Guidelines for applying FactoryTalk® AssetCentre in a 21 CFR Part 11 environment: Version 11.0 and later

Versions 11.00 through 16.00

Complying with 21 CFR Part 11: Electronic Records & Signatures

Contents

Introduction **4**
Defining Key Terms **5**
FactoryTalk® AssetCentre in a Rockwell Automation software system **6**
FactoryTalk® AssetCentre and FactoryTalk® Services Platform 6
How Studio 5000 Logix Designer fits in 8
How FactoryTalk® View Site Edition fits in 8
How PanelView Plus 6/7 and FactoryTalk® View Machine Edition fit in 9
How this compares with FactoryTalk® Optix 9
Complying with the Part 11 Regulation **10**
Table 1: Subpart B – Electronic Records 10
Table 2: Subpart C – electronic signatures 19
Guidance for Applying FactoryTalk® AssetCentre in a 21 CFR Part 11 environment **24**
Secure physical and logical access to computer hardware 25
Logically restrict access for removable storage 25
Logically manage access for mass storage devices 25
Take advantage of operating system security and domains 26
Enterprise Identity Management 26
Multi-Directory Environments 27
Leverage AssetCentre system architecture 27
SQL Server Architecture 28
Multi-Directory Architectures 28
Configure FactoryTalk® Security using Windows security and more 29
User Group and User Management 30
Secure FactoryTalk® AssetCentre 31
Configure and Secure AssetCentre Asset Tree 31
Log all FactoryTalk®-Enabled application activity to the AssetCentre database 32
Configure FactoryTalk® AssetCentre computers to automatically lock after a period of inactivity 33
Use a password-protected screen saver 34
Windows Automatic Restart Sign-On 34
Use Windows account password aging and management 34
Use AssetCentre Archive for version control 35
Use AssetCentre Archive Management of Change electronic workflow 36
Configure the system to use Archive Management of Change 36
Add users to Archive Management of Change 37
Create approval workflows 39
Accessing audit information from Archive Management of Change administration 40
Configure signing during non-continuous sessions 41
Configure automatic backup and compare of devices 42
Considerations around use of the Custom Device Asset 44
Running AssetCentre® Agent as an Application 45
Leverage AssetCentre for asset monitoring and lifecycle management 45
Setup AssetCentre Asset Lifecycle monitoring 45
Monitor security-related configurations 46
Configure Time Synchronization in a FactoryTalk® environment 50
Setup FactoryTalk® Database Management 50
Notification for database limitations 50
Automated schedules for log clean up via web client 51
Automated schedules for archive clean up via web client 51
Highlights in Version History **53**
About Rockwell Automation **54**
Ongoing 21 CFR Part 11 Product Review **54**

Publishing application notes **54**

Introduction

In 1997 the Food and Drug Administration (FDA) issued the final rule on the criteria under which the Agency will accept electronic signatures and records in lieu of handwritten signatures and records executed on paper. The scope of this regulation, US FDA 21 CFR Part 11, is significant and impacts all computer systems related to the manufacturing of a life science product (for example, oral solid dosage, biologic, or medical device). According to the rule, "This Part (21 CFR Part 11) applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted". Legacy systems, including Microsoft® Access database software and Microsoft Excel spreadsheet software, are not protected by a legacy system clause. The dollar cost of remediating these systems is calculated in the millions. However, the cost of not taking advantage of electronic records and signatures can be detrimental to the competitiveness of a company's position in its marketplace.

The purpose of this document is to provide life science manufacturers with a description of how a FactoryTalk® AssetCentre can address the technical requirements of Part 11. Each manufacturer has a set of unique needs and interpretation of Part 11; Rockwell Automation recognizes the demands of life sciences manufacturers and has created a solution that is flexible enough to address these differences. The objective is to help life sciences manufacturers quickly and cost-effectively comply with 21 CFR Part 11. This document describes how to use FactoryTalk® AssetCentre with other FactoryTalk®-enabled products to secure and log operator actions, track alarms, and log other operational data. These other FactoryTalk®-enabled products are not discussed in detail but are referenced where necessary.

Defining Key Terms

Within the regulation are seven key terms that the FDA has defined:

Closed System – An environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system. This document assumes that a closed system is used.

Open System – An environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

Electronic Record – Any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

Biometrics – A method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

Electronic Signature – A computer data compilation of any symbol or series of symbols, executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

Digital Signature – An electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

Handwritten Signature – The scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

FactoryTalk® AssetCentre in a Rockwell Automation software system

FactoryTalk® AssetCentre and FactoryTalk® Services Platform

FactoryTalk® AssetCentre provides a set of tools designed to securely and centrally manage automation production environments by securing access to the control system, tracking users' actions, managing asset configuration files, and providing backup of operating asset configurations. This includes the Archive Management of Change (MoC) which provides an electronic workflow for archive check-in and check-out with single or multiple approvals. The combination of this functionality allows for records of alterations to electronic files and the control and recording of user actions, as required by regulations such as 21 CFR Part 11.

FactoryTalk® AssetCentre uses FactoryTalk® Services Platform, a set of software components and services that are shared by many Rockwell Automation software products. FactoryTalk® Services Platform allows applications to be developed that share definitions, administration, and real-time data. This sharing of information across a system enables many of the features required to comply with regulations such as 21 CFR Part 11.

FactoryTalk® Services Platform provides FactoryTalk® software products with FactoryTalk® Diagnostics, which offers a consistent, more reliable means to communicate and pass messages back and forth between other FactoryTalk® software. This allows for the logging of event and audit messages from FactoryTalk®-enabled products to a centralized, common data repository.

A FactoryTalk® Security-enabled system allows for one-time security configuration. This means that once users and user groups have been created, all FactoryTalk® Security-enabled software products can use those same users and user groups. Creating and disabling or deleting accounts, configuring security rights, and grouping users into similar categories (typically based on role or access necessary – Role-Based Access Control) all need only be done once for the entire system.

FactoryTalk® Security-enabled products can also be linked with Microsoft Windows security, further streamlining the configuration of users and user groups for authentication and electronic signature, or "E-Signature". With later versions of FactoryTalk® Services Platform, FactoryTalk® Security includes service integration to Microsoft Entra ID, or Azure Active Directory (AD), and OpenID Connect identity providers running on top of on-premises Microsoft Active Directory, enabling a wide-variety of multi-factor authentication options. See Highlights in Version History for more information.

> FactoryTalk® AssetCentre: For additional information on FactoryTalk® AssetCentre Tips and Best Practices, refer to Rockwell Automation Knowledgebase Document ID: QA53522 – FactoryTalk AssetCentre Tip and Best Practices TOC.

FactoryTalk® AssetCentre and FactoryTalk® Service Platform's capabilities are well suited to manufacturing environments that must comply with 21 CFR Part 11, as described below in the table.

Capability	Description
Security	FactoryTalk® Security is intrinsic to FactoryTalk®-enabled products such as FactoryTalk® AssetCentre. FactoryTalk® Security allows an administrator to configure securable actions in these products using native users, or Windows-linked user and groups.
Audit	FactoryTalk®-enabled applications (e.g., FactoryTalk® View Site Edition) produce FactoryTalk® Diagnostics messages that are logged to a centralized database. FactoryTalk® AssetCentre is required to store and view FactoryTalk® Diagnostic messages internally denoted as 'Audit' messages comprehensively for all FactoryTalk® software.
Archive	Manage and version files and folders in a database-backed change control system. Archive operates in tandem with Disaster Recovery to store the 'master' version to which uploaded device configurations are compared. Automatically generated archive history captures all user interactions with the version control system. The **Archive Management of Change** functionality adds an additional layer of over-sight and control by enabling an electronic workflow that augments the existing security available for the Archive capability. Workflows can be enabled for both the check-out and check-in action separately. Workflows support single or multiple approvers. The system can be configured to escalate workflow(s) when primary approver(s) take no action.
Disaster Recovery	Scheduled and automatic backups of plant floor device configurations to the Archive ensure that the most current configuration is readily available to restore in the event of a device failure or other event. Disaster recovery supports a variety of device classes: ▪ Rockwell Automation, e.g., ControlLogix® and CompactLogix® controllers, PowerFlex® drives, Stratix switches, FactoryTalk® View Site Edition (SE) network applications, FactoryTalk® Machine Edition (ME) Runtime applications, FactoryTalk® Optix Runtime applications. ▪ 3rd party controllers, e.g., Siemens, Schneider, Mitsubishi. ▪ Devices supporting Generic File Transfer Protocol (FTP), e.g. FANUC or ABB robots. This also includes File Transfer Protocol Secure (FTPS), supported in FactoryTalk® AssetCentre v15.00 and newer, and Secure File Transfer Protocol (SFTP), supported in FactoryTalk® AssetCentre™ v16.00 and newer. ▪ Remote Computer, e.g., files and folders on a network share.

How Studio 5000 Logix Designer fits in

Studio 5000 Logix Designer is Rockwell Automation's editor for Logix Architecture controllers, such as ControlLogix® or CompactLogix®. When connected to a controller to make modifications to controller code or tag values, the software automatically generates FactoryTalk® Diagnostic audit messages aggregated by FactoryTalk® AssetCentre. Only FactoryTalk® AssetCentre can be used to comprehensively aggregate and view FactoryTalk® Diagnostic messages for all FactoryTalk®-enabled software using the 'Secure' severity. Note that FactoryTalk® AssetCentre is setup to aggregate messages from computers that are members of the same FactoryTalk® Directory, unless the Remote Agent or Remote Diagnostics connector is installed (available with FactoryTalk® AssetCentre v15.00 and newer, and FactoryTalk® Services Platform v6.50 and newer).

> FactoryTalk® AssetCentre: For more information about the Remote Agent and Remote Diagnostics configuration, refer to Rockwell Automation Knowledgebase Document ID: QA78916 - FactoryTalk AssetCentre - Remote Agent and Diagnostic Forwarding configuration.

Additionally, Logix Designer provides a service that FactoryTalk® AssetCentre uses to perform the backup task during Disaster Recovery operations. This Logix Designer service is installed when installing Studio 5000 Logix Designer.

How FactoryTalk® View Site Edition fits in

FactoryTalk® View Site Edition (SE) is a Rockwell Automation visualization software solution, used as a Human Machine Interface (HMI) or Supervisory Control and Data Acquisition (SCADA). Operators use FactoryTalk® View Site Edition to monitor manufacturing processes, make changes to process variables, and monitor and acknowledge alarms. As an operator uses the HMI client to make changes, such as those to operational parameters, or when making modifications to the HMI application, the system automatically generates FactoryTalk® Diagnostic audit messages aggregated by FactoryTalk® AssetCentre. Only FactoryTalk® AssetCentre can be used to comprehensively aggregate and view FactoryTalk® Diagnostic messages for all FactoryTalk®-enabled software using the 'Secure' severity. Note that FactoryTalk® AssetCentre is setup to aggregate messages from computers that are members of the same FactoryTalk® Directory, unless the Remote Agent or Remote Diagnostics connector is installed (available with FactoryTalk® AssetCentre v15.00 and newer, and FactoryTalk® Services Platform v6.50 and newer).

> FactoryTalk® AssetCentre: For more information about the Remote Agent configuration, refer to Rockwell Automation Knowledgebase Document ID: QA78916 - FactoryTalk AssetCentre - Remote Agent and Diagnostic Forwarding configuration.

Additionally, starting with FactoryTalk® AssetCentre version 11.00, FactoryTalk® View Site Edition version 11.00 and later network station and distributed applications can be backed up automatically. The backup includes all servers in the FactoryTalk® View Site Edition application including HMI Server(s), FactoryTalk® LiveData Server, FactoryTalk® Alarm and Events Server, and FactoryTalk® Directory Server.

How PanelView Plus 6/7 and FactoryTalk® View Machine Edition fit in

The PanelView Plus 6/7 are a family of electronic operator terminals hosting FactoryTalk® View Machine Edition (ME) on Microsoft Windows 10 IoT Core (PanelView Plus 7 Performance Series B) or Windows CE 6.0 (remaining PanelView Plus 6/7 series) embedded operating systems. Similar to FactoryTalk® View SE, FactoryTalk® View ME is used to create and deploy HMI applications used by users to interact with a system during operation, but at the machine-level.

FactoryTalk® View ME provides features to create and secure applications in environments that require 21 CFR Part 11 compliance. These features include user account management, operator audit trail, data logging, and electronic signature. The reader is strongly encouraged to review the following whitepaper to learn more about integrating FactoryTalk® AssetCentre with FactoryTalk® View Machine Edition applications running on a PanelView Plus 6/7 electronic operator interface terminal.

> FactoryTalk® Machine Edition: For additional information on applying FactoryTalk® Machine Edition 10.00 in a 21 CFR Part 11 environment, refer to FactoryTalk® View machine Edition 10.00 Complying with 21 CFR Part 11: Electronic Records & Signatures.

There are two options to enable audit logging on a PanelView Plus 6/7 terminal: forwarding of audit log information to FactoryTalk® AssetCentre, or the onboard audit feature used to record and store operator's actions locally. Onboard audit logging is recommended in order to comply with 21 CFR Part 11, in lieu of using FactoryTalk® AssetCentre as the FactoryTalk® View ME audit log repository. When a PanelView Plus 6/7 terminal is configured to forward audit log information to FactoryTalk® AssetCentre, there is no buffering or caching of audit messages in the local system.

