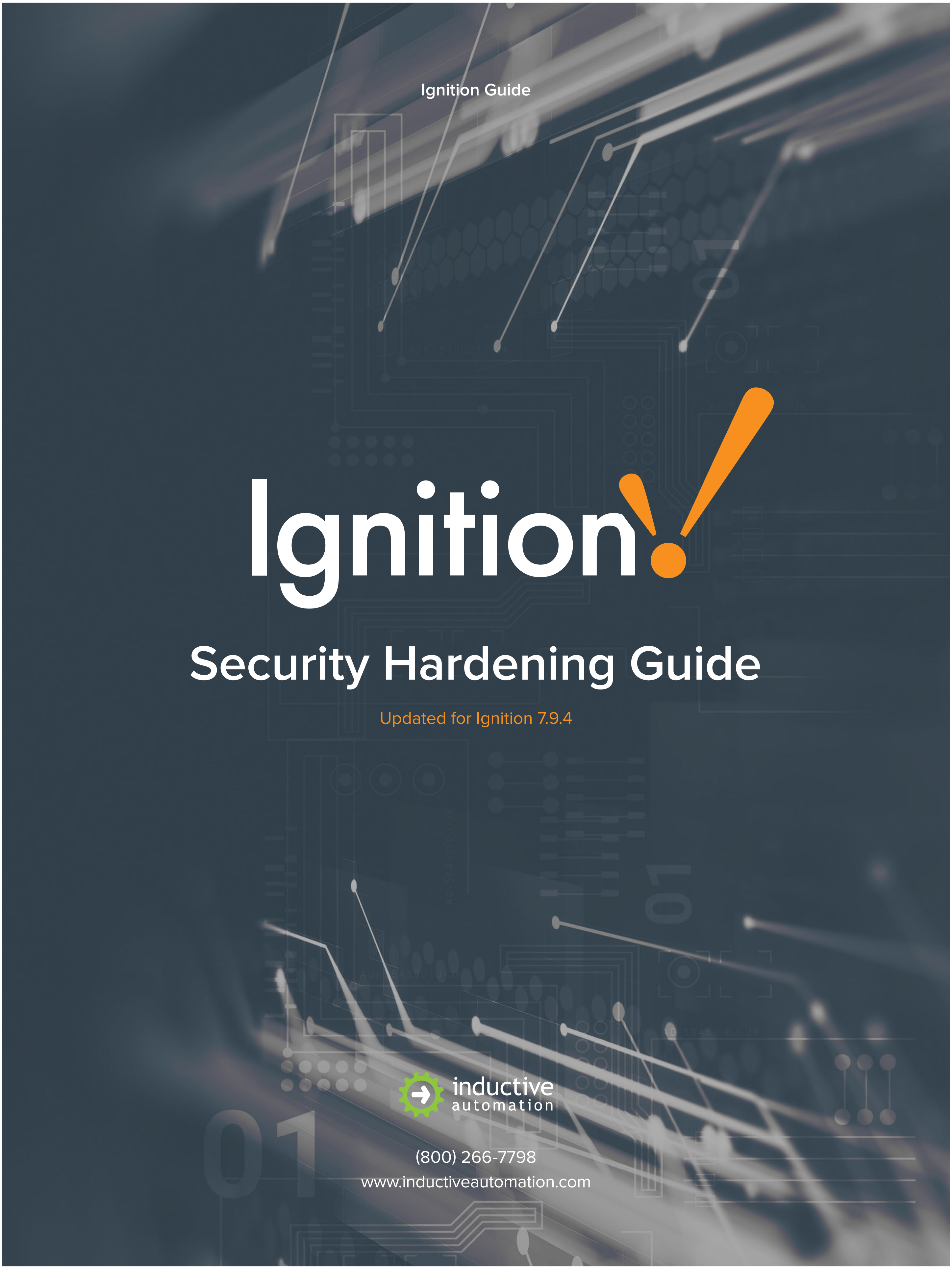


Ignition Guide

Ignition

Security Hardening Guide

Updated for Ignition 7.9.4

inductive automation

(800) 266-7798
www.inductiveautomation.com

Table of Contents

Introduction

Welcome to Inductive Automation's Ignition Security Hardening Guide. Inductive Automation is committed to security and strives to make the product as secure as possible. This document is intended to provide general guidance on how to set up and secure your Ignition installation.

