

# System 800xA

## Administration and Security

System Version 5.1

Power and productivity  
for a better world™





# **System 800xA**

## **Administration and Security**

**System Version 5.1**

---

## NOTICE

This document contains information about one or more ABB products and may include a description of or a reference to one or more standards that may be generally relevant to the ABB products. The presence of any such description of a standard or reference to a standard is not a representation that all of the ABB products referenced in this document support all of the features of the described or referenced standard. In order to determine the specific features supported by a particular ABB product, the reader should consult the product specifications for the particular ABB product.

ABB may have one or more patents or pending patent applications protecting the intellectual property in the ABB products described in this document.

The information in this document is subject to change without notice and should not be construed as a commitment by ABB. ABB assumes no responsibility for any errors that may appear in this document.

In no event shall ABB be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall ABB be liable for incidental or consequential damages arising from use of any software or hardware described in this document.

This document and parts thereof must not be reproduced or copied without written permission from ABB, and the contents thereof must not be imparted to a third party nor used for any unauthorized purpose.

The software or hardware described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license. This product meets the requirements specified in EMC Directive 2004/108/EC and in Low Voltage Directive 2006/95/EC.

## TRADEMARKS

All rights to copyrights, registered trademarks, and trademarks reside with their respective owners.

Copyright © 2003-2013 by ABB.  
All rights reserved.

Release: February 2013  
Document number: 3BSE037410-510 D

---

# Table of Contents

## About this User Manual

General .....	11
User Manual Conventions .....	11
Warning, Caution, Information, and Tip Icons .....	11
Terminology.....	12
Released User Manuals and Release Notes .....	12

## Section 1 - Introduction

### Section 2 - 800xA License Handling

Licensing Software .....	17
Software Keys.....	17
Central Licensing Service System Extension .....	17
License Expansion.....	20

### Section 3 - Security Planning

Risk Management.....	23
Physical Security .....	24
Workstation Security .....	25
Personnel Security .....	25

### Section 4 - Security Configurations

Concept.....	29
800xA Security Description .....	30
Users and Groups .....	30
Installation Account .....	30

Adding Users .....	30
Removing Users.....	32
Windows Workgroups.....	33
Windows User Groups in Domain Controller.....	36
How to Change User Permissions.....	41
Authentication problem in 800xA Workplace .....	82
How to Restrict the User Interface.....	82
How do I see... ..	88
Advanced Security Configuration .....	94
The Access Evaluation Algorithm .....	94
The Evaluation Search Order.....	95
Audit Logging.....	101
Audit Trail Configuration .....	102
Security Audit Config .....	105
Windows Audit Function .....	110
Critical Operation Authentication Support .....	113
Logover .....	119
Digital Signature .....	126
Confirmed Write .....	136
Memory Swapping.....	146
Security of External Data .....	147
Bulk Data Manager / Document Manager / Engineering Templates .....	147
Parameter Manager .....	148
Reuse Assistant .....	148
Secure Remote Connections using VPN.....	150
<b>Section 5 - Process Sectioning</b>	
Security Setting by Structuring in Plant Explorer.....	151
Setting the Security Definition Aspects in the Example.....	152
<b>Section 6 - Point of Control</b>	
Introduction .....	155
Point of Control Features .....	155

Enabling Point of Control .....	157
Configuring Point of Control.....	158
Responsibility Configuration .....	159
Section Configuration .....	164
Alarm List Responsibility Filter Configuration .....	171
Alarm Mapping .....	173
Section Lock.....	175
OPC Properties.....	176

## **Section 7 - Security Examples**

Default Security Setting of the Admin Structure.....	179
The Default Security Setting of a System Object.....	179
Security Setting on an Aspect Object Basis .....	182
Different Settings of Structure in Authority Range .....	183

## **Section 8 - System Services**

Unique Naming of Service Groups .....	185
History .....	185
History Server Provider Metrics .....	187
Lock Server.....	191
Process Object Locking Aspect .....	191
Lock Type Definition Aspect .....	194
Service Definition Aspect .....	195
Workplace Service .....	197
Tracking Function .....	197
Enable Workplace Service .....	198
Remote Interaction Function .....	198
Alarm and Event .....	199
Redundant Services .....	223
Configuration of Redundant Services .....	223
Redundant Aspect Servers .....	223
Change from Redundant to Single Configuration.....	224
Restart Redundant Configuration .....	224

Recovering from Read-only Mode ..... 225  
Aspect Server Automatic Recovery ..... 226

## **Section 9 - Scheduling Reports**

Prerequisites ..... 229  
Scheduling ..... 229  
    Creating Service Group/Service Provider Objects ..... 230  
    Scheduling Reports via the Application Scheduler ..... 233

## **Appendix A - Default Security Settings for Process Objects**

### **Appendix B - Security Checklists and Fault Search**

Security Checklists ..... 243  
Fault Search of 800xA Security ..... 244  
    Fault - Configuration Wizard only shows System Software Icon ..... 244  
    Fault - Permission granted for modify ..... 245  
    Fault - Permission not granted for modify ..... 245  
    Fault - Permission not granted for OPC Write ..... 246  
    Fault - The default permission does not apply to the wanted behavior ..... 247  
    Fault - A user is not possible to delete ..... 247

## **Appendix C - Secured Server Configuration**

### **Appendix D - Troubleshooting in 800xA Workgroups**

Problem with Hostname Lookup ..... 253  
    Fail to add Client or Server to a 800xA System ..... 254  
    Invalid Account encountered during System Software User Settings ..... 255  
    HTTP 500 - Internal Server Error Message ..... 255

### **Appendix E - System Alarm and Event Messages**

System Events for Data Access Functions ..... 260  
    OPC DA Client - AdvDsOPCServerAdapter ..... 261  
    Upload - AfwUploadServer ..... 262



Property Transfer - AfwPropertyTransfer .....262

**Appendix F - Additions in Windows  
added by 800xA**

**Index**

**Revision History**

Introduction .....269  
Revision History .....269  
Updates in Revision Index A .....270  
Updates in Revision Index B .....270  
Updates in Revision Index C .....271  
Updates in Revision Index D .....272



---

# About this User Manual

## General



Any security measures described in this document, for example, for user access, password security, network security, firewalls, virus protection, etc., represent possible steps that a user of an 800xA System may want to consider based on a risk assessment for a particular application and installation. This risk assessment, as well as the proper implementation, configuration, installation, operation, administration, and maintenance of all relevant security related equipment, software, and procedures, are the responsibility of the user of the 800xA System.

This instruction describes Industrial<sup>IT</sup> 800xA functions to administrate and set up security for your system.

## User Manual Conventions

Microsoft Windows conventions are normally used for the standard presentation of material when entering text, key sequences, prompts, messages, menu items, screen elements, etc.

## Warning, Caution, Information, and Tip Icons

This User Manual includes **Warning**, **Caution**, and **Information** where appropriate to point out safety related or other important information. It also includes **Tip** to point out useful hints to the reader. The corresponding symbols should be interpreted as follows:



Electrical warning icon indicates the presence of a hazard which could result in *electrical shock*.



Warning icon indicates the presence of a hazard which could result in *personal injury*.



Caution icon indicates important information or warning related to the concept discussed in the text. It might indicate the presence of a hazard which could result in *corruption of software or damage to equipment/property*.



Information icon alerts the reader to pertinent facts and conditions.



Tip icon indicates advice on, for example, how to design your project or how to use a certain function

Although **Warning** hazards are related to personal injury, and **Caution** hazards are associated with equipment or property damage, it should be understood that operation of damaged equipment could, under certain operational conditions, result in degraded process performance leading to personal injury or death. Therefore, **fully comply** with all **Warning** and **Caution** notices.

## Terminology

A complete and comprehensive list of terms is included in *System 800xA System Guide Functional Description (3BSE038018\*)*. The listing includes terms and definitions that apply to the 800xA System where the usage is different from commonly accepted industry standard definitions and definitions given in standard dictionaries such as Webster's Dictionary of Computer Terms.

## Released User Manuals and Release Notes

A complete list of all User Manuals and Release Notes applicable to System 800xA is provided in *System 800xA Released User Manuals and Release Notes (3BUA000263\*)*.

*System 800xA Released User Manuals and Release Notes (3BUA000263\*)* is updated each time a document is updated or a new document is released.

It is in pdf format and is provided in the following ways:

- Included on the documentation media provided with the system and published to ABB SolutionsBank when released as part of a major or minor release, Service Pack, Feature Pack, or System Revision.
- Published to ABB SolutionsBank when a User Manual or Release Note is updated in between any of the release cycles listed in the first bullet.



A product bulletin is published each time *System 800xA Released User Manuals and Release Notes (3BUA000263\*)* is updated and published to ABB SolutionsBank.



---

# Section 1 Introduction

This manual describes IndustrialIT 800xA functions to administrate and set up security for your system. The 800xA Security model is based on extensions to Windows security model.

Some of the topics covered in this manual are:

- 800xA License Handling.
- Security Planning.
- Security Configuration.
- System Services Configuring.
- Backup and Restore of the 800xA System.
- Checking a 800xA system.
- Single Node Replacement.
- Windows and 800xA Updates.
- Scheduling Reports.
- Alarms and Events.
- Secured Server Configuration.
- Security Checklist and Fault Search.
- Troubleshooting in 800xA Workgroups.
- Diagnostic Collection Tool.
- Consistency Check.





---

## Section 2 800xA License Handling

### Licensing Software

Certain 800xA System functions must be licensed before you can use them. These functions will not operate until the applicable licenses are installed. The software is licensed by relating a software key for each software feature with a unique machine identifier. Software keys are obtained from the ABB software license administration system. This section describes how to expand the licensing software and then use the licensing tool to apply for software keys as required by your system.

### Software Keys

Before you can install the 800xA software keys you must have installed the licensing software on the designated license server and all license clients, and you must have applied for and received your software keys.

### Central Licensing Service System Extension

Description on how to enable the License Usage Monitoring functionality is described below



The steps described below has to be performed as 800xA Installer.

### Enabling License Usage Monitoring Functionality

To enable the License Usage Monitoring functionality, add the License Usage aspect to the Root object in the Control Structure.

1. Select the newly created License Usage aspect in the Aspect List area.

- The License Usage aspect appears in the Preview Area as shown in [Figure 1](#). It shows a list of license features and the current usage.

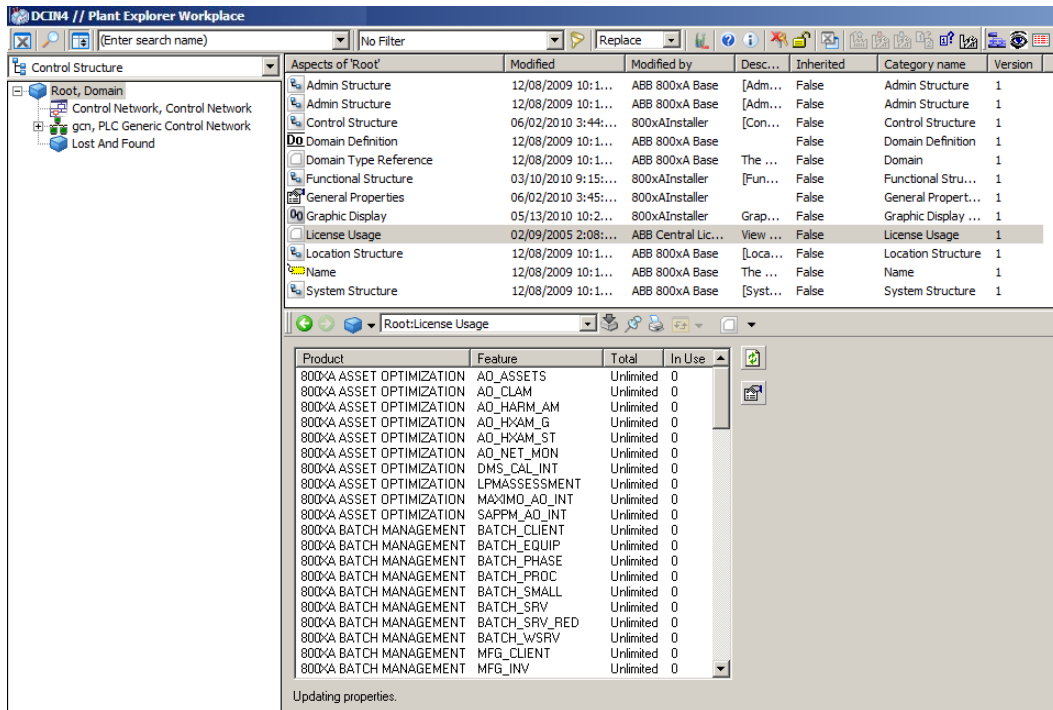


Figure 1. License Usage Aspect

- The License Usage aspect also maintains a set of General Properties in the Root object. Select the General Properties in the Aspect List area to produce a view of the General Properties aspect in the Preview area as shown in [Figure 2](#). These properties can be used to construct alarm expressions to monitor when licensed quantities are running low.



5. Select the newly created Alarm Expression aspect in the Aspect List area to produce the view in the Preview Area like the one shown in [Figure 3](#).

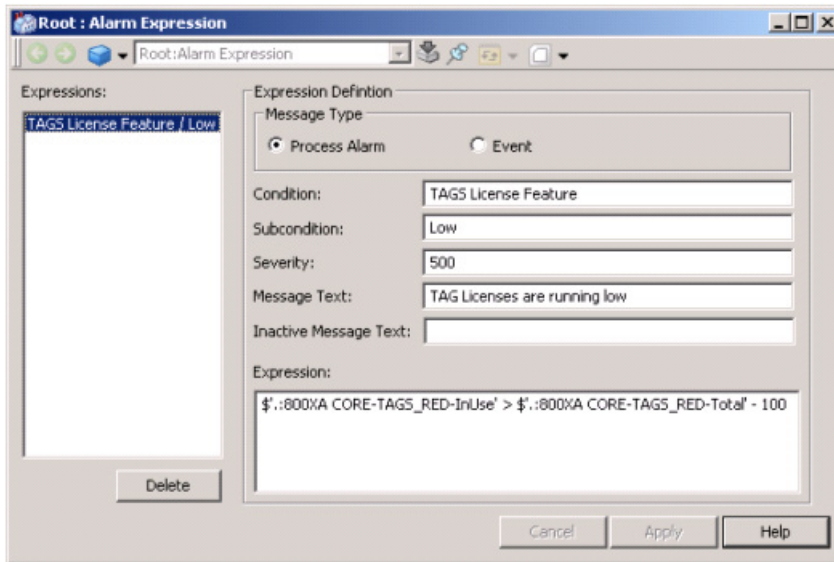


Figure 3. Alarm Expression Aspect

6. Fill out the Alarm Expression aspect according to the requirements of the system and click **Apply**.

## License Expansion

When you have ordered and received new software, you need to request new keys to expand the license.

Install your new software and follow the same steps as when requesting software keys for the first time. These steps are described below:

1. Obtain the machine ID of the workstation that the Central Licensing System software is installed on, or going to be installed on.
2. Have the registration license numbers, found on the license certified form, available.

3. Complete the license key request form provided with the software. Follow the instructions found on this form. Be sure to enter your e-mail address on the form.



An alternative is to generate and complete a new request form using the license entry program. To do this:

- Select the **License** tab on the license entry tool.
  - Click **Request SWKey**.
4. Fill in the form as necessary.
  5. Send the registration to the ABB software license administrator using one of the methods described on the registration form.
  6. Wait for the feature keys to be returned. The method by which the feature keys will be returned is selected on the registration form. The choices are Internet mail, postal mail or fax.

Internet mail is recommended. This way, the software keys will be returned as an attached *.sla* file. This is the format required by the license entry tool. In this case you simply need to detach the file and save it to a location on the license server where it may be accessed by the license entry tool.

If you choose to have the keys returned by mail, or fax, a mail address or fax number must be included on the form.

When you have received your new software keys, install them on the license server. For more information about Installing Licence Software, Requesting Software Keys and Installing Licenses on the Server, see the *System 800xA Manual Installation (3BSE034678\*)* instruction.



---

## Section 3 Security Planning

When planning for the data security of a plant installation, take the total security into consideration. It is not enough to provide a strong firewall if there is free access to the control room in the plant.

### Risk Management

Establish a detailed risk management program which covers the complete spectrum of risks. Make a crash plan. Make plans for how to recover and how to restore.

Create and implement testing procedures to ensure that the security plans act as planned. Inform your employees about the security plans for the plant and train them to act accordingly. Update the plan requirements regularly, at least once per year.

The risk management may include:

- Recovery from destruction of data information
- Destruction of data media and workstations
- Crash planning
- External personnel - do consultants have to see passwords etc.
- Security backup of data
- Virus protection
- Password
- User identity
- Internet access
- Screen locking

## Physical Security

### Backup

Make a written backup plan for programs and data. Test this plan by making a backup and restoring the data. The backup should be stored at an external and secure location.

### Destruction of Data Media and workstations

When data media (disks, CDs, or tapes) or workstation hardware are discarded, there is a risk of information being stolen. Destroy all information on these items before trashing or recycling.

### Workstation Room

Minimize the number of people who have access to the facilities in order to prevent unauthorized access.



