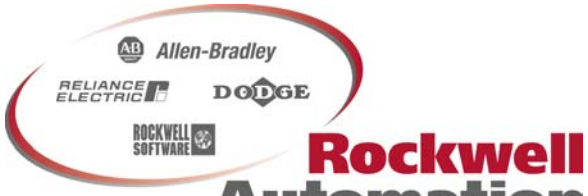
Industry White Paper

Compliance Information on 21 CFR Part 11



Bringing Together Leading Brands in Industrial Automation

Compliance Information on 21 CFR Part 11

Applying RSView SE in a 21 CFR Part 11 environment

About this document

RSView SE21 CFR Part 11 compliance statements

Applying RSView SE to the 21 CFR Part 11 regulation

- Limit access to computer hardware
- Take advantage of operating system security and domains
- Configure RSView SE user accounts to include Windows NT or 2000 users or groups.
- Change the Unspecified command security code from unlimited to restricted access
- Use a password-protected screen saver
- Prohibit access to RSView Studio, and to other software programs
- Use the DeskLock feature
- Secure RSView SE Client stations
- Log all RSView SE activity and alarms to a central ODBC/SQL database
- Use RSMACC or third-party version control software

Rockwell Products and 21 CFR Part 11

About Rockwell

- Participating in PDA Part 11 Task Group
- Completing internal gap analysis
- Publishing application notes

Detailed compliance statements

- General Provisions
- Food and Drug Administration

Compliance information

Applying RSView SE in a 21 CFR Part 11 environment

Rockwell Software, Visualization business unit

About this document

At Rockwell Software, we are often asked whether RSView Supervisory Edition complies with the electronic records and signatures portion of 21 CFR Part 11 (Title 21 – Code of Federal Regulations – Part 11). The short answer is "Yes." RSView Supervisory Edition has been designed to meet the needs of customers needing to comply with regulations such as 21 CFR Part 11. The long answer is that a software product in itself cannot be "compliant", but applied properly, can be part of a compliant system..

The main purpose of this document is to describe how to apply RSView SE in such a way that the end system meets the intent of the regulation. Rockwell Software's statement of compliance can be found on page 3 of this document and is titled "RSView SE-21 CFR Part 11 compliance statements. Guidelines on applying RSView SE can be found in the section titled "Applying RSView SE to the 21 CFR Part 11 regulation," beginning on page 5.

A copy of the 21 CFR Part 11 regulation, along with RSView-related comments, is included at the end of this document; see "Compliance Statement—Rockwell Products and 21 CFR Part 11," beginning on page 30.

RSView SE—21 CFR Part 11 compliance statements

A compliance statement for RSView SE appears below. For a copy of the 21 CFR Part 11 regulation and RSView SE-related comments, see "Compliance Statement—Rockwell Products and 21 CFR Part 11," beginning on page 30 of this document.

RSViewSupervisory Edition

RSView SE is a modular, distributed, client/server application that allows operators to open, configure, and interact locally or remotely with RSView SE applications from any computer on a network. An RSView SE application is used for monitoring and controlling automation machines and processes. Rockwell Software develops RSView SE using a sophisticated product development methodology. RSView SE was designed, developed and tested in unison with an advisory committee of life science customers whose focus was to help us create products to address 21 CFR Part 11 compliance. RSView SE version 2.1 or later can be used to build systems that meet FDA 21 CFR Part 11 regulations. Using a combination of RSView SE security, a Desklock feature, and Microsoft Windows NT or Windows 2000 domain security, a system can be created that prevents unauthorized access to data files and the operating system. RSView SE can send its activity log, alarm log, and data log information to an ODBC-compliant database such as Microsoft SQL Server or Oracle. For distributed server solutions, RSView SE can log from multiple servers into a single central ODBC-compliant database. These database packages have sophisticated security and backup features that can handle the RSView SE data in a way that meets the intent of these regulations.

RSView SE in Rockwell Software system

RSView SE and the FactoryTalk Platform

RSView SE uses FactoryTalk, a Rockwell Software framework that provides a preferred level of integration among products. One of the benefits it provides is the concept of "create tags once". This means that once tags are created in the PLC program, they can be used directly in RSView Supervisory Edition without having to create and maintain a separate tag database. Change management is seamless because of this architecture since the online or offline changes to the PLC program are controlled and logged via RSMACC, and those changes are then reflected automatically in RSView Supervisory Edition. The HMI program inherits changes to the tag database (ie. Addition of a tag, change to an element of a structure). So for example if the PV of a structure changes, this will be reflected in RSView. or take, for example, a tag needing to be added to the system. In a typical HMI system (without FactoryTalk), the PLC programmer would have to add a new tag to PLC program, which would be logged and documented, and a tag would also need to be added to the HMI system, which would also need to be logged and documented. With FactoryTalk, when the tag is added to the logic program, it is immediately available to RSView SE. There is no need to add it to the HMI tag database.

How RSMACC fits in

RSMACC (Rockwell Software Maintenance Automation Control Center) is software and services which are designed to control and track changes, measure asset health, and provide an audit trail RSMACC detects and records altered electronic files required to meet regulations like 21CFR Part 11. As we continue to help make compliance seamless for our customers, all Rockwell Software will use RSMACC to control design, operation, and maintenance changes and provide an audit trail. The RSMACC file management system allows users to archive, restrict and record the usage of any file in the system. Protect your intellectual property and manage validated programs by requiring users to check files in and out of the system. Version history on changes made to all files are recorded and stored. Validated projects can be easily marked. These files may be anything essential to the running of your plant - from PLC programs to PLC graphics to documentation and reports. RSMACC uses the Rockwell Software Security Server to proactively stop tampering before it even starts. Not only are features and functionality secured within supporting software packages, but users can also be restricted to which files and licenses they have access to.

While it is quite possible to put together a 21 CFR Part 11 compliant process without using RSMACC by using RSView SE and third party tools like SourceSafe, PVCS tracker, and paper procedures, RSMACC software and services can provide a better degree of functionality and integration.

Since the focus of this white paper is to describe how to use RSView SE to secure and log operator actions, track alarms, and log other operational data, RSMACC is not discussed in detail... See the RSMACC whitepaper "Applying RSMACC in a 21 CFR Part 11 Environment for more information on applying RSMACC to a 21 CFR Part 11 application

How FactoryTalk Diagnostics fits in

FactoryTalk Diagnostics provides a consistent way for Rockwell software products to log information to local logs, a central, system-wide repository, or RSMACC. It allow routing of configuration change messages to RSMACC software and services. This functionality provides an audit trail throughout the automation system, including changes to PLCs and HMI.

.

Applying RSView SE to the 21 CFR Part 11 regulation

Use the list of tasks below to develop RSView SE projects that comply with the U.S. government's 21 CFR Part 11 regulation.

- Limit access to computer hardware
- Take advantage of RSView Supervisory Edition's architecture
- Take advantage of operating system security and domains
- Configure RSView SE user accounts to use Windows NT/2000 security
- Change the unspecified command security code from unlimited to restricted access
- Use a password-protected screen saver
- Configure RSView SE Clients to automatically log out
- Prohibit access RSView Studio, and other software programs
- Restrict access to the application
- Use Windows account password aging and management
- Users log on requirements for computers in an RSView SE environment
- Use NTFS or other secure file system
- Set up the DeskLock feature
- Do not allow operator access to Help
- Secure RSView SE Client stations
- Log all system activity through FactoryTalk Diagnostics
- Log all RSView SE alarms to a central ODBC/SQL database
- Set up Data Logging
- Create an ODBC data source to serve as a central database
- Set up re-verification of operator identity, or supervisor signoff
- Set up Redundancy
- Use version control software

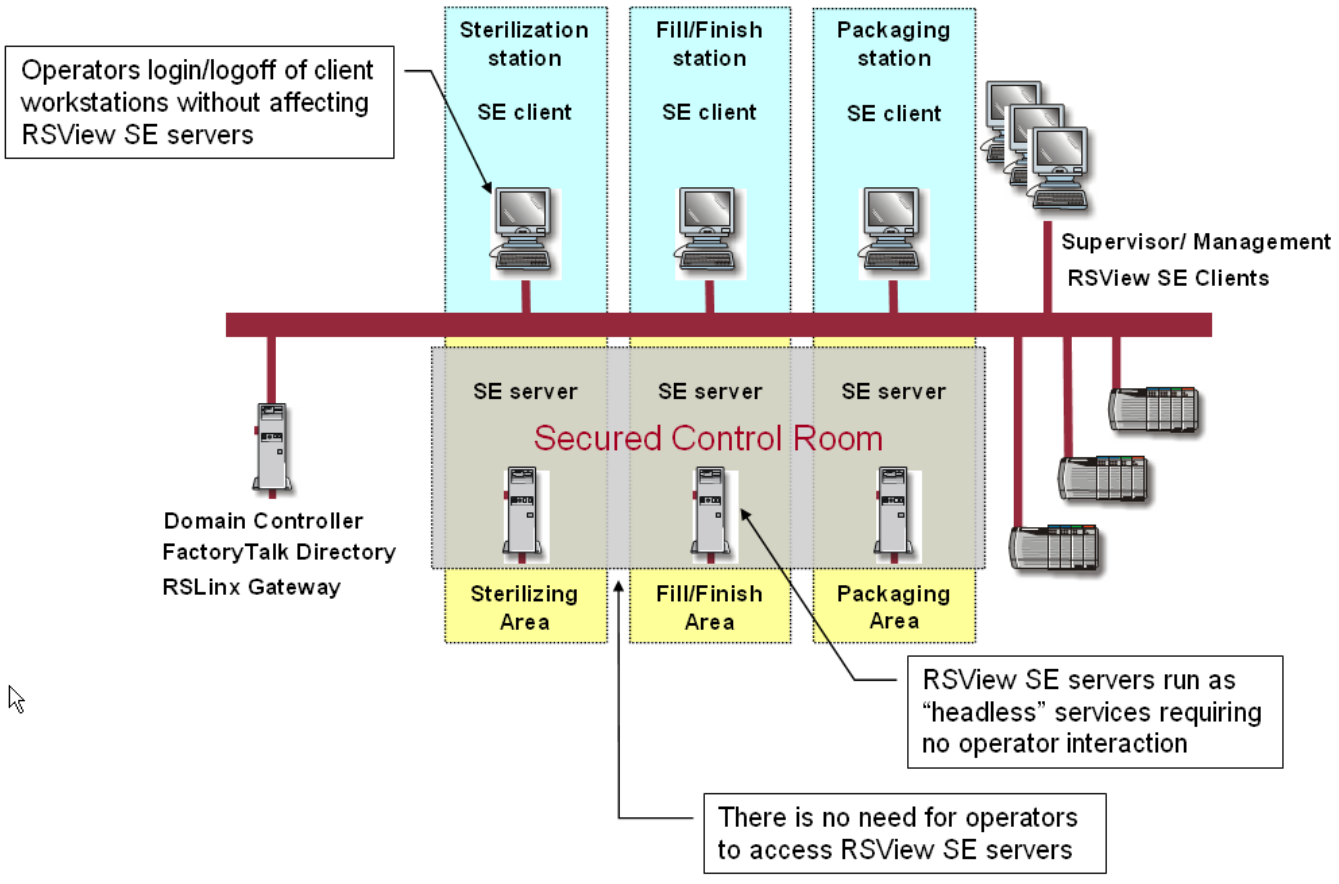
Limit access to computer hardware

Software such as Windows operating systems and RSView SE run on computer hardware; it's essential to limit operator access to this hardware. In general, an operator's only access to the computer should be via the keyboard, mouse, or touch screen. An operator with access to the power switch and a bootable disk or CD-ROM 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 protect your hardware systems.