Included in this document are guidelines specifically for the Ignition software, as well as general suggestions regarding the hardware and network where Ignition is installed. The steps provided are recommendations rather than requirements and should be reviewed for relevance in each implementation.

This guide is best used by reading and following the steps in their entirety. Security is a complex topic, and no guide can cover the complete tapestry of the topic, but this guide should provide good information toward protecting your Ignition installation, as well as covering the basics of securing your overall device architecture. To ensure you are fully covered from a security standpoint, please consult a security firm or security experts in the field.

Step 1: Secure the Gateway

By default, the **Configure** and **Status** sections of the Gateway are password-protected, and this cannot be removed. You can also optionally protect the **Home** section. You can also change the roles that are required to access any of these sections under **Configuration** > **Gateway Settings**.

Changing the 'admin' Password

The first step in securing your Ignition installation is to change the default username/password.

To change the 'admin' password:

1. On the Gateway webpage under the **Configure** section, go to **Security** > **Users, Roles**. The default user source contains the 'admin/password' combination to access the Configure section.
2. Click on **manage users** and you will see the admin user.
3. On the right side, click **edit** to change the password for the admin user.
4. Click the **checkbox** to change the existing password.
   Enter the new password, then re-type the new password to confirm it.

Locking the Gateway

Role-based user authentication can be used to lock down Gateway webpage sections as well as the Designer to prevent users from changing the configuration. Each of the Status, Home, and Configure pages can be restricted by roles independently.

To set up security for the Gateway:

1. Go to the **Configure** section of the Gateway.
2. Choose **Configuration** > **Gateway Settings** from the menu on the left.
   The **Gateway Settings** page is displayed.
3. Enter the roles the user must have in order to access the **Gateway Config Roles**, **Status Page Roles**, **Home Page Roles**, and **Designer Roles**.

Each option can accept any number of roles as long as they are separated by commas. Also, if the option is blank, any user with any role can log in. The **Global Resource Protection** will shelter the Global Resources from edits by users with roles other than what is stated here.

Enabling SSL

To enhance security in Ignition, you may opt to enable SSL encryption. This will affect all communication to and from the Gateway that is done over the HTTP protocol. This includes not only browsers interacting with the Gateway's web interface, but all Vision Client communication as well. Turning on SSL will encrypt all data sent over HTTP. This protects your installation from anyone "snooping" the data as it passes over the network. This may be important if data transferred between the Gateway and Clients is sensitive in nature. This also helps to thwart a security vulnerability known as "session hijacking."

To turn on SSL:

1. Go to the **Configure** section of the Gateway.
2. Choose **Configuration** > **Gateway Settings** from the menus on the left.
3. Select the check box for **Use SSL** and click on **Save Changes** at the very bottom of the page. After SSL is enabled, all Clients, Designers, and web browsers are redirected to the SSL port if they try to use the standard HTTP port. By default, the SSL port is 8043. You can change it to the standard SSL port of 443.

When Using SSL

Enable SSL communications in Ignition to set up secure communication to the Gateway webpage as well as Client/Designer communication with the Gateway. You need to acquire and install an SSL Certificate for Ignition. It is highly recommended that you purchase an SSL certificate from a certificate authority if you turn this feature on, and make sure you *install a Genuine SSL Certificate*.

Step 2: Device and OPC Security

Device connections have historically been made using native device communication protocols. Most PLC manufacturers created their own protocols for communication, and a variety are popular and in heavy use today. Recently, some devices have been released that have OPC UA embedded directly in the devices as well. Each category is secured in a different way.

Direct connections from Ignition to OPC UA devices are generally the most easily secured connections, although any connection can be secured, given the right configuration and network security.

OPC UA Communication

OPC UA provides built-in security whether at the server level or embedded on a device directly. First, all communication can be encrypted over TLS. Different devices/servers support different encryption levels, but when setting up endpoints be sure to choose the *signed and encrypted option*. This ensures all data sent over OPC UA will be encrypted.

Also, when configuring the Ignition OPC Server, on the settings page be sure to uncheck *Allow Untrusted Certificates*. This will require certificates to be added to the trusted list before they can communicate. Some third-party OPC Servers may require additional steps such as *manually adding the client certificate*.

