

An abstract graphic consisting of several concentric circles and arcs. Some segments of these circles are highlighted in a vibrant blue color, while the rest are thin white lines. Small white dots are scattered along the arcs, giving it a technical or digital feel.

Whitepaper

21 CFR Part 11 Compliance
with Inductive Automation's
Ignition Platform

Ignition!

Introduction

Ignition by Inductive Automation is a powerful, flexible industrial platform that supports SCADA, IIoT, MES, HMI, alarming, reporting, and more. Its unlimited licensing model and open architecture make it a top choice for manufacturers seeking scalable and adaptable solutions.

In highly regulated industries such as pharmaceuticals and biotechnology, selecting an automation platform also requires meeting strict compliance standards like 21 CFR Part 11 and data integrity requirements.

This is where Catalyx plays a key role. As an experienced automation and integration partner, Catalyx helps manufacturers implement and configure Ignition to meet both operational and regulatory needs. Catalyx's expertise ensures that each deployment aligns with FDA expectations for electronic records, electronic signatures, and data integrity.

21 CFR Part 11 defines how electronic records and signatures must be handled to ensure they are as reliable as paper-based systems. Compliance depends on secure audit trails, user access controls, and digital signatures. In parallel, maintaining data integrity is guided by ALCOA+ principles—data must be Attributable, Legible, Contemporaneous, Original, Accurate, Available, Enduring, Consistent, and Complete.

Together, Ignition and Catalyx deliver a solution that meets these requirements through built-in functionality and proven implementation strategies.

This white paper outlines how the partnership between Ignition and Catalyx supports:

- Secure user access and account management
- End-to-end data integrity
- Full 21 CFR Part 11 compliance

With Catalyx's integration expertise and Ignition's robust capabilities, pharmaceutical and biotechnology organizations can confidently achieve compliance while advancing their digital transformation.

User Account Management

Unique user accounts and credentials are a key component for compliance with Part 11 requirements. Ignition features several options for managing users and roles, allowing it to adapt to various use cases and IT environments. These options include internal (contained -within Ignition), external (managed by external database or enterprise identity provider), and Active Directory (enterprise-managed). When considering Part 11 compliance, authenticating users through Active Directory or an identity provider is considered a best practice.

Using Active Directory as an Ignition user source, access to Ignition tools and projects is granted to users with their existing username and password from the enterprise Active Directory. This ensures that all users are uniquely identified when accessing Ignition. This also ensures that the credentials of each user are held to the company policies and requirements for complexity, lockout, and forced expiration. When a user is disabled or removed from Active Directory, they will automatically be prevented from accessing Ignition without any additional administrative action.

For more complex IT environments, hybrid user sources in Ignition allow user and role authentication to be split between two types of sources. With Ignition Perspective, identity providers offer an additional option for user authentication. This method offloads the handling of user authentication from Ignition to federated login providers. This has the benefit of allowing Ignition to inherit advanced authentication features provided by the identity provider, such as two-factor or multi-factor authentication.

User Access Control

Roles should be configured to ensure users can only access the parts of Ignition for which they are authorized. When configuring a project in Ignition, these roles are referenced by configuring security properties or scripting to enable or disable specific features. Such security can be applied to tags, user interface components, projects, and the Ignition Gateway. These security settings ensure that only authorized users can read or write to tags, interact with user interface components like buttons and text boxes, or modify validated configurations. For example, the ability to acknowledge alarms could be restricted to users with a “Supervisor” role.

Roles can also be stacked together such that an action requires multiple roles. Roles should be assigned with the idea of “least permissions,” where a user has the minimum privileges and access necessary to perform their job, and nothing more. This ensures permission do not “leak” and allow a user to perform actions they are not trained or authorized for.

Additional features are available within Ignition to enhance security beyond basic login and role enforcement. Security permissions can be applied based on locations to require a specific user level and specific operator terminal to be granted access to the system. As an example, this can allow write access to the system only when a user is located locally to a piece of equipment – which is important when considering ALCOA+ principles. To further ensure account access remains unique, Ignition can be configured to automatically logout users after a period of inactivity. This helps ensure that no user intentionally or inadvertently generates records such as audit trail actions under a user account that is not their own.

