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

Versions 11.00.00 through 15.00.00

Complying with 21 CFR Part 11: Electronic Records & Signatures

Table of contents

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® View Site Edition (SE) application can address the technical requirements of Part 11. Each manufacturer has a set of unique needs and interpretations of Part 11; Rockwell Automation recognizes the demands of life sciences manufacturers and has created a solution that is flexible enough to address potential differences. The objective is to help life sciences manufacturers quickly and cost-effectively comply with 21 CFR Part 11.

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 features or repeatable actions 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 on 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® View SE in a Rockwell Automation software system

FactoryTalk® View SE and the FactoryTalk® Services Platform

FactoryTalk® View SE uses the 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.

A FactoryTalk®-enabled system provides data integrity throughout the data lifecycle, from the point of generation to data storage and visualization. By having a distributed network of FactoryTalk® Services Platform-based applications, data can be time-stamped, secured, and stored via centrally recognized servers. Redundancy and buffering also exist within several FactoryTalk® software components to deliver completeness of data records as they are being collected.

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® View SE and all other FactoryTalk-enabled products to a centralized, common data store.

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 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.

How PlantPAx® and the Library of Process Objects fits in

PlantPAx® provides a modern approach to distributed control, incorporating FactoryTalk® View SE and other FactoryTalk® products into a system-wide, factory-tested architecture, improving the system reliability and mitigating risk. The system shares common technology (Integrated Architecture® system) with all other automation disciplines in the plant. This approach creates seamless and more reliable information flow that is a key for modern regulated industries and enabling a Connected Enterprise®.

As part of PlantPAx®, the Rockwell Automation Library of Process Objects contains standardized visualization files to be used in FactoryTalk® View SE with associated controller instructions. This library creates a scalable platform that establishes consistency and ease of use by providing controller code, visualization faceplates, analytics and tools for bulk configuration. Use of the library provides standardized, repeatable code and allows for the system to grow over time. Maintenance of the library, including internal testing, is performed by Rockwell Automation following internal Rockwell Automation Quality Management System (QMS) processes to preserve the quality that was built into the library. By having a productized solution, risk and probability of impact associated with the solution and subsequent changes can be reduced, and as a result, the user testing required for each change and function can be reduced.

How FactoryTalk® AssetCentre fits in

FactoryTalk® AssetCentre provides a central set of tools securing access to the control system, tracking actions of users within the control system, and managing the plant floor configuration files through manual and automated means. More specifically, FactoryTalk® AssetCentre collects and displays information regarding user and system actions performed from any piece of FactoryTalk® software (such as FactoryTalk® View SE) throughout the control system, as required by regulations such as 21 CFR Part 11. FactoryTalk® AssetCentre also provides a means for backup and disaster recovery of the FactoryTalk® Directory and FactoryTalk® View SE application to enable business continuity.

The intent of this document is to describe how to use FactoryTalk® View SE to help secure and log operator actions, track alarms, and log other operational data. FactoryTalk® AssetCentre is not discussed in detail, but is referenced where necessary.

How FactoryTalk® ViewPoint fits in

FactoryTalk® ViewPoint provides a remote web browser-based connection to a FactoryTalk® View SE application; it is available for both FactoryTalk® View SE distributed (server/client) and standalone (station) applications. Displays from FactoryTalk® View SE are published to FactoryTalk® ViewPoint, which maintains a user security configuration separate from runtime security in FactoryTalk® View SE. To improve security management, it is recommended to leverage Windows-linked user groups, since membership is managed in the Windows domain. For most applications that must comply with 21 CFR Part 11 it is recommended that data changes via FactoryTalk® ViewPoint are disabled; FactoryTalk® ViewPoint can be configured with view-only access in a 21 CFR Part 11 regulated environment.

How ThinManager® fits in

ThinManager® software manages client devices and delivers content to them for plant floor visualization. It provides control, secures HMI applications and hardware, customizes operator experience, and simplifies management and maintenance.

In operations, ThinManager® software can display multiple FactoryTalk® View SE applications at the operator terminal on the same monitor or multiple monitors. It centralizes the terminal configuration within the ThinManager® server. During replacement of HMI hardware, minimal configuration of the ThinManager-enabled hardware is required, allowing for improved backup and disaster recovery of the system.

ThinManager® software can also help secure your HMI applications through use of the ThinManager® "E Signature" feature for electronic signing and multiple modalities for user authentication such as:

- Username and password
- RFID card
- Smartcard
- Fingerprint
- PIN

ThinManager® software can also automatically and periodically rotate passwords for any user account on a domain in which an alternate authentication method such as an RFID card or fingerprint is used in place of a password.

In compliance with 21 CFR Part 11, a non-interactive, or view-only, shadowing session of the operator terminal can be seen from the ThinManager® server for effective runtime troubleshooting, while maintaining data integrity of the logged-in operator.

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 guideline 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® View SE comply with the technical aspect of Part 11. Each customer's security and standard operating procedures (SOPs) for supporting this regulation are unique. FactoryTalk® View SE 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® View SE applies. Subsequent sections provide details on the implementation of FactoryTalk® View SE features in a 21 CFR Part 11 compliant system.

Table 1: Subpart B – electronic records

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:

Section	Requirements	FactoryTalk® View SE applies?	Application notes
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.
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 can be stored in the FactoryTalk® AssetCentre SQL Database or a SQL-compliant Open Database Connectivity (ODBC) database. See the following sections for guidance: • *Log FactoryTalk® Alarms and Events to a central ODBC database* • *Log all FactoryTalk® View SE activity to a central FactoryTalk® AssetCentre or ODBC database* FactoryTalk® View SE provides tools to read locally buffered records, but once they have been sent to the FactoryTalk® AssetCentre or ODBC database and transferred from the local buffer, 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	FactoryTalk® View SE applies?	Application notes
c)	Protection of records to enable their accurate and ready retrieval throughout the record retention period.	■ Yes ☐ No ☐ N/A	All records can be stored in the FactoryTalk® AssetCentre SQL Database or a SQL-compliant ODBC database and are available for viewing, printing, and exporting throughout the record retention period. See the following sections for guidance: • *Log FactoryTalk® Alarms and Events to a central ODBC database* • *Log all FactoryTalk® View SE activity to a central FactoryTalk® AssetCentre or ODBC database* Precautionary measures such as periodic backup of the database are procedures that customers can incorporate into their SOP. Access to these databases can be controlled to maintain data integrity.
d)	Limiting system access to authorized individuals.	■ Yes ☐ No ☐ N/A	Limiting FactoryTalk® View SE system access includes configuring FactoryTalk® Security to use Microsoft security. See the following sections for guidance: • *Take advantage of operating system security and domains* • *Configure FactoryTalk® View SE user accounts to use Microsoft Windows security and more* It also includes using other application security measures, such as FactoryTalk® View SE runtime security and FactoryTalk® View SE DeskLock, which help prevent unauthorized access to data files or the operating system. See the following sections for guidance: • *Take advantage of the FactoryTalk® View SE architecture* • *Manage FactoryTalk® View SE runtime security for users, user groups, and computers* • *Configure FactoryTalk® View SE clients to automatically sign out after a period of inactivity* • *Prohibit access to FactoryTalk® View Studio, other software programs, and Windows Help* • *Configure a startup of the client terminal in a FactoryTalk® View SE environment* • *Set up the DeskLock feature* • *Securing FactoryTalk® View SE Client terminals* *Additional security measures, such as limiting access to the operating system desktop, can be used to further restrict access. See the following sections for guidance:* • *Securing physical and logical access to computer hardware*

Section	Requirements	FactoryTalk® View SE 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® View SE provides functionality to manage secure, computer-generated, time-stamped audit trails associated with operator actions performed in the production system. See the following sections for guidance: • *Log all FactoryTalk® View SE activity to a central FactoryTalk® AssetCentre or ODBC database* • *Configuring time synchronization in FactoryTalk® View SE* FactoryTalk® View SE also provides electronic signature capabilities. Each entry in the FactoryTalk® View SE activity log is identified with: • 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 • comment entered by the operator. See the following section for guidance: • *Set up reverification of operator identity, or supervisor signoff*
f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	■ Yes ☐ No ☐ N/A	Operational steps and sequencing are a combination of controller logic and FactoryTalk® View SE. FactoryTalk® View SE supports both screen-level and tag-level security. An application can be developed to support user-initiated operational checks, which require screen security. See the following sections for guidance: • *Set up reverification of operator identity, or supervisor signoff*
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® View SE can use a combination of Microsoft Windows domain security and FactoryTalk® View SE security. See the following sections for guidance: • *Take advantage of operating system security and domains* • *Configure FactoryTalk® View SE user accounts to use Microsoft Windows security and more* • *Set up reverification of operator identity, or supervisor signoff* Customers can implement policies and administrative procedures to define authorized access to the system.

Section	Requirements	FactoryTalk® View SE applies?	Application notes

h)	Use of device (for example, terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	■ Yes ☐ No ☐ N/A	FactoryTalk® View SE uses functions such as sign in and password to validate the source of data input. See the following sections for guidance: • *Set up reverification of operator identity, or supervisor signoff* Location-specific security settings can enforce 'line of sight' by allowing certain operations only from designated terminals that are within visual range of machinery. See the following sections for guidance: • *Manage FactoryTalk® View SE runtime security for users, user groups, and computers*
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® View SE helps support this requirement by validating that only users with appropriate security rights are granted access to the system.
j)	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, to deter record and signature falsification.	☐ Yes ☐ No ■ N/A	Customers can 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:		A comprehensive system can be implemented using FactoryTalk® software and services. FactoryTalk® View SE 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® View SE 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			
Section	**Requirements**	**FactoryTalk® View SE applies?**	**Application notes**
a)	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® View SE requires an appropriate sign in and password regardless of whether customers choose to implement a closed or an open system.
11.50 Signature manifestations			
a)	Signed electronic records shall contain information associated with the signing that clearly indicates all following:		
1.	The printed name of the signer;	■ Yes ☐ No ☐ N/A	With user credentials properly configured in the system, FactoryTalk® View SE 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® View SE 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	The FactoryTalk® View SE electronic signature feature can be configured to display and record the meaning of the signature. It also allows for separate performer and approval signatures, and for comments to be added regarding the meaning of the signature.
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, 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 third-party tool.

11.70 Signature/record linking			
Section	**Requirements**	**FactoryTalk® View SE applies?**	**Application notes**
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	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 or SQL-compliant ODBC database can be protected by a username and password, thus helping to help prevent information from being altered.

Table 2: Subpart C – electronic signatures

11.100 General requirements			
Section	**Requirements**	**FactoryTalk® View SE applies?**	**Application notes**
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® View SE user accounts to use Microsoft 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 can include the verification of the identity of an individual before sanctioning an individual's electronic signature. Once a user has been sanctioned and a unique account with password has been created in the FactoryTalk® View SE system, the user is required to enter his/her sign in and password to access FactoryTalk® View SE. This process validates the identity of the user to FactoryTalk® View SE.
c)	Persons using electronic signatures shall, before 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 to recognize 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	FactoryTalk® View SE 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 on biometrics shall:		
1.	Employ at least two distinct identification components such as an identification code and password.	■ Yes ☐ No ☐ N/A	FactoryTalk® View SE 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 one, 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® View SE requires the complete user identification — unique sign in ID and password — in the initial sign in of the application. When using the FactoryTalk® View SE electronic signature feature, both the user signs in ID and password are required to perform an action. If the user logs out of FactoryTalk® View SE and again requires access, the user must reenter the sign in ID and password.
1.b.	When an individual executes one or more signings not performed during one, continuous period of controlled system access, each signing shall be executed using all 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® View SE clients. See the following sections for guidance: • *Configure FactoryTalk® View SE clients to automatically sign out after a period of inactivity* FactoryTalk® View SE can support the use of all electronic signature components where required and as mandated in the customer's SOP.
2.	Be used only by their genuine owners; and	☐ Yes ☐ No ■ N/A	The customer is responsible for confirming 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 can implement appropriate procedures to handle situations that require an electronic signature by anyone other than its genuine owner.

b)	Electronic signatures based on biometrics shall be designed to provide confidence that they cannot be used by anyone other than their genuine owners.	■ Yes ☐ No ☐ N/A	FactoryTalk® View SE 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 on use of identification codes in combination with passwords shall employ controls to provide confidence that their security and integrity. Such controls shall include:			
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® View SE 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® View SE user accounts to use Microsoft Windows security and more*
b)	Confirming that identification code and password issuances are periodically checked, recalled, or revised (for example, to cover such events as password aging).	■ Yes ☐ No ☐ N/A	FactoryTalk® View SE 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 n 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.

Section	Requirements	FactoryTalk® View SE applies?	Application notes
d)	Use of transaction safeguards to help 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 unit, and, as appropriate, to organizational management.	■ Yes ☐ No ☐ N/A	FactoryTalk® View SE 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 sign in attempts an account is suspended. See the following sections for guidance: • *Take advantage of operating system security and domains* • *Configure FactoryTalk® View SE user accounts to use Microsoft Windows security and more* FactoryTalk® View SE also provides the ability to use code for custom scripting related to security. See the following sections for guidance: • *Use of Visual Basic for Application code and Scripts in FactoryTalk® View SE*
e)	Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to help confirm that they function properly and have been altered in an unauthorized manner.	☐ Yes ☐ No ■ N/A	The customer's management procedures can include proof test and/or validation of any devices that can risk the integrity of a user's identification.

