitable for devices such as Raspberry Pi and modern industrial edge hardware.

Ignition Edge can be installed on any system that meets the minimum requirements, including industrial PCs, panel PCs, and other edge-capable hardware. In addition to manual installation, Ignition Edge is also available preinstalled on select devices offered by Solution and Alliance Partners like Opto22 and OnLogic.

## Licensing

The new Edge version of Ignition has a separate license that works in the same way as a traditional Ignition license. The Edge license is set up to only work on an Edge Gateway, so it will not work if you attempt to activate it on an Ignition Gateway. However, you can activate a full Ignition license on an Edge Gateway, although this is not recommended due to the limitations of the Edge platform.

Additionally, once a license has been activated on an Edge Gateway, the trial time for any unlicensed Edge products will be removed, and you will no longer have access. To regain access, contact your Account Representative and inform them what Edge products you need to purchase. After purchasing, the products will be added to the existing license. Reload the license on your Gateway to view and use the products.

## Core Functionality

All Edge installations are a limited version of the Ignition platform for a significantly reduced cost. This helps keep things simple, and these installations always work with other full versions of Ignition if you need additional functionality. The following features are available on all Edge Gateways, licensed or unlicensed. See [Edge Gateway](#) for more details on the the Edge Gateway.

## OPC UA Module and Drivers

Edge can create OPC UA client connections natively to other UA servers. Edge IIoT and Edge Panel allow the Edge Gateway to act as an OPC UA server, enabling other OPC UA clients to connect and

read data.

## Internal Storage

An Edge installation can store certain historical data inside Ignition.

- **Tag History:** Up to 35 days or 10 million data points of history can be stored locally. Pruning will automatically happen, and the historian is automatically enabled and not configurable. You can learn more about Tag History [here](#).
- **Alarm Journal:** The Alarm Journal will store all alarm events locally for one week of events. There are limited configuration options; the Alarm Journal can be accessed via the Edge Alarm Journal profile.
- **Audit Logs:** Like the Alarms, the audit log is limited to one week of local storage. It is not configurable.

## Projects

Edge installations have just one project. This project is created automatically if it did not exist, and it cannot be removed. The default project name is "Edge" and can be renamed. For more information, see [Edge Gateway](#) page.

## Redundancy

Two Edge Gateways can be set up with [redundancy](#). An Edge Gateway can only failover to another Edge Gateway (not a standard Ignition Gateway).

## Email Notifications

Edge Gateways can make use of the built-in [Simple One-Way Email Notification Profile](#) and [Remote Gateway Notification Profile](#), allowing the Gateway to send out email notifications.

## Edge Capabilities

Edge Gateways include several built-in capabilities that allow them to operate independently at the edge of the network while still integrating with a central Ignition system.



# Local Automation and Scripting

Edge Gateways can execute automation logic directly on the Gateway using Python scripting. This allows data processing, event handling, and automation tasks to occur locally without relying on a central Ignition server.

Scripts can run in several contexts, including:

- **Gateway Event Scripts**, which execute based on Gateway lifecycle or scheduled events
- **Tag Event Scripts**, which trigger when tag values change or alarms occur
- Expression-based scripting using the **runScript** function

These scripting capabilities enable Edge Gateways to perform local automation tasks, respond to device events, and process incoming data before forwarding it to other systems. Scripts are written in Python, a flexible and widely used programming language. For more information, see [Python Scripting](#).

## Gateway Communication

Edge Gateways can communicate with other Gateways using Gateway Network Messaging. This allows Gateways to send messages or requests to other Gateways for processing.

Gateway messaging is commonly used to distribute tasks across Gateways or forward information to centralized systems.

Messaging functionality is available through the following scripting functions:

- **system.util.sendMessage**
- **system.util.sendRequest**
- **system.util.sendRequestAsync**

## Web Services and APIs

Edge Gateways include the **WebDev module**, which allows developers to program directly against the Gateway's built-in web server.

Using the WebDev module, you can:

- Host web pages or static files
- Create REST APIs
- Allow external systems to interact with the Edge Gateway

This capability allows Edge Gateways to integrate with external applications, services, and custom tooling.

## Data Synchronization

Edge Gateways can synchronize operational data to a central Ignition Gateway. This allows data collected at the edge to be stored, analyzed, or visualized centrally.

The following data types can be synchronized:

- Tag History
- Alarm Journal events
- Audit Log records

This capability allows organizations to deploy distributed Edge systems while maintaining centralized visibility of operations.

## Enterprise Administration Module (EAM) Agent

Edge Gateways can function as agents in an Enterprise Administration Module (EAM) architecture when connected to a central Gateway running EAM.

This allows administrators to manage Edge Gateways centrally, including:

- Monitoring Gateway status
- Deploying updates
- Distributing configuration changes
- Performing remote tasks across multiple Gateways

## Edge Products

Edge Gateways can fill multiple roles and help bridge different architectures. Ignition Edge is available in two product editions: **Ignition Edge IloT** and **Ignition Edge Panel**. A license is required to activate an Edge product.

| Product                                                                                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <p><b>IIoT</b></p>   | <p><b>Ignition Edge IIoT</b> turns virtually any field device, such as a touch panel or a client terminal, into a lightweight, MQTT-enabled Edge Gateway that works seamlessly with Ignition IIoT and other common IIoT platforms, providing remote data acquisition and optional secured feedback and control. It's ideal for polling data at the device location and publishing data to an MQTT server that business systems and applications can access.</p> <p>Ignition Edge IIoT can synchronize tag history, Alarm Journal, and audit data to a central Ignition Gateway and function as an EAM agent when connected to a Gateway with the Enterprise Administration module installed.</p> |
|  <p><b>Panel</b></p> | <p><b>Ignition Edge Panel</b> includes everything in Ignition Edge IIoT, plus local visualization functionality for your HMIs. Choose between Perspective (two Sessions) or Vision (one local Client, one remote Client) as your visualization system for Edge Panel. Build future-proof, robust local control systems that are Industry 4.0-compatible. It's ideal for standalone HMIs and providing a local Client fallback for field HMIs if the network connection is lost.</p> <p>Like Ignition Edge IIoT, Ignition Edge Panel can synchronize tag history, Alarm Journal, and audit data to a central Ignition Gateway and function as an EAM agent for centralized management.</p>        |

## Ignition Edge Compared with Ignition

Because Edge is a lean solution, it does have some functionality limitations compared to full Ignition. Ignition and Ignition Edge share the same basic platform, but Edge is a leaner version of Ignition made specifically for use in on edge-of-network devices. Ignition comes with unlimited tags, Clients, and database connections, while Ignition Edge comes with unlimited tags, two Clients (one local and one remote) and no database connectivity.

- **Database Access:** Database access is disabled. This means that any database queries or bindings will not work, and the user sources that require a database connection will not be available. The Gateway Webpage has been updated to remove these features and reduce confusion. Despite this restriction, some historical storage can happen inside of Ignition.

- **Gateway and Project Backups:** A Gateway backup made in an Edge installation will work in other Edge installations, or if needed, Standard Edition Gateways as well. Although restoring a Standard Edition Gateway backup is possible in an Edge installation, it is not recommended due to the limitations of the Edge platform. You can, however, still export tags, windows, and other project resources in the Designer from Standard Edition Gateways and import them into an Edge project, or vice versa.
- **Tag Providers:** Edge Gateways only contain a single active Realtime Tag Provider. Additional providers may not be created.
- **Historian Providers:** Edge Gateways contain a single historian provider, which is an instance of the **Internal Historian (Legacy)** (named the Edge Historian Provider)
- **Third Party Modules:** Edge's core functionality determines which modules run on the platform. Third party modules will not run on an Edge Gateway unless explicitly stated as compatible with Edge.
- **Visualization:** Visualization is only supported on Edge Panel and not Edge IIoT. Additionally, Edge Panel Gateways have a limit of two Vision Clients or Perspective Sessions running concurrently.

# Edge Gateway

The Edge Gateway has many of the same options as the standard [Ignition Gateway Webpage](#) along with a few Edge-specific settings and visual changes. You can see below that after installing Edge, the traditional orange Ignition logos are replaced with new green Edge logos so a Gateway can be easily identified.

## Navigating the Edge Interface

The first time you go to the Edge Gateway Webpage, it shows you several steps to help you get started. Once you're up and running, the [Home](#) section lets you download the Designer Launcher or Vision Client Launcher, or view a Perspective project. There are some resource links to help you get started with Ignition quickly: Inductive University, Quick Start Guide or Product Documentation where you can learn about Ignition modules, as well as the Appendix which contains a complete reference for components, expressions, and scripting functions.

When you're first introduced to Ignition, the Welcome page is the landing page. It's where you'll find the Designer Launcher, Vision Client Launcher, and Perspective Sessions.

- The [Designer Launcher](#) locates all Gateways that are available on your local network. Once you open the Designer, you can access the Edge project.
- The [Vision Client Launcher](#) opens Vision Clients from any Ignition Gateway.
- The [Perspective Sessions](#) opens Perspective sessions from this Gateway.

If you're running Perspective as the visualization method for your project, you can launch a Perspective Session from the Designer, from the Gateway, or by entering the web address of the project in your web browser.

Home

Welcome

Designer

Perspective

Vision

Platform

Connections

Network

Services

Diagnostics

Welcome to Ignition

Launch Designer

Gateway Overview

| Gateway Name | Redundancy  | Gateway Version | Gateway Mode |
|--------------|-------------|-----------------|--------------|
| Ignition     | Independent | 8.3.1           | N/A          |

Gateway Notes

Welcome to your Ignition Gateway. This customizable area is intended to capture the critical details you want to document for this Gateway. You might include information about the environment (production, testing, or development), key workflows, or maintenance schedules. It's also a great place to list instructions for your team, important reminders about system health, or details about your configuration that require regular review. Use this space to keep everyone informed and ensure smooth operations across the board.

Downloads

Designer Launcher  
Bring all your data, systems and developers together into one simple, integrated development environment.

Perspective Workstation  
Open Perspective Sessions from any Ignition Gateway.

Vision Client Launcher  
Open Vision Clients from any Ignition Gateway.

Ignition Resources

Browse our extensive product documentation and free online training university for answers to all of your questions.

Kickstart Your Learning  
Check out Inductive University and learn the Ignition Platform at an industry-ready level.  
Go to Inductive University

Share, Download, & Create  
Go to the Ignition Exchange to download and post assets or entire projects.  
Browse Resources

Product Documentation  
Explore the User Manual for details about the Ignition platform and modules.  
Open User Manual

Below the Home section, are five other sections:

- Platform
- Connections
- Network
- Services
- Diagnostics

Each section provides corresponding access to configuration options for Gateway settings and status overviews for specific systems. For complete information, see the [Ignition Gateway Web Interface](#) section. Note that some settings, such as database connections, are not available for Edge.

### ❗ CIRRUS LINK MODULES

Select Cirrus Link modules will be displayed on the **Platform > Ignition Edge > Products & Modules** page. These modules will be available to install and use if your Ignition license supports them. The modules will also be available to install and use during Ignition's two hour trial period if you are either not using a license, or using Ignition in trial mode.

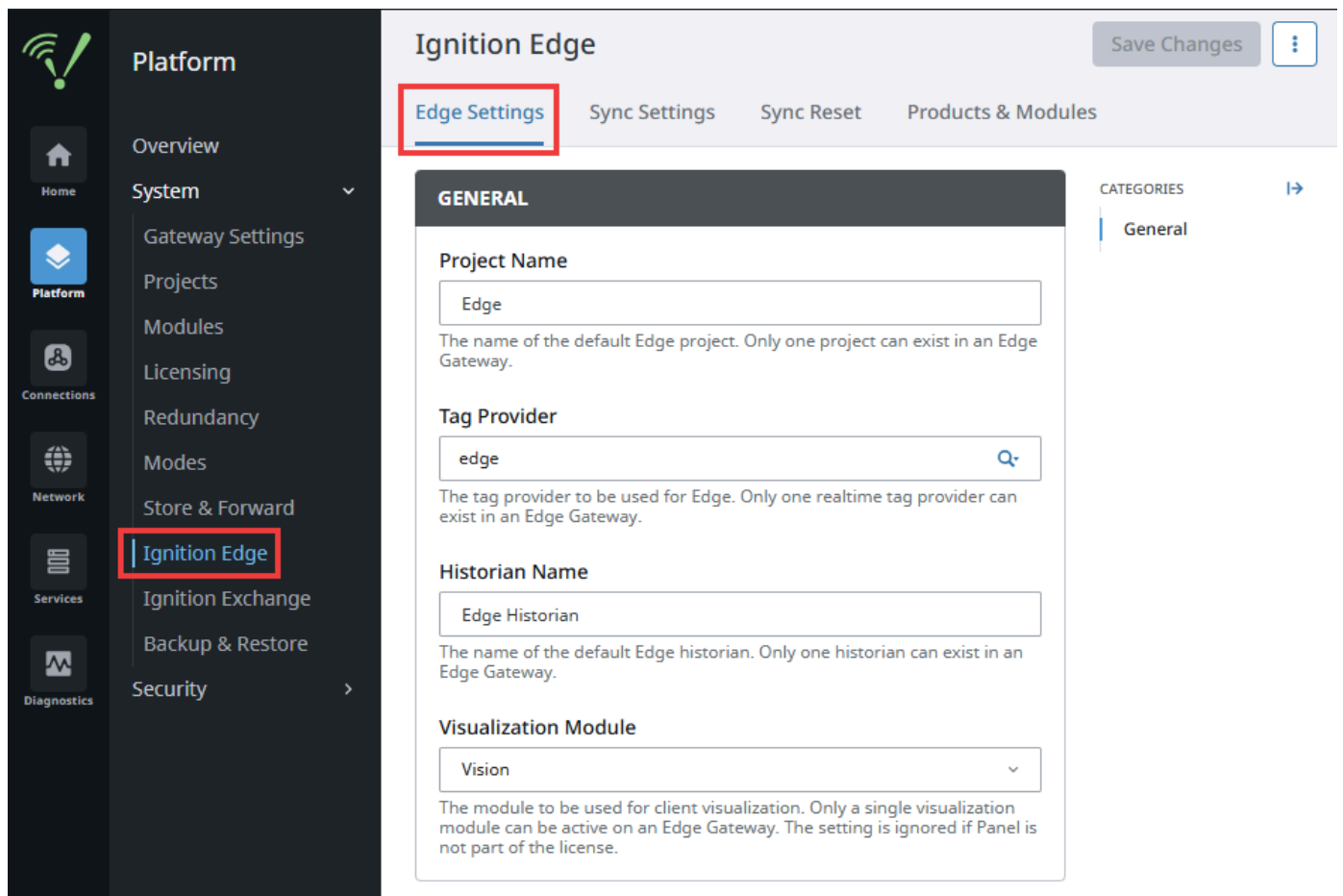
## Edge Gateway Settings

There is an additional set of Gateway Settings for Edge that are not available in Standard Ignition. These settings enable you to modify the names of the Edge project, Edge Tag Provider, and Edge Historian. You can also set the visualization method (Vision or Perspective) here if you are using the [Edge Panel](#) product.

| Edge Setting         | Description                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Project Name         | The name of the Edge project. Default is "Edge". Only one project can exist in an Edge Gateway. You can change the name of the project with this setting.                                                                                                                                                                                                                             |
| Tag Provider         | Represents the Tag Provider that is currently loaded on the Edge Gateway. Normally, only a single Tag Provider can be created on an Edge Gateway, but if the Gateway was recently switched from Standard Edition to Edge, then there could be additional Tag Providers within the Gateway's internal database. This setting allows you to select which of those Tag Providers to use. |
| Historian Name       | <p>The name of the Edge Historian. Only one historian can exist in an Edge Gateway.</p> <p><b>Caution:</b> If a historian name is changed after Tag History has already been configured for a tag under the previous historian name, the storage provider setting will need to be manually updated in the Tag Editor to match the new historian name.</p>                             |
| Visualization Module | The name of the default Edge Panel visualization method (Vision or Perspective). Only one visualization system can be used in an Edge Gateway. This value is unused if the Edge Panel product is not licensed. Default is Vision.                                                                                                                                                     |

## Accessing Edge Gateway Settings

1. To get to the settings, click **Platform > System > Ignition Edge** on the Edge Gateway.
2. Make sure you're on the **Edge Settings** tab.



3. Change the settings as desired, then click **Save Changes** at the top of the screen.

## Edge Tag Provider Page

Located under **Services > Tags**, this page allows you to change the name and description of the loaded Tag Provider.

Additionally, the **Edit** panel includes an **Allow Back-fill Data** setting, which functions in a similar manner to the same setting on Standard Gateways. See [Tag Providers](#) for more details.



The screenshot shows the 'Edit edge' dialog box in the Realtime Tag Providers interface. The dialog has a close button (X) and an information icon (i). It contains a permissions section with a tree view showing 'Public' (checked), 'Authenticated' (unchecked), 'Roles' (unchecked), 'SecurityZones' (unchecked), and 'Default' (unchecked). Below this is a note: 'Any actor attempting to edit any tag within this tag provider must have these permissions. If Public, tag editing for this provider will not be restricted.' There are two radio buttons for 'Users must belong to all of these security levels in order to edit this provider's tags.' (selected) and 'Users must belong to at least one of these security levels in order to edit this provider's tags.' (unselected). The 'ADVANCED' section has a red border and contains 'Allow Back-fill Data' (unchecked) with a description: 'If enabled, data will be allowed to arrive out of order from the source. Data from the past will be stored to history, but will not be used for alarms, scripts, or subscriptions. If false (default behavior), each value will be processed fully as it arrives.' and 'Enable Tag Reference Tracker Store' (checked) with a description: 'Enables the storing of Tag Reference entries to a database on the local Gateway for analysis in a Designer'. At the bottom are 'Cancel' and 'Save Changes' buttons.

## Edge General Alarm Settings Page

The General Alarm Settings page provides basic alarm settings including the Live Event Limit, Continuous Event Detection Window, and Notify Initial Events.

This page is located under **Services > Alarming > Settings**.

The screenshot shows the 'Alarming Settings' page. The left sidebar has a 'Services' menu with 'Overview', 'Tags', 'Alarming' (expanded), and 'Settings' (highlighted with a red box). The main content area has a header 'Alarming Settings'. Below it are two sections: 'ALARM EVALUATION' (marked \*Required) and 'EVENT SUPPRESSION' (marked \*Required). The 'ALARM EVALUATION' section has a 'Live Event Limit' input field set to 5, with a description: 'The number of "live" events (active or unacknowledged) that can exist for a single alarm at a given time. When surpassed, older events will be acknowledged automatically by the system.' The 'EVENT SUPPRESSION' section has a 'Continuous Event Detection Window (min)' input field set to 10, with a description: 'How long to store events for on shutdown, to prevent new events on startup. Prevents unacknowledged active events from being generated due to reboot. If set to 0, will not be used.' and a 'Notify Initial Events' checkbox (unchecked) with a description: 'If false, active alarms caused by the "initial state" (that is, the first value checked after being created, or after the enabled state changes) won't be sent to the notification system.'

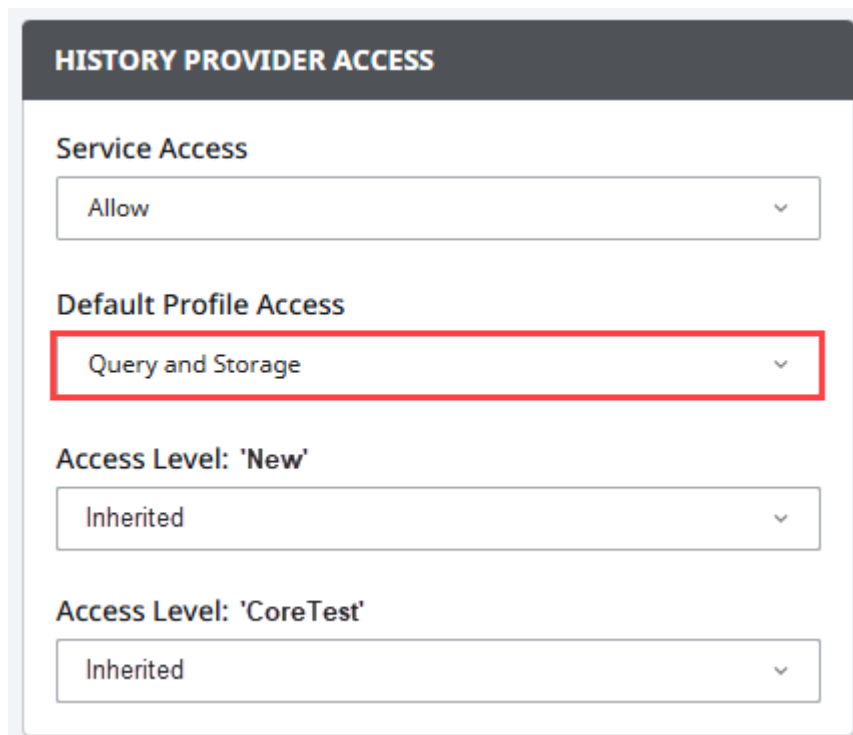
For more information about the Gateway's Alarming settings, see Alarming on the [Gateway Services](#) description page.

# Configuring Sync Services

## Data Synchronization

Synchronization allows you to sync your historian data, audit records, and alarm journal entries from the Edge Gateway to a Standard Ignition Gateway, allowing you to save past the internal data limit. The Edge Gateway will still only see the 35 days of Tag History and 7 days of Alarm Journal and Audit Log data that it can hold, but it will allow you to store the data in a more permanent database that can be viewed from other Ignition systems.

Before data can be synchronized across Gateways, your standard Gateway's system must be configured to accept Edge storage. This can be completed by navigating to the **Platform > Security > Zones** page and accessing the Manage Policy panel for the security zone you want to use for Edge storage. This is done by expanding the security zone's three dots menu and selecting **Manage Policy**. Afterwards, you can select **Query and Storage** for each section you will be receiving data from. Available sections include Alarm Journal Access, Audit Log Access, and History Provider Access.



**HISTORY PROVIDER ACCESS**

Service Access

Allow

Default Profile Access

Query and Storage

Access Level: 'New'

Inherited

Access Level: 'CoreTest'

Inherited

Once you've allowed storage access, you can navigate back to your Edge Gateway to finish configuring your synchronization settings under **Platform > System > Ignition Edge > Sync Services** page.



Due to serialization updates, Edge Sync Services data originating from an 8.3 Edge Gateway cannot be stored to an 8.1 Gateway. This includes syncing to remote history providers, remote audit logs, and remote Alarm Journals. It is recommended to first upgrade the central server hosting data to 8.3 before upgrading any remote 8.1 Gateways. See the [8.3 Upgrade Guide](#) for more information.

The following tables describe the synchronization settings.

## Main Settings

| Property            | Description                                       |
|---------------------|---------------------------------------------------|
| Remote Gateway Name | The Gateway to target for remote synchronization. |

# Remote History Sync Settings

| Property                     | Description                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remote History Provider Name | The remote History Provider to sync data to.                                                                                                                                                                                                                                                                                                                           |
| Remote History Sync Enabled  | Whether to send local tag history data to the remote system. The remote system must have the Tag Historian module installed, and allow remote storage. Default is false.                                                                                                                                                                                               |
| Max Batch Size               | The maximum number of data points that will be sent per batch to the remote Gateway.                                                                                                                                                                                                                                                                                   |
| Sync Frequency               | The frequency with which data will be sent to the remote Gateway. This setting will be used in conjunction with the sync schedule, if enabled.                                                                                                                                                                                                                         |
| Sync Frequency Units         | Units are defined as milliseconds, seconds, minutes, hours, days, weeks, months, and years.                                                                                                                                                                                                                                                                            |
| Enable Schedule              | If enabled, the data will only be synchronized during the times specified by the pattern provided.                                                                                                                                                                                                                                                                     |
| Schedule Pattern             | <p>A comma separated list of time ranges that will determine when data will be sent over the network. Accepted formats include am/pm notations, military time, and the use of colons or periods to distinguish the hour from minutes. Minutes are not required. For example, a schedule could look like the following:</p> <div>9:00-15:00, 6pm-1am, 06.30-07.30</div> |

# Remote Audit Settings

| Property                  | Description                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remote Audit Profile Name | The remote audit profile to sync data to.                                                                                                                                                                                                                                                                                                                              |
| Remote Audit Sync Enabled | Whether Remote Audit Sync is enabled. Default is false.                                                                                                                                                                                                                                                                                                                |
| Sync Frequency            | The frequency with which data will be sent to the remote Gateway. This setting will be used in conjunction with the sync schedule, if enabled.                                                                                                                                                                                                                         |
| Sync Frequency Units      | Units are defined as milliseconds, seconds, minutes, hours, days, weeks, months, and years.                                                                                                                                                                                                                                                                            |
| Enable Schedule           | If enabled, the data will only be synchronized during the times specified by the pattern provided.                                                                                                                                                                                                                                                                     |
| Schedule Pattern          | <p>A comma separated list of time ranges that will determine when data will be sent over the network. Accepted formats include am/pm notations, military time, and the use of colons or periods to distinguish the hour from minutes. Minutes are not required. For example, a schedule could look like the following:</p> <div>9:00-15:00, 6pm-1am, 06.30-07.30</div> |

## Remote Alarm Journal Settings

| Property                    | Description                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remote Alarm Journal Name   | The remote alarm journal to sync data to.                                                                                                                                                                                                                                                                                                                              |
| Remote Journal Sync Enabled | Whether Remote Alarm Journal settings are enabled. Default is false.                                                                                                                                                                                                                                                                                                   |
| Sync Frequency              | The frequency with which data will be sent to the remote Gateway. This setting will be used in conjunction with the sync schedule, if enabled.                                                                                                                                                                                                                         |
| Sync Frequency Units        | Units are defined as milliseconds, seconds, minutes, hours, days, weeks, months, and years.                                                                                                                                                                                                                                                                            |
| Enable Schedule             | If enabled, the data will only be synchronized during the times specified by the pattern provided.                                                                                                                                                                                                                                                                     |
| Schedule Pattern            | <p>A comma separated list of time ranges that will determine when data will be sent over the network. Accepted formats include am/pm notations, military time, and the use of colons or periods to distinguish the hour from minutes. Minutes are not required. For example, a schedule could look like the following:</p> <div>9:00-15:00, 6pm-1am, 06.30-07.30</div> |

Sync is unique in that if the connection to the remote Ignition Gateway is severed, the Edge Gateway will use its 35 days of storage as a Store and Forward buffer, allowing you to store up to 35 days of data before data is lost. Once the connection is restored, the Edge Gateway will send data over based on the max batch size and data frequency until all previous data is sent.

## Remote Tag Provider

The processes below describe how to set up your remote Tag Provider and allow writing to tags on your Edge server from your Central server. You'll notice during setup that there are many options to customize your remote Tag Provider and security services beyond enabling Read/Write capabilities. See the [Tag Providers](#) and [Security Zones](#) pages for complete configuration information. Before attempting to create a remote Tag Provider, make sure you have a valid [Gateway Network connection](#).

To expose Edge remote tags to your central Gateway:

- 1. Navigate on your central Gateway **Services > Tags**.
- 2. Click **Create Tag Provider +**.

Realtime Tag Providers

View 20

Create Tag Provider +

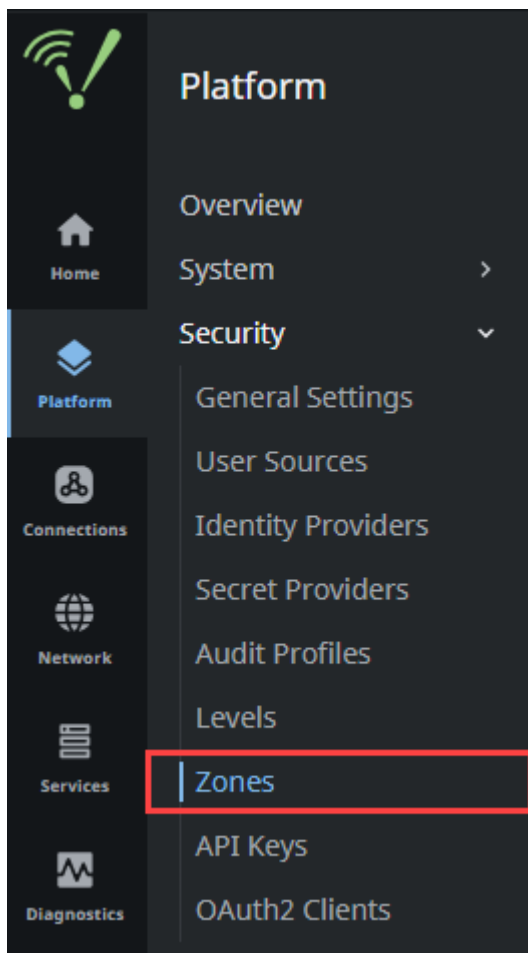
| NAME    | DESCRIPTION          | TYPE     | ENABLED |  |
|---------|----------------------|----------|---------|--|
| default | Default tag provider | Standard | True    |  |

Showing 1 of 1 items

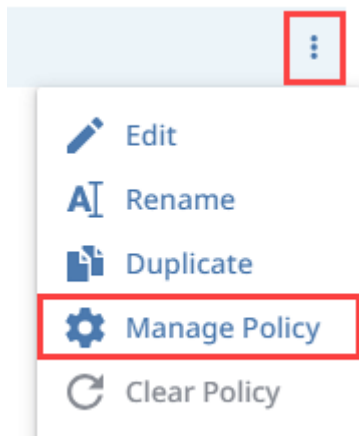
- 3. Select **Remote Tag Provider (Gateway Network)**.
- 4. Click **Next**.
- 5. Enter a name for the Tag Provider.
- 6. Under Remote Gateway, select your Edge Gateway from the Gateway dropdown.
- 7. Customize the Tag Provider settings as desired, including configuring tag read, write, and edit access levels.
- 8. Click **Create Tag Provider**.

To configure system security with Security Zones to allow writing to tags:

- 1. On the Edge Gateway, navigate to **Platform > Security > Zones**.



2. Click the three dots menu and select **Manage Policy** for an Edge Gateway's Security Zone.



### CAUTION

After policies are defined on at least two zones, the Policy setting may need to be configured to ensure your Security Zones are listed in the correct order. If your incoming connection falls into multiple security zones, the one it falls into first is the one that will be used. To update a Policy value, expand the three dots menu and select **Edit**.

3. Scroll down to the Tag Access section to change your Access Level setting to Read/Write.



4. Locate the **Access Level** setting for your Edge Tag Provider and use the dropdown to select **ReadWrite**.

**NOTE**

If you want to enable ReadWrite access for all tags in this security zone, you can select ReadWrite for the Default Provider Access Level setting.

**TAG ACCESS**

**Service Access**  

Select

**Default Profile Access Level**  

Select

**Trust Remote Security Levels**  

If checked, security levels passed from the remote Gateway will be used for determining access to tags on the local Gateway. If unchecked, or if the remote Gateway is on a version which does not support this feature, the remote Gateway's security zones and the impersonation role will be used as the security levels.

☐

**Impersonation Role Name**  

This role name will be injected into the security model of the tag for read/write/subscribe/edit operations.

**Access Level: 'default'**  

ReadWrite

Inherited

None

ReadOnly

ReadWrite

ReadWriteEdit

Cancel

Save Changes

5. Click **Save Changes**.

Follow this same procedure and select **ReadWriteEdit** to allow tags to be edited from a remote Designer.

# Edge IIoT



The Edge IIoT product (formerly known as MQTT) enables an Edge Gateway to publish data directly to an MQTT broker using the fast and lightweight MQTT messaging protocol. This allows the Edge Gateway—and the devices connected to it—to act as a remote MQTT publisher, making it possible to integrate legacy industrial equipment into modern MQTT-based data architectures.

Organizations that are deploying new smart devices that communicate through an MQTT broker can use Edge IIoT to bring existing equipment into the same system. Data collected from PLCs and other industrial devices can be transmitted efficiently to centralized systems, cloud infrastructure, or enterprise applications through the broker.

In addition to MQTT functionality, the IIoT product allows UA clients to connect to the Edge Gateway's OPC UA server, enabling external systems to read data directly from the Edge Gateway when needed.

Edge IIoT activates the following modules:

- MQTT Transmission
- Opto22 SNAP PAC Driver

## Remote Tag Provider

With Edge IIoT installed, Ignition Gateways will be able to **create remote Tag Providers**, targeting either the system provider or the one realtime Tag Provider on an Edge Gateway.

For more information about remote Tag Providers, see [Tag Providers](#).

## Expose Edge's UA Server

The IIoT product enables UA clients to connect to the UA server on Edge. Applying this product will require that the Gateway is restarted before the UA server will be available publicly.

# Install the MQTT Transmission Module

All built-in OPC UA server functionality is directly available. The MQTT Transmission module is required to leverage the third party modules listed on the [Strategic Partner Modules](#) page.

1. Download the MQTT Transmission module from the [Inductive Automation](#) website.

The screenshot shows the Inductive Automation website's 'Download Ignition' page for other operating systems and versions. The page has a dark blue header with the Inductive Automation logo and navigation links: Product, Pricing, Resources, Partners, Support, About, and a 'Download Ignition' button. Below the header, there's a breadcrumb trail: Home / Downloads / Other OS-Versions. The main heading is 'Download Ignition' with the subtitle 'Other operating systems and versions'. There are three tabs: 'Ignition', 'Version Archive', and 'Strategic Partner Modules'. The 'Version Archive' tab is active, showing 'Ignition Version:' with two dropdown menus set to '8.0' and '.9'. Below this, it says 'Ignition Version 8.0.9' with a 'STABLE' badge. There are links for 'Released February 18, 2020', 'System Requirements', and 'Release Notes'. The 'Strategic Partner Modules' section follows, stating that all third-party Ignition modules require the Ignition platform to be installed. It provides instructions on how to install third-party modules, including links to the 'Ignition installation guide' and 'module installation guide'. A table lists three modules: 'MQTT Distributor Module (30.5 MB)', 'MQTT Engine Module (25.7 MB)', and 'MQTT Transmission Module (21.8 MB)'. The 'MQTT Transmission Module' row is highlighted with a red border. The table has columns for the module name, version (all are 4.0.3), and checksum (all are sha-256). Below the table, there's a link to 'See the release notes and usage documentation for all Cirrus Link modules here.'

inductive automation.

Product Pricing Resources Partners Support About Download Ignition

Home / Downloads / Other OS-Versions

## Download Ignition

Other operating systems and versions

Ignition Version Archive Strategic Partner Modules

Ignition Version:

8.0 .9

### Ignition Version 8.0.9 STABLE

Released February 18, 2020 [System Requirements](#) [Release Notes](#)

### Strategic Partner Modules

All third party Ignition modules require the Ignition platform to be installed.

To install third party modules:

1. Install Ignition: [See Ignition installation guide](#)
2. Once Ignition is installed, download the module and install it in the Ignition Gateway: [See module installation guide](#)

| Cirrus Link Solutions MQTT Modules for Ignition                                                  | Version | Checksum                |
|--------------------------------------------------------------------------------------------------|---------|-------------------------|
| See the release notes and usage documentation for all Cirrus Link modules <a href="#">here</a> . |         |                         |
| <a href="#">MQTT Distributor Module (30.5 MB)</a>                                                | 4.0.3   | <a href="#">sha-256</a> |
| <a href="#">MQTT Engine Module (25.7 MB)</a>                                                     | 4.0.3   | <a href="#">sha-256</a> |
| <a href="#">MQTT Transmission Module (21.8 MB)</a>                                               | 4.0.3   | <a href="#">sha-256</a> |

2. Go to the **Platform** tab of your Edge Gateway to access the **System > Modules** page.
3. On the **Modules** page, click on **Install or Upgrade Module +**
4. Click on **Choose file**.

## Install or Upgrade Module



 To **install** a module, choose its \*.modl file and press "Install Module".

To **upgrade** a module, install the new version on top of the existing version.