E-Signatures can be added to Ignition projects that require extra confirmation of user permissions. Utilizing the `system.security.validateUser()` or `system.perspective.authenticationChallenge()` functions, users can be forced to provide their credentials before critical actions are performed. Multiple signatures can be required per action without logging off the current user, allowing a supervisor to E-Sign to confirm an operator action. Combining these credential validation methods with Ignition's audit trail feature ensure that user interactions with Ignition projects are thoroughly controlled, attributable, and accurate. Roles can be utilized to ensure a hierarchical security structure, ensuring that critical audit and data integrity features cannot be altered.

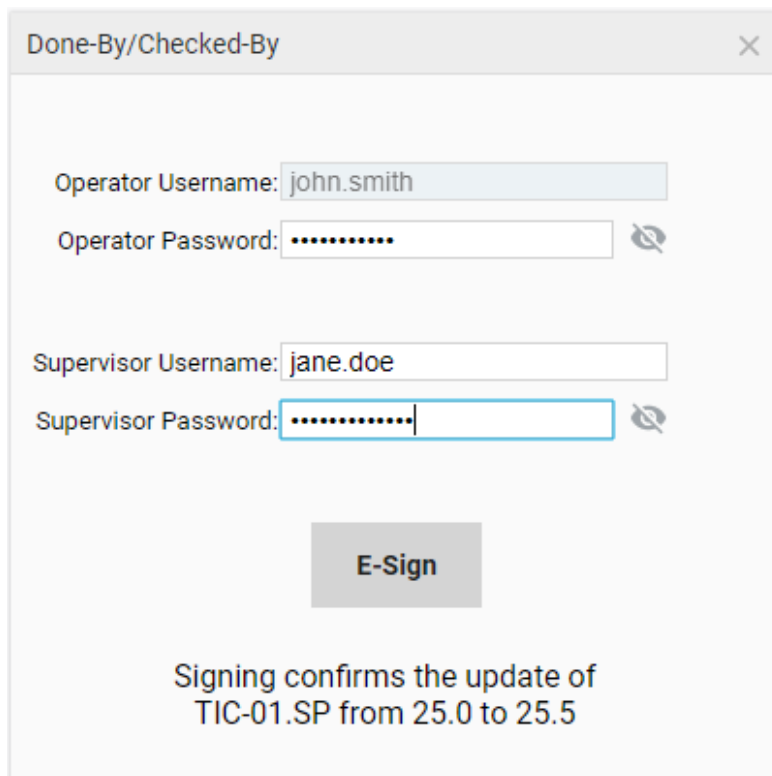


Figure 1: Example of Done-By Checked-By Capability

Data Integrity

Ignition uses databases for the Tag Historian Module, alarm journal, and audit trail, as well as when utilizing expanded functionality for project-specific purposes. Although Ignition supports connections to multiple database types, the following security considerations generally refer to Microsoft SQL Server. For security-conscious configuration details of other database types, consult with your database administrator (DBA).

To ensure data integrity of SQL databases, logins and permissions must be strictly configured for each database. An exclusive account should be configured for Ignition to connect to SQL with “read/write” access. No other users should have “write” access, as this would allow tampering with historical and audit trail data. This account should be an Active Directory managed account where possible, and the account username and password information should be shared sparingly to avoid non-Ignition use of the account. The account should only be used for this single purpose so that the password can be reset if needed without disrupting other applications or services. The built-in “sa” account should never be used for the database connection.