How this compares with FactoryTalk® Optix

It is noted that outside of FactoryTalk® AssetCentre, FactoryTalk® Optix can also be used to implement onboard audit logging by capturing operator actions, system events, and application activities directly within the Optix runtime and either storing them in a local database or forwarding to a remote database with store-and-forward capability. However, this method is meant for standalone application without integration to a larger distributed network. For comprehensive integration of audit logging, the recommended approach is to utilize FactoryTalk® View SE with FactoryTalk® AssetCentre.

> FactoryTalk® Optix: For additional information and considerations on applying FactoryTalk® Optix in a 21 FR Part 11 environment, refer to FactoryTalk® Optix Help: 21CFR Part 11 Regulation Compliance.

Complying with the Part 11 Regulation

21 CFR Part 11 is composed of two major subparts (regarding electronic records and electronic signatures) that provide guidelines that regulated companies must minimally follow to achieve the level of integrity, reliability, and consistency of electronic records and signatures acceptable to the FDA. Complying with the Part 11 regulation requires a combination of strong management procedures and computer systems that meet the technical aspect of the guidance such as application security, audit trails, and password protection.

Rockwell Automation works with the life science industry to help provide confidence that products like FactoryTalk® AssetCentre comply with the technical aspect of Part 11. Each customer's security and standard operating procedures (SOPs) for supporting this regulation are unique. FactoryTalk® AssetCentre is flexible and configurable to meet the various SOPs and implementations needed to facilitate this regulation. See tables 1 and 2 for more information on 21 CFR Part 11 and how the general functionality of FactoryTalk® AssetCentre applies. Subsequent sections provide details on the implementation of FactoryTalk® AssetCentre in a 21 CFR Part 11 compliant system.

Table 1: Subpart B – Electronic Records

Section	Requirements	AssetCentre applies?	Application notes
11.10 Controls for closed systems Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to assist with the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to help confirm that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:			
a)	Validation of systems to assist with accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	□ Yes □ No ■ N/A	System validation is unique in every case and must be done by the customer. Upon request, Rockwell Automation can assist with system validation. To support routine verification of system state, automatic comparison of asset states against a previous state can be automated: • *Configure automatic backup and compare of devices*
b)	The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	■ Yes □ No □ N/A	All records are stored in the FactoryTalk® AssetCentre SQL Database and are available for viewing, printing, and exporting throughout the records retention period using FactoryTalk® AssetCentre client. See the following sections for guidance: • *Log all FactoryTalk®-Enabled application activity to the AssetCentre database* Once records have been sent to the FactoryTalk® AssetCentre database, users can employ a standard reporting tool such as Microsoft SQL Server Reporting Services (SSRS), Ocean Data Systems Dream Report, or Smart Sights XLReporter to read the records.

Section	Requirements	AssetCentre applies?	Application notes
c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	■ Yes □ No □ N/A	All records are stored in the FactoryTalk® AssetCentre SQL Database and are available for viewing, printing, and exporting throughout the records retention period. See the following sections for guidance: • *Log all FactoryTalk®-Enabled application activity to the AssetCentre database* Additionally, asset version control can be implemented through FactoryTalk® AssetCentre, and can be managed through the records retention period: • *Use AssetCentre Archive for version control* Precautionary measures such as periodic backup of the database are procedures that customers should incorporate into their SOP. Access to these databases should be controlled to maintain data integrity.

Section	Requirements	AssetCentre applies?	Application notes
d)	Limiting system access to authorized individuals.	■ Yes □ No □ N/A	Limiting system access includes configuring FactoryTalk® AssetCentre to use FactoryTalk® Security to use Microsoft security. See the following sections for guidance: • *Secure physical and logical access to computer hardware* • *Take advantage of operating system security and domains* • *Configure FactoryTalk® Security using Windows security and more* It also includes using other application security measures, which help prevent unauthorized access to data files or the operating system. See the following sections for guidance: • *Leverage AssetCentre system architecture* • *Configure FactoryTalk® Security using Windows security and more* • *Configure FactoryTalk® AssetCentre computers to automatically lock after a period of inactivity* • *Secure FactoryTalk® AssetCentre* • *Configure and Secure AssetCentre Asset Tree* For routine security verification, asset-level monitoring can be enabled to verify lifecycle status and security configurations for adherence to desired standards. See the following sections for guidance: • *Leverage AssetCentre for asset monitoring and lifecycle management*

Section	Requirements	AssetCentre applies?	Application notes
e)	Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	■ Yes □ No □ N/A	FactoryTalk® AssetCentre provides functionality to capture secure, computer-generated, time-stamped audit trails associated with user activities. Records are captured from FactoryTalk®-enabled software on computers joined to the FactoryTalk® Directory. See the following sections for guidance: • *Log all FactoryTalk®-Enabled application activity to the AssetCentre database* • *Use AssetCentre Archive Management of Change electronic workflow* Rockwell Automation recommends utilizing a clock synchronization utility to ensure that all date and time stamps are accurate. See the following sections for guidance: • *Configure Time Synchronization in a FactoryTalk® environment* Each entry in the FactoryTalk® AssetCentre activity log identifies: • time and date the action occurred, • name of the logged-in operator who performed the action, • terminal the action was performed from, • type of operation that was performed, • value of the changed item before and after the change, and Appropriate IT policies and procedures must be established to ensure that records are held for an appropriate duration of time. See the following sections for guidance: • *Setup FactoryTalk® Database Management*

Section	Requirements	AssetCentre applies?	Application notes
f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	■ Yes □ No □ N/A	FactoryTalk® Security can be used to restrict access to authorized user accounts and can enforce signing workflows. See the following sections for guidance: • *Secure FactoryTalk® AssetCentre* • *Configure and Secure AssetCentre Asset Tree* • *Use AssetCentre Archive Management of Change electronic workflow* The system can be configured to produce events tracking attempts to access unauthorized actions. See the following sections for guidance: • *Log all FactoryTalk®-Enabled application activity to the AssetCentre database*
g)	Use of authority checks to help provide confidence that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	■ Yes □ No □ N/A	FactoryTalk® AssetCentre can use a combination of Microsoft Windows domain security and FactoryTalk® Security for authority checks. See the following sections for guidance: • *Take advantage of operating system security and domains* • *Configure FactoryTalk® Security using Windows security and more* • *Use AssetCentre Archive Management of Change electronic workflow* Customers should implement policies and administrative procedures to define authorized access to the system.
h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	■ Yes □ No □ N/A	FactoryTalk® Security can create location-specific security settings to enforce "line-of-sight" by allowing certain operations only from designated terminals and workstations. See the following sections for guidance: • *Configure FactoryTalk® Security using Windows security and more*
i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	■ Yes □ No □ N/A	Customers are responsible for hiring and training appropriate staff members with the education, training, and experience to perform assigned tasks. FactoryTalk® AssetCentre helps support this requirement by validating that only users with appropriate security rights are granted access to the system through FactoryTalk® Security.

Section	Requirements	AssetCentre applies?	Application notes
j)	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	□ Yes □ No ■ N/A	Customers should implement policies and procedures that outline the significance of electronic signatures, in terms of individual responsibility, and the consequences of falsification for both the company and the individual.
k)	Use of appropriate controls over systems documentation including:	■ Yes □ No □ N/A	A comprehensive system can be implemented using FactoryTalk® AssetCentre software and services. FactoryTalk® AssetCentre user documentation is provided in electronic (.pdf) format in the product download file. The distribution of these documents is at the customer's discretion.
1.	Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	■ Yes □ No □ N/A	All FactoryTalk® AssetCentre documents are bundled and delivered with the product. Rockwell Automation assists with controlled delivery and distribution of the correct versioning of the documents.
2.	Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	■ Yes □ No □ N/A	Rockwell Automation assists with delivery and distribution of the correct versioning of the product documents.
11.30 Controls for open systems			
	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to assist with the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to assist with, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	□ Yes □ No ■ N/A	Customers are responsible for establishing internal policies and procedures to assist with the appropriate controls that are put in place to meet regulation for an open system. Access to FactoryTalk® AssetCentre requires appropriate login and password whether customers opt to implement a closed or an open system.

Section	Requirements	AssetCentre applies?	Application notes
11.50 Signature manifestations			
a)	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:		FactoryTalk® AssetCentre records user interactions made to FactoryTalk® AssetCentre and FactoryTalk®-Enabled software via the audit trail. This includes changes to the system configuration and archive use, and records date/timestamp and user information. When implemented with the proper controls, these audits could be interpreted as an electronic signature related to those actions. See the following sections for guidance: • *Configure FactoryTalk® AssetCentre computers to automatically lock after a period of inactivity* FactoryTalk® AssetCentre Archive MoC utilizes an electronic signing workflow for archive check-out and check-in. Interaction with the workflow system (i.e., initiating, approving, or denying workflows) generates audit messages to the audit log. See the following sections for guidance: • *Use AssetCentre Archive Management of Change electronic workflow* Additional FactoryTalk®-enabled products, such as FactoryTalk® View Site Edition, may provide an electronic signature that generates an audit message captured by FactoryTalk® AssetCentre.

Section	Requirements	AssetCentre applies?	Application notes
1.	The printed name of the signer;	■ Yes □ No □ N/A	With user credentials properly configured in the system, FactoryTalk® AssetCentre with FactoryTalk® Diagnostics provides an audit trail for actions performed that is composed of a time and date stamp, operator ID and full name (if available), and the action taken. The customer can include the full name of the user in any reports.
2.	The date and time when the signature was executed; and	■ Yes □ No □ N/A	FactoryTalk® AssetCentre records the date and time associated with each action in FactoryTalk® Diagnostics.
3.	The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	■ Yes □ No □ N/A	FactoryTalk® AssetCentre audit trail records the action the user performed when the audit record was generated. When integrated with FactoryTalk® View SE electronic signature feature, the record can be configured to display and record the meaning of the signature, including performer and approver signatures.
4.	The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human-readable form of the electronic record (such as electronic display or printout).	■ Yes □ No □ N/A	FactoryTalk® AssetCentre Log View and Search present this audit trail in human readable form. FactoryTalk® AssetCentre, and the FactoryTalk® Diagnostics viewer shows the username, time, and action. These fields are available for use in any reports created from the data using a 3rd party tool.

Section	Requirements	AssetCentre applies?	Application notes
11.70 Signature/record linking			
a)	Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to provide confidence that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	■ Yes □ No □ N/A	FactoryTalk® AssetCentre Archive MoC utilizes an electronic signing workflow for archive check-out and check-in. Interaction with the workflow system (i.e., initiating, approving, or denying workflows) generates audit messages to the audit log. See the following sections for guidance: • *Use AssetCentre Archive Management of Change electronic workflow* Additionally FactoryTalk® AssetCentre records user interactions made to FactoryTalk® AssetCentre and FactoryTalk®-Enabled software via the audit trail. FactoryTalk®-enabled products, such as FactoryTalk® View Site Edition, may provide an electronic signature that generates an audit message captured by FactoryTalk® AssetCentre. All signatures and records are automatically tied to a specific user to identify who performed each action. Data records in the FactoryTalk® AssetCentre SQL Database can be protected by a username and password, thus helping to help prevent information from being altered.

Table 2: Subpart C – electronic signatures

Section	Requirements	AssetCentre applies?	Application notes
11.100 General requirements			
a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	■ Yes □ No □ N/A	Administration of system access to manage unique credentials can be performed using Microsoft Windows security and more, integrated to FactoryTalk® Security. See the following sections for guidance: • *Take advantage of operating system security and domains* • *Configure FactoryTalk® Security using Windows security and more* In addition, the FactoryTalk® Administration Console tool also allows the creation of unique credentials for each user within FactoryTalk® Security. Procedures can be implemented to deliver that user IDs do not get deleted or reassigned. It is recommended to disable user IDs rather than deleting them as a best practice.
b)	Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	□ Yes □ No ■ N/A	The customer's management procedure should include the verification of the identity of an individual prior to sanctioning an individual's electronic signature. Once a user has been sanctioned and a unique account with password has been created in the FactoryTalk® Security system, the user is required to enter his login and password to access FactoryTalk® AssetCentre. This process validates the identity of the user of FactoryTalk® AssetCentre.
c)	Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.	□ Yes □ No ■ N/A	Customers are responsible for notifying the FDA of their intention of recognizing the electronic signature to be a legally binding equivalent of traditional handwritten signatures.
1.	The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.	□ Yes □ No ■ N/A	Customers are responsible for submitting the certification to the FDA that the electronic signatures in their system are intended to be a legally binding equivalent of traditional handwritten signatures.

