

**Application Technique**

Original Instructions



**Allen-Bradley**

by ROCKWELL AUTOMATION

# FactoryTalk Security Application Technique



Contents

**FactoryTalk Security overview.....5**

    FactoryTalk Services Platform.....5

    FactoryTalk Directory .....6

    Authentication .....8

    Authorization.....9

    Commissioning a FactoryTalk Security system.....10

**Configure FactoryTalk Security .....11**

    Back up FactoryTalk Directory (optional) .....12

    General configurations in the FactoryTalk system .....14

    Harden the FactoryTalk system.....43

    Temporary access .....46

**Secure a Studio 5000 Logix Designer project ..... 51**

    Enable Studio 5000 Logix Designer project security.....52

    Restore a FactoryTalk security authority identifier.....62

**Secure a FactoryTalk View project.....65**

    Securing FactoryTalk View with role-based permissions.....66

    Securing FactoryTalk View with security codes.....73

    Specific functions that need to be secured .....78

**Secure application data in FactoryTalk AssetCentre.....87**

    Secure FactoryTalk AssetCentre.....88

    Disaster recovery for a ControlLogix project.....93

    Disaster recovery for a FactoryTalk View Site Edition project .....103

**Product policies and securable actions supported by FactoryTalk Security ..... 118**

    Product policies and securable actions of Studio 5000 Logix Designer.....118

    Product policies and securable actions of FactoryTalk View SE .....123

    Product policies and securable actions of FactoryTalk AssetCentre .....124

# Important User Information

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

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

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

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

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

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

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

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



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

---



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

---

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

---

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

---



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

---



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

---



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

---

The following icon may appear in the text of this document.



**Tip:** Identifies information that is useful and can help to make a process easier to do or easier to understand.

Rockwell Automation recognizes that some of the terms that are currently used in our industry and in this publication are not in alignment with the movement toward inclusive language in technology. We are proactively collaborating with industry peers to find alternatives to such terms and making changes to our products and content. Please excuse the use of such terms in our content while we implement these changes.

## Preface

This manual explains:

- How to use FactoryTalk® Security to implement authentication and authorization in your industrial automation system.
- How to enforce product-specific security for Studio 5000 Logix Designer®, FactoryTalk View, and FactoryTalk AssetCentre.

## Additional resources

These documents contain additional information concerning related products from Rockwell Automation®.

Resource	Description
<i>System Security Design Guidelines Reference Manual</i> , <a href="#">SECURE-RM001</a>	Provides guidelines for how to use Rockwell Automation products to improve the security of your industrial automation system.
<i>Security Configuration User Manual</i> , <a href="#">SECURE-UM001</a>	Describes how to configure and use Rockwell Automation products to achieve IEC security certification levels for products and systems.
<i>CIP Security with Rockwell Automation Products Application Technique</i> , <a href="#">SECURE-AT001</a>	Describes how to implement the Common Industrial Protocol (CIP™) Security standard in your control system.
<i>Converged Plantwide Ethernet (CPwE) Design and Implementation Guide</i> , <a href="#">ENET-TD001</a>	Provides guidelines for how to design, implement, and manage industrial Ethernet networks.
<i>Logix 5000 Controllers Security Programming Manual</i> , <a href="#">1756-PM016</a>	Describes how to configure security for the Logix Designer application and set up source protection for your logic and projects.
<i>FactoryTalk AssetCentre Getting Results Guide</i> , <a href="#">FTAC-GRO02</a>	Provides an overview of how to configure FactoryTalk AssetCentre features.



## FactoryTalk Security overview

As an integrated part of FactoryTalk Services Platform, FactoryTalk Security improves the security of an automation system by limiting access to users with a legitimate need to access the products. Security in the FactoryTalk system is accomplished through authentication and authorization. FactoryTalk Security provides authentication and authorization services to enable application-level security for all FactoryTalk-enabled products that are a part of that directory.

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

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

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

FactoryTalk Security services are integrated into the FactoryTalk Directory and are always present wherever the FactoryTalk Services Platform software is installed. Use FactoryTalk Administration Console to configure FactoryTalk Security.

## FactoryTalk Services Platform

FactoryTalk Services Platform provides a set of shared services that are used by all FactoryTalk software applications in the system.

The security services in FactoryTalk Services Platform:

- Function similarly to Windows® Active Directory.
- Provide identity management services to verify the identity of each user and grant or deny user requests to perform a particular set of actions on resources within the system.
- Manage users and user groups.
- Grant permissions to users or user groups based on role.

FactoryTalk Services Platform includes components that make up the core software services in the FactoryTalk suite of products:

- **FactoryTalk Directory server:** Acts as a central repository of configuration information that gets shared to all the computers in the FactoryTalk system. It stores the security configuration for users, groups, computers, and automation assets.
- **FactoryTalk Directory client:** Connects to the FactoryTalk Directory server as a member of the directory and gets configuration, authentication, and authorization information from the server.
- **FactoryTalk Administration Console:** Manages all configurations in the FactoryTalk system.
- **FactoryTalk Security:** Enforces security policy configurations. It secures access permissions, application settings, and resources allocation.
- **FactoryTalk Live Data:** Delivers automation data from the network to the FactoryTalk suite of products.

FactoryTalk Services Platform is installed by either of the following methods:

- A FactoryTalk product installation package, such as FactoryTalk View or Studio 5000 Logix Designer. FactoryTalk Services Platform is included in the installation package of every product that requires it.
- The [Rockwell Automation Product Compatibility and Download Center \(PCDC\)](#) website. On the **Compatibility & Downloads** page, enter **FactoryTalk Services** in the search box. FactoryTalk Services appears in your download list.

## FactoryTalk Directory

The FactoryTalk Directory defines all computers, FactoryTalk products, components, and users and groups that are in the system. Each participating computer on the network acts as a client to the FactoryTalk Directory server and can share directory services and resources.

## FactoryTalk Directory types

FactoryTalk Services Platform installs and configures two 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 configuration cannot be shared across a network or between a local and network directory on the same computer. Products such as FactoryTalk View SE (local station) and FactoryTalk View ME use the local directory.
- A **network** directory organizes project information and security settings from multiple FactoryTalk products across multiple computers on a network. Products such as FactoryTalk View SE (network distributed) and FactoryTalk Transaction Manager use the network directory.

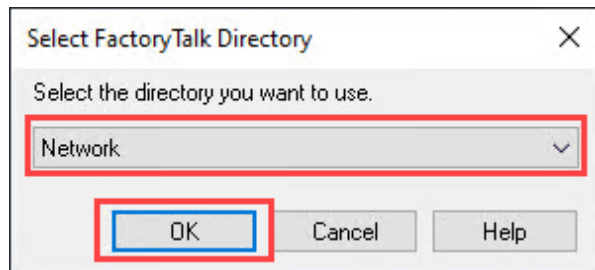
Determining which directory to use depends on the software products and whether the environment is standalone or networked. In most systems, the network directory should be used to configure FactoryTalk Security, so that policy can be applied to each computer in the system. It is also the case that if there are multiple computers that use the local directory, each computer would have to be configured locally.

## FactoryTalk Directory structure

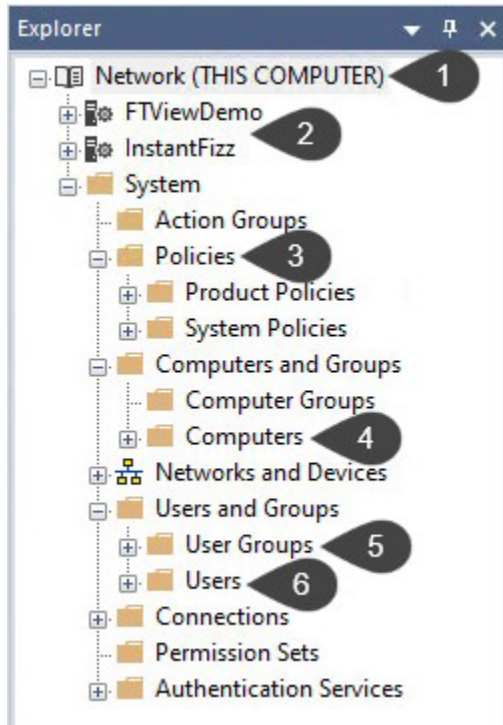
For most applications of FactoryTalk Security, the FactoryTalk network directory is where you should configure security because the settings configured here can be propagated to all the computers defined in the network directory whereas settings in the local directory can only be applied to a single computer.

### To view the structure of FactoryTalk network directory

1. Start FactoryTalk Administration Console.
2. Select **Network**, and then select **OK**.



The following image shows the structure of the default FactoryTalk network directory after installation.



Items	Description
1	The directory root, indicating the directory type (network or local) and where the directory resides.
2	FactoryTalk network applications.
3	System policies and product policies. System policies are sets of policies that apply system wide while product policies are sets of securable features for the individual products in your FactoryTalk system.
4	List of computers that are members of this FactoryTalk network directory.
5	User groups defined within the FactoryTalk Directory. These can be FactoryTalk user groups, or Windows-linked or Azure AD user groups.
6	Users defined within the FactoryTalk Directory. These can be FactoryTalk users or Windows-linked user accounts.

## Policy configuration inheritance

The FactoryTalk Directory is a hierarchical system, organized from top to bottom. In general, all settings inherit from top to bottom, that is, from parent objects to child objects. As a result, policy definitions made at the directory root (that is, the Network or Local object at the top of the tree) are inherited down through the folder structure in the system.

The inheritance model lets you establish a baseline of policies that are used with all subfolders. If you need to change a policy across many subfolders, you change the configuration at the next level up in the hierarchy, or at the directory root. This allows the configuration change to be applied at that level and inherited down to all sublevels.

You can also change policies on a specific subfolder without affecting its parent nodes in the hierarchy. Keep in mind, however, that a change in one folder cascades down to lower-level folders.

Users can be members of multiple groups or have policy settings assigned to them directly. In these situations, the configuration of the policy settings determines their access level.

To enforce the principle of “least privilege”, we recommend that you use the **Deny** checkboxes to make sure that users are always granted only the privileges of the most restrictive group of which they are a member.

When you change the **Allow**, **Deny**, or unselected configuration, remember the following:

- Grayed-out selection: You can perform this action, and the permission is inherited from a higher level.
- No selection: You cannot perform this action. This permission is inherited from a higher level.
- Solid selected Allow: You can perform this action, and the permission is granted at this folder level.
- Solid selected Deny: You cannot perform this action, and the permission is denied at this folder level. Inherited permissions cannot overrule this Deny setting.

You can change permissions across an entire set of actions. However, we recommend that you change permissions on an action-by-action basis.

Because **Deny** takes precedence, once you deny any permission, a warning message appears when you select **OK**; select **Yes** to verify the choice.

---

**IMPORTANT:** Never explicitly deny permissions to the **Administrators** group in a FactoryTalk Directory. Rather, configure specific user groups of your own and deny permissions to those groups. By denying permissions to **All Users** or **Administrators**, you lock everyone out of the system and deny permissions in all FactoryTalk-enabled products.

---

For additional information related to configuring the FactoryTalk Directory, see *Security Configuration User Manual* listed in [Additional Resources on page 4](#).

## Authentication

Authentication verifies a user’s identity and whether a request for service originates with that user.

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

FactoryTalk Services Platform supports these types of use groups and users:

- Windows-linked user groups and users
  - These are managed from the Windows domain or the workgroup, but they need to be added to the FactoryTalk Directory.
  - Settings such as password encryption, complexity requirements, and others are all controlled by Windows domain settings.
  - These use groups and users allow for single sign-on, so that users can automatically sign in to FactoryTalk applications with their Windows account.
  - If a client computer is disconnected from the Windows domain, these users will only be able to sign in if the Windows operating system is configured to cache the sign-in information.
- Azure® Active Directory (Azure AD) user groups
  - These are managed from the Azure AD that operates in the cloud and offers authentication and authorization services to various cloud-based applications. The Azure AD user groups need to be added to the FactoryTalk Directory.
  - Settings such as password encryption, users and groups, and others are all controlled by Azure AD settings.
  - These user groups and users allow for single sign-on, so that users can automatically sign in to FactoryTalk applications with their Azure AD account.
  - If the Azure AD group is updated on the Azure side, the FactoryTalk system cannot automatically synchronize the changes to the FactoryTalk Directory. You must add the group to the FactoryTalk Directory again for it to get the latest Azure AD group configuration.
- FactoryTalk user groups and users
  - These are managed within FactoryTalk Administration Console.
  - Settings such as password encryption, complexity requirements, and others are all controlled by security policies.
  - If a client computer is disconnected from the FactoryTalk Directory, users will still be able to authenticate using the local cache.

When user groups and users are linked from the Windows Active Directory, it acts as an identity provider for FactoryTalk Security, allowing users to authenticate to the system with a domain account. This allows the user management to be handled at the domain level.

Using Windows Active Directory accounts also means that the sign-in information is secured by Windows, as FactoryTalk is just passing the request to the Windows operating system.

FactoryTalk does not cache credentials for Windows-linked users or groups. By default, however, the Windows operating system caches the Windows security token for each unique user's ten most recent valid logons. For more information on cached security credentials, see Microsoft.com. This cached verifier allows Windows-linked user accounts to be authenticated even when the domain controller is not connected or able to provide authentication. Windows is responsible for encrypting this cached verifier.

However, this caching does not apply to Windows-linked groups. Neither the FactoryTalk Directory system nor the Windows operating system caches Windows domain group information; there is no way for the FactoryTalk system to determine what domain accounts are members of a Windows-linked group when disconnected from the domain. If you want to use groups in the FactoryTalk system and you expect to be disconnected from the domain, it is suggested that you use FactoryTalk user groups that contain Windows-linked users.

## Authorization

Authorization verifies a user's request to access a software resource based on the access permissions defined for that user. To manage user authorization, use system policies, product policies, or securable actions.

## System policies

System policies are sets of policies that apply system wide. For example, password length, complexity, expiration, and so on. All FactoryTalk products use the policies in the **System Policies** folder in FactoryTalk Administration Console. Policy settings are separate in the network directory and the local directory. They can apply to all users and all computers or specific users on specific computers.

## Product policies

Product policies are sets of securable features for the individual products in your FactoryTalk system, and they apply to that product in every context. For example, in the Studio 5000 Logix Designer application, set a policy controlling who can create projects. This policy does not affect other software products but will affect every instance of Studio 5000 Logix Designer that is running on a computer that is a member of this FactoryTalk Directory.

Individual products' policies are located in the **Product Policies** folder in FactoryTalk Administration Console. Product policy options vary depending on the individual products that they are associated with. You can modify these policies on a product-by-product basis for specific users, groups, and computers included within the FactoryTalk Directory.

Define security settings to restrict access to the features of individual FactoryTalk products in your system. Only users with the required level of access can use the product features that you have secured.

## Securable actions

Securable actions apply to all products that use that action in a particular context, such as an application or area. For example, **Tag > Write Value** controls whether a user or group can write to tags that are on a data server. This action applies to all software products that attempt to write to the tag on that data server.

In some cases, there are securable actions and product policies for the same capability. For example, Studio 5000 Logix Designer has a securable action and a product policy named **Firmware: Update**.

- The securable action applies to all products. If the permission to the **Firmware: Update** action is denied in an application or area, firmware in the controller from that application or area using any product (for example, ControlFLASH Plus®) cannot be updated.
- The product policy applies to only the Logix Designer application. If the permission to **Firmware: Update** is denied, firmware cannot be updated when using the Logix Designer application to configure any controller.

## Commissioning a FactoryTalk Security system

When approaching the task of commissioning a FactoryTalk Security system, pre-planning of the system security model can greatly reduce the time required. A system security model is the combination of three components:

- A security permission (an action)
- User or users authorized to perform the action
- Computer or computers from which the action is authorized

If the security models are constructed with individual user accounts, each account must be tested during commissioning. This testing process is applicable to each FactoryTalk users, Windows-linked users, Windows-linked user groups, and Azure AD groups used in a security model. That is, each security model must be tested for each user or group that is part of the model. This testing, one might correctly conclude, is time-consuming at scale.

When the system's security models make use of FactoryTalk user groups, the time to test each security model is greatly reduced. Rather than testing each user or user group in the security model, it is only necessary to test a member of the FactoryTalk user group that is part of a security model. You can use FactoryTalk users in FactoryTalk user groups to test for commissioning. Once the security model is tested, the FactoryTalk user group membership can be established using FactoryTalk users, Windows-linked user groups, Windows-linked users, or Azure AD groups.

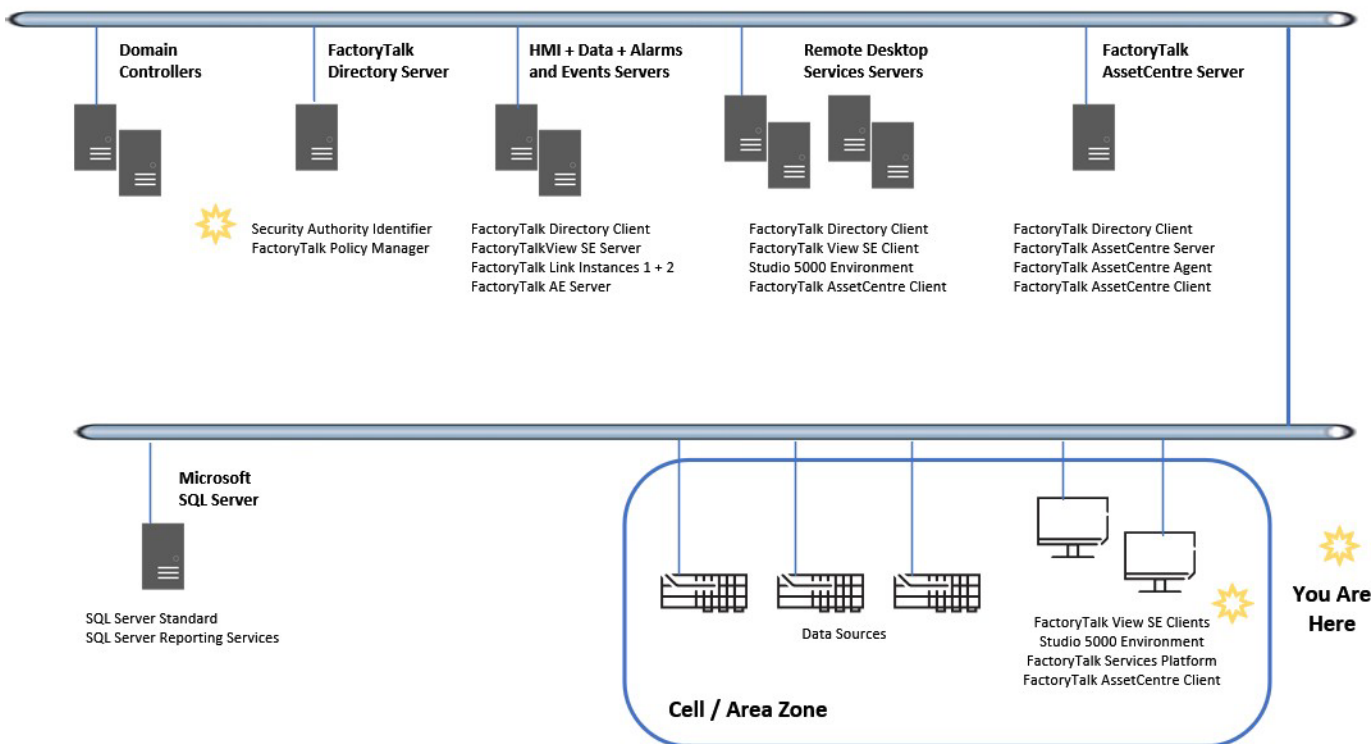
The most effective FactoryTalk configurations use FactoryTalk user groups in their security model definitions and add Windows-linked user groups or Azure AD groups to the FactoryTalk group. This best practice transfers administration of users from the FactoryTalk administrator to an IT administrator.



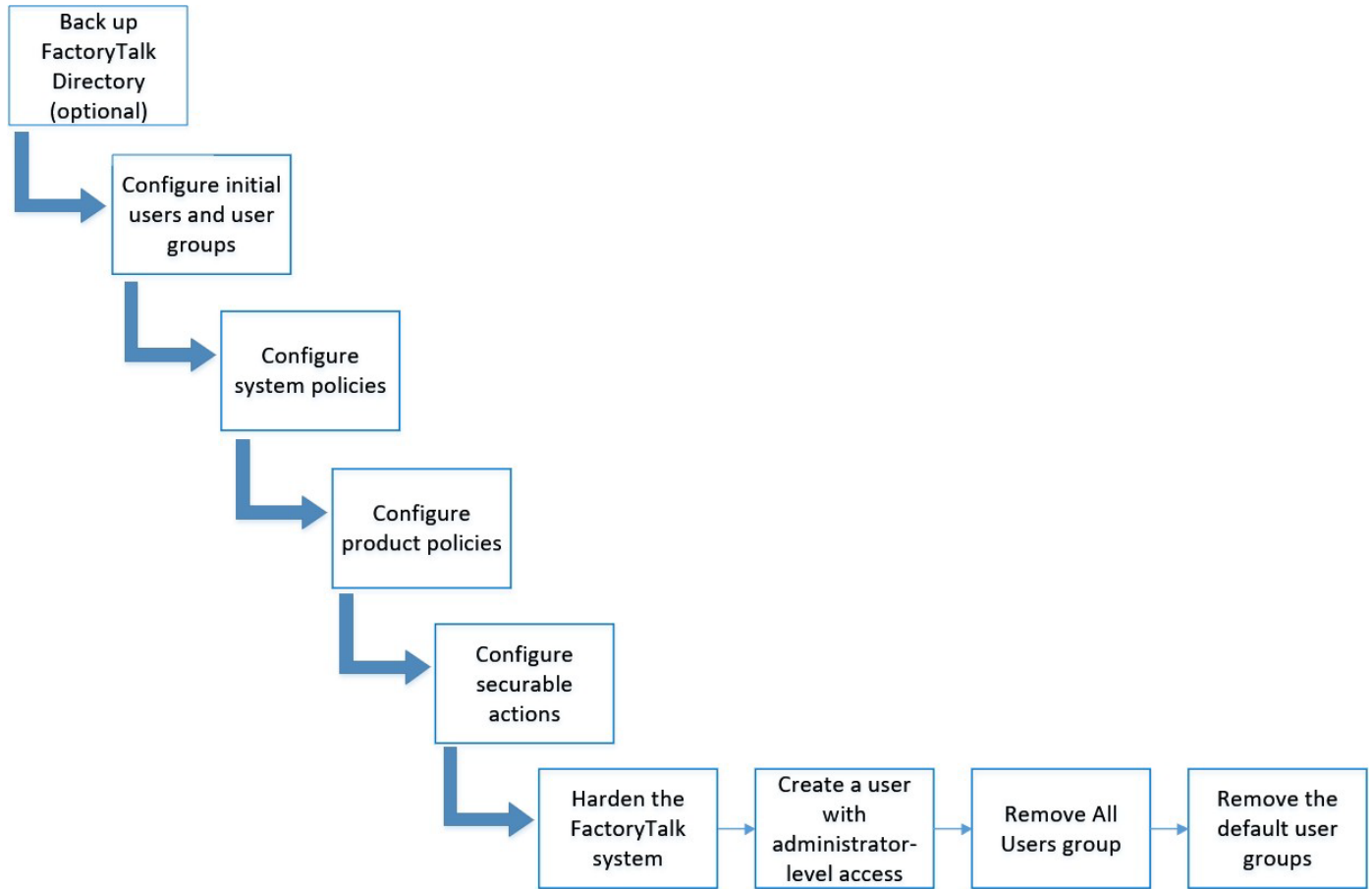
## Configure FactoryTalk Security

FactoryTalk Security controls access to and usage of FactoryTalk Directory resources by users, groups, roles, and computers. Use FactoryTalk Administration Console to configure, manage, and secure FactoryTalk Directory resources and services.

### Manufacturing Zone



Workflow

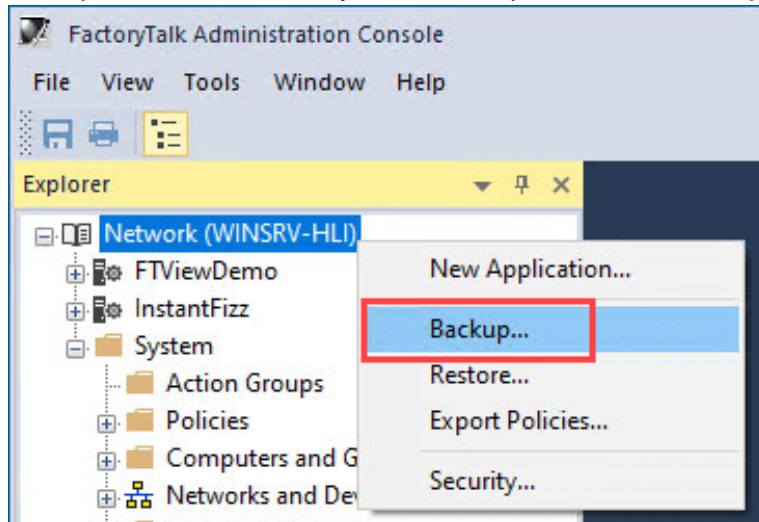


## Back up FactoryTalk Directory (optional)

Backing up the FactoryTalk Directory allows you to recover to a known working state should you make any changes that you want to undo. As you make changes to the FactoryTalk system, make sure to back up the FactoryTalk Directory.

### To back up FactoryTalk Directory

1. In FactoryTalk Administration Console, right-click the directory root, and then select **Backup**.



- In the **Backup** dialog box, configure the settings as needed, and then select **OK**.

**NOTE:** You have the option to create a password, encrypting this backup archive. Be sure to remember your password. If you encrypt a backup and forget the password, there is no way to decrypt the backup archive.

**Backup**

Specify archive name:

Specify archive location:  
 ...

**Backup Contents**

☒ **FactoryTalk Directory configuration**  
 All applications, FactoryTalk Directory System folder contents (actions, policies, computers, users, groups, connections, and permission sets), FactoryTalk Linx shortcut definitions and FactoryTalk Linx OPC UA Connector configuration for all computers configured in the directory.

☒ **FactoryTalk Linx configuration**  
 Network Browser settings (e.g. drivers) and network information (required for shortcut to operate) from this computer.

☐ **FactoryTalk Linx Gateway configuration**  
 Server configuration, UA Server Endpoint settings, Advanced Settings and UA Tag List configuration.

**File Encryption**

You have the option to now protect your backup files with a passphrase. You will be required to enter the passphrase when you restore any backup file that is passphrase protected.

NOTE: Backup files may be restored on any computer.

☐ **Encrypt file contents** (Clear the check box to create a plain text backup file)

Passphrase:

Confirm passphrase:

**OK** Cancel Help

- Select **OK** to continue with the backup.
- Select **OK**.

**FactoryTalk Administration Console**

**i** The backup was successfully completed.

**OK**

## General configurations in the FactoryTalk system

General configurations of the FactoryTalk system include user groups, users, system policies, product policies, and securable actions.

When you install FactoryTalk Services Platform on a computer for the first time, the FactoryTalk Directory is configured to allow access to all users by default. Any user who is a member of the local Windows Administrators group or who is authenticated by the Windows operating system has full access to the FactoryTalk system.

## User group and user configuration

To assign specific permissions to specific users and groups, you must create and configure user groups and user accounts. Creating user groups before adding users makes managing user access a much easier task. Users added to a group inherit the security settings of that group.

### How to choose the type of user groups or user accounts

- Windows-linked user groups and user accounts

If your system is integrated with your Windows Active Directory infrastructure and you want the administrative access to be tied to that Windows Active Directory, use Windows-linked user groups and accounts. Using Windows-linked user groups and accounts provides a convenient way to add large numbers of existing Windows user groups and accounts to the FactoryTalk system.

However, in the unlikely event that all the Windows users or groups with administrator permissions are removed from the system on the IT side, you lose administrative access to the FactoryTalk Directory. If that's a concern, a FactoryTalk user can be created as an administrator account.

- Azure AD user groups

If your system is integrated with your Azure AD infrastructure and you want the administrative access to be tied to that Azure AD, use Azure AD user groups. Using Azure AD user groups provides a convenient way to add large numbers of existing Azure AD user groups and accounts to the FactoryTalk system.

However, if the Azure AD group is updated on the Azure side, the FactoryTalk system cannot automatically synchronize the changes to the FactoryTalk Directory. You must add the group to the FactoryTalk Directory again for it to get the latest Azure AD group information.

- FactoryTalk user groups and user accounts

FactoryTalk user groups and accounts provide secure access to the FactoryTalk system independently of the level of access users have in Windows. FactoryTalk Directory user accounts provide the benefits and convenience of centralized administration within the FactoryTalk system, without needing a Windows domain. FactoryTalk user groups and accounts also retain their security settings if the FactoryTalk Directory moves to a new domain.

However, the risk is that FactoryTalk user groups and accounts cannot be managed automatically through the IT system. For example, if a user who has the only FactoryTalk administrator account is not available anymore, someone else would have to change the password of that FactoryTalk administrator account. Otherwise, no one will be able to access the system in the FactoryTalk Directory.

The most common best practice is to use Windows-linked user groups from your Windows Active Directory or Azure AD groups and add them to FactoryTalk user groups.

Thus, the recommended configuration of user groups and users is in this order:

1. Add Windows-linked user groups.
2. Add Azure AD user groups.
3. Add Windows-linked users.
4. Create FactoryTalk users.
5. Create FactoryTalk user groups to hold those groups and users created in step 1 through step 4.

---

**NOTE:** FactoryTalk user groups cannot be nested.

---

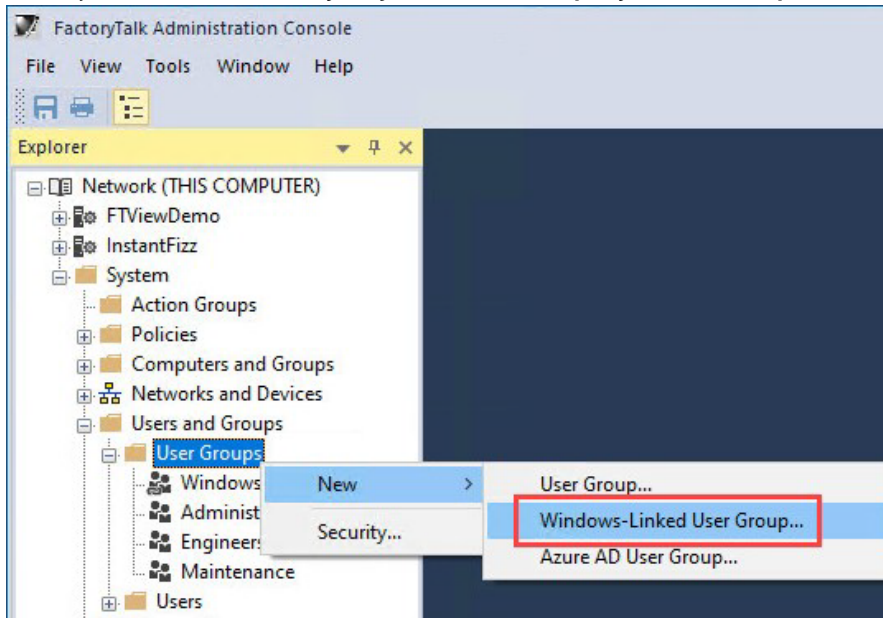
The reason of doing so is that all the individual user management is done by your IT department. If those user groups exist in the Windows Active Directory, you don't have to manage individual users in the FactoryTalk system, and instead you can assign FactoryTalk group membership based on the actual employment role rather than assigning individual users. Additionally, if a user joins or leaves the company, the user groups are managed on the IT side, and FactoryTalk user groups automatically hold all the changes.

## Add a Windows-linked user group

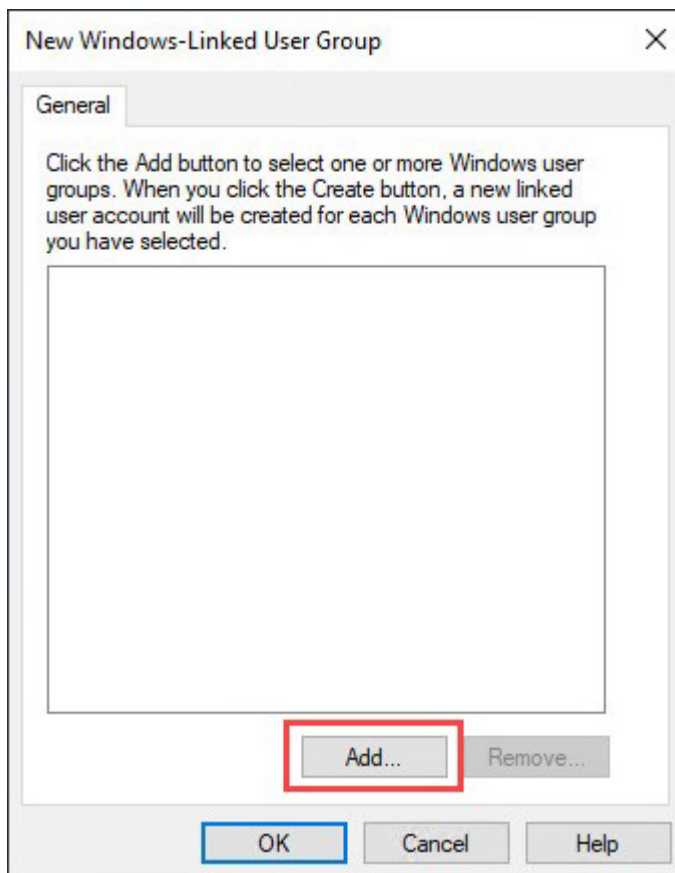
If you are in a Windows domain and you want the user groups and users that are already configured in the domain, add the Windows-linked user groups.

### To add a Windows-linked user group

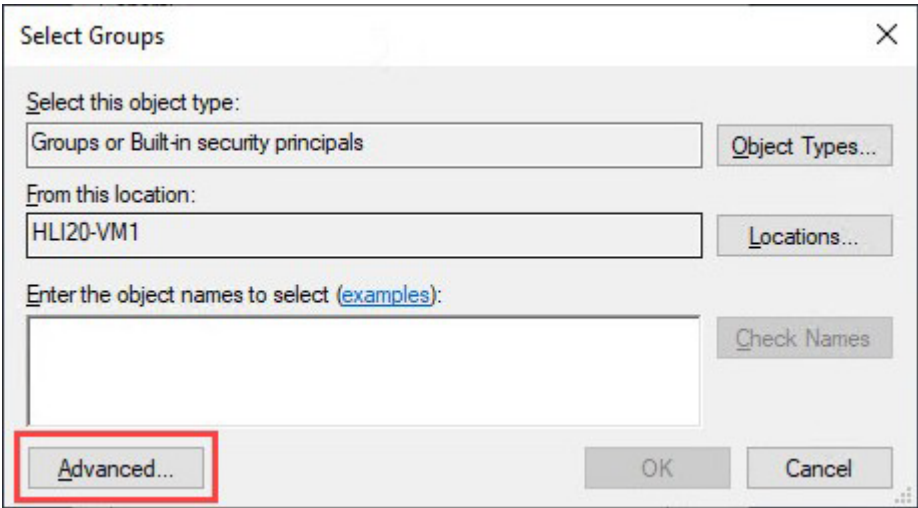
1. In FactoryTalk Administration Console, go to **System > User and Groups**, right-click **User Groups**, and then select **New > Windows-Linked User Group**.



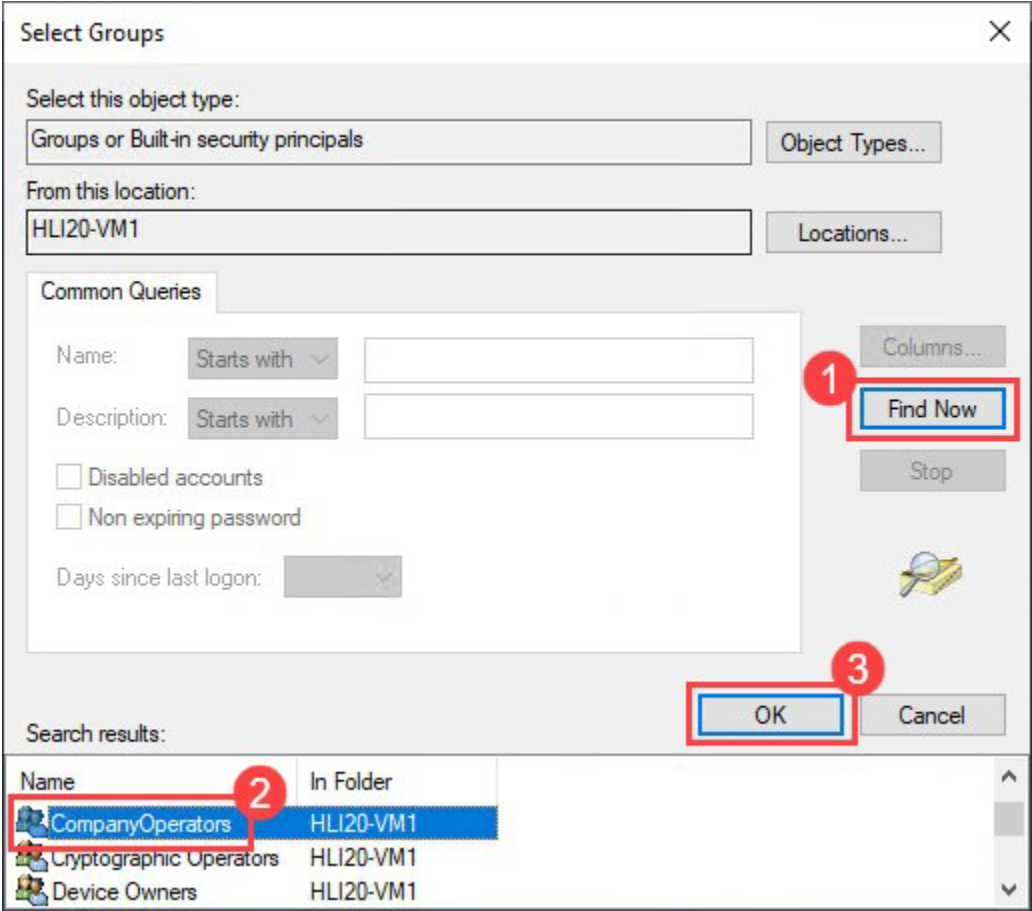
2. In the **New Windows-Linked User Group** dialog box, select **Add**.



3. In the **Select Groups** dialog box, select **Advanced**.

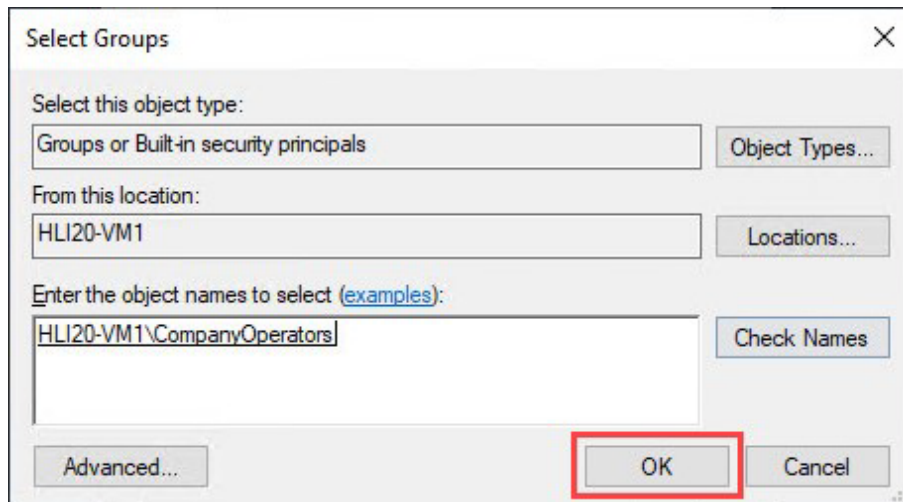


4. Select **Find Now**, select the Windows user group, **CompanyOperators** in this example, and then select **OK**.

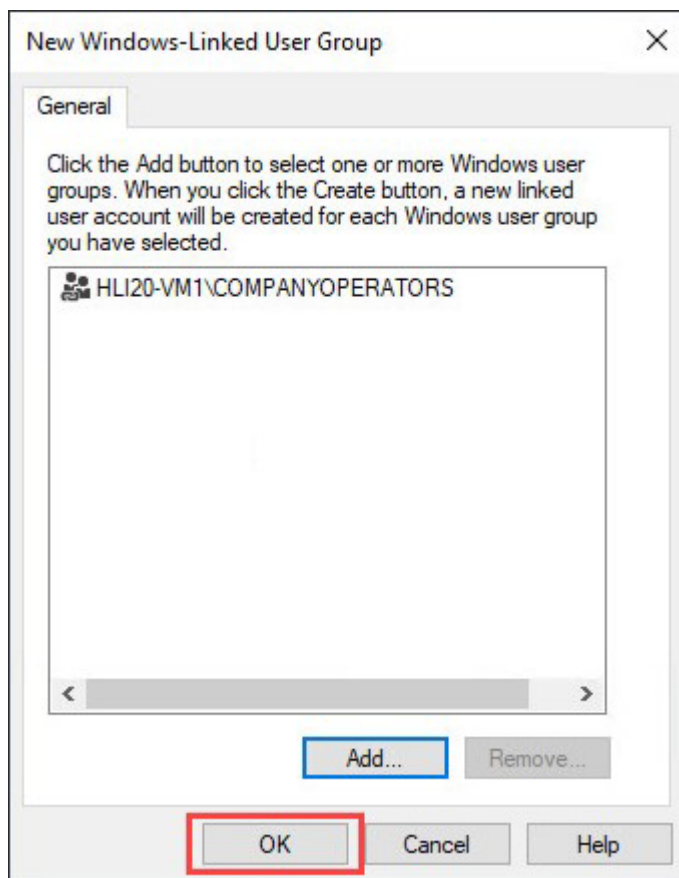




5. In the **Select Groups** dialog box, select **OK**.



6. In the **New Windows-Linked User Group** dialog box, select **OK**.



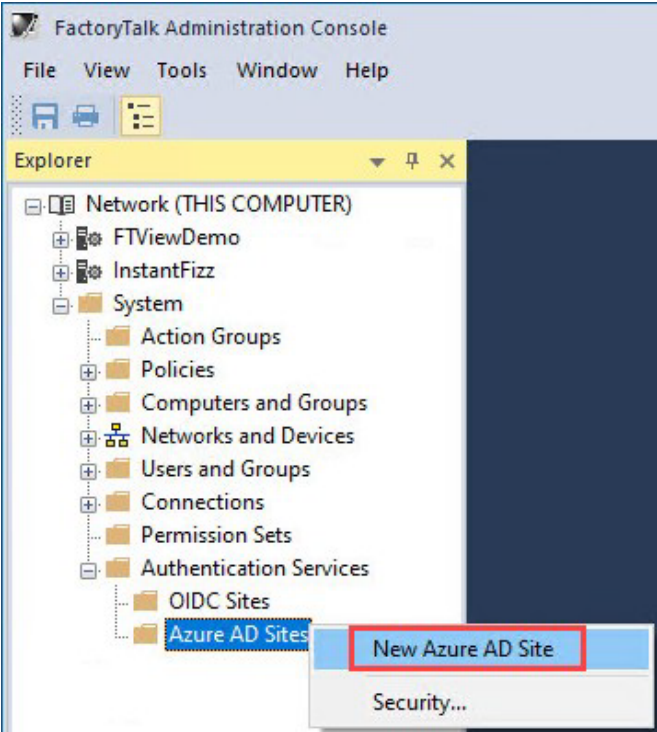
## Add an Azure AD user group

If your applications are Azure cloud-based and you want the user groups and users that are already configured in the Azure AD, use Azure AD user groups. To use Azure AD user groups, perform these key tasks:

1. Configure Azure AD in the Azure portal.
2. Add an Azure AD site in FactoryTalk Administration Console.
3. Add an Azure AD user group in FactoryTalk Administration Console.

To add an Azure AD user group

- 1.    Configure Azure AD in the Azure portal.  
For detailed instructions, see *Configure Azure Active Directory* in *FactoryTalk Services Platform Help*.
- 2.    Add an Azure AD site in FactoryTalk Administration Console.
  - a.    Right-click **Authentication Services > Azure AD Sites**, and then select **New Azure AD Site**.

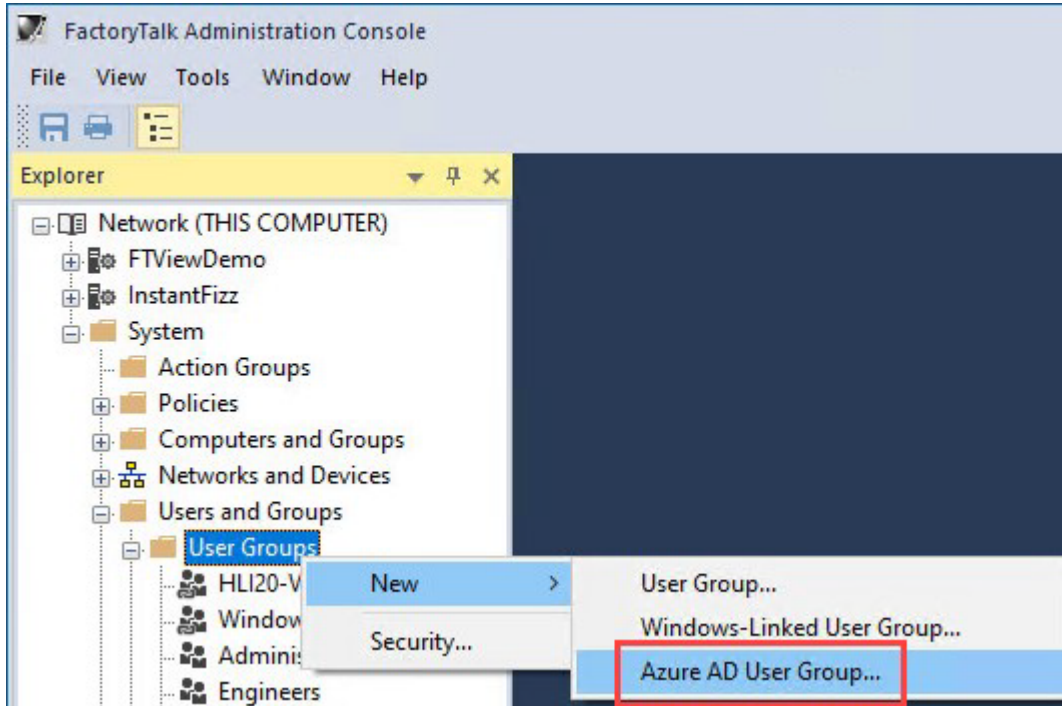


- b.    In the **New Azure AD Site** dialog box, enter information in the required boxes. For detailed instructions, select **Help**.

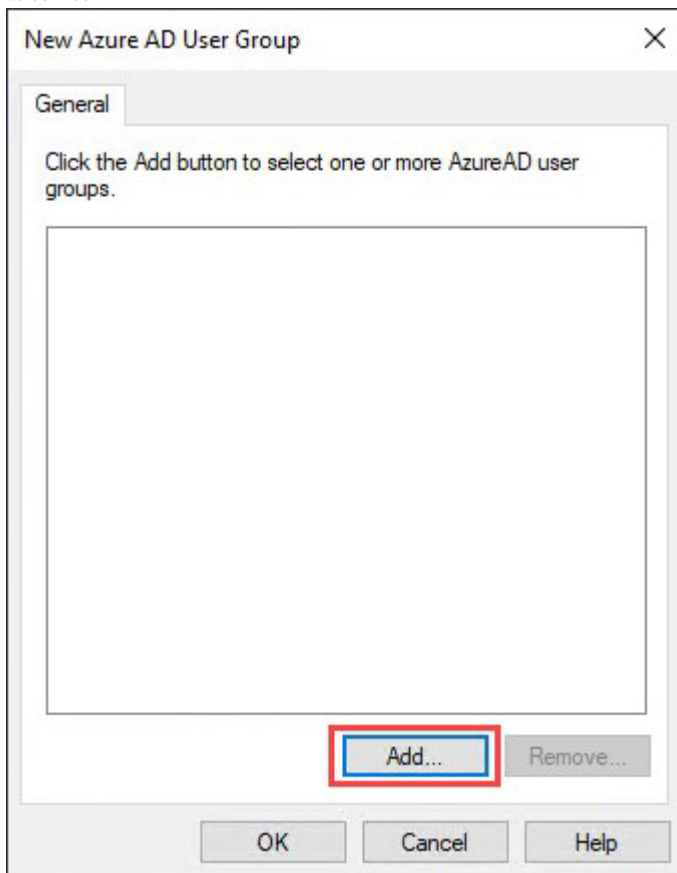
A screenshot of the 'New Azure AD Site' dialog box. It contains several input fields: 'Name' (with 'RA FTSP' entered), 'Description' (empty), 'Application(client) ID' (with a blurred value), 'Directory(tenant) ID' (with a blurred value), and 'Application(client) Secret' (with a masked value and a trash icon). At the bottom are 'OK', 'Cancel', and 'Help' buttons. The 'OK' button is highlighted with a blue border.

- c.    Select **OK**.

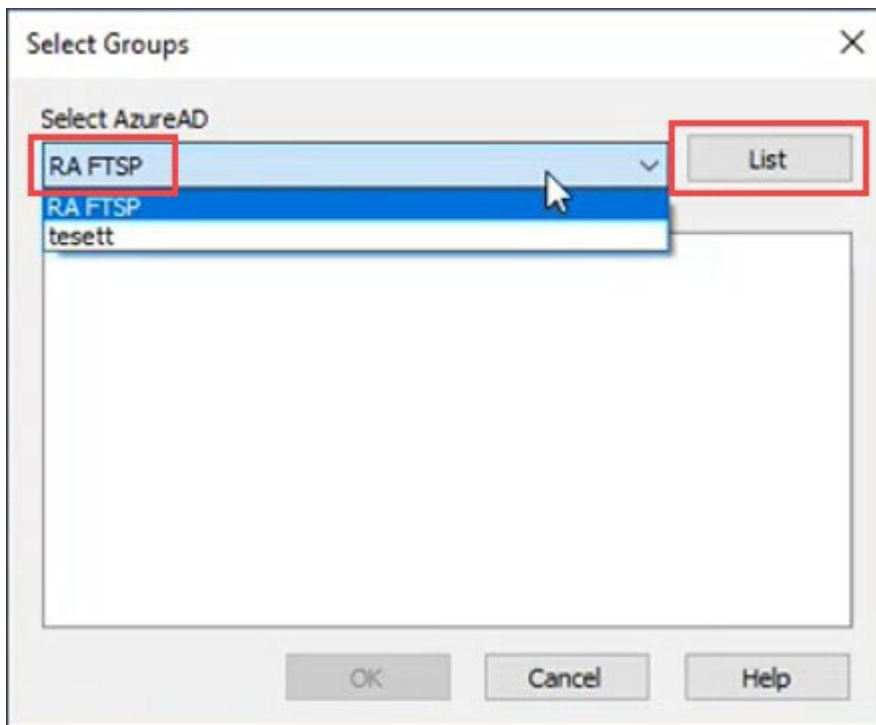
3. Add an Azure AD user group in FactoryTalk Administration Console.
  - a. Go to **System > User and Groups**, right-click **User Groups**, and then select **New > Azure AD User Group**.



- b. Select **Add**.



- c. Select the configured Azure AD site, and then select **List**.



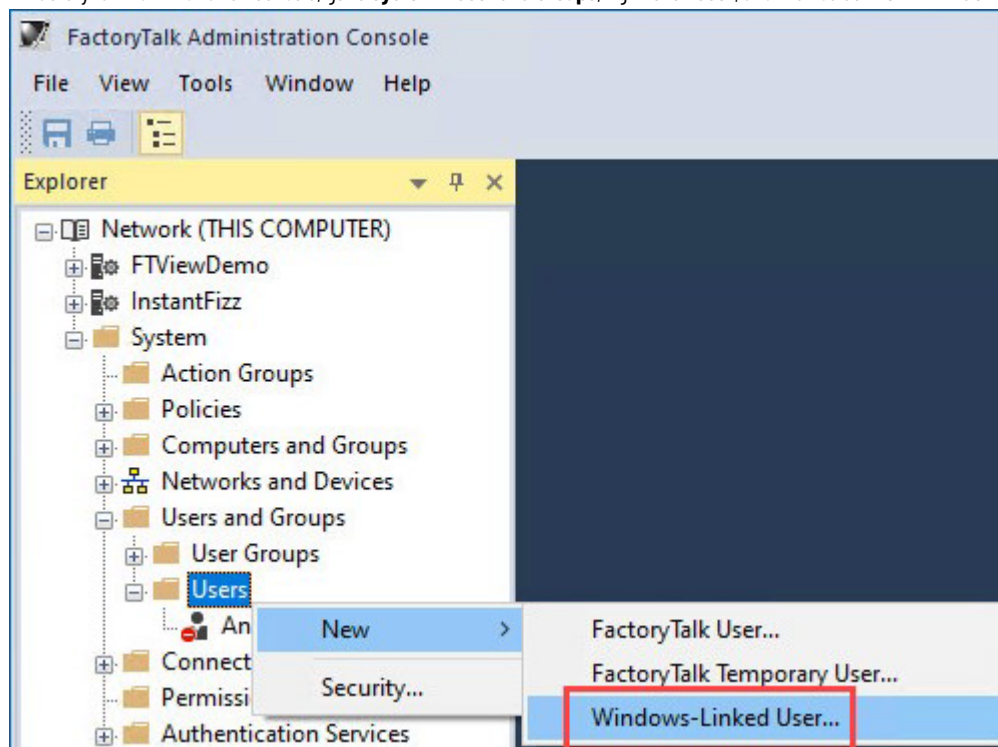
- d. Sign in to Microsoft®, select a Azure AD user group, and then select **OK**.
- e. In the **New Azure AD User Group** dialog box, select **OK**.

## Add a Windows-linked user

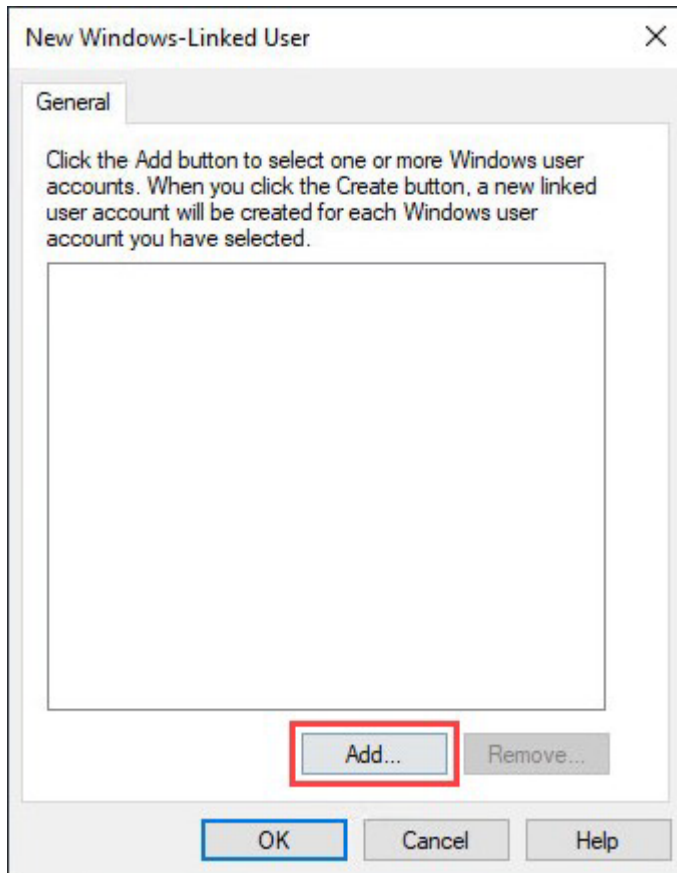
For demonstration purposes, a Windows user, *UserA* is used as an example.

