Configure System Security Features
Important User Information

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

## Preface
- Certification Requirements ........................................ 5
- Design Recommendations ........................................... 7
  - Follow Design and Engineering Best Practices ................. 7
  - Microsoft Active Directory Group Policy .................... 7
- Secure System Elements ............................................ 8
- Manual Organization ................................................ 9
- Additional Resources .............................................. 11

## Chapter 1
Configure Infrastructure Components
- Requirements ......................................................... 13
- Windows Domain .................................................... 14
- Domain Controller .................................................. 15
  - Active Directory ................................................. 16
- Create Users and Groups in the Windows Domain ............... 16
- Group Policy Management ....................................... 17
- Add Servers or Computers to the Windows Domain ............ 18

## Chapter 2
Configure FactoryTalk Components
- FactoryTalk Directory Requirements .............................. 19
- FactoryTalk Directory Components ............................... 20
- Configure the FactoryTalk Directory ............................. 21
  - Define Network Directory .................................. 23
- Configure FactoryTalk Activation Manager ..................... 26
- Configure FactoryTalk Policy Manager ......................... 26

## Chapter 3
Configure FactoryTalk Security
- FactoryTalk Security Components ................................ 31
- Configure FactoryTalk Administration Console ................. 32
  - Verify User Identity ......................................... 32
  - Select the FactoryTalk Directory ............................ 32
- Security Requirements ............................................ 33
- Configure FactoryTalk Users and Groups ....................... 34
  - Remove the All Users Group ................................ 34
  - Assign Windows-linked User Groups to FactoryTalk Directory ........................................ 36
- Configure the System Policies .................................. 42
  - Configure the Application Authorization Policy ............ 45
  - Configure the User Rights Assignment Policy .............. 46
  - Configure the Live Data Policy ............................... 49
  - Configure the Health Monitoring Policy ...................... 50
  - Configure the Audit Policy ................................ 51
  - Configure the Security Policy ............................... 52
# Table of Contents

Configure the Product Policies ........................................... 54
Configure the Product Policies Feature Security ........................ 57
  Product Policies ...................................................... 57
  Product Policies for Individual Software Applications .......... 59
Configure Feature Security for FactoryTalk AssetCentre Users ... 62
  Policy Settings ...................................................... 65
Configure Feature Security for RSLogix 5000 Users .................. 67
  Configure Feature Security for Product Policies .................. 68
  Configure Security Securable Actions ............................ 70
Configure the Security Authority Identifier ............................ 81
  Create a Permission Set ............................................ 82
  Create a Controller Logical Name .................................. 85
  Configure the Security Authority Identifier ...................... 86
  Configure Communication Restrictions ............................ 88
  Configure Data Restrictions ....................................... 89
  Configure Code Restrictions ...................................... 91

## Chapter 4

**Configure FactoryTalk AssetCentre Features**

Audit and Change Management ........................................... 96
  Create a Schedule for a Device Monitor - Change................. 97
  View and Search Logs .............................................. 110
Backup ........................................................................ 121
  Master Files ......................................................... 121
  Create a Schedule for a Disaster Recovery Operation .......... 122

**Security Checklists**

Two Types of Security Verification ...................................... 137
  Security Requirements .............................................. 137
  Acceptance Testing Verification Checklist ......................... 138
  Maintenance Verification Checklist ................................ 139

**Index** .......................................................................... 141
Preface

This manual describes the system-level configuration requirements to use a ControlLogix® 5580 controller that has achieved IEC 62443-4-2:2019 certification. In the rest of this publication, it is referred to as IEC-62443-4-2 SL 1 certification.

Rockwell Automation considered Threat level - SL 1: Protection against casual or coincidental violation when it completed activities to achieve IEC-62443-4-2 SL 1 certification.

For the definition of the SL 1 threat level and other SL threat levels, see the IEC-62443-3-3 International Standard available from the International Electromechanical Commission (IEC) at https://www.iec.ch/index.htm.

You must be trained and experienced in creating, operating, and maintaining industrial security programs before you complete the tasks described in this publication.

Certification Requirements

The following table describes the IEC-62443-4-2 SL 1 certification configuration requirements that you must meet.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meet product-level requirements</td>
<td>You must meet product-level requirements regarding IEC-62443-4-2 SL 1 certifications. ControlLogix 5580 controllers have IEC-62443-4-2 SL 1 certification. To achieve that certification, you must not only meet the system-level requirements that are described in this publication. You must also meet the product-level requirements that are described in the ControlLogix 5580 and GuardLogix® 5580 Controllers User Manual, publication 1756-UM543.</td>
</tr>
<tr>
<td>Use ControlLogix 5580 controller</td>
<td>You must use one of the controllers in the ControlLogix 5580 controller family, and the controller must use firmware revision 32.011 or later. IMPORTANT: Only the ControlLogix 5580 controllers have achieved IEC-62443-4-2 SL 1 certification. No other Logix 5000™ controllers are IEC-62443-4-2 SL 1-certified.</td>
</tr>
<tr>
<td>Controller access</td>
<td>You must actively manage physical access to the ControlLogix 5580 controller. As necessary, secure the controller’s location, for example, in a cabinet, to help prevent unauthorized users from accessing it.</td>
</tr>
</tbody>
</table>
You must include compensating countermeasures when you configure a system with a ControlLogix 5580 controller that has achieved IEC-62443-4-2 SL 1 certification. The following compensating countermeasures are **required**:

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include compensating countermeasures</td>
<td><strong>Active Directory</strong> Windows-based service that runs on a domain controller and stores information about objects on a network.</td>
</tr>
<tr>
<td>Manage physical access to the controller</td>
<td><strong>ControlFLASH™</strong> Version 15.01 or later <strong>required</strong> Software tool that is used for electronically updating firmware in hardware devices.</td>
</tr>
<tr>
<td></td>
<td><strong>ControlFLASH Plus™</strong> Version 2.00 or later <strong>required</strong> Software tool that is used for electronically updating firmware in hardware devices. ControlFLASH Plus only supports the firmware updates for CIP™ devices.</td>
</tr>
<tr>
<td></td>
<td><strong>FactoryTalk® Activation Manager</strong> Version 4.03.03 or later <strong>required</strong> Provides a secure, software-based system to apply Rockwell Automation® licenses for continuous use of FactoryTalk software and other Rockwell Automation software products.</td>
</tr>
<tr>
<td></td>
<td><strong>FactoryTalk AssetCentre</strong> Version 9.00 or later <strong>required</strong> Centralized tool used to secure, manage, version, track, and report information about assets in a system automatically. The software helps to prevent unauthorized or unwanted changes that can impact a secure control system.</td>
</tr>
<tr>
<td></td>
<td><strong>FactoryTalk Linx</strong> Version 6.11 or later <strong>required</strong> Server and communications service that is designed to deliver control system information from Allen-Bradley® control products to the FactoryTalk software portfolio and Studio5000® Logix Designer software. Supports CIP Security™.</td>
</tr>
<tr>
<td></td>
<td><strong>FactoryTalk Policy Manager</strong> Version 6.11 or later <strong>required</strong> Secure configuration tool that is one of a set of products that Rockwell Automation uses to implement CIP Security™.</td>
</tr>
<tr>
<td></td>
<td><strong>FactoryTalk Security</strong> Improves the security of an automation system by enabling the enforcement of least privilege via authentication and authorization of users.</td>
</tr>
<tr>
<td></td>
<td><strong>FactoryTalk View</strong> Version 11.00 or later <strong>required</strong> Human machine interface software for monitoring distributed multi-user applications.</td>
</tr>
<tr>
<td></td>
<td><strong>Studio 5000 Logix Designer®</strong> Version 32.00.00 or later <strong>required</strong> Comprehensive programming software that works with Rockwell Automation Logix Platforms and the Logix 5000™ family of controllers.</td>
</tr>
</tbody>
</table>

---

**Include compensating countermeasures**

**Manage physical access to the controller**
**Design Recommendations**

This publication describes the IEC-62443-4-2 SL 1 certification configuration requirements that apply to the overall Windows domain and specifically Rockwell Automation products that are used in the Domain. However, we recommend the following when you design and configure your system.

**Follow Design and Engineering Best Practices**

We recommend that you follow not only your company design guidelines but also general good engineering practices and behaviors when you configure your system.

**Microsoft Active Directory Group Policy**

Group Policy enables policy-based administration using Microsoft® Active Directory directory services. Group Policy uses directory services and security group membership to provide flexibility and support extensive configuration information. Policy settings are specified by an administrator. This is in contrast to profile settings that are specified by a user. Policy settings are created using the Microsoft Management Console (MMC) snap-in for Group Policy.

Rockwell Automation control system components are Windows-based. You can install FactoryTalk software applications on only workstations and servers that use Windows operating systems.

We strongly recommend that you implement an industry-standard configuration that is widely known and thoroughly tested. Some examples of industry-standards include Microsoft Security Baseline, Security Technical Implementation Guides (STIGs), National Institute of Standards and Technology (NIST), and Center for Internet Security (CIS) Benchmarks.
Secure System Elements

Figure 1 shows a control system that has system-level security.

**IMPORTANT** We assume that you have implemented the appropriate network segmentation and configuration. For example, you can use the Converged Plantwide Ethernet (CPwE) architecture in your network design.

For more information on how to use the CPwE architecture and general network security design, see the System Security Design Guidelines Reference Manual, publication SECURE-RM001.

**Figure 1 - Example Control System with System-level Security**

**IMPORTANT**: In this example, software that is listed as a compensating countermeasure on page 6 but is not shown in this graphic, is installed on the FactoryTalk Directory server, for example, FactoryTalk Linx software.
**Manual Organization**

This table describes how the manual is organized.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
</table>
| Chapter 1  
Configure Infrastructure Components on Page 13 | Describes the requirements to implement a Windows Domain |
| Chapter 2  
Configure FactoryTalk Components on Page 19 | Describes the required FactoryTalk software applications that are used in the control system. |
### Preface

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Chapter 3**  
Configure FactoryTalk Security on Page 31 | Describes the required FactoryTalk software application and Logix Designer application parameters that you must configure as part of the system security. |

**TIP:** FactoryTalk AssetCentre software supports distributed architectures. In that case, you can use another computer to incorporate additional configuration into the architectural design and maintenance.

---

**Chapter 4**  
Configure FactoryTalk AssetCentre Features on Page 95 | Describes how you can use FactoryTalk AssetCentre software to track all activity in the system.

**TIP:** FactoryTalk AssetCentre software supports distributed architectures. In that case, you can use another computer to incorporate additional configuration into the architectural design and maintenance.
Additional Resources

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

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP Security Application Technique, publication SECURE-AT001</td>
<td>Defines CIP Security and describes how to use it, including a list of products that are CIP-enabled and typical architectures.</td>
</tr>
<tr>
<td>ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publication 1756-UM543</td>
<td>Describes how to use ControlLogix 5580 and GuardLogix 5580 controllers.</td>
</tr>
<tr>
<td>Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1</td>
<td>Provides general guidelines for installing a Rockwell Automation industrial system.</td>
</tr>
</tbody>
</table>

You can view or publications at http://www.rockwellautomation.com/global/literature-library/overview.page.
To order paper copies of technical documentation, contact your local Allen-Bradley® distributor or Rockwell Automation sales representative.
Configure Infrastructure Components

This chapter describes the requirements that apply to a Windows infrastructure used with a Rockwell Automation® control system that includes a ControlLogix® 5580 controller with IEC-62443-4-2 SL 1 certification.

**Requirements**

To configure the infrastructure, you must complete the following tasks:

- Establish a Windows domain.
- Configure a domain controller.
- Create groups and users.
- Assign users to groups.
- Configure group policies.
- Configure workstations and servers to join the domain.

**Table**

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements</td>
<td>13</td>
</tr>
<tr>
<td>Windows Domain</td>
<td>14</td>
</tr>
<tr>
<td>Domain Controller</td>
<td>15</td>
</tr>
<tr>
<td>Create Users and Groups in the Windows Domain</td>
<td>16</td>
</tr>
<tr>
<td>Group Policy Management</td>
<td>17</td>
</tr>
<tr>
<td>Add Servers or Computers to the Windows Domain</td>
<td>18</td>
</tr>
</tbody>
</table>

**IMPORTANT**

We assume that you have unique Windows infrastructure design guidelines that you must follow when you configure a system. As such, it is assumed that you can complete the tasks to meet your company best practices.
**Windows Domain**

A Windows domain is a collection of servers or computers that share users, policies, and security principles.

Users in a Windows domain are granted access to a range of computer resources. The users are permitted actions through one user name and password combination with permissions definitions in the system.

**IMPORTANT** You must apply Microsoft® security policies to all Windows systems that are part of the industrial control system (ICS) in which an IEC-62443-4-2 SL1-compliant ControlLogix® 5580 controller is used. You must use a Domain/Active Directory to ease the management of those policies.
Domain Controller

You **must** configure a domain controller for the Windows domain. The domain controller is the main server or computer in the domain. You use the Server Manager to promote a server to the domain controller role.

The domain controller uses an Active Directory Domain Services (AD DS), also known as an Active Directory, to centralize the administration of users, policies, and security across all members of the domain.

For more information on the AD DS, see page 16.
Active Directory

Active Directory is a service that runs on a domain controller and stores information about objects on the network. Active Directory maintains a database from which you can administer user and computer accounts and configure security permissions across the network.