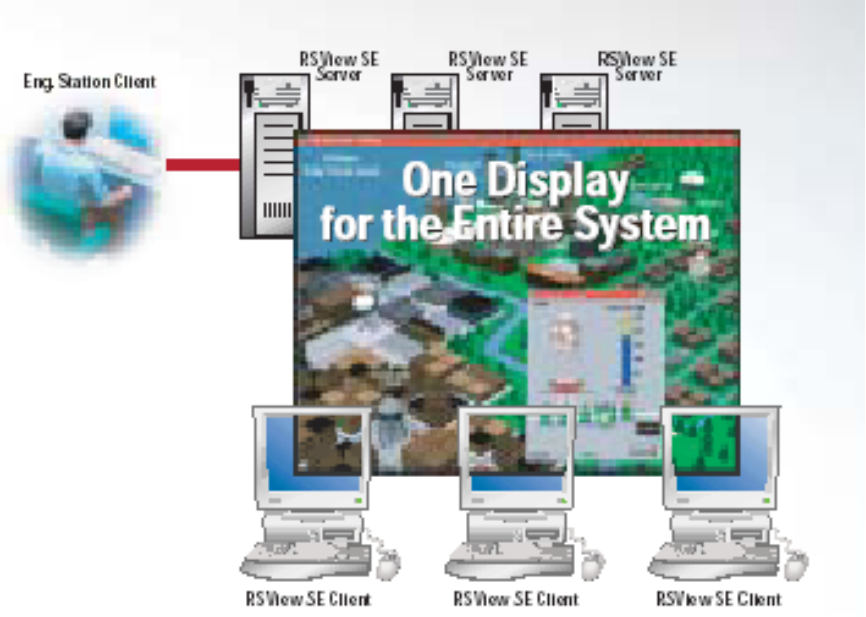
Take advantage of RSView Supervisory Edition's architecture

RSView SE Servers run as services. Since they run as services, they do not require any user to be logged on to the computer that is running the RSView SE Server. Clients can log in and out of the RSView SE Client stations without affecting the computer or software components of the RSView SE Servers. Windows password aging and management can be used at the clients while the servers are running a continuous operation. Operators at the RSView SE Client stations have no way to alter server processes or shut down the server operation. 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 onto the computer.



Create Displays Once

RSView SE requires that displays are only created, edited, and maintained in one place in a distributed application. Unique displays are stored on servers and are available to all servers and clients in the application. Since displays are maintained only in one place rather than being stored and maintained in multiple locations, changes to application are easier to manage.

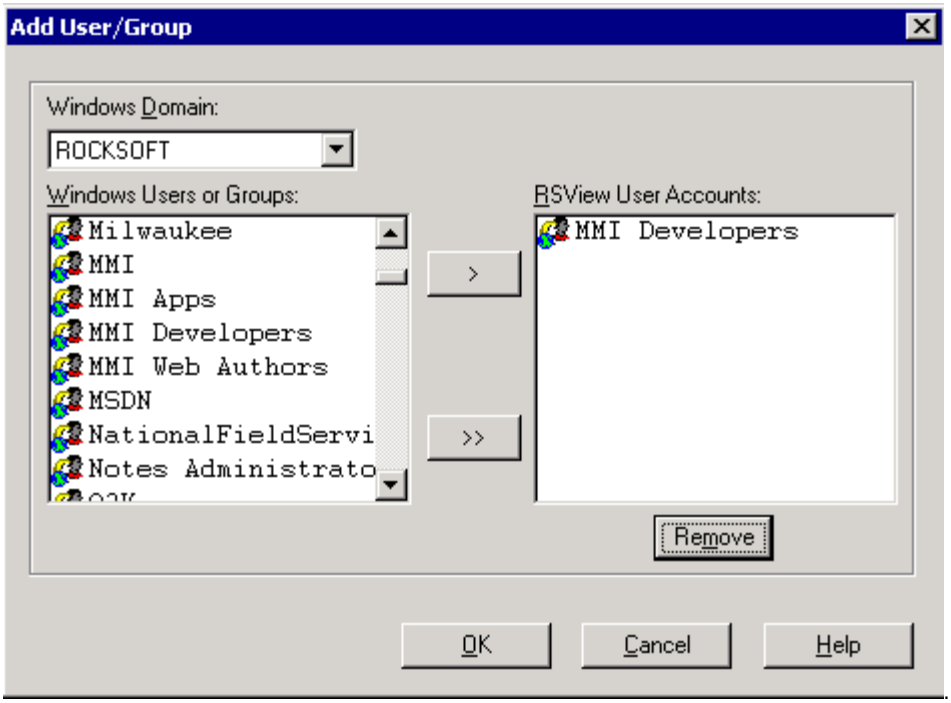


Take advantage of operating system security and domains

RSView SE makes efficient use of the security features built into the underlying Windows 2000 operating systems. For compliance, all RSView SE computers in a closed system must be part of the same Windows NT/2000 domain. All RSView SE computers must run Windows 2000 or XP Professional or Windows 2000 Server. Windows NT, 2000 and XP encrypt passwords using the operating system's built-in encryption mechanisms.

Configure RSView SE user accounts to use Windows NT/2000 security

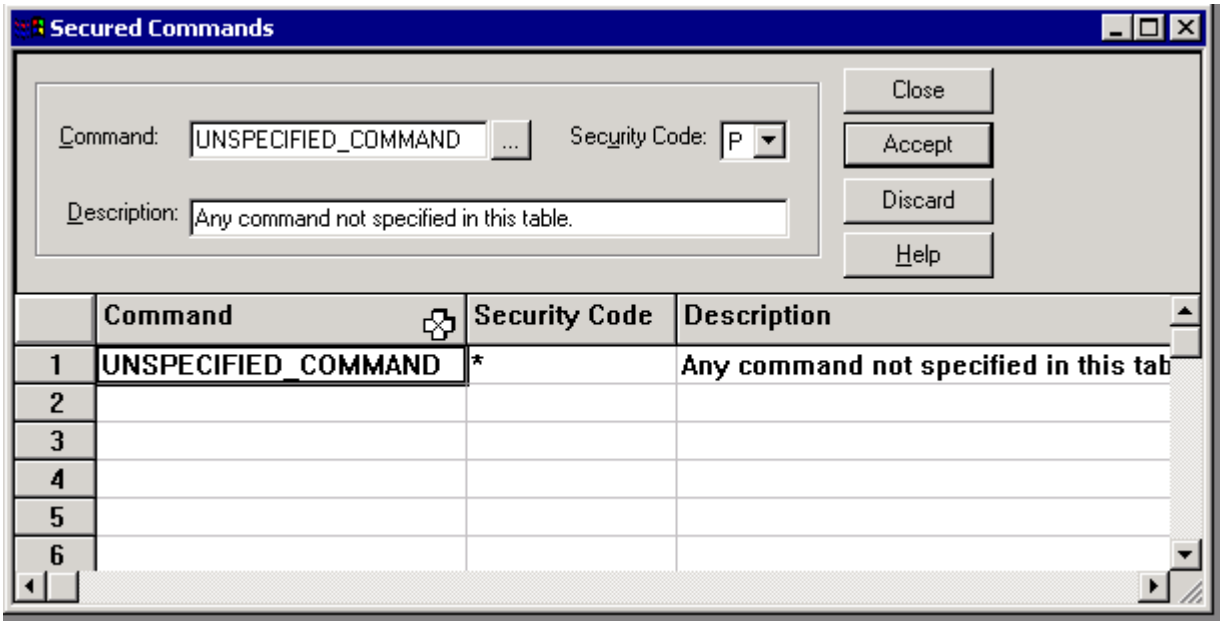
To configure RSView SE Security to use Windows NT/2000 security, from the RSView SE Application Explorer, open the RSView SE User Accounts editor. From the Setup menu select Add NT users or groups.



Manually select and add only a subset of the Windows NT/2000 users and groups to RSView SE. When you start an RSView SE project, the current Windows NT or Windows 2000 user is logged into RSView SE if that user also has an RSView SE user account.

Change the unspecified command security code from unlimited to restricted access

In the Secured Commands editor, set the security code for unspecified commands to something other than *. Choose a unique security code, such as P, that you do not assign to any other users.Changing the default security code from * to a unique code causes each RSView SE command, macro, graphic display, OLE verb, and tag to require security by default. If no other users have access to security code P, then every user is restricted from all items except those specifically allowed in the Secured Commands editor.



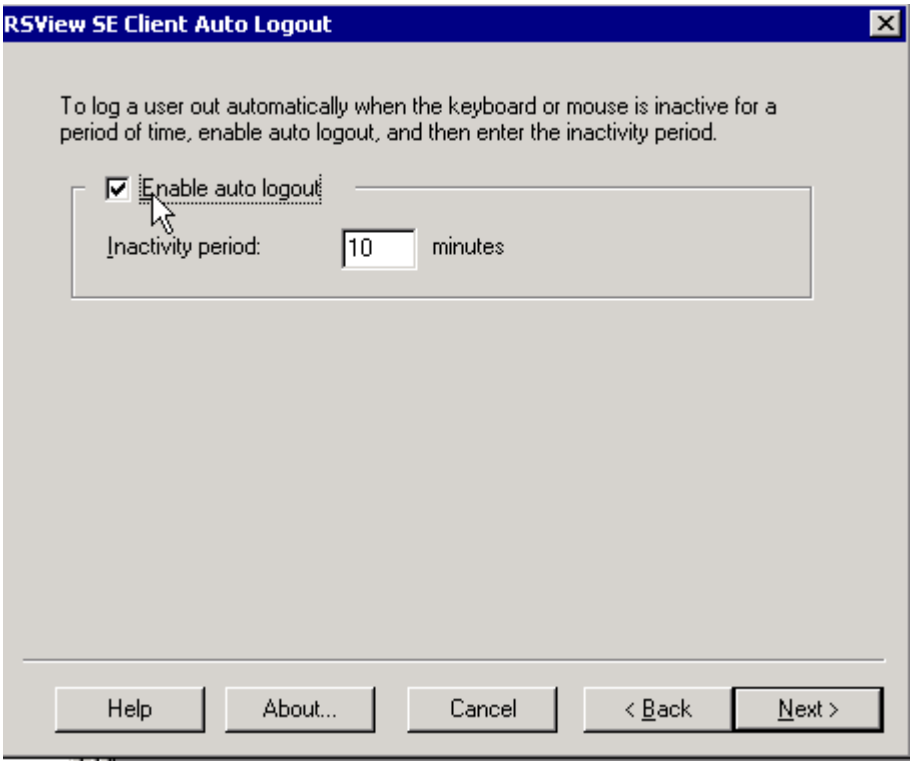
Use a password-protected screen saver

To ensure that a workstation in a closed system is not left unattended, use a Windows XP/2000 password-protected screen saver for all RSView SE Clients. To configure screen savers, from the Windows Control Panel, select Display, and click the Screen Savers tab. Add password protection to the screen saver.