Guidance for Applying FactoryTalk® View SE in a 21 CFR Part 11 controlled environment

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

- Securing physical and logical access to computer hardware
- Take advantage of operating system security and domains
- Take advantage of the FactoryTalk® View SE architecture
- Configure FactoryTalk® View SE user accounts to use Microsoft Windows security and more
- Manage FactoryTalk® View SE runtime security for users, user groups, and computers
- Configure FactoryTalk® View SE clients to automatically sign out after a period of inactivity
- Prohibit access to FactoryTalk® View Studio, other software programs, and Windows Help
- Use Windows account password aging and management
- Configure startup of the client terminal in a FactoryTalk® View SE environment
- Set up the DeskLock feature
- Securing FactoryTalk® View SE Client terminals
- Log FactoryTalk® Alarms and Events to a central ODBC database
- Log all FactoryTalk® View SE activity to a central FactoryTalk® AssetCentre or ODBC database
- Set up reverification of operator identity, or supervisor signoff
- Use version control software
- Configuring time synchronization in a FactoryTalk® View SE environment
- Use of Visual Basic for Application code and Scripts in FactoryTalk® View SE

Securing physical and logical access to computer hardware

> Applies to: FactoryTalk® View SE, Versions 11.00.00 through 15.00.00; ThinManager®, Versions 11.00.00 through 14.00.00

It is essential to limit operator access to the hardware running Windows operating systems, databases, and FactoryTalk® View SE. In general, an operator's only access to the computer can be via the keyboard, mouse, or touch screen. An operator with access to the power switch and bootable media could have direct access to the underlying file system and could potentially circumvent many of the security measures described in this document. Put measures in place to limit operator access and to help protect your hardware systems, such as through use of lockable control panels or more secure server enclosures or rooms, and through deployed architectures, such as through use of ThinManager® or a distributed FactoryTalk® View SE application.

Logically restrict access for removable storage

For systems using ThinManager® software, USB drives are blocked by the default terminal configuration. The only allowed USB devices on a ThinManager® managed terminal are a keyboard and mouse. All other devices require additional configuration by an administrator to be used on the terminal.

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'.

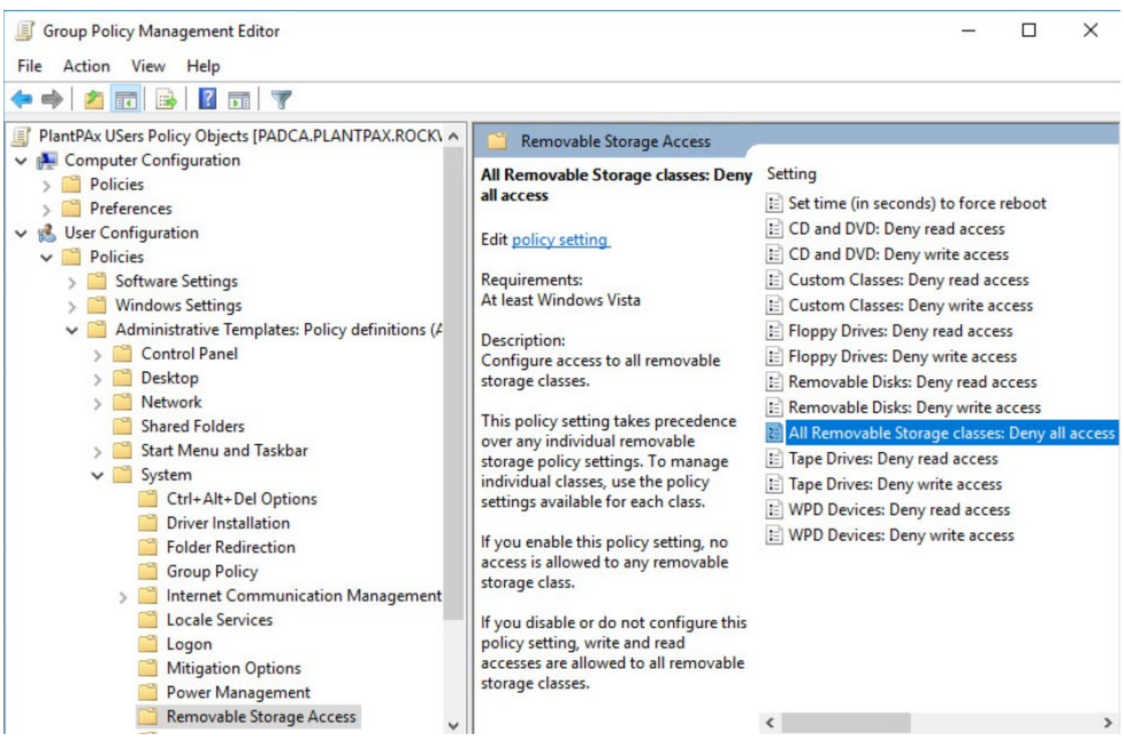

FIG 1. Configuration of policy for removable storage.

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'.

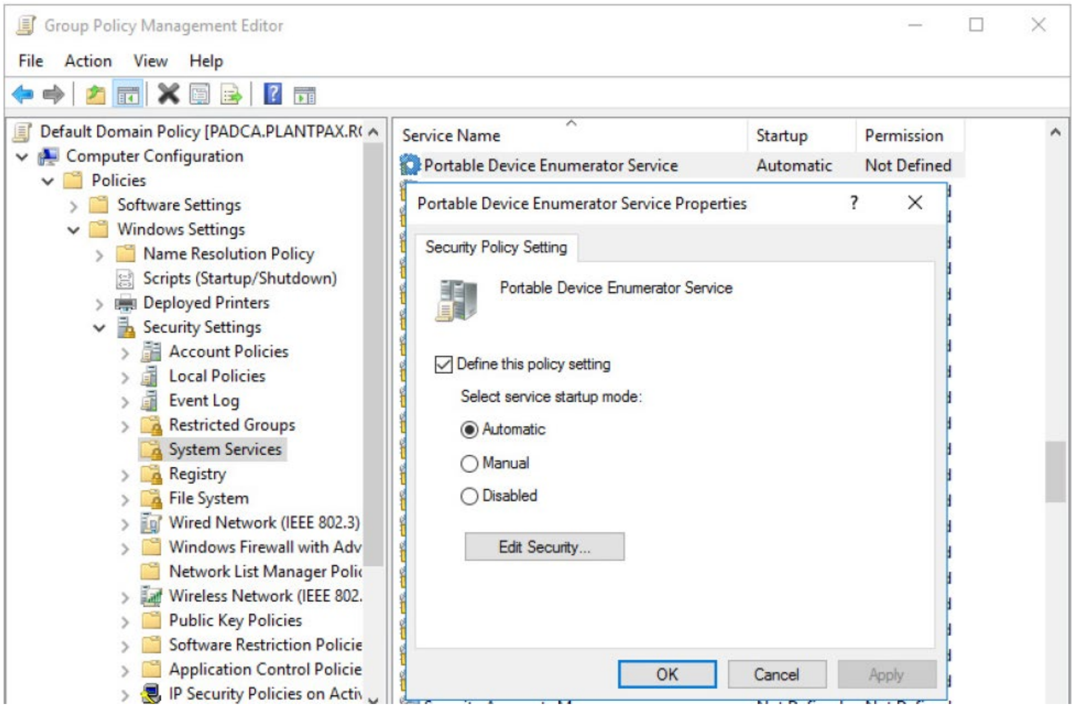

FIG 2. Configuration of a portable device enumerator service.

Logically more secure access through a more secure file system

Depending on your application, you can limit operator access and rights to parts of the file system by using NTFS. FAT and FAT32 are not more secure file systems.

> For additional information about Users Policy Objects, best practice guidance has been outlined as part of the PlantPAx® distributed control system manuals. Refer to the *PlantPAx® Users Policy Objects* section of the PlantPAx® Distributed Control System Configuration and Implementation User Manual.

Take advantage of operating system security and domains

> Applies to: FactoryTalk® View SE, Versions 11.00.00 through 15.00.00

FactoryTalk® View SE uses FactoryTalk® Security to make efficient use of the security features built into the underlying Microsoft Windows operating systems. For compliance, all FactoryTalk® View SE computers in a closed system must be part of the same Windows domain, managed by a Domain Controller. As such, managements 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® View SE client terminal based on your FactoryTalk® View SE architecture, such as enabling automatic sign in and disabling automatic sign out of a Windows service account, enabling, or disabling the screen saver, disabling USB access, etc.

See the Product Download and Compatibility Center for more information regarding compatible operating systems.

Version	Compatible Features
15.00.00[1]	FactoryTalk® View SE computers must run Windows Server 2022 (64-bit), Windows Server 2019 (64-bit), Windows 11, or Windows 10 (64-bit).
14.00.00[1]	FactoryTalk® View SE computers must run Windows Server 2022 (64-bit), Windows Server 2019 (64-bit), Windows Server 2016 (64-bit), Windows Server 2012 R2 (64-bit), Windows 11 (64-bit), or Windows 10 (64-bit).
13.00.00[1]	FactoryTalk® View SE computers must run Windows Server 2019 (64-bit), Windows Server 2016 (64-bit), Windows Server 2012 R2 (64-bit), or Windows 10 (64-bit).
12.00.00[1]	FactoryTalk® View SE computers must run Windows Server 2019 (64-bit), Windows Server 2016 (64-bit), Windows Server 2012 R2 (64-bit), or Windows 10 (64-bit).
11.00.00[1]	FactoryTalk® View SE computers must run Windows Server 2019 (64-bit), Windows Server 2016 (64-bit), Windows Server 2012 R2 (64-bit), Windows 2008 R2, Windows 10 (64-bit), Windows 8, or Windows 7.

[1] Note: Listed Microsoft operating systems encrypt passwords using the operating system's built-in encryption mechanisms.

> Applies to: FactoryTalk® View SE, Version 14.00.00 through 15.00.00

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® View SE including: one-time phone code, biometrics, radio frequency identification (RFID) cards, and NYMI bands (biometric wearable).

> 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.

Take advantage of the FactoryTalk® View Site Edition architecture

> Applies to: FactoryTalk® View SE, Versions 11.00.00 through 15.00.00

FactoryTalk® View Site Edition is run in either a distributed or station architecture. In either case, FactoryTalk® View SE servers run as services and therefore do not require any user to be logged on to the FactoryTalk® View SE server computer. Operators can sign in and out of the FactoryTalk® View SE client stations without affecting the computer or software components of the FactoryTalk® View SE servers; to facilitate this, startup and shutdown of components, that is, macros, derived tags, events, and datalogs, can also be configured to run independently of FactoryTalk® View SE Client startup and shutdown where applicable. One example configuration, enabled within HMI server properties, is shown after this.

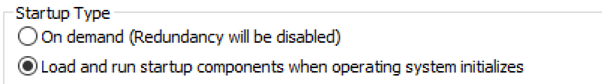

FIG 3. Startup of FactoryTalk® View SE components.

For distributed architecture, the FactoryTalk® View SE server, development studio, and data storage location can be installed on another server than the client. In this case, system security is enabled by separating the operating systems used by the operator from that of server components and engineering tools, which can be used to manage the application and data records. Operators at the FactoryTalk® View SE client terminals have no way to alter server processes or shut down the server operation.

For station architecture, where the FactoryTalk® View SE server can reside on the same server as the client, system security is enabled by using FactoryTalk® Security within the FactoryTalk® View SE application. Even if server components are run on the same computer that an operator is using, these components run as services in the background, and are not affected by the security permissions of whoever happens to be logged on to the computer. Access can be further restricted using other tools and configurations. See section *Prohibit access to FactoryTalk® View Studio, other software programs, and Windows Help* and section *Set up the DeskLock feature*.

Consideration can be given as to the startup method of the FactoryTalk® View SE client terminal, either via automatic system sign in or manual operator sign in to Windows. Automatic system sign in to the Windows operating system and launching of a specific application can be facilitated through use of ThinManager® software. See section *Configure startup of the client terminal in a FactoryTalk® View SE environment.*

Another significant advantage of the FactoryTalk® View SE architecture is support for redundant servers: redundant data servers via FactoryTalk® Linx, and redundant alarm servers via FactoryTalk® Alarms and Events FactoryTalk® Linx, FactoryTalk® Alarms and Events, and FactoryTalk® View SE HMI servers can all be configured to run on both a primary and a secondary computer. Once configured, these redundant pairs are available to any client in the system; adding additional clients does not require any additional configuration.

> Applies to: FactoryTalk® View SE, Version 15.00.00

FactoryTalk® View SE provides the option to customize the HMI project folder location to a more secure area, away from commonly accessible folders. To create a more secure application architecture, an administrator can define a more secure folder path that is accessible only to the system and authorized users, significantly reducing the risk of unauthorized access and enhancing data integrity posture.

This can be implemented during command-line installation by specifying a location for the command-line parameter: /HMIFolder="value", or following installation using the FactoryTalk® View SE tool 'HMI Projects Folder Path Config Utility':

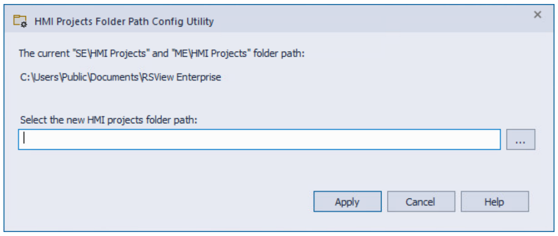

FIG 4. HMI Projects Folder Path Config Utility tool.