Protect workstation facilities with a smoke/fire detection system. If feasible, connect all alarms to a manned guard station or fire station.

### UPS

Use an Uninterrupted Power Supply (UPS) of sufficient capacity that will allow the 800xA System to be shutdown in an orderly manner during power outages. Place the UPS system on a regular maintenance schedule.

### Cables

Ensure that it is not possible to tap data from the cables inside and outside the control room.

### Process Equipment

If something is protected in the control room, the same physical or other protection shall be implemented against manual changes in the plant.



## Inventory Spare Parts

Maintain an accurate inventory of all hardware and software. If the plant uses items that are critical and hard to acquire, consider stocking spare parts. Store them in a safe place.

## Workstation Security

### Virus Check

Run a virus check daily or according to the security plan.  
Update the virus protection frequently.

### Services

Do not start services that are not needed, such as FTP and Telnet.

### Firewall

Filtering:

- Filter out unnecessary services, addresses, ports, and protocols at the router - only allow those that are needed.
- If on the Internet, for example when using the Web Browser aspect, use a stateful firewall.

### Servers

Security configuration of the server is important.

## Personnel Security

### Assigning Permissions

Ensure that all personnel positions have been assigned security level designations.

## Password Security

When establishing a reasonable password security scheme, consider the following:

- All accounts **MUST** have a password.
- Define separate accounts and different passwords for the Installation and the Service Account.
- Use a secure method (for example, an encrypted database) to remember and store information about non personal accounts (for example, the system Service Account and Administrator Account for Network Devices).
- Try to always create passwords that are at least 14 characters long.
- A strong password should have different types of characters such as upper and lower case letters, punctuation, symbols, and numbers.
- Passwords must not be hard to remember. (If they are, there is a risk that they will be written down on a piece of paper and kept where they could be discovered.)
- Create a passphrase instead of a password to establish better security. Passphrases are created using a meaningful sentence that can easily be remembered.
  - Select a few letters from the sentence to create a passphrase. For example, consider a sentence:  
*All accounts MUST have a password.*  
Select the last letter of each word in the sentence to create *lsTead*.
  - Add complexity and length to the passphrase with numerals, punctuations, and symbols.  
For example, *#2lsT?ead\*7*
- Use a password checker to evaluate the strength of the password.
- Change the Passwords periodically. Plan and use a change mechanism.
- User Accounts should normally be disabled when there are several bad logins in a row.

**Do not:**

- Reuse passwords in different projects.
- Create passwords that can easily be guessed such as:
  - User Account names
  - Direct dictionary words in any languages
  - Abbreviations, misspellings, or words spelt backwards
  - Sequence of characters or repeated characters or adjacent characters on the keyboard
  - Date of birth, name, passport number, or similar personal information
- Write down the passwords, unless the writing is stored securely.
- Leave papers on your desk containing your password or clues to your password.

**Root Accounts**

When creating root accounts, take into consideration to:

- Limit the number of users.
- Use the password security rules, refer to [Password Security](#).

**User Accounts**

When creating user accounts, take into consideration:

- Accounts should be removed when an employee leaves the company or moves into a different role within the company.
- Accounts should NOT be shared.

**Security Testing**

To make the security as good as possible, always remember to:

- Have the latest ABB approved security patches installed on the system.
- Subscribe to security mailing lists and news group.

## **Contractors**

Ensure that all personnel, including contractors, have received appropriate clearances and training.

## **Training Program**

Security Awareness and Training:

- Establish an employee security awareness and training program.
- Provide specialized security training.

---

## Section 4 Security Configurations

### Concept

The 800xA Security model is based on extensions to Windows security model. The extensions make it possible to set permissions for users or user groups on an 800xA System, a structure or part of a structure, or an Aspect Object™.

The security setting can also be limited to a single node, or all nodes. This feature makes it possible to require an operation to be performed from a node within sight of the area it controls.

Related to the security in the usage settings are roles. Roles adapt the user interface for different types of users, i.e. user groups. Some operations require an application engineer or system engineer role to be performed.

However, having the correct role does not give the user the permission to perform the operation. The permission is completely controlled by the security configuration of the system.



Note that there is a difference between role and permission. To view an object, a user requires an 800xA role like Operator or Application Engineer. To access, or manipulate an object a user requires an appropriate permission added to his/her role. This appropriate permission can only be defined by a specific Security Definition aspect and the identity of the Windows user, refer to the [User Role Default Settings](#) on page 85.

As an administrator, all permissions are available because the security is turned off.

By default a user does not have all roles. Some structures, configuration tabs, and so on, are hidden.

## 800xA Security Description

Security and auditing in an 800xA System are set with the Security Definition aspects, which are added to Aspects Objects.

The security is set by changing the Authority Range, Permissions (related to User Identity/Group/Node and Environment) and **Search** Option of a Security Definition aspect. By using these settings, the desired security level for your plant is defined.

The Audit function is setup more or less in the same way as security. Audit logging will allow the administrator to track security related events - for example attempts to access secured objects etc.



Ensure there is a valid and current Windows backup of your domain server(s).

## Users and Groups

### Installation Account

To run a task, if no specific account is mentioned, use the 800xAInstaller account.

### Adding Users



If you are running the Domain Server on a Windows 2008 Server, you must add the user that should be able to add other users to the Process Portal system to the Windows group Pre-Windows 2000 Compatible Access.

The Users icon in the Configuration Wizard activates the User Administration dialog box.



From System Version 5.1 onwards, a simplified procedure of adding users using the **System Configuration Console** is available. Refer to *System 800xA 5.1 Tools (2PAA101888\*)* for more information about the System Configuration Console tasks.

1. Open the Configuration Wizard (**Start > All Programs > ABB Industrial IT 800xA > System > Configuration Wizard**).
2. Select **System Administration** and click **Next**.
3. Select the system in which you want to configure users to and click **Next**.

4. Select **Users**, see Figure 4. Now the User Configuration dialog box is displayed.

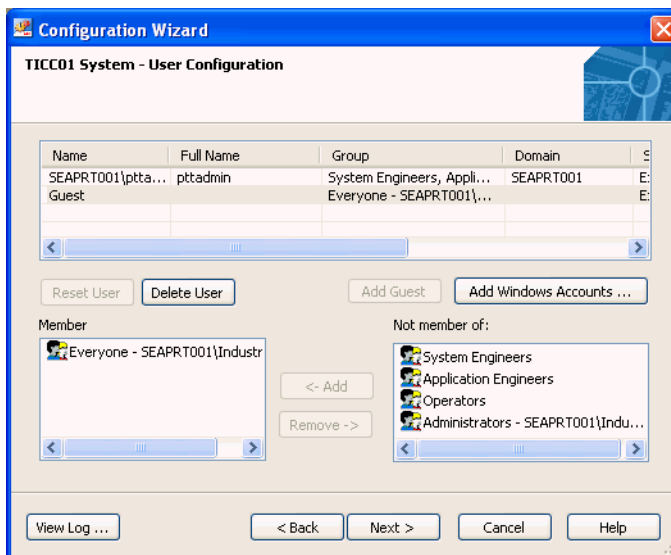


Figure 4. User Configuration Dialog Box

The top window shows the System 800xA users. Users can be added and deleted. To delete a user select the user in the top window and click **Delete User**. An easy way to move all groups in the **Not member of** text field to the **Member** text field, is to click the **Reset User** button.



You have to have both the System Engineer role and the Application Engineer role to delete a user.

To add a Windows user to a System 800xA group follow the steps:

1. Click the **Add Windows Accounts...** button.
2. The next dialog box (Figure 5) shows the Windows users of the domain that is selected in the drop-down menu. Select the Windows users you want to add to the Industrial<sup>IT</sup> 800xA System users and click **Add**.

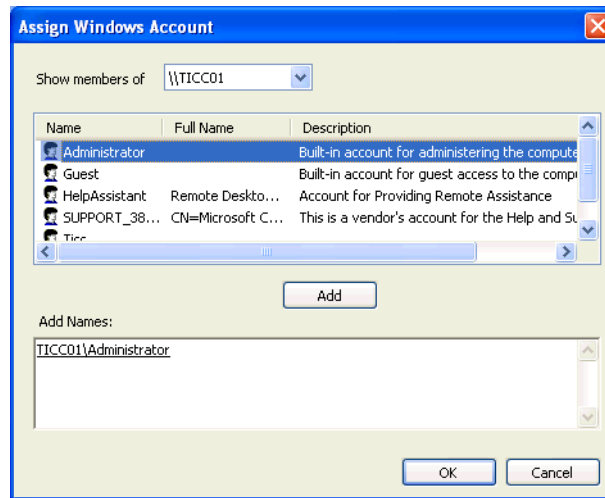


Figure 5. Assign Windows Account Dialog Box

- Repeat until all Windows users you want to add are added to the **Add Names** area then click **OK**.
- In the User Configuration dialog box, [Figure 4](#), it is possible to select the Industrial<sup>IT</sup> 800xA groups of which a Windows user must be member. Select Windows user in the top window and use the **Remove** and **Add** buttons to move Industrial<sup>IT</sup> 800xA groups to the **Member of** field.

## Removing Users

System engineers can remove users and user groups from the system.

To remove a user, select the user in the list and click **Delete**. Refer to [Figure 4](#) for more information.



Users can also be removed from the system using the System Configuration Console. Refer to *System 800xA 5.1 Tools (2PAA101888\*)* for more information about the System Configuration Console tasks.

The system engineer must wait to delete the user from the PPA system until all the entries for the selected user is overwritten in the AuditEvent list.





Backup and Restore procedures are not affected because of a change in the user account.

## Windows Workgroups

A Workgroup System should not consist of more than a combined Aspect and Connectivity Server, separate Application Servers, and five or six clients. A Workgroup becomes increasingly difficult to administrate as the number of users and nodes grows. Workgroups must be considered only for small systems with a few users. [Appendix D, Troubleshooting in 800xA Workgroups](#) provides troubleshooting information.



Fast User Switching cannot be used.

### Preparation and Configuration

The following is a short description for the preparation and configuration of the System Software User Settings during installation of Process Portal in a Windows Workgroup environment.



This procedure applies to Windows 7 operating systems. Adapt the procedure accordingly for other supported Windows operating systems.

1. As local administrator, set up all nodes as members of a Workgroup.
  - a. Select **Start** and right-click on **Computer**.
  - b. Select **Properties** from the context menu.

Control Panel > System and Security > System

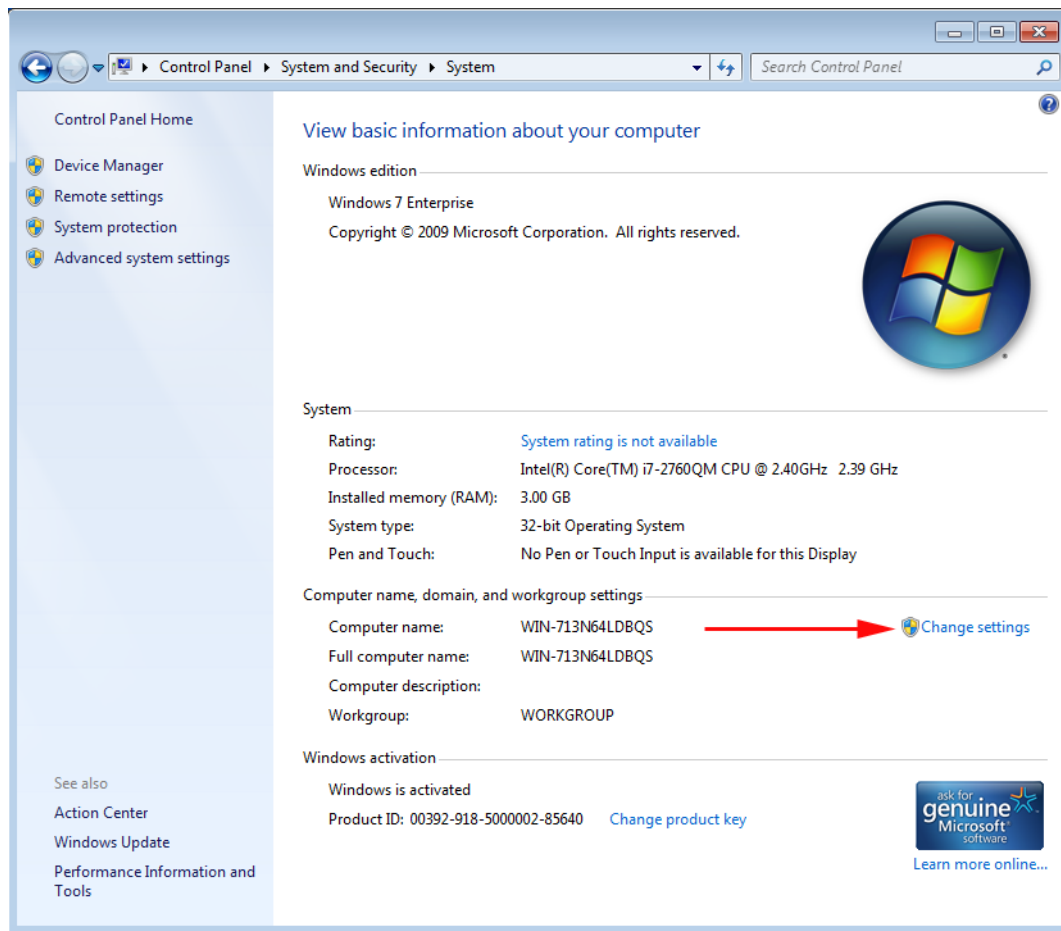
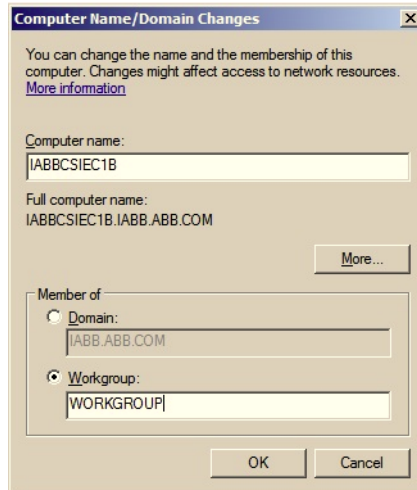


Figure 6. Change Settings from the Control Panel

- c. Click **Change settings**, the **System Properties** window is displayed.
- d. Select the **Computer Name** tab.

- e. Click **Change** to open the **Computer Name/Domain Changes** dialog shown in [Figure 7](#).



*Figure 7. Computer Name/Domain Changes Dialog Box*

- f. Type the workstation name in the Computer name field.
  - g. Select **Workgroup** in the Member of frame and give the workgroup a name.
  - h. Click **OK**.
2. Restart all nodes.
  3. Log in as 800xA Installer and install the Process Portal software on all nodes that are members of the Workgroup.
  4. When the installation has reached the System Software User Settings dialog, configure it according to [Figure 8](#). Use the local machine name as domain name.

The IndustrialITAdmin, IndustrialITUser groups, and a Service Account will be created.



Figure 8. System Software User Settings Dialog

5. Add users and user groups in Windows, according to the requirements of the system. Ensure that the set of users and user groups includes passwords (empty passwords are not allowed) and that they are identical on every node in the workgroup. For recommended user groups, refer to [How to Restrict the User Interface](#) on page 82.

## Windows User Groups in Domain Controller

Before creating 800xA users and user groups, create a domain that contains all workstations on the 800xA network.

There are two scenarios when creating user groups:

- The account that you are logged onto when running the Configuration Wizard **has permission to add user groups in the domain.** The wizard will create the groups.
- The account that you are logged onto when running the Configuration Wizard **has NO permission to add user groups in the domain.**



In the second scenario, the groups must be set up manually in the domain server before installing the 800xA System. Contact the Windows domain administrator for more information.

### User Groups Setup in the Domain Server

If the installer is not a Windows domain administrator, the IndustrialITAdmin and IndustrialITUser groups must be created manually in the Windows domain before any 800xA software is installed by a Windows domain administrator.

Use the Administrator's Tools to make a folder and install the users in Windows as shown below (to do this you have to be a domain administrator):

1. Select **Start > Control Panel > Administrative Tools > Active Directory Users and Computers**.
2. Select the domain root object. Open the context menu and select **New > Group**, see [Figure 9](#).

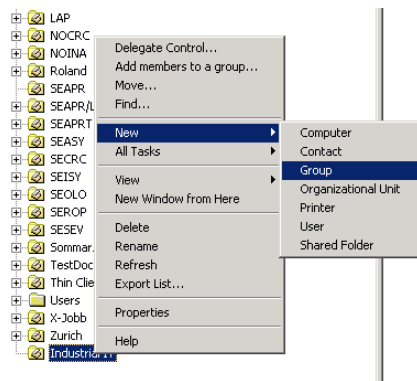


Figure 9. Creation of User Groups

3. A new dialog box opens (see [Figure 10](#)). Input the user group name in this dialog.

Set the Group Scope to Global and Group Type to Security and click on the **OK** button.

