### Table of contents

#### Preface
- About this publication ................................................................. 9
- Additional resources ........................................................................ 9

#### Chapter 1
**About FactoryTalk systems**
- About FactoryTalk systems .............................................................. 11
  - FactoryTalk Directory types ......................................................... 13
  - Accounts and groups ..................................................................... 15
  - Account types .................................................................................. 16
  - Applications and areas ................................................................. 19
  - Security in a FactoryTalk system .................................................... 19
  - Example: Two directories on one computer .................................... 20

#### Chapter 2
**Install FactoryTalk Services Platform**
- Install FactoryTalk Services Platform ............................................. 23

#### Chapter 3
**Getting started with FactoryTalk Security**
- About FactoryTalk Security ............................................................. 25
  - Security on a local directory .......................................................... 27
  - Security on a network directory ..................................................... 27
  - How security authenticates user accounts ....................................... 28
  - Things you can secure ................................................................. 28
  - Best practices .................................................................................. 31
  - Audit trails and regulatory compliance .......................................... 32
- Configure a computer to be the FactoryTalk Directory network server ................................................................................. 34
  - Configure a computer to be the network directory server ............... 35
  - Configure a network directory client computer ............................. 36
  - Check network directory server connection status ......................... 36
  - FactoryTalk Directory Server Location Utility ............................... 37

#### Chapter 4
**Manage users**
- Manage users .................................................................................. 39
  - Add a FactoryTalk user account ..................................................... 39
  - Add a Windows-linked user account .............................................. 41
  - Add group memberships to a user account .................................... 42
  - Remove group memberships from a user account ......................... 43
  - Delete a user account .................................................................. 44
Chapter 5

Manage user groups

- Manage user groups ......................................................... 47
  - Add a FactoryTalk user group ........................................... 47
  - Add a Windows-linked user group .................................. 49
  - Edit or view user group properties .................................. 50
  - Delete a user group ....................................................... 52
  - Add accounts to a FactoryTalk user group ....................... 52
  - Remove accounts from a FactoryTalk user group ............. 53

Chapter 6

Manage computers

- Manage computers ........................................................... 55
  - Add a computer ............................................................ 55
  - Delete a computer ........................................................ 56
  - Edit or view computer properties .................................... 57

Chapter 7

Add and remove user-computer pairs

- Add and remove user-computer pairs ................................. 59
  - Add a user-computer pair .............................................. 59
  - Remove a user-computer pair ........................................ 60
  - Edit or view user account properties ............................... 60

Chapter 8

Add and remove action groups

- Add and remove action groups ........................................... 63
  - Add an action group ..................................................... 63
  - Delete an action group ................................................ 64
  - Add an action to an action group ................................. 65
  - Remove an action from an action group ....................... 66

Chapter 9

Set system policies

- Authorize an application to access the FactoryTalk Directory......................................................... 68
  - FactoryTalk Service Application Authorization ......................... 69
  - FactoryTalk Service Application Authorization settings ....................... 69
  - Publisher Certificate Information ...................................... 71
  - Digitally signed FactoryTalk products .............................. 72
  - Assign user rights to make system policy changes .................. 72
    - User rights assignment policies .................................. 73
    - User Rights Assignment Policy Properties ...................... 74
    - Configure Securable Action ........................................ 75
    - Select a user or group .............................................. 76
    - Change the default communications protocol ................... 77
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default communications protocol settings</td>
<td>77</td>
</tr>
<tr>
<td>Live Data Policy Properties</td>
<td>78</td>
</tr>
<tr>
<td>Set network health monitoring policies</td>
<td>79</td>
</tr>
<tr>
<td>Health Monitoring Policy Properties</td>
<td>80</td>
</tr>
<tr>
<td>Health Monitoring Policy Properties settings</td>
<td>81</td>
</tr>
<tr>
<td>Set audit policies</td>
<td>81</td>
</tr>
<tr>
<td>Audit policies</td>
<td>83</td>
</tr>
<tr>
<td>Audit Policy Properties</td>
<td>84</td>
</tr>
<tr>
<td>Monitor security-related events</td>
<td>86</td>
</tr>
<tr>
<td>Example: Audit messages</td>
<td>86</td>
</tr>
<tr>
<td>Set system security policies</td>
<td>87</td>
</tr>
<tr>
<td>Modify account policy settings</td>
<td>88</td>
</tr>
<tr>
<td>Modify computer policy settings</td>
<td>89</td>
</tr>
<tr>
<td>Modify directory protection policy settings</td>
<td>91</td>
</tr>
<tr>
<td>Modify password policy settings</td>
<td>92</td>
</tr>
<tr>
<td>Enable single sign-on</td>
<td>93</td>
</tr>
<tr>
<td>Disable single sign-on</td>
<td>94</td>
</tr>
<tr>
<td>Account policy settings</td>
<td>94</td>
</tr>
<tr>
<td>Computer policy settings</td>
<td>96</td>
</tr>
<tr>
<td>Directory protection policy settings</td>
<td>97</td>
</tr>
<tr>
<td>Cache expiration policies</td>
<td>98</td>
</tr>
<tr>
<td>Password policy settings</td>
<td>99</td>
</tr>
<tr>
<td>Single sign-on policy settings</td>
<td>101</td>
</tr>
<tr>
<td>When to disable single sign-on</td>
<td>102</td>
</tr>
<tr>
<td>Security Policy Properties</td>
<td>103</td>
</tr>
<tr>
<td>Navigate the Policy Properties windows</td>
<td>104</td>
</tr>
<tr>
<td>Export policies to XML</td>
<td>104</td>
</tr>
<tr>
<td>Export Policies</td>
<td>105</td>
</tr>
</tbody>
</table>

**Chapter 10**

**Set product-specific policies**

Secure features of a single product                                      107
Secure multiple product features                                         108
Feature Security for Product Policies                                     110
Feature Security Policies                                                 111
Differences between securable actions and product features               111

**Chapter 11**

**Manage logical names**

Logical names                                                               114
Add a logical name                                                         115
Delete a logical name                                                      116
Add a device to a logical name                                            116
Remove a device from a logical name                                       117
Assign a control device to a logical name                                 117
Add a logical name to an area or application                              118
Table of contents

Delete a logical name from an area or application ..................................................... 119
New Logical Name ........................................................................................................... 120
Logical Name Properties ............................................................................................... 121
Device Properties .......................................................................................................... 122

Chapter 12

Resource grouping

Resource groupings .......................................................................................................... 125
Group hardware resources in an application or area ..................................................... 126
Move a resource between areas ...................................................................................... 127
Remove a device from a resource grouping .................................................................... 128
Resources Editor ............................................................................................................... 128
Select Resources .............................................................................................................. 129

Chapter 13

Secure resources

Secure resources .............................................................................................................. 131
Permissions .................................................................................................................... 132
Breaking the chain of inheritance ................................................................................... 134
Order of precedence ....................................................................................................... 136
Actions ............................................................................................................................ 137
Set FactoryTalk Directory permissions ........................................................................ 140
Set application permissions ......................................................................................... 142
Set area permissions ...................................................................................................... 143
Set System folder permissions ...................................................................................... 145
Set action group permissions ...................................................................................... 147
Set database permissions ............................................................................................. 148
Set logical name permissions ....................................................................................... 149
Allow a resource to inherit permissions ......................................................................... 151
Prevent a resource from inheriting permissions ........................................................... 151
View effective permissions ........................................................................................... 152
Effective permission icons ............................................................................................ 154

Chapter 14

Disaster Recovery

Back up a FactoryTalk system ....................................................................................... 157
Back up a FactoryTalk Directory ................................................................................. 157
Back up a System folder ............................................................................................... 160
Back up an application ................................................................................................. 161
Back up a Security Authority identifier ....................................................................... 163
Backup ........................................................................................................................... 164
Backup and restore options .......................................................................................... 166
Modify Security Authority Identifier .......................................................................... 167
Restore a FactoryTalk system ....................................................................................... 167
Restore a FactoryTalk Directory .................................................................................. 168
Restore a System folder ............................................................................................... 170
Table of contents

Appendix A
Upgrade FactoryTalk Services Platform
Upgrade FactoryTalk Services Platform........................................................................ 199
Identify the installed FactoryTalk Services Platform version........................................ 200

Appendix B
FactoryTalk Web Services
Install FactoryTalk Web Services.................................................................................... 201
Add an HTTPS site binding for FactoryTalk Web Services............................................. 202
Client computers unable to connect to FactoryTalk Web Services ............................ 203
User cannot log into FactoryTalk Web Services........................................................... 204

Legal Notices
Index
Preface

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

- FactoryTalk Help – From the Windows Start menu, select All Programs > Rockwell Software > FactoryTalk Tools > FactoryTalk Help
- FactoryTalk View Installation Guide or FactoryTalk View Help – From the Windows Start menu, select All Programs > Rockwell Software > FactoryTalk View > User Documentation and the select the appropriate Help or User Guide.
- FactoryTalk” Linx™ Help – From the Windows Start menu, select Start > All Programs > Rockwell Software > FactoryTalk Linx > FactoryTalk Linx Online Reference.
- RSLinx Classic Help – From the Windows Start menu, select Start > All Programs > Rockwell Software > RSLinx > RSLinx Classic Online Reference.
- Logix Designer application Help – In Logix Designer, select Help > Contents
• 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-GR001_-EN-E
• RSLinx Classic Getting Results Guide - Rockwell Automation Publication LINX-GR001_-EN-E
• FactoryTalk Batch Getting Results Guide - Rockwell Automation Publication BATCH-GR011_-EN-P
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. If you use both directories, then that single computer participates in two separate FactoryTalk systems.
In the network directory example above, the directory hosts two network applications: one named Waste Water and the other named 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 of the information and settings organized within the System folder, such as security settings, system policies, product policies, user accounts, and so on, apply to all applications held in the directory.

For example, if we modify security settings in the WasteWater application, the change does not affect the Water Distribution application. However, if we make a change to a security policy, the change applies to both the WasteWater application and the Water Distribution application. The security policy settings would also apply to any other new applications created in the future in this same network directory.

See also

- FactoryTalk Directory types on page 13
- Accounts and groups on page 15
- Applications and areas on page 19
- Security in a FactoryTalk system on page 19
- Example: Two directories on one computer on page 20

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, and graphic displays are stored in the HMI servers where they are created. Yet all of 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 then 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 Machine Edition 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.
Which directory you need depends upon which software products you plan to use and whether you plan to work in a stand-alone or a networked environment.

See also

Example: Two directories on one computer on page 20

Configure a network directory client computer on page 36

About FactoryTalk systems on page 11

Creating accounts for users, computers, and groups of users and computers allows you to define who can perform actions, and from where. When viewing lists of users, computers, and groups, an icon indicates the status of each account.

Security settings for accounts are stored in FactoryTalk Directory, and are separate for FactoryTalk network and local directories. As much as possible, create group accounts rather than individual accounts. This simplifies administration, and allows you to secure resources in your system by defining security permissions for the group accounts before all the individual user and computer accounts have been created. You can then add user and computer accounts to the groups at any time, and all of the individual accounts in the groups will have the security settings of those groups.

User accounts and user group accounts

You can set up accounts for users and user groups that are linked to accounts in a Windows domain or workgroup, or you can set up accounts that are separate from those in Windows.

If the security needs of your FactoryTalk system are the same as your Windows security needs, Windows-linked user or group accounts provide a convenient way to add large numbers of existing Windows user or group accounts to your FactoryTalk system. You can then administer those users or groups in Windows. Account properties — for example, whether users can change passwords — are inherited directly from the Windows accounts, and are updated automatically if they are changed in Windows.

FactoryTalk user accounts or user group accounts provide secure access to your FactoryTalk system independently of the level of access users have in Windows. If the security needs of your FactoryTalk system are different from those of your Windows network, FactoryTalk Directory user accounts provide the benefits and convenience of centralized administration, without the need for a Windows domain. FactoryTalk user group accounts also retain their security settings when you move your FactoryTalk Directory to a new domain.
Computer and computer group accounts

Sometimes it is necessary to restrict access to resources based on where a user is physically located, such as the computer the user is using to perform actions. For critical operations, this allows you to implement 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 to be 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. However, the name of a computer account must match the Windows computer name for the security settings associated with the computer to take effect. You can create accounts for computers that do not yet exist in Windows. Because a FactoryTalk local directory runs on a single computer, you can add computer accounts only to a FactoryTalk local directory.

Account status

By default, user accounts and group accounts are active, which means that the user or members of a group can access the account. The status of accounts can also be:

- Disabled, to prevent the user from accessing the account temporarily.
- Locked, if the user enters the wrong password more than a certain number of times.
- Deleted, to prevent the user from accessing the account permanently.
- Unknown, which means that information about the account could not be obtained from the network.

See also

- Account types on page 16
- Manage users on page 39
- Manage user groups on page 47
- Manage computers on page 55

Account types

When adding users to the system, you can:

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

You can also use both Windows-linked accounts and FactoryTalk accounts in a FactoryTalk Directory. For example, you might have a FactoryTalk administrator account that is not linked to an account in Windows, even if you normally use Windows-linked accounts.

**When to use FactoryTalk user accounts**

- When you need the convenience and benefits of centralized security administration across the entire distributed system, but you don’t want to rely 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.

- If you are using Windows workgroups in a FactoryTalk network directory, use FactoryTalk accounts for central user authentication. This is because 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 your Windows network are different from the security needs of your 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 your Windows network are the same as the security needs of your control system. For example:
• When your 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.

You should always have at least one Windows-linked user account that is a member of the FactoryTalk Administrators group. This prevents you from being inadvertently locked 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.

• A Windows-linked user group cannot be a member of a FactoryTalk user group. However, 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.

**See also**

*How security authenticates user accounts* on page 28

*Accounts and groups* on page 15

*Manage users* on page 39

*Manage user groups* on page 47
Applications and areas

In a FactoryTalk Directory, elements such as data servers, alarm and event 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 manage any number of separate local applications. As part of developing a FactoryTalk system, log on to either a network directory or a local directory, create an application, add HMI 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. The root of an application in a network directory can contain only one HMI server. You need to create a separate area for each HMI server you add to an application. You cannot create areas within a local application.

See also

FactoryTalk Directory types on page 13

About FactoryTalk systems on page 11

Security in a FactoryTalk system

FactoryTalk Security is intended to improve the security of an automation system by limiting access to those 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 identities of users to access a FactoryTalk system against a defined set of user accounts held in the FactoryTalk Directory. In this way, FactoryTalk can verify a user’s identity and verify 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 and allows you to define the answer to the following 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 actions that can be performed 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 you to configure security on resources in an area, while others might allow you to configure security for logic controllers and other devices.
- **Locations**—refers to the location of the authorized computers. 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.

The principle of inheritance determines how access permissions are set. For example, if you assign security to an area in an application, all of the items in the area inherit the security settings of the area. You can 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, 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**

- Permissions on page 132
- Best practices on page 31
- About FactoryTalk systems on page 11

**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. Which directory you need depends upon which
software products you plan to use and whether you plan to work in a stand-alone or a networked environment.

For example, if you use FactoryTalk View SE or FactoryTalk Transaction Manager, you will use the network directory to create and manage network applications. If you use FactoryTalk View Machine Edition, you will use the local directory to create and manage local applications. Other products, such as RSLogix 5, RSLogix 500, and FactoryTalk Linx, allow you to use 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, these project objects can be accessed 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 case of the network directory, 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).

Suppose we 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 suppose we 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.

If we change 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.

In the same way, you might have multiple user accounts, all with the same user name and password, on your computer at home. For example, you might log on to your Windows system with the user name "HomeAccount" and password "NorthAndSouth." You might create accounts and use the same user name and password to log on to your local bank, a bill-paying service, several online shopping accounts, and your online broker. Suppose you log on to your bank and change your password to "EastAndWest." This change will not affect the password for your Windows system, bill-paying service, online shopping accounts, or online broker, because each of these accounts is separate, even though each has the same user name and password.

See also

Applications and areas on page 19

FactoryTalk Directory types on page 13

About FactoryTalk systems on page 11
Chapter 2

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.

**See also**

- **Product Compatibility and Download Center**
- **FactoryTalk Web Services** on page 201
- **Upgrade FactoryTalk Services Platform** on page 199
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

About 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

FactoryTalk Security offers an integrated, cross-product solution to two universal security concerns: authentication and authorization. You must be able to authenticate identity and authorize access for each user who attempts to use your Rockwell Automation® software systems.
• **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 allows you to define the answer to the following 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 you to configure security on resources in an area, while others might allow you to configure security 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, if you assign security to an area in an application, all of the items in the area inherit the security settings of the area. You can 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 28

[Things you can secure](#) on page 28

[Best practices](#) on page 31
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, you must 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, depending on what you want to do with the product.

You may manage the following 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, begin by performing these tasks:

- Delete the Windows-linked group called 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 52
- Secure resources on page 131

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, you must 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, depending on what you want to do with the product.

Key steps in tightening 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 will ensure that you always have administrative access to the FactoryTalk Directory after you remove the Windows Administrators group in the next step.

• Remove the Windows-linked group called **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 to have full access to the FactoryTalk network directory.

• Modify security policies to secure the system.

**See also**

[Delete a user group](#) on page 52

[Secure resources](#) on page 131

**How security authenticates user accounts**

When a user attempts an action that is secured, security authenticates user names and passwords in the following 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 132

[Account types](#) on page 16

[About FactoryTalk Security](#) on page 25

**Things you can secure**

You can use **Allow** or **Deny** permissions to secure access to resources in your 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, write, and so on, and the computers, or groups of computers where they are working.

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

In a local FactoryTalk directory, actions can be performed 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, you can restrict actions such as writing values, to particular users or groups of users. In a network directory, you can also restrict actions to particular computers, or groups of computers.

You can group actions together and then assign security permissions to all of the actions in the group. For example, you want to 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 called "Punch Presses"
- The operators belong to a user group called "Operators"
- the computers within line of sight of the machinery belong to a computer group called "Heavy MachineryT"
First, you would clear the **Allow** check box for All Users and All Computers in the Punch Presses area. Next, you would select the **Allow** check box for the user group called Operators and the computer group called Heavy Machinery.

When setting permissions, **Deny** permissions are implied unless **Allow** permissions are specified explicitly. Clearing the **Allow** check box ensures that all users are denied write access, except those for whom you allow access explicitly.

**Using the Security item**

When you right-click an item in the **Explorer** window and then click **Security**, you are setting up which users or user groups on which computers may access the resource you selected.

<table>
<thead>
<tr>
<th><strong>Important:</strong></th>
<th>Right-clicking the <strong>System</strong> folder, <strong>Users and Computers</strong> folder, <strong>Users</strong> folder, or the <strong>Computers</strong> folder, and then specifying security permissions sets security on that actual folder. It does not limit users' access to the system.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To limit access to resources in the FactoryTalk system, you must right-click the resource you want to secure, click <strong>Security</strong>, and then specify security permissions for the user and computer accounts you want to access the resource.</td>
</tr>
</tbody>
</table>

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

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

**Security settings apply to all FactoryTalk products**

Security settings that you configure for resources apply to all FactoryTalk products in your system. For example, if you deny a user **Read** access to an area from a particular computer, that user will not be able to see that area in any FactoryTalk product while working from that computer.

**See also**

- **Permissions** on page 132
- **Best practices** on page 31
- **Actions** on page 137
- **About FactoryTalk Security** on page 25
Best practices

Use the following tips when setting up your 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, you can use a second administrator account to reset the password to the first one. Without a second administrator account, you can be locked out of the FactoryTalk system because a lost password to a user account is not recoverable.

- **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. When this happens depends on the **Account lockout duration** policy in Windows.

Windows-linked accounts

If you expect the need to move Windows accounts from one domain to another, avoid using individual, Windows-linked user accounts as much as possible. Use Windows-linked user group accounts instead. Windows-linked user group accounts can be moved from one domain to another, while keeping security permissions for the group accounts intact. 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. You must then recreate all of the permissions for any individual Windows-linked user accounts.

Permissions

- **Assign permissions to groups rather than to users.**
  
  Because it is inefficient to maintain user accounts directly, assign permissions to user accounts only by exception.

- **Wherever possible, remove Allow permissions instead of assigning explicit Deny permissions.** This makes administration simpler because of the order of precedence of explicit permissions over inherited permissions, and Deny permissions over Allow permissions.

- **Use Deny permissions to:**
• Exclude a subset of a group that has **Allow** permissions

• Exclude one special permission when you have already granted full control to a user or group

• Assign permissions at as high a level as possible. This provides the greatest breadth of effect with the least effort. The rights you establish should be 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, and use an account with broader permissions only when performing specific administrative tasks.