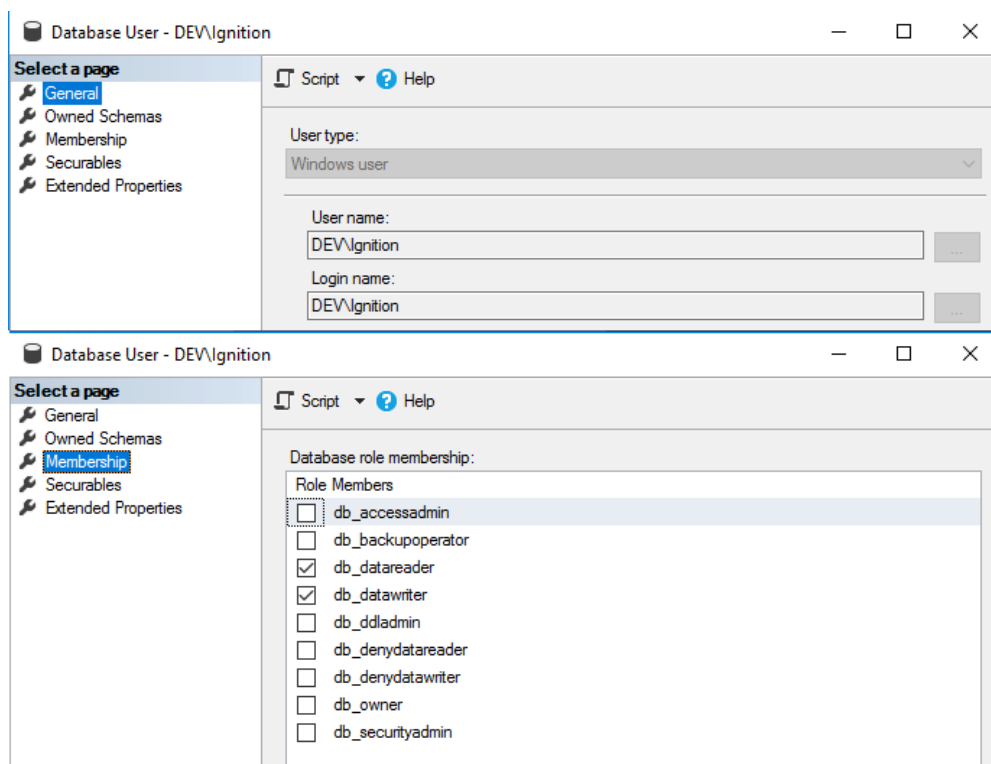


Figure 2: Configuration of Active Directory account with read/write database permissions.
(Alternatively, the user can be set as db_owner.)

Other users can be configured with read-only access to databases for querying data; however, any validated data provided by the system should be presented as read-only reports. Tools and controls are available within Ignition for creating displays to review data, such as trend charts and customizable tables. Tools are also available to generate reports to be printed or exported in read-only formats like PDFs. This allows standard validated report templates to be reused with minimal testing required. Since the report data is read-only from the data source and read-only in file type (pdf), data cannot be tampered with, contrary to processes that utilize spreadsheet-based data exports that do allow potential data tampering.

Regular scheduled full and incremental backups should be configured for long-term storage of data. The backups should be kept on a separate disk or offline media. The backups should be tested annually for corruption and restorability. Ignition provides features to schedule automatic gateway backups. Database backups can also be automated with scheduled tasks or advanced methods such as server clustering.

To further enhance data integrity within Ignition, the design of the network and related components should be considered. In an ideal setup, process equipment should be located on a network that is separate from office systems such as end-user computers. This segregation ensures that validated systems and their data cannot be tampered with intentionally or inadvertently by users who should not have access to them. In such a setup, firewall rules can be applied to allow only specific required access to Ignition between the two networks. For example, specific network ports can be opened so that users on the office network can access an Ignition client to view report data, but not access the equipment the data originated from.

When configuring connections to data sources in Ignition, unique non-expiring system accounts and passwords should be used where possible; use of anonymous connections should be avoided to ensure traceability of audit trail and log information. Secure encrypted protocols such as OPC UA are preferred to ensure data integrity across the network. Direct connections are preferable to indirect connections (such as passing data across multiple OPC servers). By keeping architectures simple, configuration and communication issues can be avoided that could otherwise impact the integrity of end data.