In this way, the domain controller uses the Active Directory service to respond to the following security requests across the domain:
- Identification
- Authentication
- Authorization

To meet IEC-62443-4-2 SL 1 certification requirements, user identification and authentication are delegated to the Windows Domain Controller via Active Directory. Authorization for capabilities of the ICS are delegated to the policy settings in the FactoryTalk® Directory, as described in Chapter 3, Configure Infrastructure Components.

Create Users and Groups in the Windows Domain

From operators and maintenance personnel to engineers, the domain controller manages users and groups in the Active Directory. You create the users and groups. We recommend that you create groups to adequately manage the personnel who operate your ICS.

Users are defined based on their roles in the ICS. To satisfy IEC-62443-4-2 SL 1 certification requirements, you must create at least two user types and assign a minimum level of user permissions for personnel to complete their assigned tasks.

The domain controller employs user types to verify and manage user identities in Active Directory. As a result, FactoryTalk Security authenticates with Active Directory to verify user identity when someone logs into the FactoryTalk Directory, as described on page 32.
Group Policy Management

You **must** define some group policies as a compensating countermeasure to meet IEC-62443-4-2 SL 1 certification requirements. The policies determine what actions users are permitted to take or not to take, for example, password maintenance or to restrict folder access.

Once you configure group policies on a domain controller, you **must** apply those policies to Organizational Units to manage privileges for users and computers in the domain.

You do not have to configure the same policies on additional domain computers. The policy settings that are used to enforce these privileges is specific to the operating system that is used in your ICS.

You **must** address the Windows Security settings that are described in the following table as appropriate for your system configuration to achieve IEC-62443-4-2 SL 1 certification:

<table>
<thead>
<tr>
<th>Windows Security Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Password                 | Define the group policy to help protect user passwords from unauthorized disclosure. You **must** configure the following:  
  - Disable storage of passwords with reversible encryption  
  - Disable display of user password  
  Define the group policy for proven, industry standard password strength. You **must** configure the following:  
  - Configure password length  
  - Configure password complexity  
  - Configure password history  
  - Configure minimum password age  
  - Configure maximum password age  
  Define the group policy to obscure the user password when it is being entered. That is, you **must** disable display of user password when it is entered. |
| User account access       | Define the group policy to unlock a user account after a configured time period. You **must** configure the following:  
  - Account lockout duration  
  - Reset account lockout duration  
  - Account lockout threshold |
| System use notification   | Define the group policy to system use notification. You **must** configure the following:  
  - Message text at logon  
  - Message title at logon |
| System inactivity lockout | Define the group policy to initiate a session lock after a configured time period of inactivity. That is, you **must** configure Machine Inactivity Limit. |
Chapter 1  Configure Infrastructure Components

Add Servers or Computers to the Windows Domain

A Windows Domain can, and often does, include multiple servers and computers. Once you define the domain controller, you must add servers and computers to the domain. In other words, system elements join the domain.

The domain centralizes all administrative settings for the workstations and servers in your application.
Chapter 2

Configure FactoryTalk Components

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>FactoryTalk Directory Requirements</td>
<td>19</td>
</tr>
<tr>
<td>FactoryTalk Directory Components</td>
<td>20</td>
</tr>
<tr>
<td>Configure the FactoryTalk Directory</td>
<td>21</td>
</tr>
<tr>
<td>Configure FactoryTalk Policy Manager</td>
<td>26</td>
</tr>
</tbody>
</table>

This chapter describes how to configure FactoryTalk® components.

FactoryTalk Directory Requirements

The FactoryTalk Directory defines all computers, FactoryTalk products, and components that are in the system.

The following requirements apply when you configure a Rockwell Automation® control system that includes a ControlLogix® 5580 controller with IEC-62443-4-2 SL 1 certification

- **You must** use FactoryTalk Directory to configure FactoryTalk Components in the system.

- **You must** use FactoryTalk Directory in a centralized manner to configure the system.

  When you use the centralized manner and connect all components to FactoryTalk Directory, you apply FactoryTalk Security policies once and they are automatically propagated to the other components in the directory.
The following graphic shows an example system that uses a FactoryTalk Directory.
Configure the FactoryTalk Directory

A **Windows administrator must** complete the following steps on the computer that hosts the FactoryTalk Directory for the ICS where a IEC-62443-4-2 SL 1-compliant ControlLogix® 5580 controller is used.


   For example, choose Start>Programs>Rockwell Software>FactoryTalk Directory Configuration Wizard.

2. Select ‘Configure the FactoryTalk Network Directory’ and click Next.
3. Type any Windows administrator user name and password for the Network Directory, and click Next.
   Use the same user name and password for Network and Local directories.

4. Click Close.
Define Network Directory

The Network Directory must be the same for all system computers. Any server can be used as the FactoryTalk Directory server.

1. Open FactoryTalk Directory Location.

For example, choose Start>Programs>Rockwell Software>Specify FactoryTalk Directory Location.

2. Click Browse (ellipsis ‘...’) on the FactoryTalk Directory Server Location Utility dialog box.

3. Type the same user name and password (with Administrator privileges) that you used to configure the Network and Windows Directory, and click OK.
4. Check Remote computer and type the FactoryTalk Directory server. For example, tp-ft.
   You can browse for a network name also.

5. Click OK.

6. Verify the desired FactoryTalk server appears in the computer hosting text box, and click OK.

7. Click OK on the message box.

This message is a reminder to restart the computer after you finish adding all servers and workstations to the FactoryTalk Directory.
8. Log on by using the server user name and password as shown in step 3.

![Log On to FactoryTalk (New Server)](image)

9. Restart the computer.
10. Repeat step 4 through step 8 for all servers and workstations in the application.
11. Shut down and restart the computer.

*FactoryTalk Administration Console*

When complete, the FactoryTalk Directory computers appear in the FactoryTalk Administration Console.

![FactoryTalk Administration Console](image)

For more information on how to use FactoryTalk Administration Console software, see Chapter 3, *Configure FactoryTalk Security on page 31.*
Configure FactoryTalk Activation Manager

FactoryTalk Activation Manager software provides a secure, software-based system to apply Rockwell Automation licenses for continuous use of FactoryTalk software and other Rockwell Automation software products.

With FactoryTalk Activation software, there is no need for a physical master disk or any physical media. Instead, activation files are generated and distributed electronically.

To download the software and learn how to use it, go to the following:

https://activate.rockwellautomation.com/

Configure FactoryTalk Policy Manager

FactoryTalk Policy Manager is a secure configuration tool that is one of a set of products that Rockwell Automation uses to implement CIP Security™.

CIP Security is a standard, open-source communication method that helps to provide a secure data transport across an EtherNet/IP™ network.

The secure data transport is used between certain connected devices to help protect the devices from threats posed by unauthorized users with malicious intent.

Rockwell Automation uses the following products to implement CIP Security:

- FactoryTalk Policy Manager
- FactoryTalk Linx
- Studio 5000® Design Environment
- CIP Security-enabled Rockwell Automation™ products, for example, the product described in this publication
For more information on CIP Security, including which products support CIP Security, see the CIP Security Application Technique, publication SECURE-AT001.

**IMPORTANT** Remember the following when you use FactoryTalk Policy Manager as you configure a system that includes an IEC-62443-4-2 SL 1-certified ControlLogix 5580 controller:

- This section describes only a subset of tasks that you must be aware of regarding IEC-62443-4-2 SL 1 certification.
- You must use the certificate-based Authentication method to meet IEC-62443-4-2 SL 1 certification requirements.

For more information on how to use FactoryTalk Policy Manager in the larger context of implementing CIP Security in control system, see the CIP Security Application Technique, publication SECURE-AT001.

You **must** complete the following tasks when you begin to use FactoryTalk Policy Manager.

1. Open FactoryTalk Policy Manager.

   For example, choose Start>Programs>Rockwell Software>FactoryTalk Policy Manager.
2. Click the + to add a zone.

3. In the Zone Properties, click Enable CIP Security.
4. Complete the following:
   a. From the Authentication Method pull-down menu, choose Certificate.
   b. From the I/O Data Security pull-down menu, choose Integrity and Confidentiality.
   c. From the Messaging Security pull-down menu, choose Integrity and Confidentiality.

   You **must** make these configuration choices to meet IEC-62443-4-2 SL 1 certification requirements.

5. Continue to use FactoryTalk Policy Manager as necessary to implement the network segmentation that is appropriate for your environment.
Notes:
# Configure FactoryTalk Security

This chapter describes how to configure FactoryTalk® Security.

## FactoryTalk Security Components

FactoryTalk Security components include server and workstation configuration settings.

## FactoryTalk Directory

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>FactoryTalk Security Components</td>
<td>31</td>
</tr>
<tr>
<td>Configure FactoryTalk Administration Console</td>
<td>32</td>
</tr>
<tr>
<td>Security Requirements</td>
<td>33</td>
</tr>
<tr>
<td>Configure FactoryTalk Users and Groups</td>
<td>34</td>
</tr>
<tr>
<td>Configure the System Policies</td>
<td>42</td>
</tr>
<tr>
<td>Configure the Product Policies</td>
<td>54</td>
</tr>
<tr>
<td>Configure the Product Policies Feature Security</td>
<td>57</td>
</tr>
<tr>
<td>Configure Feature Security for FactoryTalk AssetCentre Users</td>
<td>62</td>
</tr>
<tr>
<td>Configure Feature Security for RSLogix 5000 Users</td>
<td>67</td>
</tr>
<tr>
<td>Configure the Security Authority Identifier</td>
<td>81</td>
</tr>
</tbody>
</table>

![Diagram of FactoryTalk Security Components]
Chapter 3 Configure FactoryTalk Security

Configure FactoryTalk Administration Console

The FactoryTalk Administration Console lets you configure, manage, and secure a FactoryTalk Directory, its resources, and services.

Verify User Identity

During the logon process to the FactoryTalk Directory, FactoryTalk Security authenticates with Active Directory to verify user identity. Authorized users can then access secured parts of the application.

Select the FactoryTalk Directory

First, you must create a FactoryTalk Directory, as described in Configure the FactoryTalk Directory on page 21.

To configure the FactoryTalk Administration Console, complete these steps.

1. Open the FactoryTalk Administration Console.

   For example, choose Start>Rockwell Software®>FactoryTalk Administration Console.
2. When prompted to select a FactoryTalk Directory, choose Network, and click OK.

- Network lets you view the permissions in effect for a computer or group of computers.
- Local restricts you to viewing permissions in effect for only one computer.

**Security Requirements**

You **must** complete these tasks in FactoryTalk Administration Console.

- Create the groups (optional but recommended)
- Create the Windows-linked users.
- Assign users to the groups.
- Grant the appropriate permissions to the groups and users.

  With groups, you create a security structure without needing to know exactly the users in a group. When users are added to the group, they inherit the permissions that are granted to the group.

- Configure the system security policies.
- Configure the FactoryTalk system policies.
- Configure the FactoryTalk product policies.
Configure FactoryTalk Users and Groups

The FactoryTalk Directory stores information about user access in a control system.

To satisfy IEC-62443-4-2 SL 1 certification requirements, you must use Windows-linked users and groups. For a user to have access to any application in the ICS, they, or a group within which they exist, must be linked to the FactoryTalk Directory.

For more information on creating users and groups in the Active Directory, see page 16.

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 overwritten by the All Users group permissions.

Using the example above, if you configure an Operators Group and set the Project: Download in RSLogix 5000® to Deny, you expect that a member of the group cannot download a project to the ControlLogix® 5580 controller.

If the All Users group exists and all actions are configured to Allow, the member of the Operators Group can download the project to a ControlLogix 5580 controller.

**TIP**
This section describes how to remove the All Users group at the highest level in FactoryTalk Administration Console. We recommend that you confirm that the All Users group is removed at any level in which you manage your security configuration.
To remove the All Users group from User lists in FactoryTalk Administration Console, complete the following steps.

1. Open the FactoryTalk Administration Console.
3. On the Permissions tab of the Security Settings for Network dialog box, select the All Users group and click Remove.
4. When the All Users group is no longer listed, click OK.

Assign Windows-linked User Groups to FactoryTalk Directory

These sections describe how to link user accounts in a Windows domain into FactoryTalk security.

**IMPORTANT** You must complete the procedures, including assigning groups, roles, and areas, for domain credentials to be recognized in the FactoryTalk Directory. You must complete the tasks that are described in this section to meet IEC-62443-4-2 SL 1 certification requirements.

- Linking External Users and Groups
- Importing Active Directory Groups
Linking External Users and Groups

You must assign access rights to Windows-linked user accounts to validate that the users are authorized for the work that is approved for the group.

1. Open the FactoryTalk Administration Console and select Network.
2. Under the Network Directory, open System folder and the Users and Groups.
4. Click Add.
5. On the Select Groups dialog box, click Locations.

6. Open Entire Directory and select a domain name.

7. Click OK.
Importing Active Directory Groups

Complete these steps to import specific roles, such as supervisor, operator, maintenance, into groups.

1. Access the Select Groups dialog box as described beginning at step 2 on page 37.

2. Click Object Types, and click OK.
3. On the Select Groups dialog box, click Advanced.

4. Type at least the first few characters of the name.
5. Click Find Now to display a list of roles that you grouped previously.
6. Select all desired windows-linked groups and click OK.