**See also**

- [About FactoryTalk Security](#) on page 25
- [Account types](#) on page 16
- [Permissions](#) on page 132

**Audit trails and regulatory compliance**

To achieve compliance in regulated industries, your plant might be required to keep records that answer questions such as the following:

• 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, you need to:

• 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 in the following ways:

• 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.

To do this, develop a scheme for identifying users uniquely. However, bear in mind that user names are visible, and therefore should not contain any private information, for example, social security numbers. User names are also typed frequently, and therefore should be relatively easy to remember.

If your system is required to comply with governmental regulations, you might be forced to have multiple names for the same user if a user leaves the company, you delete the user account, and then the user is hired back again.

**Keep a record of deleted users**

To ensure that all user accounts remain unique, keep track of deleted accounts. This might also be required to satisfy audit requirements such as tracking a user’s actions throughout the system, even after the user’s account has been deleted.

To ensure that only unique user accounts can be created, enable the security policy called **Keep record of deleted accounts**. To make it easier 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 called **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 what information needs to be logged 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 you do not enable the audit policy called Audit configuration and control system changes FactoryTalk Diagnostics will not receive any audit messages, and will not be able to store them 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 you do not complete this step, FactoryTalk Diagnostics will receive the information you chose to send to it, but will not capture this information and store it in log files.

To configure FactoryTalk Diagnostics routing and logging options, choose **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, choose **FactoryTalk Diagnostics > Viewer**.
Set up audit trails of successful or unsuccessful attempts at modifying system values

The most common type of auditing activity is keeping records of failures. This helps you 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 be audited. For example, when making pharmaceutical drugs, any changes or adjustments in recipes must be recorded so that any problems that might occur later can 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 your 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 86

Audit policies on page 83

Configure a computer to be the FactoryTalk Directory network server

FactoryTalk Services Platform quietly configures both a network directory and a local directory on every computer where it is installed. Which directory you need depends upon which software products you plan to use and whether you plan to work in a stand-alone or a networked environment.

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.

After installing and activating FactoryTalk software, specify one of the computers on the network as the network directory server. In this example, Computer 1 serves as the network directory server.
Next, point the client computers on the network to the network directory server. This step allows all of the computers on the network to share FactoryTalk network directory services and resources.

In this example, 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 35
Configure a network directory client computer on page 36
Check network directory server connection status on page 36
FactoryTalk Directory Server Location Utility on page 37

Configure a computer to be the network directory server

After installing and activating FactoryTalk software, specify one of the computers on the network as the network directory server. This step allows all of the computers on the network to share FactoryTalk network directory services and resources. In the image below, Computer 1 is the network directory server computer.

To configure a computer to be the network directory server

1. On the computer that you want to use as the Network Directory Server, choose Start > All Programs > Rockwell Software > FactoryTalk Tools > Specify FactoryTalk Directory Location.

2. At the prompt, log on to the network directory with a Windows Administrator account.


4. In FactoryTalk Directory Server Configuration, click This computer to use the network directory server installed on this computer, and click OK.
Next, point the other computers on the network to that computer.

See also

Check Network Directory Server connection status on page 36
Configure a network directory client computer on page 36
FactoryTalk Directory Server Location Utility on page 37

To configure a network directory client computer

1. On each participating network directory client computer, choose Start > All Programs > Rockwell Software > FactoryTalk Tools > Specify FactoryTalk Directory Location.

2. At the prompt, log on to the network directory with a Windows Administrator account.


4. In FactoryTalk Directory Server Configuration, click Remote computer, then specify the name of the computer to use as the network directory server, and click OK.

5. When prompted to do so, log on to the network directory.

If single sign-on is enabled on the computer when you change the location of the network directory server, the single sign-on session terminates, and you must log on to the new network directory server. The user name and password you enter becomes 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 35
Check network directory server connection status on page 36
FactoryTalk Directory Server Location Utility on page 37

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.

In addition, the network directory connection status is available from the **FactoryTalk Directory Server Location Utility**.

If a connection to the network directory server is not available, you can still open a network application, but 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. Choose **Tools > FactoryTalk Directory Server Options**.
2. In the **FactoryTalk Directory Server Location Utility**, look for one of three status messages, located just above the name of the active server. The current status of the active server will be one of the following:
   - **(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 34
- [FactoryTalk Directory Server Location Utility](#) on page 37

How do I open the FactoryTalk Directory Server Location Utility?

Perform one of the following actions:

- From the **Start** menu, select **All Programs > Rockwell Software > FactoryTalk Tools > 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 35
- Configure a network directory client computer on page 36
- FactoryTalk Directory types on page 13
- Check Network Directory Server connection status on page 36
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 in which you created them.

If you have the proper security permissions, you may modify all properties for FactoryTalk user accounts. For example, you may:

- Add group memberships to the user account
- Edit the user's name and description
- Associate an e-mail address with the user’s account
- Set numerous user password options, such as whether or not a user can change the account password
- Enable, disable, or unlock the user account
- Reset the account password

Use Windows to edit Windows-linked user accounts.

See also

Add a FactoryTalk user account on page 39
Add a Windows-linked user account on page 41
Add group memberships to a user account on page 42
Manage user groups on page 47

Add a FactoryTalk user account

To create a user account that is separate from a user’s Windows account, add a FactoryTalk Directory account. This allows you to specify the account’s identity, to set up how the account operates, and to specify the groups the account belongs to.

Prerequisites

Obtain the following permissions in the Users folder in the Explorer window:

- Common > Create Children
To add a user account

1. In the **Explorer** window, expand **System > Users**.
2. Right-click the **Users** folder, point to **New**, and then click **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. (optional) Click the check box to set one or more of these settings for password access:
   - **User must change password at next logon**
   - **User cannot change password**
   - **Password never express**
7. In **Password**, type a password for the user account. **Password Policy Settings in Security Policy Properties** determine the requirements for a valid password.
8. In **Confirm**, type the same password entered above.
9. Click **OK** to add the user to the FactoryTalk Directory.

See also

- **Add a Windows-linked user account** on page 41
- **Delete a user account** on page 44
- **Password Policy Settings** on page 99
- **Account types** on page 16
- **Manage users** on page 39
Add a Windows-linked user account

Add a Windows-linked user account when the security needs of your Windows network are the same as the security needs of your 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. However, you can add Windows-linked user accounts to FactoryTalk Security user groups. This 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 your computer is disconnected from the Windows domain, you cannot add Windows-linked user accounts until your computer reconnects to the domain. However, any users who have 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**

To add a Windows-linked user account, obtain the following permissions in the Users folder in the Explorer window:

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

**To add a Windows-linked user account**

1. In the Explorer window, expand System > Users.
2. Right-click the Users folder, point to New, and then click Windows-Linked User.
4. In Select Users, select the Windows user accounts you want to link to the FactoryTalk system.
• If you know the names of the user accounts you want to add, type them in the text box. For domain accounts, use the format \DOMAIN\username, for workgroup accounts use the format COMPUTERNAME\username. To check that the user names you typed are valid, click Check Names. Correct any errors, and then click OK.

• To search for user names, or to select multiple users, click Advanced. In Select Users, click Locations, select the domain or workgroup from which you want to select users, and then click OK. Optionally, use the Common Queries settings to search by name. Click Find Now. In the list of users, select the user accounts you want to add, then click OK.

5. When you finish selecting Windows user accounts, in Select Users, click OK.

6. In New Windows-Linked User, review the list of users you added.

• To remove any users you might have added unintentionally, select the users, and then click Remove.

• To add more users, repeat steps 3, 4, and 5.

7. Click OK.

See also

Add a FactoryTalk user account on page 39
Delete a user account on page 44
Add group memberships to a user account on page 42
Remove group memberships from a user account on page 43
Manage users on page 39

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

To change the group memberships of a user account, you need the following permissions in the Users folder in the Explorer window:

• Common > List Children
• Common > Read
• Common > Write

To add group memberships to a user account

1. In the Explorer window, expand System > Users, right-click the user account that you want to add to user groups, and then click Properties.

2. On the Group Membership tab, click Add.

3. In Select User Group, select the groups to which you want the user account to belong, and then click OK.

4. In User Properties, click OK.

See also

Remove group memberships from a user account on page 43

Manage user groups on page 47

Permissions on page 132

About FactoryTalk Security on page 25

Account types on page 16

Remove group memberships from a user account

When a user account belongs to a user group, the user account automatically inherits all of the permissions assigned to the group, unless you have specifically denied permissions 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 the Explorer window, expand System > Users, right-click the user account containing the group memberships you would like to change, then click Properties.

2. Click the Group Membership tab.

3. In the list of groups, select the groups you want to remove the user account from, and click Remove.
4. In **User Properties**, click **OK**.

**See also**

- [Add group memberships to a user account](#) on page 42
- [Manage user groups](#) on page 47
- [Permissions](#) on page 132
- [About FactoryTalk Security](#) on page 25
- [Account types](#) on page 16

**Delete a user account**

Delete a user account to permanently remove the account from your FactoryTalk Directory. To help prevent you from inadvertently locking yourself out of the FactoryTalk Directory, you cannot 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, you must 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**

To delete a user account that is a member of a user group, obtain the following permissions in the **Users** folder in the **Explorer** window:

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

To delete a user account that is not a member of a user group, obtain the following permissions in the **Users** folder in the **Explorer** window:

- Common > Delete
- Common > List Children
- Common > Read
To delete a user account

- In the Explorer window, expand System > Users, right-click the user account you want to delete, and then click Delete.

  **Tip:** You can only create an account using the name of a deleted account if the security policy called 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 39
Chapter 5

Manage user groups

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

A few key points to keep in mind about user groups:

- User group accounts exist only in the FactoryTalk Directory in which you created them.
- FactoryTalk user accounts cannot be members of Windows-linked user groups.
- A Windows-linked user group cannot be a member of a FactoryTalk user group. However, 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.

See also

- Add a FactoryTalk user group on page 47
- Add a Windows-linked user group on page 49
- Add accounts to a FactoryTalk user group on page 52
- Accounts and groups on page 15
- Account types on page 16

Add a FactoryTalk user group

Create a new FactoryTalk user group so that you can administer security permissions for specified users as a group. By changing the memberships of a user account, you can quickly change the resources a user can access.

A FactoryTalk user group may contain the following:
Chapter 5  Manage user groups

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

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

Prerequisites

Obtain the following permissions in the User Groups folder in the Explorer window:

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

To add a user group account

1. In the Explorer window, expand System > User Groups.
2. Right-click the User Groups folder, point to New, and then click 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 e-mail address or group address you want to associate with this group account.
6. Click Add to add user accounts to your group. In Select User or Group, click 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. Click OK to add the selected user or group to the Members List in New User Group.
8. When you are finished creating the user group, click OK.

See also

Delete a user group on page 52
Manage user groups on page 47

Add a Windows-linked user group

If you expect the need 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 be moved 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 members of the group), modify these properties in Windows.

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

Prerequisites

1. Connect your computer to the Windows domain containing the user groups you wish to add to the FactoryTalk Directory.

2. Obtain the following permissions in the User Groups folder in the Explorer window:

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

To add a Windows-linked user group account

1. In the Explorer window, expand System > User Groups.

2. Right-click the User Groups folder, point to New, and then click Windows-linked User Group.

4. In Select Groups, select the Windows groups you want to add, and then click OK.

- If you know the names of the user group accounts you want to add, type them in the text box. For domain accounts, use the format \DOMAIN\groupname, for workgroup accounts use the format COMPUTERNAME\groupname. To check that the names you typed are valid, click Check Names. Correct any errors, and then click OK.

- To search for group names, or to select multiple groups, click Advanced. In the Select Groups dialog box that appears, click Locations and then select the domain or workgroup from which you want to select groups. Click Find Now. In the list of groups, select the group accounts you want to add, and then click OK.

5. In New Windows-Linked User Group, review the list of groups you added.

- To remove any groups you might have added unintentionally, select the groups, and then click Remove.

- To add more groups, repeat steps 3 and 4, above.

6. Click OK.

Tip: You should use a password for all Windows accounts in a Windows-linked group, otherwise you might experience intermittent security failures or an inability to log on. As a matter of good security practice, do not use blank passwords with accounts. If you do not want to use a password for Windows-linked accounts, on your local computer disable the Windows local security policy called Accounts: Limit local account use of blank passwords to console logon only.

See also

Delete a user account on page 44

Add a Windows-linked user account on page 41

Account types on page 16

Manage user groups on page 47

Edit or view user group properties

You can modify the properties of a FactoryTalk user group account that is not linked to a Windows user group account. You can only view the properties of a Windows-linked user group account. You may not change the name of a user group.

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

Obtain the following permissions in the User Groups folder in the Explorer window:

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

To edit or view user group properties

1. In the Explorer window, expand System > User Groups, right-click the user group account you want to modify, and then click Properties.

2. (optional) In the Description box, type a description of the user group. For example, use this box to 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 e-mail address or group address, if any (for example cjenkins@yourcompany.com, or maintenance@yourcompany.com), you want 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 e-mail address. For details, see the documentation supplied with your FactoryTalk-enabled product.

4. (optional) To add accounts to the group, click Add. In Select User or Group, click to select the users or user groups you would like to add to your group, and click OK.

5. (optional) To remove user accounts, click to select the users or user groups you would like to remove from your group, and click Remove.

6. Click OK.

See also

Add a FactoryTalk user group on page 47
Add a Windows-linked user group on page 49
Account types on page 16
Manage user groups on page 47
Delete a user group

Delete a user group when you no longer need a particular group account to manage a group of users. You may wish to view the properties of a user group account before you delete it.

To help prevent you from inadvertently locking yourself out of the FactoryTalk Directory, you cannot delete the Administrators group.

Prerequisites

To delete a user group account that has no members, obtain the following permissions in the User Groups folder:

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

To delete a user group account that has members, obtain the following permissions in the User Groups folder:

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

To delete a user group

- In the Explorer window, expand System > User Groups, right-click the user group account you want to delete, and then click Delete.

See also

Edit or view user group properties on page 50
Manage user groups on page 47

Add accounts to a FactoryTalk user group

Any time after you create a FactoryTalk user group, you may add or remove the user accounts that belong to it. You may not add or remove the members of a Windows-linked user group. However, you may add individual Windows-linked user accounts to FactoryTalk user groups.
Manage user groups

Chapter 5

Tip: Alternatively, you may change the groups a user belongs to. Use Group Management 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 the Explorer window, expand System > User Groups, right-click the user group account you want to modify, and then click Properties.

2. Click Add.

3. In Select User or Group, click on 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 you may add to the group. Click OK when you are finished.

See also

Remove accounts from a FactoryTalk user group on page 53
Add a FactoryTalk user group on page 47
Delete a user group on page 52
Manage user groups on page 47

Any time after you create a FactoryTalk user group, you remove the user accounts that belong to it. You may not add or remove the members of a Windows-linked user group after it has been added to the FactoryTalk Directory.

Tip: Alternatively, you may change the groups a user belongs to. Use Group Management 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 the Explorer window, expand System > User Groups, right-click the user group account you want to remove, and then click Remove.

2. In Select User or Group, click on 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 accounts you may remove. Click OK when you are finished.

See also

Add accounts to a FactoryTalk user group on page 52
Add a FactoryTalk user group on page 47
Add a Windows-linked user group on page 49

Delete a user group on page 52

Manage user groups on page 47
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.

If you have the proper security permissions, you may:

- 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

See also

Add a computer on page 55
Edit or view computer properties on page 57

Add a computer

To allow a computer to access the FactoryTalk system, add a computer to a FactoryTalk network directory. Once you have added the computer account, you can specify security settings for the computer, for example to allow or deny access to parts of the FactoryTalk system from the computer. You can also add the computer to a group account that includes multiple computers, and then specify security settings for the group.
Important: Even if the security policy called 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

Obtain the following permissions in the Computers folder in the Explorer window:

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

To add a computer account

1. In the Explorer window, expand System > Computers and Groups, right-click Computers, and then click New Computer.

2. In New Computer, in Computer name, type the name of the computer, or click Browse (...) and then select a computer.

3. (optional) In Description, type a description of the computer (for example, Operator workstation for South Building production line 1). You can also use this box to record contact information for maintenance personnel.

4. Click OK.

See also

Delete a computer** on page 56

Accounts and groups on page 15

Delete a computer

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

Prerequisites

To delete a computer account that is not a member of a computer group, obtain the following permissions in the Computers folder in the Explorer window:

- Common > Delete
- Common > List Children
- Common > Read
To delete a computer account that is a member of a computer group, obtain the following permissions in the Computers folder in the Explorer window:

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

To delete a computer

- In the Explorer window, expand System > Computers and Groups > Computers, right-click the computer account you want to delete, and then click Delete.

See also

Add a computer on page 55
Manage computers on page 55

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

Obtain the following permissions in the Computers folder in the Explorer window:

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

To edit or view computer properties

1. In the Explorer window, expand System > Computers and Groups > Computers, right-click the computer account you want to edit, and click Properties.

2. Edit the settings in General Computer Properties as needed, and click OK.

See also

Add a computer on page 55
Manage computers on page 55
Chapter 7

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 they are performing, for example, read, write, and so on, and the computers, or groups of computers where they are working.

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

You may:

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

See also

Add a user-computer pair on page 59
Remove a user-computer pair on page 60

Add a user-computer pair

Use Select User and Computer to pair a group of users, or an individual user, with a group of computers, or an individual computer. You can then specify security settings for the pair. For example, you may 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, select the filter criteria that show the users and user groups, and computers or computer groups that you want to select.

2. In the Users list, click 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. Use the following window—New FactoryTalk
User, New FactoryTalk User Group, New Windows-linked User, or New Windows-linked User Group—to specify the account settings.

3. In the Computers list, click a computer account or computer group account.

To create a new computer account, click Create New and then either Computer or Computer Group. Use New Computer or New Computer Group to specify the account settings.

4. Click OK.

See also

Remove a user-computer pair on page 60

Remove a user-computer pair

Remove a user-computer pair when you no longer need 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 that show the users and user groups, and computers or computer groups that you want to delete.

2. In the Users list, click the user account or user group account that belongs to the pair you wish to delete.

3. In the Computers list, click a computer account or computer group account that belongs to the pair you wish to delete.

4. Click Remove.

5. Click OK.

See also

Add a user-computer pair on page 59

Edit or view user account properties

Follow the steps below to view and edit the general properties of a FactoryTalk user account, such as the user name and password, a description of the user, an e-mail address for the user, and options for password access by the user. For a
Windows-linked user account, you may view, but not edit, these properties. Use Windows to edit the general properties of a Windows-linked user account.

Prerequisites

Obtain the following permissions in the Users folder in the Explorer window:

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

To edit or view user account properties

1. In the Explorer window, expand the FactoryTalk network or local directory tree, and then expand the System folder until the user account you want to view or edit is visible.

2. Right-click the user account, and then click Properties on the context menu. Edit the General User Properties settings as needed.

   You must fill out the User name, Full name, Password, and Confirm fields. Description, E-mail, and the settings for password access are optional fields.

3. Click OK.

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

See also

Add a FactoryTalk user account on page 39

Manage users on page 39
Add and remove action groups

To avoid having to set 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, you 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, you can:

- 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 63
Delete an action group on page 65
Add an action to an action group on page 65

Add an action group

You can 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, you decide:

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

Prerequisites

Obtain the following security permissions for the Action Groups folder in the Explorer window:

• Common > Read
• Common > List Children
• Common > Create Children
• Common > Write

To add an action group

• In the Explorer window, right-click the Action Groups folder and then click New Action Group.

See also

Delete an action group on page 64

Add and remove action groups on page 63

Delete an action group

When you delete an action group, any explicit permissions assigned to that group are no longer in effect. For example, suppose that we delete an action group called Operators. This action group explicitly granted Write access to an area called Mixing, for a user called Chris, from all computers. If we delete the Operators action group, Chris can no longer write to the Mixing area.

Recreating an action group using the same name as one that was deleted does not restore the security permissions of the deleted action group. If you cannot restore the FactoryTalk Directory from a backup, you must recreate all security permissions assigned to all resources that were using the action group.

Prerequisites

1. Before deleting an action group, back up the FactoryTalk Directory.

2. Obtain the following security permissions for the Action Groups folder:
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

- Obtain the following security permissions for the Action Groups folder in the Explorer window:
  - Common > Read
  - Common > List Children
  - Common > Create Children
  - Common > Write

To add an action to an action group

1. In the Explorer window, expand Action Groups, then right-click the action group you wish to edit, and click Properties.