### Import from file

**Choose File...**

No file selected.

Modules can be downloaded from [our website](#)

Cancel

Install Module

5. Navigate to the folder where you downloaded MQTT-Transmission-signed.modl, select the file, and click **Open**.
6. Click **Install Module**.
7. At the Module Certificate, select **I accept the module certificate**, and click **Accept Certificate**.

## Module Certificate



 **Cirrus Link Solutions LLC**

This certificate has been signed by a trusted Certificate Authority.

Not Valid Until  
Not Valid After  
Subject Name  
Issuer Name

Jun 5, 2023, 5:00:00 PM  
Sep 1, 2026, 4:59:59 PM  
Cirrus Link Solutions LLC  
DigiCert Trusted G4 Code  
Signing RSA4096 SHA384  
2021 CA1  
b3d50508d45e1703dea19b  
80f6cdc3d7030c1f03

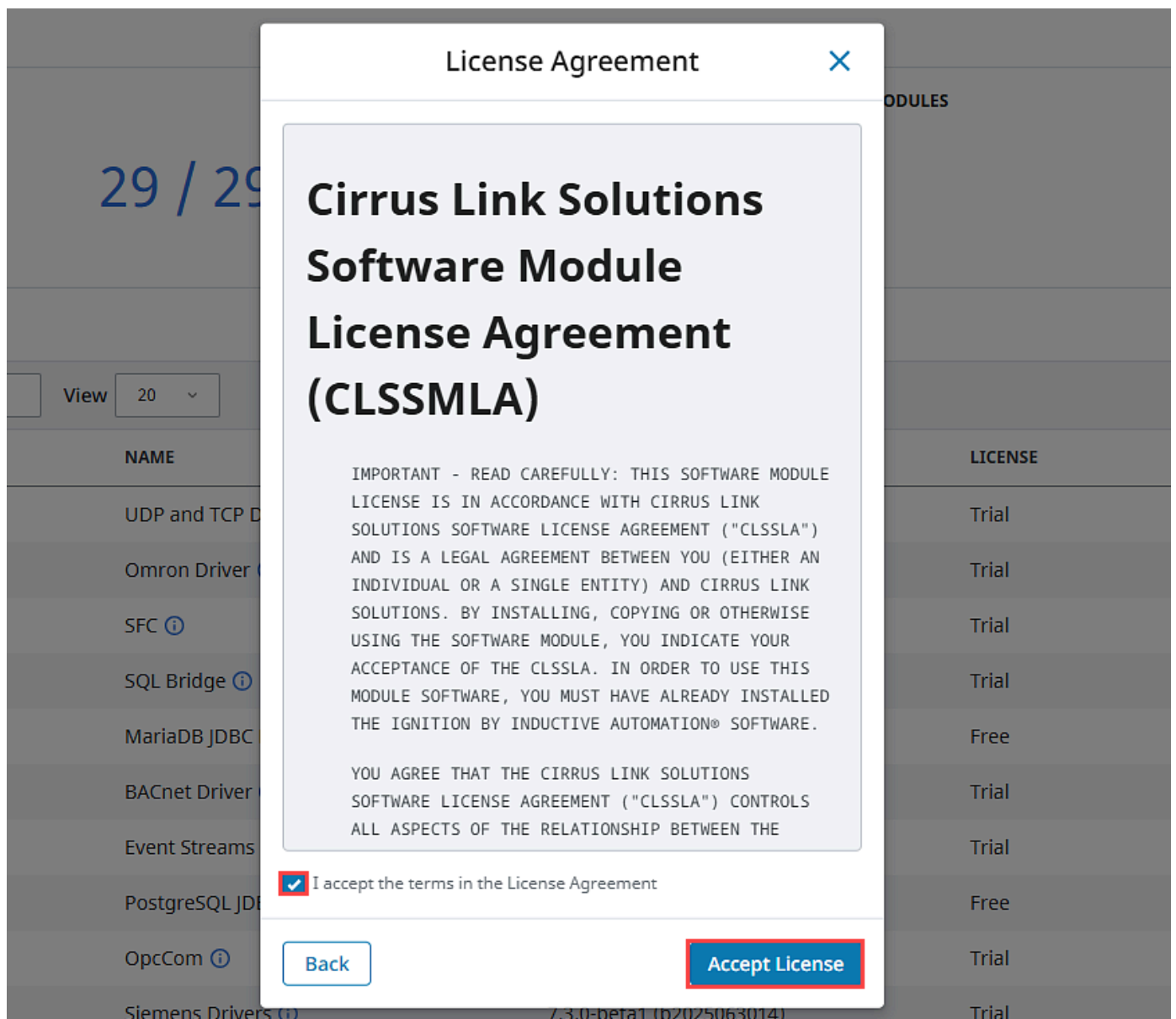
Thumbprint

☒ I accept the module certificate.

Back

Accept Certificate

8. At the License Agreement, select **I accept the terms in the License Agreement**, and click **Accept License**.



You'll see a message indicating the module was successfully installed. The module will show up on the Module page in the Edge Gateway now, and a Gateway Restart Required banner will be displayed on the bottom of the screen so that the module can become Active. For more information, check out the documentation on the Cirrus Link website <https://docs.chariot.io/display/CLD>.

## Install IIoT Opto22 SNAP Pac Driver or the Emerson ROC Driver

To install the Opto22 SNAP Pac driver or Emerson ROC driver:

1. Download the driver you want from the [Inductive Automation](#) website.
2. Go to the **Platform** tab of your Edge Gateway to access the **System > Modules** page.

3. Scroll down and click on **Install or Upgrade a Module +**
4. Next click on **Choose file**.
5. Navigate to the folder where you downloaded the driver(s) and select the file.
6. Click the **Install** button.
7. At the License agreement, select **I accept the terms in the License Agreement**, then click the **Accept License** button.

You'll now see a message indicating the driver module was successfully installed and the module is now available on the Module page in the Edge Gateway, and a Gateway Restart Required banner will be displayed on the bottom of the screen so that the module can become Active.

# Edge Panel



Ignition Edge Panel provides standalone HMI functionality at the edge of the network, allowing operators to visualize and interact with industrial systems locally. An Edge Panel installation supports one local Client running on the same system as the Edge Gateway and one remote Client that can connect from elsewhere on the network.

Edge Panel supports both the **Vision** and **Perspective** visualization modules. An Edge Gateway can run one visualization module at a time, and you can switch between Vision and Perspective by modifying the **Visualization Module** setting on the **Edge Gateway**.

In addition to the Vision and Perspective modules, an Edge Panel license includes the **Symbol Factory** image library, which provides a large collection of industrial graphics for building HMI screens. During the trial period, Ignition Edge Panel is available with a resettable two-hour trial window.

## Visualization Module

An Edge Gateway with the Panel product can launch either Perspective Sessions or Vision Clients, but not both. Ignition Edge Panel comes standard with the **Ignition Designer**.

Licensed Edge Gateways that don't have the product will refuse to launch either runtime. In addition, switching visualization to one module will fault the other, preventing the Designer from accessing resources to the faulted module. This may require a Designer restart.

By default, the visualization module is Vision. To change the visualization module:

1. On the Edge Gateway go to **Platform > System > Ignition Edge**.
2. On the **Edge Settings** tab, scroll down to the **Visualization Module** setting.



The screenshot shows the Ignition Edge configuration interface. On the left, the 'Platform' menu is visible with 'Ignition Edge' selected. The main content area displays the 'Edge Settings' tab. The 'Tag Editing Permissions' section includes a 'Visualization Module' dropdown menu, which is currently set to 'Vision'.

3. Select the visualization module you want (Vision or Perspective) using the dropdown arrow.
4. Click **Save Changes**.

## Running Vision on Panel

When the visualization module is set to Vision, only two Clients are allowed:

- One local Client that must run on the same system as the Edge Gateway.
- One Client that can be launched anywhere on the network.

## Running Perspective on Panel

When the visualization module is set to Perspective, only two Sessions are allowed. Both Sessions can run on remote systems simultaneously. Attempting to open a third Session will cause a message to appear saying that the number of running Sessions has been exceeded.

# Sessions Exceeded

The number of running client sessions has exceeded the permitted number.

LAUNCH GATEWAY

# Ignition Maker Edition



INDUCTIVE  
UNIVERSITY

Getting Started with Maker

[Watch the video](#)

## What Is Ignition Maker Edition?

Ignition Maker Edition is a community version of Inductive Automation's Ignition SCADA application. The Maker Edition enables those who want to explore and get inspired to build and automate their own projects in their home. Ignition Maker Edition is a free-license edition that is strictly available for non-commercial and personal educational use. Users are free to incorporate all of the modules and product features while creating their own projects.

### NOTE

For educational institutions, Inductive Automation has other options for a classroom setting or senior projects. Please contact our [Sales team](#) for more information.



- Home
- Welcome
- Designer >
- Perspective >
- Platform
- Connections
- Network
- Services
- Diagnostics

## Welcome to Ignition

Launch Designer 

| Gateway Overview |             |                 |              | Details |
|------------------|-------------|-----------------|--------------|---------|
| Gateway Name     | Redundancy  | Gateway Version | Gateway Mode |         |
| Ignition-3       | Independent | 8.3.1           | N/A          |         |

### Gateway Notes

[Edit Notes](#)

Welcome to your Ignition Gateway. This customizable area is intended to capture the critical details you want to document for this Gateway. You might include information about the environment (production, testing, or development), key workflows, or maintenance schedules. It's also a great place to list instructions for your team, important reminders about system health, or details about your configuration that require regular review. Use this space to keep everyone informed and ensure smooth operations across the board.

### Downloads



Designer Launcher  
Bring all your data, systems, and developers together into one simple, integrated development environment. [→](#)

# What Can Maker Edition Do?

Maker Edition can do almost anything standard Ignition can do. You can seamlessly connect all your data, design any kind of application with ease, and instantly web-deploy clients to anyone, anywhere — all from one platform.

## How Maker Edition Compares to Standard Edition

Maker Edition differs from Standard Edition Ignition in the following ways:

- Maker licenses are free. Get one now in your [IA account](#).
- Maker Gateways can support a maximum of 10 Perspective sessions.
- The Perspective Workstation is not available for Maker Edition.
- Maker Gateways can run up to 10,000 tags.
- In regards to redundancy, Maker Gateways can only be set to the [Independent](#) mode.
- You can create remote Tag Providers and Tag History Providers when the provider source is a Maker Gateway.

Ignition Maker Edition has limited module support. The table below represents Inductive Automation modules that are ready to use on Maker Gateways. Modules that aren't allowed to run on Maker will be removed during Maker's commissioning process.

| Module Name              | Description                                                                                                    |
|--------------------------|----------------------------------------------------------------------------------------------------------------|
| Alarm Notification       | Provides alarm notifications via email.                                                                        |
| Allen-Bradley Driver     | Allen-Bradley driver suite for the OPC UA module.                                                              |
| Event Streams            | Provides source and handler combinations to receive, filter, and transform event-driven data.                  |
| Historian                | Adds powerful time-series historian functionality.                                                             |
| Kafka Connector          | Allows you to connect to Kafka brokers to process data in real time.                                           |
| Logix Driver             | A driver for communicating with Allen-Bradley Logix5000 series PLCs, and includes firmware version 21 support. |
| Modbus Driver            | A driver for communicating with devices via Modbus-TCP.                                                        |
| Omron Driver             | Drivers for Omron PLCs.                                                                                        |
| OPC UA                   | Provides Ignition's OPC UA client and server functionality.                                                    |
| Perspective              | A module that provides modern, responsive HTML based graphical interfaces for Ignition projects.               |
| Reporting                | Adds reporting capability.                                                                                     |
| Serial Support (Gateway) | Adds platform-level serial comm support and system.serial functions to Gateway-scoped scripts.                 |
| SFC                      | Sequential Function Charts are customizable logic execution environments.                                      |
| Siemens Driver           | Legacy support for Siemens S7-300, S7-400, S7-1200, and S7-1500 drivers with absolute addressing.              |
| Siemens S7 Symbolic      | Support for Siemens S7-300, S7-400, S7-1200, and S7-1500 drivers with absolute and symbolic address options.   |
| SQL Bridge               | An OPC-to-SQL data logger and transaction manager.                                                             |

| Module Name    | Description                                                                                       |
|----------------|---------------------------------------------------------------------------------------------------|
| SQL Historian  | Enables time-series historian functionality to any SQL database in Maker Edition.                 |
| Twilio         | Send SMS or voice alarm notifications without a physical device.                                  |
| UDP/TCP Driver | Drivers for receiving and parsing UDP or TCP packets.                                             |
| Web Dev        | Allows you to create and serve basic web resources and respond to web requests through scripting. |

## Third Party Modules

Module authors can allow their modules to run on Maker Edition. For more information, see the [module's documentation](#).

# Ignition Cloud Edition



INDUCTIVE  
UNIVERSITY

**Ignition Cloud Edition**

[Watch the video](#)

**Ignition Cloud Edition** is a cloud architecture-based version of Ignition. Unlike standard Ignition and Ignition Edge, which are available as installable software on [Inductive Automation's downloads](#) page, Cloud Edition is available through major cloud computing marketplaces such as **Amazon Web Services (AWS)**.

Besides distribution, there are other key differences that distinguish Cloud Edition from standard Ignition or Edge, such as [device connectivity](#) and [module granularity](#).

## Purchasing and Licensing

Unlike previous versions of Ignition, Cloud Edition is purchased through cloud marketplaces and not through Inductive Automation. Cloud Edition will instead detect that it is running in a paid image or container, and therefore already be licensed, negating needing to apply a license key to the Gateway.

**New in 8.3.5** In addition to the existing Cloud Edition image, Cloud Edition is available as a container product on the AWS Marketplace, deployable through Amazon Elastic Kubernetes Service (EKS). The container product follows the same usage-based billing model as the image, with pricing determined by three factors, all of which are billed by the hour:

- A base rate
- The number of CPU cores detected
- The amount of heap memory used in gigabytes

The CPU and memory factors reflect the resource limits applied to the container when running on Amazon Elastic Kubernetes Service (EKS). The costs for these limits are listed on the Cloud Edition Container pricing page, and the limits themselves can be found on the container's Diagnostics Overview page.

When the container is started with a Gateway backup restore, the Gateway runs as Cloud Edition regardless of the edition associated with the backup.

# AWS Partner Solutions

AWS offers automated reference deployments called Partner Solutions. There are two Partner Solutions available:

- Standalone
- Cluster

Both of these Partner Solutions have already been configured with regards to security, Gateway connections, and database connectivity. See the [Ignition by Inductive Automation on AWS](#) reference page for more information.

## Core Functionality

### Cloud Connectors

With Cloud Edition comes a new type of module called **Cloud Connectors**. These new modules are more focused on cloud infrastructure rather than locally installed software. The section below details the various Cloud Connectors available for Cloud Edition.



| Cloud Connector                                                                                        | Description                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <p><b>MongoDB</b></p> | <p>The <b>MongoDB Connector module</b> allows Cloud Edition to connect to a MongoDB NoSQL database deployment. Several MongoDB Cloud Connector features include:</p> <ul style="list-style-type: none"> <li>• Taking aggregates from document data</li> <li>• Inserting, replacing, and deleting collection data</li> <li>• A MongoDB Perspective binding type</li> </ul> |
|  <p><b>Kafka</b></p>  | <p>The <b>Kafka Connector module</b> allows you to process data in real time. With Kafka, you can produce or consume events using <b>event streams</b>.</p>                                                                                                                                                                                                               |

## Redundancy

Two Cloud Edition Gateways can be set up with redundancy. Cloud Edition Gateways will only be able to failover to another Cloud Edition Gateway. It is recommended to set up redundancy between two Cloud Edition Gateways in different Availability Zones in case one Availability Zone fails.

## Module Offerings

Cloud Edition comes standard with many of Inductive Automation's most popular modules, with the main exception being the Vision module. The nature of Cloud Edition makes Perspective's web-based visualization system more suitable for cloud-based infrastructure and helps mitigate potential security risks. The modules that are generally included in Cloud Edition are listed in the table below. For the EKS container product, the listed modules are enabled and running by default.

### NOTE

IA modules that are not included with Cloud Edition cannot be licensed. Third party modules can still be added and licensed on Cloud Edition platforms.

| Module Name                   | Description                                                                                                               |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Alarm Notification            | Provides alarm notifications via email.                                                                                   |
| Cirrus Link MQTT Distributor  | Add an MQTT server that allows MQTT clients to connect to, publish, and subscribe to data.                                |
| Cirrus Link MQTT Engine       | Adds bidirectional communication with edge-of-network devices through an MQTT server.                                     |
| Cirrus Link MQTT Transmission | Publish data from edge of network Tag change events as MQTT messages.                                                     |
| EAM                           | Manage many Gateways from a central Gateway.                                                                              |
| Event Streams                 | Provides source and handler combinations to receive, filter, and transform event-driven data.                             |
| Historian                     | Adds powerful time-series historian functionality.                                                                        |
| Kafka Connector               | A module enabling communication with Kafka.                                                                               |
| MongoDB Connector             | Allows you to connect to non-relational, NoSQL databases.                                                                 |
| OPC UA                        | Provides OPC UA server and OPC UA client functionality. Device drivers are not included in Cloud Edition's OPC-UA module. |
| Perspective                   | A module that provides modern, responsive HTML based graphical interfaces for Ignition projects.                          |
| Reporting                     | Adds reporting capability.                                                                                                |
| SFC                           | Sequential Function Charts are customizable logic execution environments.                                                 |
| SQL Bridge                    | An OPC-to-SQL data logger and transaction manager.                                                                        |
| SQL Historian                 | Enables time-series historian functionality to SQL databases.                                                             |

| Module Name         | Description                                                                                          |
|---------------------|------------------------------------------------------------------------------------------------------|
| Symbol Factory      | Includes almost 4000 Scalable Vector Graphics (SVGs), making designing projects easier and smoother. |
| Twilio Notification | Send SMS or voice alarm notifications without a physical device.                                     |
| Web Dev             | Allows you to create and serve basic web resources and respond to web requests through scripting.    |

## Ignition Cloud Edition Compared with Ignition

Since Ignition Cloud Edition is more focused on cloud architecture compared to the standard version of Ignition, there are some features that differ in Cloud Edition compared to standard Ignition. The following sections detail some of these differences.

### Device Connectivity

Cloud Edition does not include any industrial device drivers to connect directly to PLCs. For security reasons, it is architecturally inadvisable to connect to a PLC or industrial device from a cloud infrastructure. However, MQTT tools are available to publish device telemetry to Cloud Edition.

### Module Granularity

Unlike a standard version of Ignition where you choose which modules you want to include, Cloud Edition comes with a packaged set of modules. See the [Module Offerings section](#) for more information.

### Availability and Commissioning

Since Cloud Edition will be available through major cloud computing platforms, this means that Cloud Edition will not appear as an option in the normal commissioning process during which users select which version of Ignition they are working with.

## Cloud Edition Gateway

In a Cloud Edition installation, there are visual changes to the Gateway, with some pages being different or removed. For example, one of the visual changes include blue Cloud Edition logos instead

of traditional orange Ignition logos. See the [Cloud Edition Gateway](#) page for more information.

## Cloud Edition Behavior with Ubuntu

Starting in Ubuntu 24.04, the `unattended-upgrades` package is enabled by default, with the `needrestart` utility configured to automatically restart services when a related package is patched. If you are running Cloud Edition on an Ubuntu 24.04+ virtual machine, Ignition will be included with these services, causing it to automatically restart if the `needrestart` utility's requirements are met.

While this behavior comes default with Ubuntu, users can opt out by following the steps below to add an exception to the `needrestart` utility.

1. Navigate to `/etc/needrestart/needrestart.conf` in the file system.
2. Add `qr(^ignition\service$) => 0` to the `$nrconf{override_rc}` section.
3. Save the file.

# AMI Access Instructions - AWS

## Prerequisites

Before launching your instance, you will need to configure the instance's network settings and add an inbound security group rule:

1. Under Network Settings, click **Edit**.
2. Verify that you are using the correct VPC and Subnet.
3. Enable **Auto-assign public IP**.
4. Select **Create security group**.
5. Click **Add security group rule**.
6. Set the Type to **HTTP**. This will expose port **80**, one of the default Gateway ports.

### DEFAULT PORTS

Default ports for accessing the Ignition Cloud Gateway are located at ports **80** and **443**.

7. Configure the Source type to specify which IP addresses can access this port.

## Gateway Access

Once you have configured and launched your instance, you can access and commission your new Gateway from the **EC2 Dashboard > Instances**:

1. Select the Ignition Cloud Edition instance.
2. Under the **Details** tab, locate the instance's **Public IPv4 address**.

Reserved Instances

Dedicated Hosts

Scheduled Instances

Capacity Reservations

▼ Images

AMIs

AMI Catalog

▼ Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

▼ Network & Security

Instance: i-0ca3e99c14b00e45f (tchaney-ignition-cloud)

Details | Security | Networking | Storage | Status checks | Monitoring | Tags

▼ Instance summary [Info](#)

Instance ID  
i-0ca3e99c14b00e45f (tchaney-ignition-cloud)

IPv6 address  
-

Hostname type  
IP name: ip-10-0-2-46.us-west-2.compute.internal

Answer private resource DNS name  
-

Public IPv4 address  
54.245.215.77 | [open address](#)

Instance state  
Running

Private IP DNS name (IPv4 only)  
ip-10-0-2-46.us-west-2.compute.internal

Instance type  
t2.medium

3. Copy the address.

4. In a new tab, paste the address and specify port `80`:

```
54.245.215.77:80
```

5. Hit **Enter**.

6. When prompted, choose the username and password for your admin user.

7. Click **Finish Setup**. You will now be redirected to the [Cloud Edition Gateway](#).

Now that you've accessed your Cloud Gateway, you can download the [Designer Launcher](#) and start working on projects. Follow the steps to [add a Designer](#) for your Cloud Gateway just like you would for any other edition of Ignition.

## Creating an EC2 Instance Using the Ignition Cloud Edition AMI

### Launch From AWS Marketplace

1. Go to the [AWS Marketplace](#) and search for **Ignition Cloud Edition**.
2. Select the [Ignition Cloud Edition AMI](#).



### Ignition Cloud Edition

By [Inductive Automation](#) | Ver 8.1.27

Starting from **\$0.91/hr** or from **\$5,200.00/yr** (35% savings) for software + AWS usage fees

Ignition Cloud Edition combines the power of the most effective industrial software and the convenience of the world's most trusted cloud computing services. Cloud Edition is a cloud platform complement to extend your Standard Ignition on-premise platform.

Purchased and installed through the AWS...

3. Once on the Ignition Cloud Edition AMI product page, click on **Continue to Subscribe**.



### Ignition Cloud Edition

By: [Inductive Automation](#) Latest Version: 8.1.27

Ignition Cloud Edition makes it easy to add the power of the cloud to your Ignition on-premise installations. Extend your enterprise operations, leverage elastic

[Show more](#)

Linux/Unix

**Continue to Subscribe**

**Save to List**

Typical Total Price  
**\$2.122/hr**

Total pricing per instance for services hosted on m6i.xlarge in US East (N. Virginia). [View Details](#)

4. You will be prompted to accept the terms of the EULA. Click **Accept Terms**.

By subscribing to this software, you agree to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You also agree and acknowledge that AWS may, on your behalf, share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the [AWS Privacy Notice](#). AWS will issue invoices and collect payments from you on behalf of the seller through your AWS account. Your use of AWS services is subject to the [AWS Customer Agreement](#) or other agreement with AWS governing your use of such services. If you are receiving a private offer from a channel partner, you may click [here](#) (for CPPO transaction) or [here](#) (for SPPO transaction) for more information on the channel partner.

**Accept Terms**

5. After AWS has fulfilled your subscription request, click on **Continue to Configuration**.



## Ignition Cloud Edition

**Continue to Configuration**

6. You will have options to select the fulfillment option, version, and region to launch the software. In most cases, you won't need to change any settings. Make your selections, then click **Continue to Launch**.

# Configure this software

Choose a fulfillment option and software version to launch this software.

Fulfillment option

64-bit (x86) Amazon Machine Image (AMI) ▼

Software version

8.1.27 (Apr 06, 2023) ▼

Region

US East (N. Virginia) ▼

Use of Local Zones or WaveLength infrastructure deployment may alter your final pricing.

**Ami Id:** ami-04f2c8c12fa668110

**Product Code:** egfci1mqqvpcddavghlc958d

[Release notes \(updated April 6, 2023\)](#)

- On the "Launch this software" page, you can quickly set up many essential services your EC2 instance will need to function properly. In this example however, we will select **Launch through EC2** under the Choose Action dropdown, and then click **Launch**.





# Ignition Cloud Edition

[< Product Detail](#) [Subscribe](#) [Configure](#) [Launch](#)

## Launch this software

Review the launch configuration details and follow the instructions to launch this software.

### Configuration details

#### Fulfillment option

64-bit (x86) Amazon Machine Image (AMI)

Ignition Cloud Edition

*running on m6i.xlarge*

#### Software version

8.1.27

#### Region

US East (N. Virginia)

[Usage instructions](#)

### Choose Action

Launch through EC2



Choose this action to launch your configuration through the Amazon EC2 console.

Launch

### NOTE

Although we can directly launch our Cloud Edition EC2 instance from this page, launching from the EC2 service will make it easier to set up other necessary elements, such as a VPC, subnet(s), and more. Additionally, the EC2 console contains other advanced settings you may be interested in configuring.

8. You will be taken to your EC2 Service in a new tab, where you can fill out information about your new EC2 instance. Begin by giving your EC2 instance a name.

## Name and tags [Info](#)

Name

testEC2

[Add additional tags](#)

### NOTE

Since we started creating the EC2 instance from the AWS Marketplace, the **Application and OS Images** section will already be filled out.

9. Select the Instance Type you want your EC2 instance to use. In this example, we are using the default selection of **m6i.xlarge**.

## ▼ Instance type [Info](#)

Instance type

m6i.xlarge

Family: m6i 4 vCPU 16 GiB Memory Current generation: true

☒ All generations

[Compare instance types](#)

The AMI vendor recommends using a m6i.xlarge instance (or larger) for the best experience with this product.

10. Select the key pair you want to use or create a new key pair. Alternatively, you can omit using a key pair, but for security purposes, this is not recommended.

## ▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Proceed without a key pair (Not recommended)

Default value ▼



[Create new key pair](#)

11. Next, configure your network settings. For more information on configuring these settings, see the [Cloud Edition - AWS Networking and Security](#) page.

12. Choose the amount of storage you want for your Root volume and EBS volume(s). You can also add or remove volumes as needed.

## ▼ Configure storage [Info](#)

[Advanced](#)

1x  GiB  ▼ Root volume (Not encrypted)

1x  GiB  ▼ EBS volume (Not encrypted)

[Remove](#)

[Add new volume](#)

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

0 x File systems

[Edit](#)

13. You can set up additional advanced settings under **Advanced details**. Once you are done, go to the **Summary** section to get a quick glimpse at the new EC2 instance's configuration, then click **Launch instance**.

▼ Summary

Number of instances [Info](#)

1

Software Image (AMI)

ignition-cloud-ubuntu-x64-8.1....[read more](#)

ami-04f2c8c12fa668110

Virtual server type (instance type)

m6i.xlarge

Firewall (security group)

New security group

Storage (volumes)

2 volume(s) - 66 GiB

Cancel

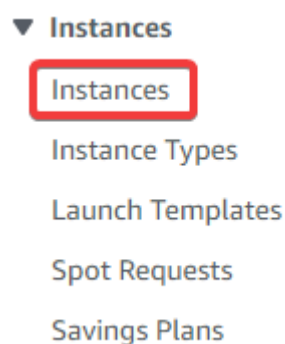
Launch instance

[Review commands](#)

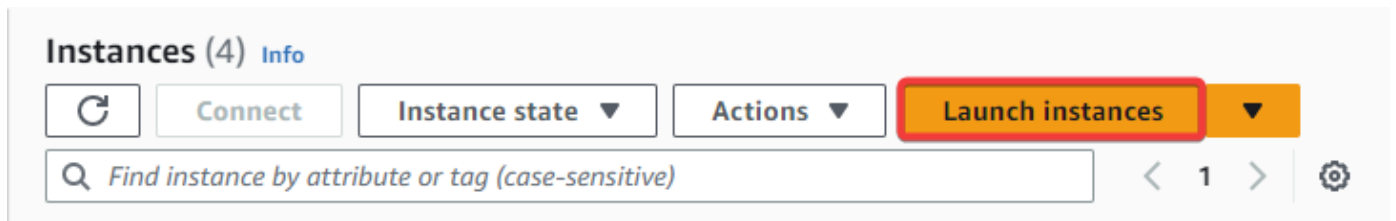
14. AWS will attempt to create your EC2 instance. Once complete, a green Success banner will show at the top of your page. To find your new EC2 instance, go back to the EC2 service in your AWS console, and click on **Instances**.

## Launch From EC2 Service

1. Go to the EC2 Service in your AWS Console.
2. Click on **Instances** under the Instances section.

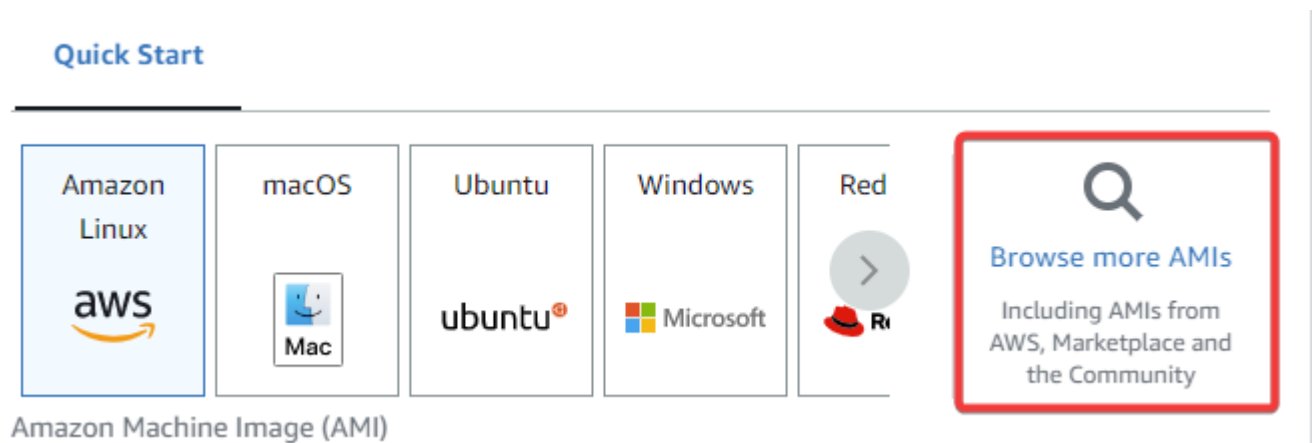


3. Click on **Launch instances**.

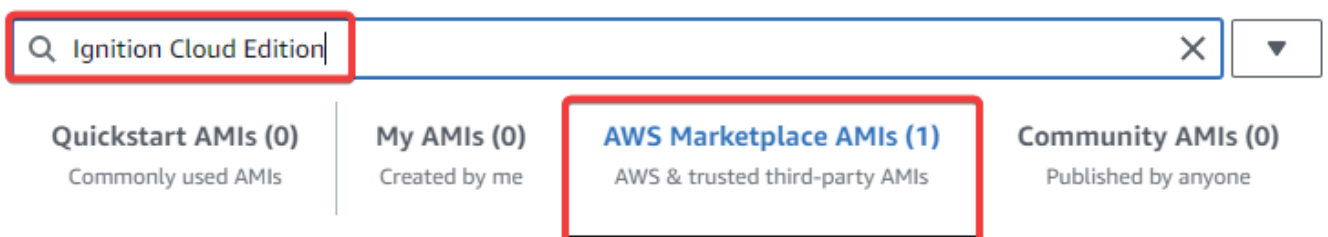


4. You will be taken to a page to fill out information about your new EC2 instance. Start by choosing a name.

5. Next, you will need to select Inductive Automation's Cloud Edition AMI. In the Application and OS Images (Amazon Machine Image) section, click on **Browse more AMIs**.



6. To find the official IA Cloud Edition AMI, enter "Ignition Cloud Edition" in the search bar at the top. The AMI will be listed under **AWS Marketplace AMIs**.



7. Once you have located the Ignition Cloud Edition AMI, click **Select**, then **Continue**.



### Ignition Cloud Edition

By [Inductive Automation](#) | Ver 8.1.27

Starting from \$0.91/hr or from \$5,200.00/yr (35% savings) for software + AWS usage fees

Ignition Cloud Edition combines the power of the most effective industrial software and the convenience of the world's most trusted cloud computing services. Cloud Edition is a cloud platform complement to extend your Standard Ignition on-premise platform. Purchased and installed through the AWS...

Select

8. You will be brought back to the EC2 creation form. From here, select the Instance type you want to use. In this example, we will leave the default selection of **m6i.xlarge**.

#### ▼ Instance type [Info](#)

Instance type

m6i.xlarge

Family: m6i 4 vCPU 16 GiB Memory Current generation: true

☐ All generations

[Compare instance types](#)

The AMI vendor recommends using a m6i.xlarge instance (or larger) for the best experience with this product.

9. Select the key pair you want to use. You can also create a new key pair, or not use a key pair at all. In our example, we will **Proceed without a key pair**.



**TIP**

For security purposes, we recommend that you use a key pair when creating your EC2 instance.

#### ▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

Proceed without a key pair (Not recommended)

Default value ▼



[Create new key pair](#)

10. You will then need to configure your network settings. For more information on configuring these settings, see the [Cloud Edition - AWS Networking and Security](#) page.
11. Configure the amount of storage you want for your Root volume and EBS volume(s). You can also add or remove volumes.

## ▼ Configure storage [Info](#)

[Advanced](#)

1x  GiB  ▼ Root volume (Not encrypted)

1x  GiB  ▼ EBS volume (Not encrypted)

[Remove](#)

[Add new volume](#)

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

0 x File systems

[Edit](#)

12. Configure any advanced settings you'd like under **Advanced details**, then proceed to the **Summary** section. Once you are satisfied with the selections, click **Launch instance**.

## ▼ Summary

Number of instances [Info](#)

[Software Image \(AMI\)](#)

Ignition Cloud Edition  
ami-04f2c8c12fa668110

[Virtual server type \(instance type\)](#)

m6i.xlarge

[Firewall \(security group\)](#)

New security group

[Storage \(volumes\)](#)

2 volume(s) - 66 GiB

[Cancel](#)

[Launch instance](#)

[Review commands](#)

13. AWS will now create your EC2 instance. Once complete, a green Success banner will show at the top of your page. To find your new EC2 instance, go back to the EC2 service in your AWS console, and click on **Instances**.



# Cloud Edition - AWS

## Networking and Security

This page details various networking and security settings you may need to configure for your Cloud Edition EC2 instance.

### Basic Networking and Security Requirements

When creating an EC2 instance and launching Cloud Edition, there are some networking and security configurations you need to define, such as opening the specific ports Ignition uses. See the [Configuring Security Groups](#) section for more details on allowing traffic through ports.

The following is a list of configurable items you typically need when connecting to a Cloud Edition EC2 instance. Note that this is not a comprehensive list; it is meant to show the fundamental features that you need to set up for your EC2 instance. See the official [AWS documentation](#) for a full list of VPC features you can utilize in your architecture.

- Virtual private clouds (VPC)
- Subnet
- IP addressing
- Routing (route tables)
- A way to route traffic

### Examples

The following examples show how to configure the bulleted items in the [Basic Networking and Security Requirements](#) section above. These examples are demonstrative, and may not reflect how you want to configure your own network and security.

#### Virtual Private Clouds (VPC)

Your AWS region will likely have a default VPC. While you can use the default VPC for your EC2 instance, the steps below will help guide you through creating a dedicated VPC.