**IMPORTANT:** The use of numbers 62443 at the beginning of names throughout this section is for example purposes only. You are not required to include the numbers as part of your naming conventions.
7. To accept the selections, click OK on the following dialog boxes.

All domain groups and roles are listed under the FactoryTalk Directory User Groups.
Configure the System Policies

This section describes how to configure System Policies permissions for groups and users to perform actions according to their security levels. The access level can be based in the domain or local groups.

The user can be a member of only one group regarding access level and associated permissions. The user has the lowest security access in both groups. For example, if you are a member of the Administrators and the Operators groups and you are denied access, you lose Administrator permissions.

To configure the System Security Policies, complete the following steps in FactoryTalk Administration Console.

1. Navigate to the System Policies option.
   
   Network > System > Policies > Policies.


![Image of Select User and Computer dialog box]

The Select User and Computer dialog box appears.

4. Select a group and click OK.
5. Return to step 3 to add more groups.

6. When all groups are added, select one group at a time in the top half of the Security Settings for System Policies dialog box.

7. In the lower half of the dialog box, set the Allow/Deny permissions, and click OK.

   You can set permissions across an entire set of actions. For example, if you click Deny in the Common category row, all common tasks are denied for the chosen group.

   You can set permissions on an action-by-action basis. For example, if you open the Common category row, you can allow or deny permission for individual tasks.

8. If an action is set to Deny, a warning message appears when you click OK, click Yes to verify the choice.
Configure the Application Authorization Policy

To configure the Application Authorization settings, complete the following steps.

1. Navigate to the Application Authorization option.

   Network>System>Policies>System Policies.

2. Right-click Application Authorization and select Properties.

3. Change settings as necessary, and click OK.

![Application Authorization Configuration](image-url)
Chapter 3  Configure FactoryTalk Security

Configure the User Rights Assignment Policy

To configure the User Rights Assignment policy settings, complete the following steps.

1. Navigate to the User Rights Assignment option.
   Network > System > Policies > System Policies.
2. Right-click User Rights Assignment and select Properties.
3. On the User Rights Assignment Properties dialog box, click the desired category and click the ellipsis button to the right of Configure Security.
4. On the Configure Securable Action dialog box, if the desired group is not listed, click Add.

The Select User and Computer dialog box appears.

5. Select a group and click OK.
6. Return to step 4 to add all desired groups.
7. Configure the ‘Allow’ or ‘Deny’ option for each group, and click OK.
Configure the Live Data Policy

To configure the Live Data Policy settings, complete the following steps.

1. Navigate to the Application Authorization option.
   
   Network>System>Policies>System Policies.

2. Right-click Live Data Policy and select Properties.

3. Change the setting if necessary, and click OK.
Configure the Health Monitoring Policy

To configure the Health Monitoring settings, complete the following steps.

1. Navigate to the Health Monitoring option.

   Network>System>Policies>System Policies.

2. Right-click Health Monitoring Policy and select Properties.

3. Change settings if necessary, and click OK.
Configure the Audit Policy

To configure the Audit Policy settings, complete the following steps.

1. Navigate to the Audit Policy option.
   
   Network > System > Policies > System Policies.

2. Right-click Audit Policy and select Properties.

3. Change settings if necessary, and click OK.
Configure the Security Policy

To configure the FactoryTalk Security Policies, complete the following steps.

1. Navigate to the Security Policy option.

   Network>System>Policies>System Policies.

3. Change settings if necessary.

**IMPORTANT** Remember the following when you make changes to the Security Policy Properties on the dialog box:

- **You must** configure the Directory Protection Policy setting **Directory cache expiration** as appropriate in your environment to maintain the least privilege.
  
The Directory cache expiration setting sets the amount of time the directory cache is valid before access is terminated.

- **The Password Policy** settings are not applicable in the FactoryTalk Directory because you configure them in the Active Directory. The choices that are made in the Active Directory take precedence.

- **The Account Policy** settings are applicable in FactoryTalk Directory. You must configure the same settings in the Active Directory, as described on page 17. You can use the same values in the Active Directory and FactoryTalk Directory or you can use different values.
  
  We recommend that you are consistent between the Active Directory and FactoryTalk Directory. That is, use the same values in each place.

- **We recommend** that you enable the **Single Sign-On** setting on this dialog box. When Single Sign-on is enabled, the user only has to log into the Active Directory and has access to the FactoryTalk Directory as well. The user is not required to enter Windows credentials to log into the FactoryTalk Directory.

4. Click **OK** to close the Security Policy Properties dialog box.

Click **Apply** if you want to apply the change but keep the dialog box open to make more changes.
Configure the Product Policies

This section describes how to configure Product Policies permissions for groups and users to perform actions according to their security levels. The access level can be based in the domain or local groups.

The user can be a member of only one group regarding access level and associated permissions. The user has the lowest security access in both groups. For example, if you are a member of the Administrators and the Operators groups and you are denied access, you lose Administrator permissions.

For information on the System Policy security settings that Rockwell Automation uses in IEC-62443-4-2 SL 1 certification verification testing see Policy Settings on page 76.

To configure the System Security Policies, complete the following steps in FactoryTalk Administration Console.

1. Navigate to the Product Policies option.

   Network>System>Policies>Policies


The Select User and Computer dialog box appears.

4. Select a group and click OK.
5. Return to step 3 to add more groups.

6. When all groups are added, select one group at a time in the top half of the Security Settings for Product Policies dialog box.

7. In the lower half of the dialog box, set the Allow/Deny permissions, and click OK.

You can set permissions across an entire set of actions. For example, if you click Deny in the Common category row, all common tasks are denied for the chosen group.

You can set permissions on an action-by-action basis. For example, if you open the Common category row, you can allow or deny permission for individual tasks.

8. If an action is set to Deny, a warning message appears when you click OK, click Yes to verify the choice.
Configure the Product Policies Feature Security

This section describes how to configure Product Policy feature security. You can configure product policy security in the following ways:

- **Product Policies** - This option lets you configure security settings for many software applications on a feature-by-feature basis on one dialog box.

- **Application-specific Policies** - This option lets you configure security settings for specific Rockwell Automation® software applications on individual dialog boxes.

**IMPORTANT** The same feature set is available for each software application regardless of which option you use to configure product policies security.

For information on the Product Policies Security choices that Rockwell Automation used in system testing, see Policy Settings on page 76.

**Product Policies**

To configure the Product Policies Feature Security, complete the following steps in FactoryTalk Administration Console.

1. Navigate to the Product Policies folder.

   Network>System>Policies.

3. On the Permissions tab of the Feature Security for Product Policies dialog box, select a group in the upper portion of the dialog box.

For example, the Administrators group is selected on the following example screen.

4. Expand the choices until you see the Feature Security list for the desired Rockwell Automation software application.

5. Check the appropriate Allow or Deny boxes, and click OK.

6. If an action is set to Deny, a warning message appears when you click OK, click Yes to verify the choice.
Product Policies for Individual Software Applications

To configure the Product Policies Feature Security for individual software applications, complete the following steps in FactoryTalk Administration Console.

This example shows how to configure feature security for RSLogix 5000®.

1. Navigate to the Feature Security option under the desired application, Network>System>Policies>Product Policies>RSLogix 5000
2. Right-click Feature Security and choose Properties.
3. On the Policy Settings tabs, click the desired category and click the ellipsis button to the right of Configure Security.
4. On the Configure Securable Action dialog box, if the desired group is not listed, click Add.

The Select User and Computer dialog box appears.

5. Select a group and click OK.
6. Return to step 4 to add all desired groups.
7. Configure the 'Allow' or 'Deny' option for each group, and click OK.
Configure Feature Security for FactoryTalk AssetCentre Users

By default, all users and the Administrators group in FactoryTalk Directory can perform any task in the FactoryTalk AssetCentre software.

To deny specific users the right to perform tasks in FactoryTalk AssetCentre, you **must** edit the Feature Security settings in the FactoryTalk Administration Console.

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

To change which users can perform tasks in FactoryTalk AssetCentre.

1. Start the FactoryTalk Administration Console.
2. Log on to the Network directory via a FactoryTalk Administrator account.
5. On the Feature Security Properties dialog box, click the desired category and click the ellipsis button to the right of Configure Security.
   
   **TIP** The steps described here apply to the other Feature Security Properties configuration.

The Select User and Computer dialog box appears.

6. On the Configure Securable Action dialog box, if the desired group is not listed, click Add.
Chapter 3  Configure FactoryTalk Security

The Select User and Computer dialog box appears.

7. Select a group and click OK.

![Select User and Computer dialog box]

8. Return to step 4 to add all desired groups.

9. Configure the ‘Allow’ or ‘Deny’ option for each group, and click OK.

![Configure Secure Action dialog box]
### Policy Settings

This table shows the policy settings and their meanings.

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>Grant User Permission to Perform This Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Address Book</td>
<td>View the Address Book. The Address Book contains addresses for sending automatic email notifications.</td>
</tr>
<tr>
<td>Edit Address Book</td>
<td>Edit or add contacts and groups in the Address Book. The Address Book contains addresses for sending automatic email notifications.</td>
</tr>
<tr>
<td>Override Archive Check In</td>
<td>Check in a file regardless of who checked it out or from where it was checked out.</td>
</tr>
</tbody>
</table>
| Configure Database Limitations | Configure the following:  
  - Maximum size of the AssetCentre database  
  - Size warning levels  
  - Maximum number of versions per archive asset  
  - Maximum size of Event, Audit, and Diagnostics logs  
  - Database capacity status refresh rate                                                                                                                                                                                                       |
| Configure Asset Inventory      | Configure the settings in the Asset Inventory window.                                                                                                                                                                                                                                                   |
| Configure Archive Options      | Turn on or off the function that allows Logix Designer application to perform archive activities, such as file check-in, without direct interaction with the FactoryTalk AssetCentre client.                                                                                                                   |
| Override Archive Undo Check    | Undo a checkout even if another user checked out the file.                                                                                                                                                                                                                                            |
| Override Removal of Local      | 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     | 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       | 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     | Set a personal working folder for checking out files. For more information on working folders and personal working folders see the FactoryTalk AssetCentre Client Help.                                                                                                                                  |
| Configure System Archive       | Set the system working folder to which all users check out files unless they have a personal working folder. For more information on working folders and system working folders, see the FactoryTalk AssetCentre Client Help.                                                                      |
| Run Archive Database Cleanup   | 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.                                                                                                                                                                                                                                              |
| Configure Assets Lifecycle     | Synchronize lifecycle information in the FactoryTalk AssetCentre server and client with the Rockwell Automation lifecycle website.                                                                                                                                                                      |
| Display Calibration Management | 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. 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. |
| 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.                                                                                                                                                                                                                                               |
### Policy Setting | Grant User Permission to Perform This Task
--- | ---
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.
Create a 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 | Configure a new search to find entries that match specified criteria in one of the logs, in the Archive History, or in Archive Check Out Status information.
Configure Feature Security for RSLogix 5000 Users

The programming software for ControlLogix 5580 controllers is the Logix Designer application. In FactoryTalk Administration Console, RSLogix 5000 is the name that is used for the software. Throughout this section, RSLogix 5000 refers to Logix Designer application.

To satisfy IEC-62443-4-2 SL 1 certification requirements, you must use Windows-linked users and groups. For a user to have access to any application in the ICS, they, or a group within which they exist, must be linked to the FactoryTalk Directory.

For more information on creating users and groups in the Active Directory, see page 16.

For example, you can link a group for users in an operator role. If the required tasks of someone in the operator role exclude downloading a Logix Designer application project to a ControlLogix 5580 controller, you set the Project: Download in RSLogix 5000 to Deny for the group. All users in the group are prevented from downloading a project to the controller.

By default, the Administrators group in FactoryTalk Directory can perform any task in software.

To deny specific users the right to perform tasks in RSLogix 5000, you must edit the Feature Security settings in the FactoryTalk Administration Console.

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

When you configure security for RSLogix 5000 users, you must configure the following:

- Configure Feature Security for Product Policies
- Configure Security Securable Actions
Configure Feature Security for Product Policies

To configure the Product Policies Feature Security, complete the following steps in FactoryTalk Administration Console.

1. Navigate to the Product Policies folder.
   Network/System/Policies.
3. On the Permissions tab of the Feature Security for Product Policies dialog box, complete the following steps.
   a. Select the applicable group.
   b. Expand the choices until you see the Feature Security list for the desired Rockwell Automation software application.
   c. Check the appropriate Allow or Deny boxes, and click OK.

Policy Settings

This table shows the policy settings and their meanings.

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>Grant User Permission to Perform This Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller: Secure</td>
<td>Secure a project or controller.</td>
</tr>
<tr>
<td>Firmware: Update</td>
<td>Update controller firmware.</td>
</tr>
<tr>
<td><strong>TIP</strong>: If the project is secured, the Securable Action (Firmware:Update) is also <strong>required</strong> to perform firmware updates. Firmware updates can be initiated within the Logix Designer application Who Active dialog box if a project is open but not when the controller is online.</td>
<td></td>
</tr>
<tr>
<td>Print: Modify Options</td>
<td>Modify print options.</td>
</tr>
<tr>
<td>Project: New</td>
<td>Create a new project, import a project, or translate PLC-5/SLC.</td>
</tr>
<tr>
<td>Toolbar: Configure</td>
<td>Move, resize, hide, or show toolbars.</td>
</tr>
<tr>
<td>Workstation: Modify Options</td>
<td>Modify workstation options</td>
</tr>
</tbody>
</table>
Configure Security Securable Actions

You must configure permissions for users and user groups to perform specific tasks in RSLogix 5000 software. You can perform the required tasks in the following ways:

- Networks and Devices
- Permission Sets
- Logical Names

Networks and Devices

To configure the permissions for specific tasks in RSLogix 5000 software via the Networks and Devices option, complete the following steps in FactoryTalk Administration Console.