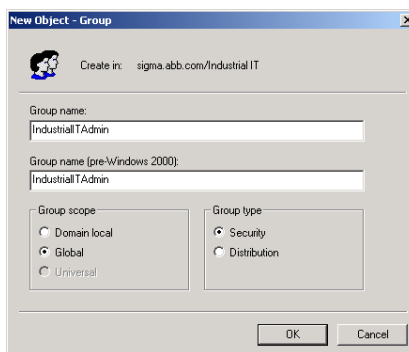


Figure 10. New Object - Group Dialog Box

Now add users to these groups:

- To the IndustrialITAdmin group you must add the persons who have **full access** to the 800xA System. This group always has at least one but no more than a limited number of users.
- To the IndustrialITUser group add **all users** of 800xA.



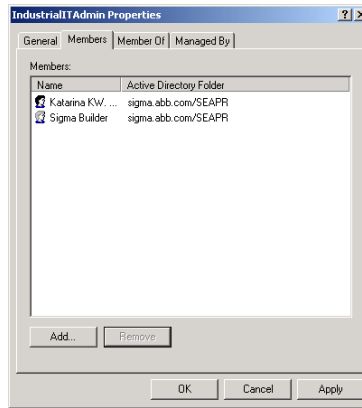
The name of this group can be changed, if required. Additionally, more groups can also be added.

Each group may then be associated with an 800xA group according to information given in the subsection [Associating a Windows Group to an 800xA Group](#) on page 39.

Add users to the groups for the IndustrialITAdmin group as shown below:

1. Select the user group (IndustrialITAdmin in this example).

2. Open the context menu and select **Properties**. A dialog window opens (refer to [Figure 11](#)).



*Figure 11. Including Users in User Groups*

3. Click on the **Add** button and browse to the user you want to add.  
To remove a member, select the user and click on the **Remove** button.
4. Add all users you want to add to the group in a similar way.
5. When all members are added, click **OK**.

### **Associating a Windows Group to an 800xA Group**

To associate a Windows group with an 800xA group follow the description below:

1. Open the User Structure in the Plant Explorer.

2. Select the User Group Definition aspect of a User Group (see [Figure 12](#)).

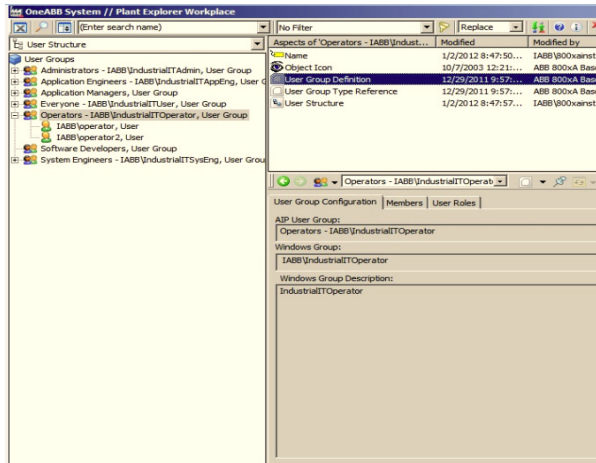


Figure 12. The User Group Definition Aspect of a User Group

3. Select the **User Group Configuration** tab.
4. Click on the **Associate Windows Group** button.
5. A dialog window opens. See [Figure 13](#).

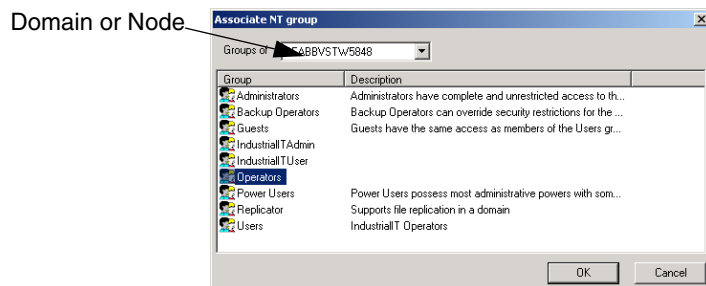


Figure 13. Group Selection

6. Select the local or domain group you want to associate to and click **OK**.
7. The Associate Windows group window closes, and the group is associated.



8. Click **Apply** or **OK** on the User Group Definition aspect view.



The Operators group of your 800xA System has now been associated with the Operators' group in Windows.  
Run a synchronization to make the members of the System and Windows group the same. All users must be members of the Everyone group.

## How to Change User Permissions

### Security Definition Aspect

The Security Definition aspect is used to set security in an 800xA System. By adding these aspects to Aspect Objects and modifying their settings, the security of a system, structure or an object level can be set.



The general principle when configuring 800xA Security is to keep it as simple as possible. A complicated security configuration is, in itself, a security problem, because it will be difficult to maintain and will encourage shortcuts.

For a small installation it may be enough to change the Default Security Definition (an aspect in the 800xA System).

A larger installation may have several operator groups with allowed permissions on different areas in the Functional Structure.

Only exceptionally should a Security Definition be put on individual Aspect Objects.

It is recommended to establish security settings based on groups instead of individual users.



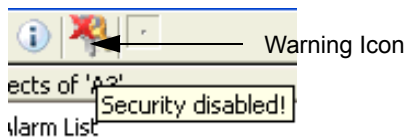
From System Version 5.1 onwards, the default security settings can be configured or modified using the System Configuration Console. Refer to *System 800xA 5.1 Tools (2PAA101888\*)* for more information.

Security settings are customized by adding and setting Security Definition aspects to Aspect Objects. The authority range of the aspect (object, structure or domain) as well as the aspect settings determines the permission.



The owner of the security aspect has permission to edit the security aspect even if the current permission prohibits editing. This prevents changes to the security aspect from becoming irreversible.

If a user belongs to the Administrators group, and thus has full access, a warning icon appears as shown below (in the icon bar of the Plant Explorer and Workplace windows).



To create and configure a Security Definition aspect the user needs Security Configure permission. If the Range is set to or from Structure the user also needs permission to change the structure aspect, normally Configure permission.

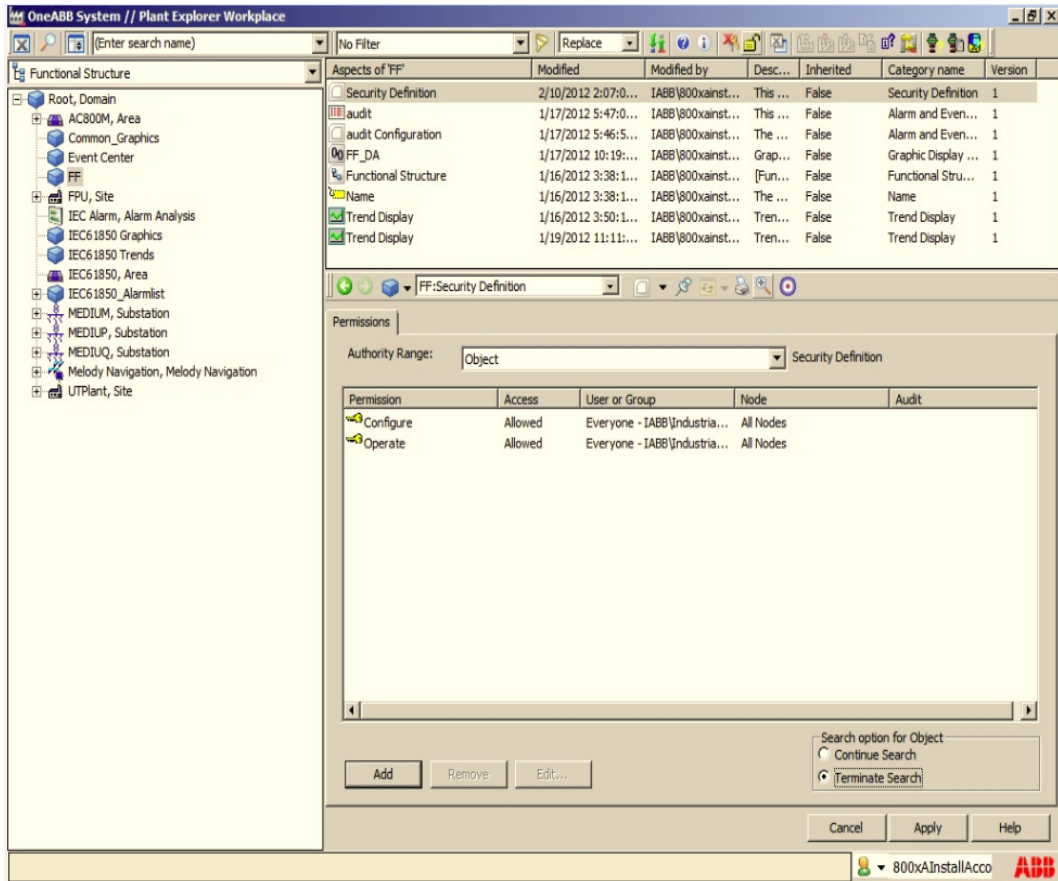


Figure 14. Security Definition Aspect Dialog Box

A Security Definition aspect specifies (see Figure 14):

- The **authority range** for which the aspect is valid
- The required **permission**, the **user identity** or **group**, **node**

- The **search option** order.



An object can have several Security Definition aspects, but with different ranges.

Configure the Security Definition by setting the following:

- **Authority Range**

The range for which the Security Definition aspect is valid, can be set to one of the following values:

- None  
default - means that the Security Definition aspect is disabled.
- Structure (in which the object resides)  
means that the permission set in this Security Definition aspect is valid in the structure on and below the object, to which the aspect is added.
- Object  
means that the permission set in this Security Definition aspect is valid for the Aspect Object, to which the aspect is added.
- Domain (only on system objects)  
can only be found in a Security Definition aspect added to a system object. Means that the permission set is valid for the whole system.



For information regarding Security Definition aspects in environments see *System 800xA Engineering 5.1 Engineering and Production Environments (3BSE045030\*)*.

**Permissions** in the Permission area (see [Figure 14](#)). Define the user **identity** or **group**, **location**, and **permission** granted or denied.

- **Permission**  
See [800xA Permissions](#) on page 52.
- **Type**  
Specify if the Permission is **Allowed** or **Denied**.  
Double-clicking on Allowed/Deny toggles the setting.
- **User or Group**  
The User or User Groups allowed or denied by the permission.

- **Node**  
Choose if the settings are valid for one, more than one, or all nodes.
- **Search Option.** This can be set to:
  - **Continue Search**  
The default setting, **Continue Search**, means that all structures, of which the Aspect Object is a member, are searched according to the evaluation order followed by a search in the system default.
  - **Terminate Search**  
**Terminate Search** means that no other Security Definition is read. This means that all permissions not granted up to the termination of Security Definition are denied.

For information about the evaluation search order, please see [The Evaluation Search Order](#) on page 95.



The search for Permission in a Structure goes from the “bottom” object in the structure and upwards and the search stops as soon as a Security Definition is found that allows or denies a permission for the user.



Double-clicking on a row anywhere but in the Access column opens the Edit dialog.



The domain object must have read permission.  
Do NOT set **Denied** for the Everyone group Read permission entry in the Security Definition aspect on the domain-object (that is the object with the same name as the created system) in the Admin Structure.  
The system must have Read access to a lot of information to be able to at least start the Plant Explorer.

### Default Settings

By default the following permissions are given to the different groups in the system:

*Table 1. Default Settings*

Group	Permission
Everyone	Read, Enter Environment
Operators	Operate, Operator Configure
System Engineers	Shutdown, Security Configure, Administrate, Supervise
Application Engineers	Configure, Tune, Download, Force I/O, Approve, Modify History, First Signature, Second Signature, Create synchronization package, Load synchronization package, Operator Configure.
Application Managers	Configure Engineering Repository, Import from Engineering Repository, Export to Engineering Repository.

### How to Set Permission

To set permission the user must have Security Configure permission.

Set the permission as described below:

1. Add a Security Definition aspect to the Aspect Object being considered.
2. Select this aspect and click on the **Add** button. See [Figure 15](#).

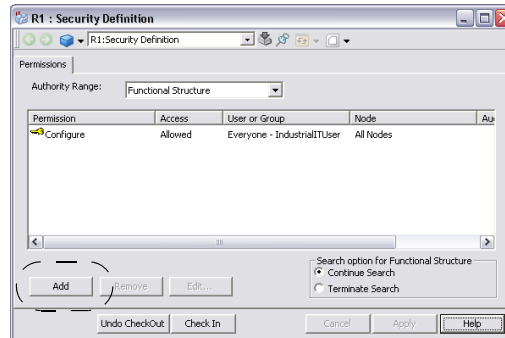


Figure 15. The Security Definition Aspects Dialog Box - Permissions

3. A new dialog window opens, see [Figure 16](#).

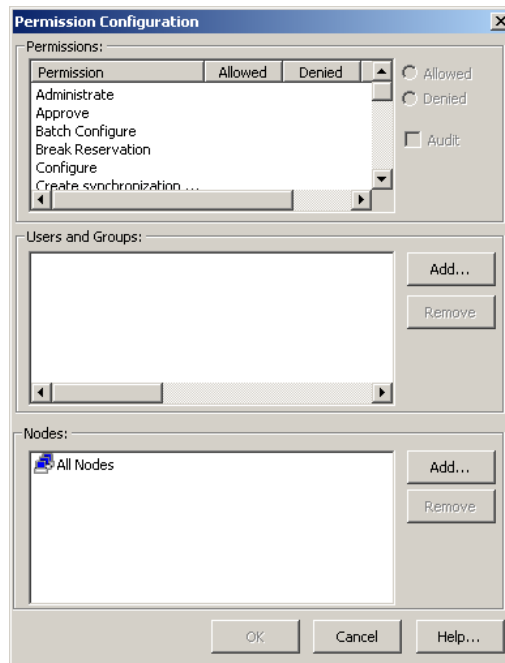


Figure 16. Permission Configuration Dialog Box

4. Select Permission and mark the **Allowed** or **Denied** check box to select the permission for the users and groups located in the window below. You can select several Permissions at the same time by using multiple selections. For information about the **Audit** check box, see [Security Audit Config](#) on page 105.
5. Click on the **Add** button for Users and Groups. A new dialog box opens.

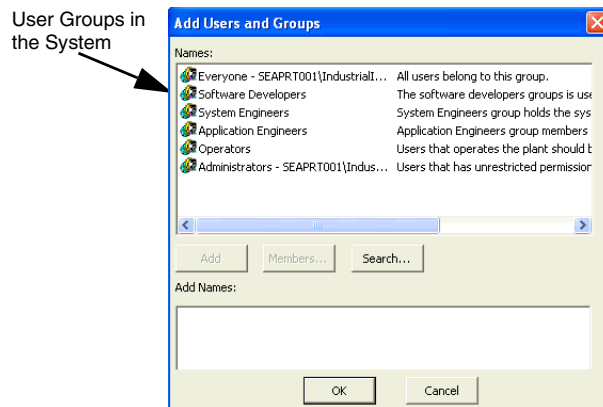


Figure 17. Add Users and Groups Dialog Box

- In this dialog box add groups of users on selected domain(s). Select the group and click **Add** followed by the **OK** button.
- If you want to see all users in a specific group, click on the group and then on the **Members...** button. A new dialog opens with the names of the



members of this group. Select one or more users and click **Add** followed by the **OK** button. See [Figure 18](#).



Figure 18. Group Members Dialog Box

6. When all selections are complete, click on the **Add** button. You can add several Users and Groups of users at the same time.
7. Next, set the nodes from which the permissions are valid.
  - If you want to set it for all nodes, just click on the **OK** button.
  - If you want to set the permission for a specific node (a specific operator workstation), click on the dialog's **Add** button. A new dialog opens.

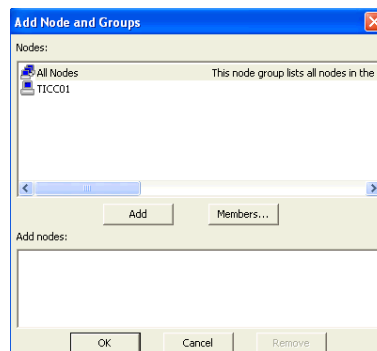
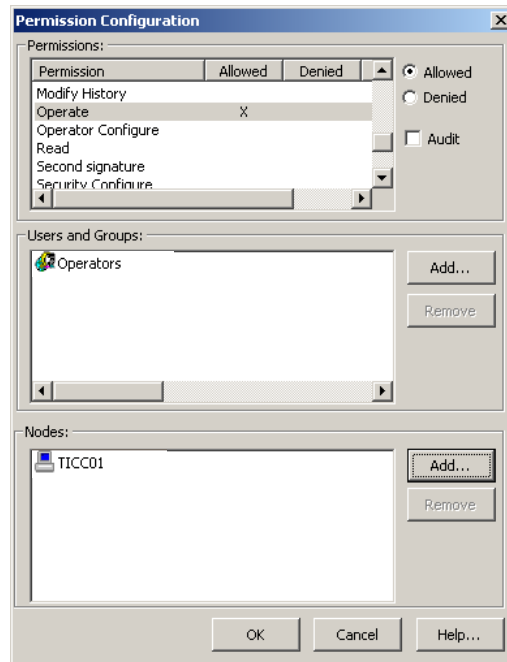


Figure 19. Add Node and Groups of Nodes Dialog Box

8. Select the desired node and click **Add**. Click on the **OK** button. The dialog now looks like what is shown in [Figure 20](#).