2. In Properties, your action group appears on the right in the Selected actions and action groups list.

3. In the Available Actions and Action Groups list, click to select the action you wish to add to the action group, and click the >> button.

4. Click OK.

See also

Add an action group on page 63
Add and remove action groups

Remove an action from an action group

If you no longer wish to manage security settings for a particular action as part of an action group, remove the action from the action group.

Prerequisites

- Obtain the following security permissions for the Action Groups folder in the Explorer window:
  - Common > Read
  - Common > List Children
  - Common > Create Children
  - Common > Write

To remove an action from an action group

1. In the Explorer window, expand Action Groups, then right-click the action group you wish to edit, and click Properties.

2. In Properties, your action group appears on the right in the Selected actions and action groups list.

3. In the Selected Actions and Action Groups list, click to select the action you wish to remove from the action group, and click the << button to remove it from the group.

4. Click OK.

See also

Add and remove action groups on page 63
Set system policies

Set system policies to manage settings that apply across the entire FactoryTalk manufacturing 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** — 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.
- **Live data policy** — the default communications protocol for a distributed FactoryTalk system.
- **Health monitoring policy** — the parameters that the health monitoring service uses when determining if a network glitch occurred and how long to wait before switching to a standby server.
- **Audit policies** — whether access checks are audited, whether access grants, denies, or both are audited, and so on.
- **Security policies** — minimum password length, complexity requirements, password expiration requirements, and so on. 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 68
- Assign user rights to make system policy changes on page 72
- Set audit policies on page 81
- Set system security policies on page 87
- Set network health monitoring policies on page 79
Authorize an application to access the FactoryTalk Directory

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

If you enable the option to verify the publisher certificate information, 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, you must 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 where you want to authorize an application to access the FactoryTalk Directory, or to block access to the directory.

2. In the Explorer window, expand the System > Policies > System Policies folders.


   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, sort the application list to view the application whose access you wish to change. To sort the application list by process name, computer name, or access allowed status, click 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, click in the desired cell in the Publisher Info column.

6. Click a process, and scroll to the right to view its access status. Check Access Allowed to provide access to the FactoryTalk Directory, or clear the check box to deny access to the FactoryTalk Directory.

7. (optional) To automatically enable access to the FactoryTalk Directory for any new process, check Enable Default Access.

8. (optional) To automatically block access to the FactoryTalk Directory for any new process, clear Enable Default Access.
9. (optional) To have publication information verified for all FactoryTalk Services Platform processes, click **Verify Publisher Info**. If the verification process fails, the process is automatically denied access.

10. Click **OK**.

**See also**

- [FactoryTalk Service Application Authorization settings](#) on page 69
- [Publisher certificate information](#) on page 71
- [Digitally signed FactoryTalk products](#) on page 72

**FactoryTalk Service Application Authorization**

How do I open FactoryTalk Application Authorization?

1. Start FactoryTalk Administration Console or FactoryTalk View Studio and then log on to the FactoryTalk Network Directory or FactoryTalk Local Directory where you want to modify application authorization policies.

2. In the Explorer window, expand the **System > Policies > System Policies** folders.

3. Double-click **Application Authorization**.

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

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

**Tip:** To configure the Application Authorization policy, you must 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 68
- [FactoryTalk Service Application Authorization settings](#) on page 69

**FactoryTalk Service Application Authorization settings**

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

If you enable the option to verify the publisher certificate information, applications that are not signed by Rockwell Automation or Microsoft are not allowed access to FactoryTalk Directory. To configure the Application
Authorization policy, you must log into FactoryTalk with an account that is a member of the FactoryTalk Administrators group.

The Application Authorization policy controls access by monitoring the following information of each application that is requesting a service token from FactoryTalk. To sort the application list by process name, computer name, or access allowed status, click the corresponding column header.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process</td>
<td>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 are displayed with gray text in the list. To sort the application list by process name, computer name, or access allowed status, click the corresponding column header.</td>
</tr>
<tr>
<td>Version</td>
<td>Shows the version number of the application that is requesting a service token.</td>
</tr>
<tr>
<td>Computer</td>
<td>Shows the computer name where the application runs. To sort the application list by process name, computer name, or access allowed status, click the corresponding column header.</td>
</tr>
<tr>
<td>Publisher Info</td>
<td>Shows the publisher name of the application. If no certificate exists, the cell is displayed with <strong>None</strong>. To view the detailed publisher certification information, click the desired cell in this column.</td>
</tr>
<tr>
<td>Access Allowed</td>
<td>Shows whether the current process is allowed to access to FactoryTalk Directory.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable default access</td>
<td>Determines whether new applications are automatically allowed access to FactoryTalk Directory. <strong>Default:</strong> Enabled <strong>To disable the default access, clear the check box. All new applications will be automatically denied access.</strong> If the default access of a FactoryTalk Directory server is disabled, you can still configure your local computer to join the directory server.</td>
</tr>
<tr>
<td>Verify publisher information</td>
<td>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. <strong>Default:</strong> Disabled <strong>To disable the publisher information verification, clear the check box. FactoryTalk Services Platform will not verify the publisher information. Applications are verified by the corresponding Access Allowed settings.</strong> Some applications of Microsoft (for example, msiexec.exe) are not signed. Some earlier versions of FactoryTalk products were not signed when they were released. You may fail to verify the publisher information on these applications.</td>
</tr>
<tr>
<td>Allow or deny an application</td>
<td>Determines whether an application is authorized to access the FactoryTalk Directory. <strong>Default:</strong> Allowed **To deny an application, clear the check box of the entry. If an application is denied access and thus fails the request for service token, a message is sent to FactoryTalk Diagnostics, for example, <strong>Login failure for application [RNASecurityTestClient.exe] on directory [Network]. The application was denied access.</strong> You can 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. See the Process name table below for details.</td>
</tr>
</tbody>
</table>
Set system policies

Chapter 9

Remove an application

To remove one or more applications from the list, select the entries and click Remove. Some applications are required by FactoryTalk and cannot be removed or denied. These entries are displayed with gray text in the list. When you try to remove one or more of these required entries, a warning message is displayed indicating that the required entries are not removed.

Refresh application authorization information

Manually refresh the list to show the latest application list. To do this, click Refresh. When refreshing the list, if a newer version of an existing application from the same computer is found, the entry will be 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.

Process name

<table>
<thead>
<tr>
<th>Process name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTDataUpdate.exe</td>
<td>FactoryTalk data update, which runs during FactoryTalk Directory configuration.</td>
</tr>
<tr>
<td>FTDCConfigurationUtility.exe</td>
<td>FactoryTalk Configuration wizard, which is only used in some special cases to repair the FactoryTalk Directory.</td>
</tr>
<tr>
<td>FTSPVStudio.exe</td>
<td>FactoryTalk Administration Console</td>
</tr>
<tr>
<td>NmspHost.exe</td>
<td>FactoryTalk namespace services</td>
</tr>
<tr>
<td>RdcyHost.exe</td>
<td>Rockwell redundancy services</td>
</tr>
<tr>
<td>RnaDirMultiplexor.exe</td>
<td>Rockwell RNA directory multiplexer</td>
</tr>
<tr>
<td>RsvcHost.exe</td>
<td>Rockwell Automation services</td>
</tr>
<tr>
<td>SilentFTDCW.exe</td>
<td>FactoryTalk Directory Silent Configuration Wizard</td>
</tr>
</tbody>
</table>

See also

Authorize an application to access the FactoryTalk Directory on page 68

Publisher Certificate Information on page 71

Digitally signed FactoryTalk products on page 72

Publisher Certificate Information

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

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

See also

Authorize an application to access the FactoryTalk Directory on page 68

FactoryTalk Service Application Authorization settings on page 69
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 they were released. You may fail to verify the publisher information on these products.

The table below shows which versions of FactoryTalk products are signed.

<table>
<thead>
<tr>
<th>Products</th>
<th>Signed since version</th>
</tr>
</thead>
<tbody>
<tr>
<td>FactoryTalk Administration Console</td>
<td>2.10.01</td>
</tr>
<tr>
<td>FactoryTalk Administration Console</td>
<td>2.31.00</td>
</tr>
<tr>
<td>FactoryTalk Batch</td>
<td>11.00</td>
</tr>
<tr>
<td>eProcedure®</td>
<td>11.00</td>
</tr>
<tr>
<td>FactoryTalk Linx</td>
<td>5.20</td>
</tr>
<tr>
<td>FactoryTalk Linx Gateway</td>
<td>3.02</td>
</tr>
<tr>
<td>FactoryTalk Historian SE</td>
<td>3.0</td>
</tr>
<tr>
<td>FactoryTalk Metrics</td>
<td>9.10</td>
</tr>
<tr>
<td>FactoryTalk Transaction Manager</td>
<td>9.10</td>
</tr>
<tr>
<td>FactoryTalk View Machine Edition</td>
<td>5.10</td>
</tr>
<tr>
<td>FactoryTalk View SE</td>
<td>5.20</td>
</tr>
<tr>
<td>Logix Designer</td>
<td>21.00</td>
</tr>
<tr>
<td>RSLogix Classic</td>
<td>2.54</td>
</tr>
<tr>
<td>RSLogix 5</td>
<td>7.40</td>
</tr>
<tr>
<td>RSLogix 500</td>
<td>8.10</td>
</tr>
<tr>
<td>RSLogix 5000</td>
<td>18.00</td>
</tr>
<tr>
<td>RSNetWorx</td>
<td>9.00</td>
</tr>
<tr>
<td>RSSecurity Emulator</td>
<td>2.10.01</td>
</tr>
</tbody>
</table>

See also

Authorize an application to access the FactoryTalk Directory on page 68

Publisher Certificate Information on page 71

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 whose user rights assignment policies you want to modify.
2. In the Explorer window, expand System > Policies > System Policies.
3. Double-click User Rights Assignment.
4. In User Rights Assignment Policies, next to the policy you want to secure and to the right of Configure Security, click Browse (...).
5. In the Configure Securable Actions, on the Policy Setting tab, click Add.
6. In Select User or Group, select the user or group of users, and in the network directory, the computer or group of computers for which you want to specify security settings, and then click OK.
7. Do one of the following, and then click OK:
   • To allow the user permission to perform the action from the specified computer or group, select the Allow check box.
   • To deny the user permissions to perform the action from the specified computer or group, select the Deny check box.
   • If you want to remove explicit Allow permissions, select the user and computer and then click Remove. If no permissions are specified, Deny is implied.

See also

User rights assignment policies on page 73
Permissions on page 132
Set system security policies on page 87

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 do the following:

- **Back up or restore FactoryTalk Directory, the System folder, or applications.** The default setting is to allow 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 your 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 is to allow administrators to change the directory server. The policy appears in only FactoryTalk network directory. Make sure you have the permissions to change the directory on the current computer and the computer you are switching to.

- **Switch between primary and secondary servers in a redundant pair.** In the FactoryTalk network directory, the default setting is to allow 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 is to allow 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 72

User Rights Assignment Policy Properties on page 74

**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 where you want to edit policies.
2. In the Explorer window, expand the FactoryTalk Network or Local Directory tree, and then expand the **System > Policies > System Policies** folders.

3. Double-click **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 72](#)
- [User rights assignment policies on page 73](#)
- [Permissions on page 132](#)
- [Set system security policies on page 87](#)

**Configure Securable Action**

**How do I open Configure Securable Action?**

1. Start FactoryTalk Administration Console or FactoryTalk View Studio and then log on to the FactoryTalk Network Directory or FactoryTalk Local Directory where you want to modify product policies.

2. In the Explorer window, expand the **System folder > Policies > Product Policies**, expand the folder for the product whose policies you want to secure, and then double-click **Feature Security**.

3. In the Feature Security Properties dialog box, click the row containing the feature you want to secure. A description of the feature appears at the bottom of the dialog box.

4. Click the Browse button beside the feature you want to secure. This opens the Configure Securable Action dialog box.
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 you can secure depend on what FactoryTalk products you have installed.

You may also 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permissions list</td>
<td>This list shows the users and computers that have <em>Allow</em> or <em>Deny</em> permissions set for this feature. To allow access to the feature, select the <em>Allow</em> check box. To deny access to the feature, select the <em>Deny</em> check box. If you clear both the <em>Allow</em> and <em>Deny</em> check boxes, the user is denied access to the feature.</td>
</tr>
<tr>
<td>Add</td>
<td>Click this button to select the user and computer for which you want to specify permissions. Once you are finished selecting a user and computer, click OK.</td>
</tr>
<tr>
<td>Remove</td>
<td>In the permissions list, click the combination of users and computers for which you want to remove security settings, and then click the <em>Remove</em> button.</td>
</tr>
</tbody>
</table>

**See also**

- [Secure features of a single product](#) on page 107
- [Effective permission icons](#) on page 154

**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:
Set system policies

• 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 47

Accounts and groups on page 15

Account types on page 16

---

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 your system is experiencing communications problems and you want to switch to DCOM for troubleshooting purposes. 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 the Explorer window, expand System > Policies > System Policies.

2. Double-click Live Data Policy.

3. Click the drop-down button to the right of Default Protocol Setting to switch the default communications protocol from TCP/IP to DCOM, or from DCOM to TCP/IP.

4. Click OK.

5. Shut down and restart all computers on the network.

See also

Live Data Policy Properties on page 78

---

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, it 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 will not attempt a TCP/IP connection and will always use 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 your network and sets the communication protocol appropriately. For example, if you upgrade 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 you install FactoryTalk Services Platform 2.10 or later for the first time on a computer, the communications default is automatically set to TCP/IP. Typically, it is not necessary or advisable to change the default setting.

<table>
<thead>
<tr>
<th>Default protocol setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| TCP/IP                   | This is an open communications protocol that typically is more reliable and has better performance than the proprietary DCOM protocol.  
  - Choose this option only if all or most of the clients and servers on your automation network have been upgraded to use FactoryTalk Services Platform v. 2.10 (CPR 9) or later.  
  - Do not choose this option if your automation network is using older versions of the FactoryTalk Automation Platform v.2.00 (CPR 7) or earlier or if your system includes many third-party OPC servers and devices.
  When this setting is changed from **DCOM** to **TCP/IP**, an audit message is logged to FactoryTalk Diagnostics indicating that the value changed from **False** to **True**. |
| DCOM                     | This is a proprietary communications protocol owned and managed by Microsoft.  
  Choose this option if:  
  - Most of the clients and servers on your automation network are using older versions of FactoryTalk Automation Platform (v. 2.00, CPR 7 or earlier)  
  - Your system includes third-party OPC servers and devices.
  When this setting is changed from **TCP/IP** to **DCOM**, an audit message is logged to FactoryTalk Diagnostics indicating that the value changed from **True** to **False**. |

See also

- [Change the default communications protocol](#) on page 77
- [FactoryTalk Directory types](#) on page 13

**Live Data Policy Properties**

How do I open **Live Data Policy Properties**?

In the **Explorer** window, expand **System > Policies > System Policies**.  
Double-click **Live Data Policy**.

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” because if the FactoryTalk Live Data service detects that some components on the network are not compatible with the selected policy setting, it 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 will not attempt a TCP/IP connection and will always use DCOM.

Change this setting only if necessary, for example, if your system is experiencing communications problems and you want to switch to DCOM for troubleshooting purposes. 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.

Important: Changing this policy setting can have unexpected results. Do not change this setting in a running production system. For changes to take effect, all computers on the network must be shut down and restarted.

See also

- Change the default communications protocol on page 77
- Default communications protocol settings on page 77
- FactoryTalk Directory types on page 13

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 the Explorer window, expand System > Policies > System Policies.
2. Double-click Health Monitoring Policy.
3. Under Rates, click to select the policy setting you wish to edit. A description of the policy appears at in the bottom pane of the window.
4. To the right of the current rate, click the **down arrow** button to enter a new number, or use the small up and down arrows to choose a higher or lower number.

5. Click **OK**.

**See also**

Health Monitoring Policy Properties settings on page 81

How do I open Health Monitoring Policy Properties?

1. Run FactoryTalk Administration Console or FactoryTalk View Studio.

2. In the Explorer window, expand the folders **System > Policies > System Policies**.

3. Double-click the **Health Monitoring Policy** icon.

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.

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.

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

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

**See also**

Set network health monitoring policies on page 79

Health Monitoring Policy Properties settings on page 81
Health Monitoring Policy Properties settings

Use the Policy Settings tab in Health Monitoring Policy Properties to fine tune the parameters that the health monitoring service uses when determining whether a network failure is occurring and how long to wait before switching to a standby server. The health monitoring service policies are described below.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Rates</th>
</tr>
</thead>
</table>
| 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. | • Default. 2 seconds  
• Minimum. 1 second  
• Maximum. 600 seconds |
| 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 it establishes 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. | • Default. 2 seconds  
• Minimum. 1 second  
• Maximum. 600 seconds |
| Maximum network glitch         | Sets the maximum duration of a network disruption before the health monitoring service determines that communications have 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. | • Default. 5 seconds  
• Minimum. 1 second  
• Maximum. 600 seconds |
| Maximum delay before server is active | 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, so when the switch back occurs, data is available to the clients as soon as possible. As soon as all clients successfully connect, the server switches over to active immediately, even if the maximum delay has not yet been reached. If the maximum delay is too short, the active server may not be able to provide high-quality service to its clients. You may notice poor client performance and a diagnostic message stating that the server has switched to active before all clients have finished connecting. | • Default. 2 minutes  
• Minimum. 0 minutes (not recommended)  
• Maximum. 60 minutes |

See also

Set network health monitoring policies on page 79
Health Monitoring Policy Properties on page 80

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, where you can view them using the FactoryTalk Diagnostics Viewer.
To set up audit policies

1. In the Explorer window, expand System > Policies > System Policies, and double-click Audit Policy.

2. In Audit Policy Properties, audit changes to configuration and control system, select one of the following from the drop-down button next to the current setting:

   - **Enabled** - Generates audit messages when configuration and control system changes occur across the FactoryTalk system. This is the default setting.
   - **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.

3. In Audit security access failures, select one of the following from the drop-down button next to the current setting:

   - **Enabled** - Generates audit messages when users fail to access objects or features because of insufficient security permissions.
   - **Disabled** - Does not generate audit messages when users fail to access secured objects or features. This is the default setting.

4. In Audit security access successes, select one of the following from the drop-down button next to the current setting:

   - **Enabled** - Generates 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 you have a specific reason for doing so, 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.

   - **Disabled** - Does not generate audit messages when users succeed in accessing objects or features because of sufficient security permissions. This is the default setting.

5. Click OK.
See also

Audit policies on page 83

Audit trails and regulatory compliance on page 32

Example: Audit messages on page 86

Audit policies

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

If you are in an industry that must comply with governmental regulations, such as U.S. Government 21 CFR Part 11, your plant must be able to answer this question. The answer is also important if your 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®, 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 should be 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 called Ingredients is secured so that only members of the Operators\Line5 group can write to it. 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 the *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. This policy should only be enabled 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 81
- [Audit trails and regulatory compliance](#) on page 32
- [Example: Audit messages](#) on page 86

**Audit Policy Properties**

How do I open Audit Policy Properties?
1. Start FactoryTalk Administration Console or FactoryTalk View Studio and then log on to the FactoryTalk Network Directory or FactoryTalk Local Directory where you want to modify audit policies.

2. In the Explorer window, expand the **System folder > Policies > System Policies**.

3. Double-click the **Audit Policy** icon.

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 you can view them using the FactoryTalk Diagnostics Viewer. Use the settings below to specify what information is audited by the FactoryTalk system.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit changes to configuration and control system</td>
<td>Determines whether to generate audit messages when configuration and control system changes occur across the FactoryTalk system.</td>
</tr>
<tr>
<td><strong>Default</strong>: Enabled</td>
<td>To disable audit logging, set this policy to <strong>Disabled</strong>. 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 <strong>Message Routing</strong> tab in <strong>Diagnostics Setup</strong>. Any changes made to the value of the <strong>Audit changes to configuration and control system</strong> policy itself are always recorded, regardless of whether audit logging is enabled or disabled. If enabled, audit information is sent to FactoryTalk Diagnostics.</td>
</tr>
<tr>
<td>Audit security access failures</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Default</strong>: Disabled</td>
<td>To record audit messages when users fail to access objects because of insufficient security permissions, set this policy to <strong>Enabled</strong>. If enabled, audit information is sent to FactoryTalk Diagnostics.</td>
</tr>
<tr>
<td>Audit security access successes</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Default</strong>: Disabled</td>
<td>To record audit messages when users succeed in accessing objects because of sufficient security permissions, set this policy to <strong>Enabled</strong>. When enabled, this policy might generate a large number of audit messages. Enable this policy only if you have a specific reason for doing so, 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.</td>
</tr>
</tbody>
</table>

**See also**

[Set audit policies](#) on page 81
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. You can 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 you have installed and the configuration options you have 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, choose 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 choose FactoryTalk Diagnostics > Viewer.