Because server components run as services, with no need for Windows logon, it is not necessary to use password-protected screen savers on the RSView SE HMI Server or FactoryTalk directory computer.

Configure RSView SE Clients to automatically log out after user inactivity

For some installations, the password-protected screen saver is not enough protection. In these cases, RSView SE Clients can be configured to automatically log out after a specified period of time. This will log them out of RSView SE client, not out of their Windows session. There is also an option available that will log the current user out and log a generic user in after it is detected that a user is idle for a specified period of time. See theRockwell Software Knowledgbase for more information.



Prohibit access to RSView Studio, and other software programs

RSView Studio, the design environment for RSView Supervisory Edition, is not intended for use by operators. They should not be given access to RSView Studio. The easiest way to do this is to not install RSView Studio on operator computers. If it is necessary to install RSView Studio on these computers, it should be secured using Desklock

Restrict access to the application

RSView Studio is used to edit a user application. Security can be applied to the application through the standard RSView Studio security options described later in this document. To restrict users from making unauthorized, changes to the application, it is recommended that access be restricted to users that are assigned with appropriate security.

Use Windows account password aging and management

User account and password management and aging is done using Windows 2000 Server. User accounts and passwords should be set up so that the passwords expire after a certain time, and with appropriate lockouts after multiple failed login attempts. This information is usually part of a company IT department Standard Operating Procedure, or SOP. For more information, refer to your Windows NT or 2000 Server documentation.

An operator at an RSView SE client can log off of RSView SE and off of Windows without affecting the RSView SE servers or other parts of the system. Where possible, operators should be required to log completely off Windows.

Users log on requirements for computers in an RSView SE environment

Each user must log onto the Windows 2000 or XP computer at the start of their session, and log out when they are done. Since RSView SE's server components run as a service, it is not necessary to have any user logged on to computers which are used as an HMI Server or FactoryTalk Directory. The RSView SE Server station should not be used as an Operator station.

Computers that are used as RSView SE Display Clients must have the actual operator log on to the computer. Do not allow the operator to allow anyone else to perform operations using their user name and password. If it is necessary for a supervisor to perform or approve certain operations, a different computer should be used. If the same computer is used, the operator should log off Windows, and the supervisor should log on. In cases where two signatures are required (ie. operator and supervisor), the approval will take place through a verification feature while the operator remains logged in to the system.

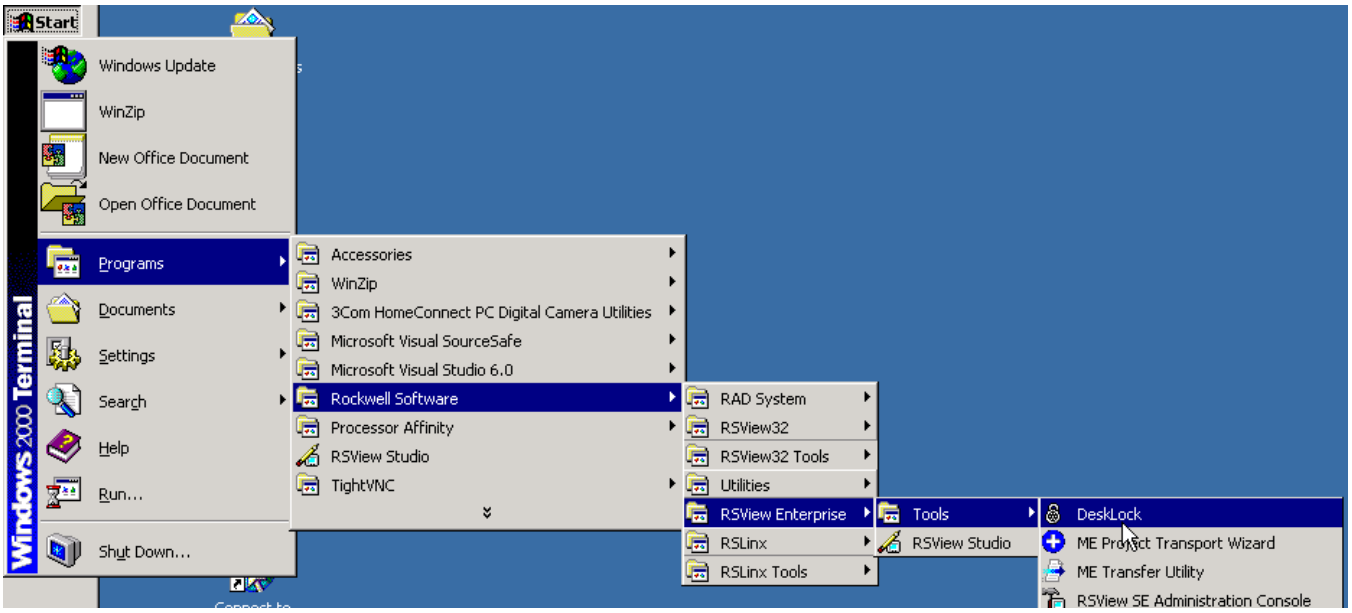
Use NTFS or other secure file system

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

Set up the DeskLock feature

To ensure that operators remain within a closed environment while running RSView SE, use the DeskLock feature. Used in conjunction with disabling switching to other applications and other security configurations noted in the DeskLock documentation, it is possible to lock operators into a closed RSView SE runtime system. The DeskLock feature and accompanying documentation are available from the RSView EnterpriseTools, which install with the RSView SE software.

Important. Before implementing the DeskLock Lock feature, carefully read the documentation. DeskLock can have far-reaching effects on your operating system. Its purpose is to replace the standard Windows 2000 desktop with a customized one intended to 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 2000 Policies.



Do not allow operator access to Help

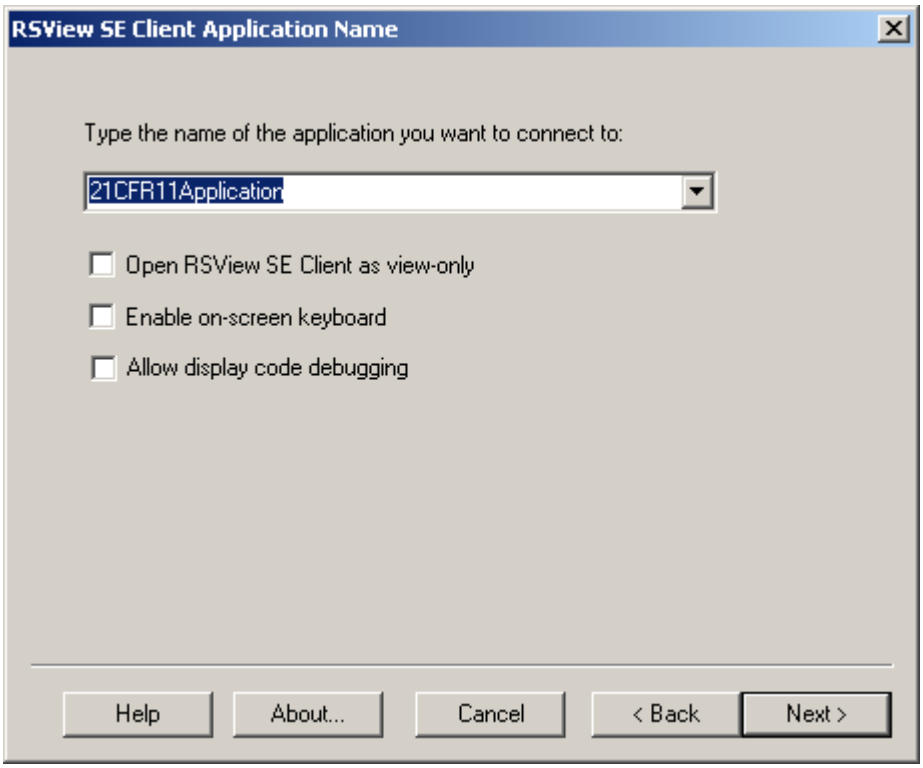
The Windows Help system is not secure, and once in help, a user can get full access to the underlying file system (still limited by their Windows account). Do not allow operator access to Windows Help.

Help can be restricted by using a combination of Desklock and overriding the F1 help keys in the RSView application. It can also be restricted using Win2000 security on the help executables.

Secure RSView SE Display Client stations

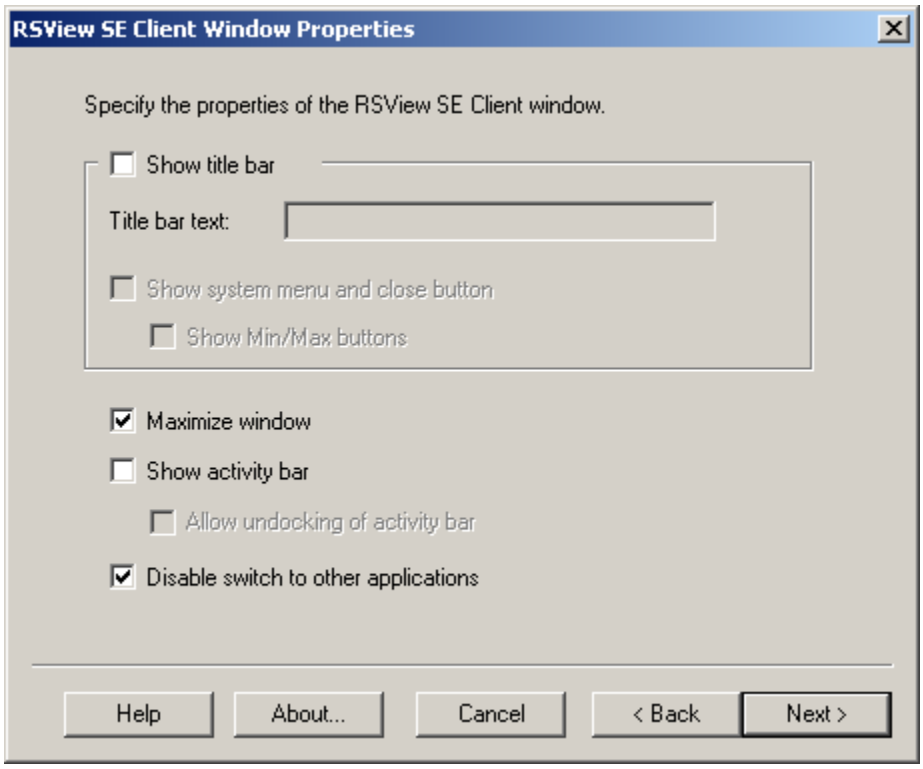
Configure clients with the following settings in the RSView SE client wizard.

RSView SE Client Application name window



- **Do not allow display code debugging.** This will allow the launching of the VBA editor, which is not secure.

In the RSView SE client window properties, disable switching to other applications, and maximize the window.