### To add a Windows-linked user

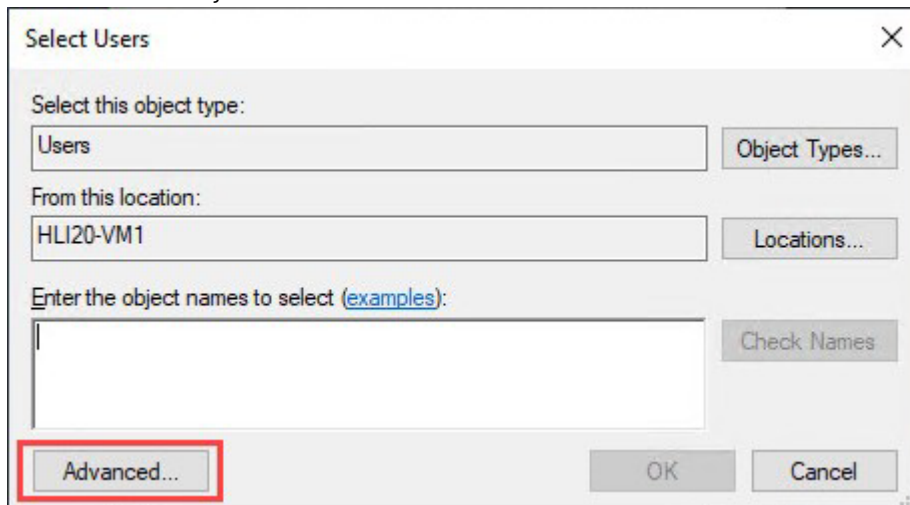
1. In FactoryTalk Administration Console, go to **System > User and Groups**, right-click **User**, and then select **New > Windows-Linked User**.



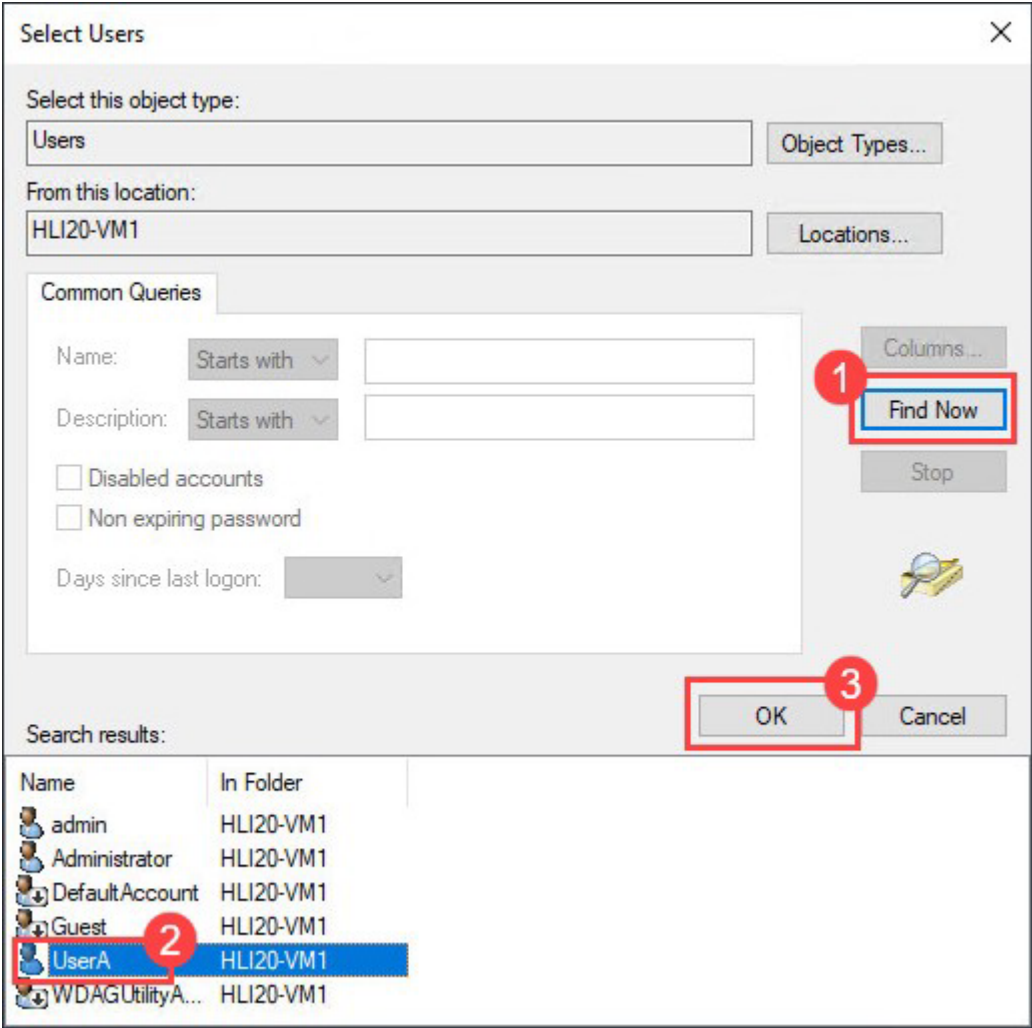
2. In the **New Windows-Linked User** dialog box, select **Add**.



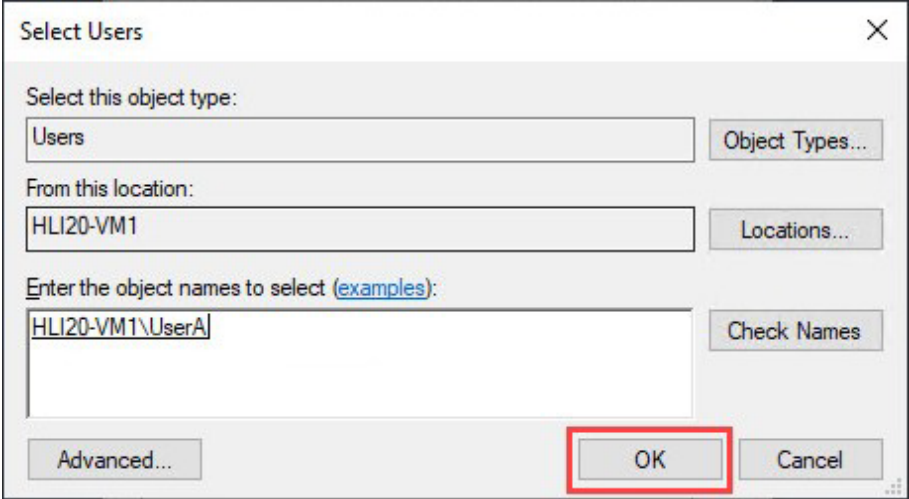
3. In the **Select Users** dialog box, select **Advanced**.



4. Select **Find Now**, select the Windows user, **UserA** in this example, and then select **OK**.

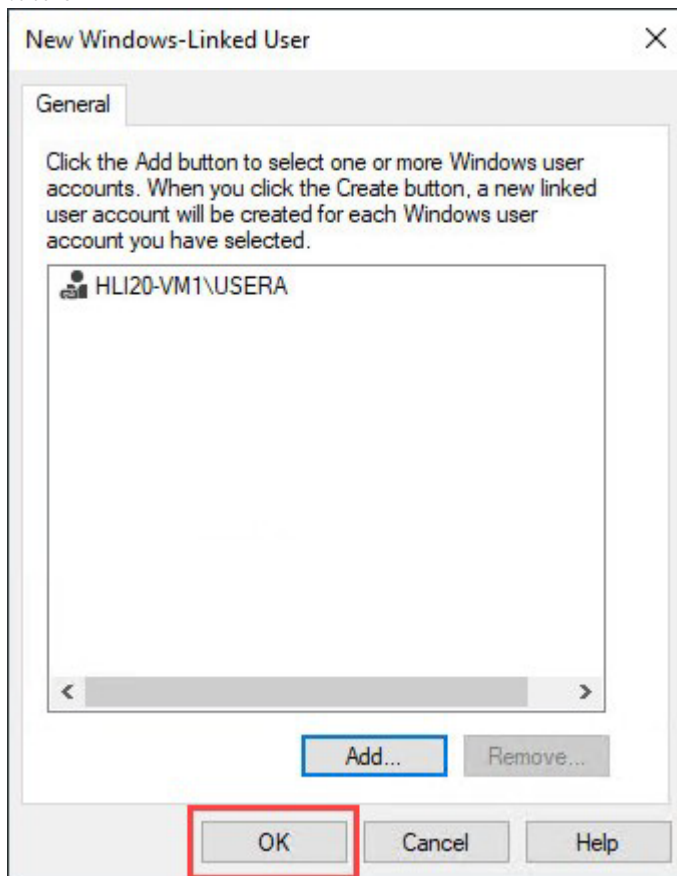


5. Select **OK**.





6. Select **OK**.

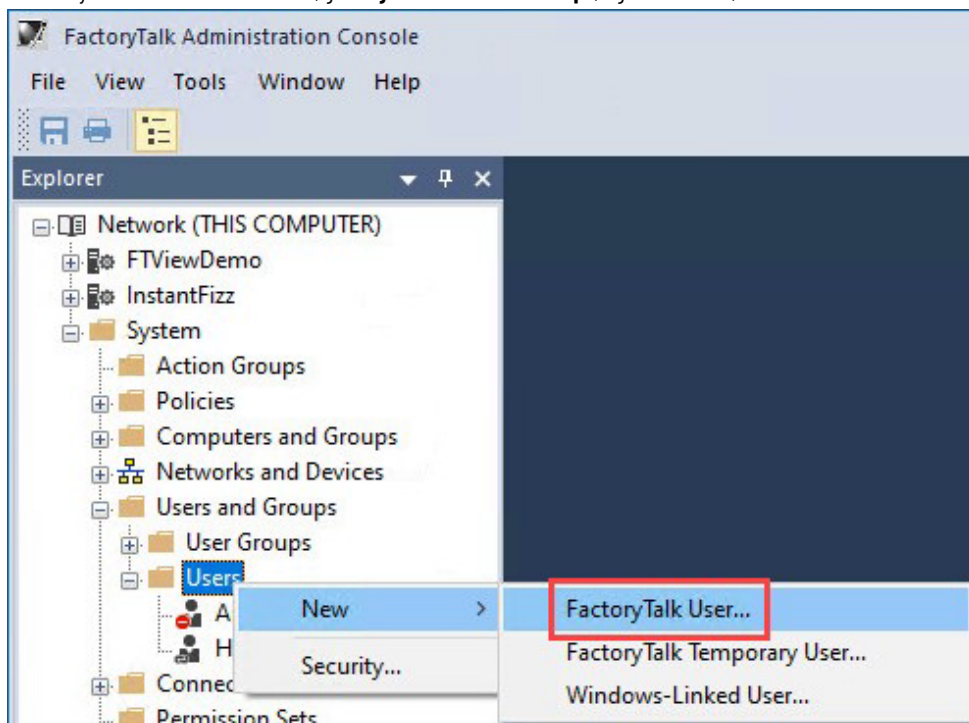


## Add a FactoryTalk user

For demonstration purposes, a FactoryTalk user, *Operator* is used as an example.

### To add a FactoryTalk user

1. In FactoryTalk Administration Console, go to **System > User and Groups**, right-click **User**, and then select **New > FactoryTalk User**.



2. Enter the username, full name, and password.

The screenshot shows the 'New FactoryTalk User' dialog box with the 'General' tab active. The following fields are populated:

- User name: Operator
- Full name: FactoryTalk Operator
- Description: (empty)
- E-mail: (empty)
- Account is disabled: ☐
- Login method: Password (selected from dropdown)
- Password: (masked with dots)
- Confirm: (masked with dots)
- User must change password at next logon: ☐
- User cannot change password: ☐
- Password never expires: ☐
- Facility Code: (empty)
- Badge ID: (empty) with a 'Scan' button
- Disable date: ☐ (empty date field)

The 'OK' button at the bottom is highlighted with a blue border.

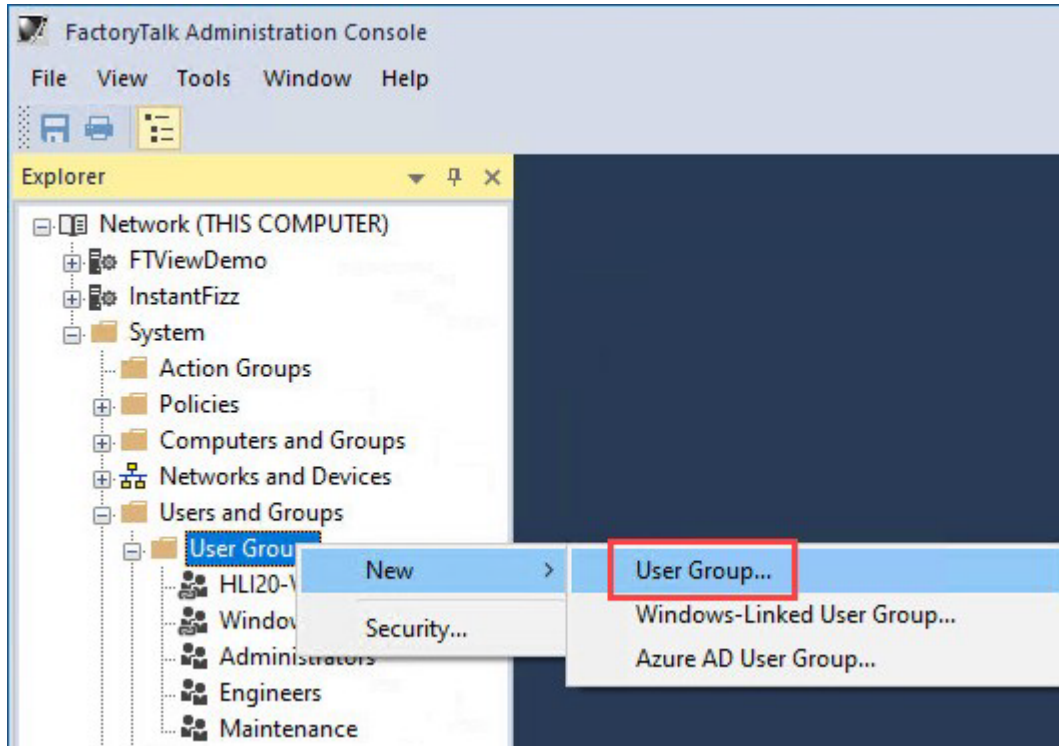
3. Select **OK**.

## Create a FactoryTalk user group

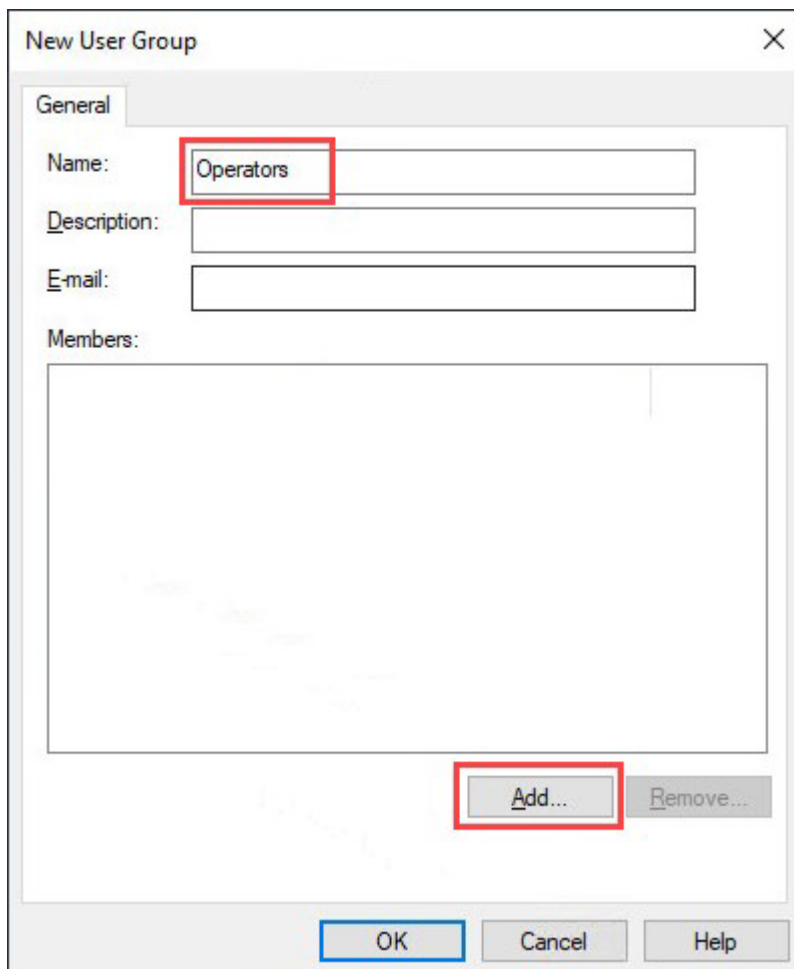
Create FactoryTalk user groups to hold Windows-link user groups, Azure AD user groups, Windows-linked users, and FactoryTalk users. The operations of adding any user group or user to a FactoryTalk user group are the same. This example uses adding a Windows-linked user group to demonstrate the steps.

## To create a FactoryTalk user group

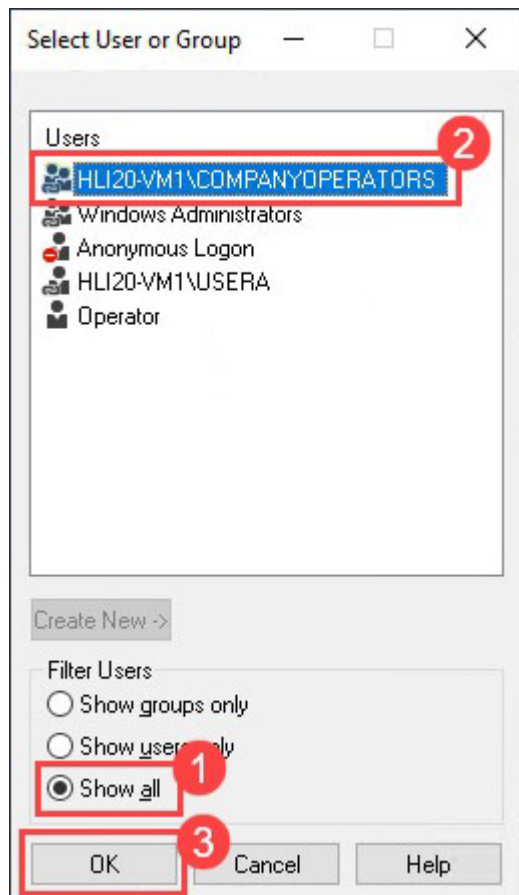
1. In FactoryTalk Administration Console, go to **System > User and Groups**, right-click **User Groups**, and then select **New > User Group**.



2. Enter a group name, for example *Operators*, and then select **Add**.



3. Select **Show all**, select the Windows-linked user group, and then select **OK**.



4. In the **New User Group** dialog box, select **OK**.

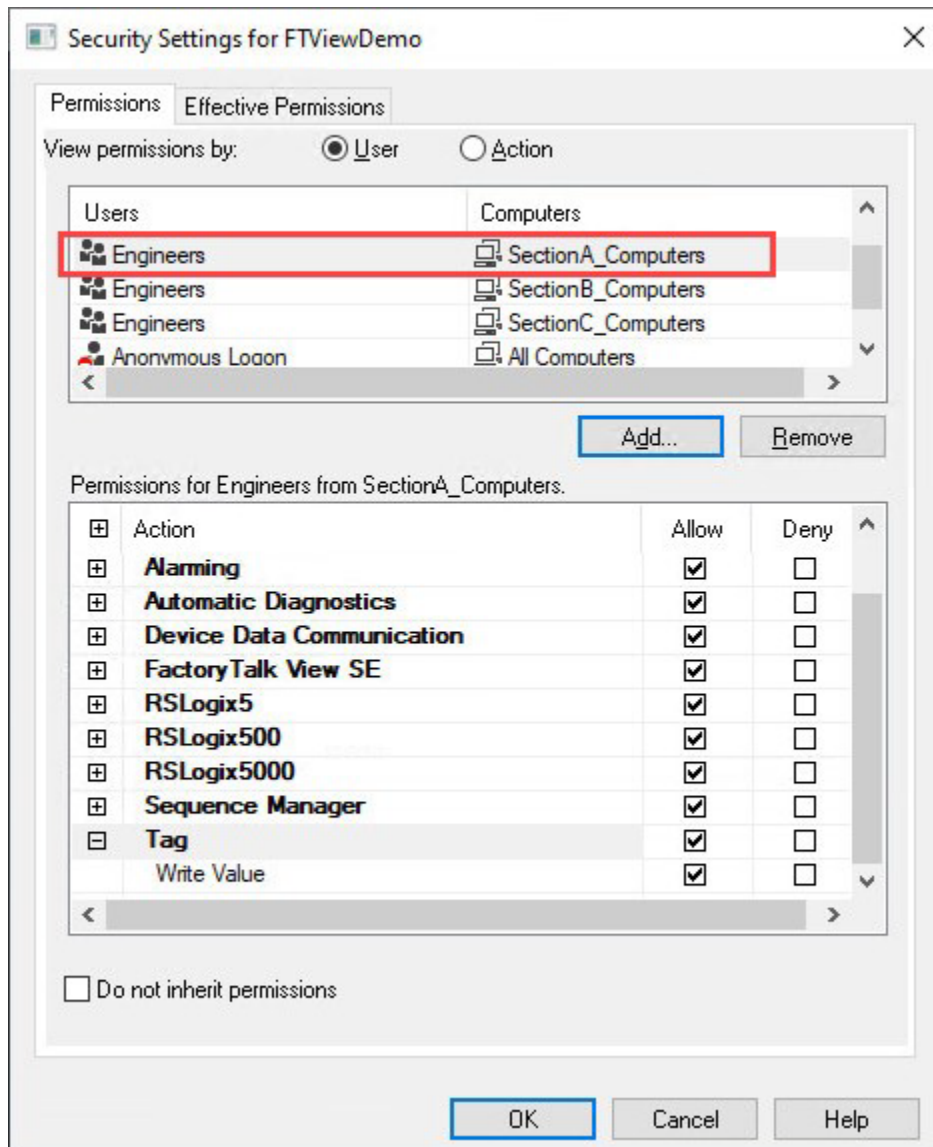
## Line of sight security

FactoryTalk Security allows security to differ based on computer location. Computer accounts are used to authenticate, and authorize or deny access to actions from individual computers in the FactoryTalk automation system. For example, use computer accounts to ensure that certain operations are performed only from computers that are located within direct view of equipment that is being controlled. This is sometimes referred to as line of sight security.

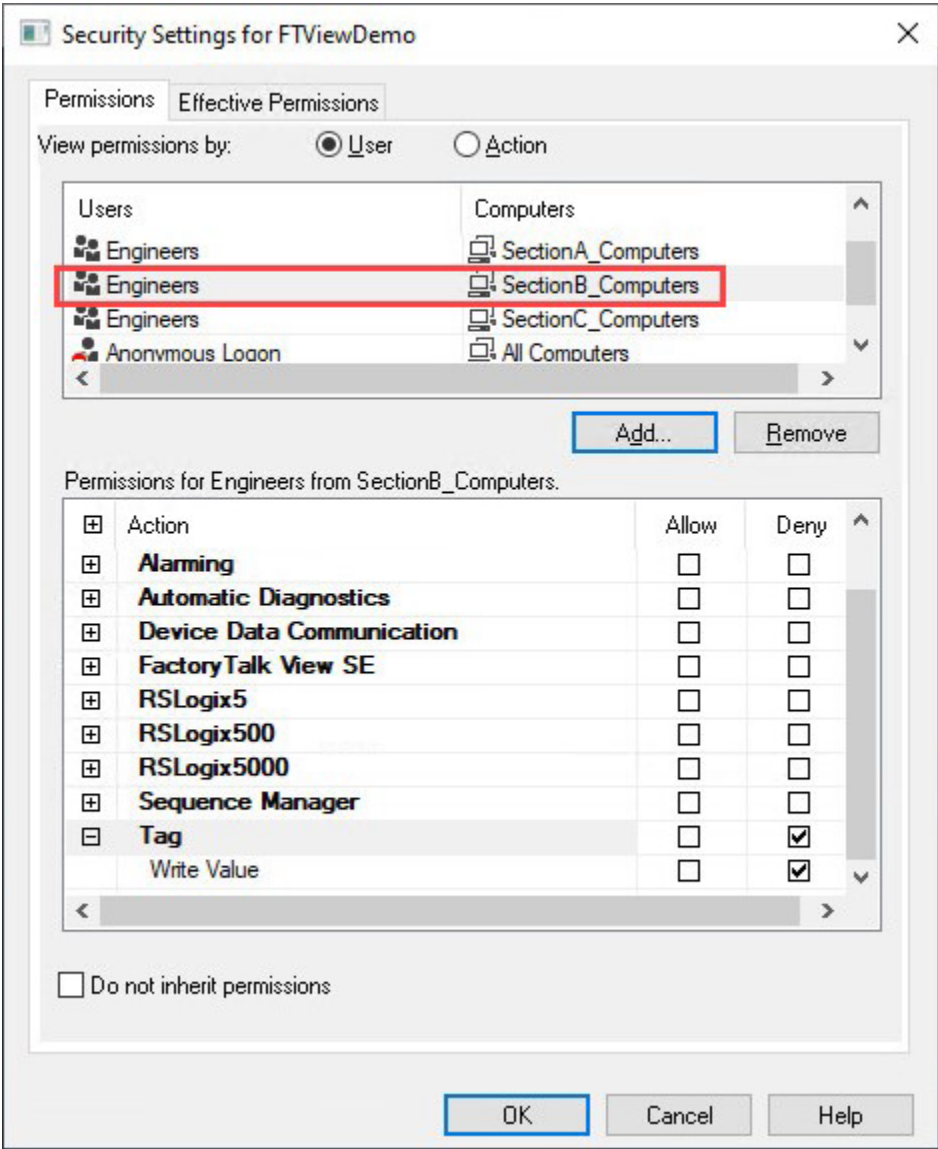
Defining security for a user or group at a specific computer or group of computers allows you to control where they have specific access. We recommend defining security at a group level to simplify long-term management.

For example, a plant has three sections, Section A, Section B, and Section C. You can create a rule that limits users using computers in Section A from performing certain actions with computers in Section B or Section C.

In this example, the Engineers group has a designated section (Section A) and has been selected as the user group and SectionA\_Computers as the location. Because the Engineers group has full access when signed in into Section A, **Allow** is selected for all actions.



Once the Engineers group has been added from the Section B and Section C computers, note that each user grouping has its own item available with which to define different permissions. In this example, the Engineers group cannot write to tags from outside of Section A, so permissions will not be granted for tag writes access.

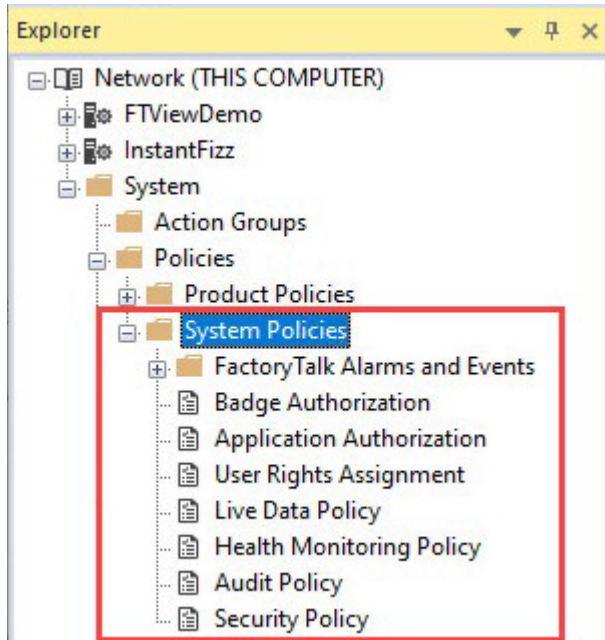


## Configure system policies

System policies are settings that affect the entire FactoryTalk system and all other FactoryTalk-enabled software products that communicate to the FactoryTalk Directory. Policy settings are separate in the network directory and the local directory.



In FactoryTalk Administration Console, navigate to **System > Policies > System Policies** to configure the system policies.



The system policies include the following categories:

- **FactoryTalk Alarms and Events**

Configure these policies if you want to change the default ports for alarm web services, system-wide severity ranges, and severity behaviors of controller status alarms and tracking events. The severity ranges defined here apply to all alarm servers connected to a particular FactoryTalk Directory. You can override the system-wide severity ranges on a per-server basis.

- **Badge Authorization**

Configure this policy if users can sign in to the FactoryTalk system with a badge and you want to add or remove services that request to use the Badge Logon function. The service that requests access to use the Badge Logon function must be trusted by Rockwell Automation.

- **Application Authorization**

Configure this policy if you want to remove any application's access to the FactoryTalk Directory. By default, FactoryTalk-enabled products and services are allowed access to the FactoryTalk Directory when joining the directory. It is highly unlikely that you need to change this policy.

- **User Rights Assignment**

Configure these policies if you want to determine which users are permitted to perform these system-wide actions:

- Backup and restore the FactoryTalk Directory, 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.

- **Live Data Policy**

Configure this policy if you want to change the default communication 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. Change this setting only if necessary, such as if the system is experiencing communication problems and it is necessary to switch to DCOM for troubleshooting purposes.

- **Health Monitoring Policy**

Configure these policies if you want to change the parameters that determine whether a network failure occurred and how long to wait before switching to a standby server in a redundancy pair, such as redundant HMI or FactoryTalk Linx servers. Changing these policies can have unexpected results. The preset default settings typically provide optimal ePciency for most networks.

- **Audit Policy**

Configure these policies if you want to enable or disable audit records for:

- Changes to the system configuration and the control system.
- Security access failures and successes.

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

- **Security Policy**

Configure these policies if you want to define general rules for implementing security across all FactoryTalk products in the system. Define policies for Windows-linked accounts in Windows.

- Account Policy Settings: Specifies how the FactoryTalk system manages policies for user, computer, and group accounts. These policies do not apply to Windows-linked accounts.
- Badge Policy Settings: Specifies how FactoryTalk user accounts can sign in using a Radio-Frequency-Identification (RFID) badge.
- Computer Policy Settings: Specifies how computer accounts in the FactoryTalk Network Directory can use remote access.
- Directory Protection Policy Settings: Specifies client computer accounts usage of the FactoryTalk Network Directory.
- DNS Alias Name: Specifies a DNS alias name associated with a computer hosting the FactoryTalk Directory server.
- Encryption Settings: Specifies the encryption and decryption algorithm used by FactoryTalk products.
- Password Policy Settings: Specifies password requirements for FactoryTalk user accounts. These policies do not apply to Windows-linked accounts.
- Single Sign-On Policy Settings: Specifies whether users can sign in to the system one time, having their credentials shared among multiple FactoryTalk applications, per directory, on a given computer.

With FactoryTalk users, the sign-in information is tracked by the FactoryTalk system. With Window-link users, it passes Windows-linked credentials from the computer a user is working on into the FactoryTalk Directory.

- If that account is valid, the user will get the associated authentication for that account.
- If that account is not valid or has permissions denied, the user will be denied permission.
- If that account doesn't exist, the user will be prompted to sign in to the FactoryTalk system.

Using single sign-on means that a user doesn't have to sign in to every application they use separately. Once signed in, all participating FactoryTalk applications that run in that directory on that computer automatically use those same credentials.

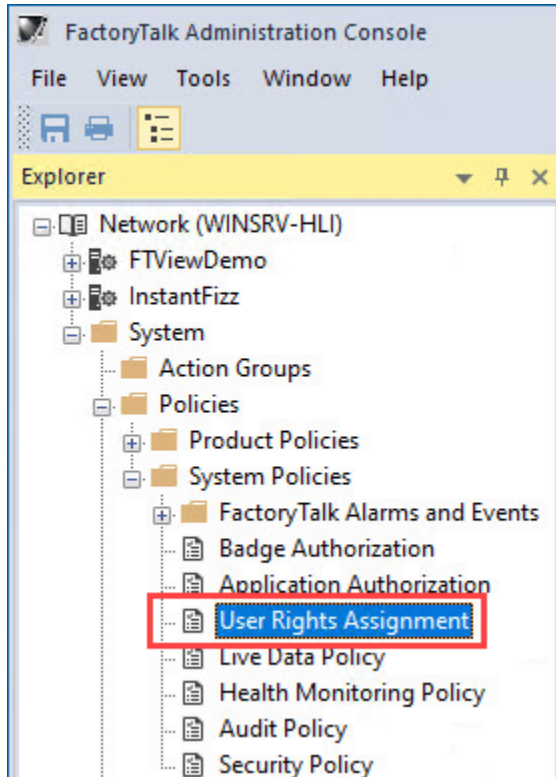
If you want to distinguish individual users' actions by requiring each user to sign in with their own FactoryTalk user accounts, it might be necessary to disable single sign-on. Also, disable single sign-on when signing in to the FactoryTalk system through Remote Desktop Services using the name of the Remote Desktop Connection server computer. Alternatively, change the security policy **Identify terminal server clients using the name of** to allow Remote Desktop Services users to connect using the name of the Remote Desktop Connection client computer.

- System Communication Settings: Specifies the communication settings in the FactoryTalk event system.
- Web Authentication/Authorization Server: Specifies security settings for FactoryTalk-enabled software web applications.

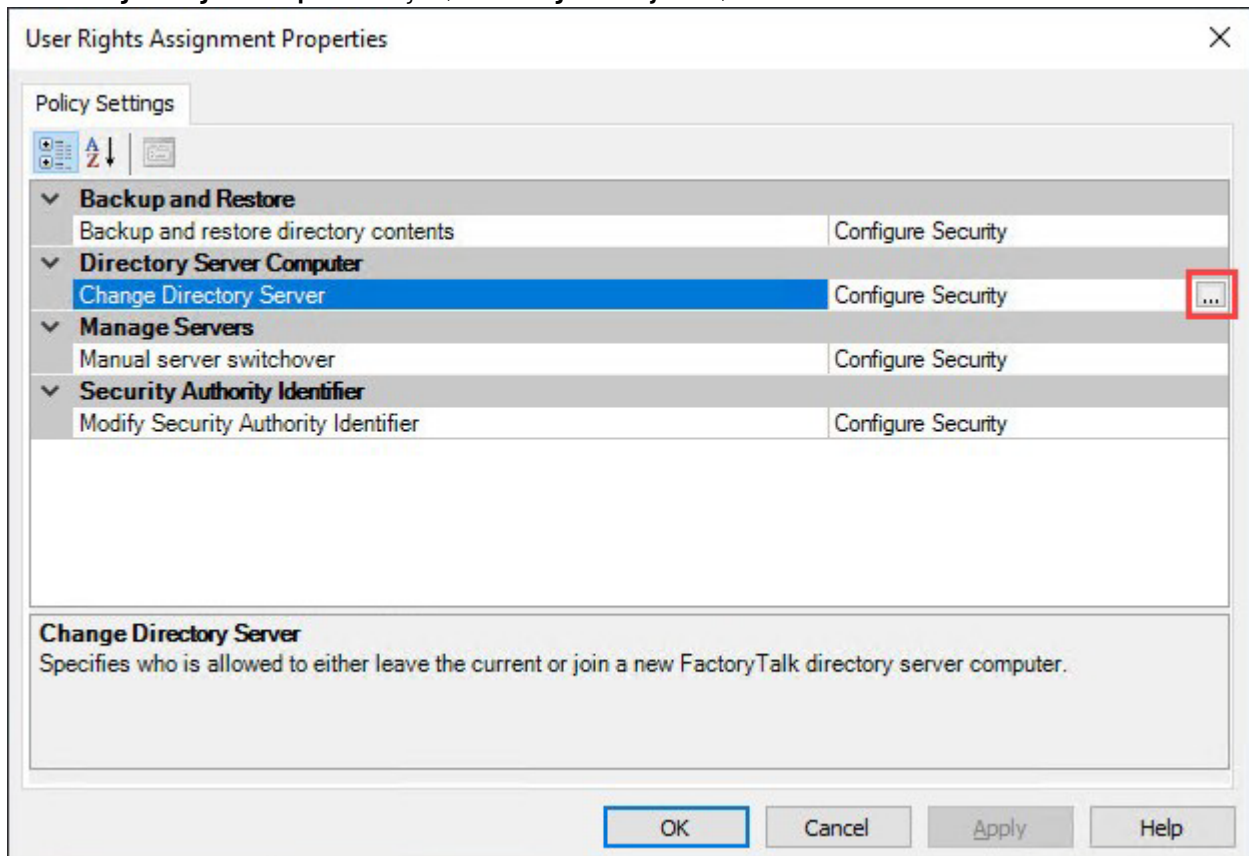
For some of the policy settings, you can specify who is able to perform a certain action. The following example demonstrates how to grant a group permission to the action of changing the directory server.

## To configure the security of an action within system policies

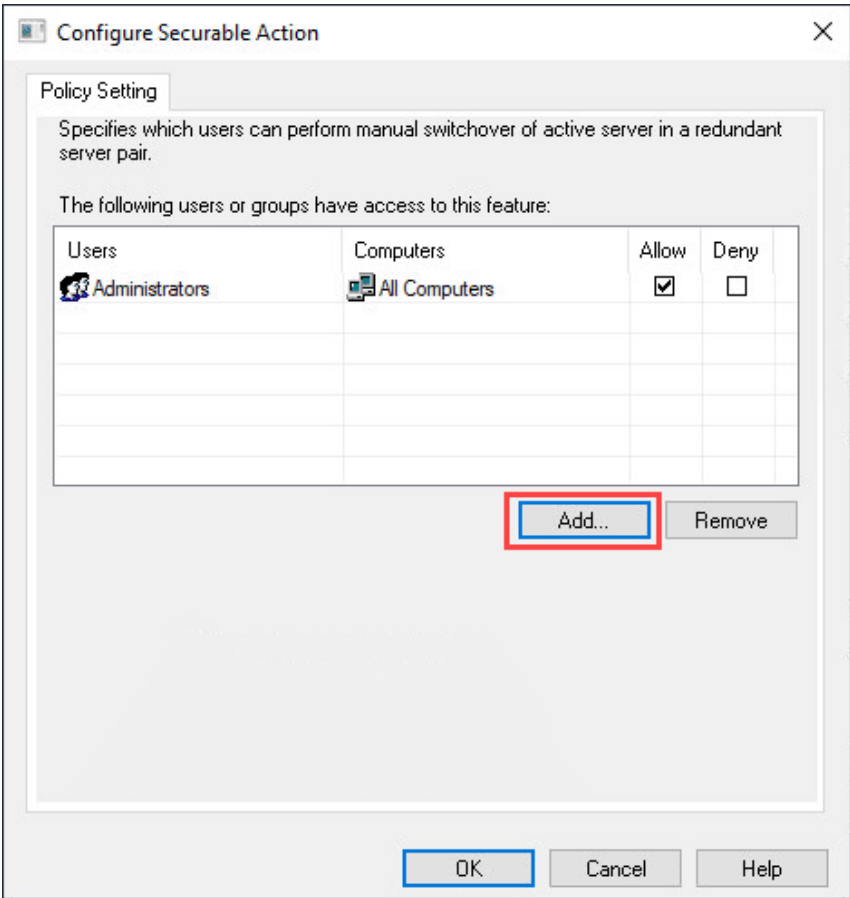
1. In FactoryTalk Administration Console, go to **System > Policies > System Policies**, double-click **User Rights Assignment**.



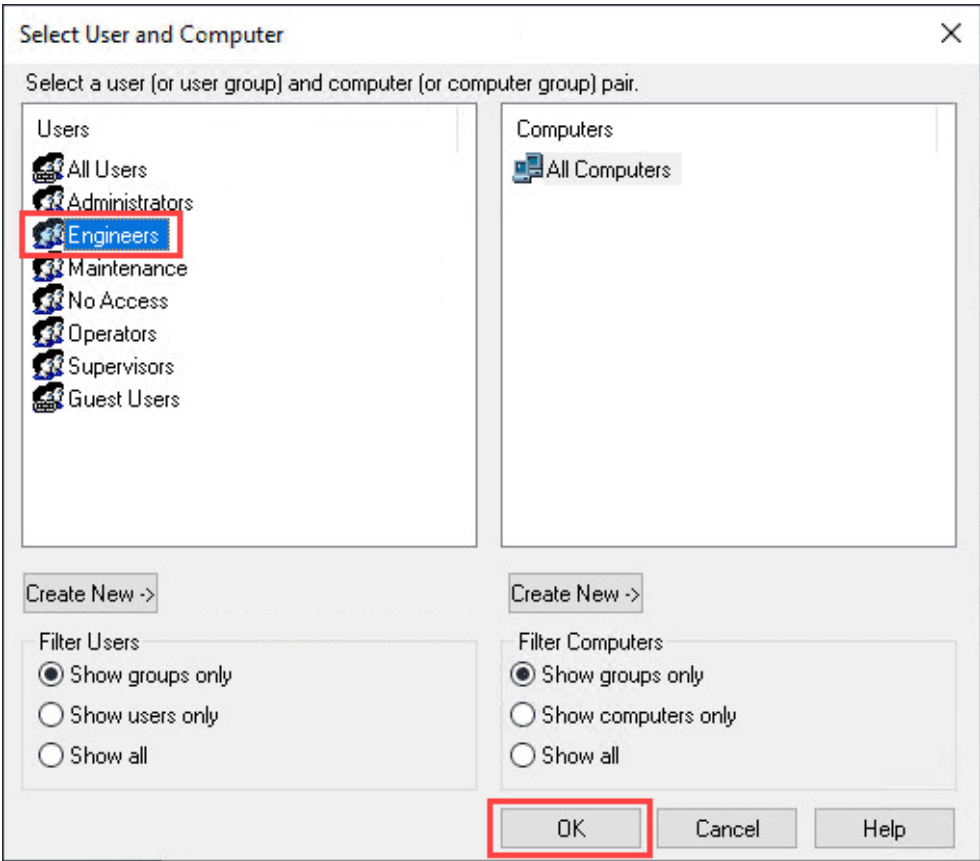
2. In the **User Rights Assignment Properties** dialog box, select **Change Directory Server**, and then select the browser button.



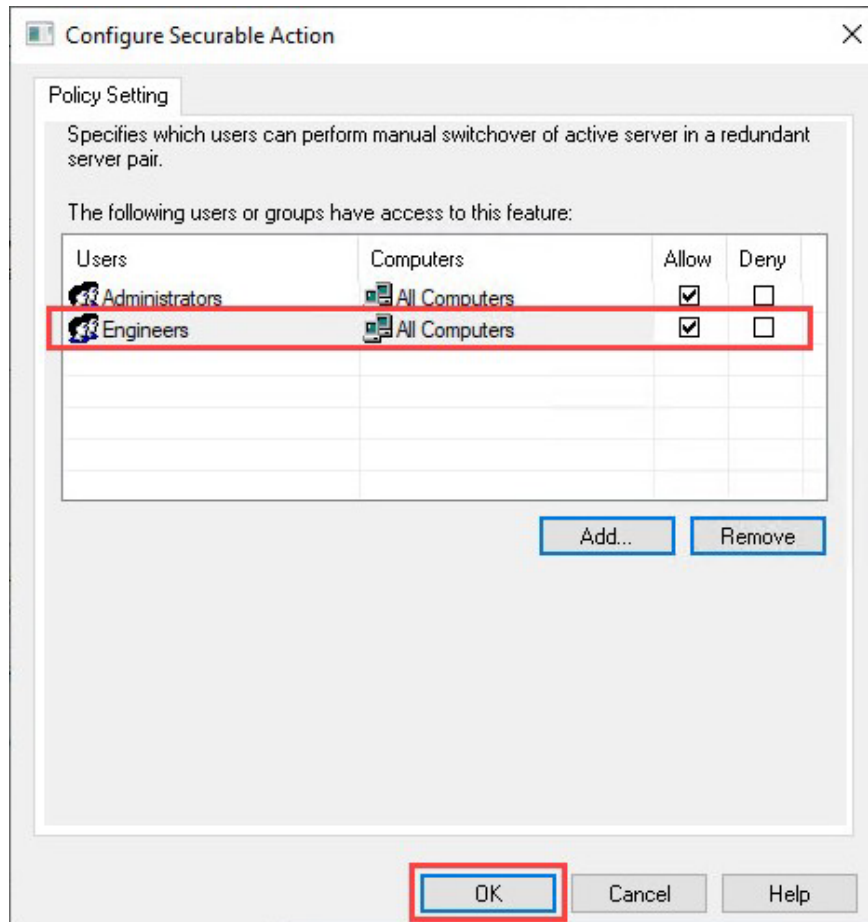
3. In the **Configure Securable Action** dialog box, select **Add**.



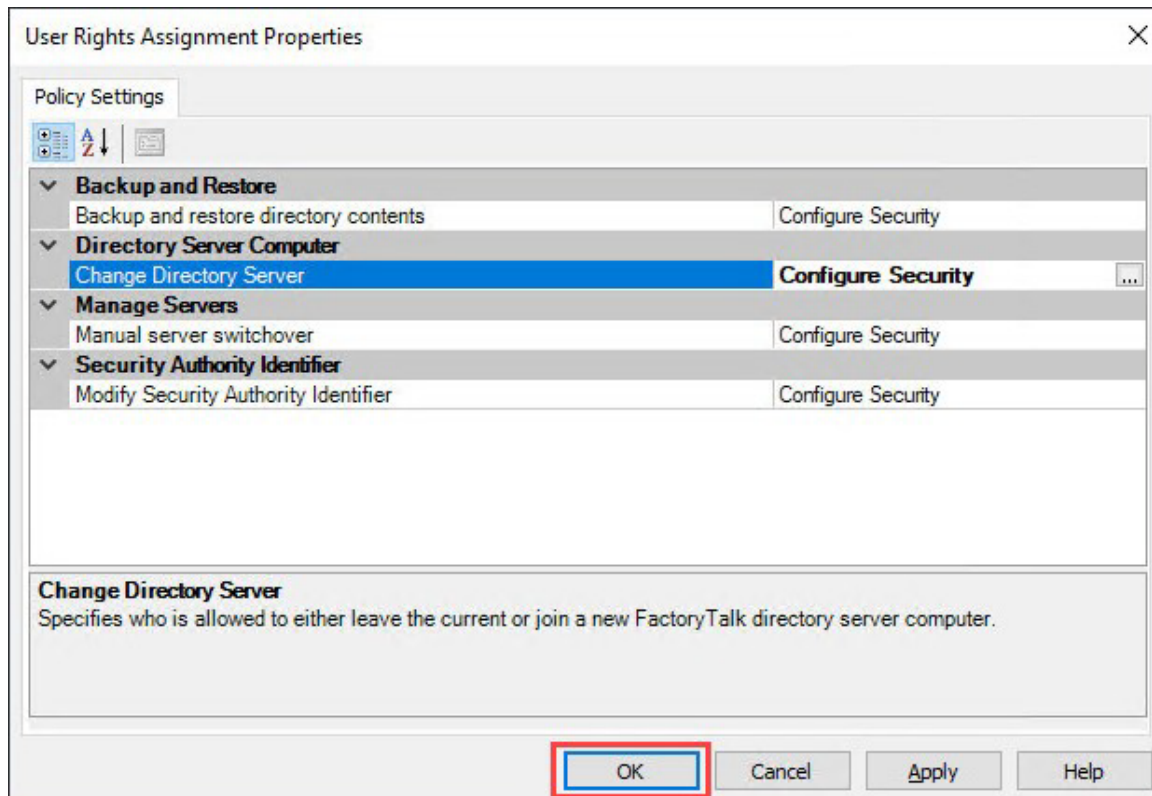
4. Select a group from the list, for example *Engineers*, and then select **OK**.



5. Select **OK**.



6. Select **OK**.



## Configure product policies

Product policies are a collection of securable features that govern the behavior of specific FactoryTalk-enabled products in the system. To help prevent users from making unwanted changes, restrict user access to individual product features. Only users with the required level of access can use the product features once secured.

A product policy applies to only one product. Configuring a user access to one product feature doesn't impact access to other products' same or similar features.

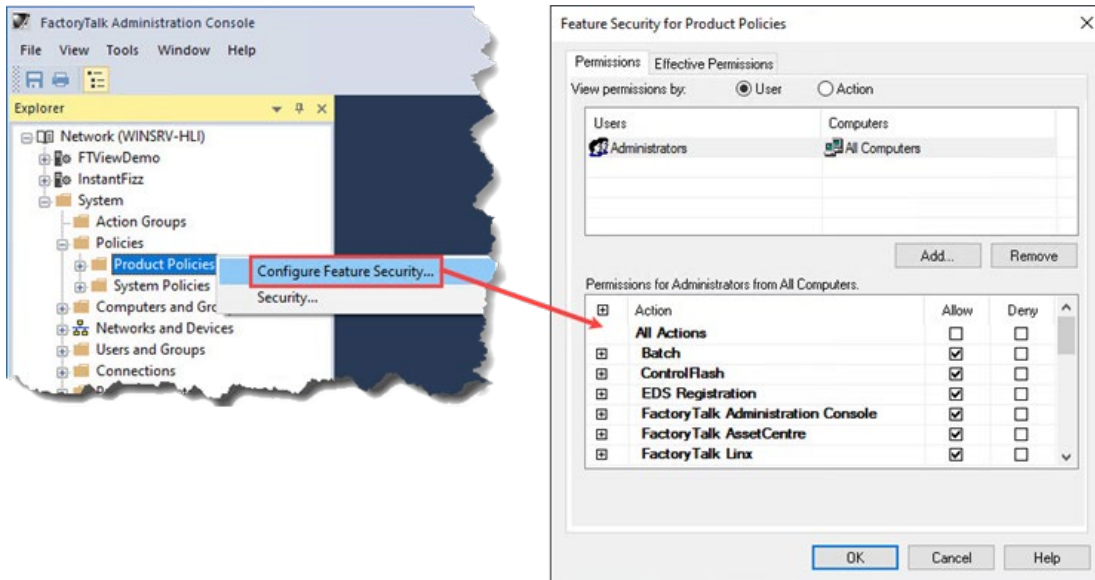
If you are not using a product, you don't need to configure product policies for it. However, if you are using a product, certain product policies will impact the operation of your system depending on what your goals are. For example, configuring the **Controller: Secure** policy restricts which users can secure a controller project.

Specific use cases for types of policies to configure are shown in later chapters.

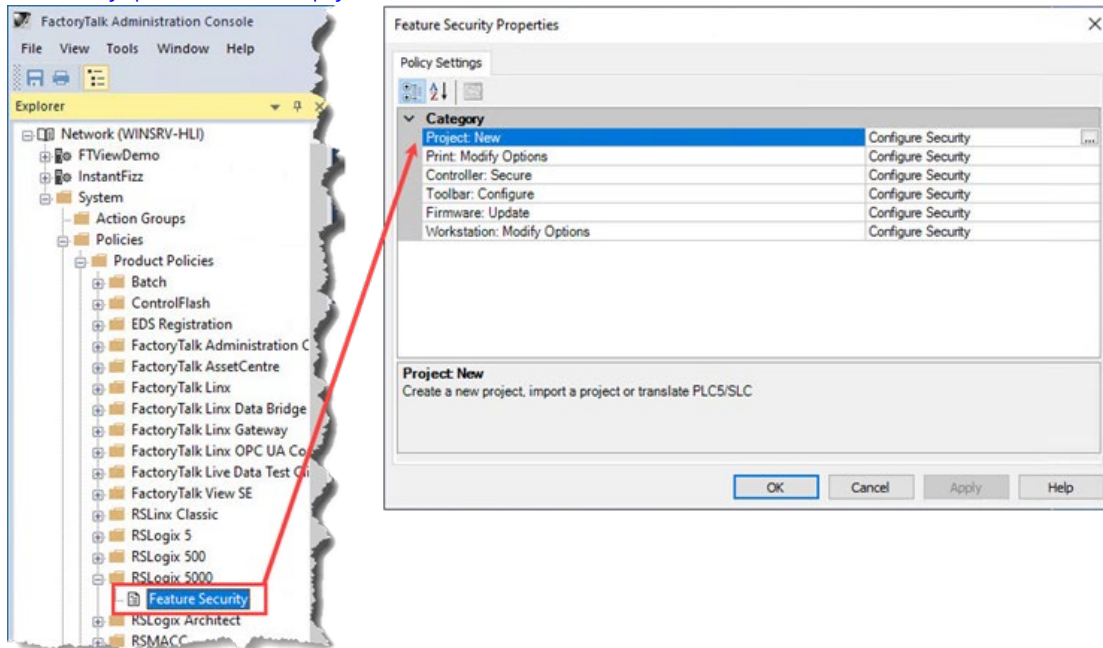
You can configure product policy security at two hierarchy levels – secure multiple products' features and secure a single product's features. The only difference between them is that the former lets you configure security settings for many software applications on a feature-by-feature basis in one dialog box, while the latter lets you configure security settings for a specific software application in one dialog box.

- [Secure multiple products' features on page 35](#)

Changes made at this level are then inherited by all sublevels.



- [Secure a single product's features on page 36](#)



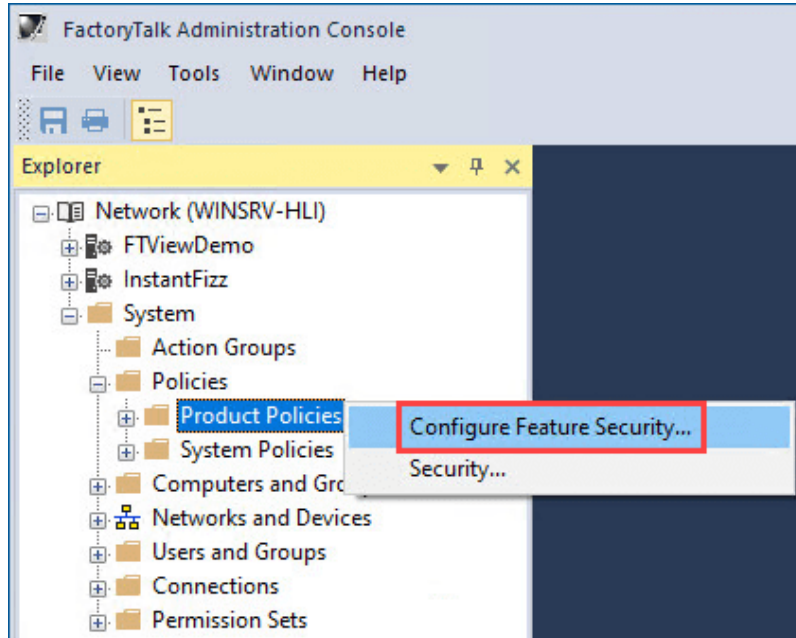


## Secure multiple products' features

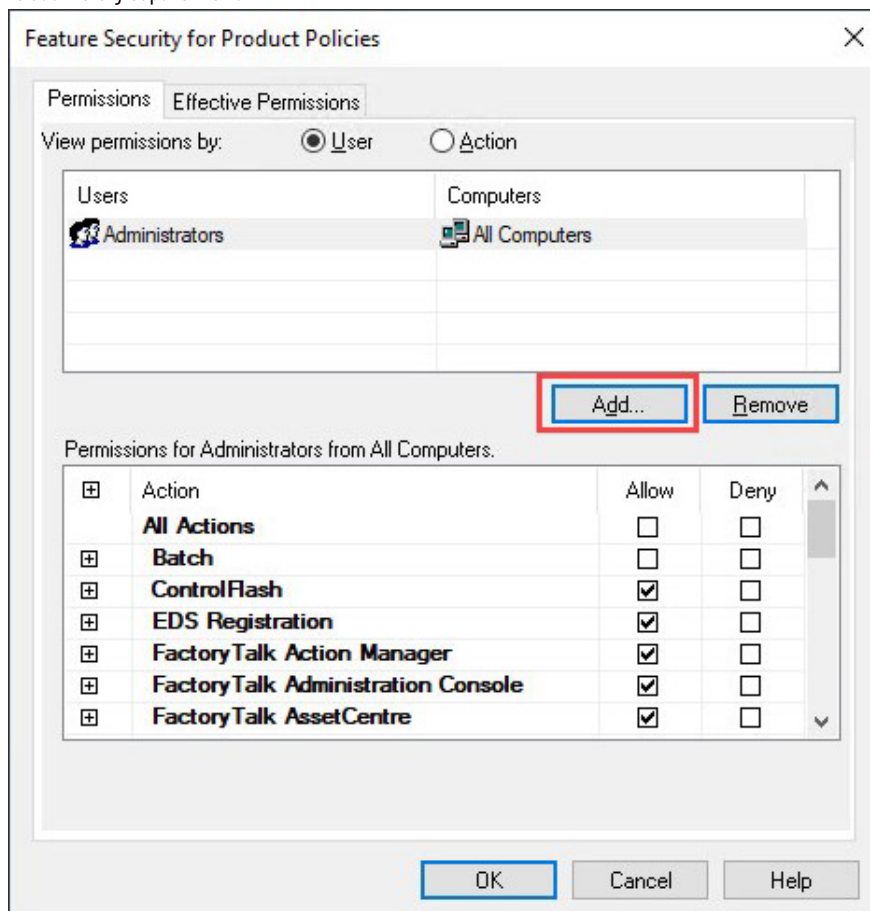
To configure security for multiple products and features at once, use the **Feature Security for Product Policies** dialog box, which contains all the feature security options for all the products.