See also

Set audit policies on page 81

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 [PASTURIZE] to processor [/NetworkPath/Line1]
• Inserted rung [XIC B3/0 OTE B3/0] 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]
• 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 83

Set system security policies

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

You can modify the following:

• Account policy settings
• Computer policy settings
• Directory protection policy settings
• Password policy settings
• Single sign-on policy settings

See also

Modify account policy settings on page 88
Modify computer policy settings on page 89
Modify directory protection policy settings on page 91
Modify account policy settings

Use Security Policy Properties to change the following user account policy settings:

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


3. 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, double-click 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.

4. 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.

5. To specify the amount of time that must expire before a locked account is reset and the user can attempt access again, click Account lockout auto reset and type a value between 0 and 999 minutes.

6. To determine whether or not the system maintains a record of deleted user accounts, double-click Keep record of deleted accounts, and select one of the following:
• **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, you may need 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 will have different account identifiers and will not inherit the security settings of the account.

7. If deleted account records are kept, you may choose whether or not to list deleted account records in the *Users* folder in the *System* tree. Double-click **Show deleted accounts in user list**, and select one of the following:

   • **Enabled**—Administrators can view details about these deleted user accounts

   • **Disabled**—Deleted accounts are not shown in the list of user accounts

8. When you have finished modifying account policy settings, click **OK**.

**See also**

- [Account policy settings](#)
- [Set system security policies](#)
- [Audit trails and regulatory compliance](#)
- [Enable single sign-on](#)

**Modify computer policy settings**

Use **Security Policy Properties** to change the following policy settings for computer accounts:

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

3. To change the requirements for connecting to the FactoryTalk Directory from a computer that does not have a FactoryTalk computer account, double-click **Require computer accounts for all client machines** and select one of the following:

- **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.

4. To determine what computer name identifies clients connecting to the FactoryTalk Directory through Remote Desktop Services, double-click **Identify terminal server clients using the name of** and select one of the following:

- **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 will be 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.

5. When you have finished modifying account policy settings, click **OK**.
### Important:

If you set **Identify terminal server clients using the name of** 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](page 96)
- [Set system security policies](page 87)
- [Enable single sign-on](page 93)

**Modify directory protection policy settings**

Use **Security Policy Properties** to change the policy settings 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 settings**

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

2. In **Security Policy Properties**, click + to expand **Directory Protection Policy Settings**.

3. 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, double-click **Support non-secure clients** and select **Deny**. Clients with FactoryTalk versions earlier than 2.50 are denied access and a **Protocol version mismatch** error occurs.

4. 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 you do not want the message to be created, double-click in **Audit non-secure client connections** and select **Disabled**.

5. 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 expire, double-click **Directory cache expiration** and...
type or select a number from 1-9999. When the time limit is reached, you
must reconnect to the server to access the files.

6. By default, you will not get warnings prior to cache expiration, but you can
still see notifications upon disconnection and cache expiration. Click in
Directory cache expiration warning and type a number from 1-24 to set
the number of hours before cache expiration when a warning notification is
displayed.

7. When you have finished modifying directory protection policy settings,
click OK.

---

Important: If you set Identify terminal server clients using the name of 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 96

Set system security policies on page 87

Enable single sign-on on page 93

Modify password policy settings

Use Security Policy Properties to set the conditions for a valid FactoryTalk
password, such as minimum and maximum password length, password complexity
requirements, and when a password expiration warning is given.

These policies do not apply to Windows®-linked user accounts.

To modify password policy settings

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

2. In Security Policy Properties, click + to expand Password Policy
Settings.

3. By default, FactoryTalk allows user passwords to contain any characters or
combinations of characters. To require users to create more secure
passwords, double-click Passwords must meet complexity requirements
and select Enabled. The complexity requirements are defined by the system
and cannot be changed.

4. If Passwords must meet complexity requirements is set to Enabled, the
minimum password length is 6 characters and this policy overrides any
setting made here. To require a longer password, double-click Minimum
password length and enter a number higher than 6. If Passwords must meet complexity requirements is set to Disabled, enter a minimum password length of up to 16 characters. If you set Minimum password length to 0, you can create user accounts without passwords.

5. By default, 3 new passwords must be created before an old password can be reused. If Previous passwords remembered is set to 0, old passwords can be reused immediately. To prevent users from keeping the same password indefinitely, double-click Passwords must meet complexity requirements and select a number between 1 and 24.

6. To require users to wait at least one day before changing their password, double-click Minimum password age and enter a number between 1 and 999.

7. To set the maximum number of days before passwords expire, double-click Maximum password age and enter a number between 1 and 999. When set to 0, passwords never expire.

8. By default, users receive a warning 14 days before their passwords expire. To change the number of days before the system begins prompting users to change their passwords, double-click Password expiration warning and enter a value between 0 and 999.

See also

Password Policy Settings on page 99
Set system security policies on page 87
Add a FactoryTalk user account on page 39

Enable single sign-on

Use Security Policy Properties to enable single sign-on capability. When the single sign-on is enabled, it allows you to log on just once, per directory, on a given computer. Once you log 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. Open the System folder, and then open Policies > System Policies and double-click Security Policy.

2. In the Single Sign-On Policy Settings list, to the right of Use single sign-on, click in the Disabled field.

3. Use the down arrow to choose Enabled, then click OK.
If single sign-on still does not seem to be working properly, it is likely that the FactoryTalk product you are using does 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 94
- Set system security policies on page 87

### Disable single sign-on

To require users to log into each FactoryTalk product separately, use Security Policy Properties to disable single sign-on capability.

#### To disable single sign-on

1. Open the System folder, and then open Policies > System Policies and double-click Security Policy.

2. In the Single Sign-On Policy Settings list, to the right of Use single sign-on, click in the Enabled field.

3. Use the down arrow to choose Disabled, then click OK.

See also

- Enable single sign-on on page 93

### Account policy settings

Use the following Account Policy Settings to specify how FactoryTalk manages policies for user, computer, and group accounts. A few additional policy settings for computer accounts are managed in Computer Policy Settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Logon session lease| 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 having access indefinitely, even after their accounts are disabled or deleted. If a user’s account has, for example, been 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. Setting this value to 0 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.  
  **Minimum:** 0 hours  
  **Maximum:** 999 hours  
  **Default:** 1 hour |
### Account lockout threshold

Sets the number of consecutive times a user can unsuccessfully attempt to log on before the account is locked. If set to 0, accounts are never locked.

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 by a process of elimination.

**Minimum:** 0 invalid logon attempts  
**Maximum:** 999 invalid logon attempts  
**Defaults:**  
- For the Network Directory, 3 invalid logon attempts.  
- For the Local Directory, 0 invalid logon attempts.

### Account lockout auto reset

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.

If set to 0, locked accounts are not reset automatically, and must be unlocked manually by a FactoryTalk administrator.

**Minimum:** 0 minutes  
**Maximum:** 999 minutes  
**Default:** 15 minutes

### Keep record of deleted accounts

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.

To keep a record of accounts that have been deleted, and force all new accounts to be unique, select **Enabled**. You can also change a policy setting to show deleted accounts in the list of users.

To discard accounts when they are deleted, select **Disabled**. 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.

If the policy is disabled and you recreate a user account with the same name, the new user account does not inherit the security settings of the old account. This is because all user accounts are identified by means of a unique identifier that is separate from the user name. When you delete a user account, the user’s access rights are deleted, but the user account’s unique identifier is not deleted.

When you create another user account with the same name, you must recreate the security settings of the account. You can do this either by adding the user account to a group that already has security settings defined for it, or you can create permissions for a user account when securing a resource.

For security and audit tracking reasons, and to satisfy compliance requirements in regulated manufacturing industries, it might be necessary to:  
- Keep a record of previously deleted accounts  
- Ensure that all user accounts can be uniquely identified in the system

**Default:** Disabled

### Show deleted accounts in list

Sets whether deleted account records are listed in the **Users** folder in the System tree. This policy works together with the **Keep record of deleted accounts** policy. If **Keep record of deleted accounts** is enabled, enabling **Show deleted accounts in user list** allows a FactoryTalk administrator to view details about accounts that have been deleted.

To hide deleted accounts in the list of users, select **Disabled**. This means that accounts that you delete are not shown in the list of user accounts, even if you keep a record of deleted accounts. Enable the **Show deleted accounts in user list** policy if you keep a record of deleted accounts (for example, for regulatory compliance), and want to view details about accounts that have been deleted.

**Default:** Disabled

---

**See also**

- [Modify account policy settings](#) on page 88  
- [Audit trails and regulatory compliance](#) on page 32  
- [Set system security policies](#) on page 87
## Computer policy settings

The policies in this table apply only to computer accounts in the FactoryTalk network directory because the FactoryTalk local directory does not permit remote access.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
Important: If you set Identify terminal server clients using the name of 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 89
Set system security policies on page 87

Directory protection policy settings

The Directory protection policy settings below apply only to computers in the FactoryTalk network directory.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support non-secure clients</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Allow 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.</td>
</tr>
<tr>
<td></td>
<td>Deny 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 Protocol version mismatch error occurs.</td>
</tr>
<tr>
<td></td>
<td>Default: Allow</td>
</tr>
<tr>
<td></td>
<td>The directory server must be disconnected from the network before you change this policy. Reconnect to the network after applying the change. Otherwise, this policy will not be properly enforced.</td>
</tr>
<tr>
<td>Audit non-secure client connections</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Enabled 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.</td>
</tr>
<tr>
<td></td>
<td>Disabled 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.</td>
</tr>
<tr>
<td></td>
<td>Default: Enabled</td>
</tr>
<tr>
<td>Directory cache expiration</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>If this is set to 0, cache files never expire.</td>
</tr>
<tr>
<td></td>
<td>Minimum: 0 hours</td>
</tr>
<tr>
<td></td>
<td>Maximum: 9999 hours</td>
</tr>
<tr>
<td></td>
<td>Default: 0 hours</td>
</tr>
<tr>
<td>Directory cache expiration warning</td>
<td>Determines when a warning notification is displayed in the notification area prior to the directory cache expiring. You can click the FactoryTalk Directory icon in the notification area to quickly view the time expiration information.</td>
</tr>
<tr>
<td></td>
<td>If this is set to 0, you will not get warnings prior to cache expiration. However, you can still see notifications upon disconnection and cache expiration.</td>
</tr>
<tr>
<td></td>
<td>Minimum: 0 hours</td>
</tr>
<tr>
<td></td>
<td>Maximum: 24 hours</td>
</tr>
<tr>
<td></td>
<td>Default: 0 hours before expiration</td>
</tr>
</tbody>
</table>
See also

Modify directory protection policy settings on page 91

Cache expiration policies

In FactoryTalk, rules for directory cache expiration are managed system-wide in Security Policy Properties. These policies determine:

- how long cache files remain available after the client computer is disconnected from the server
- if a warning is displayed before the directory cache expires

In some circumstances you may wish to customize directory cache expiration policies for a specific computer or group of computers. For example, you may wish to allow a group of laptop computers to operate without a network connection for a longer period of time, and for the cache to never expire for one of the laptops. To override the FactoryTalk network directory cache expiration policies, you may set directory cache timeout policies for a computer group or an individual computer.

You cannot modify the directory cache timeout policies 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 the following 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.

The example below shows how the cache expiration policies work.

Suppose that:

- There are 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.
Although the current setting covers the majority of your computers, you have the option to customize specific settings for some cases. Suppose you want to allow computers of Laptops to operate in a disconnected state for a longer period (for example, 7 days, that is, 168 hours). You also want to 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 91

About FactoryTalk Security on page 25

Password policy settings

Passwords for FactoryTalk user accounts can be up to 16 characters long. A set of password policies determines how long or how complex passwords must be. 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 you do not want to use a password for Windows-linked accounts, on your local computer disable the Windows local security policy called Accounts: Limit local account use of blank passwords to console logon only. Define password policies for Windows-linked accounts in Windows.

For FactoryTalk user accounts, use Security Policy Properties to adjust these password policy settings:
- Password complexity
- Minimum password length
- Number of previous passwords remembered
- Minimum password age
- Maximum password age
- Password expiration warning

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Passwords must meet complexity requirements | Determines how simple or complex passwords must be. **Disabled** means that passwords to user accounts can include any characters or combinations of characters. **Enabled** requires users to create passwords that are more secure, because passwords used for user accounts:  
- Cannot contain all of the user account name. For example, a user account called 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.  
- Must contain at least six characters (you can change the minimum value using the Minimum password length policy)  
- Must contain characters from three of the following four categories:  
  - Unaccented uppercase characters (A to Z)  
  - Unaccented lowercase characters (a to z)  
  - Numerals (0 to 9)  
  - Non-alphanumeric characters (!, @, #, %)  
If enabled, any passwords that do not meet these minimum requirements will be rejected, and the user will be prompted to create a password that satisfies the criteria. These complexity requirements are defined by the system and you cannot change them.  
**The Passwords must meet complexity requirements policy overrides the Minimum password length policy if the minimum password length is less than 6 characters. If the minimum password length is greater than 6 characters, Minimum password length takes precedence.**  
**Default:** Disabled. |
| Minimum password length                      | Sets the minimum number of characters a password to a user account must contain. A value of 0 allows you to create user accounts without passwords.  
If enabled, the Passwords must meet complexity requirements policy requires a minimum password length of 6 characters. However, if the Minimum password length policy is set to more than 6 characters, this overrides the Passwords must meet complexity requirements policy.  
Minimum: 0 characters. A value of 0 means that you can create user accounts without passwords.  
Maximum: 16 characters  
**Defaults:**  
- For the network directory, 6 characters.  
- For the local directory, 0 characters. This means that users can set the passwords to their accounts to be blank. |

---

100 Rockwell Automation Publication FTSEC-QS001M-EN-E
## Set system policies

### Previous passwords remembered

Sets the number of unique new passwords that must be created before an old password can be reused. If set to 0, old passwords can be reused immediately. This policy allows you to ensure that old passwords are not continually reused.

To maintain the effectiveness of the Previous passwords remembered policy, set the Minimum password age policy to a non-zero value to prevent passwords from being changed immediately. This policy is also necessary to make the Maximum password age policy meaningful. If this policy is set to zero, users can immediately re-use their existing passwords when their passwords expire.

- **Minimum:** 0 passwords
- **Maximum:** 24 passwords
- **Default:** 3 passwords

### Minimum password age

Sets the minimum number of days passwords must be in effect before they can be changed. If set to 0, users can change their passwords immediately following a prior change.

This policy works together with the Previous passwords remembered policy to prevent a user from changing a password repeatedly until one of the user's old password favorites can be used again.

If the value of the Minimum password age is greater than the value of the Maximum password age, the minimum password age is ignored.

- **Minimum:** 0 days
- **Maximum:** 999 days
- **Default:** 0 days. This means that users can change their passwords at any time.

### Maximum password age

Sets the maximum number of days passwords can be used before they must be changed. If set to 0, passwords never expire. When setting this value, be sure also to specify a smaller value for the Password expiration warning.

If the Maximum password age expires, the user is prompted to change the password when next logging on with the account.

If the value of the Maximum password age policy is less than the value of the Minimum password age policy, the minimum password age is ignored.

- **Minimum:** 0 days
- **Maximum:** 999 days
- **Default:** 0 days. This means that users are never prompted to change their passwords.

### Password expiration warning

Sets the number of days before passwords are due to expire that the system begins prompting users to change their passwords.

If Maximum password age is set to 0, the password expiration warning never appears.

If the value of the Password expiration warning is greater than the value of the Maximum password age, a password expiration warning appears the next time the user attempts to log on.

- **Minimum:** 0 days before expiration
- **Maximum:** 999 days before expiration
- **Default:** 14 days before expiration

---

**See also**

- Add a FactoryTalk user account on page 39
- Add a Windows-linked user account on page 41
- Set system security policies on page 87
- Security Policy Properties on page 103

---

**Single sign-on policy settings**

Use the 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 called **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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>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 necessary access rights, the action is prevented from taking place. The user is not prompted repeatedly to log on with a user name and password.</td>
</tr>
<tr>
<td>Disabled</td>
<td>Requires users to log on to each FactoryTalk product separately.</td>
</tr>
</tbody>
</table>

**See also**

- [When to disable single sign-on](#)
- [Modify computer policy settings](#)
- [Set system security policies](#)

**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 you need to be able to distinguish the actions of individual users, 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 called **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, it is likely that the FactoryTalk product you are using does 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](#)
Security Policy Properties

How do I open Security Policy Properties?

1. Start FactoryTalk Administration Console or FactoryTalk View Studio and then log on to the FactoryTalk Network Directory or FactoryTalk Local Directory where you want to modify security policies.

2. In the Explorer window, expand the System > Policies > System Policies folders.


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

Security policy includes:

- Account policy settings—including lockout policies, and whether or not a record of deleted users is kept
- Computer policy settings—such as whether a user can access FactoryTalk from any computer
- Directory protection policy settings—including how long cache files remain after the client computer logs off the server
- Password policy settings—including password complexity and how often a password must be changed
- Single sign-on policy settings—determines if users can log on to FactoryTalk just once or must log on to each FactoryTalk product separately

See also

- Modify account policy settings on page 88
- Modify computer policy settings on page 89
- Modify password policy settings on page 92
- Enable single sign-on on page 93
- Navigate the Policy Properties windows on page 104
Navigate the Policy Properties windows

All of the Product Policies and System Policies windows contain the same features to help you navigate to the property setting you want to edit.

To navigate the Policy Properties windows

- To sort the policy settings alphabetically, click the Alphabetic button.
- To sort the policy settings by category, click the Categories button.
- In the Category view, to expand or collapse lists of policy settings, click the + or – icons.
- To change a setting, click the setting you want to change, and then select or type a new value.
- To change the size of any column, move the cursor over a column heading until you see a cross-bar shape, and then click 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

Set system security policies on page 87

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. Click Export.
See also

Export Policies on page 105

Set system security policies on page 87

Export Policies

How do I open Export Policies?

- From the Tools menu, select Export Policies.

Use Export Policies to create an XML file containing the current FactoryTalk Directory policy settings.

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.

See also

Export policies to XML on page 104

Set system security policies on page 87
Set product-specific policies

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

For example, when you set up product policies for RSLinx Classic, you might restrict the ability to shut down the RSLinx Classic service to a small group of users, to prevent parts of your automation system from going down at runtime.

A product policy is a collection of securable features in a FactoryTalk product. A product policy applies to only one product—if you are denied access to a product feature, you cannot use that feature when using that product, but you may use the feature in other FactoryTalk products.

View and edit permissions:

- For features of a single product in that product’s Feature Security Properties
- For features of multiple products at the same time in Feature Security for Product Policies

Typically, you will want to restrict access to features of multiple products at once. For FactoryTalk Linx Gateway, however, you have to configure security on a feature-by-feature basis.

See also

- Secure features of a single product on page 107
- Secure multiple product features on page 108
- Differences between securable actions and product features on page 111

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 where you want to configure product policies.
2. In the Explorer window, expand System > Policies > Product Policies.

3. In the Product Policies folder, expand the folder for the product whose features you want to secure and then double-click Feature Security.

4. In Feature Security Properties, click the row containing the feature you want to secure. A description of the feature appears at the bottom of the window.

5. Configure the security settings for the feature:
   - If the product policy contains settings that you can configure using drop-down lists, configure the settings, click OK, and then skip the rest of the steps.
   - If the product policy is not configured using drop-down lists, in the column on the right, click Browse (...) beside Configure Security.

6. Use Configure Securable Action to select the users or user groups that can access the feature, and click OK.

7. Repeat steps 4-6 as needed to configure the features that make up your product policy.

8. Click OK.

See also

Feature Security for Product Policies on page 110

Permissions on page 132

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 you install provides different securable features (actions).

Click the plus (+) icon next to each FactoryTalk product to view the features you may secure.

To secure multiple product features

1. Log on to the FactoryTalk Directory where you want to configure product policies.

2. In the Explorer window, expand System > Policies.

3. Right-click Product Policies, and then click Configure Feature Security.
4. (optional) To add a user and computer to the Users list, click Add. In Select User and Computer, select a user or group of users, and a computer or group of computers, and click OK.

5. In Feature Security for Product Policies, do one of the following:

- To specify which features a selected user can perform, click User.
- To specify which users can access a selected feature, click Action. Skip to step 7.