Section	Requirements	AssetCentre applies?	Application notes
2.	Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	□ Yes □ No ■ N/A	Customers are responsible for any requested follow up of certification or testimonial to have the electronic signatures be a legally binding equivalent of traditional handwritten signatures.
11.200 Electronic signature components and controls			
a)	Electronic signatures that are not based upon biometrics shall:		
1.	Employ at least two distinct identification components such as an identification code and password.	■ Yes □ No □ N/A	FactoryTalk® AssetCentre requires the user to login to the system before any work can occur. FactoryTalk® AssetCentre can require two components for user identification: a unique sign in ID and password. In later versions, a user can also sign in through multiple factors, such as biometrics or ID cards, through integration to Azure AD and OpenID. See the following sections for guidance: • *Take advantage of operating system security and domains*
1.a.	When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.	□ Yes ■ No □ N/A	FactoryTalk® AssetCentre requires the complete user identification — unique sign in ID and password — in the initial sign in of the system. If the user logs out of the FactoryTalk® AssetCentre system and again requires access, the user must reenter the sign in ID and password. FactoryTalk® AssetCentre Archive MoC utilizes an electronic signing workflow for archive check-out and check-in. Interaction with the workflow system (i.e., initiating, approving, or denying workflows) generates audit messages to the audit log. See the following sections for guidance: • *Use AssetCentre Archive Management of Change electronic workflow* When capturing audit trail records from the FactoryTalk® View SE electronic signature feature, both the user signs in ID and password are required to perform an action.

Section	Requirements	AssetCentre applies?	Application notes
1.b.	When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.	■ Yes □ No □ N/A	The customer must implement sign out procedures to enforce user log-off at the end of any continuous period of controlled system access, and to enforce sign in at the start of the next access period. To confirm that a workstation is not left unattended, a password-protected screen saver or automatic sign out control can be used for all FactoryTalk® AssetCentre clients. See the following sections for guidance: • *Configure FactoryTalk® AssetCentre computers to automatically lock after a period of inactivity* When capturing audit trail records from the FactoryTalk® View SE electronic signature feature, both the user signs in ID and password are required to perform an action.
2.	Be used only by their genuine owners; and	□ Yes □ No ■ N/A	The customer is responsible for ensuring that the genuine owner is signing the electronic signature and that the password is not being disclosed to others.
3.	Be administered and executed to provide confidence that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.	□ Yes □ No ■ N/A	The customer should implement appropriate procedures to handle situations that require an electronic signature by anyone other than its genuine owner.
b)	Electronic signatures based upon biometrics shall be designed to provide confidence that they cannot be used by anyone other than their genuine owners.	□ Yes □ No ■ N/A	FactoryTalk® AssetCentre can support interfaces to biometric-based sign in mechanisms. See the following sections for guidance: • *Take advantage of operating system security and domains*
11.300 Controls for identification codes/passwords Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to provide confidence that their security and integrity. Such controls shall include:			

Section	Requirements	AssetCentre applies?	Application notes
a)	Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	■ Yes □ No □ N/A	Microsoft Windows security can be integrated with FactoryTalk® Security to manage user accounts used within the FactoryTalk® AssetCentre application. Microsoft Windows security maintains all sign in IDs to help prevent reuse or reassignment of previously created sign in IDs. A user's identification can be disabled or inactivated without deleting the user's sign in ID. See the following sections for guidance: • *Configure FactoryTalk® Security using Windows security and more*
b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	■ Yes □ No □ N/A	FactoryTalk® AssetCentre can use Microsoft Windows security and more to manage user accounts. Password expiration, password aging, password complexity requirements, account expiration, disabling of accounts, lockout after a system-configurable number of invalid sign in attempts, and forcing a change of password on first sign in are all security features provided by both Microsoft Windows security and FactoryTalk® Security. See the following sections for guidance: • *Use Windows account password aging and management*
c)	Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	□ Yes □ No ■ N/A	The customer is responsible for implementing loss management procedures.
d)	Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security uncoit, and, as appropriate, to organizational management.	■ Yes □ No □ N/A	FactoryTalk® AssetCentre can use Microsoft Windows security mechanisms to detect unauthorized use if rules for authorized use are maintained. For example, a rule might stipulate that after three incorrect login attempts an account is suspended. See the following sections for guidance: • *Take advantage of operating system security and domains* • *Configure FactoryTalk® Security using Windows security and more*

Section	Requirements	AssetCentre applies?	Application notes
e)	Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to help ensure that they function properly and have been altered in an unauthorized manner.	□ Yes □ No ■ N/A	The customer's management procedures should include periodic test and/or validation of any devices that may risk the integrity of a user's identification.

Guidance for Applying FactoryTalk® AssetCentre in a 21 CFR Part 11 environment

The following topics describe how FactoryTalk® AssetCentre can be used or configured to technically satisfy the requirements of the FDA 21 CFR Part 11 regulation.

- Secure physical and logical access to computer hardware
- Take advantage of operating system security and domains
- Leverage AssetCentre system architecture
- Configure FactoryTalk® Security using Windows security and more
- Secure FactoryTalk® AssetCentre
- Configure and Secure AssetCentre Asset Tree
- Log all FactoryTalk®-Enabled application activity to the AssetCentre database
- Configure FactoryTalk® AssetCentre computers to automatically lock after a period of inactivity
- Use Windows account password aging and management
- Use AssetCentre Archive for version control
- Use AssetCentre Archive Management of Change electronic workflow
- Configure automatic backup and compare of devices
- Leverage AssetCentre for asset monitoring and lifecycle management
- Configure Time Synchronization in a FactoryTalk® environment
- Setup FactoryTalk® Database Management

Secure physical and logical access to computer hardware

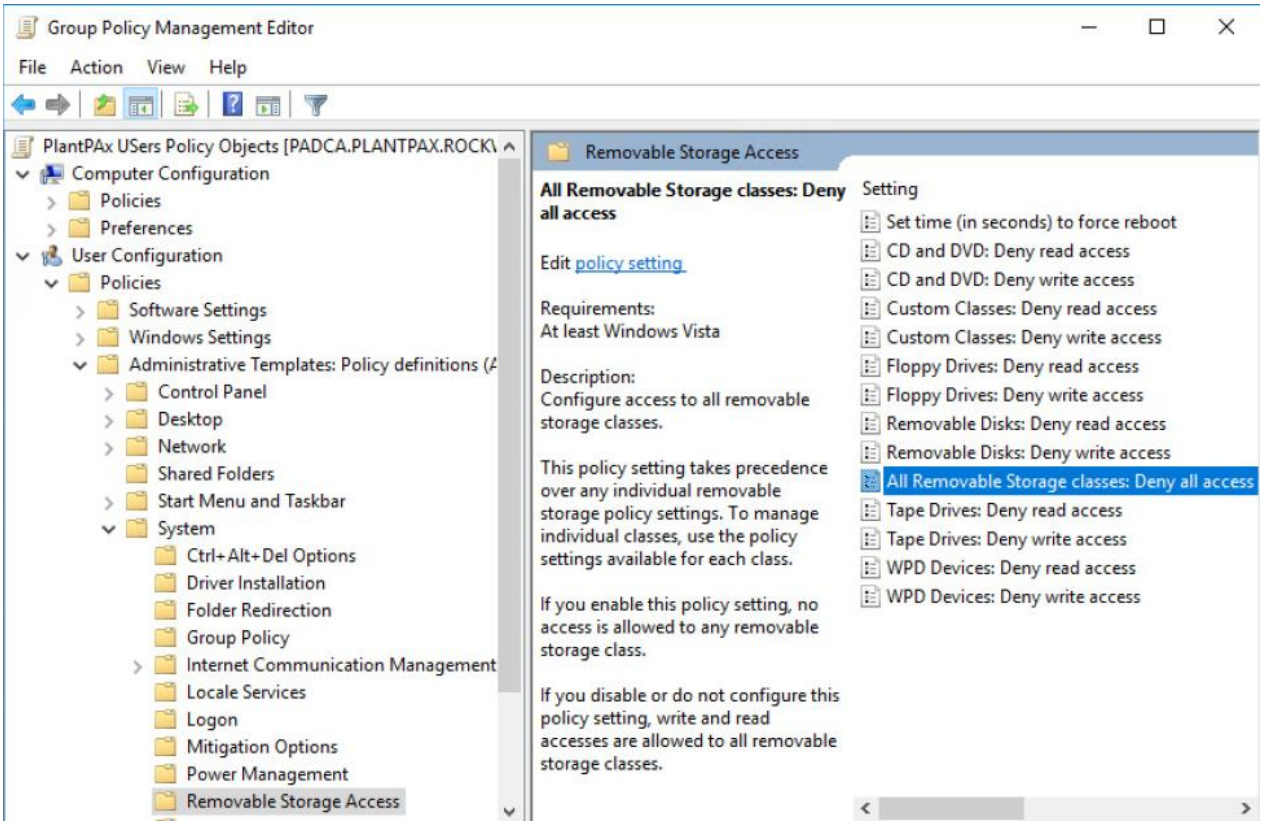
> Applies to: FactoryTalk® AssetCentre, Versions 11.00 through 16.00

It is essential to limit individuals' access to the machines running Windows operating systems and the FactoryTalk® AssetCentre Server and Agents, and the FactoryTalk® Services Platform Server (which hosts FactoryTalk® Security). In general, a user's access to the underlying file system may be through physical access points, such as access to mouse, keyboard, and physical access ports, or through network access points. It is recommended to put measures in place to limit user access and to help protect your systems, such as through use of secure server enclosures or rooms, cybersecurity protections, and through deployed architectures.

For systems employing network access as the primary method for file transfer, policies can be configured to restrict access for physical media.

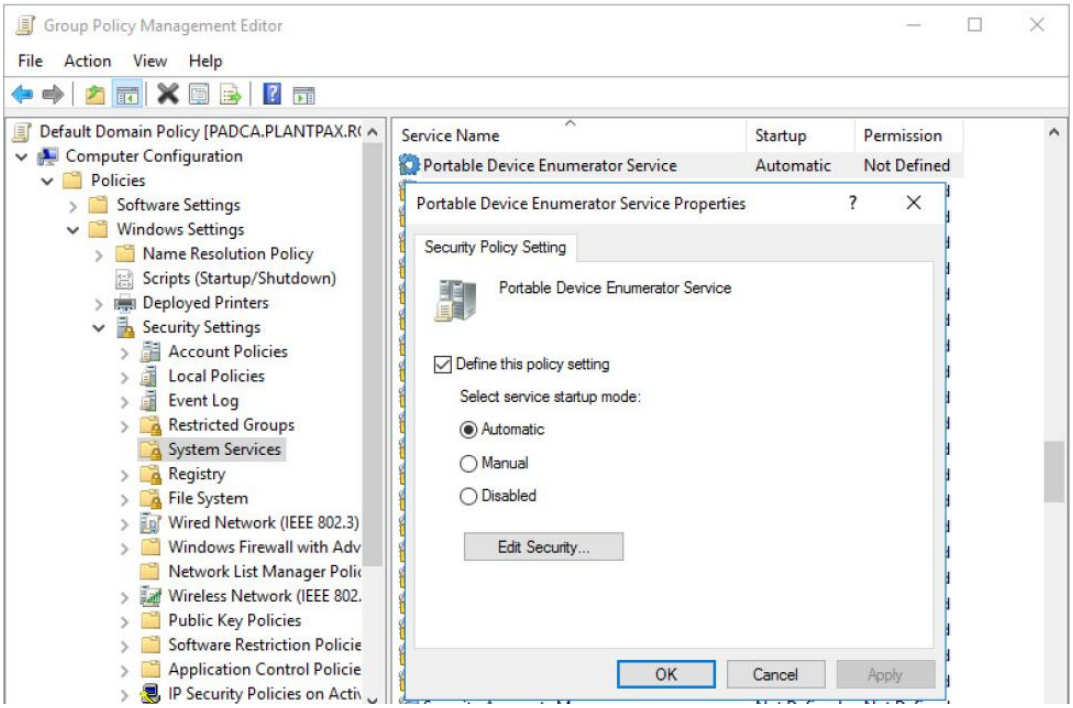
Logically restrict access for removable storage

Using the Windows operating system, you can logically restrict access to the USB Drive for appropriate users to help prevent unauthorized access. For the respective Group Policy Object (GPO), apply the user policy through the Group Policy Management Editor > User Configuration > Policies > Administrative Templates > System > Removable Storage Access. Configure the policy 'All Removable Storage classes: Deny all access' as 'Enabled'.



Logically manage access for mass storage devices

You can enforce administrator-defined policies for connected mass storage devices. For the respective GPO, apply the computer policy through the Group Policy Management Editor > Computer Configuration > Policies > Windows Settings > Security Settings > System Services. Configure the service 'Portable Device Enumerator Service Properties' by checking 'Define the policy setting' and configuring as 'Automatic'.



Take advantage of operating system security and domains

> Applies to: FactoryTalk® AssetCentre, Versions 11.00 through 16.00

FactoryTalk® AssetCentre uses FactoryTalk® Security to make efficient use of the security features built into the underlying Microsoft Windows operating systems. For compliance, all FactoryTalk® computers within a FactoryTalk® directory should be part of the same Windows domain, managed by a Domain Controller.

As such, management of security policies are typically delegated to Windows GPOs within Active Directory. In this case, work with your Active Directory administrator to apply appropriate security policies to your FactoryTalk® AssetCentre computers based on your FactoryTalk® AssetCentre architecture, such as enabling or disabling the screen saver, disabling USB access, etc.