### To secure multiple products' features

1. In FactoryTalk Administration Console, go to **System > Policies**, right-click **Product Policies**, and then select **Configure Feature Security**.

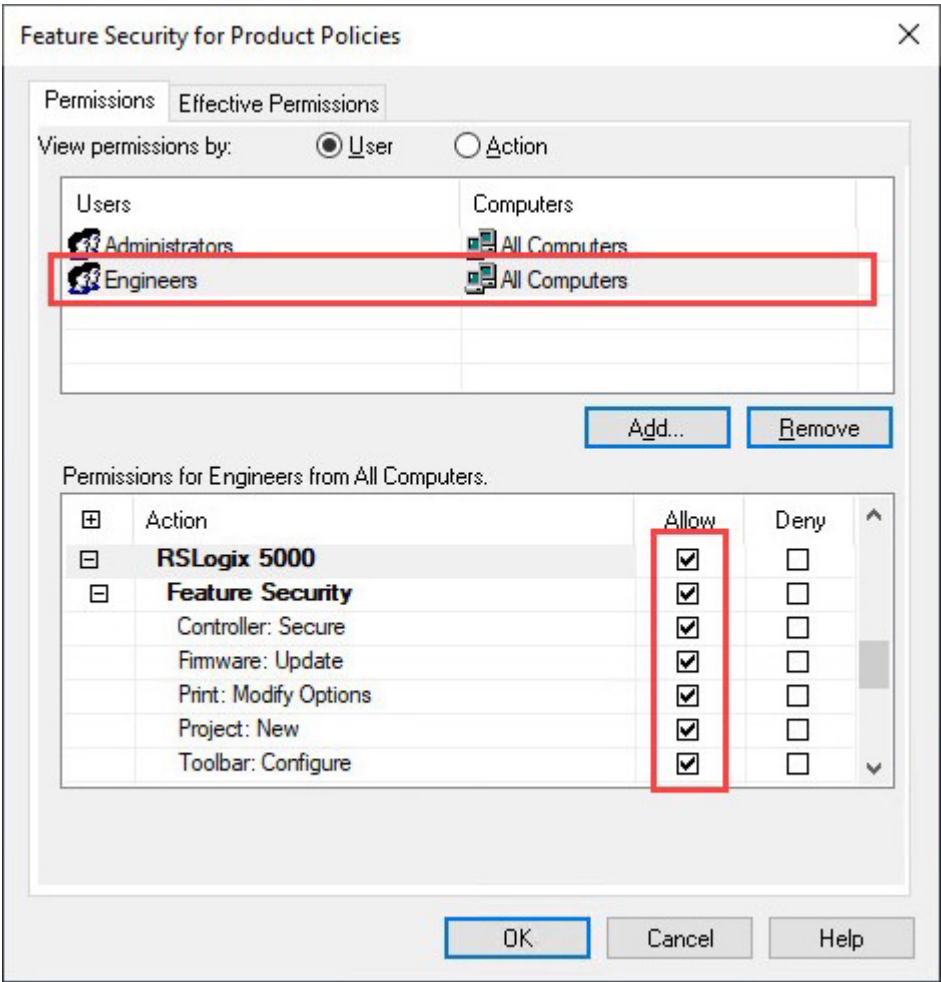


2. In the **Feature Security for Product Policies** dialog box, select the **Permissions** tab, and then select a group in the upper portion of the dialog box or select **Add** to add more groups to the list.

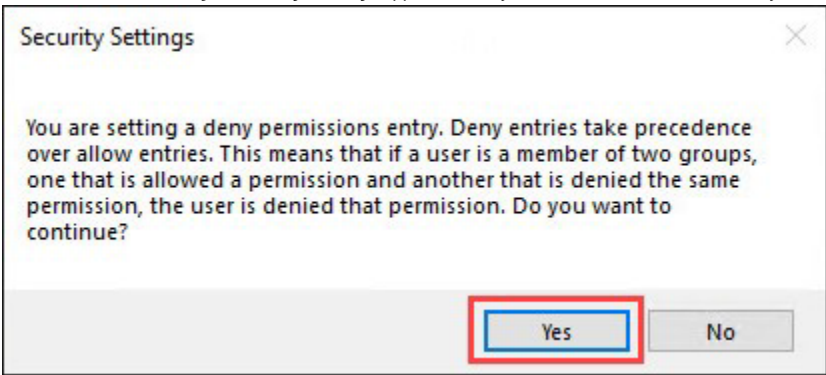


- 3. Select the user group that you want to configure security for, and then expand the choices until you see the feature security list for the desired software application.
- 4. Select the appropriate **Allow**, **Deny**, or unselected option, and then select **OK**.

In this example, the RSLogix 5000® 5000 features are allowed for the Engineers group.



- 5. Select **OK**.
- If an action is set to **Deny**, a warning message appears when you select **OK**. Select **Yes** to verify the choice.



## Secure a single product's features

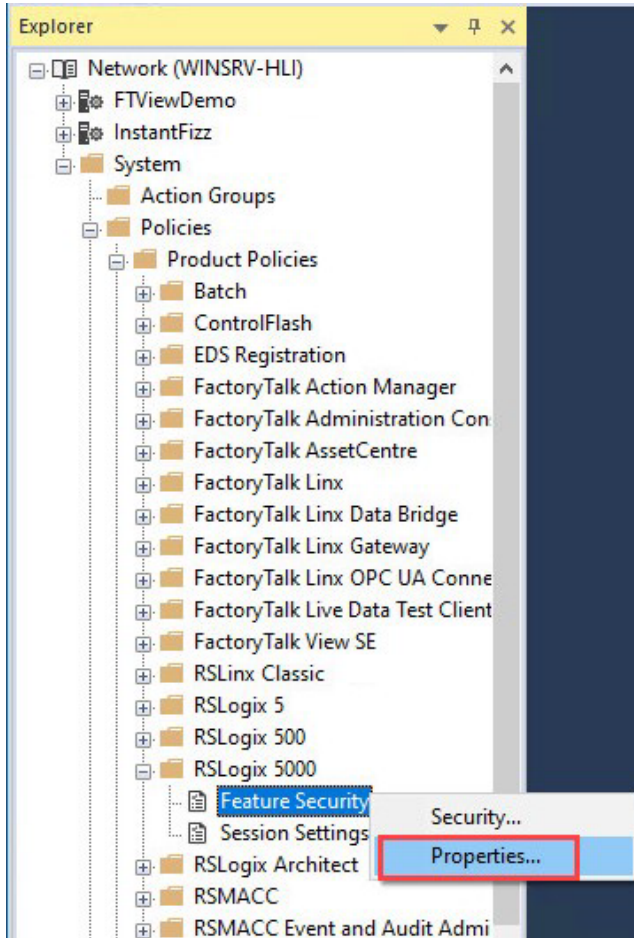
To configure security for features of a specific product, use the **Feature Security Properties** dialog box, which contains the feature security options for that product.

This example shows how to configure feature security for RSLogix 5000® or Studio 5000 Logix Designer.

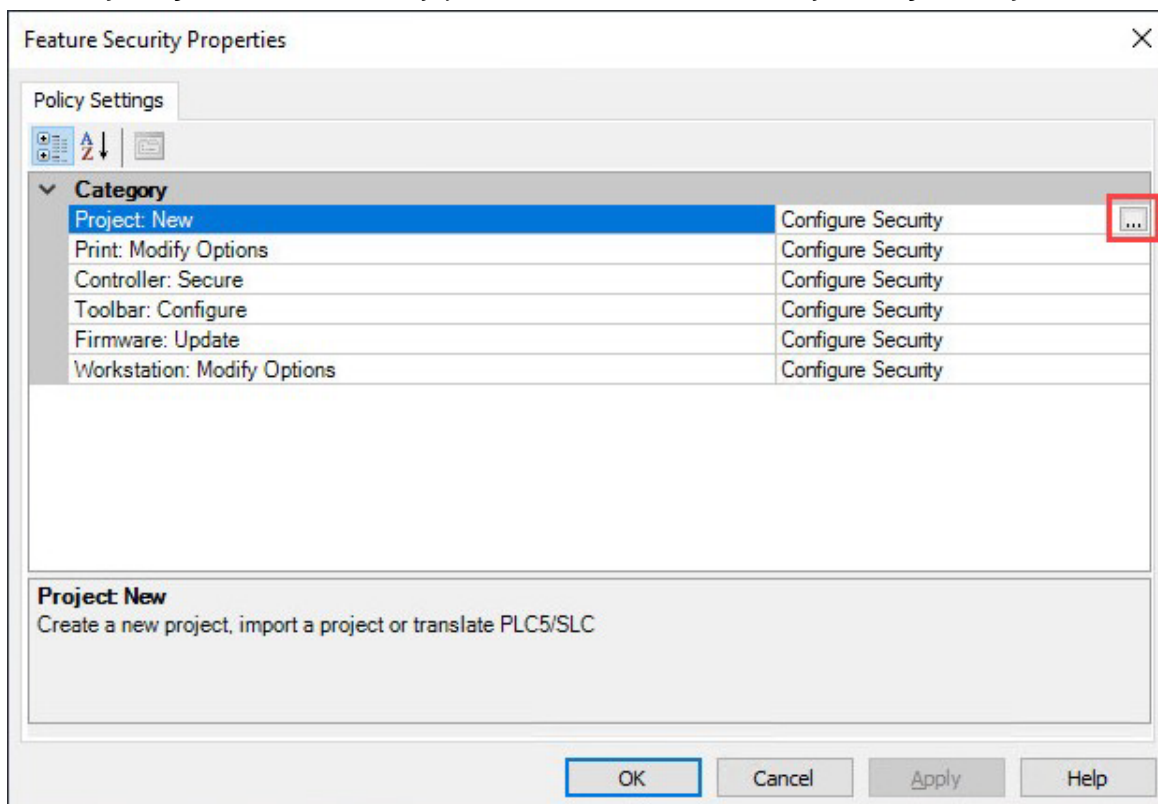


## To secure a single product's features

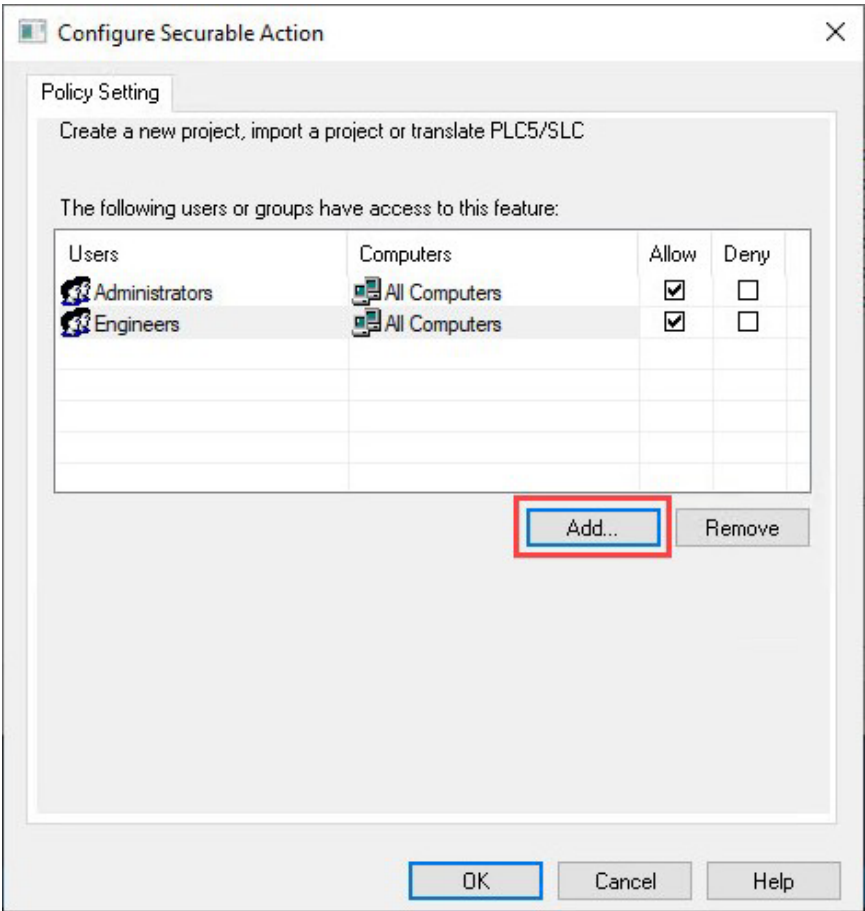
1. In FactoryTalk Administration Console, go to **System > Policies > Product Policies > RSLogix 5000**, right-click **Feature Security**, and then select **Properties**.



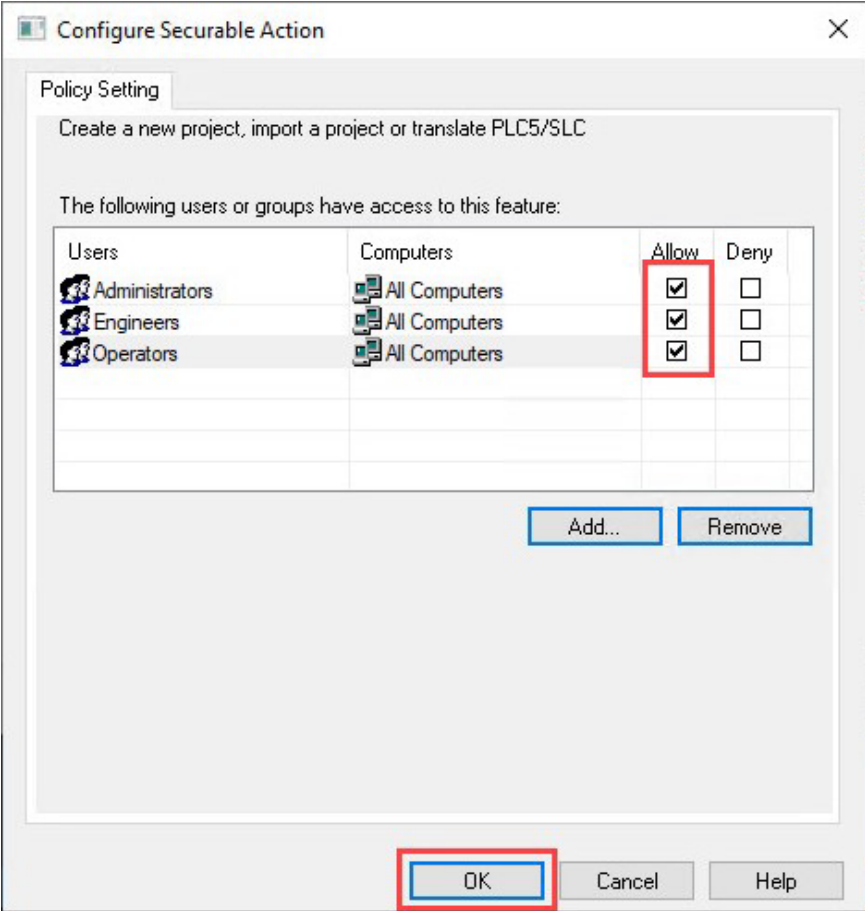
2. On the **Policy Settings** tab, select the desired category, and then select the browse button to the right of **Configure Security**.



3. In the **Configure Securable Action** dialog box, if the desired group is not listed, select **Add**.



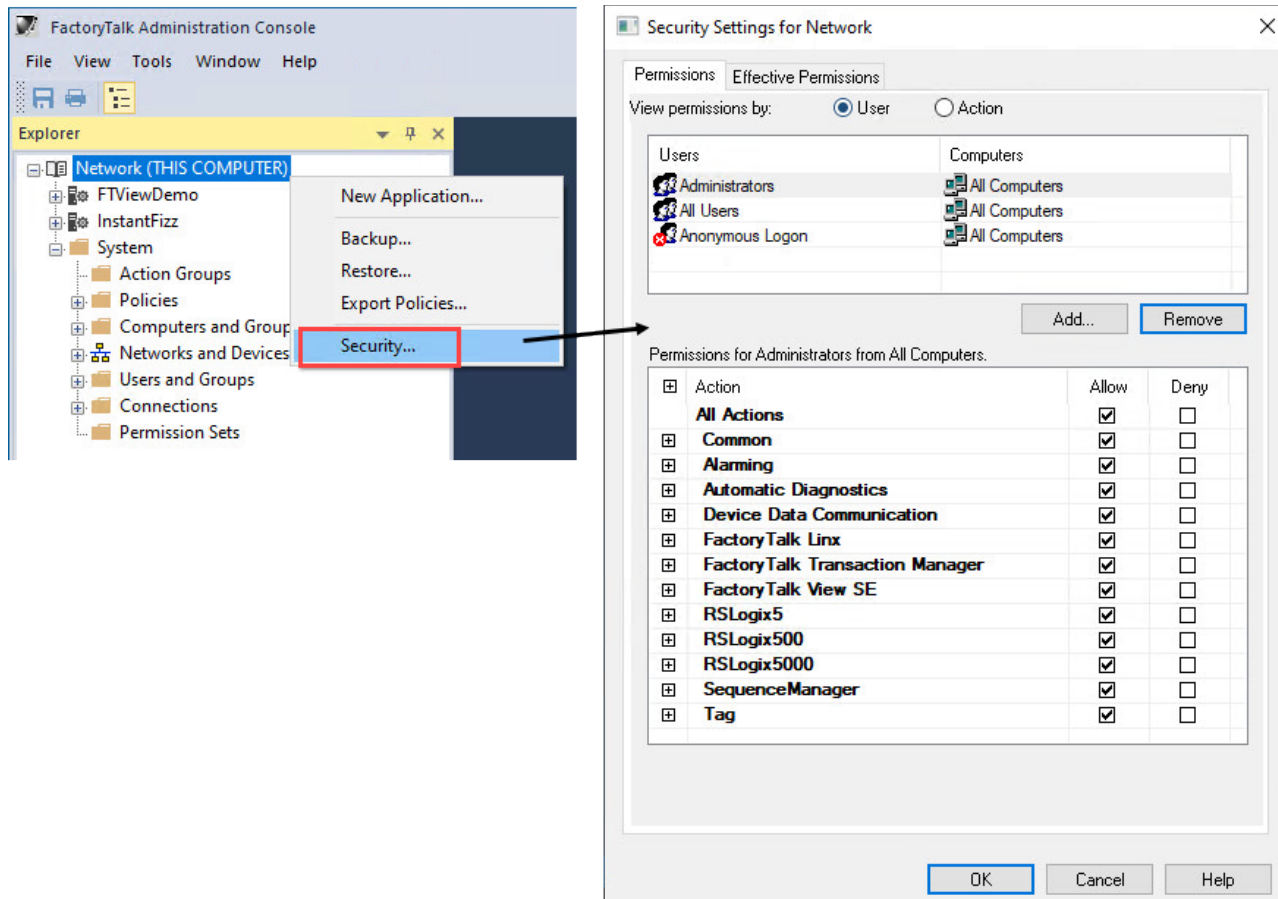
4. Select the user group that you want to configure security for, select the appropriate **Allow**, **Deny**, or unselected option, and then select **OK**.



## Configure securable actions

By configuring securable actions, you secure the resources in the FactoryTalk system and specify which users can perform what actions on that resource and from what computers. This helps ensure that only authorized personnel can perform approved actions from appropriate locations.

To configure securable actions, in FactoryTalk Administration Console, right-click a resource (for example, the directory root, an application, an area, and so on), and then set permissions to allow or deny user or groups the ability to perform certain actions.



Securable actions vary depending on the selected resource. The following list shows the securable actions from the directory root. For more details about those actions, see the documentation for your FactoryTalk products.

- **Common**

Common actions manage how a user interacts with the FactoryTalk system that is every layer of the hierarchical structure of the tree in FactoryTalk Administration Console.

Configure these common actions if you want to change the standard permissions that are not product or function specific. These common actions are usually used together with product-specific actions.

Action	Description
Configure Security	Controls whether a user or user group can change the security permissions for a resource.
Create Children	Controls whether a user or user group can create a new, related resource beneath an existing resource.
Delete	Controls whether a user or user group can delete any item within a resource.
Execute	Controls whether a user or user group can perform an executable action.
List Children	Controls whether a user or user group can view the children of a resource.
Read	Controls whether a user or user group can see a resource in the Explorer.
Write	Controls whether a user or user group can write to a resource.

- **Alarming**

Configure these actions if you want to allow or deny certain users the ability to perform alarm-specific tasks:

- Acknowledge alarms
- Enable or disable alarms
- Reset latched alarms
- Suppress or unsuppress alarms
- Shelve or unshelve alarms

- **Automatic Diagnostics**

Configure this action if you want to allow or deny certain users the ability to suppress or unsuppress diagnostic events. This action applies to when you use FactoryTalk Alarms and Events to display diagnostic events collected by Rockwell Automation controllers that support the Automatic Diagnostics feature. Such controllers are Compact GuardLogix® 5380, CompactLogix™ 5380, CompactLogix 5480, ControlLogix® 5580, and GuardLogix® 5580 controllers, and the firmware revision must be 33 or later.

- **Device Data Communication**

Configure this action if you want to allow or deny certain users the ability to inhibit or enable data communication with a Logix 5000™ controller. This action applies to when you use RSLinx® Enterprise v5.90.00 and later (renamed FactoryTalk Linx with version 6.00.00) only.

- **FactoryTalk Linx**

Configure this action if you want to allow or deny certain users the ability to browse devices, such as via FactoryTalk Linx Network Browser or Communication Setup editor.

- **FactoryTalk Transaction Manager**

Configure this action if you want to allow or deny certain users the ability to start a configuration, stop a configuration, or change a running configuration.

- **FactoryTalk View SE**

Configure these actions if you want to allow or deny certain users the ability to modify recipes in the RecipePro+ editor, or delete XY Plot or TrendPro templates. For more information, see [Product policies and securable actions of FactoryTalk View SE on page 123](#).

- **RSLogix5**

Configure these actions if you want to allow or deny certain users the ability to perform specific tasks on specific projects when using RSLogix 5. For more information, see *Getting Results with RSLogix 5*, [LG5-GR002](#).

- **RSLogix500**

Configure these actions if you want to allow or deny certain users the ability to perform specific tasks on specific projects when using RSLogix 500.

- **RSLogix5000**

Configure these actions if you want to allow or deny certain users the ability to perform specific tasks on specific projects when using Studio 5000 Logix Designer (previously known as RSLogix 5000). For more information, see [Product policies and securable actions of Studio 5000 Logix Designer on page 118](#).

- **SequenceManager**

Configure these actions if you want to allow or deny certain users the ability to run sequences and interact with sequencing parameters and step tags in the Logix family of controllers.

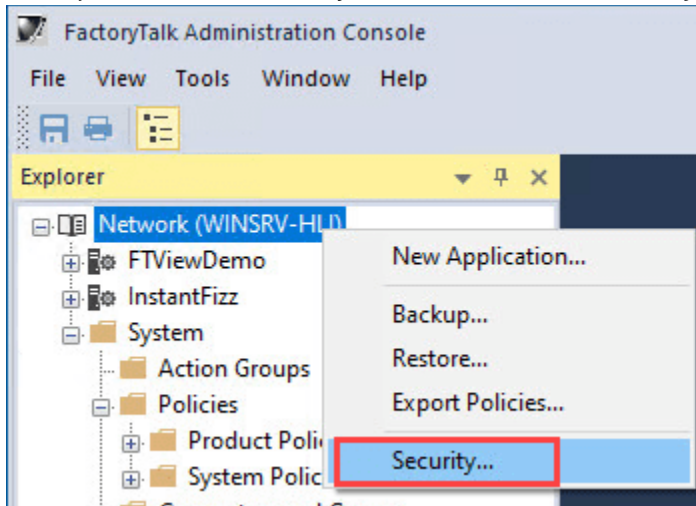
- **Tag**

Configure this action if you want to allow or deny certain users the ability to write to tags in data servers. This action applies to all software products that attempt to write to the tag on that data server.

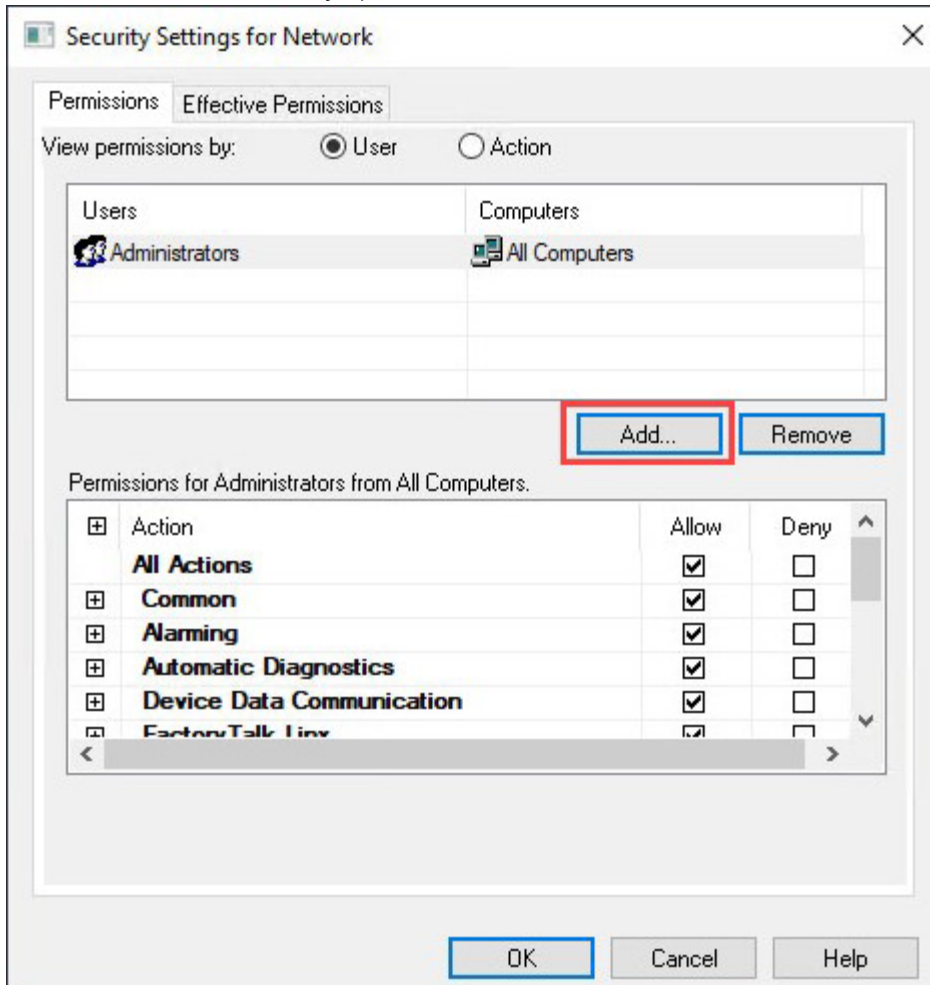
The following steps demonstrate how to grant a new user permission to all actions.

### To grant a new user permission to all actions

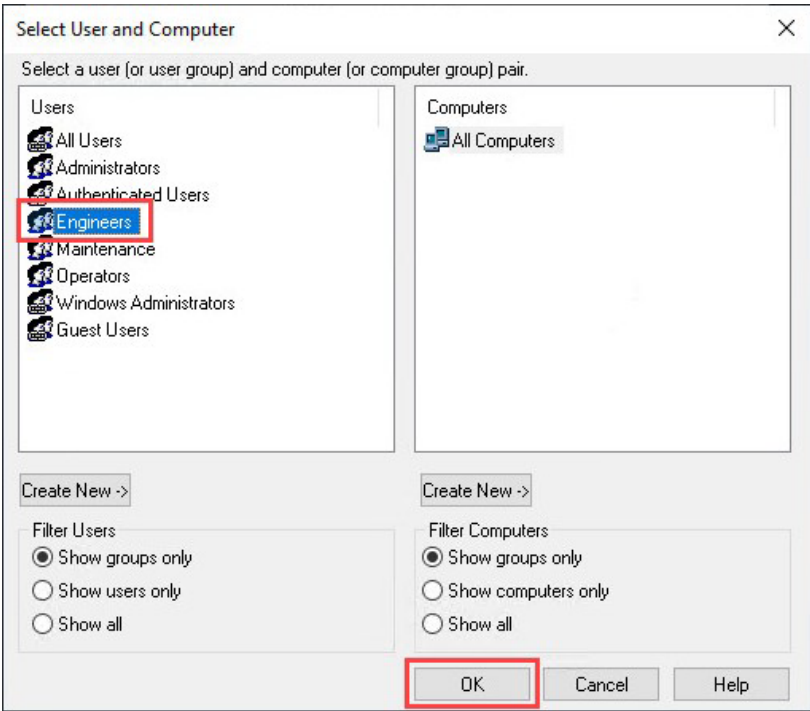
1. In FactoryTalk Administration Console, right-click **Network**, and then select **Security**.



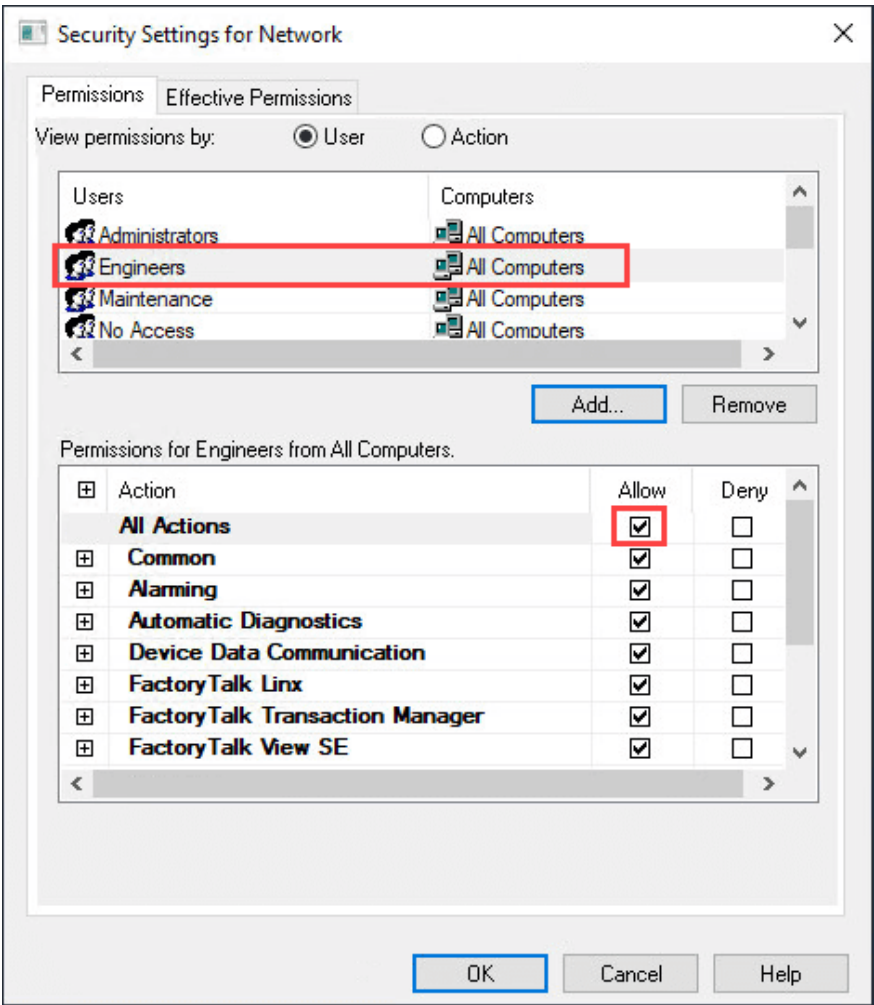
2. On the **Permissions** tab, if the desired group is not listed, select **Add**.



3. Select the desired group, and then select **OK**.



4. In the **Security Settings for Network** dialog box, select the group, and then specify what actions that group can perform. In this example, all actions are set to Allow for the Engineers group.



5. Select **OK**.

## Harden the FactoryTalk system

When performing a new installation of FactoryTalk Services Platform, you have the option to choose the standard directory type where security is open by default or the secure directory type where some of the security changes described in the following have already been applied during installation. However, when performing an upgrade, the option is not presented during the installation.

If security is open, all users who are signed in 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 administrative control to the directory. Because the network directory and local directory are separate, secure them separately.

To harden your FactoryTalk system, perform these key tasks:

- Create a FactoryTalk or Windows-linked user with administrator-level access.
- Remove the All Users Group.
- Remove the default User Groups.

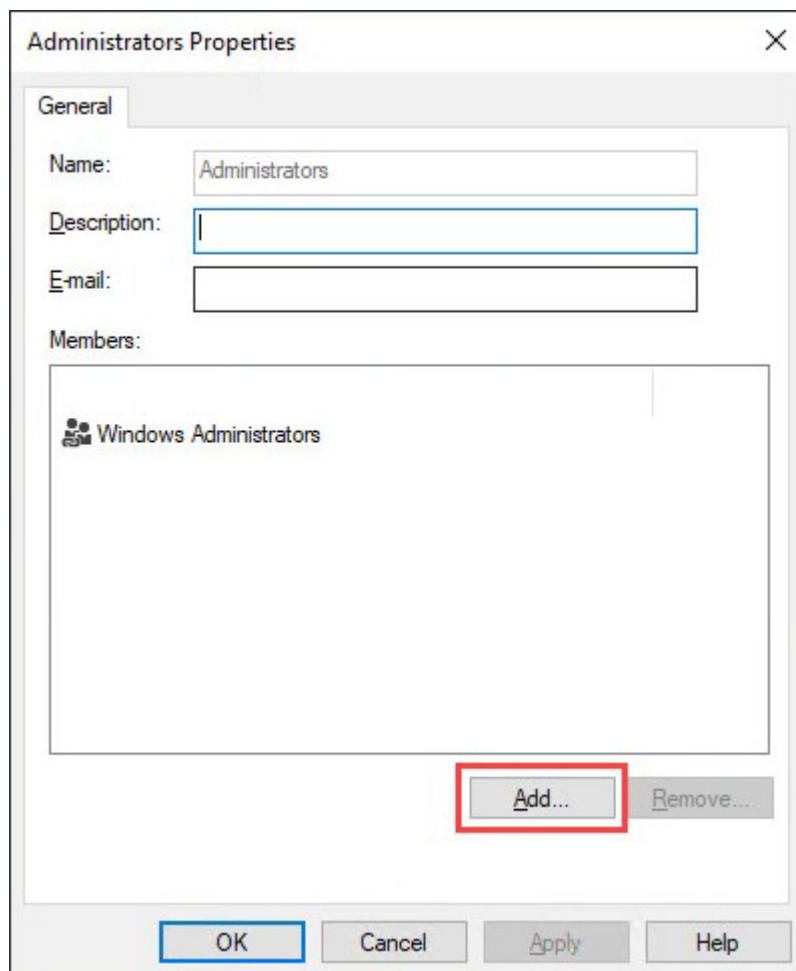
For specific steps on achieving IEC 62443-4-2:2019 certification, see *Security Configuration User Manual* listed in [Additional Resources on page 4](#).

## Grant a user group or user with administrator-level access

To ensure that you always have administrative access to the FactoryTalk Directory, create one or more Windows-linked user groups and accounts, Azure AD user groups, or FactoryTalk user groups and accounts, and then add them to the Administrators group. For instructions on how to add different types of user groups or users, see [User group and user configuration on page 14](#). The following instruction assumes that you have already created user groups or users in your system.

### To grant a user group or user with administrator-level access

1. In FactoryTalk Administration Console, go to **System > Users and Groups > User Groups**, and then double-click the **Administrators** group.
2. In the **Administrators Properties** dialog box, select **Add**.





3. In the **Select User or Group** dialog box, select the user group or user that you want to grant administrator-level access, and then select **OK**.
4. In the **Administrators Properties** dialog box, select **OK**.

## Remove the All Users group

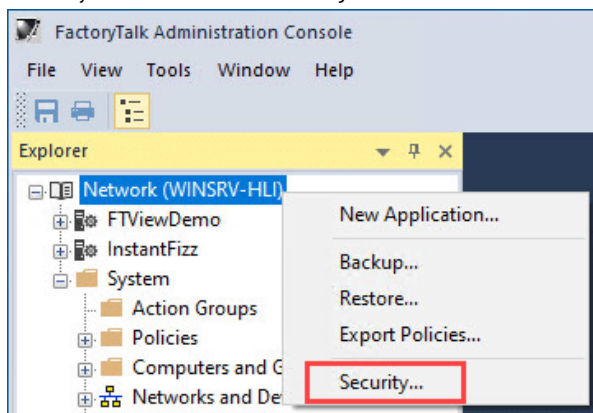
By default, a FactoryTalk Directory creates the All Users group. You must remove the group from the Users list to make sure that the permissions that you assign for specific groups are not inherited from by the All Users group permissions. When you work from the default configuration, the All Users group must be removed from the following locations:

- Directory root
- Policies folder
- Feature Security on the Product Policies folder

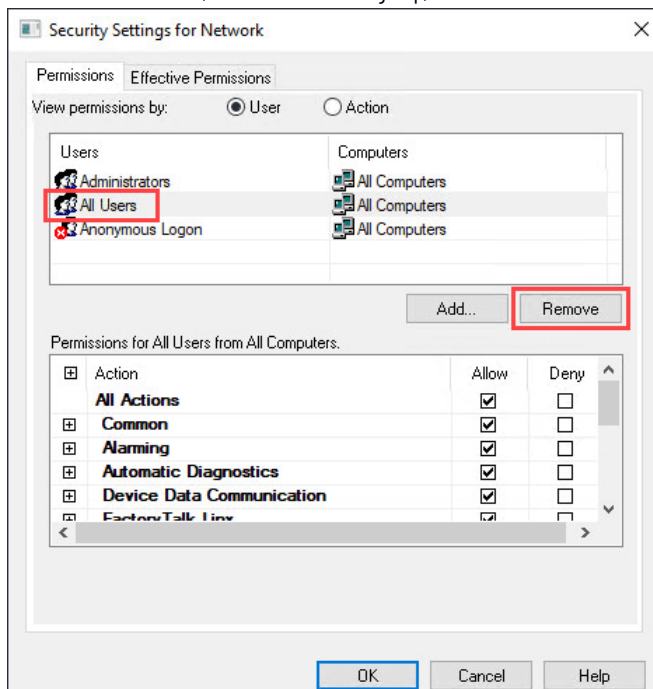
**IMPORTANT:** Before you remove the All Users group, make sure that at least one user is configured with administrative permissions. Without an administrative user, the FactoryTalk Directory can become inaccessible. Failure to create the account results in being locked out of the FactoryTalk Directory once the All Users group is removed.

### To remove the All Users group

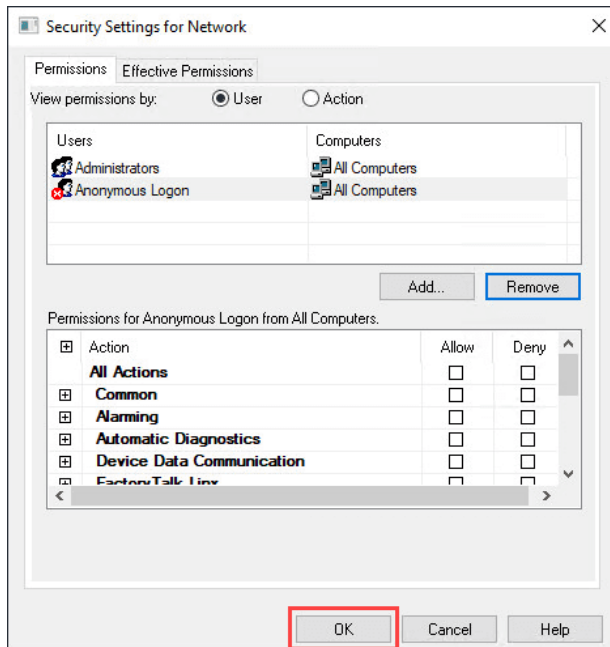
1. In FactoryTalk Administration Console, right-click **Network**, and then select **Security**.



2. On the **Permissions** tab, select the **All Users** group, and then select **Remove**.

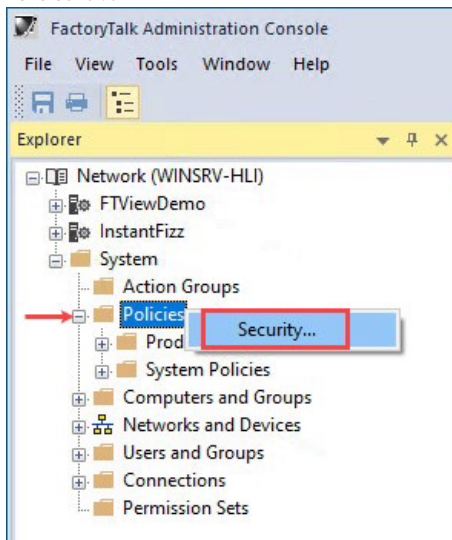




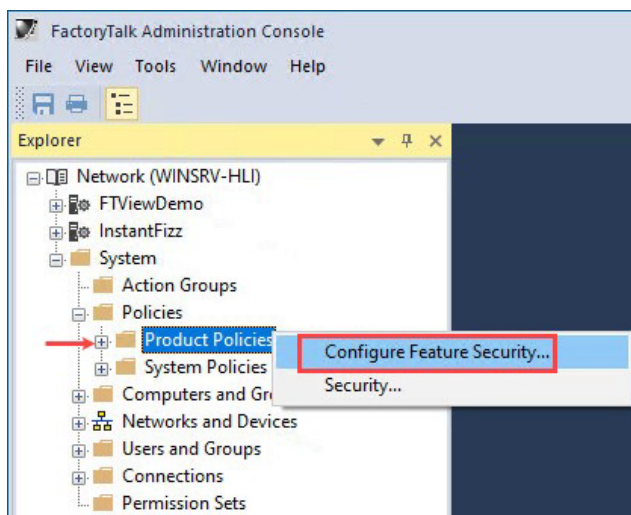
3. Select **OK**.

## 4. Repeat step 2 and step 3 from the following:

- Policies** folder



- Feature Security menu for the **Product Policies** folder



## Remove the default user groups

These user groups exist by default under **System > Users and Groups > User Groups** upon the installation of FactoryTalk Services Platform:

- Authenticated Users

This group includes all users whose identities were authenticated by Windows through a sign-in process. This includes local user accounts as well as all domain user accounts from trusted domains. By default, all users who have successfully signed in to Windows automatically have access to the FactoryTalk Directory. If you want only specific users that you configure have access to the FactoryTalk system, remove this Authenticated Users group to prevent them from having access to the FactoryTalk Directory.

- Windows Administrators

This group includes all users with Windows administrator permissions on the computer or in the domain. By default, this group is a member of the FactoryTalk Administrators group, giving them administrative access. If that's what you want, leave that default configuration in place. If you want only specific administrators that you configure have administrative access to the FactoryTalk system, remove this Windows Administrators group from the FactoryTalk Administrators group to prevent them from having access to the FactoryTalk Directory.

## Temporary access

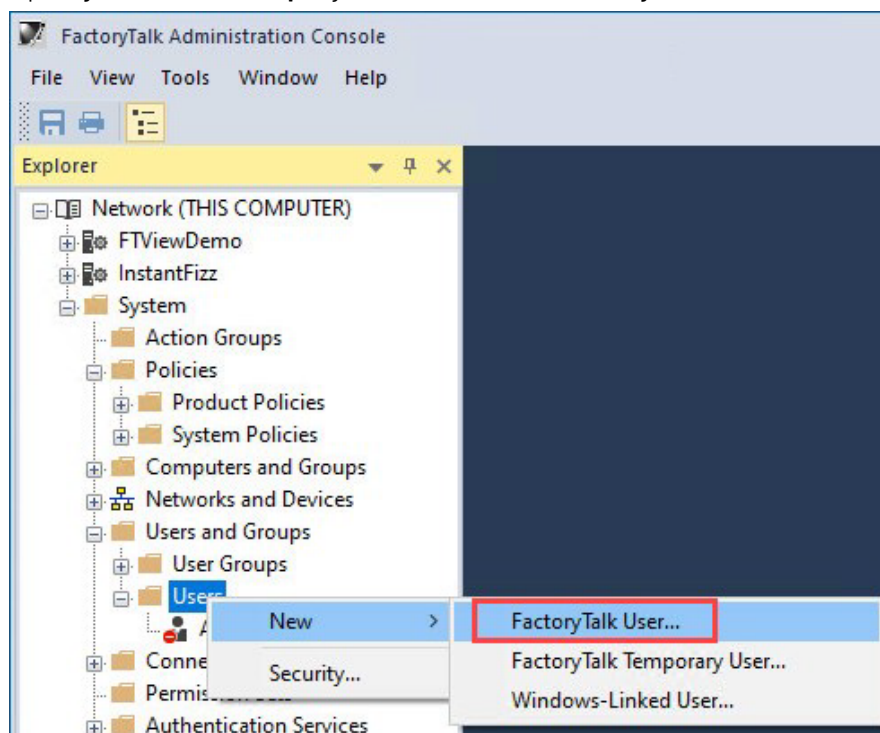
To allow users to temporarily have the permissions of another user in a different group, add a FactoryTalk user with a disabled date or a FactoryTalk temporary user. A FactoryTalk user configured with a disabled date will be automatically disabled in the specified date, whereas a temporary user requires someone to generate the password and a challenge and response process.

## Create a FactoryTalk user with a disabled date

When you create a FactoryTalk user, you have the option to configure a future date to automatically disable this user account.

### To create a FactoryTalk user with a disable date

1. Open FactoryTalk Administration Console, and then sign in as an administrative user.
2. Expand **System > Users and Groups**, right-click **User**, and then select **FactoryTalk User**.



- Enter a username, for example *TempUser*, select **Disable date**, and then specify a date to disable the account.

**New FactoryTalk User**

General Group Membership

User name: TempUser

Full name:

Description:

Email:

☐ Account is disabled

Login method: Password

Password: .....

Confirm: .....

☐ User must change password at next logon

☐ User cannot change password

☐ Password never expires

Facility Code:

Badge ID: Scan

☒ Disable date 10/31/2023

OK Cancel Help

- Select **OK**.

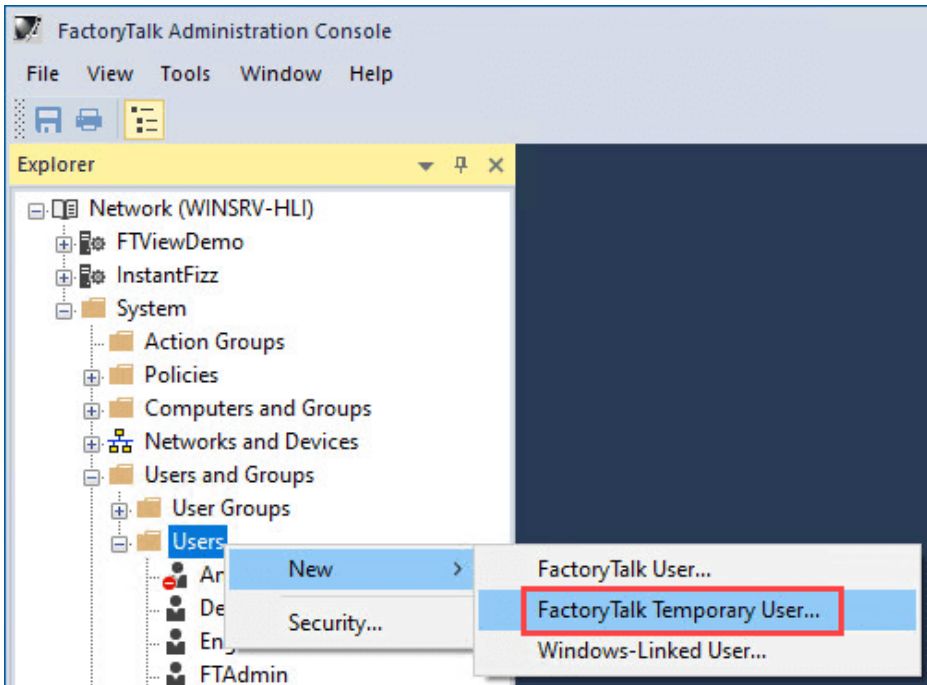
## Create a FactoryTalk temporary user

When you create a temporary user account, you'll also define who is permitted to generate this password. The password is generated through a challenge and response process that can be done over the phone. The person requesting access and the person granting access don't need to have network connectivity with each other, as long as they both have valid cached copies of (or live connections to) the same FactoryTalk Directory.

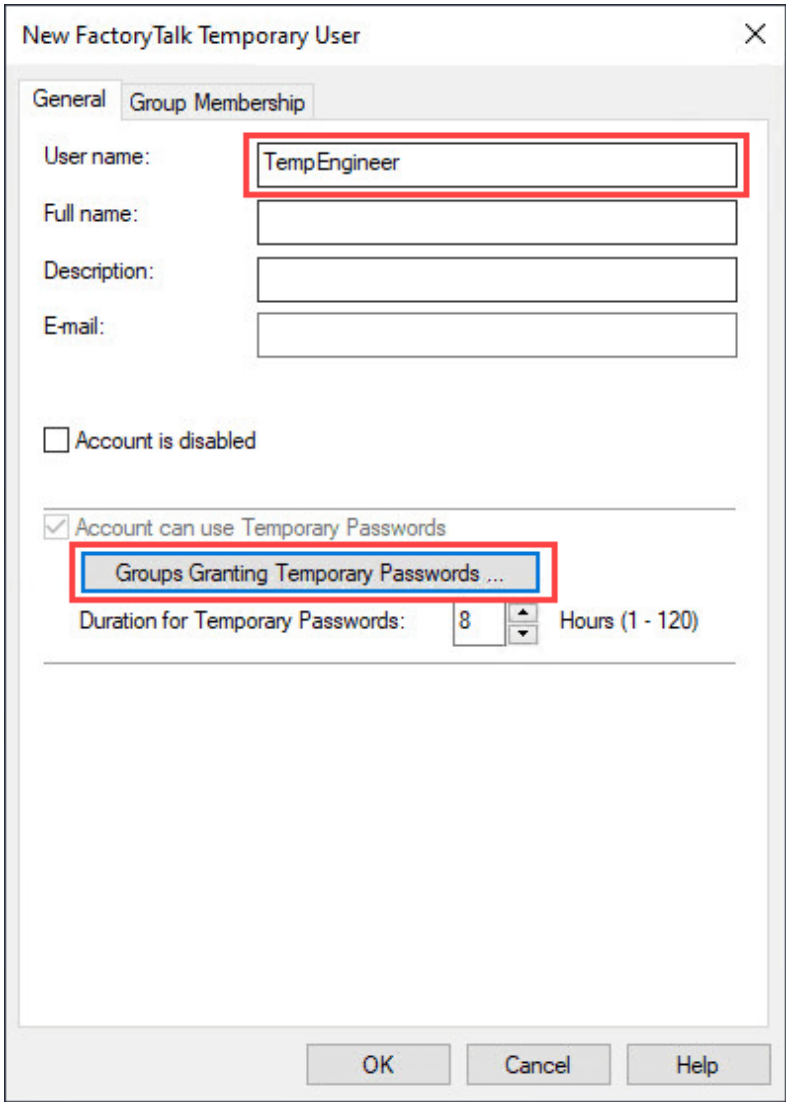
### To create a FactoryTalk temporary user

- Open FactoryTalk Administration Console, and then sign in as an administrative user.

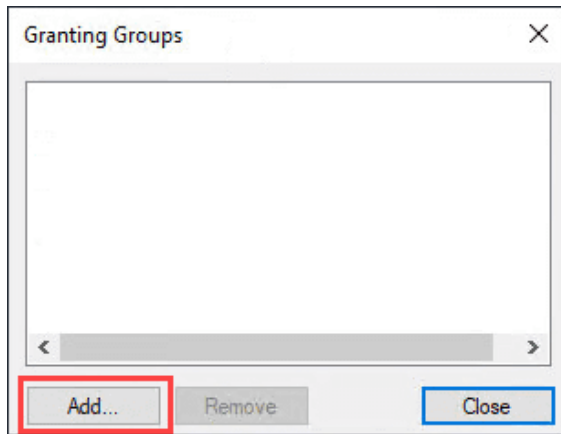
- 2. Expand **System > Users and Groups**, right-click **User**, and then select **FactoryTalk Temporary User**.



- 3. Enter a username, for example *TempEngineer*, and then select **Groups Granting Temporary Passwords**.

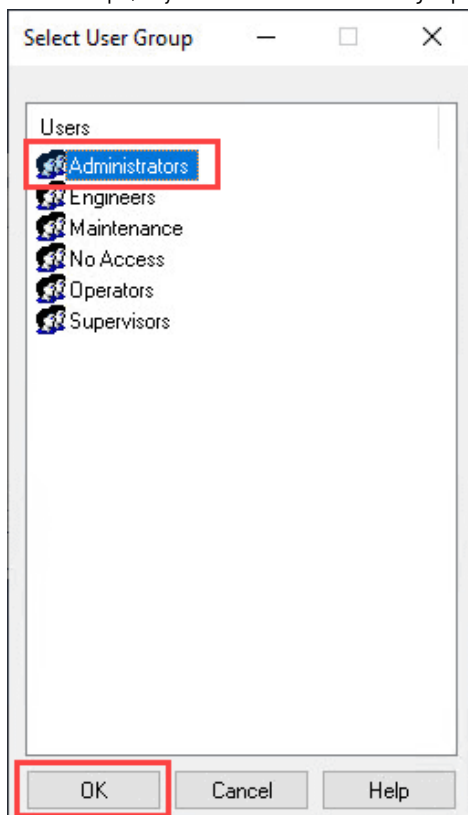


4. Select **Add**.

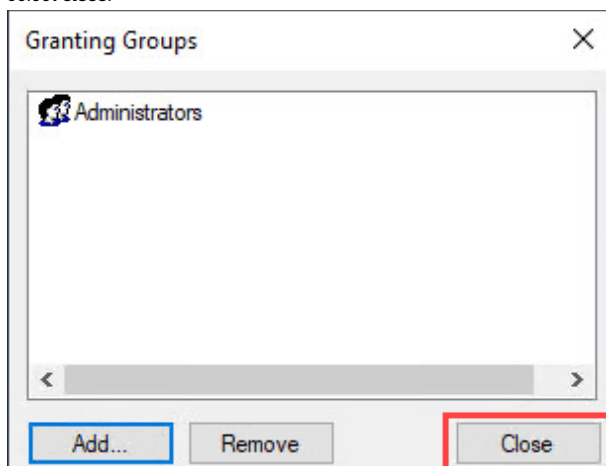


5. Select a group that can assign temporary passwords, and then select **OK**.

In this example, only users in the **Administrators** group can do so.



6. Select **Close**.



7.    Select **OK**.

New FactoryTalk Temporary User

General

Group Membership

User name:

TempEngineer

Full name:

Description:

E-mail:

☐ Account is disabled

☒ Account can use Temporary Passwords

Groups Granting Temporary Passwords ...