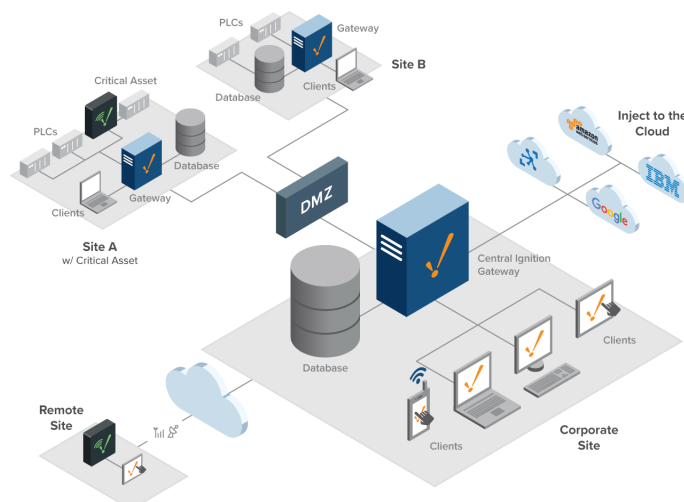


Figure 3: Example Network Diagram

Audit Trail

Ignition provides an audit trail to record contemporaneous logs of user actions within the system. Multiple audit profiles can be created and applied to projects based on specific user requirements and retention periods. By default, Ignition will record a timestamp, username, computer name, and details about each audited action. Default audited actions include tag writes, SQL commands (UPDATE, INSERT, DELETE), project changes from the Ignition Designer, and user login/logout events.

Using the `system.util.audit()` function, the the default audited actions can be extended. During any scriptable event or binding (for example, clicking a button to switch a system from Auto to Manual mode), this function can be used to add an event to the audit trail. Security challenges or E-signature events such as “Done By” and “Checked By” information can be added to every scriptable event within the audit trail. By configuring these actions in a template or dedicated Perspective view, audited actions can be simply applied throughout the project without redundant configuration or validation testing. Audit trail data can be reviewed from the Ignition Gateway or queried and presented in tables or reports.

A common example of extending the Ignition audit trail is recording when a user has changed the value of a setpoint from an HMI. For this action, an input component would be configured within a template. Using event handlers on this component, a script is utilized to detect when the value of the input is changed. When the value is changed, the `system.util.audit()` function is executed to insert an entry into the audit database table. All fields can be filled in to match builtin audit events, including the current user, current host name, and timestamp. In this example, the “action” field can be populated as “setpoint change”, and the “value” field can be populated with the old and new values for the setpoint. With this configuration completed inside a template or dedicated Perspective view, it can be reused throughout the project without extra configuration or testing.

Audit Log Viewer

Actor

Start Date

6/1/19



3

:

43

AM

▼

Action

End Date

6/6/19



11

:

59

PM

▼

Target

Search

Timestamp	Actor	Host	Action	Target	Value	Result	System	Context
6/4/19 3:42 PM	admin	Ignition	setpoint change	[PCS]PCS PLC/LIC_001/HHPv	old=93.0; new=94.0	AuditStatus[0x00000000, Severity=Good, Subcode=NotSpecified]	project=HMI	Designer
6/4/19 3:42 PM	admin	Ignition	tag write	[PCS]PCS PLC/LIC_001/HHPv	94.0	AuditStatus[0x80000000, Severity=Bad, Subcode=NotSpecified]	project=HMI	Designer
6/4/19 4:19 PM	admin	Ignition	logout			AuditStatus[0x00000000, Severity=Good, Subcode=NotSpecified]	project=HMI	Designer

Figure 4: An example audit trail log with an expanded “setpoint change” action.

Summary

Data integrity principles and Part 11 compliance are part of the framework that ensures humans receive quality medicines and treatments free of potentially harmful defects. Compliance helps provide a means to collect critical data that can be displayed without alteration as well as a system to track operator actions and events. The Ignition platform complies with Part 11 and adheres to data integrity principles.

Ignition includes a comprehensive set of user access controls and a robust audit trail. These features are designed to offer powerful default functionality while also providing users the ability to expand the default functionality. This allows the audit trail to capture any information deemed critical by an organization or individual quality group without compromising on data security and integrity.

For more information, please contact Catalyx at info@catalyx.ai.

About Catalyx

Catalyx is a global machine vision and automation company that integrates technology and people to help manufacturers and logistics providers achieve next-generation levels of quality and throughput. For over thirty years, the minds behind Catalyx have been at work maximizing operational processes across highly regulated industries by inventing new technology applications and supporting companies with deep technical expertise. With nine global offices, more than 550 team members, and over 3,000 successful projects, Catalyx has the scale, skillset, and reach to solve unique process problems at enterprise scale — and the vision to keep doing what’s never been done before. To learn more or speak with our team about 21 CFR Part 11 readiness, historian deployment, or broader automation strategy, get in touch.



info@catalyx.ai

www.catalyx.ai

USA | IRELAND | UK | CONTINENTAL EUROPE