Security Best Practices for Your Ignition System

Presenters

Don Pearson

Chief Strategy Officer

Inductive Automation

Kent Melville

Sales Engineering Manager

Inductive Automation

Guest Presenter

Joel Specht

Lead Software Engineer

Inductive Automation

Agenda

- US Govt. Cybersecurity Advisory
- Pwn2Own 2022
- Authentication Challenge
- Ignition 7.9 Support Ending
- Security Hardening Guide
- Audience Q&A

Ignition!®
by inductive automation

The Unlimited Platform for SCADA and So Much More

- **Connect, Design, Deploy Without Limits:**
  - One central hub for everything on the plant floor
  - Create any kind of industrial application
  - Web-deploy clients to desktops, industrial displays & mobile devices

- **Unlimited licensing**
- **Industrial-strength security and stability**
- **Trusted by thousands of companies worldwide**

Cybersecurity Advisory

In April, US government agencies issued a joint cybersecurity advisory about APT cyber tools targeting ICS/SCADA devices.

- The APT actors have developed custom-made tools for targeting ICS/SCADA devices that enable them to scan for, compromise, and control affected devices once they have established initial access to the OT network.
- These tools have a modular architecture and enable cyber actors to scan for targeted devices, conduct reconnaissance on device details, upload malicious configuration/code to the targeted device, back up or restore device contents, and modify device parameters.

https://www.cisa.gov/uscert/ncas/alerts/aa22-103a

CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY

Pwn2Own

- The Pwn2Own competition pits white-hat hackers against popular industrial control systems to reveal any vulnerabilities.
- Ignition was one of ten selected as targets in 2022.
- Events like Pwn2Own offer a safe way to test defenses and make improvements.
- Industrial systems are among the highest-value targets for malicious hackers, and unfortunately also among the most vulnerable.