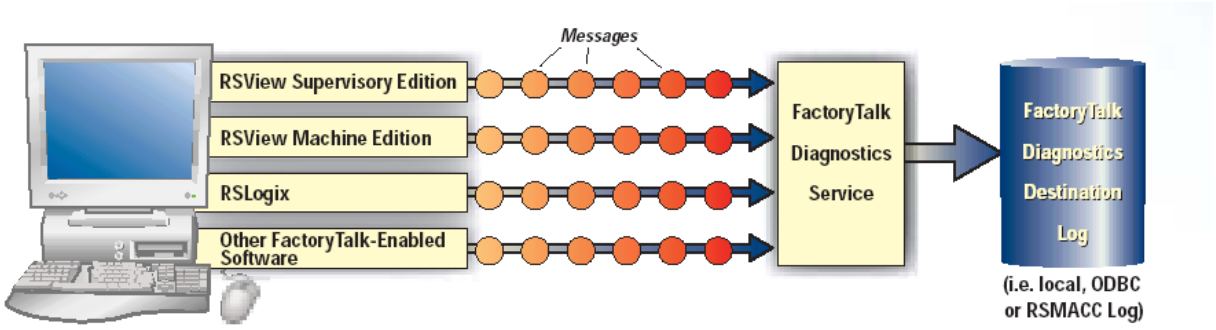


- **Show title bar**—enable only if necessary
- **Show System menu and close button** – disable to prevent operators from closing window
- **Maximize window**—enable; prevents operators from seeing or clicking items on the desktop
- **Disable switch to other applications**—enable; prevents operators from switching to other applications
- **Show Activity Bar** – enable only if necessary

In addition, use the DeskLock feature on the computer running the RSView SE Client and configure it to launch only the RSView SE client window.

Log all system activity through FactoryTalk Diagnostics

FactoryTalk Diagnostics allows you to collect, store, and examine messages from multiple Factory Talk-enabled products in a single, central location on each computer where the service is installed. So, for example, messages from RSLogix, RSView Machine Edition, RSView Supervisory Edition, and other FactoryTalk enabled products, can be routed to a single repository such as a local log, a secure database, or RSMACC.



To ensure the integrity of RSView SE activity data while still providing a backup if a central database is temporarily unavailable, use the FactoryTalk ODBC central logging capability. Should the central database be temporarily unavailable, the local logs serve as backup buffers until the central database connection is restored.

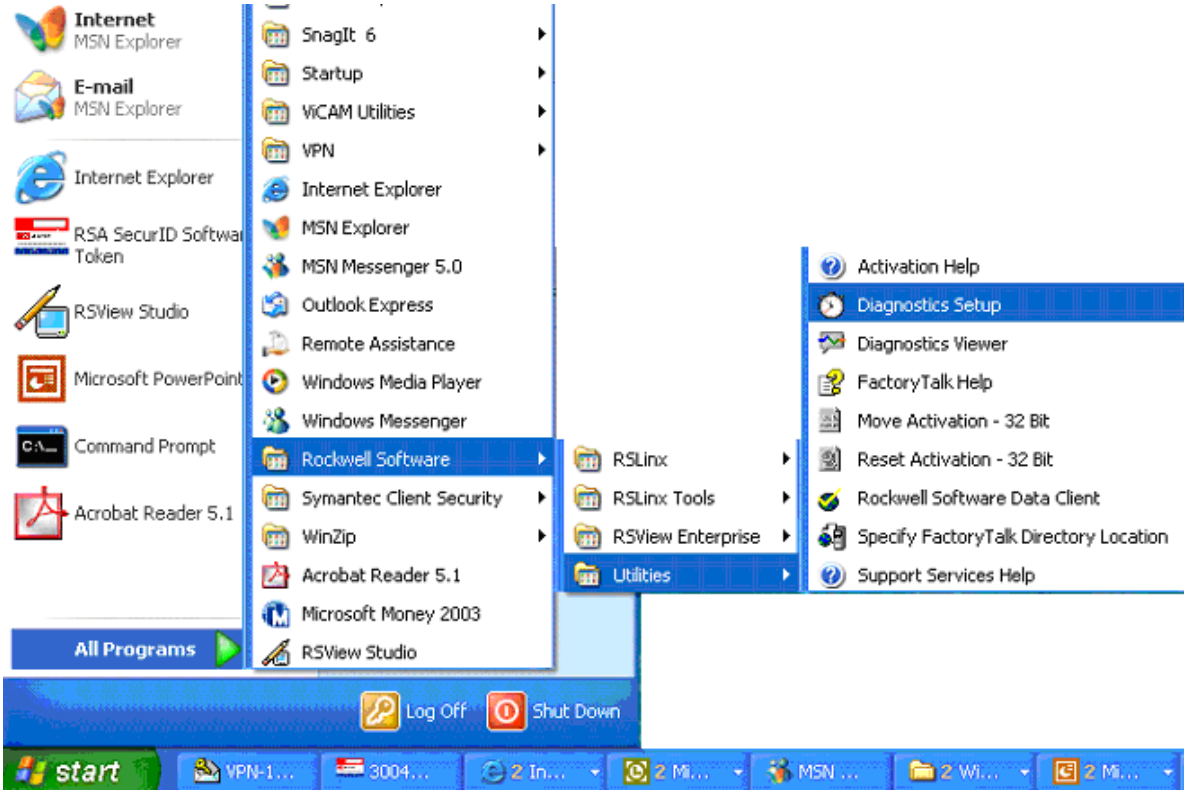
Note that the local FactoryTalk Diagnostic viewer will only access the information in the local buffer files, not the historical information that has been sent to the central database.

To use this system, follow the steps below to:

- configure the FactoryTalk Diagnostic Log
- set up a SQL Server or Oracle database
- create an ODBC data source to serve as the central database

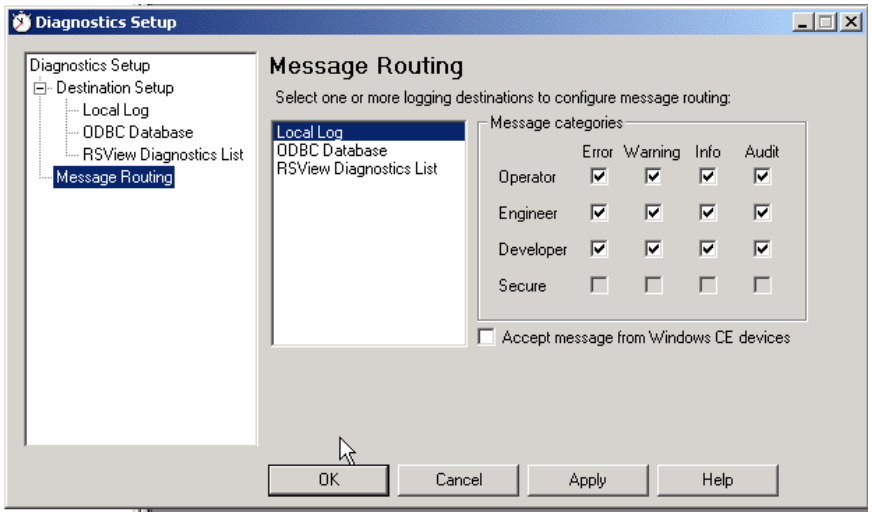
Configure the FactoryTalk Diagnostic Setup

1. From the Start Menu, choose Programs> Rockwell Software> Utilities> Diagnostics Setup.



2. Configure where you would like messages to be routed.

Use the Message Routing window to specify which categories of messages should be routed to each logging destination available on your computer. The options available to you are specific for each logging destination installed on your computer.



Each FactoryTalk-enabled product categorizes the messages that it generates using a matrix of Severity options (Error, Warning, Information, and Audit) together with Audience options (Operator, Engineer, Developer, and Secure). For example, a product might generate a series of security messages classified as Operator-Audit and Operator-Information, and also generate a series of communication messages classified as Operator-Warning, Engineer-Warning, and Developer-Error.

For example, to zero in on a problem, a plant manager might configure the Local Log on his computer to log only “Error” and “Warning” messages and ignore “Information” and “Audit” messages. On another computer, an automation system developer might want to configure the Local Log to log only messages categorized as “Engineer” messages.

Set up Secure Message category

Each FactoryTalk-enabled product classifies its own set of messages and defines the meaning of the options to fit its own purposes. Messages can be defined for particular audiences, such as operator, engineer, and developer. The **Secure** audience is reserved for messages which need to be protected and retained based on the U.S. government's 21CFR Part 11 specification for storing electronic records. Messages assigned this message type are logged to a logging destination provided by Rockwell Automation's RSMACC ™ software product.

Set up Severity options

Error. Typically, this option is assigned to the most serious kind of error message that logs events triggered by significant problems.

Warning. Typically, this option is assigned to messages that are not necessarily significant but that may cause future problems.

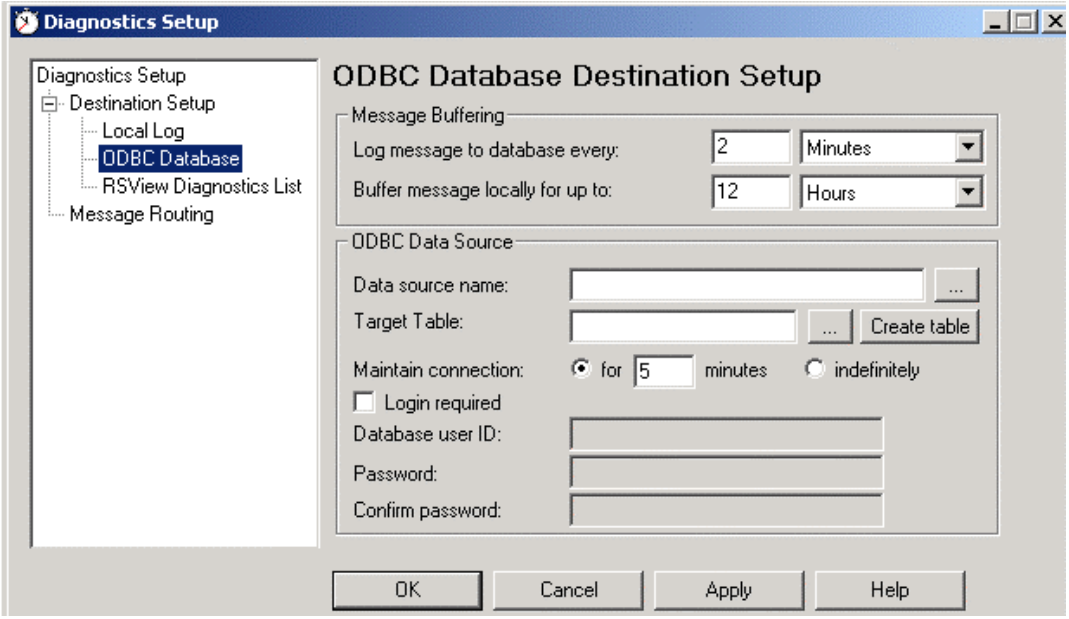
Information. Typically, this option is assigned to messages that document the essential purpose of the FactoryTalk-enabled application, which supplement and add more detail to "Audit" messages.

Audit. Typically, this option is assigned to high-level "journal" type messages which indicate activities which are essential to the technology or application purpose.

FactoryTalk Diagnostics be configured to transmit activity logs to a central, secure, redundant database for the entire application

- RSView SE Clients
- RSView ME Stations
- RSLogix
- RSSQL (future)

3. Set up Central ODBC logging.



5. Set up message buffering so if communication with central database is lost, messages will be buffered until communication with database is restored.