1. Go to the VPC Service in your AWS Console, and click on **Create VPC**.

Your VPCs (5) Info

↺

Actions ▾

Create VPC

🔍 Filter VPCs

< 1 >

⚙

**NOTE**

In addition to the VPC, you can customize Availability Zones, public and private subnets, endpoints, and more here. In this example however, we will only be configuring the VPC.

2. Configure the VPC settings you want. We are only using an IPv4 CIDR block, and not IPv6, so our configuration below is fine as is. Once you are done, click **Create VPC**.

# Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

## VPC settings

### Resources to create [Info](#)

Create only the VPC resource or the VPC and other networking resources.

☒ VPC only

☐ VPC and more

### Name tag - *optional*

Creates a tag with a key of 'Name' and a value that you specify.

testVPC

### IPv4 CIDR block [Info](#)

☒ IPv4 CIDR manual input

☐ IPAM-allocated IPv4 CIDR block

### IPv4 CIDR

10.0.0.0/24

### IPv6 CIDR block [Info](#)

☒ No IPv6 CIDR block

☐ IPAM-allocated IPv6 CIDR block

☐ Amazon-provided IPv6 CIDR block

☐ IPv6 CIDR owned by me

### Tenancy [Info](#)

Default

## Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

### Key

Q Name



### Value - *optional*

Q testVPC



Remove

Add new tag

You can add 49 more tags.

Cancel

Create VPC

3. You should now be able to select your newly created VPC when creating your EC2 instance.

▼ **Network settings** [Info](#)

VPC - required [Info](#)

vpc-016874e2683e5882a (testVPC)  
10.0.0.0/24 ▲

vpc-016874e2683e5882a (testVPC)  
10.0.0.0/24 ✓

Security group name - required

## Enabling DNS Hostnames and DNS Resolution

If you created your VPC only like in the example above, you may also need to enable DNS hostnames and/or DNS resolution. The steps below show how to enable DNS hostnames and resolution after you create your VPC.

1. Go to the VPC Service in your AWS Console.
2. Select your VPC, then click on **Actions** on the top left, followed by **Edit VPC settings**.

**Your VPCs (1/5)** [Info](#)

| <input type="checkbox"/>            | Name    | VPC ID                |           |
|-------------------------------------|---------|-----------------------|-----------|
| <input type="checkbox"/>            |         |                       |           |
| <input type="checkbox"/>            |         |                       |           |
| <input checked="" type="checkbox"/> | testVPC | vpc-016874e2683e5882a | Available |
| <input type="checkbox"/>            | -       |                       | Available |
| <input type="checkbox"/>            |         |                       | Available |

**Actions** ▲  
Create default VPC  
Create flow log  
**Edit VPC settings**  
Edit CIDRs  
Manage middlebox routes  
Manage tags  
Delete VPC

Create VPC

3. Enable DNS resolution and DNS hostnames, then click **Save**.

### VPC details

|                                                                                                         |                                                                                           |
|---------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| VPC ID                                                                                                  | Name                                                                                      |
|  vpc-016874e2683e5882a |  testVPC |

### DHCP settings

DHCP option set [Info](#)

dopt-0cc275d4f826d9492 ▼

### DNS settings

☒ Enable DNS resolution [Info](#)

☒ Enable DNS hostnames [Info](#)

### Network Address Usage metrics settings

☐ Enable Network Address Usage metrics [Info](#)

Cancel

Save

## Creating Subnets

1. Go to the Subnets Service in your AWS Console.
2. Click on **Create subnet**.

Subnets (11) [Info](#)

 Actions ▼

Create subnet

 Filter subnets

< 1 > 

3. Select the VPC to create the subnet in.

## VPC

### VPC ID

Create subnets in this VPC.

vpc-016874e2683e5882a (testVPC) ▲

Q |

vpc-016874e2683e5882a (testVPC)  
10.0.0.0/24

4. You will be prompted to configure the settings for your subnet. Fill out the form, then click **Create subnet**.

## Subnet 1 of 1

### Subnet name

Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

### Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

### IPv4 CIDR block [Info](#)

### ▼ Tags - optional

Key

Value - optional

You can add 49 more tags.

## Configuring Security Groups (IP Addresses and Ports)

You may need to create inbound or outbound rules in the security group your instance is using to allow network traffic through your firewall.

### NOTE

Ignition Cloud Edition will default to using port 80 if not using SSL and port 443 when using SSL, instead of ports 8088 and 8043, respectively. See the [Gateway Port Reference](#) page for more

information on webserver ports.

## Inbound and Outbound Rules

The following example shows how to configure your security group to allow traffic. While you can configure security group rules when creating an EC2 instance, we will configure rules through the Security Groups console.

### NOTE

Security groups allow all outgoing traffic by default, including incoming traffic in response to outgoing traffic. You will not be able to configure outbound rules when creating a new EC2 instance; however you will be able to configure outbound rules on the security group itself, as demonstrated below.

1. Go to the EC2 Service in your AWS Console.
2. Click on **Security Groups** under the Network & Security section.

#### ▼ Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

### NOTE

You can also set up security groups when creating your EC2 instance.

3. All your available security groups should show up as a list. Click on either the security group ID of the security group you want to modify, or check its checkbox to select it.



| Security Groups (1/7) <a href="#">Info</a>  |        |                      |                       |
|---------------------------------------------|--------|----------------------|-----------------------|
| <input type="text"/> Filter security groups |        |                      |                       |
| <input type="checkbox"/>                    | Name ▾ | Security group ID ▾  | Security group name ▾ |
| <input type="checkbox"/>                    | –      | sg-068e08ccc2fe1e5f4 | default               |
| <input type="checkbox"/>                    | –      | sg-0af0df6e697db993a | launch-wizard-3       |
| <input type="checkbox"/>                    | –      | sg-03ee54ca89bb744e3 | default               |
| <input checked="" type="checkbox"/>         | –      | sg-0c827a04b1141ebde | launch-wizard-4       |
| <input type="checkbox"/>                    | –      | sg-07d41c3b6061990e8 | launch-wizard-2       |
| <input type="checkbox"/>                    | –      | sg-02d23ee73d699e841 | launch-wizard-5       |
| <input type="checkbox"/>                    | –      | sg-04a21d401aa2515e7 | launch-wizard-1       |

4. You should have a few tabs to select from, including **Inbound Rules** and **Outbound Rules**. Click on the tab you want to edit the rules for, and then click on the applicable edit button.

sg-0c827a04b1141ebde - launch-wizard-4

[Details](#)
[Inbound rules](#)
[Outbound rules](#)
[Tags](#)

Inbound rules (4)

Filter security group rules

| <input type="checkbox"/> | Name ▾ | Security group rule... ▾ | IP version ▾ | Type ▾     |
|--------------------------|--------|--------------------------|--------------|------------|
| <input type="checkbox"/> | –      | sgr-02b905d9f31212c98    | IPv4         | Custom TCP |
| <input type="checkbox"/> | –      | sgr-03948004d796d0...    | IPv4         | SSH        |
| <input type="checkbox"/> | –      | sgr-0a2f47d60b741accb    | IPv4         | HTTP       |
| <input type="checkbox"/> | –      | sgr-0c64c7bbd54129a...   | IPv4         | HTTPS      |

5. Configure, add, remove, or modify your rules. Once you are finished, click on **Save rules**.

| Security group rule ID | Type <small>Info</small> | Protocol <small>Info</small> | Port range <small>Info</small> | Source <small>Info</small>                      | Description - optional <small>Info</small> |        |
|------------------------|--------------------------|------------------------------|--------------------------------|-------------------------------------------------|--------------------------------------------|--------|
| sgr-02b905d9f31212c98  | Custom TCP ▼             | TCP                          | 8060                           | Custom ▼ <input type="text" value="0.0.0.0/0"/> |                                            | Delete |
| sgr-03948004d796d0b9c  | SSH ▼                    | TCP                          | 22                             | Custom ▼ <input type="text" value="0.0.0.0/0"/> |                                            | Delete |
| sgr-0a2f47d60b741accb  | HTTP ▼                   | TCP                          | 80                             | Custom ▼ <input type="text" value="0.0.0.0/0"/> |                                            | Delete |
| sgr-0c64c7bbd54129a56  | HTTPS ▼                  | TCP                          | 443                            | Custom ▼ <input type="text" value="0.0.0.0/0"/> |                                            | Delete |

### NOTES

- The screenshot above shows a rule configuration where all IP traffic is allowed. For security purposes, we recommend configuring your rules to allow only trusted IP addresses.
- A Custom TCP rule is required to allow Gateway Network traffic, which uses port 8060.

6. Your security group should now be using the updated rules and allow traffic flow through the specified ports.

## Route Tables

Route tables are created automatically when you create your VPC. You can also create multiple custom route tables for a single VPC.

1. Go to the Route tables service in your AWS Console
2. Click on **Create route table**.

**Route tables (4)** Info


**Actions** ▼

< 1 >
 

3. You will be prompted to give your route table an optional name and select the VPC to use for your route table. Complete the form and click on **Create route table**.

### Route table settings

Name - *optional*  
Create a tag with a key of 'Name' and a value that you specify.

testRouteTable

VPC  
The VPC to use for this route table.

vpc-016874e2683e5882a (testVPC) ▲

Q

vpc-016874e2683e5882a (testVPC) ✓

Q Name X Q testRouteTable X

Remove

Add new tag

You can add 49 more tags.

Cancel Create route table

## Internet Gateway

Internet gateways allow traffic and communication between your VPC and the internet.

### NOTE

This example uses internet gateways, which are easy to set up but may be less secure than other options. For security purposes, you may want to explore different methods of connecting to the internet. See the [official AWS documentation](#) for connectivity options.

1. Go to the Internet gateway service in your AWS Console.
2. Click on **Create internet gateway**.

**Internet gateways (2)** [Info](#)

 **Actions** ▼ **Create internet gateway**

< 1 > 

3. Name your internet gateway, then click **Create internet gateway**.

**Internet gateway settings**

**Name tag**  
Creates a tag with a key of 'Name' and a value that you specify.

**Tags - optional**  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

**Key**

**Value - optional**

**Remove**

**Add new tag**  
You can add 49 more tags.

**Cancel** **Create internet gateway**

4. Your internet gateway is now created, but is detached from your VPC. To attach your internet gateway, go back to the Internet gateway service.
5. Select your internet gateway, then click on **Actions**, followed by **Attach to VPC**.

The screenshot shows the AWS Internet Gateways console. At the top, there's a header 'Internet gateways (1/3)' with an 'Info' link and a refresh button. To the right is a 'Create internet gateway' button. Below the header is a search bar labeled 'Filter internet gateways'. A table lists the internet gateways. The first row, 'testInternetGateway' with ID 'igw-03eed4d0fe2a2203b', is selected (checkbox checked) and its state is 'Detached'. The context menu for this gateway is open, showing options: 'View details', 'Attach to VPC' (highlighted with a red box), 'Detach from VPC', 'Manage tags', and 'Delete internet gateway'. Other gateways in the list include an unnamed one with ID 'igw-059bf1dcc8ae05b24' (Attached) and 'baulGW' with ID 'igw-09d166cf1f1b2bc3b' (Attached).

|                                     | Name                | Internet gateway      | State    |
|-------------------------------------|---------------------|-----------------------|----------|
| <input checked="" type="checkbox"/> | testInternetGateway | igw-03eed4d0fe2a2203b | Detached |
| <input type="checkbox"/>            | -                   | igw-059bf1dcc8ae05b24 | Attached |
| <input type="checkbox"/>            | baulGW              | igw-09d166cf1f1b2bc3b | Attached |

6. Select the VPC you want to attach the internet gateway to, then click **Attach internet gateway**.

The screenshot shows the 'Attach internet gateway' dialog box. The title is 'VPC' with a subtitle: 'Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.' Under 'Available VPCs', there's a search bar 'Select a VPC'. Below it is a list of VPCs. The first VPC, 'vpc-016874e2683e5882a - testVPC', is selected and highlighted with a red box. At the bottom right, there are 'Cancel' and 'Attach internet gateway' buttons.

## Creating a Gateway Network (AWS Instances)

After configuring your security group's inbound and outbound rules, ports, network and security, you can create a Gateway Network with two Cloud Edition Gateways hosted on AWS.

1. Go to the EC2 Service in your AWS Console.
2. Click on **Instances** under the Instances section.

▼ Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

3. Select the target AWS instance you want to connect to by clicking on the target's checkbox. Information about the instance should populate on the bottom.

| Instances (1/4) Info                               |                     |                     |                  |
|----------------------------------------------------|---------------------|---------------------|------------------|
| Find instance by attribute or tag (case-sensitive) |                     |                     |                  |
|                                                    | Name ▼              | Instance ID         | Instance state ▼ |
| <input type="checkbox"/>                           | Ignition-Test-2     | i-01aa62aa8dbd1e8ea | Running          |
| <input type="checkbox"/>                           | ignition-test-bau-2 | i-0d1bdb35653860874 | Running          |
| <input type="checkbox"/>                           | Ignition-Test       | i-02a325f5a02817257 | Running          |
| <input checked="" type="checkbox"/>                | ignition-test-bau   | i-01821a4fb385e4d2b | Running          |

4. On the **Details** tab, make a note of your target Gateway's IP address, then go to the Gateway you want to make the outgoing connection from.

**Instance: i-01821a4fb385e4d2b (ignition-test-bau)**

Details

Security

Networking

Storage

Status checks

Monitoring

Tags

▼ Instance summary Info

|                                         |                                                   |
|-----------------------------------------|---------------------------------------------------|
| Instance ID                             | Public IPv4 address                               |
| i-01821a4fb385e4d2b (ignition-test-bau) | <input type="text"/> <a href="#">open address</a> |
| IPv6 address                            | Instance state                                    |
| —                                       | Running                                           |

5. On the Gateway that will be making the outgoing connection, go to the Gateway webpage's **Config** page > **Networking** > **Gateway Network** > **Outgoing Connections** > **Create new Outgoing Gateway Connection...**

| General Settings                                            |      | Outgoing Connections | Incoming Connections | Diagnostics  | Queue Management |        |
|-------------------------------------------------------------|------|----------------------|----------------------|--------------|------------------|--------|
| Host                                                        | Port | Enabled              | Description          | Gateway Name | Redundancy Role  | Status |
| No Outgoing Gateway Connections                             |      |                      |                      |              |                  |        |
| <a href="#">→ Create new Outgoing Gateway Connection...</a> |      |                      |                      |              |                  |        |

6. Fill out the Gateway Network Settings page using the information you gathered from your AWS instance, then click **Create New Outgoing Gateway Connection**.

Main

Host

The address of the remote server, not including the port.

Port

8000

HTTP Read Timeout

60000

The maximum time, in milliseconds, allowed to read or send HTTP data to a remote machine.  
(default: 60,000)

**Create New Outgoing Gateway Connection**

7. After setting up your Outgoing Connection, navigate to the target Gateway's **Config** page > **Networking** > **Gateway Network** > **Incoming Connections**. The target Gateway should have an Incoming Connection request from the outbound Gateway. Click on **approve** to approve the certificate, then **Confirm**.

General Settings

Outgoing Connections

Incoming Connections

Diagnostics

Queue Management

Remote Certificates

| Common Name | Serial | Issuer | Status       |                                      |
|-------------|--------|--------|--------------|--------------------------------------|
| :8060       |        | Self   | Not Approved | <div>approve</div> <div>delete</div> |

| Id                              | Security | Certificate | Gateway Name | Redundancy Role | Status |
|---------------------------------|----------|-------------|--------------|-----------------|--------|
| No Incoming Gateway Connections |          |             |              |                 |        |

→

- The outbound Gateway will now show up under the certificate. Click on **More**, then **approve**, then **Confirm**.
- The Gateway will take a few seconds to establish the connection. If you run into any issues creating your Gateway Network, contact the [Support Department](#).



# Image Access Instructions - Azure

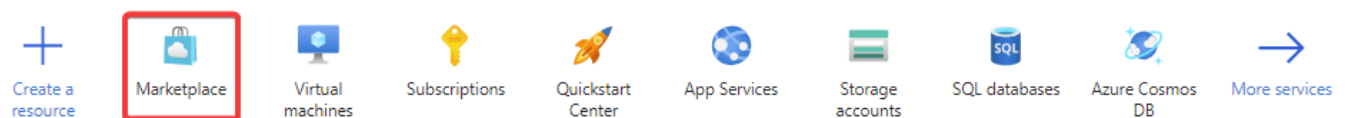
## Creating a Virtual Machine Using the Ignition Cloud Edition Image

Similar to AWS, you can create a virtual machine (VM) using the Cloud Edition Image available on the Azure Marketplace. The instructions below demonstrate how to create an Azure virtual machine running Cloud Edition.

### Create a Virtual Machine from the Azure Marketplace Listing

1. Access your Azure console.
2. Click on **Marketplace**.

#### Azure services

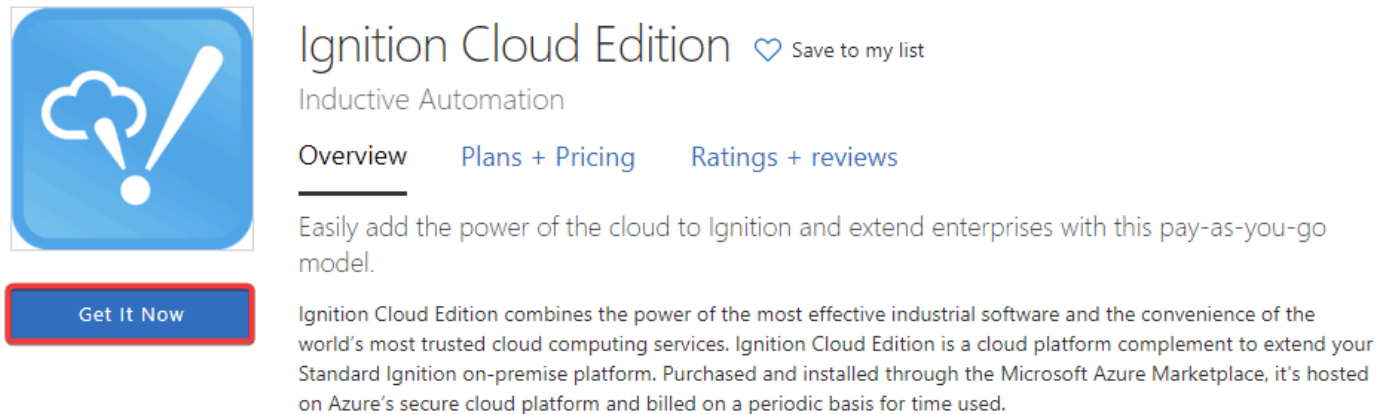


3. In the Azure Marketplace, search for "Ignition Cloud Edition". Click on the **Ignition Cloud Edition** image.



If you've created a virtual machine from the Ignition Cloud Edition Image before, steps 4 and 5 may not appear. In this case, skip to step 6.

4. On the Ignition Cloud Edition page, click **Get it Now**.



**Ignition Cloud Edition** [Save to my list](#)

Inductive Automation

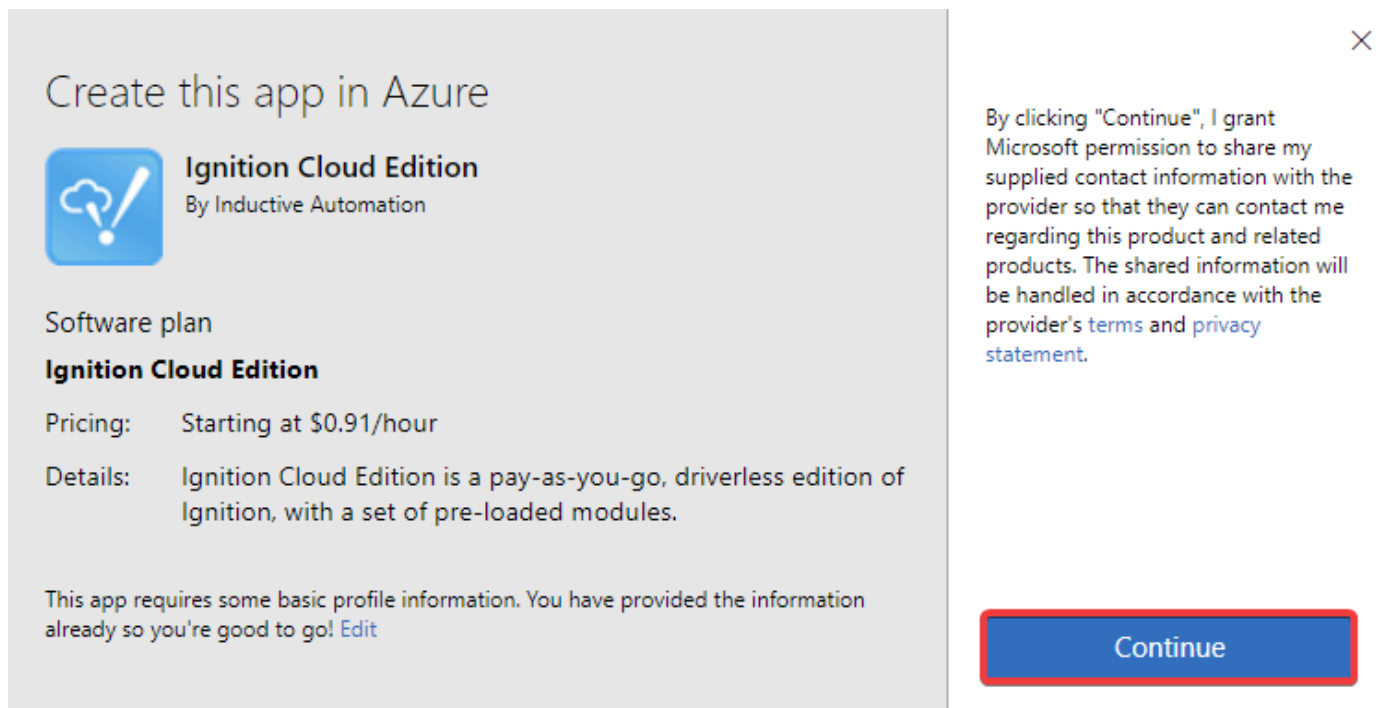
[Overview](#) [Plans + Pricing](#) [Ratings + reviews](#)

Easily add the power of the cloud to Ignition and extend enterprises with this pay-as-you-go model.

**Get It Now**

Ignition Cloud Edition combines the power of the most effective industrial software and the convenience of the world's most trusted cloud computing services. Ignition Cloud Edition is a cloud platform complement to extend your Standard Ignition on-premise platform. Purchased and installed through the Microsoft Azure Marketplace, it's hosted on Azure's secure cloud platform and billed on a periodic basis for time used.

5. Click **Continue** on the Azure popup.



Create this app in Azure

**Ignition Cloud Edition**  
By Inductive Automation

Software plan

**Ignition Cloud Edition**

Pricing: Starting at \$0.91/hour

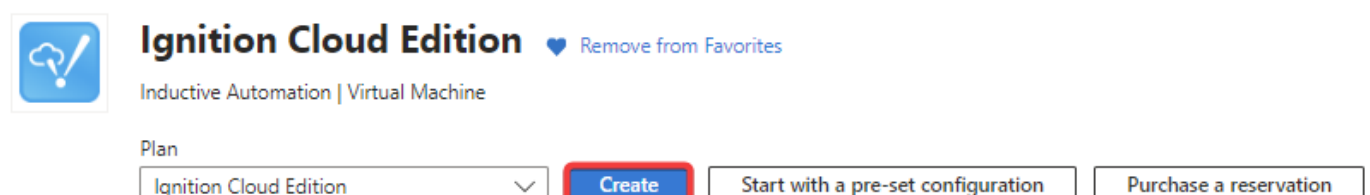
Details: Ignition Cloud Edition is a pay-as-you-go, driverless edition of Ignition, with a set of pre-loaded modules.

This app requires some basic profile information. You have provided the information already so you're good to go! [Edit](#)

By clicking "Continue", I grant Microsoft permission to share my supplied contact information with the provider so that they can contact me regarding this product and related products. The shared information will be handled in accordance with the provider's [terms](#) and [privacy statement](#).

**Continue**

6. Click **Create** on the information page.



**Ignition Cloud Edition** [Remove from Favorites](#)

Inductive Automation | Virtual Machine

Plan

Ignition Cloud Edition [Create](#) [Start with a pre-set configuration](#) [Purchase a reservation](#)

7. You will be taken to the **Create a virtual machine** page. Complete the prompts to create your VM. For specific guidance through this form, see the [Virtual Machine Creation Process Example](#) section below. Once complete, click on **Review + create**.

8. Azure will begin creating your requested resources. After your resources are finished building, click on **Go to resource** under **Next steps** to go to your VM overview.

 Delete  Cancel  Redeploy  Download  Refresh

## ✓ Your deployment is complete

Deployment name: CreateVm-inductiveautomationllc16752682122...

Subscription: [Training Division](#)

Resource group: [ignitioncloud-build-training-rg](#)

Start time: 8/15/2023, 12:21:48 PM

Correlation ID: 7eee6c7f-57f8-4afe-9bd7-9df1f9ce8d4d 

∨ Deployment details

∧ Next steps

[Setup auto-shutdown](#) Recommended

[Monitor VM health, performance and network dependencies](#) Recommended

[Run a script inside the virtual machine](#) Recommended

[Go to resource](#)

[Create another VM](#)

## Create a Virtual Machine From Your Recently Created

### NOTE

This method assumes that you have already created a previous virtual machine using the Azure Marketplace Cloud Edition Image.

1. Access your Azure console.
2. Click on **More services**.

#### Azure services

  
[Create a resource](#)

  
Virtual machines

  
Subscriptions

  
Quickstart Center

  
App Services

  
Storage accounts

  
SQL databases

  
Azure Cosmos DB

  
Kubernetes services

  
[More services](#)

3. Click **Marketplace** under the General section.

## General (24)



All resources



Deploy a custom template



Management groups



Marketplace



Recent

- Click on **Recently created** in the My Marketplace section.

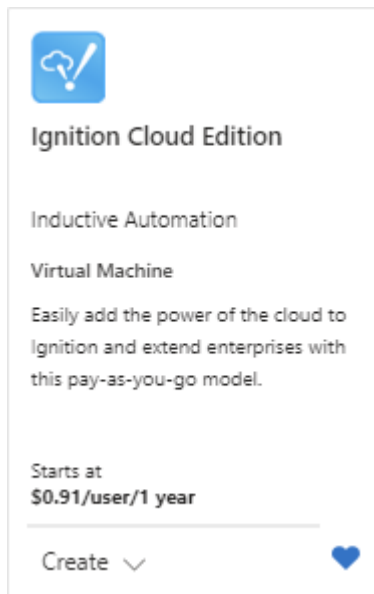
### My Marketplace

Favorites

Recently created

Private plans

- Click on the **Ignition Cloud Edition** image.



- On the Image Description page, click **Create**. This will open a wizard for you to enter details about your new VM.



## Ignition Cloud Edition [Remove from Favorites](#)

Inductive Automation | Virtual Machine

Plan

Ignition Cloud Edition

Create

Start with a pre-set configuration

Purchase a reservation

Want to deploy programmatically? [Get started](#)

7. Complete the prompts to create your VM. For specific guidance through this form, see the [Virtual Machine Creation Process Example](#) section below. Once complete, click on **Review + create**.

### NOTE

Since we started creating the VM from the image that is already located in our Subscription, we do not need to manually select a Subscription or Resource Group during this process.

8. Azure will begin creating your requested resources. After your resources are finished building, click on **Go to resource** under **Next steps** to go to your VM overview.

Delete Cancel Redeploy Download Refresh

## Your deployment is complete



Deployment name : CreateVm-8.1.27-20230622110131

Subscription : [Training Division](#)

Resource group : [ignitioncloud-build-training-rg](#)

Start time : 6/22/2023, 12:53:47 PM

Correlation ID : be8b14c9-0570-4937-b709-e8a869c032eb

> Deployment details

✓ Next steps

Go to resource

9. From the VM overview page, copy the public IP address and paste it in a different tab to access the Gateway.

## Virtual Machine Creation Process Example

This section demonstrates how to configure various settings when creating your VM.

1. The **Basics** page contains many fundamental properties, explained below.

- i. Begin by selecting your Subscription and Resource Group in the **Project details** section.

#### Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

|                    |                                   |
|--------------------|-----------------------------------|
| Subscription * ⓘ   | Training Division ▼               |
| Resource group * ⓘ | ignitioncloud-build-training-rg ▼ |

[Create new](#)

- ii. In the **Instance details** section, fill out the required fields (name, region, image, and size), and configure any other settings you'd like. The image you select should be called **Ignition Cloud Edition**.

#### Instance details

|                          |                                                                                                                         |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Virtual machine name * ⓘ | test-example ✓                                                                                                          |
| Region * ⓘ               | (US) West US 3 ▼                                                                                                        |
| Availability options ⓘ   | No infrastructure redundancy required ▼                                                                                 |
| Security type ⓘ          | Standard ▼                                                                                                              |
| Image * ⓘ                |  Ignition Cloud Edition - x64 Gen2 ▼ |

[See all images](#) | [Configure VM generation](#)

|                   |                                                                                                                                     |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| VM architecture ⓘ | <input type="radio"/> Arm64                                                                                                         |
|                   | <input checked="" type="radio"/> x64                                                                                                |
|                   |  Arm64 is not supported with the selected image. |

|                                |                                                             |
|--------------------------------|-------------------------------------------------------------|
| Run with Azure Spot discount ⓘ | <input type="checkbox"/>                                    |
| Size * ⓘ                       | Standard_DS1_v2 - 1 vcpu, 3.5 GiB memory (\$705.91/month) ▼ |

[See all sizes](#)

- iii. In the **Administrator account** section, you can choose what kind of authentication you want to use, along with other security features.

### Administrator account

Authentication type ⓘ

☒ SSH public key

☐ Password

**i** Azure now automatically generates an SSH key pair for you and allows you to store it for future use. It is a fast, simple, and secure way to connect to your virtual machine.

Username \* ⓘ

testExampleUser ✓

SSH public key source

Generate new key pair ▼

Key pair name \*

test-example\_key ✓

2. The **Disks** page will allow you to configure various storage elements, such as encryption and adding more data disks. The only settings we will change in this example are checking both **Delete with VM** settings to be true.

### VM disk encryption

Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.

Encryption at host ⓘ

☐

**i** Encryption at host is not registered for the selected subscription.  
[Learn more about enabling this feature](#) ↗

### OS disk

OS disk type \* ⓘ

Premium SSD (locally-redundant storage) ▼

Delete with VM ⓘ

☒

Key management ⓘ

Platform-managed key ▼

Enable Ultra Disk compatibility ⓘ

☐

Ultra disk is not supported for the selected VM size Standard\_DS1\_v2 in West US 3.

### Data disks for test-example

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

| LUN | Name                   | Size (GiB) | Disk type | Host caching | Delete with VM ⓘ                    |
|-----|------------------------|------------|-----------|--------------|-------------------------------------|
| 0   | Pre-defined by the ... |            |           | None ▼       | <input checked="" type="checkbox"/> |

[Create and attach a new disk](#)

[Attach an existing disk](#)

3. The **Networking** page will allow you to do things such as create a virtual network, subnets, and more.

- You can select your virtual network and configure other networking properties in the **Network interface** section. In this example, we will create a virtual network only.

### NOTE

If you are using this virtual machine for demonstrative or testing purposes, we recommend enabling the Delete public IP and NIC when VM is deleted setting.

#### Network interface

When creating a virtual machine, a network interface will be created for you.

|                                                                                                                                        |                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Virtual network *                                                                                                                      | <div>(new) testExampleVirtualNetwork</div> <div>Create new</div>                                                                  |
| Subnet *                                                                                                                               | <div>(new) default (10.2.0.0/24)</div>                                                                                            |
| Public IP                                                                                                                              | <div>(new) test-example-ip</div> <div>Create new</div>                                                                            |
| NIC network security group                                                                                                             | <div><input type="radio"/> None</div> <div><input type="radio"/> Basic</div> <div><input checked="" type="radio"/> Advanced</div> |
| <div> This VM image has preconfigured NSG rules</div> |                                                                                                                                   |
| Configure network security group *                                                                                                     | <div>(new) test-example-nsg</div> <div>Create new</div>                                                                           |
| Delete public IP and NIC when VM is deleted                                                                                            | <input checked="" type="checkbox"/>                                                                                               |
| Enable accelerated networking                                                                                                          | <input checked="" type="checkbox"/>                                                                                               |

### NOTE

The Azure Marketplace Image listing will preconfigure ports 80 and 443 (needed to access the Gateway via non-SSL and SSL, respectively) to already be open as inbound rules.

- ii. The **Load balancing** section will allow you to configure a load balancer to help with network traffic. In our example, we will leave this blank.

#### Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Place this virtual machine behind an existing load balancing solution? ☐

4. The **Management** page will allow you to configure authentication features, auto-shutdown, and more. We do not need to modify any settings here so each setting for our example will be default.



## Microsoft Defender for Cloud

Microsoft Defender for Cloud provides unified security management and advanced threat protection across hybrid cloud workloads. [Learn more](#)

✔ Your subscription is protected by Microsoft Defender for Cloud basic plan.

### Identity

Enable system assigned managed identity ⓘ

☐

### Azure AD

Login with Azure AD ⓘ

☐

⚠ This image does not support Login with Azure AD.

### Auto-shutdown

Enable auto-shutdown ⓘ

☐

### Guest OS updates

Patch orchestration options ⓘ

ⓘ Some patch orchestration options are not available for this image. [Learn more](#)

5. Next is the **Monitoring** page, in which you can set up alerts and diagnostics information. Similar to the Management page, our example will not change any of these settings.

### Alerts

Enable recommended alert rules ⓘ

☐

### Diagnostics

Boot diagnostics ⓘ

- ☒ Enable with managed storage account (recommended)  
☐ Enable with custom storage account  
☐ Disable

Enable OS guest diagnostics ⓘ

☐

6. After Monitoring, the **Advanced** page contains more specialized properties, which are explained below.

- i. **Extensions** allow you to add new features such as antivirus software, after the VM has already been deployed. See [Microsoft's documentation on extensions](#).

## Extensions

Extensions provide post-deployment configuration and automation.

Extensions ⓘ

[Select an extension to install](#)

- ii. **VM applications** contain files you can download and install on your virtual machine. One benefit of using a VM application is allowing users to update programs on the VM without also needing to also update the VM itself. You can read more about VM applications on [Microsoft's official documentation](#).

### VM applications

VM applications contain application files that are securely and reliably downloaded on your VM after deployment. In addition to the application files, an install and uninstall script are included in the application. You can easily add or remove applications on your VM after create. [Learn more](#) ↗

[Select a VM application to install](#)

- iii. **Custom data** gives users the ability to pass scripts or other data to the virtual machine as the VM is being provisioned. More information about custom data can be found on [Microsoft's official documentation](#).

### Custom data

Pass a script, configuration file, or other data into the virtual machine **while it is being provisioned**. The data will be saved on the VM in a known location. [Learn more about custom data for VMs](#) ↗

Custom data



**i** Your image must have a code to support consumption of custom data. If your image supports cloud-init, custom-data will be processed by cloud-init. [Learn more about custom data for VMs](#) ↗

- iv. The **User data** field is similar to the custom data field, with the main difference being that user data can be accessed until the VM is deleted. See [Microsoft's documentation on user data](#).

### User data

Pass a script, configuration file, or other data that will be accessible to your applications **throughout the lifetime of the virtual machine**. Don't use user data for storing your secrets or passwords. [Learn more about user data for VMs](#) ↗

Enable user data

☐

- v. The **Performance (NVMe)** section improves the disk performance of your VM when the **Higher remote disk storage performance** option is enabled. See [Microsoft's](#)

[documentation](#) on when this setting can be utilized.

### Performance (NVMe)

Enable capabilities to enhance the performance of your resources.