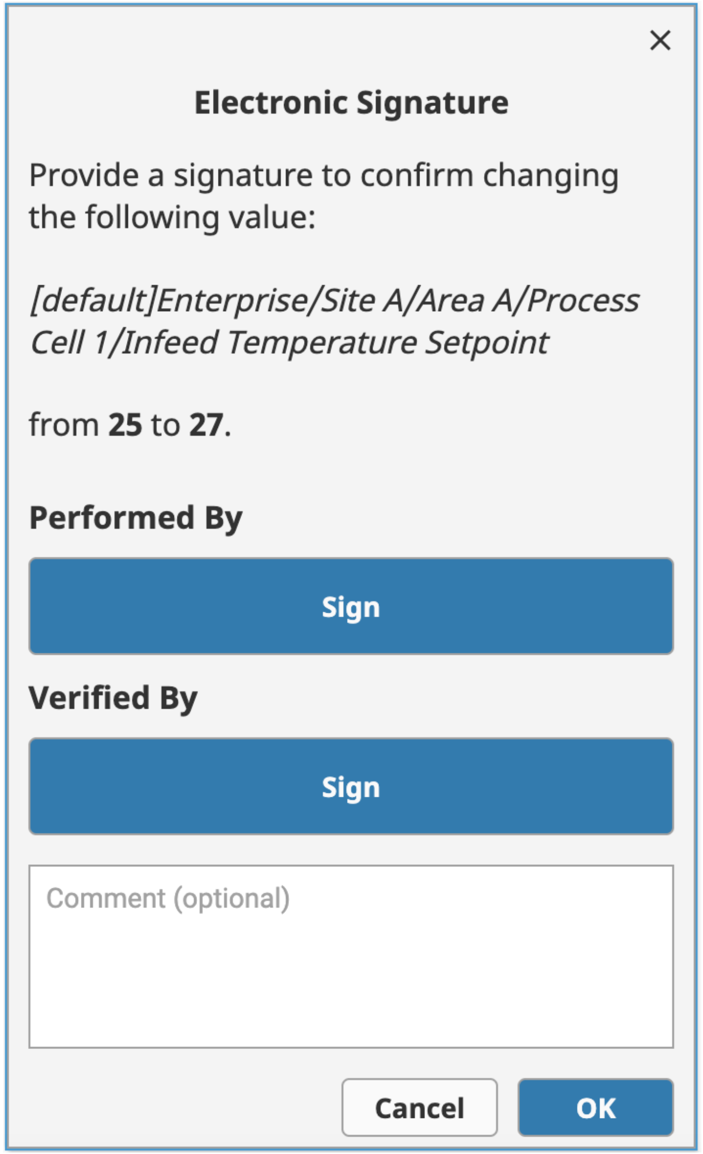
Pwn2Own

- 32 total entries from 11 total contestants
- 6 entries targeted Ignition
- 4 Ignition entries demonstrated successfully
- 1 Ignition entry was a duplicate
- 1 Ignition entry failed to be demonstrated
- All 6 entries responsibly disclosed to IA
- 1 additional report was responsibly disclosed outside of the competition by researchers who did not participate this year
- 4 critical vulnerabilities were identified by IA and fixed immediately in 8.1.17 and 7.9.20

Pwn2Own

- In response to Pwn2Own 2022, we strongly recommend all Ignition users upgrade to Ignition 8.1.17 (or 7.9.20 for 7.9 users).
- Inductive Automation has prepared a response to the Pwn2Own results and will publish a detailed report next month.
- Thank you to the ZDI and security researchers

Authentication Challenge



Electronic Signature

Provide a signature to confirm changing the following value:

[default]Enterprise/Site A/Area A/Process Cell 1/Infeed Temperature Setpoint

from **25** to **27**.

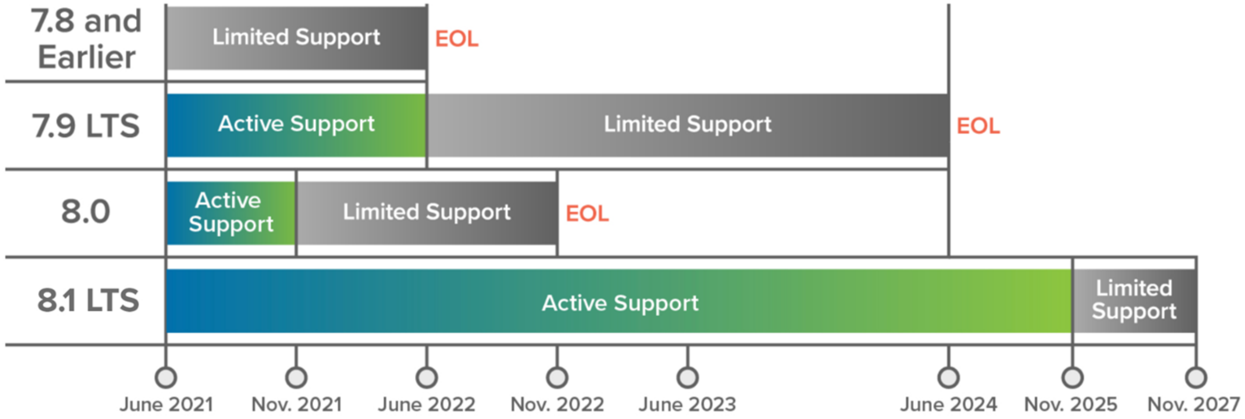
Performed By

Verified By

- The Authentication Challenge allows an operator who is currently logged into a system to document supervisor approval without logging out.
- Beneficial for both security practices and 21 CFR Part 11 regulations.
- Made up of several features:
  - Perspective redirects operator to the IdP just like any other login.
  - Supervisor provides their user credentials on the IdP’s login page.
  - The IdP validates the credentials and redirects back to the session without logging the operator out of the session or IdP.

Ignition 7.9 Support is Ending

- After June 2022, Ignition 8.0 and newer will be the only supported versions of Ignition, with 8.1 being a Long Term Support (LTS) release.
- End-of-life versions of Ignition will no longer be supported by development or support teams.
- If you're using an older limited-support version of Ignition and want to continue receiving support, you should move to a newer LTS version before June 2022.