> For additional information on the recommended System Workflow, including the steps for how to size, design, and implement a scalable distributed control system with FactoryTalk® View SE, best practice guidance has been outlined as part of the PlantPAx® distributed control system manuals. Refer to the *System Workflow* section of the PlantPAx® Distributed Control System Configuration and Implementation User Manual.

Configure FactoryTalk® View SE user accounts to use Microsoft Windows security and more

> Applies to: FactoryTalk® View SE, Versions 11.00.00 through 15.00.00

Before you can add users and user groups to the accounts list in the FactoryTalk® View SE Runtime Security editor, you have to create accounts for them in FactoryTalk® Security services. In the FactoryTalk® View SE Explorer window, right-click System > Users and Groups and select Security. Click Add, then click the Create New button and select Windows-linked user group or Windows-linked user, depending on whether you have chosen to show groups or users. It is possible to add only a subset of the Microsoft Windows users to the FactoryTalk® system, or add a Microsoft Windows group, in which all Windows users in the group inherit access. When you start a FactoryTalk® View SE project that uses the Windows Security option, the current Windows user is logged into FactoryTalk® View SE if that user has been added to the FactoryTalk® Security users list.

If you want to restrict access to the FactoryTalk® system, security accounts for the users and computers you want to help become more secure must be created in FactoryTalk®, assigned the appropriate security permissions, and reviewed. For more information, see the section *Manage FactoryTalk® View SE runtime security for users, user groups, and computers.*

> Applies to: FactoryTalk® View SE, Version 14.00.00 through 15.00.00

When performing sign in within FactoryTalk® View SE Client, users will have the option to sign in via Password, Azure AD, or OpenID Connect, depending on the service integration of Active Directory and enterprise identity management. The Azure AD or OpenID Connect user accounts can be added through the FactoryTalk® Administrator Console to allow authentication through FactoryTalk® View SE.

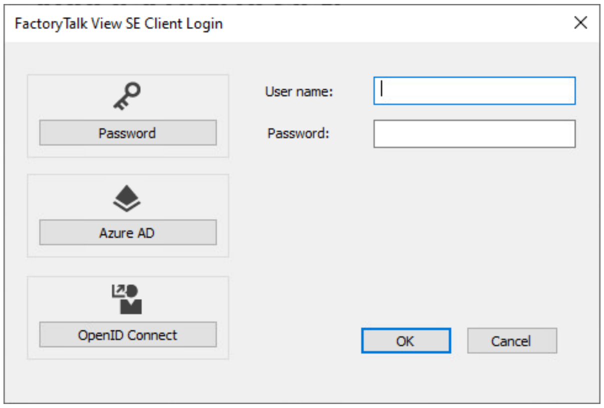

FIG 5. FactoryTalk® View SE Client via Password, Azure AD, or OpenID Connect.

Manage FactoryTalk® View SE runtime security for users, user groups, and computers

> Applies to: FactoryTalk® View SE, Versions 11.00.00 through 15.00.00

After you create users and user groups in FactoryTalk® Security, you add them to the security accounts list in the Runtime Security editor in FactoryTalk® View SE. When you add an account, you also assign the security codes that will give them access to secured HMI components. These codes run from A-P and determine which components a user has rights to at runtime

CAUTION: The Windows-linked "All Users" group is automatically added to the FactoryTalk® Runtime Security accounts. By default, this gives all users' access to all FactoryTalk® View SE runtime security codes (A-P), and all FactoryTalk® Security actions. To remove security code assignments, remove the "All Users" group and add in the new users or groups with appropriate FactoryTalk® View Security Code assignments.

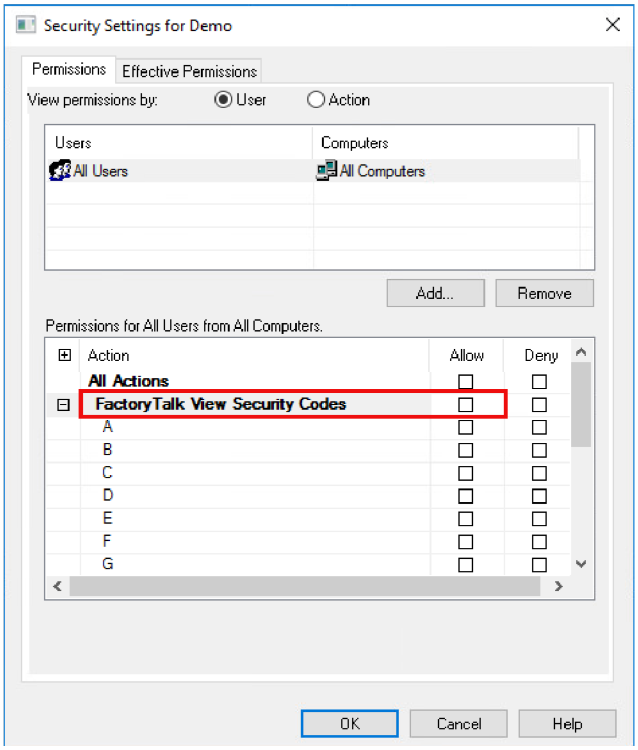

FIG 6. Removing security code assignments.

Security codes can be assigned to commands and macros, graphic displays, OLE objects, and HMI tags to manage the runtime security rights to users and user groups as required for each project.

> Applies to: PlantPAx®, Version 4.x through Version 5.x

When using FactoryTalk® View SE with a PlantPAx® distributed control system, runtime security can be configured for three different capabilities when deploying HMI faceplates from the PlantPAx® Process Library: User roles (for example, Operator, Engineer, and so forth), Area, and Line-of-sight.

To implement role-based security, security codes (A-P) for various role functions are assigned by HMI security tags, which can be configured to allow custom permissions, such as acknowledgment of alarms, bypassing permissives and interlocks, changing device security, and more. When using PlantPAx®, it is recommended that the following runtime security codes (A-P) be assigned to allow the appropriate level of access.

Group	Security Code
Operators	A
Operating Supervisor	B
Maintenance	C
Maintenance Supervisor	D
Engineering	E
Manager	F

Group	Security Code
Administrator	G
View Only	P

In PlantPAx®, area-based security and Line-of-sight are enabled through the controller via an extended tag property or tag parameter, {Cfg_Area}. To implement area-based security, FactoryTalk® area-based user groups are created for each area, and then users are granted area security rights when assigned to these user groups. To implement line-of-sight security, FactoryTalk® computer groups are created for each area, and then computers are granted area security rights when assigned to these computer groups.

> PlantPAx® Distributed Control System: For additional information about implementing runtime security with PlantPAx®, refer to the PlantPAx® Distributed Control System Configuration and Implementation User Manual.

Configure FactoryTalk® View SE clients to automatically Sign Out

> Applies to: FactoryTalk® View SE, Versions 11.00.00 through 15.00.00

When securing the FactoryTalk® View SE client, sign out controls can be used to manage out automatic user sign at the end of any continuous period of controlled system access, and to enforce sign in at the start of the next access period. This can be implemented by using controls within Windows or FactoryTalk® View SE.

Use a password-protected screen saver
When the HMI startup method requires manual operator-sign in to Windows, password-protected screen savers can be used to manage out automatic user sign out. This is to enforce that only operators with the proper credentials are accessing workstations in a closed system. For the respective GPO, apply the screen saver policy through the Group Policy Management 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.

It is noted that because FactoryTalk® View SE server components 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 on the hosts of the application servers (that is FactoryTalk® Directory server, FactoryTalk® View SE HMI server, FactoryTalk® Linx server, or FactoryTalk® Alarms and Events server)

Automatic sign out via implementation of the IdleDetect control object
For some installations, a password-protected screen saver on each client machine is not enough protection; it can be preferred to implement sign out controls within FactoryTalk® View SE instead of the Windows operating system. In these cases, FactoryTalk® View SE clients can be configured to automatically sign out after a specified period through implementation of the IdleDetect control object.

The IdleDetect control object is a FactoryTalk® View SE ActiveX object that can be installed to allow the FactoryTalk® View SE system to execute a command or macro after a period of user inactivity, such as sign out or sign in.

If the system requires that critical operations information is displayed always, coordinated configuration of IdleDetect and the sign in command can be implemented. In this case, the IdleDetect control object can be configured to sign in a default 'view-only' user instead of logging out the current user. Additionally, upon startup of the FactoryTalk® View SE client, the system can also be configured to automatically sign in the default view-only user. This can be achieved through use of a macro with the following sign in command, in which the logged in default user has view-only runtime security permissions:

- Sign in <Default Username> <Default User Password>

NOTE: The view-only user must be a named account created within FactoryTalk® and be added within the Runtime Security Editor. The user must be 'Allowed' limited runtime security codes associated with view-only permissions; for PlantPAx®, the view-only security code can be pre-assigned as code P. It is recommended to 'Deny' certain security privileges for the view-only user to help prevent privileges from being inherited. To do this, right-click your HMI application, select 'Security...', add the view-only user, and select 'Deny' for applicable permissions.

To implement automatic sign in of the default view-only user after a period of activity, create an IdleDetect object, right-click the IdleDetect object > ActiveX Events..., and attach a command or macro to EnterIdleState, such as the previously described macro.

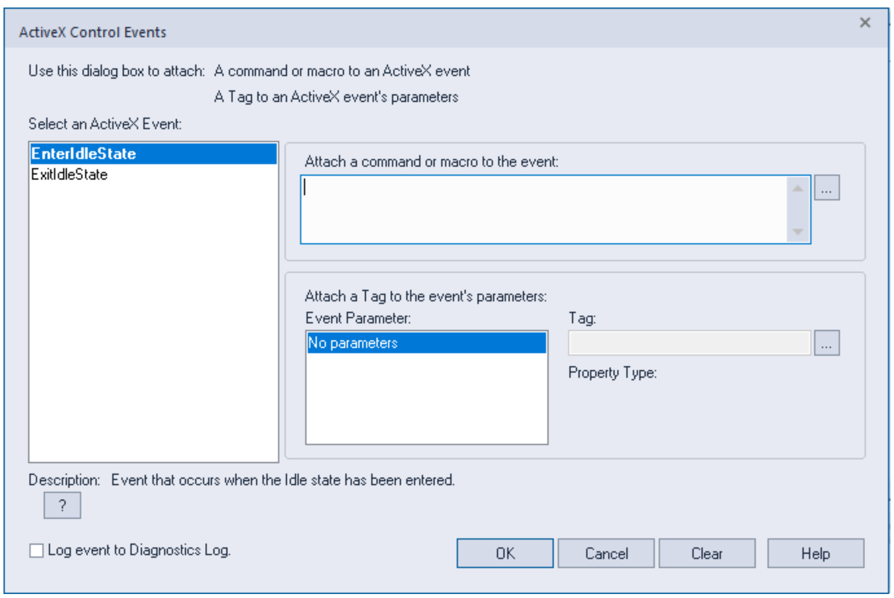

FIG 7. Configure IdleDetect.

To implement IdleDetect, the IdleDetect control object must be active on a screen always, either by embedding the object on every 'main' display or by embedding within an object that is always active, such as a header. Because IdleDetect control objects must be instantiated and configured separately, proper sign out and sign in through IdleDetect must be tested before deployment to confirm proper functioning from all screens.

> IdleDetect ActiveX Control: For additional information about implementing IdleDetect ActiveX Control, refer to the Rockwell Automation Knowledgebase Document ID: BF-132 – FactoryTalk® View SE/RSView32: Sign in another user after a period of inactivity.

NOTE: In the case where automatic sign out is handled by FactoryTalk® View SE, the Windows screen saver can be disabled. For the respective GPO, apply the screen saver policy through the Group Policy Management

Editor > User Configuration > Administrative Templates > Control Panel > Personalization. Configure the 'Enable screen saver' policy as 'Disabled'.

Automatic sign out via FactoryTalk® View SE Client Wizard
If it is not required for the FactoryTalk® View SE client application to remain open after inactivity, the FactoryTalk® View Client file can be configured to enable auto sign out after a defined period. Within FactoryTalk® View SE Client Wizard > Advanced settings > Security and debugging, check 'Enable auto sign out' with the appropriate setting for 'Inactivity period'.

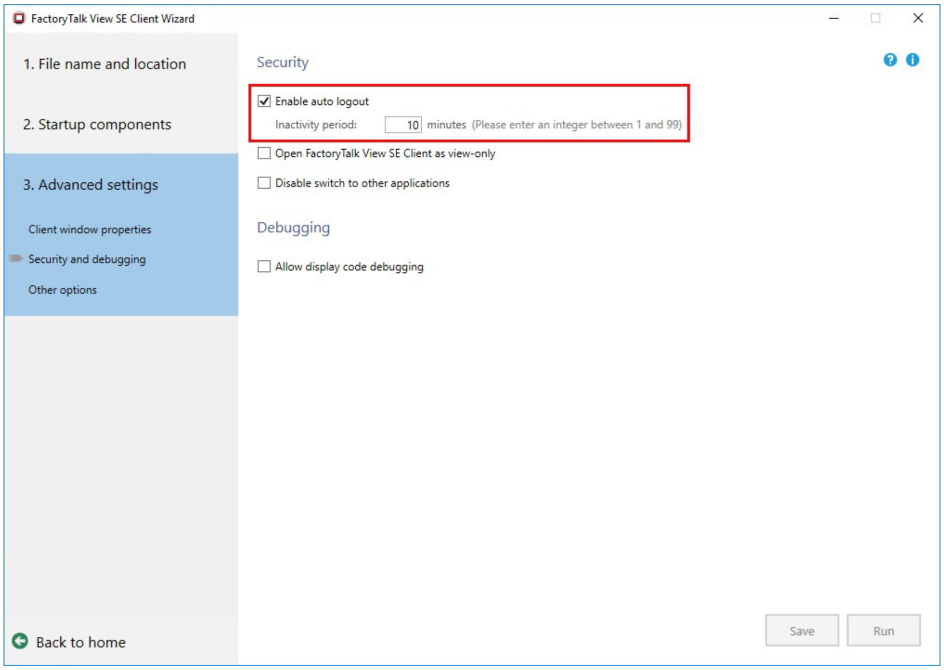

FIG 8. Automatic sign out after a specified inactivity period.