OPC UA connections also support user authentication. We recommend using a strong password and changing it periodically as defined by IT standards.

Native Device Communication

In addition to encryption between Ignition and OPC UA devices/servers, communication between Ignition and other devices should also be protected. Since these devices often do not support encryption or certificates, a common practice is to keep them on a separate private OT network. Ignition can provide a layer of separation between the OT/private and the IT/public network to make tags available securely without exposing the devices behind the scenes. Other security options include placing Ignition and devices on a VLAN network with encryption enabled, setting up routing rules on the network or using an edge-of-network computer (such as *Ignition Edge* on an IPC) to act as a bridge between the device and the network.

We recommend consulting with a network security professional to help identify which option is best for you.

MQTT

Ignition utilizes MQTT as the IIoT protocol to bring data to the cloud and this process requires additional security considerations. Data transferred between the Publisher and Broker, as well as between the Broker and Subscriber, should be sent over TLS. In addition to this encryption, Username/Password Authentication is supported and should be utilized to protect the data. MQTT also supports Access Control Lists (ACLs) which limit user access based on topic name space. These security measures should be implemented whether the broker is local or hosted in the cloud.

Step 3: Use Security Zones

A Security Zone is a list of Gateways, Computers, or IP addresses that are defined and grouped together. This group now becomes a zone on the *Gateway Network*, which can have additional policies and restrictions placed on it. While Users and Roles restrict access to specific functions within the Gateway, like making certain controls read-only for certain users and read/write for others, Security Zones provide this functionality to the Gateway Network, limiting locations instead of people to be read-only for specific actions. This allows for greater control over the type of information that is passing over the network, improving security and helping to keep different areas of the business separate, while still allowing them to interconnect.

Using Security Zones

Sometimes, in addition to knowing who the user is, it is important to know where they are sending a command from. An operator may have permissions to turn on a machine from an HMI, but if he were to log into a project on a different Gateway in the network that had remote access to those tags, it might not be a good idea to let him write to those tags from a remote location where he can't see if the physical machine is clear to run.

This is where Security Zones come in. Security Zones themselves don't define the security, they instead define an area of the Gateway Network, breaking up Gateways and network locations into manageable zones that can then have a security policy set on them. Once there are zones defined, a security policy can be assigned to each zone, and a priority of zones can be set in the event that more than one zone applies in a given situation.

Information on how to set up *Security Zones* can be found on our website.

Step 4: Define Application Security

Ignition is a software platform for creating custom applications to suit your needs. These applications could be for HMI (Human Machine Interface), SCADA (Supervisory Control and Data Acquisition), Database Front End and more. Each of the applications require customizable security. Ignition allows for security to be defined at any level from clients and projects down to individual tags.

Client Security

In Clients, security settings can be applied to individual windows or components. Users with different roles can all view the same project from the client, but the functionality and readability can change based on the roles assigned to each user. Generally, higher-level access provides full functionality to all contents of a project, and lower level access is restricted to generalized read-only privileges. However, client security settings are flexible enough to accommodate any security requirements.

Information on how to set up *Client Security* can be found on our website.

Designer Security

When several users are all working on the same project, managing changes to the project can become cumbersome. By default, all users with Designer access can modify, delete, save, and publish all resources available in the Designer. In some situations, it is desirable to limit what each user can do in the Designer. Ignition has several built-in Designer restriction methods to help in these scenarios.

Our website contains instructions for restricting *editing*, *creation*, and *protecting individual resources*.

Tag Security

Tag security is often the best way to configure security for data access. By defining security on a tag, you affect the tag across all windows in the project, as opposed to configuring component security on each component that displays or controls that tag.

If a user opens a window that has components that are bound to a tag that the user doesn't have clearance to read or write to, the component will get a forbidden overlay.

You can add read/write security to individual tags through the Designer. Custom Access Rights must be set to use the role-based permissions.

Named Queries

One of Ignition's key features is the ability to easily log, edit, and retrieve data from a SQL database. By default, all database interaction is limited to defined queries on the Ignition Gateway, which may be called from clients based on the credentials of the user. These queries can be parameterized to allow for dynamic database interaction while ensuring only relevant data is accessible. It is recommended to only use parameters for individual variables rather than allowing longer SQL chunks to prevent SQL Injection.