*Figure 20. Configuration Dialog Box*

9. Click on the **OK** button. The permission is now allowed. “Deny” is done in the same way.
10. Re-authentication is required to apply permission changes if Advanced Access Control is activated.

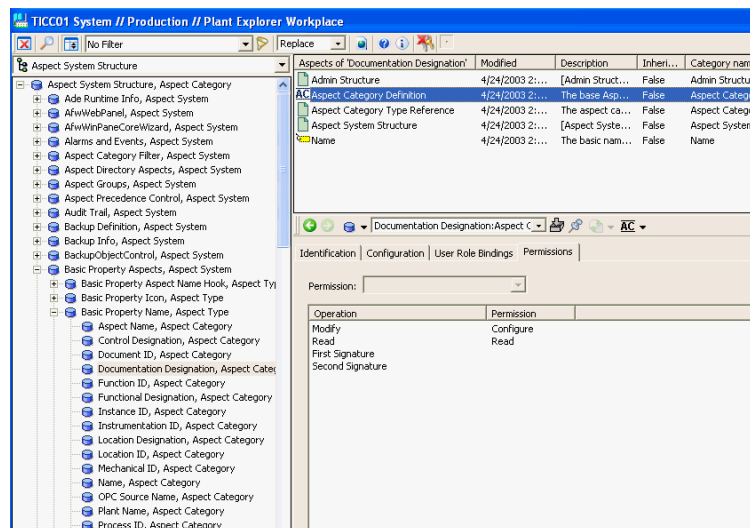
In the example above the selections made have resulted in security configuration where Operate permission is allowed for the group Operators for the node TICC01. This means that user members of the Operators’ group can operate the Functional Structure (to which the Security Definition aspect is added) from the equipment with node name TICC01.

## 800xA Permissions

The required permission is set per Aspect Category and OPC property.

The required permission for Read and Modify operations are displayed for that category. In the example in [Figure 21](#) notice that for the selected Aspect Category Read permission is required to read and Configure permission to modify.

If the required permissions for read or modify operations on an Aspect Category are not defined, then they are interpreted as read permission for read operation and configure permission for modify operation respectively.



*Figure 21. Required Permission*

The security setting in 800xA is controlled by the Security Definition aspect. Add an Security Definition aspect to the Aspect Object to set the wanted security. The security for an Aspect Object may be defined by one or more Security Definition aspects.

Avoid too many and too fine-grained security definition aspects, because mistakes based on misunderstanding of complex interdependencies may jeopardize the aim of security. Usage of Security Definition aspects should be carefully planned before implementation.

A user or group is allowed or denied access to an object based on the Granted Permission compared to the Required Permission:

- **Required** permission  
Required permission is given per Aspect Category, and defines the permission necessary to perform an operation like Read or Modify of aspects in the category.  
The required permission for Read and Write operations on Aspect Object Properties is set per property. If no permission is set the default permission is used. The default permission is Read for read operations and Operate for write operations.
- **Granted** permission  
Defines the permission for a user or group on the complete system, on a structure or on an object.

**Predefined User Permissions.** The 800xA System contains the following predefined permissions:

- **Administrate**  
Permits a user to do administration of the Aspect Object System itself, for example add new 800xA users.
- **Approve**  
Allows approval of a double authentication.
- **Batch Configure**  
Permits a user to configure a batch operation.
- **Break Reservation**  
Allows a user to break a reservation.
- **Configure**  
Permits a user to configure an aspect.
- **Create synchronization package**  
Permission to create a synchronization package.
- **Download**  
Allows download to a controller or other equipment.

- **Enter Environment**  
Permits a user to enter an environment.
- **First signature**  
Permission to make the first digital signature for an aspect.
- **Force I/O**  
Allows a user to force the value of an I/O.
- **Force SFC**  
Allows an operator to force SFC states.
- **Modify Alarm Hiding**  
Permission to modify alarm hiding configuration.
- **Modify History**  
Allows modification of version history.
- **Operate**  
This is the default permission for OPC write operation. Permits a user to operate the system. Normally given to the Operator Group.
- **Operator Configure**  
Allows an operator to do some configuration work.
- **Read**  
This is the default permission for read operation. Permits a user to read information.
- **Refresh**  
Refresh permission allows a user to make a refresh on an engineering environment.
- **Second signature**  
Permission to make the second digital signature for an aspect.
- **Security Configure**  
Permits a user to change/add permission on Aspect Objects.
- **Shutdown**  
Permits a user to shutdown an area. Not used in the default setting.
- **Supervise**  
Permits a user to supervise the process.

- **Tune**  
Permits a user to tune a process.



There may be additional permissions depending on installed system extensions.



Device Management PROFIBUS/HART system extension brings in additional permissions to work with Device Type Managers (DTMs). For more information, refer to *System 800xA Device Management PROFIBUS and HART Configuration (3BDD011934\*)*.

### Modification of 800xA Permissions for Process Objects

In order to modify permissions for process objects you can change the default required user permissions or set your own user permissions. This can be done on an object type level or on the object instance level. In both cases you must use the Property Attribute Override Aspect.



The Property Override Aspect only works on AC 800M or AC 800M High Integrity object types.

The Property Attribute Override is an aspect that allows you to override existing property permissions and authentication flags on both object types and objects, inside libraries. The Property Attribute Override aspect can be placed on an Aspect Object Type (Function Block Type, Control Module Type); thus affecting all Objects of that type.

It can also be placed on a single Aspect Object (Function block, Control Module); thus only affecting that particular object.

User defined permissions make it possible to raise the granularity of the security setting for special operations.

### Change of Process Object Type/Object Instance Required Permission

Figure 22 shows a released library (ValveLib) that contains an object type (ValveTemplate).

Its property permissions are presented in the Control Module aspect (aspect preview pane).

In order to change the property settings for variable (A) (see Figure 22) you need to create a Property Override aspect and set the new properties for (A).

In the example given in Figure 22 the write permission on property (A) is changed from *Tune* to *Administrate* and the Authenticate level is changed from *None* to *Reauthenticate*. For information about authentication see [Critical Operation Authentication Support](#) on page 113.

Then, these two aspects will merge together, with the new override settings for (A), but the original settings for (B) is still intact. The new override permissions will be inherited by all objects of that type.

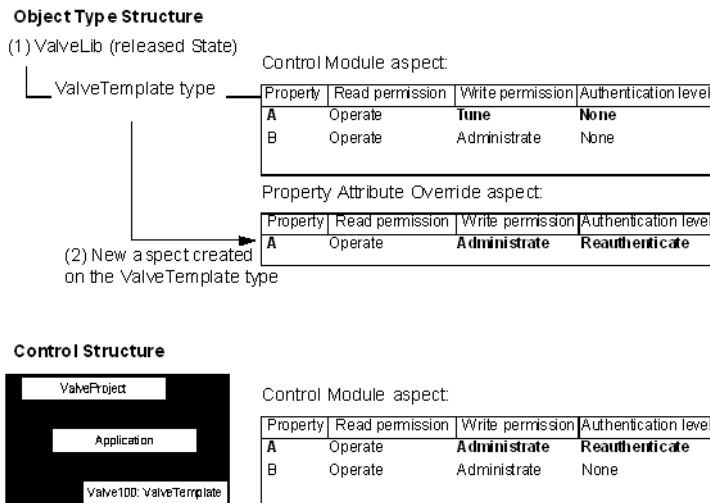


Figure 22. Property Override Attribute on Object Types

To create a Property Attribute Override aspect follow the steps below:

1. Ensure you are in the Object Type Structure and browse to the released library.
2. Right-click the type and select **New Aspect**.
3. Check **Show all** and scroll down to **Property Attribute Override**.
4. Click **Create**. A Property Attribute Override aspect will be created in the aspect pane.

You can also override property permission settings for objects. Figure 22 showed how the type ValveTemplate had the property (A) changed from None to Reauthenticate, by adding a Property Attribute Override aspect. Valve 100 received the new override setting, but so will also the next object, Valve 101, and the next etc. (they all have the same object type), see Figure 23.

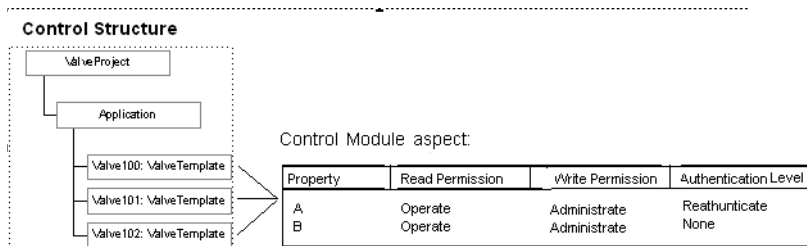


Figure 23. Property Override Aspect on Objects



The property permission settings configured in the Property Attribute Override aspect in the Plant Explorer will be lost when the corresponding variable is renamed in Control Builder. The system does not give any warning or notification that the settings are lost. No workaround exists. It is recommend to configure these settings late in a commissioning phase when the need for renaming variables is over

Suppose you need to apply an additional override setting for Valve102, for example, you want to change property (A) from Reauthenticate to Double authenticate:

1. Select Valve102 in the Control Structure and create an additional Property Attribute Override aspect for Valve102.
2. Select Double authenticate. The new aspect setting (Double authenticate) for Valve 102 will override the previous setting (Reauthenticate).



The other two objects, Valve100 and Valve101, will still have the old property authentication Reauthenticate.

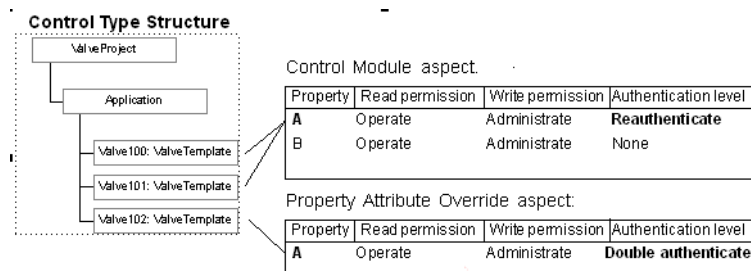


Figure 24. Property Override (A) in Valve102

In this example, Valve102 is the only object that has Double Authenticate for variable (A), but the same inherited permissions (B) as the other two valves.

### How to Add Your Own Permissions

In a plant all operators have permission for operating all valves. Some of those valves are used for emergency shutdown. Operating the emergency shutdown valves requires specific education which only a few operators have. These operators should have their own permission to operate the emergency shutdown valves. How is this accomplished? Add a new permission 'Emergency Shutdown', follow the steps below.

1. Go to the Admin Structure and expand the Inventory Object.

2. Expand the Permission object. All default Permissions are listed below. See [Figure 25](#).

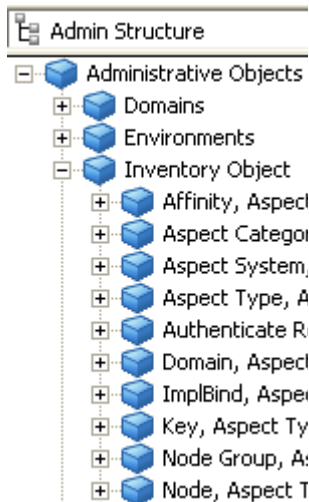


Figure 25. Permission Object

3. Right-click on the Permission object and select **New Object** from the context menu.
4. Select the Permission object of type Permission according to [Figure 26](#), and give it the name of the permission to add.

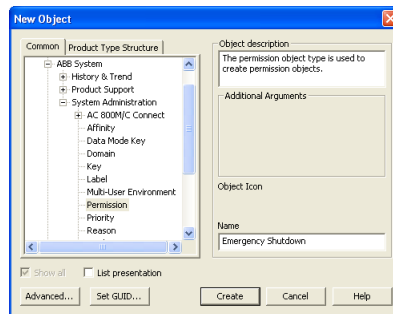


Figure 26. New Object - Permission

5. Click **Create**.
6. Select the Name aspect in the aspect list.
7. Type a description in the **Description** field, see [Figure 27](#).

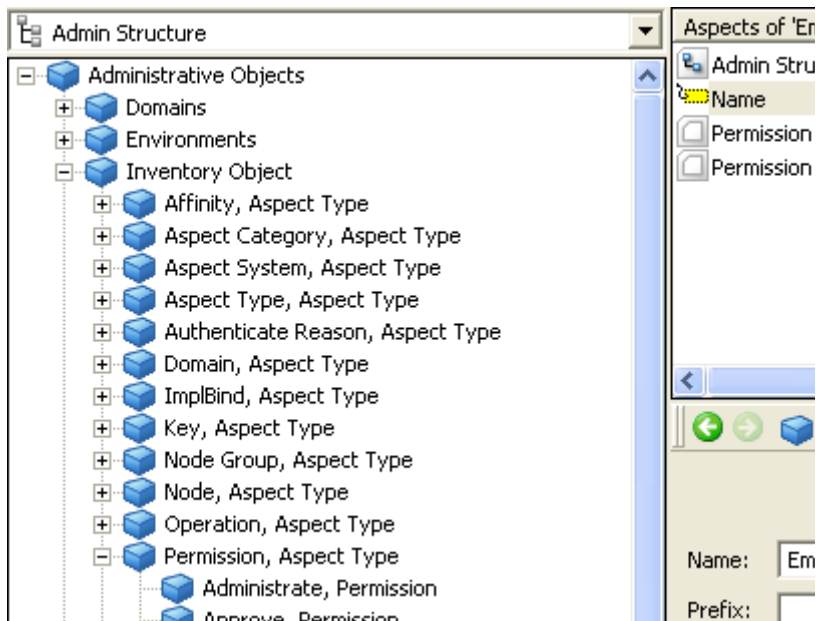


Figure 27. Name Aspect of Emergency Shutdown Object

8. Click **Apply**.

- Define in the Security Definition aspect for the system, if there are additional user groups that should have the given permission Emergency Shutdown in order to operate these valves.

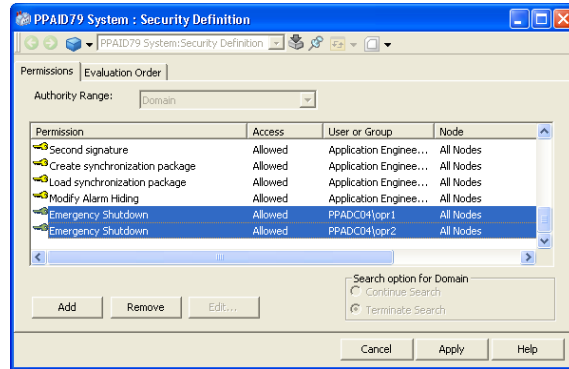


Figure 28. Emergency Shutdown Permission for Selected Operators

- Add a Property Attribute Override Aspect to the valve instances (object instances) which are used for emergency shutdown.
- Change the required permission Operate (for the operation Write) to the newly created permission Emergency Shutdown.



The new permission (Emergency Shutdown) must be exported together with the object that has been given the Property Attribute Override aspect.

### Modification of 800xA Permissions for Aspect Categories

If, for example, there are two groups of operators, normal operators and advanced operators, the normal operators have the permission to operate and the advanced operators have the permission to tune. You want to give the advanced operators possibility to configure a trend display.

Then there are two alternatives:

#### Alternative 1

Set the given permission for the Trend Display Aspect Category in the Aspect System Structure to Tune, see [Figure 29](#). Ensure that normal operators have the

permission to operate and the advanced operators have the permission to operate and to tune.

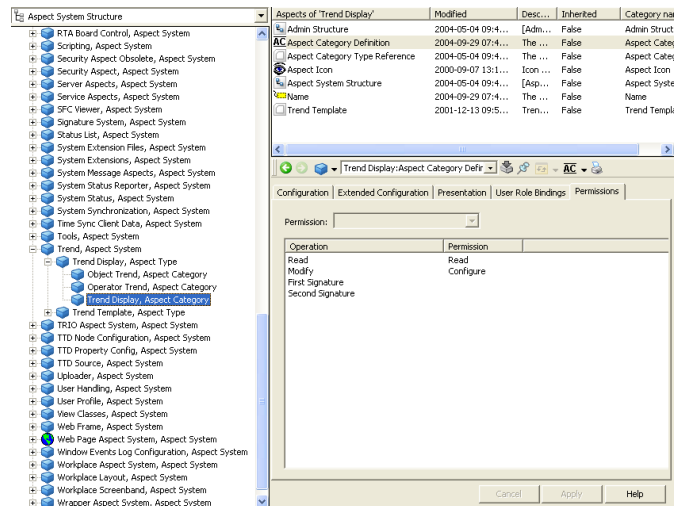


Figure 29. Aspect System Structure - Trend Display Aspect Category

### Alternative 2

1. Create your own permission 'TrendConfig'. See [How to Add Your Own Permissions](#) on page 57.
2. Give the permission to the advanced operator group. See [How to Set Permission](#) on page 46.
3. Change the required permission Configure (for the operation Modify) to the newly created permission TrendConfig for the Trend Display Aspect Category in the Aspect System Structure, see [Figure 29](#).
4. Define in the Security Definition aspect for the system, which user groups that should have the permission TrendConfig. If this is not done the consequence will be that the user group application engineer (who has the permission

Configure) can not modify a trend display. Set the given permission TrendConfig for the application engineer group.