Higher remote disk storage performance with NVMe ☐ ⓘ

**i** The selected image and size are not supported for NVMe. [See supported VM images and sizes](#) ↗

vi. The **Hosts**, **Capacity Reservations**, and **Proximity Placement Group** sections allow you to configure various settings to isolate and reserve resources.

### Host

Azure Dedicated Hosts allow you to provision and manage a physical server within our data centers that are dedicated to your Azure subscription. A dedicated host gives you assurance that only VMs from your subscription are on the host, flexibility to choose VMs from your subscription that will be provisioned on the host, and the control of platform maintenance at the level of the host. [Learn more](#) ↗

Host group ⓘ

No host groups found

### Capacity reservations

Capacity reservations allow you to reserve capacity for your virtual machine needs. You get the same SLA as normal virtual machines with the security of reserving the capacity ahead of time. [Learn more](#) ↗

Capacity reservation group ⓘ

None

### Proximity placement group

Proximity placement groups allow you to group Azure resources physically closer together in the same region. [Learn more](#) ↗

Proximity placement group ⓘ

No proximity placement groups found

- [Click here](#) for Microsoft's documentation on Hosts.
- [Click here](#) for Microsoft's documentation on Capacity Reservation.
- [Click here](#) for Microsoft's documentation on Proximity Placement Groups.

7. Finally, the **Tags** page will help you organize and consolidate various resources. See [Microsoft's recommendations on using tags](#) for more information.

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#) ↗

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

| Name ⓘ               | Value ⓘ | Resource                         |
|----------------------|---------|----------------------------------|
| <input type="text"/> | :       | <input type="text"/> 13 selected |

Below is a list of available resource tags:

- Auto-shutdown schedule
- Availability set
- Disk
- Network Interface
- Network security group
- Public IP address
- Recovery Services vault
- SQL Virtual Machine
- SSH key
- Storage account
- Virtual machine
- Virtual machine extension
- Virtual network

8. Once you have finished configuring your virtual machine, go to the **Review + Create** page. Azure will attempt to validate your settings and display a banner at the top of the page once validation is complete. Go through the summary of settings on this page. If you are satisfied with your choices, click the **Create** button.

# Cloud Edition - Azure Networking and Security

This page details various networking and security settings you may need to configure for your Cloud Edition virtual machine.

## Basic Networking and Security Requirements

The following is a list of configurable items you need when connecting to a Cloud Edition virtual machine. Note that this is not a comprehensive list; it is meant to show the fundamental features that you need to set up for your virtual machine. See the official [Azure documentation](#) for a list of networking features you can utilize in your architecture.

- Virtual network
- Subnet
- Network Security Group (NSG)
- Public IP

### NOTE

The virtual network and available subnets are configured during the same process on Azure.

Additionally, you will need to allow traffic through your firewall to the `*.microsoft.com` and `*.digicert.com` domains if you are using port 80 or 443. Without this, your Gateway will go into trial mode.

## Examples

The following examples show how to configure the bulleted items in the Basic Networking and Security Requirements section above. Each example demonstrates how to create their respective resources through both the virtual machine creation wizard and Azure services. These examples are demonstrative, and may not reflect how you want to configure your own network and security.

# Creating a Virtual Network

You can create a virtual network during the virtual machine creation process or through Azure services.

## Virtual Network - Virtual Machine Creation Process

1. Begin by accessing the **Create a virtual machine** wizard. You can find instructions on creating your virtual machine on the [Image Access Instructions - Azure](#) page.
2. Complete the wizard steps until you reach the **Networking** page. Note that the virtual network field is already filled out, using your virtual machine name as part of the name of the virtual network.

### NOTE

If you selected a Resource Group on the **Basics** page, Azure will attempt to use a pre-existing virtual network originating from the chosen Resource Group.

#### Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network \* 

(new) testExampleVM-vnet

[Create new](#)

3. From here, you could also choose another virtual network to use or configure the new virtual network. If you want to configure the new virtual network, click **Create new**. This will allow you to specify a different address range and subnet(s). In this example, we will use the default address range and subnet.

Name \*

### Address space

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

| <input type="checkbox"/> | Address range        | Addresses                     | Overlap |     |
|--------------------------|----------------------|-------------------------------|---------|-----|
| <input type="checkbox"/> | 10.3.0.0/16          | 10.3.0.0 - 10.3.255.255 (6... | None    | ... |
|                          | <input type="text"/> | (0 Addresses)                 | None    |     |

### Subnets

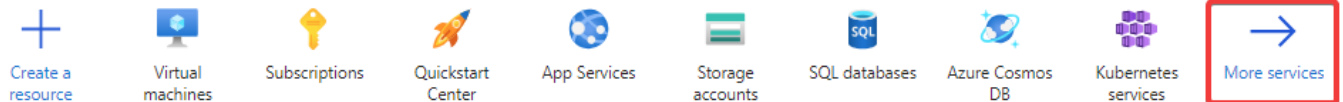
The subnet's address range in CIDR notation. It must be contained by the address space of the virtual network.

| <input type="checkbox"/> | Subnet name          | Address range        | Addresses                        |     |
|--------------------------|----------------------|----------------------|----------------------------------|-----|
| <input type="checkbox"/> | default              | 10.3.0.0/24          | 10.3.0.0 - 10.3.0.255 (256 ad... | ... |
|                          | <input type="text"/> | <input type="text"/> | (0 Addresses)                    |     |

## Virtual Network - Azure Services

1. Go to your **Azure services** on the Azure console's home page.
2. Click on **More services**.

### Azure services



3. Click on **Networking** in the Categories sidebar.

## Categories

AI + machine learning

Analytics

Compute

Containers

Databases

Integration

Mixed reality

Monitor

Networking

Security

Storage

Web & Mobile

4. Click on **Virtual networks** in the Networking foundation section.

## Network foundation



Bastions



DNS private resolvers



NAT gateways



Private DNS zones



Public IP addresses



Virtual networks



Custom IP Prefixes



DNS zones



Network managers



Private Link



Public IP Prefixes

5. Click on **Create** in the upper left corner.

## Virtual networks

Inductive Automation



Create



Manage view



Refresh



Export to CSV



Open query



Assign tags

6. A virtual network creation wizard will appear and start on the **Basics** page. Begin by selecting the **subscription**, **resource group**, and **region** your new virtual network will reside in, and give your virtual network a **name**.



Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual network](#)

### Project details

Subscription \* ⓘ Training Division

Resource group \* ⓘ ignitioncloud-build-training-rg

[Create new](#)

### Instance details

Name \* testVirtualNetwork ✓

Region \* West US 3

7. Click **Next: IP Addresses** on the bottom.

8. The **IP Addresses** page contains settings to configure address spaces and subnets. We will use the default address space and subnet here.

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

#### IPv4 address space

10.3.0.0/16 10.3.0.0 - 10.3.255.255 (65536 addresses) 

☐ Add IPv6 address space ⓘ

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

[+](#) Add subnet  Remove subnet

| <input type="checkbox"/> Subnet name | Subnet address range | NAT gateway |
|--------------------------------------|----------------------|-------------|
| <input type="checkbox"/> default     | 10.3.0.0/24          | -           |

 A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. [Learn more](#) 

9. Click **Next: Security**.

10. The **Security** page allows you to enable or disable various security settings.

 **NOTE**

Since this example is demonstrative, we are using the default Disabled settings. For security purposes however, we recommend enabling security features for your virtual network.

|                           |                                                                          |
|---------------------------|--------------------------------------------------------------------------|
| BastionHost ⓘ             | <input checked="" type="radio"/> Disable<br><input type="radio"/> Enable |
| DDoS Network Protection ⓘ | <input checked="" type="radio"/> Disable<br><input type="radio"/> Enable |
| Firewall ⓘ                | <input checked="" type="radio"/> Disable<br><input type="radio"/> Enable |

11. Click **Next: Tags** once you finish configuring security.
12. The **Tags** page allows you to group and consolidate various resources by applying the same tag. We will not set up any tags for our example.

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#) ↗

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

| Name ⓘ               | Value ⓘ                |
|----------------------|------------------------|
| <input type="text"/> | : <input type="text"/> |

13. Click **Next: Review + create**.
14. Azure will now attempt to validate your settings, and will show a banner at the top of the page once validation is complete. Review the summary of your chosen settings. If you are satisfied with your choices, click **Create**.

## Create a Network Security Group

Azure's Cloud Edition Image will come with preconfigured network security group rules with ports 80, 443, and 22 open. You can still create your own during the virtual machine creation process or through Azure services.

When creating a new network security group **from the wizard**, ports 80, 443, and 22 will be open by default. Creating a network security group through **Azure services** will require you to manually open the specified ports.



**NOTE**

Port 22 is typically used to get admin access and shell into the virtual machine. Since port 22 is open by default, it may be prudent to remove this rule depending on your network architecture. Port 80 is required to access the Gateway in a non-SSL environment, while port 443 is required to access the Gateway using SSL. Keep in mind that you will still need to [enable SSL/TLS](#) on the Gateway before using port 443.

Regardless of how you utilize your network security group, we recommend limiting access to required IP addresses only for security purposes.

## Network Security Group - Virtual Machine Creation Process

1. Begin by going to the **Create a virtual machine wizard**. You can find instructions on creating your virtual machine on the [Image Access Instructions - Azure](#) page.
2. Complete the steps until you reach the **Networking** page.
3. Azure will create a new network security group based off the name of your virtual machine. To edit it, click **Create new**.

Configure network security group \*

(new) testVirtualMachine-nsg

Create new

### **i** NOTE

When creating a network security group through the virtual machine creation wizard, the new network security group will be configured with the image's network security group rules. Ports 80, 443, and 22 will already be open and allow incoming traffic to hit those ports.

4. You will be taken to a list of **inbound** and **outbound** rules. From here, you can add more rules by clicking **Add an inbound/outbound rule** at the end of each list.

#### Inbound rules ⓘ

|                                                |   |     |
|------------------------------------------------|---|-----|
| 1010: HTTP<br>Any<br>HTTP (TCP/80)             | ✓ | ... |
| 1020: HTTPS<br>Any<br>HTTPS (TCP/443)          | ✓ | ... |
| 1030: default-allow-ssh<br>Any<br>SSH (TCP/22) | ✓ | ... |

[+ Add an inbound rule](#)

#### Outbound rules ⓘ

No results

[+ Add an outbound rule](#)

#### ⓘ NOTE

If you want to add or modify your rules later, you can edit your network security group in Azure Services.

5. After you finish configuring your network security group, click **OK** at the bottom.

## Network Security Group - Azure Services

1. Go to your **Azure services** on the Azure console's home page.
2. Click on **More services**.

#### Azure services



Create a resource



Virtual machines



Subscriptions



Quickstart Center



App Services



Storage accounts



SQL databases



Azure Cosmos DB



Kubernetes services



[More services](#)

3. Click on **Networking** in the Categories sidebar.

## Categories

AI + machine learning

Analytics

Compute

Containers

Databases

Integration

Mixed reality

Monitor

Networking

Security

Storage

Web & Mobile

- Click on **Network security groups** in the Network security section.

## Network security



DDoS protection plans



Firewalls



Network Security Perimeters



Firewall Manager



Network security groups



Web Application Firewall policies (WAF)

PREVIEW

- Click on **Create** in the upper left corner.

## Network security groups



Inductive Automation (inductiveautomation1.onmicrosoft.com)

+ Create



Manage view



Refresh



Export to CSV



Open query



Assign tags

- A network security group creation wizard will appear and start on the **Basics** page. Begin by selecting the **subscription**, **resource group**, and **region** your new network security group will reside in, and give your network security group a **name**.

### Project details

|                  |                                 |
|------------------|---------------------------------|
| Subscription *   | Training Division               |
| Resource group * | ignitioncloud-build-training-rg |

[Create new](#)

### Instance details

|          |                          |
|----------|--------------------------|
| Name *   | testNetworkSecurityGroup |
| Region * | West US 3                |

7. Click **Next: Tags** on the bottom.

8. The **Tags** page will allow you to group and consolidate various resources by applying the same tag. We will not set up any tags for our example.

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

| Name ⓘ               | Value ⓘ              |
|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> |

9. Click **Next: Review + create**.

10. Azure will now attempt to validate your settings, and will show a banner at the top of the page once validation is complete. Review the summary of your chosen settings. If you are satisfied with your choices, click **Create**.

11. After Azure has finished deploying your network security group, click on **Go to resource**.

## ✓ Your deployment is complete



Deployment name : Microsoft.NetworkSecurityGroup-20230629120945

Subscription : Training Division

Resource group : ignitioncloud-build-training-rg

Start time : 6/29/2023, 12:39:23 PM

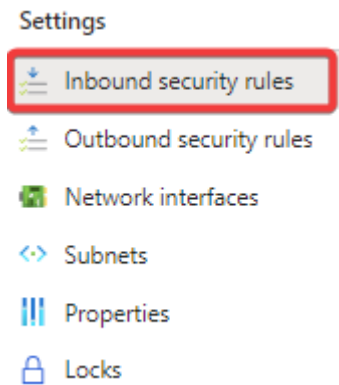
Correlation ID : a642324f-f321-40ed-9da2-f6f6cc4702b9

> Deployment details

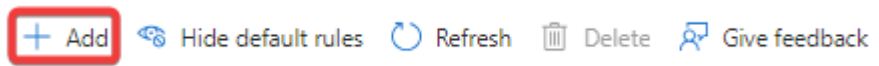
✓ Next steps

[Go to resource](#)

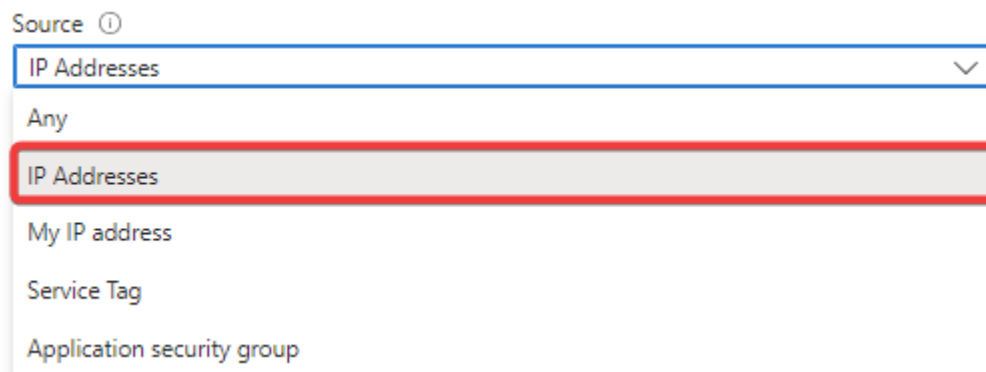
12. Once you reach your resource, you can begin specifying which ports you want to open and limiting access to your Gateway by specifying IP addresses in your inbound security rules. To do these actions, begin by clicking **Inbound security rules** in the sidebar under Settings.



13. Click on **Add** in the upper left corner.



14. Change the **Source** field's value to **IP Addresses**.



15. Two new fields will now appear. Put the IP addresses you want to allow access from in the **Source IP addresses/CIDR ranges**. If you would like to also define a port to allow traffic from, you can use the **Source port ranges** field.

A screenshot of the AWS IAM console's 'Source' field and its associated input fields. The 'Source' dropdown is set to 'IP Addresses'. Below it, the 'Source IP addresses/CIDR ranges' field contains the text '10.0.0.0/24'. Below that, the 'Source port ranges' field contains the text '\*'. The 'Source IP addresses/CIDR ranges' field has a green checkmark in the top right corner.

NOTE

Alternatively, you can also put IP addresses you want to deny access from by setting the **Action** property to "Deny".

16. Add the ports you want to be open and accessible in the **Destination port ranges** field.

Destination ⓘ  
Any

Service ⓘ  
Custom

Destination port ranges \* ⓘ  
8080

**NOTE**

If you have not done so already, you will need to open ports 80 and 443 in order to access the Gateway webpage via non-SSL and SSL, respectively.

17. Choose the **protocol** you want, as well as whether you want to **allow** or **deny** access from the specified IP.

Protocol  
☒ Any  
☐ TCP  
☐ UDP  
☐ ICMP

Action  
☒ Allow  
☐ Deny

**NOTE**

Use the TCP protocol when setting an inbound rule to open ports 80 and 443.

18. Set the **name** and **priority** of the inbound rule.

19. Click **Add**. Your inbound security rule will become active and added to your network security group.



# Creating a Public IP

You can create a Public IP in the virtual machine creation wizard or through Azure services. However, creating a public IP through Azure services will give you a few more options to configure, including:

- IP Version
- Availability Zone
- Tier
- Idle Timeout (minutes)
- DNS Name Label

## NOTE

Be careful when creating your public IP, as you will not be able to change many of its settings after creating it.

## Public IP - Virtual Machine Creation Process

1. Begin by going to the **Create a virtual machine** wizard. You can find instructions on creating your virtual machine on the [Image Access Instructions - Azure](#) page.
2. Complete the steps until you reach the **Networking** page.
3. Azure will create a new public IP based off the name of your virtual machine. To edit it, click **Create new**.

Configure network security group \*  

**Create new**

4. From here, you can set the **name**, **SKU**, and **routing preference**.

Name \*  

SKU \* ⓘ

☐ Basic ☒ Standard

Assignment ⓘ

☒ Static

Routing preference ⓘ

☒ Microsoft network ☐ Internet

Availability zone

Zone-redundant

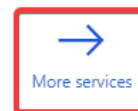
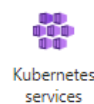
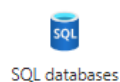
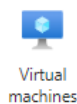
5. Make your selections, and then press **OK** at the bottom.

## Public IP - Azure Services

1. Go to your **Azure services** on the Azure console's home page.

2. Click on **More services**.

### Azure services



3. Click on **Networking** in the Categories sidebar.

### Categories

AI + machine learning

Analytics

Compute

Containers

Databases

Integration

Mixed reality

Monitor

Networking

Security

Storage

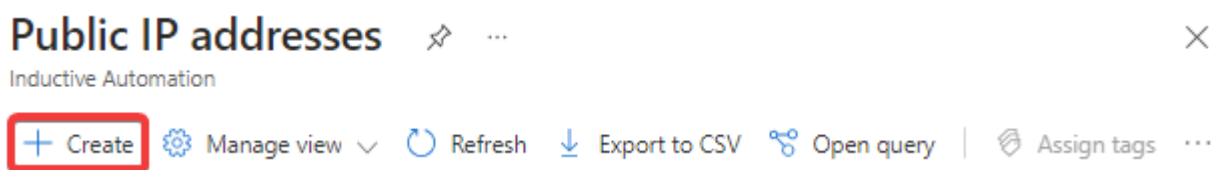
Web & Mobile

4. Click on **Public IP addresses** in the Network foundation section.

## Network foundation



5. Click **Create** in the upper left corner.



6. You will be taken to a public IP creation wizard. Begin at the **Project details** section and select the **subscription** and **resource group** you'd like to deploy your public IP in.

### Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription ⓘ \*

Resource group ⓘ \*

[Create new](#)

7. Under **Instance details**, select the **region** you want to deploy this resource in.

### Instance details

Region ⓘ \*

[Deploy to an edge zone](#)

8. The **Configuration details** section contains all the properties that are specifically related to public IP addresses. In this example, we will leave everything as the default setting.

### Configuration details

|                            |                                                                                      |
|----------------------------|--------------------------------------------------------------------------------------|
| Name *                     | <input type="text" value="testPublicIP"/>                                            |
| IP Version * ⓘ             | <input checked="" type="radio"/> IPv4<br><input type="radio"/> IPv6                  |
| SKU * ⓘ                    | <input checked="" type="radio"/> Standard<br><input type="radio"/> Basic             |
| Availability zone * ⓘ      | <input type="text" value="Zone-redundant"/>                                          |
| Tier * ⓘ                   | <input checked="" type="radio"/> Regional<br><input type="radio"/> Global            |
| IP address assignment * ⓘ  | <input type="radio"/> Dynamic<br><input checked="" type="radio"/> Static             |
| Routing preference * ⓘ     | <input checked="" type="radio"/> Microsoft network<br><input type="radio"/> Internet |
| Idle timeout (minutes) * ⓘ | <input type="text" value="4"/>                                                       |
| DNS name label ⓘ           | <input type="text"/>                                                                 |

9. Click **Next:Tags** at the bottom.

10. The **Tags** page will allow you to group and consolidate various resources by applying the same tag. We will not set up any tags for our example.

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

| Name                 | Value | Resource          |
|----------------------|-------|-------------------|
| <input type="text"/> | :     | Public IP address |

Once you are done with your tags, click **Next: Summary**.

11. Azure will now attempt to validate your settings, and will show a banner at the top of the page once validation is complete. Review the summary of your chosen settings. If you are satisfied with your choices, click **Create**.

# Cloud Edition Gateway

The Cloud Edition Gateway is very similar to a standard Ignition Gateway. Many of the features that exist on the standard Ignition platform also exist in Cloud Edition. Refer to the following sections for a brief overview of the Gateway navigation panel.

## Home

The **Home** section allows you to download the Designer Launcher, Vision Client Launcher, Perspective Workstation, or view a Perspective project. Additionally, there are resource links near the bottom of the Home page to help you get started with Ignition quickly:

- Inductive University
- Ignition Exchange
- Inductive Automation forums
- Product Documentation
- Appendix
  - Contains a complete reference for components, expressions, and scripting functions.

When you open your Cloud Edition Gateway, the Welcome page will be the landing page. It's where you'll find the Designer Launcher, Perspective Workstation, and Perspective Sessions.

- The **Designer Launcher** locates all Gateways that are available on your local network. Once you open the Designer Launcher, you can access the projects on the selected Gateway.
- The **Perspective Workstation** allows users to open Perspective Sessions on the machine Workstation is installed on.
- The **Perspective Sessions** opens Perspectives Sessions from this Gateway.

Home

Welcome

Designer

Perspective

Platform

Connections

Network

Services

Diagnostics

Welcome to Ignition

Launch Designer

Gateway Overview

Details

|              |             |                 |              |
|--------------|-------------|-----------------|--------------|
| Gateway Name | Redundancy  | Gateway Version | Gateway Mode |
| Ignition     | Independent | 8.3.0           | N/A          |

Gateway Notes

Edit Notes

Welcome to your Ignition Gateway. This customizable area is intended to capture the critical details you want to document for this Gateway. You might include information about the environment (production, testing, or development), key workflows, or maintenance schedules. It's also a great place to list instructions for your team, important reminders about system health, or details about your configuration that require regular review. Use this space to keep everyone informed and ensure smooth operations across the board.

Downloads

Designer Launcher

Bring all your data, systems, and developers together into one simple, integrated development environment.

Perspective Workstation

Open sessions from any Ignition Gateway.

# Platform

The Platform section includes information regarding the Gateway system and security. The System pages provide an overview of all the systems in your Gateway while also enabling you to drill down into specific areas and get an in-depth view of what is currently happening. Below the System pages are the Security pages, which provide several security options to safeguard data and applications in Ignition.

Platform

Overview

System

Security

Platform

Connections

Network

Services

Diagnostics

Platform Overview

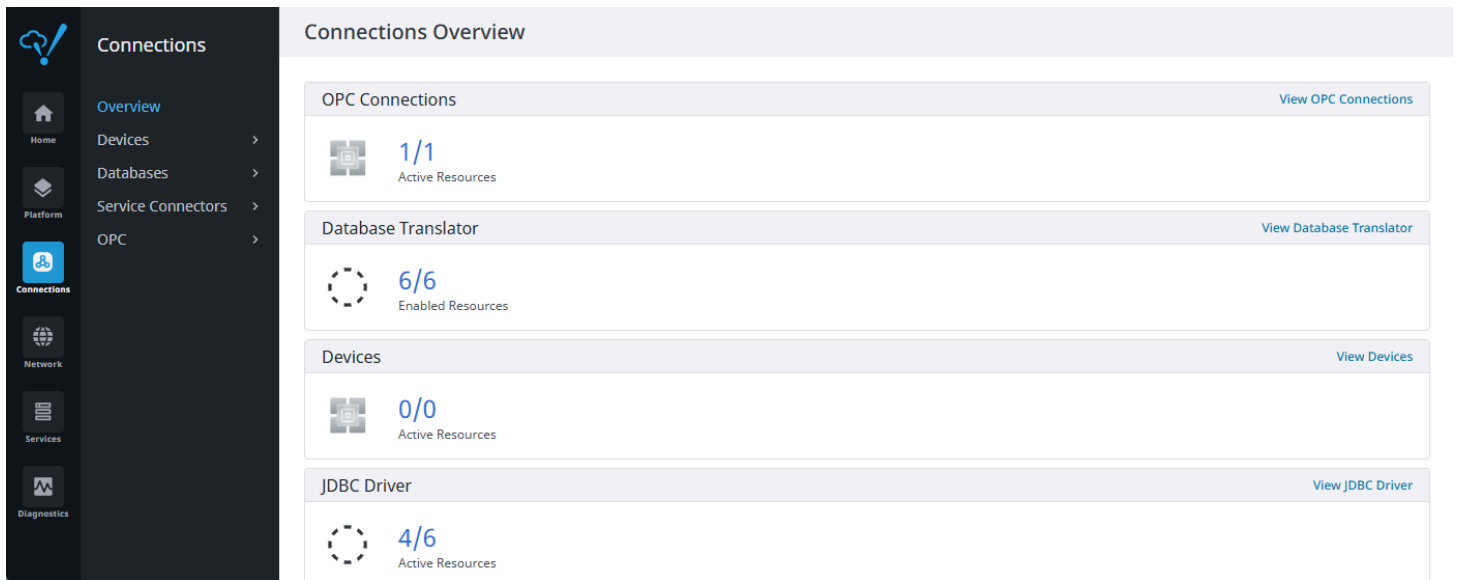
Configured Items

View All Errors

| ITEM                        | LAST UPDATED | ENABLED | STATUS    |
|-----------------------------|--------------|---------|-----------|
| > Agent Groups 1            |              |         |           |
| Agent Management            |              |         |           |
| Alarm Journal Settings      |              |         | Configure |
| Alarm Notification Profiles |              |         | Configure |
| API Token                   |              |         | Configure |
| Audit Profiles              |              |         | Configure |
| Database Connection         |              |         | Configure |
| > Database Translator 6     |              |         | Configure |
| Devices                     |              |         | Configure |
| EAM Agent Task              |              |         |           |
| Email Profile Settings      |              |         | Configure |
| > Fonts 3                   |              |         |           |
| Hardware License            |              |         |           |
| Historian                   |              |         |           |
| Holiday                     |              |         | Configure |
| > Icons 5                   |              |         |           |

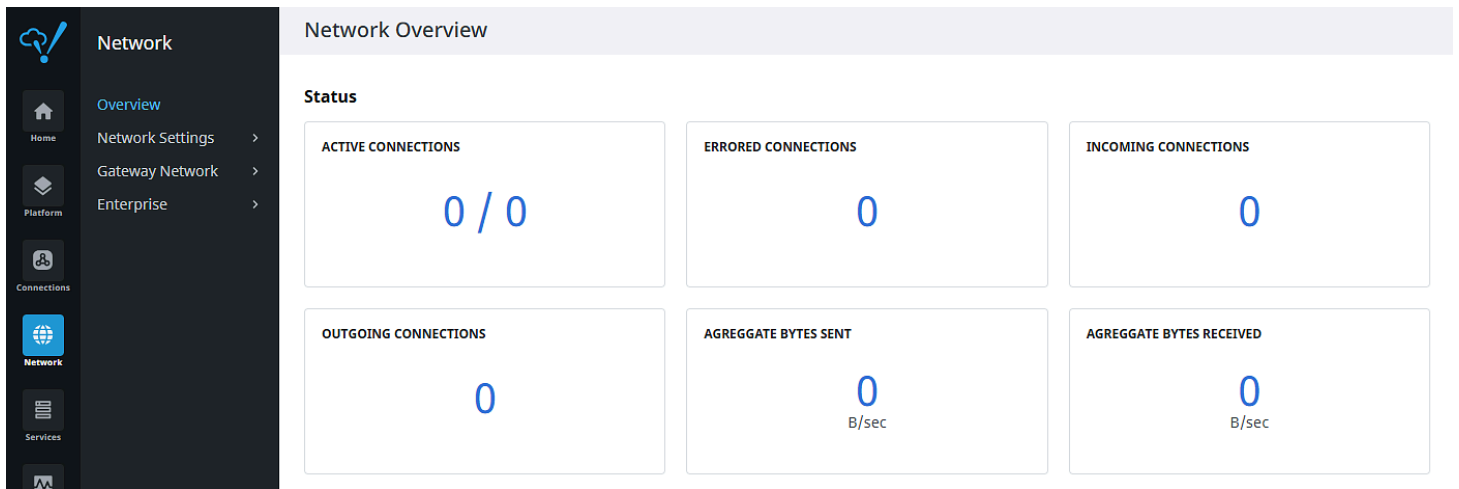
# Connections

This section includes information about Gateway connections to external systems. The list of systems displayed under the Connections section will vary depending on the installed modules.



## Network

The Network section contains settings to modify the Gateway Network and Enterprise Administration connections. The Network tab also contains the Network Overview section, which displays various status metrics about your Gateway Network.



## Services

The Services Overview page displays a status summary for all the configured connections, including the number of services currently configured, errored, or running.



Services



Overview



Historians



Tags



Alarming



Reports



SFCs



Transaction Groups



Event Streams



Network



Services



Diagnostics

Services Overview

Alarm Journal Settings

0/0

Enabled Resources

[View Alarm Journal Settings](#)

Tag Providers

2/5

Active Resources

[View Tag Providers](#)

Rosters

0/0

Enabled Resources

[View Rosters](#)

Alarm Notification Profiles

0/0

Active Resources

[View Alarm Notification Profiles](#)

# Diagnostics

The Diagnostics section provides a visual synopsis of everything in the Gateway, while giving easy access to tools like loggers and threads that help track what is currently happening with your internal Gateway system.



Diagnostics



Overview



Metrics Dashboard



Logs



Execution



Performance



Scripts



Threads



Connections



Network



Services



Diagnostics

Diagnostics Overview

Architecture

Gateway Overview

Gateway Name

Ignition

Gateway Version

8.3.0

License

licensed

Uptime

0 days, 0 hours, 6 minutes, 57 seconds

Redundancy

*Add a redundant backup gateway to protect your system from downtime caused by failures.*

[Configure Redundancy →](#)

Gateway Network

*Multiply the power of your Ignition Gateways by combining them into an enterprise network.*

[Configure Network →](#)

Connections

Performance



# Upgrading Ignition within Cloud Services

## Accessing the Ubuntu OS through SSH

The official Ignition CE platform is installed on a headless Ubuntu OS for either an AWS EC2 or Microsoft Azure Virtual Machine (VM). To perform an Ignition CE upgrade on your existing cloud environment, you will first need to SSH into the Ubuntu OS in order to perform a series of commands through its Command Line Interface (CLI). Each cloud service has their own method of directly accessing the Ubuntu OS.

### AWS EC2

The upgrade process for the official Ignition AMI being hosted on an AWS EC2 instance assumes you are running Cloud Edition (CE) on an existing AWS EC2 instance. To create a new EC2 instance with CE, launch an instance using the official CE Ignition AMI publicly available at the [AWS Marketplace](#). Once your instance is successfully running with CE, navigate to the [EC2 Management Console](#) of your AWS Account and refer to the following steps:

1. On your EC2 Management Console, navigate to the Instances page located on the left-hand side navigation panel.
2. Under the Instances page, locate the specific instance containing Ignition CE from the instances table and select its checkbox. Ensure that your instance is running properly before continuing.
3. Once selected, click on the Connect button located above the instances table to navigate to the Connect to instance page.

## Connect to instance [Info](#)

Connect to your instance [redacted] (Ignition-Test) using any of these options

**EC2 Instance Connect**

Session Manager

SSH client

EC2 serial console

Instance ID

 [redacted] (Ignition-Test)

Public IP address

 [redacted]

User name

Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ubuntu.

ubuntu

**Note:** In most cases, the default user name, ubuntu, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Cancel

Connect

4. Select the default option EC2 Instance Connect. The User name section by default will be "ubuntu", which is also the default user name specified for the AMI. Click Connect at the bottom right-hand corner to connect to the CLI of the running Ubuntu OS for your EC2 instance through your web browser.

```
aws Services Q Search [Alt+S]
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.19.0-1022-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

System information as of Wed Apr 19 15:20:40 UTC 2023

System load:  0.0244140625      Processes:           120
Usage of /:   60.6% of 7.57GB   Users logged in:    0
Memory usage: 90%              IPv4 address for eth0: 10.0.11.121
Swap usage:   0%

* Ubuntu Pro delivers the most comprehensive open source security and
  compliance features.

  https://ubuntu.com/aws/pro

* Introducing Expanded Security Maintenance for Applications.
  Receive updates to over 25,000 software packages with your
  Ubuntu Pro subscription. Free for personal use.

  https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

18 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

*** System restart required ***
Last login: Thu Apr  6 22:12:14 2023 from 13.52.6.115
ubuntu@ip-10-0-11-121:~$
```

## Microsoft Azure VM

The upgrade process for the official Ignition image hosted on Microsoft Azure assumes you are running Cloud Edition (CE) on an existing Azure VM. To create a new VM with CE, launch an instance using the official CE Ignition AMI publicly available at the [Azure Marketplace](#). Once your VM is successfully running with CE, navigate to your [Azure Portal](#) and complete the following steps:

1. On your Azure Portal homepage, navigate to the Virtual Machines page listed under Azure Services.
2. Under the Virtual Machines page, locate and select the specific VM record containing Ignition CE from the list. Ensure that your VM is running properly under the status column before continuing.

3. Inside the specific VM configuration menu, click on the Connect button located above the Essentials section to review details for establishing SSH Clients with your existing Azure VM.

The screenshot shows the 'Connect' page for a virtual machine named 'IgnitionCloud-Aaron'. The left sidebar contains a navigation menu with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Networking, Connect (selected), Disks, Size, Microsoft Defender for Cloud, Advisor recommendations, Extensions + applications, Availability + scaling, Configuration, Identity, Properties, and Locks. The main content area has a warning banner at the top: 'To improve security, enable just-in-time access on this VM.' Below this, there are tabs for RDP, SSH (selected), and Bastion. The section is titled 'Connect via SSH with client' and shows a 'Suggested method for connecting' with a green checkmark. A blue box lists prerequisites checked by Azure: 'An inbound network security group rule has been created and your client IP address can access port 22.', 'The VM's network interface has a Public IP address.', and 'The VM is running.' Below this, there are four numbered steps: 1. Open the client of your choice... 2. Ensure you have read-only access to the private key... 3. Provide a path to your SSH private key file... 4. Run the example command below to connect to your VM. Step 3 includes a text input field for the 'Private key path' with the value '~/ssh/<keyname>.pem'. Step 4 includes a code block with the command 'ssh -i <private key path> azureuser@'.

IgnitionCloud-Aaron | Connect ☆ ...  
Virtual machine

Search

Overview  
Activity log  
Access control (IAM)  
Tags  
Diagnose and solve problems

Settings

Networking  
Connect  
Disks  
Size  
Microsoft Defender for Cloud  
Advisor recommendations  
Extensions + applications  
Availability + scaling  
Configuration  
Identity  
Properties  
Locks

To improve security, enable just-in-time access on this VM. →

RDP SSH Bastion

Connect via SSH with client

^ ✓ Suggested method for connecting

Azure has checked the status for the most common prerequisites when connecting using this method.

- ✓ An inbound network security group rule has been created and your client IP address can access port 22. [Learn more](#)
- ✓ The VM's network interface has a Public IP address. [Learn more](#)
- ✓ The VM is running.