> For additional information regarding FactoryTalk® AssetCentre versions and compatible operating systems, refer to the Product Download and Compatibility Center.
>
> For additional information about Domain Controller architectures and Active Directory group policy management, best practice guidance has been outlined as part of the PlantPAx® distributed control system manuals, refer to the *Domain or Workgroup* section of the PlantPAx® Distributed Control System Configuration and Implementation User Manual.

Enterprise Identity Management

> Applies to: FactoryTalk® AssetCentre, Version 13.00 through 16.00

FactoryTalk® Services Platform allows for service integration to Microsoft Entra ID, or Azure Active Directory (AD), and OpenID Connect identity providers running on top of on-premises Active Directory. This enables enterprise identity management and a wide variety of multi-factor authentication options with FactoryTalk® AssetCentre including: one-time phone code, biometrics, radio frequency identification (RFID) cards, and NYMI bands (biometric wearable).

Multi-Directory Environments

> Applies to: FactoryTalk® AssetCentre, Version 15.00 through 16.00

In environments where multiple FactoryTalk® AssetCentre servers and FactoryTalk® Directories are deployed across separate Active Directory domains, a trusted-domain architecture may be used. This architecture is typically employed when organizational, cybersecurity, or regulatory requirements necessitate independent administration of sites or business units. FactoryTalk® AssetCentre Remote Agents and Diagnostic Connectors can be deployed to extend asset management and event monitoring capabilities across trusted domains.

Leverage AssetCentre system architecture

> Applies to: FactoryTalk® AssetCentre, Versions 12.00 through 16.00

FactoryTalk® AssetCentre system architecture includes a server, one or more desktop clients, one or more web clients, and for systems with disaster recovery, one or more agents. An Agent is a computer hosting applications, such as Studio 5000 Logix Designer, that performs disaster recovery tasks as assigned by the FactoryTalk® AssetCentre server. The system also must include a Microsoft SQL Server to host the database instance that stores information related to FactoryTalk® AssetCentre.

It is recommended that the FactoryTalk® Directory and FactoryTalk® AssetCentre system components, including server, desktop clients, and SQL Server database reside on the same local area network (LAN). For secure communications over the network, it is also recommended that transport layer security (TLS) be enabled with a certificate authority (CA) server to secure communications over the network. In cases where traffic from FactoryTalk® components must cross security zones, the network may need to be configured to permit traffic across specific port ranges and protocols.

> FactoryTalk® AssetCentre: For more information on firewall configurations, refer to: Configuring Firewalls for FactoryTalk AsstCentre.

FactoryTalk® AssetCentre servers run as services and therefore do not require any user to be logged on to the server computer. The FactoryTalk® AssetCentre agents generally run as services and do not require any user to be logged on to the agent computer. However, when a FactoryTalk® AssetCentre agent is working to perform disaster recovery operations with 3rd-party devices, such as a Siemens controller utilizing TIA Portal software, a Schneider controller utilizing EcoStruxure Control Expert software, etc., the agent requires a standard Windows user account to be logged in to the agent computer to run the Agent as an application and not as a service. In this case, it is important to use a password-protected screen saver or Windows Automatic Restart Sign-On (ARSO) to lock the desktop of the agent of the 3rd party device and protect the proper operation of the agent and security of the agent computer. Refer to section *Configure FactoryTalk® AssetCentre computers to automatically lock after a period of inactivity*.

Users can log in and out of the FactoryTalk® AssetCentre client without affecting the computer or software components of the FactoryTalk® AssetCentre servers or agents. User account management is performed for accounts with client access while the servers and agents are running a continuous operation. Users at the FactoryTalk® AssetCentre clients have no way to alter server or agent processes or shut down the operation. Even when a named user account logs onto a server and agent with running components, these components run as background services or service account applications, which are not affected by the security permissions of the logged in user.

SQL Server Architecture

> Applies to: FactoryTalk® AssetCentre, Version 11.00 through 16.00

The FactoryTalk® AssetCentre database contains critical electronic records, including audit trail data and controlled asset backups. To mitigate the risk of failures associated with the SQL Server (e.g., disk at capacity, service interruption, etc.), it is recommended to host the SQL server on a dedicated set of servers with a redundant database architecture via SQL mirroring. For AssetCentre services, it is recommended to use standalone managed service accounts (sMSA) or group-managed service accounts (gMSA) to provide automatic password management, simplified service principal name (SPN) management, and the ability to delegate the management to other administrators.

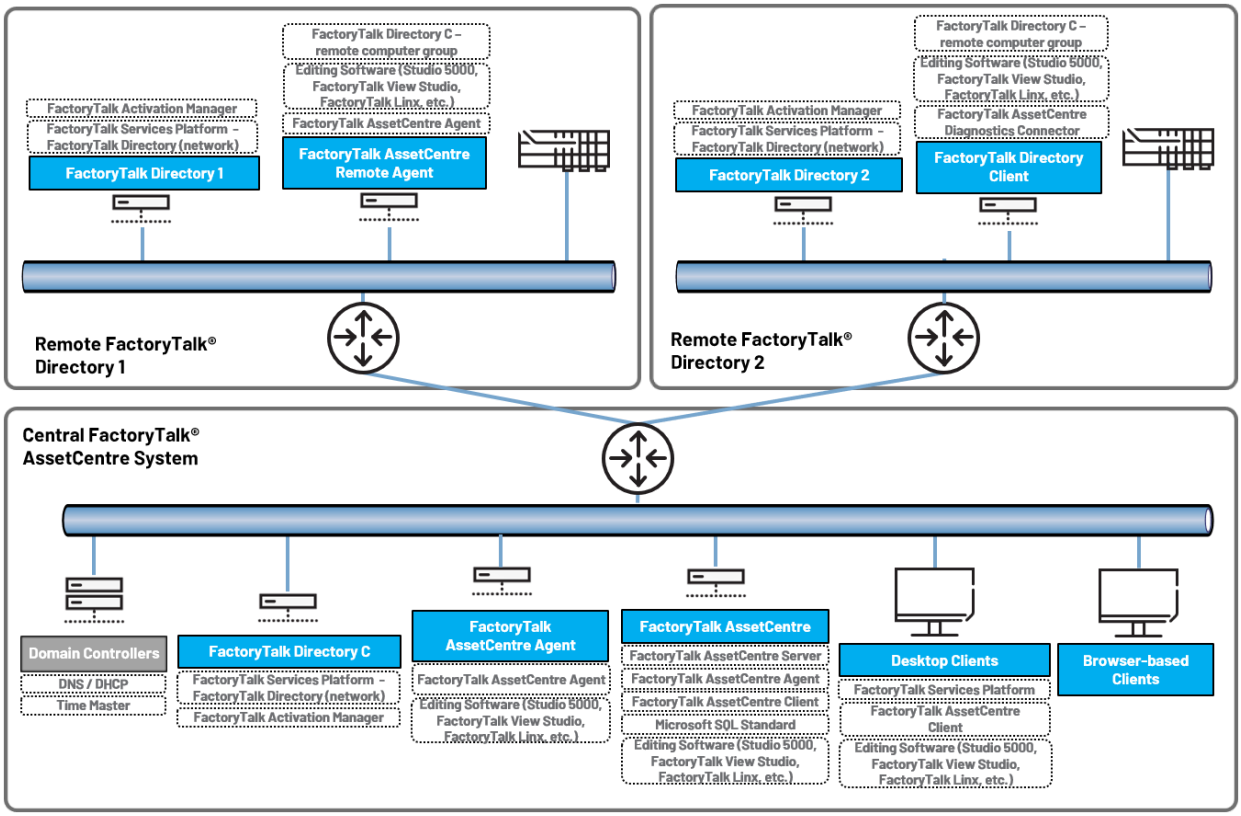
To set up SQL Server mirroring, use the Data Source Configuration Wizard to configure the mirrored SQL database for use with AssetCentre.

> FactoryTalk® AssetCentre: For additional information on FactoryTalk® AssetCentre database management, refer to Rockwell Automation Knowledgebase Document ID: QA38697 - FactoryTalk AssetCentre: Database Management.

Multi-Directory Architectures

> Applies to: FactoryTalk® AssetCentre, Version 15.00 through 16.00

In environments where multiple FactoryTalk® AssetCentre servers and FactoryTalk® Directories are required, such as in multi-site deployments or systems with parallel development environments, a multi-directory architecture can be employed. This architecture uses FactoryTalk AssetCentre Remote Agents and Diagnostic Connectors to extend asset management and event monitoring capabilities across separate FactoryTalk® directories. Remote Agents enable disaster recovery operations for assets residing in external directories, while Diagnostic Connectors provide secure forwarding of FactoryTalk® Diagnostics messages from external directories to the central AssetCentre server for centralized event visibility and reporting. With this architecture, the AssetCentre web client can be used to facilitate remote retrieval of asset files.



> FactoryTalk® AssetCentre: For additional information on FactoryTalk® AssetCentre database management, refer to Rockwell Automation Knowledgebase Document ID: QA78916 - FactoryTalk AssetCentre - Remote Agent and Diagnostic Forwarding configuration.

Configure FactoryTalk® Security using Windows security and more

> Applies to: FactoryTalk® AssetCentre, Versions 11.00 through 16.00

Before you configure FactoryTalk® AssetCentre security actions, you must create user or user group accounts in FactoryTalk® Security. Best practice for configuring the security actions of any FactoryTalk®-enabled product is to first create native FactoryTalk® Security group(s). Once the user groups have been created, assign specific product securable actions to those native FactoryTalk® Security group(s). Windows-linked user groups can then be added to FactoryTalk® Security and assigned to those native FactoryTalk® Security group(s).

Abstracting the specific Windows-linked user and group from the security configuration creates a system that is more readily validated. Written policies are created to govern which Windows-linked groups are added to the native FactoryTalk® groups, and which Windows user accounts are added to specific Windows groups. For more information on securing FactoryTalk® AssetCentre, refer to section *Secure FactoryTalk® AssetCentre*.

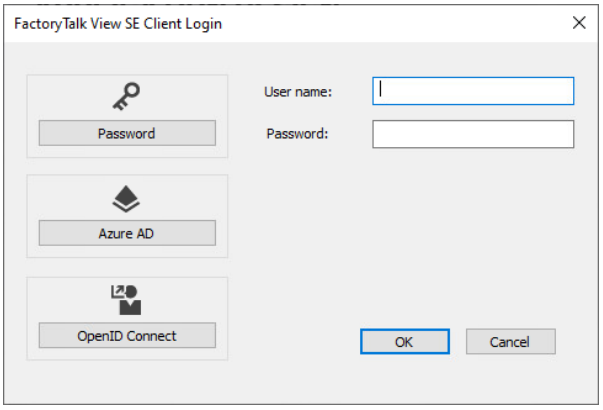
If line-of-sight security is required, it is also possible to create FactoryTalk® Security computer groups for computers in the directory. Security permissions can then be granted to the FactoryTalk® user group for the required computer group. For a robust security strategy that can be more easily tested and managed, consider nesting Windows-linked computers or user groups within native FactoryTalk® Security groups.

> FactoryTalk® AssetCentre: For additional information on creating a FactoryTalk user group, adding a Windows-linked user, and setting up line-of-sight security, refer to FactoryTalk Security Application Technique.

User Group and User Management

> Applies to: FactoryTalk® AssetCentre, Versions 13.00 through 16.00

Users have the option of using either Windows-Linked groups, Azure AD groups, or OpenID Connect for login, depending on the service integration of Active Directory and enterprise identity management. The Azure AD or OpenID Connect user accounts can be added to the native FactoryTalk® Security groups in lieu of Windows-linked groups.



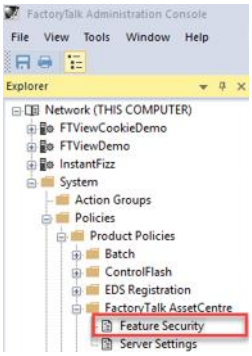
> Applies to: FactoryTalk® AssetCentre, Versions 15.00 through 16.00

During installation, upon selecting the Secure security posture option, the Windows-linked “All Users” group is automatically removed from FactoryTalk® Security configurations.

Secure FactoryTalk® AssetCentre

> Applies to: FactoryTalk® AssetCentre, Version 11.00 through 16.00

To limit the roles that individuals can fulfill in the FactoryTalk® AssetCentre it is necessary to configure system security. This is done in FactoryTalk® Security through the FactoryTalk® Administration Console system and product policies. Using security user actions can be controlled (e.g., create a schedule, view logs, access Design mode), limit asset access in the Asset Tree (e.g., view Asset Tree content), and limit Archive actions (e.g., file checkout, version pinning).

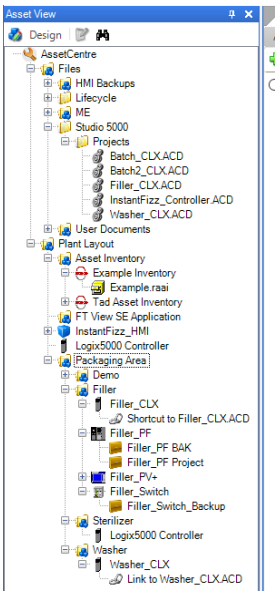


> FactoryTalk® AssetCentre: For additional information on securing FactoryTalk® AssetCentre within FactoryTalk® Security, refer to FactoryTalk Security Application Technique.