Ignition Security Hardening Guide

A Good Foundation

Defense in Depth

- Instead of relying on single point of security, create layers of hardened security.
- Multiple layers requires a much more sophisticated hack to compromise a system.
- One Example is the Purdue Model (ANSI/ISA 95).

A Good Foundation

Cybersecurity Framework

- It is an industry best practice to adhere to a formal cybersecurity framework to align security controls with organizational objectives.
- The Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is a great resource for recommendations and additional information.

Step 1: Secure the Gateway

Step 1: Secure the Gateway

- Forcing secure communication with HTTPS using an SSL/TLS certificate is the first and most important step towards securing the Gateway.
- Secure Communication
  - SSL encrypts data sent over the HTTP protocol and Web Sockets for all traffic between the Designer, Vision Clients, and Perspective Sessions.
  - Helps to thwart security vulnerabilities known as “session hijacking” like man-in-the-middle attacks, cross-site scripting (XSS), and session sniffing.

Step 1: Secure the Gateway

- **Terminology note:** “Secure Sockets Layer,” (SSL) is the predecessor to the Transport Layer Security (TLS) protocol. SSL is deprecated as a technology. However, the term “SSL” is still widely used to refer to secure communication and “TLS.” For example, modern digital certificates supporting TLS are commonly referred to as “SSL certificates.”

Step 1: Secure the Gateway

- Enabling Secure Communication
  - You will need to obtain and install an SSL Certificate for Ignition.
  - It is highly recommended that you purchase an SSL certificate from a Certificate Authority (CA) or acquire a valid SSL certificate from your IT department if you intend to enable SSL.
- Force SSL Redirect
  - 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 443.

Step 1: Secure the Gateway

- Renewing SSL Certificates
  - Most traditional SSL certificates have a cumbersome lifecycle that needs to be renewed often.
  - SSL certificate renewal process can be simplified and automated using the ACME (Automatic Certificate Management Environment) protocol.
  - Let’s Encrypt is a “free, automated, and open certificate authority (CA)” that uses an ACME server that handles SSL certificates.
  - Any domain administrator can spin up an ACME client that points to the Let’s Encrypt ACME server to obtain or renew SSL certificates.

Step 2: Locking the Gateway

Step 2: Locking the Gateway

- The gateway web site is organized into three sections, Home, Status, and Configure. By default, the Configure and Status sections are protected by the “Authenticated/Roles/Administrator” security level. Gateway sections and Designer access can be protected with role based access control.

Step 3: Device, OPC, and MQTT Security

Step 3: Device, OPC, and MQTT Security

- Traditional PLC native device communication protocols don’t support encryption, certificates, or authentication.
- Best practice is to poll these devices from as close on the network as possible and keep them on a separate private OT network.
- When data needs to be collected across a broader network, an Edge Gateway polling locally and publishing over a more secure protocol helps bridge the gap.
- 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.

Step 3: Device, OPC UA, and MQTT Security

OPC UA Communication

- OPC UA provides built-in security at the server level or embedded directly on a device.
- Choose the SignAndEncrypt security mode to ensures all data sent over OPC UA is encrypted.
- OPC UA connections also support user authentication.
  - Use a strong password (don’t leave the default)
  - Change password periodically as defined by IT standards.

Step 3: Device, OPC UA, and MQTT Security

MQTT Communication

- Data transferred between the Publisher and Broker, as well as between the Broker and Subscriber, should be sent over TLS/SSL.
- Username/Password Authentication
- MQTT also supports Access Control Lists (ACLs) which limit user access based on topic name space.
- Security measures should be implemented whether the broker is local or hosted in the cloud.

Step 4: Identity and Access Management

Step 4: Identity and Access Management

- When securing an application you must consider both authentication and authorization.
- **Authentication** determines who is logging in
- **Authorization** determines their privileges.