1. Open the client of your choice, for example [WSL on Windows](#), [Terminal on Mac](#) or [Shell on Linux](#).
2. Ensure you have read-only access to the private key. Chmod is only supported on Linux subsystems (e.g. WSL on Windows or Terminal on Mac).  

```
chmod 400 <keyname>.pem
```
3. Provide a path to your SSH private key file. [Replace/reset your SSH private key.](#) ⓘ  
Private key path
4. Run the example command below to connect to your VM.  

```
ssh -i <private key path> azureuser@
```

4. A third party SSH client of your choice will be required for completing step 3. For this example, PuTTY was used. Initial login of the SSH client will require the username specified during Azure VM creation. The default username is "azureuser".

```
azureuser@IgnitionCloud-Aaron: ~
login as: azureuser
Authenticating with public key "imported-openssh-key"
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-1038-azure x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

System information as of Tue Jun 27 19:36:11 UTC 2023

System load:  0.0               Processes:           111
Usage of /:   27.1% of 28.89GB   Users logged in:    0
Memory usage: 41%              IPv4 address for eth0: 10.0.0.4
Swap usage:   0%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
  just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

22 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

*** System restart required ***
Last login: Mon Jun 26 20:23:48 2023 from [REDACTED]
azureuser@IgnitionCloud-Aaron:~$
```

## Upgrading Ignition Cloud Edition

Once you are successfully connected to the CLI of the Ubuntu OS, you will now be able to fetch the latest version of the Ignition CE installer from the Inductive Automation's [downloads page](#).

1. Navigate to the section of Linux system installers and right-click > Copy Link Address against the link labeled: **Ignition Cloud - Linux Installer 64-bit**.
2. Enter the following command on the CLI using the link copied from the previous step.

### NOTE

The following URL <https://releases.inductiveautomation.com/nightly/8.3.0-SNAPSHOT/20230523-1027/ignition-cloud-8.3.0-SNAPSHOT-linux-64-installer.run> is a placeholder and will vary depending on address link copied from the Inductive Automation downloads page

```
wget --referer https://inductiveautomation.com/*
https://releases.inductiveautomation.com/nightly/8.3.0-SNAPSHOT/20230523-
1027/ignition-cloud-8.3.0-SNAPSHOT-linux-64-installer.run
```

3. Once the download is complete, you will need to update the installer file's permissions before it can be executed. Enter the following command on the CLI:

```
chmod 700 ignition-cloud-8.3.0-SNAPSHOT-linux-64-installer.run
```

4. Confirm that the file's permissions were changed to allow executions using **ls -l**.

```
ubuntu@ip-10-0-7-165:~$ ls
ignition-cloud-8.1.29-SNAPSHOT-linux-64-installer.run
ubuntu@ip-10-0-7-165:~$ chmod 700 ignition-cloud-8.1.29-SNAPSHOT-linux-64-installer.run
ubuntu@ip-10-0-7-165:~$ ls
ignition-cloud-8.1.29-SNAPSHOT-linux-64-installer.run
ubuntu@ip-10-0-7-165:~$ ls -l
total 1703404
-rwx----- 1 ubuntu ubuntu 1744278728 May 23 06:41 ignition-cloud-8.1.29-SNAPSHOT-linux-64-installer.run
ubuntu@ip-10-0-7-165:~$
```

5. Once the file is set as an executable, run the installer on the CLI by entering the following:

```
./ignition-cloud-8.3.0-SNAPSHOT-linux-64-installer.run
```

6. Once entered, the file will run and will first prompt you to specify where the existing Ignition install directory resides. The Cloud Edition AMI by default uses the directory **/usr/local/bin/ignition** during installation and is already specified for you on the prompt to accept by default as well. Simply hit enter to continue if all default settings were specified or specify the custom directory of your Ignition install if needed. If an existing directory is detected, you will be prompted to confirm the upgrade process.

```
INFO [IgnitionInstaller] [2023/05/23 16:58:41]: log location set to /home/ubuntu/.ignition/install/install.log
INFO [IgnitionInstaller] [2023/05/23 16:58:41]: log level set to 'INFO'

-----
Welcome to the Ignition Cloud Installer!

This wizard will help install Ignition and its core components.

Installer Help
The following slash commands can be invoked from anywhere
'//Help' to print this help message
'//Quit' to Quit to the installer
'//About' to print the current interactive
'//Back' to return to the previous step
'//Restart' to return the first step in the installer.

-----
Installation Location

Please specify the directory where Ignition will be installed. If you are
upgrading Ignition, then select the directory where Ignition is currently
installed.

[/usr/local/bin/ignition]:
Setup has located Ignition by Inductive Automation installed in:
/usr/local/bin/ignition Continuing will stop the Ignition Server and replace
this installation with the version in this installer. It is highly recommended
that you back up your gateway before proceeding with the upgrade.
Continue with upgrade? [Y/n]:
```

7. Once the upgrade process is accepted, you will also be given a few more prompts to confirm any individual module upgrades and additional module inclusions. Details of all currently installed modules will be provided. Confirm these prompts to receive the final confirmation for running the upgrade process.

```
[N] MongoDB Connector      not installed      won't install
[Y] MQTT Distributor      4.0.15.2023020918  4.0.16.2023041422
[Y] MQTT Engine           4.0.15.2023020918  4.0.16.2023041422
[Y] MQTT Transmission     4.0.15.2023020918  4.0.16.2023041422
[Y] OPC-UA                9.1.27.2023031616- 9.1.29.2023052208-
[Y] Perspective           2.1.27.2023031616- 2.1.29.2023052208-
[Y] Reporting             6.1.27.2023031616- 6.1.29.2023052208-
[Y] SFC                   5.1.27.2023031616- 5.1.29.2023052208-
[Y] SQL Bridge            10.1.27.2023031616 10.1.29.2023052208
[Y] Symbol Factory        7.1.27.2023031616- 7.1.29.2023052208-
[Y] Tag Historian         4.1.27.2023031616- 4.1.29.2023052208-
[Y] Twilio Integration and Alarm Notif 3.1.27.2023031616- 3.1.29.2023052208-
[Y] Voice Notification    6.1.27.2023031616- 6.1.29.2023052208-
[Y] WebDev                5.1.27.2023031616- 5.1.29.2023052208-
Moving on to any additional modules
Would you like to modify any additional modules? [y/N]: n

-----
Ready to Upgrade

Setup is now ready to begin upgrading Ignition on your computer.

Do you want to continue? [Y/n]: y
[#]      ] 0%: Checking existing gateway's state
[#]      ] 0%: Configuring Install Actions
[#]      ] 0%: Executing Install Actions
[#]      ] 0%: Creating a gateway backup. This may take some time...
[#]      ] 0%: Gateway backup 'backup_2023523171.gwbk' creation complete
[#]      ] 0%: Stopping Gateway. This may take some time..
```

8. The CLI will notify you when the upgrade process is complete and will also state error logs in the event of an issue. Once the upgrade process is complete, you will be prompted to both start the Ignition server and install a service for doing so. Starting the service will provide log details on what is running successfully.

```
[#####] 97%: webserver/webapps/main/favicon.ico
[#####] 97%: webserver/webdefault.xml
[#####] 97%: wrapper-license.conf
[#####] 97%: Extraction of Install artifacts complete
[#####] 97%: Starting Module customization
[#####] 97%: Module customization complete
[#####] 97%: Creating un-installer
[#####] 99%: Uninstaller Created
[#####] 99%: Starting post-install modifications
[#####] 99%: Exporting PATH and executable alias
[#####] 99%: Adjusting the install's ownership
[#####] 99%: symlink 'webserver/csr.pfx' target is missing. skipping..
[#####] 99%: symlink 'webserver/ssl.pfx' target is missing. skipping..
[#####] 99%: Running the Upgrader tool
[#####] 99%: Upgrader tool completed successfully
[#####] 99%: Installer actions complete. Performing cleanup
[#####] 99%: Install complete
```

-----  
Ignition Successfully Upgraded

The wizard has finished upgrading Ignition on your computer.

Start Ignition Now [Y/n]: y

Install Service [Y/n]: y

INFO [IgnitionInstaller] ] [2023/05/23 17:02:57]: Starting Gateway. This should only take a moment..

INFO [IgnitionInstaller] ] [2023/05/23 17:03:02]: Gateway started

INFO [IgnitionInstaller] ] [2023/05/23 17:03:02]: http://localhost:80

INFO [IgnitionInstaller] ] [2023/05/23 17:03:02]: http://localhost:80

ubuntu@ip-10-0-7-165:~\$

9. Once the Ignition service has started, you can exit the CLI and return to your instances page or navigate to your Ignition Gateway webpage.



# Launchers and Workstation

Ignition features several launchable runtimes: Vision Clients, the Designer, and Perspective Sessions. To help with managing these separate systems, Ignition Gateways provide several **launcher** programs for each runtime. These launchers are the main means of launching an Ignition runtime application. For the purposes of clarity, the following are considered launchers:

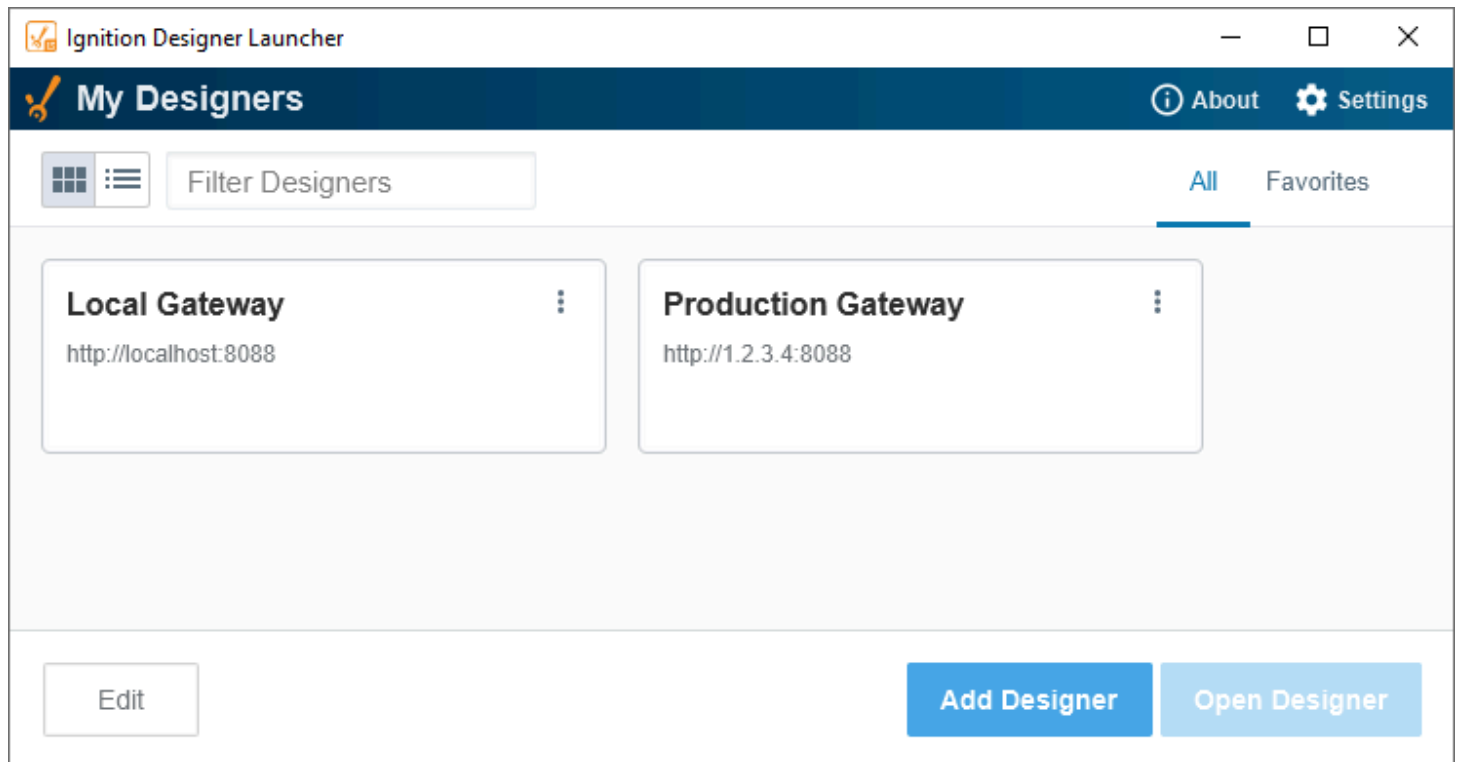
- **Designer Launcher:** launches the **Designer** against the configured Gateway.
- **Vision Client Launcher:** opens Vision Clients from an Ignition Gateway.
- **Perspective Workstation:** opens Perspective sessions from an Ignition Gateway, in a standalone desktop program.

This page describes the download and installation process shared by the application launchers mentioned above, as well as the common property settings. Some property settings are unique to a specific launcher application and will be detailed on that specific launcher application's page.

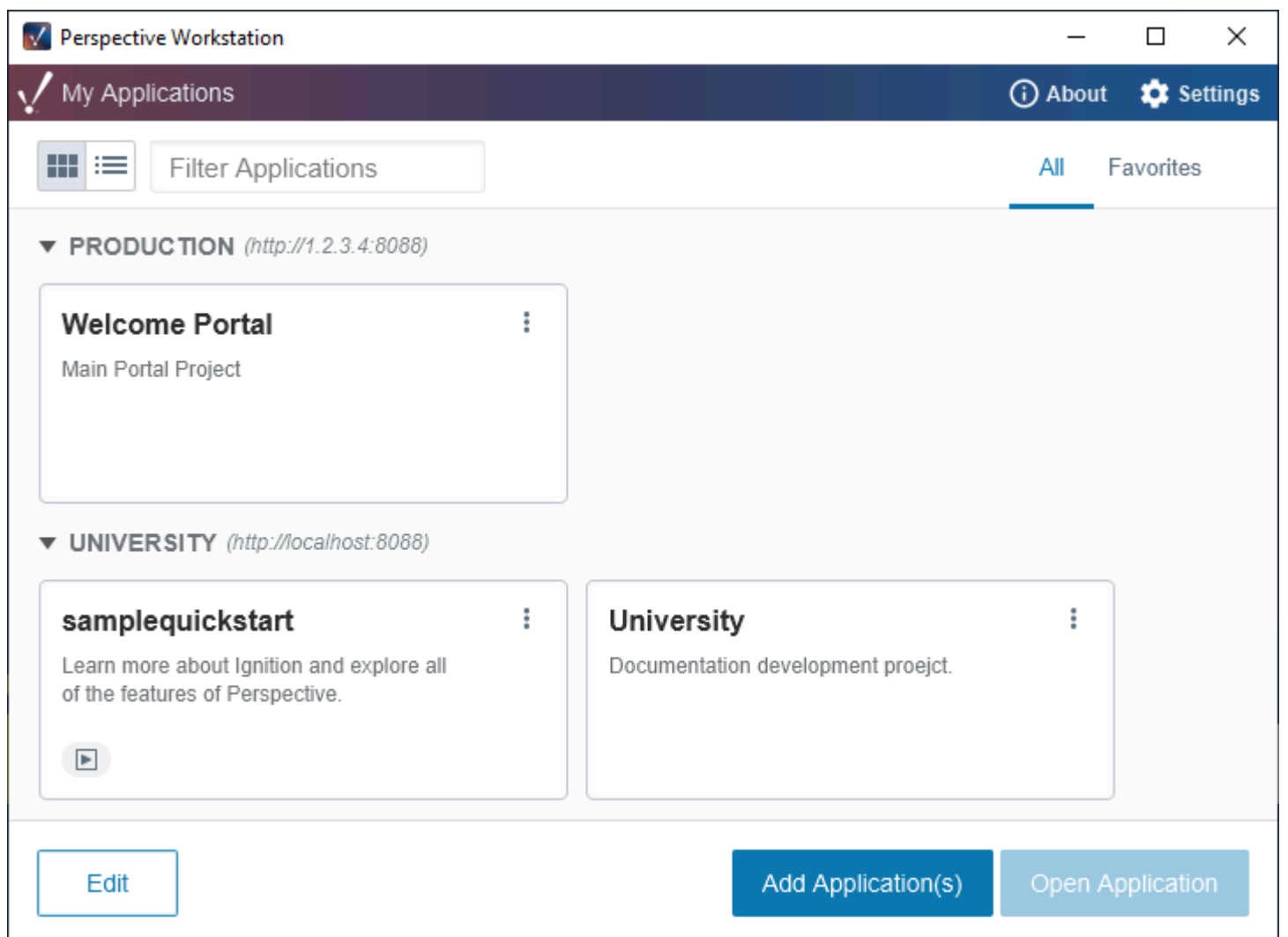
## What Is an Application?

To understand the purpose of a launcher, we need to understand what an application is. An application is a configuration in a launcher that is associated with a project.

The Ignition Designer Launcher is the launcher for the Designer. This launcher has two applications configured, the **Local Gateway** and the **Production Gateway**. Selecting either application and clicking **Open Designer** will launch the Designer for the selected Gateway.



The Vision Client Launcher and Perspective Workstation work under a similar pattern, except each application represents a project in a Gateway. Multiple projects from a single Gateway can be represented in a launcher. There is a **Welcome Portal** application under the **Production** Gateway, while the **University** Gateway features two applications that each lead to a different project.



# Launcher Download and Installation

This section demonstrates the common download and installation steps for all the launcher applications. Each launcher application has an install wizard that will guide you through the installation process. The installation steps are common for all the launchers with a few exceptions depending on the operating system you're using.

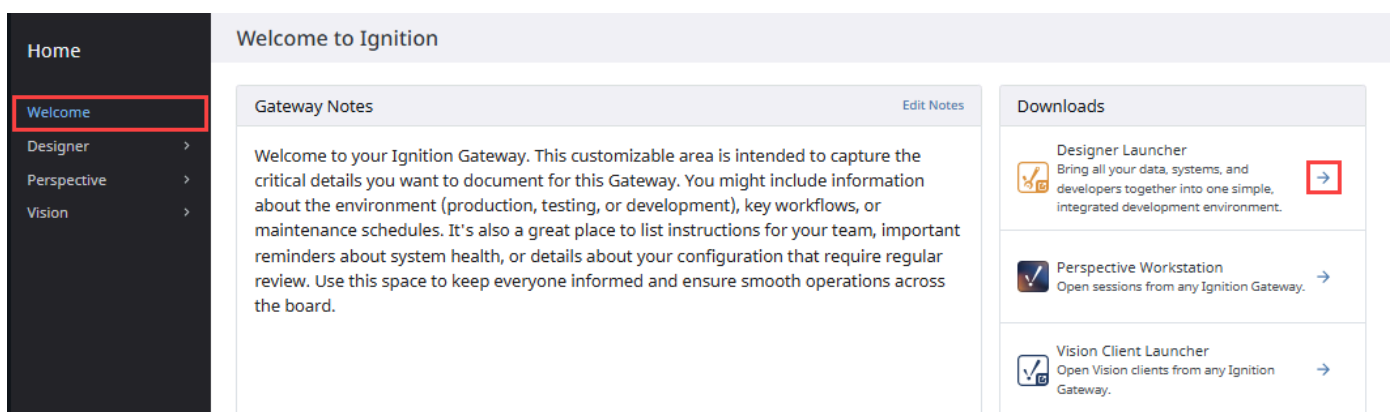
## NOTE

Although you can run the Ignition Gateway and Perspective Sessions on ARM-based desktops (such as a Raspberry Pi), the Designer, Vision Client, and Perspective Workstation cannot be run on ARM-based Linux machines. Instead, the Designer, Vision Client, or Perspective Workstation will need to be installed and run from an Intel-based machine.

An exception to this is if you are using Mac as your operating system, where only Apple Silicon Macs are supported and not x86 Macs.

For the sake of brevity, this section will focus on installing the Designer Launcher, but the steps for installing the Vision Client Launcher and Perspective Workstation are similar.

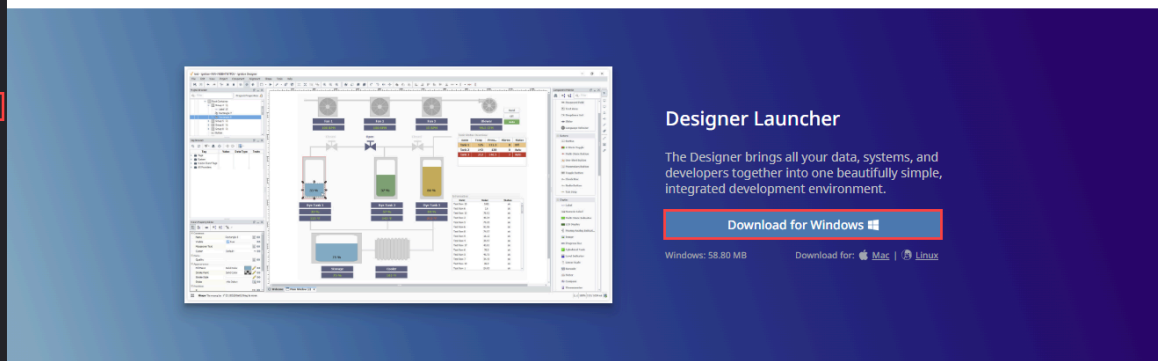
1. Go to **Home > Welcome** on the Gateway. You will see a Downloads section with options that lead to separate Download pages for each of the launchers.
2. Click the desired arrow icon and you'll be redirected. We'll click on the **Designer Launcher** arrow.



3. Your web browser will detect the operating system, and suggest the appropriate download for the Download button. Click to download the installer for the launcher.



Download the Designer Launcher



### Ignition Designer Resources

Browse our extensive product documentation and free online training university for answers to all of your questions.

|                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <p><b>Inductive University</b><br/>Check out Inductive University and learn the Ignition Platform at an industry-ready level.<br/><a href="#">Go to Inductive University</a></p> |  <p><b>Ignition Manual</b><br/>Explore the User Manual for details about the Ignition platform and modules.<br/><a href="#">Open User Manual</a></p> |  <p><b>What's New In 8.3</b><br/>Ignition 8.3 is here! Check out the new features and improvements in this release.<br/><a href="#">Learn More</a></p> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

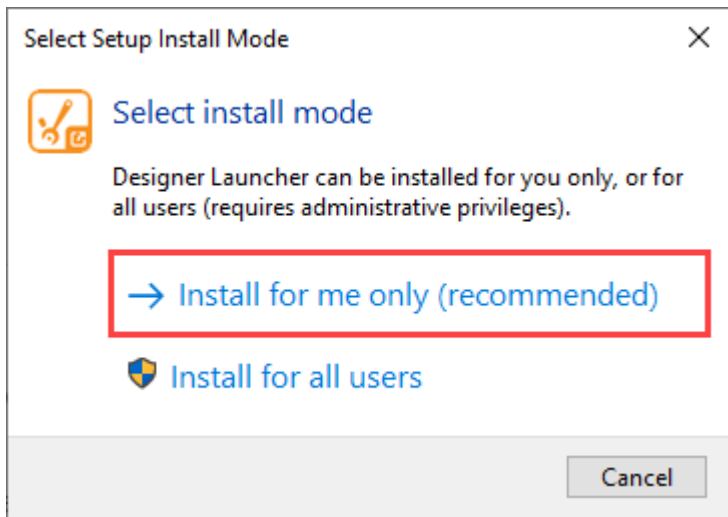
Looking for your existing Projects?

[View Projects](#)

4. Locate the installer on your local system (web browser typically store downloaded files in a "Downloads" folder), and run it.
5. Work through the install wizard. There are only a handful of options in the installer:
  - Associate with the **.designer file extension**
    - Support custom icons for .designer files
  - Associate with the **designer:// URL Protocol**
  - Create a desktop icon
6. Then, you'll select the installation directory for the launcher.

**Windows**    **Mac OS**    **Linux**

If this is a first time install, the Designer Launcher wizard has an additional step. It will prompt you to select the install mode. Installing locally installs the launcher in the user's AppData\Roaming folder whereas 'all users' installs it in Program Files.



7. Once the installation process completes, click **Finish**.

The Designer Launcher will open, allowing you to start adding applications.

## Upgrading Launchers

Whenever an application is launched from a launcher, the Launcher will check to see if it needs an update. If the Gateway containing the launched application is several revisions ahead of the Launcher, the Launcher will provide a popup notifying you that an update is available.

Manual upgrades can also be performed. Simply download and run a new launcher installer from a more recent Ignition Gateway. During installation, simply set the installation directory to the same directory as the old launcher.

You can return the Vision Client Launcher, Perspective Workstation, and Designer Launcher product versions using your operating system's terminal (PowerShell for Windows). The following tabs list the commands for returning the version number by operating system:

**Windows**

Mac OS

Linux

Vision Client

```
(Get-Item -Path 'C:\{Vision Client Launcher Installation  
Directory}\visionclientlauncher.exe').VersionInfo.ProductVersion
```

Perspective Workstation

```
(Get-Item -Path 'C:\{Perspective Workstation Installation  
Directory}\perspectiveworkstation.exe').VersionInfo.ProductVersion
```

Designer

```
(Get-Item -Path 'C:\{Designer Launcher Installation  
Directory}\designerlauncher.exe').VersionInfo.ProductVersion
```

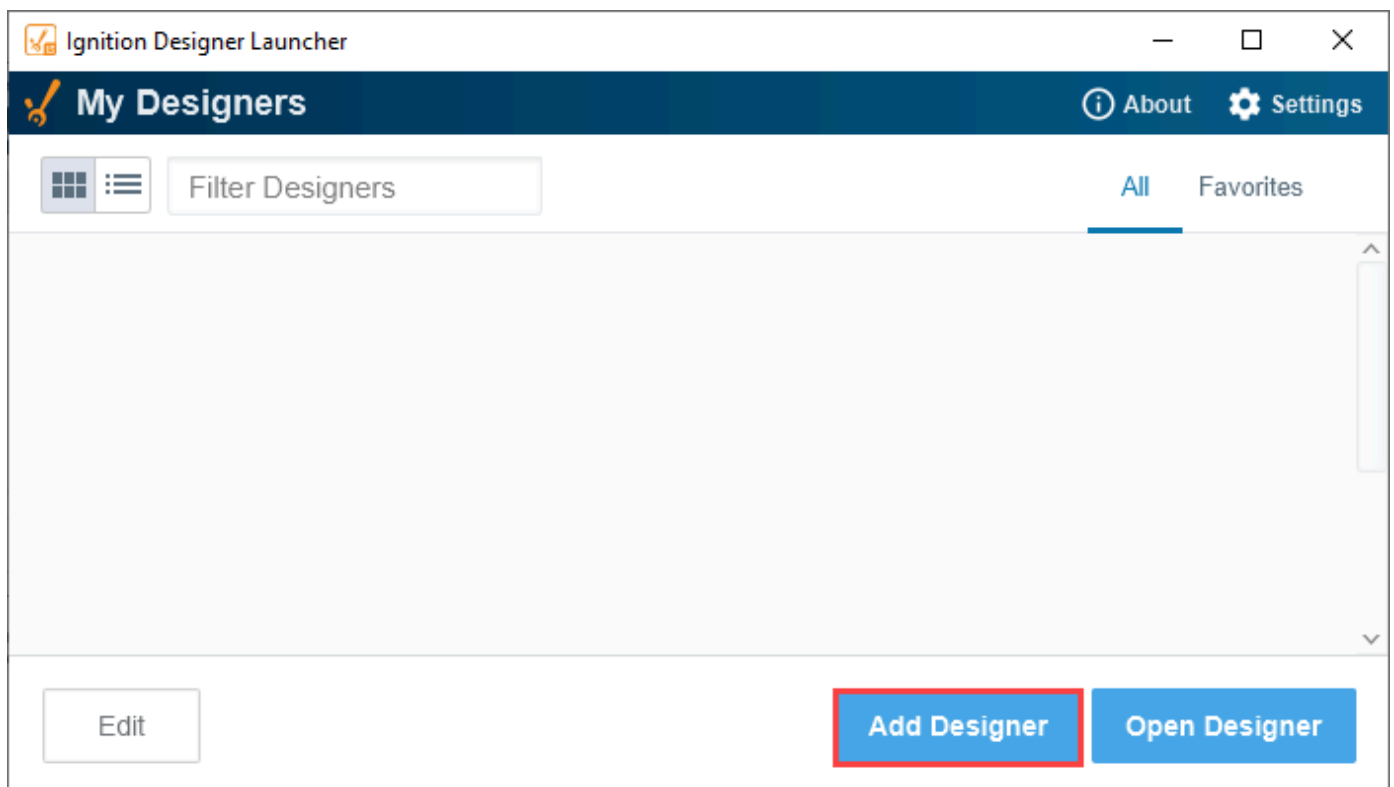
The launcher file versions will match the product version listings.

## Adding Applications

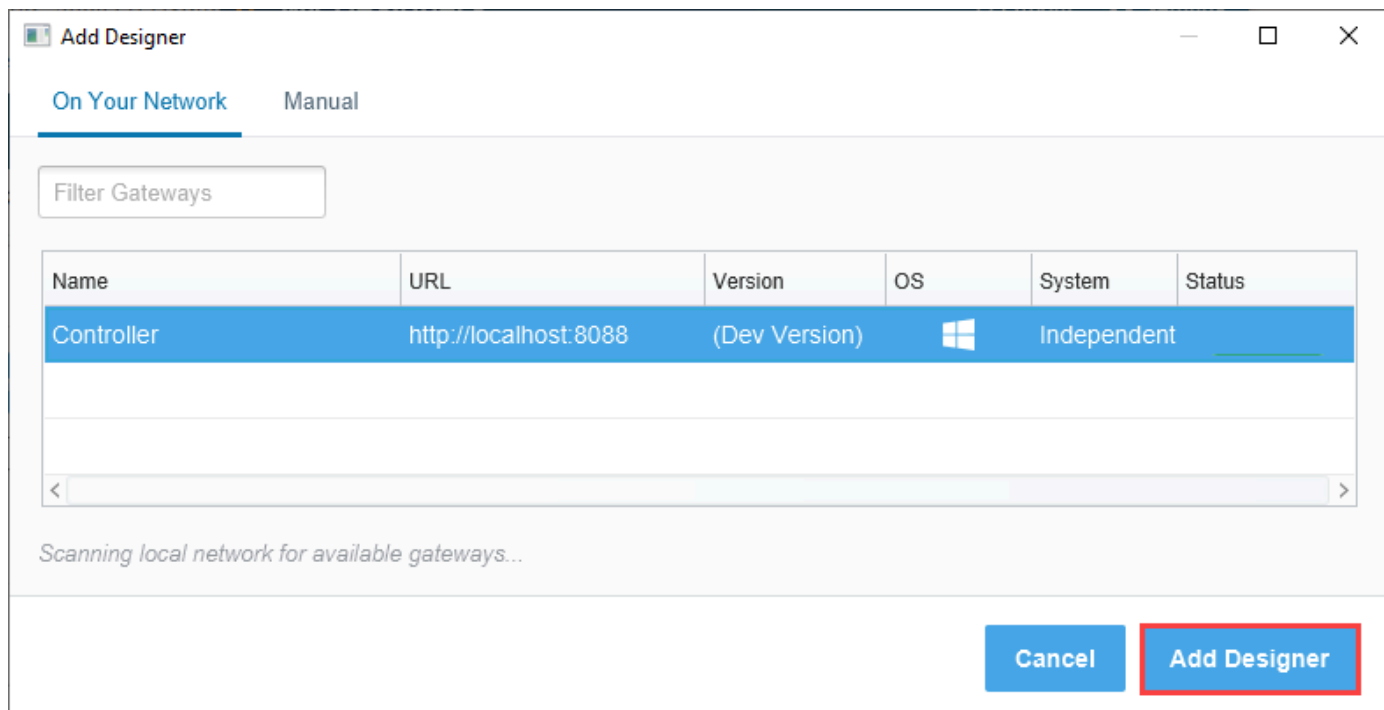
The process for adding applications/Designers to the Designer Launcher is very similar to adding applications to the Vision Client Launcher and Perspective Workstation. This section demonstrates how to add new applications.

The following Designer Launcher example is used to show how to add applications for the Designer and Vision Client Launchers and the Perspective Workstation.

1. With the launcher open, click the **Add Designer** button.

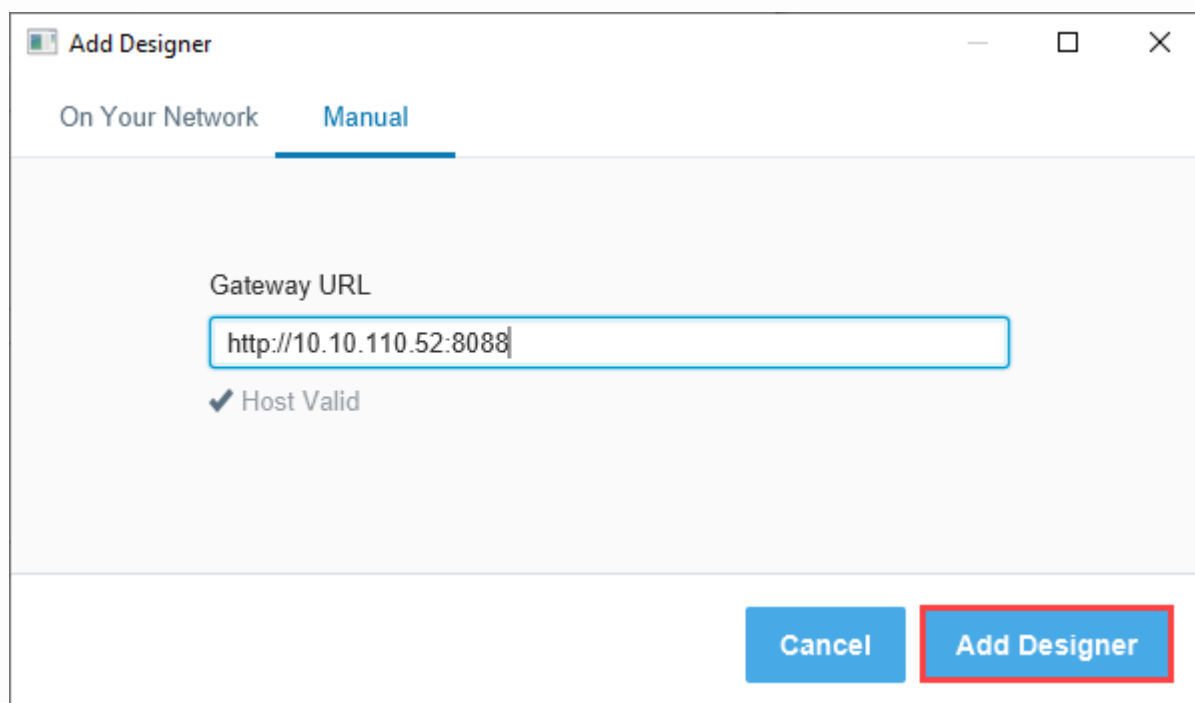


2. The launcher will browse and list all the available Gateways on your network. Select from any of the available gateways and press the **Add Designer** or **Select Gateway** button depending on which Launcher you are using.