Aspect Categories permission cannot be changed on an Aspect Instance level it can only be changed on an Aspect Category level.

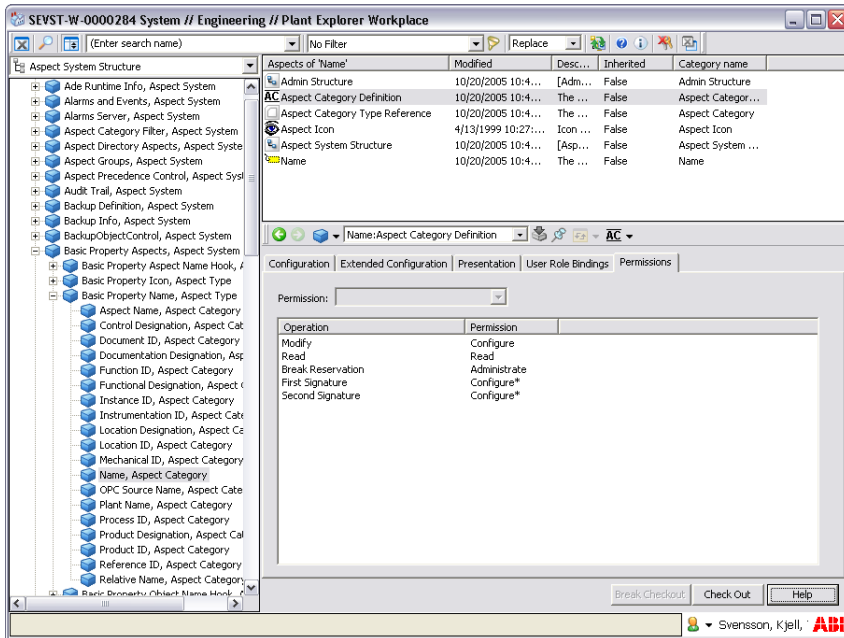


Figure 30. Configure Required Permission

### Windows Restrictions for Operators

Windows Group Policy can be used to restrict users from accessing other Windows applications. National authorities can, for example, demand such limitations.

The Group Policy described here also simplifies the startup of an Operator Workplace. The workplace is directly up and running as an Operator Workplace without any manual work by the operator.

Follow the steps below to set up a secure Operator Workplace:

1. On the Domain Controller:  
Select **Start > Control Panel > Administrative Tools > Active Directory Users and Computers**.
2. Create an Operators organizational unit, on the domain root object.  
Open the context menu and select **New > Organizational Unit**, refer to [Figure 31](#).

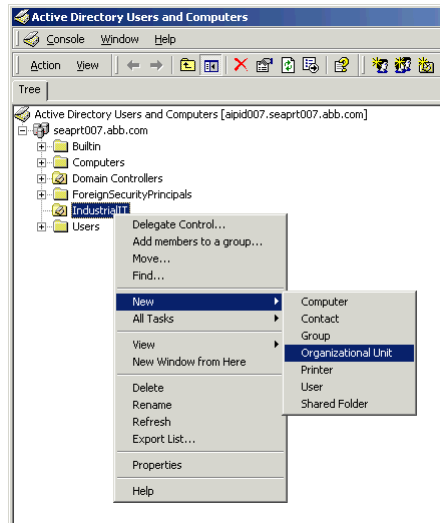


Figure 31. Creation of Organizational Units

3. Move the automatically created user groups to the Operators organizational unit. See [Figure 32](#).

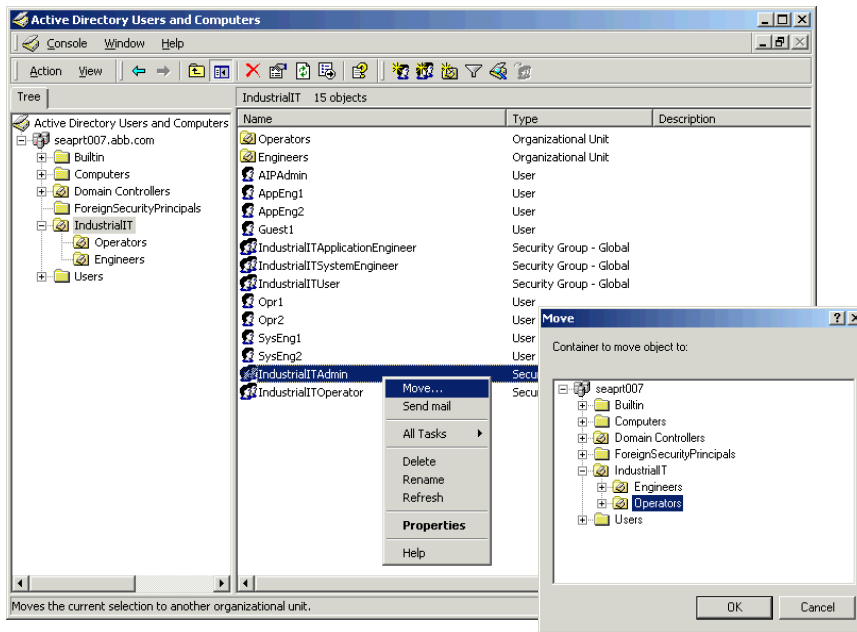


Figure 32. Move User Groups

4. Create the user Operator in the corresponding organizational unit:
  - a. Select the organizational unit **Operators** and open the context menu.
  - b. Select **New > User**.
  - c. Give the user the name **Operator**, click **Next**.
  - d. Type the password and confirmation of password in the next dialog box, click **Next**.
  - e. Confirm the user creation by clicking **Finish**.
5. Make the user Operator member of the Users group:



- a. Select **Operator** and open the context menu. Select **Add members to a group...**, see [Figure 33](#).

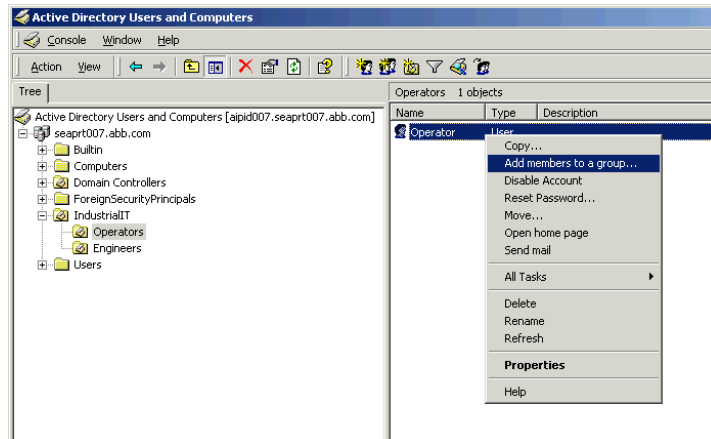


Figure 33. Add Member to Group

- b. Select the **Users** group, see [Figure 34](#).

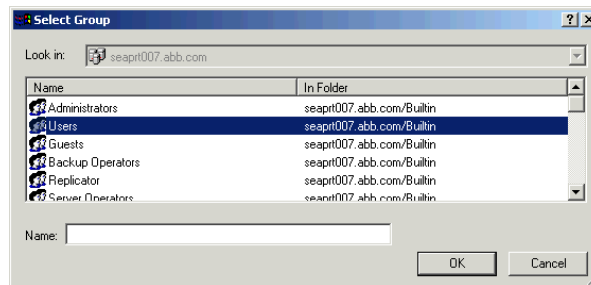
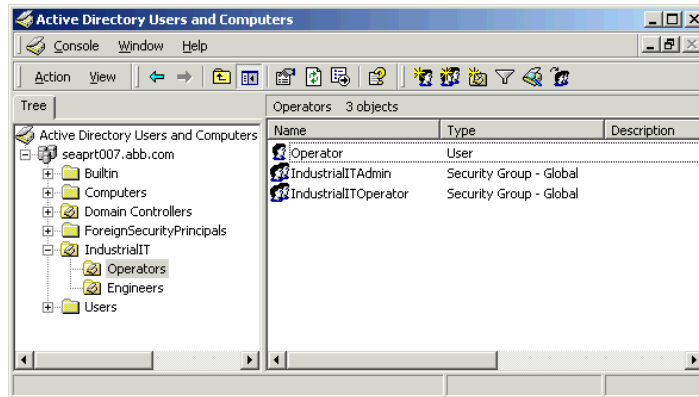


Figure 34. Select Group

6. The result of the settings made above are displayed in [Figure 35](#).



*Figure 35. Operators Organizational Unit*

7. Add the user Operator to the 800xA System and to the IndustrialITOperator group:
- Open the **Configuration Wizard** and select **System Administration**.



From System Version 5.1, a simplified procedure of adding users to the group using the System Configuration Console can be used.

- Select **Users**.
- In the User Configuration dialog box click the **Add Windows Accounts...** button.

- d. Select **Domain** in the **Show members of** drop-down menu and select the user **Operator** in the list. See [Figure 36](#).

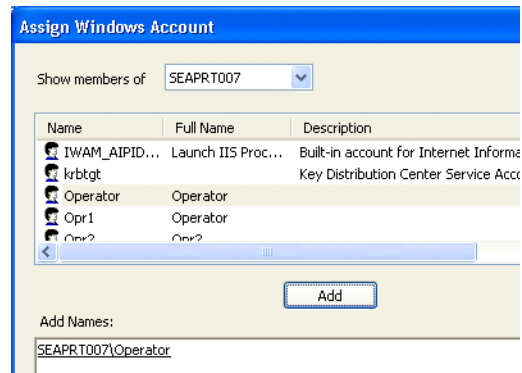


Figure 36. Assign Windows Account Dialog Box

- e. Click **Add** and then **OK**.
8. Log on as the new user Operator on a client and configure desktop:
    - a. Add a Shortcut to **Operator Workplace** through **Start > All Programs > ABB Industrial IT 800xA > System > Workplace**, see [Figure 37](#).

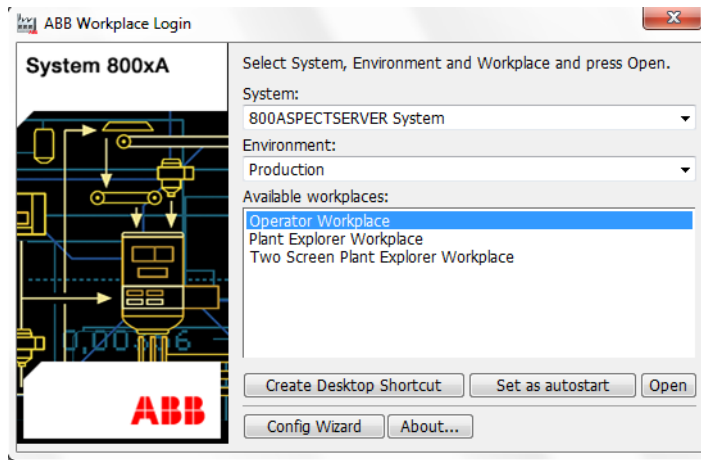


Figure 37. Adding Shortcut to Operator Workplace

9. Create a Group Policy by the name GeneralLockedOut:
  - a. Open **Group Policy Management** through **Start > Control Panel > Administrative Tools > Group Policy Management**.
  - b. Select the organizational unit **Operators** on the Domain Controller.
  - c. Open the context menu and select **Create a GPO in this domain, and link it here...**

- d. Give the new group policy a name, e.g. 'GeneralLockedOut'. See [Figure 38](#).

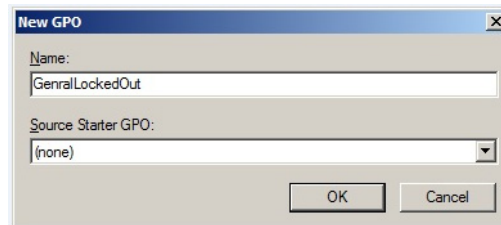


Figure 38. Group Policy Tab

10. Configure the User Configuration:
  - a. Click the **Edit** button under the Group Policy tab.
  - b. A new dialog box will appear. Expand the GeneralLockedOut structure according to [Figure 39](#).

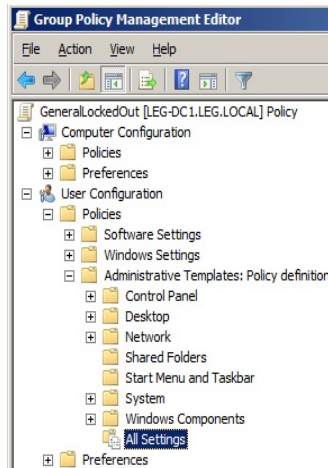


Figure 39. Group Policy Dialog Box

- c. Make the policy settings according to the tables below. You configure the settings by double clicking on the first policy in the right pane for each folder. A new dialog will appear in which you can choose **Not Configured**, **Enabled** or **Disabled**.

For the Windows Explorer folder, configure the Policies according to [Table 2](#).

*Table 2. Windows Explorer*

Policy	Setting
Turn on/Enable Classic Shell	Disabled
Removes the Folder Options menu item from the Tools menu	Enabled
Remove File menu from the Windows Explorer	Enabled
Remove "Map Network Drive" and "Disconnect Network Drive"	Enabled
Remove Search button from Windows Explorer	Enabled
Remove/Disable Windows Explorer's default context menu	Enabled
Hides the Manage item on the Windows Explorer context menu	Enabled
Only allow approved Shell extensions	Not configured
Do not track Shell shortcuts during roaming	Enabled
Hide these specified drives in My Computer	Enabled
Prevent access to drives from My Computer	Enabled
Remove/Hide Hardware tab	Enabled
Disable UI to change menu animation setting	Enabled
Disable UI to change keyboard navigation indicator setting	Enabled
Disable DFS tab	Enabled
No "Computer Near Me" in My Network Places	Enabled
No "Entire Network" in My Network Places	Enabled
Maximum number of recent documents	Not configured

Table 2. Windows Explorer (Continued)

<b>Policy</b>	<b>Setting</b>
Do not request alternate credentials	Not configured
Request credentials for network installations	Not configured

For the Start Menu & Taskbar folder, configure the Policies according to [Table 3](#).

Table 3. Start Menu &amp; Taskbar

<b>Policy</b>	<b>Setting</b>
Remove user's folders from the Start Menu	Enabled
Disable and remove links to Windows Update	Enabled
Remove common program groups from Start Menu	Enabled
Remove My Documents icon from Start Menu	Enabled
Remove Documents from Start Menu	Enabled
Disable programs on Settings menu	Enabled
Remove Network & Dial-up Connections from Start Menu	Enabled
Remove Favorites menu from Start Menu	Enabled
Remove Search menu from Start Menu	Enabled
Remove Help menu from Start Menu	Enabled
Remove Run menu from Start Menu	Enabled
Add Logoff to the Start Menu	Not configured
Disable Logoff on the Start Menu	Not configured
Disable and remove the Shut Down command	Enabled
Disable drag-and-drop context menus on the Start menu	Enabled
Disable changes to Taskbar and Start Menu Settings	Enabled
Disable context menus for the taskbar	Enabled

Table 3. Start Menu &amp; Taskbar (Continued)

<b>Policy</b>	<b>Setting</b>
Do not keep history of recently opened documents	Enabled
Clear history of recently opened documents on exit	Not configured
Disable personalized menus	Enabled
Disable user tracking	Enabled
Add "Run in Separate Memory Space" check box to Run dialog box	Not configured
Do not use the search-based method when resolving shell shortcuts	Not configured
Do not use the tracking-based method when resolving shell shortcuts	Not configured
Gray unavailable Windows Installer programs Start Menu shortcuts	Not configured

For the Desktop folder, configure the Policies according to [Table 4](#).

Table 4. Desktop

<b>Policy</b>	<b>Setting</b>
Hide all icons on desktop	Enabled
Remove My Documents icon from desktop	Not configured
Remove My Documents icon from Start Menu	Not configured
Remove Properties from the My Documents context menu	Not configured
Remove Properties from the My Computer context menu	Not configured
Hide My Network Places icon on desktop	Not configured
Hide Internet Explorer icon on desktop	Not configured
Do not add shares of recently opened documents to My Network Places	Not configured



Table 4. Desktop (Continued)

<b>Policy</b>	<b>Setting</b>
Prohibit user from changing My Documents path	Not configured
Disable adding, dragging, dropping, and closing the Taskbar's toolbars	Enabled
Disable adjusting desktop toolbars	Enabled
Don't save settings at exit	Enabled

For the Control Panel folder, configure the Policies according to [Table 5](#).

Table 5. Control Panel

<b>Policy</b>	<b>Setting</b>
Disable Control Panel	Enabled
Hide specified control panel applets	Not configured
Show only specified control panel applets	Not configured

For the System folder, configure the Policies according to [Table 6](#).