Duration for Temporary Passwords:

8

Hours (1 - 120)

OK

Cancel

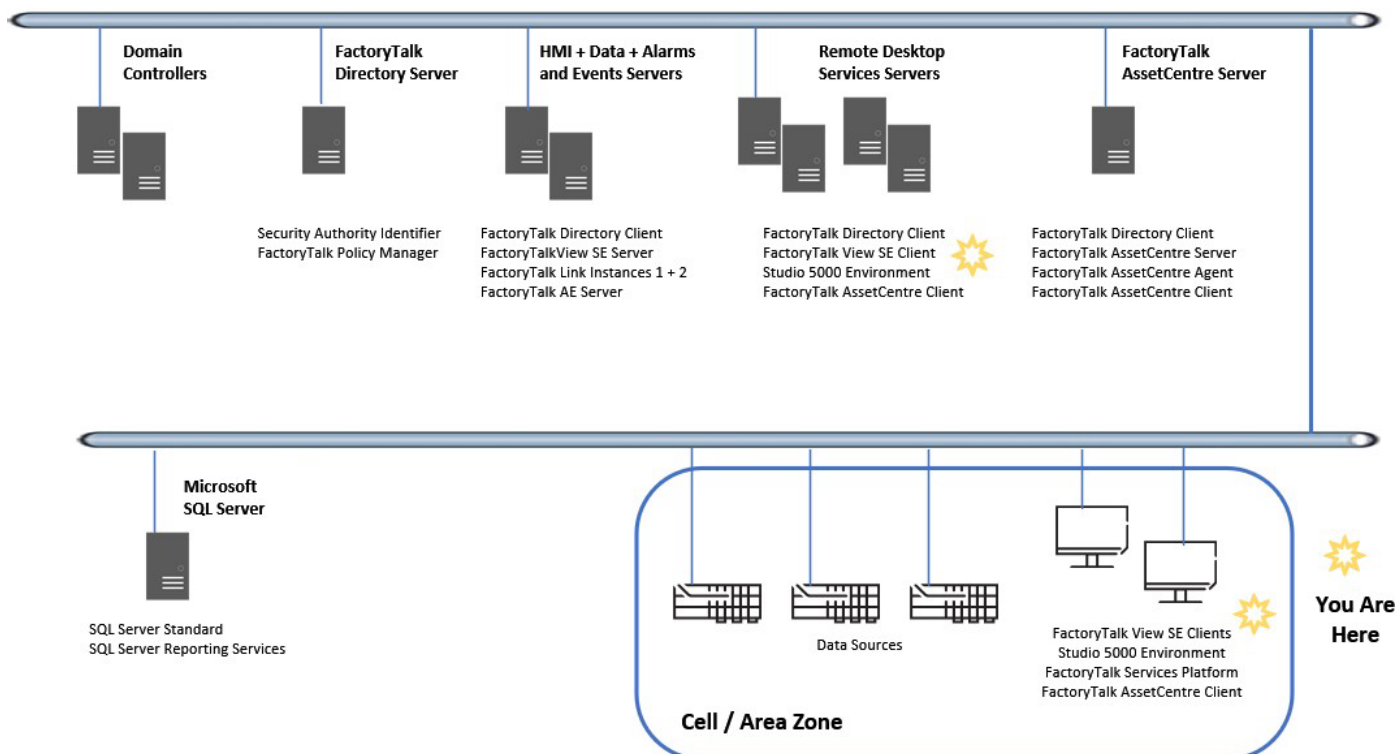
Help

## Secure a Studio 5000 Logix Designer project

Use FactoryTalk Security to secure Studio 5000 Logix Designer projects to the FactoryTalk Directory.

For more information and resources on securing a Logix Designer application, see *Logix 5000 Controllers Security Programming Manual* listed in [Additional Resources on page 4](#).

### Manufacturing Zone

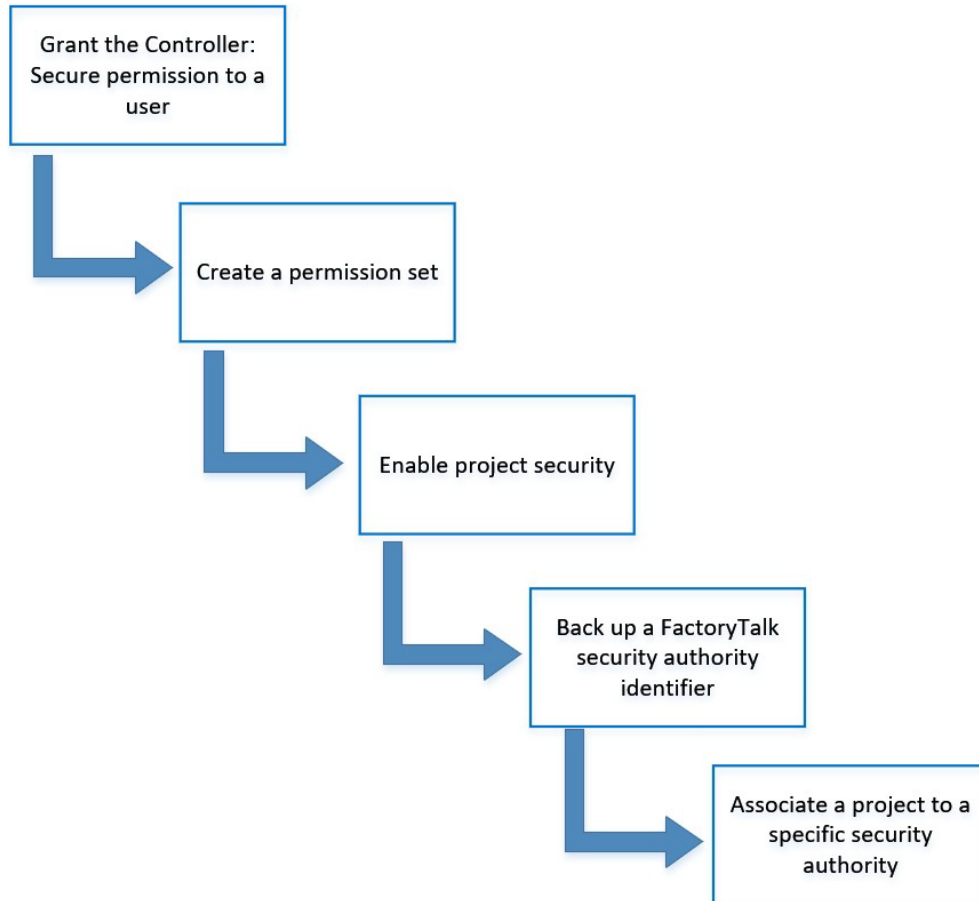


### Before you begin

The instructions in this chapter use the following software as examples. The operation steps or look of your software may vary.

- Studio 5000 Logix Designer version 34.00.00
- FactoryTalk Services Platform version 6.40.00

## Workflow



## Enable Studio 5000 Logix Designer project security

The first step in securing a Studio 5000 Logix Designer project with FactoryTalk Security is to enable the security in the project file.

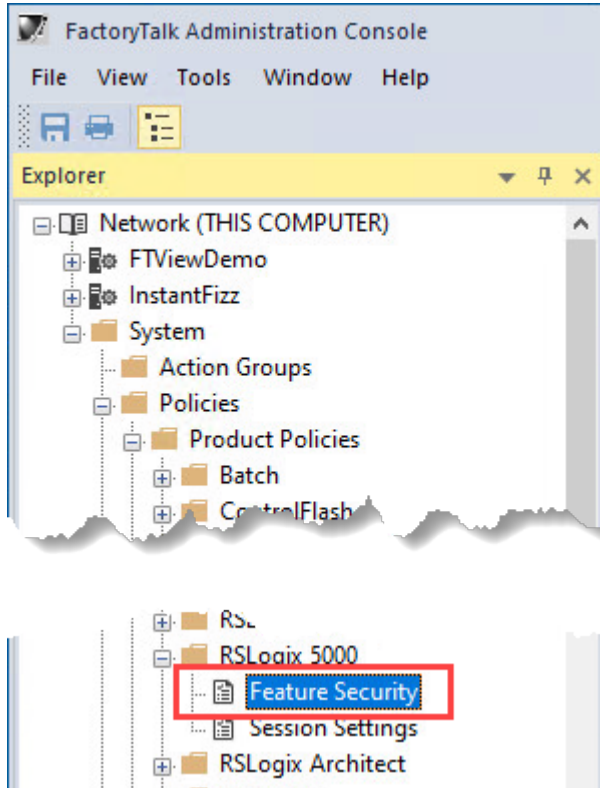
### Grant the Controller: Secure permission to a user

For a user to enable the project security, that user must be granted the **Controller: Secure** permission in the FactoryTalk Directory. By default, no users or groups have this permission.



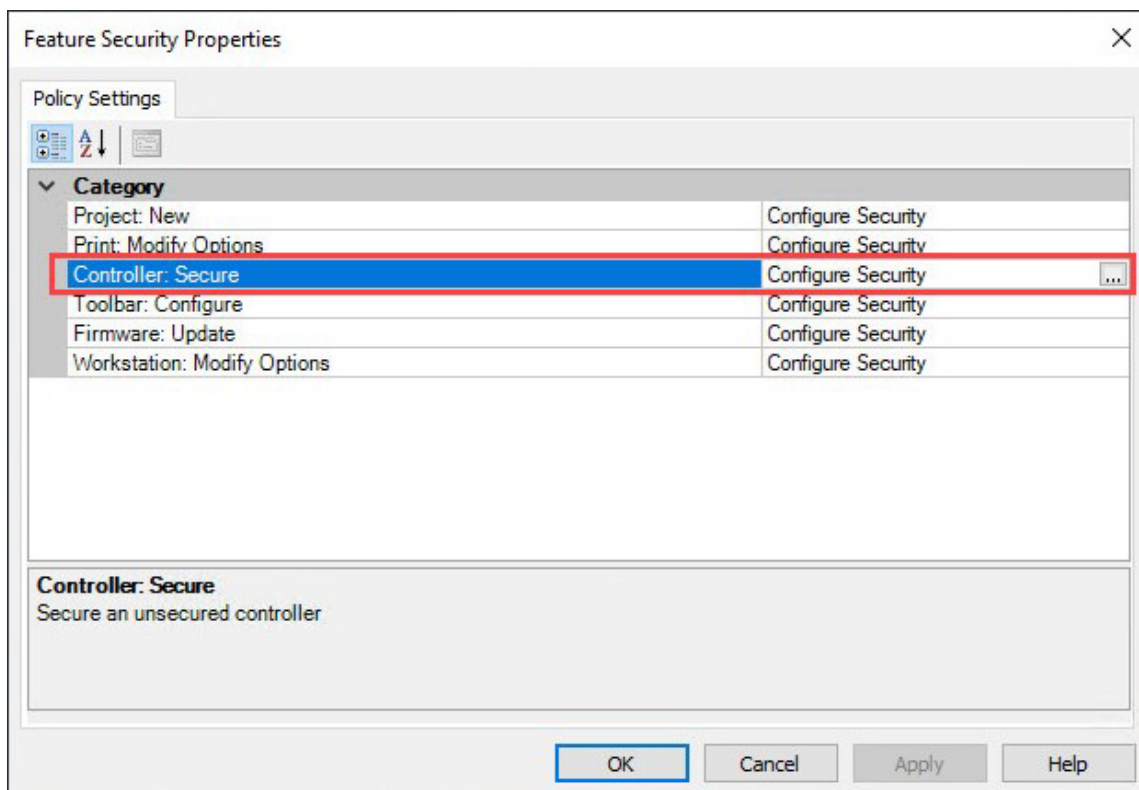
## To grant the Controller: Secure permission to a user

1. In FactoryTalk Administration Console, go to **System > Policies > Product Policies > RSLogix 5000**, and then double-click **Feature Security**.

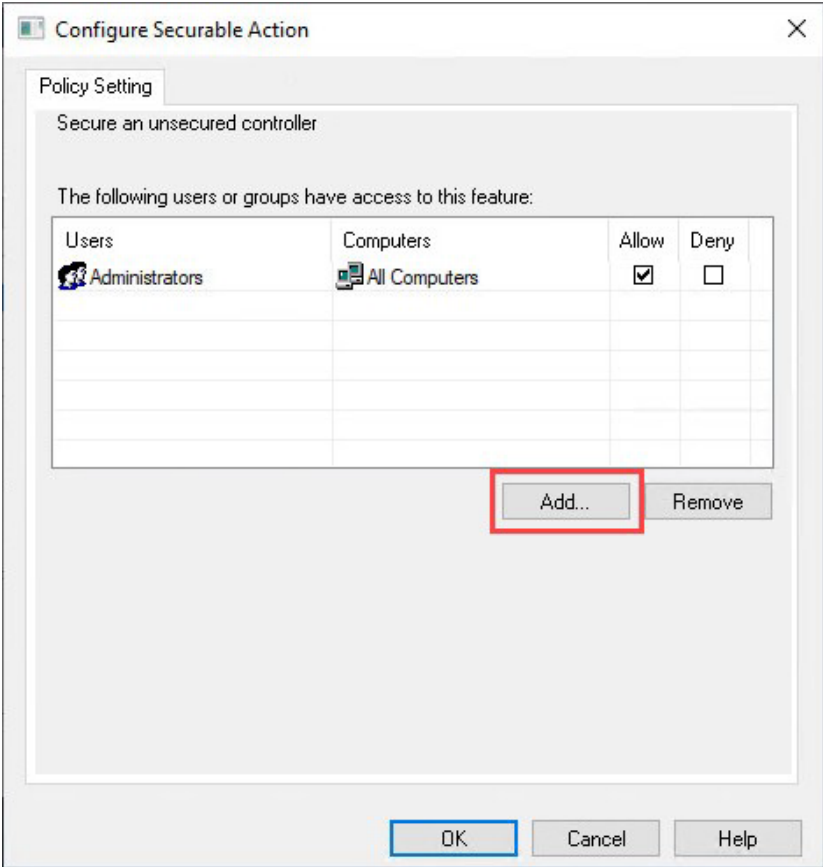


**NOTE:** RSLogix 5000 is known as Studio 5000 Logix Designer starting from version 21.00. Policies under **RSLogix 5000** apply to both RSLogix 5000 and Studio 5000 Logix Designer.

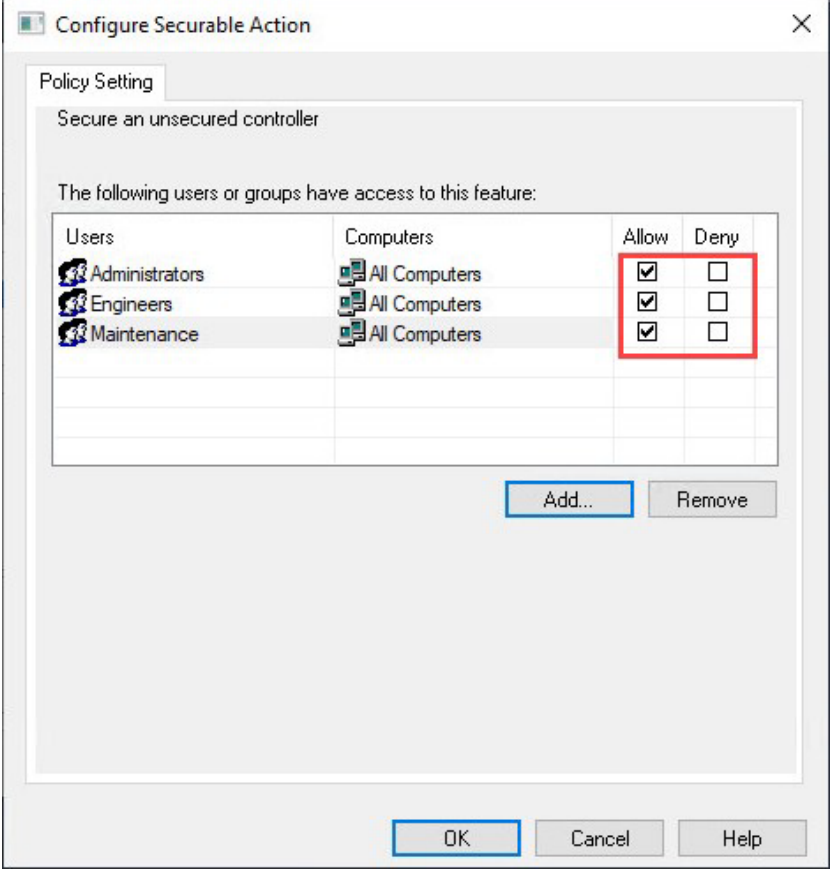
2. In the **Feature Security Properties** dialog box, select **Controller: Secure**, and then select the browse button to the right of **Configure Security**.



3. In the **Configure Securable Action** dialog box, select **Add** to add the desired group or user to the list.



4. Configure the permission for the group or user who will be able to enable the project security, and then select **OK**.



## Permission set vs. logical name

Once you enable the project security, choose one of the following to secure the project file:

- **Permission set** - A permission set lets you grant permissions for multiple groups across multiple software feature sets and the permissions are applied across many users at once.

Permission sets are available with FactoryTalk Services Platform version 2.80 or later and Studio 5000 Logix Designer version 28.00.00 or later.

- **Logical name** - A logical name is a name for the controller in the FactoryTalk Directory. It is automatically added to the FactoryTalk Directory when a Logix Designer application project is secured to a FactoryTalk Directory.

Logical names are available with FactoryTalk Services Platform version 2.10 or later.

We strongly recommend that you use a permission set to secure a project file.

- If you use a permission set, you can use the same permission set to apply security to all controllers in the system.
- If you use a logical name, you must create a logical name for each controller in the system and configure the security settings in each of the logical names.

**Controller Properties - RACE\_CookieLine**

General Major Faults Minor Faults Date/Time Advanced SFC Execution Project Redundancy  
Nonvolatile Memory Capacity Internet Protocol Port Configuration Security\* Alarm Log

Security Authority: FactoryTalk Security (INF-HLI-LOGIX01) v

☐ Use only the selected Security Authority for Authentication and Authorization

Secure With:

☒ Logical Name <Controller Name>

☐ Permission Set

☐ Restrict Communications Except Through Selected Slots

Select Slots: 0 1 2 3 4 5 6

☐ Enable Controller Web Pages

**Change Detection**

Changes To Detect: 16#FFFF\_FFFF\_FFFF\_FFFF Configure...

Audit Value: 16#EEAE\_AAE7\_EF29\_8169

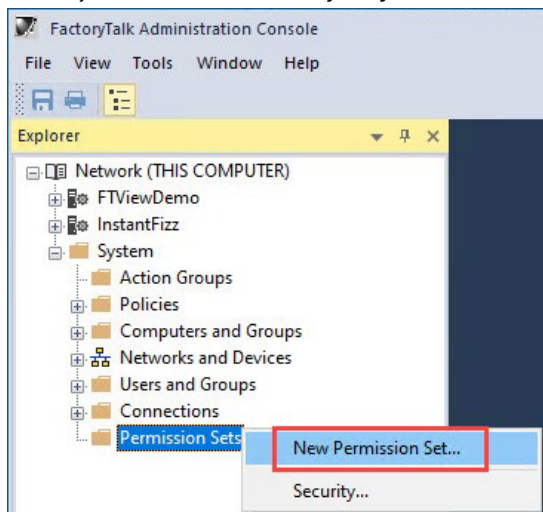
OK Cancel Apply Help

## Create a permission set

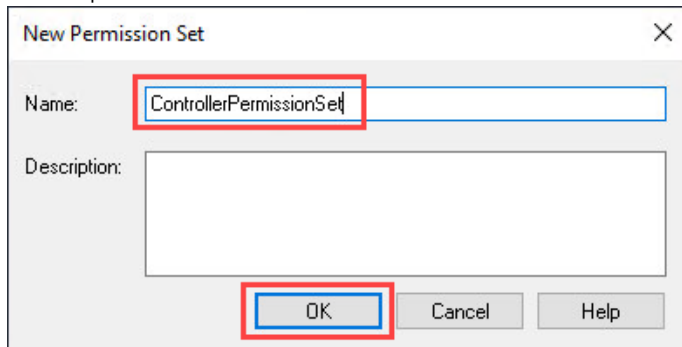
To secure a Logix Designer application project file with a permission set, create one first.

### To create a permission set

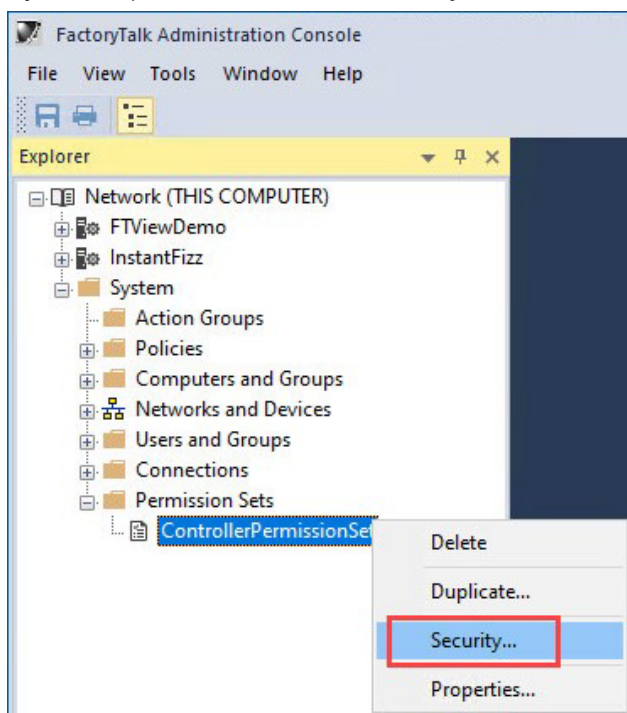
1. In FactoryTalk Administration Console, go to **System > Permission Sets**, right-click **Permission Sets**, and then select **New Permission Set**.



2. Name the permission set, and then select **OK**.



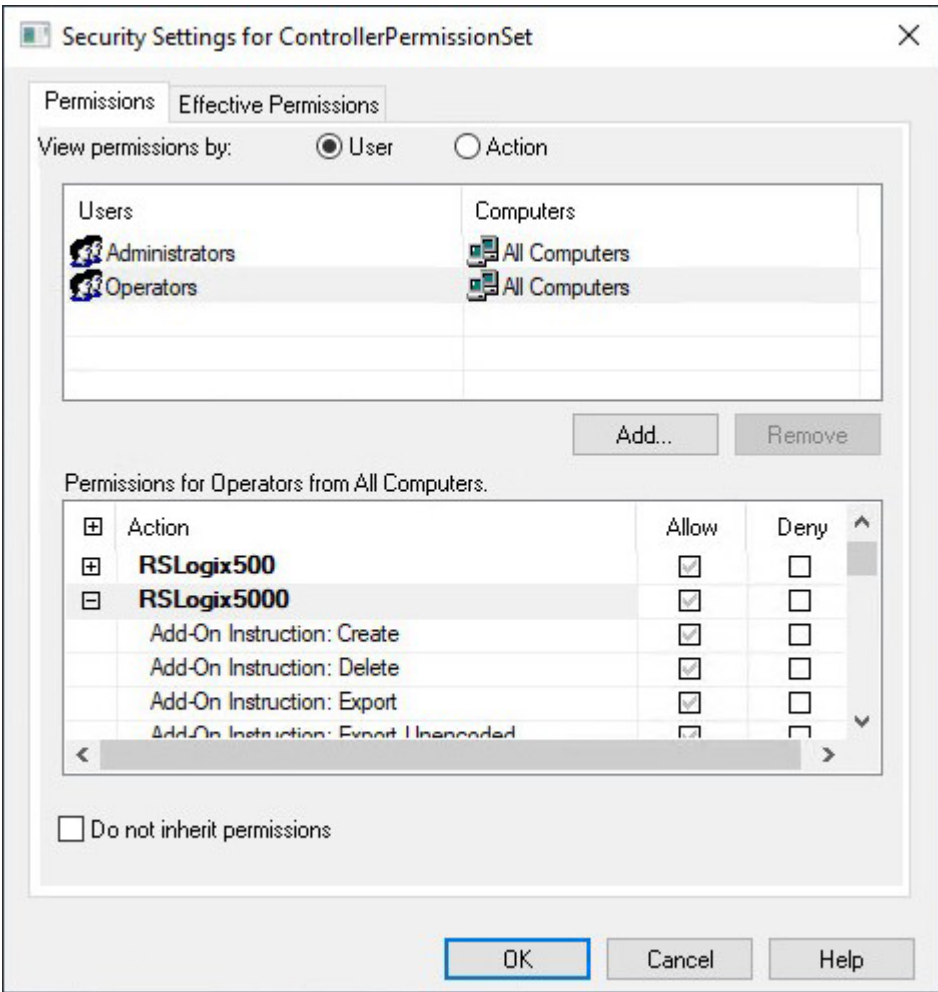
3. Right-click the permission set, and then select **Security**.



4. In the **Security Settings** dialog box, select the group for which you want to grant permissions, and then set permissions as necessary.



**Tip:** In this example, the existing checkboxes for permissions appear dimmed. This is because the permissions are inherited from its parent container, **Permission Sets**, which inherits permissions all the way up to the root directory, **Network**.



5. Once permissions are set to the desired outcome, select **OK**.



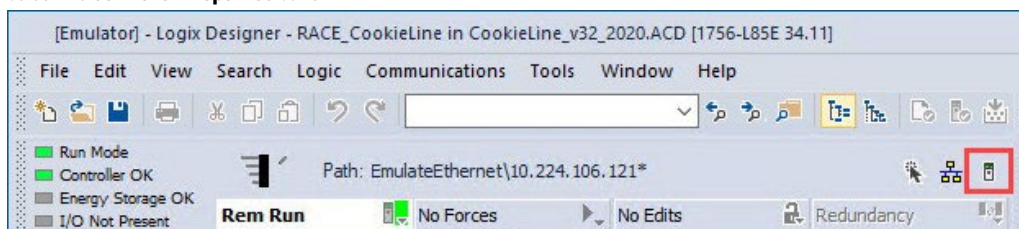
**Tip:** Permissions can be granted for multiple groups, features, and software application platforms before selecting **OK**.

## Enable project security

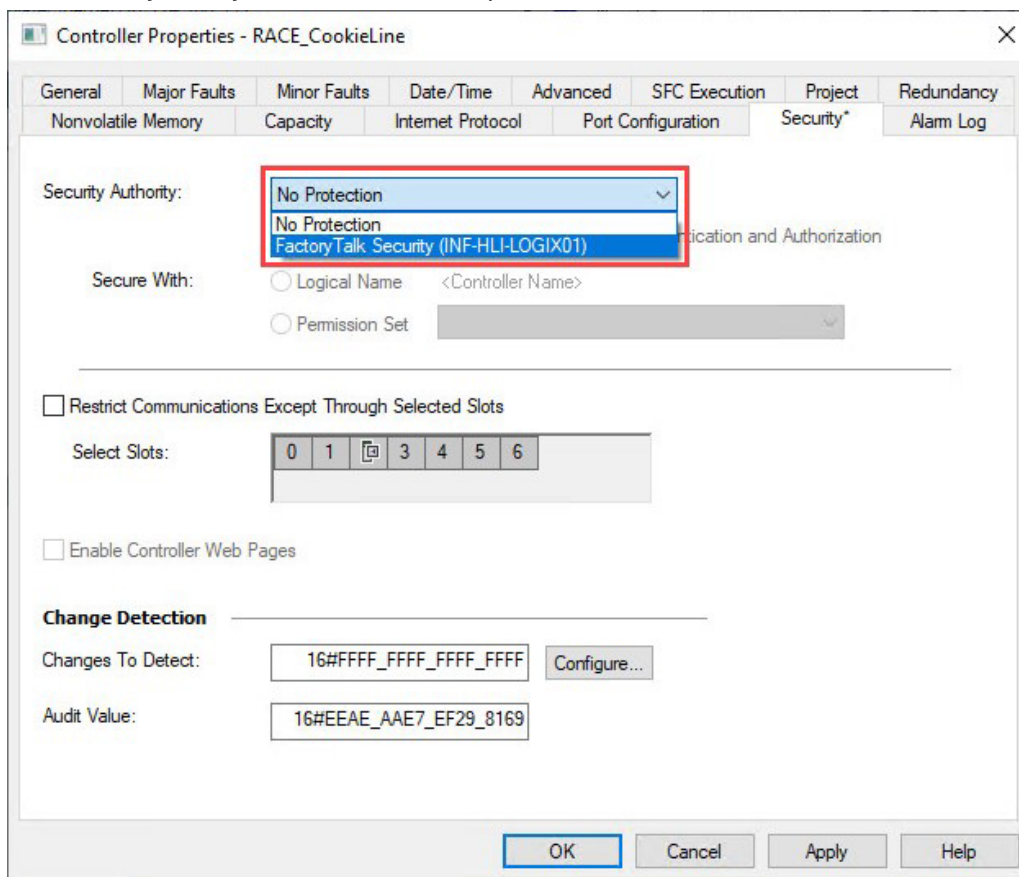
With the **Controller: Secure** permission, users can enable project security. After project security is enabled, all securable actions of RSLogix 5000 or Studio 5000 Logix Designer will take effect.

### To enable project security

1. Open a Studio 5000 Logix Designer project. Make sure the signed-in user has the **Controller: Secure** permission.
2. Select the **Controller Properties** button.

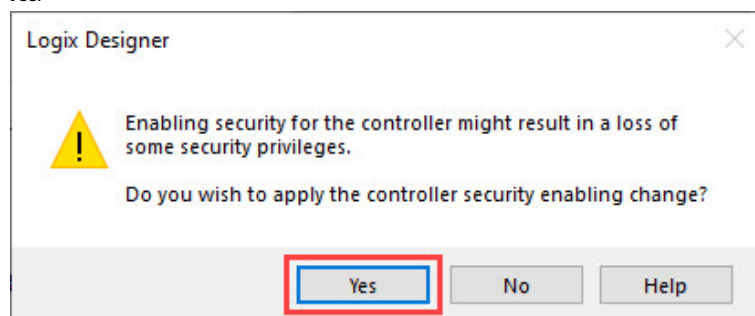


3. From the **Security Authority** list, select the desired security server, and then select **OK**.



In this example, the displayed name is the computer hosting the FactoryTalk Directory used to secure the project.

4. After selecting **OK**, a dialog box opens, alerting you that enabling security might result in a loss of some security privileges. Acknowledge this warning by selecting **Yes**.





## Associate a Studio 5000 Logix Designer project to a security authority

When configuring the project security, a **Use only the selected Security Authority for Authentication and Authorization** checkbox is available. This checkbox associates the project with a specific security authority. A security authority identifier is a unique ID generated for each FactoryTalk Directory to differentiate one directory from another. The value is represented as a 32-character hexadecimal string.

When associating a project with a specific security authority, the project is being associated with a specific FactoryTalk Directory that is identified by a security authority identifier. With this checkbox selected, users interacting with this project must be authenticated and authorized by the selected security authority. The security authority identifier of the FactoryTalk Directory where users belong must match the project's associated security authority.

**IMPORTANT:** Before associating a project with a specific security authority, we strongly recommend backing up the security authority identifier. Projects that are secured and bound to a specific security authority cannot be recovered if the security authority identifier of the FactoryTalk Directory used to secure the project no longer exists. If the identifier changes and you lose the original one, you will be locked out of the FactoryTalk Directory. There is no way to recover the original identifier or go online with secured controllers. Secured controllers can only be accessed again by clearing their memory.

**Controller Properties - RACE\_CookieLine**

General Major Faults Minor Faults Date/Time Advanced SFC Execution Project Redundancy  
Nonvolatile Memory Capacity Internet Protocol Port Configuration Security\* Alarm Log

Security Authority: FactoryTalk Security (INF-HLI-LOGIX01) ▼

☐ Use only the selected Security Authority for Authentication and Authorization

Secure With: ☐ Logical Name <Controller Name> ☒ Permission Set ControllerPermissionSet ▼

☐ Restrict Communications Except Through Selected Slots

Select Slots: 0 1 2 3 4 5 6

☐ Enable Controller Web Pages

**Change Detection**

Changes To Detect: 16#FFFF\_FFFF\_FFFF\_FFFF Configure...

Audit Value: 16#EEAE\_AAE7\_EF29\_8169

OK Cancel Apply Help

## Back up a FactoryTalk security authority identifier

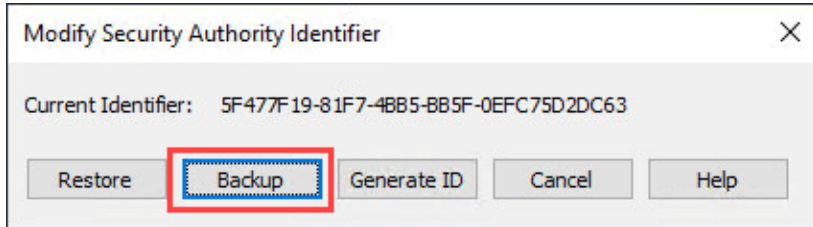
Backing up the FactoryTalk security authority identifier allows you to restore it if you have to instantiate a new FactoryTalk Directory. For example, if your FactoryTalk Directory goes wrong or something happens to the FactoryTalk Directory computer.

### To back up a FactoryTalk security authority identifier

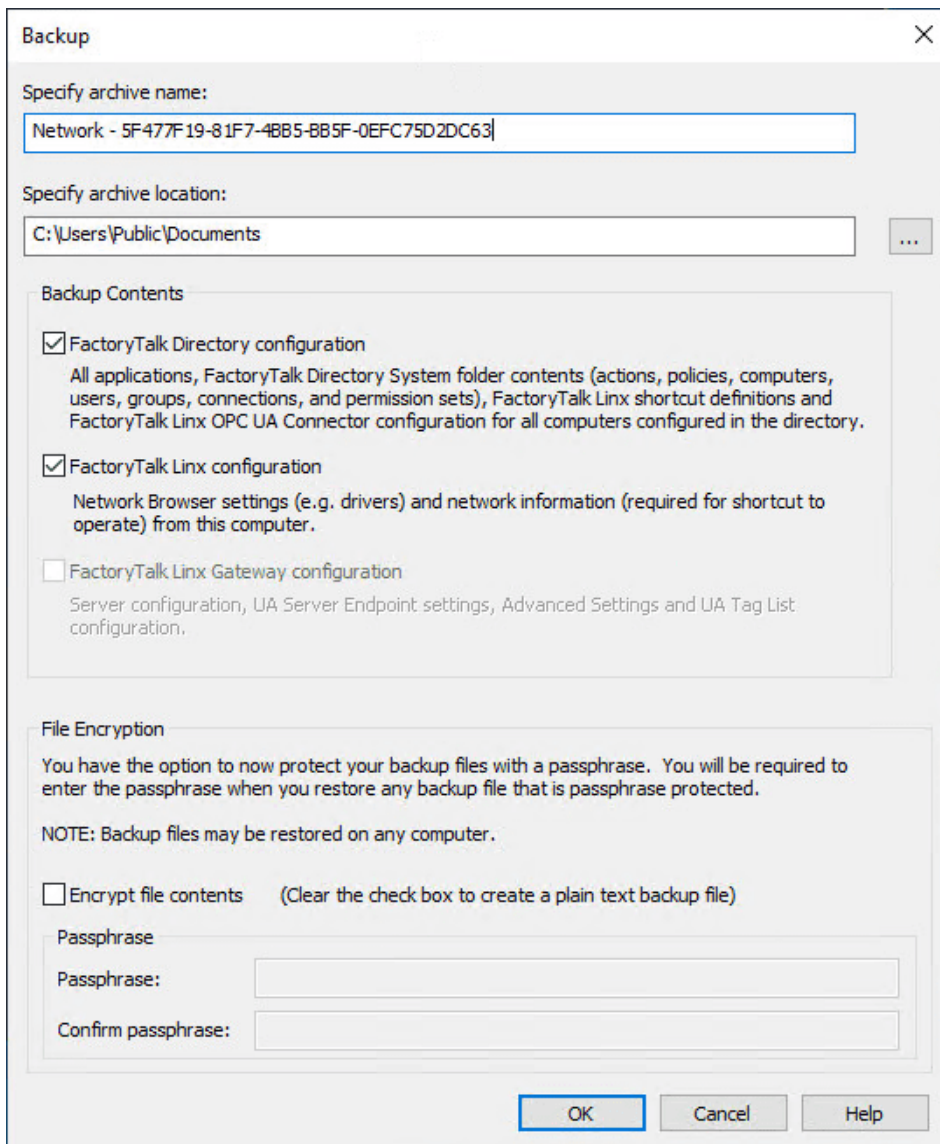
1. In FactoryTalk Administration Console, select **Tools > FactoryTalk Security Authority Identifier**.



2. Select **Backup**.

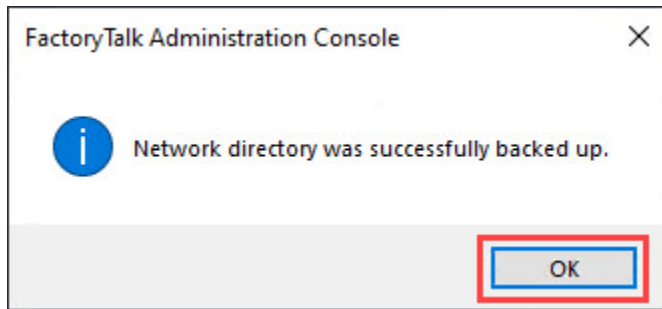


3. In the **Backup** dialog box, configure the settings as needed, and then select **OK**.





4. Select **OK** to continue with the backup.
5. Select **OK**.

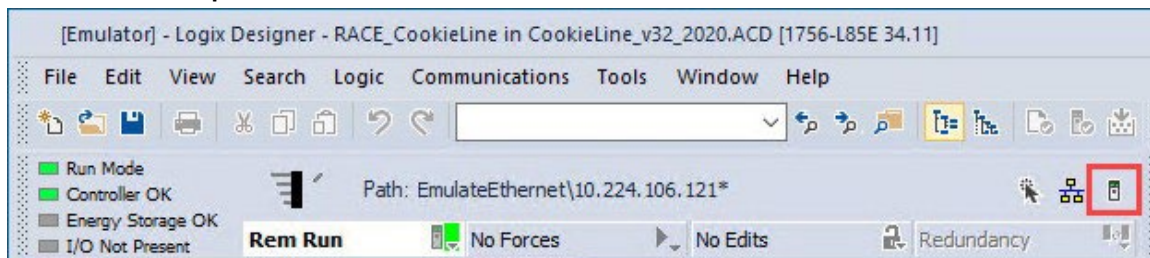


## Associate a project to a specific security authority

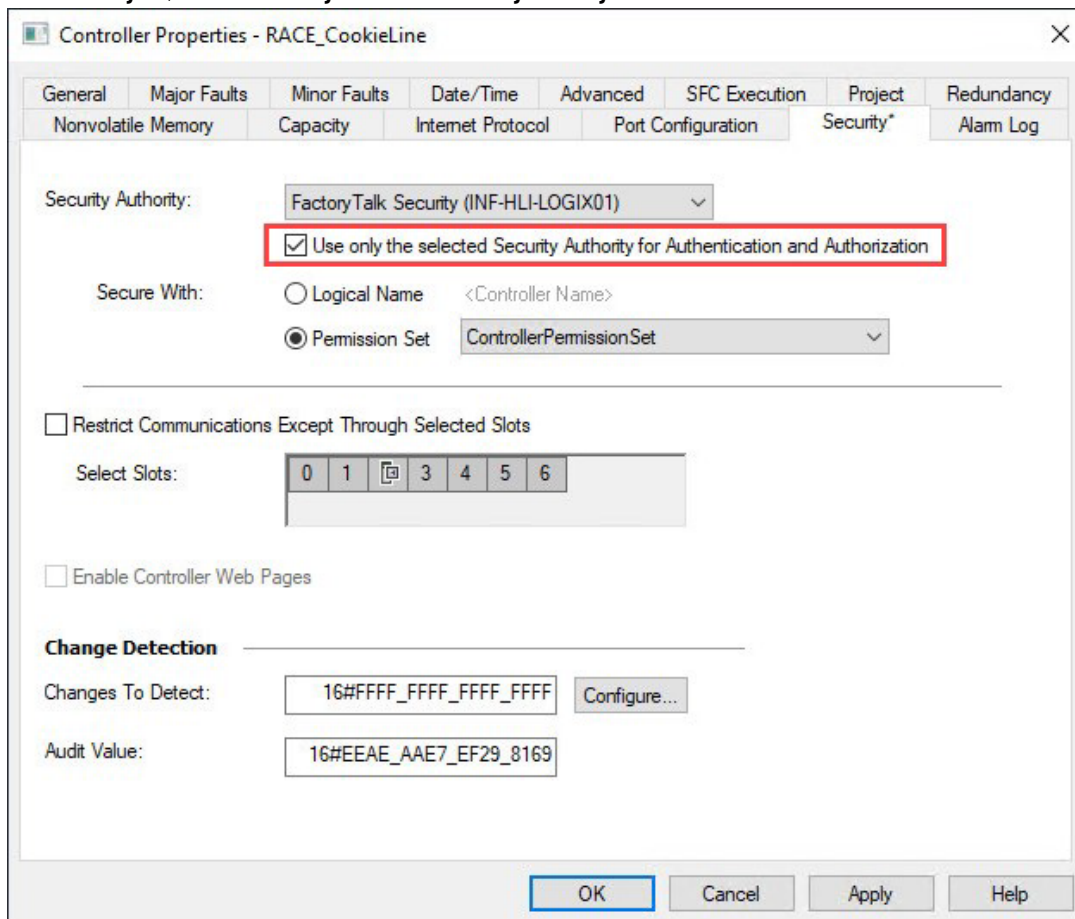
Associate a Studio 5000 Logix Designer project to a specific security authority by the unique security identifier of the FactoryTalk Security server.

### To associate a project to a specific security authority

1. Select the **Controller Properties** button.



2. On the **Security** tab, select the **Use only the selected Security Authority for Authentication and Authorization** checkbox.



3. Select **OK**.



**Tip:** You can configure security as an online edit to a running system, or you can configure security to an oLine project and then download it to the controller.

## When the security authority identifier might not match

The following are some examples of when the security authority identifier might not match the one used to secure a controller:

- FactoryTalk Directory server hardware failure

If the server hosting the FactoryTalk Directory has a hardware failure, you may need to install the software on new hardware or virtual device. When the FactoryTalk Directory server is installed on a system for the first time, the system generates a new random Security Authority ID. You must restore the original Security Authority ID before you can gain the appropriate access to the controller or project secured by the original FactoryTalk Directory server.

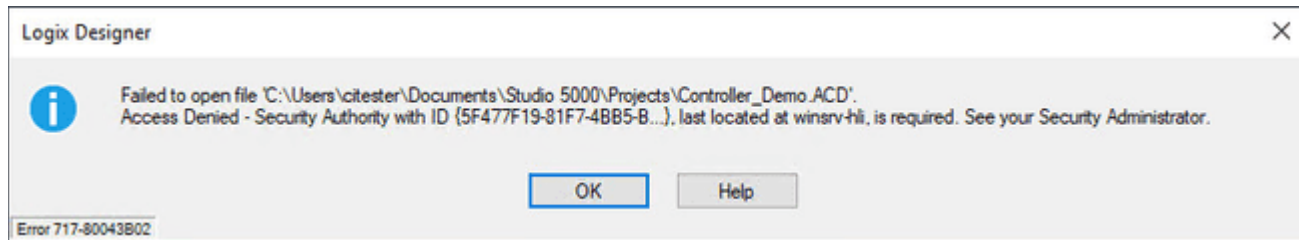
- The project or controller received from a third party

A project developed by a third party (such as an OEM) may be secured to a specific FactoryTalk Directory to protect their intellectual property. If the third party chooses to distribute the secured project, the recipients of that project may have limited access to the project.

- Unauthorized device

A device is connected to the network but is not joined to the FactoryTalk Directory. This device may have FactoryTalk Services Platform installed, and may be part of a FactoryTalk Directory, but the Security Authority IDs do not match.

In such cases, you should see the following message, indicating that the Security Authority ID of the FactoryTalk Security server does not match the value in the controller project. Therefore, Studio 5000 Logix Designer cannot open the project.



If you do not select the **Use only the selected Security Authority for Authentication and Authorization** checkbox in the **Controller Properties** dialog box and change the Security Authority ID of the FactoryTalk Security server, you will be authorized to open this project as long as the user permissions remain the same.

## Restore a FactoryTalk security authority identifier

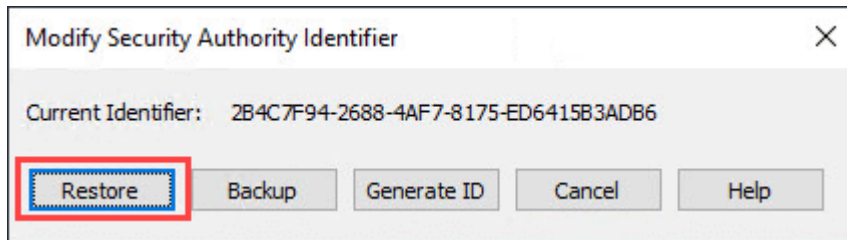
In the unlikely event that the system was modified in an unexpected way and the security authority identifier changes, you can restore the identifier that you've backed up.

### To restore a FactoryTalk security authority identifier

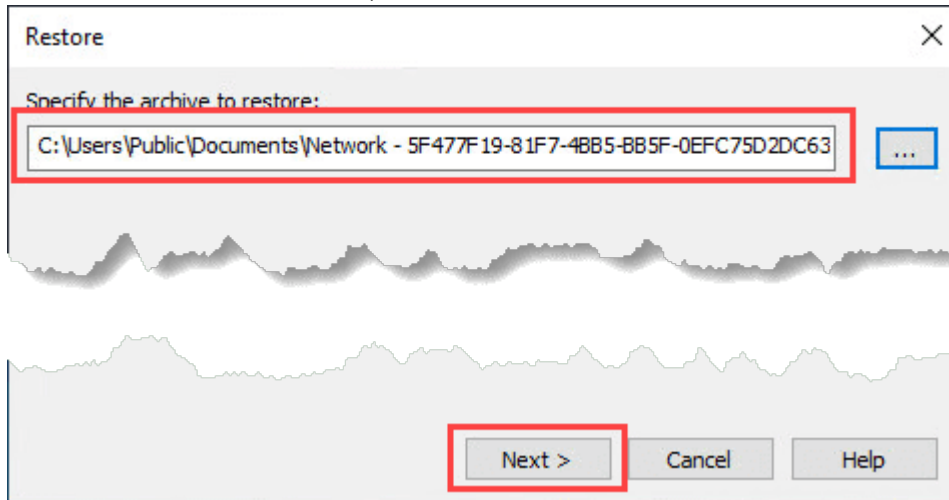
1. In FactoryTalk Administration Console, select **Tools > FactoryTalk Security Authority Identifier**.



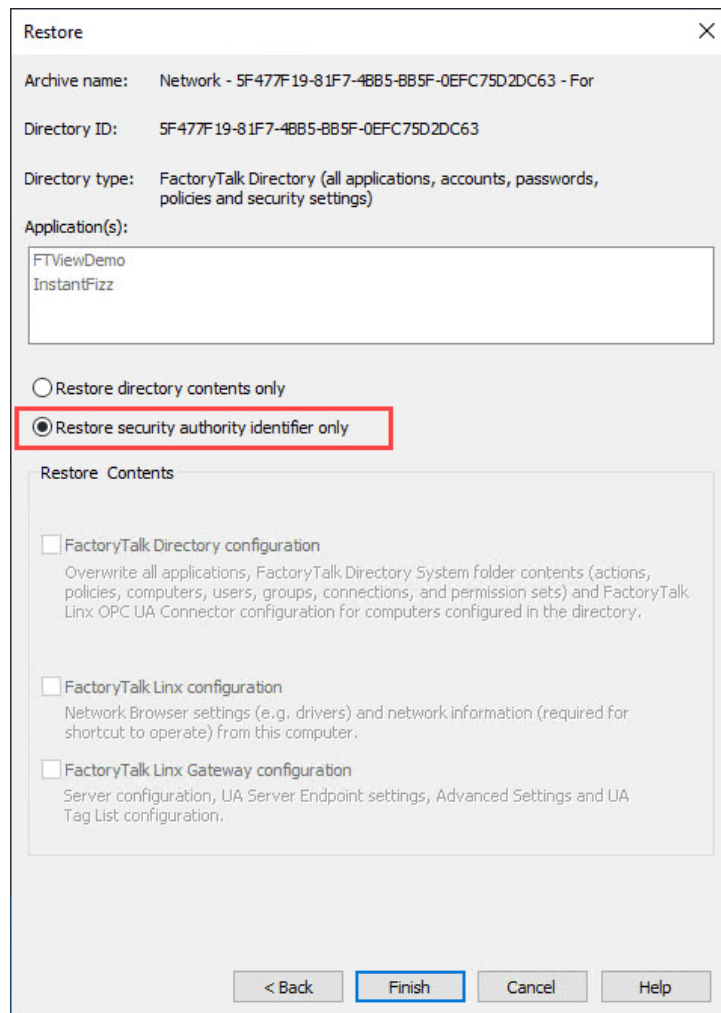
2. Select **Restore**.



3. Select the browse button to select the backup file, and then select **Next**.

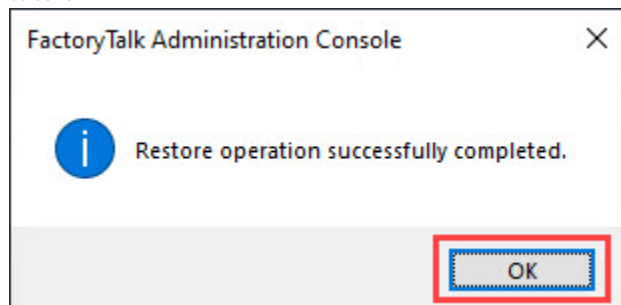


4. In the **Restore** dialog box, select the **Restore security authority identifier only** option to only restore the security authority identifier.

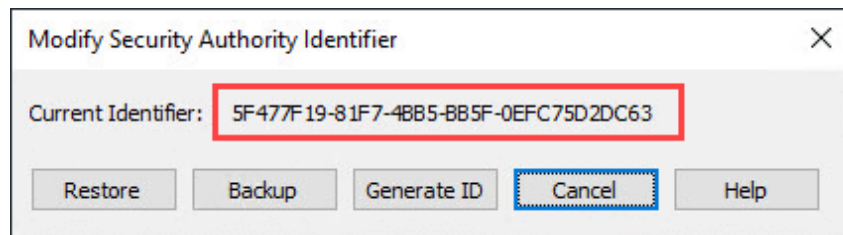


5. Select **Finish**.

6. Select **OK**.



7. Notice that the Security Authority ID is restored. Close the dialog box.

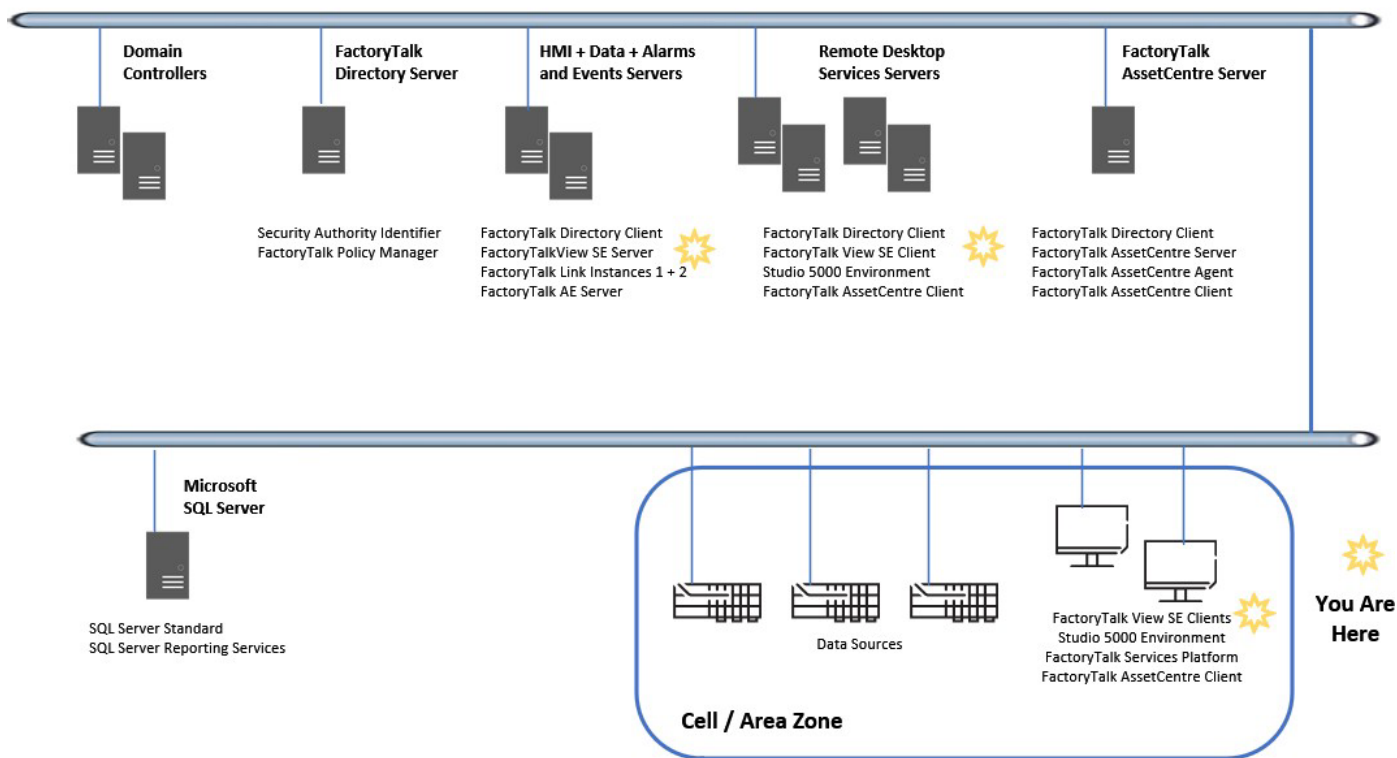


## Secure a FactoryTalk View project

Securing FactoryTalk View Site Edition (SE) includes managing permissions based on user role and assigning security codes to user groups and HMI project components.

**NOTE:** For information about deploying FactoryTalk software products on a network secured by IPSec, see the Knowledgebase Document ID: [QA46277 - Deploying FactoryTalk Software with IPSec](#).