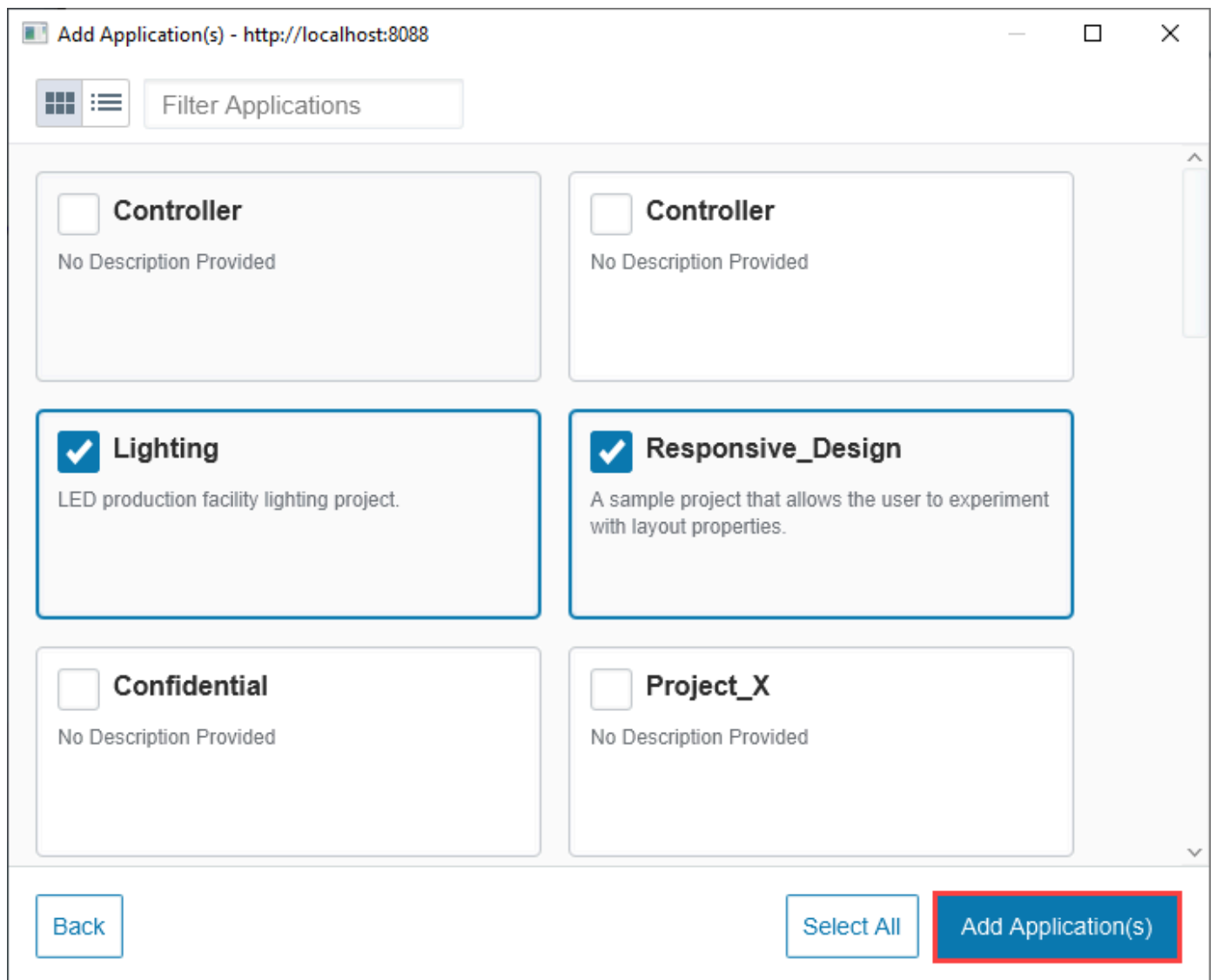


### **NOTE**

If you don't see the Gateway you're looking for, but know the IP address, you can enter it manually. Click the **Manual** tab and enter the **Gateway URL**. It will inform you if you have a valid host name. If so, click **Add Designer** or **Select Gateway** depending what launcher application you are are using.



- If you're adding an application to the Vision Client Launcher or Perspective Workstation, you'll have this extra step where you can select from any of the available projects on the Gateway. Select the desired projects, then click **Add Application(s)**.



4. Once added, the new applications will appear on the starting screen of the Launcher.

## Windows Silent Installations

The **Designer Launcher**, **Vision Client Launcher**, and **Perspective Workstation** can be installed on Windows systems from command line without any user prompts.

```
# Shows a simplified user interface
C:\Users\user\Downloads\VisionClientLauncherSetup.exe /CURRENTUSER /SILENT

# Shows no user interface at all.
C:\Users\user\Downloads\VisionClientLauncherSetup.exe /CURRENTUSER /VERYSILENT

# The following option installs silently without installing a desktop shortcut
C:\Users\user\Downloads\VisionClientLauncherSetup.exe /CURRENTUSER /VERYSILENT
/MERGETASKS="!desktopicon"
```



Using ALLUSERS may trigger a check from User Account Controls, so you may need administrator access for the following command to offer a truly silent installation:

```
C:\Users\user\Downloads\VisionClientLauncherSetup.exe /ALLUSERS /VERYSILENT
```

## Hosted Launcher Installers

Normally, each Ignition Gateway includes files for the various launchers. When you download a launcher from a Gateway, it will stream its local launcher files. However, you can override this behavior, causing the Gateway to ignore its local launcher files and instead download launchers from the internet. For more information, see the [Gateway Configuration File Reference](#) page.

Installers for Windows systems in .msi format are available on the Inductive Automation [downloads](#) page. To access them, click on either "Other operating systems and versions" or "Other Versions" on the downloads page, and scroll down to the "Launchers" section.

The `.msi` installers help make pre-deployment easier in enterprise environments and utilizes existing Windows Installer toolchain features. Notably, `.msi` installers support two features which make large-scale deployments easier:

- Transforms
- Group Policy Objects (GPOs)

You can read more about [transforms](#) and [Group Policy](#) on Microsoft's website.

If you wanted to download one of our hosted launchers, without modifying your Gateway's configuration file, you can download them directly from your web browser:

```
https://releases.inductiveautomation.com/launchers/VERSION/LAUNCHER
```

Where VERSION is the Ignition version (i.e., 8.3.0), and LAUNCHER is the name of the launcher. Launcher names are listed below.

| Launcher                | Operating System | Launcher Name                 |
|-------------------------|------------------|-------------------------------|
| Vision Client           | Windows          | visionclientlauncher.exe      |
| Vision Client           | Windows          | visionclientlauncher.msi      |
| Vision Client           | Linux            | visionclientlauncher.tar.gz   |
| Vision Client           | macOS            | visionclientlauncher.dmg      |
| Perspective Workstation | Windows          | perspectiveworkstation.exe    |
| Perspective Workstation | Windows          | perspectiveworkstation.msi    |
| Perspective Workstation | Linux            | perspectiveworkstation.tar.gz |
| Perspective Workstation | macOS            | perspectiveworkstation.dmg    |
| Designer                | Windows          | designerlauncher.exe          |
| Designer                | Windows          | designerlauncher.msi          |
| Designer                | Linux            | designerlauncher.tar.gz       |
| Designer                | macOS            | designerlauncher.dmg          |

For example, the following would download an 8.1.0 version of Perspective Workstation for Windows:

Example

<https://files.inductiveautomation.com/launchers/8.1.0/perspectiveworkstation.exe>

## Deep Link and File Association Support

If file extension and URL Protocol associations were enabled during installation, you can use deep links or File Associations to directly launch an application from anywhere without needing to open the launcher. Deep links are incorporated at the OS level and immediately open an Ignition project or Designer with a simple URL. File Associations allow crafting a customized JSON file that opens a respective launcher directly on click.

Launcher installation is still required since the URL or file is passed to the launcher to connect to the project and launch appropriately. However, this method eliminates the need to save applications within each launcher in order to launch applications.

### TRUST AND LAUNCH WARNING

When a deep link targets a Gateway that is unknown to the current operating system, a Trust and Launch warning will appear. This prompt requires the user to verify a program capable of displaying the link is installed and the necessary Designer/Vision Client launcher, Perspective Workstation, or Perspective App is installed to open it. Gateway addresses or domains are then saved in an `.ignition/clientlauncher-data/shared/known-gateways.txt` file, which applies to all launchers, for future launches. You can set the available environment variable, `IGNITION_KNOWN_GATEWAYS`, to **all** to trust all Gateway addresses and prevent this warning from appearing.

Note that locked configurations don't save the Gateway address.

## Creating Deep Links

Use the format examples listed below to create deep links for your projects based on the launcher required. You'll see each link begins with the necessary launcher, followed by the Gateway address and the project name when necessary:

- Designer Launcher:
  - To open the Designer and allow the user to choose a project: `designer://Gateway`
  - To launch a project directly: `designer://Gateway/projectName`
- Vision Client Launcher: `vision://Gateway/projectName`
- Perspective Workstation: `perspective://Gateway/projectName`

For instance, if you're targeting a Gateway at **localhost:8043** and you have a Perspective project named **demo**, your link would be `perspective://localhost:8043/demo`.

### DEEP LINKS USE HTTPS BY DEFAULT

If HTTP is required, add the [insecure query arg](#) to your link:

`perspective://localhost:8043/demo?insecure=true`.

## Query Arg Support

Deep links syntax also supports the following additional query args:

All Launchers Query Arg

| Type    | Query Arg | Description                                                                             |
|---------|-----------|-----------------------------------------------------------------------------------------|
| boolean | insecure  | Overrides the HTTPS default when set to true. For example, <code>insecure=true</code> . |

Workstation Only Query Args

| Type   | Query Arg                     | Description                                                                                                                                                                        |
|--------|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| string | mode                          | Sets the mode for launching. Options include windowed, fullscreen, and kiosk. For example, <code>mode=windowed</code> .                                                            |
| string | <code>display\${index}</code> | Maps URL paths and queries to specific displays. Displays match the index of the Identify Displays action in Workstation. When omitted the <code>/</code> mapped page is launched. |

Vision Client Launcher Only Query Args

| Type    | Query Arg | Description                                                                                                     |
|---------|-----------|-----------------------------------------------------------------------------------------------------------------|
| string  | mode      | Sets the mode for launching. Options include windowed and fullscreen. For example, <code>mode=windowed</code> . |
| integer | screen    | Sets the numeric screen index starting with 0.                                                                  |



TIP

Alongside your Vision Client Launcher query args, you can define any [Vision Client tags you want to override](#) as URL query parameters. Use the format `tag.${urlEncodedTagName}=${urlEncodedTagValue}` to override tags. Tag names and values must be URL encoded to ensure proper URL syntax conformance. The following example will override a Vision Client tag named **New Tag** with the value of **Some/path/value**:

```
tag.New%20Tag=Some%2Fpath%2Fvalue
```

# Command Line Launching

With deep links, you can use the command line to pass in a configuration and launch a project directly. For example, if we are targeting the same project as listed above, the following arguments can be used.

Windows

Mac OS

Linux

```
start "perspective://localhost:8043/demo?insecure=true"
start "vision://localhost:8043/demo?insecure=true"
start "designer://localhost:8043?insecure=true"
```

## File Associations

File Associations support a few more customizations than deep links as more information is contained in the JSON files, based on the launcher type. These files can be placed anywhere, such as on a panel PC where a project can then be launched with the launchers themselves staying hidden from the user.

New in 8.3.1

 JVM arguments are now supported in File Associations for Designers and Vision Clients.

File Extensions registered as Associations:

- Perspective Workstation: .perspective
- Vision Client Launcher: .vision
- Designer Launcher: .designer

| Perspective Workstation<br>(.perspective) | Vision Client Launcher<br>(.vision) | Designer Launcher<br>(.designer) |
|-------------------------------------------|-------------------------------------|----------------------------------|
|-------------------------------------------|-------------------------------------|----------------------------------|

```
{
  "name": "Perspective Demo",
  "project": "OnlineDemo",
  "gatewayAddress": "https://demo.ia.io:443",
  "backupAddress": null,
  "imagePath": "ig8icon.jpg",
  "launchUrl": "/data/perspective/client/OnlineDemo",
  "launchMode": "WINDOWED",
  "tabMode": "BLOCKED",
  "displayList": [
    {
      "index": 0,
      "page": "/",
      "primary": true
    },
    {
      "index": 1,
      "page": "/page2",
      "primary": false
    }
  ],
  "jvmArguments": [
    "-Dignition.perspective.designerSaveTimeout=30"
  ],
  "fallback": null,
  "fallbackReturn": null,
  "fallbackDelay": null
}
```

## Custom Shortcuts

When a shortcut to an application is created, a launchable link is placed on the desktop of the user. This link uses the configuration of the application that is saved in the launcher. This ensures that updates to the launcher are respected even if the link was created before the changes. That being said, you can override the following settings for the shortcut itself:

- "window.mode"
- "timeout"
- "screen"
- "retries"
- "init.heap"
- "max.heap"

- "fallback.application"
- "custom.jre.path"

The values for these settings can be found elsewhere in this User Manual: general launchers settings are on the [Launcher Settings](#) page, while each of the three launcher pages list settings unique to particular launcher.

**Windows**    **Mac OS**    **Linux**

---

1. Create a shortcut.
2. Right-click and select **properties**.
3. Add additional arguments to the end of the Target field:

```
...application=test window.mode=fullscreen
```

## Redirect Client Launch Cache

You can also redirect the cache directory that is used by the launcher. Typically the user's cache is in their home directory in the `.ignition` directory. This holds all the resources that are required for launching a Client as well as the resources for each launcher. Sometimes this is not desirable, for example in cases where you want a global cache that all users on a machine rely on or when you want the users client cache to reside in a different directory under AppData.

To change this directory, place a file named `redirect.txt` inside the `.ignition` directory in their user home directory. This file should have a single line in it which is an **absolute** path to the appropriate file.

## Signature Verification

The Vision Client and Designer Launchers include checks that run when launching a Designer or Vision Client to test if the Gateway is active. The default value for this check is `MODERATE`. Note that this value prevents launching against Gateway versions 8.1.33 and older.

Users can choose to adjust the security level of this check by changing the `signature.verification.strength` key in Vision Client or Designer JSON files. The path to these files differs by operating system, but they will generally look like the following:

## Vision Client

```
C:\Users\userName\.ignition\clientlauncher-data\vision-client-launcher.json
```

## Designer

```
C:\Users\userName\.ignition\clientlauncher-data\designer-launcher.json
```

The following options can be used for the `signature.verification.strength` key:

- STRICT: Revocation checks are required and legacy Gateways are disallowed.
- MODERATE: Soft fail on revocation checks and legacy Gateways are disallowed.
- AIR\_GAPPED: No revocation checks performed, but legacy Gateways are still disallowed.
- LENIENT: Soft fail on revocation checks, but legacy Gateways are allowed.
- LOOSE: No revocation checks and legacy Gateways are allowed.

For added security when launching, the Designer and Vision Client Launchers can perform signature verification against the `launchclient.jar` to verify the file and all of its contents. An error message will display if the `launchclient.jar` file's signature is invalid and launching is prohibited.



# Designer Launcher



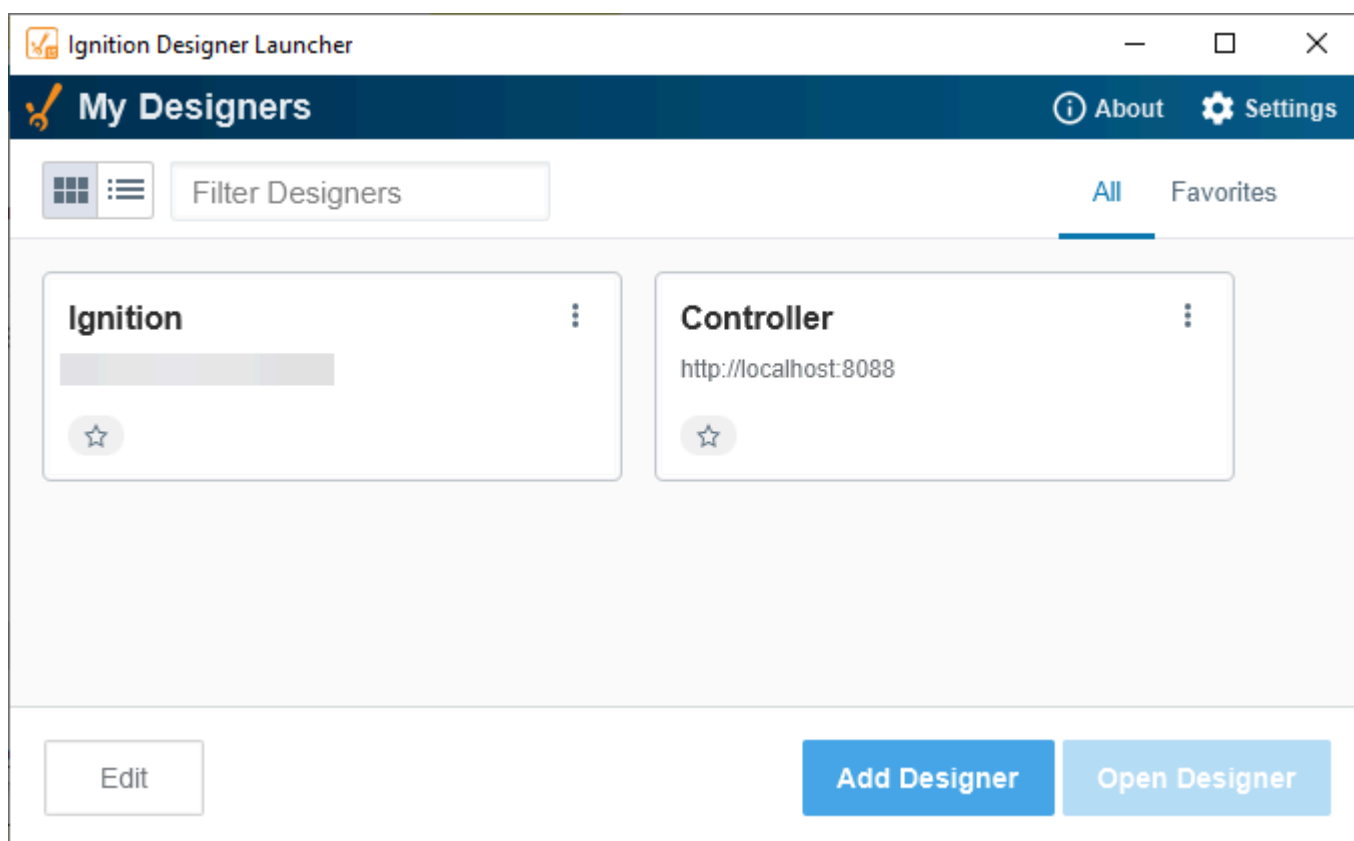
INDUCTIVE  
UNIVERSITY

## The Designer Launcher

[Watch the video](#)

The Designer Launcher is used to launch the Designer and connect to a Gateway. It displays a list of Designer cards, each representing a configured Gateway connection and its associated launch settings. From the Launcher, you can open projects, manage Designer settings, and access Gateway resources.

The Designer Launcher is available from the **Home** section of the Gateway. For information on setting up the Designer Launcher, see the [Launchers and Workstation](#) page.



Each Designer card includes a three dots menu that provides actions for managing and interacting with the Designer configuration without opening it.

| Menu Item        | Description                                          |
|------------------|------------------------------------------------------|
| Manage           | Opens the General Settings Configuration window.     |
| Go to Gateway    | Opens the Gateway in a new browser window.           |
| Create Shortcut  | Creates a desktop shortcut for the Designer.         |
| Add to Favorites | Adds the Designer to your Favorites.                 |
| Export           | Exports the Designer configuration as a JSON object. |
| Delete           | Deletes the Designer.                                |

## General Settings

The Designer Launcher provides application-specific settings for each Designer. To access these settings, click the **three dots menu** on a Designer card and select **Manage**.


Configure Controller

General

Designer Name

Controller

Gateway Address

http://localhost:8088

Timeout

Retries

Init Heap

Max Heap

30

-1

64M

1024M

JVM Arguments

ACTIONS

Export Config

Create Desktop Shortcut

Cancel

Ok

Apply

| Setting Name    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Designer Name   | Specifies the name of the Designer. This field is required.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Gateway Address | Specifies the Gateway address in the format <code>http[s]://host:port</code> .                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Timeout         | Defines the maximum number of seconds allowed for Gateway communication. If the timeout is exceeded, the Launcher aborts the request and retries it if retries are configured.                                                                                                                                                                                                                                                                                                                      |
| Retries         | <p>Defines how many times the Launcher retries a request after a communication error occurs. Available values include:</p> <ul style="list-style-type: none"> <li>• <b>-1</b>: The Launcher retries indefinitely until it is closed.</li> <li>• <b>0</b>: The Launcher does not retry after the first failure.</li> <li>• <b>1 (or greater)</b>: The Launcher retries the specified number of times. If retries are exhausted, the Launcher attempts to launch the fallback application.</li> </ul> |
| Initial Heap    | Specifies the initial heap size, in memory, allocated to the Designer.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Maximum Heap    | Specifies the maximum heap size, in memory, allocated to the Designer.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| JVM Arguments   | Specifies additional JVM arguments for the Designer. The Launcher copies the defaults from the global JVM arguments at creation time and does not update them if the global settings change.                                                                                                                                                                                                                                                                                                        |

# Perspective Workstation



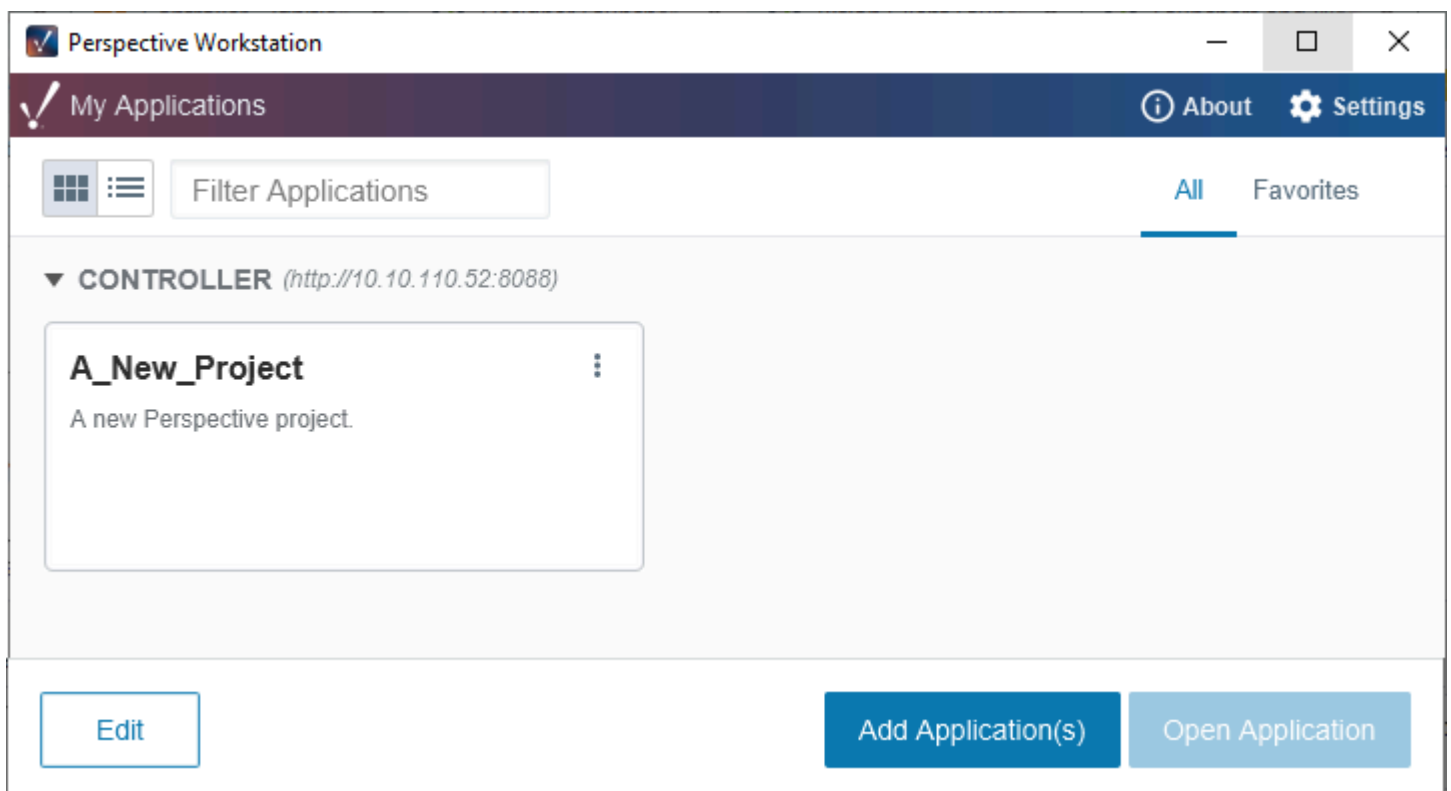
INDUCTIVE  
UNIVERSITY

## Perspective Workstation

[Watch the video](#)

Perspective Workstation is a single application that functions as both a launcher and a desktop wrapper for Perspective Sessions. It allows you to run Perspective projects as desktop applications designed for HMIs, panel PCs, and dedicated workstations.

Perspective Workstation supports both Windowed mode and full-screen Kiosk mode, which helps reduce distractions from the underlying operating system. It also provides features for managing applications on dedicated workstations with multiple monitors, allowing sessions to launch on specific displays.



### **i** NOTE

Perspective Workstation can only launch sessions from Ignition 8.1 or newer Gateways.

# Managing Workstation Settings

Perspective Workstation application settings are specific to each Perspective Session. To access Workstation settings, click the **three dots menu** for the Session application and select **Manage**. This will open the project's Configure popup where you can adjust the **Perspective Workstation Application Settings**. Some settings are automatically populated from previous setup configurations.

Some settings are automatically populated when you open the **Manage** view and navigate between configuration screens.

## Launch Modes

Perspective Workstation supports both Windowed mode and full-screen Kiosk mode. These modes determine how the Session window behaves and how much access users have to the underlying operating system.

## Tab and Window Links

The Tab/Window Links setting controls how Perspective Workstation handles links that would normally open in a new browser tab. You can configure these settings to allow links to open in the system browser, open within Workstation, or be blocked entirely.

## Multi-Monitor Support

Perspective Workstation supports multi-monitor configurations by allowing a single application to open multiple operating system windows, with each window displayed on a different monitor. Each monitor can display a different Perspective page.

When you configure multi-monitor settings, Workstation automatically detects available displays and lists them on the Page Configuration tab. You can assign a Perspective page to each display and designate a primary display for login dialogs and authentication prompts.

If the **Page** field is empty, no content appears on that display. If the field contains a **Page URL**, Workstation loads the specified page on that monitor. The **Identify Displays** option provides an on-screen overlay that helps you match display numbers to physical monitors.

### NOTE

The default Display 1 Page URL for a new application is `/`, which loads the default page configured in the Designer. For more information on configuring pages within the Designer, see [Page Configuration](#).

# Perspective Component Actions and Scripts

Perspective components can access Workstation-specific features that allow projects to control Workstation behavior.

- The [Component Events and Actions](#) page describes the Workstation component action, which allows a running Workstation application to switch launch modes.
- The [system.perspective.workstation](#) scripting namespace provides additional functions that allow you to interact with a running Workstation application.

## Perspective Workstation Application Settings

To access application settings, click the **three dots menu** for the Session application and select **Manage**. The sections below describe the available configuration options.

Configure A\_New\_Project

General

Page Configuration

Advanced

Application Name

A\_New\_Project

Launch Mode

Windowed

Tab/Window Links

Blocked

Description

A new Perspective project.

Gateway Address

http://10.10.110.52:8088

Project URL

/data/perspective/client/A\_New\_Project

http://10.10.110.52:8088/data/perspective/client/A\_New\_Project

ACTIONS

Export Config

Create Desktop Shortcut

Cancel

Ok

Apply

Perspective Workstation application settings are configured per application. To configure settings that apply to the Launcher itself, see the [Launcher Settings](#) page.

## General Application Settings

| Property         | Description                                                                                                                                                                                                                                                                                                                      |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application Name | Specifies the name of the application as it appears in the Launcher.                                                                                                                                                                                                                                                             |
| Launch Mode      | Specifies how the application launches by default. Available options include: <ul style="list-style-type: none"><li>• <b>Windowed</b>: Launches in a window.</li><li>• <b>Kiosk</b>: Launches in full-screen mode and restricts access to the operating system.</li></ul>                                                        |
| Tab/Window Links | Specifies how Workstation handles links that would normally open in a new browser tab. Available options include: <ul style="list-style-type: none"><li>• <b>Blocked</b>: Does not open.</li><li>• <b>In Window</b>: Opens within Workstation.</li><li>• <b>System Browser</b>: Opens in the system's default browser.</li></ul> |
| Description      | Provides a description of the application. The description appears on the <b>My Applications</b> screen.                                                                                                                                                                                                                         |
| Gateway Address  | Specifies the Gateway address in the format <code>http[s]://host:port</code> .                                                                                                                                                                                                                                                   |
| Project URL      | Specifies the URL path of the Perspective page that loads when the application starts.                                                                                                                                                                                                                                           |

## Page Configuration Settings

| Property          | Description                                                        |
|-------------------|--------------------------------------------------------------------|
| Identify Displays | Displays overlay labels that identify available monitors.          |
| Page              | Specifies the Perspective page to display on the assigned monitor. |
| Primary Display   | Specifies the display used for logins and authentication dialogs.  |

# Advanced Fallback Redirect Settings

Perspective Workstation provides advanced fallback redirect settings that control how an application behaves during extended Gateway outages after initial launch. Instead of immediately relying on automatic failover, you can configure Workstation to redirect users to a different application after a defined delay. These settings also allow Workstation to automatically return users to the original application once communication with the master Gateway is restored.

## Connection Settings

| Property        | Description                                                                                                              | Property Type     |
|-----------------|--------------------------------------------------------------------------------------------------------------------------|-------------------|
| Connect Timeout | Specifies how long Workstation attempts to connect to the Gateway before giving up. The duration is measured in seconds. | value:<br>integer |
| Retries         | Specifies how many connection attempts occur before Workstation redirects to the fallback application.                   | value:<br>integer |



## Fallback Redirect Settings

| Property             | Description                                                                                                                                                                   | Property Type  |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| Fallback Redirect    | Enables fallback redirect behavior for the application. The default value is false.                                                                                           | value: boolean |
| Fallback Application | Specifies the application that launches if the master Gateway connection is unavailable. The list includes applications configured in the current Workstation installation.   | value: string  |
| Auto-Return          | Enables automatic return to the original application when the Gateway becomes available again. The default value is false.                                                    | value: boolean |
| Launch Delay         | Specifies how long the application must remain disconnected before redirecting to the fallback application. The duration is measured in seconds, and the default value is 30. | value: integer |

## Perspective Workstation On-Screen Keyboard

Perspective Workstation can integrate with the operating system's on-screen keyboard. If an on-screen keyboard is enabled in the operating system, it automatically appears within a running Perspective Session when user input is required, such as when a Text Field component is selected.

 **NOTE**

The on-screen keyboard does not appear when you interact directly with Perspective Workstation configuration screens.

## Redundancy

Perspective Workstation supports redundant Gateway configurations to help maintain application availability during Gateway outages after a Session is successfully launched. When redundancy is configured, Workstation automatically attempts to connect to a backup Gateway if the master

Gateway is unavailable at startup. If the master Gateway cannot be reached, Workstation attempts to connect to the backup Gateway. If neither Gateway is available, Workstation alternates connection attempts until a connection is established or the application is closed.

## Command Line Arguments

You can launch Perspective Workstation from the command line using the arguments listed below.

| Argument                      | Description                                                                                                                                                                                                                                                                                                                    |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>application</code>      | Specifies the name of the Workstation application to launch.                                                                                                                                                                                                                                                                   |
| <code>debugPort</code>        | Specifies the debug port used by the launched application. You must specify the application to launch when you want to specify the debug port. For example, <code>.\perspectiveworkstation.exe application=test debugPort=9224</code> will work, but <code>.\perspectiveworkstation.exe debugPort=9224</code> will not work.   |
| <code>launch.mode</code>      | Overrides the application launch mode. Available values include: <ul style="list-style-type: none"><li><code>WINDOWED</code>: Launches in Windowed mode.</li><li><code>KIOSK</code>: Launches in full-screen Kiosk mode.</li></ul>                                                                                             |
| <code>browser.tab.mode</code> | Overrides the tab and window link behavior. Available values include: <ul style="list-style-type: none"><li><code>BLOCKED</code>: Does not open.</li><li><code>IN_WINDOW</code>: Opens within Workstation.</li><li><code>SYSTEM</code>: Opens in the system's default browser.</li></ul>                                       |
| <code>config.json</code>      | Specifies a configuration file to use as a temporary override. The file must be a JSON export created using the Export Launcher Config option in the Workstation Settings menu. For example,<br><code>"C:\Launchers\Perspective\Workstation.exe"</code><br><code>config.json="C:\Users\MyUser\Desktop\workstation.json"</code> |
| <code>devTools</code>         | Opens a Chromium DevTools popup with your Workstation session to help diagnose issues when debugging. As with <code>debugPort</code> , you must specify an application when using this argument.                                                                                                                               |

# System Requirements

Perspective Workstation uses JxBrowser and requires a supported 64-bit operating system. ARM-based operating systems are not supported. For more information, see the [JxBrowser System Requirements](#) documentation.

The bundled Perspective Workstation for macOS supports Apple Silicon only. An alternate build for Intel-based Macs is available from the Inductive Automation [Downloads](#) page.

# Vision Client Launcher

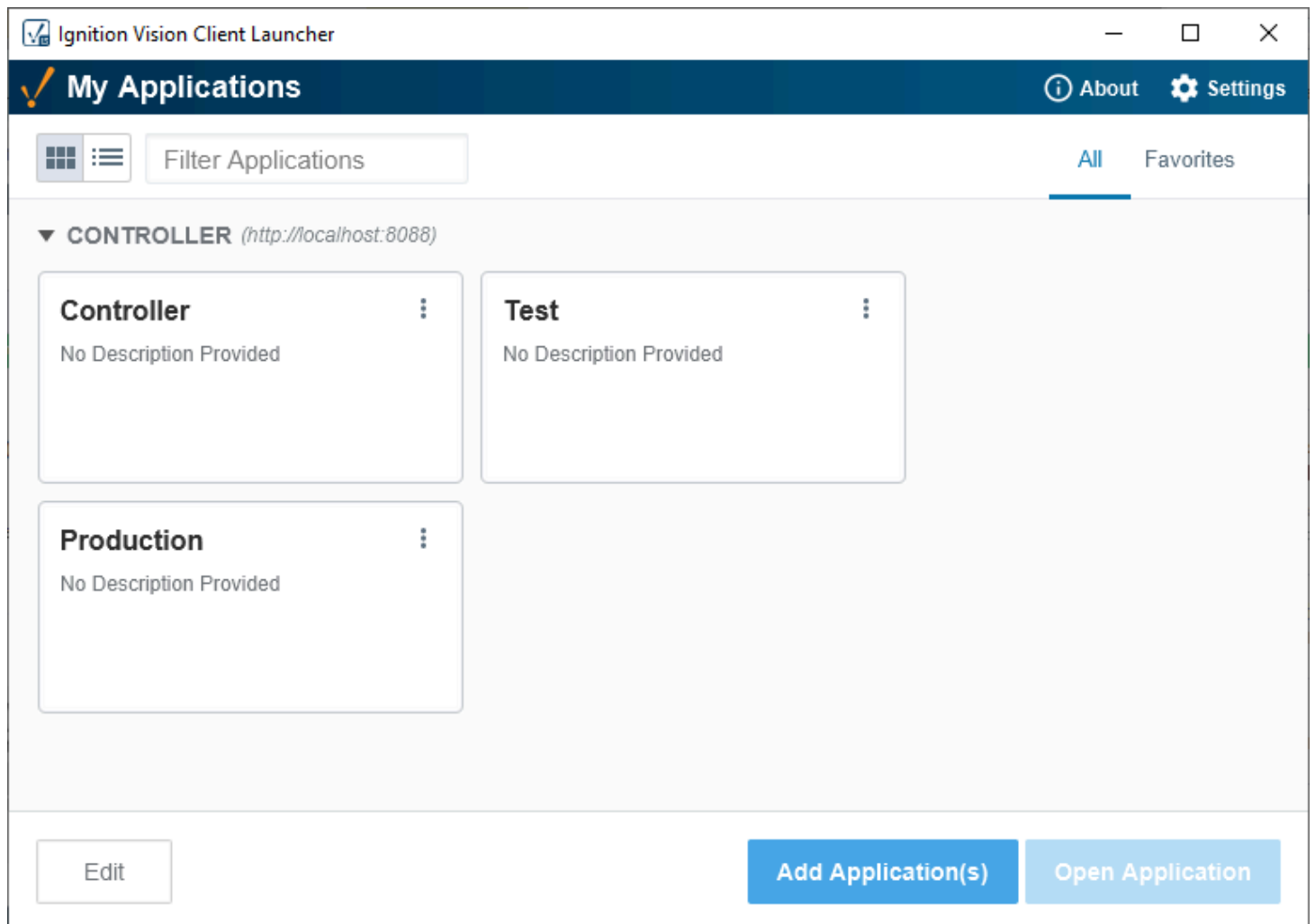


INDUCTIVE  
UNIVERSITY

## Launching a Client

[Watch the video](#)

The Vision Client Launcher opens Vision Clients from an Ignition Gateway. Once your Vision projects are added to the Vision Client Launcher, they will be displayed under **My Applications** and organized by Gateway. This page describes the unique Vision Client Launcher settings, deploying the launcher, and Command Line Arguments.