1. Navigate to Networks.
   
   Network>System

2. Right-click Networks and Devices and select Security.
3. On the Permissions tab of the Security Settings for Networks and Devices dialog box, complete the following steps.
   a. Select the applicable group.
   b. Expand the choices until you see the Feature Security list for the desired Rockwell Automation software application.
   c. Check the appropriate Allow or Deny boxes, and click OK.
Permission Sets

To configure the permissions for specific tasks in RSLogix 5000 software via the Permission Sets, complete the following steps in FactoryTalk Administration Console.

1. Navigate to the Permission Set.

   Network > System

2. Right-click Permission Sets and select Security.
3. On the Permissions tab of the Security Settings for Permission Sets dialog box, complete the following steps.
   a. Select the applicable group.
   b. Expand the choices until you see the Feature Security list for the desired Rockwell Automation software application.
   c. Check the appropriate Allow or Deny boxes, and click OK.
Logical Names

To configure the permissions for specific tasks in RSLogix 5000 software via a Logical Name, complete the following steps in FactoryTalk Administration Console.

1. Navigate to the Logical Names.

   Network>System>Networks and Devices>Logical Names

2. Right-click on the Logical Name in the tree, and select Security.
3. On the Permissions tab of the Security Settings for the Logical Name (Security_application in this example) dialog box, complete the following steps.
   a. Select the applicable group.
   b. Expand the choices until you see the Feature Security list for the desired Rockwell Automation software application.
   c. Check the appropriate Allow or Deny boxes, and click OK.
Chapter 3  Configure FactoryTalk Security

**Policy Settings**

The table below shows the policy settings that you can configure via any of the ways that are described on page 70.

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>Grant User Permission to Perform This Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add-On Instruction: Create</td>
<td>Create a new Add-On Instruction.</td>
</tr>
<tr>
<td>Add-On Instruction: Delete</td>
<td>Delete a new Add-On Instruction.</td>
</tr>
<tr>
<td>Add-On Instruction: Export</td>
<td>Export a new Add-On Instruction.</td>
</tr>
<tr>
<td>Add-On Instruction: Export Unencoded</td>
<td>Export an Add-On Instruction in clear text. <strong>TIP:</strong> Users must also be granted the Add-On Instruction: Export permission to export an Add-On Instruction, or granted the Project: Export permission to export the entire project. <strong>TIP:</strong> To export in clear text, you must clear the Encode Protected Content checkbox on the Export dialog box. You must also have the required source key or license if the component is protected with Source Protection.</td>
</tr>
<tr>
<td>Add-On Instruction: Modify</td>
<td>Edit Add-On Instruction properties, tags, logic or whether a user can configure source protection.</td>
</tr>
<tr>
<td>Add-On Instruction: View Logic</td>
<td>View the internal information in an Add-On Instruction.</td>
</tr>
<tr>
<td>Alarm: Create</td>
<td>Create new tag-based alarms. When a user who is denied the Alarm: Create permission imports a project or a project component that requires new alarms to complete the import, those alarms are created.</td>
</tr>
<tr>
<td>Alarm: Delete</td>
<td>Delete tag-based alarms. When a user who is granted the Tag: Delete permission deletes a tag that has alarms that are associated with it, those alarms are deleted.</td>
</tr>
<tr>
<td>Alarm: Modify Properties</td>
<td>Modify the properties of a tag-based alarm. <strong>TIP:</strong> When a user who is denied the Alarm: Modify Properties permission imports a project or a project component that requires changes to existing tag-based alarms, the import fails.</td>
</tr>
<tr>
<td>Alarm: Use and Evaluate</td>
<td>Enable or disable a tag-based alarm using the Use and evaluate alarm checkbox on the Alarm Properties dialog box - Advanced tab.</td>
</tr>
<tr>
<td>Alarm: Clear Alarm Log</td>
<td>Clear the contents of the alarm log from the controller.</td>
</tr>
</tbody>
</table>

**IMPORTANT** You must configure the following fields for each user type as appropriate in your environment to maintain the least privilege.

- **Controller: Modify Mode** - Controls authorization to change the controller mode to Run mode.
  
  You must actively manage physical access to the ControlLogix 5580 controller. That is, as necessary, secure the controller’s location to help prevent unauthorized users from accessing it and changing the controller mode via the keyswitch.

- **Project: Download** - Controls authorization to download a user application, that is, a Logix Designer application project, to the controller.

Remember, to satisfy IEC-62443-4-2 SL 1 certification requirements, you must create at least two user types and assign a minimum level of user permissions for personnel to complete their assigned tasks.
<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>Grant User Permission to Perform This Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm: Direct Commands</td>
<td>Respond to a tag-based alarm using the Acknowledge, Shelve, Disable, and Reset buttons on the Alarm Properties dialog box - Status tab.</td>
</tr>
<tr>
<td>Alarm Definition: Create</td>
<td>Create new alarm definitions. An alarm definition is associated with an Add-On Instruction or a defined data type. When a tag is created using a data type or an Add-On Instruction that has alarm definitions, alarms are created automatically based on the alarm definitions.</td>
</tr>
<tr>
<td>Alarm Definition: Delete</td>
<td>Delete alarm definitions. When a user who is granted the Alarm Definition: Delete permission deletes an alarm definition for a data type or an Add-On Instruction, the corresponding alarms based on the alarm definition are deleted, even if the user has not been granted the Alarm: Delete permission. When a user deletes a data type or an Add-On Instruction, all alarm definitions that are associated with that data type or Add-On Instruction are deleted, even if the user has not been granted the Alarm Definition: Delete permission.</td>
</tr>
<tr>
<td>Alarm Definition: Modify Properties</td>
<td>Modify the properties of a tag-based alarm. When a user who is denied the Alarm Definition: Modify Properties permission imports a project or a project component that requires changes to existing tag-based alarm definitions, the import fails.</td>
</tr>
<tr>
<td>Component: Modify Permission Set</td>
<td>Change which permission set is associated with a component.</td>
</tr>
<tr>
<td>Controller: Clear Faults</td>
<td>Edit the fault log, including clearing faults.</td>
</tr>
<tr>
<td>Controller: Lock/Unlock</td>
<td>Lock or unlock the controller for online edits.</td>
</tr>
<tr>
<td>Controller: Modify Mode</td>
<td>Change controller modes.</td>
</tr>
<tr>
<td>Controller: Modify Properties</td>
<td>Edit controller properties.</td>
</tr>
<tr>
<td>Controller: Modify Revision</td>
<td>Convert the .acd file to a higher revision.</td>
</tr>
<tr>
<td>Controller: Modify Type</td>
<td>Change controller types. If a user is granted Controller: Modify Revision privilege, but is denied Controller: Modify Type, in most situations the user will be unable to change the type of controller. However, during database conversion, it may be necessary to change the controller type because the old controller type is obsolete in the target revision. In this case, these users are allowed to change the controller type during conversion.</td>
</tr>
<tr>
<td>Controller: Unsecure</td>
<td>Unsecure a secured controller.</td>
</tr>
<tr>
<td>Data Log: Create</td>
<td>Create a data log.</td>
</tr>
<tr>
<td>Data Log: Modify</td>
<td>Modify a data log.</td>
</tr>
<tr>
<td>Data Log: Delete</td>
<td>Delete a data log.</td>
</tr>
<tr>
<td>Data Log: Enable/Disable</td>
<td>Enable or disable data logging.</td>
</tr>
<tr>
<td>Data Log: Read Log Data Value</td>
<td>Read a data log value.</td>
</tr>
<tr>
<td>Data Log: Clear Log Data Value</td>
<td>Clear a data log value.</td>
</tr>
<tr>
<td>Firmware: Update</td>
<td>Use the Logix Designer application to update controller firmware. The Product Policy (Firmware:Update) is also required to perform firmware updates. Firmware updates can be initiated within the Logix Designer application Who Active dialog box if a project is open, but not when the controller is online.</td>
</tr>
<tr>
<td>Language: Modify Properties</td>
<td>Associate project documentation with a language, set default language, add, or delete a language.</td>
</tr>
<tr>
<td>Language: Switch Language</td>
<td>Select another language for product documentation.</td>
</tr>
<tr>
<td>Module: Create</td>
<td>Create modules in the Controller Organizer.</td>
</tr>
<tr>
<td>Module: Create and Safety: Modify</td>
<td>Create safety I/O configuration.</td>
</tr>
<tr>
<td>Module: Delete</td>
<td>Delete modules in the Controller Organizer.</td>
</tr>
<tr>
<td>Policy Setting</td>
<td>Grant User Permission to Perform This Task</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Module: Delete and Safety: Modify</td>
<td>Delete safety I/O configuration.</td>
</tr>
<tr>
<td>Module: Maintenance High</td>
<td>Perform high impact operations such as module reset and calibration.</td>
</tr>
<tr>
<td>Module: Maintenance Low</td>
<td>Perform low impact operations such as resetting electronic fuses.</td>
</tr>
<tr>
<td>Module: Modify Properties</td>
<td>Edit module properties.</td>
</tr>
<tr>
<td>Module: Modify Properties and Safety: Modify Component</td>
<td>Modify safety I/O configuration.</td>
</tr>
<tr>
<td>Module: View Properties</td>
<td>View module properties.</td>
</tr>
<tr>
<td></td>
<td>Users with this permission can open device profiles and, when online with the controller, use the profile to interact directly with modules and carry out actions such as changing IP addresses. When this permission is denied, users cannot open device profiles.</td>
</tr>
<tr>
<td>Motion: Command Axis</td>
<td>Perform axis direct commands.</td>
</tr>
<tr>
<td>Motion: Modify Configuration</td>
<td>Modify axis, coordinate system, or motion group properties.</td>
</tr>
<tr>
<td>Nonvolatile Memory: Load</td>
<td>Load from non-volatile memory.</td>
</tr>
<tr>
<td>Nonvolatile Memory: Store</td>
<td>Store to non-volatile memory.</td>
</tr>
<tr>
<td>Phase: Create</td>
<td>Create equipment phases.</td>
</tr>
<tr>
<td>Phase: Delete</td>
<td>Delete equipment phases.</td>
</tr>
<tr>
<td>Phase: Manual Control</td>
<td>Manually control equipment phases.</td>
</tr>
<tr>
<td>Phase: Modify Properties</td>
<td>Edit equipment phases.</td>
</tr>
<tr>
<td>PLC/SLC: Modify Tag Mappings</td>
<td>Map PLC or SLC messages.</td>
</tr>
<tr>
<td>Plug-In: Display</td>
<td>Display plug-ins.</td>
</tr>
<tr>
<td>Print: Report</td>
<td>Print reports.</td>
</tr>
<tr>
<td>Program: Create</td>
<td>Create programs.</td>
</tr>
<tr>
<td>Program: Create and Safety: Modify Component</td>
<td>Create a safety program.</td>
</tr>
<tr>
<td>Program: Delete</td>
<td>Delete programs.</td>
</tr>
<tr>
<td>Program: Delete and Safety: Modify Component</td>
<td>Delete a safety program.</td>
</tr>
<tr>
<td>Program: Modify Properties</td>
<td>Edit program properties.</td>
</tr>
<tr>
<td>Program: Modify Properties and Safety: Modify Component1</td>
<td>Modify properties of a safety program.</td>
</tr>
<tr>
<td>Program: Modify Properties and Safety: Modify Component</td>
<td>Change class property of a standard program to safety.</td>
</tr>
<tr>
<td>Project: Compact</td>
<td>Compact a project file.</td>
</tr>
<tr>
<td>Project: Download</td>
<td>Download a project to a controller.</td>
</tr>
<tr>
<td>Project: Export</td>
<td>Save a project in .L5K or .L5X format.</td>
</tr>
<tr>
<td>Project: Go Online</td>
<td>Go online with a project.</td>
</tr>
<tr>
<td>Project: Modify Path</td>
<td>Set, clear, or modify the controller path associated with a given project.</td>
</tr>
<tr>
<td>Project: Open</td>
<td>Open a (read-only) version of the project.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Project: Save</td>
<td>Save a project.</td>
</tr>
<tr>
<td>Project: Save As</td>
<td>Save a project to a new .acd file.</td>
</tr>
<tr>
<td>Project: Upload</td>
<td>Upload a project from a controller.</td>
</tr>
<tr>
<td>Policy Setting</td>
<td>Grant User Permission to Perform This Task</td>
</tr>
<tr>
<td>----------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Routine: Create</td>
<td>Create a routine.</td>
</tr>
<tr>
<td>Routine: Create and Safety: Modify Component</td>
<td>Create a safety routine.</td>
</tr>
<tr>
<td>Routine: Delete</td>
<td>Delete a routine.</td>
</tr>
<tr>
<td>Routine: Delete and Safety: Modify Component</td>
<td>Delete a safety routine.</td>
</tr>
<tr>
<td>Routine: Export</td>
<td>Export a routine.</td>
</tr>
<tr>
<td>Routine: Export Unencoded</td>
<td>Export a routine in clear text.</td>
</tr>
<tr>
<td>Routine: Manual Control</td>
<td>Manually control routine logic.</td>
</tr>
<tr>
<td>Routine: Modify Logic</td>
<td>Edit routine logic.</td>
</tr>
<tr>
<td>Routine: Modify Logic and Safety: Modify Component</td>
<td>Edit safety routine logic.</td>
</tr>
<tr>
<td>Routine: Modify Properties</td>
<td>Edit routine properties, configure routine source protection.</td>
</tr>
<tr>
<td>Routine: Modify Properties and Safety: Modify Component</td>
<td>Edit safety routine properties.</td>
</tr>
<tr>
<td>Routine: View Logic</td>
<td>View the logic in a routine.</td>
</tr>
<tr>
<td>Safety: Generate/Delete Signature</td>
<td>Generate or delete a Safety Signature.</td>
</tr>
<tr>
<td>Safety: Lock/Unlock</td>
<td>Lock or unlock edits on safety application.</td>
</tr>
<tr>
<td>Safety: Modify Component</td>
<td>Create, delete, or modify safety components. <strong>TIP:</strong> The standard component privileges are required in addition to this privilege. For example, to create safety tags, the Tag: Create privilege is required in addition to the Safety: Modify Components privilege.</td>
</tr>
<tr>
<td>Safety: Modify Properties</td>
<td>Modify the controller’s safety configuration.</td>
</tr>
<tr>
<td>Safety: Create Tag Mappings</td>
<td>Create safety tags mapping.</td>
</tr>
<tr>
<td>Safety: Delete Tag Mappings</td>
<td>Delete safety tag mapping.</td>
</tr>
<tr>
<td>Safety: Modify Tag Mappings</td>
<td>Modify safety tags mapped to standard tags.</td>
</tr>
<tr>
<td>Sequence: Create</td>
<td>Create an equipment sequence.</td>
</tr>
<tr>
<td>Sequence: Delete</td>
<td>Delete an equipment sequence.</td>
</tr>
<tr>
<td>Sequence: Manually Control</td>
<td>Take manual control of an equipment sequence.</td>
</tr>
<tr>
<td>Sequence: Modify Properties</td>
<td>Modify the properties of an equipment sequence.</td>
</tr>
<tr>
<td>Tag: Create</td>
<td>Create tags.</td>
</tr>
<tr>
<td>Tag: Create and Safety: Modify</td>
<td>Create a safety tag.</td>
</tr>
<tr>
<td>Tag: Delete</td>
<td>Delete tags.</td>
</tr>
<tr>
<td>Tag: Delete and Safety: Modify Component</td>
<td>Delete a safety tag.</td>
</tr>
<tr>
<td>Tag: Delete, Safety: Modify Tag Mappings, and Safety: Modify</td>
<td>Delete standard tag that is mapped to a safety tag.</td>
</tr>
<tr>
<td>Tag: Force</td>
<td>Force tags and enable or disable existing forces.</td>
</tr>
<tr>
<td>Tag: Force and Safety: Modify Component</td>
<td>Force safety tags.</td>
</tr>
<tr>
<td>Tag: Modify Constant Property</td>
<td>Change Constant property of a tag.</td>
</tr>
<tr>
<td>Tag: Modify Constant Tag Values</td>
<td>Change values of a Constant Tag.</td>
</tr>
<tr>
<td>Tag: Modify Properties</td>
<td>Edit tag properties.</td>
</tr>
<tr>
<td>Tag: Modify Properties and Safety: Modify Component</td>
<td>Edit safety tag properties.</td>
</tr>
</tbody>
</table>
### Chapter 3  Configure FactoryTalk Security