### Manufacturing Zone

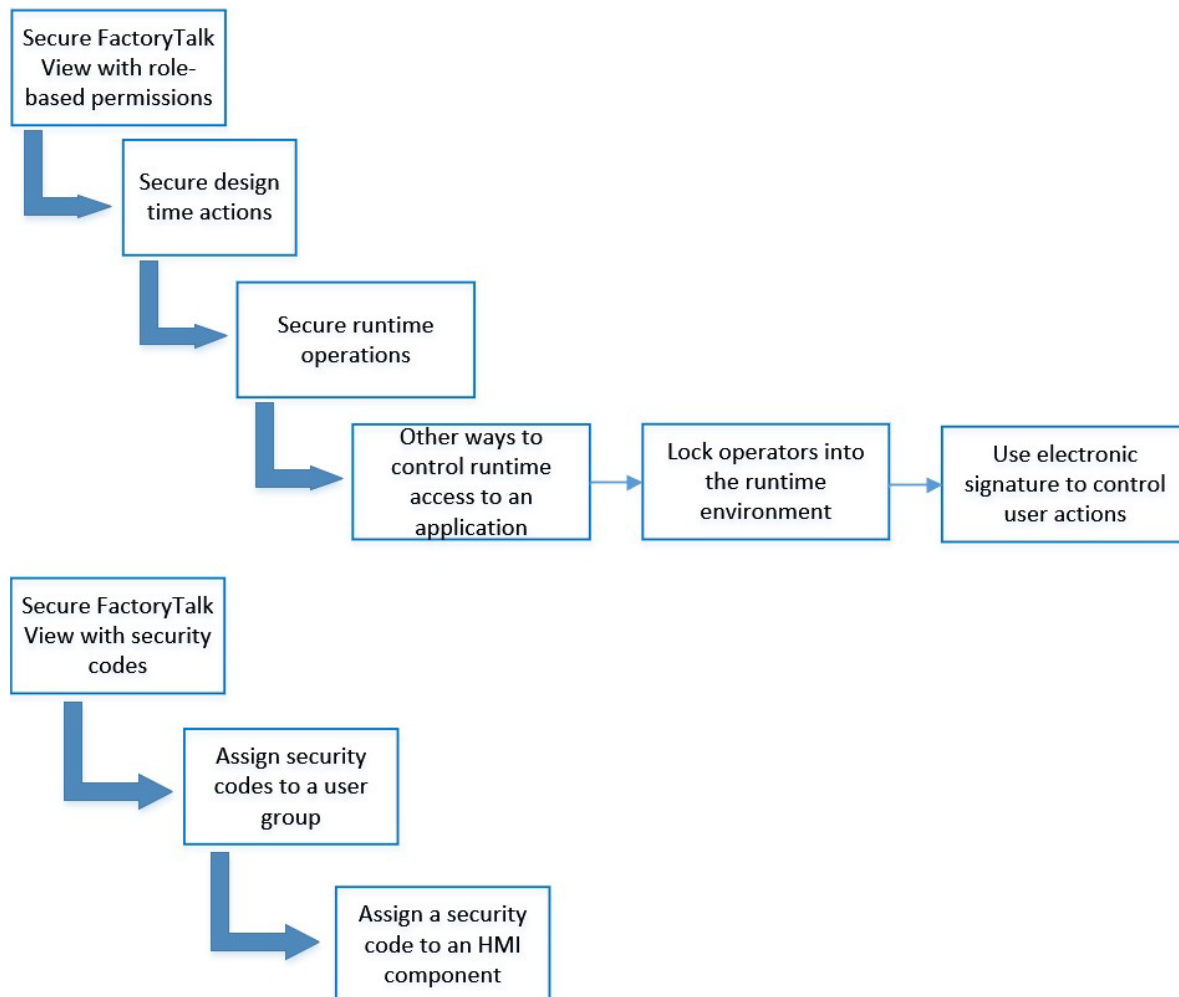


### Before you begin

The instructions in this chapter use the following software as examples. The operation steps or look of your software may vary.

- FactoryTalk View SE version 14.00.00
- FactoryTalk Services Platform version 6.40.00

## Workflow



## Securing FactoryTalk View with role-based permissions

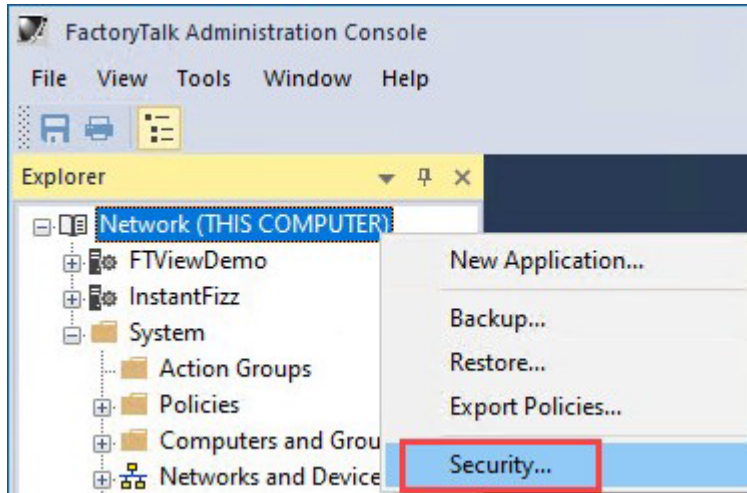
You can use role-based permissions to secure design time actions, such as actions in the RecipePro+ editor, and runtime operations, such as changing tag values, navigating displays, or executing commands.

### Secure design time actions

This section shows an example of how to allow user groups to perform certain actions in the RecipePro+ editor.

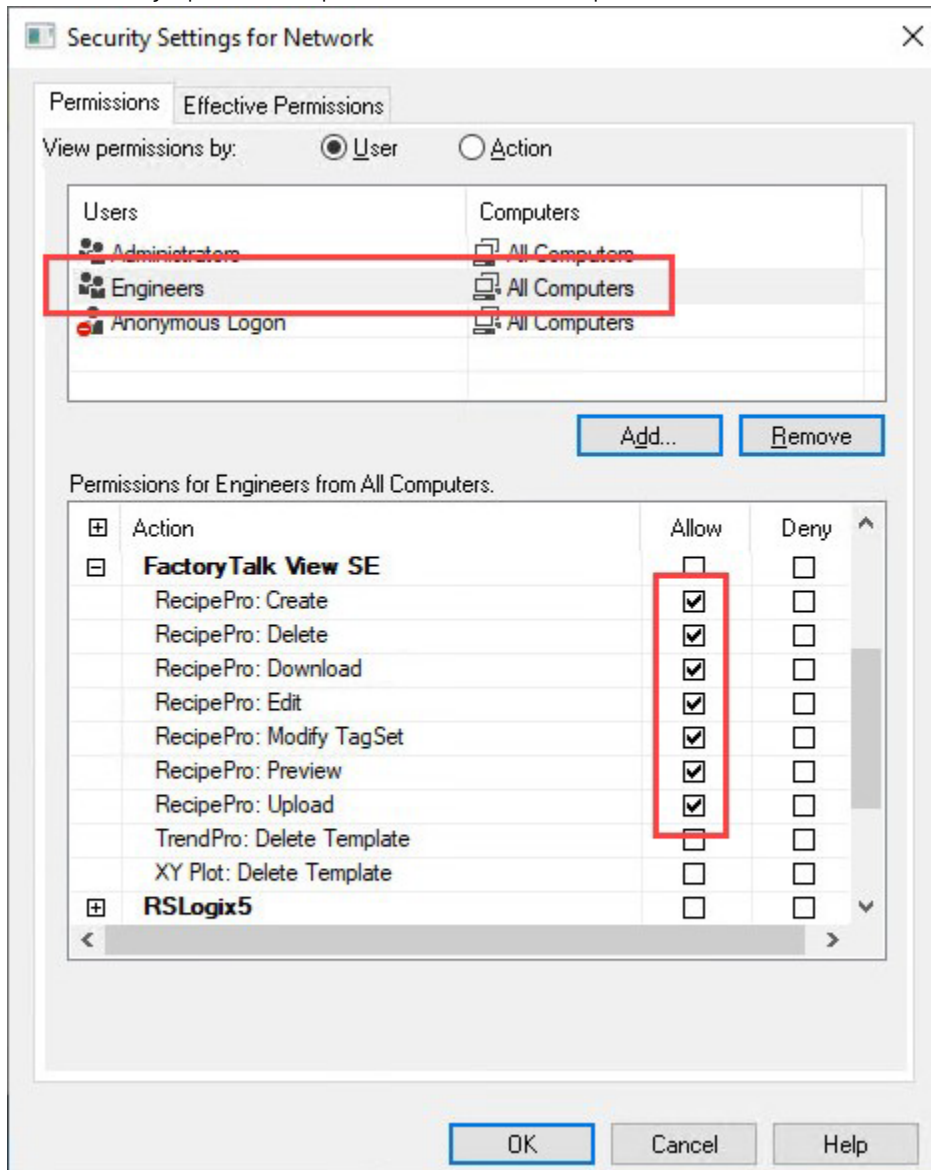
## To secure design time actions

1. In FactoryTalk Administration Console, right-click **Network**, and then select **Security**.



2. Select a group from the upper pane, and then select the **Allow** box for the RecipePro+ actions.

Users within that group are allowed to perform those actions in the RecipePro+ editor.



3. Select **OK**.



## Secure runtime operations

Use the security function **CurrentUserHasGroup** to secure runtime operations, such as changing tag values, navigating displays, or executing commands.

Unlike security codes that must be assigned to user groups and the HMI components, role-based security achieves security by controlling user groups' accessibility to those HMI components.

For example, only user groups with the same security code that is assigned to a command can run that command. Whereas with role-based security, you can configure the visibility or disabled state of a button that triggers the command. Only user groups that can see that button or its enabled state can press it to trigger the command.

---

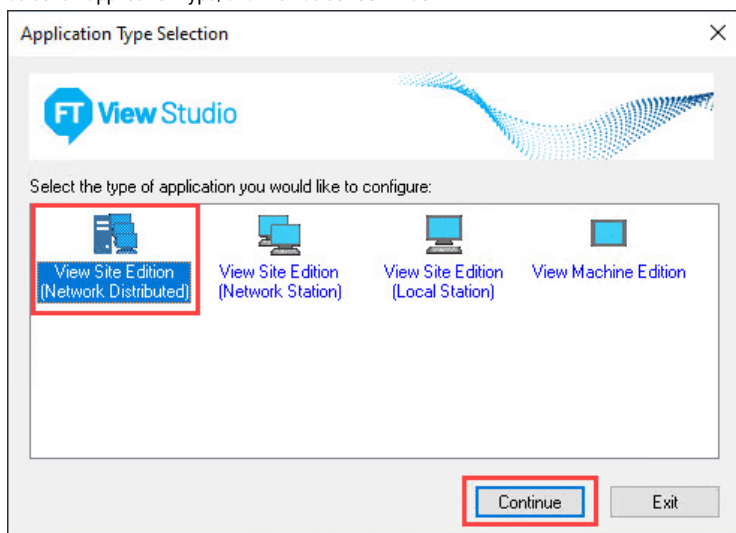
**IMPORTANT: CurrentUserHasGroup** only works for Azure AD groups that are added to the FactoryTalk Directory, provided that the Azure AD group will not be updated on the Azure side. Anytime the Azure AD group is updated on Azure, you must add the group to the FactoryTalk Directory again for it to get the latest Azure AD group information.

---

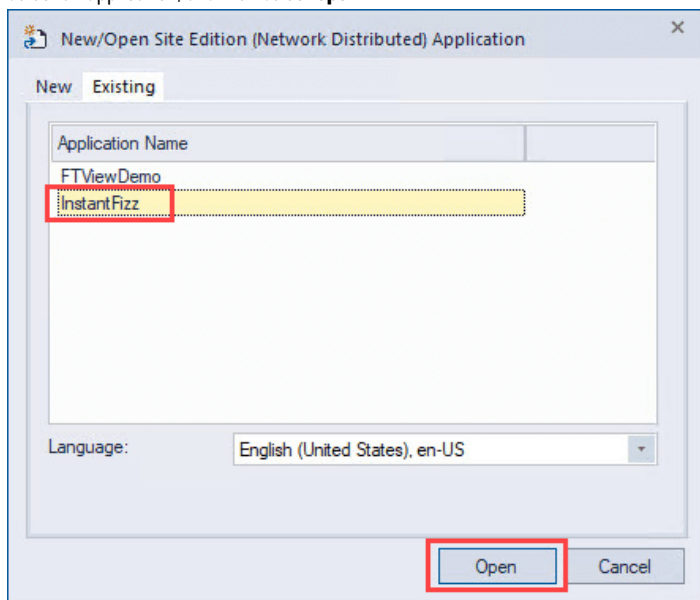
The following steps show how to disable a toggle button in a sample project InstantFizz with the **CurrentUserHasGroup** function.

### To secure runtime operations

1. Open FactoryTalk View Studio.
2. Select an application type, and then select **Continue**.

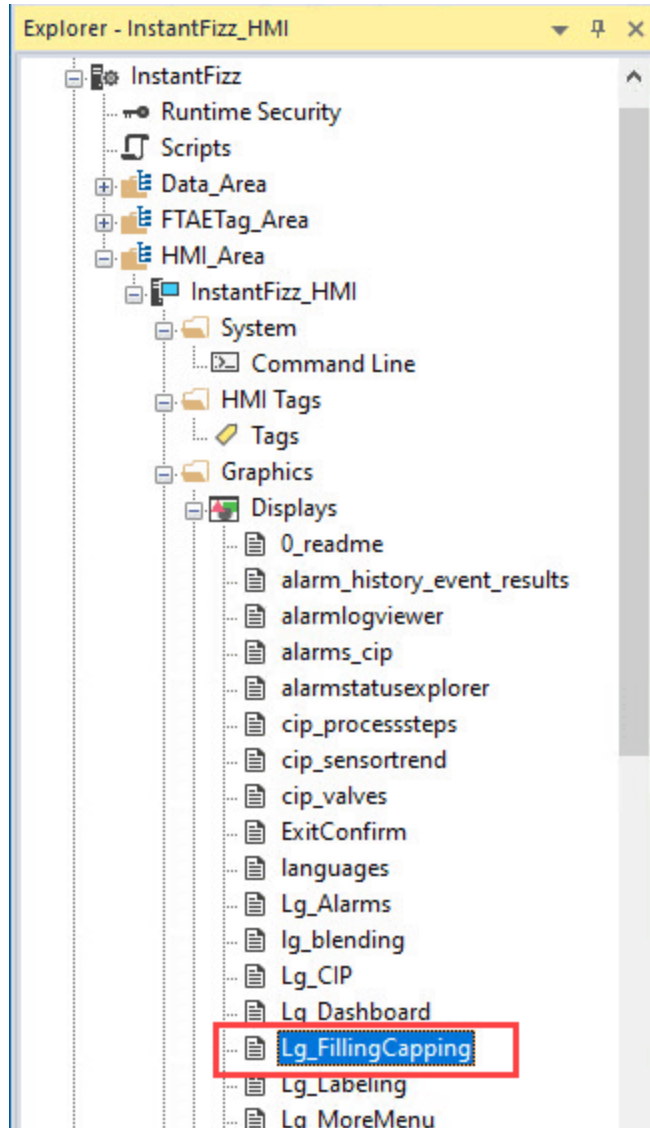


3. Select an application, and then select **Open**.

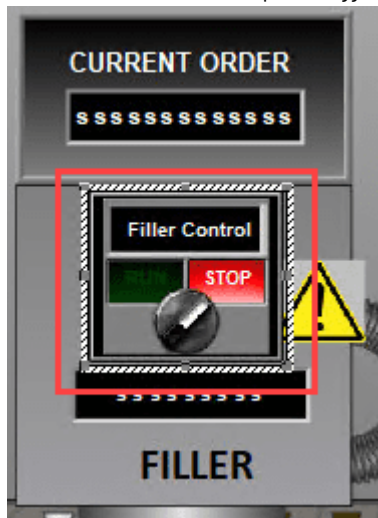


4. Select a display that contains the button you want to secure.

This example uses the **Lg-FillingCapping** display.

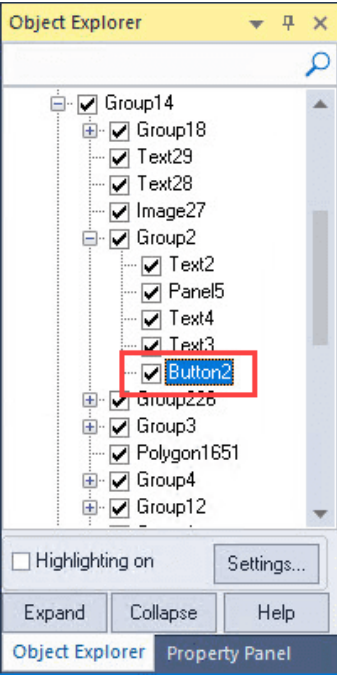


5. Double-click a button, for example the toggle button.

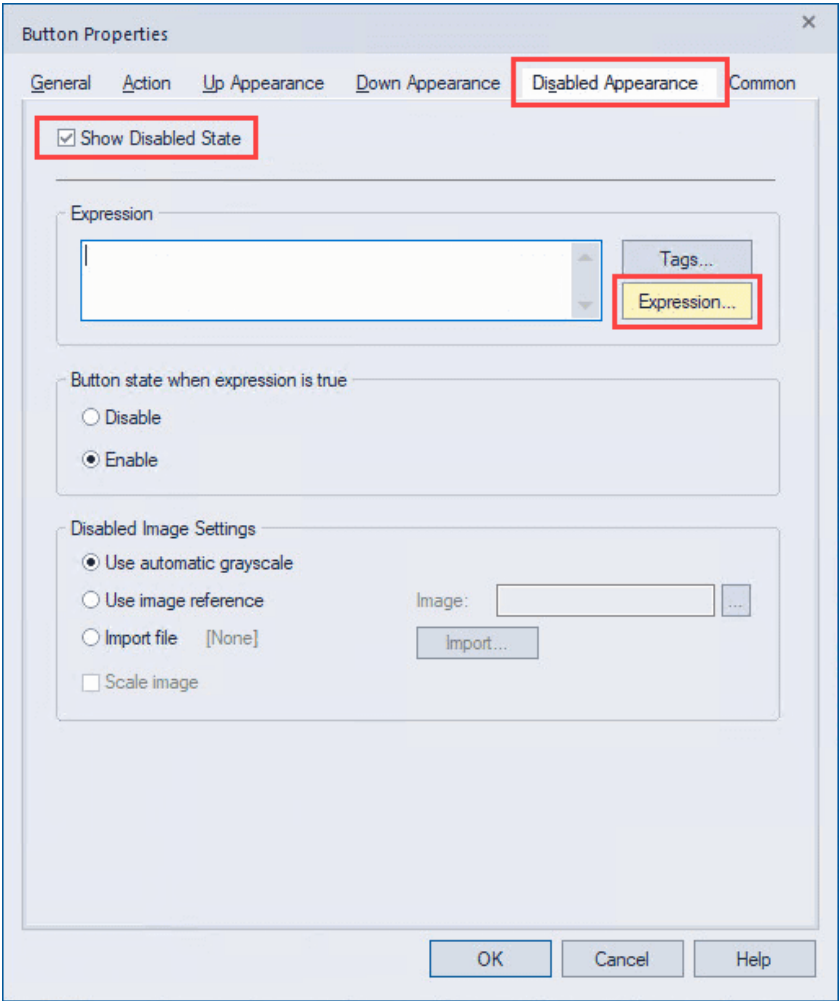




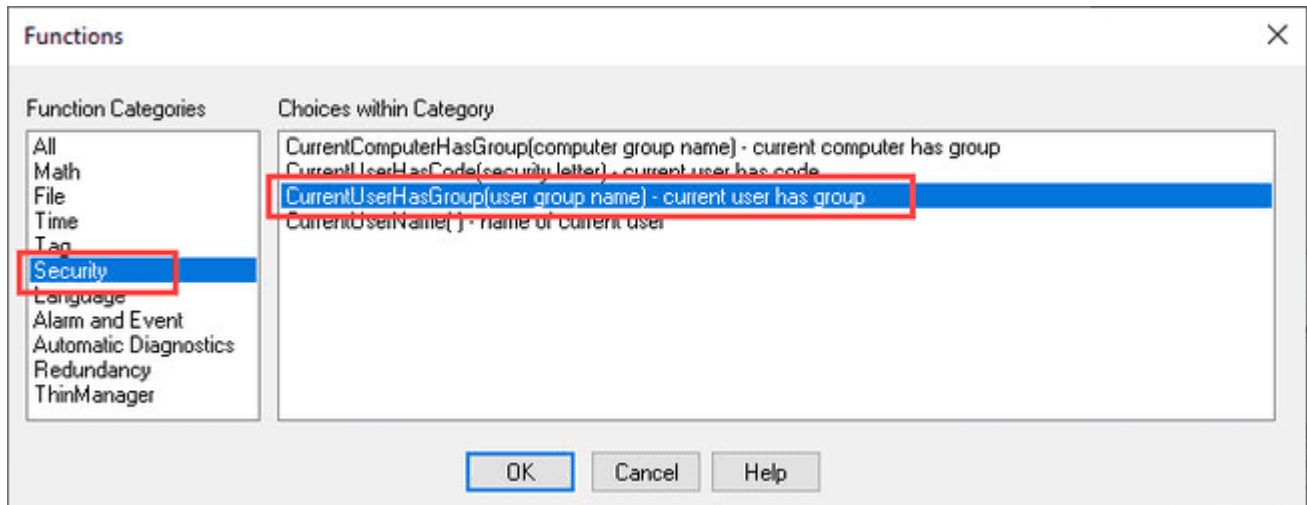
**Tip:** If you have trouble selecting an object on the display, select it in **Object Explorer**. For example, select this toggle button by selecting **Display > Group14 > Group2 > Button2**.



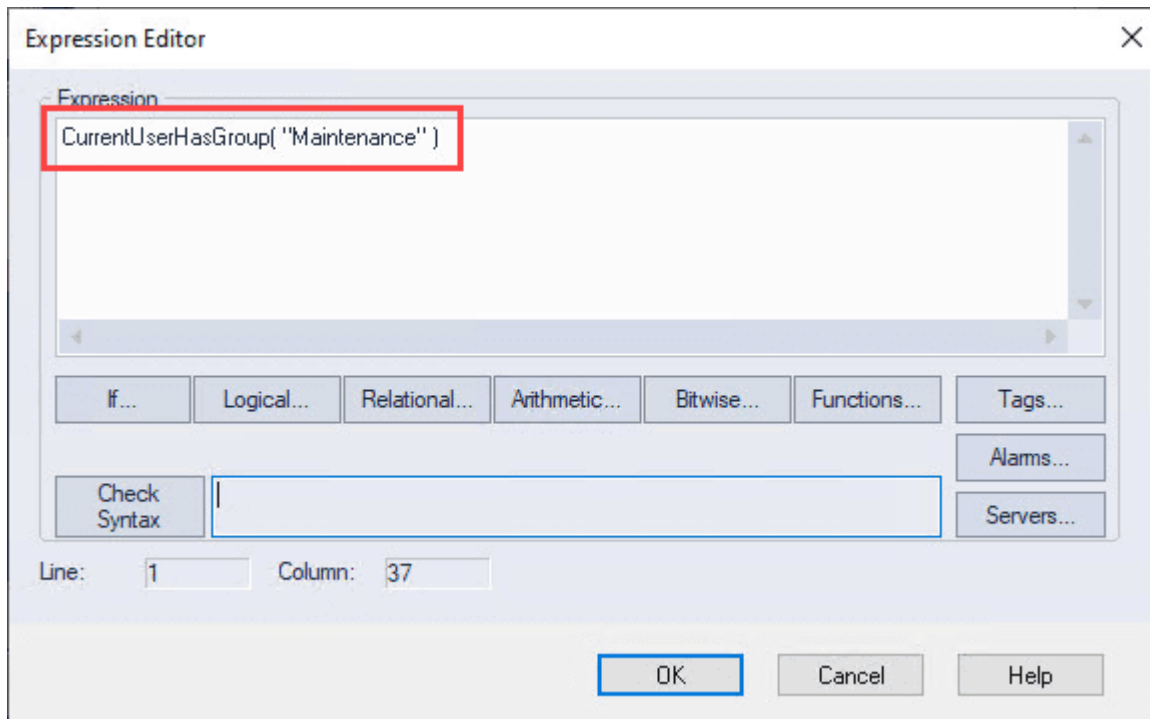
6. Select **Disabled Appearance > Show Disabled State > Expression**.



7. Select **Security > CurrentUserHasGroup(user group name)**.



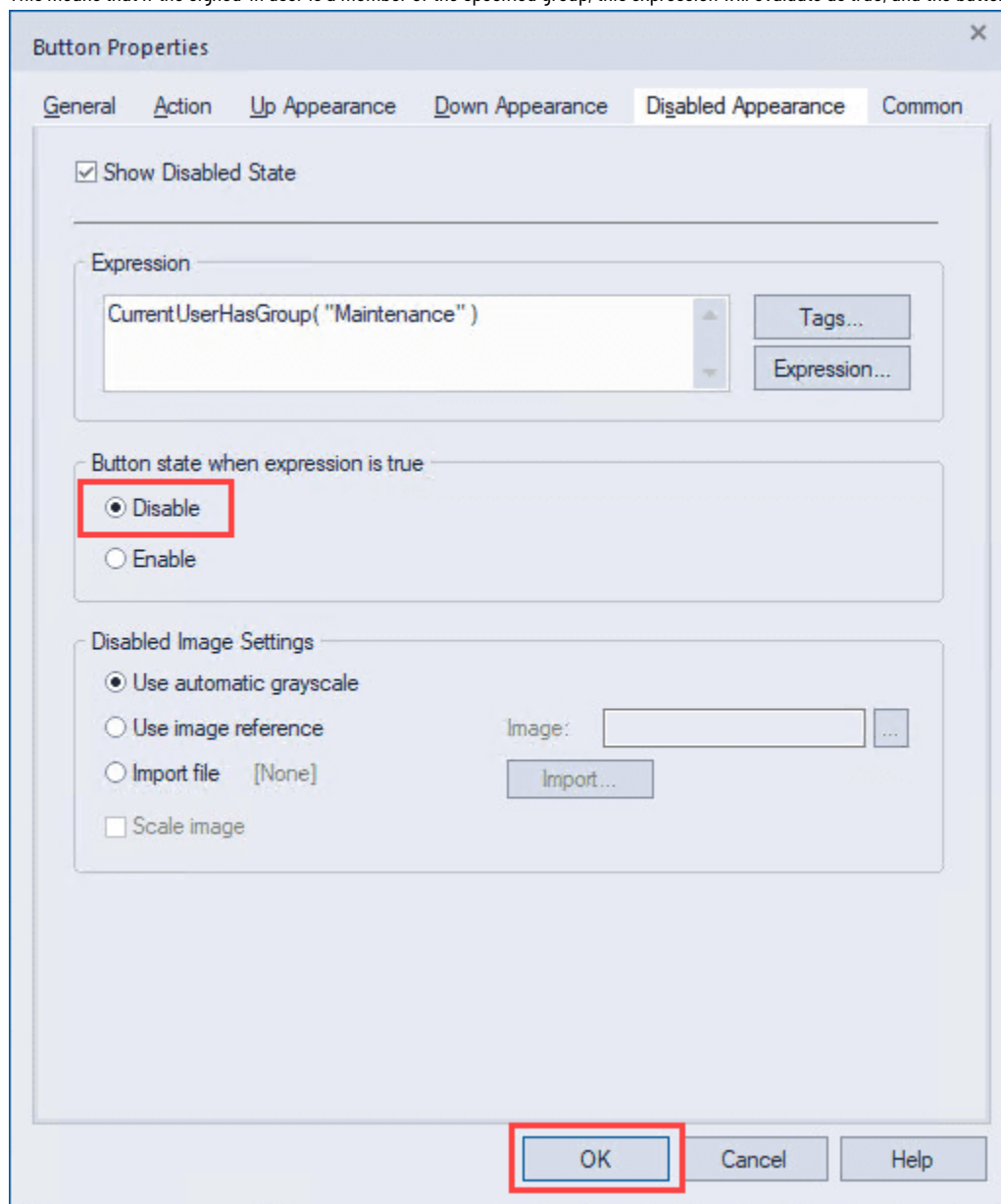
8. Select **OK**.
9. Between the parentheses, type a user group to whom the button will show as disabled.



10. Select **OK**.

11. Select **Disable**, and then select **OK**.

This means that if the signed-in user is a member of the specified group, this expression will evaluate as true, and the button will be disabled.



12. Close the **Lg-FillingCapping** display, and then select **Yes** to save the changes.

## Other ways to control runtime access to an application

To further restrict access to a FactoryTalk View SE application at runtime, you can:

- Lock operators into the runtime environment.
- Use electronic signature to control user actions.

## Lock operators into the runtime environment

To lock operators into the runtime environment, you can do one or more of the following:

- Limit the ability to manipulate graphic displays by removing the title bar or minimize and maximize buttons from selected displays.  
To do this, in the **Display Settings** dialog box, clear the **Title Bar**, **Minimize Button**, and **Maximize Button** checkboxes.
- Limit the ability to manipulate the client window by removing the title bar or minimize and maximize buttons from the client.

To do this, in the FactoryTalk View SE Client Wizard, clear the **Show title bar** and **Show system menu and close button** checkboxes.

- Prevent switching to other applications.

To do this, in the FactoryTalk View SE Client Wizard, select the **Disable switch to other applications** checkbox.

- Restrict access to the desktop with the Desklock tool.

To open Desklock, select **Start > Rockwell Software > DeskLock**.

## Use electronic signature to control user actions

To further secure commands, graphic objects, and tags, use built-in signature functions on the graphic objects or use the signature button. With electronic signature, you can control operator actions at runtime, such as:

- Setting the value of a tag.
- Running a command.
- Downloading values to controllers or devices.

## Securing FactoryTalk View with security codes

Security codes manage runtime security for HMI project components, including:

- Commands and macros
- Graphic displays
- OLE objects
- HMI tags

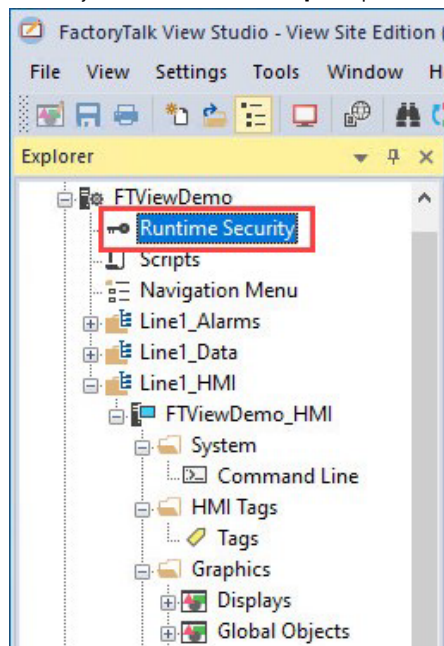
In FactoryTalk View Studio, you can secure access to HMI project components by assigning security codes (A - P) to user groups in the Runtime Security editor, to commands and macros in the Runtime Secured Commands editor, to graphic displays and OLE object animation in the Graphics editor, and to HMI tags in the Tags editor.

## Assign security codes to user groups

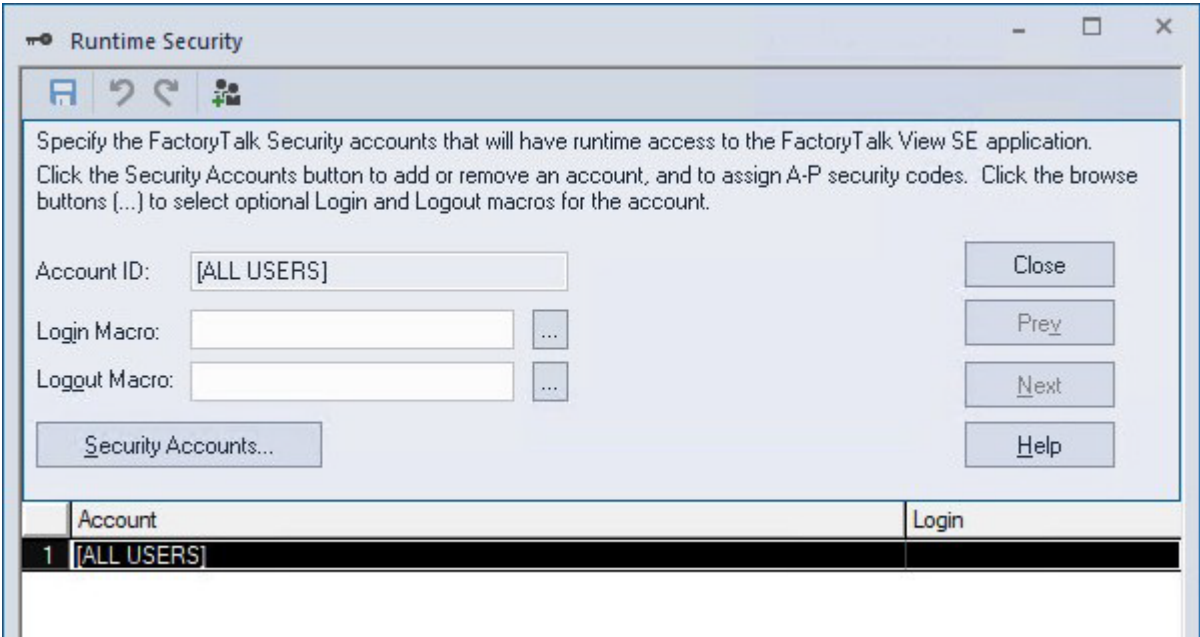
To achieve security with security codes, assign a security code to user groups and the HMI components. Only when the security code assigned to user groups matches the one assigned to the HMI component can the user groups have access to that HMI component.

### To assign security codes to a user group

1. In FactoryTalk View Studio, in the **Explorer** pane, double-click **Runtime Security**.

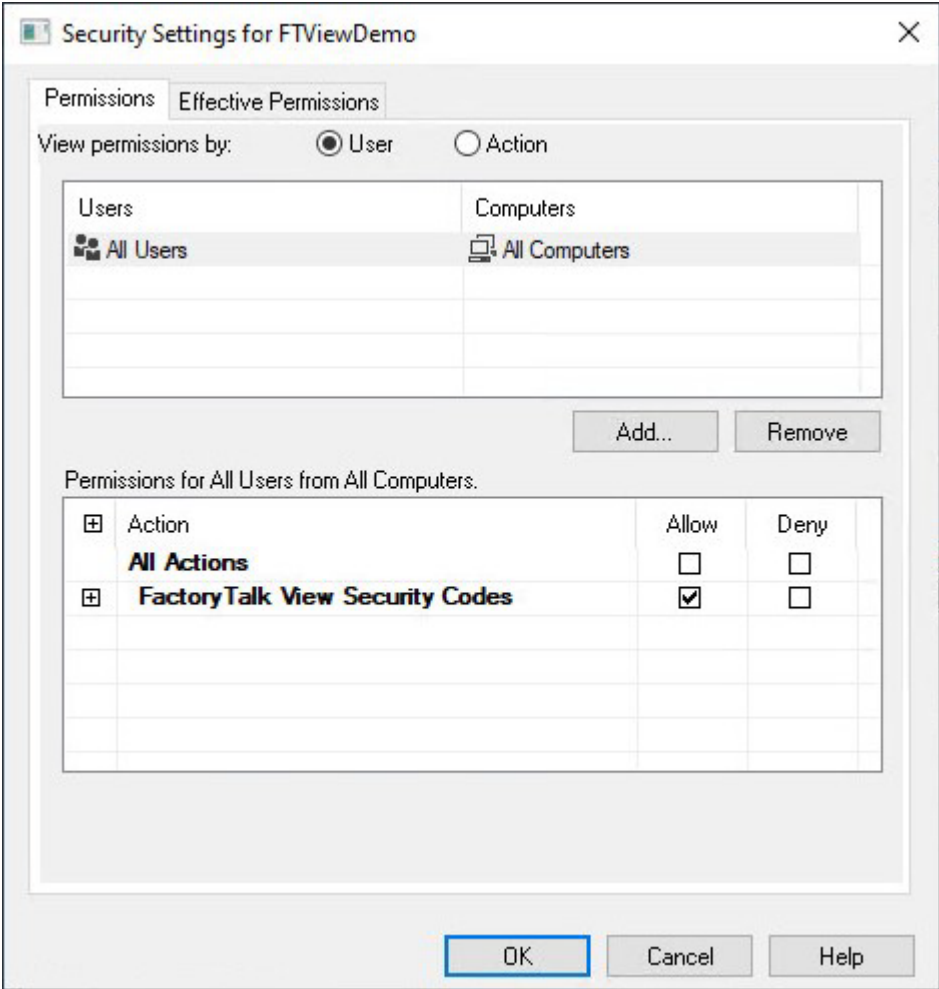


A list of all currently configured users appears in the lower pane.



- 2. To configure a new user, select 

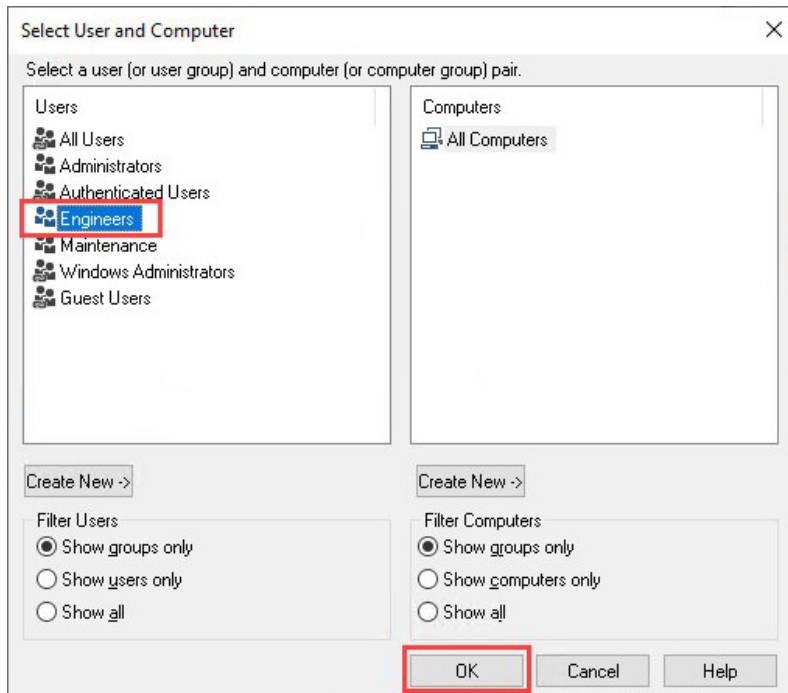
The **Security Settings** dialog box opens.



- 3. Select the **All Users** group, and then select **Remove**.
- 4. Select **Add**.

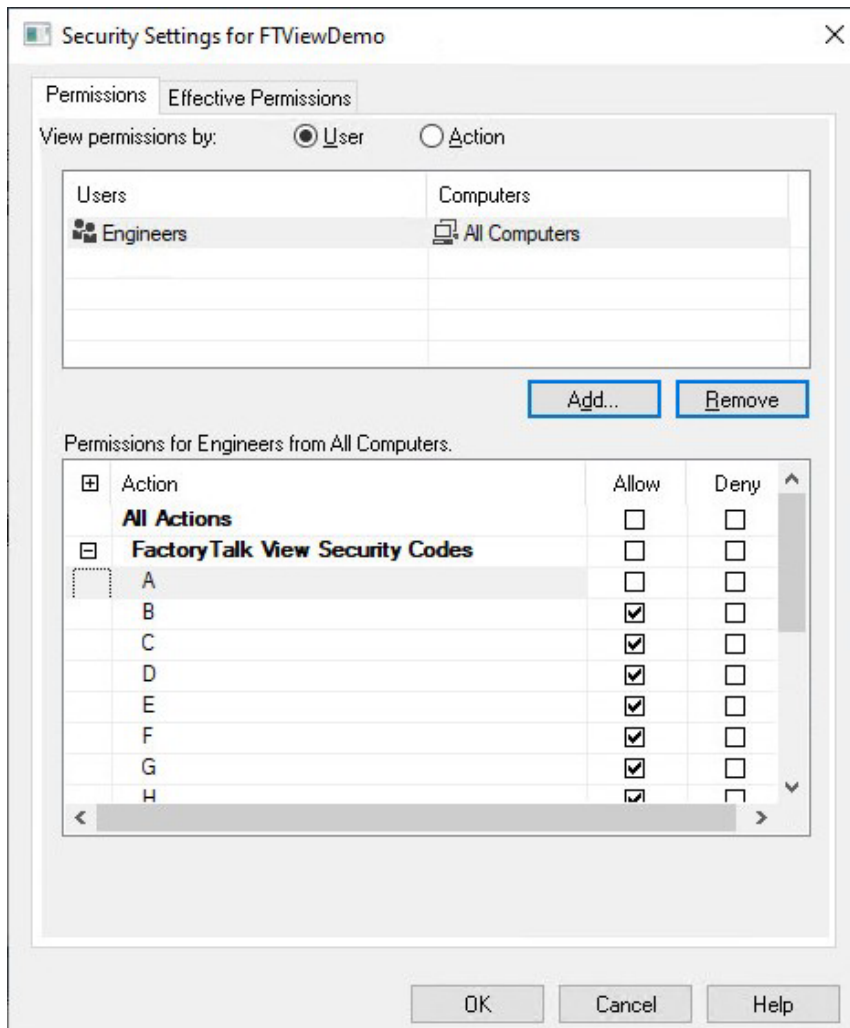


5. Select a user group (for example, **Engineers**), and then select **OK**.

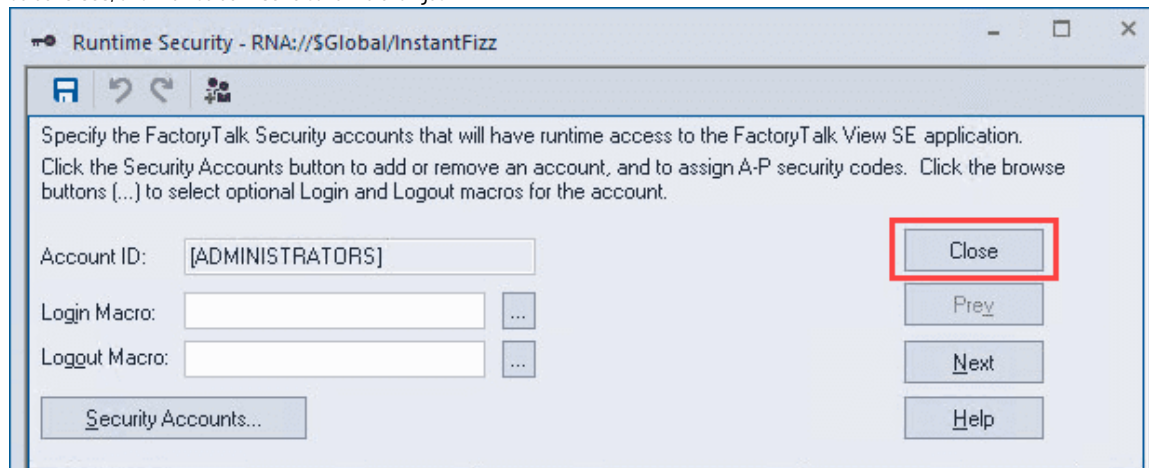


6. With the Engineers group selected, assign the security codes.

In this example, all security codes are set to **Allow** except for A. This means that the Engineers group will be denied access to HMI project components that are assigned with A.



7. Select **OK**.
8. Select **Close**, and then select **Yes** to save the changes.

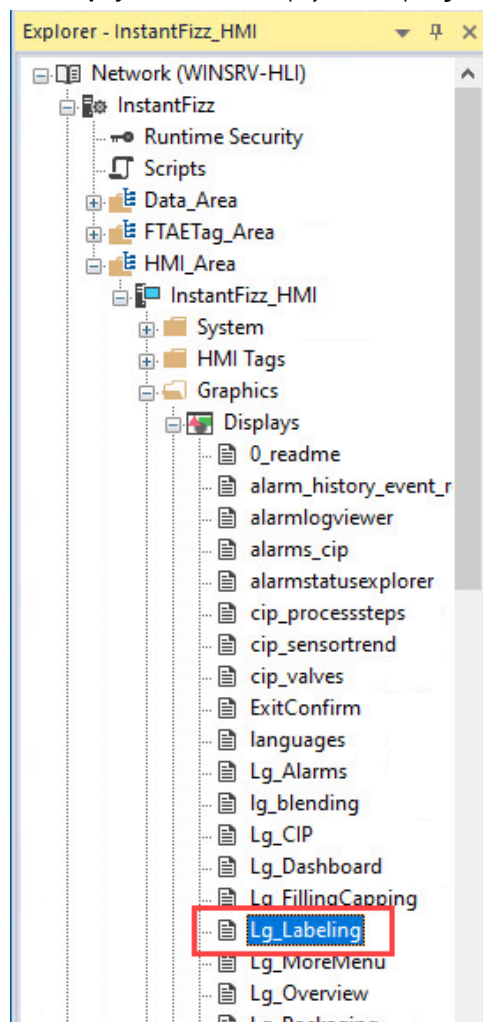


## Assign a security code to an HMI component

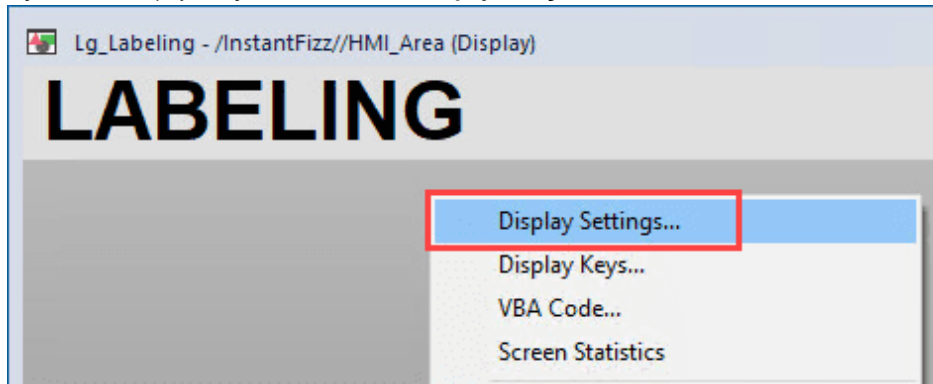
This section uses FactoryTalk View SE display security as an example. By assigning a security code to the display, only user groups that are assigned to that security code will be able to access that display.

### To assign a security code to an HMI component

1. Under **Displays**, double-click a display, for example **Lg\_Labeling**.

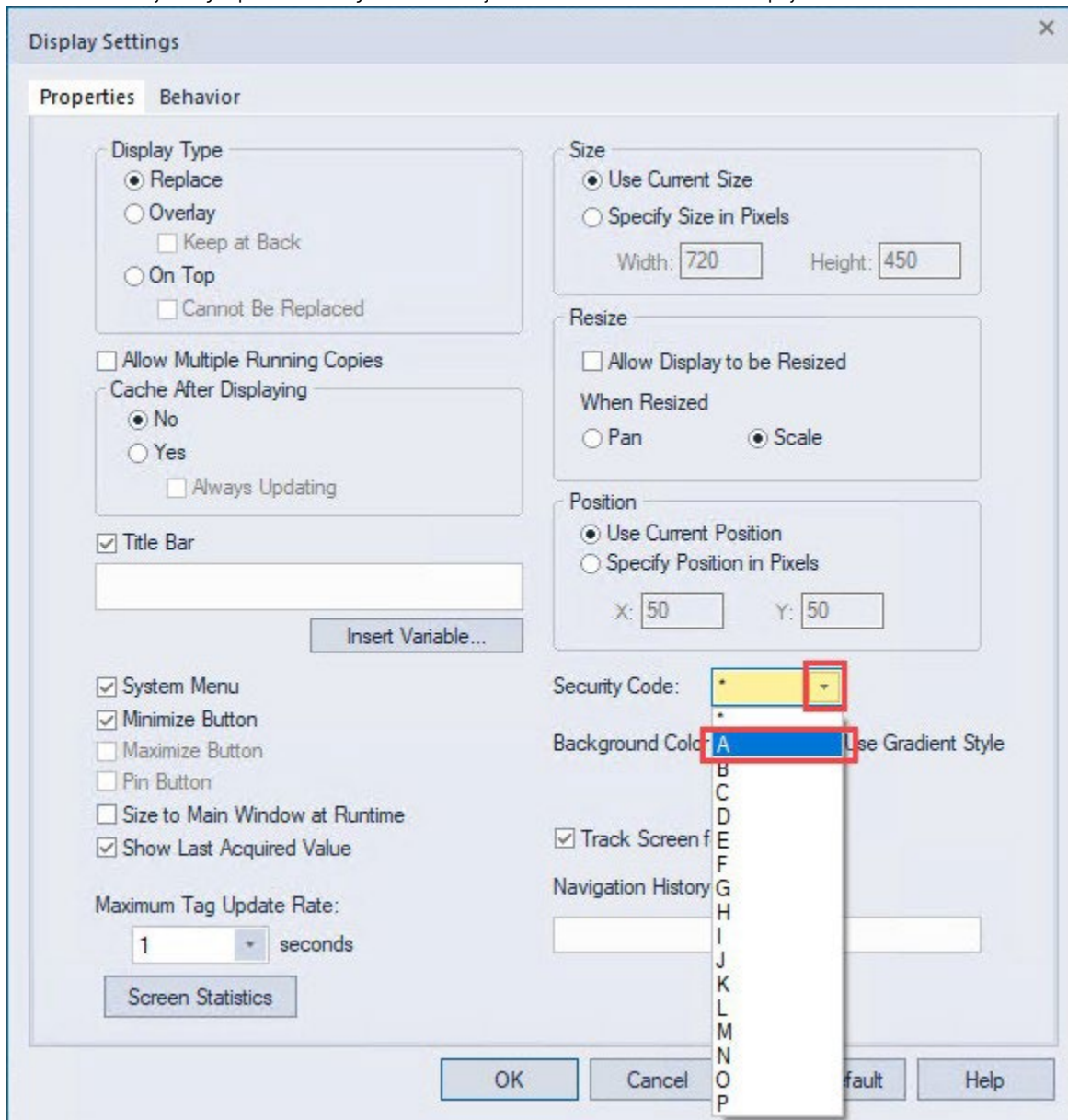


2. Right-click the display background, and then select **Display Settings**.



3. Change the **Security Code** to **A**.

This means that only user groups that are assigned with security code A will be able to access this display.



4. Select **OK**.
5. Close the display, and then select **Yes** to save the changes.

## Specific functions that need to be secured

This section explains some specific functions of FactoryTalk View SE that may need to be secured. These configurations are not mandatory but should be considered to achieve a higher level of security.

### Server side script

Server side scripts are graphic-independent and all HMI servers share script files under the same application. Because the script runs on the HMI server that triggered the script, you may want to consider:

- Who can configure the script at design time.
- Who can run the ScriptExecute command that triggers the script.

To decide who can configure the script at design time, secure the resources in the explorer of FactoryTalk View Studio with common actions such as Write or List Children.

To secure the ScriptExecute command at runtime, do one of the following:

- Configure the disabled state or visibility of the button that triggers the ScriptExecute command, so that the button is only visible or enabled to user groups that are allowed to run the command.
- Assign a security code to the ScriptExecute command via **Settings > Runtime Secured Commands** in FactoryTalk View Studio, so that only user groups with the same security code are allowed to run the command.

### HMI projects folder

By default, all HMI server projects are saved in the **HMI projects** folder on the HMI server computer located at C:\Users\Public\Documents\RSView Enterprise\SE\HMI projects. To enhance security and prevent unauthorized modifications to these projects, you can tighten the Windows folder's security settings on the HMI server computer by following these steps:

- Remove the **INTERACTIVE** group from the folder's security properties.
- Assign read-only permissions of this folder to dedicated users or user groups.

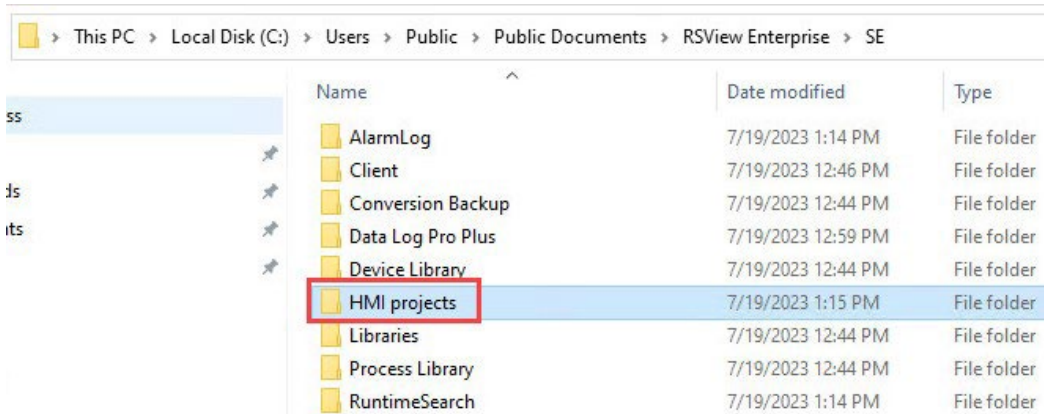
If you assign read-only permission to those users or user groups, they can only view and will not be able to write to project files. Users with read-only permission can still test run and run the FactoryTalk View SE client.

### Remove the INTERACTIVE group

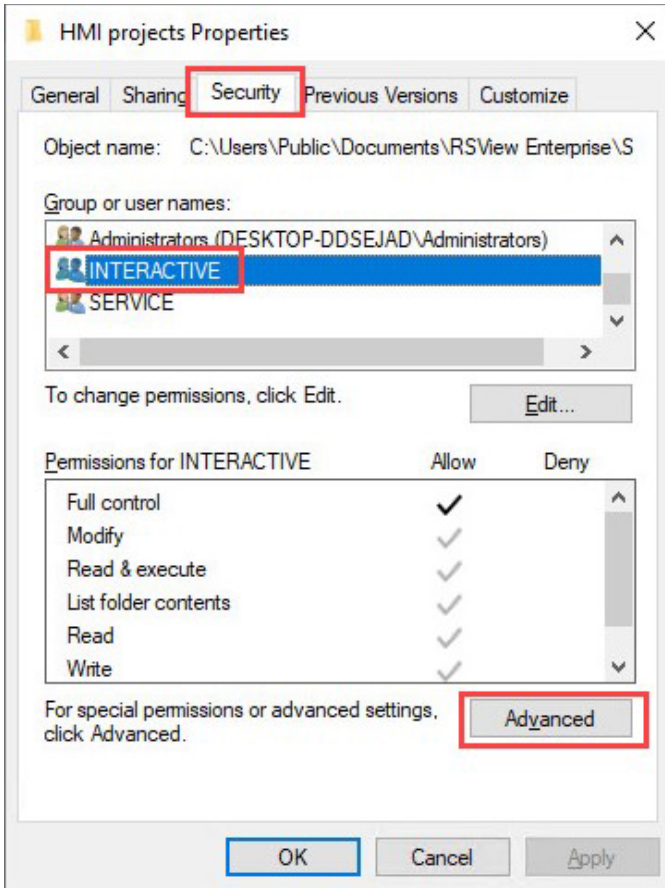
You must disable its permission inheritance first, and then remove the **INTERACTIVE** group.

#### To remove the INTERACTIVE group

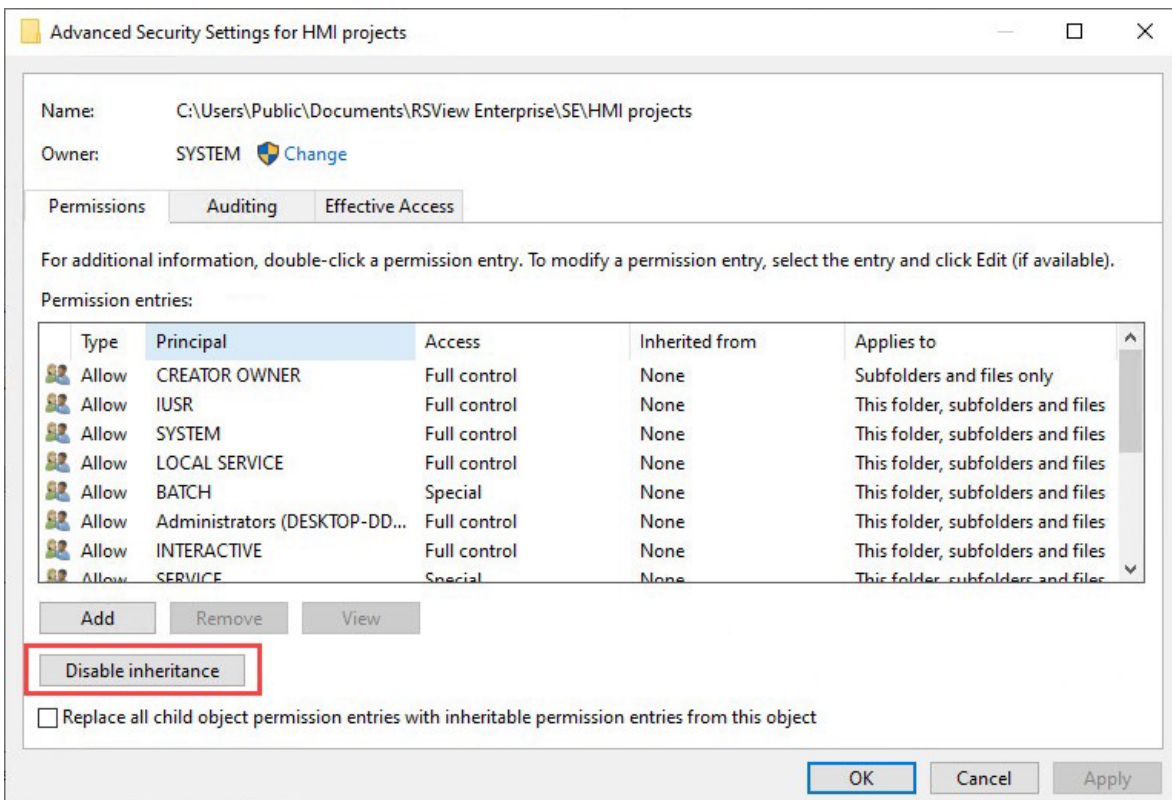
1. Go to C:\Users\Public\Documents\RSView Enterprise\SE.



2. Right-click the **HMI projects** folder, and then select **Properties**.
3. Disable the **HMI projects** folder's permission inheritance.
  - a. Select the **Security** tab, select the **INTERACTIVE** group, and then select **Advanced**.

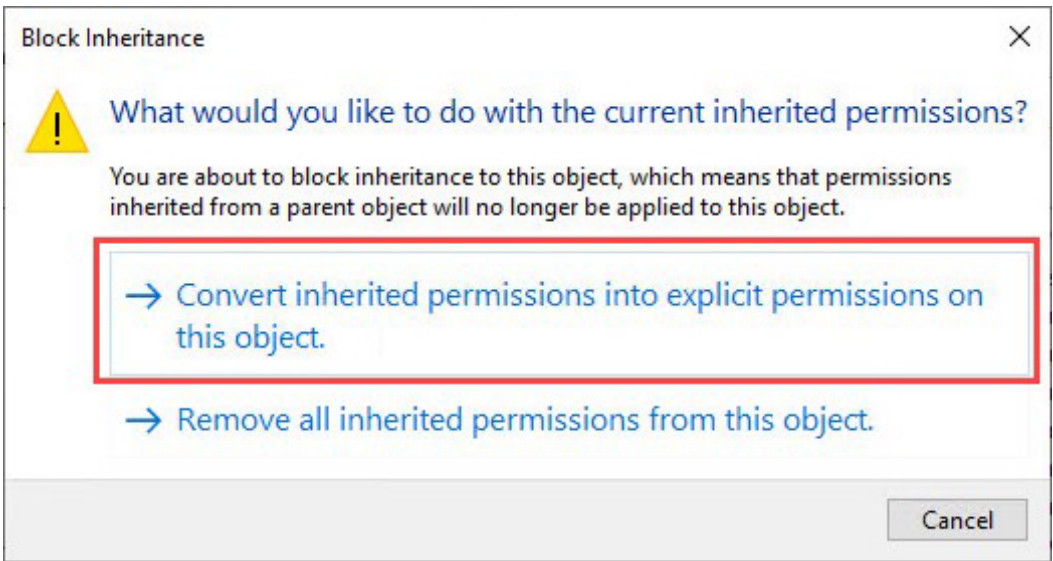


- b. Select **Disable inheritance**.

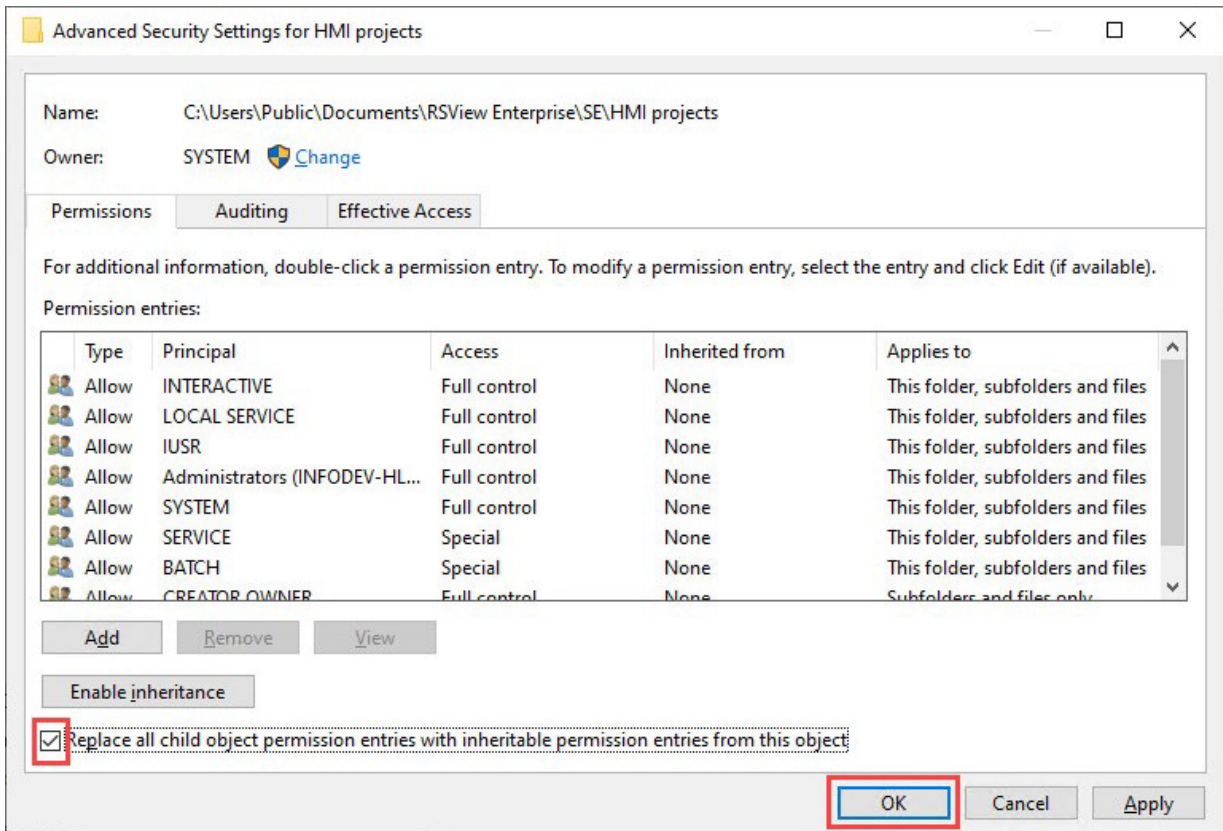




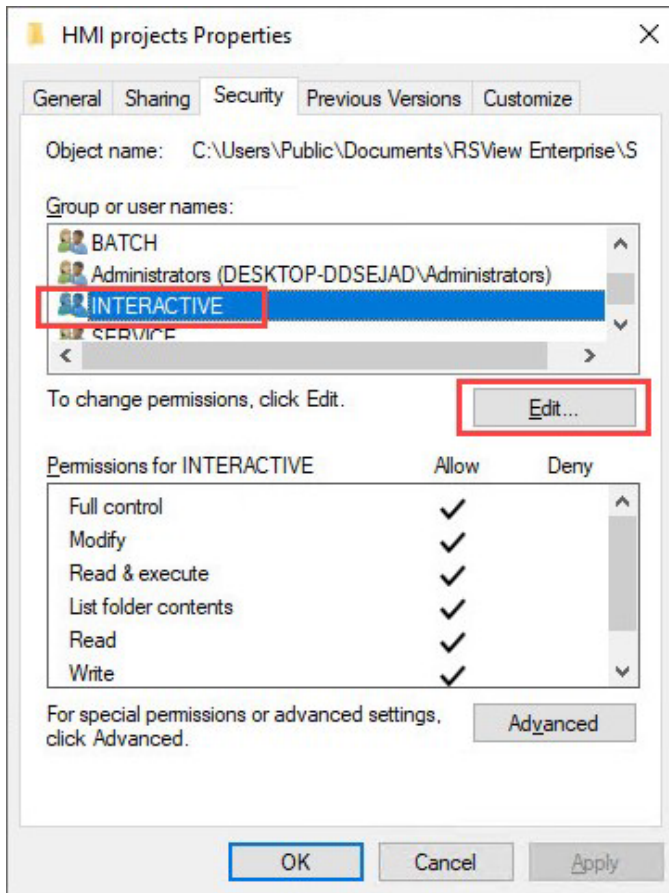
- c. Select **Convert inherited permissions into explicit permissions on this object**.



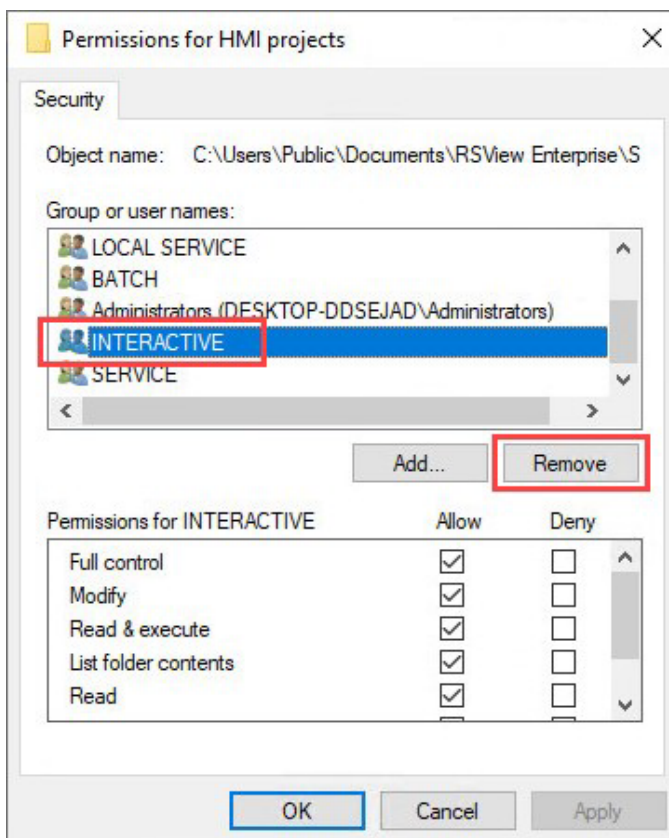
- d. Select **Replace all child object permission entries with inheritable permission entries from this object**, and then select **OK**.



4. Remove the **INTERACTIVE** group.
  - a. Make sure that INTERACTIVE is selected, and then select **Edit**.

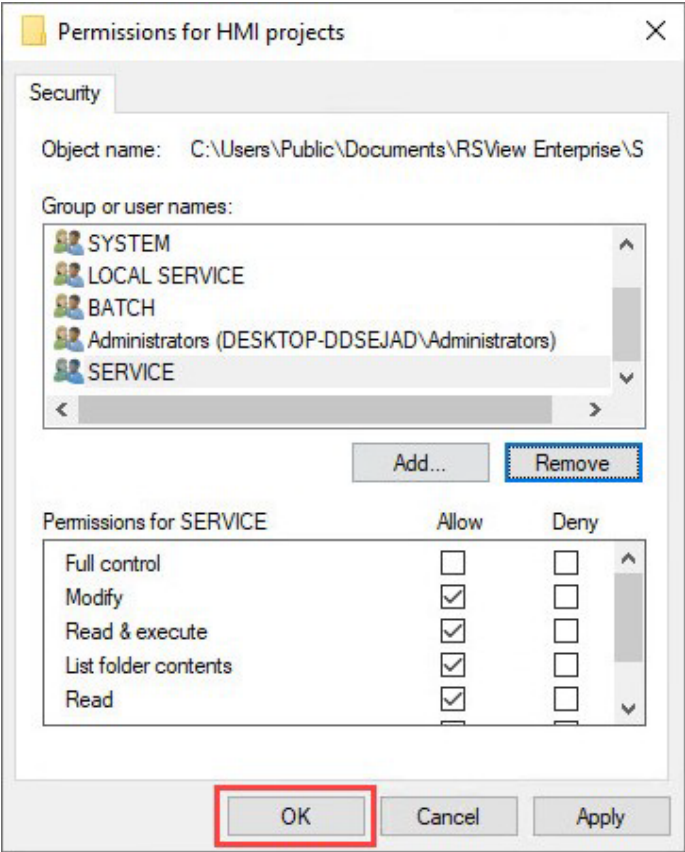


- b. Select **INTERACTIVE**, and then select **Remove**.

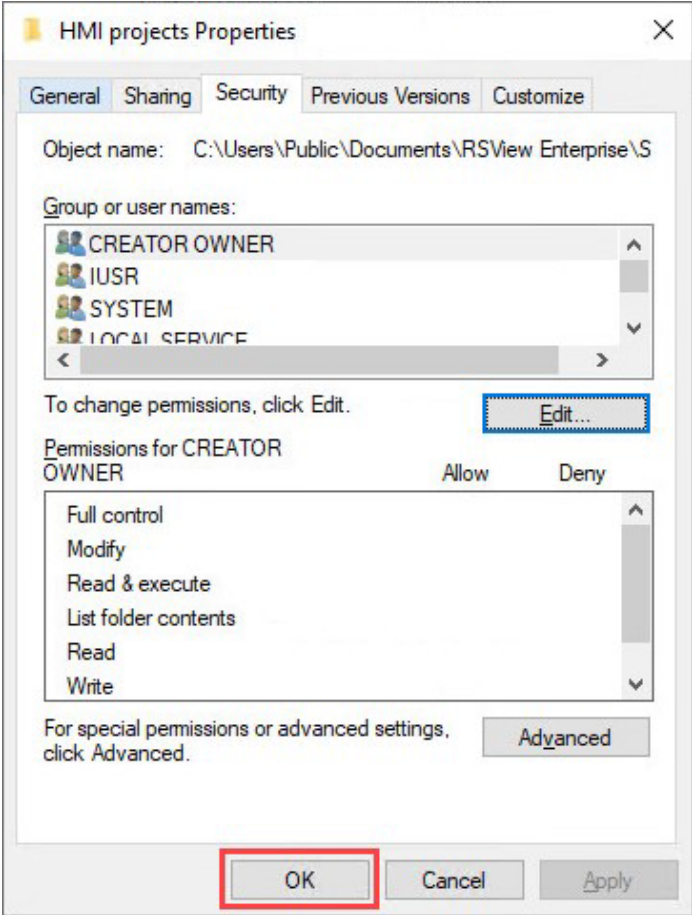




c. Select **OK**.



5. Select **OK**.

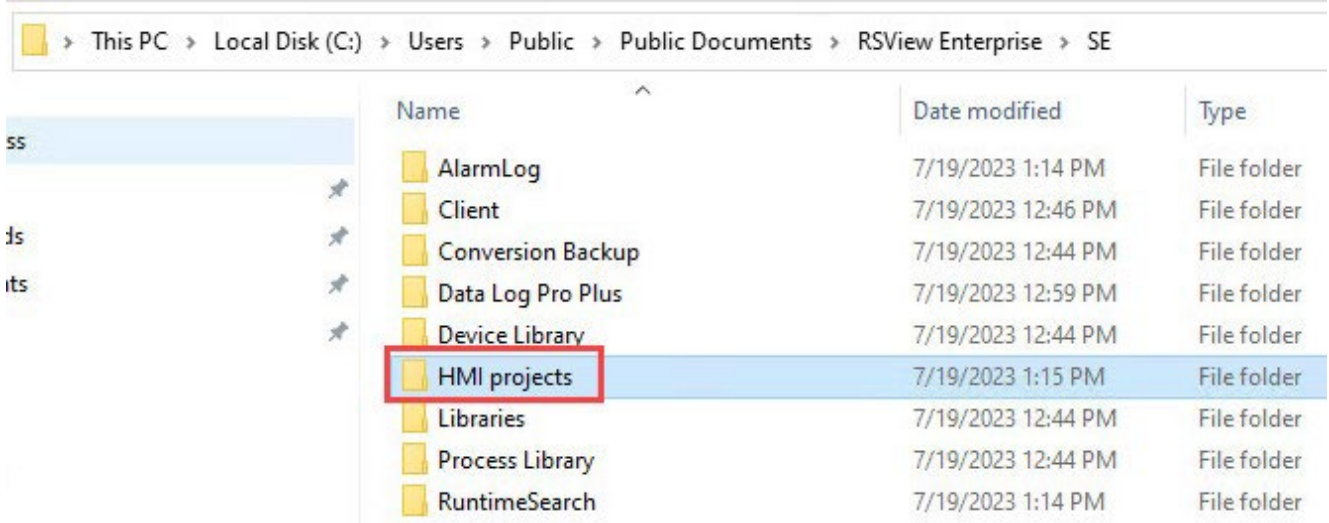


## Assign permissions of this folder to dedicated user or user groups

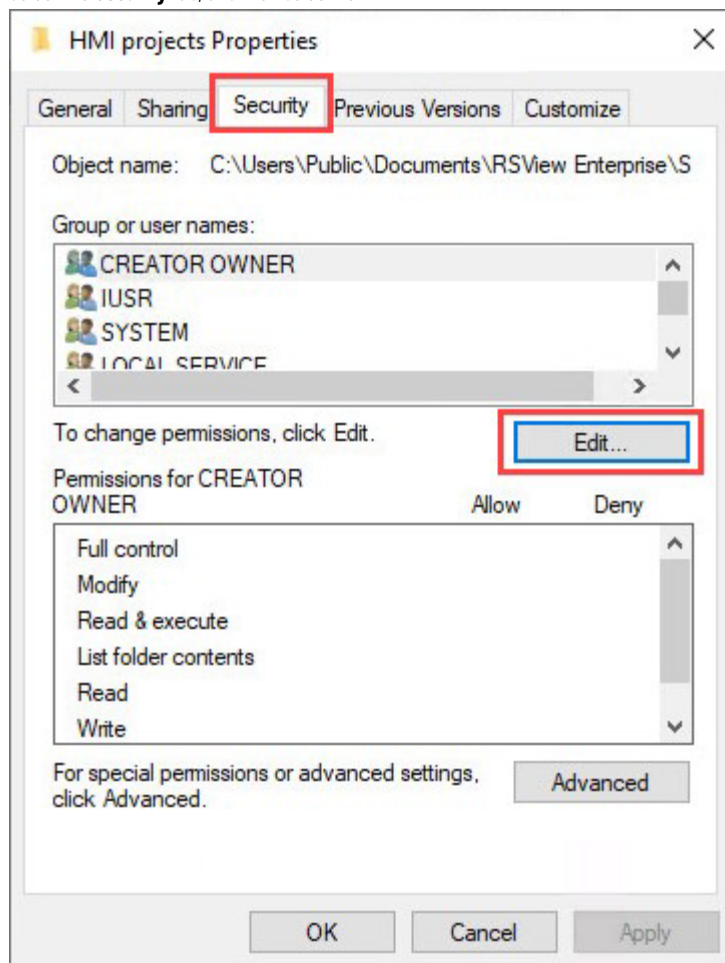
After removing the **INTERACTIVE** group, assign specific users or user groups, and then assign this folder's permissions to those users or user groups. The following steps use a new user UserA as an example.

### To assign permissions of this folder to dedicated user or user groups

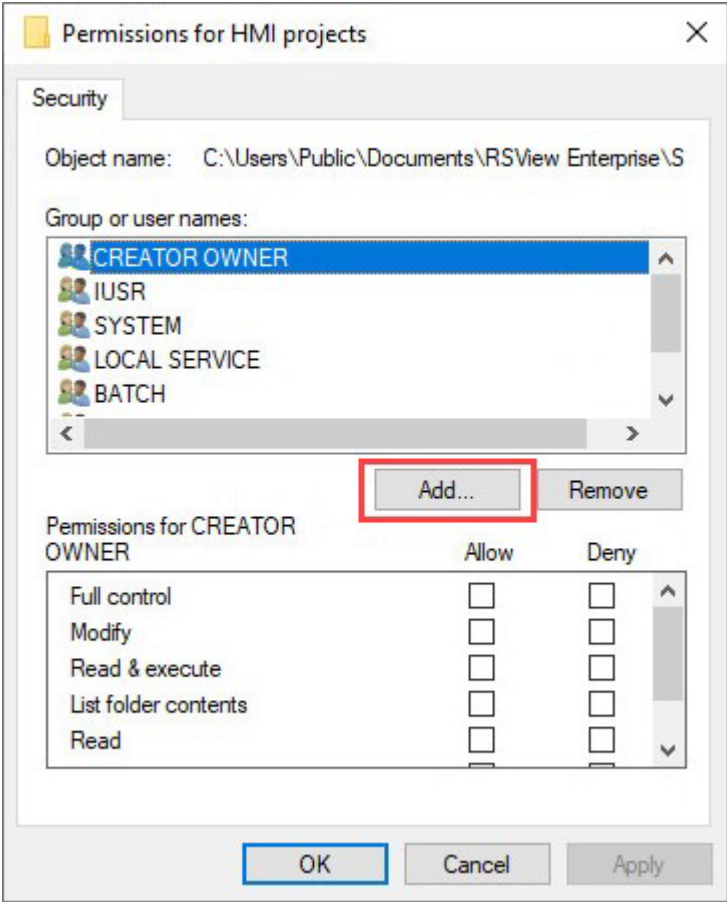
1. Go to C:\Users\Public\Documents\RSView Enterprise\SE.



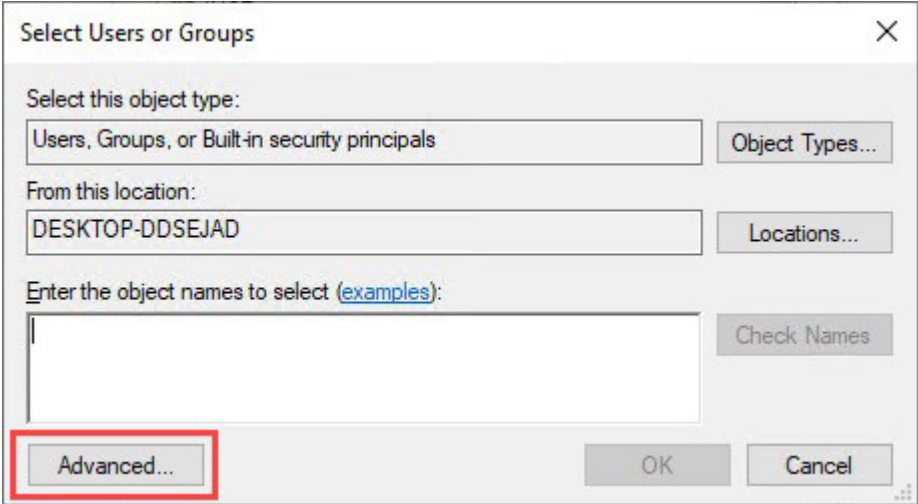
2. Right-click the **HMI projects** folder, and then select **Properties**.
3. Select the **Security** tab, and then select **Edit**.



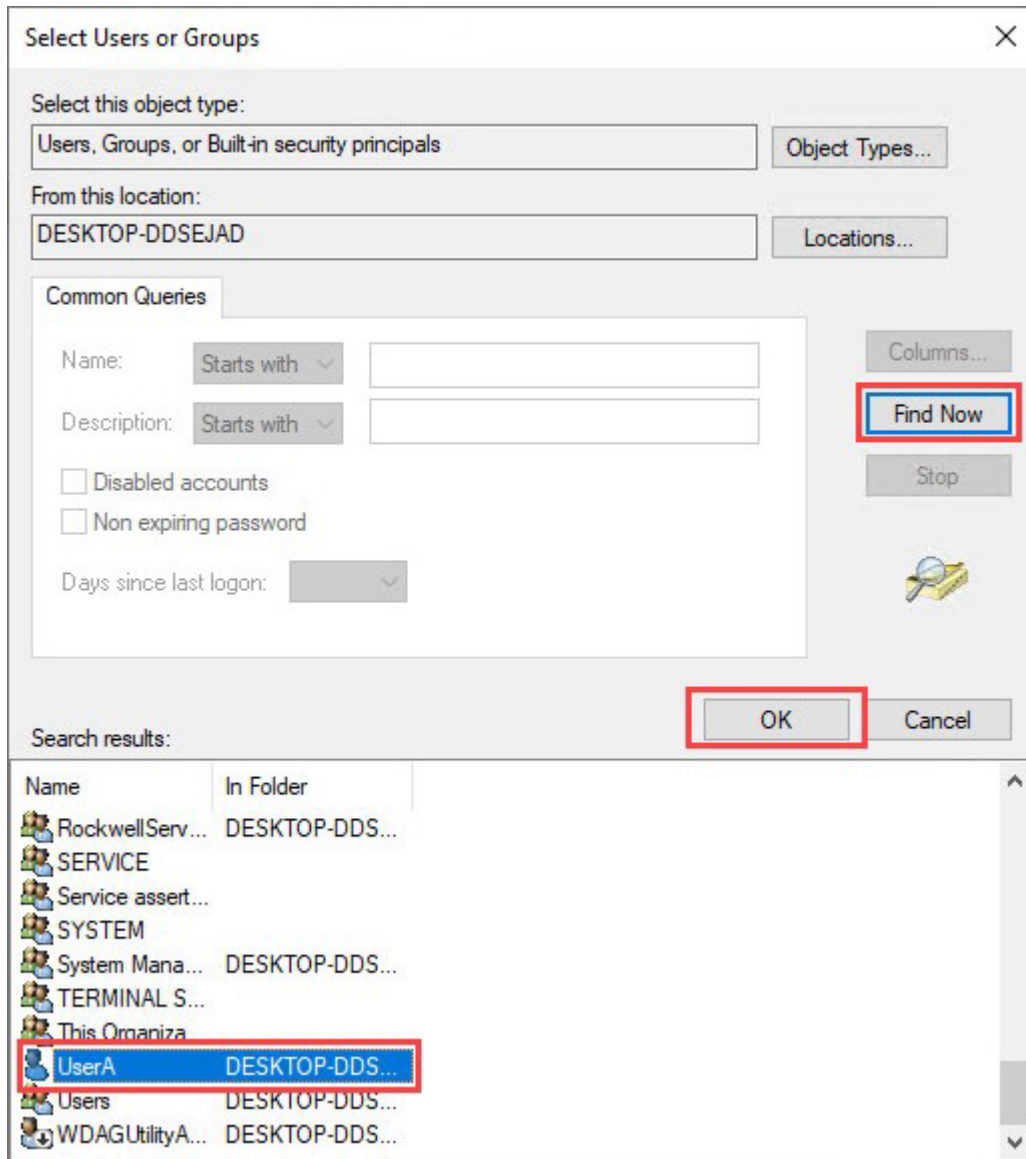
4. Select **Add**.



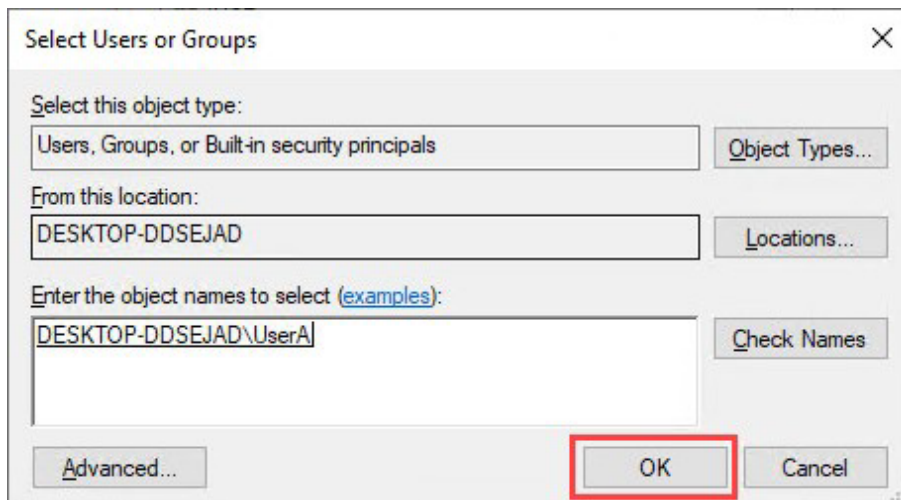
5. Select **Advanced**.



6. Select **Find Now**, select the user you want to add, for example UserA, and then select **OK**.

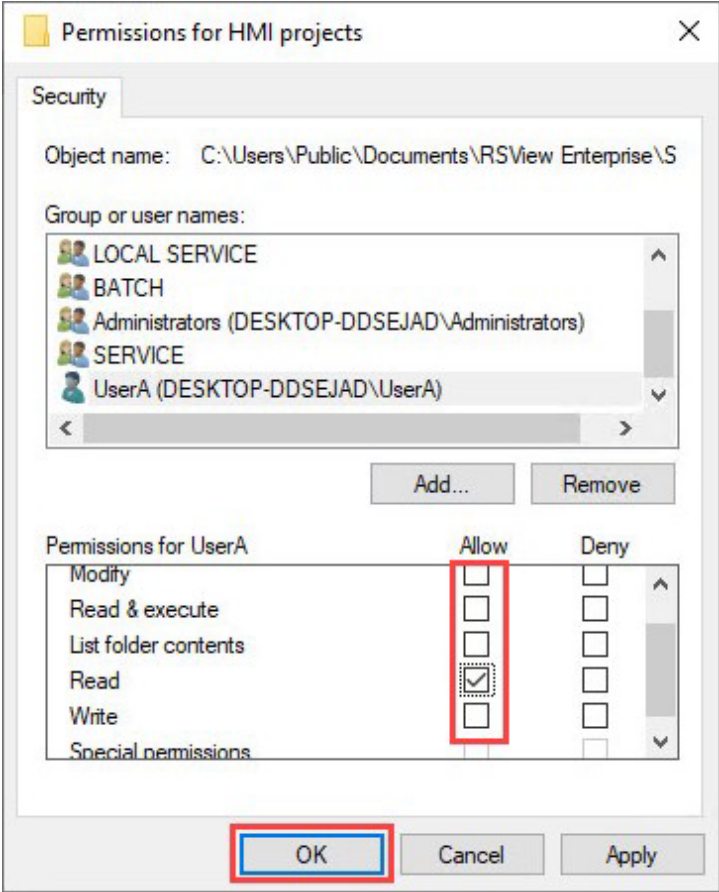


7. Select **OK**.



- 8. Clear the checkboxes for write permissions as needed, and then select **OK**.

In this example, UserA has the read-only permission. This user can test run and run the FactoryTalk View SE client.



## Secure application data in FactoryTalk AssetCentre

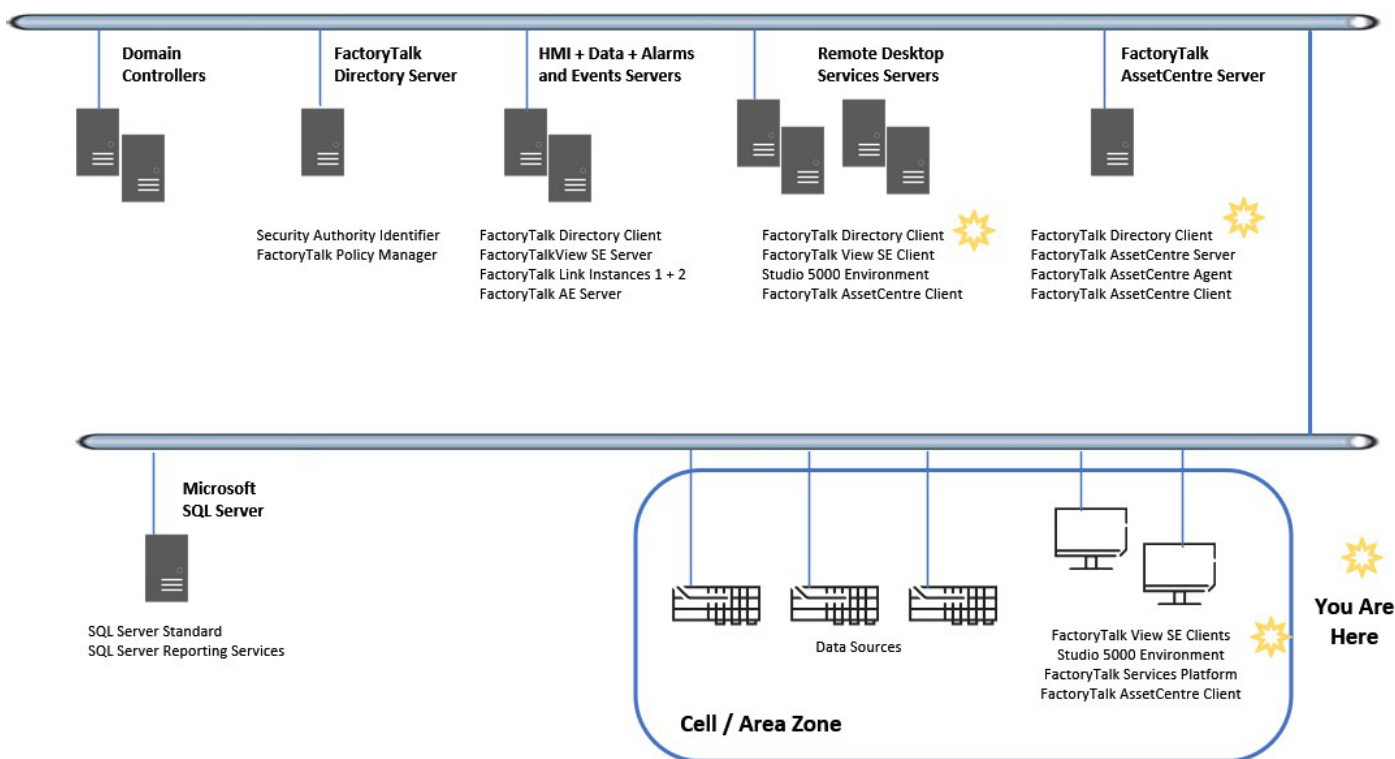
FactoryTalk AssetCentre monitors your factory automation system and provides centralized tools to minimize downtime due to unauthorized actions or failing devices.

For more information on configuring FactoryTalk AssetCentre, see *FactoryTalk AssetCentre Getting Results Guide* listed in [Additional Resources on page 4](#).



**Tip:** For information about deploying FactoryTalk software products on a network secured by IPSec, see the Knowledgebase Document ID: [QA46277 - Deploying FactoryTalk Software with IPSec](#).

### Manufacturing Zone



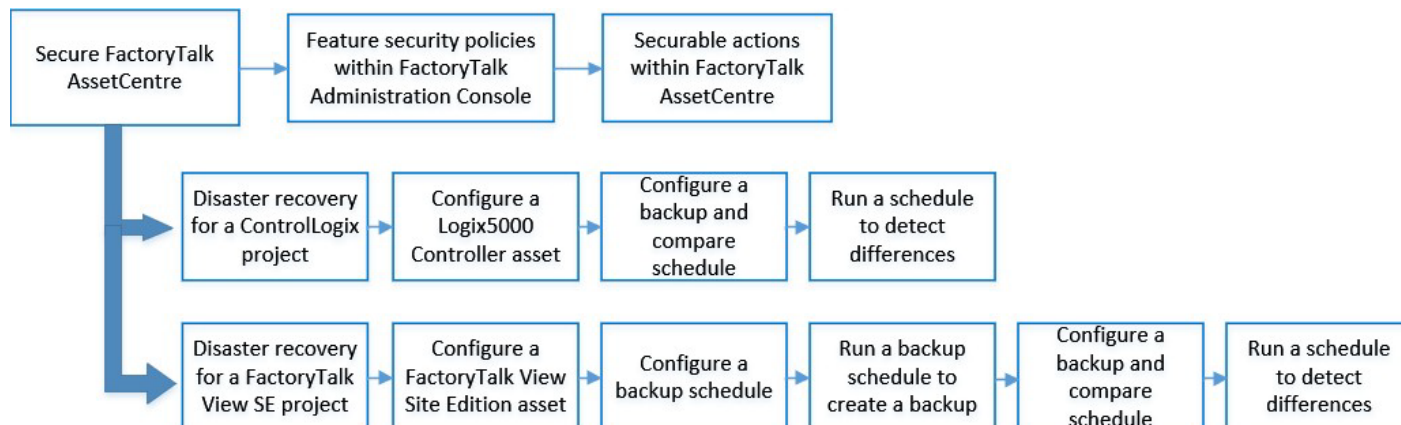
### Before you begin

The instructions in this chapter use the following software as examples. The steps or look of your software may vary.

- FactoryTalk AssetCentre version 13.00.00
- Studio 5000 Logix Designer version 34.00.00
- FactoryTalk Services Platform version 6.40.00
- FactoryTalk View SE version 14.00.00
- Microsoft SQL Server 2019



## Workflow



## Secure FactoryTalk AssetCentre

By default, all users in the FactoryTalk Directory can perform any task in FactoryTalk AssetCentre. Secure FactoryTalk AssetCentre by managing user permissions in:

- [To configure feature security policies in FactoryTalk Administration Console on page 88](#)
- [To configure securable actions in FactoryTalk AssetCentre on page 91](#)

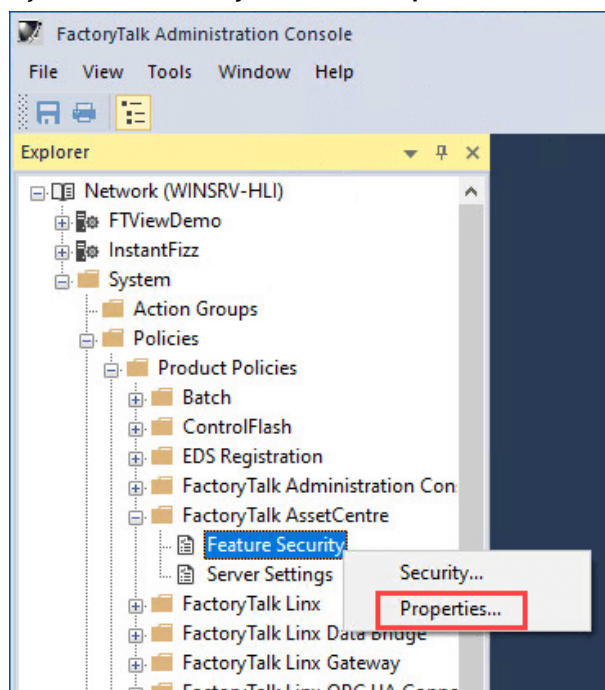
## Configure feature security policies in FactoryTalk Administration Console

Feature security policies determine who can perform certain operations within the FactoryTalk AssetCentre system. Configure feature security to limit which users can perform specific operations (especially those that may impact the system) such as **Switch to Design mode**, **View Audit Log**, and **Run Archive Database Cleanup Wizard**.

Feature security policies apply across the entire FactoryTalk AssetCentre configuration. In FactoryTalk Administration Console, you can select each policy to view the text explaining what each policy is for. For a complete list and their explanations, see [Product policies and securable actions of FactoryTalk AssetCentre on page 124](#).

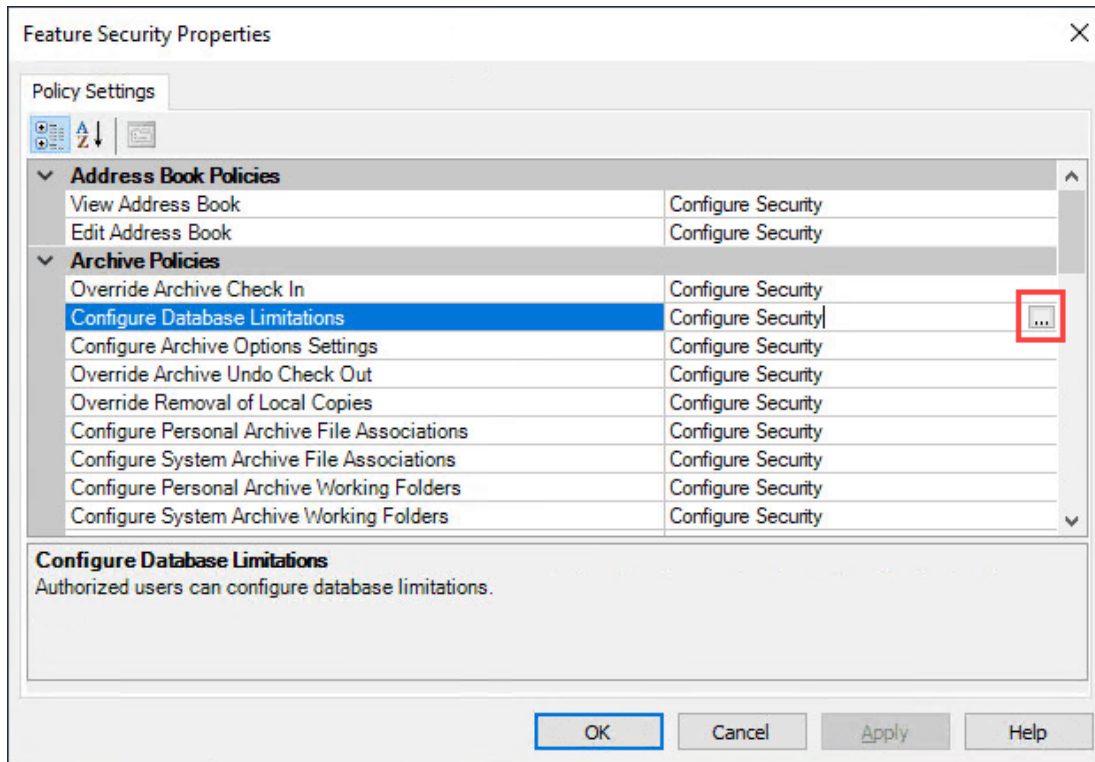
### To configure feature security policies in FactoryTalk Administration Console

1. In FactoryTalk Administration Console, go to **System > Policies > Product Policies > FactoryTalk AssetCentre**.
2. Right-click **Feature Security**, and then select **Properties**.

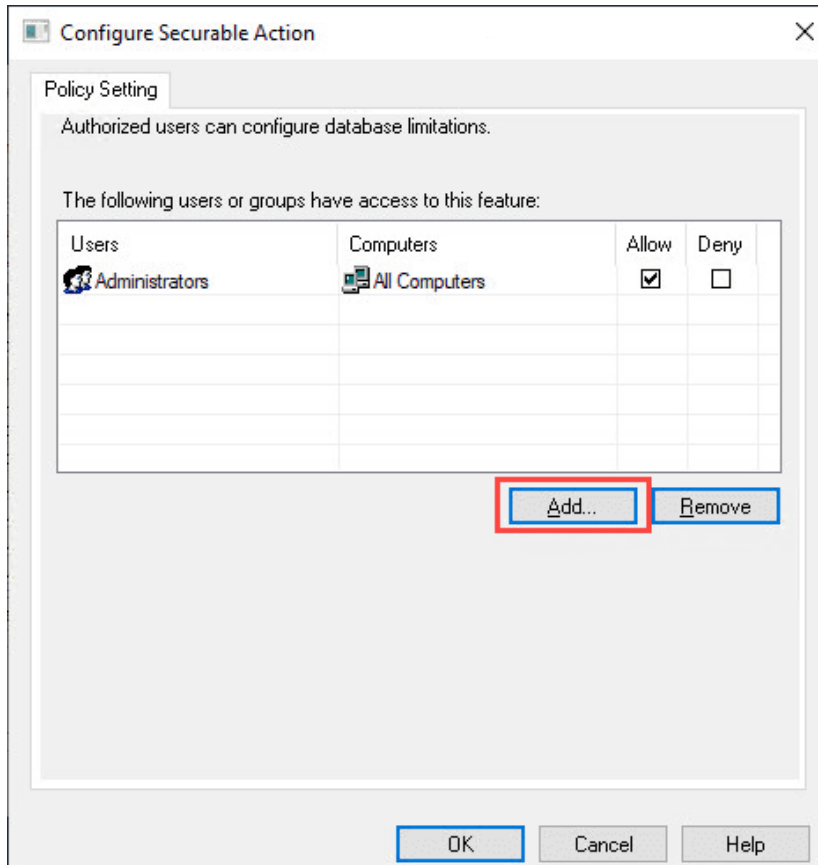




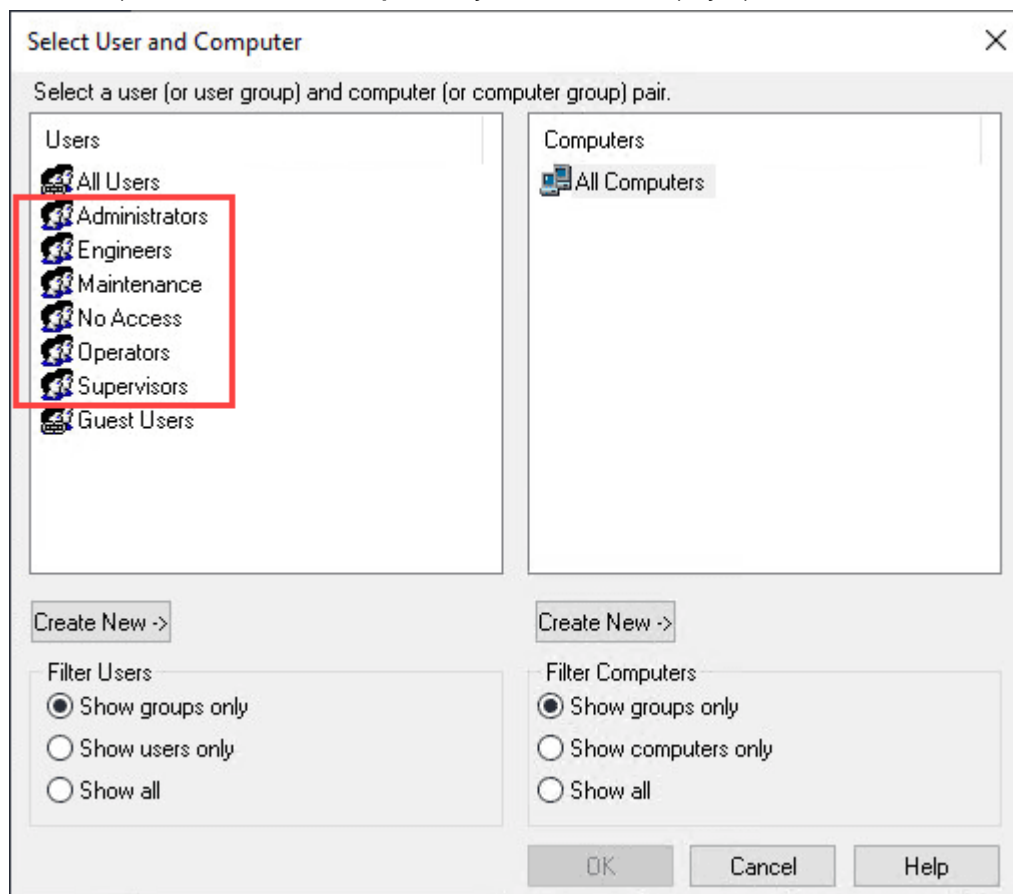
3. In the **Feature Security Properties** dialog box, choose the desired policy, and then select the browse button to the right of **Configure Security**.



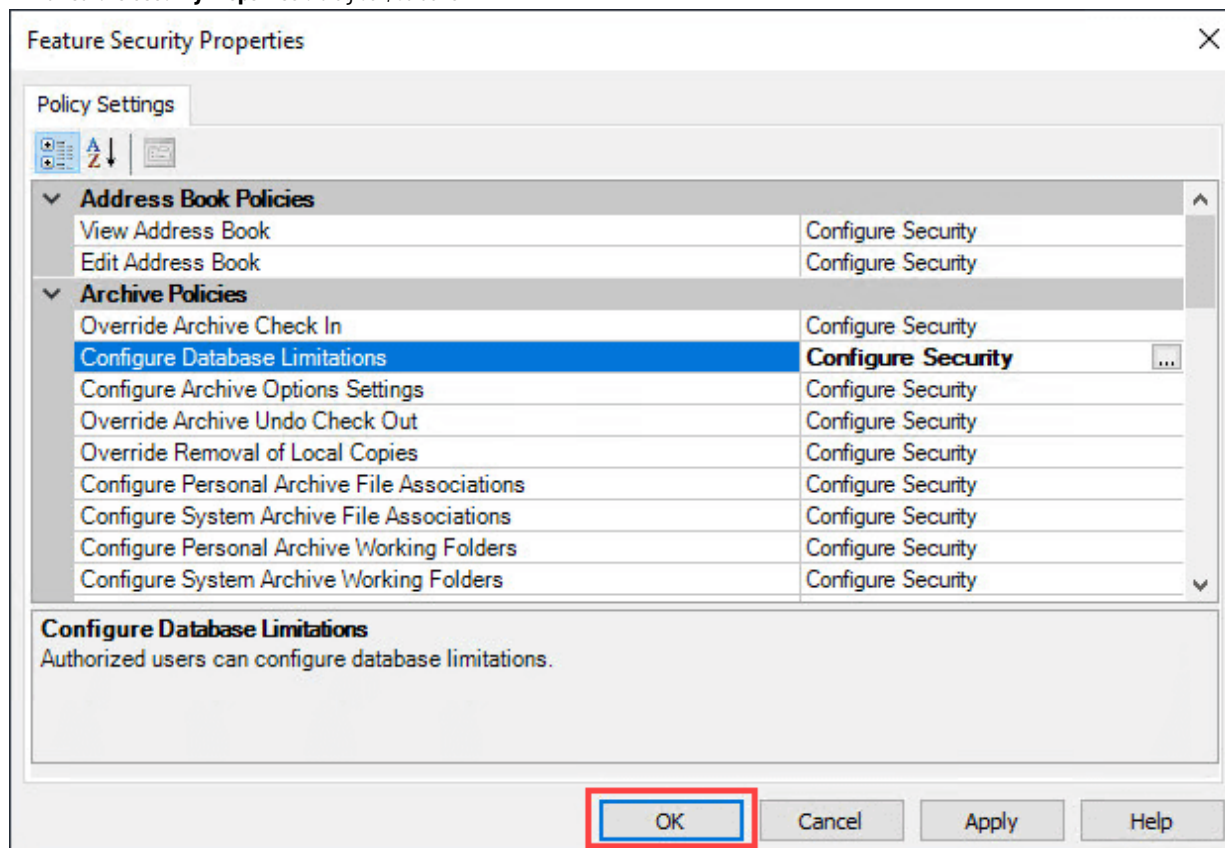
4. In the **Configure Securable Action** dialog box, if the desired group is not listed, select **Add**.



5. For this example, in the **Select User and Computer** dialog box, select one or multiple groups, and then select **OK**.



6. Configure the **Allow**, **Deny**, or unselected option for each group to the desired security configuration, and then select **OK**.
7. In the **Feature Security Properties** dialog box, select **OK**.



## Configure securable actions in FactoryTalk AssetCentre

Securable actions of FactoryTalk AssetCentre are not configured in FactoryTalk Administration Console but in FactoryTalk AssetCentre itself. Securable actions include common actions and FactoryTalk AssetCentre-specific actions.

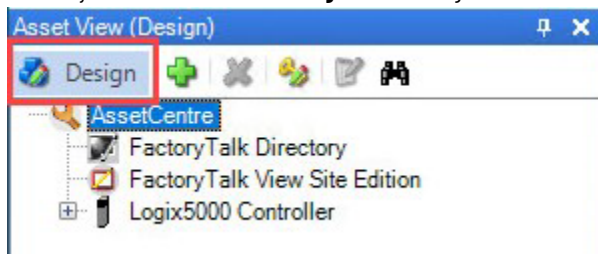
- **Common actions** manage how a user interacts with the hierarchical structure of the asset tree in FactoryTalk AssetCentre. For example, use common actions to limit a user's ability to view projects within one area and remove that user's ability to view projects in other areas.
- **FactoryTalk AssetCentre-specific actions** manage which users can perform specific actions with the assets. They work similarly to the rules in FactoryTalk Administration Console such as permission inheritance. Permission inheritance means that children inherit security permissions from their parents. You can assign explicit permissions to an asset, overriding the inherited permissions. You can also break the chain of inheritance for an asset.

For a complete list and their explanations, see [Product policies and securable actions of FactoryTalk AssetCentre on page 124](#).

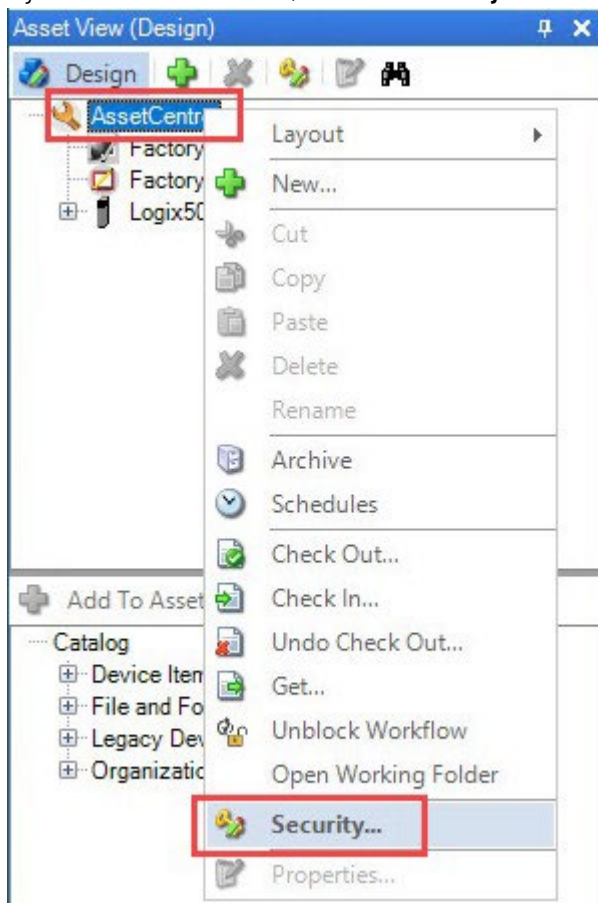
The following example configures the security of the top node of the asset tree, which is AssetCentre.

### To configure securable actions in FactoryTalk AssetCentre

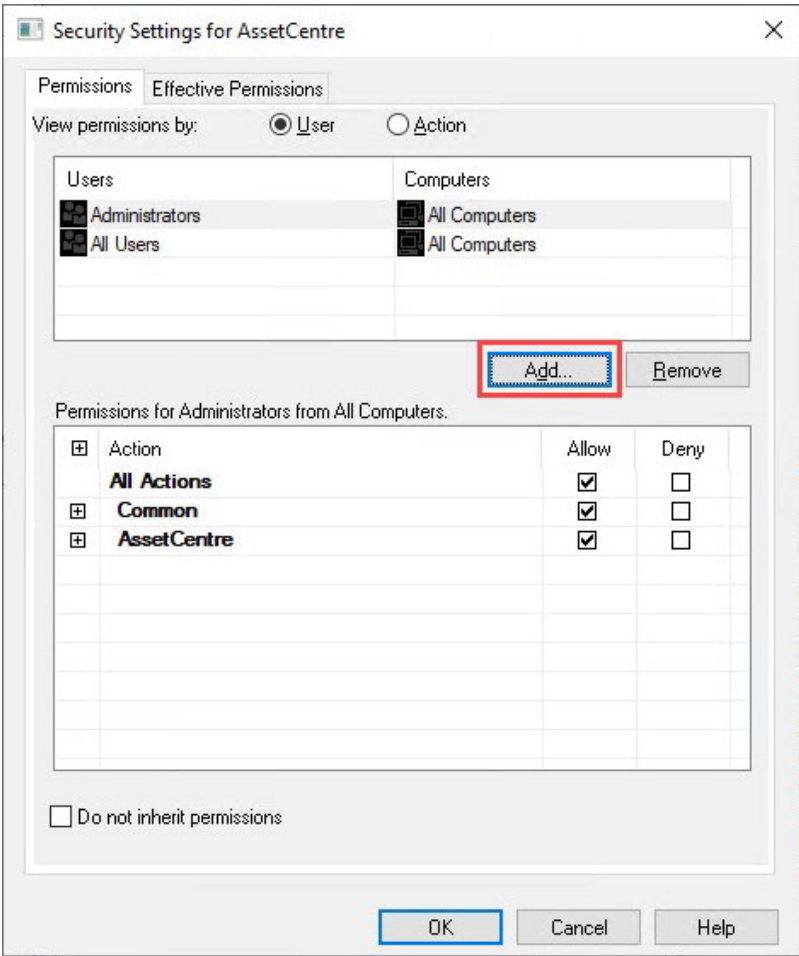
1. In FactoryTalk AssetCentre, select **Design** to enter design mode.



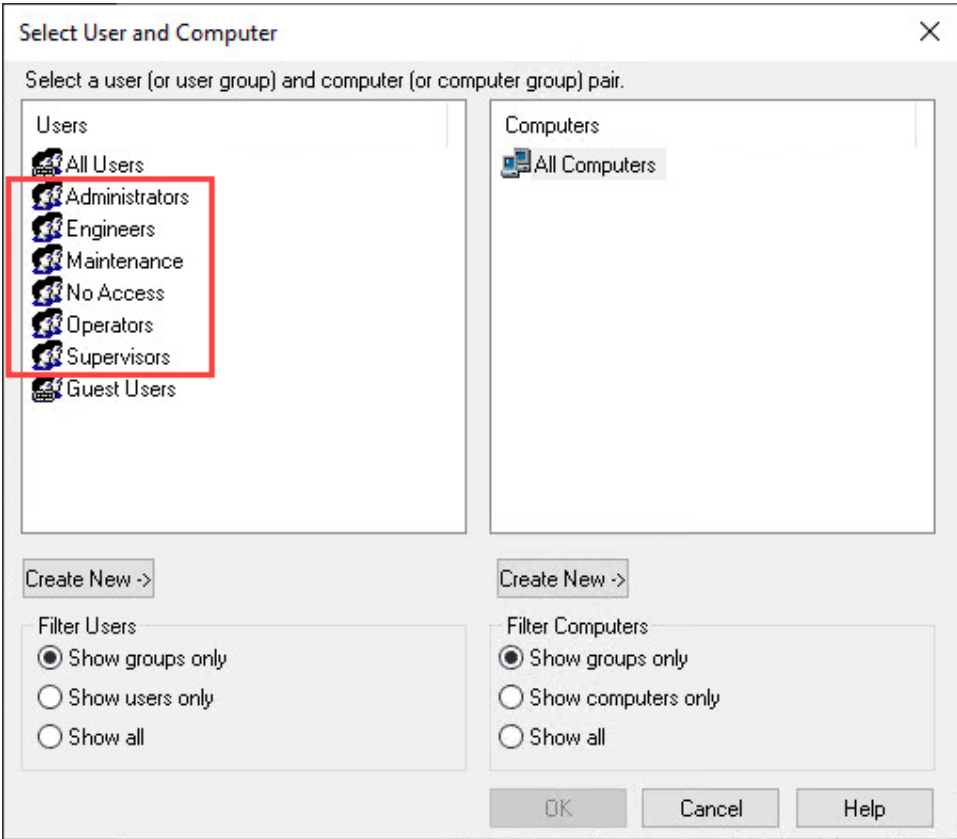
2. Right-click a node in the asset tree, and then select **Security**.



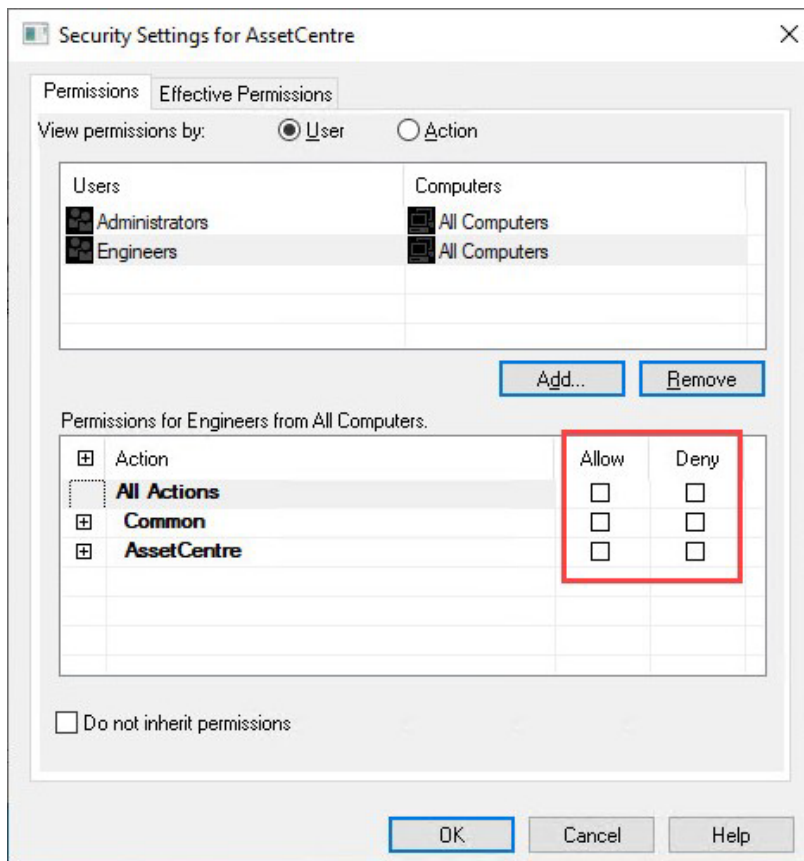
3. In the **Security Settings for AssetCentre** dialog box, if the desired group is not listed, select **Add**.



4. In the **Select User and Computer** dialog box, select the desired users or groups, and then select **OK**.



- Assign permissions to common and FactoryTalk AssetCentre-specific policies for the users and groups selected.



- Once the desired security settings are specified for the selected users and groups, select **OK**.

## Disaster recovery for a ControlLogix project

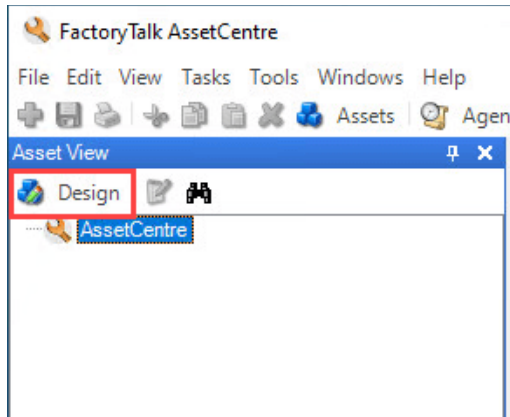
ControlLogix disaster recovery allows the automatic backup and comparison of project files running in ControlLogix controllers. Once a ControlLogix controller is configured as an asset in the FactoryTalk AssetCentre asset tree, it can be added to a disaster recovery schedule. The results of the disaster recovery schedule are added to the FactoryTalk AssetCentre event log and can also be configured to be emailed.

## Configure a Logix5000 Controller asset

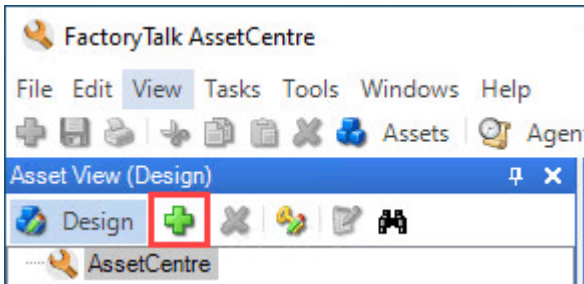
In this section, a new asset will be configured in FactoryTalk AssetCentre and point to a ControlLogix controller. An ACD file will be configured as the configuration data, which is used as the master file for compare operations.

### To configure a Logix5000 Controller asset

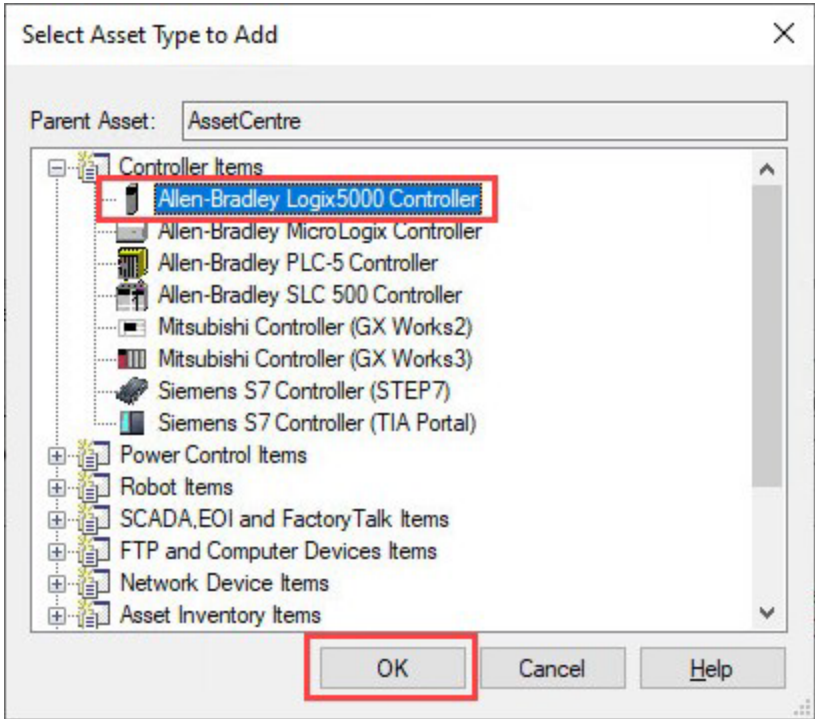
- In FactoryTalk AssetCentre, select **Design** to enter design mode.



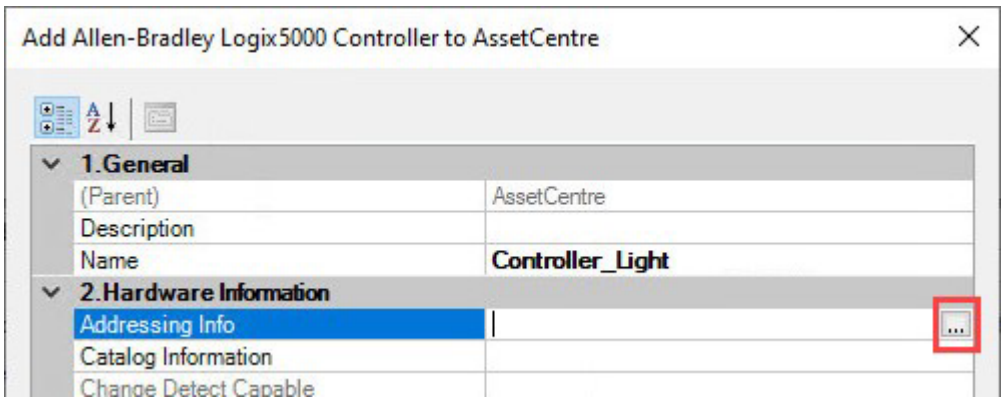
2. Select the **New** button.



3. Select **Allen-Bradley Logix5000 Controller**, and then select **OK**.

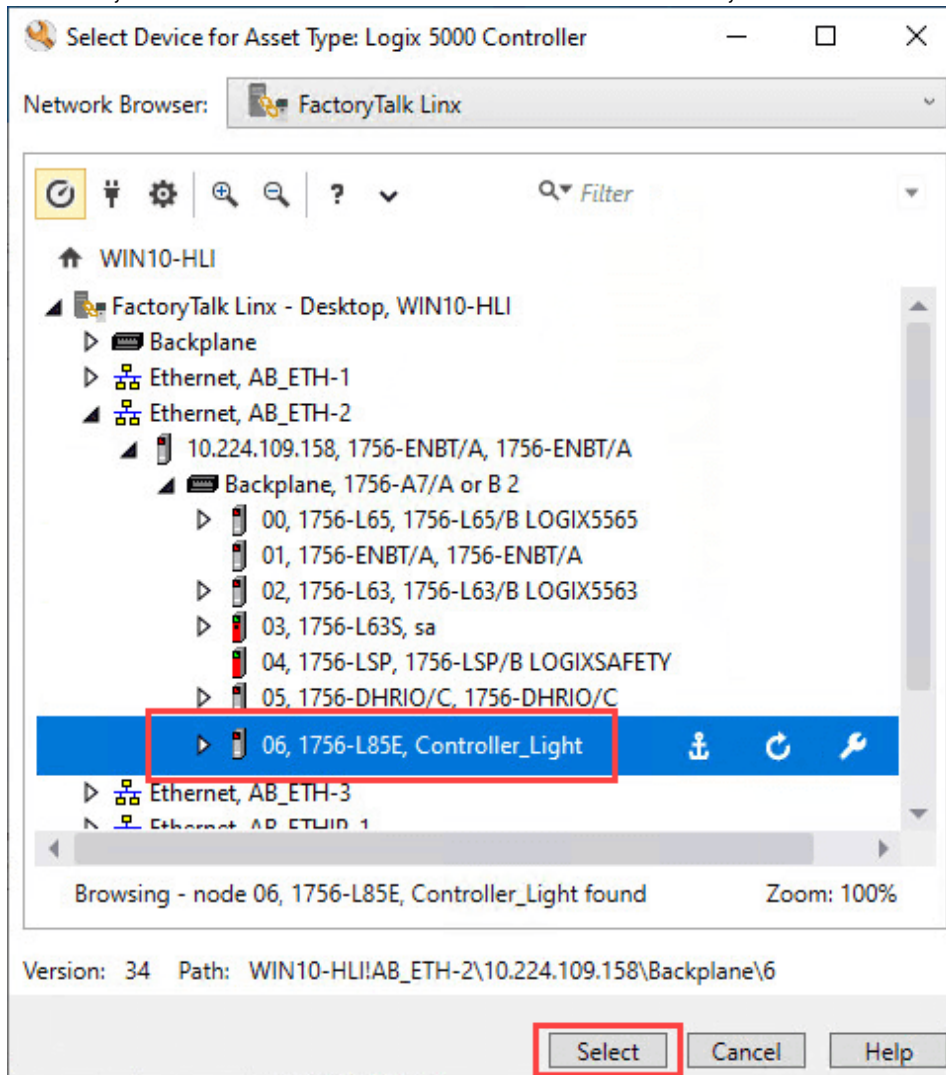


4. In the **Add Allen-Bradley Logix5000 Controller to AssetCentre** dialog box, name the controller under **1. General -> Name**, and then select the **Addressing Info** browse button.






5. Select FactoryTalk Linx or RSLinx Classic in **Network Browser**. Browse the network until you discover the desired controller, and then click **Select**.

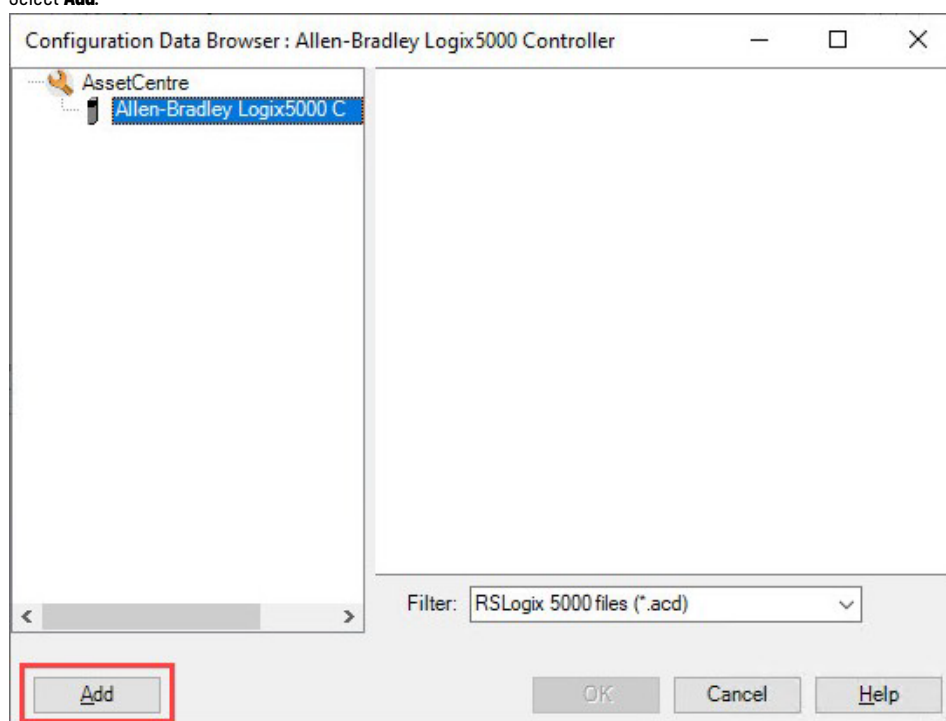


6. Select the **Configuration Data** browse button.

<b>2. Hardware Information</b>	
Addressing Info	WIN10-HLI\AB_ETH-2\10.224.109.158\Ba
Catalog Information	
Change Detect Capable	True
Configuration Data	No file selected. 
Device Name	Controller_Light
Firmware Revision	34.11
Hardware Revision	
Hardware Serial Number	
Hardware Type	1756-L85E LOGIX5585E
Manufacturer	Rockwell Automation/Allen-Bradley



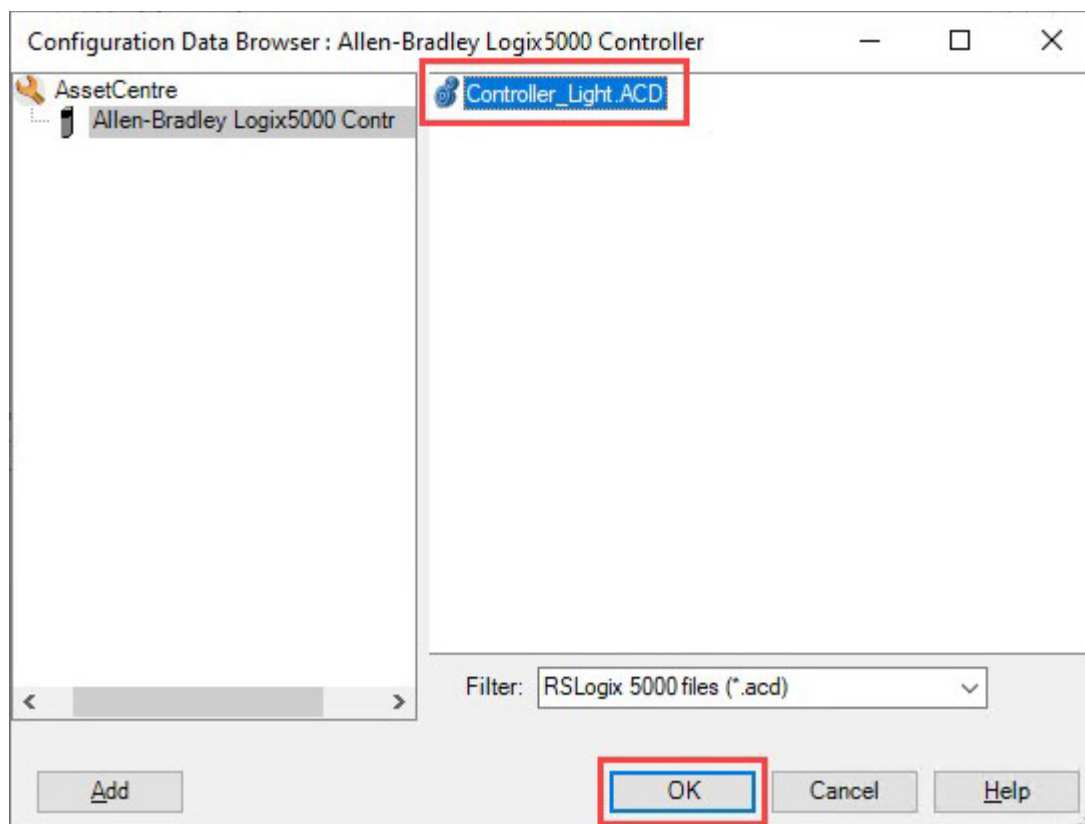
7. Select **Add**.



8. Browse for the desired ACD file, and then select **Open**.

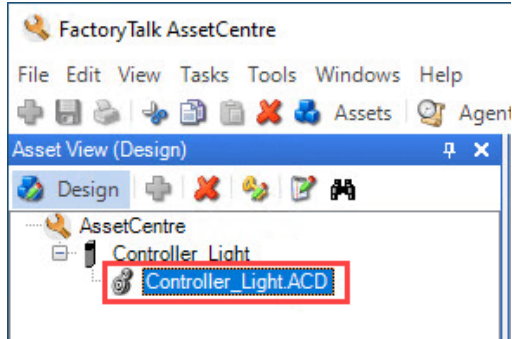
**NOTE:** Make sure that the file is not opened in Studio 5000 Logix Designer.

9. Select the ACD file, and then select **OK**.



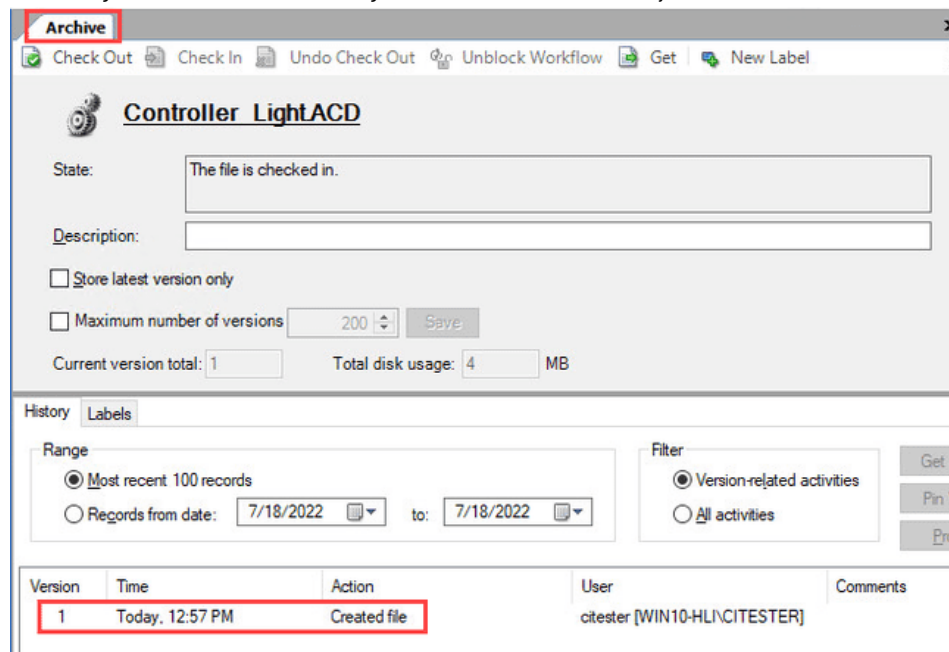
10. In the **Add Allen-Bradley Logix5000 Controller to AssetCentre** dialog box, select **OK**.

Notice that the file is added as a child node of the ControlLogix asset.



11. Select the **Design** button to exit design mode.

After adding the new asset, the asset's configuration data is added in the FactoryTalk AssetCentre archive. Notice that version 1 has been created.

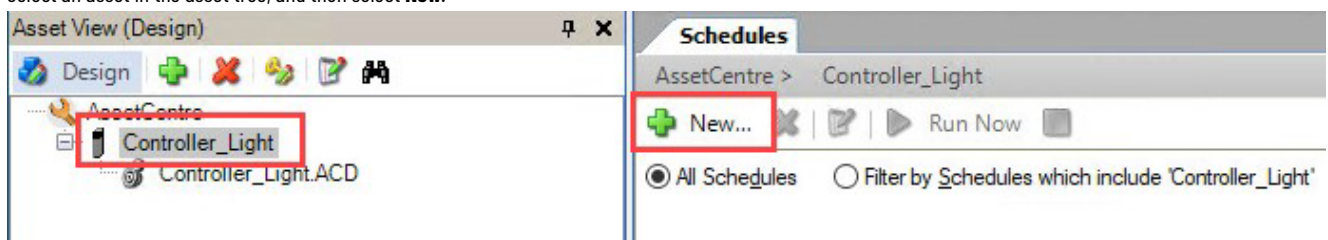


## Configure a ControlLogix backup and compare schedule

With a ControlLogix asset added to the asset tree and the configuration data configured, you can now create a backup and compare schedule to detect if the ControlLogix project is changed, and view the changes made to the previous Archive version. The changed file will be compared to the original file (version 1) during the schedule. This section introduces how to create and configure a ControlLogix backup and compare schedule.

### To configure a ControlLogix backup and compare schedule

1. In FactoryTalk AssetCentre, select **Schedules**.
2. Select an asset in the asset tree, and then select **New**.



**NOTE:** Select the Logix5000 Controller asset and not the .ACD file below the associated asset.

- On the **Schedule Properties** page, select **Disaster Recovery - Backup and Compare** in the **Operation** list, rename the schedule to the desired name, and then select **Next**.

New Schedule Wizard - Step 1 of 3

**Schedule Properties**  
Name must be unique across all schedule names.

Location:  
AssetCentre/Controller\_Light

Operation:  
Disaster Recovery - Backup and Compare

Name:  
New Schedule

Description:

Completion Email List:  
To...

Help < Back **Next >** Cancel

- On the **Timing Properties** page, configure the schedule start time and frequency (if desired to differ from the default settings), and then select **Next**.

New Schedule Wizard - Step 2 of 3

**Timing Properties**  
Please update the timing properties for this schedule.  
Clicking on Next button will create the schedule. You will not be able to return to this page.

Start Time: 10:18 AM

Timing Properties

☐ Hourly  
☒ Daily  
☐ Weekly  
☐ Monthly

Every 1 day(s)

Maximum Runtime (0.0 means no limit) : 1 Hours 0 Minutes  
Maximum Runtime is limited.

Help < Back **Next >** Cancel

5. On the **Operation Properties** page, configure the task properties as needed.

For more information on these properties, see *Allen-Bradley Logix 5000 controller operation properties for Disaster Recovery and Device Monitor* in *FactoryTalk AssetCentre Client Help*.

Controller\_Light Properties

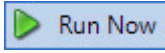
<b>1. Event settings</b>	
Master File Path Name	AssetCentre/Controller_Light/Controller_Lig
Promote New Upload to Master	True
Report Incremental Differences	False
<b>2. Asset specific properties</b>	
Always Run Events	True
Compare Options	(select and click ellipsis to edit)
Tag Filter	(select and click ellipsis to edit)
<b>3. Email notification</b>	
Event Compare Differences Detected	
Event Completed	
Event Failed	
<b>4. Attach report to email</b>	
Event Compare Differences Detected	False
Event Completed	False

6. Once complete, select **Finished**.

## Run a schedule to detect ControlLogix differences






If the ControlLogix project is changed, a backup and compare schedule can detect differences by comparison. The changed project file will be compared to the asset's current achieve version. This section introduces how to run a backup and compare schedule including a ControlLogix task and view the comparison results.

### To run a schedule to detect ControlLogix differences






1. In FactoryTalk AssetCentre, open **Schedules**. Navigate to the desired schedule, and then select  to start the schedule.

**Schedules**

AssetCentre > Controller\_Light

 New...    Run Now 


☒ All Schedules ☐ Filter by Schedules which include 'Controller\_Light'

Active	Name	Schedule Location	Operation
			
	New Schedule	AssetCentre/Controller_Light	Backup and Compare

If any changes were made to the project, the task will show that differences were found upon completion.

☒ View By Location ☐ View By Asset Type



Assets in New Schedule:

	Controller_Light	(Compare - Differences Found)	Completed at
---	------------------	-------------------------------	--------------















2. Select  Logs, and then select  Event Log

- 3. Find the most recent disaster recovery task completion with the yellow triangle **Warning** severity, and then double-click the paper clip icon to view the attachment.

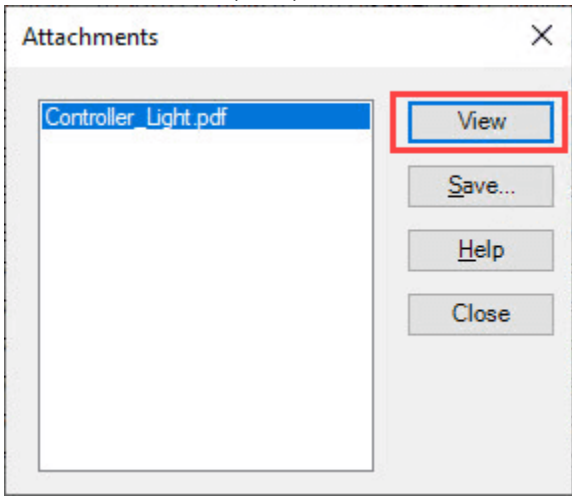
Schedules    **Logs**

Event Log    Audit Log    Diagnostics & Health Log    Quick Search Results    Quick Search        

Events - Showing up to last 500 records. Last refreshed at : 10:29:51

	Logged Time	Occurred Time ▾	Source	Location	Severity	Message
	10/26/2023 10:29:	10/26/2023 10:29:2	FactoryTalk Asset	VICKYSUN180	 Information	New Schedule - AssetCentre End of Sched
	10/26/2023 10:29:	10/26/2023 10:29:2	RA Disaster Reco	VICKYSUN180	 <b>Warning</b>	Scheduled event finished 2023-10-26 10:2
	10/26/2023 10:26:	10/26/2023 10:25:5	RA Disaster Reco	VICKYSUN180	 Information	Scheduled event started 2023-10-26 10:25:
	10/26/2023 10:25:	10/26/2023 10:25:3	FactoryTalk Asset	VICKYSUN180	 Information	New Schedule - AssetCentre Start Schedul
	10/26/2023 10:22:	10/26/2023 10:22:0	FactoryTalk Activ	VICKYSUN180	 Information	Checked out a FactoryTalk activation LGX
	10/26/2023 10:22:	10/26/2023 10:22:0	FactoryTalk Activ	VICKYSUN180	 Information	transaction = checkout
	10/26/2023 10:22:	10/26/2023 10:22:0	FactoryTalk Activ	VICKYSUN180	 Information	transaction = checkout

- 4. Select **View** to view the compare report.




- 5. View the changes in the compare report. When completed, close the compare report, and then close the **Attachment** dialog box.

## Recover a ControlLogix project

The Archive capability in FactoryTalk AssetCentre is a version control tool that helps manage asset files. If undesired changes have been made to a project file and you would like to revert to a previous version, the FactoryTalk AssetCentre Archive capability allows you to perform this action. This section introduces how to recover a ControlLogix project to a previous version from the archive.

### To recovery a ControlLogix project

- 1. In FactoryTalk AssetCentre, select  **Archive**.
- 2. Navigate the asset tree to the desired asset whose file that you want to recover, and then select the desired version that you want to revert to.



In this example, the first version of the ACD file will be restored.

**Archive**

Check Out Check In Undo Check Out Unblock Workflow

**Controller Light**

Description:

Working folder: C:\Users\Administrator\Desktop\Working Folder

Name	User	Check Out Loc
Controller_Light.ACD		

**History** Labels

Range

☒ Most recent 100 records

☐ Records from date: 10/26/2023 to: 10/26/2023

Version	Time	Action	User
2	Today, 10:29 AM	Added new version	Factory
1	Today, 10:13 AM	Created file	VICKYS

3. Select **Promote**.

**History** Labels

Range

☒ Most recent 100 records

☐ Records from date: 10/26/2023 to: 10/26/2023

Filter

☒ Version-related activities

☐ All activities

Get Version

Pin Version

**Promote**

Version	Time	Action	User	Comments
2	Today, 10:29 AM	Added new version	FactoryTalk Ser...	AgentController: VICKYSUN180 Schedule: Ne
1	Today, 10:13 AM	Created file	VICKYSUN180\...	

A new version, version 3 is created. This file will be checked out, and later changes will be compared against it.

HistoryLabels

Range

☒ Most recent 100 records

☐ Records from date: 10/26/2023 to: 10/26/2023

Filter

☒ Version-related activities

☐ All activities

Get Version

Pin Version

Promote

Version	Time	Action	User	Comments
3	Today, 10:34 AM	Promoted version "1" to "3"	VICKYSUN180\...	
2	Today, 10:29 AM	Added new version	FactoryTalk Ser...	AgentController: VICKYSUN180 Schedule: N
1	Today, 10:13 AM	Created file	VICKYSUN180\...	

4. Select **Check Out**. This file will be checked out to your working folder.

Archive

Check Out

Check In

Undo Check Out

Unblock Workflow

Get

New Label

Remove Label

Expo

Controller Light

Description:

Working folder:

C:\Users\Administrator\Desktop\Working Folder

Name	User	Check Out Location
Controller_Light.ACD		

HistoryLabels

Range

☒ Most recent 100 records

☐ Records from date: 10/26/2023 to: 10/26/2023

Filter

☒ Version-related activities

☐ All activities

Get Version

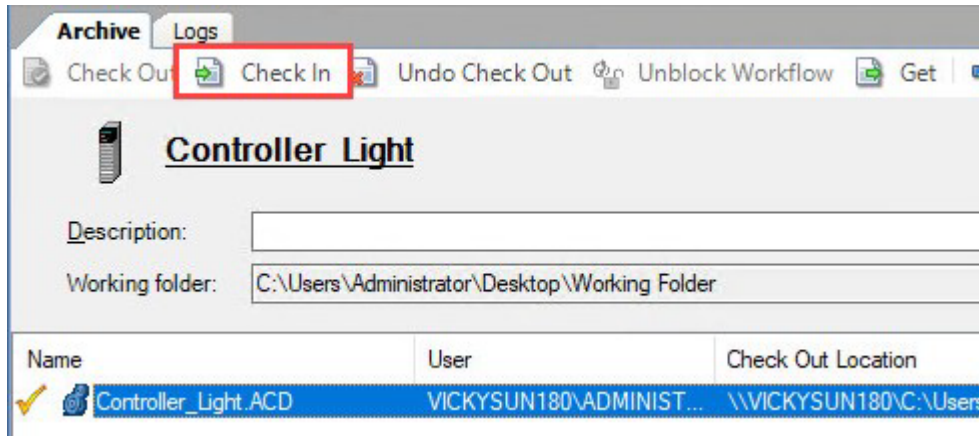
Pin Version

Promote

Version	Time	Action	User	Comments
3	Today, 10:34 AM	Promoted version "1" to "3"	VICKYSUN180\...	
2	Today, 10:29 AM	Added new version	FactoryTalk Ser...	AgentController: VICKYSUN180 Schedule: Ne
1	Today, 10:13 AM	Created file	VICKYSUN180\...	



5. You can edit the ACD file as needed, and then download it to the controller. After that, check in this file.



## Disaster recovery for a FactoryTalk View Site Edition project

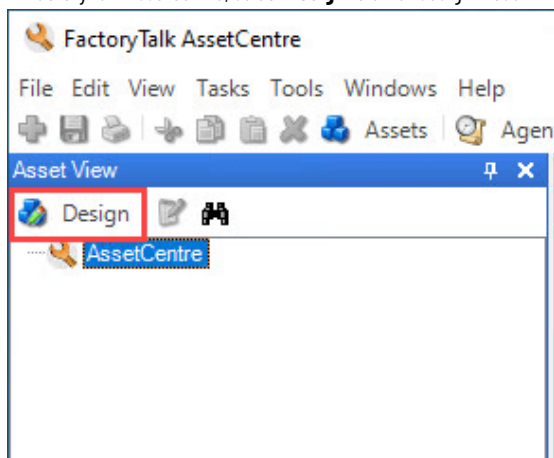
FactoryTalk View Site Edition disaster recovery allows for the automatic backup and comparison of the entire FactoryTalk View Site Edition application, including the HMI server, FactoryTalk Directory, FactoryTalk Linx, FactoryTalk Alarms and Events during production. The asset is backed up and archived as an APB file. The results of the disaster recovery schedule are added to the FactoryTalk AssetCentre event log and can be configured to be emailed.

## Configure a FactoryTalk View Site Edition asset

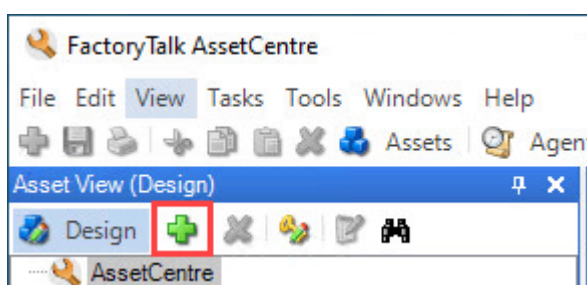
In this section, a new asset will be configured in FactoryTalk AssetCentre and point to a FactoryTalk View Site Edition application. In **Backup Configuration**, specify a FactoryTalk View SE application. In **Backup Data**, specify the backup file, which will be compared against for any changes. When you first add a new asset of FactoryTalk View SE, the backup data can either be left unspecified or an existing APB file can be chosen. If you leave the backup data unspecified, one is automatically created the first time a backup schedule runs for this asset.

### To configure a FactoryTalk View Site Edition asset

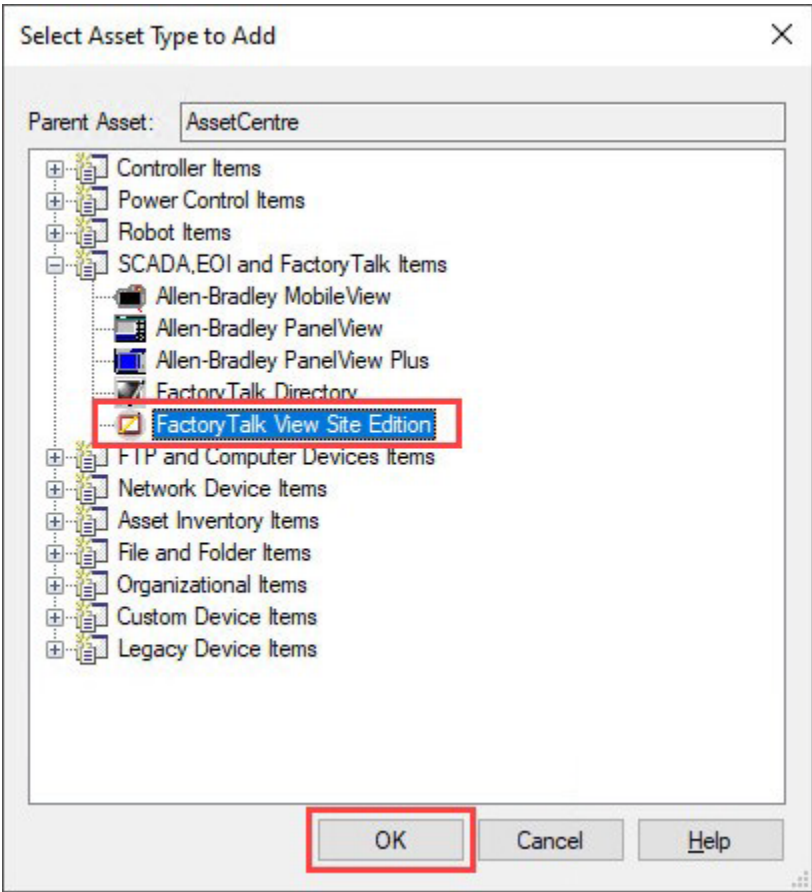
1. In FactoryTalk AssetCentre, select **Design** to enter design mode.



2. Select the **New** button.

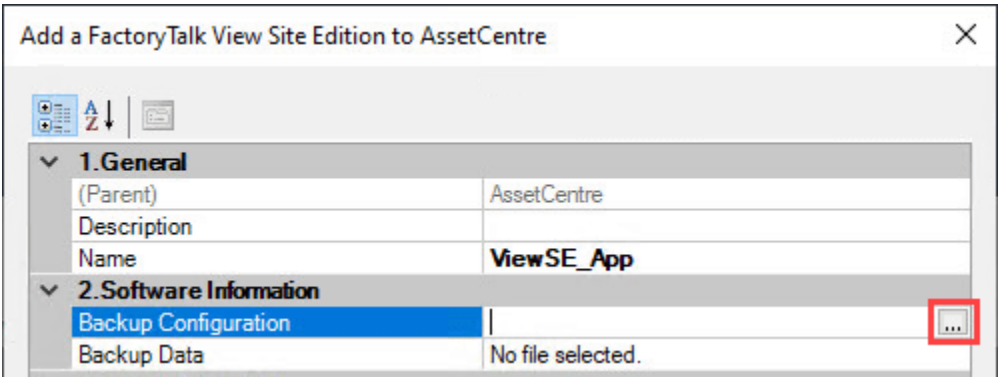


3. Select **FactoryTalk View Site Edition**, and then select **OK**.



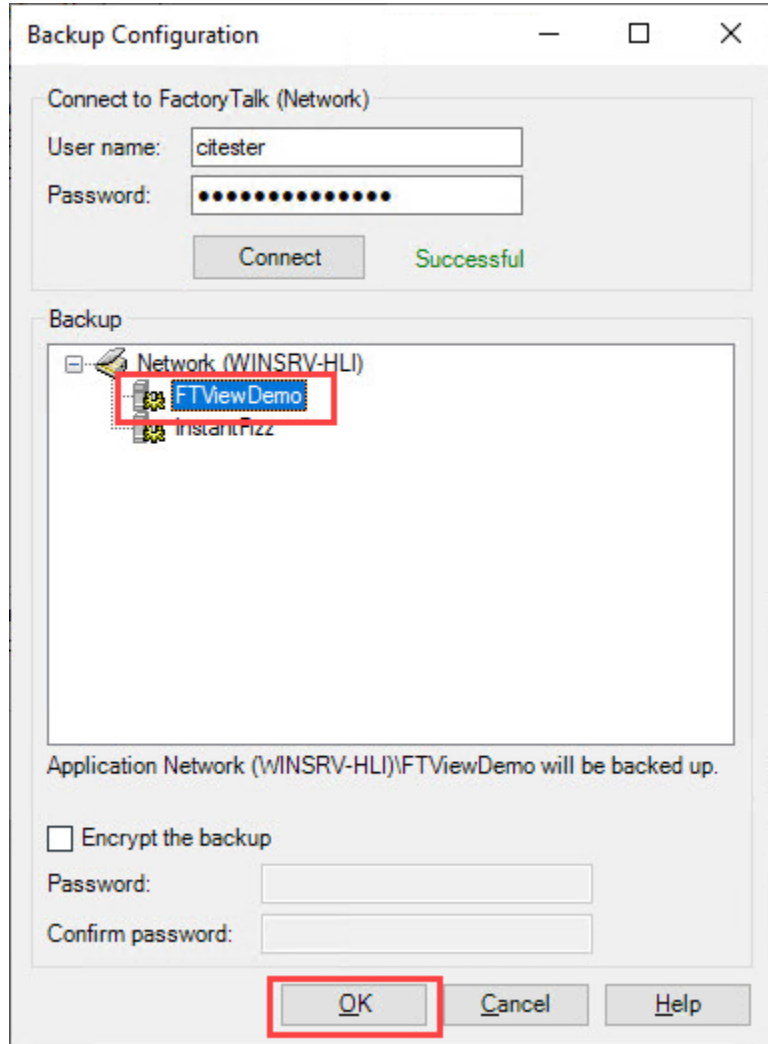
4. In the **Add a FactoryTalk View Site Edition to AssetCentre** dialog box, name the FactoryTalk View SE project under **1. General -> Name**, and then select the **Backup Configuration** browse button.

**NOTE:** In this example, the **Backup Data** property is not specified. One will be created upon the first run of a backup schedule, which will be shown in the later section.



5. In the **Backup Configuration** dialog box, enter your FactoryTalk credentials, and then select **Connect**.

Once access is granted, select the desired application, and then select **OK**.



**Tip:** You can choose to encrypt the application backup file. The password will be required when restoring the application using the FactoryTalk View SE Application Manager utility.

6. In the **Add a FactoryTalk View Site Edition to AssetCentre** dialog box, select **OK**.
7. Select the **Design** button again to exit design mode.


## Run a schedule to create a backup file

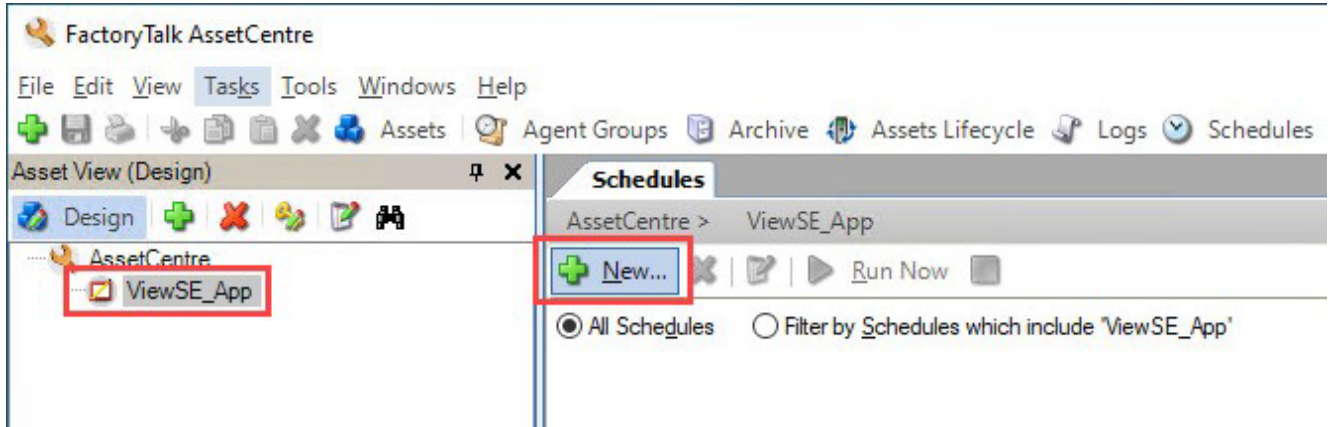
With a FactoryTalk View SE asset added to the asset tree and the backup configuration configured, you can start a backup schedule to create the backup data for the asset. During a backup and compare schedule, any further changes to the FactoryTalk View SE application will be compared against the backup data.

## Configure a FactoryTalk View SE backup schedule

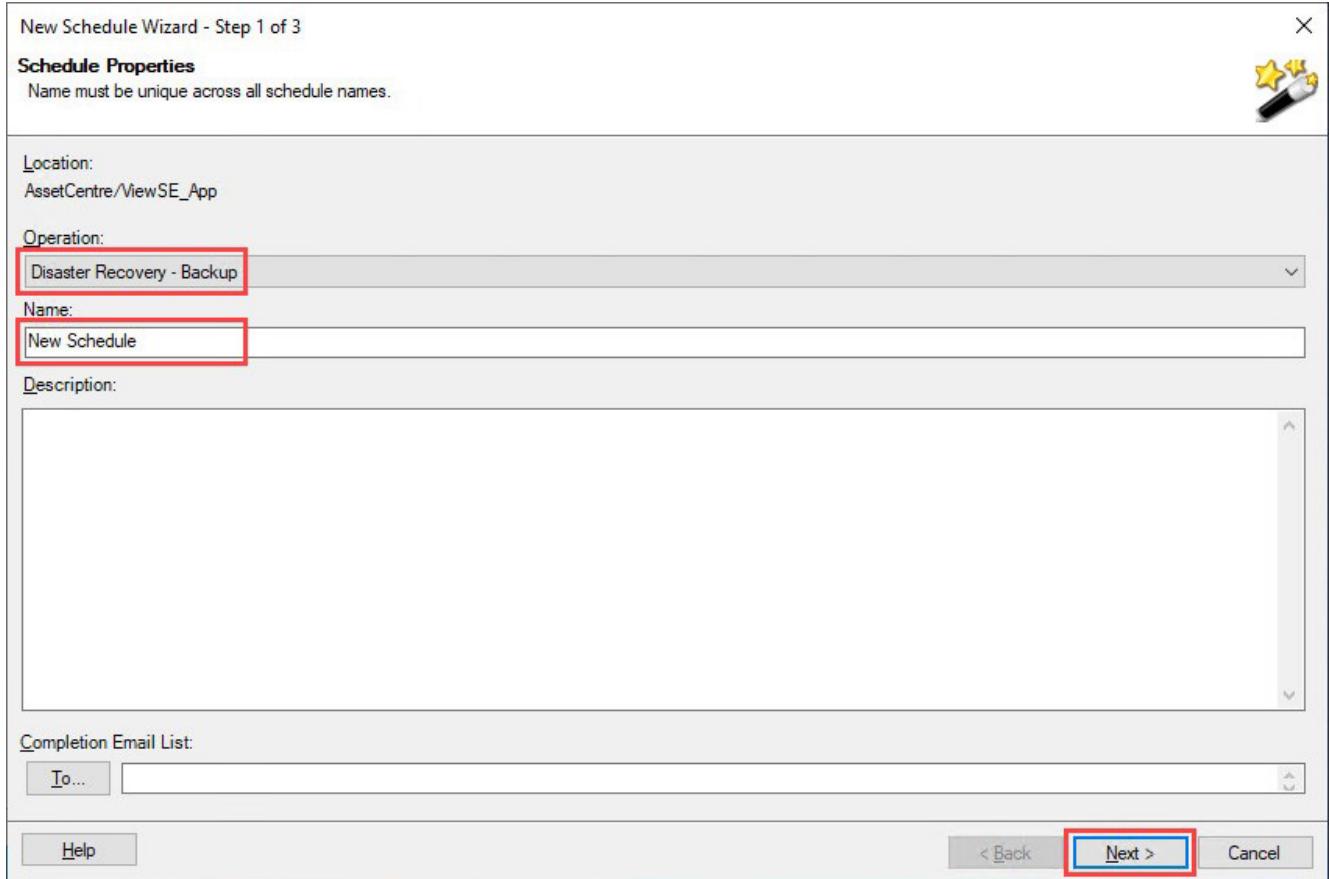
This section introduces the backup schedule configuration.

### To configure a FactoryTalk View SE backup schedule

1. In FactoryTalk AssetCentre, select  **Schedules**.
2. Select the FactoryTalk View SE asset in the asset tree, and then select **New**.



3. On the **Schedule Properties** page, select **Disaster Recovery - Backup** in the **Operation** list, rename the schedule to the desired name, then select **Next**.



4. On the **Timing Properties** page, configure the schedule start time and frequency, and then select **Next**.

New Schedule Wizard - Step 2 of 3

**Timing Properties**  
Please update the timing properties for this schedule.  
Clicking on Next button will create the schedule. You will not be able to return to this page.

Start Time: 8:42 AM

Timing Properties

☐ Hourly  
☒ Daily  
☐ Weekly  
☐ Monthly

Every 1 day(s)

Maximum Runtime (0.0 means no limit) : 1 Hours 0 Minutes  
Maximum Runtime is limited.

5. On the **Operation Properties** page, configure the task properties as needed.

For more information on these properties, see *FactoryTalk View Site Edition operation properties for Disaster Recovery* in *FactoryTalk AssetCentre Client Help*.

ViewSE\_App Properties

<b>2. Asset specific properties</b>	
Include Data log	False
<b>3. Email notification</b>	
Event Completed	
Event Failed	

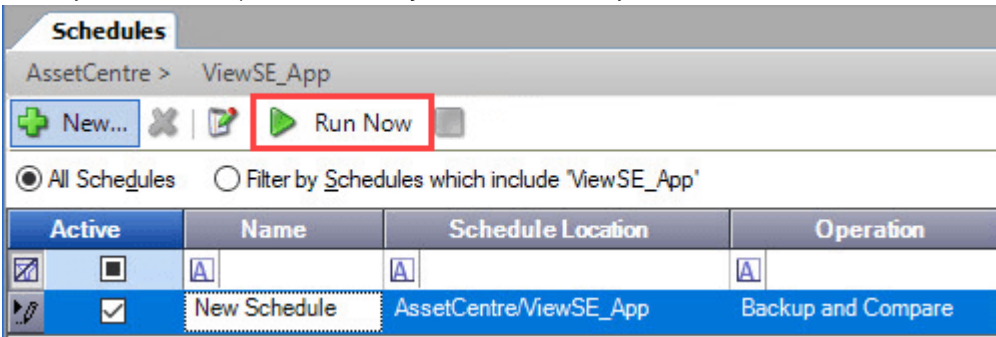
6. Select **Finished**.

## Run the backup schedule to create a FactoryTalk View SE backup

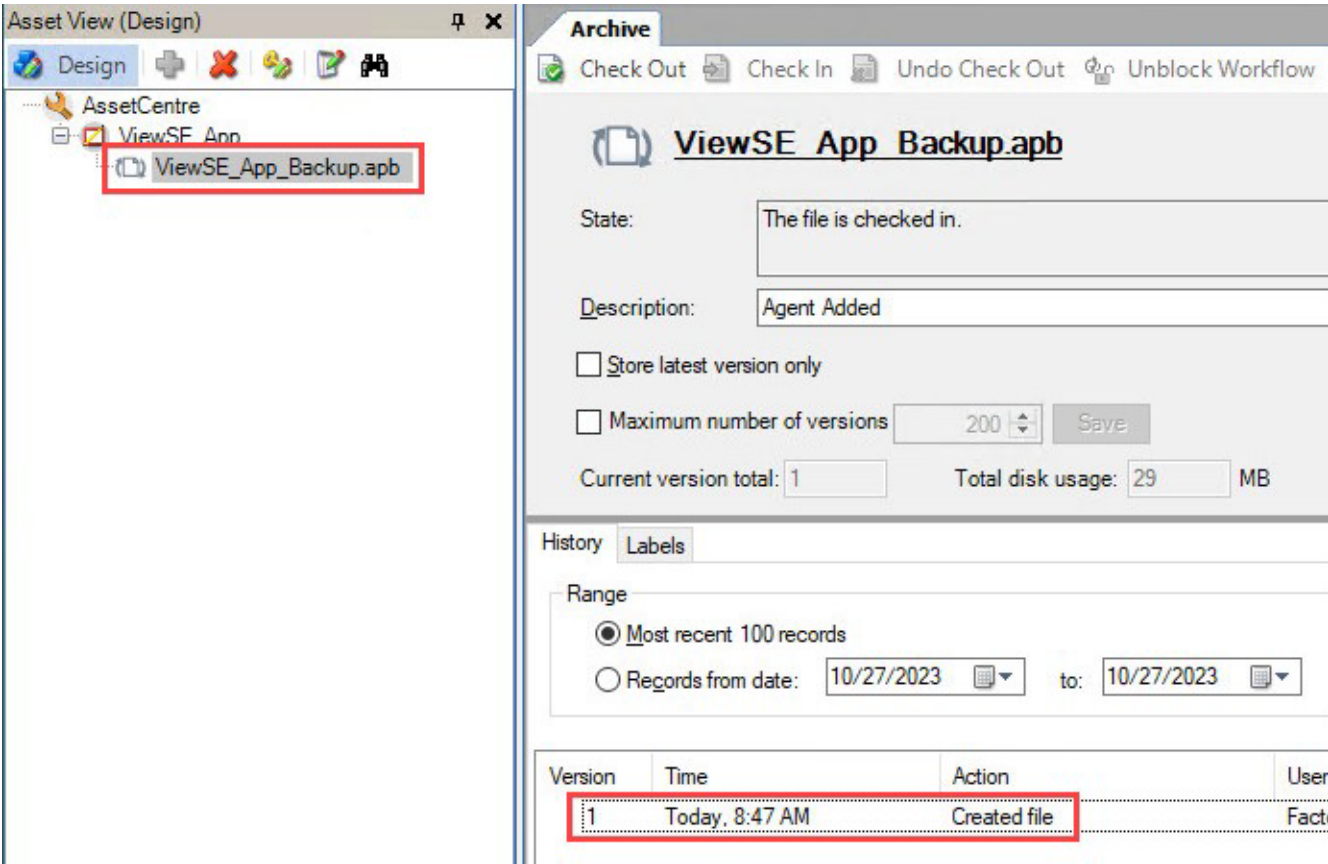
This section introduces how to run a backup schedule involving a FactoryTalk View SE project. If there is no current backup file configured, running the schedule will create the backup data for the asset.

To run a backup schedule to create a backup

- In FactoryTalk AssetCentre, open **Schedules**. Navigate to the desired FactoryTalk View SE schedule, and then select  to start the schedule.



Once the task is completed, a new backup file is added to the asset, and a version (version 1) is created in the FactoryTalk AssetCentre archive.



Run a schedule to detect application differences


If the FactoryTalk View SE application has been changed, a backup and compare schedule can detect differences by comparison. The online application file will be compared to the asset's most recent backup version in the Archive. This section introduces how to run a backup and compare schedule involving a FactoryTalk View Site Edition project and how to view the comparison results.