The Vision Client Launcher is available under the **Home** section of the Gateway Webpage on the **Vision > Download** page. More information on installing any of the Launchers can be found on the [Launchers and Workstation](#) page. For information on accessing Vision projects remotely, refer to the [Accessing Projects Remotely](#) section.

# Vision Client Application Settings

This section details settings for applications in the Vision Client Launcher. To access the settings, click on the three dots menu on the **My Applications** window and select the **Manage** option. The General tab will open. The table below describes the settings that can be applied.

# Vision Client Launcher Application Settings

| Setting Name          | Description                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application Name      | The descriptive name of the application. This is independent of the project name that corresponds to a project on the Gateway. Instead, this is the name of the application as it is defined in the Launcher.                                                                                                                                                                                                                      |
| Gateway Address       | The address to the Gateway in the format http[s]://host:port                                                                                                                                                                                                                                                                                                                                                                       |
| Description           | An optional description for the application that will be listed on the Application in the launcher. Defaults to the Project's description.                                                                                                                                                                                                                                                                                         |
| Vision Client Project | The name of the project containing Vision resources that the Application will attempt to launch. The Vision Client Project field is required.                                                                                                                                                                                                                                                                                      |
| Fallback Application  | The name of the application (configured in the same launcher) to use if the number of retries has been exceeded. The fallback is only utilized if the <b>Retries</b> setting is greater than 0.                                                                                                                                                                                                                                    |
| Image Path            | <p>This will allow the icon of the application to be set within the Designer and it will be downloaded and displayed as the icon for the application as well as the shortcuts. If no path is set, the default icon is used. If this is set to a different icon path, that icon will be used. The image path notation is a filepath on the local system.</p> <p>Supported image formats includes PNG, SVG, GIF, and JPEG files.</p> |
| Window Mode           | <p>Controls the client mode. Available options are:</p> <ul style="list-style-type: none"><li><code>window</code>: Launches the client in Windowed Mode</li><li><code>fullscreen</code>: Launches the client in Fullscreen Mode</li></ul>                                                                                                                                                                                          |
| Screen Index          | The screen index indicates which monitor to use.                                                                                                                                                                                                                                                                                                                                                                                   |
| Timeout               | The maximum number of seconds to allow for any Gateway communication. Any communication that exceeds this amount will cause the Vision Client Launcher to abort the communication and try again if configured.                                                                                                                                                                                                                     |

| Setting Name  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Retries       | <p>How many times to attempt to contact a Gateway again if an error occurred during communication. Available values are:</p> <ul style="list-style-type: none"><li>• -1 : Retry indefinitely, or until the launcher is manually closed.</li><li>• 0 : Zero retries, or abort after the first failure.</li><li>• 1 (or more): Determines the number of retries: i.e., a value of 5 means five retries. If the number of retries is exceeded, then the launcher will attempt to launch the Fallback Application.</li></ul> <p>If the number of retries is exceeded, then the Launcher will attempt to launch the Fallback Application.</p> |
| Init Heap     | The initial heap memory size for the Client.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Max Heap      | The maximum heap memory size for the Client.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| JVM Arguments | Arguments to append to client startup. These should start with a <code>-D</code> and be separated by semi-colons.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

General

Client Tag Overrides

Application Name

My Project

Gateway Address

http://localhost:8088

Description

Vision Client Project

MyProject

Fallback Application

Image Path

Window Mode

Screen Index

window

0

Timeout

Retries

Init Heap

Max Heap

30

-1

32M

256M

JVM Arguments

ACTIONS

Export Config

Create Desktop Shortcut

Cancel

Ok

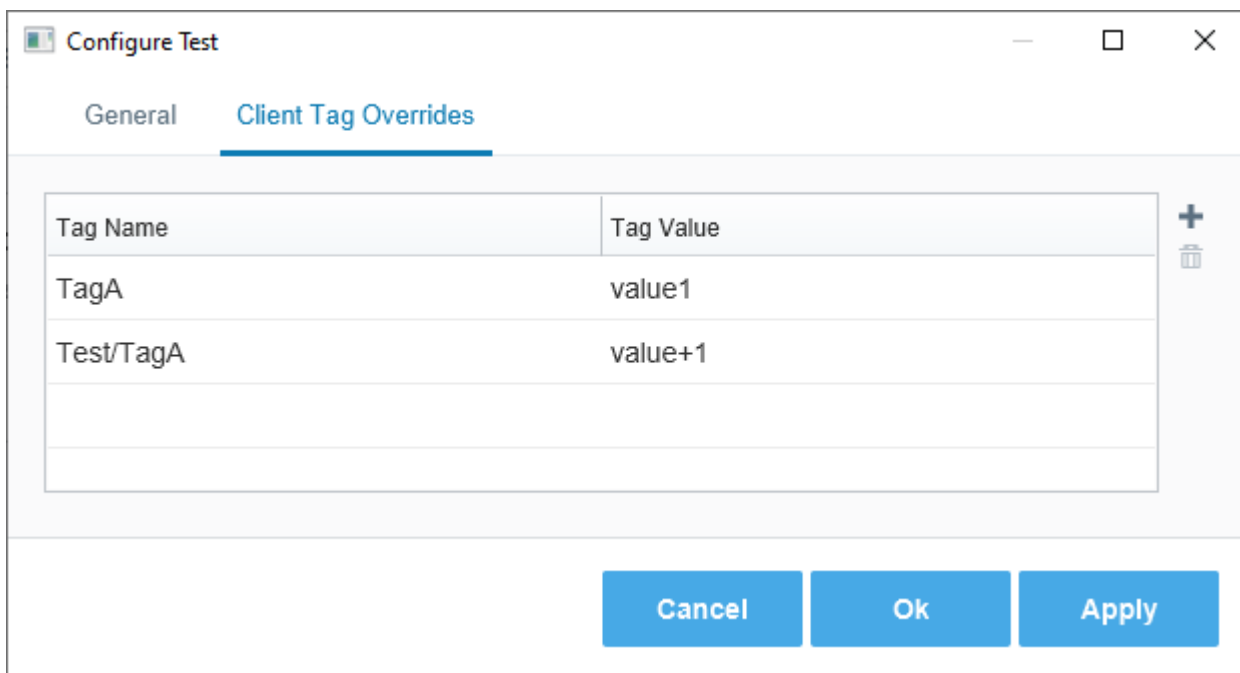
Apply

## Vision Client Tag Override Settings

Click on the **Client Tag Overrides** tab to create or update any tags. The table below shows the Client Tag Override setting that can be applied to each designer.



| Setting Name         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Client Tag Overrides | <p>Allows Client tags to be overridden on the Vision Client. These are set using the table on the application configuration screen by adding rows with the names of the tags and the corresponding values.</p> <p>When applying the overrides from command line, the tags must first be defined as launch parameters, then a value can be set on the parameters.</p> <p>Vision Client tag overrides within folders and passing Client tag overrides are supported by using a '+' icon as an escape character. This happens automatically if you are configuring overrides in the Client Launcher. To learn more about how to configure Client Tag Overrides, refer to <a href="#">Overriding Vision Client Tags</a>.</p> |



Configure Test

General **Client Tag Overrides**

| Tag Name  | Tag Value |
|-----------|-----------|
| TagA      | value1    |
| Test/TagA | value+1   |
|           |           |
|           |           |

Cancel Ok Apply

For additional application settings, refer to the [Launchers and Workstation](#) page.

## Redundancy

The Vision Client Launcher can take advantage of a redundant Gateway setup. Whenever a connection is established with a master Gateway, the backup Gateway IP address is automatically stored in the client launcher configuration file. If the master Gateway cannot be contacted the next time the client launcher is run, an attempt is made to contact the backup Gateway. If the backup cannot be contacted, the Client Launcher switches between contacting the primary Gateway and the backup Gateway until one responds or the user closes the launcher.

# Command Line/Terminal

Clients can be launched from the Client Launcher via command/terminal. When called in this way, many of the application properties may be overridden for the one call. The overrides use the same property names as noted in the [Application Property Reference Table](#), under the "JSON name" column.

Windows:

```
"C:\ClientLauncher\visionclientlauncher.exe" application=myproject  
window.mode=window
```

Linux:

```
./visionclientlauncher.sh application=myterminal window.mode=fullscreen screen=0
```

The Vision Client Launcher must be installed and have an application added for the command line/terminal commands to work. There are a few important notes when using the command line/terminal to launch a project from the Vision Client Launcher.

- The **application** argument requires the application name in the Launcher, not the project name. You can open the launcher to determine what the application name is. Adding new applications in the launcher uses the Project title by default.
- Applications may contain spaces in their name. However, when launching from the command line/terminal, spaces should be escaped with **%20**. For example, if our application was named **my project**, then we could call it with the following:

```
"C:\ClientLauncher\visionclientlauncher.exe" application=my%20project
```

# Command Line Arguments

| Argument                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>application</code>           | The name of the application to launch.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <code>window.mode</code>           | Controls the Client mode. Available options are: <ul style="list-style-type: none"><li><code>window</code>: Launches the Client in Windowed Mode</li><li><code>fullscreen</code>: Launches the Client in Fullscreen Mode</li></ul>                                                                                                                                                                                                                       |
| <code>screen</code>                | The screen index indicates which monitor to use.                                                                                                                                                                                                                                                                                                                                                                                                         |
| <code>fallback.application</code>  | The name of the application to use if the number of retries has been exceeded.                                                                                                                                                                                                                                                                                                                                                                           |
| <code>timeout</code>               | The maximum number of seconds to allow for any Gateway communication and try again if configured.                                                                                                                                                                                                                                                                                                                                                        |
| <code>retries</code>               | How many times to attempt to contact a Gateway again if an error occurs. <ul style="list-style-type: none"><li>-1 : Retry indefinitely, or until the launcher is manually closed.</li><li>0 : Zero retries, or abort after the first failure.</li><li>1 (or more): Determines the number of retries: i.e., a value of 5 means 5 retries.</li></ul> If the number of retries is exceeded, then the launcher will attempt to launch the application again. |
| <code>init.heap</code>             | The initial heap size (memory) for the Client.                                                                                                                                                                                                                                                                                                                                                                                                           |
| <code>max.heap</code>              | The maximum heap size (memory) for the Client                                                                                                                                                                                                                                                                                                                                                                                                            |
| <code>-Djavaws.launchparams</code> | Defines Client tags that can be overwritten upon launch. The use of this is an additional argument that utilizes the tag names delimited by a semicolon: <pre>// Establishes the tag names -Djavaws.launchparams="Tag1;Tag2"  // Sets values on the tags -Djavaws.launchparams.Tag1=10 -Djavaws.launchparams.Tag2=20  //An actual call would look like: "C:\ClientLauncher\visionclientlauncher.exe" application=myapp</pre>                             |

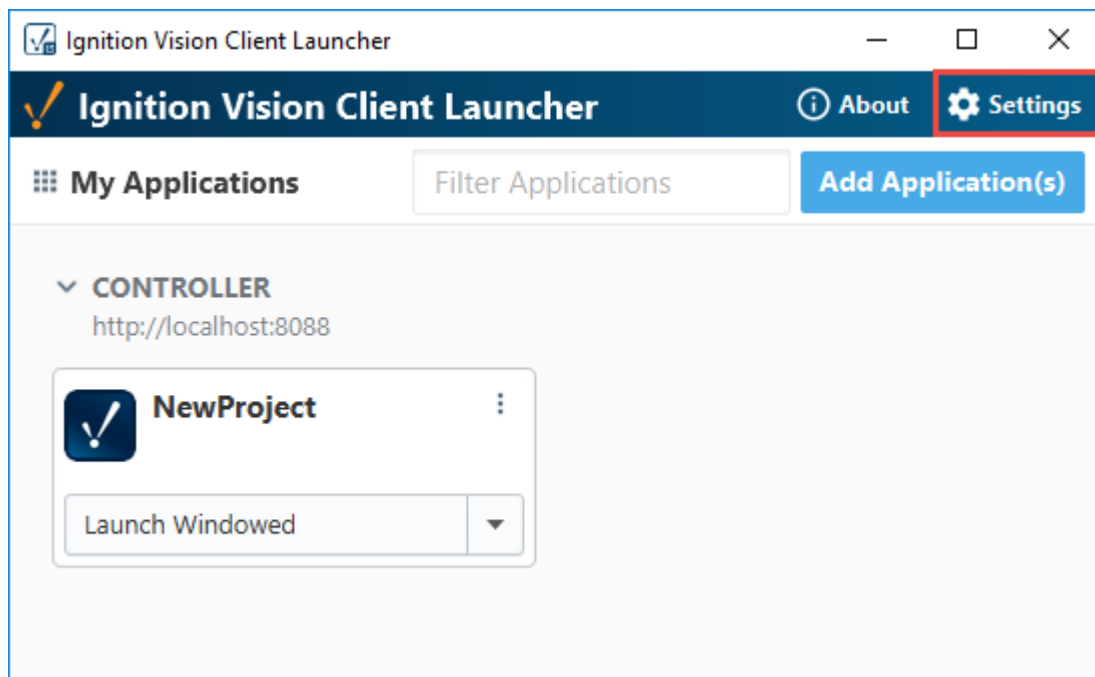
| Argument                 | Description                                                                                                                                                                                                                                                                                                                                       |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>config.json</code> | <p>Allows you to point the launcher to a launcher configuration file from command line overrides. The argument expects a path to a JSON export file, specifically the file path to the file you exported from the launcher.</p> <pre>"C:\ClientLauncher\visionclientlauncher.exe" config.json="C:\ClientLauncher\visionclientlauncher.json"</pre> |

# Vision Client Launcher Settings

You can customize your Vision Client Launcher settings through either the GUI or by modifying a [file on the local file system](#). Regardless of method, both utilize the properties specified under the [Vision Client Launcher Settings Reference Table](#).

## Launcher Settings

You can find the **Settings**  button in the upper right corner of the Vision Client Launcher.



You can choose to use the default settings or customize your Client applications. There are three different **Actions** within your **Launcher Settings** in the Vision Client Launcher:

- **Export Launcher Config:** Exports a configuration of the the Vision Client Launcher, as a JSON file (i.e., `vision-client-launcher.json`). Taking an export is useful in cases where you want multiple launcher instances to use the same settings. The content of the export file is based on the last saved configurations settings of the Launcher.
- **Import Launcher Config:** Imports your launcher configurations from a Vision Client Launcher export file.
- **Import Application Config:** Creates a new client application configuration from an export, adding a new application to the Launcher. The import file is the same generated by an [application export](#).

After updating any of the Client Launcher settings, click the **Save Changes** button. Refer to the list of additional launcher settings in the [reference table](#) below.

Ignition Vision Client Launcher

Ignition Vision Client Launcher

AboutSettings

/ Launcher Settings

CancelSave Changes

GENERAL SETTINGS

Default Application

Logging Level

INFO

Multicast Address

231.1.1.1

Multicast Port

4446

Auto Exit on Launch

NEW APPLICATION SETTINGS

Timeout

30

Retries

-1

Init Heap

Max Heap

JVM Arguments

Client Tag Overrides

| Tag Name                               | Tag Value |
|----------------------------------------|-----------|
| Click '+' to add a Client Tag Override |           |

TRUSTED CERTIFICATES

| Common Name                            | Expiration |
|----------------------------------------|------------|
| Click '+' to add a trusted Certificate |            |

ACTIONS

Export Launcher Config

Import Launcher Config

Import Application Config

## Launcher Configuration Using JSON

In addition to using the GUI, these configurations changes can be made by modifying the `vision-client-launcher.json` file (created during installation of the launcher). The file is located at:

```
{user folder}\.ignition\clientlauncher-data\vision-client-launcher.json
```

The preferred method of configuration is with the GUI, but JSON modification is useful when attempting to load multiple application configurations simultaneously.

A reference to the various properties that can be modified via JSON are listed in the [Vision Client Launcher Settings Reference Table](#). However, the JSON file has the following setting that isn't available from the GUI:

- `lock.configuration`: When set to true, the application list and individual application configurations cannot be modified. Effectively restricting the ability to add applications and edit the launcher's configurations.

## Vision Client Launcher Settings Reference Table

### Launcher Settings - Configurations for the Launcher

| Property Setting    | Description                                                                                                                                                  | JSON Name              |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| Default Application | When set, the Launcher will attempt to automatically launch the specified application when running. If left blank, no applications will automatically start. | default.application    |
| Logging Level       | Level of logging that will be used for the Launcher: INFO, TRACE, DEBUG, WARN, and ERROR.                                                                    | logger.level           |
| Multicast Address   | The address that will be used to listen for multicast broadcasts from Gateways.                                                                              | multicast.address      |
| Multicast Ports     | The port that will be used to listen for multicast broadcasts from Gateways.                                                                                 | multicast.receive.port |
| Auto Exit on Launch | Automatically close the Launcher window when a Client is started.                                                                                            | autoexit               |

### Application Defaults - Default Configurations for New Applications

| Property Setting     | Description                                                                                                                                                                                                                                                                                                                                                                                                                         | JSON Name            |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| Timeout              | Maximum number of seconds allowed for any Gateway communication. Any communication that exceeds this amount will cause the Client Launcher to abort the communication and try again if configured.                                                                                                                                                                                                                                  | timeout              |
| Retries              | <p>The number of times a Client will attempt to contact a Gateway again if an error occurred during communication. Available values are:</p> <ul style="list-style-type: none"> <li>• -1 : Retry indefinitely, or until the Launcher is manually closed.</li> <li>• 0 : Zero retries, or abort after the first failure.</li> <li>• 1 (or more): Determines the number of retries: i.e., a value of 5 means five retries.</li> </ul> | retries              |
| Initial Heap         | Amount of memory to be allocated at startup.                                                                                                                                                                                                                                                                                                                                                                                        | init.heap            |
| Max Heap             | Maximum amount of memory allocation for heap size.                                                                                                                                                                                                                                                                                                                                                                                  | max.heap             |
| JVM                  | Arguments to append to Client startup. These should start with a  and be separated by semi-colons.                                                                                                                                                                                                                                               | jvm.arguments        |
| Client Tag Overrides | Client tags and their values that are set when the Client launches.                                                                                                                                                                                                                                                                                                                                                                 | client.tag.overrides |

## Trusted Certificates

You can add security certificates to the Launcher.

While attempting to launch an application, the launcher will check against the application's host Gateway, and attempt to automatically download any required certificates. In addition, certificates can be manually added using the example below.

1. Access Vision Client Launcher settings by clicking **Settings** on the top right of the Vision Client Launcher window.
2. In the Trusted Certificates section, click the **Add**  icon.



Ignition Vision Client Launcher

✓ Ignition Vision Client Launcher

About

Settings

Launcher Settings

CancelSave Changes

GENERAL SETTINGS

Default Application

Logging Level

INFO

Multicast Address

231.1.1.1

Multicast Port

4446

Auto Exit on Launch

NEW APPLICATION SETTINGS

Timeout

30

Retries

-1

Init Heap

Max Heap

JVM Arguments

Client Tag Overrides

| Tag Name                               | Tag Value |
|----------------------------------------|-----------|
| Click '+' to add a Client Tag Override |           |

TRUSTED CERTIFICATES

| Common Name                            | Expiration |
|----------------------------------------|------------|
| Click '+' to add a trusted Certificate |            |

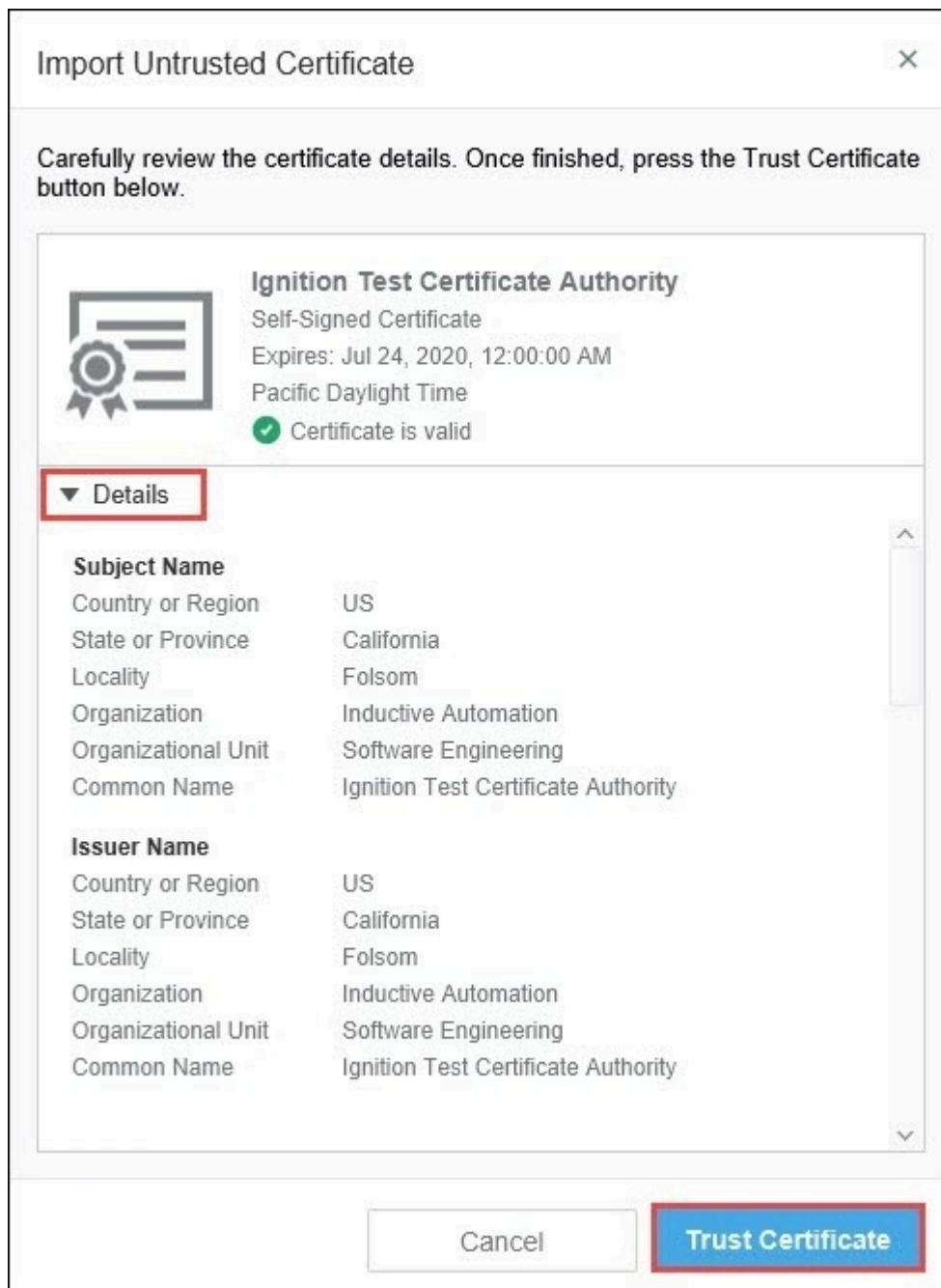
ACTIONS

Export Launcher Config

Import Launcher Config

Import Application Config

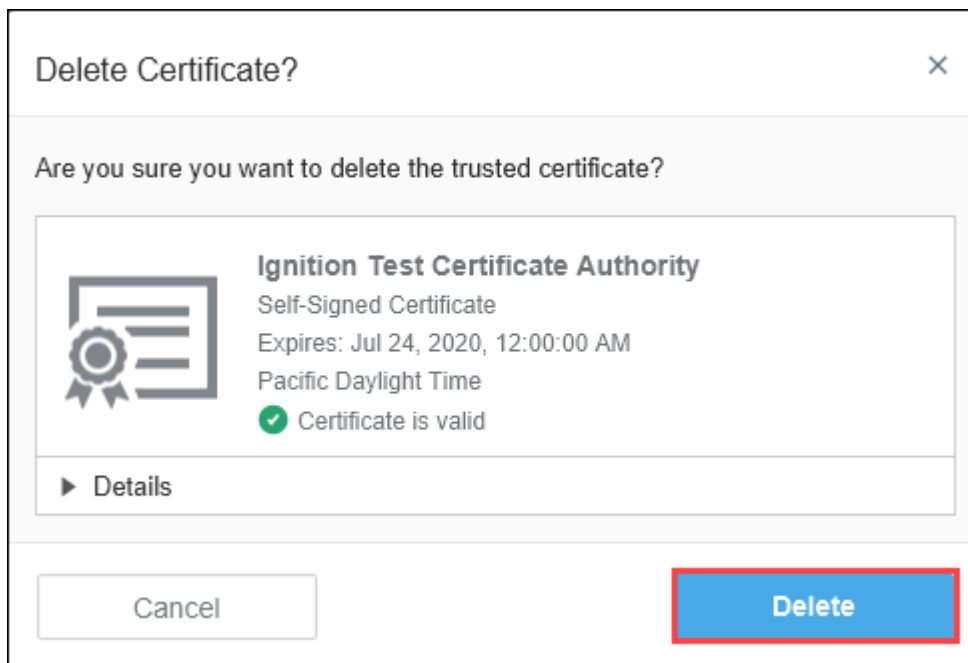
3. Navigate to the location of the certificate on your system and choose **Open**.
4. Information about the certificate is displayed. To view complete details, click the **Expand**  icon next to Details. If everything looks OK, click **Trust Certificate**.



5. Once a certificate is imported, you can view its details by clicking the **Information**  icon.

## Delete a Certificate

1. To delete an imported certificate, access Vision Client Launcher settings by clicking **Settings** on the top right of any Vision Client Launcher window.
2. In the Trusted Certificates section, select the certificate you want to delete.
3. Click the **Delete**  icon.
4. You'll get a confirmation window. If the certificate is the correct one you want to delete, click the **Delete** button.

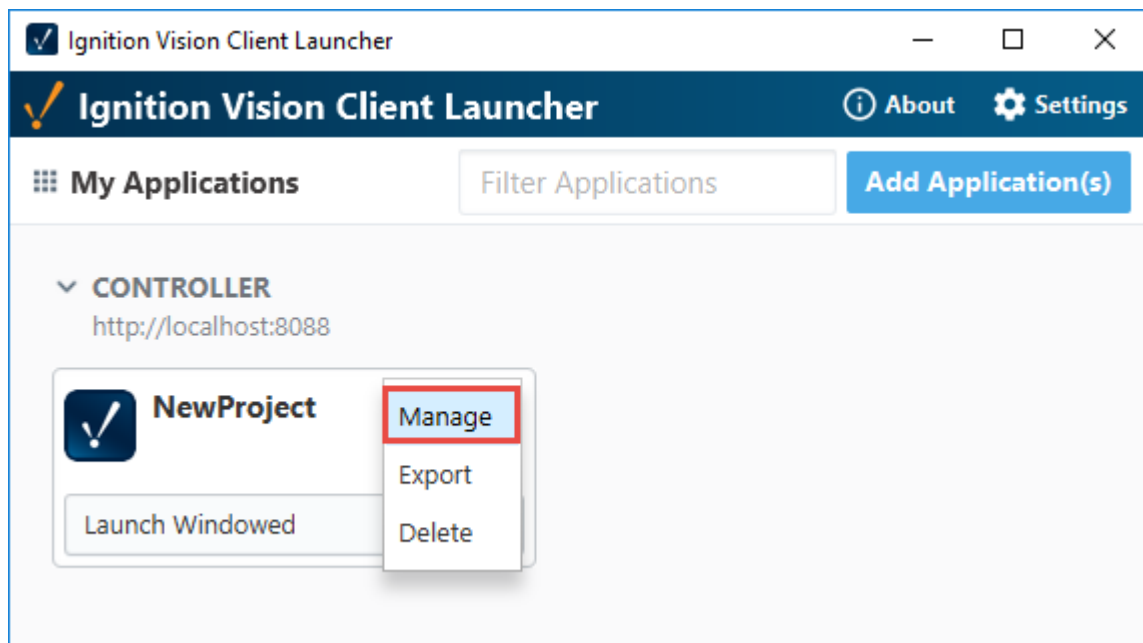


## Export a Certificate

1. To export an imported certificate, access Vision Client Launcher Settings by clicking **Settings** on the top right of any Vision Client Launcher window.
2. In the Trusted Certificates section, select the certificate you want to export.
3. Click the **Export**  icon.
4. Navigate to the location you want to save the certificate and click **Save**.

## Launcher Application Settings

For each project application, you can update the default settings by clicking the **three dots menu**  icon next to the project name, and select **Manage** to open the Manage Project Settings window. The **Export** command exports the configuration settings to a `.json` file. The **Delete** command deletes the project application from the launcher.



You can choose to use the default settings or customize your project client applications. There are three different **Actions** under **Manage Project Settings** in the Vision Client Launcher:

- **Launch Application:** Launches the your application in the Vision Client Launcher.
- **Export Config:** Exports your updates to the Vision Client Launcher file (i.e., `vision-client-launcher.json`). The resulting export file contains the last saved configuration of the application.
- **Create Desktop Shortcut:** Creates a shortcut to your application on your desktop, using the last **saved** application configuration.

When you are finished updating any of the Launcher settings, click the **Save Changes** button.

Ignition Vision Client Launcher

Ignition Vision Client Launcher

AboutSettings

/ Manage 'NewProject'

CancelSave Changes

Application Name

NewProject

Gateway Address

http://localhost:8088

Description

Vision Client Project

NewProject

Fallback Application

Image Path

VisionIcon

Window Mode

window

Timeout

30

Init Heap

32M

Screen Index

0

Retries

-1

Max Heap

256M

JVM Arguments

Client Tag Overrides

| Tag Name | Tag Value |   |
|----------|-----------|---|
|          |           | + |
|          |           | - |

Click '+' to add a Client Tag Override

ACTIONS

Launch Application

Export Config

Create Desktop Shortcut

# Application Property Reference Table

| Setting Name         | Description                                                                                                                                                                                                                                                                              | JSON Name            |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| Application Name     | The descriptive name of the application. This is independent of the project name that corresponds to a project on the Gateway. Instead, this is the name of the application as it is defined in the Launcher.                                                                            | application          |
| Project              | The Vision project that exists on the Gateway that this application will load.                                                                                                                                                                                                           | project              |
| Description          | An optional brief note about the application. The description will appear in the Launcher. If left blank, a description will not appear.                                                                                                                                                 | description          |
| Window Mode          | Controls the Client mode. Available options are: <ul style="list-style-type: none"><li><code>window</code>: Launches the Client in Windowed Mode</li><li><code>fullscreen</code>: Launches the Client in Fullscreen Mode</li></ul>                                                       | window.mode          |
| Screen Index         | The screen index indicates which monitor to use.                                                                                                                                                                                                                                         | screen               |
| Image Path           | This will allow the icon of the application to be set within the Designer and it will be downloaded and displayed as the icon for the application as well as the shortcuts. If no path is set the default icon is used. If this is set to a different icon path, that icon will be used. | image.path           |
| Fallback Application | The name of the application to use if the number of retries has been exceeded. The fallback is only utilized if the <b>Retries</b> setting is greater than 0.                                                                                                                            | fallback.application |

| Setting Name         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | JSON Name            |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| Timeout              | The maximum number of seconds to allow for any Gateway communication. Any communication that exceeds this amount will cause the Vision Client Launcher to abort the communication and try again if configured.                                                                                                                                                                                                                                                                                                                                                                                                                                      | timeout              |
| Retries              | <p>How many times to attempt to contact a Gateway again if an error occurred during communication.</p> <p>Available values are:</p> <ul style="list-style-type: none"> <li>• -1 : Retry indefinitely, or until the launcher is manually closed.</li> <li>• 0 : Zero retries, or abort after the first failure.</li> <li>• 1 (or more): Determines the number of retries: i.e., a value of 5 means five retries. If the number of retries is exceeded, then the launcher will attempt to launch the Fallback Application.</li> </ul> <p>If the number of retries is exceeded, then the Launcher will attempt to launch the Fallback Application.</p> | retries              |
| Init Heap            | The initial heap size (memory) for the Client.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | init.heap            |
| Max Heap             | The maximum heap size (memory) for the Client. Value is set using megabytes, such as 1024M.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | max.heap             |
| Client Tag Overrides | <p>Allows Client tags to be overridden on the Vision Client. These are set using the table on the application configuration screen by adding rows with the names of the tags and the corresponding values.</p> <p>When applying the overrides from command line, the tags must first be defined as launch parameters, then a value can be set on the parameters.</p> <p>Vision Client Tag overrides within folders and passing Client tag overrides are supported by using a '+' icon as an escape character. This happens automatically if you are configuring overrides in the</p>                                                                | client.tag.overrides |

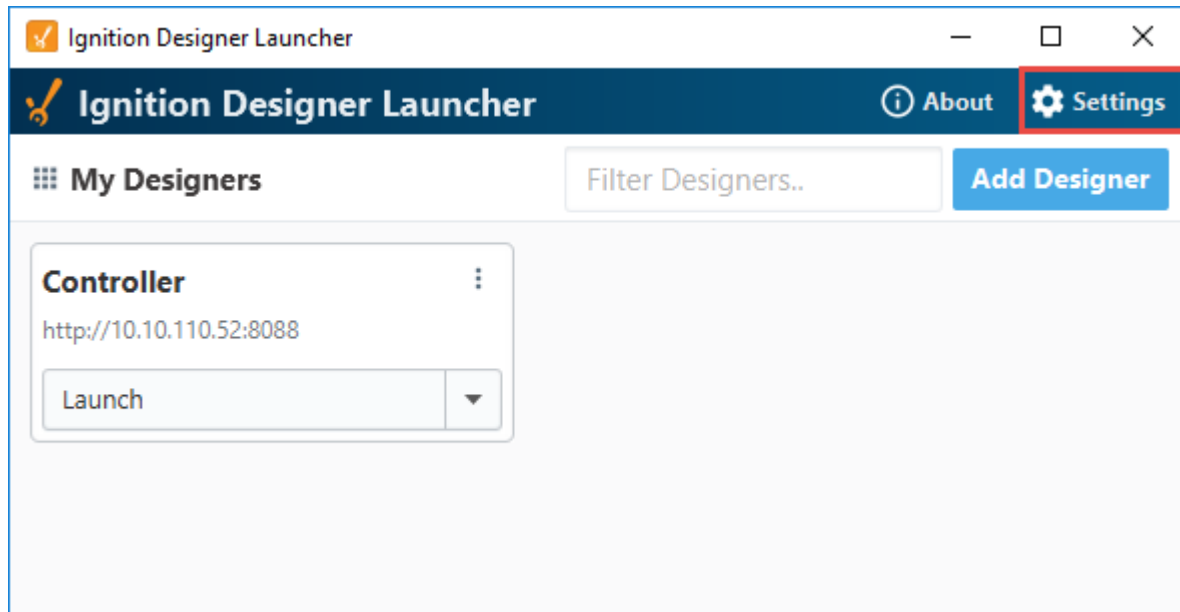
| Setting Name | Description                                                                                                                          | JSON Name |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------|-----------|
|              | Client Launcher. To learn more about how to configure Client Tag Overrides, refer to <a href="#">Overriding Vision Client Tags</a> . |           |



# Launcher Settings

## Launcher Settings

Each launcher has its own settings. To access the settings on a launcher, click **Settings** on the top right of any launcher window.