Configure and Secure AssetCentre Asset Tree

> Applies to: FactoryTalk® AssetCentre, Version 11.00 through 16.00

FactoryTalk® AssetCentre uses a hierarchical model to represent the assets within the manufacturing facility. This model is called the Asset Tree. The Asset Tree contains both physical devices (e.g., controllers or drivers) and files, folders, and collections of files in a folder structure called 'binders'. Below is an example of one such Asset Tree.



Configuring securable actions in FactoryTalk® AssetCentre can prevent specific users from seeing parts of the plant (e.g., a technician is assigned to a packaging area but has no permission to work on assets in the formulation area) or performing operations (e.g., asset checkout) within the FactoryTalk® AssetCentre version control system, called Archive. Securable actions can also limit the actions available to specific users within the FactoryTalk® AssetCentre Archive.

> FactoryTalk® AssetCentre: For additional information on configuring securable actions in FactoryTalk® AssetCentre, refer to FactoryTalk Security Application Technique.

Log all FactoryTalk®-Enabled application activity to the AssetCentre database

> Applies to: FactoryTalk® AssetCentre, Version 11.00 through 16.00

FactoryTalk® AssetCentre provides a central set of tools securing access to the control system, tracking actions of users within the control system. To implement audit and event logging with FactoryTalk® AssetCentre, the FactoryTalk® AssetCentre Diagnostics Connector or FactoryTalk® AssetCentre Client must be installed on each machine that will be a FactoryTalk® View SE client.

FactoryTalk® AssetCentre captures three different logs:

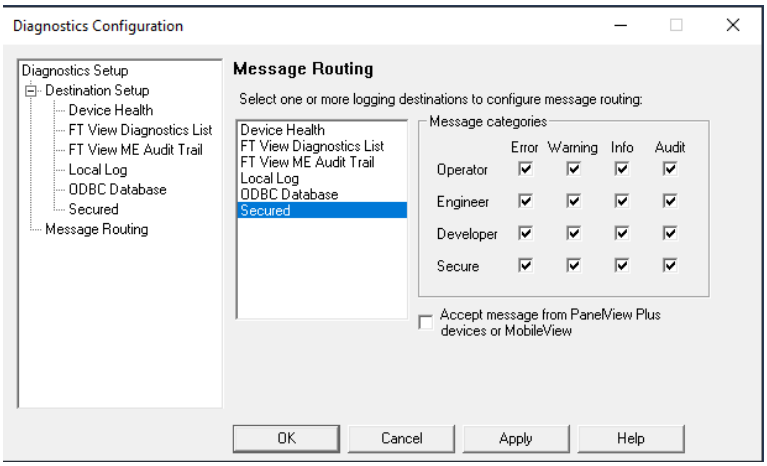
- **Event Log.** This log shows database information regarding events that occur in the system. Events are system-initiated. For example, an upload occurred, or a scheduled task completed. Event records are generated by FactoryTalk®-enabled products.
- **Audit Log.** This log shows database information regarding actions that users perform in the system, such as making edits to a Studio 5000 Logix Designer® project or opening or closing such a software product. Audit records are generated by FactoryTalk®-enabled products.
- **Diagnostics & Health Log.** The Diagnostics and Health Log provides information about the condition of automation devices. For example, a monitoring software product, such as Automatic Device Descriptive Analytics (ADDA) function, detects a problem with a device on the automation network. It reports the problem and logs the information in the Diagnostics and Health Log.

When connection is lost to the FactoryTalk® AssetCentre server, the FactoryTalk® AssetCentre Client or Diagnostics Connector stores undelivered information in a buffer until the connection is established again.

The following steps must be performed on each machine to set up FactoryTalk® AssetCentre audit and event logging:

1 From the FactoryTalk® Administration Console Tools menu, open the Diagnostics Setup editor.

2 Select Message Routing to specify which categories of messages can be routed to each logging destination (local log or ODBC data source). To capture necessary operator audit information, it is recommended that at least all checkboxes are checked for the *Secure* row and *Audit* column. However, additional testing can be required to confirm that all necessary events are captured within the audit trail, with checkboxes enabled/disabled as required.



It is also noted that due to the volume of messages generated during runtime, considerations can be given to database maintenance and audit trail report optimization to confirm optimal system performance.

> For additional information on configuring FactoryTalk® View SE audit and event logging with FactoryTalk® AssetCentre, refer to the Rockwell Automation Knowledgebase Document ID: QA18043 - Using FactoryTalk® View SE with FactoryTalk® AssetCentre.

Configure FactoryTalk® AssetCentre computers to automatically lock after a period of inactivity

> Applies to: FactoryTalk® AssetCentre, Version 11.00 through 16.00

To ensure that only operators with the proper credentials are accessing workstations in a closed system, a password-protected screen saver or Windows Automatic Restart Sign-On (ARSO) can be used on the FactoryTalk® AssetCentre client workstations.

Since FactoryTalk® AssetCentre server and most agent components, such as Studio 5000 Logix Designer, run as services with no need for an interactive Windows user to be logged on, it is not necessary to use password-protected screen savers and ARSO on the hosts of the servers or agents for standard assets.

However, when a FactoryTalk® AssetCentre agent is running to perform disaster recovery operations with 3rd party devices through the natively built-in 3rd party controllers, such as a Siemens controller utilizing TIA Portal software, a Schneider controller utilizing EcoStruxure Control Expert software, etc., the agent requires a user account to be logged in to the agent computer to run the application. In this case, it is important to use a password-protected screen saver and Windows ARSO to lock the desktop of the agent of the 3rd party devices and protect the proper operation of the agent and security of the agent computer.

Use a password-protected screen saver

To secure the AssetCentre computer after an idle period, a password-protected screen saver can be enabled on the AssetCentre computer to lock the desktop after a timeout period. For the respective GPO, apply the screen saver policy through the Group Policy Editor > User Configuration > Administrative Templates > Control Panel > Personalization. Configure the 'Enable screen saver' policy as 'Enabled', and then configure the policies 'Screen saver timeout' and 'Force-specific screen saver' as required.

Windows Automatic Restart Sign-On

To secure the AssetCentre computer on startup, Windows ARSO can be set up on the AssetCentre computer to automatically sign in on the computer and lock after a reboot.

> FactoryTalk® AssetCentre: For more information on setup of Windows Automatic Restart Sign-On, refer to the Rockwell Automation Knowledgebase Document ID: QA75769 - Windows Automatic Restart Sign-On (ARSO) for FactoryTalk AssetCentre Agent computers.

Use Windows account password aging and management

> Applies to: FactoryTalk® AssetCentre, Version 11.00 through 16.00

When FactoryTalk® AssetCentre is integrated with Windows-linked users and Windows-linked user groups, user account and password management and aging are done in Microsoft Windows by the system administrator or Active Directory administrator. User accounts and password GPOs can be configured so that, for example, the passwords expire after a certain time and with appropriate lockouts after multiple failed sign in attempts. These group policies are recommended:

- Password strength
- Account lockout
- Kerberos
- Interactive sign in

This information is part of a corporate IT department Standard Operating Procedure, or SOP.

Use AssetCentre Archive for version control

> Applies to: FactoryTalk® AssetCentre, Version 11.00 through 16.00

FactoryTalk® AssetCentre can be used to keep track of revisions of your device configurations, HMI projects, and other files and file collections. Version control software, such as FactoryTalk® AssetCentre Archive, retains all file and project components in a central repository for safekeeping. FactoryTalk® AssetCentre can represent files, folders, and a collection of files stored in a folder structure called a 'binder'. Binders are like the output files of compression utilities (e.g., WinZip).

To modify any asset configuration a user must perform a *check out*. Check-out retrieves the configuration from the repository to the local computer and locks the file in the repository preventing others from also performing check-out. The system logs the check-out recording the username, component, and check-out date and time in both the FactoryTalk® AssetCentre audit log and Archive history. When the user has completed any modifications, the user performs a check-in. During a check-in if the configuration was altered the modified file is transferred to the repository and a new version is created and the file is available for other users to check-out. The system logs the username, component, and check in date and time, and allows the user to add comments explaining the modifications to both the audit log and Archive history. This provides you with a record of all changes made. From the Archive both old and new versions are accessible.

Use AssetCentre Archive Management of Change electronic workflow

> Applies to: FactoryTalk® AssetCentre, Version 11.00 through 16.00

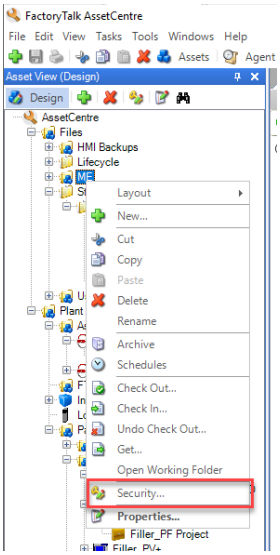
Utilizing MoC can provide additional controls to the security configured in the Asset Tree. Through the workflow additional oversight of proposed changes can be realized. For example, the workflow can be used to ensure that:

- a specific group (e.g., Engineers) must review and approve a proposed modification by a maintenance technician.
- files can only be checked in once a company's Engineering Change process was followed.

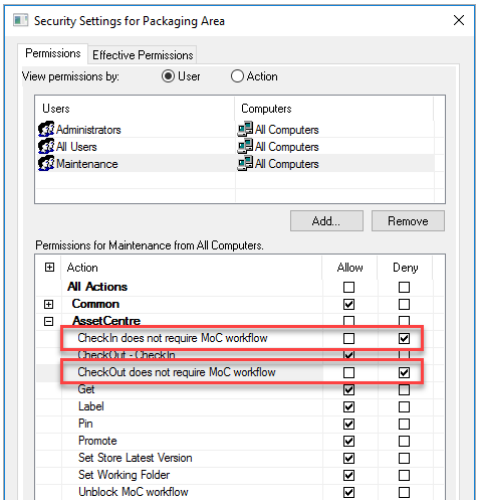
It is important to note that when enabling the Archive MoC feature, administration of users and notification configurations are managed directly through the MoC administration interface, and the audit trail records related to the Archive MoC are managed in a separate database from the AssetCentre audit trail database. This section outlines how to configure Archive MoC and considerations for management.

Configure the system to use Archive Management of Change

To configure areas within the Asset Tree to require the use of Archive MoC launch FactoryTalk® AssetCentre Client and enter *Design* mode. Next, select the container that is the parent of the Asset Tree area that is to use Archive MoC and select *Security*.

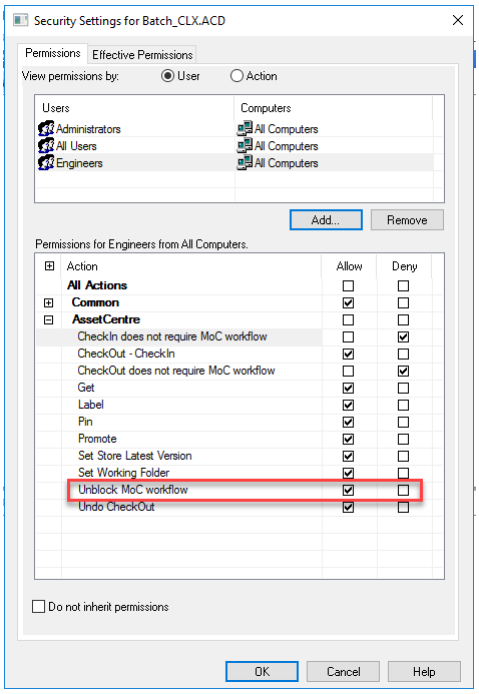


Next, select, or add, the user and computer group for which Archive MoC capability will be required. Expand the *AssetCentre* permissions group and **deny** *CheckIn does not require MoC workflow* to require users to complete Archive MoC workflow during a check-in operation. **Deny** *CheckOut does not require MoC workflow*, to require users to complete Archive MoC workflow during a check-out operation.



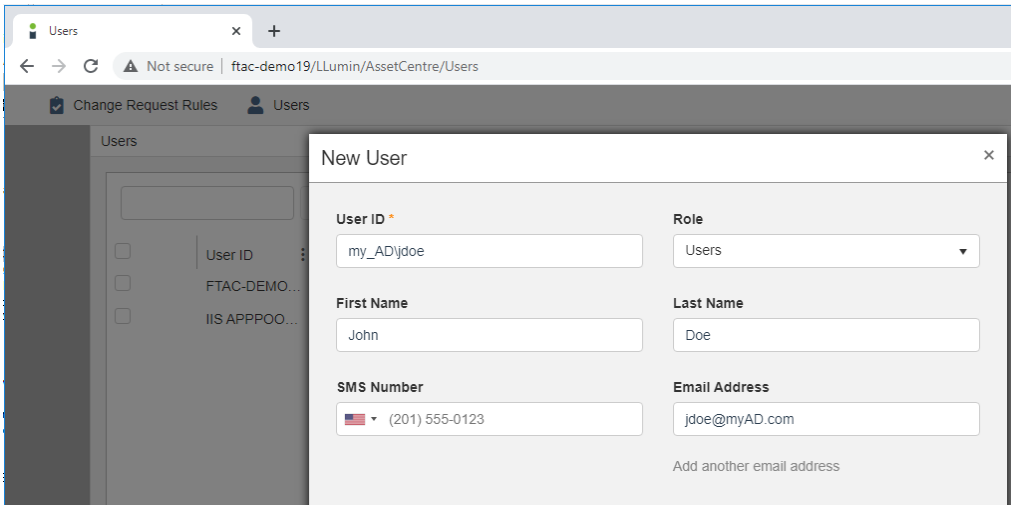
The reason that one must deny these permissions is because the system is configured to not require Archive MoC during check-in and check-out operations.