Step 4: Identity and Access Management

Authentication

- User Identification and Authentication
  - Ignition manages users through built-in IdPs but can also connect to third-party IdPs such as Okta and Duo via SAML or OpenID Connect.
- Ignition Identity Provider
  - Ignition IdP supports three main user sources:
    - Internal Authentication
    - Database Authentication
    - Active Directory Authentication
- Internal Authentication through Ignition Gateway
- Database Authentication uses external database to store data
  - Managing users is done via direct interaction with the database.

Step 4: Identity and Access Management

- Active Directory Authentication
  - Active Directory Authentication profile uses Microsoft's Active Directory over LDAP (Lightweight Directory Access Protocol) to store all the users, roles, and more that make up an Authentication profile.
  - Active Directory Groups are used for Ignition's roles and user-role mappings.
  - While using an Active Directory User Source, administration of users and roles is through Active Directory itself, and not manageable within Ignition and requires modifications be made from Active Directory.
- LDAP Protocol Security
  - To prevent snooping on authentication, encryption should be implemented.

Step 4: Identity and Access Management

- Badge Authentication
  - RFID authentication support for Ignition IdP allows you to associate badges with users.
  - With RFID enabled, users do not have to enter their username and password, and instead must have a physical badge in order to log in to the Session.
  - It is recommended that Badge Authentication Method is enabled and set to default and Badge Secret is also enabled, which will require the user to type in their password after scanning their badge.

Step 4: Identity and Access Management

- Third-Party Identity Provider
  - If your organization already has as IdP like OKTA or DUO then Ignition can also leverage those for Authentication.
  - Utilizing an external service allows you to utilize features that Ignition doesn’t support natively such as multi-factor options like push notifications or biometrics.

Step 4: Identity and Access Management

General Authentication Suggestions

- User Accounts
  - A strong password policy should be defined including password length and complexity requirements.
  - Establish a password expiration schedule and quickly removing former user accounts.
  - Generic accounts should be avoided.
- Group Access and Disabling Auto-Login
  - Generic logins pose a security risk if Auto Login is enabled because any user that launches a project is granted basic access.
  - Auto Login should be disabled and each user should have their own unique credentials.