The Settings popup window will appear, listing settings for the Launcher to use. There are some shared settings, such as those under the **General** tab.

The image shows a screenshot of the 'Designer Launcher Settings' dialog box. The 'General' tab is selected, with other tabs being 'Designer Defaults' and 'Trusted Certificates'. The settings are organized into two columns. The left column contains 'Default Designer' (a dropdown menu set to 'Controller'), 'Multicast Address' (a text box containing '231.1.1.1'), and 'Auto Exit on Launch' (an unchecked checkbox). The right column contains 'Logging Level' (a dropdown menu set to 'TRACE') and 'Multicast Port' (a text box containing '4446'). Below these settings is a section titled 'ACTIONS' containing three buttons: 'Export Launcher Config', 'Import Launcher Config', and 'Import Application Config', each with a small icon. At the bottom right of the dialog are three buttons: 'Cancel', 'Ok', and 'Apply'.

| Setting             | Value                    |
|---------------------|--------------------------|
| Default Designer    | Controller               |
| Logging Level       | TRACE                    |
| Multicast Address   | 231.1.1.1                |
| Multicast Port      | 4446                     |
| Auto Exit on Launch | <input type="checkbox"/> |

**ACTIONS**

- Export Launcher Config
- Import Launcher Config
- Import Application Config

**Buttons:** Cancel, Ok, Apply

## Property Settings

The following tables represent common property settings in the **Designer Launcher**, **Vision Client Launcher** and **Perspective Workstation**. There are a few settings that are unique to each launcher application and are addressed on the corresponding launcher page.

## General Property Settings

**General Settings (Design Launcher, Vision Client Launcher and Perspective Workstation)**

| Property Setting    | Description                                                                                                                                                       | JSON Name              |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| Default Application | When set, the Launcher will attempt to automatically launch the specified application on launcher startup. If left blank no application will automatically start. | default.application    |
| Logging Level       | Level of logging that will be used for the Launcher. Useful for our support team, but can be used to help troubleshoot problems with the Launcher.                | logger.level           |
| Multicast Address   | The address that will be used to listen for multicast broadcasts from Gateways.                                                                                   | multicast.address      |
| Multicast Port      | The port that will be used to listen for multicast broadcasts from Gateways.                                                                                      | multicast.receive.port |
| Auto Exit on Launch | Automatically close the Launcher window when an application is started.                                                                                           | autoexit               |

## Default Property Settings

Default Settings (Designer Launcher and Vision Client Launcher)

| Property Setting | Description                                                                                                                                                                                                                                                                                                                                                                                                                  | JSON Name     |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Timeout          | Maximum number of seconds allowed for any Gateway communication. Any communication that exceeds this amount will cause the Launcher to abort and try again (if multiple retries are configured).                                                                                                                                                                                                                             | timeout       |
| Retries          | <p>The number of times the Launcher will attempt to contact a Gateway when launching an application.</p> <p>Available values are:</p> <ul style="list-style-type: none"> <li>• -1 : Retry indefinitely, or until the launcher is manually closed.</li> <li>• 0 : Zero retries, or abort after the first failure.</li> <li>• 1 (or more): Determines the number of retries: i.e., a value of 5 means five retries.</li> </ul> | retries       |
| Initial Heap     | Amount of heap memory to be allocated to the application on startup.                                                                                                                                                                                                                                                                                                                                                         | init.heap     |
| Max Heap         | Maximum amount of heap memory allocated to the application.                                                                                                                                                                                                                                                                                                                                                                  | max.heap      |
| JVM Arguments    | Arguments to append to Client startup. These should start with a <code>-D</code> and be separated by semi-colons. Mostly used by our support teams to aid with troubleshooting.                                                                                                                                                                                                                                              | jvm.arguments |

Designer Launcher Settings

General

Designer Defaults

Trusted Certificates

Timeout

Retries

Init Heap

Max Heap

30

-1

JVM Arguments

Cancel

Ok

Apply

## Trusted Certificates Property Settings

The Trusted Certificates tab shows the list of trusted security certificates by their common names and their expiration dates. Users can also add, delete, view certificate details, and export by clicking the respective icons on the right-hand side of the listed certificates. More information on adding certificates is included under [Adding Security Certificates to Clients](#).

Designer Launcher Settings

General

Designer Defaults

Trusted Certificates

| Common Name | Expiration              |
|-------------|-------------------------|
|             | May 5, 2024, 9:40:58 AM |
|             |                         |
|             |                         |
|             |                         |
|             |                         |
|             |                         |
|             |                         |
|             |                         |
|             |                         |

+

i

Cancel

Ok

Apply

# Launcher JSON Configuration Files

The settings for each launcher are stored into a configuration file.

```
Linux/Mac
~/.ignition/clientlauncher-data

Windows
C:\Users\username\.ignition\clientlauncher-data
```

On Windows systems, if the Launcher was installed under "all users", then the configuration files are located in directories under:

```
C:\Users\username\AppData\Roaming\Inductive Automation\
```

In either case, each type of launcher gets its own JSON configuration file. Launcher and application settings can be modified directly from this configuration file. In addition, some administrative settings are only available in the JSON configuration file. Configuration changes must be made while the launcher is closed. Notable settings are listed below.

| Settings                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| lock.configuration            | <p>Determines if users are able to make changes to the Launcher from the GUI.</p> <p>Set to true to disable the Launcher's Settings menu, prevent users from managing any application from the GUI, and remove the ability to add new applications from the GUI. Defaults to false.</p>                                                                                                                                                                                                                     |
| version.updates.prompt        | <p>When a launcher attempts to launch an application, it checks the Gateway version against the Launcher's download version. If the Launcher has not been updated within a set number of Gateway updates versions (see version.updates.revision.diff ), the Launcher will prompt the user to upgrade the Launcher.</p> <p>Setting this property to false will disable this update check. Disabling this property is discouraged, as newer launchers could have beneficial features or security updates.</p> |
| version.updates.revision.diff | <p>Dictates the number of revision differences before a launcher will prompt the user to upgrade. Defaults to 3, meaning 3 minor version updates (for example, 8.1.0 to 8.1.3 would trigger the update prompt, but 8.1.0 to 8.1.2 would not).</p>                                                                                                                                                                                                                                                           |
| trust.store                   | <p>Allows the Launcher to specify which trust store to use. See the <a href="#">Trust Stores</a> section for more details.</p>                                                                                                                                                                                                                                                                                                                                                                              |
| allow.uri.schemes             | <p>Allows the specified URL protocols to launch applications directly from the operating system. For example, a <code>vision</code> URL protocol opens the Vision Client Launcher, while <code>mailto</code> would allow an email client to open. Accepted values include <code>perspective</code>, <code>vision</code>, <code>designer</code>, <code>tel</code>, <code>sms</code>, and <code>mailto</code>.</p> <p><b>Note:</b> This setting is scoped to Workstation only.</p>                            |

## Trust Stores

The table below lists possible values you can use to utilize different trust stores.

| trust.store value | Windows               | Mac OS                | Linux                 |
|-------------------|-----------------------|-----------------------|-----------------------|
| system            | Windows-ROOT          | KeychainStore         | ca-certificates       |
| user              | Windows-MY            | KeychainStore         | ca-certificates       |
| jvm               | Java internal cacerts | Java internal cacerts | Java internal cacerts |

The OS trust stores detailed in the table above will be used by running Designers, Vision Clients, and Perspective Workstations once launched. Default is **jvm**. which will match existing behaviors of launchers that support certificate imports from within the application. All trust store types which are not jvm require launching Clients and Designers against Gateways which include support for the specified type. Retargets also conform to this requirement. Additionally, non-jvm trust stores will map to their named Java Trust Store, with the exception of **ca-certificates**.

To change the trust.store value for your launchers, you will need to first exit the launcher (if it isn't already closed), then edit the trust.store property in your launcher's `.json` file. This file is typically located at

`C:\Users\[YOUR USERNAME]\.ignition\clientlauncher-data.`

```

1  {
2    "global": {
3      "client.defaults": {
4        "timeout": 30,
5        "retries": -1,
6        "init.heap": null,
7        "max.heap": null,
8        "use.custom.jre": false,
9        "custom.jre.path": "${JAVA_HOME}/bin/java",
10       "jvm.arguments": [],
11       "client.tag.overrides": {}
12     },
13     "autoexit": false,
14     "default.application": "",
15     "multicast.address": "231.1.1.1",
16     "multicast.receive.port": 4446,
17     "lock.configuration": false,
18     "logger.level": "INFO",
19     "version.updates.prompt": true,
20     "version.updates.revision.diff": 3,
21     "trust.store": "jvm"
22   },

```

The trust.store property is the last property in the global class

Aside from specifying the trust.store value that you would like the launcher to use, there may be additional, operating system-specific steps you need to go through.

## Windows



1. Make sure the Launcher you want to update the trust store for is closed.
2. Reinstall the .crt file. You can do this by opening the .crt file and clicking **Install Certificate...**
3. Select which user(s) you would like to install the certificate for. Note that you may need administrative permissions to install the certificate for the local machine.
4. Select the store where you want the certificate to reside.
  - If you are installing the certificate for the current user, you should put the certificate in the **Personal** store.
  - If you are installing the certificate for the local machine, you should put the certificate in the **Trusted Root Certification Authorities** store.
5. Once the wizard finishes installing the certificate, press **Finish** to complete the operation.

## MacOS

1. Make sure the Launcher you want to update the trust store for is closed.
2. Add your certificate to your operating system's KeychainStore.
3. Make sure that the certificate you added is trusted either manually or automatically.

## Linux

1. Make sure the Launcher you want to update the trust store for is closed.
2. Run the following commands in the terminal:

### Linux Terminal Commands

```
$ sudo apt-get install -y ca-certificates
$ sudo cp local-ca.crt /usr/local/share/ca-certificates
$ sudo update-ca-certificates
```

3. Your operating system will then copy any certificates to their appropriate directories and then update the certificate bundle.

### NOTE

For additional information on installing certificates in Linux's trust store, see [Ubuntu's official documentation](#).

CA certificates will instead load PEM bundles or certificate directories as defined by the CA certificates package available for most Linux distributions. Because of this, CA certificates also support two additional system properties, which are listed in the table below:

| Property                                | Description                                                                                                                             |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <code>ignition.net.ssl.certDir</code>   | System property to use when you are using ca-certificates and want your certificate to load an openssl compliant certificate directory. |
| <code>ignition.net.ssl.pemBundle</code> | System property to use when you are using ca-certificates and want your certificate to load a PEM bundle.                               |

## Adding Security Certificates to Clients

Security certificates can be installed to all of our launchers in multiple ways. This is generally only required when the Gateway hosting the application has SSL enabled, and is using either self-signed certificates or certificates signed by a certificate authority internal to a particular organization.

The process is listed below. Note that you will need to repeat the steps below for each applicable Gateway.

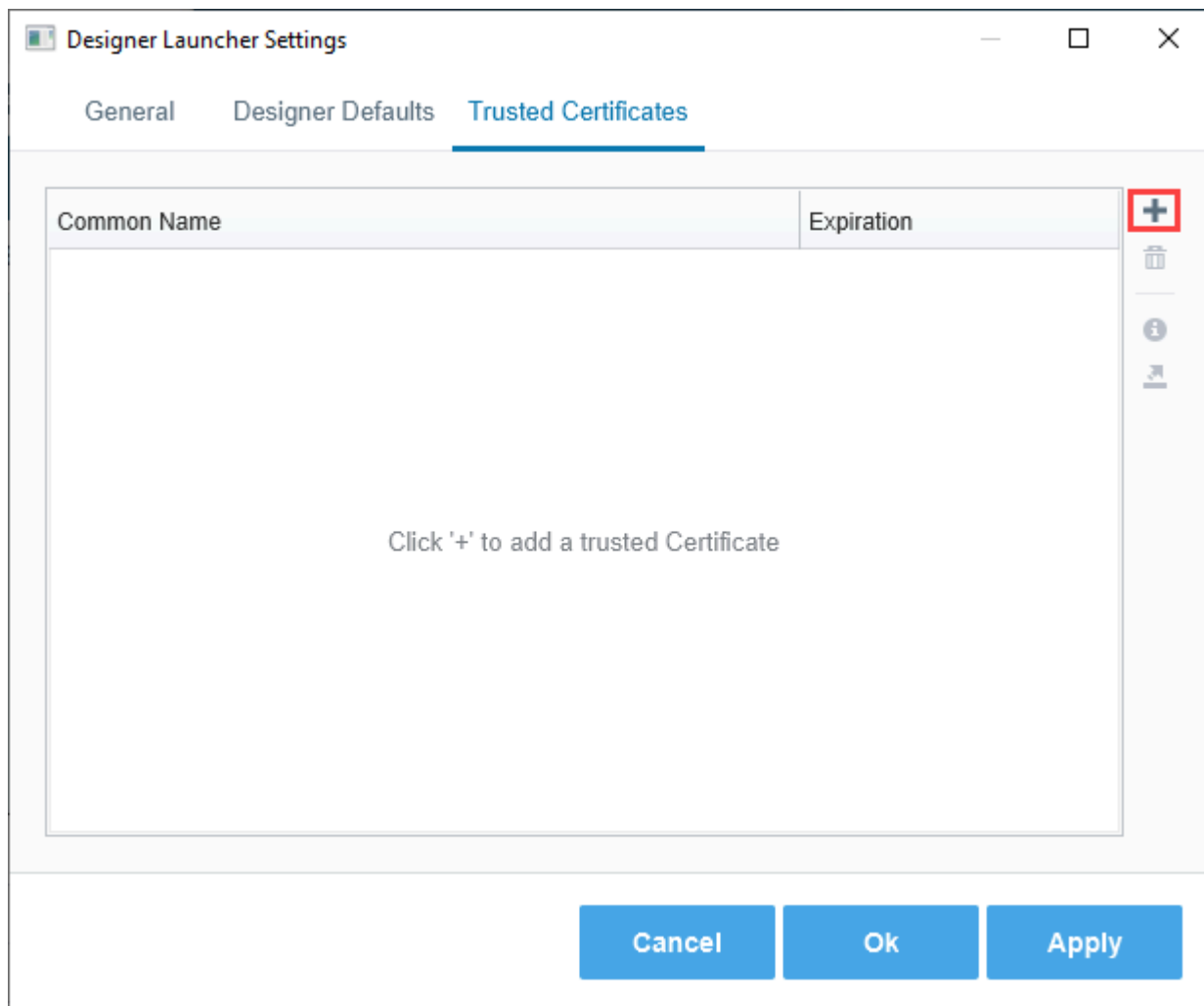
1. Navigate to the Gateway web interface.
2. Download the certificate. Most web browsers provide this functionality, usually via the address bar or some other means.
3. Once you have a copy of the certificate, place the certificate into the following directory:

```
{user folder}\.ignition\clientlauncher-data\certificates
```

When adding certificates to this directory, they are trusted immediately with no further action required by the user.

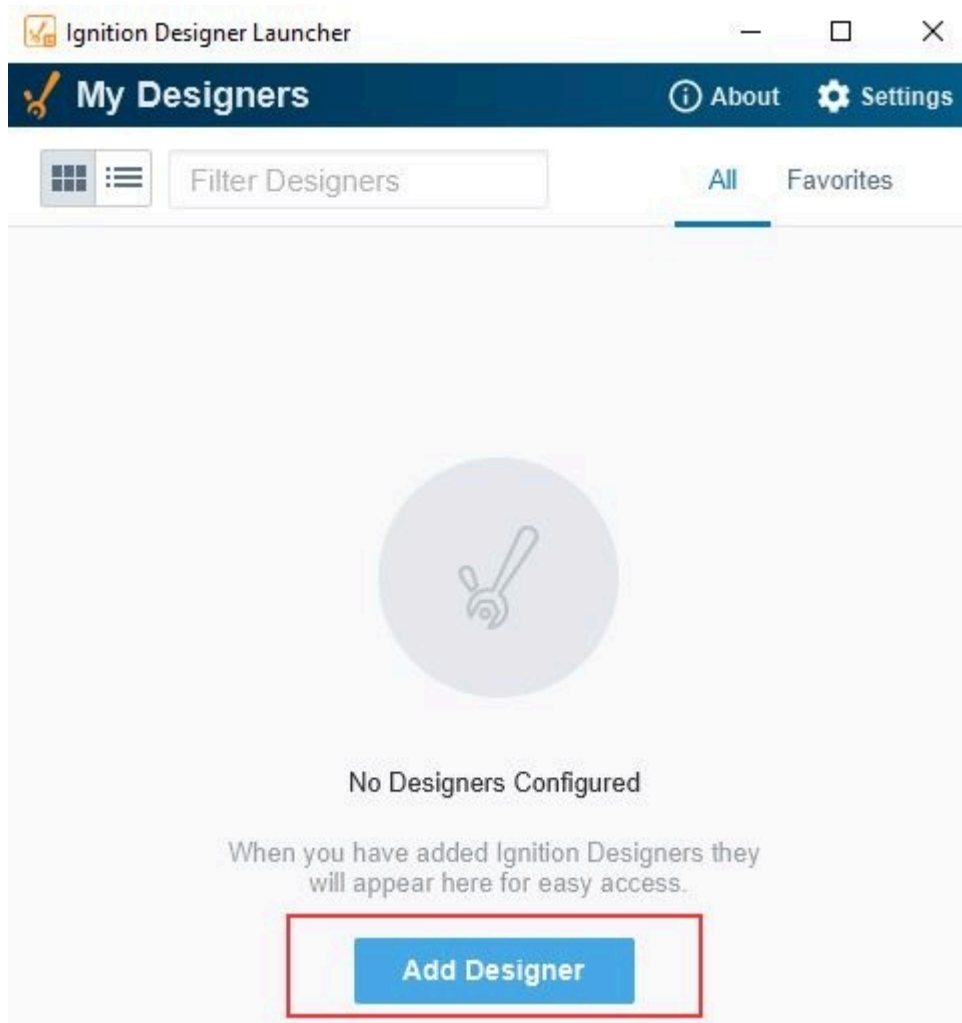
Additionally, there are two more ways to manually add security certificates to the Launcher. Both of these methods will mimic the behavior of certificates imported using a trust store. Using the Trusted Certificates tab of the Designer Launcher's settings allows any server with that certificate in its chain of trust to be trusted going forward. However, if you only want to add a single server, you should use the **Manual** tab on the **Add Designer** pop up. The process for trusting a single server's certificate uses the Designer Launcher, but the procedure is the same for the Vision Client Launcher, and the Perspective Workstation.

To add a Trusted Certificate and allow all servers with that certificate to be accepted, click the **Add**  icon on the **Trusted Certificates** tab of the Designer Launcher Settings.

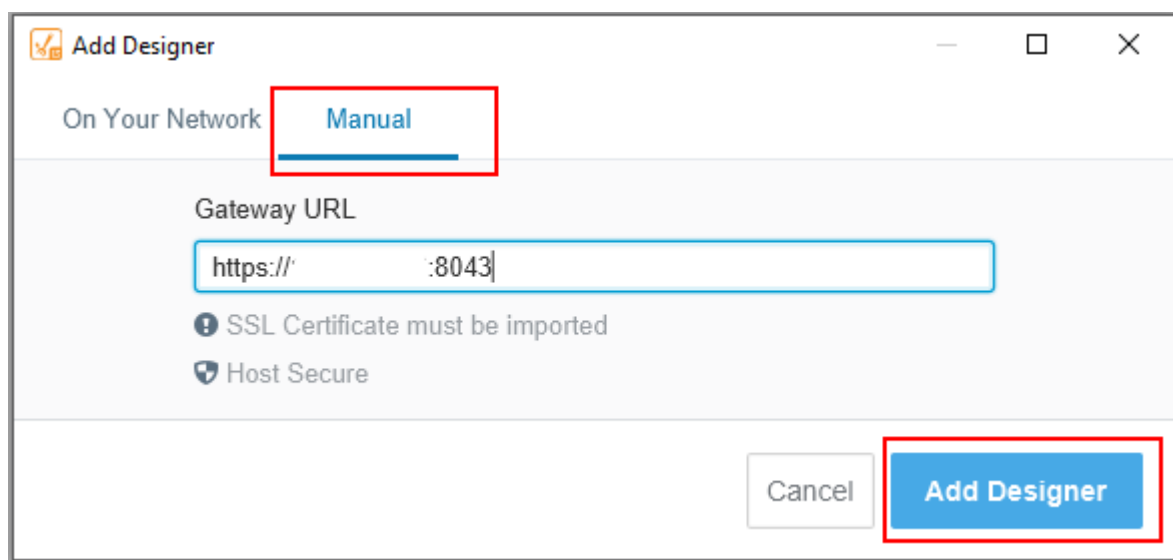


To manually trust a single server's security certificate:

1. Open the Designer Launcher, and select **Add Designer**.



2. Select **Manual**, and search for your secure Gateway server (https and port 8403). The designer launcher will detect the certificate and the message *SSL Certificate must be imported* will be displayed. To view the certificate, click on **Add Designer**.

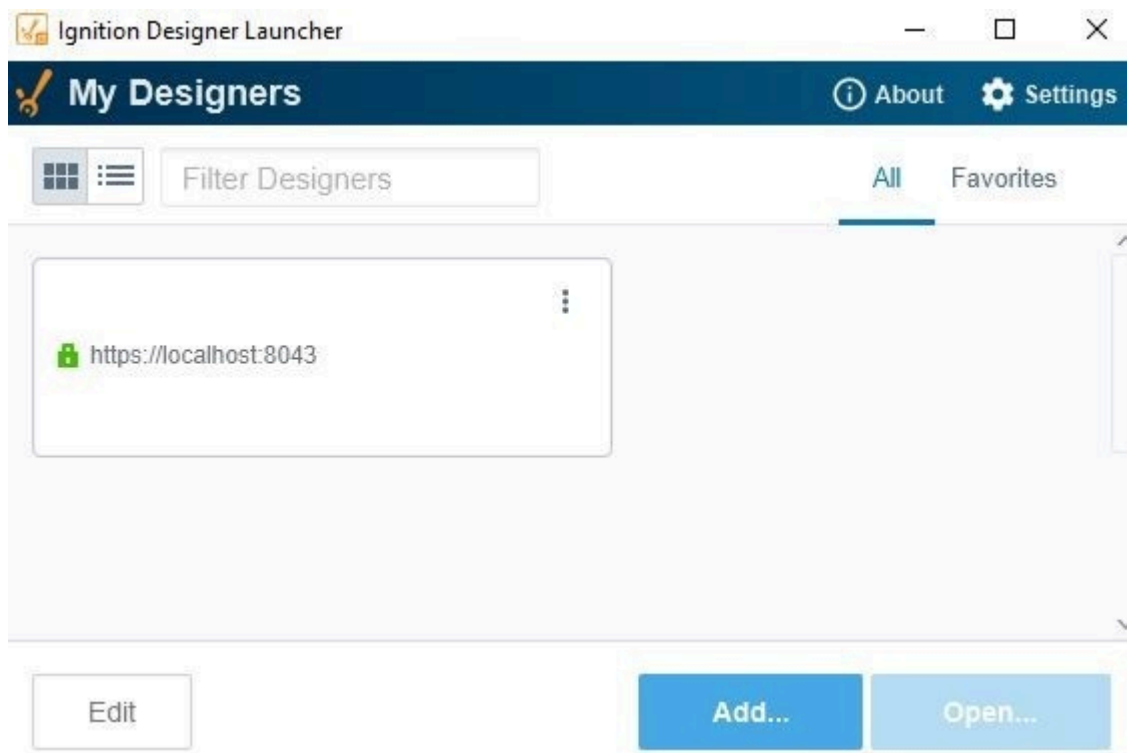


3. Once you've reviewed the certificate, select **Trust Certificate** to import the certificate.



The certificate will be imported to this directory on your client pc:  
**C:\Users{user}.ignition\clientlauncher-data\certificates.**

4. The secure designer will now be added to your Designer Launcher with a green lock icon next to the Gateway URL.



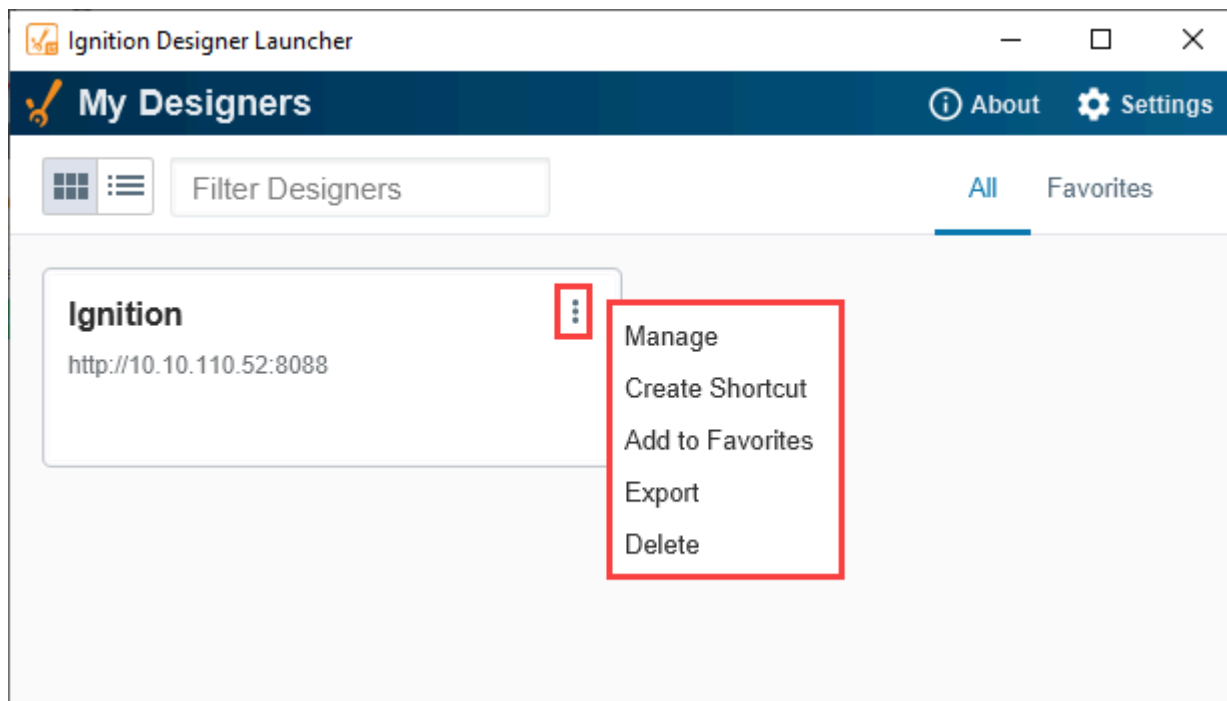
As stated above, the directory where the Trusted Certificates are now stored is under:

```
{user folder}\.ignition\clientlauncher-data\certificates
```

When the Gateway's SSL certificates are signed by a recognized Certificate Authority, no additional configuration is required on the launcher.

## Options Menu

There is a three dots menu on the applications in each of the Launchers. When you click on the three dots menu, a dropdown list appears. There are five options available.



## Launcher Options Table

| Options          | Description                                                                                                                                                                    |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Manage           | Allows you to configure/update property settings for your application. These properties are unique to each launcher application.                                               |
| Create Shortcut  | Creates a shortcut of the application and shows up as an icon on your desktop.                                                                                                 |
| Add to Favorites | Creates a Favorite in your application and puts it under the Favorites tab located in the upper right corner. Your application is marked with a star icon denoting a Favorite. |
| Export           | Exports the application launcher and configuration settings to a JSON file. It defaults to the application name and you provide the folder path.                               |
| Delete           | Deletes/removes the application name from the launcher application.                                                                                                            |

### NOTE

To view the property settings under the **Manage** option, refer to the specific launcher application: [Designer Launcher](#), [Vision Client Launcher](#) and [Perspective Workstation](#).

# Deploying Pre-Configured Launchers

In some cases, it may be desirable to deploy a pre-configured Launcher to remote clients. Doing so bypasses the installation process on the remote machine. The procedure to do so is outlined below, but in short it simply involves installing a launcher on one system, bundling the contents of the launcher into a compressed file, then moving and unzipping the file on a separate system.

The advantages of this configuration are:

1. The launcher's configuration remains the same no matter where you move the launcher to.
2. Necessary directories and launch files (including SSL certificates added to the `clientlauncher-data/certificates` directory) are copied to the local cache used when launching an Application.
3. The local cache for launching Applications remains decoupled from the launcher configuration, meaning that its footprint remains small and portable.

## NOTE

The example on this page deploys a Vision Client Launcher, but the procedure could also be used to configure and deploy Perspective Workstation and the Designer Launcher.

## Three Key Pieces to a Configured Launcher

- The launcher itself.
- The JRE for the launcher. The "jre" directory should be in the same directory as the launcher.
- The configuration JSON file. The launcher always expects this file to be located at a certain directory, otherwise the launcher will create a new, blank, file.

The steps below demonstrate how to configure a launcher, and then migrate each piece to a new file system into an appropriate location.

## Pre-Configure a Launcher

1. Install a Vision Client Launcher somewhere. Take note of the Installation directory you use, as a later step will involve finding this directory.

2. Configure each application. Be mindful of the Gateway Address setting: the deployed launcher will need to be able find the Gateway based on the address you enter.

At this point, we should have a single launcher configured with one or more applications. Next we can zip up the the launcher and its configuration files.

## Create a ZIP

In these steps, we will create a single ZIP, containing all of the required files.

1. Navigate to the Launcher's installation directory. It should look similar to the image below:

| Name                     | Date modified     | Type        | Size      |
|--------------------------|-------------------|-------------|-----------|
| jre                      | 4/26/2019 3:49 PM | File folder |           |
| clientlauncher.log       | 4/26/2019 3:49 PM | LOG File    | 1 KB      |
| unins000.dat             | 4/26/2019 3:49 PM | DAT File    | 20 KB     |
| unins000.exe             | 4/26/2019 3:48 PM | Application | 820 KB    |
| visionclientlauncher.exe | 4/22/2019 2:36 AM | Application | 21,043 KB |

2. Copy all of the files shown in Step 1, and paste them into the Client Launcher Data directory. This is the same directory that the configuration JSON file is located. The path differs by operating system, but should generally look like the following:

```
C:\Users\userName\.ignition\clientlauncher-data\
```

```
Linux

/home/user/.ignition/clientlauncher-data/
```

After pasting, the directory should look something like the following:



| Name                        | Date modified      | Type                  | Size      |
|-----------------------------|--------------------|-----------------------|-----------|
| certificates                | 3/4/2019 12:28 PM  | File folder           |           |
| jre                         | 4/26/2019 2:39 PM  | File folder           |           |
| clientlauncher.log          | 4/26/2019 3:49 PM  | LOG File              | 1 KB      |
| designer-launcher.json      | 4/26/2019 11:11 AM | JSON File             | 3 KB      |
| designerlauncher.log        | 4/26/2019 11:11 AM | LOG File              | 86 KB     |
| launchclient.jar            | 4/24/2019 10:17 AM | Executable Jar File   | 3,565 KB  |
| launchclient.jar.chk        | 4/24/2019 10:17 AM | Recovered File Fra... | 1 KB      |
| unins000.dat                | 4/26/2019 3:49 PM  | DAT File              | 20 KB     |
| unins000.exe                | 4/26/2019 3:48 PM  | Application           | 820 KB    |
| visionclientlauncher.exe    | 4/22/2019 2:36 AM  | Application           | 21,043 KB |
| vision-client-launcher.json | 4/26/2019 3:53 PM  | JSON File             | 4 KB      |
| visionclientlauncher.log    | 4/26/2019 2:30 PM  | LOG File              | 35 KB     |
| VisionIcon.ico              | 4/25/2019 2:54 PM  | Icon                  | 306 KB    |

We now have a single folder containing the launcher, a JRE, and the application configurations.

3. Navigate up a directory to the ".ignition" folder. You will see the folder we were just in: "clientlauncher-data"

| s > > .ignition     |                | Search |
|---------------------|----------------|--------|
| Name                | Date modified  |        |
| cache               | 4/23/2019 2:41 |        |
| clientlauncher-data | 4/26/2019 4:21 |        |
| .designer.prefs.bak | 4/26/2019 2:21 |        |
| clientlauncher.log  | 4/26/2019 3:30 |        |
| designer.prefs      | 4/26/2019 2:21 |        |

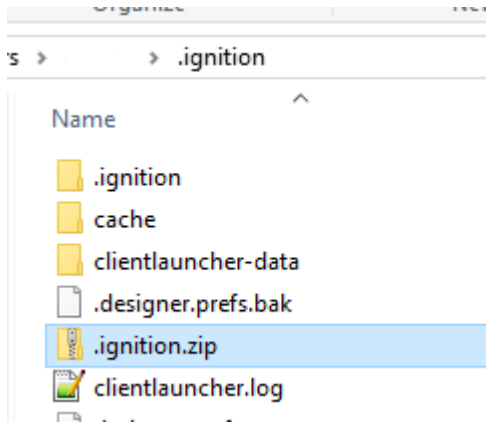
4. In this directory (the **.ignition** directory), create a new folder called **.ignition**. Note the leading period. In some operating systems you may have to attempt to rename with a trailing period as well.

```
.ignition.
```

| sers > > .ignition  |  |
|---------------------|--|
| Name                |  |
| .ignition           |  |
| cache               |  |
| clientlauncher-data |  |
| .designer.prefs.bak |  |

5. Copy the **clientlauncher-data** folder into the new **.ignition** folder. Note that you want to copy, not move. Moving would make prior application configurations on the local system unavailable.

6. Zip up the newer **.ignition** directory.



We now have a ZIP we can deploy to a new system.

## Deploying the Launcher

1. Take the ZIP, and move it to another computer.
2. Unzip the file at the user directory. The location of the directory is based on the local operating system.

Windows

C:\Users\userName

Linux

/home/user/

3. The files should be unzipped. Navigate to the launcher at:

```
{user folder}/.ignition/clientlauncher-data/visionclientlauncher
```

4. Run the Launcher. It should contain all of the configured applications.
5. At this point, consider creating a shortcut to the launcher, and placing the shortcut at a more accessible location. Alternatively, the launcher can be accessed via command line/terminal, so you could automate client launchers in a number of ways.

# Redundancy

The client launcher can take advantage of a redundant Gateway setup. Whenever a connection is established with a master Gateway, the backup Gateway IP address is automatically stored in the client launcher configuration file. If the master Gateway cannot be contacted the next time the client launcher is run, an attempt is made to contact the backup Gateway. If the backup cannot be contacted, the client launcher switches between contacting the primary Gateway and the backup Gateway until one responds or the user closes the launcher.

## Launchers and SSL

When SSL is enabled on a Gateway, the Vision Client Launcher can take advantage of the enhanced security features associated with SSL.

### Certificates Signed by a CA

When the Gateway's SSL certificates are signed by a recognized Certificate Authority, no additional configuration is required on the launcher.

### Self-Signed Certificates

When using a self-signed SSL certificate, the certificates for the Gateway must be locally accessible to the client launcher in the following directory:

```
{user folder}\.ignition\clientlauncher-data\certificates
```

When a certificate is placed in the directory above, the launcher will attempt to automatically add the certificate(s) to the local KeyStore upon application launch.

## Troubleshooting

If the Vision Client Launcher fails to launch a client for some reason, the log files can be found at:

```
{user folder}\.ignition\clientlauncher-data\
```

Each launcher has it's own log file, which are listed below:

- **Designer Launcher:** designerlauncher.log

- **Perspective Workstation:** workstation.log
- **Vision Client Launcher:** visionclientlauncher.log

## Locking the Launcher Configuration

The launcher can also be "locked", preventing users from making configuration changes to it. To learn more, see the [Launcher Settings](#) page.