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>Grant User Permission to Perform This Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag: Modify Properties and Safety: Modify Component</td>
<td>Change class property of a standard tag to safety.</td>
</tr>
<tr>
<td>Tag: Modify Properties and Safety: Modify Tag Mappings</td>
<td>Modify safety or standard tag properties of a tag contained in a safety mapping.</td>
</tr>
<tr>
<td>Tag: Modify Values</td>
<td>Change tag values.</td>
</tr>
<tr>
<td>Tag: Modify Values and Safety: Modify Component</td>
<td>Change safety tag values.</td>
</tr>
<tr>
<td>Task: Create</td>
<td>Create tasks.</td>
</tr>
<tr>
<td>Task: Delete</td>
<td>Delete tasks.</td>
</tr>
<tr>
<td>Task: Modify Properties</td>
<td>Edit task properties, including program scheduling.</td>
</tr>
<tr>
<td>Task: Modify Properties and Safety: Modify Components</td>
<td>Modify safety task properties.</td>
</tr>
<tr>
<td>Trend: Create</td>
<td>Create trends.</td>
</tr>
<tr>
<td>Trend: Delete</td>
<td>Delete trends.</td>
</tr>
<tr>
<td>Trend: Modify Properties</td>
<td>Modify trend properties.</td>
</tr>
<tr>
<td>Trend: Run</td>
<td>Run trends.</td>
</tr>
<tr>
<td>User Defined Type: Create</td>
<td>Create user-defined data types and string types.</td>
</tr>
<tr>
<td>User Defined Type: Delete</td>
<td>Delete user-defined data types and string types.</td>
</tr>
<tr>
<td>User Defined Type: Modify</td>
<td>Edit user-defined data types and string types.</td>
</tr>
</tbody>
</table>
Configure FactoryTalk Security

Chapter 3

Configure the Security Authority Identifier

You must be an authorized user to administer controller security.

| IMPORTANT | This procedure requires that you have defined FactoryTalk Product Policies. |

When you configure the Security Authority Identifier, you must choose one of the following with which to secure it:

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

  For more information on how to create a Permission Set, see below.

- **Logical Name** - A Logical Name is a name for the controller in FactoryTalk Directory.

  For more information on how to create a Logical Name, see page 85.

  **TIP** If your application includes a large number of ControlLogix 5580 controllers, we strongly recommend that you use a Permission Set to secure the Security Authority.

  If you use a Permission Set, you can configure the security settings once and they apply to all of the 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.
Create a Permission Set

Complete the following steps to create a new Permission Set in FactoryTalk Administration Console.

1. Navigate to the Product Policies folder.

   Network > System

2. Right-click Permission Sets and select New Permission Set.

3. Name the new permission set, and click OK.
4. Right-click the Permission Set name in the Permission Set folder and select Security.
5. One the Security Settings for the Permission Set, that is, Certification_62443, in this case, complete the following tasks:
   a. Select the group for which you want set permissions.
   b. Set permissions as necessary.

   In this example, the RSLogix5000, now named Studio 5000 Logix Designer, feature set permissions is opened for the ADMINISTRATOR.

   c. Click OK to apply the changes to all members of the selected group.

   **TIP** You can set permissions for as many groups and as many features across as many software applications as necessary before you click OK.
Create a Controller Logical Name

Complete the following steps to create a name for the controller in the FactoryTalk Directory.

1. Open FactoryTalk Administration Console.
2. In the Explorer window, click Network>System>Networks and Devices>Workstation name>communication driver.
3. Right-click on the controller and choose Properties.
4. On the Device Properties dialog box, from the Logical name: pulldown, choose the controller name.
   
   **TIP** If the name does not appear in the Networks and Devices tree, open RSLinx® Classic and go to the controller resource with RSWho. When you navigate to the resource in RSLinx Classic the controller path information updates in RSLinx Classic.

5. Click OK.
Configure the Security Authority Identifier

To configure the Security Authority Identifier, complete the following steps.

1. Create the project in Logix Designer application.
2. From the Tools menu, click Security and choose Log On.
3. Type an authorized user name and password and click OK.
4. Access the Controller Properties dialog box.
5. On the Security tab, complete the following steps.
   b. Click Use only the selected Security Authority for Authentication and Authorization.
   c. Chose a method with which to secure it, that is, Logical Name or Permission Set.
   d. Click Apply.

6. When the warning dialog box appears, click Yes.
Configure Communication Restrictions

This section describes how to restrict non-authorized communication modules from being added to a ControlLogix® backplane.

1. Open the Logix Designer application project.
2. Access the Controller Properties dialog box.
3. On the Security tab, complete the following steps.
   a. Click the Restrict Communications Except Through Selected Slots box.
   b. Select each number that represents an authorized communication module slot in the controller.
      Slot positions appear dimmed when selected.
   c. Click Apply.

New data communication modules must have authorized access to be installed in the selected slots.
Configure Data Restrictions

This section describes how to program Logix data tags to control external application access, such as HMI applications. The three external access tags are the following:

- Read/Write
- Read Only
- None

1. Open the Logix Designer application project.
2. Right-click a controller and choose Open Project in Designer.
3. Double-click Controller Tags.
   The tags appear in the right pane of the project.
4. To create a write restriction, on the Edit Tags tab, click Constant to create a Read Only tag.

A Constant tag cannot have its values changed programatically.
On the Monitor Tags tab, a constant tag symbol 🟠 appears in the Value column for the selected tag.

The Logix Designer compiler helps prevent write data in the reserved data.
Configure Code Restrictions

Source Protection is applied to routines and Add-On Instructions to help prevent third-party access to components. Source protection prevents logic components from being modified based on a license.

To satisfy IEC-62443-4-2 SL 1 certification requirements, you must use License-based Source and Execution Protection when you configure code restrictions.

Execution protection adds additional protection to controller logic. Execution protection makes sure the right controller has access to execute the protected program. Use this in conjunction with source protection to make sure the right programmer has access to modify the logic.

For more information on how to use License-based Source and Execution Protection, see the ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publication 1756-UM543.

Complete these steps in Offline mode to enable source protection.

1. In a Logix Designer project, right-click a controller and choose Open Project in Designer.
2. From the Tools menu Security>Configure Source Protection.
3. Insert the CmStick containing the license that you want to use to protect the component into the USB port on the computer.

   Licenses must contain the Protect permission to be used to protect components. If a license does not contain the Protect permission, it will not appear in the list of licenses.

4. Select any desired routine or Add-On Instruction to be protected, and click Protect.
5. On the Protect dialog box, complete the following steps.
   a. From the Protection Type pull-down menu, choose License.
   b. Select the license to apply.
   c. Select Protect with controller key and specific license.

6. Click OK.
Chapter 3  Configure FactoryTalk Security

Notes:
Chapter 4

Configure FactoryTalk AssetCentre Features

This chapter describes how to use FactoryTalk® AssetCentre software in a control system with components, for example, a ControlLogix® 5580 controller, that has achieved IEC-62443-4-2 SL 1 certification.

TIP: FactoryTalk AssetCentre software supports distributed architectures. In that case, you can use another computer to incorporate additional configuration into the architectural design and maintenance.
FactoryTalk AssetCentre gives you a centralized tool to secure, manage, version, track, and report information about assets in a system automatically. The software helps to prevent unauthorized or unwanted changes that can impact a secure control system.

You must complete the following:

- Add the assets that you must manage via FactoryTalk AssetCentre to the database.
- Configure feature security for FactoryTalk AssetCentre users.
- Use the Audit feature to track user action in the system.
- Configure system backup.

For more information on how to use FactoryTalk AssetCentre to perform the tasks described in this chapter, see the following:

- FactoryTalk AssetCentre online help
- FactoryTalk AssetCentre Getting Results Guide, publication FTAC-GR002

Audit and Change Management

FactoryTalk AssetCentre can track system activity in logs and record the activity information in a database.

You must manage the database size to make sure that logs are not lost and to meet IEC-62443-4-2 SL 1 certification requirements. For example, you can set the Critical and Warning limit parameters on the database size to notify an administrator that database maintenance is required.

You manage the database size via the Configure Database Limitations policy.

FactoryTalk AssetCentre uses the following logs to track system activity:

- Event Log - This log shows database information regarding events that occur in the system.
  Events are system-initiated, for example, an upload occurred, or a scheduled task completed. FactoryTalk-enabled products generate Event records.
  
- Audit Log - This log shows database information regarding actions that users perform in the system, such as making edits to a Logix Designer project or opening or closing such a software product. FactoryTalk-enabled products generate audit records.
• Diagnostic & Health Log - The Diagnostic and Health Log provides information about the condition of automation devices.

For example, a monitoring software product, such as RSNetWorx™ MD, detects a problem with a device on the automation network. It reports the problem and logs the information in the Diagnostic and Health Log.

**TIP** Initially, only previously existing data appears in the Diagnostic and Health Log if that data was imported from the RSMACC™ Network Health Solution. FactoryTalk AssetCentre does not update this data. New data is logged in the Diagnostic and Health Log only if RSNetWorx MD is installed on your system.

You can obtain log information in the following ways:

- Create a Schedule for a Device Monitor - Change Detect Operation
- View and Search Logs

---

**Create a Schedule for a Device Monitor - Change Detect Operation**

FactoryTalk AssetCentre lets you schedule operations. The results of an operation can be emailed to specified recipients, that is, if the schedule completed successfully or failed.

When you create a schedule, you must choose an operation type. The following operation types are available:

- Device Monitor - Change Detect
- Disaster Recovery - Backup
- Disaster Recovery - Backup and Compare

This section describes how to use the Device Monitor - Change Detect operation. For information on how to use the Disaster Recovery - Backup or Disaster Recovery - Backup and Compare operations, see page 122.