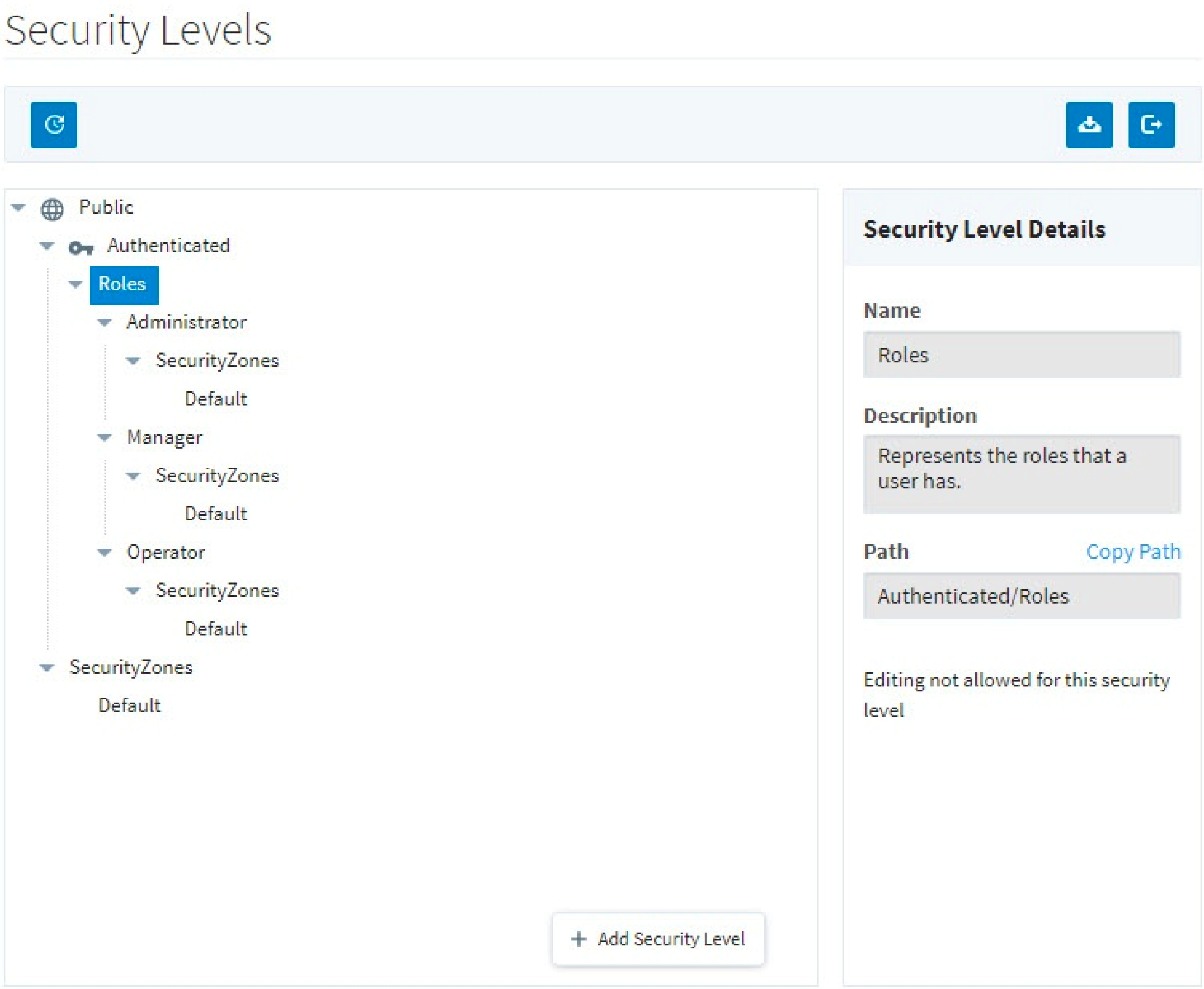
Step 4: Identity and Access Management

Authorization

- Role-Based Security
  - Each user is granted privileges by assigning one or many roles.
  - Roles are customized during development and can be defined inside Ignition or mapped to Active Directory groups or an IdP’s attributes.
- Security Zones
  - Sometimes, in addition to knowing who the user is, it is important to know where they are sending a command from.
  - Security Zones define an area of the Gateway Network into manageable zones that can then have a security policy set on them.

Step 4: Identity and Access Management

- Security Levels
  - A user-set hierarchy that defines access permissions, or roles, inside a Perspective Session.
  - Provides a way to map user roles defined from an Identity Provider (IdP) to Ignition roles.
  - With security levels, roles can be defined in order to allow certain users more or less control of the Gateway.



Security Levels

- Public
  - Authenticated
    - Roles
      - Administrator
        - SecurityZones
          - Default
      - Manager
        - SecurityZones
          - Default
      - Operator
        - SecurityZones
          - Default
  - SecurityZones
    - Default

Security Level Details

Name

Roles

Description

Represents the roles that a user has.

Path

Authenticated/Roles

Editing not allowed for this security level

Q&A

Step 5: Define Application Security

Step 5: Define Application Security

- Ignition allows for security to be defined at any level from clients and projects down to individual tags.
- Vision Client Security
  - Security settings can be applied to individual windows or components.
  - Functionality and accessibility of the same project can change based on user assigned roles.
- Perspective Views Security
  - Allows more granularity of the security in a Perspective Session.
  - Operators can be granted access to the Session, but the user management View can be restricted to a higher level role.
- Component Scripting Security
  - Both Vision and Perspective contain role-based component scripting security.
  - Ensures that non-privileged users are not allowed to run potentially harmful scripts.

Step 5: Define Application Security

- Designer Security
  - Granting someone access to the designer is giving them access to a full development IDE with the ability to execute scripts at the permission level of the user running the Ignition Service.
  - By default, all users with Designer access can modify, delete, save, and publish all resources. Ignition has several built-in Designer restriction methods to limit what each user can do in the Designer.