6. To set permissions by user:

- In the Users list, click to select the user or user group whose access you need to secure.
- In the Actions list, expand the list of products and categories as needed to locate the feature you wish to secure, and click to select the feature.
- Skip to step 8.

7. To set permissions by feature:

- In the Actions list, expand the list of products and categories as needed to locate the feature you wish to secure, and click to select the feature.
- In the Users list, click to select the user or group for whose access to the feature you need to secure.

8. Specify security settings as follows:

- To allow a user to perform the action, select the Allow check box.
- To deny a user access to the action, select the Deny check box.
- If you clear both the Allow and Deny check boxes, the user is denied access to the feature.

9. Repeat steps 5–8 as needed to secure additional product features.

10. Click OK.

See also

Secure features of a single product on page 107

Permissions on page 132

Differences between securable actions and product policy features on page 111
How do I open Feature Security for Product Policies?

1. Start FactoryTalk Administration Console or FactoryTalk View Studio and then log on to the FactoryTalk Directory where you want to configure product policies.

2. In the Explorer window, expand the Network or Local FactoryTalk Directory tree, and then expand the folders System > Policies.

3. Right-click Product Policies, and then click Configure Feature Security on the context menu. You can also right-click any of the individual product categories and then click Configure Feature Security to configure policies for just that product.

Use the Permissions tab in Feature Security for Product Policies to secure features in multiple FactoryTalk products at the same time. If you are using both a local and a network FactoryTalk Directory you must configure product policies in each directory separately.

Tip: Security for FactoryTalk Linx Gateway must be configured one feature at a time.

### Setting Description

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| View permissions by | View the same set of permissions from two different points of view:  
  • by user — Click User, select a user and then specify what product features that user can access  
  • by action — Click Action, select a product feature and then specify which users can perform the feature |
| Add            | Click Add to add a user and computer to the list.                                                                                           |
| Remove         | Click Remove to remove a user and computer from the list.                                                                                   |
| Action list    | The term action in Feature Security for Product Policies refers to a product feature. Each FactoryTalk product you install provides different securable features (actions).  
  Click the plus (+) icon next to each FactoryTalk product to view the features you may secure. For more information about each product, refer to the product’s documentation. |
| Allow          | Click to allow access to a product feature.                                                                                                 |
| Deny           | Click to deny access to a product feature.                                                                                                  |
| Allow and Deny | Clear both check boxes to deny access to the feature.                                                                                       |

See also

- Secure multiple product features on page 108
- Permissions on page 132
- Things you can secure on page 28
- Differences between securable actions and product policy features on page 111
How do I open Feature Security Properties?

1. Start FactoryTalk Administration Console or FactoryTalk View Studio and then log on to the FactoryTalk Directory where you want to configure product policies.

2. In the Explorer window, expand the System folder > Policies > Product Policies, expand the folder for the product whose policies you want to secure, and then double-click the type of product policies you want to secure for the product.

Use the Policy Settings tab in Feature Security Properties to secure a single feature of a FactoryTalk product. You may secure other features of the same product in Feature Security Properties, but this is not the most efficient way to do so.

Policy settings are completely separate in the network directory and local directory. Changes you make to the policy settings in one directory do not apply to the other directory.

See also

- Secure features of a single product on page 107
- Secure multiple product features on page 108
- Differences between securable actions and product features on page 111

Differences between securable actions and product features

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 you are denied permission to a product feature, you cannot use that product feature when using that product.

In some cases, there are securable actions and product policies for the same capability. For example, Logix Designer application has both a securable action and a product policy called Firmware: Update.

- The securable action applies to all products—if you are denied permission to the Firmware: Update action in an application or area, you cannot update firmware in the controller from that application or area using any product.
• The product policy applies to only Logix Designer application—if you are denied permission to **Firmware: Update**, you cannot update firmware 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 the **Allow** and **Deny** check boxes does not allow the policy setting to inherit security. Instead, clearing both check boxes denies access to the product feature.

For details about securable actions and product policies in a particular FactoryTalk product, see the documentation for your product.

**See also**

- [Secure features of a single product](#) on page 107
- [Secure multiple product features](#) on page 108
- [Secure resources](#) on page 131
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.

You must define logical names in FactoryTalk Administration Console before configuring security for RSLogix 5000 controllers. For all other types of control hardware, you can choose whether to associate security settings with logical names or with network relative paths.

In addition, 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.

You can:

- Add a logical name
- Delete a logical name
- Add a logical name to an area or application
- Remove a logical name from a an area or application
- Add a device to a logical name
- Remove a device from a logical name

See also

- Logical names on page 114
- Add a logical name on page 115
- Add a device to a logical name on page 116
- Assign a control device to a logical name on page 117
- Add a logical name to an area or application on page 118
A logical name is an alias that identifies a control network or device. You can use the 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.

**Why use logical names?**

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.

You must add logical names in FactoryTalk Administration Console before configuring security for RSLogix 5000 controllers. For all other types of control hardware, you can choose whether to associate security settings with logical names or with network relative paths. You might choose to add logical names as aliases for control devices with multiple paths, to associate each instance of the device with a single set of security permissions.

**What happens when you add a logical name?**

If you add 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. After defining a new logical name, you must also 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.

If you configure security on a control device identified by a network relative path, and then later you add a logical name for the device, the original security permissions are not lost; they remain associated with the path, but they do not transfer to the 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.

If you later change a control device’s logical name, the original security permissions remain associated with the first logical name. You must re-add security permissions for the device, to associate them with the new logical name.

**What happens when you delete a logical name?**

When you delete a logical name, the security system automatically uses the security permissions associated with the device's network relative path.

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."

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.

See also

Add a logical name on page 115
Delete a logical name on page 116

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.

You must add logical names in FactoryTalk Administration Console before configuring security for RSLogix 5000 controllers. For all other types of control hardware, you can choose whether to associate security settings with logical names or with network relative paths.

Follow the steps below to add a logical name without associating it with an area or application. Use Resources Editor to associate the logical name with an area or application.

Alternatively, you can 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.

To add a logical name

1. In Explorer, expand the Networks and Devices tree until Logical Names is visible.

2. Right-click Logical Names and click New Logical Name.
3. In **New Logical Name**, enter the name for your new logical name. For an RSLogix 5000 controller, type a name that is identical to the device name stored in the controller.

4. Click **OK**.

**See also**

- Add a logical name to an area or application on page 118
- Add a device to a logical name on page 116
- Delete a logical name on page 116

**Delete a logical name**

Delete a logical name from **Networks and Devices** when you no longer need the logical name as an alias for a control device or network. When you delete 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 the **Explorer** window, expand the **Networks and Devices** tree until **Logical Names** is visible.

2. Right-click on the logical name you wish to delete, and click **Delete**.

**See also**

- Add a logical name on page 115
- Delete a logical name from an area or application on page 119
- Logical names on page 114

**Add a device to a logical name**

Use **Logical Name Properties** to add control devices or networks to a logical name. When you add a device or network to a logical name, its associated devices inherit the security permissions of the logical name.

**To add devices to a logical name**

1. In the **Explorer** window, expand the **Networks and Devices** tree until the logical name you wish to edit is visible.

2. Right-click the logical name, then click **Properties**.
3. In **Logical Name Properties**, click **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. Click **OK**.

**See also**

- **Remove a device from a logical name** on page 117
- **Delete a logical name** on page 116

**Remove a device from a logical name**

Use **Logical Name Properties** to remove a device from a logical name when you longer wish to associate the device with the 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 the **Explorer** window, expand the **Networks and Devices** tree until the logical name you wish to edit is visible.

2. Right-click the logical name, then click **Properties**.

3. In **Logical Name Properties**, in the **Device members** list, click to select a device or network you wish to delete from the logical name.

4. Click **Remove**, then click **OK**.

**See also**

- **Assign a control device to a logical name** on page 117
- **Delete a logical name** on page 116

**Assign a control device to a logical name**

A logical name is an alias that identifies a control network or device. You must 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 a logical name. You may add a 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 the Networks and Devices tree until the network or device you want to create an alias for is visible.

2. Right-click on the network or device icon and click Properties.

3. In Device Properties, the Logical name list displays the current logical name the device or network it is assigned to.

4. Do one of the following:
   - To assign a new logical name, select <New...>. In New Logical Name, enter a descriptive name and click OK.
   - To select from an existing logical name, or to change the logical name associated with the device, click the Logical name drop-down and select the logical name you want to assign the device to.

5. Click 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. You must 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 117
- [Add a logical name to an area or application](#) on page 118

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. You must add logical names before configuring security for RSLogix 5000 controllers. For all other types of control hardware, you can choose whether to associate security settings with logical names or with network relative paths.

Add a logical name to an area or application when you want the permissions associated with the logical name to be inherited from that area or application.

**Prerequisites**

Obtain the following permissions in the area or application where you want to add a logical name:
• Common > Create Children
• Common > List Children
• Common > Read

To add a logical name to an area or application

1. In the Explorer window, right-click the application or area you want to add the logical name to, and click Resource Editor.

   In Resources Editor, the area or application appears selected.

2. Click Manage Resources.

3. In Select Resources, click Add New Logical Name.

4. In New Logical Name, type a name for the logical name, and click OK.

See also

Logical names on page 114

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

Obtain the following permissions for the application or area in the Explorer window:

• Common > Delete
• Common > List Children
• Common > Read

To delete a logical name from an area or application

1. In the Explorer window, 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 click Resource Editor.

3. In the Resources Editor, the application is selected in the Areas list.

4. In the Associated Resources list, click to select the logical name you wish to delete, and click Cut.

5. Click Close.
See also

Logical names on page 114

How do I open New Logical Name?

1. Start FactoryTalk Administration Console or FactoryTalk View Studio and then log on to the FactoryTalk Network Directory or FactoryTalk Local Directory where you want to edit devices.

2. Expand the Explorer tree until the application or area containing the resource grouping you want to edit is visible.

3. Right-click the application or area, and then click Resource Editor on the context menu.

4. In the Resources Editor dialog box, click Manage Resources. In the Select resources for dialog box, do one of the following:

   • To edit the devices belonging to an existing logical name, expand the Logical Names folder, right-click the logical name whose device members you want to edit, and then click Properties on the context menu.

   • To create a new logical name and add devices to it, click the Add New Logical Name button. In the New Logical Name dialog box, type a logical name and then click OK.

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.

After you create a new logical name, type a descriptive name to identify it.

   • If New Logical Name is opened from an application or area in the Explorer window, the new logical name is assigned to the application or area.

   • If New Logical Name is opened from the Logical Names tree in the Explorer window, use the Resources Editor to assign the new logical name to an application or area.
See also

Add a logical name on page 115
Add a logical name to an area or application on page 118
Resources Editor on page 128

Logical Name Properties

How do I open Logical Name Properties?

1. Start FactoryTalk Administration Console or FactoryTalk View Studio and then log on to the FactoryTalk Network Directory or FactoryTalk Local Directory where you want to edit devices.

2. Expand the Explorer tree until the application or area containing the resource grouping you want to edit is visible.

3. Right-click the application or area, and then click Resource Editor on the context menu.

4. In the Resources Editor dialog box, click Manage Resources. In the Select resources for dialog box, do one of the following:

   • To edit the devices belonging to an existing logical name, expand the Logical Names folder, right-click the logical name whose device members you want to edit, and then click Properties on the context menu.

   • To create a new logical name and add devices to it, click the Add New Logical Name button. In the New Logical Name dialog box, type a logical name and then click OK.

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.
Chapter 11  Manage logical names

### Setting Description

**Logical name**
Select a logical name to edit the control devices associated with it. To create a new logical name, select New and then, in **New Logical Name**, 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, click **Add**. You can add multiple devices to a single logical name, but you cannot add a single device to multiple logical names. To save changes, click **Apply**.

To remove a device from the selected logical name, click the device and then click **Remove**.

**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, click **Remove**.

---

**See also**

- [Add a logical name](#) on page 115
- [Add a device to a logical name](#) on page 116
- [Remove a device from a logical name](#) on page 117

**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**
This field displays the network relative path of the device whose properties you are viewing. The information in this field appears only as a reference. You cannot edit this field.
### 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 one of the following:

- To create a new logical name, select `<New...>`. In **New Logical Name**, enter a descriptive name and click **OK**.
- To select from an existing logical name, or to change the logical name associated with the device, click the **Logical name** drop-down and select the logical name you want to assign the device to.
- To remove the logical name the device is associated with, select **None**. The security system automatically uses the security permissions associated with the device’s network relative path.

### 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, click **Remove**. This removes the logical name from the resource grouping.

---

**See also**

- [Assign a control device to a logical name on page 117](#)
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 to define 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 may 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 126
Move a resource between areas on page 127
Remove a device from a resource grouping on page 128
Resource groupings on page 125

A resource grouping is a collection of hardware resources from the Networks and Devices tree that is associated with an application or area. It 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 having to set permissions for each device separately.

You can create a resource grouping in any application or area in the FactoryTalk Directory by selecting resources to be associated with the area in the Resources Editor. You may add or delete resources at any time. 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 you defined specifically for the area, or they might be inherited from the application the area is located in, or from the FactoryTalk Directory the application is located in. As always, you can set explicit permissions for a device, overriding security permissions set for its resource group. However, you set up these explicit permissions by browsing for the network or device in the **Networks and Devices** tree, not in the application or area tree.

To prevent conflicting permissions, you cannot nest resource groupings within other resource groupings, and you cannot include 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 126
- [Remove a device from a resource grouping](#) on page 128
- [Permissions](#) on page 132

### Group hardware resources in an application or area

Group hardware resources in an application of area if you prefer 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**

To group hardware resources together in an application or area, you must have the following security 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 the **Explorer** window, right-click any application or area and then click **Resource Editor**.

   The application is highlighted in the **Areas** list, which displays all applications and areas in the current FactoryTalk directory.

2. Click **Manage Resources**.

3. In **Select Resources**, expand the **Logical Names** folder or the **Networks and Devices** tree until you see the hardware resource you would like to add to the grouping.
If you would like to add a logical name, click one of the following to filter the list of logical names:

- Show only logical names not associated with areas
- Show all logical names

4. (Optional) To create a new logical name that can be added to a resource grouping, click Add New Logical Name.

5. Click on the resource you would like to add, and click the > button to move it into the Selected resources list.

6. Click OK.

See also

Move a resource between areas on page 127
Remove a device from a resource grouping on page 128
Resource groupings on page 125

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

To group hardware resources together in an application or area, you must have the following security permissions for the application or area:

- Common > Read
- Common > List Children
- Common > Configure Security

To move a resource between areas

1. In the Explorer window, right-click any application or area and then click Resource Editor.

2. In the Areas list, click the area containing the resource you want to copy.

3. In the Associated resources list, right-click the resource, and then click Cut.

4. In the Areas list, click the area you want to copy the resource to, right-click the Associated resources list again, and then click Paste.
5. Click Close.

See also

- Group hardware resources in an application or area on page 126
- Remove a device from a resource grouping on page 128
- Resource groupings on page 125

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 you remove a device 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 you click OK.

Prerequisites

Obtain the following security permissions for the application or area where the resource grouping is located:

- Common > Configure Security
- Common > List Children
- Common > Read

To remove a device from a resource grouping

1. In the Explorer window, right-click the application or area containing the resource grouping you wish to modify, and click Resource Editor.

2. In the Areas list of the Resources Editor, click the area or application containing the resource you want to delete.

3. In the Associated resources list, right-click the resource, and then click Cut.

4. Click Close.

See also

- Resource groupings on page 125

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 you want to modify resource groupings.

2. In the Explorer window, right-click any application or area and then click Resource Editor on the context menu.

Use Resources Editor to edit a resource grouping in an area or application. Click Manage Resources to add or remove resources, or to map resources to logical names.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Areas</td>
<td>This list displays the applications and areas in the FactoryTalk network directory, or the applications in the FactoryTalk local directory. Click an area or application to view the list of resources associated with it.</td>
</tr>
<tr>
<td>Associated resources</td>
<td>This list 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.</td>
</tr>
<tr>
<td></td>
<td>• To remove a resource, right-click the resource and then click Cut. When you remove 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. The changes take effect immediately when you click OK.</td>
</tr>
<tr>
<td></td>
<td>• To move a resource from one area to another, in the Areas list, click the area containing the resource you want to copy. In the Associated resources list, right-click the resource, and then click Cut on the context menu. In the Areas list, click the area you want to copy the resource to, right-click the Associated resources list again, and then click Paste.</td>
</tr>
<tr>
<td>Manage Resources</td>
<td>Click Manage Resources to add or remove resources in the selected application or area, or to map resources to logical names.</td>
</tr>
</tbody>
</table>

See also

- Group hardware resources in an application or area on page 126
- Remove a device from a resource grouping on page 128

Select Resources

Use Select Resources to associate resources with an application or area. The hardware devices can be referenced either by logical name or by network relative path. Use the following settings to specify how resources are added to the grouping.
### Setting | Description
--- | ---
Select resources to be associated with an area  | • To view the logical names for only those devices that are not already associated with an application or area, click **Show only logical names not associated with areas**. Ignore this setting if you are not using logical names with networks and devices.
• To view all logical names, even if they are already associated with an application or area, click **Show all logical names**. Ignore this setting if you are not using logical names with networks and devices.
• To add a logical name to the list of resources in the grouping, click the logical name and then click the > button. You cannot add the same network or device (represented by a logical name) to multiple resource groupings.
• To add a device using its network relative path, expand the **Networks and Devices** tree until the device you want to add is visible. Click the device and then click the > button. You cannot add the same network or device to multiple resource groupings.

Add New Logical Name | Click this button to create a new logical name for a device so that you can add the logical name to an application or area.

Delete Logical Name | Use this button to delete logical names that are no longer in use in the system, but remain visible in this dialog box. This can happen if you added a logical name, but later removed the device associated with that logical name. The **Delete Logical Name** button is disabled if the selected logical name is in use.

Selected resources | This list shows the resources that are associated with the application or area. To remove a resource from the list, click the resource and then click the < button.

**See also**

- [Group hardware resources in an application or area](#)
- [Resource groupings](#)
To secure the resources in your FactoryTalk system, you select the resource, and then 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 you have installed.

You may set security permissions for the following:

- 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 some special rules for inheriting security permissions, and includes the use of logical names, permission sets, and resource groupings. For this reason, it is covered in its own section: Secure networks and devices.

See also

Set FactoryTalk Directory permissions on page 140

View effective permissions on page 152

Actions on page 137
Permissions determine which users can perform which actions on specific resources in the system from which computers.

**Allow and Deny permissions**

There are two kinds of permissions that you can set 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, you could assign **Allow** permission to a Read action for a group of users called 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, you could assign **Deny** permissions to a Write action for a group of users called Designers from All Computers to prevent members of the Designers group from modifying the contents of the area.

You can also remove all permissions from an object by clearing both the **Allow** and **Deny** check boxes. This allows the object to inherit permissions assigned at a higher level. For example, if you remove all permissions from an area located in an application, the area 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 the **Allow** and **Deny** check boxes does not allow the policy setting to inherit security. Instead, clearing both check boxes denies access to the product feature.

**Inherited and explicit permissions**

By default, resources inherit permissions automatically from their parent resources. For example, if you assign 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.

You can 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, you can override the inherited permissions by specifying permissions explicitly for the area.

Explicit permissions are permissions you assign 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, you can stop an area from inheriting permissions from the application in which it is located by selecting the **Do not inherit permissions** check box when setting up security for the area.

When you break the chain of inheritance, you can 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 you to set permissions at as high a level as is practical, and then introduce 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. You can create your own action groups, so that you can assign security permissions to all of the actions in the group in one step rather than assigning permissions to each action separately.

**Effective permissions**

If you want to find out what actions a user or group can perform on a resource, you can view the permissions in effect (called 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, it means that permission is allowed, whether explicitly or by inheritance. If a check mark does not appear, it means that
permission is denied, whether explicitly or by inheritance. If a category (for example, Common) shows a gray check mark, it means that 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 134
- [Order of precedence](#) on page 136
- Secure resources on page 131
- View effective permissions on page 152

**Breaking the chain of inheritance**

By default, resources inherit permissions automatically from their parent resources. For example, if you assign 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.

You can 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, you can 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, you can stop an area from inheriting permissions from the application in which it is located by selecting the **Do not inherit permissions** check box when setting up security for the area. When you break the chain of inheritance, you can 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 can be inherited only as far up the network directory or local directory tree as the chain of inheritance remains intact. For example, if you select the **Do not inherit permissions** check box for an area, 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, you should only do so when absolutely necessary.

The principle of inheritance allows you to set permissions at as high a level as is practical, and then introduce exceptions at lower levels where necessary.