Prohibit access to FactoryTalk® View Studio, other software programs, and Windows Help

> Applies to: FactoryTalk® View SE, Versions 11.00.00 through 15.00.00; ThinManager®, Versions 11.00.00 through 14.00.00

FactoryTalk® View Studio is not intended for use by operators; they cannot be given access to FactoryTalk® View Studio. The easiest way to do this is not to install FactoryTalk® View Studio and other engineering tools on operator computers. If it is necessary to install FactoryTalk® View Studio or engineering tools on these computers. The computers can be secured using ThinManager® software or DeskLock. Another option is to add security for specific user groups at the Application level or at the GPO level.

Prohibit access to FactoryTalk® View Studio and other software programs

If you are using ThinManager® software, you can easily restrict what an operator can access on their client device. ThinManager® allows you to deliver only the authorized application. If you use a feature in your Display Client™ called AppLink™ (Application Link), you can further restrict access to computer resources by providing only the application without the Windows Desktop and taskbar. Further restriction is easy to implement on a ThinManager® terminal by adding the Key Block Module. By default, it blocks Ctrl + Alt + Del and other shortcut keys that allow an operator to exit the application, pull up Task Manager, and get to unauthorized areas within the Windows Operating System.

> For additional information, see the *Remote Desktop Services Displays Client™* and *Key Block Module* sections of the ThinManager® User Manual.

To restrict access at the FactoryTalk® application level in the Windows operating system, from within FactoryTalk® View Studio in the Explorer window, browse to System > Policies > Product Policies. Select the applicable software, open Feature Security, and for the applicable policy, Configure Security for the specified users or user groups.

To restrict access to the software at the GPO level, apply the user policy through the Group Policy Management Editor > User Configuration > Policies > Administrative Templates > System. Configure the policy 'Don't run specified Windows applications' as 'Enabled', and type any application software to create an access restriction. Example: Regedit.exe.

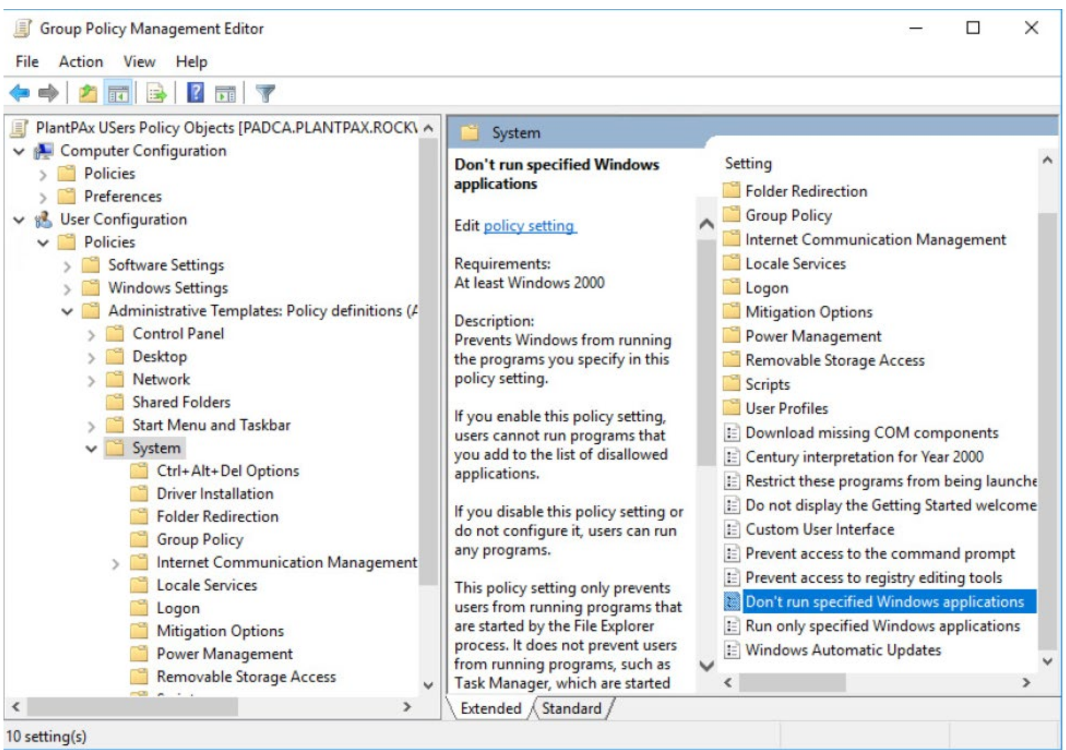

FIG 9. Configuration of policy for software access.

Prohibit access to Windows Help

The Windows Help system is not more secure, and once in Help, a user can get full access to the underlying file system (still limited by their Windows account). Do not allow operators to have access to Windows or FactoryTalk® View SE Help

Help can be restricted by using a combination of DeskLock and overriding the F1 help keys in the FactoryTalk® View SE application. It can also be restricted using Windows security on the help executables.

Use Windows account password aging and management

> Applies to: FactoryTalk® View SE, Versions 11.00.00 through 15.00.00

When FactoryTalk® View SE 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.

> Applies to: ThinManager®, Versions 11.00.00 through 14.00.00

ThinManager® software, when used in a FactoryTalk® View SE environment, can automatically and periodically rotate passwords for any user account on a domain if using an alternate authentication method such as RFID card or fingerprint in place of a password.

Configure Startup of the client terminal in a FactoryTalk® View SE environment

> Applies to: FactoryTalk® View SE, Versions 11.00.00 through 15.00.00

Several methods can be used for startup of the FactoryTalk® View SE client terminal, such as automatic system sign in or manual operator sign in to Windows. Considerations as to sign in requirements for the computer can differ depending on the method used.

Automatic system sign in by a Windows service account

A common method for startup of the FactoryTalk® View SE client terminal is through an automatic system sign in with a Windows service account. In this case, automatic sign in of the Windows service account can be facilitated through use of ThinManager® software or manual configuration of the Windows operating system.

Once logged in, the Windows service account can be given limited desktop and software access through a combination of application-level security, GPO-level security, and implementation of DeskLock. Upon sign in, the FactoryTalk® View SE client can be configured to automatically launch, for example, by DeskLock, and sign in with view-only permissions. The benefits of this method allow for reduced operator interaction with the Windows operating system and reduces the risk of unauthorized access. Additionally, this allows critical operation information to be displayed on the terminal always.

The FactoryTalk® View SE client can also be configured to automatically sign out the current user and close all displays after a period of mouse or keyboard inactivity. To configure FactoryTalk® View SE controls such as IdleDetect, refer to section *Configure FactoryTalk® View SE clients to automatically sign out.*

Manual Operator sign in to Windows

A combination of automatic system sign in by a Windows service account, implementation of DeskLock, FactoryTalk® View SE security, and a default view-only account setup with read-only security rights is used to help secure the Windows computer, but still provide the read-only visibility required by operators. However, if this method is not used, for example, when implementing operator sign in to Windows, sign in requirements is advised. The following are recommendations in this case:

Each user must sign in to the Windows computer at the start of their session, and sign out when they are done Since the FactoryTalk® View SE server components run as services, it is not necessary to have any user logged on to computers that are used to host servers used in the application (that is FactoryTalk® Directory server, FactoryTalk® View SE HMI server, FactoryTalk® Linx server, or FactoryTalk® Alarms and Events server). Operators cannot use FactoryTalk® View SE servers as operator stations.

Computers that are used as FactoryTalk® View SE display clients must have the actual operator sign in to the computer. Operators can never allow anyone else to perform operations using their username and password. If it is necessary for a supervisor to perform or approve certain operations, another computer can be used, or the electronic signature feature can be used. If the same computer is used, the operator can sign out Windows, and the supervisor can sign in. In cases where two signatures are required (that is operator and supervisor), the approval will take place by using the electronic signature feature while the operator remains logged in to the system; in this case, the electronic signature will be attributed with the respective signer within the audit trail.

The FactoryTalk® View SE client computer can also be configured to automatically sign out the current user and close all displays after a period of mouse or keyboard inactivity. To configure the password-protected screen saver, refer to section *Configure FactoryTalk® View SE clients to automatically sign out.*

Set up the DeskLock feature

> Applies to: FactoryTalk® View SE, Versions 11.00.00 through 15.00.00

To confirm that operators remain within a closed environment while running FactoryTalk® View SE, use the DeskLock feature. When DeskLock is used while disabling switching to other applications and other security configurations noted in the DeskLock documentation, it is possible to lock operators into a closed FactoryTalk® View SE runtime system. The DeskLock tool and accompanying documentation are available on the Windows Start menu, and are installed with the FactoryTalk® View SE software.

CAUTION: Do not implement the DeskLock feature without first carefully reading the documentation. DeskLock can have far-reaching effects on your operating system. Its purpose is to replace the standard Windows desktop with a customized one intended to help prevent operators from having access to operating system functionality, such as restarting Windows or shutting down tasks. If you do not leave a way for the administrator to access this functionality, there could be no access to it at all. DeskLock also configures Windows Policies.

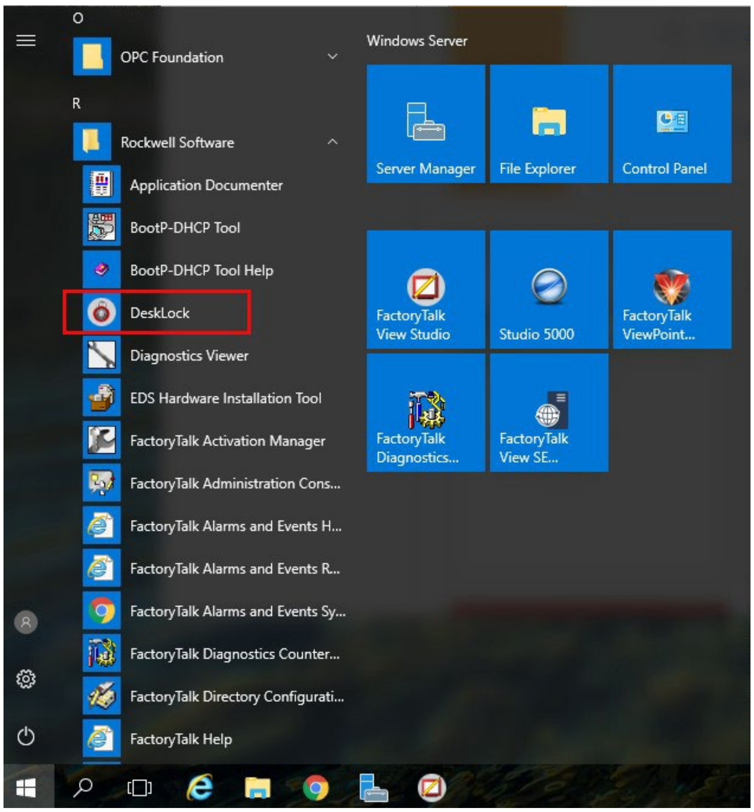

FIG 10. DeskLock feature.

Securing FactoryTalk® View SE Client terminals

> Applies to: FactoryTalk® View SE, Versions 11.00.00 through 15.00.00

Configure clients as shown after this. You can NOT allow display code debugging as this will allow the launching of the Visual Basic for Applications (VBA) editor, which is not more secure. Also, disable the ability to switch to other application as this opens access to other programs.

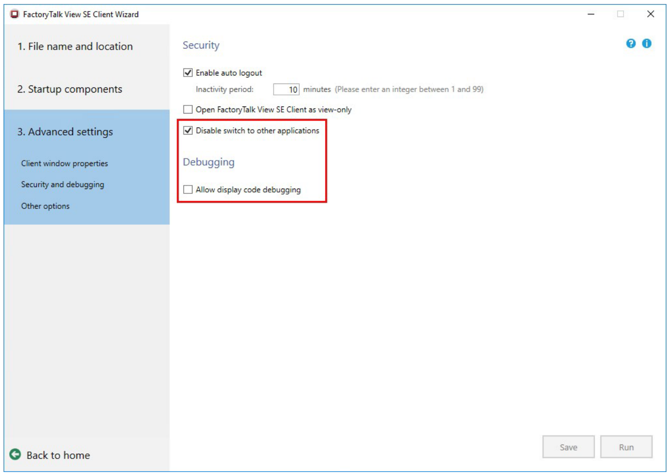

FIG 11. FactoryTalk® View SE Client wizard.

In the FactoryTalk® View SE Client Window Properties dialog box, make the following selections:

Enable/Disable	Property	How this helps
Disable	Show Title Bar	Enable only if necessary. By enabling the title bar, this can provide access to the desktop.
Disable	Show system menu and close button	This will help prevent users from closing the client window.
Enable	Maximize Window	Helps prevent users from seeing or clicking items on the desktop.
Disable	Show Diagnostics List	Enable only if necessary.