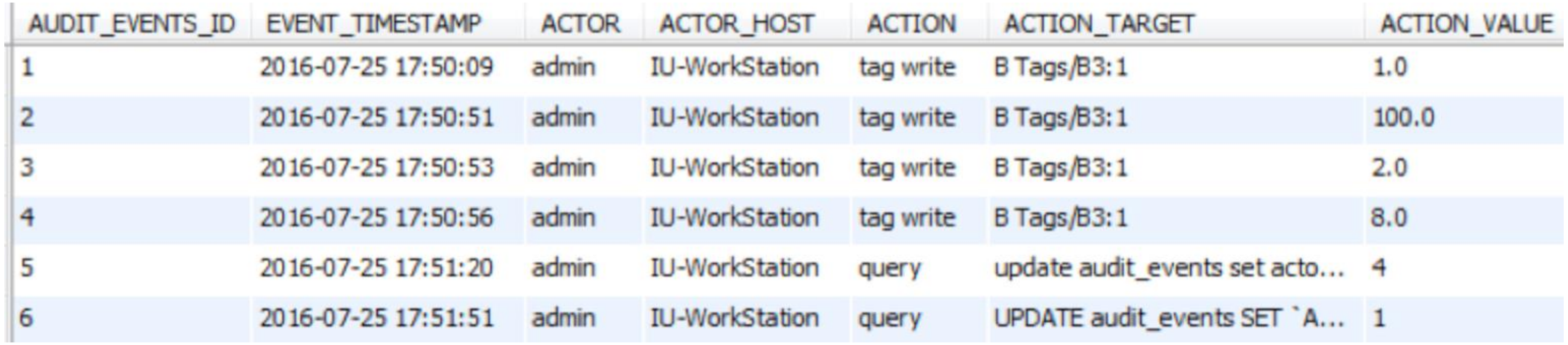
Step 5: Define Application Security

- Tag Security
    - The best way to configure security for data access.
    - Tag security definitions apply for that tag across all windows and components that use the specified tag in the project.
    - You can add read/write security to individual tags through the Designer.
- Named Queries
    - All database interaction can be limited to defined queries on the Ignition Gateway, which may be called from clients based on the credentials of the user.
    - It is recommended to only use parameters to allow for dynamic database interaction while ensuring only relevant data is accessible.
    - 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.

Step 6: Set Up Audit Logging

Step 6: Set Up Audit Logging

- Audit Profiles allow Ignition to record details about specific events that occurred.
  - By default, only tag writes, SQL UPDATE, SQL INSERT, and SQL DELETE statements are recorded, allowing you to keep track of which user wrote to which tag, or modified which table.
  - The time-stamp is also recorded, so you can easily track the changes, outline, and order of events.
- Once 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

Step 7: Protect the Database

Step 7: Protect the Database

- It is not recommend to use 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 support SSL encryption of the connection between Ignition and the database.
- SSL can be enabled on a different server by following information available for your database’s JDBC driver and internal security settings.

Step 8: Locking Down the Operating System (OS)

Step 8: Locking Down the Operating System (OS)

- It is important to understand how Ignition fits within the operating environment.
- Ignition Privileged Users
  - Users who can modify projects in the Designer and in the Gateway, are able to write Python applications with all privileges granted to the Ignition process

Step 8: Locking Down the Operating System (OS)

- Ignition Process
    - Ignition is designed to run 24/7 with a persistent OS, trusted communication protocols, plus access to devices and databases.
    - The Ignition Process is executed by a user-specified service account on the gateway and is theoretically capable of all privileged OS actions and is implicitly trusted.
- Apply the *Principle of Least Privilege*
    - Do not user “root” or “domain admin” account as Ignition service account.
    - Minimize privileges of Ignition computer and service account on larger network.
    - Minimize Ignition permissions on external databases and systems.
        - API access is often safer than direct access.
    - Segment network with zones and accreditation boundaries.

Step 8: Locking Down the Operating System (OS)

- Removing Unnecessary Programs
  - Each program is a potential entry point for an attacker.
  - 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 limit operating system vulnerabilities, 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.