If permissions are not assigned at any level, **Deny** is implied.
See also

Permissions on page 132

Order of precedence on page 136

See also

Breaking the chain of inheritance on page 134

Permissions on page 132
Secure resources on page 131

Actions

When setting up security you specify which actions a user or group can perform on a selected resource. In a FactoryTalk network directory, you can also specify which computer or group of computers a user can perform the action from.

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 you have 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 window from a computer or group of computers.

<table>
<thead>
<tr>
<th>Resource type</th>
<th>Result of Denying &quot;Read&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network directory or local directory</td>
<td>Prevents users from seeing the directory or its contents.</td>
</tr>
<tr>
<td>Application</td>
<td>Prevents users from seeing the application or its contents. Denying Read does not prevent users from reading tag values from data servers in the application.</td>
</tr>
<tr>
<td>Area</td>
<td>Prevents users from seeing the area or its contents. Denying Read does not prevent users from reading tag values from data servers in the area.</td>
</tr>
<tr>
<td>System folder</td>
<td>Prevents users from seeing the System folder or its contents. Denying Read does not prevent users from reading tag values for devices in the Networks and Devices tree.</td>
</tr>
<tr>
<td>Networks and Devices tree</td>
<td>Prevents users from seeing the Networks and Devices tree and its contents. Denying Read does not prevent users from reading tag values for a particular device.</td>
</tr>
<tr>
<td>Individual network or device in the Networks and Devices tree</td>
<td>Prevents users from seeing the network or device and its contents. Denying Read does not prevent users from reading tag values for a particular device.</td>
</tr>
</tbody>
</table>

Write

Controls whether a user or group can write to the resource from a computer or group of computers.

<table>
<thead>
<tr>
<th>Resource type</th>
<th>Result of Denying &quot;Write&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network directory or local directory</td>
<td>Prevents users from modifying the properties of any item in the directory. For example, denying Write prevents users from modifying the description of an application, area, or the properties of a data server. However, if Create Children is allowed, the user or group can create applications in the directory, add areas to an application, and add data servers to areas.</td>
</tr>
<tr>
<td>Application</td>
<td>Prevents users from modifying the properties of any item in the application. For example, denying Write 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 Create Children is allowed, the user or group can add areas or data servers to an application, and can add data servers to areas.</td>
</tr>
<tr>
<td>Area</td>
<td>Prevents users from modifying the properties of any item in the area. For example, denying Write prevents users from modifying the description of the area, or the properties of data servers within the area. However, if Create Children is allowed, the user or group can add areas or data servers within the area.</td>
</tr>
</tbody>
</table>
System folder

Prevents users from modifying the properties of any item in the System folder. For example, denying Write prevents users from modifying policy settings, and the properties of user accounts, such as an account’s description or group memberships. Denying Write 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 Write action.

Networks and Devices tree

Prevents users from defining or undefining logical names for networks or devices. Denying Write does not prevent users from writing tag values to devices.

Individual network or device in the Networks and Devices tree

Prevents users from defining or undefining logical names for the network or device. Denying Write 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 clicking Security on the context menu.

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 directory tree while working from a computer or group of computers.

<table>
<thead>
<tr>
<th>Resource type</th>
<th>Result of Denying &quot;Create Children&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network directory or local directory</td>
<td>Prevents users from creating applications or areas.</td>
</tr>
<tr>
<td>Application</td>
<td>Prevents users from creating areas or data servers in the application.</td>
</tr>
<tr>
<td>Area</td>
<td>Prevents users from seeing the area or its contents. Denying Read does not prevent users from reading tag values from data servers in the area.</td>
</tr>
<tr>
<td>System folder</td>
<td>Prevents users from creating user, computer, or group accounts. Denying Create Children has no effect on policies.</td>
</tr>
<tr>
<td>Networks and Devices tree</td>
<td>Create Children 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.</td>
</tr>
<tr>
<td>Individual network or device in the Networks and Devices tree</td>
<td>Create Children 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.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Resource type</th>
<th>Result of Denying &quot;Delete&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network directory or local directory</td>
<td>Prevents users from deleting any item in the directory, for example, applications, areas, data servers, or user accounts.</td>
</tr>
<tr>
<td>Application</td>
<td>Prevents users from deleting the application, or any item within it, for example, areas, or data servers.</td>
</tr>
<tr>
<td>Area</td>
<td>Prevents users from deleting the area, or any item within it, for example, data servers within the area.</td>
</tr>
<tr>
<td>System folder</td>
<td>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 Write permission, because updating the group memberships of accounts is controlled by the Write action.</td>
</tr>
<tr>
<td>Networks and Devices tree</td>
<td>The Delete 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.</td>
</tr>
<tr>
<td>Individual network or device in the Networks and Devices tree</td>
<td>The Delete 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.</td>
</tr>
</tbody>
</table>

Tag actions: Write Value

Controls whether a user or group can write to tags in data servers from a computer or group of computers. This action can be configured 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 you have additional FactoryTalk products 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 action groups you have added. If you have not added any action groups, this category does not appear.

**See also**

- [Things you can secure](#) on page 28
- [Account types](#) on page 16
- [Differences between securable actions and product policy features](#) on page 111
- [Effective permission icons](#) on page 154
- [Secure features of a single product](#) on page 107

**Set FactoryTalk Directory permissions**

Set permissions on your FactoryTalk Directory folder in order 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

Obtain the following security permissions for the FactoryTalk application:

- Common > Read
- Common > Configure Security

To set FactoryTalk Directory permissions

1. In the Explorer window, right-click on the FactoryTalk network or local directory, then click Security.

2. In Security Settings for [Local or Network], in the Permissions tab, do one of the following:

   - To set permissions by user:
     - Click User.
     - In the Users and Computers list, select a user and computer.
     - In the Action list, expand the category that contains the action you want to secure, and click on the action to select it.

   - To set permissions by action:
     - Click Action.
     - In the Action list, expand the category that contains the action you want to secure, and click on the action to select it. If the list of actions is blank, add users and computers first.
     - In the Users and Computers list, select a user and computer.

3. Click Allow or Deny.

4. (optional) To control access to the action by another user or group, click Add and select the user or group, and computer or group to add, and click OK.

5. When you have finished configuring security for the FactoryTalk Directory, click OK.

See also

View effective permissions on page 152
Set application permissions

Set permissions on your application in order 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 you have associated a resource grouping 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

Obtain the following security permissions for the application:

- Common > Read
- Common > Configure Security

To set application permissions

1. In the Explorer window, right-click on the application you want to secure, then click Security.

2. In Security Settings, in the Permissions tab, do one of the following:
• To set permissions by user:
  • **Click User.**
  • In the **Users and Computers** list, select a user and computer.
  • In the **Action** list, expand the category that contains the action you want to secure, and click on the action to select it.

• To set permissions by action:
  • **Click Action.**
  • In the **Action** list, expand the category that contains the action you want to secure, and click on the action to select it. If the list of actions is blank, add users and computers first.
  • In the **Users and Computers** list, select a user and computer.

3. Click **Allow** or **Deny**, or clear both boxes. 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, click **Add**, and in **Select User and Computer**, select the user or group, and computer or group to add, and click **OK**.

5. When you have finished configuring security for the application, click **OK**.

**See also**

- View effective permissions on page 152
- Add a user-computer pair on page 59
- Secure resources on page 131
- Actions on page 137

### 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, you could 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 you have associated a resource grouping 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**

Obtain the following security permissions for the area:

• Common > Read
• Common > Configure Security

**To set area permissions**

1. In the Explorer window, expand the application, right-click on the area you wish to secure, and click Security.

2. In Security Settings, in the Permissions tab, do one of the following:

   • To set permissions by user:
     • Click User.
     • In the Users and Computers list, select a user and computer.
     • In the Action list, expand the category that contains the action you want to secure, and click on the action to select it.

   • To set permissions by action:
     • Click Action.
     • In the Action list, expand the category that contains the action you want to secure, and click on the action to select it. If the list of actions is blank, add users and computers first.
     • In the Users and Computers list, select a user and computer.
3. Click **Allow** or **Deny**, or clear both boxes. 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, click **Add**, and in **Select User and Computer**, select the user or group, and computer or group to add, and click **OK**.

5. When you have finished configuring security for the area, click **OK**.

**See also**

- [View effective permissions on page 152](#)
- [Add a user-computer pair on page 59](#)
- [Actions on page 137](#)
- [Secure resources on page 131](#)

### Set System folder permissions

Set permissions on your **System** folder in order 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 the Explorer window, right-click the System folder or the subfolder you would like to secure, and then click Security.

2. In Security Settings, in the Permissions tab, do one of the following:
   - To set permissions by user:
     - Click User.
     - In the Users and Computers list, select a user and computer.
     - In the Action list, expand the category that contains the action you want to secure, and click on the action to select it.
   - To set permissions by action:
     - Click Action.
     - In the Action list, expand the category that contains the action you want to secure, and click on the action to select it. If the list of actions is blank, add users and computers first.
     - In the Users and Computers list, select a user and computer.

3. Click Allow or Deny, or clear both boxes. 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, click Add, and in Select User and Computer, select the user or group, and computer or group to add, and click OK.
5. When you have finished configuring security for the System folder, click OK.

See also

View effective permissions on page 152
Add a user-computer pair on page 59
Actions on page 137
Secure resources on page 131

Set action group permissions

Set permissions on your action group in order 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

Obtain the following security permissions for the action group you want to secure:

- Common > Read
- Common > Configure Security

To set action group permissions

1. In the Explorer window, expand the network directory tree, the System folder, and the Action Groups folder, right-click on the action group you want to secure, and then click Security.

2. In Security Settings, in the Permissions tab, do one of the following:

   - To set permissions by user:
     - Click User.
     - In the Users and Computers list, select a user and computer.
     - In the Action list, expand the category that contains the action you want to secure, and click on the action to select it.
• To set permissions by action:
  • Click Action.
  • In the Action list, expand the category that contains the action you want to secure, and click on the action to select it. If the list of actions is blank, add users and computers first.
  • In the Users and Computers list, select a user and computer.

3. Click Allow or Deny, or clear both boxes. 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, click Add, and in Select User and Computer, select the user or group, and computer or group to add, and click OK.

5. When you have finished configuring security for the action group, click OK.

See also

View effective permissions on page 152
Add a user-computer pair on page 59
Add and remove action groups on page 63
Actions on page 137
Secure resources on page 131

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

Obtain the following security permissions for the database you want to secure:

• Common > Read
• Common > Configure Security
To set database permissions

In the Explorer window, expand System > Connections > Databases, right-click on the database you want to secure, and then click Security.

1. In Security Settings, in the Permissions tab, do one of the following:
   - To set permissions by user:
     - Click User.
     - In the Users and Computers list, select a user and computer.
     - In the Action list, expand the category that contains the action you want to secure, and click on the action to select it.
   - To set permissions by action:
     - Click Action.
     - In the Action list, expand the category that contains the action you want to secure, and click on the action to select it. If the list of actions is blank, add users and computers first.
     - In the Users and Computers list, select a user and computer.

2. Click Allow or Deny, or clear both boxes. Clear both Allow and Deny to make the folder inherit its security settings from a resource higher in the directory tree.

3. (optional) To control access to the folder by another user or group, click Add, and in Select User and Computer, select the user or group, and computer or group to add, and click OK.

4. When you have finished configuring security for the database, click OK.

See also

- View effective permissions on page 152
- Add a user-computer pair on page 59
- Actions on page 137
- Secure resources on page 131

Set logical name permissions

Set permissions on your logical name in order 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

Obtain the following security permissions for the logical name:
• Common > Read
• Common > Configure Security

To set logical name permissions

1. In the Explorer window, expand the System > Logical Names, right-click on the logical name you want to secure, and then click Security.

2. In Security Settings, in the Permissions tab, do one of the following:
   • To set permissions by user:
     • Click User.
     • In the Users and Computers list, select a user and computer.
     • In the Action list, expand the category that contains the action you want to secure, and click on the action to select it.
   • To set permissions by action:
     • Click Action.
     • In the Action list, expand the category that contains the action you want to secure, and click on the action to select it. If the list of actions is blank, add users and computers first.
     • In the Users and Computers list, select a user and computer.

3. Click Allow or Deny, or clear both boxes. 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, click Add, and in Select User and Computer, select the user or group, and computer or group to add, and click OK.

5. When you have finished configuring security for the logical name, click OK.

See also

Secure resources on page 131
Permissions determine which users can perform which actions on specific resources in the system from which computers. **Allow** and **Deny** are the two kinds of permissions you can set on resources.

Allow a resource to inherit permissions when you would like the selected resource to have the same permissions as its parent resource. For example, if you assign security to an area in an application, all of the items in the area inherit the security settings of the area, and 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 the **Explorer** window, right-click on the resource you want to secure, then click **Security**.

2. In **Security Settings**, in the **Permissions** tab, clear the **Do not inherit permissions** check box, located at the bottom of the window.

3. To remove explicit permissions, clear the black check mark in the **Allow** or **Deny** check box. Inherited permissions appear as gray check marks. You cannot remove inherited permissions, but you can override them with explicit permissions.

4. Click **OK**.

**Tip:** Security settings that you configure for resources apply to all FactoryTalk products in your system in the current FactoryTalk directory. For example, if you deny a user and computer **Read** access to an area, that user and computer will not be able to see the area in any of the FactoryTalk products in your system.

**See also**

- Prevent a resource from inheriting permissions on page 151
- Secure resources on page 131
- Effective permission icons on page 154
- Permissions on page 132
- Secure resources on page 131

When you break the chain of inheritance, the resource no longer inherits permissions from its parent resources. For example, you can stop an area from inheriting permissions from the application in which it is located by selecting the **Do not inherit permissions** check box when setting up security for the area.
To prevent a resource from inheriting permissions

1. In the Explorer window, right-click on the resource you want to secure, then click Security.

2. In Security Settings, in the Permissions tab, select the Do not inherit permissions check box, located at the bottom of the window.

3. Do one of the following and then click OK:
   - To use the inherited permissions that were formerly applied to the resource as explicit permissions, click Copy the current permissions from the parent object to this object. Use this option when you want to use the permissions the resource inherits from its parent as a starting point for specifying explicit permissions, rather than specifying explicit permissions from scratch.
   - To remove all inherited permissions from the resource, click Remove all inherited permissions from this object. Use this option when you want to specify explicit permissions from scratch.

When you remove all inherited permissions, Read and Configure Security permissions are automatically granted to the Administrators group. The Administrators group must always be granted both of these permissions.

**Tip:** Security settings that you configure for resources apply to all FactoryTalk products in your system in the current FactoryTalk directory. For example, if you deny a user and computer Read access to an area, that user and computer will not be able to see the area in any of the FactoryTalk products in your system.

See also

- Allow a resource to inherit permissions on page 151
- Secure resources on page 131
- Effective permission icons on page 154
- Permissions on page 132

**View effective permissions**

To determine what permissions are currently in effect for a resource, use the Effective Permissions tab in Security Settings. In this tab, you can 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, you must be using a FactoryTalk network directory, because a FactoryTalk local directory is restricted to a single computer.

**Prerequisites**

Obtain the following 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 the **Explorer** window, expand the FactoryTalk network or local directory tree until the resource for which you want to view effective permissions is visible.

2. Right-click the resource, and then click **Security**.

3. In **Security Settings**, click the **Effective Permissions** tab.

4. To test the permissions for a user or user group, under **User or group**, click **Browse (...)** and browse for the user or user group whose permissions you would like to see.

5. To test the permissions for a computer or a computer group, under **Computer or computer group**, click **Browse (...)** and browse for the computer or computer group whose permissions you would like to see.

6. Click **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 132

Secure resources on page 131

Effective permission icons

In Security Settings, check boxes indicate which permissions are in effect for an action.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>A blank check box beside an action means that no permissions are assigned. If both the Allow and Deny check boxes are cleared beside an action, Deny is implied for the action. However, a blank check box shown beside the name of a group of actions, for example, All Actions or Common, means that some of the actions within that group do not have permissions assigned. If collapsed, you must expand the group to see which actions do not have permissions assigned.</td>
</tr>
<tr>
<td>☑</td>
<td>A black check mark means that Allow or Deny permissions have been assigned explicitly.</td>
</tr>
<tr>
<td>☐</td>
<td>A gray check mark means that Allow or Deny permissions have been inherited.</td>
</tr>
</tbody>
</table>

The following examples show how the Allow and Deny columns indicate what permissions have been set for the resource.

Inherited permissions

The gray check marks show that Allow permissions are inherited for all actions.

Explicit permissions
If you click **Allow** beside **All Actions**, the check boxes have black check marks. This means that you have overridden the inherited values and explicitly granted **Allow** on **All Actions**. If the inherited permissions change later, the change will not affect this security setting.

**Explicit Deny permissions without inheritance**

![Permissions for Administrators from All Computers](image)

In this example, the resource does not inherit permissions from its parent (in this illustration, we are configuring security for the FactoryTalk network directory, which has no parent). If you have set all actions to **Allow**, and then you click **Deny** beside **Read**, the following happens:

- The **All Actions** and **Common** check boxes are cleared. Because they represent groups of actions, the blank check boxes beside **All Actions** and **Common** mean that not all of the actions within those groups have check marks in the **Allow** column. You must expand the group to see which actions do not have **Allow** permissions.
- For the **Read** action, the **Allow** check box is cleared.

**Explicit Deny permissions with inheritance**

![Permissions for Administrators from All Computers](image)

In this example, the resource inherits permissions from its parent (for example, an area might inherit permissions from an application). If you have set all actions to **Allow**, and then you click **Deny** beside **Read**, the following happens:

- The **All Actions** and **Common** check boxes are cleared, but because they previously inherited permissions, they now contain gray check marks. You must expand the group to see which actions do not have **Allow** permissions.
• For the Read action, the Allow check box is cleared, but because it previously inherited permissions, the Read check box now contains a gray check mark. Because explicit permissions take precedence over inherited permissions, these check boxes indicate that Read access is denied.

Using the "Do not inherit permissions" check box

Select the Do not inherit permissions check box to remove all inheritance from the resource. You can then set permissions for the resource as shown in the example shown above.

See also

Allow a resource to inherit permissions on page 151

Prevent a resource from inheriting permissions on page 151

Secure resources on page 131
Disaster Recovery

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.

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 157
- Back up an application on page 161
- Back up a System folder on page 160
- Backup and restore options on page 166

Back up a FactoryTalk Directory

Back up a FactoryTalk Directory to move a development FactoryTalk system to a
run-time FactoryTalk system, or to simply 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, click Tools > Security Authority Identifier. In Modify Security Authority Identifier, click 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 double-click User Rights Assignment.

To back up a FactoryTalk Directory

1. In Explorer, right-click the Network or Local Directory icon.

2. From the context menu, choose Backup.

3. Use the default name or type another name for the backup file.

   Tip: 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.

4. Use the default archive location or specify another location by clicking Browse, selecting a location, and then clicking OK in the Browse for Folder window.

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 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.

6. In the **Backup** window, click **OK**.

   Unless you specified a different file name, FactoryTalk Administration Console creates a directory backup file with its current security authority identifier 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.

7. After backing up a directory, 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 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, choose **Rockwell Software > RSLinx > Backup Restore Utility**.
   - **FactoryTalk Linx servers:** See FactoryTalk Linx documentation.
   - **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.

See also

- [Restore a FactoryTalk Directory](#) on page 168
- [Backup](#) on page 164
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. Open System > Policies > System Policies, and double-click User Rights Assignment.

**To back up a System folder**

1. Right-click the System folder, then click 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 clicking Browse, selecting a location, and then clicking 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, click **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.

**See also**

- [Restore a system folder](#) on page 183
- [Backup resources](#) on page 166
- [Backup](#) on page 164
- [Backup and restore options](#) on page 166

**Back up an application**

Back up an application and create an archive file so that later you can:

- 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.

- An application typically contains areas (in a network directory), resource grouping information, and references to data servers, device servers, alarm servers, and HMI servers.
- 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 individual application**

1. In **Explorer**, right-click the application you want to back up, and click **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 clicking **Browse**, selecting a location, and then clicking **OK** in the **Browse for Folder** window.

4. To back up the application without including the System folder, clear the **Backup System in archive** check box. To include the System folder in the backup, select the **Backup System in archive** 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. 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.

6. In the **Backup** window, click **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.

7. 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.

• **RSLinx Classic data servers**, run the RSLinx Backup Restore utility to back up and restore the data server configuration. From the Windows Start menu, choose Rockwell Software > RSLinx > Backup Restore Utility.