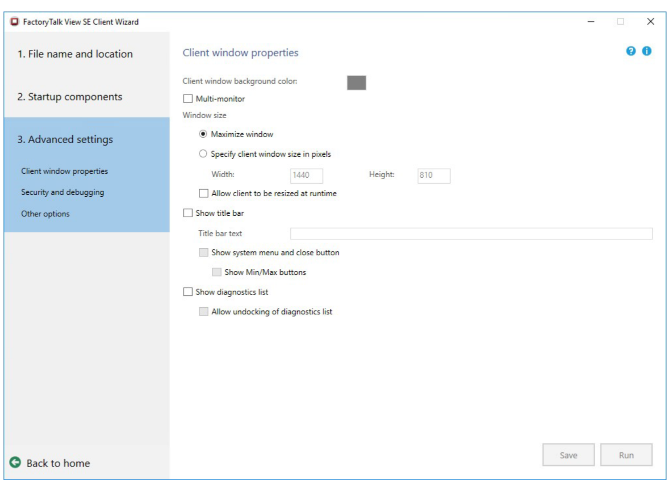

FIG 12. FactoryTalk® View SE Client window properties.

In addition, you can use the DeskLock tool on the computer running the FactoryTalk® View SE Client and configure it to launch only the FactoryTalk® View SE client window.

Log FactoryTalk® Alarms and Events to a central ODBC Database

> Applies to: FactoryTalk® View SE, Versions 11.00.00 through 15.00.00

One advantage of using FactoryTalk® Alarms and Events is that annunciation of this information is through common controls like the Alarm and Event Summary and the Alarm and Event Banner. These common objects allow users to perform alarm actions such as acknowledging and shelving alarms, no matter where the alarm originated — a server-based alarm triggered in a server or a device-based alarm triggered in a controller.

FactoryTalk® Alarms and Events generate four types of messages for logging that are logged to separate database tables:

- **Historical alarm and event messages.** These logs record all alarm activity that occurs at runtime. The Alarm and Event historian manages connections between alarm servers and databases, and logs data from each alarm server to an alarm history database. They can be routed to an ODBC database. NOTE: While alarm acknowledgments from the FactoryTalk® Alarms and Events objects are captured with this message type, these messages can be presented alongside the **Alarm audit logs** to give a full picture of operator activity, for example, alarm acknowledgments from a PlantPAx® faceplate.
- **Alarm audit logs.** These logs are generated in response to actions performed on alarms, such as modifying or acknowledging an alarm, including any alarm acknowledgment comments. They can be routed to an ODBC database, or to the FactoryTalk® AssetCentre database if installed.
- **Alarm event (diagnostic) logs.** These logs inform operators of system activity, in the form of information, error, and warning messages. They can be routed to an ODBC database, or to the FactoryTalk® AssetCentre database if installed.
- **Alarm Diagnostics & Health log.** The Diagnostics and Health Log allow a device's diagnostics and health information to be displayed in the Automatic Device Descriptive Analytics (ADDA) Viewer and can be routed to the FactoryTalk® AssetCentre database if installed.

With the configuration of FactoryTalk® Alarms and Events, it is possible to store all **Historical alarm and event messages** in one centralized alarm database. When connection is lost to the controller, the controller stores undelivered information in a buffer, including time stamps, alarm state, and associated tag values, until the connection is established again.

The remaining three message types, **Alarm audit logs**, **Alarm event (diagnostics) logs**, and **Alarm Diagnostics & Health logs** are stored in a separate database, covered in the section Log *all FactoryTalk® View SE activity to a central FactoryTalk® AssetCentre or ODBC Database*.

To set up FactoryTalk® Alarms and Events logging, follow the following steps:

- Create an ODBC data source to serve as a central database
- Configure FactoryTalk® Alarms and Events to log historical alarm and event messages
- Visualize the alarm and events data

Let's review each in more detail.

Create an ODBC data source to serve as a central database

To create an ODBC data source, follow the instructions in the FactoryTalk® View SE documentation, or you can configure it from Windows Control Panel > Administrative Tools > Data Sources (ODBC). The following steps assume that a Microsoft SQL Server database is being used.

1 On the System DSN tab, click *Add* to create a data source.

2 Scroll through the list of drivers and select SQL Server. Click *Finish*.

3 Respond to prompts from the wizard to create a data source to SQL Server. When you finish typing your entries, click *Next*.

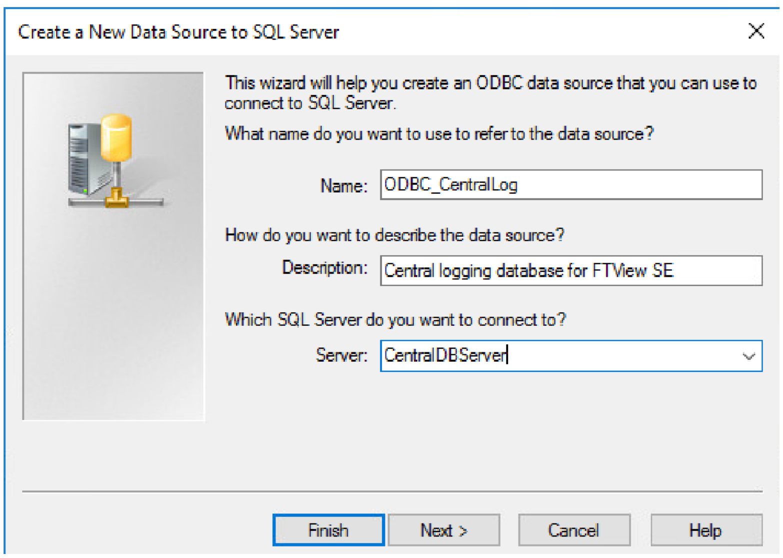

FIG 13. Create an ODBC data source.

4 A t the next window, select the option, "With Windows NT authentication using the network sign in ID". Click *Next*.

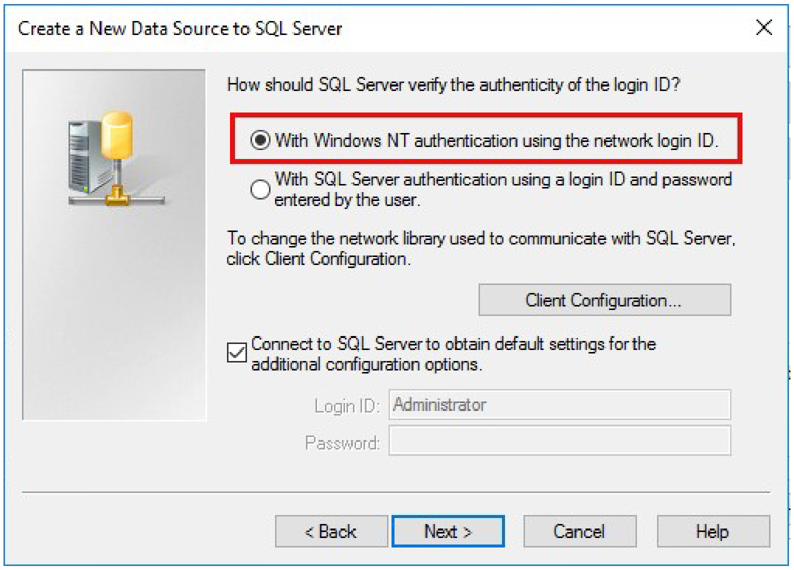

FIG 14. SQL server sign in ID verification.

5 Continue working through the wizard, selecting options and clicking *Next*. When you finish, test the communications to your new ODBC data source.

This ODBC data source can now serve as the central data source.

Configure FactoryTalk® Alarms and Events to log historical alarm and event messages

The following steps must be performed in order to log alarm historical activity:

1 Within the FactoryTalk® Administration Console, the alarm database must be defined within FactoryTalk® System > Connections > Databases.

2 For each FactoryTalk® Alarms and Events alarm server and FactoryTalk® Linx data server in an application, alarm and event history logging must be enabled, and a Microsoft SQL database must be selected.

The Alarm and Event Historian then routes FactoryTalk® alarm and event-related data to the alarm history database. Database definitions are stored in the FactoryTalk® Directory and must be shared by multiple alarm servers in an application.

Visualize the alarm and events data

When FactoryTalk® View SE is used with FactoryTalk® AssetCentre, alarm events can be displayed on TrendPro, alongside production data and operator actions. This creates a comprehensive tool that puts context around changing setpoint data, alarms that were triggered, and what operator actions were taken that can have affected a process.

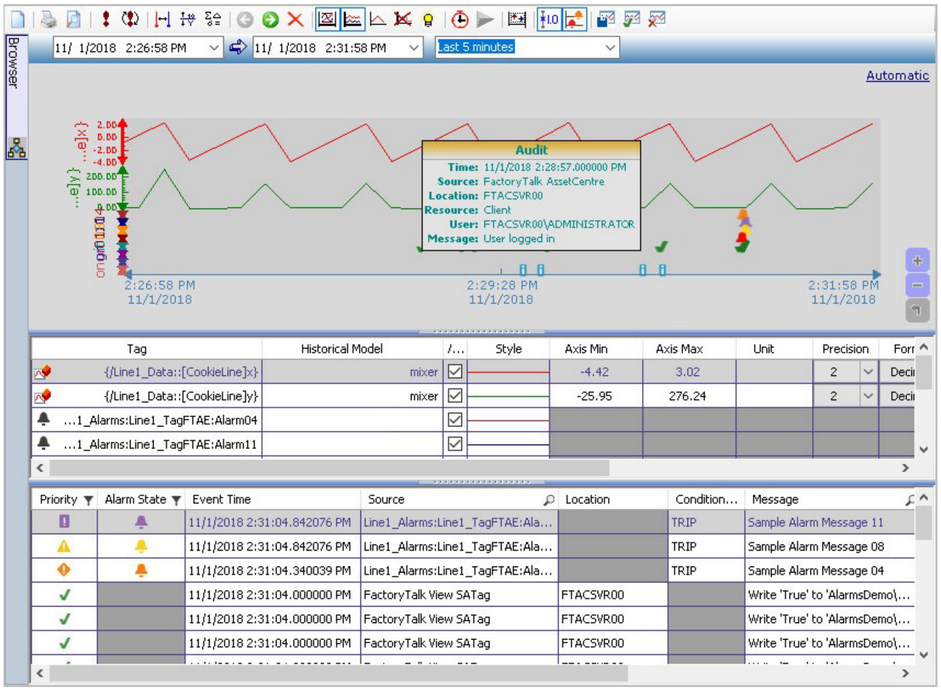

FIG 15. Audit log, production data and alarm events.

> FactoryTalk® View SE: For additional information about using FactoryTalk® Alarms in FactoryTalk® View SE, refer to the FactoryTalk® View SE User's Guide.
>
> FactoryTalk® Alarms and Events: For additional information about configuring FactoryTalk® Alarms and Events, refer to the FactoryTalk® Alarms and Events System Configuration Guide.

Log all FactoryTalk® View SE activity to a central FactoryTalk® AssetCentre or ODBC Database

FactoryTalk® View SE provides many options to comply with regulatory requirements for logging of operator activity. This includes integration to FactoryTalk® AssetCentre for a scalable security and data integrity solution, or built-in FactoryTalk® View SE options for a compliant, yet flexible solution.

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.

With the configuration of FactoryTalk® Diagnostics, it is possible to store the **Event Log, Audit Log,** and **Diagnostics & Health Log** in the centralized FactoryTalk® AssetCentre database. 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.

In a system where FactoryTalk® AssetCentre is not used, **Event Log** and **Audit Log** information can be configured within FactoryTalk® Diagnostics to send to a centralized ODBC Database.

The two methods for capturing data in a FactoryTalk® system:

- Via FactoryTalk® AssetCentre Database
- Via ODBC Database

Logging FactoryTalk® View SE activity via the FactoryTalk® AssetCentre Database

> Applies to: FactoryTalk® View SE, Versions 11.00.00 through 15.00.00; FactoryTalk® AssetCentre, Versions 11.00.00 through 13.00.00

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.

To use FactoryTalk® AssetCentre audit and event logging, follow the following steps:

- Configure FactoryTalk® Alarms and Events to track activity
- Visualize the FactoryTalk® AssetCentre audit data

Let's review each in more detail.

Configure FactoryTalk® AssetCentre to track activity
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.

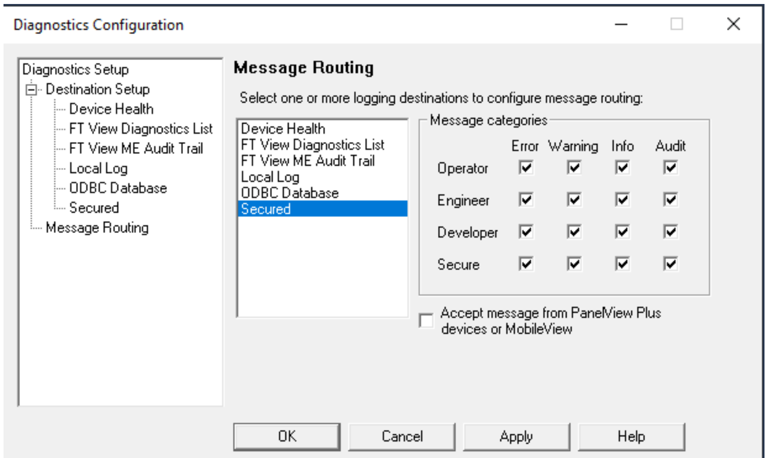

FIG 16. Diagnostics message routing with FactoryTalk® AssetCentre.

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.

> FactoryTalk® AssetCentre: 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.