Log all RSView SE alarms to a central ODBC/SQL database

To ensure the integrity of RSView SE alarm data while still providing a backup if the central database is temporarily unavailable, use the Central Logging ability of RSView SE. Should the central database be temporarily unavailable, the local logs serve as backup buffers until the central database connection is restored.

Note that RSView SE's own log file viewers will only access the information in the local buffer files, not the historical information that has been sent to the central database.

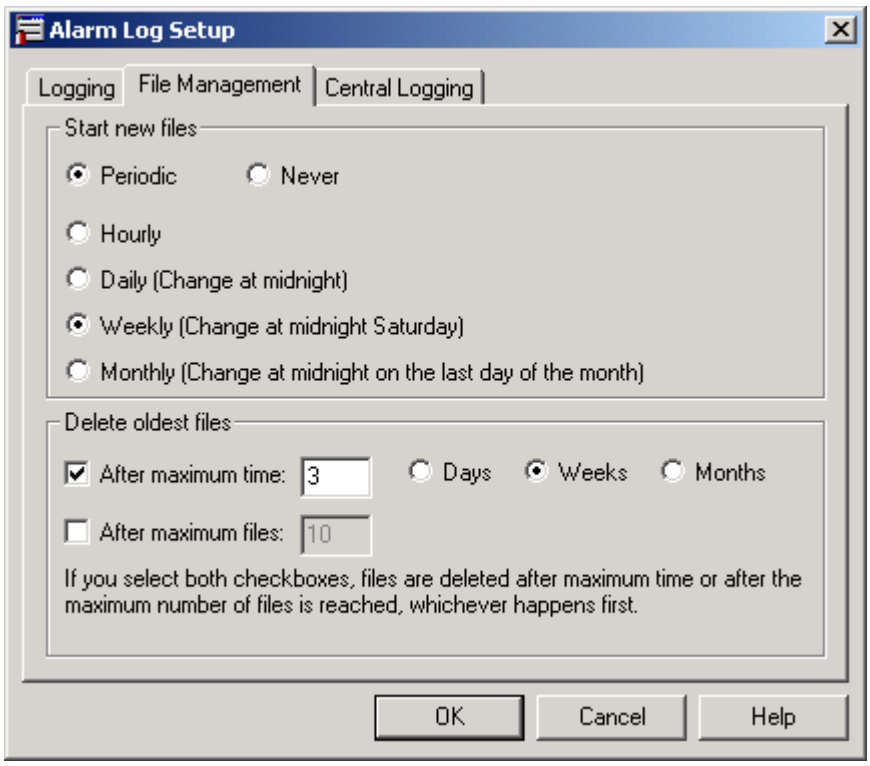
To use this system, follow the steps below to:

- configure the RSView SE Alarm Log
- set up a SQL Server or Oracle database
- create an ODBC data source to serve as the central database

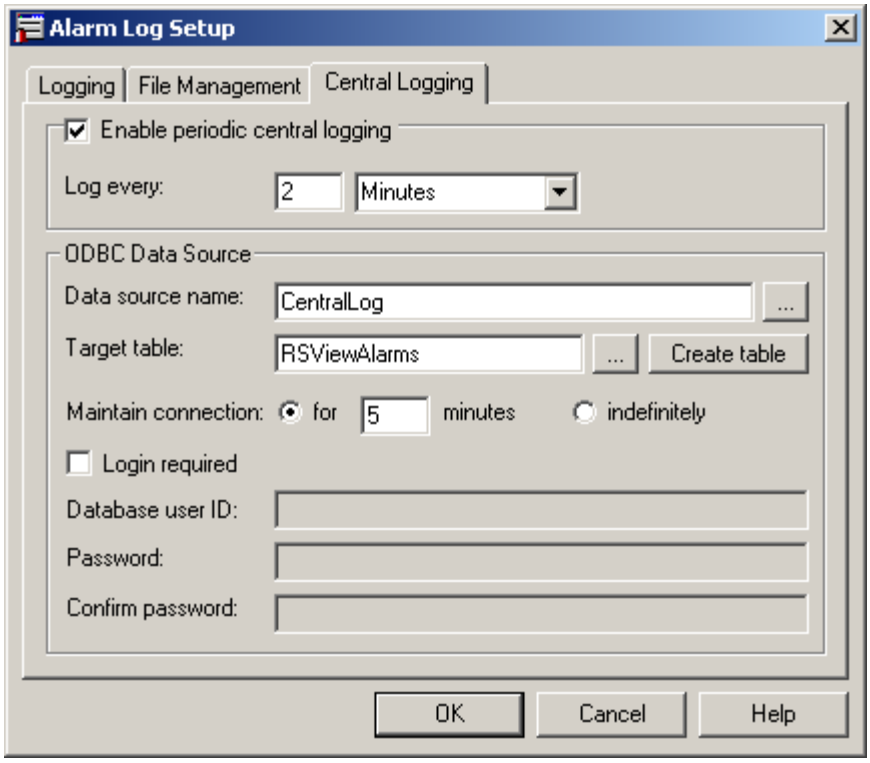
Configure the RSView SE Alarm Log

1. From the RSView SE Tools menu, open the Alarm Log Setup editor.
2. On the Setup tab, leave the default settings.
3. On the File Management tab, configure settings to start a new alarm log file once per week, and delete the oldest files after 3 weeks.

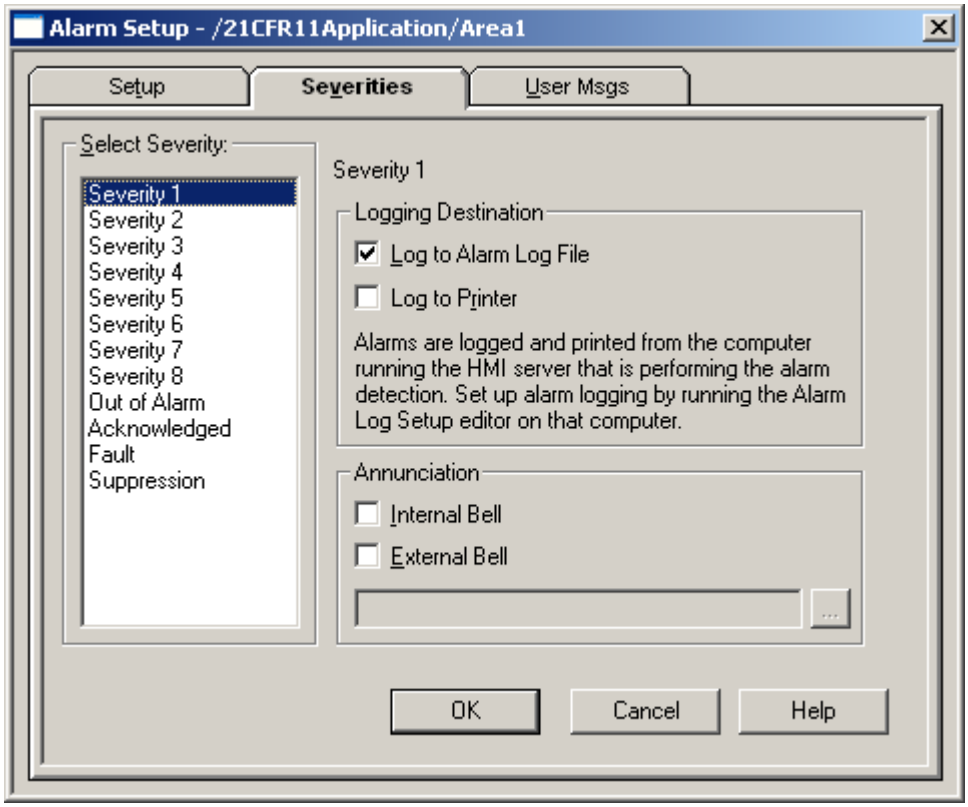
Note that this is not deleting records from the central database, but rather information from the local buffer. This should only be done after the information has already been sent to the central database. While it is possible to configure it to never delete these buffer files, realize that this would eventually fill up the hard drive unless some other method were used to delete files.



4. On the Central logging tab, enable periodic central logging every two minutes or less. Configure the ODBC data source to point to a SQL Server, Oracle, or other database. Configure it to maintain connections for at least twice as long as the logging period, or indefinitely. The login information does not need to be specified if the database allows NT Authentication, otherwise a valid database user ID and password must be specified



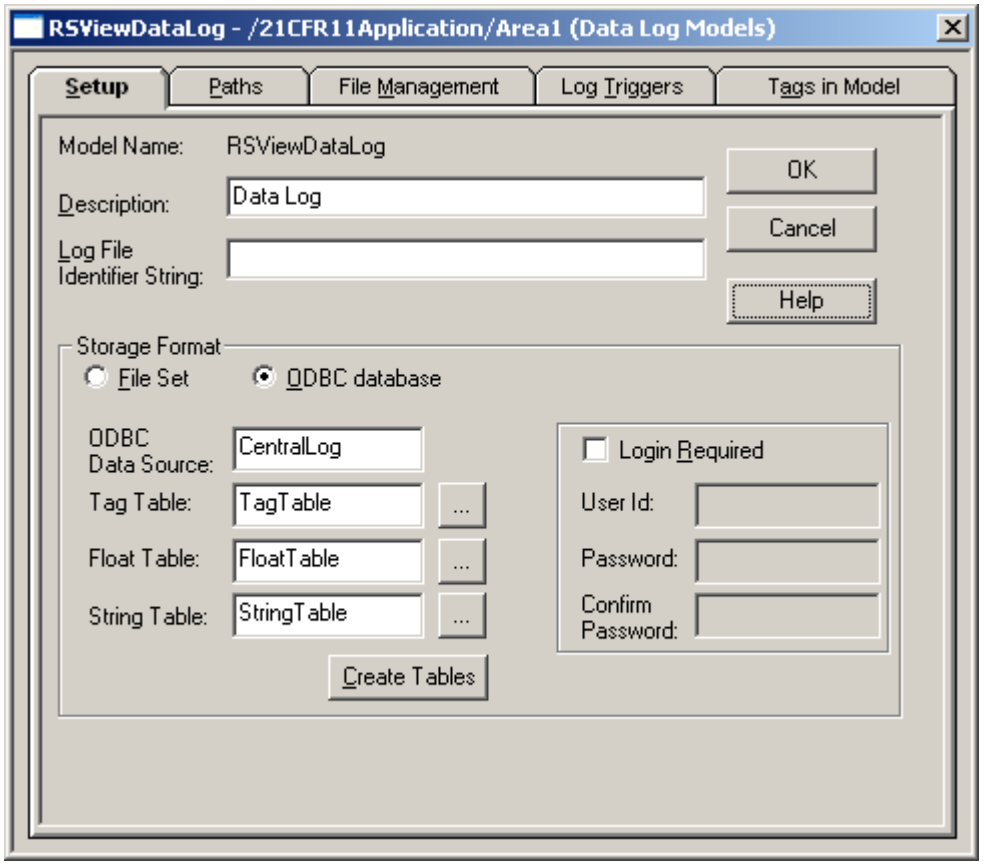
5. In the Alarm Setup editor, configure each severity to log to the alarm log file. Logging alarms to the printer is optional.



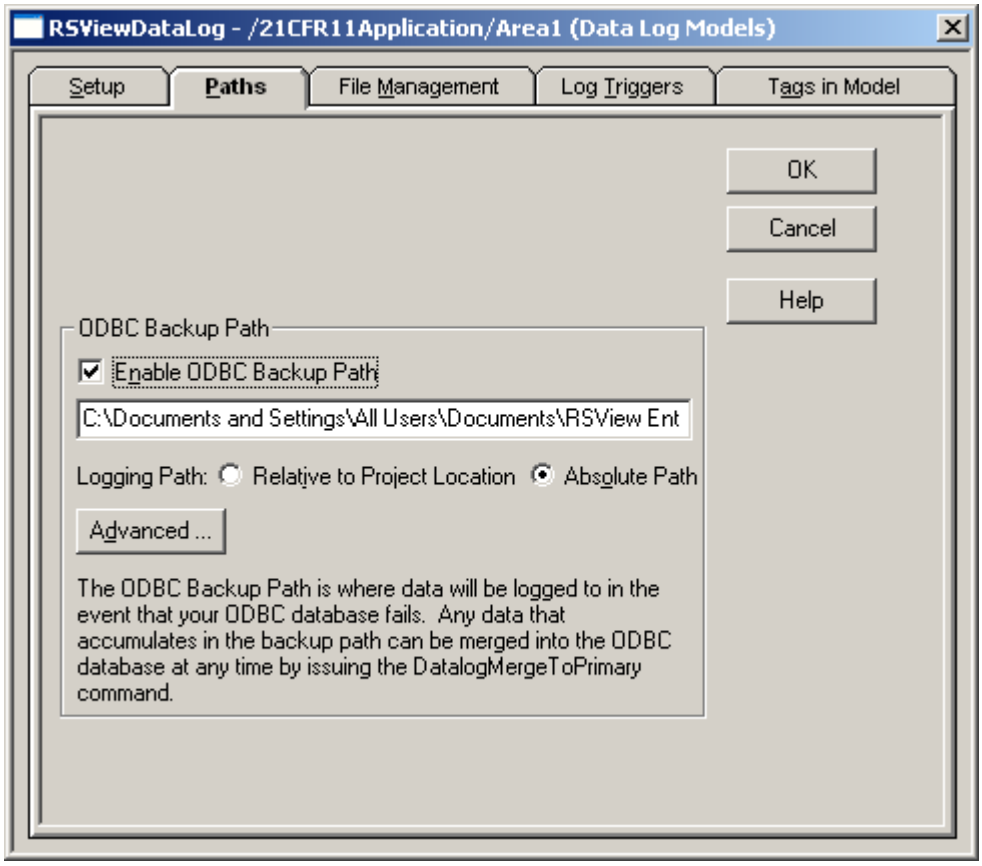
Set up Data Logging

If your application requires Data Logging, you will log t o a secure ODBC database.

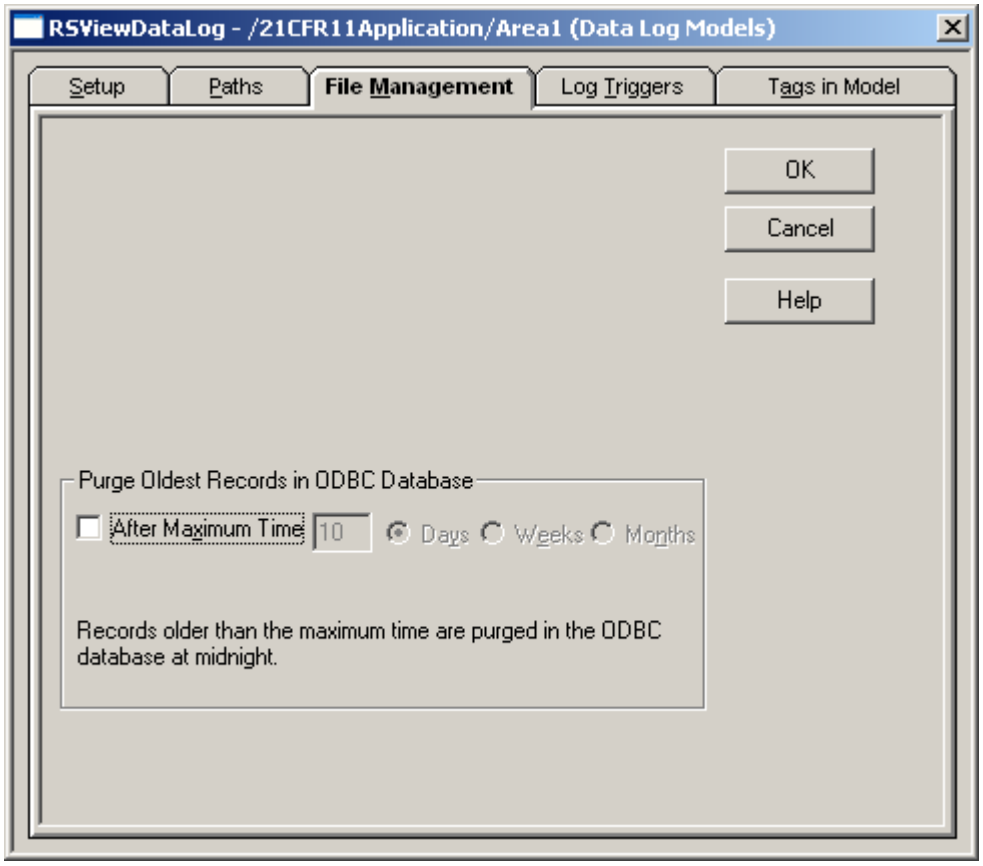
1. From the RSView SE Application Explorer, right click on Data Log Models, and click New.
2. On the Setup tab, select ODBC database as the storage format.



3. In the paths tab, configure an ODBC backup path. 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 Standard Operating Procedures



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

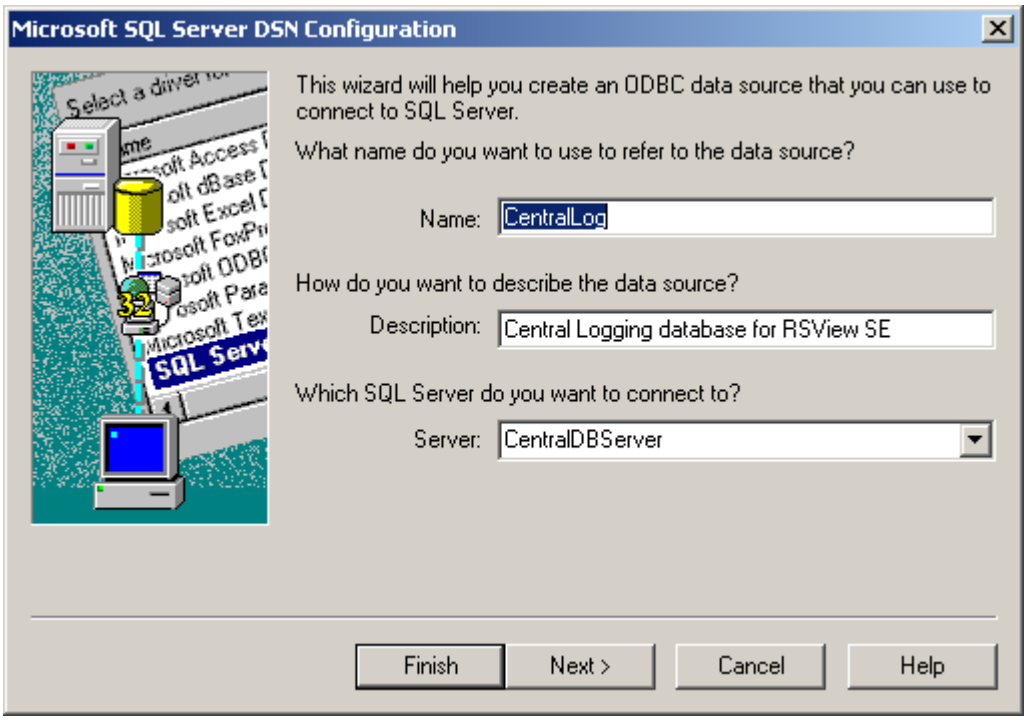


Create an ODBC data source to serve as a central database

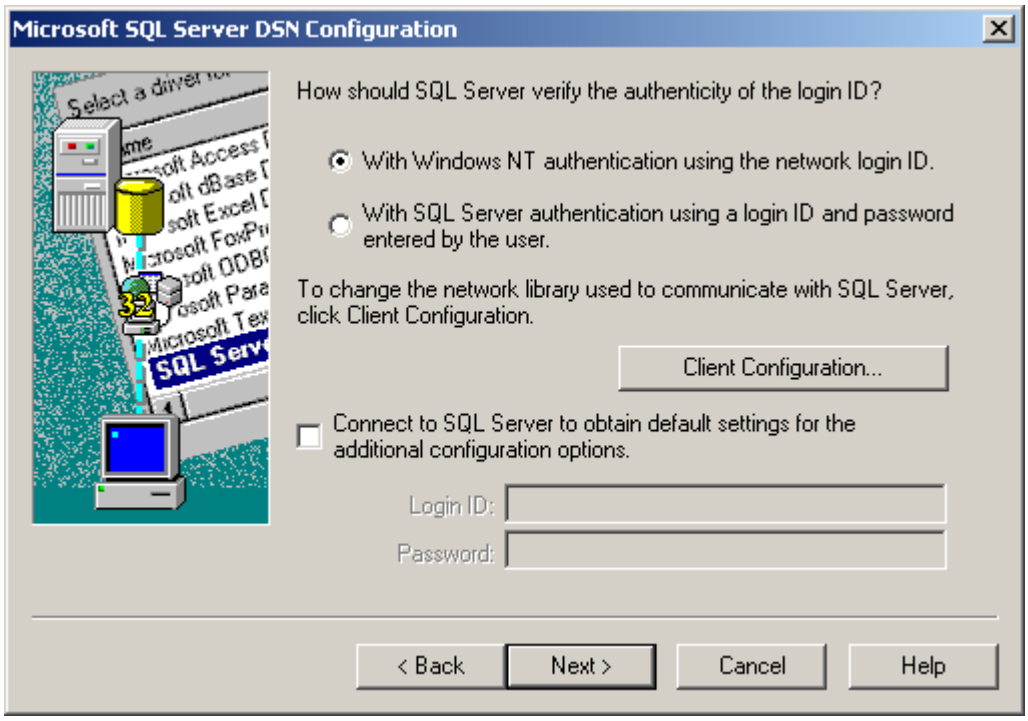
To create an ODBC data source, you follow the instructions in the RSView SE documentation, or you can configure it from the Windows Control Panel > Administrative Tools.

1. From the Create New Data Source window, select System Data Source as the data source, and then click Next.
2. Scroll through the list of drivers and select SQL Server. Click Next, and then click Finish.

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



4. At the next window, select the option, "With Windows NT authentication using the network login ID." Click Next.



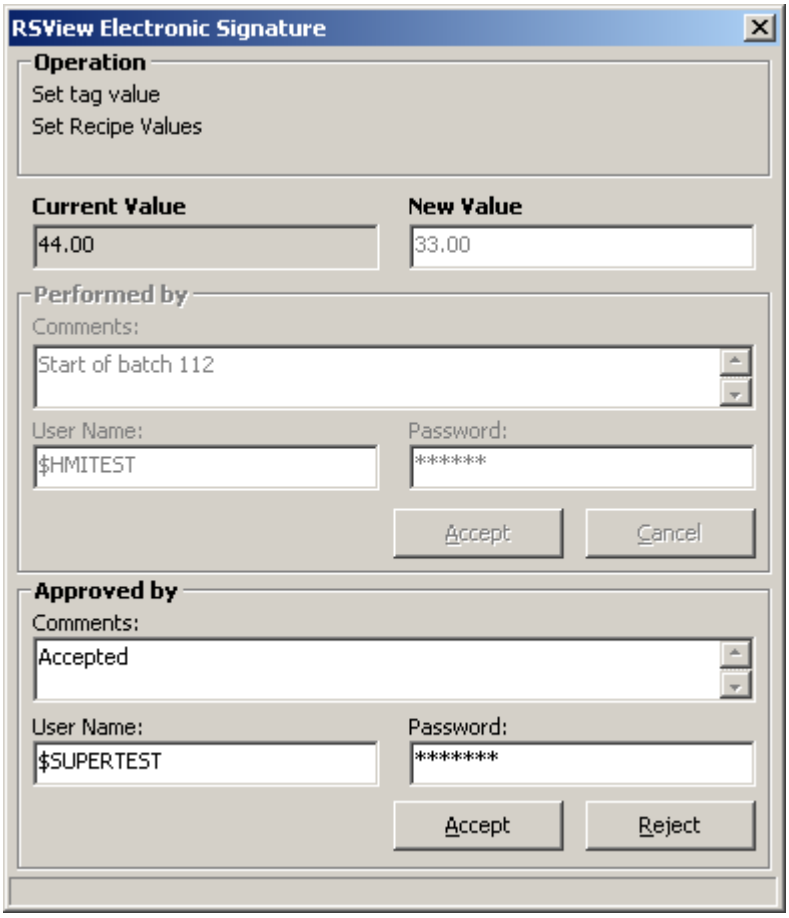
5. Continue working through the wizard, selecting options and clicking Next. When you finish, test the communications to your new ODBC data source.

Set up re-verification of operator identity, or supervisor signoff

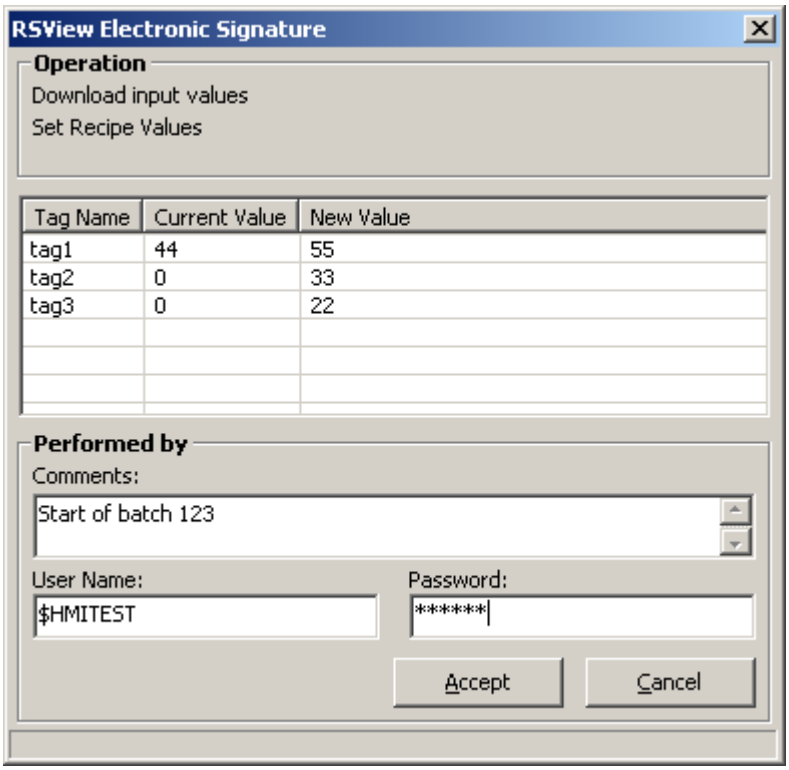
Once an operator is logged onto Windows and RSView SE Client, all operations are logged with the user name, and there is nothing in the 21 CFR Part 11 regulations that specifically requires an operator to enter both pieces of identification (user name and password) again. Although it is not required by the 21 CFR Part 11 regulations, some companies have a "re-verification" of operator identity, or authentication "on demand" for specific crucial operations, or specific supervisor signoff as part of their procedures. It may also be required by other sections of the Title 21 CFR Operations that can be secured include:

- Setpoint change
- RSView command
- Recipe download

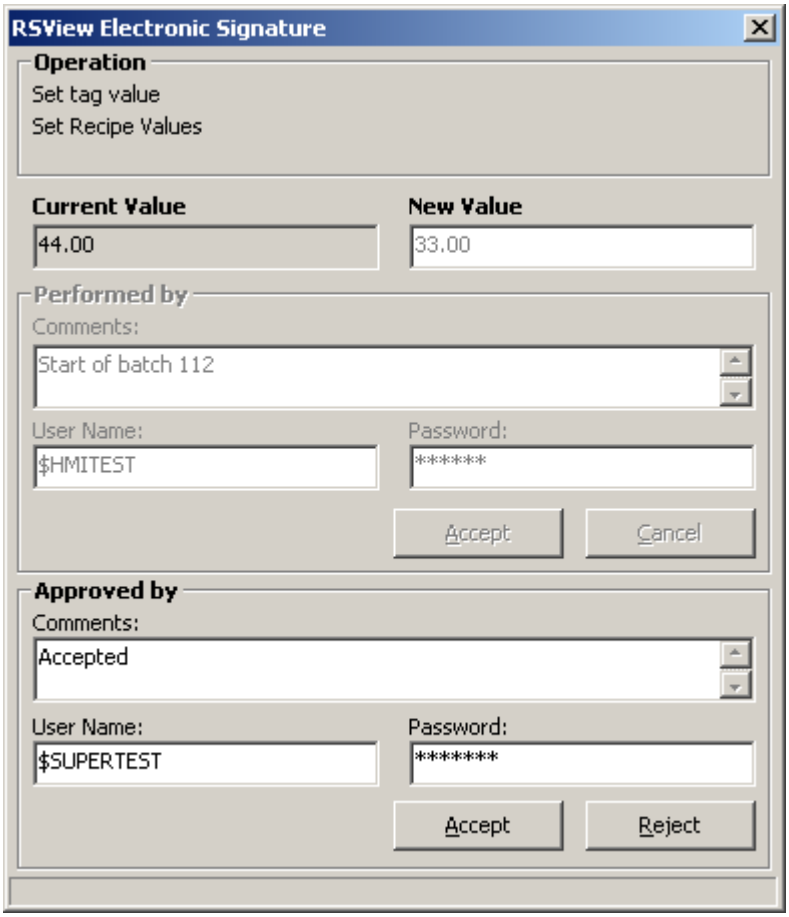
Approval by a supervisor can be required.



Recipe input values on a display can be edited and set to require authentication by performer and approver can be required.



Username, old value, new value, comments, and approver are logged to the FactoryTalk Diagnostics list, and can be routed to any or all audit destinations of choice (such as the local log, a central, secure ODBC repository, and RSMACC).



Set up Redundancy

While the 21 CFR Part 11 regulation does not specifically call out the need for redundancy, good manufacturing practices sometimes do require redundant configurations to ensure maximum system availability. RSView SE Servers, FactoryTalk Servers, and Linx servers can be set up to fail over to a backup servers, and when the primary comes back up, the primary will assume responsibility for HMI server activities. During server disruptions, the redundant systems provided by RSView Supervisory Edition are completely transparent to clients. Clients will receive information from the standby servers within 5 seconds of the failure. During server disruptions, users do not have to restart their RSView SE Client software to continue using the system. Once the system has switched to the redundant servers, clients continue functioning normally. While the fail-over is taking place, operators can continue to use input fields in graphic displays. Display fields remain at their last known values, and values downloaded to programmable controllers remain buffered until the fail-over is complete.

HMI servers manage the synchronization of alarms, so alarm states are kept synchronized between the primary and secondary servers. This means that if there are five unacknowledged alarms on the primary HMI server when fail-over occurs, the same five alarms will be unacknowledged on the secondary server after fail-over. Alarm states are also kept synchronized when the system switches back to the primary server. For information on how to set up redundancy, consult the RSView SE user manual or the white paper titled “Ensuring system availability in RSView Supervisory Edition applications”

Use version control software

RSMACC can be used to keep track of revisions to your RSView SE projects, RSMACC provides preferred integration with RSView SE and other Rockwell Software products. You can also use third-party version control software such as Microsoft SourceSafe, or you can contact your Rockwell Software representative regarding a complete system including RSMACC software and services. Version control software retains all of the 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 user name, component, and checkout date and time. The user modifies the component in RSView SE, closes RSView SE, and then checks the component back in. The version control software logs the user name, component, and check in date and time, and allows the user to add comments explaining the modifications. This provides you with a record of all changes you made and when you made them.

Compliance Statement

Rockwell Products and 21 CFR Part 11

Rockwell Software, HMI business unit

About Rockwell

Rockwell International, the parent corporation of Rockwell Automation, is a global leader in electronic controls and communications.

Rockwell's electronics businesses have leading market positions, well-known brands, and global presence. Rockwell International's three main businesses are:

- **Rockwell Automation—**Rockwell's largest business, Rockwell Automation is ranked first in North America and holds a solid first-tier ranking globally.
- **Rockwell Electronic Commerce—**Rockwell is a leading supplier of customer call center systems for a variety of well-known consumer service companies including Lands' End, L.A. Cellular, Marriott, National Car Rental, and GTE.

From corporate headquarters in Milwaukee, Rockwell coordinates a business representing $7 billion dollars in annual sales with 25,0000 employees in more than 200 facilities throughout the world. During the past five years, these businesses (automation, avionics & communications, and electronic commerce) have experienced an average annual growth rate of 18%. Rockwell is a recognized world leader in technology. Total Rockwell-funded R&D equals 8.5% of sales. Our world-class Science Center in Thousand Oaks, California gives us access to over 400 scientists and engineers and provides us with a depth of basic research that keeps our businesses on the cutting edge of technology.

Rockwell Automation manages a $4.4 billion dollar business with 64 manufacturing locations, 620 sales and support offices, 5,600 distributors and agents, and 25,000 employees. Rockwell Automation is a global company committed to serving needs locally with representatives in more than 80 countries. The worldwide support network includes service representatives, application engineers, technical instructors, and sales engineers. One in every five Rockwell Automation employees is in the field, and each of these employees is specifically charged with serving customer needs.

Rockwell Automation is committed to providing customers with high-quality automation solutions. Our solutions are engineered in facilities registered to ISO 9000 and ISO 14001 standards, and our products comply with standards such as the European CE directives. This commitment to quality is what helped make Rockwell Automation the leading supplier of industrial automation solutions in North America.

Rockwell Automation is a major supplier to the pharmaceutical industry. We are the undisputed supplier of choice to the North American market and are a first-tier supplier globally. Our products are widely used in every aspect of validated pharmaceutical manufacturing.

With our market position comes a responsibility to serve the special needs of our pharmaceutical customers. Acceptance of our products by governmental agencies is essential to being successful in this industry. Rockwell has a long, rich history of acceptance worldwide and is committed to maintaining that acceptance into the future. To that end, we have devoted key resources to ensuring that our products continually meet the needs experienced by the pharmaceutical industry.

The most current and urgent need in the industry today is compliance with the FDA's Electronic Records; Electronic Signatures regulation 21 CFR Part 11. This regulation is one of the U.S. government's first attempts to regulate specific feature sets of technology. Shifting the

focus to what the technology does, as opposed to how well it is made, is significant. Both industry manufacturers and suppliers have been struggling with the implications of this shift for the last several years.

Rockwell has taken a proactive role to understand what compliance to Part 11 means at the automation level. We have taken several significant steps to ensure compliance now and in the future. Some of the most important actions taken to date include:

- Participating in the PDA Part 11 Task Group
- Completing internal gap analysis
- Publishing application notes

Participating in PDA Part 11 Task Group

The PDA (Parenteral Drug Association) formed this task group to provide a set of best practices for Part 11 compliance. This group is viewed as the authority on Part 11 compliance from an implementation perspective. The task group includes representatives from the pharmaceutical industry, suppliers to the industry, consultants, and the FDA. The FDA's representative, an advisor to the group, is Paul Motise, Consumer Safety Officer, Office of Enforcement, Office of Regulatory Affairs, U.S. Food and Drug Administration. Rockwell is one of two automation suppliers on the task group. We have two members participating in the core group and two additional members on the extended team. Involvement in this group gives Rockwell direct access to accurate and up-to-date interpretations of the regulation and compliance practices as they evolve. We also view this opportunity as a way of adding balance to interpretations and recommended practices so that they remain practical and easily accessible by the entire pharmaceutical industry.

Completing internal gap analysis

Rockwell has undertaken and nearly completed a gap analysis of most of our software products in relation to 21 CFR Part 11. 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 RSView SE projects that comply with the U.S. government's 21 CFR Part 11 regulation. Rockwell is in the process of producing additional documentation that details recommended practices for product compliance. We will publish additional documentation on the Web-based Rockwell Software Knowledgebase: http://support.rockwellautomation.com.

Detailed compliance statements

21 CFR Part 11 is copied below, with RSView SE-related comments added in ***bold italics***.

PART 11-ELECTRONIC RECORDS;
ELECTRONIC SIGNATURES

Subpart A-General Provisions

11.1 Scope.

11.2 Implementation.

11.3 Definitions.

Subpart B-Electronic Records

11.10 Controls for closed systems.

11.30 Controls for open systems.

11.50 Signature manifestations.

11.70 Signature/record linking.

Subpart C-Electronic Signatures

11.100 General requirements.

11.200 Electronic signature components and controls.

11.300 Controls for identification codes/pass-words.

AUTHORITY: 21 U.S.C. 321-393; 42 U.S.C. 262.
SOURCE: 62 FR 13464, Mar. 20, 1997, unless otherwise noted.

Subpart A-General Provisions

§ 11.1 Scope.

(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full hand-written signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with § 11.2, unless paper records are specifically required.

(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

115
Food and Drug Administration, HHS § 11.10

§ 11.2 Implementation.

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

> ***RSView SE- Electronic records take the form of Activity Logs , Alarm Logs and Data Logs sent to an SQL-compliant ODBC database. Electronic Signatures are user names and passwords, both in the operating system (Windows NT 4 or Windows 2000) and in RSView SE.***

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

(1) The requirements of this part are met; and

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.)

> ***RSView SE—It is the end user's responsibility to determine which types of submissions the agency will accept in electronic form. For those submissions that the agency will accept in electronic form, the end user must consult with the intended agency as noted above.***

§ 11.3 Definitions.

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

(1) *Act* means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).

(2) *Agency* means the Food and Drug Administration.

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

(4) *Closed system* means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

> ***RSView SE—This document assumes a closed system is used.***

(5) *Digital signature* means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

(6) *Electronic record* means 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.

(7) *Electronic signature* means 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.

RSView SE—When RSView SE is configured to use Windows NT or 2000 domain security, the user's Windows XP or Windows 2000 user name and password are considered to be an electronic signature.

(8) *Handwritten signature* means 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.

(9) *Open system* means 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.

RSView SE—This document assumes a closed system is used.

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 ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

RSView SE—System validation is unique in every case and must be done by the end user. Because electronic records are not stored in a format or location to which end users have access, they cannot be altered.

(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.

RSView SE—Records are kept in an SQL-compliant ODBC database. RSView SE has tools to read locally buffered records, but once they have been sent to the ODBC database and removed from the local buffer, users must use a separate reporting tool such as Microsoft Access, Microsoft SQL Server tools, or Crystal Reports to read the records

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

RSView SE—Records are kept in an SQL-compliant ODBC database.

Using a combination of RSView SE security, RSView SE Desktop Lock, and Windows NT or Windows 2000 security, a system can be created that prevents unauthorized access to data files or the operating system.

(d) Limiting system access to authorized individuals.

RSView SE—Limiting system access includes configuring RSView SE to use Windows NT or Windows 2000 security. It also includes other security measures that physically prevent unauthorized personnel from accessing the system. In addition to procedures that require operators to log out of the RSView SE and Windows XP/2000, password-protected screen savers and automatic logout can be used to ensure that workstations are not left unattended for longer than a specified period of time.

(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.

RSView SE—Each entry into the RSView SE activity log is identified with the time and date the action occurred and the name of the logged-in operator who performed the action.

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

RSView SE—Operational steps and sequencing are a combination of PLC logic and RSView SE. RSView SE supports both screen-level and tag-level security. An application can be developed to support user-initiated operational checks, which require screen security.

(g) Use of authority checks to ensure 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.

RSView SE—RSView SE uses Windows NT or Windows 2000 domain security. Use separate administrative procedures in the NT/2000 domain to ensure that only authorized individuals access the systems.

(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

RSView SE—RSView SE users Windows 2000 or Windows NT domain security.

(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.

RSView SE—This is the responsibility of the end user.

(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

RSView SE—This is the responsibility of the end user.

(k) Use of appropriate controls over systems documentation including:

(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

RSView SE—Revision and change control procedures can be implemented using version control software such Microsoft SourceSafe or PVCS Tracker. A comprehensive system can be implemented using RSMACC software and services.

RSView SE user documentation is provided both in electronic (.pdf) format on the product CD and hard copy format. The distribution of these documents is at the user's discretion.

§ 11.30 Controls for open systems.

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure 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 ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

RSView SE—This document does not cover open systems.

§ 11.50 Signature manifestations.

(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

(1) The printed name of the signer;

RSView SE—RSView SE requires that a user be logged in to Windows prior to launching RSView SE clients, or performing any actions. The system records in the activity and alarm logs each action the logged-in user performs, along with a date, time, and the RSView/Windows user name/ID. The full name of the user, i(f different from the Windows User ID) should be included in any reports, and the mapping between the Full Name and User ID done via the reporting tool, using a database join.

(2) The date and time when the signature was executed; and

RSView SE—RSView SE records in the activity and alarm logs the date, time, and user name associated with each action.

(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

RSView SE—RSView SE provides a number of activity categories. The meaning of each command is implied. For example, acknowledging an alarm with the Acknowledge command is interpreted as reviewing it and then acknowledging its existence. Similarly, setting a tag value with the Set command implies the user initiated the action and therefore approves it and is responsible for the action.

(b) 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).

RSView SE—The RSView SE activity log viewer shows the user name, time, and action. Any reports created from the data using a third-party tool could also show the fields.

§ 11.70 Signature/record linking.

Electronic signatures and hand-written signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means

All data records stored in SQL Server or Oracle are protected by a user name and password, thus preventing information from being altered.

117
Food and Drug Administration, HHS § 11.300
Subpart C-Electronic Signatures

§ 11.100 General requirements.

(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

RSView SE—Only one user should be allowed to use a given Windows NT/2000 domain account and password.

(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.

RSView SE—This is the responsibility of the end user.

(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

(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.

RSView SE—This is the responsibility of the end user.

(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.

RSView SE—This is the responsibility of the end user.

§ 11.200 Electronic signature components and controls.

(a) Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

RSView SE—A Windows NT/2000 password (which RSView SE then uses) contains an identification code (user name) and password.

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

RSView SE—The user signs on at the start of a session using two distinct identification components (user name and password). The user name is then logged as a single electronic signature component. If the user logs out and then requires access again, the user must re-enter the user name and password.

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

RSView SE—The end user must implement logout procedures to enforce user log off at the end of any continuous period of controlled system access, and to enforce log on at the start of the next access period.

RSView SE—This is the responsibility of the end user.

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

RSView SE—It would require two individuals to re-use a user name and password. First, a user would need to reveal to a second person his or her user name and password. The second person would then have to use it. The potential problem where an NT administrator assigns a user's password and then uses the account can be solved by physically disallowing anyone with Windows NT/2000 domain administrative privileges access to the RSView SE stations in the closed system.

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

RSView SE—Biometric-based logon mechanisms are commercially available, but they are outside the scope of this document.

§ 11.300 Controls for identification codes/passwords.

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure 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.

RSView SE—This is enforced by Windows NT/2000 security, and RSView SE can be configured to use NT Security to manage user names.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

RSView SE—This can be enforced by Windows NT/2000 security.

(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.

RSView SE—It is the responsibility of the end user to determine and enforce this, using Windows NT/2000 security.

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

RSView SE—An example of a transaction safeguard: As part of a logon macro, or a button action from an initial display, , an operator might be required to enter a separate piece of information or answer a question presented in a dialog presented by VBA display code. The user's response can be examined in VBA to determine whether the user name and password are being used improperly. If so, the information can be reported immediately to system security and/or management.

Windows NT/2000 security mechanisms can detect unauthorized use if rules for unauthorized use are maintained, for example, a rule might stipulate that three incorrect log-in attempts generates a suspension of the account.

(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

RSView SE—This is the responsibility of the end user.

Rockwell Software

For more information on the latest pricing or a demonstration of any Rockwell Software package, please contact your local Rockwell Automation Sales office or Allen-Bradley distributor. For the very latest on Rockwell Software products, visit us at:

www.software.rockwell.com

Reach us now at www.rockwellautomation.com

Wherever you need us, Rockwell Automation brings together leading brands in industrial automation including Allen-Bradley controls, Reliance Electric power transmission products, Dodge mechanical power transmission components, and Rockwell Software. Rockwell Automation's unique, flexible approach to helping customers achieve a competitive advantage is supported by thousands of authorized partners, distributors and system integrators around the world.

Americas Headquarters, 1201 South Second Street, Milwaukee, WI 53201-2496, USA, Tel: (1) 414 382-2000, Fax: (1) 414-382-4444
European Headquarters SA/NV, Boulevard du Souverain 36, 1170 Brussels, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific Headquarters, 27/F Citicorp Centre, 18 Whitfield Road, Causeway Bay, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Allen-Bradley · Reliance Electric · Dodge · Rockwell Software · Rockwell Automation

Doc ID 21CFR-WP003A-EN-E