• **FactoryTalk Linx servers**, see the FactoryTalk Linx Getting Results Guide.

• **FactoryTalk Alarms and Events Logs**, use Microsoft SQL Server tools to back up and restore database files.

• **FactoryTalk Transaction Manager**, back up and restore project files using the Configuration menu.

• **FactoryTalk Batch**, copy the FactoryTalk Batch files back to the same directory locations. See FactoryTalk Batch documentation for help.

• **Other products**, back up and restore product-specific information separately. See product documentation for help.

See also

- Restore (Application) on page 184
- Backup and restore options on page 166
- Backup on page 164

**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, click 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.
   • 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. Click OK.

5. (optional) If prompted, select Yes to overwrite the existing backup archive.

6. In the confirmation window, click OK.

See also

- Restore a Security Authority identifier on page 173
- Generate a Security Authority identifier on page 180
- Modify Security Authority Identifier on page 167

Backup

How do I open Backup?

1. Run FactoryTalk Administration Console.

2. In the Explorer window, right-click the directory icon, an application, or the System folder.

3. On the context menu, 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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify archive name</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• 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, <em>Network - 72CE22CE-5175-4C26-98AE-3ABE5AC7F8EC.bak</em> or <em>Local - C56SC77A-4664-4EC6-9779-1EC729BA8A0.bak</em>. 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.</td>
</tr>
<tr>
<td></td>
<td>• 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 <em>System.bak</em>.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Specify archive location</td>
<td>Use the default archive location or type the path where you want to save the backup file. Alternatively, click <em>Browse</em>, select a folder, and click <em>OK</em>. The default archive location is <em>C:\Users\Public\Documents</em>.</td>
</tr>
<tr>
<td>Backup System in archive</td>
<td>The <em>Backup System in archive</em> check box is available only if you are backing up an application.</td>
</tr>
<tr>
<td></td>
<td>• To include the contents of the System folder in the backup archive, select this check box.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• To back up only the application without the System folder, clear this check box.</td>
</tr>
<tr>
<td></td>
<td>• Choose this option when you want to add an application to an existing FactoryTalk Directory without overwriting the settings held in the System folder.</td>
</tr>
<tr>
<td>File Encryption</td>
<td>Choose whether or not to encrypt the archive file. Encrypting the file protects it against unauthorized use.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• To encrypt file contents, select the <em>File Encryption</em> check box.</td>
</tr>
<tr>
<td></td>
<td>• To save the archive file without encryption, clear this check box.</td>
</tr>
<tr>
<td>Passphrase</td>
<td>Type a passphrase for the archive file you want to encrypt.</td>
</tr>
<tr>
<td></td>
<td>The passphrase must meet the following requirements:</td>
</tr>
<tr>
<td></td>
<td>• Any alphanumeric character or other characters</td>
</tr>
<tr>
<td></td>
<td>• Minimum length: 0</td>
</tr>
<tr>
<td></td>
<td>• Maximum length: 64</td>
</tr>
<tr>
<td>Confirm passphrase</td>
<td>Type the same passphrase you typed in the <em>Passphrase</em> field.</td>
</tr>
</tbody>
</table>
### Important:

Remember the passphrase if you choose to encrypt your file contents. The archive file cannot be restored without the correct passphrase.

### See also

- [Back up an application](#) on page 161
- [Back up a FactoryTalk Directory](#) on page 157
- [Back up a System folder](#) on page 160
- [Backup and restore options](#) on page 166

### 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.

<table>
<thead>
<tr>
<th>To backup or restore</th>
<th>Create this type of backup archive</th>
</tr>
</thead>
<tbody>
<tr>
<td>An individual application without the System folder</td>
<td>Application</td>
</tr>
<tr>
<td>Multiple applications without the System folder</td>
<td>Application</td>
</tr>
<tr>
<td></td>
<td>Create separate archives for each application.</td>
</tr>
<tr>
<td>The System folder, without restoring applications</td>
<td>System folder</td>
</tr>
<tr>
<td></td>
<td>• You cannot restore only the System folder from an Application or FactoryTalk Directory archive.</td>
</tr>
<tr>
<td>An individual application and the System folder</td>
<td>Application</td>
</tr>
<tr>
<td></td>
<td>• Select the <strong>Backup system in archive</strong> check box. Selecting this check box overwrites the contents of the System folder in the FactoryTalk Directory, including accounts, security settings, and policy settings.</td>
</tr>
<tr>
<td>Multiple applications and the System folder</td>
<td>Application</td>
</tr>
<tr>
<td></td>
<td>• Create separate archives for each application, and select the <strong>Backup system in archive</strong> check box in at least one of the archives.</td>
</tr>
<tr>
<td></td>
<td>• If the applications come from different FactoryTalk Directories, remember that you can restore only one System folder into a single FactoryTalk Directory.</td>
</tr>
<tr>
<td>An entire FactoryTalk Directory including all applications, the System folder, and the security authority identifier</td>
<td>FactoryTalk Directory</td>
</tr>
<tr>
<td></td>
<td>• You cannot restore individual applications, or only the System folder, from a FactoryTalk Directory archive.</td>
</tr>
<tr>
<td>The FactoryTalk Directory security authority identifier only</td>
<td>FactoryTalk Directory</td>
</tr>
<tr>
<td></td>
<td>• Use <strong>Modify Security Authority Identifier</strong> to create this backup archive, which contains only the security authority identifier.</td>
</tr>
<tr>
<td></td>
<td>• To restore this backup archive, use <strong>Modify Security Authority Identifier</strong>.</td>
</tr>
<tr>
<td></td>
<td>• It is strongly recommended to make a backup of the directory with the new identifier after restoring the security authority identifier.</td>
</tr>
</tbody>
</table>
See also

- Back up a FactoryTalk Directory on page 157
- Back up an application on page 161
- Back up a System folder on page 160
- Back up a security authority identifier on page 163
- Backup on page 164

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, backup, or restore the unique Security Authority Identifier for a FactoryTalk Directory. The User Rights Assignment > Modify Security Authority Identifier permission is required to generate, backup, 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 180
- Back up a Security Authority identifier on page 163
- Restore a Security Authority identifier on page 173

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

You may 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 can overwrite existing data that affects all applications.

See also

- [Restore a FactoryTalk Directory](#) on page 168
- [Restore an application](#) on page 172
- [Restore a System folder](#) on page 170
- [Verify security settings after restoring a FactoryTalk system](#) on page 175
- [Backup and restore options](#) on page 166

**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.

**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 you want to restore into, and create a backup archive of the existing directory.

**To restore a FactoryTalk Directory**

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. Close all applications held in the directory that you are restoring into.
2. Right-click **Network** or **Local**, and click **Restore**.

3. In **Restore**, click **Browse**, select the backup file (*.bak) you want to restore, and click **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. Click **Next**.

5. If the backup file is encrypted, **Restore Backup File** opens. Type the passphrase that was used during the backup operation.

   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.

   After you enter the correct passphrase, **Restore** shows the type of archive you are restoring and what applications are contained in the archive. You cannot select individual applications. 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.

6. To restore the FactoryTalk Directory contained in the selected archive, click **Finish**.

   If you restore an archive created in an earlier version of the FactoryTalk platform into a later version, the restore process 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, suppose you restore an archive created under FactoryTalk Automation Platform 2.00 (CPR 7) into a FactoryTalk Directory that has been upgraded to FactoryTalk Services Platform 2.10 (CPR 9) 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.

8. If you are hosting servers on different computers than those that were 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 Directory on page 175
- Add a computer on page 55
- Back up a FactoryTalk Directory on page 157

**Restore a System folder**

To overwrite the contents of the existing System folder with the contents in the backup archive, you can 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

**Tip:** 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.

**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.

**To restore a System folder**

1. In the *Explorer* window, right-click *Network* or *Local*, and click *Restore*.

2. Click *Browse*, and then select the backup archive file you want to restore. (The default name is *System.bak*.) Click *OK* to close the browse window, and then click *Next*.

3. If the backup file is encrypted, *Restore Backup File* opens. Type the passphrase that was used during the backup operation.

   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.

4. After entering the correct passphrase, click *Finish* to restore the System folder.

   If you restore an archive created in an earlier version of the FactoryTalk platform into a later version, the restore process 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, suppose you restore an archive created under FactoryTalk Automation Platform 2.00 (CPR 7) into a FactoryTalk Directory that has been upgraded to FactoryTalk Services Platform 2.10 (CPR 9) 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.

5. After restoring the System folder, back up and restore project files and databases from your individual software products.

6. Verify security settings, and perform any follow-up tasks.

**See also**

- [Verify security settings after restoring a FactoryTalk Directory](#) on page 175
- [Backup and restore options](#) on page 166
- [Back up a System folder](#) on page 160
- [Restore a FactoryTalk system](#) on page 167
Chapter 14
Disaster Recovery

Restore an application

To restore an application from one computer to another, or to copy an application within the same directory, you can restore an application. If the System folder was backed up with the application, you can choose whether or not to restore it.

When you restore an application without the System folder:

- Any references will be 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.

Tip: 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.

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 the Explorer window, right-click Network or Local, and click Restore.
2. In Restore, click Browse, and then select the backup archive file (ApplicationName.bak) that you want to restore. Click OK, then click Next.
3. If the backup file is encrypted, Restore Backup File opens. Type the passphrase that was used during the backup operation.

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.

4. Restore shows information about the application you are restoring. Choose one of the following restore options:
• Check **Restore System**. This overwrites user, computer, and group accounts, passwords, policy settings, and security settings for all applications in the FactoryTalk Directory.

• Clear **Restore System**. If you restore an application to a different directory or to a different computer, you will need to manually recreate security permissions for FactoryTalk users and groups in the restored application.

5. To restore the application with its original name, click **Finish**. To restore an application with a different name, select the **Restore into a new application named** check box, type the name, and then click **Finish**.

If you type an optional name, the system leaves the original application intact and restores the backup as a new application, in effect copying the application.

6. If you restored 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 you restored an application with its System folder, verify that the security settings managed through the System folder are correct, and make edits as needed.

**See also**

- [Verify security settings after restoring a FactoryTalk system](#) on page 175
- [Back up an application](#) on page 161
- [Restore a FactoryTalk system](#) on page 167

**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, click Restore.

3. In Restore, click Browse (...) to specify the archive to restore, then click 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-9779-1EC729B3A8A0.bak.

4. (optional) If the backup file was encrypted, in Restore Backup File, type the passphrase to unlock the backup file, then click OK.

5. In Restore, select Restore security authority identifier only, then click 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 163

Generate a Security Authority identifier on page 180
After you restore a FactoryTalk Directory backup archive, check to see that the FactoryTalk Directory security settings on the new FactoryTalk system meet your requirements, and make adjustments as needed.

Depending upon your FactoryTalk configuration, you may need to do one or more of the following tasks after you restore 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
- Restore the alarm log database

See also

- Update computer accounts in the network directory on page 175
- Recreate a Windows-linked user account on page 176
- Update Windows-linked user groups on page 177
- Update security settings for networks and devices on page 177
- Restore the alarm log database on page 178

After you restore any backup archive that includes a System folder, you may need to update computer accounts to allow them 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.

After restoring a directory in a new domain, update computer accounts to allow the client computers access to the network directory, as outlined below.

**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 57
- [Delete a computer](#) on page 56
- [Add a computer](#) on page 55
- [Verify security settings after restoring a FactoryTalk system](#) on page 175

**Recreate a Windows-linked user account**

You cannot move individual Windows-linked user accounts from one domain to another. You can move only Windows-linked user group accounts to a new domain. This allows you to retain all of the security permissions for the group.

If you are using individual Windows-linked user accounts, you will need to recreate these accounts when restoring your FactoryTalk Directory to a new FactoryTalk system.

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

2. Expand **Account Policy Settings**, then click on **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 177
Delete a user account on page 44
Add a Windows-linked user account on page 41
Add accounts to a FactoryTalk user group on page 52
Verify security settings after restoring a FactoryTalk system on page 175

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.

You may need to 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 are then updated automatically. This allows you to move your applications to a different domain without having to change or recreate each user account separately.

If your 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 177

Update security settings for networks and devices

After you restore an entire FactoryTalk Directory you may need to update security settings for networks and devices in order to secure them in the new domain.

The Networks and Devices tree shows information about the networks and devices that are connected to the local computer. The contents of the Networks and Devices tree are not included in the backup archive, but any security settings that are defined for networks and devices are included in the backup archive.
If an archive is restored on a computer that is 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 your security settings are accurate for the resources in your new FactoryTalk system, and make edits as needed.

**To update security settings for networks and devices**

1. In the **Explorer** window, click to expand **Networks and Devices** to view the networks and devices in your FactoryTalk system.

2. To check the security settings for a network or device, right-click on its icon, then click **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.

3. Review and edit user action permissions as needed.

**See also**

- [Restore alarm log database](#) on page 178
- [Verify security settings after restoring a FactoryTalk system](#) on page 175

---

**Restore alarm log database**

If your FactoryTalk system includes Microsoft SQL Server databases for logging historical data, including FactoryTalk Alarms and Events logs, restore any data from the development FactoryTalk system that you want to deploy to the new system. Next, re-establish a connection between a database definition, held in the directory, and its associated Microsoft SQL Server database.

**To restore historical data**

1. On any computer in the network directory, run FactoryTalk Administration Console.

2. From the **Explorer** window, 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 click **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 175
- [Restore a FactoryTalk system](#) on page 167
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. Click Start > Settings > 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:

- 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 the Explorer area, right-click the Local icon and then restore a local backup archive created with the earlier version of the FactoryTalk platform software.

7. Click 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 167

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**, click **Generate ID**.

3. In the confirmation window, click **Yes**.

4. (optional) Click **Backup** to back up the current directory with the new identifier.

5. Click **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 163](#)
- [Restore a Security Authority identifier on page 173](#)
- [Modify Security Authority Identifier on page 167](#)

**Restore**

How do I open Restore?

1. Run FactoryTalk Administration Console.

2. At the top of the Explorer window, right-click the Directory icon.

3. On the context menu, click **Restore**.

Use **Restore** to specify the name of the backup file you wish to use to restore all or part of a FactoryTalk Directory.

Select one of these archive types:
Chapter 14  Disaster Recovery

- A full FactoryTalk Directory backup archive. This will be named with its security authority identifier (for example, Network - 72CE2C2E-5175-4C26-984E-3ABE5AC7F8EC.bak or Local - C565C77A-4664-4E6C-9779-1EC729B3A8A0.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 directory you are restoring into before continuing with the restore process.

An archive file created under FactoryTalk Automation Platform 2.00 (CPR 7) can be restored into a FactoryTalk Directory that has been upgraded to FactoryTalk Services Platform 2.10 (CPR 9) or later. The restore operation 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.

See also

- Restore a FactoryTalk Directory on page 168
- Restore a System folder on page 170
- Restore an application on page 172
- Verify security settings after restoring a FactoryTalk system on page 175

How do I open Restore?

1. Run FactoryTalk Administration Console.
2. At the top of the Explorer window, right-click the Directory icon.
3. On the context menu, 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, click 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive name</td>
<td>The name of the backup archive file to be restored.</td>
</tr>
</tbody>
</table>
| Archive type  | Identifies the type of information held within the backup archive file.  
FactoryTalk Directory - Identifies an archive file that contains the contents of an entire directory, including all applications and the System folder.  
**Important:** 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. You cannot select individual applications. When you restore an entire directory, all of the applications included in that directory are also restored. |
| Restore       | Only appears when an application is open in the FactoryTalk Directory, which prevents a full restore. If hidden, the entire FactoryTalk Directory will be restored. Select which portions of the FactoryTalk Directory to restore:  
  + 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  
    Only restores the security authority identifier. Applications, users, computers, groups, passwords, policies, and security settings are not restored.  
    Back up your directory and remove the old bindings from all controllers and controller projects before continuing. Backup the directory with the new identifier after the restore process is complete. |

**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.

**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 168*

**Restore (System folder)**

How do I open Restore?

1. Run FactoryTalk Administration Console.
2. At the top of the Explorer window, right-click the Directory icon.
3. On the context menu, 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 clicking **Finish** to restore a System folder.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive name</td>
<td>The name of the backup archive file to be restored.</td>
</tr>
<tr>
<td>Archive type</td>
<td>Identifies the type of information held within the backup archive file.</td>
</tr>
<tr>
<td></td>
<td><strong>System Only</strong> - 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.</td>
</tr>
<tr>
<td>Application(s)</td>
<td>(none) - Confirms that applications are not included in the backup archive to restored.</td>
</tr>
</tbody>
</table>

**See also**

- [Restore a System folder](#) on page 170
- [Backup and restore options](#) on page 166

**Restore (Application)**

How do I open Restore?

1. Run FactoryTalk Administration Console.

2. At the top of the Explorer window, right-click the Directory icon.

3. On the context menu, 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, click **Cancel** to exit or **Back** to select a different archive file.

If the **System** folder was backed up with the application, you can 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Backup files</strong></td>
<td><strong>ApplicationName.bak</strong> file.</td>
</tr>
<tr>
<td><strong>Archive type</strong></td>
<td>Identifies the type of information held within the backup archive file.</td>
</tr>
<tr>
<td></td>
<td>- Application and System - Identifies an archive file that contains both an application and a System folder.</td>
</tr>
<tr>
<td></td>
<td>- Application - Identifies an archive file that contains only an application.</td>
</tr>
<tr>
<td><strong>Application(s)</strong></td>
<td>The name of the application or applications held in the backup archive file.</td>
</tr>
<tr>
<td><strong>Restore System</strong></td>
<td>If the backup archive file includes a System folder, this option is available.</td>
</tr>
<tr>
<td></td>
<td>- To restore the application and the System folder, select Restore System. Restoring the System folder <strong>overwrites all user and computer accounts and groups, passwords, policy settings, and security settings for all applications</strong> in the FactoryTalk Directory.</td>
</tr>
<tr>
<td></td>
<td>- To restore the application without restoring the System folder, clear Restore System. Restoring the System folder <strong>overwrites all user and computer accounts and groups, passwords, policy settings, and security settings for all applications</strong> in the FactoryTalk Directory.</td>
</tr>
<tr>
<td></td>
<td>If you restore 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.</td>
</tr>
<tr>
<td><strong>Restore into a new application named:</strong></td>
<td>Choose whether to overwrite an existing application or create a new application.</td>
</tr>
<tr>
<td></td>
<td>- To restore the contents of the backup archive file into an application with a new name, select Restore into a New Application Named, then type a unique name. When you click Finish, 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 serves to copy the archived application into the directory.</td>
</tr>
<tr>
<td></td>
<td>- To restore an existing application with its original name, clear Restore into a New Application Named. When you click Finish, the system confirms that you want to overwrite the existing application of the same name. Click Yes to restore the application.</td>
</tr>
</tbody>
</table>

**See also**

[Restore an application](#) on page 172

**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 182
- Restore an application on page 172
- Restore a System folder on page 170
- Restore a Security Authority identifier on page 173

Reconfigure a FactoryTalk Directory

The 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.

Normally, all configuration of FactoryTalk Directory is done automatically during installation of FactoryTalk Services Platform, so there is no need to run the FactoryTalk Directory Configuration Wizard. Use FactoryTalk Directory Configuration Wizard when circumstances require a manual configuration of FactoryTalk Directory.

The FactoryTalk Directory Configuration Wizard is intended for use by FactoryTalk administrators.

Run the FactoryTalk Directory Configuration Wizard if:

- An error occurred while you were installing the FactoryTalk Services Platform, or a message appeared instructing you to run the wizard manually.
- You upgraded an existing FactoryTalk Directory from FactoryTalk® Automation Platform version 2.0, but during the upgrade a valid FactoryTalk Administrator account could not be found for the directory.
- You installed FactoryTalk Services Platform from a remote client (such as Remote Desktop Services). The FactoryTalk Directory cannot be configured from a remote client. You must run the FactoryTalk Directory Configuration Wizard at the Windows console on the computer.
- You cannot access the FactoryTalk administrator account in the network directory or local directory. Running the wizard resets a locked administrator account, or allows you to change an expired password for the
Select a FactoryTalk Directory to configure

The first step in configuring a FactoryTalk Directory is to select which FactoryTalk directory you wish to configure from the first page in the FactoryTalk Directory Configuration Wizard.

To select a FactoryTalk Directory to configure

1. From the Start menu, choose All Programs > 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

   If you choose both directories, the wizard steps you through both tasks, beginning with the network directory.