Visualize the FactoryTalk® AssetCentre audit data

When FactoryTalk® View SE is used with FactoryTalk® AssetCentre, operator actions logged to the audit log can be displayed on TrendPro, alongside production data and alarm events. This creates a comprehensive tool that puts context around changing setpoint data, alarms that were triggered, and what operator actions were taken that can affect a process. Refer to the section *Log FactoryTalk® Alarms and Events to a central ODBC Database* for more information on alarms.

Logging FactoryTalk® View SE activity via ODBC Database

> Applies to: FactoryTalk® View SE, Versions 13.00.00 through 15.00.00; FactoryTalk® Services Platform, Versions 6.31.00 through 6.50.00

For smaller-scale systems, FactoryTalk® View SE provides several built-in options for the capture of HMI activity to an ODBC Database. For systems that do not have FactoryTalk® AssetCentre, ODBC Database message routing for audit logs can be configured for use, activated through FactoryTalk® View SE licensing. And for systems that do not require the high availability of FactoryTalk® Historian SE, ODBC Data Logs can be configured within FactoryTalk® View SE to capture controller data.

To use ODBC database logging, follow the following steps:

- Create an ODBC data source to serve as the central database
- Configure FactoryTalk® Diagnostics to track activity
- Configure the FactoryTalk® View SE data log, using Data Log Models or DataLogPro

- Visualize the FactoryTalk® View SE data log

Let's review each in more detail.

Create an ODBC data source to serve as a central database
To create an ODBC data source, refer to guided steps detailed in section *Log FactoryTalk® Alarms and Events to a central ODBC Database.* This ODBC data source can now serve as the central data source.

Configure FactoryTalk® Diagnostics to track activity
The following steps must be performed on each machine that will be a FactoryTalk® View SE client. It is noted that while FactoryTalk® Diagnostics information can be captured via the ODBC Database, FactoryTalk® AssetCentre can provide an integrated, more secure option for audit and event data logging.

1 From FactoryTalk® Activation Manager, verify that the machine is licensed with the latest FactoryTalk® View SE activation. Applicable versions of FactoryTalk® View SE activations will automatically include the license 'Enable Audit severity to ODBC database' in FactoryTalk® Activation Manager.

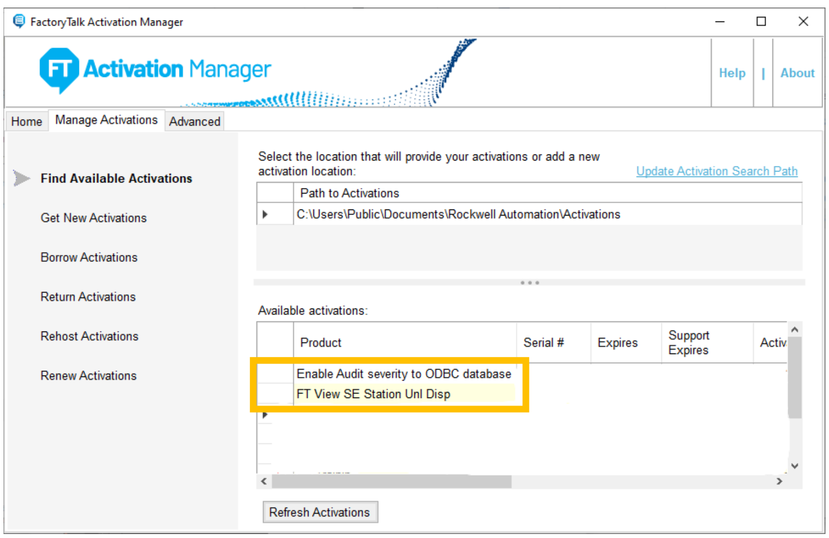

FIG 17. FactoryTalk® Activation Manager with the latest FactoryTalk® View SE license to 'Enable Audit severity to ODBC database' available.

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

3 Under Destination Setup, select *Local Log* to configure settings for the local sign in this computer.

4 Leave the Logging path at its default. Make sure that the maximum log size is large, for example 25,600 KB Overwrite events as needed.

5 Select ODBC Database to configure settings for logging to the central ODBC data source.

6 For Message Buffering, log messages to the database every two minutes or less, and buffer messages locally for at least 12 hours.

7 Configure the ODBC data source to point to the SQL Server or other ODBC data source you configured earlier Maintain connections for at least twice as long as the logging period, or indefinitely.

8 If you configured the ODBC data source database to allow NT Authentication, you do not need to enter sign in information.

9 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.

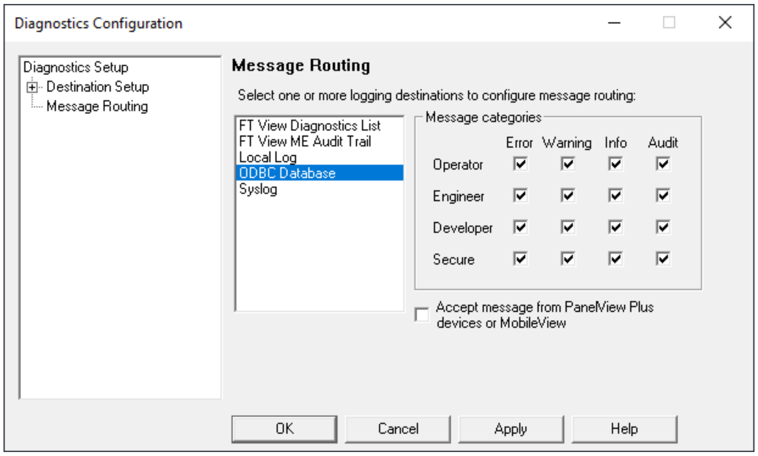

FIG 18. Diagnostics message routing with ODBC Database, where FactoryTalk® AssetCentre is not installed. Note: Audit and Secure checkboxes are disabled without the latest FactoryTalk® View SE license to 'Enable Audit severity to ODBC database' available.

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, refer to the Rockwell Automation Knowledgebase Document ID: QA52576 - FactoryTalk View SE: Audit log configuration settings.

Configure the FactoryTalk® View SE data log, using Data Log Models

If your application requires Data Logging, you can log to a more secure database, such as an ODBC Database, which provides administrative capabilities for data and security management. One option is to use a Data Logs Model:

1 From the FactoryTalk® View Studio, open the Data Log Model for your HMI Server.

2 Output in the Setup tab, select ODBC database as the storage format.

3 Output in the Paths tab, configure an ODBC backup path.

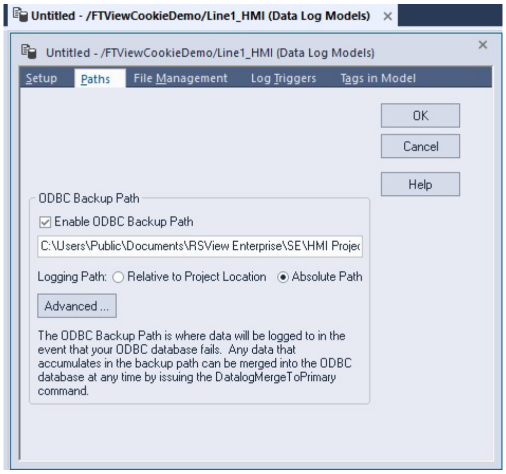

FIG 19. Sign in to a more secure ODBC database.

If the connection to the ODBC database is temporarily broken, backup information will be kept in this location. This location must be secured using the operating system security or using DeskLock so that operators cannot modify the files. When the ODBC database becomes available again, the DatalogMergeToPrimary command must then be used to merge the backup data into the primary database. This can be done by running the DatalogMergeToPrimary every day using Event Detector, or through written SOPs.

4 On the File Management tab, do not configure purging of old records. All management of historical records can be handled in the ODBC database.

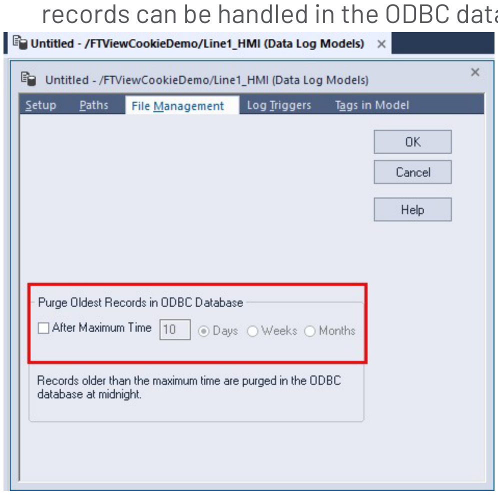

FIG 20. ODBC database file management.

Configure the FactoryTalk® View SE data log, using DataLogPro

Starting with version 14, FactoryTalk® View SE also provides the option for DataLogPro, a built-in data log engine with database management capabilities that stores historical data in InfluxDB™. The InfluxDB can be installed locally, or with version 15, can be installed in a remote location.

1 If using a remote InfluxDB, from within the FactoryTalk® View Studio, open Connections > Databases, and create a database connection to the remote InfluxDB, specifying the Definition name, URL, Token, and Organization name.

2 From the FactoryTalk® View Studio, open DataLogPro for your HMI Server.

3 From within Settings, configure the DataLogPro database to Connect to a Local database or Remote database. If using a remote InfluxDB, specify the Database connection created previously. Configure the Storage duration; to configure the Storage duration to log indefinitely, uncheck the Storage duration box.

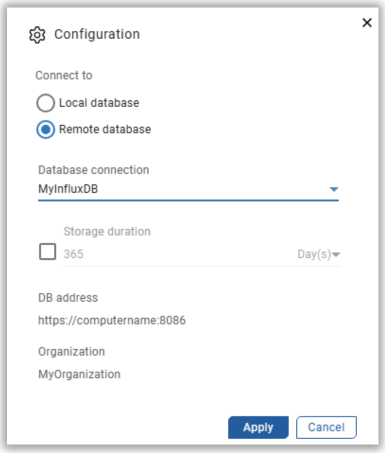

FIG 21. InfluxDB remote database configuration.

For a remote database, if the HMI server loses connection to the remote InfluxDB, it starts logging data to the built-in InfluxDB with the same storage duration as the remote InfluxDB. Once the connection to the remote InfluxDB is restored, all the data logged to the built-in InfluxDB will be synchronized to the remote InfluxDB.

Additional consideration can be given to defining the system of record when using InfluxDB in a redundant HMI architecture, in which the database is duplicated to two locations. In the case for a local database configuration, data is logged to the active and standby HMI servers. In the case for a remote database configuration, the active server logs data to the remote InfluxDB while the standby server logs data to the built-in InfluxDB. If one server is disconnected, once the DataLogPro service starts again, the data that is missing during that period is automatically synchronized between the two servers.

Finally, considerations for the use of DataLogPro and InfluxDB include implementation of a user management strategy and database management strategy, including backup and restore, which are handled through interfaces and tools from within InfluxDB, outside of the FactoryTalk® Studio software. Proper logical and physical security measures can be implemented on the underlying infrastructure to provide the needed data security and data integrity measures for InfluxDB.

> FactoryTalk® View SE installs InfluxDB OSS 2.7. For more information on how to use and access data of the database, see InfluxDB OSS v2 documentation.

Visualizing the FactoryTalk® View SE datalog

The TrendPro and Data Grid objects are built-in options to visualize FactoryTalk® View SE Data Logs from the HMI. The TrendPro object provides options to overlay the Data Log information with alarms and operator activity logged by the FactoryTalk® system to provide context for operator activity. The Data Grid object provides the option to display Data Log or ODBC information in a tabular format on the HMI.

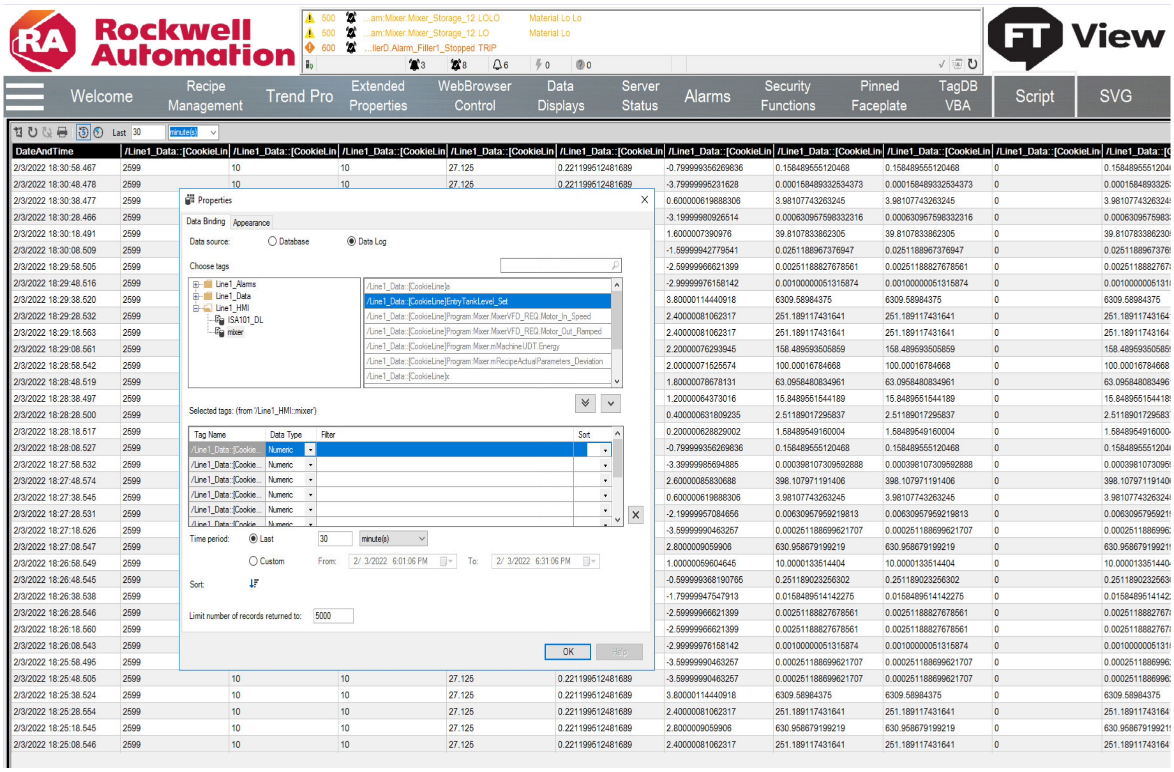

FIG 22. Data Grid object for displaying Data Log or ODBC data from the HMI.