You can use the Device Monitor - Change Detect operation type with ControlLogix 5580 controllers when the controllers are configured for change detection.
Chapter 4  Configure FactoryTalk AssetCentre Features

When the schedule for a Device Monitor - Change Detect operation is active, the controller is monitored. When a change is detected, change entries from the controller log are collected into a report.

**IMPORTANT**  To create schedules, you **must** have the following permissions:

- Create a new schedule
- Edit a schedule
- Command a schedule

For more information on how to set permissions, see Configure Feature Security for FactoryTalk AssetCentre Users on page 62.

To create a schedule for a Device Monitor - Change Detect operation, you **must** complete the following tasks:

- **Set up Agent Groups and Agent Computers Within Them**
- **Create an Agent Group**
- **Create an Agent Computer**
- **Create the Schedule**
- **Edit Recipient List for Device Monitor - Change Detect Schedule Operation**

**Set up Agent Groups and Agent Computers Within Them**

FactoryTalk AssetCentre uses agents to perform Device Monitor - Change Detect operations. Agents are programs that communicate with the FactoryTalk AssetCentre server and perform tasks on behalf of the server. Agents let work be distributed and shared among multiple computers to spread processing load and speed up operations.

When a server needs an agent to perform a task, it locates the computer that is running the operation and assigns the task to that agent. The agent then reports the task's completion to the server.
Configure FactoryTalk AssetCentre Features  Chapter 4

FactoryTalk AssetCentre Agent Groups is a plug-in that helps you to manage the agents into groups. With this plug-in, the agent computers that are connected to the same FactoryTalk AssetCentre server are not required to have the same configuration. This plug-in lets you:

- Create agent groups, assign agent computers to the agent groups, and identify an agent group for an asset
- Assign backup and compare schedule tasks on an asset to the agent computers that belong to the asset’s agent group
- Monitor the status of agent computers in the Agent Status pane, the Agent Group Creation and Agent Assignment pane, and the Assets per Agent Group pane.

For more information about how to add a physical agent computer into FactoryTalk AssetCentre system instead of managing agent computers in agent groups, see the online help.

For more information on how to learn about more Agent Groups configurations, see the online help.

Create an Agent Group

Agent Groups plug-in manages the usage of agents. By default, there is one System Default agent group, which cannot be renamed or deleted. The System Default agent group is used for scheduled searches, and by default for a Device Monitor - Change Detect operation.

If you must create a new agent group, complete the following steps.

1. Confirm that FactoryTalk AssetCentre is in Design mode.
2. From the View menu, choose Agent Groups.
3. Click the Add Agent Group button on the Agent group Creation and Agent Assignment toolbar.

The Add an Agent Group dialog box opens.

4. On the Add an Agent Group dialog box, enter the name and a description for the agent group. The description is optional.

   **TIP** The maximum number of agent groups that you can create depends on your licensed agent group capacity. By default, you can create one agent group in addition to the existing System Default agent group.

5. Click OK.
Create an Agent Computer

You can create an agent computer in Agent Groups to monitor the physical agent computers.

To create an agent computer, complete the following steps:

1. Confirm that FactoryTalk AssetCentre is in Design mode.
2. From the View menu, choose Agent Groups.
3. Select an agent group, or an agent computer under the group where you want to add the agent computer.

Otherwise, the agent computer is created under System Default agent group.
4. Click the Add Agent Computer button on the Agent Group Creation and Agent Assignment toolbar.

The Add an Agent Computer dialog box opens.

5. On the Add an Agent Computer dialog box, enter the name, location, and the description for the agent computer.

6. Click OK.
Create the Schedule

**IMPORTANT** To create schedules, you must have the following permissions:
- Create a new schedule
- Edit a schedule
- Command a schedule

For more information on how to set permissions, see Configure Feature Security for FactoryTalk AssetCentre Users on page 62.

To create the schedule, complete the following steps.

1. From the View menu, choose Schedules.

2. Click the New button.
3. On the New Schedule Wizard: Step 1 of 3 dialog box, complete the following steps:
   a. Select an Operation type. This example uses Disaster Recovery - Backup.
   b. Name the schedule. You must enter a unique name for the schedule.
   c. Describe the operation. (optional)
   d. Enter email addresses. The End of Schedule report that is generated at the end of the controller idle time is sent to the addresses listed in this field.

If you have multiple e-mail addresses you want to include, separate the addresses in the Completion Email List field with semicolons (;), or, if you have View Address Book permission, select the contacts or groups from the FactoryTalk Address Book.

For more information about the End of Schedule report, see Device Monitor - Change Detect Schedule Results on page 109.

For more information on a particular field, see the online help.
4. You **must** configure the fields on the New Schedule Wizard: Step 2 of 3 dialog box. The configurable fields are as follows:

   - **Controller Idle** - When a change occurs, change entries from the controller log on the ControlLogix 5580 controller log are collected into a report.

   After the change entries are collected, the Controller Idle time starts. If no more changes are collected before the Controller Idle time expires, an End of Schedule report is sent to the addresses that are listed in the Completion Email list that is shown in step 1 on page 104.

   If more changes occur and, thus, are collected from the controller log into the report, the Controller Idle time period starts again.

   - **Maximum Runtime** - The amount of time that the schedule should collect changes into a report before sending the End of Schedule report to the addresses that are listed in the Completion Email list that is shown in step 1 on page 104.

   The Controller Idle time is not reached if changes are continuous, so you can use the Maximum Runtime to force a report to be generated.

   **IMPORTANT** Changes are not lost. New change entries that are listed in the controller log but are not included in the report that is emailed when the Maximum Runtime time expires, are collected for a new report.

5. Click Next.
Chapter 4  Configure FactoryTalk AssetCentre Features

New Schedule Wizard - Step 2 of 3
Timing Properties
Please update the timing properties for the schedule. Clicking on 'Next' button will create the schedule. You will not be able to return to this page.

Controller Idle: 0 Hours 10 Minutes
Maximum Runtime (0.0 means no limit): 1 Hours 0 Minutes
Maximum Runtime is limited

Help  Back  Next  Cancel
6. Complete the New Schedule Wizard: Step 3 of 3 dialog box.

   In the tree on the left side of the dialog box, if assets are used to create the schedule, check boxes appear selected next to each asset in the schedule.

7. If necessary, clear a box not to include that asset in the schedule.

   The schedule that you created is active unless you clear the Activate the Schedule box. For more information on a particular field, see the online help.

8. Click Finished.
Chapter 4 Configure FactoryTalk AssetCentre Features

**Edit Recipient List for Device Monitor - Change Detect Schedule Operation**

**IMPORTANT** To configure a recipients list for schedule results, you **must** have the following permissions:

- Edit a schedule
- Command a schedule

For more information on how to set permissions, see Configure Feature Security for FactoryTalk AssetCentre Users on page 62.

If you did not enter all desired email addresses on the first step of setting up the schedule, as described in step 3 on page 104, you can edit the list from the Schedules tab.

To edit the list of email addresses on the Schedules tab, complete the following steps.

1. Confirm that the schedule is not active.

   If necessary, clear the check box in the Active column for the chosen schedule.

2. Click the button in the Completion Email List to update the e-mail list.

3. Update the Contacts and Groups dialog box, and click OK.
**Device Monitor - Change Detect Schedule Results**

The Device Monitor - Change Detect schedule generates an End of Schedule report. The report indicates that the schedule has completed.

**Activate the Schedule**

When you activate the Device Monitor - Change Detect schedule, the controller is monitored. When a change is detected, change entries from the controller log are collected into a report.

To activate the schedule, check the box in the Active column.

For more information on how to use the Device Monitor - Change Detect operation, see the following:

- FactoryTalk AssetCentre online help
- FactoryTalk AssetCentre Getting Results Guide, publication FTAC-GR002
View and Search Logs

You can search for and show specified records from 1 log at a time. For example, you can search for log entries where a specific user performed a task on a specific computer.

You can perform searches in the following ways:

- Scheduled searches are used to execute a search on a recurring basis and works well for detecting specific conditions and user behaviors in log data. For instance, you can create a scheduled search to detect unsafe programming practices among your maintenance staff by searching the Audit Log for edits that are made to program files at the end of each shift.

  You can run scheduled searches manually to show search results immediately. Scheduled search results can be delivered via e-mail. Search results can be printed and saved in .PDF format.

- Unscheduled searches are used for one-time purposes or when there is an immediate need, such as searching the Audit Log to determine if anyone made a change in a control system that was working previously but now is down and preventing production.

  **TIP** In addition to searching logs, you can search the Archive History Log and the Archive Check Out Status.

  To perform a quick search without complex conditions instead of the full searches described in this manual, see the FactoryTalk AssetCentre online help.

To view logs and configure and run searches, complete the following tasks:

- View Logs
- Create a Search
- Set Search Security
- Run Searches
- View and Print Search Results
View Logs

Viewing a particular log shows the latest entries for that log only.

**IMPORTANT** To view logs, you must have the following permissions:
- View Audit Log
- View Event Log
- View Diagnostic and Health Log

For more information on how to set permissions, see *Configure Feature Security for FactoryTalk AssetCentre Users* on page 62.

To view logs, complete the following steps.

1. From the View menu, choose Logs.
2. To view the desired log, click the appropriate button in the Logs tab.

When you click a log type, detailed information is shown. For example, the following graphic shows details about recent events in a FactoryTalk AssetCentre Event log.

For more information about viewing logs in FactoryTalk AssetCentre, see the online help.
Create a Search

You can use FactoryTalk AssetCentre searches to show specified log records, for example, an Event Log or Audit Log.

**IMPORTANT** To create unscheduled searches, you **must** have the Create a Search permission. To create scheduled searches, you **must** have the following permissions:

- Create a Schedule
- Edit a Schedule
- View a Schedule
- Command a Schedule

For more information on how to set permissions, see [Configure Feature Security for FactoryTalk AssetCentre Users on page 62](#).

To create a search, complete the following steps.

1. From the View menu, choose Searches.
2. Click the New button.

3. When the New Search Wizard dialog box appears, complete the following steps.
   a. Enter a unique name for the search.
   b. Add a description (optional).
   c. Select the search data source

4. Complete one of the following tasks.
   a. To create an unscheduled search for the selected log, click Finished.
   b. To create a scheduled search to run later, click Schedule, complete the New Schedule Wizard dialog box.
5. If you create a scheduled search, when the next New Schedule Wizard dialog box appears, configure the search as necessary and click Finish.

For more information about creating searches in FactoryTalk AssetCentre, see the online help.

Set Search Security

You can set security for a search definition to determine which users can set security for, save, execute, and delete the search.

**IMPORTANT** To modify security settings for a search, you must have the following permissions:

- Configure Security - For more information on how to set permissions, see Configure Feature Security for FactoryTalk AssetCentre Users on page 62.
- Read and Write permissions as described in product policies security permissions in Configure the Product Policies on page 54.

Do not deny yourself Read permission or you can no longer show the Security Settings dialog box to change security for the selected search definition.
To set search security, complete the following steps.

1. From the View menu, choose Searches.

2. On the Searches tab, select the search for which you want to change security.

3. From the View menu, choose Security.
4. When the Security Settings dialog box appears, select the user and permissions for the selected search definition.

![Security Settings dialog box](image)

5. Click OK.

The following table describes the Common permissions that apply to searches.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Lets the Selected User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Security</td>
<td>Modify the Read, Write, Execute, and Delete settings for this search</td>
</tr>
<tr>
<td>Read</td>
<td>Show these security settings for this search</td>
</tr>
<tr>
<td>Write</td>
<td>Save this search</td>
</tr>
<tr>
<td>Execute</td>
<td>Run this search</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete this search</td>
</tr>
</tbody>
</table>

For more information about how to configure search security in FactoryTalk AssetCentre, see the online help.
Run Searches

To run schedules, you can perform one of the following tasks:

- Activate scheduled searches.
- Manually run a scheduled or unscheduled search.

**TIP** If you do not want to wait for a search's next run time, we recommend that you run the search manually.
   Running a scheduled search manually does not affect that search's next scheduled run time.

**IMPORTANT**
- To run a search, you **must** have Execute permission, as shown in step 4 on page 117.
- To activate and deactivate scheduled searches, you **must** have Command a Schedule permission. For more information on how to set the Command a Schedule permission, see Configure Feature Security for FactoryTalk AssetCentre Users on page 62.
- To run a search immediately, you **must** have the appropriate permission for the type of search you are going to run. For example, View Audit Log, View Event Log, or View Diagnostic & Health Log permission. For more information on how to set permissions, see Configure Feature Security for FactoryTalk AssetCentre Users on page 62.
To activate scheduled searches so that they run at their next scheduled run time, complete the following steps.

1. From the View menu, choose Searches.

2. Next to the searches you want to activate, select the Active check box.
To run a scheduled or unscheduled search immediately, complete the following steps:

1. From the View menu, choose Searches.

2. Select the search that you want to run and click the Run Now button.

For more information about how to run searches in FactoryTalk AssetCentre, see the online help.

View and Print Search Results

After you run a search, the results appear on a separate tab. Use the Report tab to view and navigate the results of a search you have run, and export and print the search’s results.

To preview a search, click the Preview tab.

For more information about how to view and print search results in FactoryTalk AssetCentre, see the online help.
**Backup**

When you configure a schedule, you must choose an operation type. The following operation types are available:

- Device Monitor - Change Detect
- Disaster Recovery - Backup
- Disaster Recovery - Backup and Compare

**IMPORTANT** This section describes how to use the Disaster Recovery operations. For information on how to use the Device Monitor - Change Detect operation, see page 97.