Table 6. System

<b>Policy</b>	<b>Setting</b>
Don't display welcome screen at logon	Enabled
Century interpretation for Year 2000	Not configured
Code signing for device drivers	Not configured
Custom user interface	Not configured
Disable the command prompt	Enabled
Disable registry editing tools	Enabled
Run only allowed Windows applications	Not configured

Table 6. System (Continued)

Policy	Setting
Don't run specified Windows applications	Not configured
Disable Autoplay	Enabled
Download missing COM components	Enabled
Restrict these programs from being launched from Help	Enabled

Table 7. Log On/Log Off

Policy	Setting
Disable Task Manager	Enabled
Disable Lock Computer	Enabled

11. Configure the Operator Workplace:
  - a. Log on as Administrator on a client and go to the User Structure in the Plant Explorer.
  - b. Expand the Operators group, and select the user Operator.
  - c. Select the Workplace Profile Values aspect in the aspect list.
  - d. For the **Default Workplace** mark the **Local** radio button and a default workplace setting in the **ObjectName** field, refer to [Figure 40](#).

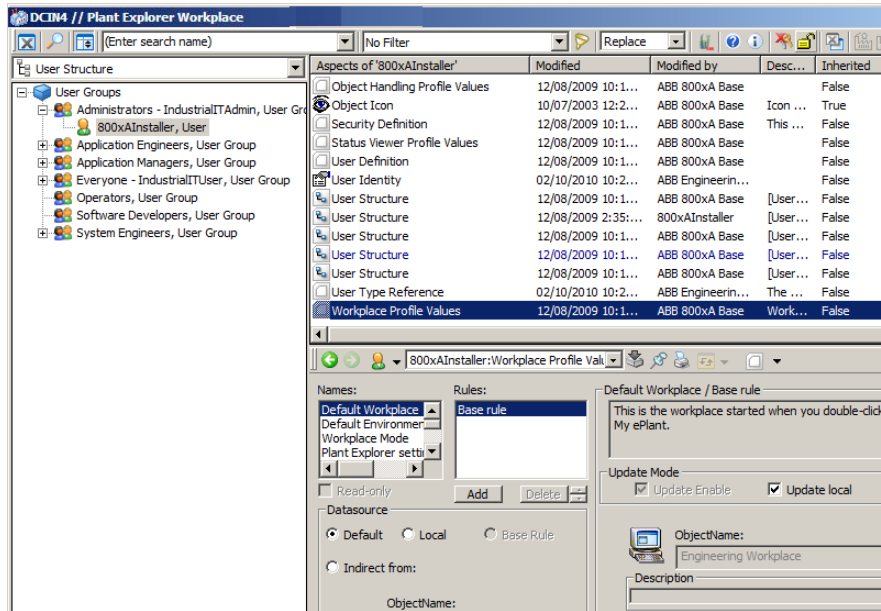


Figure 40. Default Workplace

e. Click **Apply**.

- f. For the **WorkplaceMode** mark the **Local** radio button and select **Operator Workplace Mode** in the **Workplace Mode** field, see [Figure 41](#). Click **Apply**.

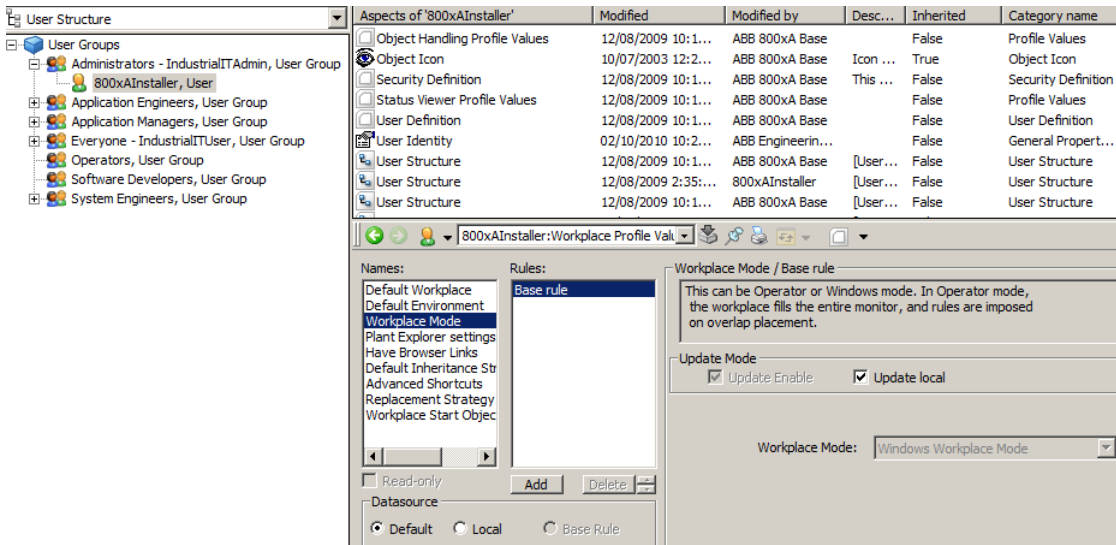


Figure 41. Workplace Mode

- g. For the **WorkplaceStartObject** mark the **Local** radio button and select a default object name in the **ObjectName** field, see [Figure 42](#). Click **Apply**.

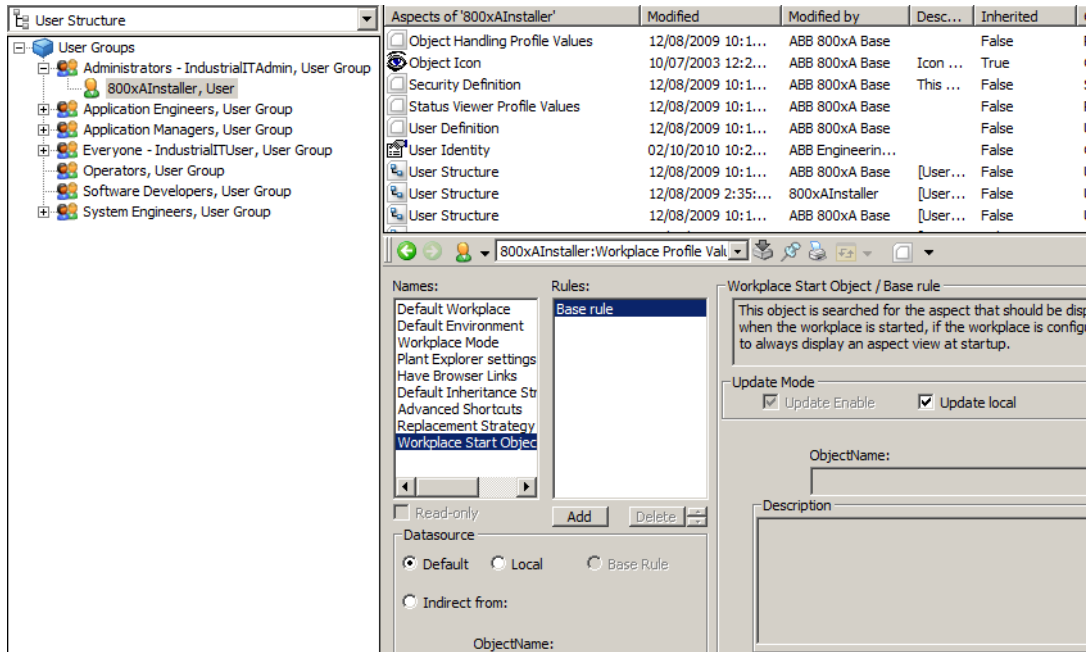


Figure 42. Workplace Start Object

12. Log on as Operator on the client and test the settings you have made.

### Configuring Access on Domain Servers

When using the Domain Controller (DC) node as a combination of Aspect server, Connectivity server, and Operator station client, the 800xA system users may be required to login to these node(s). This is prevented on a DC node in the Windows 2008 server. In this case, set a group policy security setting *Allow log on locally* for the 800xA system users.

When the *Allow log on locally* policy is edited, it will override the default policy settings defined by the *Default Domain Controllers* policy. The groups that are listed in the default policy must always be added to this new policy to allow any configured user to be able to log in to the DC node.



It is not recommended to change the default policy setting as it will lower the overall security of the 800xA System and can be potentially risky. It is the responsibility of the user of the 800xA System to assess the risks and the consequences before changing the *Default Domain Controllers* policy settings.

**User Rights Assignment.** Execute the following steps to configure the security settings for user rights:

1. Select **Group Policy Management** from **Control Panel > System and Security > Administrative Tools**.
2. Right-click **Group Policy Objects in Domains**.
3. Select **New** from the context menu to add a new Group Policy Object.

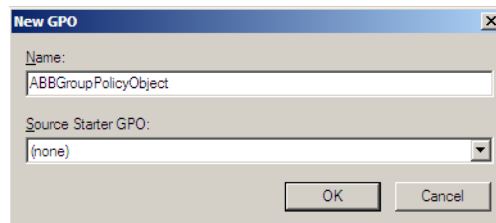


Figure 43. New Group Policy Object

4. Enter a name for the Group Policy Object, in this case, **ABGroupPolicyObject** and click **OK**.
5. Select the **Domain Controllers** organization unit (folder) in the **Group Policy Management** console and select **Link an Existing GPO** (refer to [Figure 44](#)).

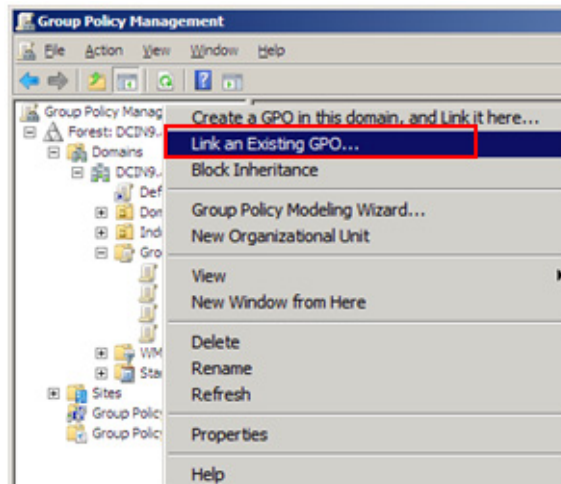


Figure 44. Linking an Existing GPO

6. Select the **ABBGroupPolicyObject** from the **Select GPO** dialog box and click **OK**.
7. Modify the order of group policies linked to the **Domain Controllers** organization unit.



A list of linked policies is displayed in the right pane where the order can be changed. Use the **Up** arrow button to move the **ABBGroupPolicyObject** above the *Default Domain Controller* policies to effectively override the default policies.

8. In the **Group Policy Management Editor** dialog, right-click **Computer Configuration** and select **Edit** from the context menu.
9. Navigate to **User Rights Assignment** in **Computer Configuration > Policies > Windows Settings > Security Settings**.
10. Right-click **Allow log on locally** and select **Properties** from the context menu.

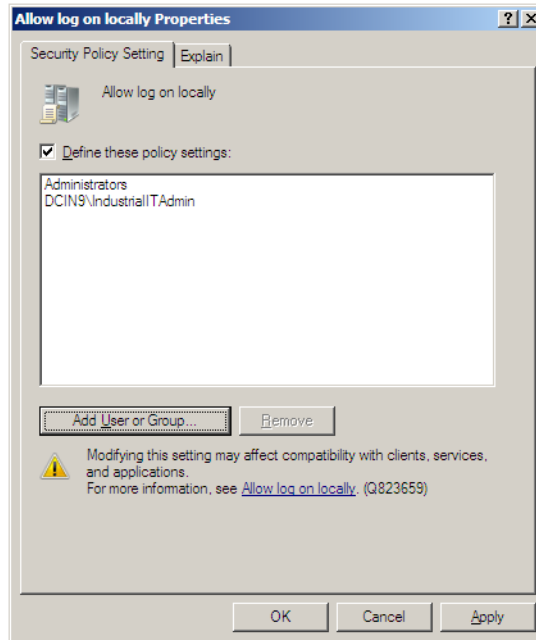


Figure 45. Setting the Allow log on locally Properties

11. In the *Allow log on locally* policy list for **ABBGroupPolicyObject**, add:
  - Administrators (mandatory)
  - Account Operators, Backup Operators, Print Operators, Server Operators (not mandatory but this avoids removing rights after overriding the default policy)
  - Required group of users, for example, IndustrialITAdmin (allows only 800xA admin users to log on) or IndustrialITUsers (allows any 800xA users to log on).
12. Select the **Define these policy settings** check box.
13. Click **Apply** and then click **OK** to save the changes.



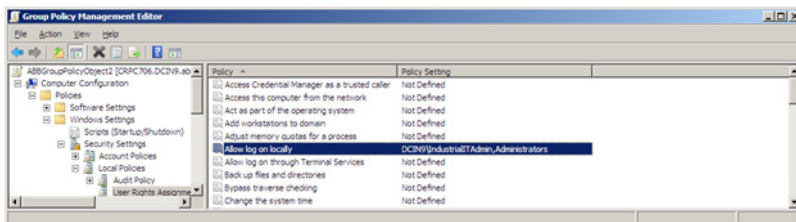


Figure 46. Group Policy Management Editor after setting the User Rights Assignment

Figure 47 shows the **Group Policy Management** dialog with the security settings done for the newly created group policy object.

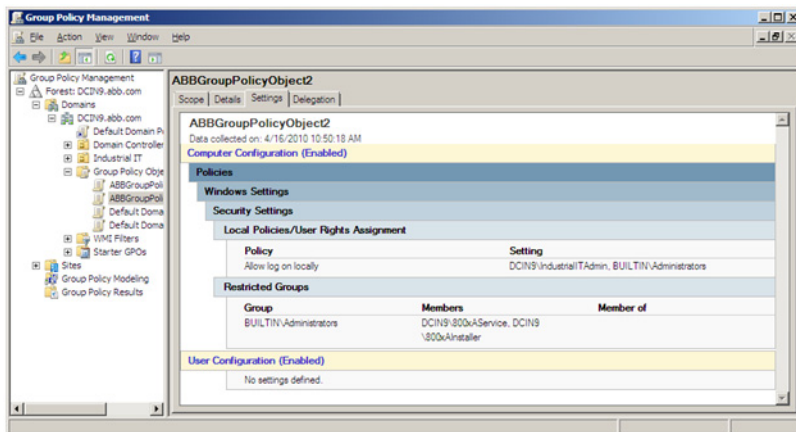


Figure 47. Group Policy Object with the Security Settings



This change may take several minutes before becoming effective. To force this change to immediately take effect, reboot the DC node or use the command `gpupdate /force` in an Administrator Command Prompt.

## Authentication problem in 800xA Workplace

Function in Windows to map a disc drive to remote node with a different user compared to the user logged in will cause authentication problem in System 800xA.



Never check the “Remember my password” check box as in [Figure 48](#).



Figure 48. Connect dialog in disc mapping

## How to Restrict the User Interface

User roles help to customize the environment to suit the needs of each user. This means that the operations which the user needs to take act on are visible for him/her. The user **role** is used to adapt the user interface to work typical for 800xA groups. For example configuration dialogs are removed from users with an **Operator Role**.

The user roles are associated with the 800xA groups. By adding a Windows user to an 800xA group he/she is assigned a role.

The following User Roles exist:

- Operator Role - must be held by all operators in a plant. The role makes it possible to use process control dialogs, acknowledge alarms etc.

- Safety Operator Role - must be held by an operator in a plant, that are trusted to perform safety related operations. The role makes it possible to modify data that is protected with write confirmation in the AC800M H1 Controller.
- Application Engineer Role - allows a user to do engineering operations and work with objects and applications built for objects (programs, graphics etc.)
- System Engineer Role - must be held by a user that works with service, node or user administration.
- Application Manager Role - must be held by a user that should work with the Engineering Repository.

The default security configuration (permission and roles) is provided with the assumption that different users typically do different tasks. The assumption is that users with the role **Operator** control the process, but do not tune or configure. The role **Application Engineer** tunes the process and makes all application configurations. Finally the role **System Engineer** handles the physical configuration like server configurations, adding users, and setting up security.

The figure below is an example of what the three different user roles can see in a context menu for the same object.

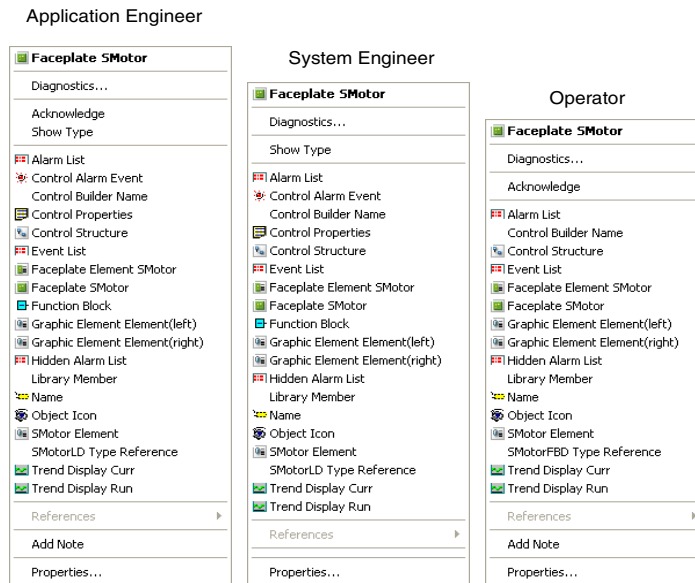


Figure 49. Example of Context Menus for the three different User Roles

It is possible to have an Operator that is allowed to make application configuration changes by giving the Operator the additional role of Application Engineer and the permissions associated for the Application Engineer group. Another alternative is to change the granted permission for that individual directly.