> Applies to: FactoryTalk® View SE, Version 15.00.00

For countries observing Daylight Savings Time (DST), it is essential to distinguish entries based on their capture order during the time change. All FactoryTalk® database logging options store data sequentially as logged. Use the TrendPro and Data Grid to display data sequentially from various historical data sources, including Datalog Pro, FactoryTalk® Alarms and Events, FactoryTalk® Diagnostics, and FactoryTalk® Historian SE.

For data stored with the computer's local time, such as Data Logs logged to an ODBC database, the Data Grid object is recommended to distinguish unique entries during DST and deliver clear traceability. To achieve this, add the "Date Time Logged in UTC" as an auto-generating column with a unique UTC time stamp for each new entry. This can be done by creating a column with a 'Default Value or Binding' in the Table Design within Microsoft SQL Server. This approach helps differentiate data with redundant time stamps during DST.

The "Date Time of data generation" and the "Date Time Logged in UTC" are not captured simultaneously. Confirm that the meaning of these time stamps is clear if used.

Set up reverification of operator identity, or supervisor signoff

> Applies to: FactoryTalk® View SE, Versions 11.00.00 through 15.00.00

Once an operator is logged on to the Windows and FactoryTalk® View SE client, all operations are logged with the username. Some companies have a 'reverification' of operator identity for specific crucial operations, or specific supervisor sign off as part of their procedures. FactoryTalk® View SE provides this level of security through its signature and authorization capability. When using this functionality, users are prompted to enter their electronic signature and obtain verification from a supervisor, if needed, before trying to perform a setpoint change, enter text for a recipe name or batch information to a tag, or issue a command. These activities are then logged to the FactoryTalk® View SE activity log and any external ODBC log. The information logged includes username, old value, new value, operator comments regarding why the change was made, and who approved the change.

At runtime, the click of the button will present a window in which the new value of the tag can be entered. This window also provides the place where an electronic signature, in the form of a username and password, is entered to confirm the identity of the operator that is performing the change. The approval of the operation can require that an approver will also enter an electronic signature. The window provides space for a user comment about the operation to be entered. Any of these options can be enabled or disabled through the FactoryTalk® View SE property page.

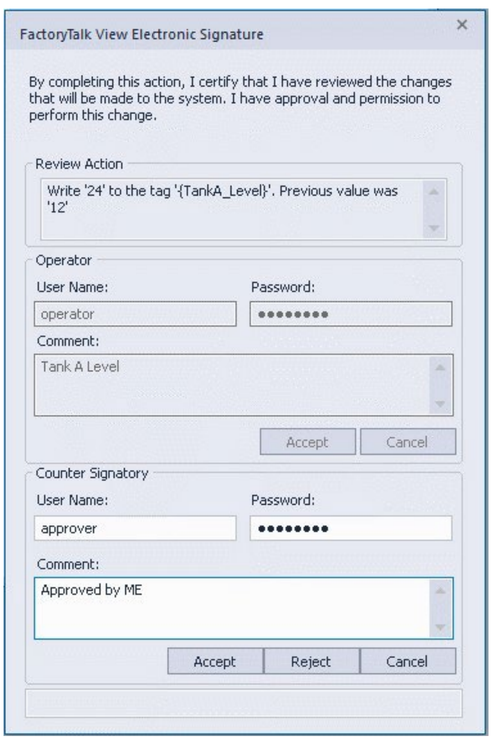

FIG 23. Reverification of operator identity.

All electronic signature authentication and required information, such as a comment and valid data range, are verified before the tag value is written or the command is issued. If a username or password is incorrect at runtime, the value will not be changed and a warning message will be shown. If an option is enabled, then information must be entered for that option; a warning message will be shown if any information is left blank. FactoryTalk® View SE will log any information about the tag written and any warnings or errors to the activity log. The log entry will record the name of the user who made the change, the original value of the tag, what it was changed to, who approved it, and any comment that was entered. The format of the information message is shown in the following example:

> ESign: Operation: Change Temp Setpoint, value change for 'Tag1' from 35 to 50 Performed by Operator ID OPERATOR FULLNAME Approved by Supervisor ID SUPERVISOR FULLNAME, Comment: changed per order 345B

FactoryTalk® View SE includes built-in objects and the FactoryTalk® View SE Signature Button ActiveX control, which provide the electronic signature authentication feature. The subsequent sections describe how to implement electronic signature features with built-in and ActiveX object types. Compatibility information regarding electronic signature features for built-in objects are listed after this:

Version	Compatible Features
14.00.00 through 15.00.00	E-Signature is configurable with the following built-in objects: maintained button, latched button, interlocked button, ramp button, control list selector, and piloted control list selector. Embedded variables that are numeric, string, and date and time are supported in electronic signature confirmation messages.
13.00.00 through 15.00.00	E-Signature is configurable with the following built-in objects: multistate button.
11.00.00 through 15.00.00	E-Signature is configurable with the following built-in objects: command button, numeric input, and string input.

This section will cover the following guidance and considerations for implementing electronic signatures:

- Configuration of electronic signature features with FactoryTalk® View SE built-in objects
- Configuration of the electronic signature features with the FactoryTalk® View SE Signature Button ActiveX control
- Configure diagnostics and message routing
- Considerations for implementing electronic signatures with recipe management

Let's review each in more detail.

Configuration of electronic signature features with FactoryTalk® View SE built-in objects

If you choose to implement an electronic signature using one of the FactoryTalk® View SE built-in input objects, configure them as follows:

1 Add the built-in object to a FactoryTalk® View graphic by selecting it on the FactoryTalk® View SE object toolbar and drawing it on the display.

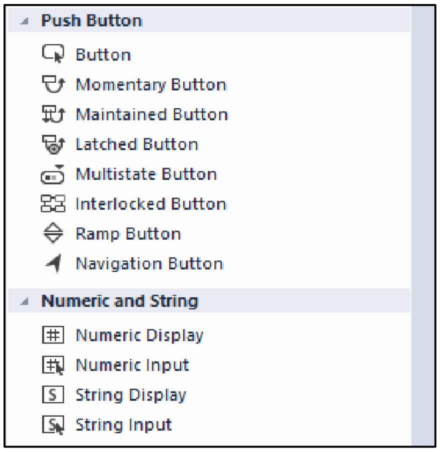

FIG 24. FactoryTalk® View SE object toolbar

2 Configure settings on the object properties dialog for the respective built-in object, as shown after this:

Connections tab

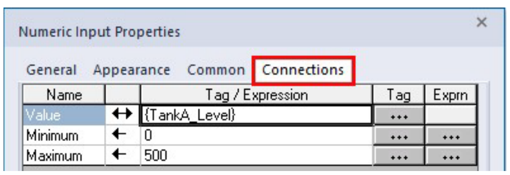

FIG 25. Built-in object, connection properties.

General tab

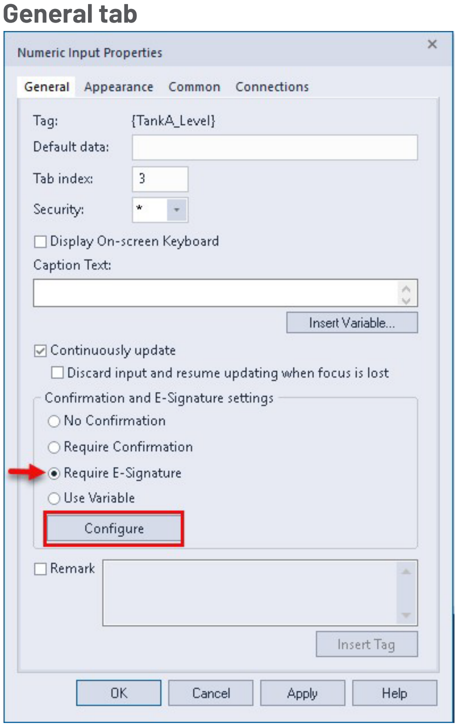

FIG 26. Built-in object, general properties.

Configure the Electronic Signature options:

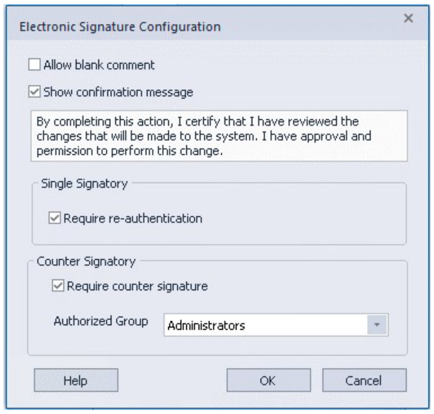

FIG 27. Built-in object, configure e-signature settings.

Because security can be set on the input object on the display, it is not necessary to specify a group that is able to perform the write action. At runtime, when a new value is entered, the current user will be asked to reauthenticate with their password before the change is committed.

3 Click OK to close the Electronic Signature Configuration dialog box, and *OK* to close the object properties dialog.

4 Test-run the display in FactoryTalk® View Studio Click on the input object and enter the new value or string. When you attempt to write the new value, the FactoryTalk® View Electronic Signature runtime dialog window will pop up - complete with the information fields as required by the E-signature configuration:

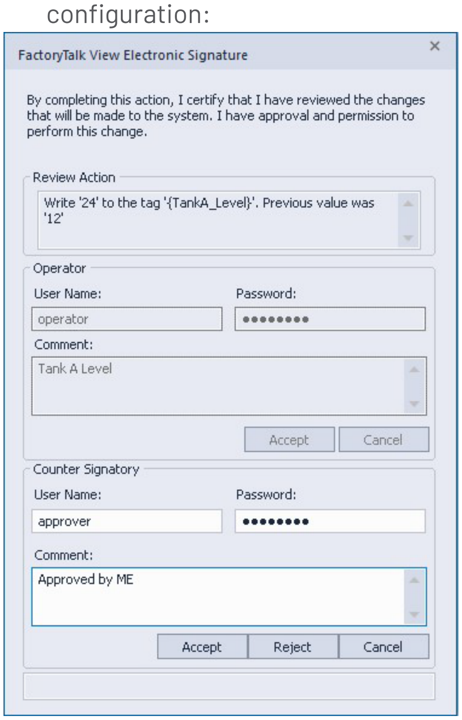

FIG 28. Input object e-signature verification.

5 You must have the user groups configured, and be logged in as a user that is with rights to write a new value to initiate the action.

6 Check the Diagnostics List to see the entries documenting successful and unsuccessful setpoint changes.

7 Close the display when you are done testing the signature feature on your object.

8 To test the display in the client, configure a FactoryTalk® View SE client.

Configuration of the electronic signature features with the FactoryTalk® View SE Signature Button ActiveX control

If you choose to implement an electronic signature using the Signature Button ActiveX control, configure the button as follows:

1 Add the signature button control to a FactoryTalk® View display by clicking the Objects Menu and selecting ActiveX Control.

2 Draw a rectangle on the display for the button, and then select the "FactoryTalk® View SE Signature Button" from the ActiveX objects list as shown after this:

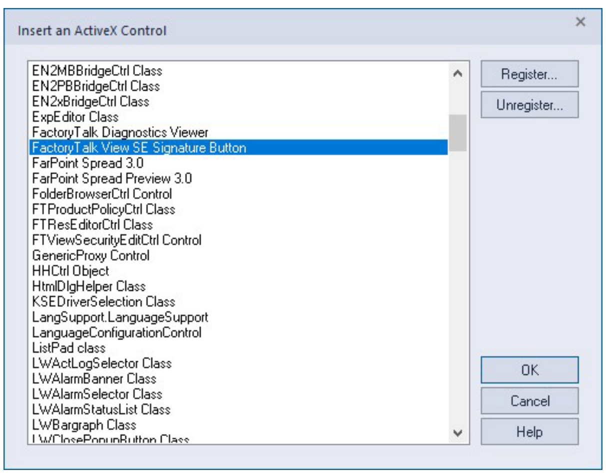

FIG 29. Signature button, ActiveX control.

3 To verify the change, add a numeric display object to the display, then link the object to the tag whose setpoint will be downloaded.

4 Save the display. Give it a unique name in the application.

5 Double-click the Signature Button to open the custom property pages, and configure settings on each tab as follows:

General tab

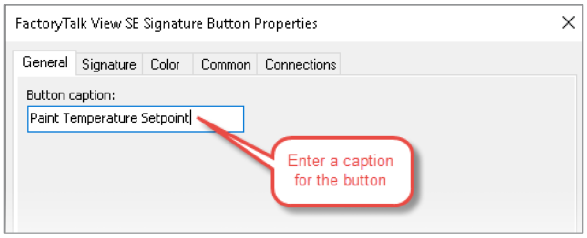

FIG 30. Signature button, general properties.