It is recommended that administrator also restrict access to a special Archive MoC permission *Unblock MoC Workflow* that can be used to terminate a workflow prior to its natural completion. To do so select, or add, the user and computer group that should have access to this permission and **allow** access. The administrator should **deny** access to *Unblock MoC Workflow* to user and user groups that should be use this function.



Add users to Archive Management of Change

To use the Archive MoC users must be added to the system. To operate properly the users added must be members of a Windows domain. By default, during installation the AD user account of the person performing the software installation is added to the system as an administrator.



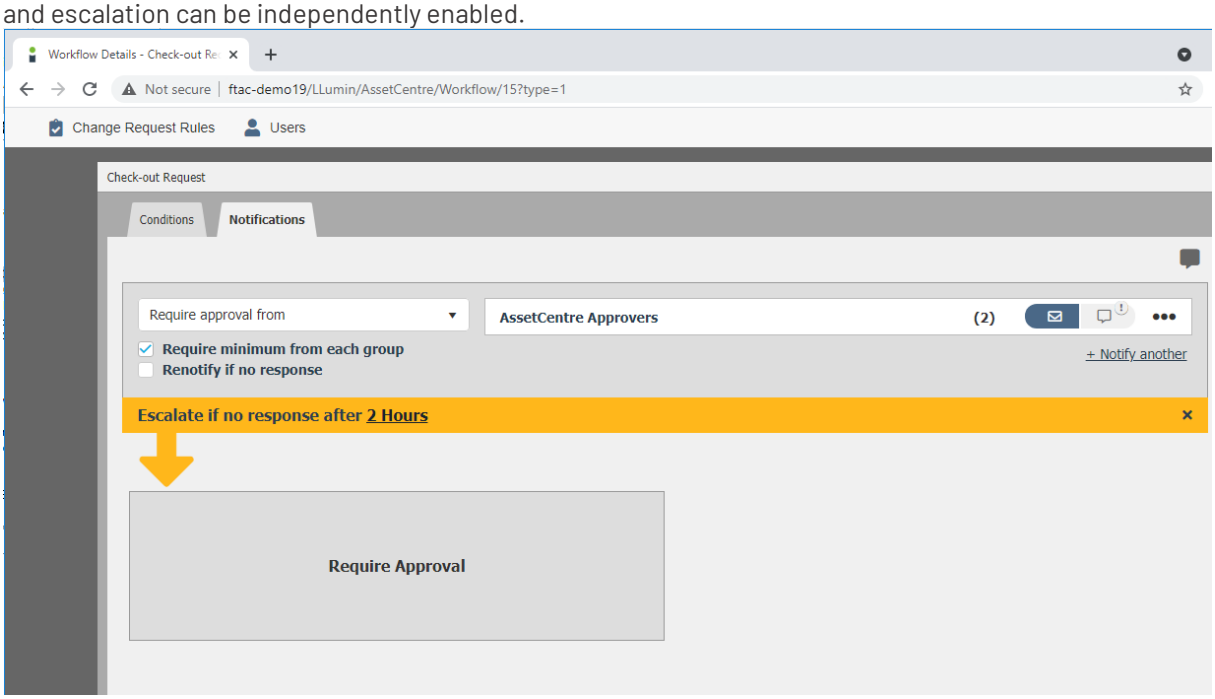
When adding users, it is necessary to add a valid email address. This enables the system to notify both the requestor (workflow initiator) and the workflow approver(s). When a workflow is started by a requestor, notifications are sent to the requestor and approver(s). The requestor notice confirms the workflow initiation. The approver's notification contains a link to a web page, hosted on the AssetCentre Server, that allows for approval or denial of the requestor's request. Once the approver(s) has taken action the requestor receives a new notice informing them of the approver(s) decision.

Once a check-out workflow is initiated the Archive file, folder, or binder (an Archive object) is locked until the workflow is approved or denied. If it is approved only the requestor has permission to perform the check-out operation. If the request is denied, the Archive object is unlocked. In some cases, it may be necessary to unlock the Archive object before the workflow can be completed. The special command *Unblock MoC Workflow* can be used for this purpose. For example, if someone initiated a workflow request that was not resolved before a weekend, it might be necessary to unblock the workflow if a change was necessary during the weekend. This would also allow a different person to initiate the request during the weekend.

The SMS option is also available for notification. It is important to note that it is not possible to access the approval portal from the SMS message.

Create approval workflows

To complete the configuration of Archive Management of Change an administrator must configure the approval workflows. The system supports separate workflows for check-out and check-in. The workflow can require approval from the first person from a group of approvers to respond, or some number of approvers, greater than one up to the total group membership, that are members of the group. The MoC system supports renotification, if no approver action takes place within a specified time, and escalation to a different approver group if no action approver action takes place within a specified time. Both renotification and escalation can be independently enabled.



The MoC system also supports a checklist workflow that requires the requestor to complete a checklist prior to initiating the workflow. This is most effectively used as part of a check-in workflow. For example, the checklist requires the requestor to confirm they have followed company's engineering change process, updated drawings, and executed peer-review of the changes.

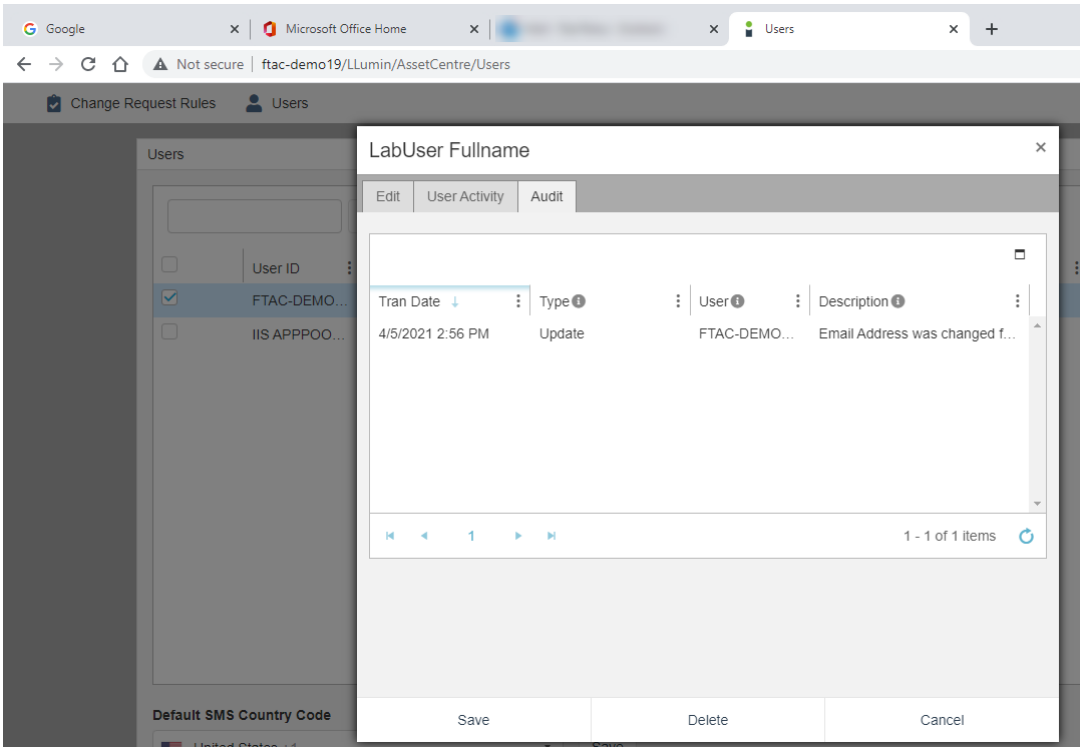
Accessing audit information from Archive Management of Change administration

User interactions with Archive MoC workflows (i.e., requesting, approving or denying) generate audit messages that are captured by the FactoryTalk® AssetCentre central database and are viewable in the AssetCentre client. While interactions with the MoC Administration interface to manage users or change a workflow are **not** logged to the AssetCentre audit trail database, these administrative actions **do** generate audit messages that are captured in the MoC database.

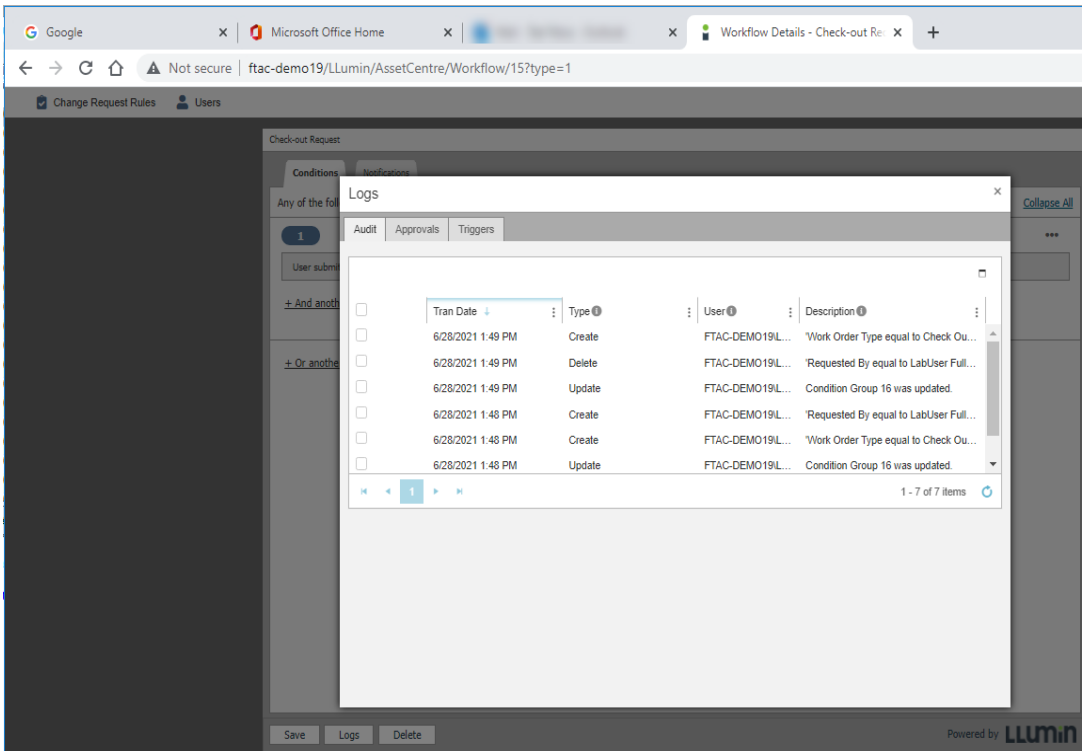
Users interested in combining the audit messages from MoC administration and normal use of the FactoryTalk® AssetCentre system can use the publicly available SQL Views to create reports that combine the data sources. The following Rockwell Automation knowledge base articles document database views that can be used for this purpose.

> FactoryTalk® AssetCentre: For information on working with Archive Management of Change website, refer to the FactoryTalk® AssetCentre Getting Results Guide.
>
> FactoryTalk® AssetCentre: For more information on FactoryTalk® AssetCentre database views, refer to the Rockwell Automation Knowledgebase Document ID: IN38723 - FactoryTalk AssetCentre Database Views Schema.
>
> FactoryTalk® AssetCentre: For more information on FactoryTalk AssetCentre Archive Management of Change 21 CFR Compliance, refer to the Rockwell Automation Knowledgebase Document ID: QA62222 - FactoryTalk AssetCentre Archive Management of Change 21 CFR Compliance.

Alternately, the MoC administration audit messages can be viewed from the MoC Administration interface. Audits for user management are captured on an individual user account basis. To view, select the user of interest and use the "View' button. The image below shows an audit captured when managing a user account.



Audits related to managing a workflow are accessed by placing the workflow rule in to edit mode, and then selecting the “Logs” button.



Configure signing during non-continuous sessions

Signing for Archive MoC approval workflows is initiated when logging on to the desktop on which the web browser is launched and when logging into the Archive MoC web page for the first time. To enforce re-signing after a non-continuous session, it is therefore important that the desktop session or web browser session is unique to the user.

In order to configure re-signing of the web browser session at each launch of the Archive MoC web page, work with your system administrator to set up the proper policies for web browser security settings.

Configure automatic backup and compare of devices

> Applies to: FactoryTalk® AssetCentre, Version 11.00 through 16.00

To ensure that the correct device configurations are operating the manufacturing system FactoryTalk® AssetCentre offers several different Disaster Recovery capabilities.