Note that an Application Engineer does not have an Operator Role by default. This means that there are tasks an Operator can perform, that an Application Engineer can not.

It is recommended to add the System Engineer to the Application Engineer group. It is also recommended to add the Application Engineer to the Operator group.

## User Role Default Settings

In the User Structure the User Groups and the Users must be defined. For each User Group there is a User Group Definition.

The Role a user has is set per User Group and defines what User Interfaces the users will have. By assigning a user different roles, you give him/her a means to interact with more or less of the system's values, settings etc.

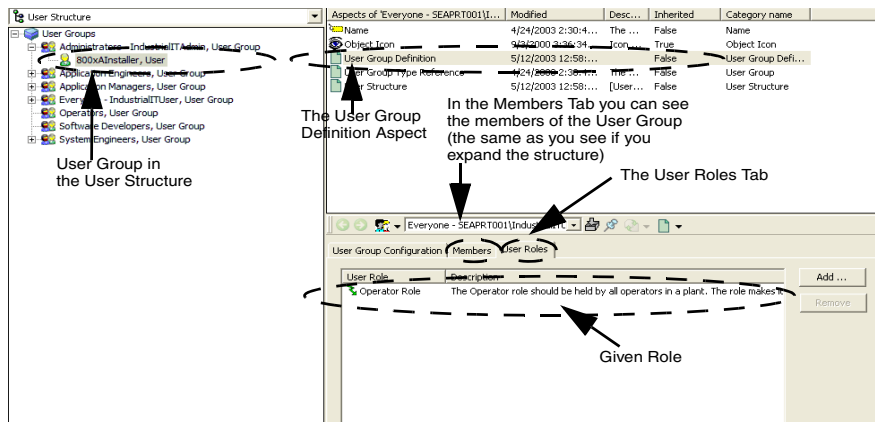


Figure 50. The User Group Definition Aspect

**Occupying a role**, like Operator, System Engineer, **does not mean** that the 800xA user unconditionally **has permission to perform a task**.



Permissions have nothing to do with the role of the user. Permissions are defined by the Security Definition aspects and Windows user identity only.

For default permission settings see [800xA Permissions](#) on page 51.

There are five predefined user groups in the 800xA System:

- **Everyone**  
A group that contains all the 800xA users.
- **Administrators**  
A group with the security system disabled, that is, a member of this group have full access to everything in the aspect system.

- **Operators**  
A group of all Operators. Performs process operations.
- **Application Engineers**  
A group of all application engineers. Performs application engineering.
- **Application Managers**  
A group of all application managers. A member of this group configures and works with the Engineering Repository.
- **System Engineers**  
A group for all system engineers. Performs system engineering.

The role(s) for a group, or a user, is set under the tab **Roles** in the User Structure.



It simplifies the user handling if all groups above are associated with the corresponding Windows groups.



You can add/delete User Groups according to the information in the [Adding Users](#) on page 30.



During configuration, commissioning and operation, avoid using a user's identity who is also a member of the Administrators group. All members of the Administrators group are running the system with the security system disabled.

**Guest.** If you access 800xA and are not a member of the Everyone group you **will have no role**. You are a Guest in 800xA and have a very limited access to information. However, you need to be a member of the Windows group IndustrialITUser to be able to start a workplace.



The default security configuration allows a guest to only read aspects. By default no guest account is created.

To add a Guest account follow the steps below:

1. Select **Start > All Programs > ABB Industrial IT 800xA > System > Configuration Wizard > System Administration > Users**.

- Click the **Add Guest** button. See [Figure 51](#).

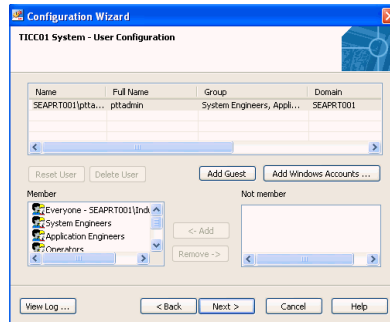


Figure 51. Add Guest

- Click **Next**.
- Click **Finish** in the Apply Settings dialog box.
- The Guest account is now created, see [Figure 52](#).

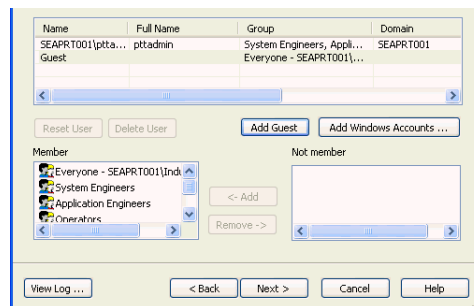


Figure 52. Guest Account

### User Role Configuration

The Aspect Category Definition aspect for an aspect Category object in the Aspect System Structure contains a **Role** tab used to configure the **Role** required for an operation.

This definition may be changed to meet you requirements.



Do not change the **Role** definitions before you are very familiar with 800xA and its security model.

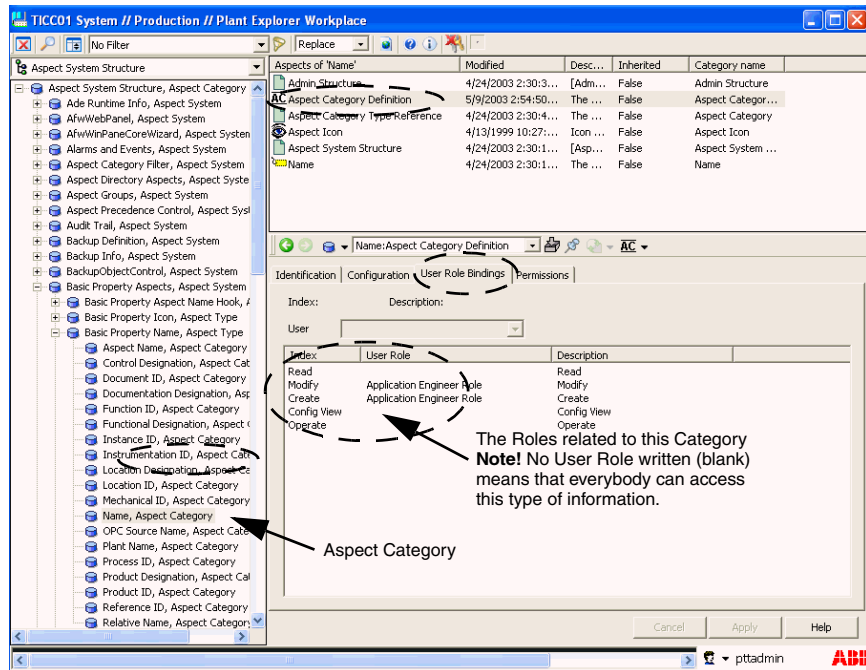


Figure 53. The Role Definition Tab of an Aspect Category

The selected user role controls the required **Role** for the different operations. If, for example, an **Application Engineer** role is necessary to read the category, a user with an **Operator** Role will not even see that the category exists.

How do I see...

**A Security Report?**

In the system you will find a Security Report aspect. You can use this aspect to get a printed report showing the security settings of the system and to compare a new



security report with an old one so that you can see changes in the security settings of the system.



From System Version 5.1 onwards, it is possible to create and view a Security Report using the System Configuration Console. Refer to *System 800xA 5.1 Tools (2PAA101888\*)* for more information.

To add a Security Report aspect follow the step below:

1. Add a Security Report to any object in any structure by opening the context menu in the aspect list and select **New Aspect**. Select a Security Report aspect in the list and click **Create**. See [Figure 54](#).

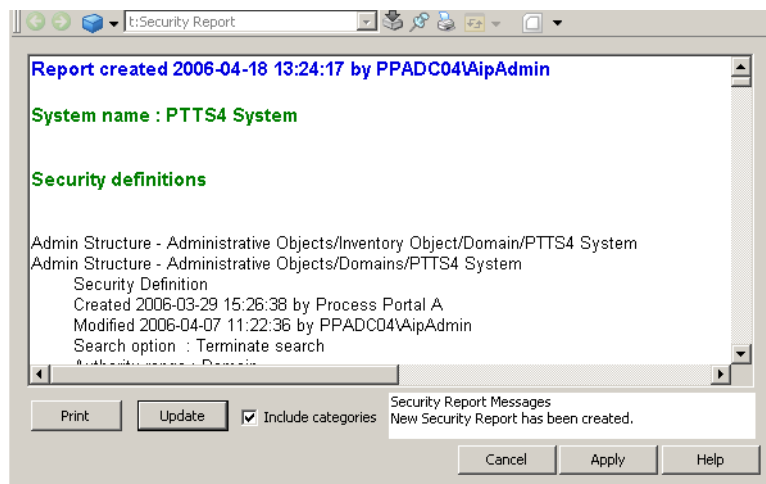


Figure 54. Security Report Aspect

If you press the **Update** button you get an updated security report, in which you can see if any changes in the security settings for the system has been made since the last security report was made.

If you click the **Print** button you get the security report printed.

By checking the **Include categories** check box information about required permission, required role, required authentication and required signature for the different Aspect Categories is displayed.

### What can you see in the Security Report?

- **System Security**  
In the first section you can see the security settings for the complete system.
- **Groups and Users**  
In the second section you can see the different user groups and the users in each group. See [Figure 55](#)

#### Groups and users

```

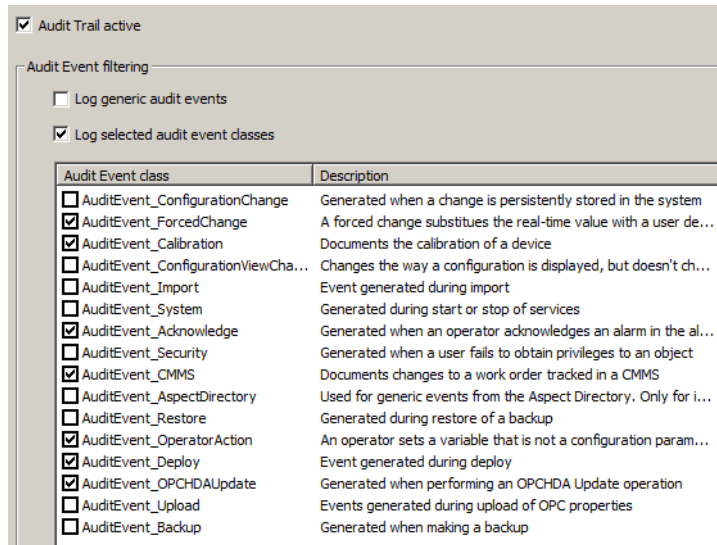
Everyone - SEAPRT002\IndustrialITUser
  SEAPRT002\AppEng1      App Eng 1
  SEAPRT002\SysEng2      Sys Eng 2
  SEAPRT002\Opr2         Operator 2
  SEAPRT002\SysEng1      Sys Eng 1
  SEAPRT002\aipadmin     AIPAdmin
  SEAPRT002\Opr1         Operator 1
Software Developers
System Engineers - SEAPRT002\IndustrialITSystemEngineer
  SEAPRT002\SysEng2      Sys Eng 2
  SEAPRT002\SysEng1      Sys Eng 1
  SEAPRT002\aipadmin     AIPAdmin
Application Engineers - SEAPRT002\IndustrialITApplicationEngineer
  SEAPRT002\AppEng1      App Eng 1
  SEAPRT002\SysEng1      Sys Eng 1
  SEAPRT002\aipadmin     AIPAdmin
Operators - SEAPRT002\IndustrialITOperator
  SEAPRT002\Opr2         Operator 2
  SEAPRT002\Opr1         Operator 1
Administrators - SEAPRT002\IndustrialITAdmin
  SEAPRT002\aipadmin     AIPAdmin

```

Figure 55. Groups and User

- **Audit Configuration**

In the third section you can see the audit configuration of the system. See [Figure 56](#).



*Figure 56. Audit Configuration*

For information about Audit Events refer to [Audit Trail Configuration](#) on page 102.

### **My granted permission for an object?**

To see your granted permission for an object, go to the object in the Plant Explorer and select it. Open the context menu for the object and select **Details**.

Select the **Permission** tab and you can see what is allowed and denied to you, refer to [Figure 57](#).

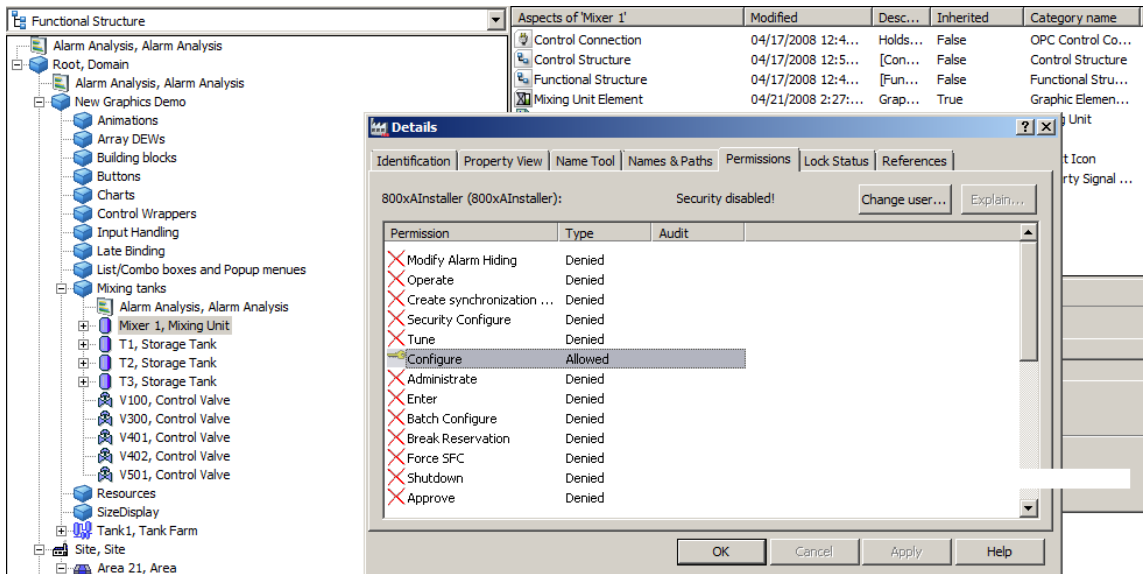


Figure 57. Aspect/Context/Properties/Permission

### My granted permission for an aspect?

You see the permission in the same way as you see it for an object. The **Permission** tab shows the operations that require a permission. It also shows whether the permission is granted.

### Granted permission for another user?



You need to have the permission Security Configure to use this method.

When making the security configuration in a system it might be convenient to see how the security for an object is set for a specific person or group. You can easily do this in the following way:

1. Select the object in Plant Explorer.

2. Open the context menu and select **Details**.
3. A dialog window opens, see [Figure 58](#). Select the **Permissions** tab.

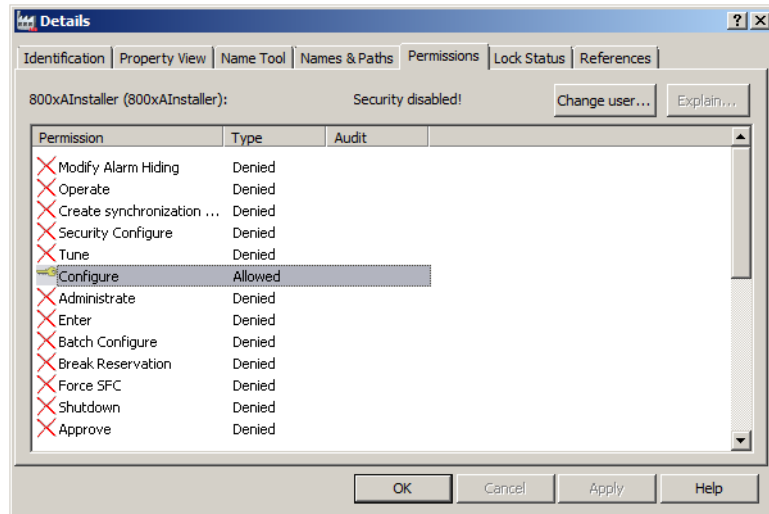


Figure 58. Object Properties Dialog Box - Permissions Tab

4. Click on the **Change User...** button.

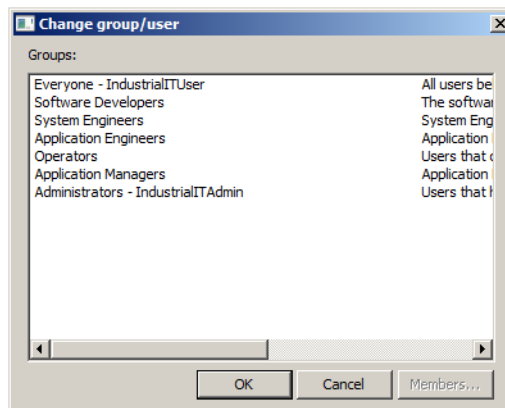


Figure 59. Select User

5. Select a user in the same way you do as when you want to configure the Security.

### **Explain Dialog**

You can click the Explain button and a dialog window appears, describing how the security rules are propagated to the object at the selected level. The permission is shown as a red cross in the functional structure. The security setting will show up by clicking on the marked node.