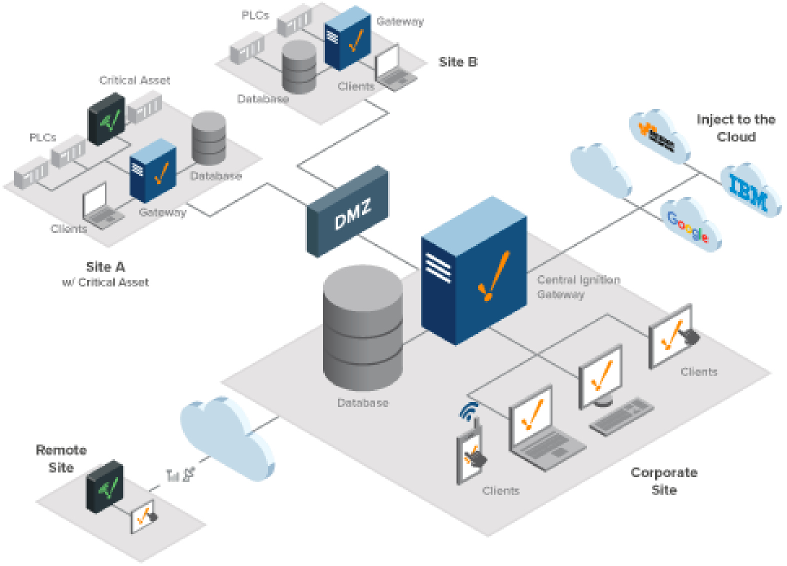
Step 9: Hardening the Environment

Step 9: Hardening the Environment

- Firewalls and Ports
    - Firewalls should be in place to restrict network traffic.
    - When starting a new Ignition project, close all ports and then only open those that are necessary and in use.
- As your architectures get more complex, it is also important to pay attention to which ports need to be open in which directions. you may also be able to restrict traffic through the firewall to specific servers.

Step 9: Hardening the Environment

- Redundant Servers
  - Firewalls must be set up on any redundant server to protect the redundancy system from external attacks.
  - The firewall on the main server should only accept incoming connections from the backup server IP address on the Gateway Network port (8060).
- DMZ Architecture
  - A “demilitarized zone” contains a subnetwork to accommodate exposed, outward connecting services.
  - Acts as a point of contact between the organization’s internal network and untrusted networks, such as the internet.
  - Extra layer of security to the local network.



Step 10: Keep Ignition Up-to-Date

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.

Ignition Security Hardening Guide

https://inductiveautomation.com/resources/article/ignition-security-hardening-guide

Ignition®
by inductive automation

Ready to Try Ignition for Yourself?

Download the full version for free at:
inductiveautomation.com

inductiveuniversity.com

Ignition User Manual also available at:
docs.inductiveautomation.com

The 10th Annual Ignition Community Conference

ICCX

XPERIENCE & XPLORE

In-Person: Sept. 20-21 | Virtual: Oct. 3-5

International Distributors

Australia	iControls Pty Ltd.	www.icontrols.com.au
Brazil	FG Automação Industrial	www.fgltda.com.br
Central America	NV Tecnologías S.A.	www.nvtecnologias.com
France	AXONE-iO	www.axone-io.com
Italy	EFA Automazione S.p.A	www.efa.it
Norway	Autic System AS	www.autic.no
South Africa	Element8	https://element8.co.za
Switzerland	MPI Technologies	https://mpi.ch

Contact International Distribution Manager Annie Wise at: awise@inductiveautomation.com

Questions & Comments

Ignition by inductive automation

Call us at: **800-266-7798**

Melanie Hottman
Director of Sales
x247

Jim Meisler
x227

Ramin Rofagha
x251

Lester Ares
x214

Vannessa Garcia
x231

Shane Miller
x218

Maria Chinappi
x264

Myron Hoertling
x224

Robert Graves
x142

DJ Parsons
x150

Roman Couvrette
x163

Abran Mathews
x151

Justin Reis
x186

Thank You

Stay connected to us on social media
& subscribe to news feeds: