



# FactoryTalk Security System Configuration Guide

Rockwell Automation Publication FTSEC-QS001Q-EN-E - March 2021  
Supersedes Publication FTSEC-QS001P-EN-E - September 2020



Quick Start

Original Instructions

## Important User Information

Read this document and the documents listed in the additional resources section about installation, configuration, and operation of this equipment before you install, configure, operate, or maintain this product. Users are required to familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.

Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with applicable code of practice.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.



**WARNING:** Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.

---



**ATTENTION:** Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.

---

**IMPORTANT** Identifies information that is critical for successful application and understanding of the product.

---

Labels may also be on or inside the equipment to provide specific precautions.



**SHOCK HAZARD:** Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.

---



**BURN HAZARD:** Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.

---



**ARC FLASH HAZARD:** Labels may be on or inside the equipment, for example, a motor control center, to alert people to potential Arc Flash. Arc Flash will cause severe injury or death. Wear proper Personal Protective Equipment (PPE). Follow ALL Regulatory requirements for safe work practices and for Personal Protective Equipment (PPE).

---

<b>Preface</b>	Summary of changes ..... 9
	About this publication ..... 9
	Additional resources .....10
	Legal Notices.....10
	<b>Chapter 1</b>
<b>About FactoryTalk systems</b>	FactoryTalk systems..... 13
	FactoryTalk Directory types ..... 15
	Accounts and groups..... 16
	Account types ..... 18
	Applications and areas..... 20
	Security in a FactoryTalk system ..... 20
	Example: Two directories on one computer ..... 22
	<b>Chapter 2</b>
<b>Install FactoryTalk Services Platform</b>	Install FactoryTalk Services Platform ..... 25
	Install FactoryTalk System Services and FactoryTalk Policy Manager. 26
	<b>Chapter 3</b>
<b>Getting started with FactoryTalk Security</b>	FactoryTalk Security ..... 29
	Security on a local directory ..... 31
	Security on a network directory..... 31
	How security authenticates user accounts .....32
	Things you can secure.....32
	Best practices.....34
	Audit trails and regulatory compliance .....36
	Configure a computer to be the FactoryTalk Directory network server 38
	Configure a computer to be the network directory server .....39
	Configure a network directory client computer .....39
	Check network directory server connection status..... 40
	FactoryTalk Directory Server Location Utility ..... 41
	<b>Chapter 4</b>
<b>Manage users</b>	Manage users .....43
	Add a FactoryTalk user account .....43
	Add a Windows-linked user account.....45
	Add group memberships to a user account ..... 46
	Remove group memberships from a user account.....47
	Delete a user account ..... 48

	<b>Chapter 5</b>	
<b>Manage user groups</b>	Manage user groups .....	51
	Add a FactoryTalk user group .....	52
	Add a Windows-linked user group .....	53
	Edit or view user group properties .....	55
	Delete a user group .....	56
	Add accounts to a FactoryTalk user group .....	56
	Remove accounts from a FactoryTalk user group .....	57
	 <b>Chapter 6</b>	
<b>Manage computers</b>	Manage computers .....	59
	Add a computer .....	59
	Delete a computer .....	60
	Edit or view computer properties .....	61
	 <b>Chapter 7</b>	
<b>Add and remove user-computer pairs</b>	Add and remove user-computer pairs.....	63
	Add a user-computer pair.....	63
	Remove a user-computer pair .....	65
	Edit or view user account properties.....	65
	 <b>Chapter 8</b>	
<b>Add and remove action groups</b>	Add and remove action groups .....	67
	Add an action group.....	67
	Delete an action group.....	68
	Add an action to an action group.....	69
	Remove an action from an action group.....	69
	 <b>Chapter 9</b>	
<b>Set system policies</b>	Authorize an application to access the FactoryTalk Directory .....	72
	FactoryTalk Service Application Authorization .....	73
	FactoryTalk Service Application Authorization settings .....	73
	Publisher Certificate Information .....	75
	Digitally signed FactoryTalk products.....	76
	Authorize a service to use FactoryTalk Badge Logon .....	76
	FactoryTalk Badge Authorization .....	77
	FactoryTalk Badge Authorization settings.....	77
	Assign user rights to make system policy changes .....	78
	User rights assignment policies.....	79
	User Rights Assignment Policy Properties .....	80
	Configure Securable Action .....	80

Select a user or group.....	81
Change the default communications protocol .....	82
Default communications protocol settings .....	82
Live Data Policy Properties.....	83
Set network health monitoring policies .....	84
Health Monitoring Policy Properties .....	85
Set audit policies .....	86
Audit policies .....	87
Audit Policy Properties .....	89
Monitor security-related events.....	90
Example: Audit messages .....	91
Set system security policies .....	91
Modify Account Policy Settings .....	92
Modify Computer Policy Settings.....	93
Modify Directory Protection Policy Settings .....	95
Modify Password Policy Settings.....	96
Modify Badge login policies .....	98
Enable single sign-on.....	99
Disable single sign-on.....	100
Account Policy Settings .....	100
Computer Policy Settings.....	102
Directory Protection Policy Settings .....	103
Cache expiration policies .....	105
Password Policy Settings.....	106
Single Sign-On Policy Settings .....	109
When to disable single sign-on .....	110
Security Policy Properties.....	110
Navigate the Policy Properties windows .....	111
Export policies to XML.....	112

## Chapter 10

### Set product-specific policies

Secure features of a single product .....	114
Secure multiple product features .....	114
Feature Security for Product Policies .....	115
Feature Security Policies.....	116
Differences between securable actions and product policies .....	116

## Chapter 11

### Manage logical names

Logical names.....	119
Add a logical name .....	121
Delete a logical name .....	122
Add a device to a logical name.....	122

Remove a device from a logical name ..... 122  
 Assign a control device to a logical name ..... 123  
 Add a logical name to an area or application ..... 124  
 Delete a logical name from an area or application ..... 124  
 New Logical Name..... 125  
 Logical Name Properties..... 126  
 Device Properties ..... 126

**Chapter 12**

**Resource grouping**

Resource groupings ..... 129  
 Group hardware resources in an application or area..... 130  
 Move a resource between areas ..... 131  
 Remove a device from a resource grouping ..... 131  
 Resources Editor ..... 132  
 Select Resources ..... 133

**Chapter 13**

**Secure resources**

Secure resources ..... 135  
     Permissions ..... 135  
         Breaking the chain of inheritance ..... 138  
         Order of precedence ..... 139  
         Actions ..... 140  
 Set FactoryTalk Directory permissions ..... 144  
 Set application permissions ..... 145  
 Set area permissions ..... 147  
 Set System folder permissions ..... 148  
 Set action group permissions ..... 149  
 Set database permissions ..... 151  
 Set logical name permissions..... 152  
 Allow a resource to inherit permissions ..... 153  
 Prevent a resource from inheriting permissions ..... 154  
 View effective permissions..... 154  
 Effective permission icons ..... 156

**Chapter 14**

**Disaster Recovery**

Back up a FactoryTalk system ..... 159  
     Back up a FactoryTalk Directory ..... 160  
     Back up a System folder..... 162  
     Back up an application..... 164  
     Back up a Security Authority identifier ..... 166  
     Backup FactoryTalk Linx configuration..... 167  
     Backup..... 168

Backup and restore options.....	170
Modify Security Authority Identifier.....	171
Restore a FactoryTalk system .....	172
Restore a FactoryTalk Directory.....	172
Restore a System folder .....	175
Restore an application .....	176
Restore a Security Authority identifier .....	179
Restore FactoryTalk Linx configuration.....	180
Verify security settings after restoring a FactoryTalk system .....	181
Update computer accounts in the network directory .....	181
Recreate a Windows-linked user account.....	182
Update Windows-linked user groups .....	183
Update security settings for Networks and Devices .....	183
Update security settings for the FactoryTalk Linx OPC UA Connector .....	184
Restore database connections .....	185
Restore an earlier system after upgrading FactoryTalk platform software .....	185
Generate a Security Authority identifier.....	187
Restore .....	188
Restore (FactoryTalk Directory).....	189
Restore (System folder) .....	190
Restore (Application) .....	190
Restore (Security Authority Identifier) .....	192
Restore Backup File.....	193
Use commands to back up and restore.....	193
FactoryTalk Directory Configuration Wizard.....	196
Select a FactoryTalk Directory to configure.....	197
Configure FactoryTalk Network Directory.....	197
Network directory and the FactoryTalk Directory Configuration Wizard .....	198
Configure FactoryTalk Local Directory.....	199
Local directory and the FactoryTalk Directory Configuration Wizard .....	200
Product support for network and local directories .....	201
Enter an administrator user name and password .....	202
Reset an expired password.....	203
Change Password (local).....	203
Change Password (network) .....	204
Summary .....	205
Default passwords.....	206

<b>Upgrade FactoryTalk Services Platform</b>	<p><b>Appendix A</b></p> <p>Upgrade FactoryTalk Services Platform..... 209</p> <p>Identify the installed FactoryTalk Services Platform version .....210</p>
<b>FactoryTalk Web Services</b>	<p><b>Appendix B</b></p> <p>Install FactoryTalk Web Services..... 211</p> <p>Add an HTTPS site binding for FactoryTalk Web Services .....212</p> <p>Client computers unable to connect to FactoryTalk Web Services ..... 213</p> <p>User cannot log into FactoryTalk Web Services.....214</p>
<b>Introduction to FactoryTalk Policy Manager and FactoryTalk System Services</b>	<p><b>Appendix C</b></p> <p>FactoryTalk Policy Manager and FactoryTalk System Services ..... 215</p> <p>Install FactoryTalk System Services and FactoryTalk Policy Manager 216</p> <p>Start FactoryTalk System Services ..... 217</p> <p>Log on to FactoryTalk Policy Manager ..... 217</p> <p>Navigate FactoryTalk Policy Manager .....218</p> <p>FactoryTalk Policy Manager Global Settings..... 219</p> <p>FactoryTalk Policy Manager planning ..... 220</p> <p>FactoryTalk Policy Manager component considerations..... 222</p> <p>Authentication methods .....223</p> <p>Security Groups .....223</p> <p>Zones ..... 224</p> <p style="padding-left: 20px;">Add a zone..... 225</p> <p>Conduits..... 225</p> <p style="padding-left: 20px;">Add a conduit..... 226</p> <p>Devices .....227</p> <p style="padding-left: 20px;">Discovery .....227</p> <p style="padding-left: 20px;">Add a device to a zone .....227</p> <p style="padding-left: 20px;">FactoryTalk Linx devices ..... 229</p> <p style="padding-left: 20px;">Ports ..... 229</p> <p style="padding-left: 40px;">Add a port ..... 230</p> <p style="padding-left: 20px;">Replace a device..... 230</p> <p style="padding-left: 20px;">Remove the security policy from a device ..... 231</p> <p>Ranges .....232</p> <p style="padding-left: 20px;">Add a range.....232</p> <p>Deploy a security model.....233</p> <p>Backup and restore security models .....234</p> <p style="padding-left: 20px;">Backup FactoryTalk System Services.....235</p> <p style="padding-left: 20px;">Restore FactoryTalk System Services .....235</p>

**Index**



## Summary of changes

This manual includes new and updated information. Use these reference tables to locate changed information.

Grammatical and editorial style changes are not included in this summary.

## Global changes

None in this release.

## New or enhanced features

This table contains a list of topics changed in this version, the reason for the change, and a link to the topic that contains the changed information.

Topic Name	Reason
<a href="#">Account Policy Settings</a> on <a href="#">page 100</a>	The default value of the <b>Account lockout threshold</b> for the Local Directory and Network Directory is changed from 0 invalid logon attempts to 3 invalid logon attempts.
<a href="#">Back up a FactoryTalk Directory</a> on <a href="#">page 160</a>	Enhanced to provide a backup step for FactoryTalk Linx configurations.
<a href="#">Back up an application</a> on <a href="#">page 164</a>	Enhanced to provide a backup step for FactoryTalk Linx configurations.
<a href="#">Back up a System folder</a> on <a href="#">page 162</a>	Enhanced to provide a backup step for FactoryTalk Linx configurations.
<a href="#">Restore a FactoryTalk Directory</a> on <a href="#">page 189</a>	Enhanced to provide a restore step for FactoryTalk Linx configurations.
<a href="#">Restore a System folder</a> on <a href="#">page 190</a>	Enhanced to provide a restore step for FactoryTalk Linx configurations.
<a href="#">Restore an application</a> on <a href="#">page 176</a>	Enhanced to provide a restore step for FactoryTalk Linx configurations.
<a href="#">Use command line to back up and restore</a> on <a href="#">page 193</a>	New topic that introduces the command lines can be used to backup and restore FactoryTalk Directory, System folder, and applications.

## About this publication

This *Quick Start Guide* provides you with information on using FactoryTalk Services Platform with FactoryTalk Security.

Before using this guide, review the FactoryTalk Services Platform Release Notes for information about required software, hardware, and anomalies.

After using this guide, you will be more familiar with how FactoryTalk Services Platform uses:

- FactoryTalk Directory types
- User accounts
- Computer accounts
- Local and network security options

- Authentication methods
- Password management
- Security policies

## Additional resources

For more information on system security download the [System Security Design Guidelines](#) (publication SECURE-RM001) from the Rockwell Automation Literature Library.

For more information on the products and components discussed in this guide, the following manuals and Help files are available with the software:

- FactoryTalk® Help – Go to **Rockwell Software > FactoryTalk Tools > FactoryTalk Help**
- FactoryTalk View Installation Guide or FactoryTalk View Help – Go to **Rockwell Software > FactoryTalk View > User Documentation** and then select the appropriate Help or User Guide.
- FactoryTalk® Linx™ Help – Go to **Rockwell Software > FactoryTalk Linx > FactoryTalk Linx Online Reference**.
- RSLinx® Classic Help – Go to **Rockwell Software > RSLinx > RSLinx Classic Online Reference**.
- Studio 5000 Logix Designer® application Help – In Logix Designer, select **Help > Contents**
- FactoryTalk Batch Administrator's Guide – Go to **Rockwell Software > FactoryTalk Batch Suite > FactoryTalk Batch > Online Books > FactoryTalk Batch > Batch Administrator's Guide**
- FactoryTalk® Transaction Manager Help
- FactoryTalk® AssetCentre Help

The Rockwell Automation® Literature Library also has related Getting Results Guides that can be viewed online or downloaded:

- FactoryTalk Linx Getting Results Guide - [Rockwell Automation Publication LNXENT-GROO1 -EN-E](#)
- RSLinx Classic Getting Results Guide - [Rockwell Automation Publication LINX-GROO1 -EN-E](#)
- FactoryTalk Batch Getting Results Guide - [Rockwell Automation Publication BATCH-GRO11 -EN-P](#)
- FactoryTalk Policy Manager Getting Results Guide - [Rockwell Automation Publication FTALK-GROO1 -EN-E](#)

## Legal Notices

Rockwell Automation publishes legal notices, such as privacy policies, license agreements, trademark disclosures, and other terms and conditions on the [Legal Notices](#) page of the Rockwell Automation website.

### End User License Agreement (EULA)

You can view the Rockwell Automation End User License Agreement (EULA) by opening the license.rtf file located in your product's install folder on your hard drive.

---

The default location of this file is:

C:\Program Files (x86)\Common Files\Rockwell\license.rtf.

## Open Source Software Licenses

The software included in this product contains copyrighted software that is licensed under one or more open source licenses.

You can view a full list of all open source software used in this product and their corresponding licenses by opening the index.html file located your product's OPENSOURCE folder on your hard drive.

The default location of this file is:

C:\Program Files (x86)\Common Files\Rockwell\Help\FactoryTalk  
Services Platform\Release Notes\OPENSOURCE\index.htm

You may obtain Corresponding Source code for open source packages included in this product from their respective project web site(s).

Alternatively, you may obtain complete Corresponding Source code by contacting Rockwell Automation via the **Contact** form on the Rockwell Automation website: <http://www.rockwellautomation.com/global/about-us/contact/contact.page>. Please include "Open Source" as part of the request text.

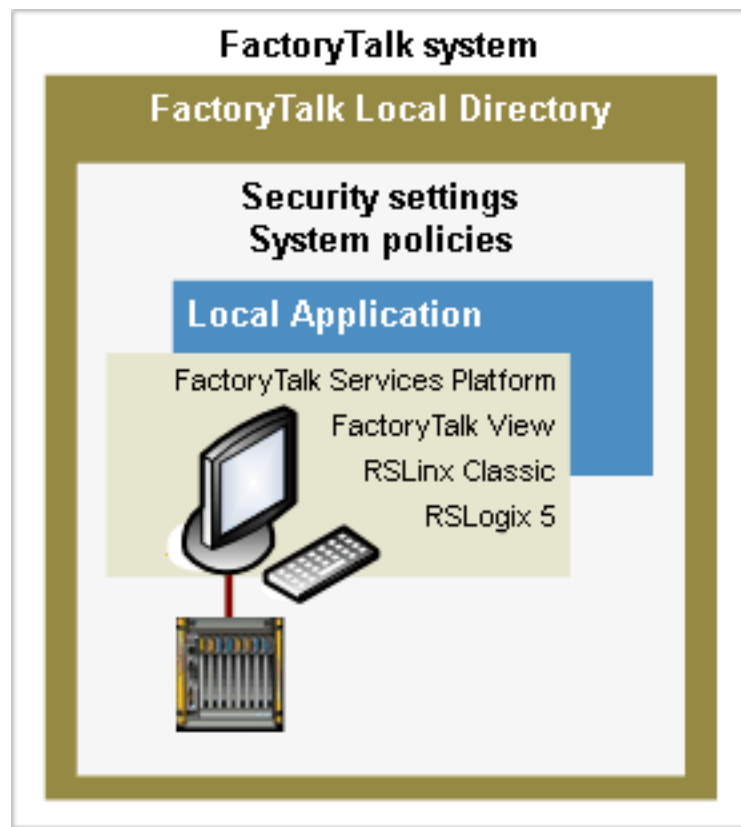


## About FactoryTalk systems

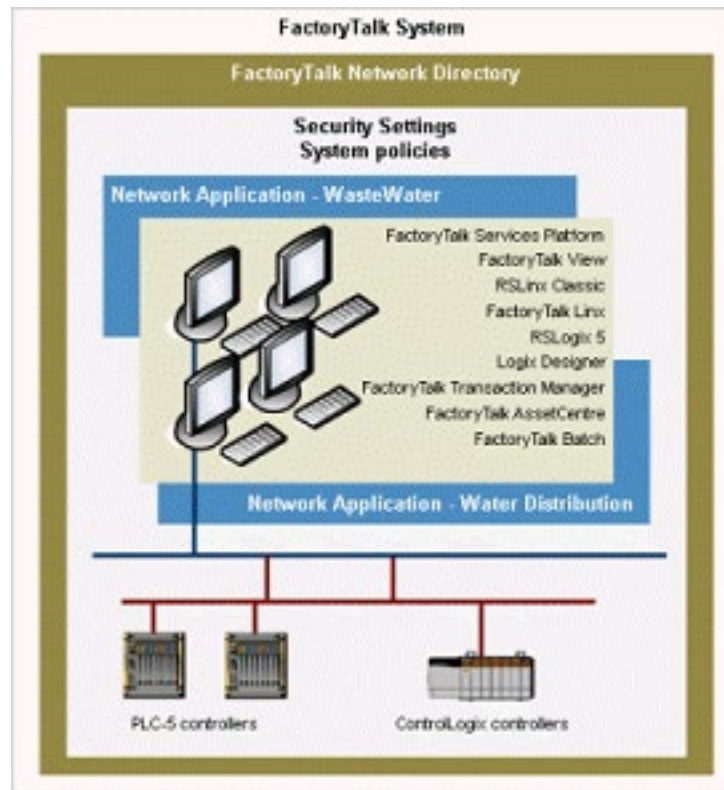
### FactoryTalk systems

A FactoryTalk® system is composed of software products, services, and hardware devices participating together and sharing the same FactoryTalk Directory and FactoryTalk services.

For example, a FactoryTalk system may be as simple as FactoryTalk® Services Platform, FactoryTalk View, RSLinx® Classic, and RSLogix™ 5 all installed on the same computer, communicating with a single programmable logic controller, and all participating in the same local application held in a local directory.



A FactoryTalk system may be much more complex, with software products and hardware devices participating in multiple network applications distributed across a network, all sharing the same network directory.



A single computer can host both a local directory and a network directory. The two directories are completely separate and do not share any information. When using both directories, that single computer participates in two separate FactoryTalk systems.

In the network directory example above, the directory hosts two network applications: Waste Water and Water Distribution. All of the areas, data servers, HMI servers, device servers, and alarm and event servers organized within each application are specific to that application. None of the application-specific information is shared with any other application in the directory. However, all information and settings organized within the System folder, such as security settings, system policies, product policies, and user accounts apply to all applications held in the directory.

For example, modifying security settings in the Waste Water application does not affect the Water Distribution application. However, making a change to a security policy applies the change to both the Waste Water application and the Water Distribution application. The security policy settings also apply to any other new applications created in this same network directory.

### See also

[FactoryTalk Directory types](#) on [page 15](#)

[Accounts and groups](#) on [page 16](#)

[Applications and areas](#) on [page 20](#)

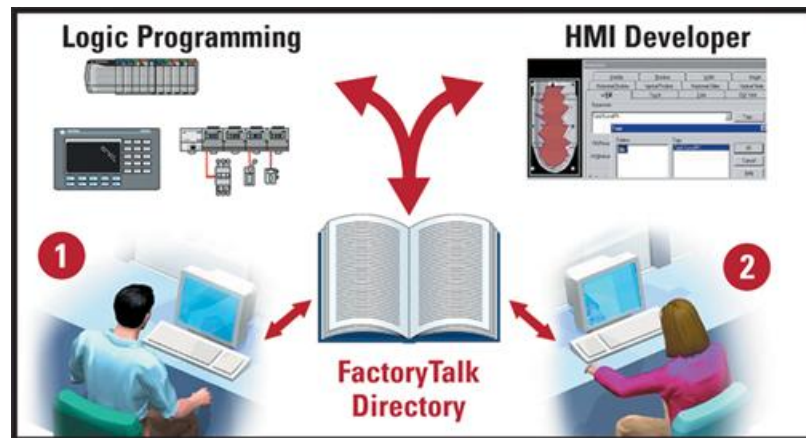
[Security in a FactoryTalk system](#) on [page 20](#)

[Example: Two directories on one computer](#) on [page 22](#)

## FactoryTalk Directory types

The FactoryTalk Directory is the centerpiece of the FactoryTalk Services Platform. FactoryTalk Directory provides a central lookup service for all products participating in an application. Rather than a traditional system design with multiple, duplicated databases or a central, replicated database, FactoryTalk Directory references tags and other system elements from multiple data sources—and makes the information available to clients through a lookup service.

Tags are stored in their original environments, such as logic controllers. Graphic displays are stored in the HMI servers where they are created. This information is available, without duplication, to any FactoryTalk product participating in an application.



For example, at workstation 1, a logic programmer programs PLC tags using RSLogix™ and saves the project. At workstation 2, an engineer using FactoryTalk View SE has immediate access to the tags created in the PLC program, without creating an HMI tag database. Tags are available for immediate use anywhere within the application, even before the logic program is downloaded to the controller. As the logic program is edited, most tag information is updated, and new tags are available immediately across the system.

With RSLogix 5000® controllers, tags reside within the hardware itself. With Allen-Bradley® PLC-5® and SLC™ 500 devices, and with third-party controllers, tags reside within data servers, such as RSLinx Classic and FactoryTalk® Linx™. Tags are not held within a common database, nor are they duplicated in multiple databases. Instead, the FactoryTalk Directory references tags from their source locations and passes the information on to the software products that need it, such as FactoryTalk View SE and FactoryTalk Transaction Manager.

## A single computer can host two types of directories

The FactoryTalk Services Platform installs and configures two completely separate and independent directories: a local directory and a network directory. Each directory can hold multiple applications.

- In a **local directory**, all project information and security settings are located on a single computer, and the FactoryTalk system cannot be shared across a network or from the network directory on the same computer. Products such as FactoryTalk View SE (Local) and FactoryTalk View ME use the local directory.
- A **network directory** organizes project information and security settings from multiple FactoryTalk products across multiple computers on a network. Products such as FactoryTalk View SE and FactoryTalk Transaction Manager use the network directory.

Determining the appropriate directory depends upon the software products and whether the environment is stand-alone or networked.

### See also

[Example: Two directories on one computer](#) on [page 22](#)

[Configure a network directory client computer](#) on [page 39](#)

[FactoryTalk systems](#) on [page 13](#)

## Accounts and groups

Create accounts for users, computers, and groups of users and computers to define who can perform actions, and from where.

Security settings for accounts are stored in FactoryTalk Directory, and are separate for FactoryTalk network and local directories. As much as possible, secure resources by defining security permissions for the group accounts. Add user and computer accounts to the groups, and all individual accounts in the groups have the security settings of those groups.

### User accounts and user group accounts

Accounts for users and user groups can link to accounts in a Windows® domain or workgroup, or be separate from those in Windows.

If the FactoryTalk system security needs are the same as the Windows security needs, using Windows-linked user or group accounts provides a convenient way to add large numbers of existing Windows user or group accounts to the FactoryTalk system. Account properties — for example, whether users can change passwords — are inherited directly from the Windows accounts, and update automatically when changed in Windows. Separate account administration is not required.



FactoryTalk user accounts or user group accounts provide secure access to the FactoryTalk system independently of the level of access users have in Windows. If the security needs of the FactoryTalk system are different from those of the Windows network, FactoryTalk Directory user accounts provide the benefits and convenience of centralized administration, without needing a Windows domain. FactoryTalk user group accounts also retain their security settings if the FactoryTalk Directory moves to a new domain.

## Computer and computer group accounts

Sometimes restricting access to resources based on a user's physical location is necessary. Some critical operations require line-of-sight security, to ensure that computers are located within view of the equipment they are controlling. For example, a system designer might determine that a piece of equipment is operated from one specific operator workstation or group of workstations physically located within a clear view of the machine.

Computer accounts and computer group accounts are not linked to Windows. Accounts for computers that do not yet exist in Windows can be created in a local FactoryTalk Directory. However, the name of a computer account must match the Windows computer name for the security settings associated with the computer to take effect. Because a FactoryTalk local directory runs on a single computer, add computer accounts only to a FactoryTalk local directory.

## Account status

By default, user accounts and group accounts have active status, which means that the account can be used to access resources. Other possible account statuses are:

- Disabled, prevents the user from accessing the account temporarily.
- Locked, the wrong password was entered more than a certain number of times.
- Deleted, prevents the user from accessing the account permanently.
- Unknown, information about the account could not be obtained from the network.

## See also

[Account types](#) on [page 18](#)

[Manage users](#) on [page 43](#)

[Manage user groups](#) on [page 51](#)

[Manage computers](#) on [page 59](#)

## Account types

FactoryTalk supports these account types:

- FactoryTalk user accounts that are separate from Windows accounts.
- Windows-linked user accounts that are linked to existing user accounts in a Windows domain or workgroup.
- Windows-linked user groups that determine access for all of the Windows accounts in the group. To specify different permissions for some users in the Windows-linked group, add Windows-linked user accounts for those users.

Both Windows-linked accounts and FactoryTalk accounts can be in a FactoryTalk Directory. Example: A FactoryTalk administrator account that is unique to the FactoryTalk Directory and FactoryTalk user accounts that are linked to Windows user accounts.

### When to use FactoryTalk user accounts

- For the convenience and benefits of centralized security administration across the entire distributed system, without reliance on a Windows domain. This is often necessary when your organization's IT department controls administration of Windows users, and does not allow you to modify accounts in Windows.
- For central user authentication when using Windows workgroups in a FactoryTalk network directory. For all FactoryTalk products, FactoryTalk Directory is the central authority for user authentication, allowing you administer user accounts centrally, rather than locally on each computer. You can use Windows-linked accounts with Windows workgroups in a local directory.
- When the security needs of the Windows network are different from the security needs of the control network. For example:
  - When all operators share the same Windows account to gain access to the computer.
  - When the computer is always logged on under a particular Windows account, FactoryTalk accounts allow different operators to gain different levels of access to the control system, independently of their access to Windows.
  - When the computer automatically logs on to the Windows network after restarting (for example, after a power failure), so that it can run control programs automatically. FactoryTalk accounts allow operators to log on and off the control system independently of Windows.

### When to use Windows-linked user accounts

- When the security needs of the Windows network are the same as the security needs of the control system. For example:

- When the control system is located in its own domain, perhaps separately from business systems, and user accounts and passwords can be shared between Windows and FactoryTalk software programs.
- When operators can log on and off computers with their own Windows accounts, and the software programs they use start automatically.

## When to use Windows-linked user group accounts

If you expect the need to move Windows accounts from one domain to another, use Windows-linked user group accounts. Windows-linked user group accounts, and the user accounts they contain, can be moved from one domain to another while keeping security permissions for the group accounts intact. Individual Windows-linked user accounts must be deleted and then re-created in the new domain, causing all security permissions for the user accounts to be lost.

Always have at least one Windows-linked user account that is a member of the FactoryTalk Administrators group. This prevents an inadvertent lock out of the FactoryTalk system. If the Windows-linked administrator account is locked out, for example because the user exceeds the maximum number of logon tries, the Windows domain administrator can reset the account. Alternatively, the user can wait until Windows automatically resets and frees the locked-out account. When this happens depends on the account lockout duration policy in Windows. For details, see Windows Help.

## Rules for using FactoryTalk accounts and Windows-linked accounts

- FactoryTalk user accounts cannot be members of Windows-linked user groups.
- Both of the Windows-linked user group and individual Windows-linked user accounts can be members of FactoryTalk user groups. This allows you to use FactoryTalk user groups when setting permissions.
- A FactoryTalk user account or Windows-linked user account can be a member of more than one FactoryTalk user group.



Note: If an action is set to **Deny** for the user in any one group, then the **Deny** takes precedence over any **Allow** setting in a different group of which the user is a member.

## See also

[How security authenticates user accounts](#) on [page 32](#)

[Accounts and groups](#) on [page 16](#)

[Manage users](#) on [page 43](#)

[Manage user groups](#) on [page 51](#)

[Secure resources](#) on [page 135](#)

## Applications and areas

In a FactoryTalk Directory, elements such as data servers, alarm and event servers, device servers, HMI servers, and project information are organized into *applications*. A FactoryTalk Directory holds any number of applications, stores information about each application, and makes that information available to FactoryTalk products and services.

A FactoryTalk network directory can manage any number of separate network applications. Likewise, a FactoryTalk local directory can manager any number of separate local applications. When developing a FactoryTalk system, log on to either a network directory or a local directory, create an application, add device servers, data servers, and optional alarm and event servers.

*Areas* organize and subdivide applications in a network directory into logical or physical divisions. For example, separate areas might correspond with separate manufacturing lines in one facility, separate plants in different geographical locations, or different manufacturing processes.

HMI Servers are added and configured using FactoryTalk View Studio, but their status can be viewed in FactoryTalk Administration Console. The root of an application in a network directory can contain only one HMI server. Create a separate area for each HMI server added to an application. Areas cannot be created within a local application.

### See also

[FactoryTalk Directory types](#) on [page 15](#)

[FactoryTalk systems](#) on [page 13](#)

## Security in a FactoryTalk system

FactoryTalk Security is intended to improve the security of an automation system by limiting access to users with a legitimate need. Security in FactoryTalk is accomplished through authentication and authorization. Security services are managed separately in the FactoryTalk local directory and the FactoryTalk network directory.

### Authentication

FactoryTalk authenticates the user's identities to access a FactoryTalk system against a defined set of user accounts held in the FactoryTalk Directory. FactoryTalk verifies a user's identity and that a request for service actually originates with that user.

## Authorization

FactoryTalk authorizes user requests to access resources in a FactoryTalk system against a set of defined access permissions held in the FactoryTalk Directory.

## Securing resources

FactoryTalk Security addresses both authentication and authorization concerns by helping define the answer to this question:

*"Who can carry out what actions upon which secured resources from which locations?"*

- *Who*—refers to users and groups of users. Different users need different access rights.
- *Actions*—refers to the operations to perform on a resource, such as read, write, update, download, create, delete, edit, insert, and so on.
- *Secured resources*—refers to the objects for which actions are secured. Each FactoryTalk product defines its own set of resources. For example, some products might allow configuring security on resources in an area, while others might allow configuring security for logic controllers and other devices.
- *Locations*—refers to the location of the authorized computers. For example, allowing values to be downloaded to a controller only from workstations that are located within a clear line of sight to the plant floor machinery to adhere to safety requirements.

The principle of inheritance determines how access permissions are set. For example, when assigning security to an area in an application, all of the items in the area inherit the security settings of the area. Override this behavior by setting up security for one or more of the individual objects inside the area as well.

When a user attempts to log on to a FactoryTalk system, FactoryTalk Security verifies the user's identity. If the user is authenticated, FactoryTalk Security continues to check the user's level of access to the system, to authorize the actions the user performs on secured resources.

System-wide policies dictate some security settings. For example, setting up a policy that requires users to change their passwords once every 90 days.

## See also

[Permissions](#) on [page 135](#)

[Best practices](#) on [page 34](#)

[FactoryTalk systems](#) on [page 13](#)

## Example: Two directories on one computer

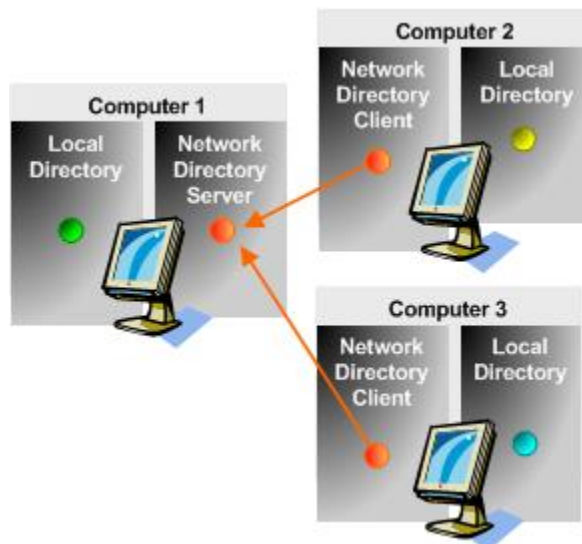
Different software products have different requirements for the FactoryTalk Directory. Both directories are installed and configured as part of installing the FactoryTalk Services Platform. The directory needed depends upon which software products are used and whether working in a stand-alone or a networked environment.

For example, if using FactoryTalk View SE or FactoryTalk Transaction Manager, use the network directory to create and manage network applications. If using FactoryTalk View ME, use the local directory to create and manage local applications. Other products, such as RSLogix 5, RSLogix 500, and FactoryTalk Linx, allow using either directory.

Even though a local directory and a network directory reside on the same computer, all of their project information and security settings remain completely separate and cannot be shared, including:

- User accounts, passwords, security permissions
- System-wide policy settings, including security and audit policies
- Project information, such as applications, areas, and their contents

The graphic below shows three computers. Each computer has both a local directory and a network directory configured. Each directory holds objects, which represent project information, such as applications, references to data servers, and security settings, including user accounts. In each local directory, access to these project objects is only by software products installed on that same local computer. The network directory, however, can share references to its objects across a network.



For example, suppose each colored icon above represents the project information and security settings that are part of a FactoryTalk system. The local directories on each computer hold completely separate sets of information (represented by the green, blue, and yellow icons). In the network directory case, all client computers that point to the same network directory server computer share the same set of information across the network (represented by the orange icons).

Run FactoryTalk Administration Console on Computer 3, log on to the network directory, and create a user account named "Terry" with the password "OpenSesame." The change is actually made in the network directory server, held on Computer 1, and immediately reflected on each network directory client computer. "Terry" can now log on to the network directory from any of the three computers.

Now create a user account named "Terry" with the password "OpenSesame" in each Local Directory on every computer. Even though the user name and password are the same, each user account is a separate object in each local directory.

When changing the password in the local directory on Computer 1, the change does not affect the user account held in the network directory server on the same computer, nor does it affect the user accounts held in the local directories on computers 2 and 3.

### See also

[Applications and areas](#) on [page 20](#)

[FactoryTalk Directory types](#) on [page 15](#)

[FactoryTalk systems](#) on [page 13](#)





## Install FactoryTalk Services Platform

### Install FactoryTalk Services Platform

FactoryTalk Services Platform and FactoryTalk Security software are not installed separately — FactoryTalk Security is an integrated part of the FactoryTalk Services Platform.

FactoryTalk Services Platform is installed from either:

- A FactoryTalk product installation disc, such as FactoryTalk View (FactoryTalk Services Platform software is included on the installation disc of every product that requires it); or,
- The Rockwell Automation Product Compatibility and Download Center (PCDC) website. On the Compatibility & Downloads page, click **Find Downloads**. On the **Find Downloads** page, in the **Search** box, type "FTSP". **FTSP-Download FT Services Platform** appears in your download list.

To install FactoryTalk Services Platform, you must log on to Windows with a user account that is a member of the Windows Administrators group on the local computer.

Install FactoryTalk Services Platform on every computer where you plan to develop or run Network or Local applications. During installation several components are installed on the computer, if any prerequisite software components are not present on a computer, the installation program will attempt to install the software.

Platform components and services currently include:

- FactoryTalk Directory
- FactoryTalk Security
- FactoryTalk Diagnostics
- FactoryTalk Live Data
- FactoryTalk Administration Console – a stand-alone tool for configuring, managing, and securing applications.

All of these components and services install together as a platform, integrated into the software install process for each FactoryTalk-enabled product.

FactoryTalk Web Services is not installed by default, and must be installed separately.

**Tip:** FactoryTalk Services Platform establishes a Network Directory server when installed, other computers on which FactoryTalk Services Platform is installed will be client computers. Determine which computer in the system is going to be used as the directory server and note this computer name. After FactoryTalk Services Platform is installed on the client computers, run the **FactoryTalk Directory Server Location Utility** and identify the computer name of the Network Directory server.

## Network security

For the latest network security considerations when using Rockwell Automation products, visit the Rockwell Automation Knowledgebase.

For information about:

- File extensions created by Rockwell Automation software, firewall rules, and service dependences, see Knowledgebase Document ID: [PN826 - Security considerations when using Rockwell Automation Software Products](#).
- TCP/UDP ports used by Rockwell Automation products, see Knowledgebase Document ID: [BF7490 - TCP/UDP Ports Used by Rockwell Automation Products](#).

## See also

[Product Compatibility and Download Center](#)

[FactoryTalk Web Services](#) on [page 211](#)

[Upgrade FactoryTalk Services Platform](#) on [page 209](#)

## Install FactoryTalk System Services and FactoryTalk Policy Manager

FactoryTalk Services Platform version 6.11.00 includes two optional components that are used to manage CIP Security; FactoryTalk System Service and FactoryTalk Policy Manager.

FactoryTalk System Services provides these core security services:

- **Authentication Service**  
Authenticates users and validates user resource requests. Validate user credentials against the FactoryTalk Directory and FactoryTalk security policy settings to obtain privileges associated with the user.
- **Certificate Service**  
Issues and manages X.509v3 certificates for use within the FactoryTalk system.
- **Deployment Service**  
Translates the security policy model defined using FactoryTalk Policy Manager to CIP configurations that are delivered to endpoints.
- **Diagnostics Service**

Makes FactoryTalk audit and diagnostic logs available as a web service.

- Policy Service

Used to build and manage CIP network trust models and define security policy for the CIP endpoints.

Use FactoryTalk Policy Manager to configure, deploy, and view the FactoryTalk system security policy configuration.

FactoryTalk Policy Manager is dependent upon the FactoryTalk System Service and must be installed together on the network directory server. FactoryTalk Policy Manager is a web service, and does not need to be installed on additional computers.

On a new installation of FactoryTalk Services Platform 6.11.00 select **Customize** on the first page of the installation wizard to include these items in the installation process.

### **To install FactoryTalk System Service and FactoryTalk Policy Manager when FactoryTalk Services Platform 6.10 is already installed**

1. Log in to FactoryTalk on the computer hosting the FactoryTalk network directory,
2. Run FTUpdater to make sure you have the latest update of FactoryTalk Services Platform.
3. Run FactoryTalk Services Platform setup.exe.
4. In the FactoryTalk Security installation wizard, select **Modify**.
5. Expand the item for FactoryTalk Services Platform v6.10.00.
6. Select **FactoryTalk Policy Manager**. FactoryTalk System Service is automatically selected.
7. Select **Modify**.
8. The installation proceeds.

### **See also**

FactoryTalk Policy Manager



## Getting started with FactoryTalk Security

This chapter introduces you to key parts of FactoryTalk Security, including:

- FactoryTalk Administration Console
- Action groups
- Policies
- Computers and groups
- Networks and devices
- Users and groups
- Single sign-on
- Tightening security

### FactoryTalk Security

FactoryTalk Security improves the security of your automation system by limiting access to those with a legitimate need. FactoryTalk Security authenticates the identities of users, and authorizes user requests to access a FactoryTalk system against a set of defined user accounts and access permissions held in the FactoryTalk local directory or FactoryTalk local directory.

### Integrated security services for your FactoryTalk system

FactoryTalk Security provides security services integrated into both the FactoryTalk local directory and the FactoryTalk local directory. In a local directory, all project elements are located on a single computer, and the FactoryTalk Administration Console system cannot be shared across a network. A network directory organizes information about project elements from multiple FactoryTalk products across multiple computers on a network. Even though a local directory and a network directory are always present on the same computer, all of their project elements remain completely separate and cannot be shared.

### Authentication and authorization

Using FactoryTalk Security with Rockwell Automation software for an integrated, cross-product solution to two universal security concerns: authentication and authorization.

- **Authenticate**—verify a user's identity and verify that a request for service actually originates with that user.

- **Authorize**—verify a user's request to access a software resource against defined access permissions.

FactoryTalk Security addresses both authentication and authorization concerns and defines the answer to the question:

*"Who can carry out what actions upon which secured resources from where?"*

- *Who*—refers to users and groups of users. Different users need different access rights.
- *What actions*—refers to the actions that can be performed on a resource, such as read, write, update, download, create, delete, edit, insert, and so on.
- *Which secured resources*—refers to the objects for which actions are secured. Each FactoryTalk product defines its own set of resources. For example, some products might allow security configuration on resources in an area, while others might allow security configuration for logic controllers and other devices.
- *Where*—allows security to differ based on machine location. It is sometimes important to restrict certain actions to specific workstations. For example, for safety reasons, it might be necessary to allow downloading values to a controller only from workstations that are located within a clear line of sight to the plant floor machinery that are affected by the downloads.

The principle of inheritance determines how access permissions are set. For example, assigning security to an area in an application, all of the items in the area inherit the security settings of the area. Override this behavior by setting up security for one or more of the individual objects inside the area.

At runtime, when a user attempts to log on to a FactoryTalk system, FactoryTalk Security verifies the user's identity. If the user is authenticated, FactoryTalk Security continues to check the user's level of access to the system, in order to authorize the actions the user performs on secured resources.

System-wide policies dictate some security settings. For example, you can set up a policy that requires users to change their passwords once every 90 days.

### See also

[How security authenticates user accounts](#) on [page 32](#)

[Things you can secure](#) on [page 32](#)

[Best practices](#) on [page 34](#)

[Permissions](#) on [page 135](#)

[Secure resources](#) on [page 135](#)

## Security on a local directory

By default, security is open in the FactoryTalk local directory. All users who have successfully logged on to Windows have full access to the local directory.

Because the network directory and local directory are separate, secure them separately. Some Rockwell Automation software products require the FactoryTalk network directory, others require the FactoryTalk local directory, and some require both directories to be configured.

Manage on a local directory:

- User accounts, passwords, and security permissions
- System-wide policy settings, including security and audit policies
- Product information, such as applications, areas, and their contents

To tighten security on a stand-alone system, perform these tasks:

- Delete the Windows-linked group named **Authenticated Users**. This prevents all users who have successfully logged on to Windows from automatically having access to the FactoryTalk local directory.
- Remove security settings that allow all users to have full access to the FactoryTalk local directory.
- Modify security policies to secure the system.

### See also

[Delete a user group](#) on [page 56](#)

[Secure resources](#) on [page 135](#)

## Security on a network directory

By default, security is open in the FactoryTalk network directory. This means that all users who are logged on to Windows with a user account that is a member of the local Windows Administrators group on any computer connected to the network directory have full access to the directory.

Because the network directory and local directory are separate, secure them separately. Some Rockwell Automation software products require the FactoryTalk network directory, others require the FactoryTalk local directory, and some require configuring both directories.

Key steps to tighten security in a distributed system on a network include:

- Create one or more FactoryTalk user accounts or Windows-linked user accounts, then add those accounts to the **FactoryTalk Administrators** group. This retains administrative access to the FactoryTalk Directory after removing the Windows Administrators group in the next step.
- Remove the Windows-linked group named **Authenticated Users**. This prevents all user accounts on any local computer connected to the network directory from automatically having access to the network directory.
- Remove the security settings that allow all users full access to the FactoryTalk network directory.

- Modify security policies to secure the system.

### See also

[Delete a user group](#) on [page 56](#)

[Secure resources](#) on [page 135](#)

## How security authenticates user accounts

When a user attempts an action that is secured, security authenticates user names and passwords in this order:

1. Against the list of FactoryTalk user accounts. If a match is found, the user is allowed to proceed.
2. Against the list of Windows-linked user accounts. If a match is found, the user is allowed to proceed.
3. Against the list of accounts in a Windows-linked user group. If a match is found for the user name and password in a Windows-linked user group, the user is allowed to proceed, even if no Windows-linked user account is present for that user.

To prevent some users in a Windows-linked group from having access to the FactoryTalk system, create Windows-linked accounts for those users, and then set permissions to deny access to those user accounts.

### See also

[Permissions](#) on [page 135](#)

[Account types](#) on [page 18](#)

[FactoryTalk Security](#) on [page 29](#)

## Things you can secure

Use **Allow** or **Deny** permissions to secure access to resources in the system. Resources include:

- The FactoryTalk network directory or local directory
- The System folder and its contents
- Applications
- Areas
- Servers
- Control networks
- Hardware devices



## Security for resources is always tied to users, actions, and computers

Security for resources is always tied to users or groups of users, the actions they are performing, for example, read or write, and the computers, or groups of computers where they are working.

This helps ensure that only authorized personnel can perform actions on the equipment and resources in the system from appropriate locations, for example, computers located within line of sight of equipment.

In a local FactoryTalk directory, a user can perform actions only from the local computer.

## Set permissions to restrict actions to users, user groups, computers, or computer groups

For each resource, for example, an application, or an area within it, restrict actions such as writing values, to particular users or groups of users. In a network directory, actions can be restricted to particular computers, or groups of computers.

Group actions together and assign security permissions to all actions in the group. For example, assign permissions to an area so that only operators working on computers located within the line of sight of heavy machinery can write values to the programmable controllers in that area.

Suppose that:

- The area is named "Punch Presses"
- The operators belong to a user group named "Operators"
- The computers within line of sight of the machinery belong to a computer group named "Heavy Machinery"

First, clear **Allow** for **All Users and All Computers** in the Punch Presses area. Next, select **Allow** for the user group Operators and the computer group Heavy Machinery.

When setting permissions, **Deny** permissions are implied unless **Allow** permissions are specified explicitly. Clearing **Allow** ensures that all users are denied write access, except those explicitly allowed access.

## Using the Security item

Right-click an item in the **Explorer** and select **Security**, to set up which users or user groups on which computers may access the selected resource.

**IMPORTANT** Right-clicking the **System** folder, **Users and Computers** folder, **Users** folder, or the **Computers** folder, and specifying security permissions sets security on that actual folder. It does not limit users' access to the system.

To limit access to resources in the FactoryTalk system, right-click the resource to secure, select **Security**, and specify security permissions for the user and computer accounts allowed to access the resource.

---

## Security settings are separate in the network and local directory

Security settings are completely separate in the network directory and local directory. Changes made to the security settings in the network directory do not affect the local directory and vice versa. If using both a network directory and a local directory, set up security in each directory separately.

## Security settings apply to all FactoryTalk products

Security settings configured for resources apply to all FactoryTalk products in the system. For example, when denying a user **Read** access to an area from a particular computer, that user cannot see that area in any FactoryTalk product while working from that computer.

## See also

[Permissions](#) on [page 135](#)

[Best practices](#) on [page 34](#)

[Actions](#) on [page 140](#)

[FactoryTalk Security](#) on [page 29](#)

## Best practices

Use these tips when setting up the FactoryTalk system to achieve efficient management of user authentication and authorization.

## Administrator accounts

- Always have more than one user account that is a member of the FactoryTalk Administrators group. If the password to one administrator account is lost, use a second administrator account to reset the password to the first one. A lost password to a user account is not recoverable. A second administrator account prevents being locked out of the FactoryTalk system if the first administrator password is lost.
- Always have at least one Windows-linked user account that is a member of the FactoryTalk Administrators group. If the Windows-linked administrator account is locked out, for example because the

user exceeds the maximum number of logon tries, the Windows domain administrator can reset the account. Alternatively, the user can wait until Windows automatically resets and frees the locked-out account. The wait time depends on the Account lockout duration policy in Windows.

## Windows-linked accounts

If Windows accounts might move from one domain to another, avoid using individual, Windows-linked user accounts. Use Windows-linked user group accounts instead. Windows-linked user group accounts can move from one domain to another, while keeping security permissions for the group accounts intact. Windows-linked user accounts must be deleted and then recreated in the new domain, causing the loss of all security permissions for the user accounts. If this occurs all permissions for any individual Windows-linked user accounts must be recreated.

## Permissions

- Assign permissions to groups rather than to users.
- Assign permissions to user accounts only by exception. Maintaining user accounts directly is inefficient.
- Wherever possible, remove **Allow** permissions instead of assigning explicit **Deny** permissions. The order of precedence of explicit permissions over inherited permissions makes administration simpler, and **Deny** permissions take precedence over **Allow** permissions.
- Use **Deny** permissions to:
  - Exclude a subset of a group that has **Allow** permissions
  - Exclude one special permission when full control to a user or group is already granted
- Assign permissions at the highest level possible. This provides the greatest breadth of effect with the least effort. Establish rights that are adequate for the majority of users. For example, assign security to areas rather than to objects within areas.
- Administrators should use an account with restrictive permissions to perform routine, non-administrative tasks. Use an account with broader permissions only when performing specific administrative tasks.

## See also

[FactoryTalk Security](#) on [page 29](#)

[Account types](#) on [page 18](#)

[Permissions](#) on [page 135](#)

## Audit trails and regulatory compliance

To achieve compliance in regulated industries, the plant might be required to keep records that answer these questions:

- Who performed a particular operation on a specific resource?
- Where did the operation occur?
- When did the operation occur?
- Who approved the operation?

To answer these questions:

- Ensure that all users are uniquely identifiable in the system
- Keep a record of deleted users
- Log information about user and system activity to diagnostic log files
- Set up audit trails of successful or unsuccessful attempts at modifying system values

### Ensure that all users are uniquely identifiable in the system

When choosing user names, ensure that they are unique.

- A user should have the same user name on every computer. This is mostly for convenience, both for the user and for the administrator.
- A particular user name should always refer to the same person. A system in which the same user name refers to more than one person is never really secure.

Develop a scheme for identifying users uniquely. Keep in mind that user names are visible, and should not contain any private information, for example, social security numbers. User names are also typed frequently, and should be relatively easy to remember.

If the system is required to comply with governmental regulations, multiple names for the same user may be necessary. This may occur if a user leaves the company and their user account is deleted, then the user is rehired.

### Keep a record of deleted users

To ensure that all user accounts remain unique, keep track of deleted accounts. This might also be an audit requirement, such as tracking a user's actions throughout the system, even after the user's account was deleted.

To ensure that only unique user accounts are created, enable the security policy **Keep record of deleted accounts**. To avoid a trial-and-error process of creating unique user accounts, make deleted accounts visible in lists of users by enabling the security policy **Show deleted accounts in user list**.

## Log information about user and system activity to diagnostic log files

Logging information consists of two steps:

1. Choose the information to log and then send the information to FactoryTalk Diagnostics. For example, enable audit logging to record what changes were made to security policies or other objects, who made the changes, and when they were made. If the **Audit configuration and control system changes** policy is not enabled, FactoryTalk Diagnostics does not receive any audit messages, and cannot store the audit messages in log files.
2. Configure FactoryTalk Diagnostics to store the information in log files. For example, configure FactoryTalk Diagnostics to store audit information for Operators in local log files. If this step is not completed, FactoryTalk Diagnostics receives the chosen information sent to it, but does not capture this information to store in log files.

To configure FactoryTalk Diagnostics routing and logging options, select **FactoryTalk Diagnostics Setup** from the **Tools** menu on each computer where the FactoryTalk Administration Console or FactoryTalk View is installed. To view diagnostic messages, from the **Tools** menu, select **FactoryTalk Diagnostics > Viewer**.

## Set up audit trails of successful or unsuccessful attempts at modifying system values

The most common type of auditing activity is recording failures. This helps trace failures, and isolate and correct their causes.

In some industries it is also common, or mandated by law, that certain types of successful user activity is audited. For example, when making pharmaceutical drugs, any changes or adjustments in recipes must be recorded. Recording this activity allows any problems that might occur to be traced to a specific batch of the product.

Auditing object access success or failure is controlled by system-wide audit policies. Enable these policies if the plant requires them. Audit information is sent to FactoryTalk Diagnostics. Use the FactoryTalk Diagnostics Viewer to monitor security-related events.

### See also

[Monitor security-related events](#) on [page 90](#)

[Audit policies](#) on [page 87](#)

## Configure a computer to be the FactoryTalk Directory network server

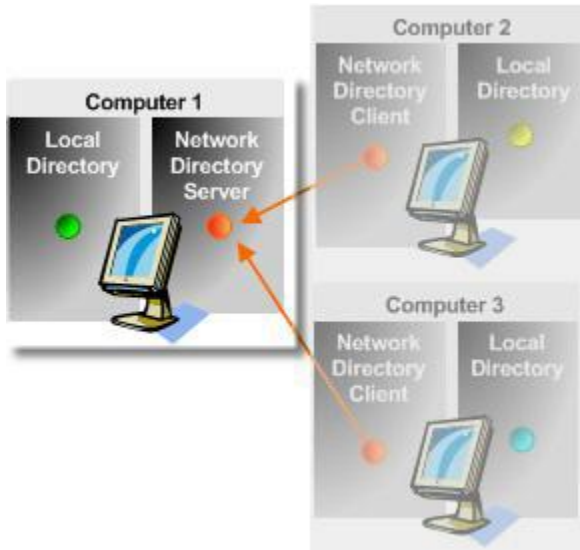
FactoryTalk Services Platform configures both a network directory and a local directory on every computer where it is installed.

Use a network directory to organize project information and security settings from multiple FactoryTalk products across multiple computers on a network. After installing and activating FactoryTalk software, specify one of the computers on the network as the network directory server. All computers on the network to share FactoryTalk network directory services and resources.

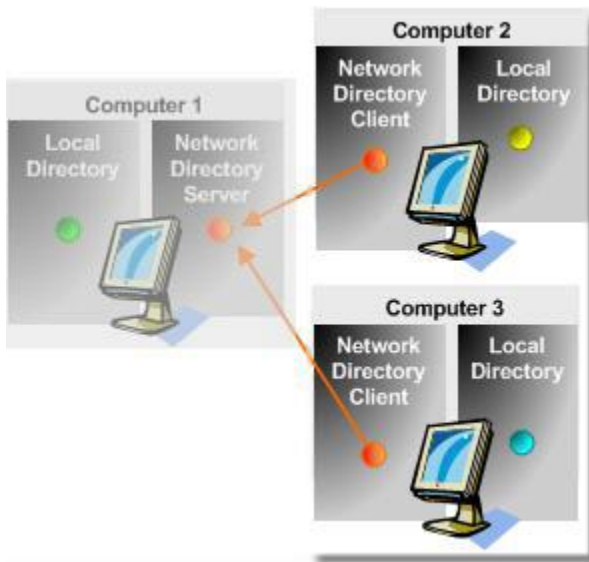
Products such as FactoryTalk View SE and FactoryTalk Transaction Manager use the network directory.

### Example: Network directory

Computer 1 serves as the network directory server.



Client computers (Computer 2 and Computer 3) are configured to point to Computer 1 as the network directory server computer.



**See also**

[Configure a computer to be the network directory server](#) on [page 39](#)

[Configure a network directory client computer](#) on [page 39](#)

[Check network directory server connection status](#) on [page 40](#)

[FactoryTalk Directory Server Location Utility](#) on [page 41](#)

## Configure a computer to be the network directory server

After installing and activating FactoryTalk software, specify one computer on the network as the network directory server. All computers on the network can share FactoryTalk network directory services and resources.

After configuring the network directory server, configure the client computers to reference the network directory.

### To configure a computer to be the network directory server

1. On the computer to use as the Network Directory Server, go to **Rockwell Software > FactoryTalk Tools** and open **Specify FactoryTalk Directory Location**.
2. At the prompt, log on to the network directory with a Windows Administrator account.
3. In **FactoryTalk Directory Server Location Utility**, select **Browse**.
4. In **FactoryTalk Directory Server Configuration**, select **This computer** to use the network directory server installed on this computer, and select **OK**.

**See also**

[Check network directory server connection status](#) on [page 40](#)

[Configure a network directory client computer](#) on [page 39](#)

[FactoryTalk Directory Server Location Utility](#) on [page 41](#)

## Configure a network directory client computer

After specifying one of the computers on the network as the network directory server, use the **Specify FactoryTalk Directory Location** utility to point each computer in the network to the FactoryTalk Directory network directory server.

### To configure a network directory client computer

1. On each participating network directory client computer, go to **Rockwell Software > Specify FactoryTalk Directory Location**.
2. At the prompt, log on to the network directory with a Windows Administrator account.
3. In **FactoryTalk Directory Server Location Utility**, select **Browse**.

4. In **FactoryTalk Directory Server Configuration**, select **Remote computer**, then specify the name of the computer to use as the network directory server, and select **OK**.
5. When prompted, log on to the network directory.

If single sign-on is enabled on the computer when the location of the network directory server changes, the single sign-on session terminates. Log on to the new network directory server. The user name and password entered become the new single sign-on credentials for all participating FactoryTalk products on the computer.

### See also

[Configure a computer to be the network directory server](#) on [page 39](#)

[Check network directory server connection status](#) on [page 40](#)

[FactoryTalk Directory Server Location Utility](#) on [page 41](#)

## Check network directory server connection status

When a connection to the FactoryTalk network directory server is lost, the system sends an error message to FactoryTalk Diagnostics. Likewise, when the connection is restored, the system sends an information message to FactoryTalk Diagnostics. Run the **FactoryTalk Diagnostics Viewer** to check FactoryTalk Diagnostics for connection and error messages.

The network directory connection status is available from the **FactoryTalk Directory Server Location Utility**.

When opening a network application and a connection to the network directory server is not available, the information is based on the data held in a local cache. While disconnected, FactoryTalk Administration Console operates in read-only mode and does not allow most commands and operations.

### To check network directory server connection status

1. In FactoryTalk Administration Console select **Tools > FactoryTalk Directory Server Options**.
2. If a **User Account Control** prompt appears, select **Yes**.
3. In the **FactoryTalk Directory Server Location Utility**, next to **Computer hosting directory server**, the current status of the active server is displayed. Either:
  - **(connected)** — All FactoryTalk products and components participating in a FactoryTalk system, located on the current computer, are connected to and communicating with the network directory server computer.
  - **(read-only)** — The FactoryTalk system on the current computer is disconnected from the network directory server and is retrieving information from a local cache.



- **(unknown)** — The connection status is temporarily unknown because the system is starting up, waiting to determine which server is active, or is unable to determine the current state.

### See also

[Configure a computer to be the FactoryTalk Directory network server](#) on [page 38](#)

[FactoryTalk Directory Server Location Utility](#) on [page 41](#)

How do I open the FactoryTalk Directory Server Location Utility?

Either:

- Go to **Rockwell Software > Specify FactoryTalk Directory Location**.
- From the **FactoryTalk Administration Console**, select **Tools > FactoryTalk Directory Server Options**.

Use the **FactoryTalk Directory Server Location Utility** to:

- Specify the computer that is hosting the network directory server
- Point each computer on the network to the network directory server computer

### See also

[Configure a computer to be the network directory server](#) on [page 39](#)

[Configure a network directory client computer](#) on [page 39](#)

[FactoryTalk Directory types](#) on [page 15](#)

[Check network directory server connection status](#) on [page 40](#)

## FactoryTalk Directory Server Location Utility



## Manage users

### Manage users

Use FactoryTalk Administration Console to add and delete FactoryTalk Directory and Windows-linked user accounts. User accounts exist only in the FactoryTalk Directory where the account was created.

Management of FactoryTalk user accounts includes:

- Adding group memberships to the user account
- Editing the user's name and description
- Associating an email address with the user's account
- Setting user password options
- Changing the user account password
- Enabling, disabling, or unlocking the user account
- Resetting the account password

Use Windows administrative tools to edit Windows-linked user accounts.

---

**IMPORTANT** Managing users requires explicit permissions. To verify permissions, in FactoryTalk Administration Console **Explorer**, expand **System**, then right-click **Users and Groups** and select **Security**. Confirm the permissions listed in the prerequisites for the task are present with the logged in user account.

---

### See also

[Add a FactoryTalk user account](#) on [page 43](#)

[Add a Windows-linked user account](#) on [page 45](#)

[Add group memberships to a user account](#) on [page 46](#)

[Manage user groups](#) on [page 51](#)

### Add a FactoryTalk user account

To create a user account that is separate from a user's Windows account, add a FactoryTalk Directory account. FactoryTalk Directory accounts are managed by the FactoryTalk Administrator and specify the account's identity, account policy, and group membership independent of the Windows account settings.

### Prerequisites

Obtain these permissions for the **Users** folder in the **Explorer** window:


- Common > Create Children
- Common > List Children

- Common > Read

## To add a user account

1. In **Explorer**, expand **System > Users**.
2. Right-click the **Users** folder, point to **New**, and then select **User**.
3. In **New FactoryTalk User**, type a short name for the user in **User Name**, and the full name of the user in **Full name**.
4. (optional) In **Description**, record information about the user, such as the user's position or phone number.
5. (optional) In **E-mail**, add a single e-mail address. Some FactoryTalk products may send messages to this e-mail address.
6. In **Login method** select how the user logs on to FactoryTalk.
  - **Password**. The user types the user name and password to logon.
  - **Badge only**. The user taps the badge on the card reader to logon.
  - **Password and Badge**. The user taps the badge on the card reader and types the username and password to logon.

Badge logon is not supported on remote clients connecting via Remote Desktop Services. To log on using an RFID badge, connect an rf IDEAS card reader to the computer hosting the FactoryTalk Services Platform.

7. If a password method was selected, in **Password**, type a password for the user account. **Password Policy Settings** in **Security Policy Properties** determine the requirements for a valid password.
  -  **Tip:** The maximum password length is 64 characters. However, the dialog box only displays 35 characters. Characters not shown are still included in the password.
8. In **Confirm**, type the same password entered in the previous step.
9. (optional) If a password method was selected for login, select the user's password validity settings:

- **User must change password at next logon**
  - Select to force the user to change the account password at next system log on.
  - Clear to allow the user to keep the same password.
- **User cannot change password**
  - Select to prevent the user from changing the account password.
  - Clear to allow the user to change the account password.
- **Password never expires**
  - Select to allow the user to continue using the same password indefinitely.
  - Clear to require that the user change the account password at intervals specified by the security policy **Password Policy Settings**.

10. In **Badge ID** type the identification number of the badge assigned to the user account.

Select **Scan** and then tap the badge on the card reader to obtain the **Badge ID** value from the badge.

11. Select **OK** to add the user to the FactoryTalk Directory.

## See also

[Add a Windows-linked user account](#) on [page 45](#)

[Delete a user account](#) on [page 48](#)

[Password Policy Settings](#) on [page 106](#)

[Account types](#) on [page 18](#)

[Manage users](#) on [page 43](#)

## Add a Windows-linked user account

Add a Windows-linked user account when the security needs of the Windows network are the same as the security needs of the FactoryTalk system. When accessing FactoryTalk resources using a Windows-linked account, the FactoryTalk Directory relies on Windows to determine whether the user's name and password are valid, and whether the account is enabled or locked out. Adding Windows-linked user accounts to FactoryTalk Security user groups allows the FactoryTalk Directory to determine a Windows-linked user's level of access to the FactoryTalk system independently of the user's level of access to a Windows domain.

Add user accounts to the FactoryTalk network directory or local directory from the list of users or groups in a Windows domain or workgroup. If the computer is disconnected from the Windows domain, reconnect to the domain before adding Windows-linked user accounts. Any users who previously logged on to the Windows domain from that computer can log on to FactoryTalk using their Windows-linked user account while the computer is disconnected from the Windows domain.

## Prerequisites

Adding a Windows-linked user account requires these permissions:

- Common > Create Children
- Common > List Children
- Common > Read

## To add a Windows-linked user account

1. In FactoryTalk Administration Console **Explorer**, expand **System > Users**.

2. Right-click the **Users** folder, point to **New**, and select **Windows-Linked User**.
3. In **New Windows-Linked User**, select **Add**.
4. In **Select Users**, select the Windows user accounts to link to the FactoryTalk system.
  - If known, type the names of the user accounts to add in the text box. For domain accounts, use the format DOMAIN\username, for workgroup accounts use the format COMPUTERNAME\username. To validate the user names, select **Check Names**. Correct any errors, and select **OK**.
  - To search for user names, or to select multiple users, select **Advanced**. In **Select Users**, select **Locations**, select the domain or workgroup from which to select users, and select **OK**.  
Alternatively, use the **Common Queries** settings to search by name. Select **Find Now**. In the list of users, select the user accounts to add, and select **OK**.
5. When finished selecting Windows user accounts in **Select Users**, select **OK**.
6. In **New Windows-Linked User**, review the list of users.
  - To remove any users added unintentionally, select the users, and select **Remove**.
  - To add more users, repeat steps 3, 4, and 5.
7. Select **OK**.

### See also

[Add a FactoryTalk user account](#) on [page 43](#)

[Delete a user account](#) on [page 48](#)

[Add group memberships to a user account](#) on [page 46](#)

[Remove group memberships from a user account](#) on [page 47](#)

[Manage users](#) on [page 43](#)

## Add group memberships to a user account

To quickly change the permissions for a user account to those of an existing FactoryTalk user group, assign the user account to the user group. New group memberships take effect only when the user logs off FactoryTalk and then logs on again.

### Prerequisites

Changing the group memberships of a user account requires these permissions:

- Common > List Children
- Common > Read
- Common > Write

### To add group memberships to a user account

1. In FactoryTalk Administration Console **Explorer**, expand **System > Users**, right-click the user account, and select **Properties**.
2. On the **Group Membership** tab, select **Add**.
3. In **Select User Group**, select the groups to which the user account belongs, and then select **OK**.
4. In **User Properties**, select **OK**.

### See also

[Remove group memberships from a user account](#) on [page 47](#)

[Manage user groups](#) on [page 51](#)

[Permissions](#) on [page 135](#)

[FactoryTalk Security](#) on [page 29](#)

[Account types](#) on [page 18](#)

## Remove group memberships from a user account

When a user account belongs to a user group, the user account automatically inherits all permissions assigned to the group, unless permissions are specifically denied for the user account.

Delete a group from **Group Membership User Properties** to remove the link between the permissions of the user account and the permissions assigned to that user group.

Changes to group memberships take effect only when the user logs off FactoryTalk and then logs on again.

### To remove group memberships from a user account

1. In FactoryTalk Administration Console **Explorer**, expand **System > Users**, right-click the user account containing the group memberships to change, and select **Properties**.
2. Select the **Group Membership** tab.
3. In the list of groups, select the groups and select **Remove**.
4. In **User Properties**, select **OK**.

## See also

[Add group memberships to a user account](#) on [page 46](#)

[Manage user groups](#) on [page 51](#)

[Permissions](#) on [page 135](#)

[FactoryTalk Security](#) on [page 29](#)

[Account types](#) on [page 18](#)

## Delete a user account

Delete a user account to permanently remove the account from the FactoryTalk Directory. To prevent inadvertently locking an account out of the FactoryTalk Directory, do not delete the last user account that is a member of the Administrators group.

To delete a user account from both a network directory and a local directory, delete the account from one directory, log off that directory, log on to the second directory, and then delete the account in the second directory.

To temporarily prevent a user from logging on to FactoryTalk, disable the FactoryTalk user account.

## Prerequisites

Deleting a user account that is a member of a user group requires these permissions:

- Common > Delete
- Common > List Children
- Common > Read
- Common > Write

Deleting a user account that is not a member of a user group requires these permissions:

- Common > Delete
- Common > List Children
- Common > Read

## To delete a user account

- In FactoryTalk Administration Console **Explorer**, expand **System > Users**, right-click the user account, and then select **Delete**.



Tip: You can only create an account using the name of a deleted account if the security policy **Keep record of deleted accounts** is disabled. You must still recreate the security settings of the user accounts.



## See also

[Add a FactoryTalk user account](#) on [page 43](#)



## Manage user groups

### Manage user groups

Use FactoryTalk Administration Console to add and delete FactoryTalk and Windows-linked user group accounts. Add both FactoryTalk and Windows-linked user accounts to FactoryTalk user group accounts. Windows-linked user groups, and the user accounts they contain, can move from one domain to another while keeping security permissions for the group accounts intact.

FactoryTalk Services Platform includes these built-in user groups:

Group Name	Description
Administrators	Add user accounts to the Administrators user group to grant those user accounts full control of areas, applications, users, and groups in the FactoryTalk Directory. These permissions are defined by default.
Engineers	No users or permissions are defined by default in FactoryTalk Services Platform. Other software may use this group to establish permission sets.
Maintenance	No users or permissions are defined by default in FactoryTalk Services Platform. Other software may use this group to establish permission sets.

Key points about user groups:

- User group accounts exist only in the FactoryTalk Directory in which created.
- FactoryTalk user accounts cannot be members of Windows-linked user groups.
- Both of the Windows-linked user group and individual Windows-linked user accounts can be members of FactoryTalk user groups. This allows use of FactoryTalk user groups when setting permissions.
- A FactoryTalk user account or Windows-linked user account can be a member of more than one FactoryTalk user group.

- 
- IMPORTANT**
- Managing user groups requires explicit permissions. To verify permissions, in FactoryTalk Administration Console **Explorer**, expand **System**, then right-click **Users and Groups** and select **Security**. Confirm the permissions listed in the prerequisites for the task are present with the logged in user account.
  - If an action is set to **Deny** for the user in any one group, then the **Deny** takes precedence over any **Allow** setting in a different group of which the user is a member.
- 

### See also

[Add a FactoryTalk user group](#) on [page 52](#)

[Add a Windows-linked user group](#) on [page 53](#)

[Add accounts to a FactoryTalk user group](#) on [page 56](#)

[Accounts and groups](#) on [page 16](#)

[Account types](#) on [page 18](#)

## Add a FactoryTalk user group

Create a new FactoryTalk user group to administer security permissions for specified users as a group. Change the memberships of a user account to quickly change the resources a user can access.

A FactoryTalk user group can contain:

- FactoryTalk user accounts
- Windows-linked user accounts
- FactoryTalk user group accounts

Use **New User Group** to add a FactoryTalk user group account to the FactoryTalk Directory that is separate from a Windows user group account. Then specify the group account's identity (for example, the name of the group) and the user accounts that are members of the group.

### Prerequisites

Adding a FactoryTalk user group requires these permissions:

- Common > Create Children
- Common > List Children
- Common > Read

### To add a user group account

1. In FactoryTalk Administration Console **Explorer**, expand **System > User Groups**.
2. Right-click the **User Groups** folder, point to **New**, and select **User Group**.
3. Type a name for the group in the **Name** box.
4. (optional) Enter any notes about the group in the **Description** box.
5. (optional) In the **E-mail** box, type only one email address or group address to associate with this group account.
6. Select **Add** to add user accounts to the group. In **Select User or Group**, select to select the users or groups to add to the new user group account. Under **Filter Users**, choose from the following:
  - **Show groups only**
  - **Show users only**
  - **Show all**
  - **Create New**

7. Select **OK** to add the selected user or group to the **Members List** in **New User Group**.
8. Select **OK** when finished creating the user group.

### See also

[Delete a user group](#) on [page 56](#)

[Manage user groups](#) on [page 51](#)

## Add a Windows-linked user group

To move Windows accounts from one domain to another, create Windows-linked user group accounts instead of individual Windows-linked user accounts. Windows-linked user group accounts, and the user accounts they contain, can move from one domain to another while keeping security permissions for the group accounts intact.

Add user groups from a Windows domain or workgroup to the FactoryTalk system to allow the user accounts in the group to access the FactoryTalk system. To modify the properties of a Windows-linked user group, (for example the group's name, or which user accounts are group members), modify these properties in Windows.

When adding a Windows-linked user group account, all user accounts in the Windows user group have access to the FactoryTalk system. To prevent some users in a Windows-linked group from accessing the FactoryTalk system, create Windows-linked user accounts for those users, and set permissions to deny access to those user accounts.

### Prerequisites

1. Connect the computer to the Windows domain containing the user groups to add to the FactoryTalk Directory.
2. Obtain these permissions in the **User Groups** folder in FactoryTalk Administration Console **Explorer**:
  - Common > Create Children
  - Common > List Children
  - Common > Read

### To add a Windows-linked user group account

1. In FactoryTalk Administration Console **Explorer**, expand **System > User Groups**.
2. Right-click the **User Groups** folder, point to **New**, and select **Windows-Linked User Group**.
3. In **New Windows-Linked User Group**, select **Add**.
4. In **Select Groups**, select the Windows groups, and select **OK**.

- If known, type the names of the user group accounts in the text box. For domain accounts, use the format *DOMAIN\groupname*, for workgroup accounts use the format *COMPUTERNAME\groupname*. To validate the names, select **Check Names**. Correct any errors, and select **OK**.
  - To search for group by name or description, or to select multiple groups, select **Advanced**.
- a. In **Select Groups**, select **Locations** and select the domain or workgroup from which to select groups.
    - b. Under **Common Queries**, complete the information with which to search the directory:
      - Name: Choose whether to search for a name that starts with the specified values or is an exact match to the specified value and then type the search string.
      - Description: Choose whether to search for a description that starts with the specified values or is an exact match to the specified value and then type the search string
      - Disabled accounts: Select to include disabled accounts when searching.
      - Non expiring password: Select to include accounts that have passwords that never expire when searching.
      - Days since last logon: Specify to look for accounts based on how long it has been since the account successfully logged on/
    - c. Select **Find Now**.
    - d. In the list of groups, select the group accounts to add, and select **OK** to close **Advanced Select Groups**.
    - e. The groups selected are listed under **Enter the object name to select**. Select **Check Names** to verify the names and then select **OK** to close **Select Groups**.
  5. In **New Windows-Linked User Group**, review the list of groups.
    - To remove any groups added unintentionally, select the groups, and select **Remove**.
    - To add more groups, repeat steps 3 and 4.
  6. Select **OK**.



Tip: Use a password for all Windows accounts in a Windows-linked group, otherwise intermittent security failures or an inability to log on may occur. To follow good security practice, do not use blank passwords with accounts. To avoid using a password for Windows-linked accounts, on the local computer disable the Windows local security policy **Accounts: Limit local account use of blank passwords to console logon only**.

## See also

[Delete a user account](#) on [page 48](#)

[Add a Windows-linked user account](#) on [page 45](#)

[Account types](#) on [page 18](#)

[Manage user groups](#) on [page 51](#)

## Edit or view user group properties

Modify the properties of a FactoryTalk user group account that is not linked to a Windows user group account. View the properties of a Windows-linked user group account. The name of a user group cannot change.

Group memberships added to a user group account take effect only when the user logs off FactoryTalk and then logs on again.

### Prerequisites

Editing or viewing user group properties requires these permissions:

- Common > List Children
- Common > Read
- Common > Write

### To edit or view user group properties

1. In FactoryTalk Administration Console **Explorer**, expand **System > User Groups**, right-click the user group account, and select **Properties**.
2. (optional) In the **Description** box, type a description of the user group. For example, record information about where the group is located, what part of the system is relevant to the group, or contact information for the leader of the group.
3. (optional) In the **E-mail** box, type only one email address or group address (for example **cjenkins@yourcompany.com**, or **maintenance@yourcompany.com**), to associate with this account. Ensure that the address you typed is a valid address, and that you typed the address correctly. Some FactoryTalk-enabled products can send messages or notifications to an email address. For details, see the documentation supplied with your FactoryTalk-enabled product.
4. (optional) To add accounts to the group, select **Add**. In **Select User or Group**, select the users or user groups to add to the group, and select **OK**.
5. (optional) To remove user accounts, select the users or user groups to remove from the group, and select **Remove**.
6. Select **OK**.

### See also

[Add a FactoryTalk user group](#) on [page 52](#)

[Add a Windows-linked user group](#) on [page 53](#)

[Account types](#) on [page 18](#)

[Manage user groups](#) on [page 51](#)

## Delete a user group

Delete a user group when a particular group account is no longer needed to manage a group of users. Before deleting the user group, view the properties of the user group account.

To help prevent inadvertent lock out of the FactoryTalk Directory, the Administrators group cannot be deleted.

### Prerequisites

Deleting a user group account that has no members requires these permissions:

- Common > Delete
- Common > List Children
- Common > Read

Deleting a user group account that has members requires these permissions:

- Common > Delete
- Common > List Children
- Common > Read
- Common > Write

### To delete a user group

- In FactoryTalk Administration Console **Explorer**, expand **System > User Groups**, right-click the user group account, and then select **Delete**.

### See also

[Edit or view user group properties](#) on [page 55](#)

[Manage user groups](#) on [page 51](#)

## Add accounts to a FactoryTalk user group

Any time after creating a FactoryTalk user group, add or remove the user accounts that belong to the group. Members of a Windows-linked user group cannot be added or removed. However, individual Windows-linked user accounts can be added to FactoryTalk user groups.



Tip: Alternatively, change the groups to which a user belongs. Use **Group Membership User Properties** to add or remove user groups from a FactoryTalk or Windows-linked user account.



## To add accounts to a FactoryTalk user group

1. In FactoryTalk Administration Console **Explorer**, expand **System > User Groups**, right-click the user group account, and select **Properties**.
2. Select **Add**.
3. In **Select User or Group**, select each user or user group to add to the user group account. Use the options under **Filters** to show only users, only user groups, or all accounts. Select **OK** when finished.

### See also

[Remove accounts from a FactoryTalk user group](#) on [page 57](#)

[Add a FactoryTalk user group](#) on [page 52](#)

[Delete a user group](#) on [page 56](#)

[Manage user groups](#) on [page 51](#)

## Remove accounts from a FactoryTalk user group

After creating a FactoryTalk user group, members can be added or removed at any time. However, after a Windows-linked user group is added to the FactoryTalk Directory, its members cannot be deleted or removed.



Tip: Alternatively, change the groups to which a user belongs. Use **Group Membership User Properties** to add or remove groups from either a FactoryTalk or Windows-linked user account.

## To remove accounts from a FactoryTalk user group

1. In FactoryTalk Administration Console **Explorer**, expand **System > User Groups**, right-click the user group account, and select **Remove**.
2. In **Select User or Group**, select each user or user group to remove from the user group account. Use the options under **Filters** to show only users, only user groups, or all account.
3. Select **OK** when finished.

### See also

[Add accounts to a FactoryTalk user group](#) on [page 56](#)

[Add a FactoryTalk user group](#) on [page 52](#)

[Add a Windows-linked user group](#) on [page 53](#)

[Delete a user group](#) on [page 56](#)

[Manage user groups](#) on [page 51](#)



## Manage computers

### Manage computers

Use FactoryTalk Administration Console to manage the computer accounts in a FactoryTalk network directory. The FactoryTalk local directory does not make use of computer accounts because all activity on the directory is restricted to the local computer.

Tasks related to managing computers:

- Add a computer
- Delete a computer
- Add group memberships
- Remove group memberships
- Change the name of a client computer
- Change the name of a server computer
- Set the override directory cache policies

---

**IMPORTANT** Managing computers requires explicit permissions. To verify permissions, in FactoryTalk Administration Console **Explorer**, expand **System**, then right-click **Computers and Groups** and select **Security**. Confirm the permissions listed in the prerequisites for the task are present with the logged in user account.

---

### See also

[Add a computer](#) on [page 59](#)

[Edit or view computer properties](#) on [page 61](#)

### Add a computer

To allow a computer to access the FactoryTalk system, add a computer to a FactoryTalk network directory. After adding the computer account, specify security settings for the computer that allow or deny access to parts of the FactoryTalk system or add the computer to a group account, and then specify security settings for the group.

---

**IMPORTANT** Even if the security policy **Require computer accounts for all client machines** is disabled, you must still create computer accounts for any computers hosting servers – for example, Terminal Servers, Rockwell Automation Device Servers (FactoryTalk Linx), OPC data servers, Tag Alarm and Event Servers, or HMI servers.

---

### Prerequisites

Adding computer accounts requires these permissions:

- Common > Create Children

- Common > List Children
- Common > Read

### To add a computer account

1. In FactoryTalk Administration Console **Explorer**, expand **System > Computers and Groups**, right-click **Computers**, and then select **New Computer**.
2. In **New Computer**, in **Computer name**, type the name of the computer, or select **Browse (...)** and then choose a computer name.
3. (optional) In **Description**, type descriptive information about the computer (Example: Operator workstation for South Building production line 1, for maintenance contact *maintenance@yourcompany.com*).
4. Select **OK**.

### See also

[Delete a computer](#) on [page 60](#)

[Accounts and groups](#) on [page 16](#)

## Delete a computer

Delete a computer from the FactoryTalk network directory to remove its access to the FactoryTalk system.

### Prerequisites

Deleting a computer account that is not a member of a computer group requires these permissions:

- Common > Delete
- Common > List Children
- Common > Read

Deleting a computer account that is a member of a computer group requires these permissions:

- Common > Delete
- Common > List Children
- Common > Read
- Common > Write

## To delete a computer

- In FactoryTalk Administration Console **Explorer**, expand **System > Computers and Groups > Computers**, right-click the computer account, and then select **Delete**.

## See also

[Add a computer](#) on [page 59](#)

[Manage computers](#) on [page 59](#)

## Edit or view computer properties

Modify the name of a computer, its description, and the computer groups to which it belongs in **General Computer Properties**.

## Prerequisites

Editing or viewing computer properties requires these permissions:

- Common > List Children
- Common > Read
- Common > Write

## To edit or view computer properties

1. In FactoryTalk Administration Console **Explorer**, expand **System > Computers and Groups > Computers**, right-click the computer account, and select **Properties**.
2. Edit these settings in **General Computer Properties** as appropriate:
  - **Computer name**. Type the new Windows computer name for the computer, or select **Browse (...)** to browse for the compute
  - **Description**. Enter or edit a description of the computer, or other data about the computer account, such as contact information.
  - **Add**. Select to add this computer to one or more computer groups.
  - **Remove**. Select to remove this computer from a group.
3. Select **OK** to apply the edits to the computer.

## See also

[Add a computer](#) on [page 59](#)

Change a computer name in the FactoryTalk network directory

[Manage computers](#) on [page 59](#)



## Add and remove user-computer pairs

### Add and remove user-computer pairs

Security for FactoryTalk resources is always tied to users or groups of users, the actions the users perform, for example, read, write, and so on, and the computers, or groups of computers where the users work.

This ensures that only authorized personnel can perform actions on the equipment and resources in the system from appropriate locations, for example, computers located within line of sight of equipment.

Available options are:

- Add a user-computer pair
- Remove a user-computer pair

### See also

[Add a user-computer pair](#) on [page 63](#)

[Remove a user-computer pair](#) on [page 65](#)

### Add a user-computer pair

How do I open Select User and Computer?

1. In the FactoryTalk Administration Console Explorer, right-click an item and select **Security**.
2. On the **Permissions** tab, select **Add**.

-OR-

1. In the FactoryTalk Administration Console Explorer, expand **System > Policies > Product Policies** and open a **Feature Security** item.
2. From the **Feature Security Properties Policy Setting** tab, select **Configure Security**.
3. In **Configure Securable Action**, select **Add**.

Use **Select User and Computer** to pair a group of users, or an individual user, with a group of computers, or an individual computer. Then, specify security settings for the pair. For example, set permissions for a resource that allow or deny access to the pair.

### Prerequisites

- Obtain the appropriate permissions to specify security settings on the selected resource.

## To add a user-computer pair

1. Navigate to **Select User and Computer**.
  2. Under **Filter Users**, to limit the user accounts displayed in the **Users** list and define the type of user accounts that can be created, select either:
    - **Show groups only**

New user groups and Windows-linked groups can be created if needed
    - **Show users only**

New FactoryTalk User and Windows-linked user accounts can be created if needed
    - **Show all**

New accounts cannot be created when this option is selected.
  3. (optional) To create a new user or group account, select **Create New**, choose the type of account to create, and then specify the account settings.
  4. In the **Users** list, select a user account or user group account.
  5. Under **Filter Computers**, to limit the computer accounts displayed in the **Computers** list and define the type of computer accounts that can be created, select either:
    - **Show groups only**

New computer group accounts can be created if needed
    - **Show users only**

New computer accounts can be created if needed
    - **Show all**

New computer accounts cannot be created when this option is selected.
  6. (optional) To create a new computer or computer group account, select **Create New**, choose the type of account to create, and then specify the account settings.
  7. In the **Computers** list, select a computer account or computer group account.
  8. Select **OK**.
- The selected user-computer pair displays in the permissions list. Explicit permissions can now be configured for the pair.

## See also

[Remove a user-computer pair](#) on [page 65](#)



## Remove a user-computer pair

How do I open Select User and Computer?

1. In the FactoryTalk Administration Console Explorer, right-click an item and select **Security**.
2. On the **Permissions** tab, select **Add**.

-or-

1. In the FactoryTalk Administration Console Explorer, expand **System > Policies >Product Policies** and open a **Feature Security** item.
2. From the **Feature Security Properties Policy Setting** tab, select **Configure Security**.
3. In **Configure Securable Action**, select **Add**.

Remove a user-computer pair when it is longer necessary to specify permissions on a resource for the pair.

### Prerequisites

- Obtain the appropriate permissions to specify security settings on the selected resource.

### To remove a user-computer pair

1. Navigate to **Select User and Computer**, select the filter criteria to show the list of the users and user groups, and computers or computer groups to delete.
2. In the **Users** list, select the user account or user group account that belongs to the pair being deleted.
3. In the **Computers** list, select a computer account or computer group account that belongs to the pair being deleted.
4. Select **Remove**.
5. Select **OK**.

### See also

[Add a user-computer pair](#) on [page 63](#)

## Edit or view user account properties

Use these steps to view and edit the general properties of a FactoryTalk user account, such as user name and password, user description, user email address, and user login method. These properties are only viewable for a Windows-linked user account and cannot be edited. Use Windows to edit the general properties of a Windows-linked user account.

## Prerequisites

Obtain these permissions in the **Users** folder in FactoryTalk Administration Console **Explorer**:

- Common > List Children
- Common > Read
- Common > Write

## To edit or view user account properties

1. In FactoryTalk Administration Console **Explorer**, expand the FactoryTalk network or local directory tree. Expand the **System > Users and Groups** folder to see the user account.
2. Right-click the user account, and select **Properties**. Edit the **General User Properties** settings as needed.
3. Select **OK**.



Tip: Changing the properties of a FactoryTalk user account in one FactoryTalk directory does not modify the properties in the other, even if the account has the same name in both directories. Before editing the properties of a user account, log on the FactoryTalk directory that contains the user account.

## See also

[Add a FactoryTalk user account](#) on [page 43](#)

[Manage users](#) on [page 43](#)

## Add and remove action groups

### Add and remove action groups

To avoid setting permissions for individual actions, group actions together to grant or deny permissions for a set of actions in one step.

When adding an action group, decide:

- The name of the action group
- What actions belong to that group

Use action groups to assign permissions based on any convenient grouping. For example:

- A person's role or job (operator, supervisor, maintenance engineer, and so on)
- The equipment a person has access to (hoppers, mixers, ovens, and so on)

When setting security using action groups:

- Add an action group
- Add actions to an action group
- Remove actions from an action group
- Delete an action group

### See also

[Add an action group](#) on [page 67](#)

[Delete an action group](#) on [page 69](#)

[Add an action to an action group](#) on [page 69](#)

### Add an action group

Group actions together to grant or deny permissions for a set of actions in one step rather than having to set permissions for each action separately.

When adding an action group, decide:

- The name of the action group
- What actions belong to that group

### Prerequisites

Obtain these security permissions for the **Action Groups** folder in **Explorer**:

- Common > Read

- Common > List Children
- Common > Create Children
- Common > Write

### To add an action group

- In FactoryTalk Administration Console **Explorer**, right-click the **Action Groups** folder and select **New Action Group**.

### See also

[Delete an action group](#) on [page 68](#)

[Add and remove action groups](#) on [page 67](#)

## Delete an action group

When an action group is deleted, any explicit permissions assigned to that group are no longer in effect.

For example, suppose an action group named "Operators" was used to explicitly grant write access to an area named "Mixing" for a user account "Chris". If the "Operators" action group is deleted, "Chris" can no longer write to the "Mixing" area. Creating another "Operators" action group will not restore "Chris" the ability to write to "Mixing".

If an action group is inadvertently deleted and restoring the FactoryTalk Directory from a backup is not feasible, all security permissions assigned to the resources that were using the action group must be recreated.

### Prerequisites

1. Before deleting an action group, back up the FactoryTalk Directory.
2. Deleting an acting group requires these security permissions for the **Action Groups** folder:
  - Common > Read
  - Common > List Children
  - Common > Delete

### To delete an action group

1. In FactoryTalk Administration Console **Explorer**, expand the **Action Groups** folder.
2. Right-click the action group and select **Delete**.

## See also

[Add an action group](#) on [page 67](#)

[Add and remove action groups](#) on [page 67](#)

## Add an action to an action group

To manage security settings for an action as part of an existing action group, add the action to the action group.

### Prerequisites

Adding an action to an action group requires these permissions for the **Action Groups** folder in FactoryTalk Administration Console **Explorer**:

- Common > Read
- Common > List Children
- Common > Create Children
- Common > Write

### To add an action to an action group

1. In FactoryTalk Administration Console **Explorer**, expand **Action Groups**, then right-click the action group to edit, and select **Properties**.
2. In **Properties**, the action group appears on the right in the **Selected actions and action groups** list.
3. In the **Available Actions and Action Groups** list, select the action to add to the action group, and select >>.
4. Select **OK**.

## See also

[Add an action group](#) on [page 67](#)

[Add and remove action groups](#) on [page 67](#)

## Remove an action from an action group

To stop managing security settings for a particular action as part of an action group, remove the action from the action group.

### Prerequisites

Removing an action from an action group requires these security permissions for the **Action Groups** folder in FactoryTalk Administration Console **Explorer**:

- Common > Read
- Common > List Children
- Common > Create Children

- Common > Write

### To remove an action from an action group

1. In FactoryTalk Administration Console **Explorer**, expand **Action Groups**, right-click the action group to edit, and select **Properties**.
2. In **Properties**, the action group appears on the right in the **Selected actions and action groups** list.
3. In the **Selected Actions and Action Groups** list, select the action to remove from the action group, and select << to remove it from the group.
4. Select **OK**.

### See also

[Add and remove action groups](#) on [page 67](#)

## Set system policies

Set system policies to manage settings that apply across the entire FactoryTalk system. Policy settings are separate in the network directory and the local directory.

Navigate to **System > Policies > System Policies** to view and edit the following:

- **Application Authorization**  
Determines whether applications can access the FactoryTalk Directory.
- **User Rights Assignment**  
Determines which users can perform system-wide actions, such as backing up and restoring the contents of the FactoryTalk Directory, changing the directory server computer, performing a manual switchover to a redundant server, and modifying the security authority identifier.
- **Live Data Policy**  
Determines the default communications protocol for a distributed FactoryTalk system.
- **Health Monitoring Policy**  
Defines the parameters that the health monitoring service uses when determining if a network error occurred and how long to wait before switching to a standby server.
- **Audit Policy**  
Defines which activities generate an audit message.
- **Security Policy**  
Defines the security policies applied to FactoryTalk account, divided into these categories: account policy, computer policy, directory protection policy, password policy, and single sign-on policy. These policies do not apply to Windows-linked accounts. Define policies for Windows-linked accounts in Windows.

### See also

[Authorize an application to access the FactoryTalk Directory](#) on page [72](#)

[Assign user rights to make system policy changes](#) on [page 78](#)

[Set audit policies](#) on [page 86](#)

[Set system security policies](#) on [page 91](#)

[Set network health monitoring policies](#) on [page 84](#)

## Authorize an application to access the FactoryTalk Directory

Use **FactoryTalk Service Application Authorization** to authorize applications to access the FactoryTalk Directory.

If the option to verify the publisher certificate information is enabled, applications that are not signed by Rockwell Automation or Microsoft® are not allowed access to the FactoryTalk Directory.



Tip: To configure the **Application Authorization** policy, log into FactoryTalk with an account that is a member of the FactoryTalk Administrators group.

### To authorize an application to access the FactoryTalk Directory

1. Log on to the FactoryTalk network directory or FactoryTalk local directory.
2. In FactoryTalk Administration Console **Explorer**, expand the **System > Policies > System Policies** folders.
3. Right-click **Application Authorization** and select **Properties**.

The **Application Authorization** policy controls access by monitoring information about each application that is requesting a service token from FactoryTalk.

4. In **FactoryTalk Service Application Authorization**, review the list of the applications that can be authorized. To sort the application list by process name, computer name, or access allowed status, select the corresponding column header at the top of the window.  
Some applications are required by FactoryTalk and cannot be removed or denied. These entries are displayed with gray text in the list.
5. (optional) To view the publisher certificate information for a process, select the desired cell in the **Publisher Info** column.
6. Select a process, and scroll to the right to view its access status. Select **Access Allowed** to provide access to the FactoryTalk Directory, or clear to deny access to the FactoryTalk Directory.
7. (optional) To automatically enable access to the FactoryTalk Directory for any new process, select **Enable Default Access**.
8. (optional) To automatically block access to the FactoryTalk Directory for any new process, clear **Enable Default Access**.
9. (optional) To verify publication information for all FactoryTalk Services Platform processes, select **Verify Publisher Info**. If the verification process fails, the process is automatically denied access.
10. Select **OK**.



## See also

[FactoryTalk Service Application Authorization settings](#) on [page 73](#)

[Publisher Certificate Information](#) on [page 75](#)

[Digitally signed FactoryTalk products](#) on [page 76](#)

## FactoryTalk Service Application Authorization

How do I open FactoryTalk Service Application Authorization?

1. Log on to the FactoryTalk Network Directory or FactoryTalk Local Directory.
2. In FactoryTalk Administration Console **Explorer**, expand **System** > **Policies** > **System Policies**.
3. Right-click **Application Authorization** and then select **Properties**.

Use **FactoryTalk Service Application Authorization** to authorize the applications that have access to FactoryTalk Directory. By default FactoryTalk Services Platform processes are automatically allowed access.

If the **Verify publisher information** option is enabled, applications that are not signed by Rockwell Automation or Microsoft are not allowed access to FactoryTalk Directory.



Tip: To configure the Application Authorization policy, log into FactoryTalk with an account that is a member of the FactoryTalk Administrators group.

## See also

[Authorize an application to access the FactoryTalk Directory](#) on [page 72](#)

[FactoryTalk Service Application Authorization settings](#) on [page 73](#)

## FactoryTalk Service Application Authorization settings

Use **FactoryTalk Service Application Authorization** settings to authorize the applications that have access to FactoryTalk Directory.

If the **Verify Publisher Info** option is selected, applications that are not signed by Rockwell Automation or Microsoft are not allowed access to FactoryTalk Directory.

The **Application Authorization** policy controls access by monitoring the information of each application that is requesting a service token from FactoryTalk. To configure the **Application Authorization** policy, log into FactoryTalk with an account that is a member of the FactoryTalk Administrators group.

To sort the application list by process name, version number, computer name, publisher, or access allowed status, select the corresponding column header.

Column	Description
Process	Shows the process name of the application that is requesting a service token. Some applications are required by FactoryTalk and cannot be removed or denied. These entries appear with gray text in the list. To sort the application list by process name, computer name, or access allowed status, select the corresponding column header.
Version	Shows the version number of the application that is requesting a service token.
Computer	Shows the computer name where the application runs. To sort the application list by process name, computer name, or access allowed status, select the corresponding column header.
Publisher Info	Shows the publisher name of the application. If no certificate exists, the cell displays with <b>None</b> . To view the detailed publisher certification information, select the desired cell in this column.
Access Allowed	Shows whether the current process is allowed to access to FactoryTalk Directory and determines whether an application is authorized to access the FactoryTalk Directory. To deny an application, clear the check box of the entry. If an application is denied access and fails the request for service token, a message is sent to FactoryTalk Diagnostics, for example, <i>Login failure for application [RNASecurityTestClient.exe] on directory [Network]. The application was denied access.</i> View the messages using the FactoryTalk Diagnostics Viewer. Some applications are required by FactoryTalk and cannot be removed or denied. These entries are displayed with gray text in the list.

Use these settings to specify how FactoryTalk allows access to the FactoryTalk Directory.

Setting	Description
Enable Default Access	Determines whether new applications are automatically allowed access to FactoryTalk Directory. <b>Default:</b> Enabled To disable the default access, clear the check box. All new applications are automatically denied access. If the default access of a FactoryTalk Directory server is disabled, you can still configure your local computer to join the directory server.
Verify Publisher Info	Determines whether to verify the publisher certificate information of FactoryTalk applications. If enabled, FactoryTalk Services Platform verifies whether the application requesting a service token is signed by Rockwell Automation or Microsoft. Any application not signed by them will fail to receive a service token. <b>Default:</b> Disabled To disable the publisher information verification, clear the check box. FactoryTalk Services Platform does not verify the publisher information. Applications are verified by the corresponding <b>Access Allowed</b> settings. Some earlier versions of Microsoft applications (for example, msiexec.exe) and FactoryTalk products were not signed when released. The publisher information on these applications may fail verification.

Remove	To remove one or more applications from the list, select the entries and select <b>Remove</b> . Some applications are required by FactoryTalk and cannot be removed or denied. These entries appear with gray text in the list. When removing one or more of these required entries, a warning message displays indicating that the required entries are not removed.
Refresh	Manually refresh the list to show the latest application list. Select <b>Refresh</b> . When refreshing the list, if a newer version of an existing application from the same computer is found, the entry is updated to reflect the new version or certificate information. Save the changes before refreshing. Any changes that are not saved will be lost when refreshing.

## Required FactoryTalk Processes

Process name	Description
FTDataUpdate.exe	FactoryTalk data update, which runs during FactoryTalk Directory configuration.
FTConfigurationUtility.exe	FactoryTalk Configuration wizard, which is only used in special cases to repair the FactoryTalk Directory.
FTExportPolicy.exe	Controls FactoryTalk export of policy settings during backup.
FTSetDirSvr.exe	Used to set the FactoryTalk Directory.
FTSPVStudio.exe	FactoryTalk Administration Console
ImportExportTool.exe	Used to import and export FactoryTalk information.
NmspHost.exe	FactoryTalk namespace services
RdcyHost.exe	Rockwell redundancy services
RnaDirMultiplexor.exe	Rockwell RNA directory multiplexer
RsvcHost.exe	Rockwell Automation services
SilentFTDCW.exe	FactoryTalk Directory Silent Configuration Wizard

## See also

[Authorize an application to access the FactoryTalk Directory](#) on [page 72](#)

[Publisher Certificate Information](#) on [page 75](#)

[Digitally signed FactoryTalk products](#) on [page 76](#)

## Publisher Certificate Information

Use **Publisher Certificate Information** to view digital signature details and verify the identity and authenticity of software.

Field	Description
Issued to	Shows the publisher name (or a portion of the name) of the entity to which the certificate is issued.
Issued by	Shows the name (or a portion of the name) of the issuer.
Status	Shows the status of the certificate, for example, valid, revoked, or expired.
Serial #	Shows the unique serial number (or a portion of the serial number) of the certificate.
Date signed	Shows the date when the binary was signed.
Valid from	Shows the beginning date of the period for which the certificate is valid.
Valid to	Shows the ending date of the period for which the certificate is valid.

**See also**

[Authorize an application to access the FactoryTalk Directory](#) on [page 72](#)

[FactoryTalk Service Application Authorization settings](#) on [page 73](#)

[Digitally signed FactoryTalk products](#) on [page 76](#)

**Digitally signed FactoryTalk products**

FactoryTalk Services Platform 2.51 or later provides the ability to verify whether an application requesting a service token is signed by Rockwell Automation. The access to FactoryTalk Directory is denied if the certification is not signed by Rockwell Automation.

Some earlier versions of FactoryTalk products were not signed when released. These products may fail to verify the publisher information.

This table shows which versions of FactoryTalk products are signed.

Products	Signed since version
FactoryTalk Administration Console	2.10.01
FactoryTalk Administration Console	2.31.00
FactoryTalk Batch	11.00
eProcedure®	11.00
FactoryTalk Linx	5.20
FactoryTalk Linx Gateway	3.02
FactoryTalk Historian SE	3.0
FactoryTalk Metrics	9.10
FactoryTalk Transaction Manager	9.10
FactoryTalk View ME	5.10
FactoryTalk View SE	5.10
Logix Designer	21.00
RSLinx Classic	2.54
RSLogix 5	7.40
RSLogix 500	8.10
RSLogix 5000	18.00
RSNetWorx	9.00
RSSecurity Emulator	2.10.01

**See also**

[Authorize an application to access the FactoryTalk Directory](#) on [page 72](#)

[Publisher Certificate Information](#) on [page 75](#)

**Authorize a service to use FactoryTalk Badge Logon**

Use **FactoryTalk Badge Authorization** to authorize services to use the FactoryTalk Badge Logon function.

The service that requests access to use the FactoryTalk Badge Logon function must be trusted by Rockwell Automation.



Note: To configure the Badge Authorization policy, log on to FactoryTalk with an account that is a member of the FactoryTalk Administrators group.

## To authorize a service to use the FactoryTalk Badge Logon

1. Log on to the FactoryTalk network directory or FactoryTalk local directory.
2. In FactoryTalk Administration Console **Explorer**, expand the **System > Policies > System Policies** folders.
3. Right-click **Badge Authorization** and select **Properties**.

The **Badge Authorization** policy controls access by monitoring each service that is requesting the FactoryTalk Badge Logon function.

4. In **FactoryTalk Badge Authorization**, click Add to permit access to a service that is requesting the FactoryTalk Badge Logon function.
5. Click **OK**.

## See also

[FactoryTalk Badge Authorization](#) on [page 77](#)

[FactoryTalk Badge Authorization settings](#) on [page 77](#)

## FactoryTalk Badge Authorization

How do I open FactoryTalk Badge Authorization?

1. Log on to the FactoryTalk Network Directory or FactoryTalk Local Directory.
2. In FactoryTalk Administration Console Explorer, expand **System > Policies > System Policies**.
3. Right-click **Badge Authorization** and then select **Properties**.

Use **FactoryTalk Badge Authorization** to authorize services to use the FactoryTalk Badge Logon function.

The service that requests access to use the FactoryTalk Badge Logon function must be trusted by Rockwell Automation.



Note: To configure the Badge Authorization policy, log on to FactoryTalk with an account that is a member of the FactoryTalk Administrators group.

## See also

[Authorize a service to use the FactoryTalk Badge Logon](#) on [page 76](#)

[FactoryTalk Badge Authorization settings](#) on [page 77](#)

## FactoryTalk Badge Authorization settings

Use **FactoryTalk Badge Authorization** to authorize services to use the FactoryTalk Badge Logon function.

The service that requests access to use the FactoryTalk Badge Logon function must be trusted by Rockwell Automation.



Note: To configure the Badge Authorization policy, log on to FactoryTalk with an account that is a member of the FactoryTalk Administrators group.

To sort the service list by process name, select the column header.

Column	Description
Process	Shows the process name of the service that is requesting the access to use the FactoryTalk Badge Logon function. The FactoryTalk services are not displayed in the list.

Use these settings to specify how FactoryTalk allow access to the services that are requesting to use the FactoryTalk Badge Logon function.

- **Add.** Used to open the **Select Application** dialog box to select a service that is requesting the FactoryTalk Badge Logon function.
- **Remove.** Used to remove one or more services that is using the FactoryTalk Badge Logon function.

**See also**

[Authorize a service to use the FactoryTalk Badge Logon](#) on [page 76](#)

[FactoryTalk Badge Authorization](#) on [page 77](#)

**Assign user rights to make system policy changes**

In **User Rights Assignment Policy Properties**, specify which users are permitted to:

- Back up or restore FactoryTalk Directory, the System folder, or applications
- Change the FactoryTalk Directory server computer
- Switch between primary and secondary servers in a redundant pair (for example, HMI servers, or data servers)
- Modify the security authority identifier

Policy settings are completely separate in the network directory and local directory. The network directory and local directory also have different default policy settings.

**To assign user rights to system policy changes**

1. Log into the FactoryTalk directory.
2. In FactoryTalk Administration Console **Explorer**, expand **System > Policies > System Policies**.
3. Right-click **User Rights Assignment** and select **Properties**.
4. In **User Rights Assignment Policies**, next to the policy to secure and to the right of **Configure Security**, select **Browse (...)**.

5. In **Configure Securable Action**, on the **Policy Setting** tab, select **Add. Select User or Group** opens.
6. (optional) Use the filter options to restrict the accounts shown in the lists.
7. Choose the user or group account, then select **OK**. The user or group is added to the list on the **Policy Setting** tab.
  - To allow the user permission to perform the action from the specified computer or group, select **Allow**.
  - To deny the user permissions to perform the action from the specified computer or group, select **Deny**.
  - To remove explicit **Allow** permissions, select the user and computer and select **Remove**. If no permissions are specified, **Deny** is implied.
8. When finished, select **OK** to apply the policy changes.

### See also

[User rights assignment policies](#) on [page 79](#)

[Permissions](#) on [page 135](#)

## User rights assignment policies

In FactoryTalk, administrators control the rights that users have to access the system. Settings that apply to the entire FactoryTalk directory are especially important to secure. User rights assignment policies specify which users are permitted to perform:

- **Back up or restore FactoryTalk Directory, the System folder, or applications.** The default setting allows all users to back up and restore the directory and its contents. Securing backup and restore operations prevents an unauthorized user from:
  - Copying applications or user account information in the FactoryTalk system
  - Intentionally or inadvertently overwriting the contents of FactoryTalk Directory, including applications, user, computer, and group accounts, passwords, policy settings, and security settings
- **Change the FactoryTalk Directory server computer.**

The default setting allows administrators to change the directory server. The policy appears in only FactoryTalk network directory. Verify the permissions to change the directory on the current computer and the computer being switched to.
- **Switch between primary and secondary servers in a redundant pair.**

In the FactoryTalk network directory, the default setting allows all users to switch between primary and secondary servers (such as HMI servers or data servers). Because redundancy is available in only the FactoryTalk network directory, this policy setting appears in only the FactoryTalk network directory.

- **Modify the security authority identifier.**

The default setting allows all users to modify the identifier.

Policy settings are completely separate in the network directory and local directory. The network directory and local directory also have different default policy settings.

### See also

[Assign user rights to make system policy changes](#) on [page 78](#)

[User Rights Assignment Policy Properties](#) on [page 80](#)

## User Rights Assignment Policy Properties

How do I open User Rights Assignment Policy Properties?

1. Start FactoryTalk Administration Console or FactoryTalk View Studio and then log on to the FactoryTalk Network Directory or FactoryTalk Local Directory.
2. In **Explorer**, expand the FactoryTalk Network or Local Directory tree, and then expand the **System > Policies > System Policies** folders.
3. Select **User Rights Assignment**.

In **User Rights Assignment Policy Properties**, specify which users are permitted to:

- Back up or restore FactoryTalk Directory, the System folder, or applications
- Change the FactoryTalk Directory server computer
- Switch between primary and secondary servers in a redundant pair (for example, HMI servers, or data servers)
- Modify the security authority identifier

Policy settings are completely separate in the network directory and local directory. The network directory and local directory also have different default policy settings.

### See also

[Assign user rights to make system policy changes](#) on [page 78](#)

[User rights assignment policies](#) on [page 79](#)

[Permissions](#) on [page 135](#)

## Configure Securable Action

How do I open Configure Securable Action?

1. In FactoryTalk Administration Console **Explorer**, expand the **System > Policies > Product Policies**.



2. Expand the product folder, then right-click **Feature Security** and select **Properties**.
3. In **Feature Security Properties**, select the row containing the feature category.
4. Next to **Configure Security**, select **Browse(...)**.

Use **Configure Securable Action** to view or set the permissions that determine access to a single feature for a user or group of users working from a computer or group of computers connected to the FactoryTalk network directory. The product policy features that can be secured depend on what FactoryTalk products are installed.

Use this window to configure permissions for the actions in **User Rights and Assignment Properties**.

In a FactoryTalk local directory, all security settings apply to only the local computer.

Setting	Description
Permissions list	Shows the users and computers that have <b>Allow</b> or <b>Deny</b> permissions set for this feature. To allow access to the feature, select <b>Allow</b> . To deny access to the feature, select <b>Deny</b> . If both <b>Allow</b> and <b>Deny</b> are cleared, the user is denied access to the feature.
Add	Select to add users and computers to the permissions list to set explicit permissions.
Remove	In the permissions list, select the combination of users and computers for which to remove security settings, and select <b>Remove</b> .

## See also

[Secure features of a single product](#) on [page 114](#)

[Effective permission icons](#) on [page 156](#)

## Select a user or group

Use **Select User or Group** to select a user account or FactoryTalk user group account. You can then specify security settings for the user or group.

Use the options under **Filters** to show only users, only user groups, or all accounts you may add to the group.

### To select a user or group

1. Right-click the FactoryTalk user group account you wish to modify and click **Properties**.
2. In **User Group Properties**, click **Add**.
3. At the bottom of **Select User or Group**, select the filter criteria that show the users or groups you want to select.
4. Do one of the following:

- In the list of users and groups, select a user account or user group account.
  - To create a new user account, click **Create New** and then click the type of account you want to create.
5. When you are finished selecting a user or group account, click **OK**.

### See also

[Manage user groups](#) on [page 51](#)

[Accounts and groups](#) on [page 16](#)

[Account types](#) on [page 18](#)

## Change the default communications protocol

To change the default communications protocol for a distributed FactoryTalk system, use **Live Data Policy Properties**.

Change this setting only if necessary. For example, if the system experiences communications problems and troubleshooting requires switching to DCOM. Thoroughly test communications before deploying this change to a running production system. Keep in mind that many factors affect communications, including firewalls, closed ports, and differences in network architectures and configurations.

### To change the default communications protocol

1. In FactoryTalk Administration Console **Explorer**, expand **System > Policies > System Policies**.
2. Right-click **Live Data Policy** and select **Properties**.
3. From the list to the right of **Default Protocol Setting**, switch the default communications protocol from **TCP/IP** to **DCOM**, or from **DCOM** to **TCP/IP**.
4. Select **OK**.
5. Shut down and restart all computers on the network.

### See also

[Live Data Policy Properties](#) on [page 83](#)

## Default communications protocol settings

In a FactoryTalk distributed system, the communications protocol affects communications between client and server services and between the FactoryTalk Directory and servers on the network. This setting is considered a "default" because if the FactoryTalk Live Data service detects that some components on the network are not compatible with the selected policy setting, the service overrides the policy and uses whichever setting is most likely to ensure uninterrupted communications. For example, for third-party

servers and RSLinx Classic, FactoryTalk Live Data does not attempt a TCP/IP connection and always uses DCOM.

Use the **Policy Settings** tab of **Live Data Policy Properties** to set the default protocol from **TCP/IP** to **DCOM** or vice versa.

The FactoryTalk Services Platform installation process evaluates the services and components on the network and sets the communication protocol appropriately. For example, if upgrading from an earlier version of the FactoryTalk platform to FactoryTalk Services Platform 2.10 (CPR 9) or later, the communications default is automatically set to DCOM. If installing FactoryTalk Services Platform 2.10 or later for the first time on a computer, the communications default is automatically set to TCP/IP. Typically, changing the default setting is not necessary or advisable

Default protocol setting	Description
TCP/IP	<p>An open communications protocol that typically is more reliable and has better performance than the proprietary DCOM protocol.</p> <ul style="list-style-type: none"> <li>Choose this option only if all or most of the clients and servers on the automation network are upgraded to use FactoryTalk Services Platform v. 2.10 (CPR 9) or later.</li> <li>Do not choose this option if the automation network is using older versions of the FactoryTalk Automation Platform v.2.00 (CPR 7) or earlier or if the system includes many third-party OPC servers and devices.</li> </ul> <p>When this setting is changed from <b>DCOM</b> to <b>TCP/IP</b>, an audit message is logged to FactoryTalk Diagnostics indicating that the value changed from <b>False</b> to <b>True</b>.</p>
DCOM	<p>A proprietary communications protocol owned and managed by Microsoft.</p> <p>Choose this option if:</p> <ul style="list-style-type: none"> <li>Most of the clients and servers on the automation network are using older versions of FactoryTalk Automation Platform (v. 2.00, CPR 7 or earlier)</li> <li>The system includes third-party OPC servers and devices</li> </ul> <p>When this setting is changed from <b>TCP/IP</b> to <b>DCOM</b>, an audit message is logged to FactoryTalk Diagnostics indicating that the value changed from <b>True</b> to <b>False</b>.</p>

## See also

[Change the default communications protocol](#) on [page 82](#)

[FactoryTalk Directory types](#) on [page 15](#)

## Live Data Policy Properties

How do I open Live Data Policy Properties?

1. In FactoryTalk Administration Console **Explorer**, expand **System > Policies > System Policies**.
2. Right-click **Live Data Policy** and select **Properties**.

Use the **Policy Settings** tab of **Live Data Policy Properties** to select a default communications protocol for a distributed FactoryTalk system.

This setting affects communications between client and server services and between the FactoryTalk Directory and servers on the network. This setting is considered a "default". If the FactoryTalk Live Data service detects that some

components on the network are not compatible with the selected policy setting, the service overrides the policy and uses whichever setting is most likely to ensure uninterrupted communications. For example, for third-party servers and RSLinx Classic, FactoryTalk Live Data does not attempt a TCP/IP connection and always uses DCOM.

Change this setting only if necessary, such as if the system is experiencing communications problems and it is necessary to switch to DCOM for troubleshooting purposes. Thoroughly test communications before deploying this change to a running production system. Many factors affect communications, including firewalls, closed ports, and differences in network architectures and configurations.

---

**IMPORTANT** Changing this policy setting can have unexpected results. Do not change this setting in a running production system. For changes to take effect, shut down and restart all computers on the network.

---

### See also

[Change the default communications protocol](#) on [page 82](#)

[Default communications protocol settings](#) on [page 82](#)

[FactoryTalk Directory types](#) on [page 15](#)

## Set network health monitoring policies

Use **Health Monitoring Policy Properties** to fine tune the parameters that the system uses when determining whether a network failure is occurring and how long to wait before switching to a Standby server.

A network failure occurs when a server is temporarily unable to communicate with other computers because of network traffic and fluctuations. During a network failure, even though the computers in the redundant server pair cannot communicate, the active server remains active and the standby server remains on standby.



Tip: Changing health monitoring policy settings can have unexpected results. The preset default settings typically provide optimal efficiency for most networks.

### To set network health monitoring policies

1. In FactoryTalk Administration Console **Explorer**, expand **System > Policies > System Policies**.
2. Right-click **Health Monitoring Policy** and select **Properties**.
3. Under **Rates**, select the policy setting to edit. A description of the policy appears at in the bottom pane of the window.
4. To the right of the current rate, select the **down arrow** to enter a new number, or use the small up and down arrows to choose a higher or lower number.
5. Select **OK**.

## See also

[Health Monitoring Policy Properties](#) on [page 85](#)

## Health Monitoring Policy Properties

How do I open Health Monitoring Policy Properties?

1. In **Explorer**, expand **System > Policies > System Policies**.
2. Right-click **Health Monitoring Policy** and select **Properties**.

Use **Policy Settings** in **Health Monitoring Policy Properties** to change parameters that determine whether a network failure is occurring and how long to wait before switching to a standby server.



Tip: To monitor system health messages, use the FactoryTalk Diagnostics Viewer.

A network failure occurs when a server is temporarily unable to communicate with other computers because of network traffic and fluctuations. During a network failure, even though the computers in a server pair cannot communicate, the active server remains active and the standby server remains on standby.

When these policy settings are applied, the changes affect all computers that are clients of the FactoryTalk network directory server. The changes take effect immediately, as soon as the network directory server notifies the client computers of the changes.

---

**IMPORTANT** Changing health monitoring policy settings can have unexpected results. The preset default settings typically provide optimal efficiency for most networks.

---

The health monitoring service policies settings are:

Setting	Description	Rates
Computer detection interval	Sets the amount of time that the health monitoring service waits between its attempts to detect the existence of a computer on the network. If the service does not receive a response, it continues its detection attempts at the specified intervals. Once a connection is made, the health monitoring service stops sending "Computer detection" requests and begins sending "Network failure detection" requests to the computer.	<ul style="list-style-type: none"> <li>• <b>Default.</b> 2 seconds</li> <li>• <b>Minimum.</b> 1 second</li> <li>• <b>Maximum.</b> 600 seconds</li> </ul>
Network failure detection interval	Sets how often the health monitoring service attempts to verify the health of the network connection to remote computers. The health monitoring service begins sending "Network failure detection" requests after establishing the existence of a computer on the network. This request expects a reply back from the remote computer within the amount of time specified. If a reply is received, then the network connection is considered to be healthy. If a reply is not received, the service continues sending "Network failure detection" requests at the specified intervals until the amount of time specified as the "Maximum network glitch" is reached.	<ul style="list-style-type: none"> <li>• <b>Default.</b> 2 seconds</li> <li>• <b>Minimum.</b> 1 second</li> <li>• <b>Maximum.</b> 600 seconds</li> </ul>
Maximum network glitch	Sets the maximum duration of a network disruption before the health monitoring service determines that communications failed. If a network disruption lasts longer than this amount of time, the health monitoring service generates a diagnostic message and begins sending "Machine detection" requests to verify the existence of the standby server.	<ul style="list-style-type: none"> <li>• <b>Default.</b> 5 seconds</li> <li>• <b>Minimum.</b> 1 second</li> <li>• <b>Maximum.</b> 600 seconds</li> </ul>

Maximum delay before server is active	<p>Sets the maximum amount of time during a switch back that the server becoming active waits for clients to be ready for the switch. The purpose of the delay is to allow clients to establish connections to the server that is ready to become active. When the switch back occurs, data is available to the clients as soon as possible.</p> <p>As soon as all clients successfully connect, the server switches over to active immediately, even if the maximum delay was not yet reached.</p> <p>If the maximum delay is too short, the active server may not be able to provide high-quality service to its clients. Poor client performance and a diagnostic message stating that the server switched to active before all clients finish connecting may be observed.</p>	<ul style="list-style-type: none"> <li>• <b>Default.</b> 2 minutes</li> <li>• <b>Minimum.</b> 0 minutes (not recommended)</li> <li>• <b>Maximum.</b> 60 minutes</li> </ul>
---------------------------------------	---	--

**See also**

[Set network health monitoring policies](#) on [page 84](#)

**Set audit policies**

Use **Audit Policy Properties** to specify what security-related information is recorded while the system is being used. Audit policies include whether access checks are audited, whether access grants, denies, or both are audited, and so on. Audit messages are sent to FactoryTalk Diagnostics, and are viewed using the FactoryTalk Diagnostics Viewer.

**To set up audit policies**

1. In FactoryTalk Administration Console **Explorer**, expand **System > Policies > System Policies**.
2. Right-click **Audit Policy** and select **Properties**.
3. In **Audit Policy Properties**, for each policy setting listed choose either **Enabled** or **Disabled**.

**f. Audit changes to configuration and control system**

- **Enabled** (default) - Generates audit messages when configuration and control system changes occur across the FactoryTalk system.
- **Disabled** - Does not route audit messages to FactoryTalk Diagnostics log files, even if logging destinations are configured for audit messages on the **Message Routing** tab in **FactoryTalk Diagnostics Setup**.

Any changes made to the value of the **Audit changes to configuration and control system** policy itself are always recorded, regardless of whether audit logging is enabled or disabled. If enabled, audit information is sent to FactoryTalk Diagnostics.

**g. Audit security access failures**

- **Enabled** - Generates audit messages when users fail to access objects or features because of insufficient security permissions.

- **Disabled** (default) - Does not generate audit messages when users fail to access secured objects or features.

#### h. **Audit security access successes**

- **Enabled** - Generates audit messages when users succeed in accessing objects or features because of sufficient security permissions.
- **Disabled** (default) - Does not generate audit messages when users succeed in accessing objects or features because of sufficient security permissions.

When enabled, this policy might generate a large number of audit messages. Enable this policy only if there is a specific reason, for example, testing or troubleshooting whether users are able to access particular features or objects in the system. If enabled, audit information is sent to FactoryTalk Diagnostics.

4. Select **OK**.

### See also

[Audit policies](#) on [page 87](#)

[Audit trails and regulatory compliance](#) on [page 36](#)

[Example: Audit messages](#) on [page 91](#)

## Audit policies

Auditing user actions in a control system helps answer "who changed this process variable, when, and why?"

In an industry that must comply with governmental regulations, such as U.S. Government 21 CFR Part 11, the plant must be able to answer this question. The answer is also important if the plant manufactures products with critical tolerances, or if unmanaged changes could negatively affect product quality or risk consumer safety.

An audit trail records:

- The specific, authenticated user who is authorized to access the manufacturing system
- The action taken—typically an operation that affects the manufacturing control system or that creates, modifies, or deletes some element of the manufacturing process
- The resource—an object such as a PLC-5<sup>®</sup>, application, tag, or command, on which the user performs an action
- The computer from which the user performed the action
- The date and time when the user performed the action

Like other FactoryTalk policy settings, audit policies are managed separately in the network directory and the local directory.

## Auditing changes to the system configuration, and to the control system

The FactoryTalk system generates and sends audit messages to FactoryTalk Diagnostics. A system-wide policy setting controls whether audit records are generated and logged. If the system policy is enabled, then FactoryTalk Diagnostics routes the audit messages to various logging destinations, including the FactoryTalk® Audit Log. If the system policy is disabled, then FactoryTalk Diagnostics ignores audit messages generated by FactoryTalk components and FactoryTalk products and does not route them for logging.

Each FactoryTalk product defines its own rules for auditing changes. This means that the messages that appear in the FactoryTalk Diagnostics Viewer vary, depending on what products are installed. If the setting **Audit changes to configuration and control system** is enabled, audit messages are generated when any configuration and control system changes occur across the FactoryTalk system.

## Auditing security access failures and successes

Whenever a user attempts to access a secured resource, FactoryTalk Security can generate audit messages if the user was denied or granted access.

For example, suppose an area named Ingredients is secured so that only members of the OperatorsLine5 group can write to the area. If the **Audit object access success** policy is enabled, every time an operator is granted write access to this area, a message is logged to FactoryTalk Diagnostics. If **Audit object access failure policy** is enabled, every time an operator is refused **Write** access to this area, a message is logged to FactoryTalk Diagnostics.

Object access failures do not necessarily represent deliberate attempts to compromise the security of the system. For example, an object access failure message is logged if a user is denied **Configure Security** permission and right-clicks the **Users and Groups** folder.

Auditing security access success can consume large amounts of system resources. Enable this policy only when necessary, for example, while testing the system, or if required in industries that must comply with governmental regulations.

Examples of messages for auditing security access failures and successes:

- User NETWORK\JSMITH attempted to perform action COMMON\WRITE from NETWORK\DOMAIN\COMPUTER5 on [OPC data server][RNA://\$Global/Norms Bakery/Ingredients/RecipeDataServer] and was granted access
- User NETWORK\JSMITH attempted to perform action COMMON\CONFIGURE SECURITY from



NETWORK\DOMAIN\COMPUTER5 on [directory]{\$System} and was denied access

## See also

[Set audit policies](#) on [page 86](#)

[Audit trails and regulatory compliance](#) on [page 36](#)

[Example: Audit messages](#) on [page 91](#)

## Audit Policy Properties

How do I open Audit Policy Properties?

1. Start FactoryTalk Administration Console or FactoryTalk View Studio and log on to the FactoryTalk Network Directory or FactoryTalk Local Directory.
2. In **Explorer**, expand the **System** folder > **Policies** > **System Policies**.
3. Select **Audit Policy**.

Use **Audit Policy Properties** to specify what security-related information is recorded while the system is being used. Audit policies include whether access checks are audited, whether access grants, denies, or both are audited, and so on. Audit messages are sent to FactoryTalk Diagnostics, where they can be viewed using the FactoryTalk Diagnostics Viewer. Use these settings to specify what information is audited by the FactoryTalk system.

Setting	Description
Audit changes to configuration and control system	<p>Determines whether to generate audit messages when configuration and control system changes occur across the FactoryTalk system.</p> <p><b>Default:</b> Enabled</p> <p>To disable audit logging, set this policy to <b>Disabled</b>.</p> <p>If this policy is disabled, audit messages are not routed to FactoryTalk Diagnostics log files, even if logging destinations are configured for audit messages on the <b>Message Routing</b> tab in <b>Diagnostics Setup</b>.</p> <p>Any changes made to the value of the <b>Audit changes to configuration and control system</b> policy itself are always recorded, regardless of whether audit logging is enabled or disabled. If enabled, audit information is sent to FactoryTalk Diagnostics.</p>
Audit security access failures	<p>Determines whether to generate an audit message when a user attempts an action and is denied access to the secured object or feature because of insufficient security permissions.</p> <p><b>Default:</b> Disabled</p> <p>To record audit messages when users fail to access objects because of insufficient security permissions, set this policy to <b>Enabled</b>. If enabled, audit information is sent to FactoryTalk Diagnostics.</p>

Audit security access successes

Determines whether to generate an audit message when a user attempts an action and is granted access to the secured object or feature because the user has the required security permissions.

**Default:** Disabled

To record audit messages when users succeed in accessing objects because of sufficient security permissions, set this policy to **Enabled**. When enabled, this policy might generate a large number of audit messages. Enable this policy only if there is a specific reason for doing so, for example, testing or troubleshooting whether users can access particular features or objects in the system.

If enabled, audit information is sent to FactoryTalk Diagnostics.

**See also**

[Set audit policies](#) on [page 86](#)

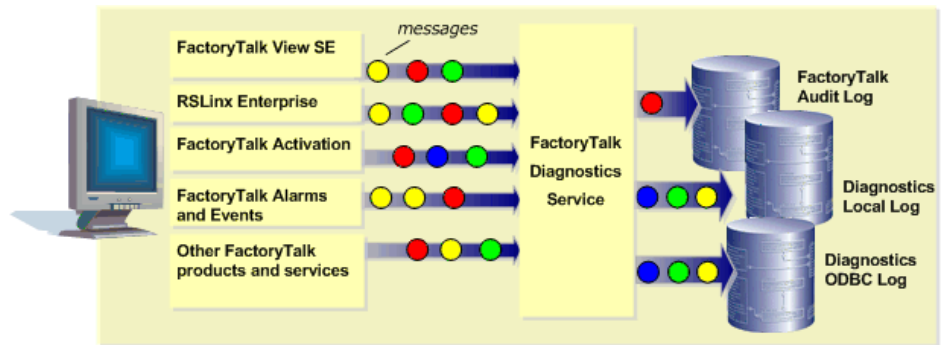
[Audit trails and regulatory compliance](#) on [page 36](#)

[Audit policies](#) on [page 87](#)

**Monitor security-related events**

Monitor security-related events to find out if changes are made to security policies or other objects, who made the changes, and when they were made. Monitor security-related events by setting up audit policies.

In a FactoryTalk automation system, Rockwell Automation software products monitor system activity and generate detailed diagnostic messages. Meanwhile, FactoryTalk Diagnostics collects these activity, warning, error, and audit messages from all participating products throughout a distributed system and routes them to Local Logs on each computer. Depending on the products installed and the configuration options set, FactoryTalk Diagnostics can also route these messages to other centralized logging destinations, such as an ODBC database or FactoryTalk® AssetCentre Audit Log.



To configure FactoryTalk Diagnostics routing and logging options, select **FactoryTalk Diagnostics Setup** from the **Tools** menu on each computer where the FactoryTalk Administration Console is installed.

To view diagnostic messages, from the **Tools** menu select **FactoryTalk Diagnostics > Viewer**.

**See also**

[Set audit policies](#) on [page 86](#)

**Example: Audit messages**

If the setting **Audit changes to configuration and control system** is enabled in **Audit Policy**, audit messages are generated when any configuration and control system changes occur across the FactoryTalk system.

Examples of messages for adding and removing control system components:

- Added area [Line2] to application [Network/Paper Mill]
- Removed area [Line1b] from application [Network/PaperMill]
- Added graphic display [Overview] to area [Network/Paper Mill/Line2]
- Removed user [BBilly] from directory [Network/System]
- Downloaded project [PASTEURIZE] to processor [/NetworkPath/Line1]
- Inserted rung [XIC B3/o OTE B3/o] in processor [XYZ/File 2/Rung 10]

Examples of messages for modifying control system values:

- Modified properties of user [JSmith] in directory [Network/System]
- Modified properties of server [Line2HMI] in application [Network/Paper Mill]
- Forced I/O [I1:2/15] in processor [TABLET10] from [OFF] to [ON]
- Changed security policy [Enforce password history] in directory [Network/System] from [0] to [5]
- Changed value of tag [HighPressureLimit] in processor [TABLET10] from [100] to [125]
- Changed value of tag [MaxFeederSpeed] in area [Network/Paper Mill/Line1] from [200] to [300]
- Changed name of graphic display [Line1Overview] in area [Network/Paper Mill/Line2] from [Line1Overview] to [Line2Overview]

**See also**

[Audit policies](#) on [page 87](#)

**Set system security policies**

Use **Security Policy Properties** to define general rules for implementing security across all FactoryTalk products in the system.

- **Account Policy Settings:** Specify how FactoryTalk manages policies for user, computer, and group accounts.
- **Computer Policy Settings:** Specify how computer accounts in the FactoryTalk network directory can use remote access.
- **Directory Protection Policy Settings:** Specifies client computer accounts usage of the FactoryTalk network directory.
- **Password Policy Settings:** Configures password requirements for FactoryTalk user accounts.

- **Single Sign-On Policy Settings:** Controls whether users can log on once to the FactoryTalk system, or must log on to each FactoryTalk product separately.

## See also

[Modify Account Policy Settings](#) on [page 92](#)

[Modify Computer Policy Settings](#) on [page 93](#)

[Modify Directory Protection Policy Settings](#) on [page 95](#)

[Modify Password Policy Settings](#) on [page 96](#)

[Enable single sign-on](#) on [page 99](#)

## Modify Account Policy Settings

Use **Account Policy Settings** to change these security policy properties:

- Logon session lease
- Account lockout threshold
- Account lockout auto reset
- Keep record of deleted accounts
- Show deleted accounts in user list

## To modify Account Policy Settings

1. In FactoryTalk Administration Console **Explorer**, expand **System > Policies > System Policies**.
2. Right-click **Security Policy** and select **Properties**.
3. In **Security Policy Properties**, select **+** to expand **Account Policy Settings**.
4. To set the maximum number of hours that a user can remain logged on before the system checks whether the user's account is still valid, select **Logon session lease**, and type a value from 0-999. Setting this value to 0 allows the logon session to be used indefinitely, allowing users to have continuous access, even if their accounts are disabled or deleted.
5. To set the number of consecutive times a user can unsuccessfully attempt to log on before the account is locked, double-click **Account lockout threshold**, and type a value from 0-999. If set to 0, accounts are never locked no matter how many consecutive times a user attempts to log on. An invalid logon attempt occurs if the user attempts to log on and specifies a correct user name but an incorrect password.

A locked account cannot be used until the **Account lockout auto reset** period expires, or until the account is reset by a FactoryTalk administrator. This helps prevent an unauthorized user from gaining access to the system by guessing a password through a process of elimination.

6. To specify the amount of time that must expire before a locked account is reset and the user can attempt access again, select **Account lockout auto reset** and type a value between 0 and 999 minutes.
7. To determine if the system maintains a record of deleted user accounts, select **Keep record of deleted accounts**, and select one:
  - **Enabled**—Accounts are permanently disabled, but remain flagged in the system with a unique identifier. New accounts must have unique names. For security, audit tracking, and compliance requirements, it may be necessary to keep a record of deleted accounts.
  - **Disabled**—Accounts are fully deleted from the system, allowing new accounts to use the same name. However, the new accounts have different account identifiers and do not inherit the security settings of the account.
8. If deleted account records are kept, choose whether or not to list deleted account records in the **Users** folder in the **System** tree. Select **Show deleted accounts in user list**, and select one:
  - **Enabled**—Administrators can view details about these deleted user accounts
  - **Disabled**—Deleted accounts are not shown in the list of user accounts
9. When finished modifying Account Policy Settings, select **OK**.

### See also

[Account Policy Settings](#) on [page 100](#)

[Audit trails and regulatory compliance](#) on [page 36](#)

[Enable single sign-on](#) on [page 99](#)

## Modify Computer Policy Settings

Use **Computer Policy Settings** to change these security policy properties:

- Whether or not a user can connect to the FactoryTalk Directory from a client computer that does not have a computer account in the network directory
- How client computers connect to the FactoryTalk Directory through Remote Desktop Services, and how the computer name appears in the FactoryTalk Diagnostics log of actions.

These settings apply only to computers in the FactoryTalk network directory because the FactoryTalk local directory does not permit remote access.

## To modify Computer Policy Settings

1. In FactoryTalk Administration Console **Explorer**, expand **System > Policies > System Policies**.
2. Right-click **Security Policy** and select **Properties**.
3. In **Security Policy Properties**, select + to expand **Computer Policy Settings**.
4. To change the requirements for connecting to the FactoryTalk Directory from a computer that does not have a FactoryTalk computer account, select **Require computer accounts for all client machines** and select one:
  - **Enabled**—allows users to log on to FactoryTalk only if they are logging on from a client computer that has an account in the FactoryTalk Directory. Remote Desktop Services clients can still log on to FactoryTalk Directory without computer accounts if the **Identify terminal server clients using the name of** policy is set to **Server Computer**. See step 4.
  - **Disabled**—allows users to log on to FactoryTalk from any client computer, even if that computer has no computer account in the FactoryTalk network directory.
5. To determine what computer name identifies clients connecting to the FactoryTalk Directory through Remote Desktop Services, select **Identify terminal server clients using the name of** and select one:
  - **Terminal client**—Client computers must have computer accounts in the FactoryTalk Directory to access FactoryTalk applications, unless the **Require computer accounts for all client machines** policy is disabled. This combination of settings is useful for diagnostic logging because the name of the client computer where actions originate can be logged.

**Terminal Client** logs actions using the name of the client computer where the user is connecting to the Remote Desktop Connection (RDC) client computer. The computer name logged in FactoryTalk Diagnostics is different for each client connecting via Remote Desktop Services.
  - **Server computer**—allows client computers to connect through Remote Desktop Services without requiring accounts in the FactoryTalk Directory, even if the **Require computer accounts for all client machines** policy is **Enabled**.

**Server computer** logs actions using the name of the Remote Desktop Connection server computer. The computer name logged in FactoryTalk Diagnostics will be the same for all users connecting via Remote Desktop Services.
6. When finished modifying Account Policy Settings, select **OK**.

---

**IMPORTANT** setting the **Identify terminal server clients using the name of** policy to **Server Computer**, disable single sign-on because the computer name is saved as part of the single sign-on user's credentials, and might affect the level of access a Remote Desktop Services user has to the FactoryTalk system.

---

## See also

[Computer Policy Settings](#) on [page 102](#)

[Enable single sign-on](#) on [page 99](#)

## Modify Directory Protection Policy Settings

Use **Directory Protection Policy Settings** to change the security policy properties that determine:

- If computers with FactoryTalk versions less than 2.50, which are considered non-secure, can access a directory server with FactoryTalk CPR 9 SR5 or later, and if so, whether or not an audit message is generated
- How long cache files remain available after a client computer disconnects from the server, and if a warning message displays

These settings apply only to computers in the FactoryTalk network directory.

## To modify Directory Protection Policy Settings

1. In FactoryTalk Administration Console **Explorer**, expand **System** > **Policies** > **System Policies**.
2. Right-click **Security Policy** and select **Properties**.
3. In **Security Policy Properties**, expand **Directory Protection Policy Settings**.
4. By default, FactoryTalk allows client computers with FactoryTalk versions earlier than 2.50 to connect to and retrieve information from a directory server computer with FactoryTalk 2.50 or later. To change this policy, change the **Support non-secure clients** setting to **Deny**. Clients with FactoryTalk versions earlier than 2.50 are denied access and a **Protocol version mismatch** error occurs.
5. By default, an audit message is created when a client computer with a FactoryTalk version earlier than 2.50 connects to a directory server computer with FactoryTalk 2.50 or later. If the message should not be created, change the **Audit non-secure client connections** setting to **Disabled**.
6. By default, cache files never expire. Instead, the cache files remain available after the client computer is disconnected from the server. To set a time limit for when cache files should expire, change the **Directory cache expiration** setting by typing or selecting a number of hours between 1 and 9999. When the time limit is reached, the client computer must reconnect to the server to continue to access the files.

7. By default, no warnings appear prior to cache expiration, but notifications can appear upon disconnection and cache expiration. To enable cache expiration warnings, change the **Directory cache expiration warning** setting by typing a number between 1 and 24. A warning notification appears this number of hours before cache expiration.
8. Configure the **Security authorization policy** to determine whether the client computer is authorized with directory files from server or local client cache files.
  - **Require directory update from server before authorizing** means the client computer is authorized using directory files from the server.
  - **Use local client cache** means the client computer is authorized using local client cache files. The amount of time for the client computer to wait before transferring cache files is configured in Directory cache transfer waiting time.
9. Configure the **Directory cache transfer waiting time** policy to determine how long the client computer waits before transferring cache files. Enter a number of seconds from 5 through 600. This policy only applies to when **Security authorization policy** is set to **Use local client cache**.
10. When finished modifying directory protection policy settings, select **OK**.

---

**IMPORTANT** If setting the **Identify terminal server clients using the name of** policy to **Server Computer**, disable single sign-on because the computer name is saved as part of the single sign-on user's credentials, and might affect the level of access a Remote Desktop Services user has to the FactoryTalk system.

---

## See also

[Computer Policy Settings](#) on [page 102](#)

[Enable single sign-on](#) on [page 99](#)

## Modify Password Policy Settings

Use **Password Policy Settings** to set security policy properties that control the conditions for a valid FactoryTalk password, such as minimum and maximum password length, password encryption method, password complexity requirements, and when a password expiration warning is given.

These policies do not apply to Windows-linked user accounts. Backing up the FactoryTalk system folder before making changes to **Password Policy Settings** is recommended.



**IMPORTANT** Be aware of these items before modifying **Password Policy Settings**:

- Previous releases used the MD5 cryptographic hashing algorithm to encode passwords. If compatibility with FactoryTalk Services Platform version 3.00 or earlier is required the **MD5** password encryption method must be selected. MD5 is an older algorithm that has known security vulnerabilities. Using the **SHA-256** encryption method is recommended.
- If **Passwords must meet complexity requirements** is set to **Enabled**, the minimum password length is 6 characters and cannot be decreased using the **Minimum password length** setting. Setting **Minimum password length** to a value greater than 6 is enforced.

## To modify Password Policy Settings

1. In FactoryTalk Administration Console **Explorer**, expand **System > Policies > System Policies**.
2. Right-click **Security Policy** and select **Properties**.
3. In **Security Policy Properties**, select > to expand **Password Policy Settings**.
4. In **Password encryption method** select the down arrow and select **SHA-256** or **MD5**.

Changing the password encryption method invalidates current user passwords.

5. Select **Passwords must meet complexity requirements** and select **Enabled** to require users to create more secure passwords.
6. Select **Minimum password length** and type a number between 0 and 64 to define the number of character required in a user password. Set **Minimum password length** to 0 to create user accounts without passwords.
7. Select **Previous passwords remembered** and type a number between 1 and 24 to prevent users from keeping the same password indefinitely. By default, three new passwords must be created before reusing an old password. If **Previous passwords remembered** is set to 0, old passwords can be reused immediately.
8. Select **Minimum password age** and type a number between 1 and 999 to require users to wait at least one day before changing their password.
9. Select **Maximum password age** and type a number between 1 and 999 to set the maximum number of days before passwords expire. When set to 0, passwords never expire.
10. Select **Password expiration warning** and enter a value between 0 and 999 to change the number of days before the system begins prompting users to change their passwords. By default, users receive a warning 14 days before their passwords expire.
11. Select **OK** or **Apply** to apply the new settings.

12. If the password encryption method was changed, choose how to process the change on all of the current FactoryTalk user accounts.
  - Select **Disable all FactoryTalk user accounts** to review each user account and select unique passwords for each.
  - Select **Reset all FactoryTalk user passwords immediately** to set a new password on all user accounts and require users to specify a new password the next time they logon.

This option updates these property settings on the FactoryTalk user accounts:

Policy	Setting
User must change password at next logon	Enabled
User cannot change password	Disabled
Password never expires	Disabled

### See also

[Password Policy Settings](#) on [page 106](#)

[Add a FactoryTalk user account](#) on [page 43](#)

[Back up a System folder](#) on [page 162](#)

## Modify Badge login policies

Use **Badge Login Policy Settings** to specify how FactoryTalk user accounts can login using an RFID badge. Badge login policies include whether login using a badge is enabled, whether facility codes are required, the badge provider, and the data format used by the badge. After this policy is enabled and configured login options are available in FactoryTalk user account properties and Badge IDs can be added to the FactoryTalk user account.

### To set badge login policies

1. In FactoryTalk Administration Console **Explorer**, expand **System > Policies > System Policies**.
2. Double click **Security Policy** and select **Badge Policy**.
3. In **Badge Policy** field, configure these policy settings:
  - i. **Allow badge login**
    - Select **Enabled** to permit FactoryTalk user accounts to include an associated badge ID to log on.
  - j. **Number of bits in ID**
    - Specify the length of bits that will be extracted from the badge as the Badge ID.
  - k. **Number of trailing parity bits to strip**
    - Specify the length of bits that will be ignored when extracting the data from the badge.

- l. **Use Facility Code**
    - **Yes** - Check the Facility Code in the badge identification number first, when the login is processed.
    - **No** - Ignored the Facility Code in the badge identification number when the login is processed.
  - m. **Number of Facility Code**
    - Specify the length of bits that will be extracted from the badge as the Facility Code.
  - n. **Facility code**
    - Type the facility code that embedded in the badge. The embedded facility code is provided by the badge manufacturer.
4. Select **OK**.

### See also

[Security Policy Properties](#) on [page 110](#)

Badge Login Policy Settings

User Properties settings

Set login options for a FactoryTalk user account

## Enable single sign-on

Use **Single Sign-On Policy Settings** to configure security policy properties to enable single sign-on capability. When single sign-on is enabled, only one log on, per directory, on a given computer is allowed. Once logged on, all participating FactoryTalk products that run in that directory on that computer automatically use those same security credentials.

### To enable single sign-on

1. In FactoryTalk Administration Console **Explorer**, expand **System > Policies > System Policies**.
2. Right-click **Security Policy** and select **Properties**.
3. In **Security Policy Properties**, select > to expand **Single Sign-On Policy Settings**.
4. To the right of **Use single sign-on**, select the down arrow.
5. Choose **Enabled**, then select **OK**.

If single sign-on still does not seem to be working properly, the FactoryTalk product in use may not support the single sign-on capability. Some FactoryTalk products always require users to log on, even if single sign-on is enabled.

**See also**

[Disable single sign-on](#) on [page 100](#)

[Security Policy Properties](#) on [page 110](#)

**Disable single sign-on**

To require users to log into each FactoryTalk product separately, configure **Single Sign-On Policy Settings** to disable single sign-on capability.

**To disable single sign-on**

1. In FactoryTalk Administration Console **Explorer**, expand **System > Policies > System Policies**.
2. Right-click **Security Policy** and select **Properties**.
3. In **Security Policy Properties**, select > to expand **Single Sign-On Policy Settings**.
4. To the right of **Use single sign-on**, select the down arrow.
5. Choose **Disabled**, then select **OK**.

**See also**

[Enable single sign-on](#) on [page 99](#)

**Account Policy Settings**

Use **Account Policy Settings** to specify how FactoryTalk manages policies for user, computer, and group accounts. Additional policy settings for computer accounts are managed in **Computer Policy Settings**.

Setting	Description
Logon session lease	<p>Sets the maximum number of hours that a user can remain logged on before the system checks whether the user's account is still valid. Use this setting to prevent logged on users from retaining access indefinitely, even after their accounts are disabled or deleted.</p> <p>For example, if a user's account is disabled or its password changed, and the account name and password cannot be reauthenticated, the logon session becomes invalid. The user can no longer access secure system resources until the user logs on successfully again.</p> <p>Setting this value to <b>0</b> allows the logon session to be used indefinitely, allowing users to have continuous access, and preventing the system from automatically reauthenticating users. This means that the system does not check whether the user's account is still valid.</p> <p><b>Minimum:</b> 0 hours  <b>Maximum:</b> 999 hours  <b>Default:</b> 1 hour</p>

Account lockout threshold	<p>Sets the number of consecutive failed log-on attempts that will cause an account to be locked. If set to <b>0</b>, accounts are never locked.</p> <p>An invalid logon attempt occurs if the user attempts to log on and specifies a correct user name but an incorrect password.</p> <p>A locked account cannot be used until the <b>Account lockout auto reset</b> period expires, or until the account is reset by a FactoryTalk administrator. This helps prevent an unauthorized user from gaining access to the system by guessing a password using a process of elimination.</p> <p><b>Minimum:</b> 0 invalid logon attempts  <b>Maximum:</b> 999 invalid logon attempts</p> <p><b>Defaults:</b></p> <ul style="list-style-type: none"> <li>• For the Network Directory, 3 invalid logon attempts.</li> <li>• For the Local Directory, 3 invalid logon attempts.</li> </ul>
Account lockout auto reset	<p>Specifies the amount of time that must expire before a locked account is reset, allowing the user to attempt access again. Type a value between 0 and 999 minutes to specify the amount of time a user must wait before using the account again to gain access to the system.</p> <p>If set to <b>0</b>, locked accounts are not reset automatically. A FactoryTalk administrator and must unlock the account manually.</p> <p><b>Minimum:</b> 0 minutes  <b>Maximum:</b> 999 minutes</p> <p><b>Default:</b> 15 minutes</p>
Keep record of deleted accounts	<p>Determines whether user accounts can be permanently deleted with no record retained in the system, or flagged as deleted and be permanently disabled, with a record of the deleted account retained in the system.</p> <p>To keep a record of accounts that were deleted, and force all new accounts to be unique, select <b>Enabled</b>. Also, change a policy setting to show deleted accounts in the list of users.</p> <p>To discard accounts when they are deleted, select <b>Disabled</b>. This means that if a user account is deleted, a user account can be recreated again later with the same user name. If the policy is enabled and a user account is deleted, a user account cannot be recreated again later with the same user name, because its record still exists in the system.</p> <p>If the policy is disabled and user account with the same name is recreated, the new user account does not inherit the security settings of the old account. The reason is that all user accounts are identified by means of a unique identifier that is separate from the user name. When deleting a user account, the user's access rights are deleted, but the user account's unique identifier is not deleted.</p> <p>When creating another user account with the same name, recreate the security settings of the account. Either add the user account to a group that already has security settings defined, or create permissions for a user account when securing a resource.</p> <p>For security and audit tracking reasons, and to satisfy compliance requirements in regulated manufacturing industries, it might be necessary to:</p> <ul style="list-style-type: none"> <li>• Keep a record of previously deleted accounts</li> <li>• Ensure that all user accounts can be uniquely identified in the system</li> </ul> <p><b>Default:</b> Disabled</p>

Show deleted accounts in list	<p>Sets whether deleted account records are listed in the <b>Users</b> folder in the <b>System</b> tree. This policy works together with the <b>Keep record of deleted accounts</b> policy. If <b>Keep record of deleted accounts</b> is enabled, enabling <b>Show deleted accounts in user list</b> allows a FactoryTalk administrator to view details about accounts that were deleted.</p> <p>To hide deleted accounts in the list of users, select <b>Disabled</b>. This means that accounts that are deleted are not shown in the list of user accounts, even if keeping a record of deleted accounts. Enable the <b>Show deleted accounts in user list</b> policy to keep a record of deleted accounts (for example, for regulatory compliance), and to view details about accounts that were deleted.</p> <p><b>Default:</b> Disabled</p>
-------------------------------	--

**See also**

[Modify Account Policy Settings](#) on [page 92](#)

[Audit trails and regulatory compliance](#) on [page 36](#)

[Security Policy Properties](#) on [page 110](#)

**Computer Policy Settings**

**Computer Policy Settings** control how computer accounts can access the FactoryTalk Directory remotely. These settings apply only to computer accounts in the FactoryTalk network directory because the FactoryTalk local directory does not permit remote access.

Setting	Description
Require computer accounts for all client machines	<p>Determines whether client computers can access the FactoryTalk network directory without having a computer account in the network directory. Disable this policy to allow users to connect remotely from any computer, even if the computer does not have a computer account in the FactoryTalk Directory.</p> <p>Even when this setting is disabled, create computer accounts for any computers hosting <b>servers</b> – for example, Rockwell Automation Device Servers (FactoryTalk Linx, OPC data servers, Tag Alarm and Event Servers, or HMI servers. Without the server computer accounts, configuring the servers from client computers on the network is not possible. The FactoryTalk network directory Server cannot locate these servers on the network without their computer accounts.</p> <p><b>Enabled</b> allows users to log on to FactoryTalk only if they are logging on from a client computer that has an account in the FactoryTalk Directory. Even if set to Enabled, Remote Desktop Services clients can still log on to FactoryTalk Directory without computer accounts if the <b>Identify terminal server clients using the name of</b> policy is set to <b>Server Computer</b>.</p> <p><b>Disabled</b> allows users to log on to FactoryTalk from any client computer, even if that computer has no computer account in the FactoryTalk network directory.</p> <p><b>Default:</b> Enabled</p>

Identify terminal server clients using the name of	<p>Determines what computer name identifies clients connecting to the FactoryTalk Directory through Remote Desktop Services. This policy also affects whether client computers connecting through Remote Desktop Services require computer accounts in the FactoryTalk Directory.</p> <p><b>Server Computer</b> allows client computers to connect through Remote Desktop Services without requiring accounts in the FactoryTalk Directory, even if the <b>Require computer accounts for all client machines</b> policy is <b>Enabled</b>. This is possible because the FactoryTalk Directory behaves as if the client computer were accessing the FactoryTalk Directory from the Remote Desktop Connection computer.</p> <p>If set to <b>Terminal Client</b> and the <b>Require computer accounts for all client machines</b> policy is <b>Enabled</b>, client computers must have computer accounts in the FactoryTalk Directory to access FactoryTalk applications.</p> <p>If set to <b>Terminal Client</b> and the <b>Require computer accounts for all client machines</b> policy is <b>Disabled</b>, client computers do not require computer accounts in the FactoryTalk Directory to access FactoryTalk applications. This combination of settings is useful for diagnostic logging because the name of the client computer where actions originate can be logged.</p> <p>The <b>Identify terminal server clients using the name of</b> policy also determines which computer name appears in the FactoryTalk Diagnostics Log of actions performed on the system over a Remote Desktop Services connection:</p> <p><b>Terminal Client</b> logs actions using the name of the client computer where the user is connecting to the Terminal Server. The computer name logged in FactoryTalk Diagnostics will be different for each client connecting via Remote Desktop Services.</p> <p><b>Server Computer</b> logs actions using the name of the Terminal Server computer for all users. The computer name logged in FactoryTalk Diagnostics will be the same for all users connecting via Remote Desktop Services.</p> <p><b>Default:</b> Terminal Client</p>
--	--

---

**IMPORTANT** If setting the **Identify terminal server clients using the name of** policy to **Server Computer**, disable single sign-on because the computer name is saved as part of the single sign-on user's credentials, and might affect the level of access a Remote Desktop Services user has to the FactoryTalk system.

---

## See also

[Modify Computer Policy Settings](#) on [page 93](#)

[Security Policy Properties](#) on [page 110](#)

## Directory Protection Policy Settings

The **Directory Protection Policy Settings** specify client computer accounts usage of the FactoryTalk network directory.

Setting	Description
Support non-secure clients	<p>Determines whether client computers with FactoryTalk versions earlier than 2.50 can access a directory server computer with FactoryTalk CPR 9 SR5 or later. The policy is ignored if client computers are installed with FactoryTalk 2.50 or later.</p> <p><b>Allow</b> means client computers with FactoryTalk versions earlier than 2.50 can connect to and retrieve information from a directory server computer with FactoryTalk 2.50 or later.</p> <p><b>Deny</b> means only client computers with FactoryTalk 2.50 can connect to and retrieve information from a directory server computer with FactoryTalk 2.50 or later. Clients with FactoryTalk versions earlier than 2.50 are denied access and a <b>Protocol version mismatch</b> error occurs.</p> <p><b>Default:</b> Allow</p> <p>Disconnect the directory server from the network before changing this policy. Reconnect to the network after applying the change. Otherwise, this policy is not properly enforced.</p>
Audit non-secure client connections	<p>Determines whether an audit message is created when client computers with FactoryTalk versions earlier than 2.50 connect to a directory server computer with FactoryTalk 2.50 or later.</p> <p><b>Enabled</b> means an audit message is created when a client computer with a FactoryTalk version earlier than 2.50 connects to a directory server computer with FactoryTalk 2.50 or later.</p> <p><b>Disabled</b> means an audit message is not created when a client computer with a FactoryTalk version earlier than 2.50 connects to a directory server computer with FactoryTalk 2.50 or later.</p> <p><b>Default:</b> Enabled</p>
Directory cache expiration	<p>Determines how long the cache files remain available after the client computer is disconnected from the server. Once this time elapses, reconnect to the directory server to access the latest data files.</p> <p>If set to 0, cache files never expire.</p> <p><b>Minimum:</b> 0 hours</p> <p><b>Maximum:</b> 9999 hours</p> <p><b>Default:</b> 0 hours</p>
Directory cache expiration warning	<p>Determines when a warning notification displays in the notification area prior to the directory cache expiring. Select FactoryTalk Directory in the notification area to quickly view the time expiration information.</p> <p>If set to 0, warnings do not appear prior to cache expiration. However, notifications can be seen upon disconnection and cache expiration.</p> <p><b>Minimum:</b> 0 hours</p> <p><b>Maximum:</b> 24 hours</p> <p><b>Default:</b> 0 hours before expiration</p>
Security authorization policy	<p>Determines whether the client computer is authorized with directory files from server or local client cache files.</p> <p><b>Require directory update from server before authorizing</b> means the client computer is authorized using directory files from the server.</p> <p><b>Use local client cache</b> means the client computer is authorized using local client cache files. The amount of time for the client computer to wait before transferring cache files is configured in Directory cache transfer waiting time.</p>
Directory cache transfer waiting time	<p>Sets how long the client computer waits before transferring cache files. This only applies to when security authorization uses local client cache.</p> <p><b>Minimum:</b> 5 seconds</p> <p><b>Maximum:</b> 600 seconds</p> <p><b>Default:</b> 5 seconds</p>



## See also

[Modify Directory Protection Policy Settings](#) on [page 95](#)

[Cache expiration policies](#) on [page 105](#)

## Cache expiration policies

In FactoryTalk, rules for directory cache expiration are managed system-wide by the **Directory Protection Policy Settings** security policy properties. These policies determine:

- How long cache files remain available after the client computer disconnects from the server
- If a warning displays before the directory cache expires

Directory cache expiration policies for a specific computer or group of computers can be customized. For example, to allow a group of laptop computers to operate without a network connection for a longer time period, and for the cache to never expire for one of the laptops. To override the FactoryTalk network directory cache expiration policies, set directory cache timeout policies for a computer group or an individual computer.

The directory cache timeout policies cannot be modified in a FactoryTalk local directory.



Tip: The directory cache timeout policies are not supported if the client computer is installed with FactoryTalk Services Platform version 2.40 or earlier.

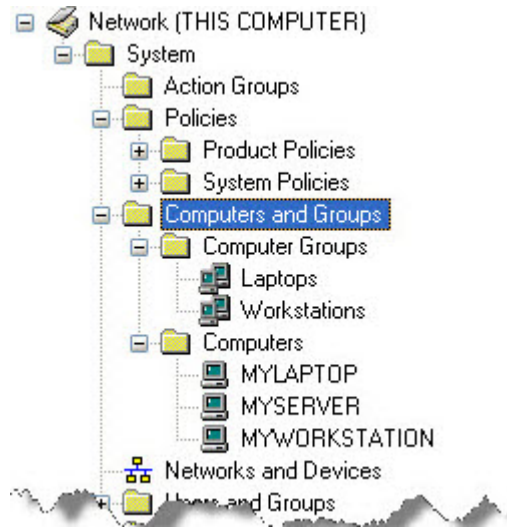
The cache expiration policies in FactoryTalk are applied in this order of precedence:

- By default, all computers in the directory adopt the directory cache expiration policy.
- Computer group cache expiration policies take precedence over the directory cache expiration policy. If a computer is assigned to multiple computer groups, the computer adopts the cache expiration of the first assigned computer group in alphabetical order.
- Computer cache expiration policies take precedence over the directory cache expiration policies of any of its computer groups.

This example shows how the cache expiration policies work.

Suppose that:

- Three computers connected to the FactoryTalk network directory server. MYLAPTOP is a member of computer group Laptops. MYWORKSTATION is a member of computer group Workstations.



The current setting covers the majority of your computers. Optionally, customize specific settings for some cases. For example, to allow computers of Laptops to operate in a disconnected state for a longer period (for example, 7 days, that is, 168 hours). Also, turn off the cache expiration functionality for computer *MYSERVER*.

To achieve these results,

- In the computer group policy setting of Laptops, select to override the directory cache expiration policy and set the computer group cache expiration value to **168**.
- In the computer policy setting of *MYSERVER*, select to override the directory cache expiration policy and set the computer cache expiration value to **0**.

### See also

[Modify Directory Protection Policy Settings](#) on [page 95](#)

[FactoryTalk Security](#) on [page 29](#)

## Password Policy Settings

For FactoryTalk user accounts, use **Password Policy Settings** to configure these security property settings:

- Password encryption method
- Password complexity
- Minimum password length
- Number of previous passwords remembered
- Minimum password age
- Maximum password age
- Password expiration warning

Passwords for FactoryTalk user accounts can be up to 64 characters long. A set of password policies determines the length and complexity of passwords. As a matter of good security practice, do not use blank passwords with accounts.

To help avoid intermittent security failures or an inability to log on, always use a password for all Windows-linked accounts. If not using a password for Windows-linked accounts, on the local computer disable the Windows local security policy **Accounts: Limit local account use of blank passwords to console logon only**. Define password policies for Windows-linked accounts in Windows.

Setting	Description
Password encryption method	<p>Determines how the password is encrypted when stored in the FactoryTalk Directory.</p> <ul style="list-style-type: none"> <li>• <b>MD5</b> - A 128-bit hash algorithm that is used with previous versions of FactoryTalk Services Platform. Retained for backwards compatibility, but has known security vulnerabilities.</li> <li>• <b>SHA-256</b> - A 256-bit hash algorithm that meets modern security requirements. Where possible, transitioning systems to use SHA-256 password encryption method is strongly recommended.</li> </ul>
Passwords must meet complexity requirements	<p>Determines how simple or complex passwords must be.</p> <p><b>Disabled</b> means that passwords to user accounts can include any characters or combinations of characters.</p> <p><b>Enabled</b> requires users to create passwords that are more secure, because passwords used for user accounts:</p> <ul style="list-style-type: none"> <li>• Cannot contain <i>all</i> of the user account name. For example, a user account named John12 cannot have the password John1234. However, the password 12John is permitted. This check is case sensitive so John12 could have the password jOHn12.</li> <li>• Must contain at least six characters (change the minimum value using the <b>Minimum password length</b> policy)</li> <li>• Must contain characters from three of these four categories: <ul style="list-style-type: none"> <li>• Unaccented uppercase characters (A to Z)</li> <li>• Unaccented lowercase characters (a to z)</li> <li>• Numerals (0 to 9)</li> <li>• Non-alphanumeric characters (!, @, #, %)</li> </ul> </li> </ul> <p>If enabled, any passwords that do not meet these minimum requirements are rejected, and the user is prompted to create a password that satisfies the criteria. These complexity requirements are defined by the system and cannot change.</p> <p>The <b>Passwords must meet complexity requirements</b> policy overrides the <b>Minimum password length</b> policy if the minimum password length is less than six characters. If the minimum password length is greater than six characters, <b>Minimum password length</b> takes precedence.</p> <p><b>Default:</b> Disabled.</p>

<p>Minimum password length</p>	<p>Sets the minimum number of characters a user account password to a must contain. A value of <b>0</b> allows you to create user accounts without passwords.</p> <p>If enabled, the <b>Passwords must meet complexity requirements</b> policy requires a minimum password length of six characters. However, if the <b>Minimum password length</b> policy is set to more than six characters, this overrides the <b>Passwords must meet complexity requirements</b> policy.</p> <p><b>Minimum: 0 characters.</b></p> <hr/> <p><b>IMPORTANT</b> A value of <b>0 characters</b> enables the creation of user accounts without passwords.</p> <hr/> <p><b>Maximum: 64 characters</b></p> <p><b>Defaults:</b></p> <ul style="list-style-type: none"> <li>• For the network directory, <b>6 characters</b>.</li> <li>• For the local directory, <b>0 characters</b>. Users can set the passwords to their accounts to be blank.</li> </ul>
<p>Previous passwords remembered</p>	<p>Sets the number of unique new passwords that must be created before reusing an old password. This policy ensures that old passwords are not continually reused.</p> <p>To maintain the effectiveness of the <b>Previous passwords remembered</b> policy, set the <b>Minimum password age</b> policy to a non-zero value to prevent passwords from being changed immediately. This policy is also necessary to make the <b>Maximum password age</b> policy meaningful.</p> <p>If this policy is set to <b>0 passwords</b> users can immediately re-use their existing passwords when their passwords expire.</p> <p><b>Minimum: 0 passwords</b></p> <p><b>Maximum: 24 passwords</b></p> <p><b>Default: 3 passwords</b></p>
<p>Minimum password age</p>	<p>Sets the minimum number of days passwords must be in effect before they can change. If set to <b>0</b>, users can change their passwords immediately following a prior change.</p> <p>This policy works together with the <b>Previous passwords remembered</b> policy to prevent a user from changing a password repeatedly until one of the user's old password favorites can be used again.</p> <p>If the value of the <b>Minimum password age</b> is greater than the value of the <b>Maximum password age</b>, the minimum password age is ignored.</p> <ul style="list-style-type: none"> <li>• <b>Minimum: 0 days</b></li> <li>• <b>Maximum: 999 days</b></li> <li>• <b>Default: 0 days</b>. Users can change their passwords at any time.</li> </ul>

Maximum password age	<p>Sets the maximum number of days passwords can be used before they must change. If set to <b>0</b>, passwords never expire. When setting this value, be sure also to specify a smaller value for the <b>Password expiration warning</b>.</p> <p>If the <b>Maximum password age</b> expires, the user is prompted to change the password when next logging on with the account.</p> <p>If the value of the <b>Maximum password age</b> policy is less than the value of the <b>Minimum password age</b> policy, the minimum password age is ignored.</p> <ul style="list-style-type: none"> <li>• <b>Minimum: 0 days</b></li> <li>• <b>Maximum: 999 days</b></li> <li>• <b>Default: 0 days.</b> Users are never prompted to change their passwords.</li> </ul>
Password expiration warning	<p>Sets the number of days before passwords are due to expire that the system begins prompting users to change their passwords.</p> <p>If <b>Maximum password age</b> is set to 0, the password expiration warning never appears.</p> <p>If the value of the <b>Password expiration warning</b> is greater than the value of the <b>Maximum password age</b>, a password expiration warning appears the next time the user attempts to log on.</p> <ul style="list-style-type: none"> <li>• <b>Minimum: 0 days before expiration</b></li> <li>• <b>Maximum: 999 days before expiration</b></li> <li>• <b>Default: 14 days before expiration</b></li> </ul>

## See also

[Add a FactoryTalk user account](#) on [page 43](#)

[Add a Windows-linked user account](#) on [page 45](#)

[Security Policy Properties](#) on [page 110](#)

## Single Sign-On Policy Settings

Use **Single Sign-On Policy Settings** in **Security Policy Properties** to set whether users can log on once to the FactoryTalk system, or must log on to each FactoryTalk product separately.

Disable single sign-on if users will be connecting through Remote Desktop Services using the name of the Remote Desktop Connection server computer. This is determined through the computer policy setting **Identify terminal server clients using the name of**. The computer name is saved as part of the single sign-on user's credentials, and might affect the level of access a user has to the FactoryTalk system.

Setting	Description
Enabled	Requires users to log on to the FactoryTalk system only once. The system checks the user's access rights as the user performs actions after logging on. If the user has the required access rights, the action is allowed to proceed. If the user does not have the required access rights, the action is prevented from taking place. The user is not prompted repeatedly to log on with a user name and password.
Disabled	Requires users to log on to each FactoryTalk product separately.

## See also

[When to disable single sign-on](#) on [page 110](#)

[Modify Computer Policy Settings](#) on [page 93](#)

[Security Policy Properties](#) on [page 110](#)

## When to disable single sign-on

If multiple users are sharing the same Windows user account, but have different FactoryTalk user accounts, it might be necessary to disable single sign-on. This is because with single sign-on enabled, the last user that logged on to FactoryTalk is automatically logged on to all subsequent FactoryTalk products. If the ability to distinguish the actions of individual users is necessary, disable single sign-on to force all users to identify themselves to each FactoryTalk product they use.

There is no way to log all users off all FactoryTalk products simultaneously. This is because some products might need to run without interruption in the background. To log all users off all FactoryTalk products simultaneously, log off Windows. Logging off Windows also shuts down all FactoryTalk products that were started in the Windows session, regardless of how many users were logged on.

Also disable single sign-on when logging on to FactoryTalk through Remote Desktop Services using the name of the Remote Desktop Connection **server** computer. Alternatively, change the security policy **Identify terminal server clients using the name of** to allow Remote Desktop Services users to connect using the name of the Remote Desktop Connection **client** computer.

If single sign-on still does not seem to be working properly, the FactoryTalk product in use may not support the single sign-on capability. Some FactoryTalk products always require users to log on, even if single sign-on is enabled.

## See also

[Enable single sign-on](#) on [page 99](#)

[Security Policy Properties](#) on [page 110](#)

## Security Policy Properties

How do I open Security Policy Properties?

In the **Explorer** window, expand **System > Policies > System Policies** and double-click **Security Policy**.

Use **Security Policy Properties** to define general rules for implementing security across all FactoryTalk products in the system. To modify security policies, obtain the appropriate permissions for the **System Policies** folder in the **Explorer**.

- **Account Policy Settings:** Specify how FactoryTalk manages policies for user, computer, and group accounts.
- **Badge Policy Settings:** Specify how FactoryTalk user accounts can log on using a Radio-Frequency-Identification (RFID) badge.
- **Computer Policy Settings:** Specify how computer accounts in the FactoryTalk network directory can use remote access.
- **Directory Protection Policy Settings:** Specifies client computer accounts usage of the FactoryTalk network directory.
- **Password Policy Settings:** Configures password requirements for FactoryTalk user accounts.
- **Single Sign-On Policy Settings:** Controls whether users can log on once to the FactoryTalk system, or must log on to each FactoryTalk product separately.

### See also

[Modify Account Policy Settings](#) on [page 92](#)

[Modify Computer Policy Settings](#) on [page 93](#)

[Modify Directory Protection Policy Settings](#) on [page 95](#)



[Modify Password Policy Settings](#) on [page 96](#)

[Modify Badge login policies](#) on [page 98](#)

## Navigate the Policy Properties windows

All **Product Policies** and **System Policies** windows contain the same features to navigate to the property setting.

### To navigate the Policy Properties windows

- To sort the policy settings alphabetically, select **Alphabetic:** 
- To sort the policy settings by category, select **Categories:** 
- To expand or collapse the list of policy settings in a category, select the arrow next to the category name.
- To change a setting, select the setting, then choose or type a new value.
- To change the size of any column, move the cursor over a column heading until a cross-bar shape appears, then select and drag to expand or reduce the column size.
- To resize the description of a selected setting, drag the top part of the description pane at the bottom of the window.

### See also

[Assign user rights to make system policy changes](#) on [page 78](#)

[Set audit policies](#) on [page 86](#)

[Security Policy Properties](#) on [page 110](#)

## Export policies to XML

Export policies to save current FactoryTalk Directory policy settings to an XML file. Use an XML or text comparison tool to determine policy changes between exported policy files.

The exported policies are limited to the policies accessible by the logged on user. If the logged-on user does not have Read, Execute, or List Children permissions for a policy or its parent folders, that policy is not exported.

### Prerequisites

Obtain permissions for each policy to be exported:

- Common > Read
- Common > Execute
- Common > List Children

### To export policies to XML

1. From the **Tools** menu, select **Export Policies**.
2. Enter or browse to a path for the XML file.
3. Select **Export**.

### See also

Export Policies

[Set system security policies](#) on [page 91](#)



## Set product-specific policies

To prevent users of a FactoryTalk product from making unwanted changes, restrict user access to individual product features. Only users with the required level of access can use the product features once secured.

Example: Configure product policies for RSLinx Classic, to restrict the ability to shut down the RSLinx Classic service to only the group *Network admins*, to prevent system operators from inadvertently shutting down RSLinx Classic during run time.

A product policy is a collection of securable features in a FactoryTalk product. A product policy applies to only one product—if a user account is denied access to a product feature, that feature cannot be used when using that product, but the feature can still be used in other FactoryTalk products if the feature was not secured in that product.

To view and edit permissions:

- For features of a single product. In **Explorer**, expand **System> Policies > Product Policies**. Expand the folder for the product, right-click **Feature Security** and then select **Properties**. **Feature Security Properties** opens. The configurable permissions are listed under **Category**. Select **Configure Security** next to the category of permissions being edited and then choose the users or groups that will be allowed or denied access to the feature.
- For features of multiple products. In **Explorer**, expand **System> Policies**. Right-click **Product Policies** and select **Configure Feature Security** to open **Feature Security for Product Policies**. Then select to allow or deny permissions as needed for the products in the FactoryTalk Directory.

### See also

[Secure features of a single product](#) on [page 114](#)

[Secure multiple product features](#) on [page 114](#)

[Differences between securable actions and product features](#) on [page 116](#)

## Secure features of a single product

To restrict access to one or more features of a single FactoryTalk property, use **Feature Security Properties**.

### To secure features of a single product

1. Log on to the FactoryTalk Directory.
2. In FactoryTalk Administration Console **Explorer**, expand **System > Policies > Product Policies**.
3. In the **Product Policies** folder, expand the folder for the product.
4. Right-click **Feature Security** and select **Properties**.
5. In **Feature Security Properties**, select the row containing the feature. A description of the feature appears at the bottom of the window.
6. Configure the security settings for the feature:
  - If the product policy contains settings that are configured using lists, configure the settings, select **OK**, and skip the rest of the steps.
  - If the product policy is not configured using lists, in the column on the right, select **Browse (...)** beside **Configure Security**.
7. Use **Configure Securable Action** to select the users or user groups that have permission to access the feature, and select **OK**.
8. Repeat steps 4-6 as needed to configure the features that make up the product policy.
9. Select **OK**.

### See also

[Feature Security for Product Policies](#) on [page 115](#)

[Permissions](#) on [page 135](#)

## Secure multiple product features

Use **Feature Security for Product Policies** to secure features of multiple FactoryTalk products at once. The term *action* in **Feature Security for Product Policies** refers to a product feature. Each FactoryTalk product installed provides different securable features (actions).

Select **plus (+)** next to each FactoryTalk product to view the features to secure.

### To secure multiple product features

1. Log on to the FactoryTalk Directory.
2. In FactoryTalk Administration Console **Explorer**, expand **System > Policies**.
3. Right-click **Product Policies**, and select **Configure Feature Security**.
4. (optional) To add a user and computer to the **Users** list, select **Add**. In **Select User and Computer**, select a user or group of users, and a computer or group of computers, and select **OK**.

5. In **Feature Security for Product Policies**, either:
  - Select **User** to specify which features a selected user can perform.
  - Select **Action** to specify which users can access a selected feature. Skip to step 7.
6. To set permissions by user:
  - In the **Users** list, select the user or user group to secure their access.
  - In the **Actions** list, expand the list of products and categories as needed to locate the feature to secure, and select the feature. Skip to step 8.
7. To set permissions by feature:
  - In the **Actions** list, expand the list of products and categories to locate the feature to secure, and select the feature.
  - In the **Users** list, select the user or group whose access to the feature is being secured.
8. Specify security settings, either:
  - Select **Allow** to allow a user to perform the action.
  - Select **Deny** to deny a user access to the action.

If both **Allow** and **Deny** are cleared, the user is denied access to the feature.
9. Repeat steps 5–8 as needed to secure additional product features.
10. Select **OK**.

## See also

[Secure features of a single product](#) on [page 114](#)

[Permissions](#) on [page 135](#)

[Differences between securable actions and product policies](#) on [page 116](#)

## Feature Security for Product Policies

How do I open Feature Security for Product Policies?

1. In the **Explorer** window, expand **System > Policies**.
2. Right-click **Product Policies**, then click **Configure Feature Security**.

Use the **Permissions** tab in **Feature Security for Product Policies** to secure features in multiple FactoryTalk products at the same time.



Tip: Security for FactoryTalk Linx Gateway must be configured one feature at a time.

If using both a local and a network FactoryTalk Directory configure product policies in each directory separately.

Setting	Description
View permissions by	View the same set of permissions from two different points of view: <ul style="list-style-type: none"> <li>• by user – Select <b>User</b>, select a user and then specify what product features that user can access</li> <li>• by action – Select <b>Action</b>, select a product feature and then specify which users can perform the feature</li> </ul>

Add	Select <b>Add</b> to add a user and computer to the list.
Remove	Select <b>Remove</b> to remove a user and computer from the list.
Action list	The term action in <b>Feature Security for Product Policies</b> refers to a product feature. Each FactoryTalk product installed provides different securable features (actions). Select <b>plus (+)</b> next to each FactoryTalk product to view the features to secure. For more information about each product, refer to the product's documentation.
Allow	Select to allow access to a product feature.
Deny	Select to deny access to a product feature.
Allow and Deny	Clear both to deny access to the feature.

**See also**

[Secure multiple product features](#) on [page 114](#)

[Permissions](#) on [page 135](#)

[Things you can secure](#) on [page 32](#)

[Differences between securable actions and product policies](#) on [page 116](#)

**Feature Security Policies**

How do I open Feature Security Properties?

1. Start FactoryTalk Administration Console or FactoryTalk View Studio and then log on to the FactoryTalk Directory.
2. In **Explorer**, expand **System > Policies > Product Policies** and then expand the folder for the product.
3. Right-click **Feature Security** and select **Properties**.

Use the **Policy Settings** tab in **Feature Security Properties** to configure the security policy settings available for a FactoryTalk product. Each FactoryTalk product has a different set of security policy settings that can be configured to allow or deny access to the feature by specific users or groups.

Policy settings are completely separate in the network directory and local directory. Changes made to the policy settings in one directory do not apply to the other directory.

**See also**

[Secure features of a single product](#) on [page 114](#)

[Secure multiple product features](#) on [page 114](#)

[Differences between securable actions and product policies](#) on [page 116](#)

**Differences between securable actions and product policies**

A product policy is a collection of securable features in a FactoryTalk product. A product policy is different than a securable action in these ways:

- A securable action applies to all products that use that action in a particular context—such as an application or area.

- A product policy applies to only one product—if denied permission to a product feature, that product feature cannot be used when using that product.

In some cases, there are securable actions and product policies for the same capability. For example, that Logix Designer application has both a securable action and a product policy named **Firmware: Update**.

- The securable action applies to all products—if denied permission to the **Firmware: Update** action in an application or area, firmware in the controller from that application or area using any product cannot be updated.
- The product policy applies to only Logix Designer application—if denied permission to **Firmware: Update**, firmware cannot be updated when using Logix Designer application to configure any controller.

Unlike securable actions for resources, product policies do not inherit security settings. When specifying permissions for product policies, clearing both **Allow** and **Deny** does not allow the policy setting to inherit security. Instead, clearing both denies access to the product feature.

For details about securable actions and product policies in a particular FactoryTalk product, see the documentation for the product.

### See also

[Secure features of a single product](#) on [page 114](#)

[Secure multiple product features](#) on [page 114](#)

[Secure resources](#) on [page 135](#)



## Manage logical names

A logical name is an alias that identifies a control network or device. Use a logical name to provide a shorter or more intuitive name to identify a device, instead of using its network relative path. Logical names also change the way devices inherit security permissions. Control devices with identical logical names share security permissions across different control networks and across different computers, without requiring identical driver names or relying on identical network paths.

Define logical names in FactoryTalk Administration Console before configuring security for RSLogix 5000 controllers. For all other types of control hardware, choose whether to associate security settings with logical names or with network relative paths.

A logical name can be part of a resource grouping assigned to an area or application. If a logical name is assigned to an area, it inherits the security permissions of the area.

### See also

[Logical names](#) on [page 119](#)

[Add a logical name](#) on [page 121](#)

[Add a device to a logical name](#) on [page 122](#)

[Assign a control device to a logical name](#) on [page 123](#)

[Add a logical name to an area or application](#) on [page 124](#)

## Logical names

A logical name is an alias that identifies a control network or device. Use logical names to provide a shorter or more intuitive name to identify a device instead of using its network relative path. Logical names also change the way devices inherit security permissions.

Consider these questions:

Question	Answer
Why use logical names?	<ul style="list-style-type: none"> <li>• Control devices with identical logical names share security permissions across different control networks and across different computers, without requiring identical RSLinx Classic driver names or relying on identical network paths.</li> <li>• Logical names are required to configure security for RSLogix 5000 controllers.</li> <li>• Logical names can be used as aliases for control devices with multiple paths, so that each instance of the device is associated with a single set of security permissions.</li> </ul>
What happens when a logical name is added?	<ul style="list-style-type: none"> <li>• After adding a logical name for a control device, the security system automatically uses the security permissions associated with that name, rather than with the device's network relative path, to determine access permissions.</li> <li>• After defining a new logical name, establish security permissions for the control device. Be sure to add an identical logical name for the control device on each computer on the network that has access to the device, if the different computers have different relative paths to the device.</li> <li>• If security is configured for a control device identified by a network relative path, and then later a logical name for the device is added, the original security permissions are not lost; they remain associated with the path, but they do not transfer to the logical name. As a result, the original security permissions are no longer accessible, because security now attempts to access the security permissions using the name, not the path.</li> <li>• If a control device's logical name is changed, the original security permissions remain associated with the first logical name. Re-add security permissions for the device, to associate them with the new logical name.</li> </ul>
What happens when a logical name is deleted?	<ul style="list-style-type: none"> <li>• When a logical name is deleted, the security system automatically uses the security permissions associated with the device's network relative path.</li> <li>• The logical name and its associated security permissions still exist in the security system after a name is deleted. For example, suppose the name "MyPLC1" is assigned to Device1 on Computer A and Computer B, and each computer has a different relative path to Device1. When a user attempts to perform an action on Device1 from either computer, the security system checks the permissions associated with "MyPLC1." Now suppose we delete the name "MyPLC1" on Computer A, but leave it assigned on Computer B. If a user attempts to perform an action on Device1 from Computer A, security uses the permissions associated with the Device1's network relative path. If a user attempts to perform an action on Device1 from Computer B, however, security uses the permissions associated with the logical name "MyPLC1."</li> <li>• Do not delete logical names for RSLogix 5000 controllers. Because RSLogix 5000 controllers do not have network relative paths, deleting a logical name can cause unexpected results.</li> </ul>



## See also

[Add a logical name](#) on [page 121](#)

[Delete a logical name](#) on [page 122](#)

[Assign a control device to a logical name](#) on [page 123](#)

[Logical Name Properties](#) on [page 126](#)

## Add a logical name

Add a logical name to **Networks and Devices** to create an alias that identifies a control network or a device. Use a logical name to provide a shorter or more intuitive name to identify a device, instead of using its network relative path. Logical names also change the way devices inherit security permissions. Control devices with identical logical names share security permissions across different control networks and across different computers, without requiring identical driver names or relying on identical network paths.

Add logical names in FactoryTalk Administration Console before configuring security for RSLogix 5000 controllers. For all other types of control hardware, choose whether to associate security settings with logical names or with network relative paths.

Logical names can be added and configured in advance of creating areas or applications.

## To add a logical name

1. In FactoryTalk Administration Console **Explorer**, expand **Networks and Devices** until **Logical Names** is visible.
2. Right-click **Logical Names** and select **New Logical Name**.
3. In **New Logical Name**, enter the name. For a RSLogix 5000 controller, type a name that is identical to the device name stored in the controller.
4. Select **OK**.

The logical name is created and can be assigned to an area or application using **Resources Editor**.



Tip: Alternatively, select an area or application and add a logical name to it. This assigns the logical name to the area or application so that it immediately inherits the security permissions of that area or application.

## See also

[Add a logical name to an area or application](#) on [page 124](#)

[Add a device to a logical name](#) on [page 122](#)

[Delete a logical name](#) on [page 122](#)

## Delete a logical name

Delete a logical name from **Networks and Devices** when not needed as an alias for a control device or network. After deleting a logical name, the security permissions for the devices associated with it revert to the permissions of the device or network.

---

**IMPORTANT** Because RSLogix 5000 controllers do not use network relative paths, deleting a logical name associated with a RSLogix 5000 controller can cause unexpected results.

---

### To delete a logical name

1. In FactoryTalk Administration Console **Explorer**, expand **Networks and Devices** until **Logical Names** is visible.
2. Right-click the logical name and select **Delete**.

### See also

[Add a logical name](#) on [page 121](#)

[Delete a logical name from an area or application](#) on [page 124](#)

[Logical names](#) on [page 119](#)

## Add a device to a logical name

Use **Logical Name Properties** to add control devices or networks to a logical name so that they inherit the security permissions of the logical name.

### To add devices to a logical name

1. In FactoryTalk Administration Console **Explorer**, expand **Networks and Devices** until the logical name is visible.
2. Right-click the logical name, then select **Properties**.
3. In **Logical Name Properties**, select **Add**.
4. In **Device Browser**, select a device, or type the network relative path to a device that does not exist yet, but will be added later.
5. When finished, select **OK**.

### See also

[Remove a device from a logical name](#) on [page 122](#)

[Delete a logical name](#) on [page 122](#)

## Remove a device from a logical name

Use **Logical Name Properties** to remove a device association from a logical name.

---

**IMPORTANT** Do not remove an RSLogix 5000 controller from a logical name. Because RSLogix 5000 controllers do not use network relative paths, removing the device from a logical name can cause unexpected results.

---

## To remove a device from a logical name

1. In FactoryTalk Administration Console **Explorer**, expand **Networks and Devices** until the logical name is visible.
2. Right-click the logical name, then select **Properties**.
3. In **Logical Name Properties**, in the **Device members** list, select a device or network.
4. Select **Remove**, then **OK**.

## See also

[Assign a control device to a logical name](#) on [page 123](#)

[Delete a logical name](#) on [page 122](#)

## Assign a control device to a logical name

A logical name is an alias that identifies a control network or device. Add logical names in FactoryTalk Administration Console before configuring security for RSLogix 5000 controllers. If assigned to an area or application, a logical name inherits the security permissions of that area or application.

Use **Device Properties** to assign a control device to an existing logical name or add the device to a new logical name.

## To assign a control device to a logical name

1. Expand **Networks and Devices** until the network or device is visible.
2. Right-click the network or device and select **Properties**.
3. In **Device Properties**, the **Logical name** list displays the current logical name the device or network it is assigned to.
4. Either:
  - Assign a new logical name. Select **<New...>**. In **New Logical Name**, enter a descriptive name and select **OK**.
  - Select from an existing logical name or change the logical name associated with the device. Select the **Logical name** drop-down and select the logical name to assign the device to.
5. Select **OK**.
6. If different computers have different relative paths to the device, add an identical logical name for the control device on each computer on the network that has access to the device.



Tip: If you change the logical name of a control device, the security permissions remain associated with the first logical name. Re-add security permissions for the device to associate them with the new logical name.

## See also

[Remove a device from a logical name](#) on [page 122](#)

[Add a logical name to an area or application](#) on [page 124](#)

## Add a logical name to an area or application

Devices with identical logical names share security permissions across different control networks and across different computers, even if those devices are configured with different driver names or network paths. Add logical names before configuring security for RSLogix 5000 controllers. For all other types of control hardware, choose whether to associate security settings with logical names or with network relative paths.

Add a logical name to an area or application when the permissions associated with the logical name are inherited from that area or application.

### Prerequisites

Adding a logical name requires these permissions for the area or application:

- Common > Create Children
- Common > List Children
- Common > Read

### To add a logical name to an area or application

1. In FactoryTalk Administration Console **Explorer**, right-click the application or area, point to **Logical Name** and then select **New**.
2. In **New Logical Name**, type a name and select **OK**.

### See also

[Logical names](#) on [page 119](#)

[Delete a logical name from an area or application](#) on [page 124](#)

## Delete a logical name from an area or application

Delete a logical name from an area or an application to break the link between the logical name and the permissions associated with the area or application. .

### Prerequisites

Deleting a logical name requires these permissions for the application or area:

- Common > Delete
- Common > List Children
- Common > Read

## To delete a logical name from an area or application

1. In FactoryTalk Administration Console **Explorer**, expand the local or network directory tree until the application or area that contains the logical name is visible.
2. **Right-click** the application or area icon, and select **Resource Editor**.
3. In the **Resources Editor**, the application is selected in the **Areas** list.
4. In the **Associated Resources** list, select the logical name to delete, and then select **Cut**.
5. Select **Close**.

### See also

[Logical names](#) on [page 119](#)

[Add a logical name to an area or application](#) on [page 124](#)

## New Logical Name

How do I open New Logical Name?

In the **Explorer** window, expand the FactoryTalk network or local directory tree until the application or area where you would like to assign the logical name is visible, right-click the area or application, point to **Logical Name**, and click **New**.

Alternately, open **New Logical Name** from the **Resources Editor** or the **Logical Names** tree in the **Explorer** (if available).

Use **New Logical Name** to create an alias for the path to a device. A logical name associates security permissions directly with the name, rather than with the path. This allows you to associate a network or device with a single set of security permissions. Devices with identical logical names share security permissions across different control networks and across different computers.

---

**IMPORTANT** When using RSLogix 5000® controllers, you must use logical names to add a mapping between FactoryTalk Administration Console and the devices.

---

After creating a new logical name, type a descriptive name to identify it.

- If **New Logical Name** is opened from an application or area in FactoryTalk Administration Console **Explorer**, the new logical name is assigned to the application or area.
- If **New Logical Name** is opened from **Select Resources**, use **Logical Name Properties** to assign the new logical name to an application or area.

### See also

[Add a logical name](#) on [page 121](#)

[Add a logical name to an area or application](#) on [page 124](#)

[Resources Editor](#) on [page 132](#)

## Logical Name Properties

How do I open Logical Name Properties?

In the **Explorer** window, expand the FactoryTalk network or local directory tree until the application or area where you would like to assign the logical name is visible, right-click the area or application, point to **Logical Name**, and click **New**.

Alternately, open **New Logical Name** from the **Resources Editor** or the **Logical Names** tree in the **Explorer** (if available).

Use **Logical Name Properties** to:

- View the control devices associated with a logical name
- Add or remove control devices from a logical name
- View or remove the area associated with a control device via its resource grouping

Use the following settings to edit the properties of a logical name.

Setting	Description
Logical name	Select a logical name to edit the control devices associated with it. To create a new logical name, select <b>New</b> and then, in <b>New Logical Name</b> , type a logical name. For a RSLogix 5000 controller, type a name that is identical to the device name stored in the controller. Devices with identical logical names share security permissions across different control networks and across different computers, even if those devices are configured with different driver names or network paths. After defining a logical name, create security permissions for the control device. The new security permissions that you define are now associated with the logical name. Any security permissions defined earlier, before a logical name was added, remain associated with the device's network relative path, and are not copied to the logical name. Because RSLogix 5000 devices do not use network relative paths, define logical names for RSLogix 5000 devices before configuring security.
Device members	This list shows the network relative paths of the devices that are referenced by the selected logical name. To add devices to the selected logical name, select <b>Add</b> . You can add multiple devices to a single logical name, but you cannot add a single device to multiple logical names. To save changes, select <b>Apply</b> . To remove a device from the selected logical name, select the device and then select <b>Remove</b> .
Area associated with	If the selected logical name is a member of a hardware resource grouping, this field shows the area from which the logical name inherits its security permissions. The information in this field appears only as a reference. You cannot edit this field. To remove the logical name from the area, select <b>Remove</b> .

### See also

[Add a logical name](#) on [page 121](#)

[Add a device to a logical name](#) on [page 122](#)

[Remove a device from a logical name](#) on [page 122](#)

## Device Properties

For control hardware displayed in the **Networks and Devices** tree, use **Device Properties** to:

- View network relative paths
- Add a device to a new logical name
- Assign a control device to an existing logical name
- Change the logical name associated with the device
- Remove a device from a logical name
- Remove the control device from a resource grouping

---

**IMPORTANT** Do not remove RSLogix 5000 controllers from a logical name. Because RSLogix 5000 controllers do not use network relative paths, removing the device from a logical name can cause unexpected results.

---

Setting	Description
Device path	Displays the network relative path of the device. This setting is read-only.
Logical name	<p>Associates a device with a logical name. Select a logical name to view the area associated with the logical name. The area indicates the resource grouping to which the logical name belongs. Do either:</p> <ul style="list-style-type: none"> <li>• To create a new logical name, select <b>&lt;New...&gt;</b>. In <b>New Logical Name</b>, enter a descriptive name and select <b>OK</b>.</li> <li>• To associate the device with an existing logical name, or to change the logical name associated with the device, under <b>Logical name</b> select the logical name.</li> <li>• To remove the logical name the device is associated with, select <b>None</b>. The security system automatically uses the security permissions associated with the device's network relative path.</li> </ul>
Area associated with	If the selected logical name is a member of a hardware resource grouping, this setting displays the area from which the logical name inherits its security permissions. This setting is read-only.
Remove	To remove the logical name from the area, select <b>Remove</b> . This removes the logical name from the resource grouping.

## See also

[Assign a control device to a logical name](#) on [page 123](#)





## Resource grouping

A resource grouping is a collection of hardware resources from the **Networks and Devices** tree that is associated with an application or area. Grouping hardware resources under an application or area allows defining of security permissions for a set of control hardware in one step, rather than having to set permissions for each device separately. Hardware in a resource grouping can be defined by its network relative path or by its logical name.

To manage the security of control hardware through an application or area, use the **Resources Editor** to:

- Group hardware resources in an application or area.
- Move a resource between areas.
- Remove devices from a resource grouping.

### See also

[Group hardware resources in an application or area](#) on [page 130](#)

[Move a resource between areas](#) on [page 131](#)

[Remove a device from a resource grouping](#) on [page 131](#)

[Resource groupings](#) on [page 129](#)

## Resource groupings

A resource grouping is a collection of hardware resources from the **Networks and Devices** tree that is associated with an application or area. A resource grouping is not a separate account type.

Grouping resources under an application or area allows granting or denying security permissions for a set of control hardware in one step, rather than setting permissions for each device separately.

Create a resource grouping in any application or area in the FactoryTalk Directory by selecting resources to associate with the area in the **Resources Editor**. A resource grouping automatically inherits the security settings of the application or area where the resource group is located.

These security permissions might be explicit permissions defined specifically for the area, or they might be inherited from the application in which the area is located, or from the FactoryTalk Directory in which the application is located. If needed, set explicit permissions for a device that override the security permissions set for its resource group by browsing for the network or device in the **Networks and Devices** tree.

To prevent conflicting permissions, these configurations are not permitted:

- Nesting resource groupings within other resource groupings.
- Including the same network or device in multiple resource groupings within the same FactoryTalk Directory.

### See also

[Group hardware resources in an application or area](#) on [page 130](#)

[Remove a device from a resource grouping](#) on [page 131](#)

[Permissions](#) on [page 135](#)

## Group hardware resources in an application or area

Group hardware resources to manage their security settings through the application or area. Devices in a resource grouping inherit security permissions from their associated application or area.

### Prerequisites

Grouping hardware resources together requires these permissions for the application or area:

- Common > Read
- Common > List Children
- Common > Configure Security

### To group hardware resources in an application or area

1. In FactoryTalk Administration Console **Explorer** right-click any application or area and then select **Resource Editor**.
2. In **Resources Editor**, select **Manage Resources**. **Select Resources** opens
3. (optional) To create a new logical name that can be added to a resource grouping, select **Add New Logical Name**.
4. Select the resource, either:

- Select the logical name of the resource. Expand the **Logical Names** tree until the device is visible.

To filter the list of logical names:

- Select **Show only logical names not associated with areas** to view the logical names for only those devices that are not already associated with an application or area.
- Select **Show all logical names** to view all logical names even if they are already associated with an application or area.
- Select the resource using its network relative path, expand the **Networks and Devices** tree until the device is visible.

5. After selecting the resource in the tree, use the > to move it into the **Selected resources** list.
6. When finished, select **OK**.

### See also

[Move a resource between areas](#) on [page 131](#)

[Remove a device from a resource grouping](#) on [page 131](#)

[Resource groupings](#) on [page 129](#)

## Move a resource between areas

Use the **Resources Editor** to move a hardware resource from one application or area to another. The device or control network that is moved inherits the security permissions of its new area or application.

### Prerequisites

Moving hardware resources between areas requires these permissions for the application or area:

- Common > Read
- Common > List Children
- Common > Configure Security

### To move a resource between areas

1. In FactoryTalk Administration Console **Explorer**, right-click any application or area and then select **Resource Editor**.
2. In the **Areas** list, select the area containing the resource to copy.
3. In the **Associated resources** list, right-click the resource, and then select **Cut**.
4. In the **Areas** list, select the area to copy the resource to, right-click the **Associated resources** list again, and then select **Paste**.
5. When finished, select **Close**.

### See also

[Group hardware resources in an application or area](#) on [page 130](#)

[Remove a device from a resource grouping](#) on [page 131](#)

[Resource groupings](#) on [page 129](#)

## Remove a device from a resource grouping

Remove a device from a resource grouping to break the link between its security permissions and those of the application or area to which it belongs.

When a device is removed from a resource grouping, the security permissions for the device revert to what they were for either the logical name of the device — if the device is associated with a logical name — or for the network relative path of the device. The changes take effect immediately when applied.

### Prerequisites

Removing a device from a resource group requires these permissions for the application or area:

- Common > Configure Security
- Common > List Children
- Common > Read

### To remove a device from a resource grouping

1. In FactoryTalk Administration Console **Explorer**, right-click the application or area containing the resource grouping, and select **Resource Editor**.
2. In the **Areas** list of the **Resources Editor**, select the area or application containing the resource to delete.
3. In the **Associated resources** list, right-click the resource, and then select **Cut**.
4. When finished, select **Close**.

### See also

[Resource groupings](#) on [page 129](#)

## Resources Editor

How do I open Resources Editor?

1. Start FactoryTalk Administration Console or FactoryTalk View Studio and then log on to the FactoryTalk Network Directory or FactoryTalk Local Directory where the resource groupings to modify are located.
2. In the **Explorer** window, right-click any application or area and select **Resource Editor** on the context menu.

Use **Resources Editor** to edit a resource grouping in an area or application. Select **Manage Resources** to add or remove resources, or to map resources to logical names.

Setting	Description
Areas	Displays the applications and areas in the FactoryTalk network directory, or the applications in the FactoryTalk local directory. Select an area or application to view the list of resources associated with it.

Associated resources	Shows the hardware devices located in the application or area. Devices that are represented by logical names are displayed using their logical names. Devices that are represented by network relative paths are shown by their network relative paths. <ul style="list-style-type: none"> <li>• <b>To remove a resource</b>, right-click the resource and then select <b>Cut</b>. When removing a device from a resource grouping, the security permissions for the device revert to what they were for either logical name of the device, if the device is associated with a logical name, or for the network relative path of the device. Select <b>OK</b> and the changes take effect immediately.</li> <li>• <b>To move a resource from one area to another</b>, in the <b>Areas</b> list, select the area containing the resource to copy. In the <b>Associated resources</b> list, right-click the resource, and select <b>Cut</b>. In the <b>Areas</b> list, select the area to copy the resource to. Right-click the <b>Associated resources</b> list again, and select <b>Paste</b>.</li> </ul>
Manage Resources	Select <b>Manage Resources</b> to add or remove resources in the selected application or area, or to map resources to logical names.

## See also

[Group hardware resources in an application or area](#) on [page 130](#)

[Remove a device from a resource grouping](#) on [page 131](#)

## Select Resources

Use **Select Resources** to associate resources with an application or area. Referenced the hardware devices by logical name or by network relative path. Use these settings to specify how resources are added to the grouping.

Setting	Description
Select resources to be associated with an area	<ul style="list-style-type: none"> <li>• To view the logical names for only those devices that are not already associated with an application or area, select <b>Show only logical names not associated with areas</b>. Ignore this setting if not using logical names with networks and devices.</li> <li>• To view all logical names, even those already associated with an application or area, select <b>Show all logical names</b>. Ignore this setting if not using logical names with networks and devices.</li> <li>• To add a logical name to the list of resources in the grouping, select the logical name and select <b>&gt;</b>. The same network or device (represented by a logical name) cannot be added to multiple resource groupings.</li> <li>• To add a device using its network relative path, expand the <b>Networks and Devices</b> tree until the device is visible. Select the device and select <b>&gt;</b>. The same network or device cannot be added to multiple resource groupings.</li> </ul>
Add New Logical Name	Select to create a new logical name for a device.
Delete Logical Name	Delete logical names that are no longer in use in the system, but remain visible in this dialog box. This occurs if the device associated with a logical name was deleted. <b>Delete Logical Name</b> is disabled if the selected logical name is in use.
Selected resources	Shows the resources that are associated with the application or area. To remove a resource from the list, select the resource and select <b>&lt;</b> .

## See also

[Group hardware resources in an application or area](#) on [page 130](#)

[Resource groupings](#) on [page 129](#)



## Secure resources

### Secure resources

To secure the resources in the FactoryTalk system, select the resource, and use **Allow** or **Deny** permissions to specify which users can perform what actions on that resource from what computers. This helps ensure that only authorized personnel can perform approved actions from appropriate locations.

Common actions include the ability to see the resource, to edit or delete it, and to add additional items to the resource. Additional securable actions might appear, depending on which FactoryTalk products installed.

Set security permissions for:

- FactoryTalk local or network directory
- Applications
- Areas
- System folder
- Action groups
- Policies
- Computers and Computer Groups
- Users and User Groups
- Connections, including databases
- Networks and devices

Security for networks and devices follows special rules for inheriting security permissions, and includes the use of logical names, permission sets, and resource groupings. For this reason, security for networks and devices is covered in its own section.

### See also

[Permissions](#) on [page 135](#)

[Set FactoryTalk Directory permissions](#) on [page 144](#)

[View effective permissions](#) on [page 154](#)

[Actions](#) on [page 140](#)

Secure networks and devices

### Permissions

Permissions determine which **users** can perform which **actions** on specific **resources** in the system from which **computers**.

## Allow and Deny permissions

Set two kinds of permissions on resources:

- **Allow** permissions grant users permission to perform actions on resources from all computers or from only certain computers on a network. For example, in a FactoryTalk network directory, for a resource such as an area containing various servers, assign **Allow** permission to a **Read** action for a group of users named Designers from All Computers. This allows members of the Designers group to view the contents of the area from any computer on the network.
- **Deny** permissions prevent users from performing actions on resources from all computers or from only certain computers on a network. In a FactoryTalk local directory, security permissions apply to only the local computer. In a network directory, for an area containing various servers, assign **Deny** permissions to a **Write** action for a group of users named Designers from All Computers to prevent members of the Designers group from modifying the contents of the area.

Remove all permissions from an object by clearing both **Allow** and **Deny**. This allows the object to inherit permissions assigned at a higher level. For example, remove all permissions from an area located in an application, the area then inherits permissions from the application.

If no permissions are assigned to a resource at any level, Deny is implied.

**Product policies** do not inherit security settings. When specifying permissions for product policies, clearing both **Allow** and **Deny** does not allow the policy setting to inherit security. Instead, clearing both denies access to the product feature.

## Inherited and explicit permissions

By default, resources inherit permissions automatically from their parent resources. For example, if assigning security to an area in an application, all of the items in the area inherit the security settings of the area, and the area inherits security settings from the application. The top of the hierarchy is the network directory or local directory.

Networks and devices that are referenced by logical names, rather than by network relative paths, inherit permissions differently than other resources.

Override inherited permissions two ways:

- **Set up explicit permissions** for resources at a lower level of the hierarchy. For example, if an area inherits permissions from an application, override the inherited permissions by specifying permissions explicitly for the area.



Explicit permissions are permissions assigned deliberately to the resource, for users, groups, or computers, and actions. Explicit permissions take precedence over inherited permissions.

- **Break the chain of inheritance** at a level in the Network Directory or Local Directory tree. For example, stop an area from inheriting permissions from the application in which it is located by selecting **Do not inherit permissions** when setting up security for the area. When breaking the chain of inheritance, specify whether to remove all permissions from resources below the break (which then implies Deny permission), or whether to use the permissions that are inherited by the resource at the break as explicit permissions.

The principle of inheritance allows setting permissions at as high a level as is practical, and then introducing exceptions at lower levels where necessary. If permissions are not assigned at any level, Deny is implied. When the system evaluates the level of access provided to a user, computer, or group, Deny permissions are evaluated before Allow permissions, explicit permissions override inherited permissions, and where conflicting permissions exist, Deny takes precedence over Allow.

## Categories of permissions for actions

The actions that users can perform on resources are grouped into categories. The Common category is common to all FactoryTalk products. Create action groups to assign security permissions to all of the actions in the group in one step, rather than assigning permissions to each action separately.

## Effective permissions

To find out what actions a user or group can perform on a resource, view the permissions in effect (effective permissions) for the resource. The effective permissions are shown in the **Effective Permissions** tab of the **Security Settings** for the resource.

**Effective Permissions** shows the permissions that are granted to the selected user, computer, or group. When calculating effective permissions, the system takes into account the permissions in effect from group membership, as well as any permissions inherited from the parent object.

If a check mark appears for an action, permission is allowed, whether explicitly or by inheritance. If a check mark does not appear, permission is denied, whether explicitly or by inheritance. If a category (for example, Common) shows a gray check mark, one or more – but not all – of the actions inside the category is allowed. Expand the category to see which permissions within it are allowed or denied.

## See also

[Breaking the chain of inheritance](#) on [page 138](#)

[Order of precedence](#) on [page 139](#)

[Secure resources](#) on [page 135](#)

[View effective permissions](#) on [page 154](#)

## Breaking the chain of inheritance

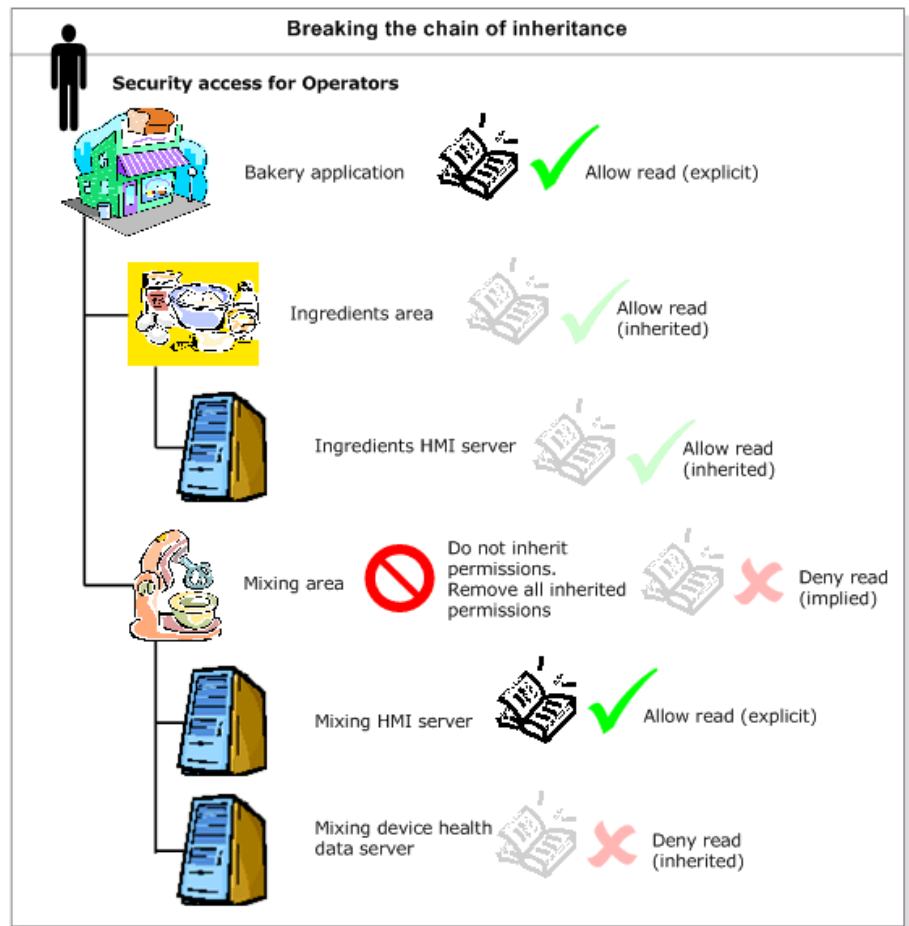
By default, resources inherit permissions automatically from their parent resources. For example, if assigning security to an area in an application, all of the items in the area inherit the security settings of the area, and the area inherits security settings from the application. The top of the hierarchy is the network directory or local directory.

Override inherited permissions in two ways:

- **Set up explicit permissions** for resources at a lower level of the hierarchy. For example, if an area inherits permissions from an application, override the inherited permissions by specifying permissions explicitly for the area.
- **Break the chain of inheritance** at a level in the network directory or local directory tree. For example, stop an area from inheriting permissions from the application in which it is located by selecting **Do not inherit permissions** when setting up security for the area. When breaking the chain of inheritance, specify whether to remove all permissions from resources below the break (which then implies **Deny** permission), or whether to use the permissions that are inherited by the resource at the break as explicit permissions.

Permissions are inherited only as far up the network directory or local directory tree as the chain of inheritance remains intact. For example, when **Do not inherit permissions** for an area is selected, items that inherit permissions inside the area can inherit permissions only as far as the area. They cannot inherit permissions from the application in which the area is

located. Because breaking the chain of inheritance complicates administration, only do this when absolutely necessary.



The principle of inheritance allows setting permissions at as high a level as is practical. Then, introduce exceptions at lower levels where necessary.

If permissions are not assigned at any level, **Deny** is implied.

### See also

[Permissions](#) on [page 135](#)

[Order of precedence](#) on [page 139](#)

[Secure resources](#) on [page 135](#)

## Order of precedence

When the system evaluates the level of access a user, computer, or group has, these rules apply:

- **Deny permissions are implied.** If no permissions are assigned to a resource, **Deny** is implied. Use implied **Deny** permissions rather than explicit **Deny** permissions wherever possible, because this simplifies administration.

- **Deny permissions are evaluated before Allow permissions.** For example, if the *Operators* group is explicitly denied access to a data server, but an individual user account in the group (*Jane*) is explicitly allowed access, the **Deny** rule for the group account takes precedence over the **Allow** rule for the individual account, and *Jane* cannot access the data server as long as she is a member of the *Operators* group.
- **Explicit permissions override inherited permissions.** For example, assume your application has an area named *Baking*, and *Operators* are allowed **Read** access to the area. If a rule is applied to the *Operators* group that specifically denies *Read* access to an HMI server in the *Baking* area, the **Deny** permission takes precedence over the **Allow** permission.

This means that an explicit **Allow** permission overrides an inherited **Deny** permission, and an explicit **Deny** permission overrides an inherited **Allow** permission.

- **If conflicting explicit permissions are set at the same level, Deny takes precedence over Allow.** For example, the *Operators* are explicitly denied group access to a data server, but an individual user account (*Jane*) is explicitly allowed access to the data server. **Deny** takes precedence over **Allow**, and *Jane* cannot access the data server if she is a member of the *Operators* group. This happens because conflicting explicit permissions are set on the same resource. To allow *Jane* access to the data server, deny the *Operators* group access to the resource at a higher level in the hierarchy (for example, the area in which the data server is located), and then explicitly allow exceptions for the data server.

### See also

[Breaking the chain of inheritance](#) on [page 138](#)

[Permissions](#) on [page 135](#)

[Secure resources](#) on [page 135](#)

## Actions

When setting up security, specify which actions a user or group can perform on a selected resource. In a FactoryTalk network directory, specify from which computer or group of computers a user can perform the action.

A group of common actions are installed by default with the FactoryTalk Services Platform. However, different sets of actions apply to different resources in the directory. Additional securable actions might appear, depending on which FactoryTalk products are installed. For details about using those actions, see the documentation for your FactoryTalk products.

## Read

Controls whether a user or group can see the resource in the **Explorer** from a computer or group of computers.

Resource type	Result of Denying "Read"
Network directory or local directory	Prevents users from seeing the directory or its contents.
Application	Prevents users from seeing the application or its contents. Denying <b>Read</b> does not prevent users from reading tag values from data servers in the application.
Area	Prevents users from seeing the area or its contents. Denying <b>Read</b> does not prevent users from reading tag values from data servers in the area.
System folder	Prevents users from seeing the <b>System</b> folder or its contents. Denying <b>Read</b> does not prevent users from reading tag values for devices in the Networks and Devices tree.
Networks and Devices tree	Prevents users from seeing the Networks and Devices tree and its contents. Denying <b>Read</b> does not prevent users from reading tag values for a particular device.
Individual network or device in the Networks and Devices tree	Prevents users from seeing the network or device and its contents. Denying <b>Read</b> does not prevent users from reading tag values for a particular device.

## Write

Controls whether a user or group can write to the resource from a computer or group of computers.

Resource type	Result of Denying "Write"
Network directory or local directory	Prevents users from modifying the properties of any item in the directory. For example, denying <b>Write</b> prevents users from modifying the description of an application, area, or the properties of a data server. However, if <b>Create Children</b> is allowed, the user or group can create applications in the directory, add areas to an application, and add data servers to areas.
Application	Prevents users from modifying the properties of any item in the application. For example, denying <b>Write</b> prevents users from modifying the description of the application, the descriptions of areas within the application, or the properties of data servers within the application or its areas. However, if <b>Create Children</b> is allowed, the user or group can add areas or data servers to an application, and can add data servers to areas.
Area	Prevents users from modifying the properties of any item in the area. For example, denying <b>Write</b> prevents users from modifying the description of the area, or the properties of data servers within the area. However, if <b>Create Children</b> is allowed, the user or group can add areas or data servers within the area.
System folder	Prevents users from modifying the properties of any item in the System folder. For example, denying <b>Write</b> prevents users from modifying policy settings, and the properties of user accounts, such as an account's description or group memberships. Denying <b>Write</b> also prevents deleting user and group accounts, if the accounts have group memberships associated with them. This is because the group memberships are updated automatically when an account is deleted, and updating group memberships is controlled by the <b>Write</b> action.
Networks and Devices tree	Prevents users from defining, modifying, or removing logical names for networks or devices. Denying <b>Write</b> does not prevent users from writing tag values to devices.
Individual network or device in the Networks and Devices tree	Prevents users from defining, modifying, or removing logical names for the network or device. Denying <b>Write</b> does not prevent users from writing tag values to devices.

## Configure Security

Controls whether a user or group can change the security permissions for the resource, while working from a computer or group of computers, by using FactoryTalk Administration Console and selecting **Security** for the resource.

Denying **Configure Security** has the same effect on all types of securable resources. For example, if a user is denied **Configure Security** for an area, the user cannot change the security settings of the area, such as allowing or denying users permission to perform actions in the area, while working from the specified computer or group of computers.

Similarly, denying **Configure Security** on the **Users and Groups** folder prevents users from setting security permissions for the **Users and Groups** folder. Denying **Configure Security** on the **Users and Groups** folder **does not** limit the access users have to resources in the system.

## Create Children

Controls whether a user or group can create a new, related resource beneath an existing resource in the FactoryTalk Administration Console directory tree while working from a computer or group of computers.

Resource type	Result of Denying "Create Children"
Network directory or local directory	Prevents users from creating applications or areas.
Application	Prevents users from creating areas or data servers in the application.
Area	Prevents users from seeing the area or its contents. Denying <b>Read</b> does not prevent users from reading tag values from data servers in the area.
System folder	Prevents users from creating user, computer, or group accounts. Denying <b>Create Children</b> has no effect on policies.
Networks and Devices tree	<b>Create Children</b> is not available because users cannot add items to the Networks and Devices tree. Networks and Devices is populated automatically, based on the networks and devices that are available to your local computer.
Individual network or device in the Networks and Devices tree	<b>Create Children</b> is not available because users cannot add items to the Networks and Devices tree. Networks and Devices is populated automatically, based on the networks and devices that are available to your local computer.

## List Children

Controls whether a user or group can list the children of the resource from a computer or group of computers.

Denying **List Children** has the same effect on all types of securable resources. For example, if **List Children** access is denied to an application, the user or group can see the application, but not its contents while working from the specified computer or group of computers.

Unlike the **Read** action, **List Children** does allow the user to see the resource that contains other resources, for example, the application that contains areas or data servers.

## Execute

Controls whether a user or group can perform an executable action from a computer or group of computers. The **Execute** action is used primarily for **Product Policy Feature Security** settings.

Instead of using the **Execute** action, each FactoryTalk product can use its own actions to secure its executable features. For details about what, if anything, the **Execute** action does in a particular FactoryTalk product, see the documentation for that product.

## Delete

Resource type	Result of Denying "Delete"
Network directory or local directory	Prevents users from deleting any item in the directory, for example, applications, areas, data servers, or user accounts.
Application	Prevents users from deleting the application, or any item within it, for example, areas, or data servers.
Area	Prevents users from deleting the area, or any item within it, for example, data servers within the area.
System folder	Prevents users from deleting any item in the System folder, for example, user, computer, or group accounts. If a user, computer, or group account has group memberships associated with it, deleting the account also requires <b>Write</b> permission, because updating the group memberships of accounts is controlled by the <b>Write</b> action.
Networks and Devices tree	The <b>Delete</b> action is not available because users cannot remove items from the Networks and Devices tree. Networks and Devices is populated automatically, based on the networks and devices that are available to your local computer.
Individual network or device in the Networks and Devices tree	The <b>Delete</b> action is not available because users cannot remove items from the Networks and Devices tree. Networks and Devices is populated automatically, based on the networks and devices that are available to your local computer.

## Tag actions: Write Value

Controls whether a user or group can write to tags in data servers from a computer or group of computers. Configure this action on the network directory or local directory, an application, or an area.

The **Write Value** action does not prevent users from writing values to tags in specific hardware devices. **Write Value** prevents writing values to all of the tags managed by a data server.

If additional FactoryTalk products are installed, they might install additional Tag actions. For details about these actions, see Help for your FactoryTalk products.

## User Action Groups

This category contains the added action groups. If no action groups were added, this category does not appear.

### See also

[Things you can secure](#) on [page 32](#)

[Account types](#) on [page 18](#)

[Differences between securable actions and product policies](#) on [page 116](#)

[Effective permission icons](#) on [page 156](#)

[Secure features of a single product](#) on [page 114](#)

## Set FactoryTalk Directory permissions

Set permissions on your FactoryTalk Directory folder to control whether a user or group can:

- See the directory or its contents (**Read**)
- Modify the properties of any item in the directory (**Write**)
- Add applications, areas, and data servers to the directory (**Create Children**)
- Change the security settings of the directory (**Configure Security**)
- View child folders within the directory (**List Children**)
- Write tags in data servers (**Write Value**)
- Perform other product-specific actions
- Perform actions defined in user action groups



Tip:

- Denying **Write** prevents users from modifying the properties of any item in the directory. However, if **Create Children** is allowed, the user or group can add items to the directory.
- The **Write Value** action does not prevent users from writing values to tags in specific hardware devices.

## Prerequisites

Setting FactoryTalk Directory permissions requires these permissions:

- Common > Read
- Common > Configure Security

## To set FactoryTalk Directory permissions

1. In FactoryTalk Administration Console **Explorer**, right-click the FactoryTalk network or local directory, and select **Security**.
2. In **Security Settings for [Local or Network]**, in the **Permissions** tab, either:



- Set permissions by user:
    - Select **User**.
    - In **Users and Computers**, select a user and computer.
    - In **Action**, expand the category that contains the action to secure, and select the action.
  - Set permissions by action:
    - Select **Action**.
    - In **Action**, expand the category that contains the action to secure, and select the action. If the list of actions is blank, add users and computers first.
    - In **Users and Computers**, select a user and computer.
3. Select **Allow** or **Deny**.
  4. (optional) To control access to the action by another user or group, select **Add** and select the user or group, and computer or group, and select **OK**.
  5. When finished configuring security for the FactoryTalk Directory, select **OK**.

### See also

Security Settings-Permissions

Security Settings-Effective Permissions

Security Settings-Inherit Permissions

[Actions](#) on [page 140](#)

[Secure resources](#) on [page 135](#)

## Set application permissions

Set permissions on the application to control whether a user-computer pair can:

- See the application or its contents (**Read**)
- Modify the properties of any item in the application (**Write**)
- Add areas or data servers to the application (**Create Children**)
- Change the security settings of the application (**Configure Security**)
- View the contents of the application (**List Children**)
- Delete the application or any item within it (**Delete**)
- Write tags in data servers (**Write Value**)
- Perform other product-specific actions
- Perform actions defined in user action groups

If a resource grouping is associated with the application, the networks or devices in the resource grouping inherit the security permissions of the application.



Tip:

- Denying **Read** does not prevent users from reading tag values from data servers in the application.
- Denying **Write** prevents users from modifying the properties of any item in the application. However, if **Create Children** is allowed, users can add areas or data servers to an application.
- The **Write Value** action does not prevent users from writing values to tags in specific hardware devices.

## Prerequisites

Setting application permissions requires these security permissions:

- Common > Read
- Common > Configure Security

## To set application permissions

1. In FactoryTalk Administration Console **Explorer**, right-click the application to secure, then select **Security**.
2. In **Security Settings**, in the **Permissions** tab, either:
  - Set permissions by user:
    - Select **User**.
    - In **Users and Computers**, select a user and computer.
    - In **Action**, expand the category that contains the action to secure, and select the action.
  - Set permissions by action:
    - Select **Action**.
    - In **Action**, expand the category that contains the action to secure, and select the action. If the list of actions is blank, add users and computers first.
    - In **Users and Computers**, select a user and computer.
3. Select **Allow** or **Deny**, or clear both. Clear both **Allow** and **Deny** to make the application inherit its security settings from the FactoryTalk Directory folder.
4. (optional) To control access to the action by another user or group, select **Add**, and in **Select User and Computer**, select the user or group, and computer or group to add, and select **OK**.
5. When finished configuring security for the application, select **OK**.

## See also

[View effective permissions](#) on [page 154](#)

[Add a user-computer pair](#) on [page 63](#)

[Secure resources](#) on [page 135](#)

[Actions](#) on [page 140](#)

## Set area permissions

Set permissions on an area in order to control whether a user-computer pair can:

- See the area or its contents (**Read**)
- Modify the properties of any item in the area (**Write**)
- Add areas or data servers to the area (**Create Children**)
- Change the security settings of the area (**Configure Security**)
- View the contents of the area (**List Children**)
- Delete the area or any item within it (**Delete**)
- Write tags in data servers (**Write Value**)
- Perform other product-specific actions
- Perform actions defined in user action groups

For example, set **Read** and **Write** permissions to the Ingredients area within an application to allow the operators of the Ingredients machinery to read and write values to and from controllers in their own area, but only when using computers located within sight of the equipment.

If a resource grouping is associated with the area, the networks or devices in the resource grouping inherit the security permissions of the area.



Tip:

- Denying **Read** does not prevent users from reading tag values from data servers in the area.
- Denying **Write** prevents users from modifying the properties of any item in the area. However, if **Create Children** is allowed, users can add areas or data servers within the area.
- The **Write Value** action does not prevent users from writing values to tags in specific hardware devices.

## Prerequisites

Setting area permissions requires these security permissions:

- Common > Read
- Common > Configure Security

## To set area permissions

1. In FactoryTalk Administration Console **Explorer**, expand the application, right-click the area to secure, and select **Security**.
2. In **Security Settings**, in the **Permissions** tab, either:
  - Set permissions by user:
    - Select **User**.
    - In **Users and Computers**, select a user and computer.
    - In **Action**, expand the category that contains the action to secure, and select the action.

- Set permissions by action:
  - Select **Action**.
  - In **Action**, expand the category that contains the action to secure, and select the action. If the list of actions is blank, add users and computers first.
  - In **Users and Computers**, select a user and computer.
- 3. Select **Allow** or **Deny**, or clear both. Clear both **Allow** and **Deny** to make the area inherit its security settings from a resource higher in the FactoryTalk Directory tree.
- 4. (optional) To control access to the action by another user or group, select **Add**. In **Select User and Computer**, select the user or group, and computer or group to add, and select **OK**.
- 5. When finished configuring security for the area, select **OK**.

### See also

[View effective permissions](#) on [page 154](#)

[Add a user-computer pair](#) on [page 63](#)

[Actions](#) on [page 140](#)

[Secure resources](#) on [page 135](#)

## Set System folder permissions

Set permissions on the **System** folder to control whether a user-computer pair can:

- See the System folder or its contents (**Read**)
- Modify the properties of any item in the System folder (**Write**)
- Add user, user group, computer, or computer group accounts (**Create Children**)
- Change the security settings of the System folder (**Configure Security**)
- View the contents of the System folder (**List Children**)
- Delete the System folder or any item within it (**Delete**)
- Write tags in data servers (**Write Value**)
- Perform other product-specific actions
- Perform actions defined in user action groups



Tip:

- Denying **Read** does not prevent users from reading tag values for devices in the **Networks and Devices** tree.
- Denying **Write** prevents users from modifying the properties of any item in the **System** folder. Denying **Write** also prevents deleting user and group accounts, if the accounts have group memberships associated with them.
- Denying **Create Children** has no effect on policies.
- If a user, computer, or group account has group memberships associated with it, deleting the account also requires **Write** permission, because updating the group memberships of accounts is controlled by the Write action.
- The **Write Value** action does not prevent users from writing values to tags in specific hardware devices.

## Prerequisites

Obtain the following security permissions for the **System** folder:

- Common > Read
- Common > Configure Security

## To set System folder permissions

1. In FactoryTalk Administration Console **Explorer**, right-click the **System** folder or the subfolder to secure, and select **Security**.
2. In **Security Settings**, in the **Permissions** tab, either:
  - Set permissions by user:
    - Select **User**.
    - In **Users and Computers**, select a user and computer.
    - In **Action**, expand the category that contains the action to secure, and select the action.
  - Set permissions by action:
    - Select **Action**.
    - In **Action**, expand the category that contains the action to secure, and select the action. If the list of actions is blank, add users and computers first.
    - In **Users and Computers**, select a user and computer.
3. Select **Allow** or **Deny**, or clear both. Clear both **Allow** and **Deny** to make the **System** folder inherit its security settings from the FactoryTalk Directory folder.
4. (optional) To control access to the action by another user or group, select **Add**, and in **Select User and Computer**, select the user or group, and computer or group to add, and select **OK**.
5. When finished configuring security for the **System** folder, select **OK**.

## See also

[View effective permissions](#) on [page 154](#)

[Add a user-computer pair](#) on [page 63](#)

[Actions](#) on [page 140](#)

[Secure resources](#) on [page 135](#)

## Set action group permissions

Set permissions on an action group to control whether a user-computer pair can:

- See the action group (**Read**)
- Modify the properties of the action group (**Write**)
- Change the security settings of the action group (**Configure Security**)

- Delete the action group (**Delete**)
- Perform actions defined in another user action group

## Prerequisites

Setting action group permissions requires these security permissions:

- Common > Read
- Common > Configure Security

## To set action group permissions

1. In FactoryTalk Administration Console **Explorer**, expand the network directory tree, the **System** folder, and the **Action Groups** folder, right-click the action group to secure, and select **Security**.
2. In **Security Settings**, in the **Permissions** tab, either:
  - Set permissions by user:
    - Select **User**.
    - In the **Users and Computers** list, select a user and computer.
    - In the **Action** list, expand the category that contains the action to secure, and select the action.
  - Set permissions by action:
    - Select **Action**.
    - In **Action**, expand the category that contains the action to secure, and select the action. If the list of actions is blank, add users and computers first.
    - In **Users and Computers**, select a user and computer.
3. Select **Allow** or **Deny**, or clear both. Clear both **Allow** and **Deny** to make **Action Groups** or the individual action group inherit its security settings from a resource higher in the directory tree.
4. (optional) To control access to the selected action by another user or group, Select **Add**. In **Select User and Computer**, select the user or group, and computer or group to add, and select **OK**.
5. When finished configuring security for the action group, select **OK**.

## See also

[View effective permissions](#) on [page 154](#)

[Add a user-computer pair](#) on [page 63](#)

[Add and remove action groups](#) on [page 67](#)

[Actions](#) on [page 140](#)

[Secure resources](#) on [page 135](#)

## Set database permissions

Set permissions on a database to specify which user-computer pairs can:

- See the database
- Modify the properties of the database (**Write**)
- Change the security settings of the database (**Configure Security**)
- Delete the database within it (**Delete**)
- Perform actions defined in a user action group

## Prerequisites

Setting database permissions requires these security permissions:

- Common > Read
- Common > Configure Security

## To set database permissions

1. In FactoryTalk Administration Console **Explorer**, expand **System > Connections > Databases**, right-click the database, and select **Security**.
2. In **Security Settings**, in the **Permissions** tab, either:
  - Set permissions by user:
    - Select **User**.
    - In **Users and Computers**, select a user and computer.
    - In **Action**, expand the category that contains the action to secure, and select the action.
  - Set permissions by action:
    - Select **Action**.
    - In **Action**, expand the category that contains the action to secure, and select the action. If the list of actions is blank, add users and computers first.
    - In **Users and Computers**, select a user and computer.
3. Select **Allow** or **Deny**, or clear both. Clear both **Allow** and **Deny** to make the folder inherit its security settings from a resource higher in the directory tree.
4. (optional) To control access to the folder by another user or group, select **Add**, and **Select User and Computer**, select the user or group, and computer or group to add, and select **OK**.
5. When finished configuring security for the database, select **OK**.

## See also

[View effective permissions](#) on [page 154](#)

[Add a user-computer pair](#) on [page 63](#)

[Actions](#) on [page 140](#)

[Secure resources](#) on [page 135](#)

## Set logical name permissions

Set permissions on the logical name to control whether a user-computer pair can:

- See the logical name (**Read**)
- Modify the properties of the logical name (**Write**)
- Change the security settings of the logical name (**Configure Security**)
- Delete the logical name (**Delete**)
- Perform actions defined in a user action group

## Prerequisites

Setting logical name permissions requires these security permissions:

- Common > Read
- Common > Configure Security

## To set logical name permissions

1. In FactoryTalk Administration Console **Explorer**, expand **System** > **Logical Names**, right-click the logical name, and select **Security**.
2. In **Security Settings**, in the **Permissions** tab, either:
  - Set permissions by user:
    - Select **User**.
    - In **Users and Computers**, select a user and computer.
    - In **Action**, expand the category that contains the action to secure, and select the action.
  - Set permissions by action:
    - Select **Action**.
    - In **Action**, expand the category that contains the action to secure, and select the action. If the list of actions is blank, add users and computers first.
    - In **Users and Computers**, select a user and computer.
3. Select **Allow** or **Deny**, or clear both. Clear both **Allow** and **Deny** to make **Action Groups** or the individual action group inherit its security settings from a resource higher in the directory tree.



4. (optional) To control access to the selected action by another user or group, select **Add**, and in **Select User and Computer**, select the user or group, and computer or group to add, and select **OK**.
5. When finished configuring security for the logical name, select **OK**.

## See also

[Secure resources](#) on [page 135](#)

## Allow a resource to inherit permissions

Permissions determine which users can perform which actions on specific resources in the system from which computers. Set **Allow** and **Deny** permissions on resources.

Allow a resource to inherit permissions when the selected resource has the same permissions as its parent resource. For example, if assigning security to an area in an application, all of the items in the area inherit the security settings of the area. By default, the area inherits security settings from the application. The top of the hierarchy is the network directory or local directory.

## To allow a resource to inherit permissions

1. In FactoryTalk Administration Console **Explorer**, right-click the resource, then select **Security**.
2. In **Security Settings**, on the **Permissions** tab, clear **Do not inherit permissions**.
3. To remove explicit permissions, clear the black check mark next to **Allow** or **Deny**. Inherited permissions appear as gray check marks and cannot be removed. However, explicit permissions supersede inherited permissions.
4. Select **OK**.



Tip: Security settings configured for resources apply to all FactoryTalk products in the system in the current FactoryTalk directory. For example, if a user and computer are denied **Read** access to an area, that user and computer cannot see the area in any of the FactoryTalk products in the system.

## See also

[Prevent a resource from inheriting permissions](#) on [page 154](#)

[Secure resources](#) on [page 135](#)

[Effective permission icons](#) on [page 156](#)

[Permissions](#) on [page 135](#)

## Prevent a resource from inheriting permissions

When the chain of inheritance is broken, the resource no longer inherits permissions from its parent resources. For example, when setting up security for an area, selecting **Do not inherit permissions** stops the area from inheriting permission from the application in which it is located

### To prevent a resource from inheriting permissions

1. In FactoryTalk Administration Console **Explorer**, right-click the resource, then select **Security**.
2. In **Security Settings**, on the **Permissions** tab, select **Do not inherit permissions**.
3. Do one and select **OK**:
  - To use the inherited permissions that were formerly applied to the resource as explicit permissions, select **Copy the current permissions from the parent object to this object**. Modify this permissions set as needed. Changes made to the parent object permissions are not applied to this resource after the chain of inheritance is broken.
  - To remove all inherited permissions from the resource, select **Remove all inherited permissions from this object**. Grant explicit permissions to the resource as needed.

When removing all inherited permissions, **Read** and **Configure Security** permissions are automatically granted to the **Administrators** group. Always grant the **Administrators** group both of these permissions.



Tip: Security settings configured for resources apply to all FactoryTalk products in the system in the current FactoryTalk directory. For example, when denying a user and computer **Read** access to an area, that user and computer cannot see the area in any of the FactoryTalk products in the system.

### See also

[Allow a resource to inherit permissions](#) on [page 153](#)

[Secure resources](#) on [page 135](#)

[Effective permission icons](#) on [page 156](#)

[Permissions](#) on [page 135](#)

## View effective permissions

To determine what permissions are currently in effect for a resource, use the **Effective Permissions** tab in **Security Settings**. View the permissions in effect for:

- a user or group of users, and
- a computer or group of computers

For example, in **Security Settings** for an area, the **Effective Permissions** tab can show whether the selected users and computers can read the contents of the area.

To view the permissions in effect for a computer or group of computers, use a FactoryTalk network directory, because a FactoryTalk local directory is restricted to a single computer.

## Prerequisites

Viewing effective permissions requires these security permissions for the resource (for example, an application) or the container (for example, an area) the resource is located in:

- Common > Read
- Common > Configure Security

## To view effective permissions

1. In FactoryTalk Administration Console **Explorer**, expand the FactoryTalk network or local directory tree until the resource is visible.
2. Right-click the resource, and select **Security**.
3. In **Security Settings**, select the **Effective Permissions** tab.
4. To test the permissions for a user or user group, under **User or group**, select **Browse (...)** and browse for the user or user group.
5. To test the permissions for a computer or a computer group, under **Computer or computer group**, select **Browse (...)** and browse for the computer or computer group.
6. Select **Update Permissions List** to show the permissions currently in effect for the selected users and computers.

The Effective permissions list does not show separate columns for **Allow** and **Deny** permissions, and does not distinguish between explicit and inherited permissions. Instead, the presence or absence of a check mark in the **Allowed** column indicates the permissions in effect on the resource for the selected user and computer, or group:

- If a check mark appears beside an action, the action is allowed, whether explicitly or by inheritance.
- If a check mark does not appear beside an action, the action is denied, whether explicitly or by inheritance.
- If an action category (for example, Common or Alarming) shows a gray check mark, one or more—but not all—of the actions inside the category are allowed. Expand the category to see which actions are allowed or denied.

## See also

[Permissions](#) on [page 135](#)

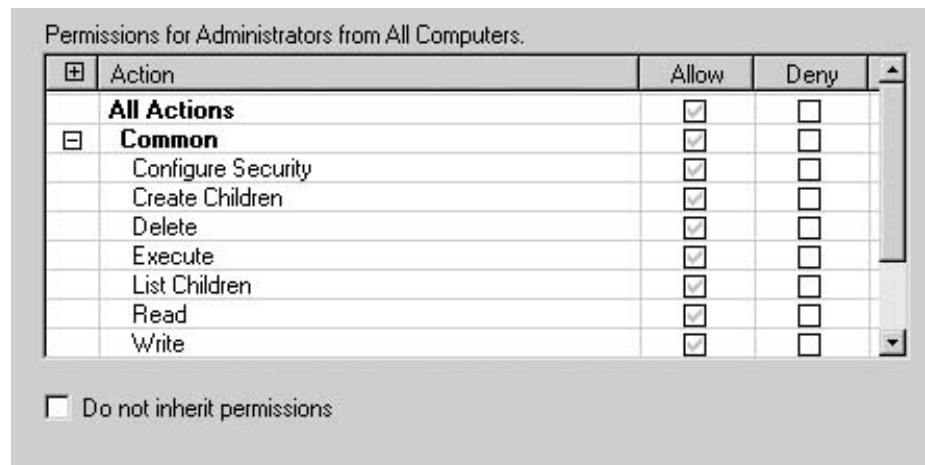
[Secure resources](#) on [page 135](#)

**Effective permission icons** **Security Settings** indicate which permissions are in effect for an action.

Icon	Description
<input type="checkbox"/>	Cleared box beside an action means that no permissions are assigned. If both <b>Allow</b> and <b>Deny</b> are cleared beside an action, <b>Deny</b> is implied for the action. A cleared option shown beside the name of a group of actions, for example, <b>All Actions</b> or <b>Common</b> , means that some of the actions within that group do not have permissions assigned. If collapsed, expand the group to see which actions do not have permissions assigned.
<input checked="" type="checkbox"/>	A black check mark means that <b>Allow</b> or <b>Deny</b> permissions were assigned explicitly.
<input checked="" type="checkbox"/>	A gray check mark means that <b>Allow</b> or <b>Deny</b> permissions were inherited.

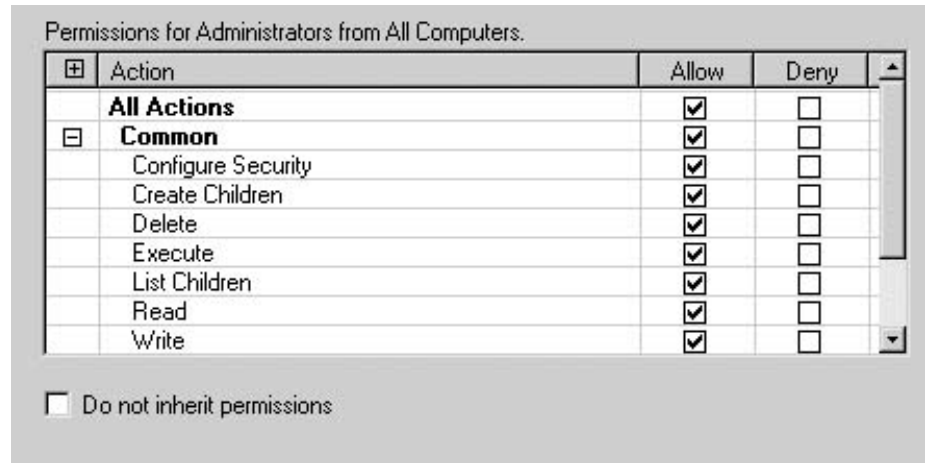
These examples show how the **Allow and Deny** columns indicate what permissions were set for the resource.

## Inherited permissions



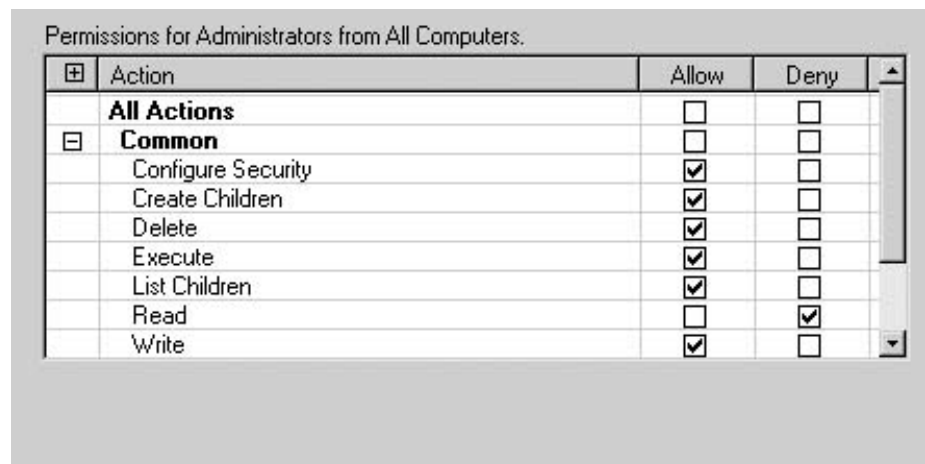
The gray check marks show that **Allow** permissions are inherited for all actions.

## Explicit permissions



If **Allow** is selected beside **All Actions**, black check marks appear. This means the inherited values are overridden and **Allow** on **All Actions** is explicitly granted. If the inherited permissions change later, the change does affect this security setting.

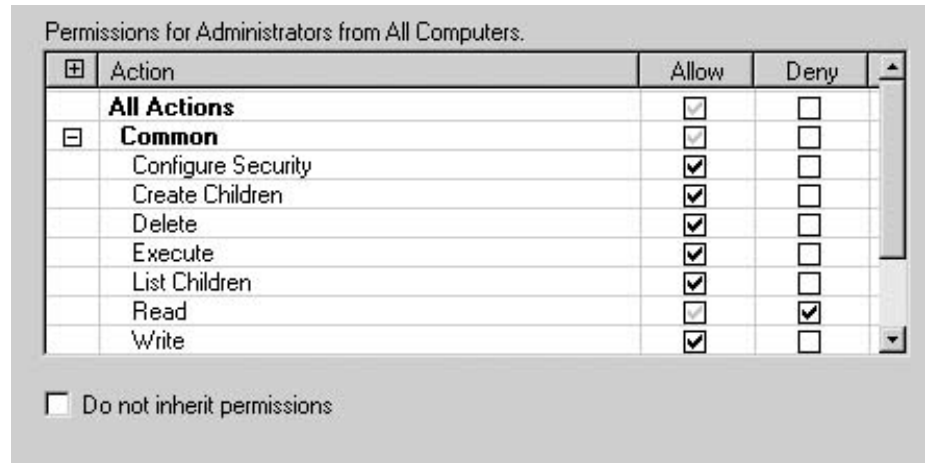
## Explicit Deny permissions without inheritance



In this example, the resource does not inherit permissions from its parent (this illustration shows configuring security for the FactoryTalk network directory, which has no parent). If all actions are set to **Allow**, and then **Deny** beside **Read** is selected:

- **All Actions** and **Common** are cleared. Because they represent groups of actions, the cleared options beside **All Actions** and **Common** mean that not all of the actions within those groups are selected in the **Allow** column. Expand the group to see which actions do not have **Allow** permissions.
- For the **Read** action, **Allow** is cleared.

## Explicit Deny permissions with inheritance



In this example, the resource inherits permissions from its parent (for example, an area might inherit permissions from an application). If all actions are set to **Allow**, and **Deny** beside **Read** is selected:

- **All Actions** and **Common** are cleared, but because these options previously inherited permissions, they now contain gray check marks. Expand the group to see which actions do not have **Allow** permissions.
- For the **Read** action, **Allow** is cleared, but because it previously inherited permissions, **Read** now contains a gray check mark. Because explicit permissions take precedence over inherited permissions, these selections indicate that **Read** access is denied.

### Using "Do not inherit permissions"

Select **Do not inherit permissions** to remove all inheritance from the resource. Set permissions for the resource as shown in the previous example.

### See also

[Allow a resource to inherit permissions](#) on [page 153](#)

[Prevent a resource from inheriting permissions](#) on [page 154](#)

[Secure resources](#) on [page 135](#)

## Disaster Recovery

### Back up a FactoryTalk system

Create FactoryTalk backup files to preserve and restore a FactoryTalk system in case of a systems failure. If a FactoryTalk Directory is inaccessible or corrupt, use the FactoryTalk Directory Configuration Wizard to repair it.

For safekeeping and disaster recovery, or to move a FactoryTalk system from one set of computers to another, backup and restore an archive containing one of the following:

- An entire FactoryTalk Directory with all of its applications and its System folder.
- Only an individual application, with or without the System folder. An application archive file typically contains areas (in a network directory), resource grouping information, and references to data servers, device servers, alarm servers, and HMI servers.
- Only a System folder. The System folder includes a list of user, computer, and group accounts, passwords, system policy settings, product policy settings, system security settings, action groups, and alarm and event database definitions.

The backup process creates an archive file that contains only objects and references to objects held within the FactoryTalk Directory. The archive file does not contain project files that are specific to individual products.

FactoryTalk Services Platform 6.10 applies a new encryption algorithm to the backup file for enhanced security. Backups created using FactoryTalk Services Platform 6.10 can only be restored to host computers that are also running FactoryTalk Services Platform 6.10 or later. Backups created using FactoryTalk Services Platform 2.90 or later can be restored onto host computers that are running FactoryTalk Services Platform 6.10.

---

**IMPORTANT** Take care to choose the correct backup options when creating a backup archive. Restoring from the wrong type of backup archive can overwrite existing data that affects all applications.

---

### See also

[Back up a FactoryTalk Directory](#) on [page 160](#)

[Back up an application](#) on [page 164](#)

[Back up a System folder](#) on [page 162](#)

[Backup and restore options](#) on [page 170](#)

## Back up a FactoryTalk Directory

Back up a FactoryTalk Directory to move a development FactoryTalk system to a run-time FactoryTalk system, or to create a backup for disaster recovery purposes.

When you back up an entire FactoryTalk Directory, the archive file includes:

- All objects, references to objects held within the FactoryTalk Directory, and the security authority identifier. The archive file does not contain project files that are specific to individual products.
- All applications associated with that directory. Typically an application contains areas (in a network directory), resource grouping information, and references to data servers, device servers, alarm servers, and HMI servers.
- The System folder, which includes a list of user, computer, and group accounts, passwords, system policy settings, product policy settings, system security settings, action groups, and alarm and event database definitions.



Tip: To back up a FactoryTalk Directory without its security authority identifier, or to back up only the security authority identifier, select **Tools > Security Authority Identifier**. In **Modify Security Authority Identifier**, select **Backup** and follow the on-screen instructions.

### Prerequisites

- Obtain the security permissions needed to perform backup and restore operations. Open **System > Policies > System Policies**, and open **User Rights Assignment**. Under **Backup and Restore > Backup and restore directory contents** select **Configure Security** and verify access permissions have been granted.

### To back up a FactoryTalk Directory

1. In FactoryTalk Administration Console **Explorer**, right-click the **Network** or **Local Directory** icon, then select **Backup**.
2. In **Specify archive name**, use the default name or type another name for the backup file.



Tip: It is recommended to not change the default archive name. The default name contains the leading digits of the security authority identifier which allows you to easily identify the archive file associated with a specific directory.

3. In **Specify archive location** use the default archive location or use **Browse** to open the **Browse for Folder** window and specify another location.
4. In **Backup Contents**:
  - Select **FactoryTalk Directory configuration** to back up the entire FactoryTalk Directory.



- (optional) Select **FactoryTalk Linx configuration** to back up shortcut and driver configurations.
5. To encrypt your archive file, select the **Encrypt file contents** check box, and then enter the same passphrase in the **Passphrase** and **Confirm passphrase** fields. If you clear this check box, your backup archive file will not be encrypted or protected.

**Encrypt file contents** is not available if your operating system does not support the proper level of encryption.

---

**IMPORTANT** Remember the passphrase when choosing to encrypt the file contents. The archive file cannot be restored without the correct passphrase.

---

6. Select **OK**.

Unless a different file name was specified, FactoryTalk Administration Console creates a directory backup file with its current security authority identifier in the default location or in the location specified. If a backup file with the same name already exists in the location selected, the system asks whether to overwrite the existing file.

7. After backing up a directory, perform backups of project files and databases from individual software products that are participating in the FactoryTalk system.

If the applications include:

- **HMI servers:** Back up FactoryTalk View files separately. See FactoryTalk View documentation for help.
- **RSLinx Classic data servers:** Run the RSLinx Backup Restore utility to back up the data server configuration. From the **Windows Start** menu, select **Rockwell Software > RSLinx > Backup Restore Utility**.
- **FactoryTalk Linx servers:** The base configuration of the FactoryTalk Linx server is included in the backup, including redundancy and alarms and events configurations.



Note: If the FactoryTalk Linx configuration option is not selected, make a copy of the file `RSLinxNG.xml` and keep it with your backup archive to retain device, driver, and shortcut configurations. By default the file is located in `C:\ProgramData\Rockwell\RSLinxEnterprise`.

- **FactoryTalk Linx Data Bridge:** Open FactoryTalk Linx Data Bridge, select **File > Export configuration**. Keep the exported file with your backup archive.
- **FactoryTalk Linx Gateway:**
  - For FactoryTalk Linx Gateway version 6.20 and earlier, make a copy of the `FTLinxGateway.xml` file and keep it with your backup archive. By default the file is located in `C:\ProgramData\Rockwell\FactoryTalk Linx Gateway`.
  - For FactoryTalk Linx Gateway version 6.21, make a copy of the `FTLinxGateway.db` file and keep it with your backup archive.

By default the file is located in

C:\ProgramData\Rockwell\FactoryTalk Linx Gateway.



Note: If there are two files named as FTLinxGateway.db-shm and FTLinxGateway.db-wal under the folder C:\ProgramData\Rockwell\FactoryTalk Linx Gateway, make a copy of these two files together with FTLinxGateway.db file.

- **FactoryTalk Linx OPC UA Connectors:** The base configuration for the OPC UA Connector can be restored. After the restore operation is completed, you will need to regenerate a certificate and enter a password to return the OPC UA Connector to full operation.
- **FactoryTalk Alarms and Events Logs:** Use Microsoft SQL Server® tools to back up and restore database files.
- **FactoryTalk Transaction Manager:** Back up project files using the **Configuration** menu. See FactoryTalk Transaction Manager documentation for help.
- **FactoryTalk Batch:** Copy the FactoryTalk Batch files back to the same directory locations. See FactoryTalk Batch documentation for help.
- **Other products:** Back up product-specific information separately. See product documentation for help.

---

**IMPORTANT** FactoryTalk Services Platform 6.10 applies a new encryption algorithm to the backup file for enhanced security. Backups created using FactoryTalk Services Platform 6.10 can only be restored to host computers that are also running FactoryTalk Services Platform 6.10 or later. Backups created using FactoryTalk Services Platform 2.90 or later can be restored onto host computers that are running FactoryTalk Services Platform 6.10.

---

## See also

[Restore a FactoryTalk Directory](#) on [page 172](#)

[Backup](#) on [page 168](#)

[Back up a System folder](#) on [page 162](#)

[Back up an application](#) on [page 164](#)

[Backup and restore options](#) on [page 170](#)

## Back up a System folder

Back up a **System** folder to create a backup archive that contains:

- The list of user, computer, and group accounts
- Action groups
- Passwords
- Policy settings
- Security settings
- Alarm and event database definitions

Restoring a **System** folder archive to a FactoryTalk Directory overwrites the contents of the existing System folder with the contents in the backup archive.

## Prerequisites

- Obtain the security permissions needed to perform backup and restore operations. Expand **System > Policies > System Policies**, and open **User Rights Assignment**.

## To back up a System folder

1. In FactoryTalk Administration Console **Explorer**, right-click the **System** folder, then select **Backup**.
2. Use the default name or type another name for the backup file.
3. Use the default archive location or specify another location by selecting **Browse**, selecting a location, and then selecting **OK** in the **Browse for Folder** window.
4. Select a file encryption option:
  - To encrypt your archive, select **Encrypt file contents** and then enter the same passphrase in the **Passphrase** and **Confirm passphrase** fields.
  - To create an archive without encryption, clear **Encrypt file contents**. This creates a plain text file with no password protection.

**Encrypt file contents** will not be available if your operating system does not support the proper level of encryption.
5. In the **Backup** window, select **OK**.

Unless you specified a different file name, FactoryTalk Administration creates a **System.bak** file in the default location or in the location you specified. If a backup file with the same name already exists in the location you've chosen, the system asks whether you want to overwrite the existing file.

---

**IMPORTANT** FactoryTalk Services Platform 6.10 applies a new encryption algorithm to the backup file for enhanced security. Backups created using FactoryTalk Services Platform 6.10 can only be restored to host computers that are also running FactoryTalk Services Platform 6.10 or later. Backups created using FactoryTalk Services Platform 2.90 or later can be restored onto host computers that are running FactoryTalk Services Platform 6.10.

---

## See also

[Restore \(System folder\)](#) on [page 190](#)

[Restore a System folder](#) on [page 175](#)

[Backup resources](#) on [page 170](#)

[Backup](#) on [page 168](#)

[Backup and restore options](#) on [page 170](#)

## Back up an application

An application typically contains areas (in a network directory), resource grouping information, and references to data servers, device servers, alarm servers, and HMI servers.

Back up an application and create an archive file to:

- Restore the application to a FactoryTalk Directory on a different computer
- Duplicate the application with a different name within the same directory

Optionally, include the System folder in the archive. The System folder includes a list of user, computer, and group accounts, passwords, system policy settings, product policy settings, system security settings, action groups, and alarm and event database definitions.

### Prerequisites

- Obtain the security permissions needed to perform backup and restore operations. Open **System > Policies > System Policies**, and double-click **User Rights Assignment**.

### To back up an application

1. In FactoryTalk Administration Console **Explorer**, right-click the selected application, and select **Backup**.
2. Use the default name or enter another name for the backup file.
3. Use the default archive location or specify another location by selecting **Browse**, selecting a location, and then selecting **OK** in the **Browse for Folder** window.
4. To exclude the **System** folder in the backup, clear the **System Directory configuration** check box. To include the System folder in the backup, select the **System Directory configuration** check box.



Tip: You can still choose to restore only the application from the backup archive file later even if you include the System folder in the backup.

5. (optional) Select **FactoryTalk Linux configuration** to back up shortcut and driver configurations.
6. To encrypt your archive file, select the **Encrypt file contents** check box, and then enter the same passphrase in the **Passphrase** and **Confirm passphrase** fields. If you clear this check box, your backup archive file will not be encrypted or protected.

The **Encrypt file contents** check box will not be available if your operating system does not support the proper level of encryption.

---

**IMPORTANT** Remember the passphrase if you choose to encrypt your file contents. The archive file cannot be restored without the correct passphrase.

---

7. In the **Backup** window, select **OK**.

Unless you specified a different file name, FactoryTalk Administration creates an **ApplicationName.bak** file for the application in the default location, or in the location you specified. If a backup file with the same name already exists in the location you've chosen, the system asks whether you want to overwrite the existing file.

8. After backing up an application, back up and restore project files and databases separately from individual software products that are participating in the FactoryTalk system.

If your applications include:

- **HMI servers**, back up and restore FactoryTalk View files separately. See FactoryTalk View documentation for help.**HMI servers:** Back up FactoryTalk View files separately. See FactoryTalk View documentation for help.
- **RSLinx Classic data servers:** Run the RSLinx Backup Restore utility to back up the data server configuration. From the **Windows Start** menu, select **Rockwell Software > RSLinx > Backup Restore Utility**.
- **FactoryTalk Linx servers:** The base configuration of the FactoryTalk Linx server is included in the backup, including redundancy and alarms and events configurations.



Note: If the FactoryTalk Linx configuration option is not selected, make a copy of the file `RSLinxNG.xml` and keep it with your backup archive to retain device, driver, and shortcut configurations. By default the file is located in `C:\ProgramData\Rockwell\RSLinxEnterprise`.

- **FactoryTalk Linx Data Bridge:** Open FactoryTalk Linx Data Bridge, select **File > Export configuration**. Keep the exported file with your backup archive.
- **FactoryTalk Linx Gateway:**
  - For FactoryTalk Linx Gateway version 6.20 and earlier, make a copy of the `FTLinxGateway.xml` file and keep it with your backup archive. By default the file is located in `C:\ProgramData\Rockwell\FactoryTalk Linx Gateway`.
  - For FactoryTalk Linx Gateway version 6.21, make a copy of the `FTLinxGateway.db` file and keep it with your backup archive. By default the file is located in `C:\ProgramData\Rockwell\FactoryTalk Linx Gateway`.
- **FactoryTalk Linx OPC UA Connectors:** The base configuration for the OPC UA Connector can be restored. After the restore operation is completed, you will need to regenerate a certificate and enter a password to return the OPC UA Connector to full operation.
- **FactoryTalk Alarms and Events Logs:** Use Microsoft SQL Server tools to back up and restore database files.



Note: If there are two files named as `FTLinxGateway.db-shm` and `FTLinxGateway.db-wal` under the folder `C:\ProgramData\Rockwell\FactoryTalk Linx Gateway`, make a copy of these two files together with `FTLinxGateway.db` file.

- **FactoryTalk Transaction Manager:** Back up project files using the **Configuration** menu. See FactoryTalk Transaction Manager documentation for help.
- **FactoryTalk Batch:** Copy the FactoryTalk Batch files back to the same directory locations. See FactoryTalk Batch documentation for help.
- **Other products:** Back up product-specific information separately. See product documentation for help.

---

**IMPORTANT** FactoryTalk Services Platform 6.10 applies a new encryption algorithm to the backup file for enhanced security. Backups created using FactoryTalk Services Platform 6.10 can only be restored to host computers that are also running FactoryTalk Services Platform 6.10 or later. Backups created using FactoryTalk Services Platform 2.90 or later can be restored onto host computers that are running FactoryTalk Services Platform 6.10.

---

## See also

[Restore \(Application\)](#) on [page 190](#)

[Backup and restore options](#) on [page 170](#)

[Backup](#) on [page 168](#)

[Update security settings for Networks and Devices](#) on [page 183](#)

[Update security settings for the FactoryTalk Linx OPC UA Connector](#) on [page 184](#)

## Back up a Security Authority identifier

Each FactoryTalk Directory has a unique Security Authority identifier generated during installation. Back up a Security Authority identifier to save the identifier in case of disaster.

Secure controller projects and controllers running secure projects can only be accessed when the FactoryTalk Directory Security Authority identifier matches the identifier saved in the project. This prevents unauthorized access to a controller or controller project if moved or copied to a different FactoryTalk Directory.

## Prerequisites

- Obtain the following permissions from **System > System Policies > User Rights Assignment**:
  - Modify Security Authority Identifier

## To back up the security authority identifier

1. In FactoryTalk Administration Console, select **Tools > FactoryTalk Security Authority Identifier**.

2. In **Modify Security Authority Identifier**, select **Backup**.
3. (optional) In **Backup**, set the backup archive options:
  - **Specify archive name:** Type the name for the backup archive.
  - **Specify archive location:** Type or browse to a path for the backup archive.
  - **Specify backup contents:**
    - Select **FactoryTalk Directory configuration** to back up the entire FactoryTalk Directory.
    - Select **FactoryTalk Linx configuration** to back up shortcut and driver configurations.
  - **Encrypt file contents:** Select to protect the backup archive with a passphrase, then enter the passphrase into the passphrase fields. Clear to save the backup archive as plain text.
4. Select **OK**.
5. (optional) If prompted, select **Yes** to overwrite the existing backup archive.
6. In the confirmation window, select **OK**.

---

**IMPORTANT** FactoryTalk Services Platform 6.10 applies a new encryption algorithm to the backup file for enhanced security. Backups created using FactoryTalk Services Platform 6.10 can only be restored to host computers that are also running FactoryTalk Services Platform 6.10 or later. Backups created using FactoryTalk Services Platform 2.90 or later can be restored onto host computers that are running FactoryTalk Services Platform 6.10.

---

## See also

[Restore a Security Authority identifier](#) on [page 179](#)

[Generate a Security Authority identifier](#) on [page 187](#)

[Modify Security Authority Identifier](#) on [page 171](#)

## Backup FactoryTalk Linx configuration

FactoryTalk Services Platform provides an option to back up the FactoryTalk Linx drivers and shortcuts configured on the same computer where the backup operation is initiated. If the application utilizes distributed FactoryTalk Linx data servers, you must perform a backup on each computer to ensure all of the configurations settings are retained. Refer to [Restore FactoryTalk Linx configuration](#) on [page 180](#) to find steps to restore FactoryTalk Linx configuration on the local workstation and distributed data servers.

## Prerequisites

- Identify the FactoryTalk Linx data servers used by the application.
- Identify the host machines of the distributed FactoryTalk Linx servers.
- Identify if FactoryTalk Linx is configured to utilize CIP Security.



Tip: To check the CIP security information, from the **Communications** tab of FactoryTalk Administration Console, right click the top element in the communication tree and select **Properties**. In the **Device Properties** dialog box, select the **CIP Security** tab.

## To back up FactoryTalk Linx configuration

1. In FactoryTalk Administration Console **Explorer**, right-click the **Network** or **Local Directory** icon, then select **Backup**.
2. In **Specify archive name**, use the default name or type another name for the backup file.



Tip: It is recommended to not change the default archive name. The default name contains the leading digits of the security authority identifier which allows you to easily identify the archive file associated with a specific directory.

3. In **Specify archive location** use the default archive location or use **Browse** to open the **Browse for Folder** window and specify another location.
4. In **Backup Contents**:
  - Select **FactoryTalk Linx configuration** to save the FactoryTalk Linx drivers and shortcuts configured on this computer.



Note: This option is grayed out if the FactoryTalk Linx is not installed or the installed FactoryTalk Linx version is earlier than 6.21.00.

- (optional) Select **FactoryTalk Directory configuration** to back up the entire FactoryTalk Directory.
5. To encrypt your archive file, select the **Encrypt file contents** check box, and then enter the same passphrase in the **Passphrase** and **Confirm passphrase** fields. If you clear this check box, your backup archive file will not be encrypted or protected.

**Encrypt file contents** is not available if your operating system does not support the proper level of encryption.

6. Select **OK**.
7. For distributed system, go to the host workstation of the distributed FactoryTalk Linx data server and perform the backup process above again.

---

**IMPORTANT** To ensure all the configurations settings are retained, user performing the backup of a distributed system must go to each FactoryTalk Linx Data server and back up the configurations.

---

## See also

[Backup](#) on [page 168](#)

[Restore a FactoryTalk Directory](#) on [page 172](#)

## Backup

How do I open Backup?



In the **Explorer** window, right-click the directory icon, an application, or the **System** folder, then click **Backup**.

Use **Backup** to specify:

- The name and location of a backup file
- Whether or not to include the System folder in the backup (application backup only)
- Whether or not to encrypt the backup archive
- A passphrase for the encrypted archive, if used

Setting	Description
Specify archive name	<p>Use the default archive name or type a name for the archive file. The extension .bak is added automatically. You do not have to type it.</p> <ul style="list-style-type: none"> <li>• By default, an archive file that contains a backup of an entire FactoryTalk Directory (including all applications, all user and computer accounts and groups, passwords, policy settings, and security settings) is named with its current security authority identifier, for example, <b>Network - 72CE2C2E-5175-4C26-98AE-3ABE5AC7F8EC.bak</b> or <b>Local - C565C77A-4664-4E6C-9779-1EC729B3A8A0.bak</b>. It is recommended that you do not change the default archive name. The default name contains the leading digits of the security authority identifier which allows you to easily identify the archive file associated with a specific directory.</li> <li>• By default, an archive file that contains a backup of a System folder (including user and computer accounts and groups, passwords, policy settings, and security settings) is named <b>System.bak</b>.</li> <li>• By default, an archive file that contains a backup of a single application is named the same as the application. If you are backing up an application, you can optionally also include the contents of the System folder in the backup archive.</li> </ul>
Specify archive location	<p>Use the default archive location or type the path where you want to save the backup file. Alternatively, select <b>Browse</b>, select a folder, and select <b>OK</b>.</p> <p>The default archive location is <b>C:\Users\Public\Documents</b>.</p>
FactoryTalk Directory configuration	<p>Select this option to back up the entire FactoryTalk Directory. The archive file includes:</p> <ul style="list-style-type: none"> <li>• All objects, references to objects held within the FactoryTalk Directory, and the security authority identifier. The archive file does not contain project files that are specific to individual products.</li> <li>• All applications associated with that directory. Typically an application contains areas (in a network directory), resource grouping information, and references to data servers, device servers, alarm servers, and HMI servers.</li> <li>• The System folder, which includes a list of user, computer, and group accounts, passwords, system policy settings, product policy settings, system security settings, action groups, and alarm and event database definitions.</li> <li>• FactoryTalk Linx OPC UA Connector configurations for all computers configured in the directory.</li> </ul>
FactoryTalk Linx configuration	<p>Select this option to back up all FactoryTalk Linx shortcut configurations and associated paths. The configuration file does not contain CIP security information.</p> <p>The backup operation can only save the FactoryTalk Linx drivers and shortcuts configured on this workstation.</p> <p>Refer to <a href="#">Backup FactoryTalk Linx configuration</a> on <a href="#">page 167</a> to find how to backup a distributed system.</p> <p>Refer to <a href="#">Restore FactoryTalk Linx configuration</a> on <a href="#">page 180</a> to find how to restore a distributed system.</p>
System Directory configuration	<p>The <b>System Directory configuration</b> box is checked by default when you are backing up the System folder. Moreover, it is available if you are backing up an application.</p> <ul style="list-style-type: none"> <li>• To include the contents of the System folder in the backup archive, select this check box.</li> <li>• Choose this option when you want to restore only one application from a FactoryTalk Directory, but want to include all user and computer accounts and groups, passwords, policy settings, and security settings from the original FactoryTalk Directory.</li> <li>• To back up only the application without the System folder, clear this check box.</li> <li>• Choose this option when you want to add an application to an existing FactoryTalk Directory without overwriting the settings held in the System folder.</li> </ul>

Setting	Description
Application Directory configuration	The Application Directory configuration box is checked by default when you are backing up the selected application. The application data server settings and the FactoryTalk Linx OPC UA Connector configuration for all computers configured in the application will be saved.
File Encryption	Choose whether or not to encrypt the archive file. Encrypting the file protects it against unauthorized use. The check box will not be available if your operating system does not support the proper level of encryption. To use the file encryption, install your FactoryTalk software on one of the supported operating systems. <ul style="list-style-type: none"> <li>• To encrypt file contents, select the <b>File Encryption</b> check box.</li> <li>• To save the archive file without encryption, clear this check box.</li> </ul>
Passphrase	Type a passphrase for the archive file you want to encrypt. The passphrase must meet the following requirements: <ul style="list-style-type: none"> <li>• Any alphanumeric character or other characters</li> <li>• Minimum length: 0</li> <li>• Maximum length: 64</li> </ul>
Confirm passphrase	Type the same passphrase you typed in the <b>Passphrase</b> field.

---

**IMPORTANT** Remember the passphrase if you choose to encrypt your file contents. The archive file cannot be restored without the correct passphrase.

FactoryTalk Services Platform 6.10 applies a new encryption algorithm to the backup file for enhanced security. Backups created using FactoryTalk Services Platform 6.10 can only be restored to host computers that are also running FactoryTalk Services Platform 6.10 or later. Backups created using FactoryTalk Services Platform 2.90 or later can be restored onto host computers that are running FactoryTalk Services Platform 6.10.

---

### See also

[Back up an application](#) on [page 164](#)

[Back up a FactoryTalk Directory](#) on [page 160](#)

[Back up a System folder](#) on [page 162](#)

[Backup and restore options](#) on [page 170](#)

## Backup and restore options

Use backup and restore options to select which data in the FactoryTalk Directory should be backed up or restored.

---

**Important:** Restoring from the wrong type of backup archive can overwrite existing data that affects all applications.

FactoryTalk Services Platform 6.10 applies a new encryption algorithm to the backup file for enhanced security. Backups created using FactoryTalk Services Platform 6.10 can only be restored to host computers that are also running FactoryTalk Services Platform 6.10 or later. Backups created using FactoryTalk Services Platform 2.90 or later can be restored onto host computers that are running FactoryTalk Services Platform 6.10.

---

To backup or restore

Create this type of backup archive

An individual application without the System folder	Application
Multiple applications without the System folder	Application Create separate archives for each application.
The System folder, without restoring applications	System folder <ul style="list-style-type: none"> <li>You cannot restore only the System folder from an Application or FactoryTalk Directory archive.</li> </ul>
An individual application and the System folder	Application <ul style="list-style-type: none"> <li>Select <b>Backup system in archive</b>. Selecting this item overwrites the contents of the System folder in the FactoryTalk Directory, including accounts, security settings, and policy settings.</li> </ul>
Multiple applications and the System folder	Application <ul style="list-style-type: none"> <li>Create separate archives for each application, and select <b>Backup system in archive</b> in at least one of the archives.</li> <li>If the applications come from different FactoryTalk Directories, remember that you can restore only one System folder into a single FactoryTalk Directory.</li> </ul>
An entire FactoryTalk Directory including all applications, the System folder, and the security authority identifier	FactoryTalk Directory <ul style="list-style-type: none"> <li>Cannot be used to restore individual applications, or only the System folder.</li> </ul>
The FactoryTalk Directory security authority identifier only	FactoryTalk Directory <ul style="list-style-type: none"> <li>Use <b>Modify Security Authority Identifier</b> to create this backup archive, which contains only the security authority identifier.</li> <li>To restore this backup archive, use <b>Modify Security Authority Identifier</b>.</li> <li>It is strongly recommended to make a backup of the directory with the new identifier after restoring the security authority identifier.</li> </ul>

## See also

[Back up a FactoryTalk Directory](#) on [page 160](#)

[Back up an application](#) on [page 164](#)

[Back up a System folder](#) on [page 162](#)

[Back up a Security Authority identifier](#) on [page 166](#)

[Backup](#) on [page 168](#)

## Modify Security Authority Identifier

How do I open Modify Security Authority Identifier?

- In FactoryTalk Administration Console, select **Tools > FactoryTalk Security Authority Identifier**.

Use **Modify Security Authority Identifier** to generate, back up, or restore the unique Security Authority Identifier for a FactoryTalk Directory. The **User Rights Assignment > Modify Security Authority Identifier** permission is required to generate, back up, or restore the identifier.

Secure controller projects and controllers running secure projects can only be accessed when the FactoryTalk Directory Security Authority identifier matches the identifier saved in the project. This prevents unauthorized access to a controller or controller project if moved or copied to a different FactoryTalk Directory.

**See also**

[Generate a Security Authority identifier](#) on [page 187](#)

[Back up a Security Authority identifier](#) on [page 166](#)

[Restore a Security Authority identifier](#) on [page 179](#)

**Restore a FactoryTalk system**

After backing up an entire FactoryTalk Directory, individual application, System folder, or security authority identifier in an archive file, restore these resources to:

- Recover from a data loss
- Move a development FactoryTalk system to a run-time system
- Copy FactoryTalk Directory components to another computer

Restore the following:

- An entire FactoryTalk Directory
- Only an individual application, with or without the System folder
- Only a System folder

- 
- IMPORTANT**
- Choose the correct backup options when creating a backup archive. Restoring from the wrong type of backup archive overwrites existing data that affects all applications.
  - An archive file created using FactoryTalk Services Platform 6.10 cannot be restored on a computer running an earlier version of FactoryTalk Services Platform.
  - Archive files created using FactoryTalk Services Platform 2.90 or later can be restored on a computer running FactoryTalk Services Platform 6.10.
- 

**See also**

[Restore a FactoryTalk Directory](#) on [page 172](#)

[Restore an application](#) on [page 176](#)

[Restore a System folder](#) on [page 175](#)

[Verify security settings after restoring a FactoryTalk system](#) on [page 181](#)

[Backup and restore options](#) on [page 170](#)

**Restore a FactoryTalk Directory**

To move an entire FactoryTalk system from one computer to another, restore a FactoryTalk Directory backup archive. As a safeguard, create a backup archive of the directory first, before performing a restore operation.

- 
- IMPORTANT**
- *Do not restore* an archive file created under FactoryTalk Services Platform 2.10 (CPR 9) or later into a FactoryTalk Directory that is currently running FactoryTalk Automation Platform 2.00 (CPR 7). This restore scenario is not supported and may have unexpected results.
  - A FactoryTalk Directory archive file that is automatically created when you install or upgrade FactoryTalk Services Platform 2.50 or later can only be restored on the same computer.
  - An archive file created using FactoryTalk Services Platform 6.10 cannot be restored on a computer running an earlier version of FactoryTalk Services Platform.
  - Archive files created using FactoryTalk Services Platform 2.90 or later can be restored on a computer running FactoryTalk Services Platform 6.10.
- 

Restoring an archive created in an earlier version of the FactoryTalk platform into a later version automatically updates the data in the System folder to be compatible with the later version, while retaining the original data from the archive.

For example, restoring an archive created under FactoryTalk Services Platform 2.9 (CPR 9) into a FactoryTalk Directory upgraded to FactoryTalk Services Platform 6.10 (CPR 11) or later. The restore process retains the original user accounts and all system-wide security and policy settings, but also updates the System folder to include new options and policies.

## Prerequisites

1. Obtain the security permissions needed to perform backup and restore operations. Open **System > Policies > System Policies**, and then double-click **User Rights Assignment**.
2. Shut down all FactoryTalk software products, components, and services, except FactoryTalk Administration Console and FactoryTalk Help.
3. Log on to the directory to restore into, and create a backup archive of the existing directory.

## To restore a FactoryTalk Directory

1. In FactoryTalk Administration Console **Explorer**, verify that the applications located in the restore directory are not currently expanded or being used by another product or component. Close all applications held in the directory.
2. Right-click **Network** or **Local**, and select **Restore**.
3. In **Restore**, select **Browse**, select the backup file (\*.bak) to restore, and select **Open**.

By default, an archive file for a network directory or local directory is named with its current security authority identifier, for example, *Network - 72CE2C2E-5175-4C26-98AE-3ABE5AC7F8EC.bak* or *Local - C565C77A-4664-4E6C-9779-1EC729B3A8A0.bak*.

4. Select **Next**.
5. If the backup file is encrypted, **Restore Backup File** opens. Type the passphrase used during the backup operation.

---

**IMPORTANT** An error message opens if the passphrase entered is not correct. Enter the passphrase again. If the wrong passphrase is entered three times, Restore Backup File closes. Select the archive file and try again.

---

After you enter the correct passphrase, **Restore** shows the type of archive and what applications are contained in the archive.

6. In **Restore Contents**:

- Select **FactoryTalk Directory configuration** to restore the entire FactoryTalk Directory.

The entire FactoryTalk Directory will be restored, including all applications, all user and computer accounts and groups, passwords, policy settings, security settings, and the security authority identifier.

- (optional) Select **FactoryTalk Linx configuration** to restore shortcut and driver configurations.



Note: When restoring FactoryTalk Linx configuration, the existing drivers will be replaced and new drivers will be restored. Running shortcuts will be affected unless they are reconfigured.

7. Select **Finish**.



Note: A warning dialog box appears after user select **Finish**, read the warning messages and click **OK** if you decide to continue.

8. After restoring a FactoryTalk Directory, verify FactoryTalk security settings, and perform any follow-up tasks, such as copying in application configuration .xml files and updating passwords.
9. If hosting servers on different computers than those configured in the restored directory, the following additional steps are required:
  - Add the new computers into the FactoryTalk Directory.
  - Change the server host computer names on the server property pages.
  - Restart the computers hosting FactoryTalk Linx and Tag Alarm and Event Servers. This is necessary to ensure the alarm servers start up.

## See also

[Verify security settings after restoring a FactoryTalk system](#) on [page 181](#)

[Update security settings for the FactoryTalk Linx OPC UA Connector](#) on [page 184](#)

[Add a computer](#) on [page 59](#)

[Back up a FactoryTalk Directory](#) on [page 160](#)

## Restore a System folder

To overwrite the contents of the existing System folder with the contents in the backup archive, restore an archive that contains only a System folder.

A System folder archive includes the following:

- The list of user, computer, and group accounts
- Action groups
- Passwords
- Policy settings
- Security settings
- Alarm and event database definitions

Restoring an archive created in an earlier version of the FactoryTalk platform into a later version automatically updates the data in the System folder to be compatible with the later version, while retaining the original data from the archive.

For example, an archive created under FactoryTalk Services Platform 2.90 (CPR 9) restored into a FactoryTalk Directory that has been upgraded to FactoryTalk Services Platform 6.10 (CPR 11) or later. The restore process retains the original user accounts and all system-wide security and policy settings, but also updates the System folder to include new options and policies.

### Prerequisites

1. Obtain the security permissions needed to perform backup and restore operations. Open **System > Policies > System Policies**, and then double-click **User Rights Assignment**.
2. Create the system-only backup archive.
3. Shut down all FactoryTalk software products, components, and services, except FactoryTalk Administration Console and FactoryTalk Help.
4. Log on to the directory you want to restore into, and create a backup archive of the existing directory.

---

**IMPORTANT** Do not restore an archive file created under FactoryTalk Services Platform 2.10 (CPR 9) or later into a FactoryTalk Directory that is currently running FactoryTalk Services Platform 2.00 (CPR 7). This restore scenario is not supported and may have unexpected results.

An archive file created using FactoryTalk Services Platform 6.10 cannot be restored on a computer running an earlier version of FactoryTalk Services Platform.

Archive files created using FactoryTalk Services Platform 2.90 or later can be restored on a computer running FactoryTalk Services Platform 6.10.

---

## To restore a System folder

1. In FactoryTalk Administration Console **Explorer**, right-click **Network** or **Local**, and select **Restore**.
2. Select **Browse**, and then select the backup archive file to restore. The default name is **System.bak**.
3. Select **OK** to close the browse window, and then select **Next**.
4. If the backup file is encrypted, **Restore Backup File** opens. Type the passphrase that was used during the backup operation.

---

**IMPORTANT** An error message opens if the passphrase entered is not correct. Enter the passphrase again. If the wrong passphrase is entered three times, **Restore Backup File** closes. Select the archive file and try again.

---

5. In **Restore Contents**, select **System Directory configuration** to restore the entire FactoryTalk Directory.
6. Select **Finish**.
 

Note: A warning dialog box appears after user select **Finish**, read the warning messages and click **OK** if you decide to continue.
7. After restoring the System folder, back up and restore project files and databases from individual software products.
8. Verify security settings, and perform any follow-up tasks.

## See also

[Verify security settings after restoring a FactoryTalk system](#) on [page 181](#)

[Backup and restore options](#) on [page 170](#)

[Back up a System folder](#) on [page 162](#)

## Restore an application

To restore an application from one computer to another, or to copy an application within the same directory, restore an application. If the System folder was backed up with the application, choose whether or not to restore it.

When restoring an application without the System folder:

- Any references are broken from the application to objects that do not exist in the installed System tree, for example, network or device addresses.
- Security does not work for user accounts, user groups, and computers that do not exist in the installed System folder.

---

**IMPORTANT**

- Do not restore an archive file, created under FactoryTalk Services Platform 2.10 (CPR 9) or later, into a FactoryTalk Directory that is currently running FactoryTalk Automation Platform 2.00 (CPR 7). This restore scenario is not supported and may have unexpected results.
- An archive file created using FactoryTalk Services Platform 6.10 cannot be restored on a computer running an earlier version of FactoryTalk Services Platform.
- Archive files created using FactoryTalk Services Platform 2.90 or later can be restored on a computer running FactoryTalk Services Platform 6.10.

---



## Prerequisites

1. Obtain the security permissions needed to perform backup and restore operations. Open **System > Policies > System Policies**, and then double-click **User Rights Assignment**.
2. Create the application archive, with or without a System folder.
3. Shut down all FactoryTalk software products, components, and services, except FactoryTalk Administration Console and FactoryTalk Help.
4. Log on to the directory you want to restore into, and create a backup archive of the existing directory.

## To restore an application

1. In FactoryTalk Administration Console **Explorer**, right-click **Network** or **Local**, and select **Restore**.
2. In **Restore**, select **Browse**, and then select the backup archive file (**ApplicationName.bak**) to restore. Select **OK**, then select **Next**.
3. If the backup file is encrypted, **Restore Backup File** opens. Type the passphrase that was used during the backup operation.

---

**IMPORTANT** An error message opens if the passphrase entered is not correct. Enter the passphrase again. If the wrong passphrase is entered three times, **Restore Backup File** closes. Select the archive file and try again.

---

4. In **Restore Contents**:
  - (optional) Select **Restore System** to overwrites user, computer, and group accounts, passwords, policy settings, and security settings for all applications in the FactoryTalk Directory. Clear **Restore System**. If restoring an application to a different directory or to a different computer, manually recreate security permissions for FactoryTalk users and groups in the restored application.
  - (optional) Select **FactoryTalk Linx configuration** to restore shortcut and driver configurations.



Note: When restoring FactoryTalk Linx configuration, the existing drivers will be replaced and new drivers will be restored. Running shortcuts will be affected unless they are reconfigured.

5. To restore the application with its original name, select **Finish**. To restore an application with a different name, select the **Restore into a new application named** check box, type the name, and then select **Finish**.


If a different name was entered, the system leaves the original application intact and restores the backup as a new application.



Note: A warning dialog box appears after user select **Finish**, read the warning messages and click **OK** if you decide to continue.

6. If restoring an application without the System folder:

- Restore references from the application to objects that do not exist in the installed System tree, either by adding these items manually or modifying the application to use the objects that are available.
  - Manually reset any existing security settings in the restored application to reference users, user groups, computers, and computer groups defined in the current System folder.
7. If restoring an application with its System folder, verify that the security settings managed through the System folder are correct, and make edits as needed.
  8. If restoring an application that includes a FactoryTalk Linx OPC UA Server that requires authentication, verify that the security settings on the **OPC UA Servers** properties page are correct and make edits as needed.
  9. If restoring an application that includes a FactoryTalk Linx OPC UA Connector, close all the opening FactoryTalk Linx OPC UA Connector interfaces before restoring the UA Connector. If the restored UA Connector is not responding, restart your computer and try again.
  10. If restoring a FactoryTalk Linx server, copy the appropriate configuration file into the product's ProgramData folder (by default, C:\ProgramData\Rockwell\  - FactoryTalk Linx - RSLinxNG.xml
  - FactoryTalk Linx Gateway
    - For FactoryTalk Linx Gateway version 6.20 and earlier, make a copy of the FTLinxGateway.xml file and keep it with your backup archive. By default the file is located in  
C:\ProgramData\Rockwell\FactoryTalk Linx Gateway.
    - For FactoryTalk Linx Gateway version 6.21, make a copy of the FTLinxGateway.db file and keep it with your backup archive. By default the file is located in  
C:\ProgramData\Rockwell\FactoryTalk Linx Gateway.

 Note: If there are two files named as FTLinxGateway.db-shm and FTLinxGateway.db-wal under the folder C:\ProgramData\Rockwell\FactoryTalk Linx Gateway, make a copy of these two files together with FTLinxGateway.db file.
  11. If restoring a FactoryTalk Linx Data Bridge, open FactoryTalk Linx Data Bridge, select **File > Import configuration** and browse to the location where you stored the exported configuration file.

## See also

[Verify security settings after restoring a FactoryTalk system](#) on [page 181](#)

[Update security settings for the FactoryTalk Linx OPC UA Connector](#) on [page 184](#)

[Back up an application](#) on [page 164](#)

[Restore a FactoryTalk system](#) on [page 172](#)

## Restore a Security Authority identifier

Each FactoryTalk Directory has a unique Security Authority identifier generated during installation. Restore a Security Authority identifier to replace the current identifier with an identifier from a backup file.

Secure controller projects and controllers running secure projects can only be accessed when the FactoryTalk Directory Security Authority identifier matches the identifier saved in the project. This prevents unauthorized access to a controller or controller project if moved or copied to a different FactoryTalk Directory.

---

**IMPORTANT** After restoring a new Security Authority identifier, controllers and controller projects secured with the previous identifier cannot be accessed.

---

### Prerequisites

1. Obtain the following permissions from **System > System Policies > User Rights Assignment**:
  - Modify Security Authority Identifier
2. Back up the FactoryTalk Directory.
3. Use Logix Designer to remove security from any controllers and controller projects in the FactoryTalk Directory.
4. Shut down all FactoryTalk software products, components, and services except FactoryTalk Administration Console.

### To restore the security authority identifier

1. In FactoryTalk Administration Console, select **Tools > FactoryTalk Security Authority Identifier**.
2. In **Modify Security Authority Identifier**, select **Restore**.
3. In **Restore**, select **Browse (...)** to specify the archive to restore, then select **Next**.

By default, an archive file for a security authority identifier is named with that identifier. For example, *Network - 72CE2C2E-5175-4C26-98AE-3ABE5AC7F8EC.bak* or *Local - C565C77A-4664-4E6C-9779-1EC729B3A8Ao.bak*.

4. (optional) If the backup file was encrypted, in **Restore Backup File**, type the passphrase to unlock the backup file, then click select **OK**.
5. In **Restore**, select **Restore security authority identifier only**, then select **Finish**.
6. (optional) Use Logix Designer to add security to any controllers and controller projects in the FactoryTalk Directory.

## See also

[Back up a Security Authority identifier](#) on [page 166](#)

[Generate a Security Authority identifier](#) on [page 187](#)

[Modify Security Authority Identifier](#) on [page 171](#)

## Restore FactoryTalk Linx configuration

The FactoryTalk Linx configuration saved with a FactoryTalk backup can be restored to return a computer to the configuration when the backup was created. This is helpful when a computer needs to be replaced or refreshed resulting from a significant hardware or operating system failure. The FactoryTalk Linx configuration saved from the local workstation or distributed data servers can be restored to a individual computers.

## Prerequisites

1. Obtain the security permissions needed to perform backup and restore operations. Open **System > Policies > System Policies**, and then double-click **User Rights Assignment**.
2. Shut down all FactoryTalk software products, components, and services, except FactoryTalk Administration Console and FactoryTalk Help.
3. Log on to the directory to restore into, and create a backup archive of the existing directory.

## To restore FactoryTalk Linx configuration

1. In FactoryTalk Administration Console **Explorer**, right-click **Network** or **Local**, and select **Restore**.
2. In **Restore**, select **Browse**, select the backup file (\*.bak) to restore, and select **Open**.
3. Select **Next**.
4. If the backup file is encrypted, **Restore Backup File** opens. Type the passphrase used during the backup operation.

An error message opens if the passphrase entered is not correct. Enter the passphrase again. If the wrong passphrase is entered three times, Restore Backup File closes. Select the archive file and try again.

5. In **Restore Contents**:
  - Select **FactoryTalk Linx configuration** to restore shortcut and driver configurations.



Note:

- Restoring the FactoryTalk Link configuration will impact the running system because existing drivers and shortcuts will be replaced with drivers and shortcuts from the backup file. Reconfigure the shortcuts after restore completed.
- This option is grayed out if the FactoryTalk Linx is not installed or the installed FactoryTalk Linx version is earlier than 6.21.00.

- Select **FactoryTalk Directory configuration** to restore the entire FactoryTalk Directory.

The entire FactoryTalk Directory will be restored, including all applications, accounts, passwords, policies, security settings, and FactoryTalk Linx OPC UA Connector configuration for computers configured in the directory.

6. Select **Finish**.



Note: A warning dialog box appears after user select **Finish**, read the warning messages and click **OK** if you decide to continue.

7. If hosting servers on different computers than those configured in the restored directory, the following additional steps are required:
- Add the new computers into the FactoryTalk Directory.
  - Change the server host computer names on the server property pages.
  - Restart the computers hosting FactoryTalk Linx and Tag Alarm and Event Servers. This is necessary to ensure the alarm servers start up.

## Verify security settings after restoring a FactoryTalk system

After restoring a FactoryTalk Directory backup archive, verify the FactoryTalk Directory security settings on the new FactoryTalk system meet your requirements, and make adjustments as needed.

Depending upon your FactoryTalk configuration, do one or more of the following tasks after restoring the FactoryTalk Directory:

- Update computer accounts in the network directory
- Recreate Windows-linked user accounts
- Update Windows-linked user groups
- Update security settings for Networks and Devices
- Update security settings for FactoryTalk Linx OPC UA Connector
- Restore database connections

### See also

[Update computer accounts in the network directory](#) on [page 181](#)

[Recreate a Windows-linked user account](#) on [page 182](#)

[Update Windows-linked user groups](#) on [page 183](#)

[Update security settings for Networks and Devices](#) on [page 183](#)

[Restore database connections](#) on [page 185](#)

## Update computer accounts in the network directory

After restoring any backup archive that includes a System folder, update computer accounts to allow access to the network directory.

If the system policy **Require computer accounts for all client machines** is enabled, then only client computers that have been added to the list of

computers in the network directory can access that directory. When a backup archive is restored, the directory automatically adds the computer on which the network directory server resides, and the client computer from which the restore operation was performed, to the System folder in the network directory.

### To update computer accounts in the network directory

1. Log on to FactoryTalk Administration Console as administrator on either the network directory server computer or the client computer where the restore was performed.
2. Rename existing computer accounts from the old domain to easily map them to computers on the new domain. This retains any security settings that were applied to the computer accounts in the old domain.
3. Delete computer accounts that no longer exist in the new domain, and that do not map to computers in the new domain.
4. Add computer accounts to allow computers on the network access to the restored network directory.



Tip: If you delete a computer account and then recreate it, its security settings are lost. To map computers from one domain to another, rename the computer accounts rather than deleting and recreating them.

### See also

[Edit or view computer properties](#) on [page 61](#)

[Delete a computer](#) on [page 60](#)

[Add a computer](#) on [page 59](#)

[Verify security settings after restoring a FactoryTalk system](#) on [page 181](#)

## Recreate a Windows-linked user account

When using individual Windows-linked user accounts, recreate these accounts when restoring your FactoryTalk Directory to a new FactoryTalk system.

---

**IMPORTANT** Only Windows-linked user group accounts move to a new domain, individual Windows-linked user accounts do not move. This allows you to retain all of the security permissions for the group.

---

### Prerequisites

- Restore the FactoryTalk Directory on the run-time network.
- Complete any follow-up tasks needed to recreate the development FactoryTalk Directory on the run-time network.

## To recreate a Windows-linked user account

1. In FactoryTalk Administration Console **Explorer**, expand **System > Policies > System Policies**, and double-click **Security Policy**.
2. Expand **Account Policy Settings**, then select **Show deleted accounts in user list**. Enable this setting.
3. Delete the old account.
4. Create the new account.
5. Recreate all the security permissions for the new account. Choose one of the following:
  - Add the user account to a group that already has security settings defined for it
  - Create permissions for a user account when securing a resource

### See also

[Update Windows-linked user groups](#) on [page 183](#)

[Delete a user account](#) on [page 48](#)

[Add a Windows-linked user account](#) on [page 45](#)

[Add accounts to a FactoryTalk user group](#) on [page 56](#)

[Verify security settings after restoring a FactoryTalk system](#) on [page 181](#)

## Update Windows-linked user groups

When the System folder is restored to a new Windows domain, Windows-linked user groups that existed in the original domain may no longer exist in the new domain.

Change the original Windows-linked groups to groups that exist in the new domain. Security settings that refer to the Windows-linked groups in the new domain update automatically. Move your applications to a different domain without having to change or recreate each user account separately.

If the system uses local workstation accounts as part of a Windows workgroup, Windows-linked user accounts lose their security settings after the System folder is restored.

### See also

[Update security settings for Networks and Devices](#) on [page 183](#)

## Update security settings for Networks and Devices

After restoring an entire FactoryTalk Directory, update security settings for **Networks and Devices** to secure them in the new domain.

The **Networks and Devices** tree displays information about the networks and devices connected to the local computer. The contents of the **Networks and**

**Devices** tree are not included in the backup archive, however the backup archive does include any security settings defined for networks and devices.

If an archive is restored on a computer connected to the same networks and devices using the same drivers or logical names, the security settings restored from the archive file take effect. Check to make sure security settings are accurate for the resources in the new FactoryTalk system, and make edits as needed.

## To update security settings for Networks and Devices

1. In FactoryTalk Administration Console **Explorer**, select **Networks and Devices** to view the networks and devices in your FactoryTalk system.



Tip: To check the security settings for a network or device, right-click its icon, then select **Security**. Use **Security Settings** to view permissions by user or by action, and to see if permissions are inherited from higher levels in the FactoryTalk directory tree.

2. Review and edit user action permissions as needed.

## See also

[Restore database connections](#) on [page 185](#)

[Verify security settings after restoring a FactoryTalk system](#) on [page 181](#)

## Update security settings for the FactoryTalk Linx OPC UA Connector

After restoring an entire FactoryTalk Directory on a replacement or re-imaged computer, update security settings for the FactoryTalk Linx OPC Connector if the OPC UA Server requires authentication. The user credentials for the OPC UA Server are encrypted and tied to the private key of the original computer, so replacing the computer removes the stored credentials.

If an archive is restored on the same computer and the computer is not re-imaged, the credentials are included in the restore, but should be verified to ensure proper operation.

## To update security settings for the FactoryTalk Linx OPC UA Connector

1. In FactoryTalk Administration Console **Explorer**, right-click a FactoryTalk Linx OPC UA Connector, then click **Properties**.
2. Click **OPC UA Servers**.
3. Select a server from the **OPC UA Servers** list to edit its properties
4. Under **Authentication Settings** review and edit the user name and password as needed.



## See also

[Restore database connections](#) on [page 185](#)

[Verify security settings after restoring a FactoryTalk system](#) on [page 181](#)

## Restore database connections

If the FactoryTalk system being restored includes Microsoft SQL Server databases for logging historical data, including FactoryTalk Alarms and Events logs, the connection to the database must be restored to re-establish a connection between a database definition, held in the directory, and its associated Microsoft SQL Server database.

### To restore database connections

1. On any computer in the network directory, run FactoryTalk Administration Console.
2. From **Explorer**, open **System > Connections > Databases**.
3. Double-click the database definition to open its properties, update the SQL Server host computer name if it has changed, and then select **OK**.  
The system checks for database tables and creates them, if they do not exist.

## See also

[Verify security settings after restoring a FactoryTalk system](#) on [page 181](#)

[Restore a FactoryTalk system](#) on [page 172](#)

## Restore an earlier system after upgrading FactoryTalk platform software

An archive file created using FactoryTalk Services Platform 6.10 cannot be restored on a computer running an earlier version of FactoryTalk Services Platform. You must use the archive file created before you installed FactoryTalk Services Platform 6.10 to revert to a previous version.

Before restoring to an earlier system, keep the following in mind:

- Following the instructions in this topic overwrites all data in the FactoryTalk Directory and returns it to the state it was in before upgraded. For example, any applications, security settings, or system policies will be lost. If you want to keep any of this data, back up the network directory and local directory now.
- When reverting from FactoryTalk Services Platform 2.10 (CPR 9) or later to an earlier version of the platform, you must restore backup archives for both the network directory and the local directory, even if you plan to use only one of the directories.
- If you upgraded to FactoryTalk Services Platform version 2.10 (CPR 9) or later, backups of the earlier version of the local directory and

- network directory were automatically created. You can use those backups to revert to an earlier version.
- Do not restore an archive file created with FactoryTalk Services Platform 2.10 (CPR 9) or later into a FactoryTalk Directory that is running FactoryTalk Services Platform 2.00 (CPR 7). This is not supported and may have unexpected results.
  - As part of re-installing an earlier version of FactoryTalk Services Platform or FactoryTalk Automation Platform, you will need to enter the FactoryTalk administrator user name and passwords that were saved in the backup archive of the FactoryTalk Directory.

### To restore an earlier system after upgrading FactoryTalk platform software

1. Uninstall all FactoryTalk software products that are incompatible with the version of the FactoryTalk platform you plan to use.
  - a. To verify the version of the FactoryTalk platform software that a product requires, see the product's installation documentation.
  - b. Go to **Control Panel > Uninstall a program** or **Programs and Features**.
  - c. Uninstall FactoryTalk Services Platform.
  - d. Uninstall **Windows Firewall Configuration Utility**.
2. Restart your computer.
3. Delete the folders **C:\ProgramData\Rockwell\RNAServer** and **C:\ProgramData\Rockwell\RNAClient**.
4. Install the version of the FactoryTalk platform software you plan to use. If the version is 2.10 (CPR 9) or later, skip to the next step after installation. If the version is 2.00 (CPR 7), do the following:
  - On the **Overview** page of the FactoryTalk Directory Configuration Wizard, select both **FactoryTalk Network Directory** and **FactoryTalk Local Directory** and then select **Next**.
  - If prompted, enter a FactoryTalk administrator user name and password for each directory.
5. Install earlier versions of all software products that are compatible with the version of the FactoryTalk platform software you plan to use. To verify the version of the FactoryTalk platform software that a product requires, see the product's installation documentation.
6. Run FactoryTalk Administration Console and log on to the Local Directory. In **Explorer**, right-click the **Local** icon and then restore a local backup archive created with the earlier version of the FactoryTalk platform software.

7. Select **File > Log Off** to log off the local directory, and then log on to the network directory. Right-click the **Network** icon and then restore a network backup archive created with the earlier version of the FactoryTalk platform software.

## See also

[Restore a FactoryTalk system](#) on [page 172](#)

## Generate a Security Authority identifier

Each FactoryTalk Directory has a unique Security Authority identifier generated during installation. Generate a Security Authority identifier to change the Security Authority identifier assigned to the FactoryTalk Directory.

Secure controller projects and controllers running secure projects can only be accessed when the FactoryTalk Directory Security Authority identifier matches the identifier saved in the project. This prevents unauthorized access to a controller or controller project if moved or copied to a different FactoryTalk Directory.

---

**IMPORTANT** After generating a new Security Authority identifier, controllers and controller projects secured with the previous identifier cannot be accessed.

---

## Prerequisites

1. Obtain the following permissions from **System > System Policies > User Rights Assignment**:
  - Modify Security Authority Identifier
2. Back up the FactoryTalk Directory.
3. Use Logix Designer to remove security from any controllers and controller projects in the FactoryTalk Directory.
4. Shut down all FactoryTalk software products, components, and services except FactoryTalk Administration Console.

## To generate a Security Authority identifier

1. In FactoryTalk Administration Console, select **Tools > FactoryTalk Security Authority Identifier**.
2. In **Modify Security Authority Identifier**, select **Generate ID**.
3. In the confirmation window, select **Yes**.
4. (optional) select **Backup** to back up the current directory with the new identifier.
5. Select **Close**.
6. (optional) Use Logix Designer to add security to any controllers and controller projects in the FactoryTalk Directory.

## See also

[Back up a Security Authority identifier](#) on [page 166](#)

[Restore a Security Authority identifier](#) on [page 179](#)

[Modify Security Authority Identifier](#) on [page 171](#)

## Restore

How do I open Restore?

1. In the **Explorer** window, verify that the applications located in the directory that you are restoring into are not currently expanded or being used by some other product or component.
2. Right-click **Network** or **Local**, and click **Restore**.

Use **Restore** to specify the name of the backup file to use to restore all or part of a FactoryTalk Directory.

Select one of these archive types:

- A full FactoryTalk Directory backup archive. This will be named with its security authority identifier (for example, *Network - 72CE2C2E-5175-4C26-98AE-3ABE5AC7F8EC.bak* or *Local - C565C77A-4664-4E6C-9779-1EC729B3A8Ao.bak*). It contains all applications, and all user and computer accounts and groups, passwords, policy settings, and security settings.
- A System folder archive. A System folder archive contains a backup of a System folder, including user and computer accounts and groups, passwords, policy settings, and security settings. It is named **System.bak** by default.
- An application archive. This archive contains a backup of the application, and may contain a backup of the System folder. By default, an application archive file has the same name as the application.

Before restoring an archive file, shut down all FactoryTalk software products, components, and services, except FactoryTalk Administration Console and FactoryTalk Help, then create a backup archive of the target directory before continuing with the restore process.

An archive file created under FactoryTalk Automation Platform 2.00 (CPR 7) and restored into a FactoryTalk Directory that has been upgraded to FactoryTalk Services Platform 2.10 (CPR 9) or later automatically updates the data in the **System** folder to be compatible with FactoryTalk Services Platform 2.10 or later, while leaving the original data unchanged.

- 
- IMPORTANT**
- Do not restore an archive file created under FactoryTalk Services Platform 2.10 (CPR 9) or later into a FactoryTalk Directory that is running FactoryTalk Automation Platform 2.00 (CPR 7). This restore scenario is not supported and may have unexpected results.
  - An archive file created using FactoryTalk Services Platform 6.10 cannot be restored on a computer running an earlier version of FactoryTalk Services Platform.
  - Archive files created using FactoryTalk Services Platform 2.90 or later can be restored on a computer running FactoryTalk Services Platform 6.10.
-

## See also

[Restore a FactoryTalk Directory](#) on [page 172](#)

[Restore a System folder](#) on [page 175](#)

[Restore an application](#) on [page 176](#)

[Verify security settings after restoring a FactoryTalk system](#) on [page 181](#)

## Restore (FactoryTalk Directory)

How do I open Restore?

1. In the **Explorer** window, verify that the applications located in the directory that you are restoring into are not currently expanded or being used by some other product or component.
2. Right-click **Network** or **Local**, and click **Restore**.

After selecting a FactoryTalk Directory archive to restore, verify the restoration settings are correct to finish the restore operation. If this is not the correct backup archive, select **Cancel** to exit or **Back** to select a different archive file.

Backup files that are created automatically when upgrading to FactoryTalk Services Platform 2.50 or later can only be restored on the same computer.

- 
- IMPORTANT**
- Do not restore an archive file created under FactoryTalk Services Platform 2.10 (CPR 9) or later into a FactoryTalk Directory that is running FactoryTalk Automation Platform 2.00 (CPR 7). This restore scenario is not supported and may have unexpected results.
  - An archive file created using FactoryTalk Services Platform 6.10 cannot be restored on a computer running an earlier version of FactoryTalk Services Platform.
  - Archive files created using FactoryTalk Services Platform 2.90 or later can be restored on a computer running FactoryTalk Services Platform 6.10.
- 

Setting	Description
Archive name	The name of the backup archive file to restore.
Directory type	Identifies the type of information held within the backup archive file. <b>FactoryTalk Directory</b> - Identifies an archive file that contains the contents of an entire directory, including all applications and the System folder. <b>Important:</b> Restoring the System folder overwrites all user and computer accounts and groups, passwords, policy settings, and security settings for all applications in the FactoryTalk Directory.
Application(s)	Lists the names of the applications held in the backup archive file. When you restore an entire directory, all of the applications included in that directory are also restored.
FactoryTalk Directory configuration	Restores applications, users, computers, groups, passwords, policies, security settings, and FactoryTalk Linx OPC UA Connector configuration for computers configured in the directory.
FactoryTalk Linx configuration	Restore shortcut and driver configurations of FactoryTalk Linx. Only FactoryTalk Linx configurations exist on the local PC can be restored. Refer to <a href="#">Restore FactoryTalk Linx configuration</a> on <a href="#">page 180</a> to find how to restore a distributed system.



Tip: After restoring from a backup archive, manually back up and restore project files and databases from other software products participating in the FactoryTalk system, and check security settings and computer accounts.

**See also**

[Restore a FactoryTalk Directory](#) on [page 172](#)

**Restore (System folder)**

How do I open Restore?

1. In the **Explorer** window, verify that the applications located in the directory that you are restoring into are not currently expanded or being used by some other product or component.
2. Right-click **Network** or **Local**, and click **Restore**.

After selecting a system-only archive file, **Restore** displays the archive name and the archive type.

Restoring a **System** folder moves the following system-wide settings from one FactoryTalk Directory to another:

- The list of user, computer, and group accounts
- Action groups
- Passwords
- Policy settings
- Security settings
- Alarm and event database definitions

Review the following settings before selecting **Finish** to restore a System folder.

Setting	Description
Archive name	The name of the backup archive file to restore.
Directory type	Identifies the type of information held within the backup archive file. <b>System Only</b> - Restoring the System folder overwrites all user and computer accounts and groups, passwords, policy settings, and security settings for all applications in the FactoryTalk Directory.
Application(s)	<b>Archive does not contain any application</b> - Confirms that applications are not included in the backup archive to restore.
System Directory configuration	This option is selected by default to restore the entire <b>System</b> folder. Restoring the <b>System</b> folder overwrites all user and computer accounts and groups, passwords, policy settings, and security settings for all applications in the FactoryTalk Directory.

**See also**

[Restore a System folder](#) on [page 175](#)

[Backup and restore options](#) on [page 170](#)

**Restore (Application)**

How do I open Restore?

1. In the **Explorer** window, verify that the applications located in the directory that you are restoring into are not currently expanded or being used by some other product or component.
2. Right-click **Network** or **Local**, and click **Restore**.

After selecting a FactoryTalk Directory archive to restore, verify the restoration settings are correct to finish the restore operation. If this is not the correct backup archive, select **Cancel** to exit or **Back** to select a different archive file.

If the **System** folder was backed up with the application, choose whether to restore it along with the application.

Backup files that are created automatically when upgrading to FactoryTalk Services Platform 2.50 or later can only be restored on the same computer.

- 
- IMPORTANT**
- Do not restore an archive file created under FactoryTalk Services Platform 2.10 (CPR 9) or later into a FactoryTalk Directory that is running FactoryTalk Automation Platform 2.00 (CPR 7). This restore scenario is not supported and may have unexpected results.
  - An archive file created using FactoryTalk Services Platform 6.10 cannot be restored on a computer running an earlier version of FactoryTalk Services Platform.
  - Archive files created using FactoryTalk Services Platform 2.90 or later can be restored on a computer running FactoryTalk Services Platform 6.10.
- 

Setting	Description
Archive name	The name of the backup archive file to be restored. By default, the archive name is <b>ApplicationName.bak</b> file.
Directory type	Identifies the type of information held within the backup archive file. <ul style="list-style-type: none"> <li>• <b>Application and System</b> - Identifies an archive file that contains both an application and a System folder.</li> <li>• <b>Application</b> - Identifies an archive file that contains only an application.</li> </ul>
Application(s)	The name of the application or applications held in the backup archive file.
System Directory configuration	Select or clear this option to your need: <ul style="list-style-type: none"> <li>• To restore the application and the System folder, select <b>Restore System</b>. Restoring the System folder <b>overwrites all</b> user and computer accounts and groups, passwords, policy settings, and security settings for all applications in the FactoryTalk Directory.</li> <li>• To restore the application without restoring the System folder, clear <b>Restore System</b>. Restoring the System folder overwrites all user and computer accounts and groups, passwords, policy settings, and security settings for all applications in the FactoryTalk Directory.</li> </ul> <p>When restoring an application without its associated System folder to a different directory or to a different computer, security permissions for FactoryTalk users and groups need to be manually recreated in the restored application.</p>
FactoryTalk Linx configuration	Select this option to restore the FactoryTalk Linx shortcuts and drivers configuration. Only FactoryTalk Linx configurations exist on the local PC can be restored. Refer to <a href="#">Restore FactoryTalk Linx configuration</a> on <a href="#">page 180</a> to find how to restore a distributed system.

Setting	Description
Restore into a new application named:	<p>Choose whether to overwrite an existing application or create a new application.</p> <ul style="list-style-type: none"> <li>• To restore the contents of the backup archive file into an application with a new name, select <b>Restore into a New Application Named</b>, then enter a unique name. When <b>Finish</b> is selected, the system leaves the original application intact and restores the backup archive as a new application in the directory. When both applications are the same, it copies the archived application into the directory.</li> <li>• To restore an existing application with its original name, clear <b>Restore into a New Application Named</b>. When <b>Finish</b> is selected, the system confirms to overwrite the existing application of the same name. Select <b>Yes</b> to restore the application.</li> </ul>

**See also**

[Restore an application](#) on [page 176](#)

**Restore (Security Authority Identifier)**

How do I open Restore?

1. In the **Explorer** window, verify that the applications located in the directory that you are restoring into are not currently expanded or being used by some other product or component.
2. Right-click **Network** or **Local**, and click **Restore**.

Setting	Description
Archive name	The name of the backup archive file to be restored. By default, the archive name is <b>ApplicationName.bak</b> file.
Directory type	<p>Identifies the type of information held within the backup archive file.</p> <ul style="list-style-type: none"> <li>• <b>FactoryTalk Directory</b> - Identifies an archive file that contains the contents of an entire directory, including all applications and the System folder.</li> <li>• <b>Application and System</b> - Identifies an archive file that contains both an application and a System folder.</li> <li>• <b>Application</b> - Identifies an archive file that contains only an application.</li> <li>• <b>System Only</b> - Restoring the System folder overwrites all user and computer accounts and groups, passwords, policy settings, and security settings for all applications in the FactoryTalk Directory.</li> </ul>
Application(s)	The name of the application or applications held in the backup archive file.
Restore directory contents only	Restores applications, users, computers, groups, passwords, policies, and security settings. The security authority identifier is not restored.
Restore security authority identifier only	<p>Only restores the security authority identifier. Applications, users, computers, groups, passwords, policies, and security settings are not restored.</p> <p>Back up your directory and remove the old bindings from all controllers and controller projects before continuing. Back up the directory with the new identifier after the restore process is completed.</p>
FactoryTalk Directory configuration	Restores applications, users, computers, groups, passwords, policies, and security settings. This option is only available when Restore directory contents is selected.
FactoryTalk Linx configuration	Select this option to restore the FactoryTalk Linx shortcuts and drivers configuration. Only FactoryTalk Linx configurations exist on the local PC can be restored.



## See also

[Restore an application](#) on [page 176](#)

## Restore Backup File

Use **Restore Backup File** to enter the passphrase which was used during the archive file backup operation. The archive file cannot be restored without the correct passphrase.

The passphrase must meet the following requirements:

- Any alphanumeric character or other characters
- Minimum length: 0
- Maximum length: 64

An error message opens if the passphrase you entered is not correct. Enter the passphrase again. If the wrong passphrase is entered three times, **Restore Backup File** closes. Select the archive file and try again.

## See also

[Restore \(FactoryTalk Directory\)](#) on [page 189](#)

[Restore an application](#) on [page 176](#)

[Restore a System folder](#) on [page 175](#)

[Restore a Security Authority identifier](#) on [page 179](#)

## Use commands to back up and restore

FactoryTalk Services Platform supports backing up and restoring directory, system, and application via the user interface. From FactoryTalk Services Platform version 6.21, the **FTSysBackupRestore Tool** provides an option to use commands to back up and restore directory, system, and applications.

Parameter	Required/Optional	Description
-s	Required	Specifies the FactoryTalk Directory scope. Only "Global" and "Local" scopes are supported.
-sso	Required	Uses single sign-on for authentication.
-b	Required	Command for backup, which is conflict with the -r command.
-r	Required	Command for restore, which is conflict with the -b command.
-bak	Required	Specifies the location to save the backup file or the location where restore file can be found. (For example: -bak c:\aa.bak) <ul style="list-style-type: none"> <li>• For backup operation, the existing files will be replaced while creating new files.</li> <li>• For restore operation, make sure the file already exists in the system.</li> </ul>
-ftd	Optional	The whole FactoryTalk directory. The -sys and -app commands will be ignored if the -ftd is used.
-sys	Optional	The FactoryTalk System directory.
-app	Optional	Specifies the FactoryTalk application. Specific application names are needed when using this parameter.

Parameter	Required/Optional	Description
-ido	Optional	Used to restore the FactoryTalk Directory identifier. It's only valid with command -r.
-prod	Optional	Specifies the product names. (For example: -prod "FactoryTalk Linx")
-e	Optional	Used to encrypt the backup file.
-ep	Optional	Specifies the passphrase used to encrypt or decrypt the backup file. Use the Data Protection API to encrypt the passphrase. The encrypted passphrase needs to convert to base64 string with UTF-8 encoding. The FTSysBackupRestoreTool will also use the same algorithm to decrypt the passphrase. Refer to <a href="https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography.protecteddata.protect?view=netframework-4.7.2#System_Security_Cryptography_ProtectedData_Protect_System_Byte___System_Byte___System_Security_Cryptography_DataProtectionScope_">C# API and sample code</a> https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography.protecteddata.protect?view=netframework-4.7.2#System_Security_Cryptography_ProtectedData_Protect_System_Byte___System_Byte___System_Security_Cryptography_DataProtectionScope_. <b>Note:</b> If the passphrase contains a " ", it should be type as " " in command line. For example, if the passphrase is ~ ! @ # \$ % ^ & * ( ) _ + - = { } [ ]   \ : " ; ' < > , . ? / , when you use the passphrase to encrypt or decrypt the backup file in commands, you should type the passphrase as " ~ ! @ # \$ % ^ & * ( ) _ + - = { } [ ]   \ : " ; ' < > , . ? / " .
-pp	Optional	The plain passphrase is used to encrypt or decrypt the backup file. The command will be ignored when "-ep" command is used or the "-e" command is not used. <b>Note:</b> If the passphrase contains a " ", it should be type as " " in command line. For example, if the passphrase is ~ ! @ # \$ % ^ & * ( ) _ + - = { } [ ]   \ : " ; ' < > , . ? / , when you use the passphrase to encrypt or decrypt the backup file in commands, you should type the passphrase as " ~ ! @ # \$ % ^ & * ( ) _ + - = { } [ ]   \ : " ; ' < > , . ? / " .
-f	Optional	Used to force replace the opened applications if needed.
-ow	Optional	Used to overwrite the existing applications.

### Examples of using the command line:

- Back up the FactoryTalk Directory
 

```
"C:\Program Files (x86)\Common
Files\Rockwell\FTSysBackupRestoreTool.exe" -b -s
Global -sso -bak
C:\Users\Administrator\Desktop\ftd1.bak -ftd -e -pp
"~!@#$%^&*( )_+-={ } [ ] | \ : " ; ' < > , . ? / "
"C:\Program Files (x86)\Common
Files\Rockwell\FTSysBackupRestoreTool.exe" -b -s
Global -sso -bak
C:\Users\Administrator\Desktop\ftd2.bak -ftd -ido -
prod "FactoryTalk Linx" -e -ep AQANCMnd8BF/Cl+s
"C:\Program Files (x86)\Common
Files\Rockwell\FTSysBackupRestoreTool.exe" -b -s
Global -sso -bak
C:\Users\Administrator\Desktop\identifier.bak -ido
```
- Back up an application
 

```
"C:\Program Files (x86)\Common
Files\Rockwell\FTSysBackupRestoreTool.exe" -b -s
```

```
Global -sso -bak
C:\Users\Administrator\Desktop\application1.bak -app
A1 -sys
"C:\Program Files (x86)\Common
Files\Rockwell\FTSysBackupRestoreTool.exe" -b -s
Global -sso -bak
C:\Users\Administrator\Desktop\application2.bak -app
A1 -sys -prod "FactoryTalk Linx"
```

- Back up the System folder

```
"C:\Program Files (x86)\Common
Files\Rockwell\FTSysBackupRestoreTool.exe" -b -s
Global -sso -bak
C:\Users\Administrator\Desktop\System.bak -sys
```

- Restore the FactoryTalk Directory

```
"C:\Program Files (x86)\Common
Files\Rockwell\FTSysBackupRestoreTool.exe" -r -s
Global -sso -bak
C:\Users\Administrator\Desktop\ftd1.bak -ftd -e -pp
"!@#%$%^&*()_+-={}|[]\:"';'<>,.?/"
"C:\Program Files (x86)\Common
Files\Rockwell\FTSysBackupRestoreTool.exe" -r -s
Global -sso -bak
C:\Users\Administrator\Desktop\ftd2.bak -ftd -ido -
prod "FactoryTalk Linx" -e -ep AQANCMnd8BF/C1+s
"C:\Program Files (x86)\Common
Files\Rockwell\FTSysBackupRestoreTool.exe" -r -s
Global -sso -bak
C:\Users\Administrator\Desktop\identifier.bak -ido
```

- Restore an application

```
"C:\Program Files (x86)\Common
Files\Rockwell\FTSysBackupRestoreTool.exe" -r -s
Global -sso -bak
C:\Users\Administrator\Desktop\application1.bak -app
A1 -sys
"C:\Program Files (x86)\Common
Files\Rockwell\FTSysBackupRestoreTool.exe" -r -s
Global -sso -bak
C:\Users\Administrator\Desktop\application2.bak -app
A1 -sys -prod "FactoryTalk Linx"
```

- Restore the System folder

```
"C:\Program Files (x86)\Common
Files\Rockwell\FTSysBackupRestoreTool.exe" -r -s
Global -sso -bak
C:\Users\Administrator\Desktop\system.bak -sys
```



Note: For an encrypted bak file created in FactoryTalk Services Platform version 3.00 and before, if no passphrase was entered, the restore commands should be like:

```
"C:\Program Files (x86)\Common
Files\Rockwell\FTSysBackupRestoreTool.exe" -r
-s Global -sso -bak
C:\Users\Administrator\Desktop\Network.bak -
ftd -e
```

## FactoryTalk Directory Configuration Wizard

How do I run the FactoryTalk Directory Configuration Wizard?

1. On the computer where FactoryTalk Services Platform is installed, log on to Windows with a user account that is a member of the local Windows Administrators group.
2. Click **Start > All Programs > Rockwell Software > FactoryTalk Tools > FactoryTalk Directory Configuration Wizard**.

FactoryTalk Directory products share a common address book, finding and providing access to plant floor resources, such as data tags and graphic displays.

Configuration of the FactoryTalk Directory is automatic during installation of FactoryTalk Services Platform. Use FactoryTalk Directory Configuration Wizard when circumstances require a manual configuration of FactoryTalk Directory. The FactoryTalk Directory Configuration Wizard is for use by FactoryTalk administrators.

Run the FactoryTalk Directory Configuration Wizard if:

- An error occurs while installing the FactoryTalk Services Platform, or a message displays instructing to run the wizard manually.
- A valid FactoryTalk Administrator account could not be found for the directory during an upgrade of an existing FactoryTalk Directory from FactoryTalk® Automation Platform version 2.0.
- If FactoryTalk Services Platform was installed from a remote client (such as Remote Desktop Services). The FactoryTalk Directory cannot be configured from a remote client. The FactoryTalk Directory Configuration Wizard must be run at the Windows console on the computer.
- The FactoryTalk administrator account in the network directory or local directory is not accessible. Running the wizard resets a locked administrator account, or changes an expired password for the administrator account. Alternatively, have another user whose account is a member of the FactoryTalk Administrators group reset your locked account or password for you.

If the administrator account was disabled, have another user enable the account in FactoryTalk Administration Console. The last FactoryTalk administrator account in a directory cannot be disabled. If no other user is available, or the password to another administrator account is not known (for example, because that user left the organization), contact Rockwell Automation Technical Support.

### See also

[Select a FactoryTalk Directory to configure](#) on [page 197](#)

[Network directory and account access](#) on [page 197](#)

[Network directory and the FactoryTalk Directory Configuration Wizard](#) on page 198

[Local directory and account access](#) on page 199

[Product support for network and local directories](#) on page 201

## Select a FactoryTalk Directory to configure

The first step in configuring a FactoryTalk Directory is to select which FactoryTalk directory to configure from the first page in the **FactoryTalk Directory Configuration Wizard**.

### To select a FactoryTalk Directory to configure

1. Go to **Rockwell Software > FactoryTalk Tools > FactoryTalk Directory Configuration Wizard**.
2. In **FactoryTalk Directory Configuration Wizard**, under **Configure settings**, choose one or both of the following:
  - Configure the FactoryTalk Network Directory
  - Configure the FactoryTalk Local Directory
3. Select **Next**.

### See also

[Enter an administrator user name and password](#) on page 202

[Reset an expired password](#) on page 203

[Network directory and the FactoryTalk Directory Configuration Wizard](#) on page 198

[Local directory and the FactoryTalk Directory Configuration Wizard](#) on page 200

[Product support for network and local directories](#) on page 201

## Configure FactoryTalk Network Directory

To configure (or reconfigure) a FactoryTalk network directory or to upgrade an existing FactoryTalk network directory, logging on is required. This allows the **FactoryTalk Directory Configuration Wizard** to access the directory and configure it. To configure the FactoryTalk network directory, run the **FactoryTalk Directory Configuration Wizard** at the computer that is the FactoryTalk network directory server.



Tip: Configuring the FactoryTalk network directory from a remote computer is not allowed.

Depending on what accounts are available in the network directory, log on using:

- Any **Windows** administrator account that is a member of the local Windows administrators group on the computer where the FactoryTalk network directory server is located.

- Any **FactoryTalk** account that is a member of the FactoryTalk Administrators group in the network directory.

Log on using an existing FactoryTalk administrator account to reset the password of the account if it has expired. If your account has been locked or disabled, have another user whose account is a member of the FactoryTalk Administrators group enable the account or reset your password.

---

**IMPORTANT** Keep your administrator user name and password in a safe place. To enable the administrator account, both the original user name and password to the account are required. If either is lost, the account cannot be enabled.

---

If the administrator account is disabled, the **FactoryTalk Directory Configuration Wizard** cannot enable the account. Instead, have another user enable the account in FactoryTalk Administration Console. The last FactoryTalk administrator account in a directory cannot be disabled.

If no other user is available, or the password to another administrator account is not available (for example, because that user left the organization), contact Rockwell Automation Technical Support.

## See also

[Network directory and the FactoryTalk Directory Configuration Wizard](#) on [page 198](#)

[Reset an expired password](#) on [page 203](#)

[Change Password \(network\)](#) on [page 204](#)

[Summary](#) on [page 205](#)

FactoryTalk Directory Configuration Wizard

Running the FactoryTalk Directory Configuration Wizard to reconfigure the FactoryTalk network directory performs these operations:

- Backs up the original directory.  
The backup file is named **NetworkInstall\*.bak** and is located in **C:\ProgramData\Rockwell\RNAServer\Backups**. The location of the backup files is also logged to FactoryTalk Diagnostics. View the diagnostic log files using the FactoryTalk Diagnostics Viewer.
- Adds the Windows Administrators group to the FactoryTalk Administrators group, if an error occurred while you were installing or upgrading the FactoryTalk Services Platform on a computer for the first time, or if a valid administrator account could not be found.

This means that any user account that is a member of the local Windows Administrators group on any computer connected to the network directory has administrative access to the directory.

## Network directory and the FactoryTalk Directory Configuration Wizard

- Updates policies in the directory and adds the \$AnonymousLogon account to the directory, if an error occurred while upgrading an existing FactoryTalk Directory.

This account is given **Common > Read** and **Common > List Children** access to the FactoryTalk Directory. This account is used when FactoryTalk products require service access to the directory.

- Changes the password, if the password to a FactoryTalk account has expired, and the account is a member of the FactoryTalk Administrators group.
- Resets the account, if a FactoryTalk administrator account becomes locked.

### See also

[Configure FactoryTalk Network Directory](#) on [page 197](#)

[Reset an expired password](#) on [page 203](#)

[Change Password \(network\)](#) on [page 204](#)

[Summary](#) on [page 205](#)

## Configure FactoryTalk Local Directory

To configure (or reconfigure) a FactoryTalk local directory, or to upgrade an existing FactoryTalk local directory, logging on is required. This allows the **FactoryTalk Directory Configuration Wizard** to access the directory and configure it. Reconfiguring the FactoryTalk local directory allows you to reset the password of an expired administrator account.

Depending on what accounts are available in the local directory, log on using:

- Any **Windows** administrator account that is a member of the local Windows administrators group on the local computer.
- Any **FactoryTalk** account that is a member of the FactoryTalk Administrators group in the local directory.

Log on using an existing FactoryTalk administrator account to enable the account if it has become locked, or if the password to the account has expired. Alternatively, have another user whose account is a member of the FactoryTalk Administrators group enable the account or reset the password.

---

**IMPORTANT** Keep the administrator user name and password in a safe place. To enable the administrator account, both the original user name and password to the account are required. If either is lost, the account cannot be enabled.

---

If the administrator account was disabled, the **FactoryTalk Directory Configuration Wizard** cannot enable the account. Instead, have another user enable the account in FactoryTalk Administration Console. The last FactoryTalk administrator account in a directory cannot be disabled.

If no other user is available, or the password to another administrator account is not available (for example, because that user left the organization), contact Rockwell Automation Technical Support.

## See also

[Select a FactoryTalk Directory to configure](#) on [page 197](#)

[Local directory and the FactoryTalk Directory Configuration Wizard](#) on [page 200](#)

[Enter an administrator user name and password](#) on [page 202](#)

[Change Password \(local\)](#) on [page 203](#)

[Product support for network and local directories](#) on [page 201](#)

## Local directory and the FactoryTalk Directory Configuration Wizard

Running the FactoryTalk Directory Configuration Wizard to reconfigure the FactoryTalk local directory performs these operations:

- Backs up the original directory.

The backup file is named **LocalInstall\*.bak**, and is located in **C:\ProgramData\Rockwell\RNAServer\Backups**. The location of the backup files is also logged to FactoryTalk Diagnostics. Use FactoryTalk Diagnostics Viewer to view the diagnostic log files.

- Adds the Windows Administrators group to the FactoryTalk Administrators group if an error occurred while installing or upgrading the FactoryTalk Services Platform on a computer for the first time, or if a valid administrator account could not be found.

This means that any user account that is a member of the local Windows Administrators group on the local computer has administrative access to the directory.

- Adds the Windows Authenticated Users group to the local directory, allowing any user who is logged on to Windows to access the local directory.



Tip: The Windows Authenticated Users group includes all users and computers whose identities have been authenticated. The Authenticated Users group is used to override security in the local directory by granting access to all authenticated Windows user accounts. Authenticated Users does not include Guest even if the Guest account has a password.

- Updates policies in the directory, and adds the \$AnonymousLogon account to the directory, if an error occurred while upgrading an existing FactoryTalk Directory.

This account is given **Common > Read and Common > List Children** access to the FactoryTalk Directory. This account is used when FactoryTalk products require service access to the directory.



- Changes the password, if the password to a FactoryTalk account that is a member of the FactoryTalk Administrators group expires.
- Resets the account if a FactoryTalk administrator account becomes locked.

## See also

[Configure FactoryTalk Local Directory](#) on [page 199](#)

[Change Password \(local\)](#) on [page 203](#)

[Enter an administrator user name and password](#) on [page 202](#)

[Product support for network and local directories](#) on [page 201](#)

FactoryTalk Directory Configuration Wizard

## Product support for network and local directories

FactoryTalk® Directory allows products to share a common address book, which finds and provides access to plant-floor resources, such as data tags and graphic displays.

The FactoryTalk® Services Platform includes two separate directories: a local directory and a network directory.

- In a **local directory**, a Directory Server, all project information, and all participating software products are located on a single computer. Local applications cannot be shared across a network.
- A **network directory** organizes project information from multiple FactoryTalk® products across multiple computers on a network.

Which directory to configure depends upon which software products are part of the FactoryTalk system. The table below shows which products require a network directory, which require a local directory, and which use either directory.

Product	Network Directory	Local Directory
FactoryTalk® Administration Console	Yes	Yes
FactoryTalk® AssetCentre	Yes	No
FactoryTalk Batch	Yes	Yes
FactoryTalk Historian Classic	Yes	No
FactoryTalk Historian for Batch	Yes	No
FactoryTalk® Linx™	Yes	Yes
FactoryTalk® Linx™ Gateway	Yes	Yes
FactoryTalk Metrics	Yes	No
FactoryTalk® Portal	Yes	No
FactoryTalk® ProductionCentre®	Yes	No
FactoryTalk Scheduler	Yes	No
FactoryTalk® Transaction Manager	Yes	No
FactoryTalk® View Machine Edition (ME)	No	Yes
FactoryTalk® View Site Edition (SE)	Yes	No
FactoryTalk View SE Local	No	Yes

Logix Designer	Yes	No
RSAutomation Desktop®	Yes	No
RSBizWare™ BatchCampaign™	Yes	Yes
RSBizWare eProcedure®	Yes	Yes
RSLinx® Classic	Yes	Yes
RSLogix™ 5	Yes	Yes
RSLogix 500®	Yes	Yes
RSLogix 5000®	Yes	Yes*
RSMACC™	Yes	Yes
RSNetWorx™	Yes	Yes

\*The FactoryTalk local directory is not supported in RSLogix 5000 v20 software.

## See also

[Select a FactoryTalk Directory to configure](#) on [page 197](#)

## Enter an administrator user name and password

Enter a Windows Administrator account user name and password. If the user name and password are accepted, the directory is configured and the **FactoryTalk Directory Configuration Wizard** summary is displayed.

## Prerequisites

1. If not already on the second page of the **FactoryTalk Directory Configuration Wizard**, go to **Rockwell Software > FactoryTalk Tools >** and open **FactoryTalk Directory Configuration Wizard**.
2. In **FactoryTalk Directory Configuration Wizard**, select the directory you want to configure, and select **Next**.

## To enter an administrator user name and password

1. In **Administrator User Name**, enter a Windows Administrator account or FactoryTalk Administrator account user name.
2. In **Password**, enter the password that corresponds to the user name you entered.
3. Select **Next**.

## See also

[Select a FactoryTalk Directory to configure](#) on [page 197](#)

[Reset an expired password](#) on [page 203](#)

[Configure FactoryTalk Network Directory](#) on [page 197](#)

[Configure FactoryTalk Local Directory](#) on [page 199](#)

[Default passwords](#) on [page 206](#)

## Reset an expired password

When using the FactoryTalk Directory Configuration Wizard, if the password to the administrator account has expired, **Change Password** opens automatically. It cannot be opened manually.



Tip: Alternatively, use FactoryTalk Administration Console or FactoryTalk View Studio instead of the FactoryTalk Directory Configuration Wizard to change an account password.

### To reset an expired password

1. In **New password**, enter the new password for the administrator account.
2. In **Confirm new password**, enter the same password entered in **New password**, and select **OK**.

Depending on how the FactoryTalk security policies are configured, minimum password length and password complexity requirements might apply.

### See also

[Configure FactoryTalk Network Directory](#) on [page 197](#)

[Configure FactoryTalk Local Directory](#) on [page 199](#)

[Default passwords](#) on [page 206](#)

## Change Password (local)

The **Change Password** window appears automatically if the FactoryTalk local directory contains an administrator account with an expired password. There is no way to make this window appear manually if there is no administrator account with an expired password in the directory.

To change the password to an account manually, use FactoryTalk Administration Console instead of the FactoryTalk Directory Configuration Wizard.

If no other user is available and the password to the FactoryTalk administrator account has been lost or forgotten, contact Rockwell Automation Technical Support.

Setting	Description
Administrator user name	Displays the user name of the expired administrator account.
Old password	Displays asterisks (*) as a placeholder for the old password typed for the expired account.
New password	Type the new password to the account.

Confirm new password	<p>Type the same password as in the <b>New password</b> box.</p> <p>Depending on how the FactoryTalk security policies are configured, a minimum password length and password complexity requirements might apply. Check with the FactoryTalk administrator for specific requirements.</p> <p>If the new password is rejected, check that the new password:</p> <ul style="list-style-type: none"> <li>• Is not the same as any of the last 3 passwords used for the account</li> <li>• Does not contain all of the user account name. For example, a user account named John12 cannot have the password John1234. However, the password 12John is permitted. This check is also case sensitive so John12 could have the password jOHn12.</li> <li>• Is at least six characters long</li> <li>• Contains characters from three of the following four categories:             <ul style="list-style-type: none"> <li>• Unaccented uppercase characters (A to Z)</li> <li>• Unaccented lowercase characters (a to z)</li> <li>• Numerals (0 to 9)</li> <li>• Non-alphanumeric characters (!, @, #, %)</li> </ul> </li> </ul>
----------------------	--

---

**IMPORTANT** Keep a record of the administrator user name and password in a safe place. To enable the administrator account, you must have both the original user name and password to the account. If either is lost, the account cannot be enabled.

---

**See also**

[Configure FactoryTalk Local Directory](#) on [page 199](#)

[Summary](#) on [page 205](#)

[Default passwords](#) on [page 206](#)

**Change Password (network)**

When running the Configuration Wizard, if your administrator account has an expired password, **Change Password** appears automatically. There is no way to make this window appear manually if there is no administrator account with an expired password in the directory.

To change the password to an account manually, use FactoryTalk Administration Console or FactoryTalk View Studio instead of the FactoryTalk Directory Configuration Wizard.

If no other user is available and you cannot remember the password to your FactoryTalk administrator account, contact Rockwell Automation Technical Support.

Use the following settings to reset the password in your FactoryTalk network directory.

Setting	Description
Administrator user name	This box displays the user name you typed for the expired administrator account in the previous step of the wizard.
Old password	This box displays asterisks (*) as a placeholder for the old password you typed for the expired account in the previous step of the wizard.

New password	Type the new password to the account.
Confirm new password	<p>Type the same password you typed in the <b>New password</b> box.</p> <p>Depending on how the FactoryTalk security policies are configured, a minimum password length and password complexity requirements might apply. Check with your FactoryTalk administrator if the suggestions below do not work.</p> <p>If the wizard will not accept your new password, make sure that your new password:</p> <ul style="list-style-type: none"> <li>• Is not the same as any of the last 3 passwords you used for the account</li> <li>• Does not contain all of the user account name. For example, a user account named John12 cannot have the password John1234. However, the password 12John is permitted. This check is also case sensitive so John12 could have the password jOHn12.</li> <li>• Is at least six characters long</li> <li>• Contains characters from three of the following four categories: <ul style="list-style-type: none"> <li>• Unaccented uppercase characters (A to Z)</li> <li>• Unaccented lowercase characters (a to z)</li> <li>• Numerals (0 to 9)</li> <li>• non-alphanumeric characters (!, @, #, %)</li> </ul> </li> </ul>

If no other user is available and you cannot remember the password to your FactoryTalk administrator account, contact Rockwell Automation Technical Support.

## See also

[Reset an expired password](#) on [page 203](#)

[Configure FactoryTalk Network Directory](#) on [page 197](#)

[Summary](#) on [page 205](#)

[Default passwords](#) on [page 206](#)

## Summary

How do I open Summary?

Click **OK** in the second wizard screen--**Reconfigure a Network Directory** or **Reconfigure a Local Directory**.

When the FactoryTalk Directory Configuration Wizard finishes, **Summary** shows a list of what the FactoryTalk Directory Configuration Wizard did, together with any errors that might have occurred. These errors are also logged to FactoryTalk Diagnostics and can be reviewed using the FactoryTalk Diagnostics Viewer.

If an error occurred while running the FactoryTalk Directory Configuration Wizard, review the errors shown in **Summary**, and refer to the list of common errors below. After resolving the likely problems, run the wizard again.

Common causes for errors include:

- **Insufficient disk space.** Clear some disk space and then run the wizard again.
- **You are not logged on as an administrator.** You must be logged on as an administrator to run the FactoryTalk Directory Configuration Wizard. To run the wizard because an error occurred during installation for the first time on a computer, you must be logged on as a Windows local administrator.
- **The FactoryTalk Directory is in read-only mode.** This error applies to only the FactoryTalk network directory. This error appears as a warning when your computer cannot communicate with the FactoryTalk network directory server, or if the network connection is lost while configuring the directory. Make sure both your computer and the FactoryTalk network directory are connected to the network. You do *not* need to run the wizard again after reconnecting to the FactoryTalk network directory server.
- **You are attempting to configure the FactoryTalk Directory from a remote computer.** You cannot use Remote Desktop Services to configure a FactoryTalk Directory. You must configure a FactoryTalk local directory at the local computer. You must configure a FactoryTalk network directory at the computer that is the FactoryTalk network directory server.

## See also

FactoryTalk Directory Configuration Wizard

## Default passwords

If you are trying to configure a directory but you are being prompted for a password you don't have, this might be because you are upgrading from FactoryTalk Automation Platform version 2.00.

In version 2.00, you had to create passwords for FactoryTalk administrator accounts in both the network directory and the local directory.

To upgrade existing directories to FactoryTalk Services Platform version 2.10 or later, you must supply the original user name and password for the FactoryTalk administrator accounts.

- For the FactoryTalk local directory, the original default user name was Administrator, and the password field was left blank.
- For the FactoryTalk network directory, the original default user name was Administrator, but you were prompted to provide a password.

If you cannot remember the password to an existing directory, you cannot access that directory. Contact Rockwell Automation Technical Support.

## See also

[Enter an administrator user name and password](#) on [page 202](#)

[Reset an expired password](#) on [page 203](#)





## Upgrade FactoryTalk Services Platform

### Upgrade FactoryTalk Services Platform

In a distributed FactoryTalk System, all computers must run the same FactoryTalk Services Platform major release, referred to as Coordinated Product Release (CPR). While not required, Rockwell Automation also recommends that all computers run the same FactoryTalk Services Platform minor release and patch levels. For the latest compatibility information, refer to the Product Compatibility and Download Center.

During the upgrade, the installer automatically:

- Creates a backup file for any FactoryTalk Directory already configured on the computer.
- Updates existing Local Directory and Network Directories with support for new product policies, system policies, and features.
- Leaves existing settings unchanged, including user and group accounts, security settings, and policy settings.

### Prerequisites

- Obtain the installation disc of a FactoryTalk-enabled product  
or
- Obtain the standalone FactoryTalk Services Platform installation file downloaded from the Rockwell Automation Product Compatibility and Download Center.

### To upgrade FactoryTalk Services Platform

1. On the FactoryTalk Network Directory server, back up the FactoryTalk Directory.
2. (optional) Upgrade client computers:
  - s. Log in to the computer as a user in the **Windows Administrators** group.
  - t. Shut down all Rockwell Automation software products running on the computer.
  - u. Insert the product disc and select FactoryTalk Services Platform, or run the standalone FactoryTalk Services Platform installation file.
  - v. Once installation is complete, restart the computer.

3. Upgrade the FactoryTalk Network Directory server:
  - w. Log in to the computer as a user in the **Windows Administrators** group.
  - x. Shut down all Rockwell Automation software products running on the computer.
  - y. Disconnect the computer from the network, so client computers cannot connect during the upgrade.
  - z. Use **Windows Control Panel** to uninstall FactoryTalk Services Platform.
  - aa. Insert the product disc and select FactoryTalk Services Platform, or run the standalone FactoryTalk Services Platform installation file.
  - bb. Once installation is complete, restart the computer.
  - cc. Reconnect the computer to the network.

### See also

[Product Compatibility and Download Center](#)

[Back up a FactoryTalk Directory](#) on [page 160](#)

[Restore a FactoryTalk Directory](#) on [page 172](#)

Identify the installed FactoryTalk Services Platform version to determine if an upgrade of FactoryTalk Services Platform is necessary.

## Identify the installed FactoryTalk Services Platform version

### To identify the installed FactoryTalk Services Platform version

1. Open the Windows **Control Panel**.
2. Open **Add or Remove Programs**.
3. In the list of installed programs, FactoryTalk Services Platform appears, with the version number shown beside it.

## FactoryTalk Web Services

FactoryTalk Web Services allow web-enabled Rockwell Automation software products to access FactoryTalk services over a network using the Hypertext Transfer Protocol (HTTP) or the Hypertext Transfer Protocol over Secure Socket Layer (HTTPS).

The FactoryTalk Security Web Service allows clients to interact with the FactoryTalk Directory for authentication and authorization. The web service also provides support for products running in environments such as Linux and Java.

For details about using FactoryTalk Web Services with your FactoryTalk-enabled product, see your product documentation.

---

**IMPORTANT** If deploying FactoryTalk Web Services in an environment where privacy of the network communications might be at risk, add an HTTPS site binding to encrypt all client connections to FactoryTalk Web Services.

---

### See also

[Install FactoryTalk Web Services](#) on [page 211](#)

[Add an HTTPS site binding for FactoryTalk Web Services](#) on [page 212](#)

## Install FactoryTalk Web Services

FactoryTalk Web Services is installed from any FactoryTalk-enabled product CD that includes FactoryTalk Services Platform, version 2.10.02 (CPR 9 Service Release 2) or later. It is an optional component and is not installed automatically with FactoryTalk Services Platform.

For most applications, install FactoryTalk Web Services on the computer that is the FactoryTalk Network Directory server. Specific FactoryTalk-enabled products using FactoryTalk Web Services might also have additional installation requirements. For details, see the documentation supplied with your FactoryTalk-enabled product.

### To install FactoryTalk Web Services

1. Log on to the FactoryTalk Network Directory Server computer with a user account that is a member of the **Windows Administrators** group.
2. Go to the Windows **Control Panel** and open **Programs and Features**.
3. Select **FactoryTalk Services Platform**, then select **Change**.

4. Follow the instructions on the screen to modify the existing installation.
5. In the list of program features, click **FactoryTalk Web Services**, then click **This feature, and all subfeatures, will be installed on local hard drive**.
6. Click **Next**, then follow the instructions to finish the installation.

## See also

[Add an HTTPS site binding for FactoryTalk Web Services](#) on [page 212](#)

## Add an HTTPS site binding for FactoryTalk Web Services

If deploying FactoryTalk Web Services in an environment where privacy of the network communications might be at risk, add an HTTPS site binding to encrypt all client connections to FactoryTalk Web Services.

## Prerequisites

- Install FactoryTalk Web Services.
- Configure Internet Information Services (IIS) to use web server security.

## To add an HTTPS binding for FactoryTalk Web Services

1. On the FactoryTalk server, from **Control Panel**, select **Administrative Tools > Internet Information Services (IIS) Manager**.
2. From **Connections**, select **Default Web Site**.
3. From **Actions**, select **Bindings**.
4. In **Site Bindings**, select **Add**.
5. In **Add Site Binding**, specify the following the binding properties:
  - **Type:** Select **HTTPS**.
  - **IP Address:** Select **All Unassigned**.
  - **Port:** Enter **443**.
  - **SSL Certificate:** Select the SSL certificate for the FactoryTalk Web Services server.
6. Click **OK**, then click **Close**.
7. From **Connections**, select **FactoryTalk**.
8. In **/FactoryTalk Home**, double-click **SSL Settings**, select **Require SSL**, then select **Accept**.
9. From **Actions**, select **Apply**.

## See also

[Microsoft TechNet: Configure Web Server Security \(IIS 7\)](#)

## Client computers unable to connect to FactoryTalk Web Services

Possible cause and solution:

- Lack of network connectivity.

Check the network connection of the client computer and verify that it can connect to other network resources.

Check the network connection of the FactoryTalk Web Services host computer and verify that it can connect to network resources and accept inbound connections.

- Required software is not installed on the FactoryTalk Web Services host computer.

Verify Microsoft .NET Framework 4.8 is installed on the FactoryTalk Web Services host computer. If it is not installed, install it using the FactoryTalk Services Platform installation media.

Verify Internet Information Services (IIS) is installed on the FactoryTalk Web Services host computer. If it is not installed, install it using **Control Panel** (Windows) or **Administrative Tools** (Windows Server).

- Internet Information Services (IIS) is not listening on the default ports on the FactoryTalk Web Services host computer.

On the FactoryTalk Web Services host computer, open a browser and connect to the login URL:

**HTTP:**

<http://localhost:80/FactoryTalk/Security/WebService/200810.asmx>

**HTTPS:**

<https://localhost:443/FactoryTalk/Security/WebService/200810.asmx>

If the FactoryTalk Web Services page does not appear, IIS is either not running properly or is configured to listen on another port. Use IIS Manager to check the configuration and update client computer FactoryTalk Web Services paths to use a non-default port if necessary.

- The firewall on the FactoryTalk Web Services host computer does not allow incoming traffic on the ports configured in IIS Manager.

On the client computer, open a browser and connect to the login URL. Replace *server\_path* with the fully qualified domain name of the FactoryTalk Web Services host computer and replace the port number with the port number configured in IIS Manager:

**HTTP:**

[http://server\\_path:80/FactoryTalk/Security/WebService/200810.asmx](http://server_path:80/FactoryTalk/Security/WebService/200810.asmx)

**HTTPS:**

[https://server\\_path:443/FactoryTalk/Security/WebService/200810.asmx](https://server_path:443/FactoryTalk/Security/WebService/200810.asmx)

If the FactoryTalk Web Services page does not appear, verify that the firewall on the FactoryTalk Web Services host computer allows incoming traffic to the ports configured in IIS Manager.

## See also

FactoryTalk communications

[How to change the TCP port for IIS services](#)

## User cannot log into FactoryTalk Web Services

Possible cause and solution:

- User account does not have permission to log into FactoryTalk Web Services

1. On the FactoryTalk Web Services host computer, open a browser and connect to the login URL. Replace the port number with the port number configured in Internet Information Services (IIS) Manager:

**HTTP:**

`http://localhost:80/FactoryTalk/Security/WebService/200810.asmx`

**HTTPS:**

`https://localhost:443/FactoryTalk/Security/WebService/200810.asmx`

2. Select **Login**.
3. In **userName**, enter the user name for an account already configured in the FactoryTalk Network Directory.
4. In **password**, enter the password for the account.
5. In **encryptionAlgorithm**, type `ClearText` then click the **Invoke** button.

If the page returns an XML string, the user account is valid for use with FactoryTalk Web Services.

- User account has been disabled or locked in FactoryTalk Directory. Contact the FactoryTalk administrator to verify account status.

## See also

[Client computers unable to connect to FactoryTalk Web Services on page 213](#)

## Introduction to FactoryTalk Policy Manager and FactoryTalk System Services

### FactoryTalk Policy Manager and FactoryTalk System Services

Use FactoryTalk® Policy Manager to configure, deploy, and view the system communication security policies.

FactoryTalk Policy Manager divides the system security policy into different components.

Use these components to design security models that control the permissions and usage of devices within the system.

- Zones - Groups of devices.
- Devices - Computers, controllers, modules, HMI panels, and drives.
- Conduits - Communication routes between components.

FactoryTalk Policy Manager depends on FactoryTalk System Services for certificate services, policy deployment, and authentication.

FactoryTalk System Services provides these services on the FactoryTalk directory server:

- Authentication Service  
Authenticates users and validates user resource requests. Validate user credentials against the FactoryTalk Directory and FactoryTalk security policy settings to obtain privileges associated with the user.
- Certificate Service  
Issues and manages X.509v3 certificates for use within the FactoryTalk system.
- Deployment Service  
Translates the security policy model defined using FactoryTalk Policy Manager to CIP configurations that are delivered to endpoints.
- Diagnostics Service  
Makes FactoryTalk audit and diagnostic logs available as a web service.
- Policy Service  
Used to build and manage CIP network trust models and define security policy for the CIP endpoints.

FactoryTalk System Services provides the policy authority, certificate authority, identity services, and deployment services required to enforce

security policies configured using FactoryTalk Policy Manager that are based on the ODVA™ CIP Security™ standard.

CIP Security helps protect an EtherNet/IP connected device from malicious communications by:

- Applying authentication rules and rejecting messages sent by untrusted people or untrusted devices.
- Verifying that data has not been altered during transmission and reject data that fails the integrity check.
- Helps prevent viewing of EtherNet/IP data by unauthorized parties for additional confidentiality

CIP Security features work with these Rockwell Automation products:

- FactoryTalk Linx version 6.11 or later
- ControlLogix® 5580 Controllers version 32.00 or later
- 1756-EN4TR ControlLogix Module
- Kinetix® 5300 Drives
- Kinetix 5700 Drives
- PowerFlex® 755T
- 1783-CSP CIP Security Proxy

Creating and deploying a security model with FactoryTalk Policy Manager supports these core security properties

Property	Description
Device Identity	X.509v3 Digital Certificates are used to provide cryptographically secure identities to devices.
Device Authentication	TLS (Transport Layer Security) and DTLS (Datagram Transport Layer Security) cryptographic protocols are used to help provide secure transport of EtherNet/IP traffic.
Data Integrity	Hashes or HMAC (keyed-Hash Message Authentication Code) are used as a cryptographic method of providing data integrity and message authenticity to EtherNet/IP traffic.
Data Confidentiality	Data encryption is used to encode messages or information to help prevent reading or viewing of EtherNet/IP data by unauthorized parties.

**See also**

[Navigating FactoryTalk Policy Manager](#) on [page 218](#)

[FactoryTalk Policy Manager planning](#) on [page 220](#)

**Install FactoryTalk System Services and FactoryTalk Policy Manager**

FactoryTalk System Services and FactoryTalk Policy Manager are components of FactoryTalk Services Platform version 6.20.00. These components are used to manage CIP Security.



**IMPORTANT**

FactoryTalk Policy Manager is dependent upon FactoryTalk System Services and both components must be installed together on the network directory server.

## To install FactoryTalk System Services and FactoryTalk Policy Manager

1. Run FactoryTalk Policy Manager Setup.exe.
2. Follow the steps of the installation wizard.
3. (optional) Select **Customize** to add or remove components to install.
4. Select **Install**.
5. Agree to the EULA.
6. The installation proceeds.

## Start FactoryTalk System Services

After installation FactoryTalk System Services starts automatically. Some situations may require manually starting the services.

### To start the service

1. Go to the Windows **Services** snap-in (services.msc).
2. In the services list, scroll down to the **FactoryTalk System Services** item.
3. Right-click **FactoryTalk System Services** and select **Start**.

### See also

[Log on to FactoryTalk Policy Manager](#) on [page 217](#)

## Log on to FactoryTalk Policy Manager

Logging on to FactoryTalk Policy Manager checks the credentials of your user account to determine the access to resources and the ability to make changes to security policy.

### To log on to FactoryTalk Policy Manager

1. Open FactoryTalk Policy Manager  
The **FactoryTalk Log On** window opens.
2. In **Username**, type your FactoryTalk user name.
3. In **Password**, type your password.
4. Select **Show password** to display the password you typed. Not recommended if your workstation is easily viewed by others.
5. Select **LOG ON**.

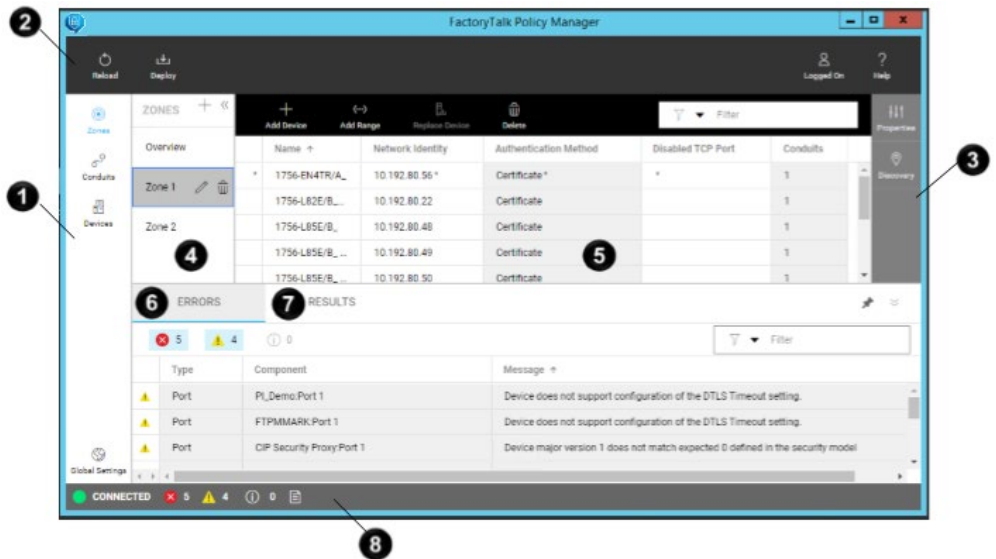
**IMPORTANT** FactoryTalk Policy Manager must be able to connect to FactoryTalk System Services to log in successfully. If FactoryTalk System Services is not running, the error message **FactoryTalk System Services Cannot Be Reached** displays when you try to log in. Select **EXIT POLICY MANAGER** to close the error message. To resolve this error, attempt to start FactoryTalk System Services.

**See also**

[Start FactoryTalk System Services](#) on [page 217](#)

**Navigate FactoryTalk Policy Manager**

FactoryTalk Policy Manager displays the different configurable items in a security policy model. The FactoryTalk Policy Manager Title Bar displays the current status of the model being configured. Models that are "saved" are local to the FactoryTalk Policy Manager database. Once they are deployed the status is not shown. If you make a change to a deployed model, the "Saved" status will display again until the changes made are deployed.



This table provides a reference to the items in the display:

Item	Description
1	FactoryTalk Policy Manager navigation bar. Use this bar to move between the different components of the security model. Also use to access <b>Global Settings</b> .
2	FactoryTalk Policy Manager main menu bar. Use to deploy security model, to log on or log off FactoryTalk, and to access Help and Release Notes.
3	FactoryTalk Policy Manager configuration bar. Use to edit the properties of existing components or to discover devices to add to the security model
4	Zones list. Displays all the zones configured in the model. Select a zone to edit the devices in the zone. Use the Zones list to quickly edit zone properties or delete zones.
5	Content pane. Displays a table that contains items that can be configured by either clicking the item in the table to directly edit the settings or by selecting the item and then selecting <b>Properties</b> from the configuration bar. Contains the FactoryTalk Policy Manager toolbar that contains the actions available for the items. Actions that are not displayed on the toolbar can be viewed by clicking the <b>More actions</b> icon (vertical ellipsis).
6	Errors pane. Displays the errors, warning, and information messages received from model validation and FactoryTalk System Services when the model is deployed. Errors can be filtered and sorted by message, type, and component.

Item	Description
7	Results pane. Displays the results of the last model deployment. The results can be saved to file for document retention.
8	Status bar. Displays the connection status to FactoryTalk System Services. Use the page icon to toggle the display of the deployment results and error pane.

**See also**

[FactoryTalk Policy Manager Global Settings](#) on [page 219](#)

**FactoryTalk Policy Manager  
Global Settings**

How do I open Global Settings?

- In the FactoryTalk Policy Manager navigation bar, select **Global Settings**.

Use **Global Settings** to define the settings that are applied to all devices contained in the model. FactoryTalk Policy Manager sends this information along with your certificate information to identify the different components and establish the trust relationships. We recommend completing the **Global Settings** information before using the certificate authentication method.

This table describes the settings:

Property	Descriptions
General	
• Model Name	The name of the security model managed by this instance of FactoryTalk Policy Manager.
Certificate Settings	
• Organization	The name of your organization.
• City/Locality	The legally registered location of your organization.
State/Province	If applicable, the State or Province in which your organization is using the certificate.
• Country	The country in which your organization operates.
Port settings	
• DTLS timeout	Enter a value between 1 and 3600 seconds. The default value is 12 seconds. If a device does not support the timeout functionality, a warning appears in the <b>Device Properties</b> pane.
Security Eventing Settings	
• Enable security eventing using Syslog server	When selected, FactoryTalk Policy Manager configures the devices in the security policy model to send Syslog messages. The devices send the messages to the specified server for storage using the chosen protocol. These settings apply to all devices that support security eventing.
• Server Settings	Use these settings to identify the location of the Syslog server.
IP Address.	Select to identify the Syslog server by IP address.
Hostname	Select to identify the Syslog server by DNS hostname.
Port number.	Identify the communications port on the server to receive the Syslog messages. Default port number is 514.
Protocol.	Select <b>UDP</b> for low-priority logging. UDP is not a guaranteed reliability protocol, log data that is transferred using UDP can be lost in transit due to various network problems. Select <b>TCP</b> for log data that cannot tolerate loss and which must be retained.

Property	Descriptions
<ul style="list-style-type: none"> <li>Filter Settings</li> </ul>	Use these settings to filter the event messages that are logged to the Syslog server.
Event types that will generate messages	<p><b>Failures only.</b> Select to log events upon failures related to model deployment, device discovery, component connections and component authentications or authentications.</p> <p><b>Failures and successes.</b> Select to log all success and failure events related to model deployment, device discovery, component connections and component authentications or authorizations.</p>
Lowest level of severity to log	<p>Log messages that are greater than or equal to the severity level selected. Defined severity levels from highest to lowest are:</p> <ul style="list-style-type: none"> <li><b>Emergency</b> - System is unusable.</li> <li><b>Alert</b> - Action must be taken immediately.</li> <li><b>Critical</b> - Critical operational conditions such as device hardware major faults.</li> <li><b>Error</b> - Error conditions in software applications and device hardware minor faults.</li> <li><b>Warning</b> - Warning conditions in software applications and hardware.</li> <li><b>Notice</b> - Significant conditions that may require special handling.</li> <li><b>Information</b> - Informational messages about software or hardware operations.</li> <li><b>Audit</b> - Messages from the auditing service.</li> <li><b>Debug</b> - Messages about the programmatic operations of the software.</li> </ul>
<ul style="list-style-type: none"> <li>Message Settings</li> </ul>	<p>Specify which details to include in the event log message.</p> <ul style="list-style-type: none"> <li><b>Sequence ID</b> - Uniquely identify the type and purpose of the message.</li> <li><b>Time quality</b> (sync info, time zone accuracy) - Describes the system time mechanism used by the message originator.</li> </ul>
<ul style="list-style-type: none"> <li>Time resolutions</li> </ul>	<p>Defines the level of precision used in the timestamp of the log messages.</p> <ul style="list-style-type: none"> <li><b>Seconds</b></li> <li><b>Milliseconds</b></li> <li><b>Microseconds</b></li> <li><b>Nanoseconds</b></li> </ul>

Changes made to these settings are saved after pressing ENTER or selecting another field.

**See also**

[Authentication methods](#) on [page 223](#)

[FactoryTalk Policy Manager component considerations](#) on [page 222](#)

[FactoryTalk Policy Manager planning](#) on [page 220](#)

**FactoryTalk Policy Manager planning**

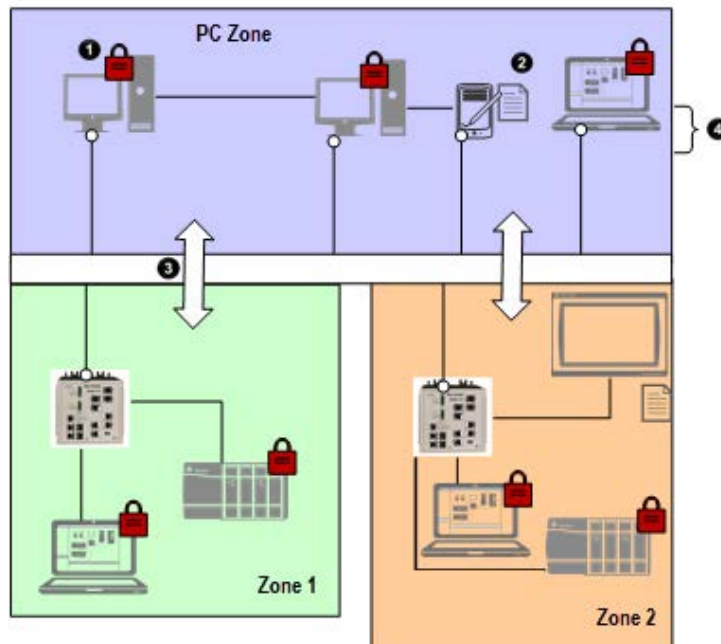
Implementing a CIP Security policy requires preparation and planning before deployment. At a minimum, gather this information:

- Number of zones.
- Security requirements for each zone.
- Devices assigned to each zone.
- Required trust relationships:

- Zones and devices
- Devices to devices
- IP Addresses of all devices to be included in the policy.

This diagram depicts a simple deployment consisting of three zones

- The PC Zone which contains mobile devices, servers, and administrative computers.
- Zone 1 which contains a switch, controller system, and administrative computer.
- Zone 2 which contains a switch, monitoring panel, controller system, programming system, and maintenance computer.
- The PC Zone is connected to both plant zones by separate conduits



Item	Description
①	Items with a lock are CIP Security capable.
②	Items with a list are not CIP Security capable and are trusted by their IP address.
③	Conduits connect the security zones enable secure communication between devices in different zones.
④	The zones are represented by different blocks. Each device within the block trusts the other devices in the block and can communicate with devices in zones that are connected by conduits.

### See also

[Zones](#) on [page 224](#)

[Conduits](#) on [page 225](#)

[Devices](#) on [page 227](#)

## FactoryTalk Policy Manager component considerations

When designing a security model using FactoryTalk Policy Manager consider these items.

- Devices.  
Identify which devices are included in the security model.
- Conduits.  
Identifies the communication pathways in the security model.  
Determine whether the pathways are zone-to-zone, zone-to-device, or device-to-device.
- Zones.  
Identifies a group of logical or physical devices to which security settings are applied.  
Devices within a zone trust each other.
- Pre-shared keys (PSK).  
A key based on a shared secret that is provided to devices to establish trust.
- Certificates.  
Used to establish a devices identity by providing information about ownership of a public key.
- Security options  
When a certificate is used as the authentication method additional security checks are available to be used with messaging and I/O data.
  - **Integrity Only**  
Checks whether data was altered and whether the data was sent by a trusted entity. Altered and/or untrusted data is rejected.
  - **Integrity & Confidentiality**  
Checks integrity and encrypts the data so the corresponding decryption key is required to read the data. Rejects altered and/or untrusted data.
- Devices that cannot support CIP Security.  
Some devices do not support CIP Security and cannot authenticate themselves to the system. Decide how these devices will be included in the system. There are two approaches:
  - Use a CIP Proxy device. A CIP Proxy device can be placed in front of the non-CIP securable device. The CIP Proxy device controls the communication to the device it proxies and can sign and encrypt data from the device.
  - Use a trusted IP address. The device is assigned an IP address that is trusted by the system and permitted to communicate within the security zone. However, these devices are not able to sign or encrypt communications.

Use FactoryTalk Policy Manager to combine these components into a security policy model to deploy to your FactoryTalk system.

**See also**

[Zones](#) on [page 224](#)

[Conduits](#) on [page 225](#)

[Devices](#) on [page 227](#)

**Authentication methods**

FactoryTalk Policy Manager supports these authentication methods:

Name	Description
Certificate	Established by the use of an X.509v3 certificate granted by a trusted certificate authority.
Pre-shared key	Established by presentation of a shared secret key that is propagated to trusted devices in the system. A pre-shared key can be created manually or FactoryTalk Policy Manager can automatically generate pre-shared keys for distribution to the devices in your system.
Trusted IP	Established by identifying an IP address as trusted by the security model. A set of IP addresses can be defined as a trusted range on your network. Appropriate for use with devices that are not CIP Security capable.

**Ingress/Egress rules**

The Ingress/Egress Object is a set of rules that govern which network nodes can communicate to the device and through the device:

- Ingress Rules determine which other nodes can communicate with this device.
- Egress rules determine how the device can communicate with other nodes.

To learn more about the Ingress/Egress rules, visit the ODVA website.

**See also**

Zone properties

Conduit properties

Device properties

**Security Groups**

FactoryTalk Services Platform includes these built-in security groups that are used to define rights and privileges for users.

FactoryTalk Policy Manager users can be granted the following rights:

Right	Group	Permissions
View	Administrator Engineers Maintenance	All security policy artifacts and global settings are read-only. <b>Login/Logout</b> is active on the main toolbar. <b>Help</b> is active on the main toolbar.
Edit	Administrator	All security policy items and global settings can be modified. Zones can be added, edited or deleted. Conduits can be added, edited or deleted. Devices can be added, discovered, edited or deleted. Ethernet ports can be added and configured. Trusted IP ranges can be added and configured. Security policy models can be deployed. All controls are active.
Deploy	Administrator Engineers Maintenance	The security policy can be deployed to devices. Devices can be replaced in the security model. Security policy items and global settings are read-only. <b>Deploy</b> is active on the main toolbar. <b>Replace Device</b> is active on the zone toolbar. <b>Replace Device</b> is active on the device toolbar.

The controls available in FactoryTalk Policy Manager reflect the user rights granted to the logged in user account.



Tip: If you are logged on using an Administrator account but FactoryTalk Policy Manager is only permitting viewing of devices, zones, and conduits, verify that the FactoryTalk Directory services are running and that the computer is connected to the FactoryTalk Directory.

**See also**

Read-only mode

[Devices](#) on [page 227](#)

Deployment

**Zones**

Zones are security policy groups to which devices are assigned. Once a device is assigned to a zone, the device uses the policy default settings of that zone.

Zones establish the rules for data integrity, data privacy, and the authentication method used to authenticate trusted devices. When configuring a zone, use the **CIP Security Communication** settings within the zone properties to establish these controls:

- Authentication method
- I/O data security
- Messaging security
- Port usage

**See also**

[Add a zone](#) on [page 225](#)



Edit zone properties

Delete a zone

Zone properties

Configure port properties

## Add a zone

Add zones to establish areas of security policy. Devices assigned to the zone trust each other. Edit the zone properties to enable CIP Security and configure the related settings. CIP Security is not enabled by default.

### To add a zone

1. In the FactoryTalk Policy Manager navigation bar, select **Zones**.
2. On the toolbar next to **ZONES**, select **Add [+]**.

Adds a new zone to the list with these default values:

- **Name** - Zone #
- **Description** - None
- **Enable CIP Security** - Not selected by default.

Select to enable configuration of CIP Security related settings.

### See also

Zone properties

Edit zone properties

Delete a zone

## Conduits

Conduits create trusted communication pathways outside of zones. Conduits require two endpoints, such as:

- Two different zones.
- Two different devices.
- A zone and a device.

Conduits support two authentication methods:

- Trusted IP

Trusted IP assigns a trust relationship to an asset based on its IP address.

- Certificate

Certificate authentication methods establish the identity of the device through the use of a certificate from a trusted authority. This enables configuration of integrity and confidentiality options for communication over the conduit using the public key associated with the certificate.

---

**IMPORTANT** If an endpoint is a zone and the conduit uses certificate authentication, devices in that zone that don't support CIP Security will not use the certificate for communication. The CIP Security capable devices will trust the non-CIP Security devices using Trusted IP.

---

## See also

[Add a conduit](#) on [page 226](#)

Edit conduit properties

Delete a conduit

Conduit properties

## Add a conduit

Add a conduit to connect two endpoints. Endpoints can be either a device or a zone.

Conduits must adhere to these rules:

- Each combination of endpoints must be unique.
- Duplicate conduits are not permitted.
- One of the endpoints must be CIP Security capable.
- If one endpoint is a zone, the other endpoint cannot be a device within that zone.

## To add a conduit

1. In the FactoryTalk Policy Manager navigation bar, select **Conduits**.
2. On the toolbar, select **Add [+]**.

**CONDUIT PROPERTIES** pane opens.

3. In **Endpoint 1**, next to **Select an endpoint** select **Browse for Endpoint [...]**. **Select Endpoint** opens.
4. Choose a zone or device to assign as the first endpoint of the conduit.



Tip: In **Filter**, type part of the name to list only endpoints that match that criteria.

After selecting the endpoint, select **OK**.

5. In **Endpoint 2**, next to **Select an endpoint** select **Browse for Endpoint [...]**. **Select Endpoint** opens.

After selecting the endpoint, select **OK**.

6. Choose a zone or device to assign as the second endpoint of the conduit.
7. Select **Next** to create the conduit.

The conduit is created and its properties can be configured as needed.

**See also**

Conduit properties

Edit conduit properties

Delete a conduit

**Devices**

Devices are the modules, drives, controllers, HMI panels, computers, CIP Proxy devices, and servers that work together to create a FactoryTalk system. Add devices that share security requirements and that should trust each other to a zone. A device can have one or more ports that are added to the security model. Devices can be added manually or discovered by querying the network for devices.

Devices are connected to other devices or zones by conduits.

**See also**

[Discover devices](#) on [page 227](#)

[Add a device to a zone](#) on [page 227](#)

Add a device to the device list

Configure port properties

[Remove the security policy from a device](#) on [page 231](#)

**Discovery**

Use **Discovery** to traverse your system and find devices. Devices found in discovery can be added to the device list and assigned to zones. Discovery can be useful for populating a list of devices or for checking that the devices added to the list manually are accurately identified.

**See also**

Discovery pane

Discover devices

Navigate the Discovery pane

Perform a search from the Discovery pane

Add drivers from the Discovery pane

**Add a device to a zone**

Add a device to a zone to include it in the FactoryTalk Policy Manager security model. Alternatively, use discovery to find devices on the network. If you are using a CIP Proxy device, there are two ways in which devices are added to the model:

- Add the *proxy device*, then identify the device that is being proxied.

- Add the *proxied device*, which automatically detects and adds the proxy device.

## To add a device

1. In the FactoryTalk Policy Manager navigation bar, select:
  - **Zones** and then select a zone in the **Zones** table to add a device to the selected zone's device list.
  - **Devices** to add a device. By default the device is unassigned.
2. On the toolbar, select:
  - **Add Device [+]** to manually add a device to the current device table by selecting its catalog number or to add a generic device.
  - **Discovery** to select and add devices **[+]** found on the network to the current device table.

**Tip:**


  - To add a device you can also:
    - Drag and drop a device from Discovery to the device table.
    - Use the Add command from the context menu in Discovery.
    - When you add a proxy device you are prompted to select a proxied device.

**DEVICE PROPERTIES** opens.

3. (optional) In **Device Name**, type a name for the device. Generic devices are automatically named Device <number>. Devices selected by catalog number or discovered are already named.
4. (optional) In **Description**, type a description of the device. The description of generic devices is empty by default. Devices selected by catalog number or discovered may have an existing description.
5. For generic devices, in **Catalog Number**, select the ellipsis [...] and choose the catalog number for the device from the list.
 

**Tip:** Filter the list of catalog numbers by typing a portion of the catalog number in the space provided.
6. (optional) In **Vendor**, type the name of the device manufacturer. If a Rockwell Automation/Allen-Bradley catalog number was provided, this setting is completed by default and cannot be modified.
7. In **Firmware Revision**, choose the applicable firmware revision. This setting is required to apply CIP Security settings to the device ports. FactoryTalk Policy Manager automatically assigns the latest firmware version to devices added using a catalog number or using Discovery.
8. (optional) Enable **CIP Security capable** if the device supports CIP Security. It is not possible to change this setting after deploying the security policy model.

CIP Security is associated with the **Catalog Number** and **Firmware Revision** properties. When both values are known the **CIP Security capable** setting is automatically enabled or disabled and is not editable.

9. Under **Ports** select the pencil icon  next to the port to configure port properties, such as the port name, description, EtherNet driver name, IP address, and protocols used by the device.

**See also**

Configure port properties

Edit device properties

Delete a device

Device properties

[Replace a device](#) on [page 230](#)

**FactoryTalk Linx devices**

The **CIP Security** tab of the FactoryTalk Linx server workstation can be used to view CIP security status and reset CIP security to clear CIP security configuration.

These are the settings on the **CIP Security** tab of the **Device Properties** dialog box.

Setting	Description
CIP Security Configuration	Shows the FactoryTalk Linx workstation CIP security configuration status. <b>Configured</b> Means the FactoryTalk Linx workstation is configured to utilize CIP security with FactoryTalk Policy Manager. <b>Factory Default / Disabled Settings</b> Means the FactoryTalk Linx workstation CIP security configuration has been cleared. All security settings is now in Factory default mode (CIP Security is disabled). <b>Reset CIP Security permission required.</b> Means the logged on user doesn't have the security permission to reset CIP security configuration. Go to <b>System &gt; Policies &gt; Product Policies &gt; FactoryTalk Linx &gt; Feature Security</b> to obtain the permission.
Reset CIP Security	Click this button to clear CIP security configuration for the FactoryTalk Linx workstation.

Use FactoryTalk Policy Manager to configure, deploy, and view the FactoryTalk system CIP security policy configuration that includes FactoryTalk Linx servers.

**Ports**

A port represents a physical socket of a device that allows communication with another device using CIP Security.

FactoryTalk Linx Devices, CIP Proxy devices and Rockwell Automation devices that are identified by catalog number have only a single port.

CIP Proxy devices and proxied devices have an additional section in PORT PROPERTIES indicating the paired device.

Add ports to Generic Devices to add them to the security policy model.

## See also

[Add a port](#) on [page 230](#)


Configure port properties

Port properties


## Add a port

Generic devices can have ports added to them to match their configuration.

### To add a port

1. In the FactoryTalk Policy Manager navigation bar, select **Devices** to and then select a generic device from the FactoryTalk Policy Manager device list.
2. In the **PORT PROPERTIES** pane, select the pencil icon  next to the device name to open the **DEVICE PROPERTIES** pane.
3. Under **Ports** select the plus [+] icon.

A new port adds to the **Ports** list.

4. Select the pencil icon  next to the port number to configure port properties, such as the port name, description, EtherNet driver, IP address, and protocols used by the device.

## See also

Configure port properties

Port properties

## Replace a device

Replacing a device is used when a device that has already been configured and enabled for CIP Security has failed or needs to be rotated out for maintenance. Device replacement enables the identity and the security configuration of the previous device to be assigned to the replacement device. The communications port on a device must be reset after replacement to apply the security policy settings.

### To replace a device

1. In the FactoryTalk Policy Manager navigation bar, select:
  - **Zones** and then select a zone in the **Zones** table to replace a device on the selected zone's device table.
  - **Devices** to replace any device on the FactoryTalk Policy Manager device list.
2. In the device table, select the name of the device to replace.

The selected device properties display in **DEVICE PROPERTIES**.

3. On the FactoryTalk Policy Manager toolbar, select **Replace Device**. **Deploy Configuration to Replace Device** displays.
4. In **Deploy Configuration to Replace Device** choose when to reset the communication ports on the device:
  - Choose **During policy deployment** to reset the ports automatically as part of the replacement process.
  - Choose **After deployment** to manually reset the ports at a later time. The security policy is not being enforced on the device until the ports are reset.
5. Select **Deploy**. Deployment results are displayed as the deployment occurs.

### See also

Deployment results

## Remove the security policy from a device

If the security model has been deployed and the device communications have been reset the device is constrained by the security policy. Even if FactoryTalk Policy Manager and FactoryTalk System Services are uninstalled the security policy configured for the device is still in effect.

Use these steps to remove the security policy if necessary.

### To remove the security policy from a device

1. In the FactoryTalk Policy Manager navigation bar, select **Devices** and then select the device. **PORT PROPERTIES** are displayed.
2. In the **Policies** area, change the security policies for the device.
  - In **Zone**, choose either **Unassigned** or a zone that is not CIP Security enabled.
3. Deploy the security model and choose to reset the communications channels **During deployment**.

The device security configuration will be reset to none.

The device can then be removed from the model or reconfigured as necessary.



Tip: You can remove the security policy from the device by deleting the device from the security policy model. The changes take place during the next deployment.

### See also

Edit device properties

Delete a device

[Deploy a security model](#) on [page 233](#)

## Ranges

If there are groups of devices that are not CIP Security capable, they can be incorporated into the security model using a trusted IP range.

A trusted IP range is a contiguous set of IP addresses that are known to contain good devices, but that cannot use certificates or pre-shared keys to authenticate identities or authorize access.

When a device has an IP address within a defined trusted IP range, the authentication method for the device is set to **None**.

### See also

[Add a range](#) on [page 232](#)

[Authentication methods](#) on [page 223](#)

## Add a range

Add a range to define a set of IP addresses to assign to a zone. A device range is useful for devices that do not support CIP Security, but that need to be part of the security policy model.

### To add a range

1. In the FactoryTalk Policy Manager navigation bar, select:
  - **Zones** and then select a zone in the **Zones** list to add a device range to the selected zone's device list.
  - **Devices** to add an unassigned device range to the FactoryTalk Policy Manager device list.
2. On the toolbar, select **Add Range**. The **RANGE PROPERTIES** pane opens.
3. In **Name**, type a name for the range.
4. (optional) In **Description**, type a description of the range.
5. In **Start IP Address**, type the first IP address in the range being defined.
6. In **End IP Address**, type the last IP address in the range being defined.
7. (optional) In **Zone**, select the security zone to assign to this range. If adding a range from within the **Zone** list, the range is automatically assigned to the currently selected zone.

### See also

[Discovery](#) on [page 227](#)

[Add a zone](#) on [page 225](#)



## Range properties

**Deploy a security model**

After the zones, conduits, and devices have been configured, the security policy model can be deployed.

Before a deployed security policy becomes active, communications must be reset to all configured devices, resulting in a short loss of connectivity. During deployment, there is the option of resetting the communication as part of deployment, or deploying the changes without resetting the communication channel so that the reset can occur at a different time than the deployment process.

Once the model is deployed and communications reset on the device, the device will only accept communications from other devices in the same zone or using conduits configured to enable communications with other security zones or devices. The device can still send communication to other devices.

Before deploying a security model, make sure that all devices are operational and have network access.

If changes are made the policy after it is deployed, an asterisk (\*) will appear next to the device, indicating that the configured policy has not been deployed to that device.

You can perform a differential deployment to only deploy the security configuration to devices that have been changed since last deployment. This type of deployment would include any changes made in the model configuration or changes made to the physical device, such as when a device is replaced for maintenance.

**To deploy a security model**

1. On the FactoryTalk Policy Manager toolbar, select **Deploy**.
2. Review the **Deploy** dialog:
  - dd. In **Deployment scope** choose whether to perform a full deployment or a differential deployment.
    - Select **Changed device communication ports only** for differential deployment.
    - Select **All device communication ports in the model** for full deployment.
  - ee. The list of devices identifies the devices that will be configured when this model is deployed. Scroll down or select **More details** to review the list.



Tip: The list may contain devices that you have not modified directly. This can happen modification of one device impacted a related device. If the list contains unexpected devices, select **CANCEL** and then change the model as needed.

- ff. Choose when to reset the communication channels for the items includes in the security policy model.
- **During policy deployment**  
When this option is selected, the communication port will be closed and re-opened on the device during the deployment process. Similar to resetting the network card on a computer, the device stays functional but is disconnected from the network for a few moments. Using this option applies the new policy to the device at the same time that the policy is deployed.
  - **After deployment**  
When this option is selected, the security policy settings will be deployed to the device but are not in effect. The communications ports will need to be reset before the security policy will be used. This option is useful if there is a scheduled maintenance reset process in your environment that can be relied upon to perform this function.
- gg. Select **DEPLOY**.
3. The **Results** pane updates with the results of the deployment as it occurs.  
Once deployment is complete a summary report is provided listing the successes, failures, and errors encountered during the process.

### See also

[Devices](#) on [page 227](#)

[Conduits](#) on [page 225](#)

[Zones](#) on [page 224](#)

Deployment results

Create backup files to preserve and restore the security models for your system in case of a systems failure.

These are the considerations related to using backup and restore with FactoryTalk Policy Manager:

- The FactoryTalk Policy Manager security model is stored by FactoryTalk System Services in a policy database.
- Create a backup after a policy deployment to keep the backup files synchronized with the current security policy.

### See also

FactoryTalk System Services

## Backup and restore security models

[Deploy a security model](#) on [page 233](#)

## Backup FactoryTalk System Services

Backup FactoryTalk System Services to save copy of the the security model and its associated certificates. After it has been created the FactoryTalk System Services backup file is included with the FactoryTalk Services Platform backup when it is performed.

---

**IMPORTANT** Backing up FactoryTalk System Services requires administrator privileges.

---

### To backup FactoryTalk System Services databases

1. Open a command prompt as an Administrator.
2. In the command prompt window type :  

```
cd C:\Program Files (x86)\Rockwell
Software\FactoryTalk System Services.
```
3. Run the backup utility by typing one of these commands:
  - `FtssBackupRestore -B`  
Creates a plain text backup of the data.
  - `FtssBackupRestore -B -P "password"`  
or
  - `FtssBackupRestore -B -P password`  
Creates an encrypted backup of the data using the password supplied after the `-P` parameter. Quotation marks are optional. This password must be supplied to restore the data.
4. The file `backup.zip` file is created. This file will be included in the FactoryTalk Services Platform Backup.

Verify the file is present in this location:

```
C:\ProgramData\Rockwell\RNAServer\Global\RnaStore\FTS
S_Backup
```



Tip: The **ProgramData** folder is hidden by default in Windows File Explorer.

### See also

[Backup and restore security models](#) on [page 234](#)

[Restore FactoryTalk System Services](#) on [page 235](#)

## Restore FactoryTalk System Services

Restore FactoryTalk System Services to return the FactoryTalk System Services databases to a known good state.

---

**IMPORTANT** Restoring FactoryTalk System Services requires administrator privileges.

---

## To restore FactoryTalk System Services databases

1. Verify the **backup.zip** file is present in this location:  
C:\ProgramData\Rockwell\RNA Server\Global\RnaStore\FTSS\_Backup
2. Open a command prompt as an Administrator.
3. In the command prompt window type :  
cd C:\Program Files (x86)\Rockwell Software\FactoryTalk System Services.
4. Run the FactoryTalk System Services Backup & Restore Utility by typing one of these commands:
  - FTSSBackupRestore -R  
Restores a plain text backup of the databases.
  - FTSSBackupRestore -R -P "password"
  - or
  - FTSSBackupRestore -R -P password  
Restores an encrypted backup of the databases that is decrypted using the password supplied after the -P parameter. Quotation marks are optional.

### See also

[Backup and restore security models](#) on [page 234](#)

# Index

## A

**accounts** 16, 18, 45, 46, 47, 52, 55, 78, 92  
     administrator 34, 39, 196, 198, 202, 204  
     computer 181  
     user 13, 20, 22, 29, 31, 32, 34, 36, 45  
**action groups** 67, 68, 69, 135, 149, 152  
**actions** 20, 29, 36, 67, 68, 69, 212  
**after restoring** 170, 181  
**allow and deny permissions** 135, 154  
**application** 13, 20, 29, 31, 73, 76, 78, 124, 129, 130  
**application authorization policy** 73  
**area** 20, 29, 124, 129, 130, 131, 135  
**audit policies** 86, 91

## B

**back up** 68, 78, 79, 170  
**best practices** 34

## C

**chain of inheritance** 135  
**client computer** 22, 38, 39, 91, 110, 209  
**common actions** 135  
**computer account** 60, 61, 181

## D

**devices** 13, 20, 82, 122, 124, 129, 130, 133, 135

## E

**effective permissions** 135, 154

## G

**groups** 20, 34, 46, 47, 52, 55, 56, 67, 81, 129, 130, 131, 183

## I

**inheritance** 135, 154

## L

**list children** 45, 46, 52, 55, 56, 60, 61, 67, 68, 69, 112, 124, 130, 131, 198  
**local applications** 20, 22, 201

## M

**multiple applications** 15, 170

## N

**networks** 119, 122, 124, 129, 130, 133, 135

## O

**order of precedence** 34, 139

## P

**permissions** 20, 22, 29, 31, 32, 34, 46, 47, 52, 55, 56, 60, 61, 67, 68, 69, 78, 79, 86, 112, 114, 119, 122, 124, 129, 130, 131, 135, 139, 149, 152, 154  
**policies** 13, 20, 22, 29, 31, 36, 71, 78, 79, 82, 86, 87, 91, 92, 99, 100, 109, 110, 111, 112, 113, 114, 135, 185, 198, 204, 209  
**ports** 214

## R

**read** 29, 135, 139, 154, 198  
**resource groups** 129, 130, 131, 133, 135  
**resources** 29, 38, 39, 45, 52, 63, 68, 87, 124, 129, 130, 131, 133, 135, 196, 201  
**restore** 68, 78, 79, 159, 170, 181, 184, 185, 193  
**runtime security** 29

## S

**security authority identifier** 78, 79, 170  
**server** 13, 15, 20, 22, 38, 39, 40, 73, 78, 79, 82, 109, 110, 135, 139, 184, 201, 209, 211, 212  
**single sign-on** 39, 91, 99, 100, 109, 110  
**stand-alone system** 15, 22, 31  
**system folder** 13, 78, 79, 135, 170, 183

## T

**tag actions** 15, 196, 201  
**test** 82, 154  
**tighten security** 31

**troubleshoot 82, 86**

**U**

**upgrade 82, 185, 196, 206, 209, 210**

**user rights assignment 78, 79**

**W**

**write 20, 29, 46, 55, 56, 60, 61, 63, 67, 68,  
69, 87, 135, 149**

# Rockwell Automation support

Use these resources to access support information.

<b>Technical Support Center</b>	Find help with how-to videos, FAQs, chat, user forums, and product notification updates.	<a href="http://rok.auto/support">rok.auto/support</a>
<b>Knowledgebase</b>	Access Knowledgebase articles.	<a href="http://rok.auto/knowledgebase">rok.auto/knowledgebase</a>
<b>Local Technical Support Phone Numbers</b>	Locate the telephone number for your country.	<a href="http://rok.auto/phonesupport">rok.auto/phonesupport</a>
<b>Literature Library</b>	Find installation instructions, manuals, brochures, and technical data publications.	<a href="http://rok.auto/literature">rok.auto/literature</a>
<b>Product Compatibility and Download Center (PCDC)</b>	Get help determining how products interact, check features and capabilities, and find associated firmware.	<a href="http://rok.auto/pcdc">rok.auto/pcdc</a>

## Documentation feedback

Your comments help us serve your documentation needs better. If you have any suggestions on how to improve our content, complete the form at [rok.auto/docfeedback](http://rok.auto/docfeedback).

## Waste Electrical and Electronic Equipment (WEEE)



At the end of life, this equipment should be collected separately from any unsorted municipal waste.





Rockwell Automation maintains current product environmental information on its website at [rok.auto/pec](http://rok.auto/pec).

Allen-Bradley, expanding human possibility, Logix, Rockwell Automation, and Rockwell Software are trademarks of Rockwell Automation, Inc.

EtherNet/IP is a trademark of ODVA, Inc.

Trademarks not belonging to Rockwell Automation are property of their respective companies.

Rockwell Otomasyon Ticaret A.Ş. Kar Plaza İş Merkezi E Blok Kat:6 34752, İçerenköy, İstanbul, Tel: +90 (216) 5698400 EEE Yönetmeliğine Uygundur

Connect with us.    

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

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444

EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640

ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846