3. Click Next.

See also

Enter an administrator user name and password on page 193

Reset an expired password on page 193

What reconfiguring a network directory does on page 189

What reconfiguring a local directory does on page 190
To configure a new FactoryTalk network directory or to upgrade an existing FactoryTalk network directory, you must log on. This allows the 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. You cannot configure the FactoryTalk network directory from a remote computer, for example.

Depending on what accounts are available in the network directory, you might be prompted to 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

You can also 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.

**Important:** Keep your 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.

Alternatively, have another user whose account is a member of the FactoryTalk Administrators group enable your account for you, or reset your password.

If your administrator account was disabled, you cannot use the FactoryTalk Directory Configuration Wizard to enable the account. Instead, have another user enable your account for you in FactoryTalk Administration Console. The last FactoryTalk administrator account in a directory cannot be disabled.

If no other user is available, or you do not know the password to another administrator account (for example, because that user left the organization), contact Rockwell Automation Technical Support.

**See also**

- What reconfiguring a network directory does on page 189
- Reset an expired password on page 193
- Summary on page 196
- FactoryTalk Directory Configuration Wizard on page 197
Reconfiguring the FactoryTalk network directory does different things, depending on the state of the directory when you run the wizard. The wizard can do any of the following:

- Whenever you run the wizard to reconfigure the FactoryTalk network directory, the wizard backs up the original directory. The backup file is called `NetworkInstall*.bak` and is located in `C:\ProgramData\Rockwell\RNAServer\Backups`. The location of the backup files is also logged to FactoryTalk Diagnostics. You can view the diagnostic log files using the FactoryTalk Diagnostics Viewer.

- 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, running the wizard manually the first time adds the Windows Administrators group to the FactoryTalk Administrators group. 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.

- If an error occurred while you were upgrading an existing FactoryTalk Directory, running the wizard manually the first time updates policies in the directory, and adds the $AnonymousLogon account to the 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.

- If the password to a FactoryTalk account has expired, and the account is a member of the FactoryTalk Administrators group, running the wizard allows you to change the password.

- If a FactoryTalk administrator account becomes locked (for example, because of too many invalid logon attempts), the wizard allows you to reset the account.

See also

- [Configure or reconfigure a network directory](#) on page 188
- [Reset an expired password](#) on page 193
- [Change Password](#) on page 195
- [Summary](#) on page 196
- [FactoryTalk Directory Configuration Wizard](#) on page 197

To configure a new FactoryTalk local directory, or to upgrade an existing FactoryTalk local directory, you must log on. This allows the wizard to access the directory and configure it. Reconfiguring the FactoryTalk local directory allows...
you to reset a disabled administrator account and upgrade policies.

Depending on what accounts are available in the local directory, you might be prompted to 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

You can also 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.

**Important:** Keep your 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.

Alternatively, have another user whose account is a member of the FactoryTalk Administrators group enable your account for you, or reset your password.

If your administrator account was disabled, you cannot use the FactoryTalk Directory Configuration Wizard to enable the account. Instead, have another user enable your account for you in FactoryTalk Administration Console. The last FactoryTalk administrator account in a directory cannot be disabled.

If no other user is available, or you do not know the password to another administrator account (for example, because that user left the organization), contact Rockwell Automation Technical Support.

See also

- Select a FactoryTalk Directory to configure on page 187
- What reconfiguring a local directory does on page 190
- Enter an administrator user name and password on page 193
- Reset an expired password on page 193
- Product support for network and local directories on page 192

**What reconfiguring a local directory does**

Reconfiguring a local directory does different things, depending on the state of the directory when you run the wizard. The wizard can do any of the following:

- Whenever you run the wizard to reconfigure the FactoryTalk local directory, the wizard backs up the original directory. The backup file is called `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.

- 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, running the wizard manually the first time adds the Windows Administrators group to the FactoryTalk Administrators group. 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.

- When run manually for the first time, the wizard also adds the Windows Authenticated Users group to the local directory, allowing any user who is logged on to Windows to access the local directory.

- The Authenticated Users group is a Windows user group that includes all users and computers whose identities have been authenticated. Authenticated Users does not include Guest even if the Guest account has a password. The Authenticated Users group is used to override security in the local directory by granting access to all authenticated Windows user accounts.

- If an error occurred while you were upgrading an existing FactoryTalk Directory, running the wizard manually the first time updates policies in the directory, and adds the $AnonymousLogon account to the 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.

- If the password expires to a FactoryTalk account that is a member of the FactoryTalk Administrators group, running the wizard allows you to change the password.

- If a FactoryTalk administrator account becomes locked (for example, because of too many invalid logon attempts), the wizard allows you to reset the account.

See also

Configure or reconfigure a local directory on page 189

Select a FactoryTalk Directory to configure on page 187

Enter an administrator user name and password on page 193

Product support for network and local directories on page 192

Reconfigure a FactoryTalk Directory on page 186
Chapter 14  Disaster Recovery

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 you need depends upon which software products are part of your FactoryTalk system. The table below shows which products require a network directory, which require a local directory, and which can use either directory.

<table>
<thead>
<tr>
<th>Product</th>
<th>Network Directory</th>
<th>Local Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>FactoryTalk Administration Console</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>FactoryTalk AssetCentre</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>FactoryTalk Batch</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>FactoryTalk Historian Classic</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>FactoryTalk Historian for Batch</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>FactoryTalk Linx</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>FactoryTalk Linx Gateway</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>FactoryTalk Metrics</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>FactoryTalk Portal</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>FactoryTalk® ProductionCentre®</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>FactoryTalk Scheduler</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>FactoryTalk Transaction Manager</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>FactoryTalk View Machine Edition</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>FactoryTalk View SE</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>FactoryTalk View SE Local</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Logix Designer</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>RSAutomation Desktop®</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>RSBizWare™ BatchCampaign™</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>RSBizWare eProcedure®</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>RSLinx Classic</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>RSLogix™ 5</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>RSLogix 500®</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>RSLogix 5000®</td>
<td>Yes</td>
<td>Yes*</td>
</tr>
<tr>
<td>RSMACC™</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>RSNetWorx</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
The FactoryTalk local directory is not supported in RSLogix 5000 v20 software.

See also

*Select a FactoryTalk Directory to configure* on page 187

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* closes.

Prerequisites

1. If you are not already on the second page of the wizard, choose *All Programs* > *Rockwell Software* > *FactoryTalk Tools* > *FactoryTalk Directory Configuration Wizard*.

2. In *FactoryTalk Directory Configuration Wizard*, select the directory you want to configure, and click *Next*.

To enter an administrator user name and password

1. Click in *Administrator User Name*.

2. Type a Windows Administrator account or FactoryTalk Administrator account user name.

3. Click in *Password*, and type the password that corresponds to the user name you entered.

4. Click *Next*.

See also

*Select a FactoryTalk Directory to configure* on page 187

*Reset an expired password* on page 193

*Configure or reconfigure a network directory* on page 188

*Configure or reconfigure a local directory* on page 189

*Default passwords* on page 198

Reset an expired password

If the password to your 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 change an expired password

1. In the New password field, type the new password to the account.

2. In the Confirm new password field, type the same password you typed in the New password box, and click OK.

Depending on how the FactoryTalk security policies are configured, minimum password length and password complexity requirements might apply.

See also

Configure or reconfigure a network directory on page 188

Configure or reconfigure a local directory on page 189

Default passwords on page 198

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 you cannot remember the password to your FactoryTalk administrator account, contact Rockwell Automation Technical Support.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator user name</td>
<td>This box displays the user name you typed for the expired administrator account in the previous step of the wizard.</td>
</tr>
<tr>
<td>Old password</td>
<td>This box displays asterisks (*) as a placeholder for the old password you typed for the expired account in the previous step of the wizard.</td>
</tr>
<tr>
<td>New password</td>
<td>Type the new password to the account.</td>
</tr>
</tbody>
</table>
Confirm new password

Type the same password you typed in the New password box. 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.

If the wizard will not accept your new password, make sure that your new password:

- Is not the same as any of the last 3 passwords you used for the account
- Does not contain all of the user account name. For example, a user account called 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.
- Is at least six characters long
- Contains characters from three of the following four categories:
  - Unaccented uppercase characters (A to Z)
  - Unaccented lowercase characters (a to z)
  - Numerals (0 to 9)
  - Non-alphanumeric characters (!, @, #, %)

Important: Keep your 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 or reconfigure a local directory on page 189
Summary on page 196
Default passwords on page 198

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 | Type the same password you typed in the New password box.

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.

If the wizard will not accept your new password, make sure that your new password:

- Is not the same as any of the last 3 passwords you used for the account
- Does not contain all of the user account name. For example, a user account called 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.
- Is at least six characters long
- Contains characters from three of the following four categories:
  - Unaccented uppercase characters (A to Z)
  - Unaccented lowercase characters (a to z)
  - Numerals (0 to 9)
  - non-alphanumeric characters (!, @, #, %)

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 193
- [Configure or reconfigure a network directory](#) on page 188
- [Summary](#) on page 196
- [Default passwords](#) on page 198

### 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 seen through 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](#) on page 197

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.

The 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.

Normally, all configuration of the FactoryTalk Directory is done automatically during installation of FactoryTalk Services Platform, so there is no need to run the FactoryTalk Directory Configuration Wizard. Use FactoryTalk Directory Configuration Wizard when circumstances require a manual configuration of FactoryTalk Directory. The FactoryTalk Directory Configuration Wizard is intended for use by FactoryTalk administrators.
See also

- Product support for network and local directories on page 192
- Select a FactoryTalk Directory to configure on page 187
- Enter an administrator user name and password on page 193
- Reset an expired password on page 193

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 193
- Reset an expired password on page 193
Appendix A

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


2. (optional) Upgrade client computers:
   a. Log in to the computer as a user in the Windows Administrators group.
   b. Shut down all Rockwell Automation software products running on the computer.
c. Insert the product disc and select FactoryTalk Services Platform, or run the standalone FactoryTalk Services Platform installation file.

d. Once installation is complete, restart the computer.

3. Upgrade the FactoryTalk Network Directory server:
   a. Log in to the computer as a user in the Windows Administrators group.
   b. Shut down all Rockwell Automation software products running on the computer.
   c. Disconnect the computer from the network, so client computers cannot connect during the upgrade.
   d. Use Windows Control Panel to uninstall FactoryTalk Services Platform.
   e. Insert the product disc and select FactoryTalk Services Platform, or run the standalone FactoryTalk Services Platform installation file.
   f. Once installation is complete, restart the computer.
   g. Reconnect the computer to the network.

See also

Product Compatibility and Download Center

Back up a FactoryTalk Directory on page 157

Restore a FactoryTalk Directory on page 168

Identify the installed FactoryTalk Services Platform version

Identify the installed FactoryTalk Services Platform version to determine if an upgrade of FactoryTalk Services Platform is necessary.

To identify the installed FactoryTalk Services Platform version

1. On the Windows Start menu, click Control Panel.
2. Double-click Add or Remove Programs.
3. In the list of installed programs, FactoryTalk Services Platform appears, with the version number shown beside it.
Appendix B

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 201
Add an HTTPS site binding for FactoryTalk Web Services on page 202

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. Click Start > Control Panel > 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 202

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)

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 4.6 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:**

  **HTTPS:**

  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 \textit{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:

\textbf{HTTP:}
http://\textit{server\_path}:80/FactoryTalk/Security/WebService/200810.asmx

\textbf{HTTPS:}
https://\textit{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.

\textbf{See also}

\textit{How to change the TCP port for IIS services}

\textbf{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:

\textbf{HTTP:}

\textbf{HTTPS:}

2. Select \textit{Login}.

3. In \textit{userName}, enter the user name for an account already configured in the FactoryTalk Network Directory.

4. In \textit{password}, enter the password for the account.

5. In \textit{encryptionAlgorithm}, type \textit{ClearText} then click the \textit{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 203
Copyright notice

Copyright © 2018 Rockwell Automation Technologies, Inc. All Rights Reserved. Printed in USA.

This document and any accompanying Rockwell Software products are copyrighted by Rockwell Automation Technologies, Inc. Any reproduction and/or distribution without prior written consent from Rockwell Automation Technologies, Inc. is strictly prohibited. Please refer to the license agreement for details.

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.

Other Licenses

The software included in this product contains copyrighted software that is licensed under one or more open source licenses. Copies of those licenses are included with the software. Corresponding Source code for open source packages included in this product can be located at the web site(s) identified below and/or in the product documentation.

You may alternately obtain complete Corresponding Source code by contacting Rockwell Automation via our 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.

The following open source software is used in this product:

<table>
<thead>
<tr>
<th>Software</th>
<th>Copyright</th>
<th>License Name</th>
<th>License Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>AngularJS</td>
<td>Copyright 2010-2017 Google, Inc.</td>
<td>MIT License</td>
<td>AngularJS 1.5.9 License</td>
</tr>
<tr>
<td>Boost C++ libraries</td>
<td>Copyright Beman Dawes, David Abrahams, 1998-2005.</td>
<td>Boost Software License, Version 1.0</td>
<td>Boost C++ Libraries 1.0 License</td>
</tr>
<tr>
<td>Bootstrap</td>
<td>Copyright 2011-2017 Twitter, Inc.</td>
<td>MIT License</td>
<td>Bootstrap 3.3.7 License</td>
</tr>
<tr>
<td></td>
<td>Copyright 2011-2017 The Bootstrap Authors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flatbuffers</td>
<td>Copyright 2017 Google, Inc.</td>
<td>Apache License, Version 2.0</td>
<td>FlatBuffers 1.6.0 License</td>
</tr>
<tr>
<td>jQuery</td>
<td>Copyright 2005, 2014 JS Foundation and other contributors</td>
<td>MIT License</td>
<td>jQuery 2.1.1 License</td>
</tr>
<tr>
<td>OpenSans</td>
<td>Copyright 2017 Google, Inc.</td>
<td>Apache License, Version 2.0</td>
<td>OpenSans License</td>
</tr>
<tr>
<td>tinyxml2</td>
<td>Copyright 2017 Lee Thomason</td>
<td>zlib License</td>
<td>tinyxml2 2.2.0 License</td>
</tr>
</tbody>
</table>
Trademark Notices


Any Rockwell Automation logo, software or hardware product not mentioned herein is also a trademark, registered or otherwise, of Rockwell Automation, Inc.

Other Trademarks

Kepware is a registered trademark of Kepware Technologies. OPC is a trademark owned by OPC Foundation. EtherNet/IP is a trademark of ODVA.

Microsoft, Access, ActiveX, SQL Server, Surface, Visual Basic, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Java and Oracle are trademarks of Oracle Corporation.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Limited.

All other trademarks are the property of their respective holders and are hereby acknowledged.

Warranty

This product is warranted in accordance with the product license. The product’s performance may be affected by system configuration, the application being performed, operator control, maintenance, and other related factors. Rockwell Automation is not responsible for these intervening factors. The instructions in this document do not cover all the details or variations in the equipment, procedure, or process described, nor do they provide directions for meeting every possible contingency during installation, operation, or maintenance. This product’s implementation may vary among users.

This document is current as of the time of release of the product; however, the accompanying software may have changed since the release. Rockwell Automation, Inc. reserves the right to change any information contained in this document or the software at any time without prior notice. It is your responsibility to obtain the
most current information available from Rockwell when installing or using this product.

Environmental compliance


Contact Rockwell Automation

Customer Support Telephone — 1.440.646.3434

Online Support — http://www.rockwellautomation.com/support/
Index

A
accounts 15, 16
   administrator 16, 31, 35, 36
   computer 15, 28, 55, 56, 57, 59, 60, 89, 94, 96
   user 39, 47
action groups 63, 64, 65, 66, 131, 132, 137, 140
actions 65, 66, 137
after restoring 166, 167, 168, 172, 173, 175, 176, 177, 178, 181, 182
application 11, 19, 20, 23, 25, 27, 36, 67, 68, 69, 71, 72, 73
   local 11, 19, 20, 23, 187
   network 11, 19, 20, 36
application authorization policy 68, 69
area 83, 86, 97, 111, 113, 115, 116, 125, 126, 127, 131, 132, 143, 151
audit policies 20, 27, 32, 67, 81, 83, 84, 86
authenticated users 27, 189

B
back up 73, 74, 157, 160, 161, 163, 164, 166, 167
best practices 19, 25, 28, 31

C
chain of inheritance 132, 134, 136, 151
client computer 34, 35, 36, 37, 55, 80, 89, 96, 102, 103, 175, 203, 204
common actions 131, 137
computer account 28, 55, 56, 57, 59, 60, 89, 94, 96, 164, 168, 175, 181

d
devices 77, 114, 116, 117, 122, 125, 126, 128, 131, 137, 177

E
effective permissions 132, 152, 154

G
groups 11, 15, 16, 19, 28, 31, 42, 43, 47, 49, 50, 52, 53, 63, 131, 137

I
inheritance 19, 25, 132, 134, 136, 151, 152, 154

L
list children 39, 41, 42, 44, 47, 49, 50, 52, 55, 56, 57, 60, 63, 64, 65, 66,
   104, 105, 118, 119, 126, 127, 128, 137, 140, 142, 143, 145, 190
local applications 11, 19, 20, 23, 187, 192

M
multiple applications 13, 166

N
networks 25, 28, 79, 80, 113, 114, 115, 116, 117, 120, 121, 122, 125,
   129, 131, 132, 137, 142, 143, 145, 175, 177

O
order of precedence 31, 98, 136

P
permissions 15, 16, 19, 25, 27, 31, 131, 140, 142, 143, 145, 147, 148,
   149, 151, 152, 154
plan your system 13, 20, 23, 35
policies 32, 67, 72, 73, 74, 78, 80, 81, 83, 84, 87, 104, 105, 107, 108, 110,
   111
ports 77, 78, 203

R
read 19, 25, 28, 132, 136, 137, 142, 143, 145, 151, 152, 154, 189, 190
rename 175
resource groups 113, 120, 121, 122, 125, 126, 127, 128, 129, 131, 142,
   143, 157, 161
resources 64, 72, 73, 157, 166, 167, 168, 170, 172, 173, 178, 179
restore 64, 72, 73, 157, 166, 167, 168, 170, 172, 173, 175, 176, 177, 178,
   179, 181, 182, 183, 184, 185
runtime security 25, 107, 157, 167, 176

S
security authority identifier 157, 163, 164, 166, 167, 173, 180, 181,
   182, 185
server 19, 20, 23, 34, 35, 36, 37, 55, 72, 73, 74, 77, 78, 79, 80, 81, 89, 91,
   96, 97, 136
Index

single sign-on  25, 36, 87, 88, 89, 91, 93, 94, 96, 101, 102, 103
stand-alone system  13, 20, 23, 27, 34
system folder  11, 28, 50, 72, 73, 74, 75, 84, 93, 94, 111, 131, 137, 145,
147, 157, 160, 161, 164, 167, 168, 170, 172, 175, 177, 181, 182, 183, 184,
185

T

tag actions  13, 137, 140, 142, 143, 145, 186, 192, 197
test  77, 78, 152
tighten security  27
troubleshoot  77, 78, 81, 84

U

upgrade  77, 179, 199
user rights assignment  67, 72, 73, 74

W

write  28, 137, 143, 145
Rockwell Automation support

Rockwell Automation provides technical information on the web to assist you in using its products. At http://www.rockwellautomation.com/support you can find technical and application notes, sample code, and links to software service packs. You can also visit our Support Center at https://rockwellautomation.custhelp.com for software updates, support chats and forums, technical information, FAQs, and to sign up for product notification updates.

In addition, we offer multiple support programs for installation, configuration, and troubleshooting. For more information, contact your local distributor or Rockwell Automation representative, or visit http://www.rockwellautomation.com/services/online-phone.

Installation assistance

If you experience a problem within the first 24 hours of installation, review the information that is contained in this manual. You can contact Customer Support for initial help in getting your product up and running.

<table>
<thead>
<tr>
<th>United States or Canada</th>
<th>1.440.646.3434</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outside United States or Canada</td>
<td>Use the Worldwide Locator available at <a href="http://www.rockwellautomation.com/locations">http://www.rockwellautomation.com/locations</a>, or contact your local Rockwell Automation representative.</td>
</tr>
</tbody>
</table>

New product satisfaction return

Rockwell Automation tests all of its products to ensure that they are fully operational when shipped from the manufacturing facility. However, if your product is not functioning and needs to be returned, follow these procedures.

<table>
<thead>
<tr>
<th>United States</th>
<th>Contact your distributor. You must provide a Customer Support case number (call the phone number above to obtain one) to your distributor to complete the return process.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outside United States</td>
<td>Please contact your local Rockwell Automation representative for the return procedure.</td>
</tr>
</tbody>
</table>

Documentation feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete the feedback form, publication RA-DU002.