You can use Disaster Recovery to create a back-up of the files associated with different devices in the system.

Disaster Recovery verifies your devices’ program and configuration files against protected master files to make quick and accurate file recovery possible.

**Master Files**

A master file is a designated version of an asset’s configuration data file. You can initially update a master file from the physical device, for example, a controller, or save it directly from the programming software, that is, Logix Designer application.

A master file is added to the FactoryTalk AssetCentre Archive tool. The file is **required** for some FactoryTalk AssetCentre functions.

Disaster Recovery provides two types of operations:

- **Backup** - Stores a backup copy of files that are associated with a number of devices in the application.

- **Backup and Compare** - Retrieves a copy of the files that are associated with a device asset. If differences are found and you choose to store the uploaded device files, the retrieved copy of files that are associated with the device asset are promoted as the new master file stored in Archive.
Create a Schedule for a Disaster Recovery Operation

You can configure either a Backup or Backup and Compare Disaster Recovery operation when you create a schedule.

**IMPORTANT** To create schedules, you must have the following permissions:
- Create a new schedule
- Edit a schedule
- Command a schedule

For more information on how to set permissions, see *Configure Feature Security for FactoryTalk AssetCentre Users* on page 62.

To create a schedule for a disaster recovery operation, you must complete the following tasks:
- Set up Agent Groups and Agent Computers Within Them
- Create an Agent Group
- Create an Agent Computer
- Create a Schedule for a Disaster Recovery Operation
- Set Up Recipient Lists for Disaster Recovery Schedule Results

*Set up Agent Groups and Agent Computers Within Them*

FactoryTalk AssetCentre uses agents to perform Disaster Recovery operations. Agents are programs that communicate with the FactoryTalk AssetCentre server and perform tasks on behalf of the server. Agents let work be distributed and shared among multiple computers to spread processing load and speed up operations.

When a server needs an agent to perform a task, it locates the computer that is running the operation and assigns the task to that agent. The agent then reports the task’s completion to the server.
FactoryTalk AssetCentre Agent Groups is a plug-in that helps you to manage the agents into groups. With this plug-in, the agent computers that are connected to the same FactoryTalk AssetCentre server are not required to have the same configuration. This plug-in lets you to:

- Create agent groups, assign agent computers to the agent groups, and identify an agent group for an asset
- Assign backup and compare schedule tasks on an asset to the agent computers that belong to the asset’s agent group
- Monitor the status of agent computers in the Agent Status pane, the Agent Group Creation and Agent Assignment pane, and the Assets per Agent Group pane.

For more information about how to add a physical agent computer into FactoryTalk AssetCentre system instead of managing agent computers in agent groups, see the online help.

For more information on how to learn about more Agent Groups configurations, see the online help.

Create an Agent Group

Agent Groups plug-in manages the usage of agents. By default, there is one System Default agent group, which cannot be renamed or deleted. The System Default agent group is used for scheduled searches, and by default for any Disaster Recovery tasks.

If you must create a new agent group, complete the following steps.

1. Confirm that FactoryTalk AssetCentre is in Design mode.
2. From the View menu, choose Agent Groups.
3. Click the Add Agent Group button on the Agent group Creation and Agent Assignment toolbar.

![Add Agent Group dialog box](image)

The Add an Agent Group dialog box opens.

4. On the Add an Agent Group dialog box, enter the name and a description for the agent group. The description is optional.

   **TIP** The maximum number of agent groups that you can create depends on your licensed agent group capacity. By default, you can create one agent group in addition to the existing System Default agent group.

5. Click OK.

![Add an Agent Group dialog box](image)
Create an Agent Computer

You can create an agent computer in Agent Groups to monitor the physical agent computers.

To create an agent computer, complete the following steps:

1. Confirm that FactoryTalk AssetCentre is in Design mode.
2. From the View menu, choose Agent Groups.

3. Select an agent group, or an agent computer under the group where you want to add the agent computer.

Otherwise, the agent computer is created under System Default agent group.
4. Click the Add Agent Computer button on the Agent Group Creation and Agent Assignment toolbar.

The Add an Agent Computer dialog box opens.

5. On the Add an Agent Computer dialog box, enter the name, location, and the description for the agent computer.

6. Click OK.
Create a Schedule for a Disaster Recovery Operation

You can configure the following Disaster Recovery operations when you create a schedule:

- Backup
- Backup and Compare Disaster Recovery

**IMPORTANT** To create schedules, you must have the following permissions:

- Create a new schedule
- Edit a schedule
- Command a schedule

For more information on how to set permissions, see Configure Feature Security for FactoryTalk AssetCentre Users on page 62.

To create a schedule, complete the following steps.

1. In the asset tree, select the container or device for which you want to schedule an operation.

**TIP** Multiple assets can be included in the same scheduled operation by creating a scheduled operation for a container. For example, one container can contain multiple controllers.

Scheduling a Backup operation for the container backs up all devices in that container in one operation.

For all of a device's schedule properties to be available for modification, make sure each device to be added to a schedule has its Configuration Data that is defined in the device's properties.
2. From the View menu, choose Schedules.

3. Click the New button.
4. On the New Schedule Wizard: Step 1 of 3 dialog box, complete the following steps:
   a. Select an Operation type. This example uses Disaster Recovery - Backup.
   b. Name the schedule. - You must enter a unique name for the schedule.
   c. Describe the operation. (optional)
   d. Enter email addresses. - The chosen Disaster Recovery report that is generated at the end of the schedule is sent to the addresses listed in this field.

If you have multiple e-mail addresses you want to include, separate the addresses in the Completion Email List field with semicolons (;), or, if you have View Address Book permission, select the contacts or groups from the FactoryTalk Address Book.

The report that is sent from this field is the End of Schedule Report.

For more information about the End of Schedule report, see Set Up Recipient Lists for Disaster Recovery Schedule Results on page 132.

For more information on a particular field, see the online help.
5. You must configure all fields on the New Schedule Wizard: Step 2 of 3 dialog box, and click Next.

**TIP** To create a start time that does not begin on the hour or half hour, type the time (and AM or PM) in the field. It is possible to create a schedule that does not run on a specific date.

For example, if you choose to have a schedule run on the 31st day of every month, the schedule does not execute in months that do not have 31 days.

For more information on a particular field, click Help.
6. Complete the New Schedule Wizard: Step 3 of 3 dialog box.

In the tree on the left side of the dialog box, check boxes appear selected next to each asset in the schedule, if assets are used to create the schedule.

7. If necessary, clear a box not to include that asset in the schedule.

Properties for the selected device appear on the right side of the dialog box. For more information on how to complete the shown properties for the selected device, see the online help.

The schedule that you created is active unless you clear the Activate the Schedule box. For more information on a particular field, see the online help.

8. Click Finished.
Set Up Recipient Lists for Disaster Recovery Schedule Results

There are two different types of Disaster Recovery schedule reports you can send to specified recipients when a schedule completes:

- **End of Schedule report** - This general report summarizes information such as a Backup and Compare schedule’s start and stop times and whether there were any differences between the contents of the physical device and the asset’s master file that is stored in Archive.

  This report is configured through the Schedules tab.

- **Backup report or Backup and Compare report** - These more detailed, operation-specific reports include information such as asset and hardware details, the agent computer that ran the schedule, and the name and location of the master file used in a Compare.

  For Backup and Compare operations, the Backup and Compare report indicates if differences were found. To include the detail of what these differences were, attach the Compare Report file to the e-mail notifications. Both the Backup report and Backup and Compare report are configured through an asset’s scheduled operation properties.

---

**IMPORTANT** To configure a recipients list for schedule results, you **must** have the following permissions:

- Edit a schedule
- Command a schedule

For more information on how to set permissions, see Configure Feature Security for FactoryTalk AssetCentre Users on page 62.
To send a Backup report or Backup and Compare report at the end of a schedule, complete these steps.

1. On the Schedules tab, select the schedule that contains the asset for which you want to send a report.
2. Select the asset that is associated with the schedule and complete its operation properties.
3. If necessary, click the button in the Completion Email List to update the e-mail list.

4. Check the box in the Active column to activate the schedule.

**TIP** After a Backup and Compare operation completes, if no differences are found, the Compare Report file is attached to e-mail notifications if, in the device properties under Attach Report to email, you set the Event Completed field to True.

If differences are found, the Compare Report file is attached to e-mail notifications if you set the Event Compare Differences Detected field to True.

For more information, see the online help.
Run a Schedule

You can activate a schedule so that it **runs at its next scheduled time.** You did this automatically if you selected the Activate the Schedule box in the wizard when you created the schedule. You can also activate schedules from the Schedules tab.

To run a schedule immediately, you can **run schedules manually.** Choosing to run a schedule manually immediately runs the schedule and sends e-mail notifications to your recipient list instead of waiting for the operation’s next run time. Running a schedule manually does not affect that schedule’s next run time.

**IMPORTANT**  To run schedules, you **must** have the Command a schedule permission.

To active a schedule, you **must** have the Edit a schedule permission.

For more information on how to set permissions, see **Configure Feature Security for FactoryTalk AssetCentre Users on page 62.**

To activate an existing schedule that you did not activate when you created the schedule, click the Active checkbox next to the schedule you want to activate.

If the selected schedule is to run daily at 4:00 p.m., the schedule runs next at 4:00 p.m. today (or 4:00 p.m. tomorrow if it is already later than 4:00 p.m. today).
To run a schedule immediately without waiting for its next scheduled run time, complete the following steps.

**IMPORTANT** You cannot manually run a schedule that has Running status.

1. On the Schedules tab, select a schedule with Waiting to Run status.
2. Click the Run Now button.

Once the schedule is run manually, it returns to Waiting to Run status. If running the schedule manually causes the schedule to run past its start time, FactoryTalk AssetCentre does not attempt to run the previously scheduled operation. Instead, the message The schedule has tripped but did not run because it is already running and is logged to the AssetCentre Event Log and the schedule waits to run again at its next start time.

**TIP** When you move, copy, or delete assets in the asset tree, the schedules for those assets are also moved, copied, or deleted. For information about the impacts moving, copying, and deleting assets have on schedules, refer to the online help.

To learn about additional schedule tasks, for example, stopping schedules, changing schedule run times, setting asset defaults for schedules, or renaming, filtering, and deleting schedules, not covered in this publication, refer to the online help.

For more information on how to use the Disaster Recovery operation, see the following:

- FactoryTalk AssetCentre online help
- FactoryTalk AssetCentre Getting Results Guide, publication FTAC-GR002
Appendix A

Security Checklists

This section provides checklists to verify the intended operation of security functions in your system.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two Types of Security Verification</td>
<td>137</td>
</tr>
<tr>
<td>Security Requirements</td>
<td>137</td>
</tr>
<tr>
<td>Acceptance Testing Verification Checklist</td>
<td>138</td>
</tr>
<tr>
<td>Maintenance Verification Checklist</td>
<td>139</td>
</tr>
</tbody>
</table>

Two Types of Security Verification

You must verify security functions at the following intervals:

- Factory and Site Acceptance testing when the system is first installed.
- Routine maintenance during system operation.

Differences exist between the tasks that you must perform to verify the intended operation of the security functions at each interval.

Security Requirements

IEC-62443-4-2 SL 1 certification requirements exist with the following parts of the implementation:

- Configuring the Windows infrastructure
- Configuring the FactoryTalk® Components
- Configure FactoryTalk Security
- Configuring FactoryAssetCentre
Acceptance Testing Verification Checklist

During acceptance testing, inspect and audit the settings for each requirement that is described in Table 1 in a method that is appropriate for your application according to your company’s best practices.

For example, you can perform the following actions to confirm that you configured the system to meet specific IEC-62443-4-2 SL1 certification requirements:

- In the Windows domain, try to create a password that does not meet the group policy definition.
- Try to complete a task in the system that is not permitted for the user type that you are logged into the system as.
  
  This applies in the Active Directory or FactoryTalk Directory.
- Try to log into the system as a user that is not permitted to log in.

The following table describes the IEC-62443-4-2 SL 1 certification configuration requirements.

### Table 1 - Acceptance Testing Verification Checklist

<table>
<thead>
<tr>
<th>Part of System Installation</th>
<th>Requirement</th>
<th>Task Verified (✓)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller Access</td>
<td>Install the ControlLogix® 5580 controller in a secure location</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For more information, see the Develop a Secure Application chapter in the ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publication 1756-UM543.</td>
<td></td>
</tr>
<tr>
<td>Configure the Windows Domain</td>
<td>Configure a domain controller</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Create at least two user types and assign a minimum level of user permissions to each type.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Create groups to which you add users.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Define group policies on the domain controller, including the following required settings.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Password settings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User account access settings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System use notification settings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System inactivity lockout setting</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Apply the group policies to the Organizational Units in the domain</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Add servers and computers to the windows domain</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Assign users and computers to the appropriate Organizational Units.</td>
<td></td>
</tr>
<tr>
<td>Configure the FactoryTalk Components</td>
<td>Configure FactoryTalk Directory on a host computer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Add computers to the FactoryTalk Directory</td>
<td></td>
</tr>
<tr>
<td>Configure FactoryTalk Security</td>
<td>Complete the following tasks in FactoryTalk Administration Console</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Assign Windows-linked user groups to FactoryTalk Directory by linking to external users and groups or importing Active Directory groups. At least two user types are required.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configure the System Security policies</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configure Feature Security for FactoryTalk AssetCentre users</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configure Feature Security for RSLogix 5000® users, including the Controller: Modify Mode and Project: Download privileges</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configure the Security Authority Identifier in the Logix Designer application project</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configure FactoryTalk Policy Manager to implement CIP Security</td>
<td></td>
</tr>
</tbody>
</table>
Table 1 - Acceptance Testing Verification Checklist

<table>
<thead>
<tr>
<th>Part of System Installation</th>
<th>Requirement</th>
<th>Task Verified (✓)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure FactoryTalk AssetCentre</td>
<td>Add the assets that you must manage via FactoryTalk AssetCentre to the database.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manage the database size to make sure that logs are not lost.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Create Device Monitor - Change Detect schedules to track user action in the system.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Create Disaster Recovery schedules to perform planned system backups.</td>
<td></td>
</tr>
</tbody>
</table>

**Maintenance Verification Checklist**

During routine maintenance, inspect and audit the settings for each requirement that is described in Table 2.