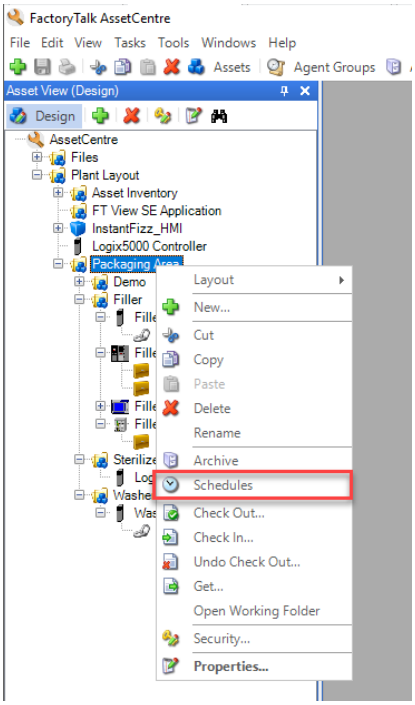
Capability	Description
Disaster Recovery for Rockwell Automation	Perform automated backup for Rockwell Automation controllers, drives, Electronic Operator Interface devices, switches, HMI application. For most Rockwell Automation devices, a detailed comparison report is available.
Disaster Recovery for Generic FTP	Perform automated backup of devices that host an FTP server (e.g., FANUC robots) It may be possible to generate detailed comparison report for some of the files retrieved via the capability
Disaster Recovery for Siemens TIA Portal (Starting with V13.00)	Perform automated backup of supported Siemens S7-1200, S7-1500, and ET200 controllers using TIA Portal programming software, with the minimum version being v15.1 and the maximum version being v19 (as of the release of FactoryTalk AssetCentre v16.00). It is possible to generate detailed comparison report(s) for some of the files retrieved via the capability

Capability	Description
Disaster Recovery for Schneider Control Expert (Starting with V15.00)	Perform automated backup of supported Schneider M340 and M580 controllers using Control Expert programming software, with the minimum version being v15.2 and the maximum version being v16.0 (as of the release of FactoryTalk AssetCentre v16.00). Note: Unity DIF or Control Expert DIF must also be installed with the Control Expert programming software. For version compatibility, please refer to BF32007 - Patch: Update controllers disaster recovery, FactoryTalk AssetCentre 15.00. It is possible to generate detailed comparison report(s) for some of the files retrieved via the capability
Disaster Recovery for Mitsubishi (Starting with V13.00)	Perform automated backup of supported Mitsubishi iQ-R and iQ-F controllers GX Works3 (minimum version v1.095Z), and Q, L, and F controllers using GX Works 2 (minimum version v1.615R). It is possible to generate detailed comparison report for some of the files retrieved via the capability
Disaster Recovery for Remote Computers	Perform automated backup of files and folder hosted on a Microsoft Windows file share. It may be possible to generate detailed comparison report for some of the files retrieved via the capability

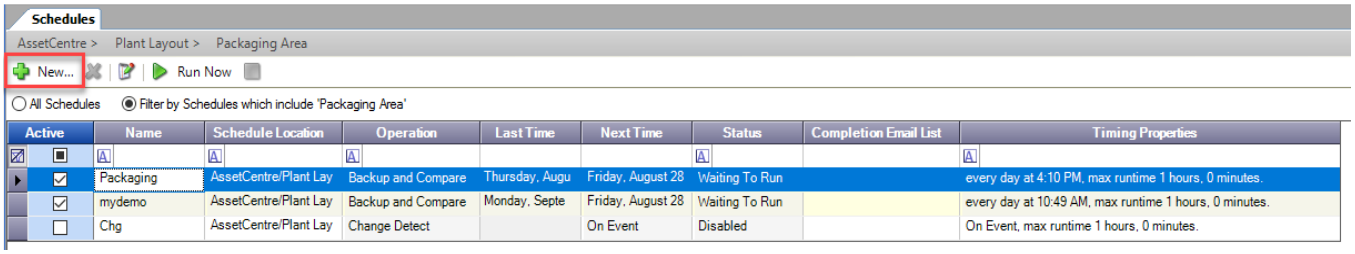
The basic operation of the capabilities is to automatically retrieve the configuration of an asset (e.g., ControlLogix controller, 3rd party device) and store the resultant artifact in the FactoryTalk® AssetCentre Archive. In some instance it is possible to automatically backup a device configuration and compare the new artifact to a 'master' version stored in the FactoryTalk® AssetCentre Archive. When using a backup and compare schedule the system can be configured to only create a new Archive version when differences are detected.
To use disaster recovery a schedule is created, to start this process launch the FactoryTalk® AssetCentre Client and enter *Design* mode. Next select the Asset Tree container that is parent of the assets upon which the schedule will operate. When generating a schedule, the system will automatically add all assets (e.g., physical devices) to the schedule. Right-click and select *Schedules.*

Considerations around use of the Custom Device Asset

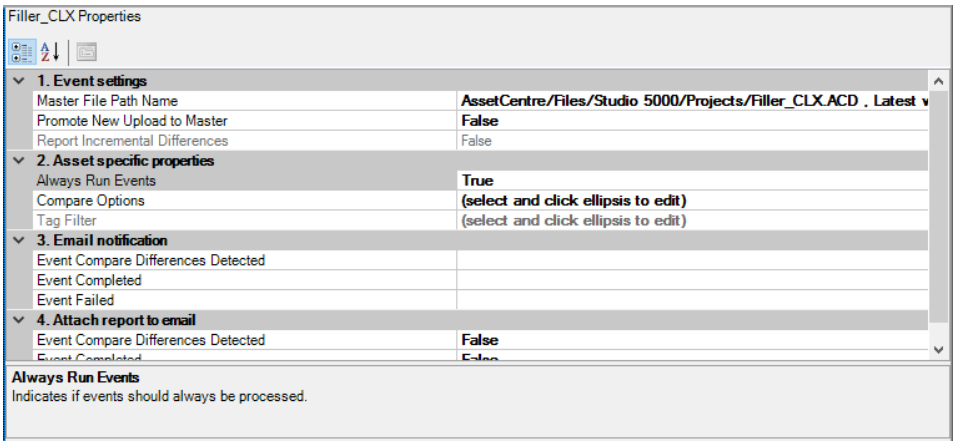
FactoryTalk® AssetCentre provides the option of a Custom Device asset that enables scheduled operations for assets that are not natively part of FactoryTalk® AssetCentre. While this option provides flexibility for custom device support, this solution relies on customer-managed scripts and third-party software interfaces that may limit system supportability or upgradability. As a result, it is recommended to use native AssetCentre device integrations.



This opens the Schedule View in FactoryTalk® AssetCentre Client. This view will show all schedules that contain the container selected above. Next, select New to launch the schedule creation workflow. The wizard allows a choice of schedule type, Backup or Backup&Compare, and the frequency that the schedule is executed.



Finally, after the new schedule is instantiated the operation of each asset can be customized, if desired. The asset type being operated upon determines what customization options are presented.



Running AssetCentre® Agent as an Application

While it is standard to run the agent as a service, the agent **must run as an application** in the case of 3rd party devices. To prevent unintended access to the desktop, agent computer can be auto-locked through configuration of a password-protected screen saver and through setup of Windows ARSO. Refer to section *Configure FactoryTalk® AssetCentre computers to automatically lock after a period of inactivity*.

Leverage AssetCentre for asset monitoring and lifecycle management

FactoryTalk® AssetCentre provides centralized monitoring of assets, including change detection for security configurations, firmware revision status, and lifecycle status. To help manufacturing systems remain secure, supportable, and within validated state, setup AssetCentre to track asset security configurations and identify End of Life assets.

Setup AssetCentre Asset Lifecycle monitoring

> Applies to: FactoryTalk® AssetCentre, Versions 11.00 through 16.00

Asset Lifecycle monitoring provides the lifecycle information for Rockwell Automation hardware devices in the system. It shows the lifecycle status in the form of a list that allows users to manage the hardware life cycle and manage which device needs to be upgraded or replaced.

> FactoryTalk® AssetCentre: For more information on setting up AssetCentre Asset lifecycle, refer to the Rockwell Automation Knowledgebase Document ID: QA40307 - FAQ: FactoryTalk AssetCentre Assets Lifecycle.
>
> FactoryTalk® AssetCentre: For more information on viewing Asset Lifecycle through the web client, refer to the Rockwell Automation Knowledgebase Document ID: QA75306 - FactoryTalk AssetCentre Web Client Asset Lifecycle FAQ.

Monitor security-related configurations

> Applies to: FactoryTalk® AssetCentre, Version 16.00; Studio 5000 Logix Designer V31.00 through 38.00

Security Compliance enables organizations to assess and verify the security configuration of Logix 5000 controllers that are configured within the FactoryTalk AssetCentre asset tree. It compares the discovered controller configuration against customer-defined or vendor-recommended security rules, helping teams identify non-compliant settings and validate that critical security requirements are being enforced.

> The Security Compliance feature requires a **Security Compliance activation license** on the **FactoryTalk AssetCentre server**.

Security Compliance operates by running scheduled Security Posture Checks against supported Logix 5000 controllers in the asset tree. During each scan, the system communicates directly with the controller to collect configuration information and evaluate settings such as controller mode, key switch position, firmware revision, security configuration, and safety signature state against the applicable compliance rules.

This feature introduces a **Security Posture Check** schedule type and a web-based dashboard for viewing compliance results. Both schedule configuration and dashboard management are available exclusively through the FactoryTalk AssetCentre Web Client.

The dashboard displays the results of the most recent Security Posture Check. Each scheduled execution generates a report that is recorded in the FactoryTalk AssetCentre event log and can be downloaded as an attachment. Reports are available in two formats:

- **Summary Report** – Groups exceptions by category for a high-level compliance overview.
- **Detailed Report** – Lists individual rule violations, providing granular visibility into non-compliant settings.

The Security Posture Check results for individual controllers can be viewed using either the Card or Table views. Each view includes a properties panel that compares the controller's actual configuration against the expected configuration defined by the applicable compliance rules.

Compliance rules are managed through the **Manage Security Posture Check** editor, located under the **Security Compliance** section of the Web Client. The editor includes a *Default* rule that applies broadly across supported controllers, as well as additional rules that can be scoped to specific controller bulletins or product families. Each rule contains identifying metadata and a collection of compliance criteria organized into four categories:

- **General**
- **Firmware**
- **Security**

- **Safety**

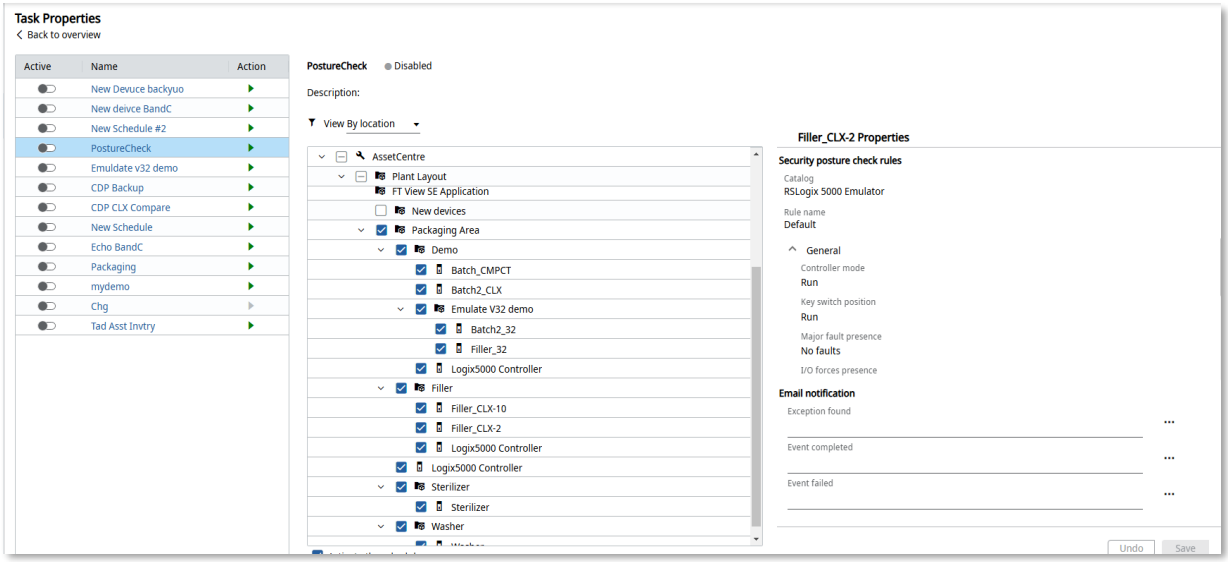
This flexible rule framework enables organizations to tailor compliance requirements to their security standards while maintaining visibility into controller security posture across their automation environment.