This feature can be turned off to allow any SQL query to be run directly from an open client. While this can be powerful for adding flexibility to the platform, it also leaves the data potentially exposed. If client-authored queries are enabled, be sure to use SSL and not use auto-login or any shared accounts.

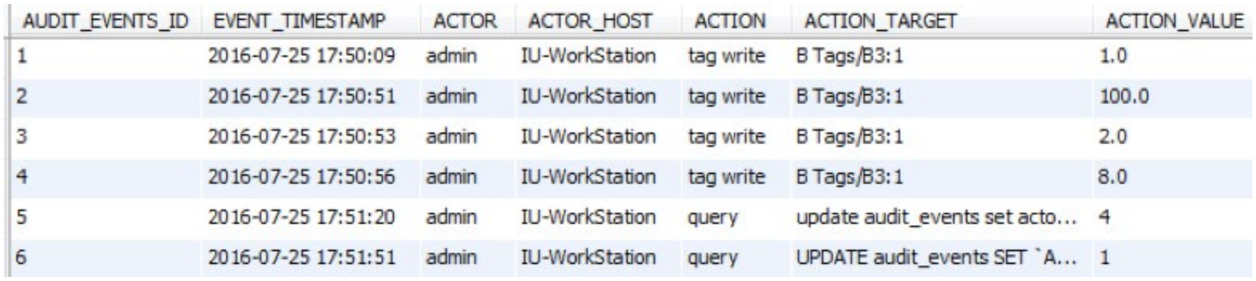
Access to these named queries can be limited using the normal Ignition permission model including roles and security zones.

If upgrading from a previous version (Ignition 7.9.3 and before), unrestricted client queries will not be disabled by default for existing projects. Secure the system by either converting existing queries to named queries or limit client queries to appropriate roles and security zones.

Step 5: Set Up Audit Logging

Audit Profiles allow Ignition to record details about specific events that occurred. Audit Profiles are simple to set-up, and immediately start to record events. By default, only tag writes, SQL UPDATE, SQL INSERT, and SQL DELETE statements are recorded. This allows you to keep track of which user wrote to which tag, or modified which table. Furthermore, a time-stamp is recorded, so you can easily track the changes and outline and order of events.

Once some changes have been made to a tag or a database table, Ignition will begin recording.



AUDIT_EVENTS_ID	EVENT_TIMESTAMP	ACTOR	ACTOR_HOST	ACTION	ACTION_TARGET	ACTION_VALUE
1	2016-07-25 17:50:09	admin	IU-WorkStation	tag write	B Tags/B3:1	1.0
2	2016-07-25 17:50:51	admin	IU-WorkStation	tag write	B Tags/B3:1	100.0
3	2016-07-25 17:50:53	admin	IU-WorkStation	tag write	B Tags/B3:1	2.0
4	2016-07-25 17:50:56	admin	IU-WorkStation	tag write	B Tags/B3:1	8.0
5	2016-07-25 17:51:20	admin	IU-WorkStation	query	update audit_events set acto...	4
6	2016-07-25 17:51:51	admin	IU-WorkStation	query	UPDATE audit_events SET `A...	1

More Information regarding *Audit Profiles* can be found on our website.

Step 6: Protect the Database

Different databases offer different authentication options. We recommend not using a database owner account such as **root** or **sa**. A separate user account with limited privileges should be created for the database connection with the Ignition Gateway.

Most modern databases also support SSL encryption of the connection between Ignition and the database. If the database is running on a different server, SSL can be enabled by following information available for your database's JDBC driver and internal security settings. Refer to the documentation for your database for more information on enabling SSL JDBC connections from Ignition.