Routine maintenance verification is performed after the system is configured and operating. The security settings that are required to meet IEC-62443-4-2 SL1 certification were verified during system installation.

During routine maintenance, we recommend that you verify requirements are met via specific tasks.

Table 2 - Maintenance Verification Checklist

<table>
<thead>
<tr>
<th>Part of System Maintenance</th>
<th>Requirement</th>
<th>Task to Verify Requirement Is Met</th>
<th>Task Verified (✓)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller Access</td>
<td>Restrict access to controller to authorized users only</td>
<td>Verify that the controller still resides in a secure location.</td>
<td></td>
</tr>
<tr>
<td>Configure the Windows Domain</td>
<td>Domain controller configured</td>
<td>Review audit logs to verify that the domain controller configuration is correct.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Active Directory configured</td>
<td>Review audit logs to verify that the Active Directory configuration is correct.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>At least two user types exist in the Active Directory, and that a minimum level of permissions is assigned to each type.</td>
<td>Review that the correct user types were created in the domain and the correct permissions were configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Correct users exist in correct groups.</td>
<td>Review that the groups contain the correct users.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The following required Group Policies are correctly defined on the domain controller.</td>
<td>Review that the Group Policy settings are correct.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Password settings</td>
<td>Review the audit and event logs to track system use. This task applies to the User account access, System use notification, and system inactivity lockout settings. It does not apply to the password settings.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User account access settings</td>
<td>Review the audit and event logs to track system use. This task applies to the User account access, System use notification, and system inactivity lockout settings. It does not apply to the password settings.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System use notification settings</td>
<td>Review the audit and event logs to track system use. This task applies to the User account access, System use notification, and system inactivity lockout settings. It does not apply to the password settings.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System inactivity lockout settings</td>
<td>Review the audit and event logs to track system use. This task applies to the User account access, System use notification, and system inactivity lockout settings. It does not apply to the password settings.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Correct servers and computers exist in the windows domain</td>
<td>Review audit logs to verify that the correct computers exist in the Windows domain.</td>
<td></td>
</tr>
<tr>
<td>Configure the FactoryTalk Components</td>
<td>FactoryTalk Directory is configured on the host computer</td>
<td>Verify that the FactoryTalk Directory is configured on the correct centralized host computer.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Correct computers exist in the FactoryTalk Directory</td>
<td>Verify that correct computers exist in the FactoryTalk Directory.</td>
<td></td>
</tr>
</tbody>
</table>
## Security Checklists

### Configure FactoryTalk Security

The following exist in FactoryTalk Administration Console

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Task to Verify Requirement Is Met</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correct Windows-linked user groups are assigned to FactoryTalk Directory.</td>
<td>Review the user groups that are in the FactoryTalk Directory to verify that the Windows-linked user groups are assigned correctly. At least two user types, with appropriate permission, must exist.</td>
</tr>
<tr>
<td>System Security policies are configured correctly.</td>
<td>Review the System Security settings to verify that they are correct. Review audit logs in FactoryTalk AssetCentre.</td>
</tr>
<tr>
<td>Feature Security for FactoryTalk AssetCentre users is configured correctly.</td>
<td>Review the Feature Security settings for FactoryTalk AssetCentre users to verify that they are correct. Review audit logs in FactoryTalk AssetCentre.</td>
</tr>
<tr>
<td>Feature Security for RSLogix 5000 users is configured correctly.</td>
<td>Review the Feature Security settings for RSLogix 5000 users to verify that they are correct. Review audit logs in FactoryTalk AssetCentre.</td>
</tr>
<tr>
<td>The Security Authority Identifier is configured in the Logix Designer application project</td>
<td>Review the Logix Designer application project (RSLogix 5000 project) that is used with the IEC-62443-4-2 SL 1 certified ControlLogix 5580 controller to verify that it includes correct Security Authority Identifier configuration.</td>
</tr>
</tbody>
</table>

### Configure FactoryTalk AssetCentre

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Task to Verify Requirement Is Met</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appropriate assets exist in the FactoryTalk AssetCentre database.</td>
<td>Review the Asset tree to verify that the asset list in the database is correct.</td>
</tr>
<tr>
<td>Logs are not being lost from the FactoryTalk AssetCentre database.</td>
<td>Review the database size to verify that is it sufficiently sized so logs are not lost.</td>
</tr>
<tr>
<td>Device Monitor - Change Detect schedules are tracking user action in the system.</td>
<td>Review the event log to verify that user actions are not lost.</td>
</tr>
<tr>
<td>Disaster Recovery schedules back up the system as desired.</td>
<td>Review the event log to verify that the system is being correctly backed up.</td>
</tr>
</tbody>
</table>

### Table 2 - Maintenance Verification Checklist

<table>
<thead>
<tr>
<th>Part of System Maintenance</th>
<th>Requirement</th>
<th>Task to Verify Requirement Is Met</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure FactoryTalk Security</td>
<td>The following exist in FactoryTalk Administration Console</td>
<td>Review the user groups that are in the FactoryTalk Directory to verify that the Windows-linked user groups are assigned correctly. At least two user types, with appropriate permission, must exist.</td>
</tr>
<tr>
<td></td>
<td>System Security policies are configured correctly.</td>
<td>Review the System Security settings to verify that they are correct. Review audit logs in FactoryTalk AssetCentre.</td>
</tr>
<tr>
<td></td>
<td>Feature Security for FactoryTalk AssetCentre users is configured correctly.</td>
<td>Review the Feature Security settings for FactoryTalk AssetCentre users to verify that they are correct. Review audit logs in FactoryTalk AssetCentre.</td>
</tr>
<tr>
<td></td>
<td>Feature Security for RSLogix 5000 users is configured correctly.</td>
<td>Review the Feature Security settings for RSLogix 5000 users to verify that they are correct. Review audit logs in FactoryTalk AssetCentre.</td>
</tr>
<tr>
<td></td>
<td>The Security Authority Identifier is configured in the Logix Designer application project</td>
<td>Review the Logix Designer application project (RSLogix 5000 project) that is used with the IEC-62443-4-2 SL 1 certified ControlLogix 5580 controller to verify that it includes correct Security Authority Identifier configuration.</td>
</tr>
</tbody>
</table>
## Index

### A
- **active directory** 6, 16
  - group policy management 17
  - groups and users 16

### C
- **CIP Security** 26
- **code**
  - restrictions in Logix Designer 91
- **communication**
  - restriction in Logix Designer 88
- **compensating countermeasures**
  - active directory 6
  - ControlFLASH 6
  - ControlFLASH Plus 6
  - FactoryTalk Activation Manager 6, 26
  - FactoryTalk AssetCentre 6
  - FactoryTalk Linx 6
  - FactoryTalk Policy Manager 6, 26 . . . 29
  - FactoryTalk Security 6
  - FactoryTalk System Services 6
  - FactoryTalk View 6
  - Studio 5000 Logix Designer 6
- **configuration**
  - code restrictions in Logix Designer 91
  - communication restriction in Logix Designer 88
  - data restrictions in Logix Designer 89
- **configure**
  - FactoryTalk Activation Manager 26
  - FactoryTalk Directory 21 . . . 25
  - FactoryTalk Policy Manager 26 . . . 29
- **controller logical name**
  - create in FactoryTalk Administration Console 85
  - ControlFLASH 6, 8
  - ControlFLASH Plus 6
  - **controller**
  - enable security 81
  - **controller logical name**
  - controller name in FactoryTalk Directory 81

### D
- **data**
  - restrictions in Logix Designer 89
- **domain controller** 8, 15
  - group policy management 17
  - manage groups and users 16

### E
- **enable**
  - controller security 81

### F
- **FactoryTalk Activation Manager** 6, 26
  - configure 26
- **FactoryTalk Administration Console**
  - configure FactoryTalk Directory 32
  - configure FactoryTalk Directory users and groups 34 . . . 41
  - configure feature security
    - FactoryTalk AssetCentre 62 . . . 66
    - RSLogix 5000 67 . . . 80
  - configure product policies 54 . . . 56
  - configure product policies feature security 57 . . . 61
  - configure system policies 42 . . . 53
  - create controller logical name 85
  - create permission sets 82 . . . 84
  - permission sets 72, 74
  - security requirements 33
- **FactoryTalk AssetCentre** 6, 8
  - audit and change management 96
  - configure feature security 62 . . . 66
  - logs 96
    - view and search 110
  - policy settings 65
- **FactoryTalk Directory** 8
  - configure 21 . . . 25
  - controller logical name 81
  - managed by FactoryTalk Administration Console 32
  - network directory 23
  - requirements 19
  - users and groups 34 . . . 41
- **FactoryTalk Linx** 6
- **FactoryTalk Policy Manager** 6, 26 . . . 29
  - configure 26 . . . 29
- **FactoryTalk Security** 6
- **FactoryTalk System Services** 6
- **FactoryTalk View** 6, 8
- **feature security**
  - FactoryTalk AssetCentre
    - configure 62 . . . 66
  - product policies
    - configure with FactoryTalk Administration Console 57 . . . 61
  - RSLogix 5000
    - configure in FactoryTalk Administration Console 67 . . . 80
Index

G
group policies
manage in domain controller 17

L
Logix Designer
  code restrictions 89
  communication restriction 88
  data restrictions 89
  permission sets 81
  security authority identifier 81

logs
  FactoryTalk AssetCentre 96
  view and search 110

N
network
directory definition 23

P
permission sets 72, 74, 81
  create in FactoryTalk Administration Console 82 . . . 84

policies
  group policy in domain controller 17
  product 54 . . . 56
  feature security 57 . . . 61
  system 42 . . . 53

policy settings
  FactoryTalk AssetCentre 65
  RSLogix 5000
    action permissions 76
    feature security 69

product policies
  configure with FactoryTalk Administration Console 54 . . . 56
  feature security 57 . . . 61
  configure with FactoryTalk Administration Console 57 . . . 61

product-level requirements 5

R
requirements
  active directory 6, 16
  group policy management 17
  groups and users 16
  compensating countermeasures 6
  configure FactoryTalk AssetCentre feature security 62 . . . 66
  configure RSLogix 5000 feature security 67 . . . 80
  ControlFLASH 6
  ControlFLASH Plus 6

FactoryTalk Activation Manager 6, 26
FactoryTalk Administration Console 33
FactoryTalk AssetCentre 6
audit and change management 96
FactoryTalk Directory 19
FactoryTalk Linx 6
FactoryTalk Policy Manager 6, 26 . . . 29
FactoryTalk Security 6
FactoryTalk System Services 6
FactoryTalk View 6
product-level 5
Studio 5000 Logix Designer 6
Windows infrastructure 13

restrict
  code in Logix Designer 91
  communication in Logix Designer 88
  data in Logix Designer 89

RSLogix 5000
  policy settings
    action permissions 76
    feature security 69

S
security
  enable controller 81

Studio 5000 Logix Designer 6, 8

system policies
  configure with FactoryTalk Administration Console 42 . . . 53

T
threat level
  SL 1 5

U
users and groups
  in active directory 16
  in FactoryTalk Directory 34 . . . 41

W
Windows
  active directory 16
  domain 14
  domain controller 8, 15
  Infrastructure 13
**Rockwell Automation Support**

Use the following resources to access support information.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct Dial Codes</td>
<td>Find the Direct Dial Code for your product. Use the code to route your call directly to a technical support engineer.</td>
<td><a href="http://www.rockwellautomation.com/global/support/direct-dial.page">http://www.rockwellautomation.com/global/support/direct-dial.page</a></td>
</tr>
</tbody>
</table>

**Documentation Feedback**

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete the How Are We Doing? form at http://literature.rockwellautomation.com/idc/groups/literature/documents/du/ra-du002__en-c.pdf.

---


Allen-Bradley, ControlLogix, FactoryTalk, KineticX, PanelView, Rockwell Automation, Rockwell Software, RSLinx, RSLogix 5000, RSNetworx, Stratix, and Studio 5000 Logix Designer are trademarks of Rockwell Automation, Inc. Microsoft is a trademark of Microsoft Corporation.

CIP, CIP Security and EtherNet/IP are trademarks of ODVA, Inc.

Trademarks not belonging to Rockwell Automation are property of their respective companies.

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

www.rockwellautomation.com

---

**Power, Control and Information Solutions Headquarters**

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

Publication SECURE-UM001A-EN-P - March 2019

Copyright © 2019 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.