The following Security Posture Check **rule-level settings** define the desired security and configuration state for Logix controllers. These settings are used to assess controller compliance against established standards and identify deviations from the expected posture:

Setting	What You Set or Settings Options	Settings that may (partially) apply to 21 CFR part 11	Values/Constraints
Rule-Level Settings			
Rule Name	Identifies the Rule	N/A	Required; the *Default* role cannot be deleted.
Controller Type	Target controller family (or families) the rule applies to	N/A	Drop-down selection of various ControlLogix, CompactLogix, and FactoryTalk Logix Echo controller families.
Product String	Narrows the rule to specific catalog number(s)	N/A	Exact match (e.g., **1756-L84ES**) or 'fuzzy' match with **wildcard *** (e.g., **1756-L8***); quotation marks "" raise match priority. Each device matches only one active rule; the highest-priority match wins, and the *Default* rule is the lowest priority.
General group			
Controller Mode	Options are **Skip** or **Run** (Run Mode or Remote Run Mode)	Configuration control that protects data integrity of the source (§11.10(a) intent, (e), (h))	Default value is **Run**
Key Switch position	Options are **Skip**, **Remote**, and **Run**	Configuration control that protects data integrity of the source (§11.10(a) intent, (e), (h))	Default value is **Run**
Major Fault presence	Options are **Skip** or **Not Present** (no faults)	N/A	Default value is **Not Present**
I/O Forces presence	Options are **Skip** or **Not Present** (I/O forces disabled)	N/A	Default value is **Skip**
I/O Forces state	Options are **Skio** or **Inactive** (I/O Forces inactive)	N/A	Default value is **Skip**
SFC Forces presence	Options are **Skip** or **Not Present** (SFC forces disabled)	N/A	Default value is **Skip**
SFC Forces state	Options are **Skio** or **Inactive** (SFC Forces inactive)	N/A	Default value is **Skip**

Setting	What You Set or Settings Options	Settings that may (partially) apply to 21 CFR part 11	Values/Constraints
Firmware Group			
Major Version	Options are Operator '**>=**' or '**==**' plus a version number	Version control of the system that originates the data (§11.10(a) intent)	Example: **>= 36** accepts *v36 or later*; **== 36** accepts *only v36*
Minor Version	Options are Operator '**>=**' or '**==**' plus a version number	Version control of the system that originates the data (§11.10(a) intent)	Combined with major, e.g., **>= 36** and **>= 11** accepts *36.11 or later*; **== 36** and **== 11** accepts *only 36.11*
Security Group			
Change to detect bit mask	Checkbox; when selected, enter a bit mask value	Detecting unauthorized change; supports record integrity (§11.10(e), (h))	Default value is for the checkbox to be unchecked; default mask **16#FFFF_FFFF_FFFF_FFFF** (all Changes-to-Detect items selected)
Security Authority state	Options: **Skip · No security · Secured, but not bound to a security authority · Secured and bound to a Primary Security Authority** (enter FT Directory server name) · **Secured and bound to a Primary and Secondary Security Authority** (enter primary and secondary FT Directory server names)	Limiting access to authorized individuals; authority checks (§11.10(d), (g))	Default value is **Secured, but not bound to a security authority**
Controller Web Pages	Options: **Skip · Enabled · Disabled**	Closing off uncontrolled access paths (§11.10(d), (g))	Default value is **Disabled**
Security Group – only applicable for safety controllers			
Safety Application State	Options: **Skip · Locked** (safety lock enabled)	Configuration control that protects data integrity of the source (§11.10(a) intent, (e), (h))	Default value is **Skip**
Safety Signature	Options: **Skip · Applied** (safety signature applied)	Configuration control that protects data integrity of the source (§11.10(a) intent, (e), (h))	Default value is **Skip**
Protect Signature in Run Mode	Options: **Skip · Signature deletion inhibited**	Configuration control that protects data integrity of the source (§11.10(a) intent, (e), (h))	Default value is **Skip**
Safety Task Major Fault Presence	Options: **Skip · Not Present** (no faults)		Default value is **Not Present**

To fully configure security posture check, users must both create a **Security Compliance – Security Posture Check** schedule type through the FactoryTalk AssetCentre web client AND configure the rules shown above in the *Security Compliance* section in the web client.



> For more information on setting up security posture check schedules, refer to the FactoryTalk® AssetCentre Getting Results Guide.

Configure Time Synchronization in a FactoryTalk® environment

> Applies to: FactoryTalk® AssetCentre, Version 11.00 through 16.00

FactoryTalk® leverages the Windows Time service (W32tm.exe) on the underlying Windows operating system to synchronize its software components and confirm the security of Active Directory authentication. All servers in the FactoryTalk® environment, including FactoryTalk® AssetCentre servers, clients, and databases, can be synchronized to excellent reliability authoritative time server in Coordinated Universal Time (UTC) to enable accurate time stamps on alarms and diagnostics logs. In a domain, the time synchronization source is provided by the domain controller that authenticates the FactoryTalk® AssetCentre computer.

> FactoryTalk® AssetCentre: For more information on the importance of time synchronization for FactoryTalk® AssetCentre, refer to the Rockwell Automation Knowledgebase Document ID: QA6748 - FactoryTalk AssetCentre: Time Synchronization.

Setup FactoryTalk® Database Management

Effective FactoryTalk® AssetCentre database management is essential for maintaining system performance, reliability, and long-term data accessibility. The AssetCentre database serves as the central repository for audit records, event logs, asset inventory information, lifecycle data, version history, and other records that support compliance activities. As the volume of stored information grows over time, routine database maintenance is highly recommended.

To help facilitate database maintenance, AssetCentre provides schedules for archive and log clean up and tools for database shrinking to help with database maintenance.

It is important to note that database management should also be aligned with the organization's data retention and business continuity requirements. Consideration should be given to coordinating database maintenance activities around database backup schedules via IT-managed backup and recovery processes to ensure AssetCentre databases are protected and retained for the organization's defined retention period.

> FactoryTalk® AssetCentre: For more information on Database Management best practices, refer to the Rockwell Automation Knowledgebase Document ID: QA38697 - FactoryTalk AssetCentre: Database Management.
>
> FactoryTalk® AssetCentre: For more information on Database Management Frequently Asked Questions, refer to the Rockwell Automation Knowledgebase Document ID: QA52221 - FactoryTalk AssetCentre Database Management FAQs.

Notification for database limitations

> Applies to: FactoryTalk® AssetCentre, Version 11.00 through 16.00

As FactoryTalk® AssetCentre contains electronic records that are key for compliance activities, it is highly recommended to have a method for notifying the administrator when the database is approaching limits that may impact database performance and continued record collection.

FactoryTalk® AssetCentre provides methods for notifying the administrator when the FactoryTalk® AssetCentre database is approaching maximum size, warning levels, maximum number of versions per archive asset, and more.

> FactoryTalk® AssetCentre: For information on configuring FactoryTalk® AssetCentre database limitation options, refer to the FactoryTalk® AssetCentre Getting Results Guide.

Automated schedules for log clean up via web client

> Applies to: FactoryTalk® AssetCentre, Version 13.00 through 16.00

Through the course of normal operation, the Audit and Event logs of the FactoryTalk® AssetCentre system can grow quite large. As a direct consequence, the MSSQL database size will also expand. Due to these considerations, it is possible for an administrator of the system to remove older log messages.

The user then uses the Log Cleanup Wizard to manage the log files. To do this, users identify a group of logs (Event, Audit, or Diagnostic and Health) to remove from the system's database. The user inputs the type of log files to remove, and the date up to which they should be removed. For example, entering a date of 10/28/2007 will remove all log files up to and including that day. Once the utility has been run, the logs will be removed from the database.

As these electronic records are key for compliance activities, it is imperative to have a backup and disaster recovery process setup in conjunction with the configuration of the AssetCentre database clean up. Work with your IT administrator to set up the appropriate database maintenance processes, such as database backups, prior to configuration of AssetCentre database management tools; during backup and clean up of the FactoryTalk AssetCentre system, a maintenance window should be planned and user access to the system should be limited.

To coordinate database clean up activities, it is recommended to perform manual database clean up from the FactoryTalk AssetCentre client after confirmation of proper database backup and retention.

> FactoryTalk® AssetCentre: For more information on properly backing up and restoring the FactoryTalk® AssetCentre Microsoft SQL Server, refer to the FactoryTalk AssetCentre Installation Guide.
>
> FactoryTalk® AssetCentre: For more information on the Log Cleanup Utility, refer to the Rockwell Automation Knowledgebase Document ID: QA10791 - FactoryTalk AssetCentre Log Clean-up Utility.

Automated schedules for archive clean up via web client

> Applies to: FactoryTalk® AssetCentre, Version 15.00 through 16.00

The Archive Cleanup Wizard is used to remove versions of archived files from the database, thereby clearing space. Removed versions are removed from the database, but the version number and associated notes can be retained in the archive for the purposes of record-keeping. The Archive Cleanup Wizard can be run manually from the FactoryTalk AssetCentre Client, or the archive cleanup can be scripted to run via command.

As these electronic records are key for compliance activities, it is imperative to have a backup and disaster recovery process setup in conjunction with the configuration of the AssetCentre database clean up. Work with your IT administrator to set up the appropriate database maintenance processes, such as database backups, prior to configuration of AssetCentre database management tools; during backup and clean up of the FactoryTalk AssetCentre system, a maintenance window should be planned and user access to the system should be limited.

To coordinate database clean up activities, it is recommended to perform manual database clean up from the FactoryTalk AssetCentre client after confirmation of proper database backup and retention.

> FactoryTalk® AssetCentre: For more information on properly backing up and restoring the FactoryTalk® AssetCentre Microsoft SQL Server, refer to the FactoryTalk AssetCentre Installation Guide.
>
> FactoryTalk® AssetCentre: For more information on the Archive Cleanup Wizard, refer to the Rockwell Automation Knowledgebase Document ID: QA41682 - FactoryTalk AssetCentre Archive Cleanup Wizard.

Highlights in Version History

The following table provides an overview of notable changes with each version of FactoryTalk® AssetCentre, specific to features relevant to US FDA 21 CFR Part 11:

Version		Highlights
16.00	Security compliance capability	Version 16.00 enables monitoring of Logix system configuration to provide monitoring of assets for adherence to desired standards, such as for security or data integrity.
	Air-gapped lifecycle updates	Version 16.00 enables view of asset lifecycle information in networks that are isolated from the internet for more flexible lifecycle management.
	Expanded database maintenance	Version 16.00 expands functions of the web client to include database maintenance of audit, events, diagnostics, and health information for better system management, including index defragmentation and database shrink operations.
15.00	Added archive management	Version 15.00 adds functions of the web client to include database maintenance of archives for better system performance and management.
	Cross FactoryTalk Directory operation	Version 15.00 enables forwarding of FactoryTalk® Diagnostics from remote systems to a central FactoryTalk® AssetCentre system, enabling more integrated audit and asset management for systems not contained within the same FactoryTalk® Directory.
13.00	Expanded authentication capabilities	Starting with FactoryTalk® Services Platform version 6.40, compatible with FactoryTalk® AssetCentre version 13.00, various enhanced authentication methods are supported via service integration to Microsoft Entra ID, or Azure Active Directory (AD), and OpenID Connect identity providers running on top of on-premises Active Directory. This enables a wide variety of multi-factor authentication options including: one-time phone code, biometrics, radio frequency identification (RFID) cards, and Nymi bands.
	Database maintenance	Version 13.00 enables the web client to support database monitoring and management to improve lifecycle management of event, audit, and diagnostic and health log data, archive size.
12.00	Enhanced security	Version 12.00 of FactoryTalk® AssetCentre meets CIS benchmark.
11.00	Archive Management of Change	Version 11.00 includes Archive Management of Change to provide an additional layer of over-sight and control to the Archive, by adding an electronic workflow that augments the existing security available for the Archive capability. Workflows can be enabled for both the check-out and check-in action separately via two new security policies. Workflows support single or multiple approvers with support for escalation when no action is taken.
	Database security enhancement	Version 11.00 includes use of virtual service accounts (VSA), group Managed Services Accounts (gMSA), or Managed Service Accounts (MSA) during installation of FactoryTalk® AssetCentre, allowing

About Rockwell Automation

Rockwell Automation, Inc. (NYSE: ROK), the world's largest company dedicated to industrial automation and information, makes its customers more productive and the world more sustainable. Headquartered in Milwaukee, Wis., Rockwell Automation employs about 20,000 people serving customers in more than 80 countries.

Ongoing 21 CFR Part 11 Product Review

Rockwell Automation regularly reviews our software products in relation to 21 CFR Part 11 regulation. As industry interpretations of the regulation evolve, Rockwell Automation continues to provide updated guidance on compliant implementation of our Rockwell solutions, in keeping with compliance practices found across the industry. In general, the software products we have evaluated have been judged as either "compliant" or "can be made compliant". Many of our products' standard features and complementary technologies support 21 CFR Part 11 when implemented properly.

Publishing application notes

This document includes detailed recommendations for developing FactoryTalk® AssetCentre projects that comply with the U S government's 21 CFR Part 11 regulation. For additional guidance on other Rockwell Automation products and solutions, refer to the Rockwell Automation Knowledgebase Document ID: QA75467 - 21 CFR Part 11 guidelines for Rockwell Automation products.

Connect with us.

rockwellautomation.com — expanding **human possibility**®

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Rockwell Automation is a trademark of Rockwell Automation, Inc. Trademarks not belonging to Rockwell Automation are property of their respective companies.

Publication FTALK-WP023B-EN-P — September 2026
Copyright© 2026 Rockwell Automation, Inc. All rights reserved. Printed in USA.