Signature tab

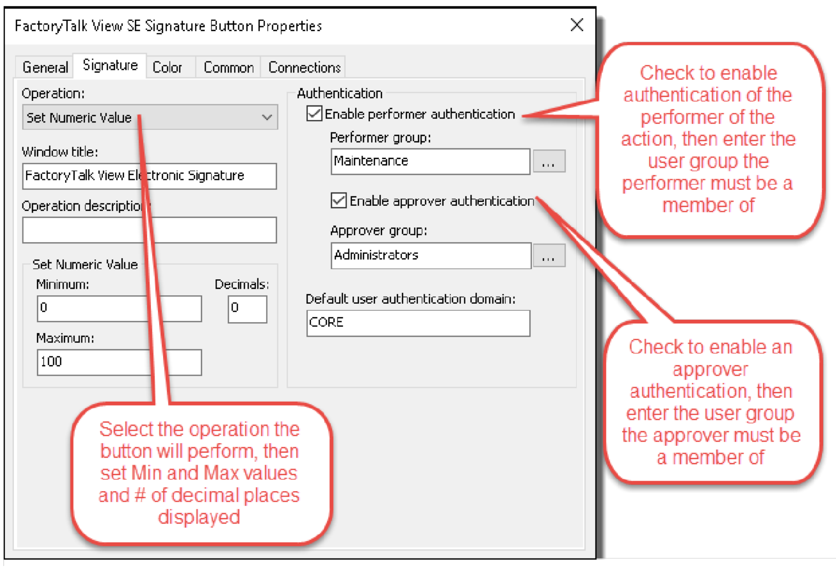

FIG 31. Signature button, signature properties.

Connections tab

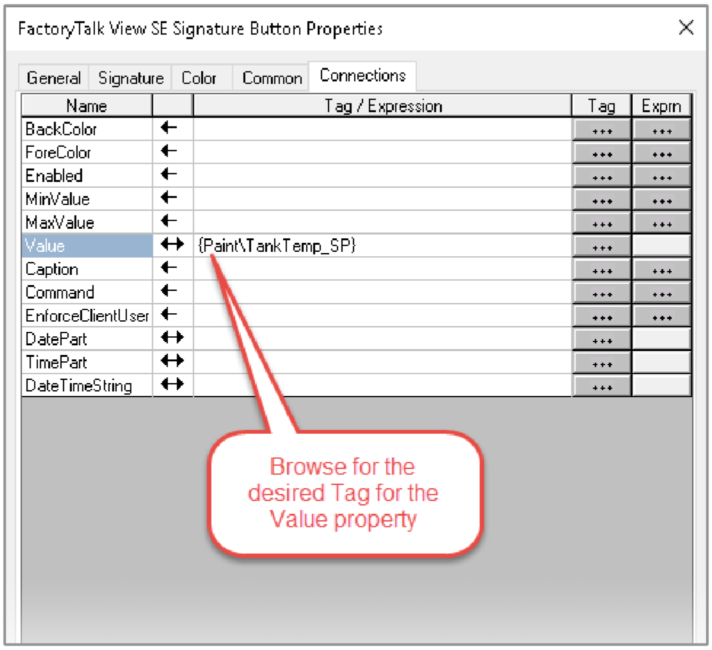

FIG 32. Signature button, connection properties.

6 Click *OK* to close the Signature Button Properties dialog box.

7 Test-run the display in FactoryTalk® View Studio. Click the Signature Button to show the FactoryTalk® View Electronic Signature runtime dialog window and complete the information fields that pop up. You must have the user groups configured and be logged in as a user that is a member of the designated "Performer" group to initiate the action.

8 Check the Diagnostics List to see the entries documenting successful and unsuccessful setpoint changes.

9 Close the display when you are done testing the signature button.

10 To test the display in the client, configure a FactoryTalk® View SE client.

Configure diagnostics and message routing

Regardless of which object is being used with the electronic signature feature, message destinations must be configured so that the audit messages generated are routed properly. See the *section Log all FactoryTalk® View SE activity to a central FactoryTalk® AssetCentre or ODBC database* for guidance on message routing.

> Applies to: ThinManager®, Version 13.00.00 through 14.00.00

And FactoryTalk® View SE electronic signature capabilities, ThinManager® also supports electronic signature, or E Signature, functionality with logging to FactoryTalk® AssetCentre or a SQL-compliant ODBC database. Logging of the E Signature events are possible through FactoryTalk® View SE with VBA code.

> ThinManager®: For additional information on using ThinManager® with E Signature events, refer to the ThinManager® Events White Paper.

Considerations for implementing electronic signatures with recipe management
A user can require features for recipe management from within the HMI, integrated with electronic signatures. A common solution for recipe implementation can include FactoryTalk® View SE integration to an ODBC recipe database, using FactoryTalk® Transaction Manager or custom PowerShell or VBA scripting to facilitate the recipe database connection. With this solution, FactoryTalk® View SE HMI objects, configured to require electronic signatures, can be used to initiate the recipe upload, download, modification, and more for a compliant recipe management solution.

For systems that require less complex parameter management, the FactoryTalk® View SE built-in tool, Recipe Pro+, can be used to provide a commercial off-the-shelf for parameter management. This includes storage of parameter values in a Recipe Pro+ file within the HMI project, and Recipe Pro commands to initiate download or upload of parameters. With this option, FactoryTalk® View SE HMI objects, configured to require electronic signatures, can be used to initiate the parameter download or upload. This option is most suitable in applications where parameters are not changed frequently and do not require version management, such as machine parameters. Consideration can be given to the use of the Recipe Pro+ Editor object to create, duplicate, edit, and preview the recipes, which provide broad access for recipe management for authorized users without reverification signoff.

Use version Control software

> Applies to: FactoryTalk® View SE, Versions 11.00.00 through 15.00.00; FactoryTalk® AssetCentre, Versions 11.00.00 through 13.00.00

FactoryTalk® AssetCentre can be used to track revisions to your FactoryTalk® View SE projects. FactoryTalk® AssetCentre provides preferred integration with FactoryTalk® View SE and other Rockwell Automation software products. Version control software such as FactoryTalk® AssetCentre retains all project components in a central repository for safekeeping. To modify any portion of the project, a user must check out the component. The version control software logs the username, component, and checkout date and time. The user modifies the component in FactoryTalk® View SE, closes FactoryTalk® View SE, and then checks the component back in. The version control software logs the username, component, and checks in date and time, and allows the user to add comments explaining the modifications. Electronic workflows can also be implemented, requiring review and approval of check-in and check out, with Archive Management of Change. This provides you with a record of all changes you made and when you made them. You can also have access to both the old and new versions of the checked-out component.

The following enhanced integration features are enabled when used with FactoryTalk® AssetCentre:

Project management and disaster recovery with FactoryTalk® AssetCentre
FactoryTalk® AssetCentre includes asset support for FactoryTalk® View SE for fully automated application backup, version management, and a compare report showing changes between versions. The asset is included with FactoryTalk® AssetCentre Disaster Recovery for Rockwell Automation. The asset leverages the enhanced Application Manager with FactoryTalk® View SE, with the ability to back up running projects; no need to shut down an HMI application to back up.

> FactoryTalk® AssetCentre: For additional information on applying FactoryTalk® AssetCentre in a 21 CFR Part 11 environment, refer to Guidelines for applying FactoryTalk® AssetCentre in a 21 CFR part 11 environment.

Configuring Time Synchronization in a FactoryTalk® View SE environment

> Applies to: FactoryTalk® View SE, Versions 11.00.00 through 15.00.00

FactoryTalk® View SE 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® View SE environment, including FactoryTalk® 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® View SE client.

> FactoryTalk® View SE: For additional information on FactoryTalk® View SE Distributed System design considerations, refer to the Rockwell Automation Knowledgebase Document ID: IN3416 - FactoryTalk View SE Distributed System Design Considerations.

When integrating FactoryTalk® View SE with FactoryTalk® Alarms and Events, synchronization of the controller to an authoritative time server is also required to enable accurate time stamps for FactoryTalk® Alarms and Events. One method of synchronizing the controller within an Integrated Architecture® is to use CIP Sync over the Ethernet network. In this case, consideration can be given to the architecture, hardware selection, and configurations required to support implementation of CIP Sync.

> Time Synchronization: For additional information about implementing time synchronization of the controller, refer to Knowledgebase Document ID: QA8202 - Controller Clock setting and time synchronization between racks, ControlLogix® (various methods). For additional information on time synchronization and CIP Sync, refer to the manual, Integrated Architecture® and CIP Sync Configuration.

Use of Visual Basic for Application code and Scripts in FactoryTalk® View SE

> Applies to: FactoryTalk® View SE, Versions 11.00.00 through 15.00.00

FactoryTalk® View SE provides users the ability to integrate its graphics with Visual Basic for Application (VBA) and integrate Scripts on the HMI server for custom scripting, external application integration, and more. While VBA and Scripts provide powerful tools for application development, consideration can be given on the impact on risk and testing associated with highly custom code.

As described by Good Automated Manufacturing Practice (GAMP) methodologies published by the International Society of Pharmaceutical Engineers (ISPE), as complexity of the computerized system increases, risk to the system functionality increases. After, with increased risk, the requirements and complexity of functional testing can also increase. This is reflected in the GAMP-5 categorization of computer systems (Categories 1...5); Category 1 yields the least risk while Category 5 yields the most risk concerning computerized system validation. The final decision to define the category is up to the End User and determined based on the complexity of the End User's system.

To reduce complexity of the computerized system, in line with GAMP-5 guidance and methodologies, it is recommended that the use of Scripts and VBA is limited to essential functionalities that cannot be performed through other built-in, configurable methods. Rockwell Automation also provides standardized programming solutions, such as the Library of Process Objects as part of PlantPAx®, to reduce customization and risk.

> Library of Projects Objects, Version 5.0: For additional information about using the Library of Process Objects, refer to the white paper, Compliance Guidance for Validated Industries with Library of Process Object 5.0.

When implementing scripts, consideration can be given to the impact of script execution on computer resource utilization. Scripts can be configured to run on a shared thread (synchronous) or on its own thread (asynchronous). VBA runs on a shared, single thread and called in response to events that occur in a graphic display at runtime. As requests are called and queued, there are variable limits to what the queue can hold. Because of this, the Scripts and VBA code can be short, concise, and not continuously running.

An example of VBA code that can be implemented concisely includes the creation of additional security prompts. In this case, a sign in macro or button action can be created that requires the operator to enter a separate piece of information or answer a question to validate the sign in ID. The user's response can be examined in VBA code to determine whether the signs in ID and password are being used improperly. If so, the information can be reported immediately to system security and/or management.

> FactoryTalk® View SE: For additional information about using Scripts and VBA in FactoryTalk® View SE, refer to the FactoryTalk® View SE User's Guide.

Highlights in Version History

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

Version		Highlights
15.00.00	Application Security	Version 15.00 adds the ability for the administrator to customize the HMI Project Folder path for enhanced data security and prevention of unauthorized modifications to the HMI application.
14.00.00	Enhanced E-signature options	Version 14.00 adds E-signature functionality to built-in maintained button, latched button, interlocked button, ramp button, control list selector, and piloted control list selector objects, with options for customized diagnostic audit messages, building on built-in object e-signature capabilities. Embedded variables that are numeric, string, and date and time are supported in electronic signature confirmation messages.
	Improved system security resiliency and management	Starting with FactoryTalk® Services Platform version 6.40, compatible with FactoryTalk® View SE version 14.00, 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.
13.00.00	Enhanced E-signature and Diagnostic Audit Message options	Version 13.00 adds E-signature functionality to built-in multistate button objects, with options for customized diagnostic audit messages extended to string inputs, building on built-in object e-signature capabilities.
12.00.00	Enhanced Diagnostic Audit Message options	Version 12.00 adds options for customized diagnostic audit messages for numeric inputs when setting a tag value. For example, the current value and new value can be included in the audit message.
11.00.00	Application backup and disaster recovery	FactoryTalk® View SE, starting with version 11.00, provides an enhanced Application Manager that supports all application types and enables FactoryTalk® AssetCentre 9.00 and newer to automatically backup FactoryTalk® View SE Network Station and Network-Distributed Applications.
	Enhanced E-signature options	Version 11.00 adds E-signature functionality to built-in input, button, and list selector objects making e-signature authentication and approvals more flexible to implement.
	Visualize operator actions	FactoryTalk® View SE, starting with version 11.00, offers built-in objects to view operator actions through FactoryTalk® Diagnostics. When used with FactoryTalk® AssetCentre version 9.00 and newer, FactoryTalk® View SE enables plotting of audited operator actions and runtime comments along with time series data, system events, and alarms through use of the TrendPro trending object. This enhancement associates data points on a trend with related operator actions and information, providing a valuable tool for troubleshooting and decision-making. Historical data sources include both FactoryTalk® Historian SE and FactoryTalk® View SE data logs. Historical trending data is now available through FactoryTalk® ViewPoint 12.00.
	Centralized FactoryTalk® Alarms and Events	FactoryTalk® View SE, starting with version 11.00, standardizes use of FactoryTalk® Alarms & Events provide granular control, intuitive user interface (UI) components, and an integrated alarm history across the entire system.

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® View SE 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.

Publication FTALK-WP024D-EN-P – March 2025 | Supersedes Publication FTALK-WP024C-EN-P – February 2024