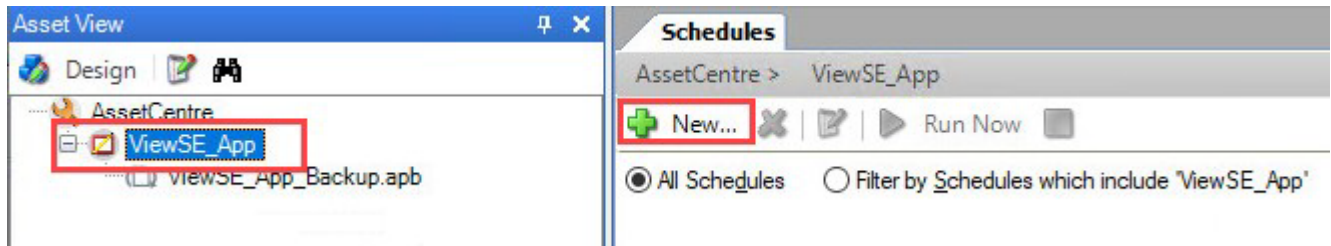
Configure a FactoryTalk View SE backup and compare schedule

This section introduces the backup and compare schedule configuration.

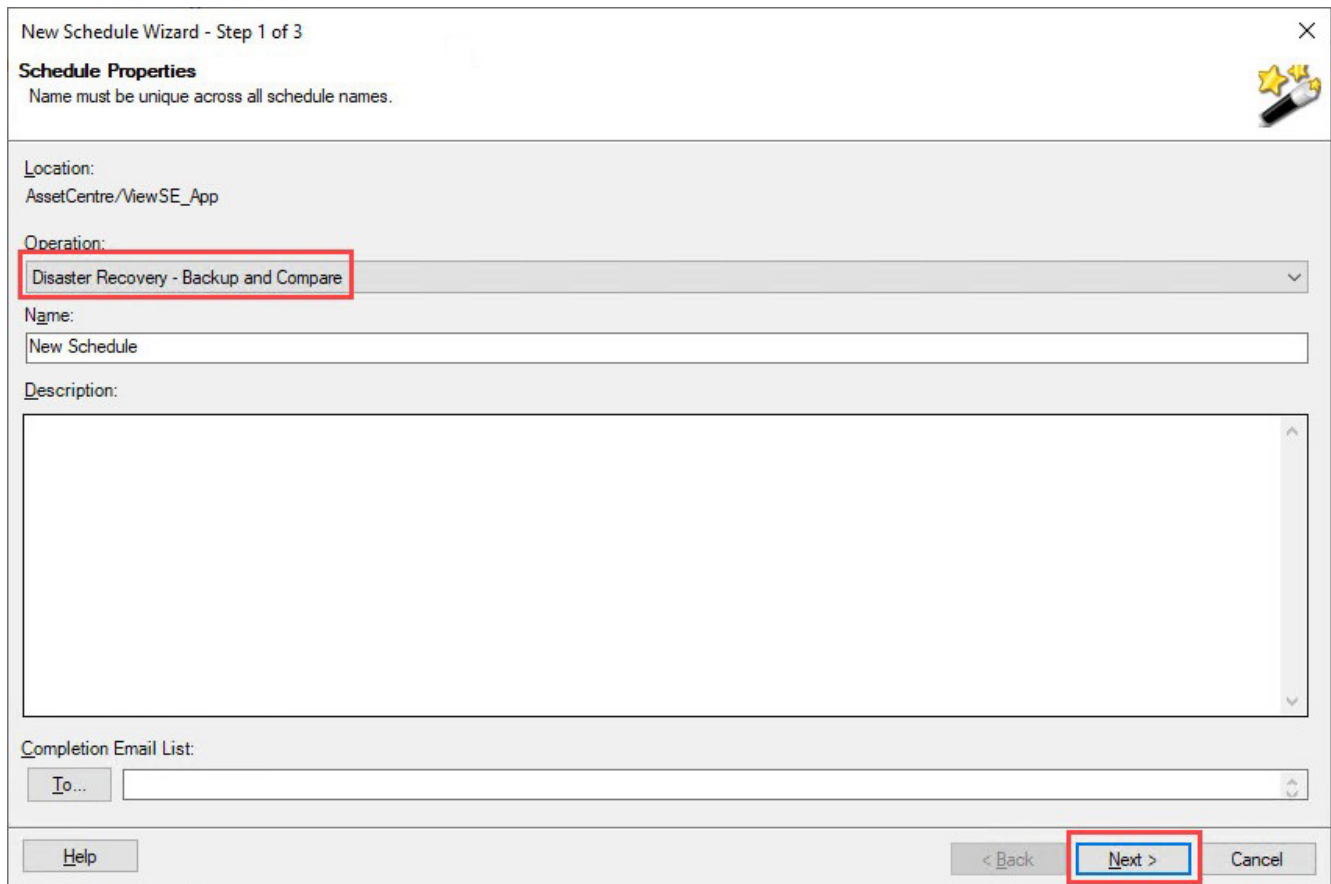


## To configure a FactoryTalk View SE backup and compare schedule

1. In FactoryTalk AssetCentre, select  **Schedules**.
2. Select an asset, and then select **New**.



3. On the **Schedule Properties** page, select **Disaster Recovery - Backup and Compare** in the **Operation** list, rename the schedule to the desired schedule name, and then select **Next**.



New Schedule Wizard - Step 1 of 3

**Schedule Properties**  
Name must be unique across all schedule names.

Location:  
AssetCentre/ViewSE\_App

Operation:  
Disaster Recovery - Backup and Compare

Name:  
New Schedule

Description:

Completion Email List:  
To...

Help < Back **Next >** Cancel



4. On the **Timing Properties** page, configure the schedule start time and frequency, and then select **Next**.

New Schedule Wizard - Step 2 of 3

**Timing Properties**  
Please update the timing properties for this schedule.  
Clicking on Next button will create the schedule. You will not be able to return to this page.

Start Time: 1:50 PM

Timing Properties

☐ Hourly      Every 1 day(s)

☒ Daily

☐ Weekly

☐ Monthly

Maximum Runtime (0.0 means no limit) : 1 Hours 0 Minutes  
Maximum Runtime is limited.

Help      < Back      **Next >**      Cancel

5. On the **Operation Properties** page, configure the task properties as needed.
- For more information on these properties, see *FactoryTalk View Site Edition operation properties for Disaster Recovery* in *FactoryTalk AssetCentre Help*.

ViewSE\_App Properties

1. Event settings

Backup Compare Partner	AssetCentre/ViewSE_App/ViewSE_App_
Create New Backup Version	Always

2. Asset specific properties

Compare Options	(select and click ellipsis to edit)
Create New Backup Version Due to Unmatch	True
Include Data log	False

3. Email notification

Event Compare Differences Detected	
Event Completed	
Event Failed	

4. Attach report to email

Event Completed Differences Detected	True
--------------------------------------	------

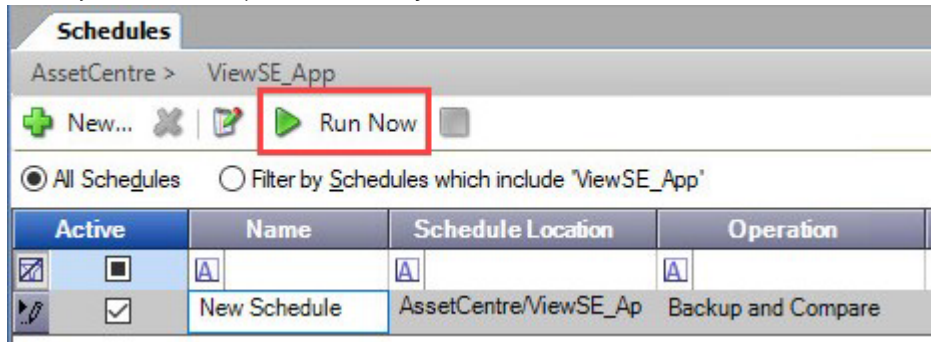
6. Select **Finished**.

## Run a backup and compare schedule to detect application differences

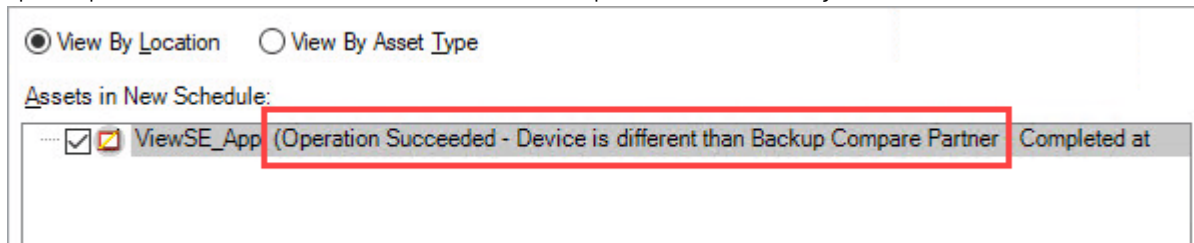
This section introduces how to run a backup and compare schedule involving a FactoryTalk View SE project.

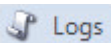
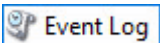
## To run a backup and compare schedule to detect application differences

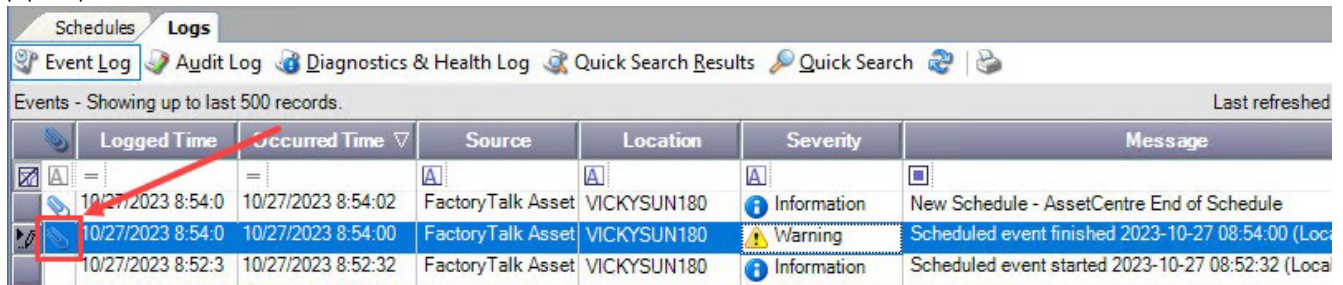
1. In FactoryTalk AssetCentre, open **Schedules**. Navigate to the desired schedule, and then select  to start the schedule.



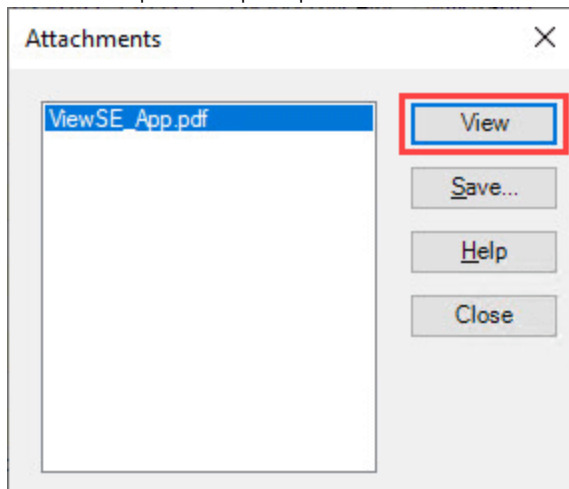
Upon completion, the task shows that differences were found. This is expected because of the changes made in the earlier section.



2. Select , and then select .
3. Find the most recent disaster recovery task completion with the yellow triangle Warning severity for the FactoryTalk View SE project, and then double-click the paper clip icon to view the file.



4. Select **View** to open the compare report.




5. Once you have completed viewing the compare report, close the compare report, and then close the **Attachment** dialog box.

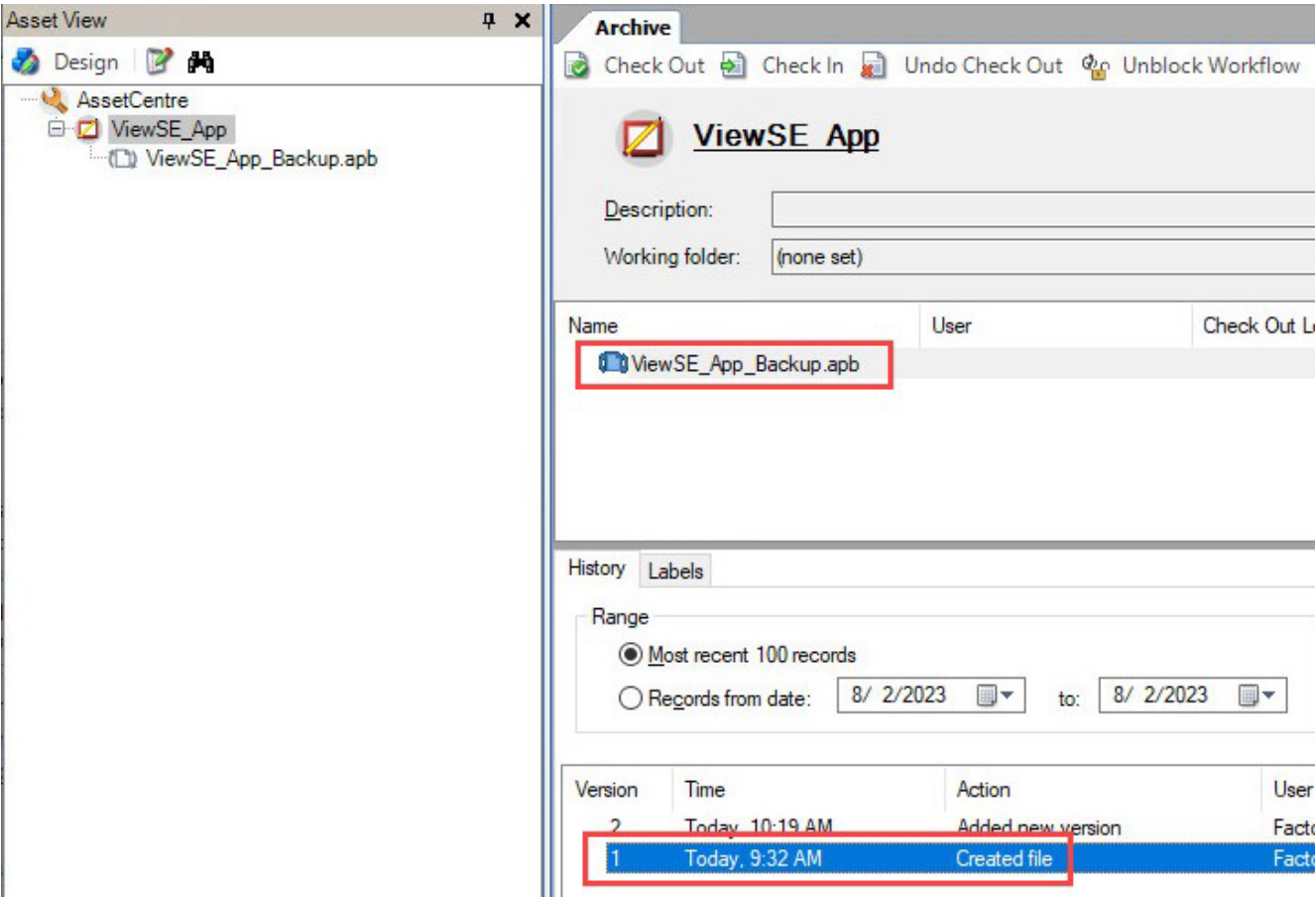
## Recover a FactoryTalk View SE application


The Archive capability in FactoryTalk AssetCentre is a version control tool that helps manage asset files. If undesired changes have been made to a project file and you would like to revert to a previous version, the FactoryTalk AssetCentre Archive capability allows you to perform this action. This section introduces how to recover a FactoryTalk View SE archived to a previous version from the archive.

### To recover a FactoryTalk View SE application

1. In the FactoryTalk AssetCentre, select  **Archive**.
2. Navigate the asset tree to the desired asset whose file that you want to recover, and then select the desired version that you want to revert to.

In this example, the first version of the application will be restored.

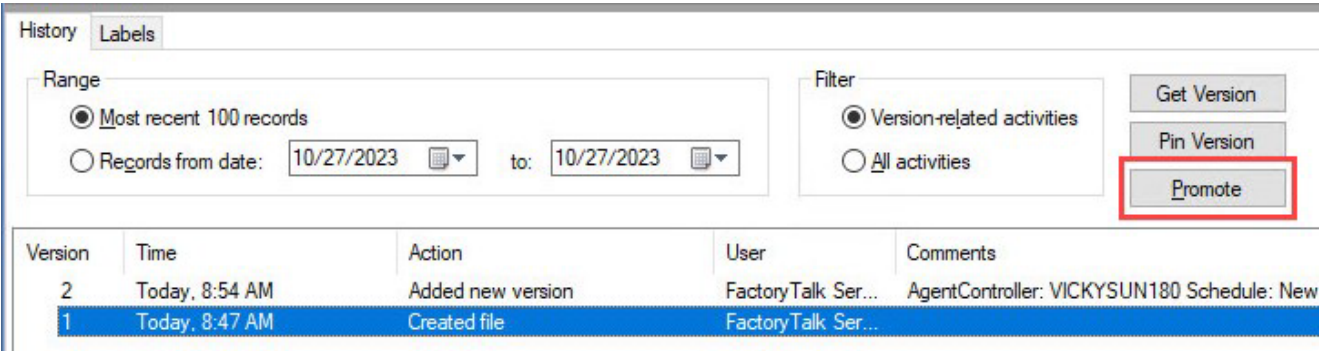


Name	User	Check Out L
 ViewSE_App_Backup.apb		

Version	Time	Action	User
2	Today, 10:19 AM	Added new version	Facto
1	Today, 9:32 AM	Created file	Facto

3. Select **Promote**.



Version	Time	Action	User	Comments
2	Today, 8:54 AM	Added new version	FactoryTalk Ser...	AgentController: VICKYSUN180 Schedule: New
1	Today, 8:47 AM	Created file	FactoryTalk Ser...	

A new version, version 3 is created. This file will be checked out, and later changes will be compared against it.

The screenshot shows the 'History' tab in the FactoryTalk AssetCentre interface. The 'Range' section has 'Most recent 100 records' selected. The 'Filter' section has 'Version-related activities' selected. The 'Get Version', 'Pin Version', and 'Promote' buttons are visible. The history table shows three versions:

Version	Time	Action	User	Comments
3	Today, 9:03 AM	Promoted version "1" to "3"	VICKYSUN180\...	
2	Today, 8:54 AM	Added new version	FactoryTalk Ser...	AgentController: VICKYSUN180 Schedule: N
1	Today, 8:47 AM	Created file	FactoryTalk Ser...	

4. Select **Check Out**. This file will be checked out to your working folder.

The screenshot shows the 'Archive' tab in the FactoryTalk AssetCentre interface. The 'Check Out' button is highlighted with a red box. The 'ViewSE App' is selected. The 'Description' field is empty, and the 'Working folder' is 'C:\Users\Administrator\Desktop\Working Folder'. The history table is visible below:

Version	Time	Action	User	Comments
3	Today, 9:03 AM	Promoted version "1" to "3"	VICKYSUN180\...	
2	Today, 8:54 AM	Added new version	FactoryTalk Ser...	AgentController: VICKYSUN180 Schedule: N
1	Today, 8:47 AM	Created file	FactoryTalk Ser...	

5. Use **FactoryTalk View SE Application Manager** to restore the application. After that, check in this file.

The screenshot shows the 'Archive' tab in the FactoryTalk AssetCentre interface. The 'Check In' button is highlighted with a red box. The 'ViewSE App' is selected. The 'Description' field is empty, and the 'Working folder' is 'C:\Users\Administrator\Desktop\Working Folder'. The history table is visible below:

Version	Time	Action	User	Comments
3	Today, 9:03 AM	Promoted version "1" to "3"	VICKYSUN180\...	
2	Today, 8:54 AM	Added new version	FactoryTalk Ser...	AgentController: VICKYSUN180 Schedule: N
1	Today, 8:47 AM	Created file	FactoryTalk Ser...	



## Export HMI server components

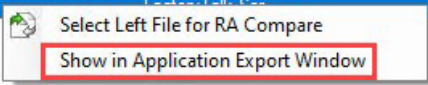
You can also use the Application Export function in FactoryTalk AssetCentre to export the HMI server components. These following steps introduce how to recover displays from an archived application by using this function.

### To export HMI server components

- 1. In the FactoryTalk AssetCentre, select  **Archive**.
- 2. Select an asset whose file that you want to recover, right-click the desired version (**Version 1** in this example), and then select **Show in Application Export Window**.

3. You can get a writable copy if needed. Select **OK**.

Version	Time	Action	User	Comments
2	Today, 10:19 AM	Added new version	FactoryTalk Ser...	AgentController:
1	Today, 9:32 AM	Created file	FactoryTalk Ser...	



- Select Left File for RA Compare
- Show in Application Export Window

Get

☒ Get writable copy

☒ Recursively get files from subfolders

☐ Overwrite checked-out files

☐ Override local name:

ViewSE\_App\_Backup.apb

☐ Override working folders with path:

Browse...

Comments:

OK Cancel Help

- 4. Select the browse button under **Server Name**.

Export ViewSE\_App\_Backup.apb: Version 1

<input type="checkbox"/>	Area	Server Type	Server Name	Primary Host	Secondary Host
<input type="checkbox"/>	Line1_HMI	HMI Server	FTViewDemo_HMI	VICKYSUN180	Unavailable

☐ Export FactoryTalk Directory backup file

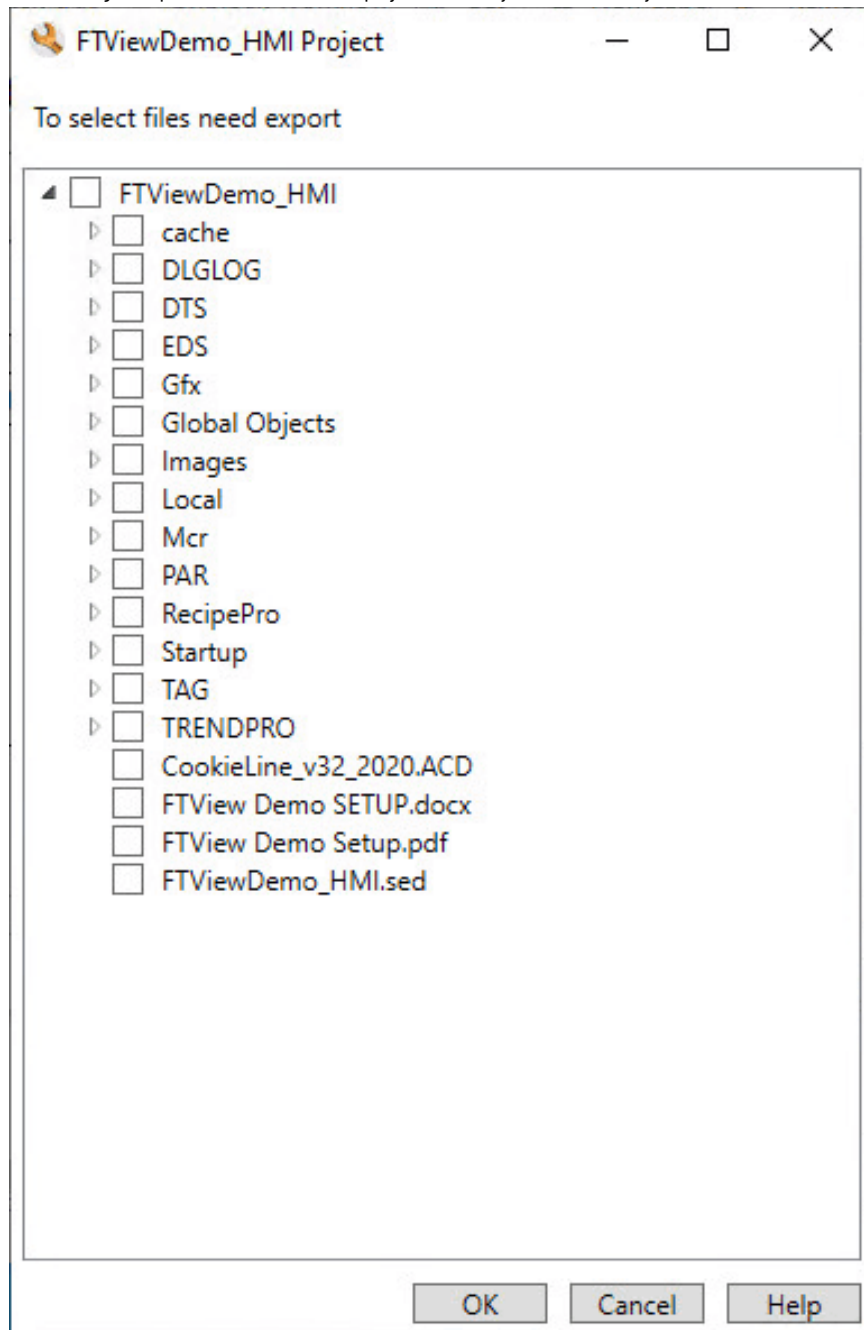
Target Folder:

Export Cancel Help



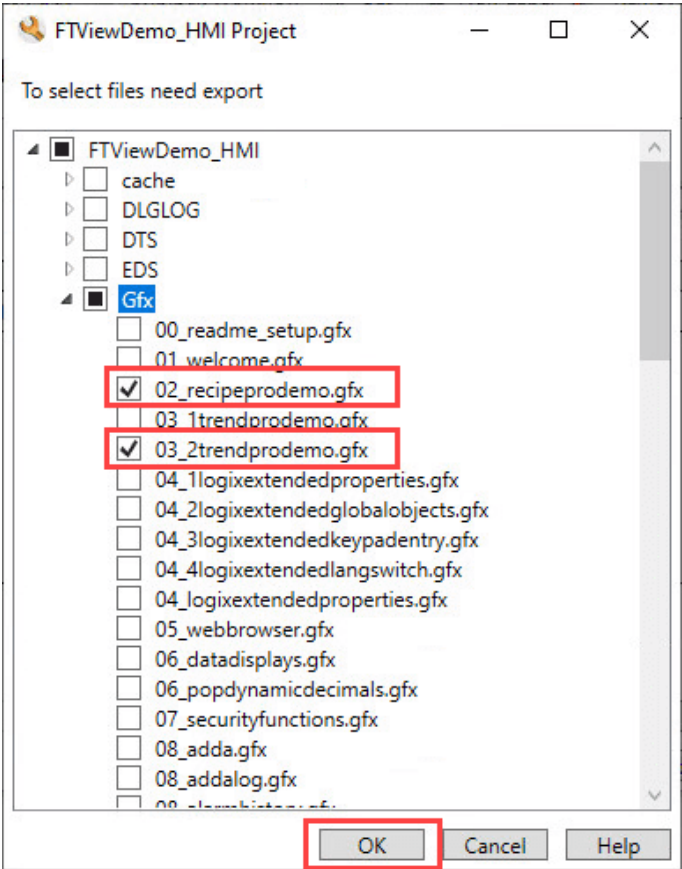
**Tip:** The application export dialog box extracts the HMI server project from the FactoryTalk View SE application file (APB). This function allows you to export specific files out of the HMI server project without having to check out the application from the archive.

A new dialog box opens with the HMI server project files. They are all cleared by default.




- 5. Select the files that you want to recover, and then select **OK**.

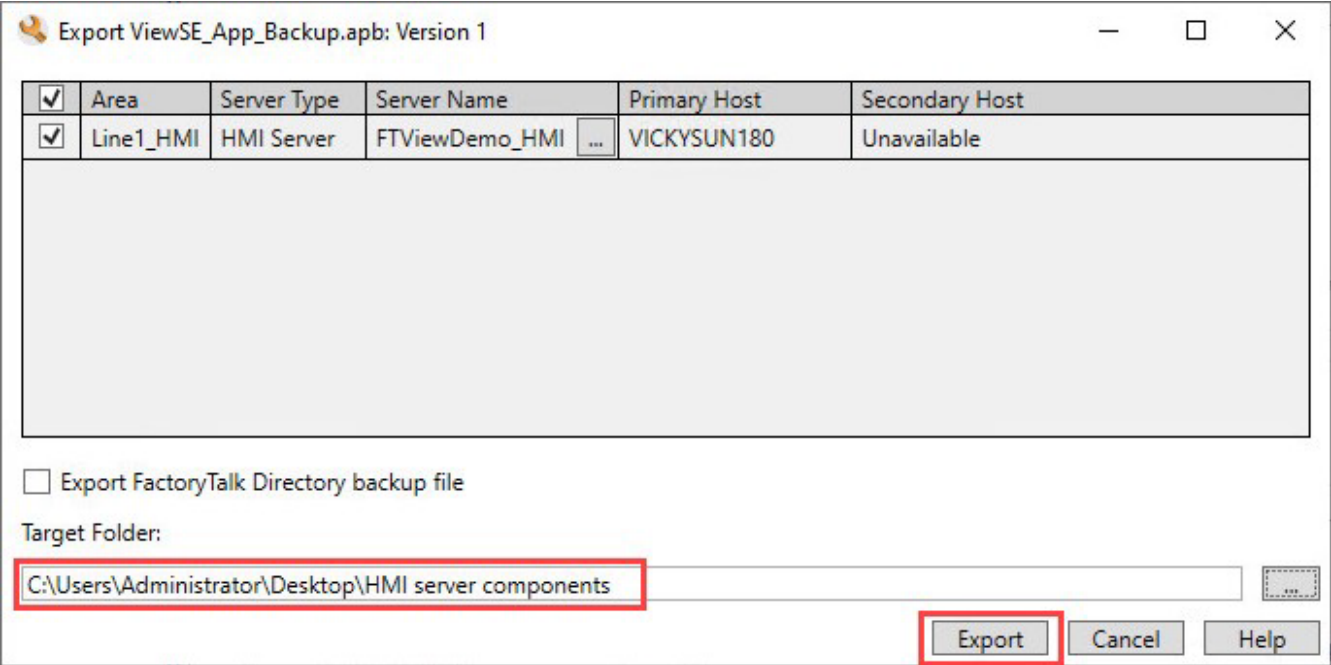
In this example, two displays are selected.



- 6. Select a target folder to export the files, and then select **Export**.

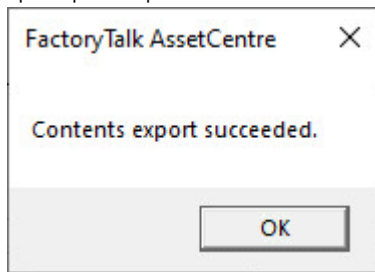
 **Tip:** Hover over the items to see the last time they were modified.

In this example, the desktop is selected as the target folder.

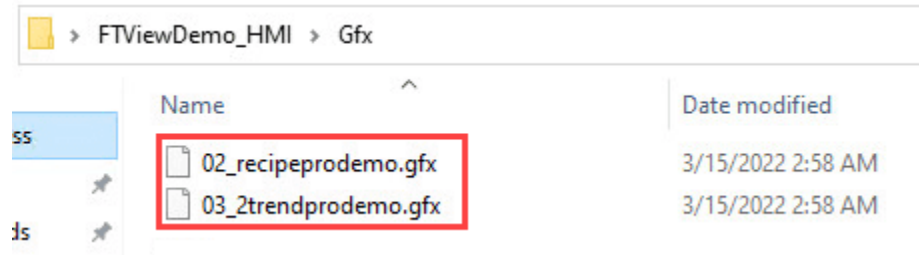




7. Upon export completion, select **OK**.



The displays are exported in the designated folder.



## Product policies and securable actions supported by FactoryTalk Security

This appendix lists the product policies and securable actions of Studio 5000 Logix Designer, FactoryTalk View SE, and FactoryTalk AssetCentre.

### Product policies and securable actions of Studio 5000 Logix Designer

The product policies and securable actions cover Studio 5000 Logix Designer version 21 or later, RSLogix 5000 version 20, and Logix 5000 controllers.

This table lists FactoryTalk Security Product Policies.

Grant access to these actions	To allow a user to
Controller: Secure	Secure a project or controller.
Firmware: Update	Update controller firmware. <b>Tip:</b> If the project is secured, the Securable Action (Firmware:Update) is also required to perform firmware updates. Firmware updates can be initiated within the <Product_Name_RSL5K> application WhoActive dialog box if a project is open but not when the controller is online.
Print: Modify Options	Modify print options.
Project: New	Create a new project, import a project or translate <P5>/<SLC>.
Toolbar: Configure	Move, resize, hide or show toolbars.
Workstation: Modify Options	Modify workstation options.

This table lists FactoryTalk Security Securable Actions.

Grant access to these actions	To allow a user to
Add-On Instruction: Create	Create an Add-On Instruction.
Add-On Instruction: Delete	Delete an Add-On Instruction.
Add-On Instruction: Export	Export an Add-On Instruction.
Add-On Instruction: Export Unencoded	Export an Add-On Instruction in clear text. <b>Tip:</b> Users must also be granted the <b>Add-On Instruction: Export</b> permission to export an AOI, or granted the <b>Project: Export</b> permission to export the entire project. <b>Tip:</b> To export in clear text, you must clear the <b>Encode Protected Content</b> checkbox on the Export dialog box. You must also have the required source key or license if the component is protected with Source Protection.
Add-On Instruction: Modify	Edit Add-On Instruction properties, tags, logic or whether a user can configure source protection.
Add-On Instruction: View Logic	View the internal information in an Add-On Instruction.
Alarm Definition: Create	Create new alarm definitions. An alarm definition is associated with an Add-On Instruction (AOI) or a defined data type. When a tag is created using a data type or an AOI that has alarm definitions, alarms are created automatically based on the alarm definitions.
Alarm Definition: Delete	Delete alarm definitions. When a user who is granted the <b>Alarm Definition: Delete</b> permission deletes an alarm definition for a data type or an Add-On Instruction (AOI), the corresponding alarms based on the alarm definition are deleted, even if the user has not been granted the <b>Alarm: Delete</b> permission.

	When a user deletes a data type or an AOI, all alarm definitions associated with that data type or AOI are deleted, even if the user has not been granted the <b>Alarm Definition: Delete</b> permission.
Alarm Definition: Modify Properties	Modify the properties of a tag-based alarm. When a user who is denied the <b>Alarm Definition: Modify Properties</b> permission imports a project or a project component that requires changes to existing tag-based alarm definitions, the import fails.
Alarm Definition: Modify Required Use	Modify Required to be used and evaluated for all alarm instances. When a user is denied this permission, the user will be unable to modify the <b>Required to be used and evaluated for all alarm instances</b> in the <Product_Name_RSL5K> application and Logix Services.
Alarm: Clear Alarm Log	Clear the contents of the alarm log from the controller.
Alarm: Configure Direct Commands	Respond to a tag-based alarm using the <b>Acknowledge</b> , <b>Shelve</b> , <b>Disable</b> , and <b>Reset</b> buttons on the <b>Alarm Properties</b> dialog box - <b>Status</b> tab.
Alarm: Create	Create new tag-based alarms. When a user who is denied the <b>Alarm: Create</b> permission imports a project or a project component that requires new alarms to complete the import, those alarms are created.
Alarm: Delete	Delete tag-based alarms. When a user who is granted the <b>Tag: Delete</b> permission deletes a tag that has alarms associated with it, those alarms are deleted.
Alarm: Modify Properties	Modify the properties of a tag-based alarm. <b>Tip:</b> When a user who is denied the <b>Alarm: Modify Properties</b> permission imports a project or a project component that requires changes to existing tag-based alarms, the import fails.
Alarm: Modify Use	Modify Use and evaluate alarm. Marks all alarm instances as active and ready for evaluation. This checkbox is cleared by default. Enable or disable a tag-based alarm using the <b>Use and evaluate alarm</b> checkbox on the <b>Alarm Properties</b> dialog box - <b>Advanced</b> tab.
Component: Modify Permission Set	Change which permission set is associated with a component.
Controller: Clear Faults	Edit the fault log, including clearing faults.
Controller: Lock/Unlock	Lock or unlock the controller for online edits.
Controller: Modify Mode	Change controller modes.
Controller: Modify Properties	Edit controller properties.
Controller: Modify Revision	Convert the .acd file to a higher revision.
Controller: Modify Type	Change controller types. If a user is granted <b>Controller: Modify Revision</b> privilege, but is denied <b>Controller: Modify Type</b> , in most situations the user will be unable to change the type of controller.
Controller: Unsecure	Unsecure a secured controller.
Data Log: Create	Create a data log.
Data Log: Modify	Modify a data log.
Data Log: Delete	Delete a data log.
Data Log: Enable/Disable	Enable or disable data logging.
Data Log: Read Log Data Value	Read a data log value.
Data Log: Clear Log Data Value	Clear a data log value.
Firmware: Update	Use the <Product_Name_RSL5K> application to update controller firmware.

## Appendix A Product policies and securable actions supported by FactoryTalk Security

	The Product Policy (Firmware:Update) is also required to perform firmware updates. Firmware updates can be initiated within the <Product_Name_RSL5K> application <b>WhoActive</b> dialog box if a project is open, but not when the controller is online.
Language: Modify Properties	Associate project documentation with a language, set default language, add or delete a language.
Language: Switch Language	Select a different language for product documentation.
Module: Create	<p>Create modules in the Controller Organizer.</p> <ul style="list-style-type: none"> <li>If <b>Module: Create</b> is denied, the <b>New module</b> and <b>Paste</b> options are not enabled on the I/O tree menu. The <b>Import Module</b> option is enabled.</li> </ul> <p>A message displays that states that <b>Module: Create</b> must be granted. Selecting <b>OK</b> to import a module is not successful, and the dialog box closes.</p> <ul style="list-style-type: none"> <li>If the <b>Select Module Type</b> dialog box is open and <b>Module: Create</b> is denied, the <b>Create</b> option is enabled unless you select a different module in the dialog box.</li> </ul> <p>If you select <b>Create</b>, the create wizard launches.</p> <p>If the create wizard is open and <b>Module: Create</b> is denied, you can perform all the steps to configure the module. When you select <b>OK</b> to create the module, you receive the error <b>Module: Create</b> needs to be granted.</p>
Module: Create and Safety: Modify Component	<p>Create safety I/O configuration.</p> <ul style="list-style-type: none"> <li>Denying <b>Safety: Module Component</b> does not affect the ability to create a safety module.</li> <li>If <b>Module: Create</b> is granted, but <b>Safety: Module Component</b> is denied, you can create safety modules.</li> </ul>
Module: Delete	<p>Delete modules in the Controller Organizer.</p> <ul style="list-style-type: none"> <li>If <b>Module: Delete</b> is denied, the <b>Cut</b> and <b>Delete</b> options are not enabled on the I/O tree menu.</li> <li>If you select the <b>Cut</b> or <b>Delete</b> option, you receive a confirmation message, then a <b>Module: Delete</b> is denied message. When you select <b>OK</b>, you receive the error <b>Module: Delete</b> needs to be granted.</li> </ul>
Module: Delete and Safety: Modify Component	<p>Delete safety I/O configuration.</p> <ul style="list-style-type: none"> <li>Denying <b>Safety: Module Component</b> does not affect the ability to delete a safety module, or a sub-tree that contains safety modules.</li> <li>If <b>Module: Delete</b> is granted, but <b>Safety: Module Component</b> is denied, you can delete a safety module, or a sub-tree that contains safety modules.</li> </ul>
Module: Maintenance High	Perform high impact operations such as module reset and calibration.
Module: Maintenance Low	Perform low impact operations such as resetting electronic fuses.
Module: Modify Properties	<p>Edit module properties.</p> <p>If <b>Module: Module Properties</b> is denied, edit the configuration in the profile, including the Module Definition in an Add-On Profile.</p> <p>When you select <b>OK</b> or <b>Apply</b>, you receive the error <b>Module: Modify Properties</b> needs to be granted.</p>
Module: Modify Properties and Safety: Modify Component	<p>Modify safety I/O configuration.</p> <ul style="list-style-type: none"> <li><b>Safety: Module Component</b> affects only safety-related areas of profiles.</li> <li>If <b>Safety: Module Component</b> is denied, the <b>Safety Network Number</b> dialog box on the <b>General</b> page of either a Classic or Add-On Profile cannot be opened.</li> <li>If the <b>Safety Network Number</b> dialog box is already open when <b>Safety: Module Component</b> is changed from granted to denied, then you can complete the operation to change the <b>Safety Network Number</b> and successfully apply the updates.</li> <li>If <b>Safety: Module Component</b> is denied, all controls that modify safety-related configuration are disabled when you select a different page, or select a different menu option. Some controls such as the <b>Safety Input RPI</b> on the</li> </ul>

	<p><b>Safety</b> page, remain enabled, but only if the <b>Safety</b> page is current when <b>Safety: Module Component</b> changed from granted to denied.</p> <ul style="list-style-type: none"> <li>If <b>Safety: Module Component</b> is denied, the <b>Advanced Connection Reaction Time Limit Configuration</b> dialog box on the <b>Safety</b> page cannot be open.</li> </ul> <p>If the <b>Advanced Connection Reaction Time Limit Configuration</b> is already open when <b>Safety: Module Component</b> is changed from granted to denied, then you can complete the operation to change and accept the updates and they are successfully applied.</p> <p>If there are pending edits to any safety-related control when <b>Safety: Module Component</b> is changed from granted to denied, then you can accept the updates and they are successfully applied.</p>
Module: View Properties	<p>View module properties.</p> <p>Users with this permission can open device profiles and, when online with the controller, use the profile to directly interact with modules and carry out actions such as changing IP addresses.</p> <p>When this permission is denied, users cannot open device profiles.</p>
Motion: Command Axis	Perform axis direct commands.
Motion: Modify Configuration	Modify axis, coordinate system, or motion group properties.
Nonvolatile Memory: Load	Load from non-volatile memory.
Nonvolatile Memory: Store	Store to non-volatile memory.
Phase: Create	Create equipment phases.
Phase: Delete	Delete equipment phases.
Phase: Manual Control	Manually control equipment phases.
Phase: Modify Properties	Edit equipment phases.
PLC/<SLC>: Modify Tag Mappings	Map PLC or <SLC> messages.
Plug-In: Display	Display plug-ins.
Print: Report	Print reports.
Program: Create	Create programs.
Program: Create and Safety: Modify Component	Create a safety program.
Program: Delete	Delete programs.
Program: Delete and Safety: Modify Component	Delete a safety program.
Program: Modify Properties	Edit program properties.
Program: Modify Properties and Safety: Modify Component	Modify properties of a safety program.
Program: Modify Properties and Safety: Modify Component	Change class property of a standard program to safety.
Project: Compact	Compact a project file.
Project: Download	Download a project to a controller.
Project: Export	Save a project in .L5K or .L5X format.
Project: Go Online	Go online with a project.
Project: Modify Path	Set, clear, or modify the controller path associated with a given project.
Project: Open	<p>Open a (read-only) version of the project.</p> <p>If users do not have the ability to open and view the project, they do not have the ability to do anything else with it.</p>
Project: Save	Save a project.
Project: Save As	Save a project to a new .acd file.

## Appendix A Product policies and securable actions supported by FactoryTalk Security

Project: Upload	Upload a project from a controller.
Routine: Create	Create a routine.
Routine: Create and Safety: Modify Component	Create a safety routine.
Routine: Delete	Delete a routine.
Routine: Delete and Safety: Modify Component	Delete a safety routine.
Routine: Export	Export a routine.
Routine: Export Unencoded	Export a routine in clear text.
Routine: Manual Control	Manually control routine logic.
Routine: Modify Logic	Edit routine logic.
Routine: Modify Logic and Safety: Modify Component	Edit safety routine logic.
Routine: Modify Properties	Edit routine properties, configure routine source protection.
Routine: Modify Properties and Safety: Modify Component	Edit safety routine properties.
Routine: View Logic	View the logic in a routine.
Safety: Generate/Delete Signature	Generate or delete a Safety Signature.
Safety: Lock/Unlock	Lock or unlock edits on safety application.
Safety: Lock/Unlock	Modify safety lock or unlock passwords.
Safety: Modify Component	<p>Create, delete, or modify safety components.</p> <p><b>Tip:</b> The standard component privileges are required in addition to this privilege. For example, to create safety tags, the <b>Tag: Create</b> privilege is required in addition to the <b>Safety: Modify Components</b> privilege.</p> <ul style="list-style-type: none"> <li>If <b>Module: Create</b> is denied, the <b>New module</b> and <b>Paste</b> options are not enabled on the I/O tree menu. The <b>Import Module</b> option is enabled.</li> </ul> <p>A message displays that states that <b>Module: Create</b> must be granted. Selecting <b>OK</b> to import a module is not successful, and the dialog box closes.</p> <ul style="list-style-type: none"> <li>If the <b>Select Module Type</b> dialog box is open and <b>Module: Create</b> is denied, the <b>Create</b> option is enabled unless you select a different module in the dialog box.</li> </ul> <p>If you select <b>Create</b>, the create wizard launches.</p> <p>If the create wizard is open and <b>Module: Create</b> is denied, you can perform all the steps to configure the module. When you select <b>OK</b> to create the module, you receive the error <b>Module: Create</b> needs to be granted.</p>
Safety: Modify Properties	Modify the controller's safety configuration.
Safety: Modify Tag Mappings	Create safety tag mapping.
Safety: Modify Tag Mappings	Delete safety tag mapping.
Safety: Modify Tag Mappings	Modify safety tags mapped to standard tags.
Sequence: Create	Create an equipment sequence.
Sequence: Delete	Delete an equipment sequence.
Sequence: Manual Control	Take manual control of an equipment sequence.
Sequence: Modify Properties	Modify the properties of an equipment sequence.
Tag: Create	Create tags.
Tag: Create and Safety: Modify Component	Create a safety tag.
Tag: Delete	Delete tags.



Tag: Delete and Safety: Modify Component	Delete a safety tag.
Tag: Delete, Safety: Modify Tag Mappings, and Safety: Modify	Delete standard tag that is mapped to a safety tag.
Tag: Force	Force tags and enable or disable existing forces.
Tag: Force and Safety: Modify Component	Force safety tags.
Tag: Modify Constant Property	Change Constant property of a tag.
Tag: Modify Constant Tag Values	Change values of a Constant Tag.
Tag: Modify Properties	Edit tag properties.
Tag: Modify Properties and Safety: Modify Component	Edit safety tag properties.
Tag: Modify Properties and Safety: Modify Component	Change class property of a standard tag to safety.
Tag: Modify Properties and Safety: Modify Tag Mappings	Modify safety or standard tag properties of a tag contained in a safety mapping.
Tag: Modify Values	Change tag values.
Tag: Modify Values and Safety: Modify Component	Change safety tag values.
Task: Create	Create tasks.
Task: Delete	Delete tasks.
Task: Modify Properties	Edit task properties, including program scheduling.
Task: Modify Properties and Safety: Modify Component	Modify safety task properties.
Trend: Create	Create trends.
Trend: Delete	Delete trends.
Trend: Modify Properties	Modify trend properties.
Trend: Run	Run trends.
User Defined Type: Create	Create user-defined data types or string types.
User Defined Type: Delete	Delete user-defined data types or string types.
User Defined Type: Modify	Edit user-defined data types or string types.

1 A safety program's max scan time can be reset, regardless of the protection.

2 The safety task max scan time and max/min interval scan timers can be reset, regardless of the protection.

## Product policies and securable actions of FactoryTalk View SE

This table lists FactoryTalk Security Product Policies.

This policy setting	Controls whether users can
Configure FTView SE Website	Have access to the FactoryTalk View SE Website configurator.

This table lists FactoryTalk Security Securable Actions.

To do this	You need these additional security permissions
Create a recipe	RecipePro: Create
Delete a recipe	RecipePro: Delete

## Appendix A Product policies and securable actions supported by FactoryTalk Security

Download a recipe	RecipePro: Download
Duplicate a recipe	RecipePro: Create
Edit a recipe	RecipePro: Edit
Modify a tag set	RecipePro: Edit RecipePro: Modify TagSet
Import a recipe	RecipePro: Create RecipePro: Edit RecipePro: Modify TagSet
Rename a recipe	RecipePro: Edit
Upload a recipe	RecipePro: Edit RecipePro: Upload
Upload and create a recipe	RecipePro: Create RecipePro: Upload
RecipeProDownload command	RecipePro: Download
RecipeProUpload command	RecipePro: Edit RecipePro: Upload

## Product policies and securable actions of FactoryTalk AssetCentre

This table lists FactoryTalk Security Product Policies.

This policy setting	Controls whether users can
View Address Book	View the Address Book (which contains addresses for the purpose of sending automatic email notifications).
Edit Address Book	Edit or add contacts and groups in the Address Book (which contains addresses for the purpose of sending automatic email notifications).
Override Archive Check In	Check in a file regardless of who checked it out or from where it was checked out.
Configure Database Limitations	Configure the total maximum size of the AssetCentre database, the size warning levels, the maximum number of versions per archive asset, the maximum size of Event, Audit, and Diagnostics logs, and the database capacity status refresh rate.
Configure Archive Options Settings	Turn on or off the function that allows Logix Designer to perform archive activities, such as file check-in, without direct interaction with the FactoryTalk AssetCentre client.
Override Archive Undo Check Out	Undo a check out even if a different user checked out the file.
Override Removal of Local Copies	Choose to keep local copies of checked-in files on their computer. If this right is allowed, the user can keep local copies. If this right is denied, the user is not given this option.
Configure Personal Archive File Associations	Configure which software product launches when opening a particular type of file. If a personal file association is set, it will take precedence over the system file association.
Configure System Archive File Associations	Configure which software product launches when opening a particular type of file. This setting applies unless the user has specified a personal file association.
Configure Personal Archive Working Folders	Set a personal working folder for checking out files.
Configure System Archive Working Folders	Set the system working folder to which all users check out files unless they have a personal working folder.
Run Archive Database Cleanup Wizard	Run the Archive Database Cleanup Wizard to delete unused versions of files.
Allow Empty Comment at Check In	Leave the comment field empty as they check in an asset.
Allow Empty Comment at Check Out	Leave the comment field empty as they check out an asset.

Clear the Get Writable Copy checkbox by default	Enable or clear the Get Writable Copy checkbox during get. Denying this permission enables the Get Writable Copy checkbox; a Get retrieves a writable copy of an Archive object. Allowing this permission (by default) clears the Get Writable Copy checkbox; a Get retrieves a read-only copy of an Archive object.
Store latest version only	Choose to store only the latest version in the Archive.
Set maximum versions	Configure the total maximum number of versions stored in the Archive.
Configure Asset Inventory Settings	Configure the settings in the Asset Inventory window.
Configure Assets Lifecycle Sync	Synchronize life cycle information in the FactoryTalk AssetCentre server and client with the <a href="#">Rockwell Automation life cycle website</a> .
Display Calibration Management Data*	View Calibration Management data in FactoryTalk AssetCentre.
Perform Calibration Management*	Access Calibration Management functionality in ProCalV5 software.
Administer Calibration Users*	Administer users, groups, and permissions in ProCalV5 software. Note that this policy only determines if the user is automatically added to the Administrator group in the ProCalV5 software. Once the user is added to ProCalV5, changing this policy for an AssetCentre user does not change the user's ProCalV5 security permissions.
Configure Database Maintenance	Configure automatic database maintenance, manually analyze, or rebuild index fragmentation.
Switch to Design mode	Enter Design mode, in which the user can edit the asset tree.
View Event Log	Show the Event Log and run a search on the Event Log.
View Audit Log	Show the Audit Log and run a search on the Audit Log.
View Diagnostics and Health Log	Show the Diagnostics and Health Log and run a search on the Diagnostics and Health Log.
Change Diagnostics and Health Log Message	Change the status of or add a comment to a Diagnostics and Health Log record.
View Diagnostics and Health Log Status	View a status history for a Diagnostics and Health Log record.
Run Log Database Cleanup Wizard	Run the Log Database Cleanup Wizard to remove old records from the logs. Data can be exported and saved in a separate file.
Enable or Disable DTMs*	Enable and disable DTMs in the DTM Catalog.
Edit DTM Network*	Show the DTM Networks dialog box to edit the DTM network.
Run PDC Field Edition*	Use the Process Device Configuration Field Edition software.
Create a new schedule	Create a schedule.
Edit a schedule	Change existing schedules.
Delete a schedule	Delete schedules.
View a schedule	Show the Schedules tab.
Command a schedule	Issue commands to a schedule, such as making the schedule active or running the schedule immediately.
Create a search	Set up a new search to find entries matching specified criteria in one of the logs, in the Archive History, or in Archive Check Out Status information.

\* Starting from FactoryTalk AssetCentre version 10.00, process device capabilities are not supported. The policies marked with asterisk are only kept for viewing purposes if you have upgraded FactoryTalk AssetCentre from version 9.00 or earlier.

This table lists FactoryTalk Security Securable Actions.

This action...	Allows you to...
AssetCentre	
CheckIn does not require MoC workflow	Turn off Management of Change workflow when checking in selected files and binders associated with the selected asset. Select <b>Deny</b> box to require Management of Change workflow on check-in operation.

## Appendix A Product policies and securable actions supported by FactoryTalk Security

CheckOut - CheckIn	Check out or check in files associated with the selected asset.
CheckOut does not require MoC workflow	Turn off Management of Change workflow when checking out files and binders associated with the selected asset. Select <b>Deny</b> box to require Management of Change workflow on check-out operation.
Get	Get a copy of the file or files associated with the selected asset from <b>Archive</b> .
Label	Apply a descriptive Label to a version of a file associated with the selected asset in <b>Archive</b> .
Pin	Pin a version of a file associated with the selected asset.
Promote	Store an old version of the file as the most recent version.
Set Store Latest Version	Specify that only the most recent version of the file associated with the selected file asset should be retained.
Set Working Folder	Set the working folder for files associated with the selected asset.
Unblock MoC workflow	Reset the Management of Change workflow status of files and binders associated with the selected asset.
Undo CheckOut	Undo a check-out operation for files associated with the selected asset. See Help. Select <b>Help &gt; Contents</b> . Open the Archive topic and click the <b>Undo a check-out</b> topic.
<b>Common</b>	
Configure Security	Change security settings for the selected asset.
Create Children	Add assets underneath the selected asset (only if the selected asset is a container or device-type asset).
Delete	Delete the selected asset from the asset tree.
Execute	This setting is not applicable in this release of the FactoryTalk AssetCentre software.
List Children	Show children of the selected asset. If a user does not have this right, they will not be able to expand the selected asset to see assets that it contains. If you set this right to <b>Allow</b> , also set the <b>Read</b> right for this asset to <b>Allow</b> .
Read	Show the selected asset in the asset tree. Show the selected asset's properties.
Write	Change the selected asset's properties.

# Rockwell Automation Support

Use these resources to access support information.

Technical Support Center	Find help with how-to videos, FAQs, chat, user forums, and product notification updates.	<a href="https://rok.auto/support">rok.auto/support</a>
Knowledgebase	Access Knowledgebase articles.	<a href="https://rok.auto/knowledgebase">rok.auto/knowledgebase</a>
Local Technical Support Phone Numbers	Locate the telephone number for your country.	<a href="https://rok.auto/phonesupport">rok.auto/phonesupport</a>
Literature Library	Find installation instructions, manuals, brochures, and technical data publications.	<a href="https://rok.auto/literature">rok.auto/literature</a>
Product Compatibility and Download Center (PCDC)	Get help determining how products interact, check features and capabilities, and find associated firmware.	<a href="https://rok.auto/pcdc">rok.auto/pcdc</a>

## Documentation feedback

Your comments help us serve your documentation needs better. If you have any suggestions on how to improve our content, complete the form at [rok.auto/docfeedback](https://rok.auto/docfeedback).

## Waste Electrical and Electronic Equipment (WEEE)



At the end of life, this equipment should be collected separately from any unsorted municipal waste.

Rockwell Automation maintains current product environmental information on its website at [rok.auto/pec](https://rok.auto/pec).

Rockwell Otomasyon Ticaret A.Ş. Kar Plaza İş Merkezi E Blok Kat:6 34752 İçerenköy, İstanbul, Tel: +90 (216) 5698400 EEE Yönetmeliğine Uygundur

Connect with us.

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

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444

EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640

ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846