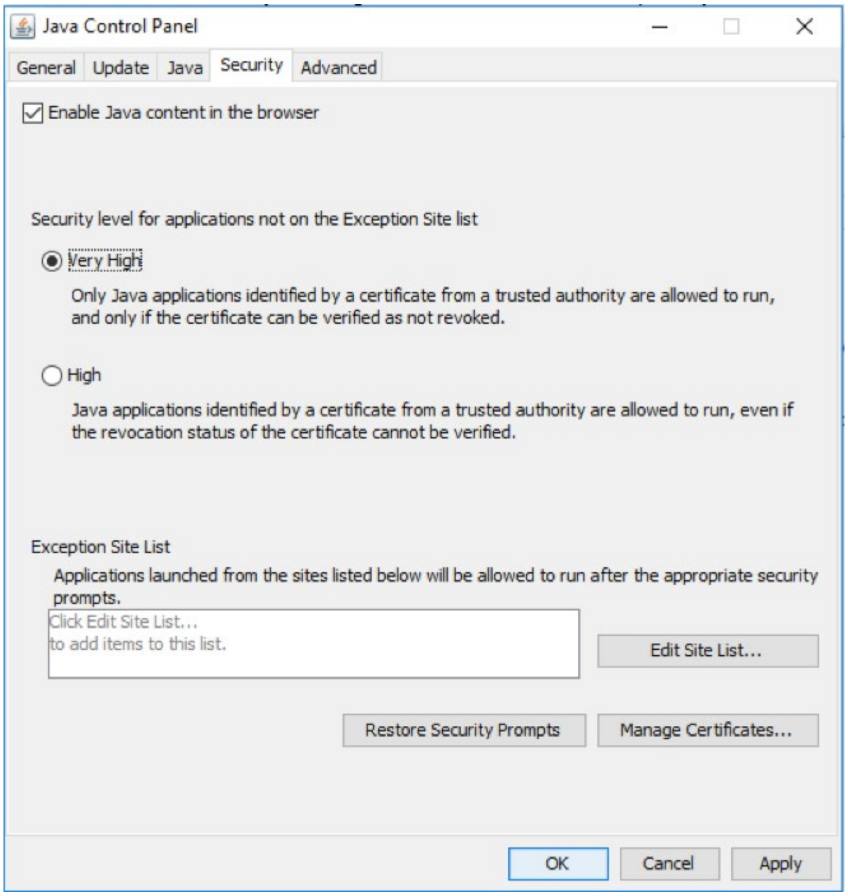
Step 7: Securing Java

Ignition runs on the Java engine, requiring Java to be installed on both the server and the client machines. Java security breaches can be avoided by securing these Java installations, especially on the client machines where users may be browsing the internet. On our website, we also have a *white paper* which goes over Java security in greater detail.

Change Java Security Settings

To prevent untrusted applications from running on your machine, change the security level to **Very High**.

Setting the Security levels through the Java Control Panel



Java Control Panel

☑ Enable Java content in the browser

Security level for applications not on the Exception Site list

● Very High

Only Java applications identified by a certificate from a trusted authority are allowed to run, and only if the certificate can be verified as not revoked.

○ High

Java applications identified by a certificate from a trusted authority are allowed to run, even if the revocation status of the certificate cannot be verified.

Exception Site List

Applications launched from the sites listed below will be allowed to run after the appropriate security prompts.

Click Edit Site List...
to add items to this list.

1. In the Java Control Panel, click on the **Security** tab.
2. Select **Very High**.
3. Click **Apply**.
4. Click **OK** to save changes made to the Java Control Panel.

Java Control Panel - Java 8u20 and later versions

Disable Java Plugin in Web Browsers

Most Java vulnerabilities to date have been through the web browser Java plugin. Since Ignition utilizes Java Web Start rather than running as an applet, this plugin is unnecessary and should be disabled to eliminate the attack vector. We recommend disabling the plugin for each browser individually rather than deselecting the "Enable Java content in the browser" setting in the Java Control Panel. By doing so you will have the convenience of opening the quick-launch JNLP files (Clients and Designers). If not, Clients and Designers will need to be opened from Ignition's *native launchers*. *Java's website* outlines how the plugin can be disabled for each browser.

Keep Java Up-to-Date

Oracle is constantly fixing bugs and any vulnerabilities that are found so we recommend installing new updates in a timely manner to protect the system.

Step 8: Locking Down the Operating System (OS)

Removing Unnecessary Programs

Each program is a potential entry point for an attacker so removing unnecessary software and having a vetted list of allowed software can limit vulnerabilities. Not all programs require administrative access and should be run using the minimum credentials required.

Patches and Service Packs

To prevent zero-day attacks and limit operating-system vulnerabilities, it is recommended to keep up-to-date on OS patches and service packs.

Remote Services

On Windows, Remote Registry and Windows Remote Management should be disabled.

On Linux and Mac OS, disable root for everything but 'physical' console.

Firewalls and Ports

Firewalls should be in place to restrict network traffic. We recommend closing all ports and then only opening those that are necessary. The following ports or the *default ports* used in Ignition. Only open the ports you are using.

Ports

PORT	OPERATION	PROTOCOL	CONFIGURABLE	DESCRIPTION
8088	Listening	tcp	Yes	Default port setting to access the Ignition Gateway
8043	Listening	tcp	Yes	Default SSL port setting to access the Ignition Gateway

PORT	OPERATION	PROTOCOL	CONFIGURABLE	DESCRIPTION
102	Listening	tcp	No	Siemens Step7
2222	Listening	tcp	No	Allen Bradley Drivers (Ethernet/IP I/O DMA)
4096	Listening	tcp	Yes	Default port for Ignition OPC UA server
4446	Listening	udp/broadcast	Yes	Default receive port for a multicast messages that makes the Gateway discoverable on a local network
5060	Listening	tcp/SIP	No	Send Voice Notification to SIP server
5500	Listening	tcp	Yes	Default port for OPC browse of external tags
6501	Listening	tcp	No	Server fallback port
8000	Listening	tcp/RTP	No	Transfer/com for SIP server
8750	Listening	tcp	No	Port used for Redundancy/Network Configuration
9600	Listening	tcp	No	Omron FINS
17342	Listening	tcp	No	Receive Port for SMS with Alarming
45900	Listening	tcp	No	Callback port for the Mobile Module
44818	Listening	tcp	No	Allen Bradley Drivers (Ethernet/IP Symbolic/General)
135	Outgoing	tcp	No	Default port for DCOM communication (old OPC DA servers)
389	Outgoing	tcp	Yes	Default port for Active directory if this is being used
465	Outgoing	tcp	No	SMTP protocol used if Alarming is configured
502	Outgoing	tcp	Yes	Default Modbus port
1433	Outgoing	tcp	Yes	Default MSSQL port used for connection
1521	Outgoing	tcp	Yes	Default Oracle port used for connection
3050	Outgoing	tcp	Yes	Default Firebirdsql port used for connection
3306	Outgoing	tcp	Yes	Default MySQL port used for connection

Redundant Servers

Firewalls must be set up on any server doing redundancy in order to protect the redundancy system from external attacks. The firewall on the main server should only accept incoming connections on port 8750 from the back-up server IP address.

Step 9: Active Directory and Authentication Sources

Ignition security is based on the roles that are assigned to specific users. These users are can be pulled from a variety of user sources. Details for *Internal Authentication*, *Database Authentication*, and *Active Directory Authentication* can be found on our website. Regardless of the source, in user authentication it is important to secure the connection as well as ensure the proper access is applied to each user.

Group Access and Disabling Auto Login

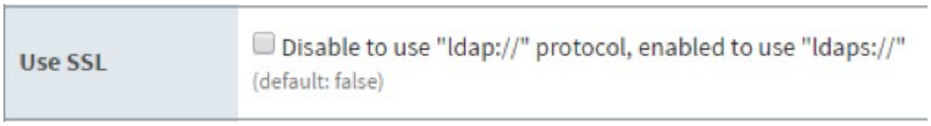
Generic logins pose a security risk in any system. If Auto Login is enabled, any user that launches a project is granted basic access. To mitigate this risk, each user should have their own unique login and Auto Login should be disabled. If a seamless experience is desired with no log-on prompt, *SSO* (Single Sign On) can be enabled in conjunction with Active Directory. This allows the windows username to be automatically used as credentials in Ignition. User groups should be given minimum access to the application and then additional roles added as needed. This prevents users from having unintended access in the application.

User Accounts

To ensure User Account integrity, a strong password policy should be defined include password length and complexity requirements. Establishing a password expiration schedule and quickly removing former user accounts is strongly recommended. Generic accounts should be avoided.

LDAP Protocol Security

The active directory User Source communicates with a Microsoft Active Directory server through the LDAP protocol. To prevent snooping on authentication, encryption should be implemented. In the advanced options for a new Active Directory User Source Ignition has a setting to force LDAPS.



Use SSL	□ Disable to use "ldap://" protocol, enabled to use "ldaps://" (default: false)

Step 10: Keep Ignition Up-to-Date

Inductive Automation recognizes that software security requires constant effort and maintenance. Security updates are released periodically to ensure continued protection and keeping up-to-date with these updates is strongly recommended.