## **Advanced Security Configuration**

### **The Access Evaluation Algorithm**

Several Security Definition aspects can define the security for the same Aspect Object. When an access is validated, the security aspects are evaluated in a certain order until the access is granted or denied.

The evaluation order is as follows:

- Within a Security Definition aspect entries for a specific node are evaluated before entries for all nodes. “Deny” entries are evaluated before “Allow” entries.
- A Security Definition aspect that has only the object as its range is evaluated before the security aspects associated with structure aspects.
- Security Definition aspects associated with structures are evaluated in a configured order. This order is configured globally for the system so that the security for one structure always has precedence over one another.
- If the access is neither granted nor denied by any of the security aspects that directly control the authority for the object, the Security Definition aspect that sets the default for the user created system is evaluated.
- If no Security Definition aspect allows or denies a permission, the permission is denied.

The evaluation order of structures and which structures to be searched are configured in the Security Definition aspect that sets the system default security.

When you access an Aspect Object in a structure, the system searches for a Security Definition aspect added to the object. If it does not find the aspect, the system goes “upwards” to the parent structures in the evaluation order and looks for this aspect. It does so until it finds a Security Permission aspect which is valid.



If a user is a member of **two** groups, one of which is granted permission and one which is denied permission, **the result will always be denied, since “deny” entries are evaluated before “allow” entries.**

When a Security Definition aspect is found, the system analyzes its information:

- Which person or group of persons is allowed to do which action (Permission, Type, User of Group and Node)?
- What range is set (Authority Range/Environmental Range)?
- What node(s) can access the object(s)?
- Must the search go on or not (Search Option for...)?

Based on this information the granted permission is set.

## The Evaluation Search Order

When an object is accessed, and the **Search Order** is set to **Continue Search** the system goes into every structure where the object is present. The search will go on according to the order in the **Evaluation Search Order** list.

From top to bottom. When a Security Definition is found that gives security information about the user, the search stops. For example, if a member of the Operator group is accessing an Aspect Object, and this object has a Security Definition aspect with a Permission for Operators, this Permission is valid.

If no valid security setting is found in the structures in the Evaluation Search Order list, the system goes on to the Default Settings in the System Object in the Admin Structure.

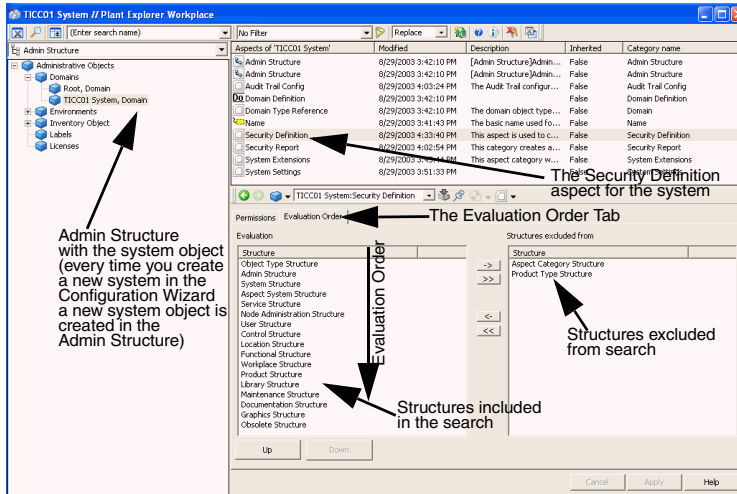


Figure 60. Evaluation Order List in the Admin Structure

Initially, the Evaluation Order List has a default setting as shown in Figure 60. You may easily change this to meet your demands by selecting the structure you want to move and then click on the left/right arrow.

If you click on the double arrow to the left, all structures are moved to the left Evaluation Order window, and the system will go through all structures when setting the security.



If you click on the double arrow to the right, you get a question dialog as shown in [Figure 61](#), warning you that all Security Definitions with Structure Range will be disabled.

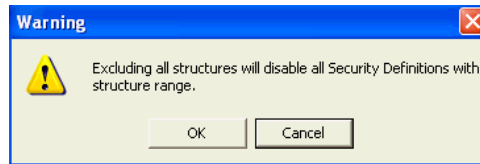


Figure 61. Excluding All Structures Warning

For example, if there is a structure in the Location Structure and the Functional Structure according to [Figure 62](#) and [Figure 63](#), the object **Object “A”** (occurring in both structures) will have the permission to operate denied to the group Operators, despite the fact that the **Security Definition** on the object itself says that **Operate** is **Allowed**.

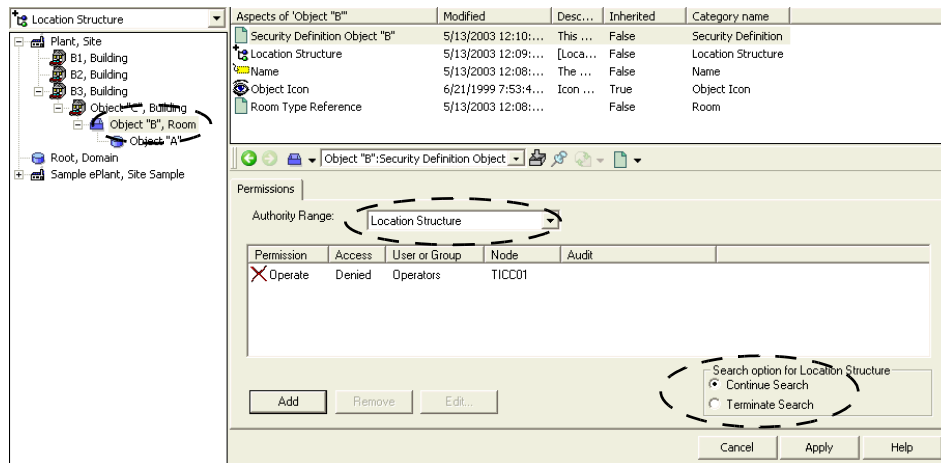


Figure 62. Security Setting for the Location Structure and its Aspect Objects

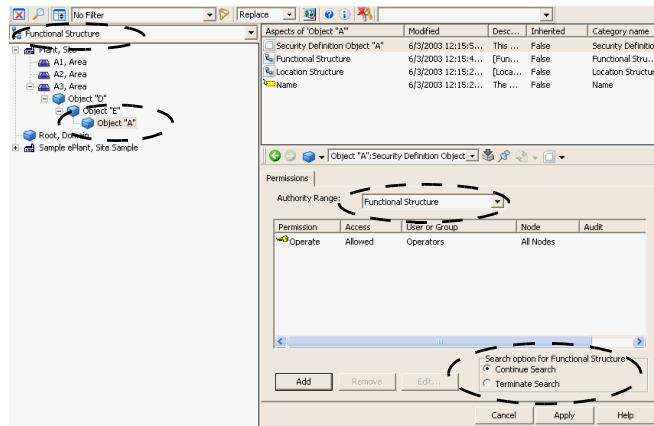


Figure 63. Security Setting for the Functional Structure and its Aspect Objects

The reason for this is; When you access Object “A”, the system looks on the added Security Definition aspect. It finds that the Search Option is Structure. This means that the evaluation order for structures should be used.

Next the system looks for what Structure aspects are added to the Aspect Object, in order to evaluate which structure must be examined first. The system finds two structure aspects: the Location Structure aspect and the Functional Structure aspect.

According to the Evaluation Order list (see [The Evaluation Search Order](#) on page 99) the Location Structure should be examined first.

The Object “A” has no Security Definition aspect valid for the Location Structure, and therefore the search goes on to the object’s parent in the Location Structure - Object “B”. This object has a Security Definition aspect with a Location Structure setting. This aspect has the permission denied to the group Operators.

A Security Definition aspect for the group Operators that has a valid permission is found.

The Security Definition aspect added to Object “B” in the Location Structure is set to Location Structure, and therefore the setting in it is also valid for Object “A”. For this reason the permission Operate on Object “A” is denied to the group Operators.

The result is that the settings for **Operation** on object **Object “A”** is denied to Operators, despite the fact that the Security Definition on the object itself says that it is allowed.

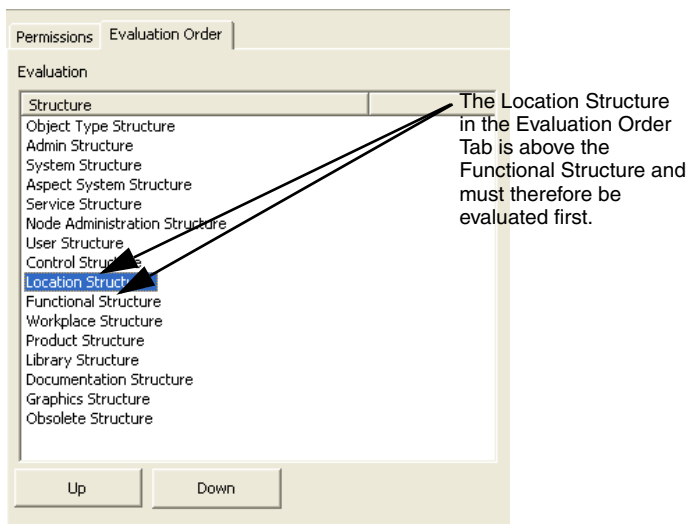


Figure 64. Evaluation Order

Always take the above information into account when checking the security of an object.

The easiest way to see the permissions of an object is to select its properties in the context menu and look in the **Permission** tab.

### Access Example for Object with Structure Authority Setting

This is an example of how the system searches for the security setting when accessing an object. The text is related to [Figure 65](#).

Suppose that object T33 is accessed in the Functional Structure. The system goes to the Security Definition aspect and indicates that the Authority Range is the Functional Structure.



The **object** authority- and environmental **range setting** to a **structure** in the Security Definition aspect gives the system the information that it has to go and look in all Security Definition settings for **the object in all structures** according to the Evaluation Order.

The next step is for the system to analyze the Structure aspects to find out in which structures the object resides. It finds one Functional and one Location structure aspect. (Arrow #I in [Figure 65](#).)

The next step is to analyze the Evaluation order. In this example the system will find that the Location Structure shall be evaluated before the Functional Structure. (Arrow #II.)

The system queries the Location Structure and looks for a Security Definition. If no valid Security Definition is found in the Location Structure for this particular user, the search will be repeated in the Functional Structure. (Arrow #III and #IV.)



The ranking order between the structures must be considered. If a user accesses an object in the Functional Structure, its Security Definition settings for the Location Structure can be valid for the accessing user.

If for example you have a Security Definition aspect on the Aspect Object for the Objects Functional Structure and one for the Aspect Objects Location Structure, the system will first go through the Aspect Object **parent** in the Location Structure looking for valid Security Definition settings for the user.

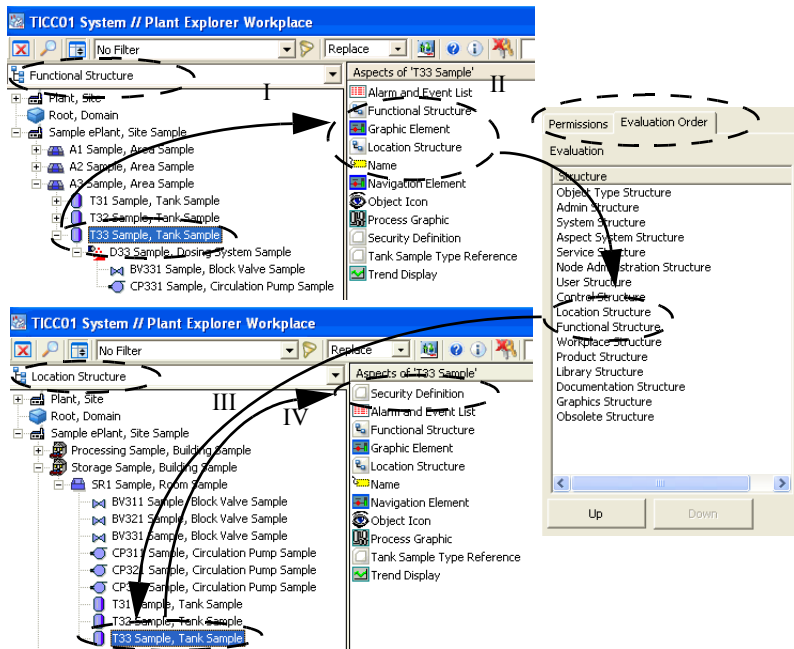


Figure 65. The Security Search Order when Accessing a Security Definition Aspect with Authority Range Setting for the Functional Structure.

## Audit Logging

The Security and Access Control System allows audit of operator actions and security.

The audit logs can be viewed in the alarm and event list. This makes it possible to see the effect of an operation. The audit log contains the following information:

- Date and time for the operation.
- Node from which the operation was performed.
- User name of the individual performing the operation.
- Type of operation.
- Object, property or aspect affected by the operation.



- Additional information from the involved aspect system..  
Audit Logging is not possible if using the Service Account.

## Audit Trail Configuration

The Audit trail function is controlled with the Audit Trail Configuration aspect that allows filtering of the audit event categories to suit the desired audit requirements in the system. The Audit Trail Configuration controls the audit settings for the entire system. Filtering is not possible on object level.

There can only be one Audit Trail Configuration aspect in a system. It is placed in the Admin Structure. You must have the Security Configure permission to be able to configure the settings for the Audit Trail Configuration aspect.

To configure the Audit Trail Configuration aspect follow the steps below:

1. Open the Admin Structure in the Plant Explorer and expand Administrative Objects.
2. Expand Domains and select the object with the name of the system. By default this is <server node name>System.
3. Double-click on the Audit Trail Config aspect to open the configuration view. See [Figure 66](#).
4. Mark the **Audit Trail active** check box and the **Audit Event filtering** area will become active.
5. If you select the **Log generic audit events** check box all the audit events which are predefined in the system without details will be logged.  
If you select the **Log selected audit event classes** check box, you will be allowed to choose which audit event message classes to exclude.

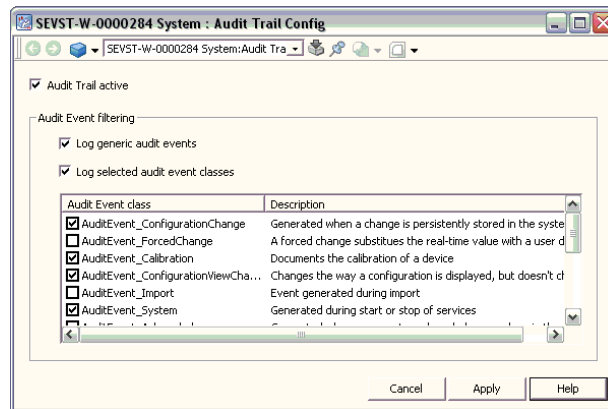


Figure 66. Audit Trail Configuration Dialog Box

The following message classes can be used for the audit trail:

- **AuditEvent\_ConfigurationChange** - Generated when a change is persistently stored in the system.
- **AuditEvent\_ForcedChange** - A forced change substitutes the real-time value with a user defined value that is subsequently used instead of the actual change.
- **AuditEvent\_Calibration** - Generated for different calibration events.
- **AuditEvent\_ConfigurationViewChange** - Changes the way a configuration is displayed, but does not change the process.
- **AuditEvent\_Import** - Event generated when import/export start and stop.
- **AuditEvent\_System** - Generated during start or stop of services.
- **AuditEvent\_Acknowledge** - Generated when an operator acknowledges an alarm in the alarm list.
- **AuditEvent\_Security** - Generated when a user is allowed/denied access to an object.
- **AuditEvent\_CMMS** - Document changes to a work order tracked in a Computerized Maintenance Management System.

- **AuditEvent\_AspectDirectory** - Used for generic events from the Aspect Directory. Only for internal system use.
- **AuditEvent\_Restore** - Generated during a restore of a backup.
- **AuditEvent\_OperatorAction** - Generated when an Operator changes a process value. The event contains the FromValue, the value before the change, and the ToValue, the changed value.
- **AuditEvent\_Upload** - Events generated during upload of OPC properties.



The FromValue is read immediately before the value is changed and can therefore be different from the value that the Operator sees when the change is made.



It is possible to disable audit for single object properties. See *System 800xA 5.1 Configuration (3BDS011222\*)* for more information.

- **AuditEvent\_Backup** - Generated when making a backup.



There may be additional classes depending on the system extensions installed.

- **AuditEvent\_Deploy** - Events generated during deploy.
  - **AuditEvent\_OPCHDAUpdate** - Generated when performing an OPCHDA Update operation.
  - **AuditEvent\_AC800MStatusMonitoring** - Generated when performing an upload operation for AC 800M Status Monitoring.
6. Click **Apply**.
  7. Re-authentication is required to apply changes in the Audit Trail Configuration if Advanced Access Control is activated.



You can override the description on the OPC property name by modifying the Control Connection Aspect. This is done on either object- or instance level. This is accomplished by selecting the property to modify in the Property Info Tab within the Control Connection Aspect and then enter a new value in the Description field. This value is shown in the description column in the Audit Trail log instead of the standard text if logging has been activated. Please note that this not is valid for AC 800M, since AC 800M do not use the Control Connection Aspect.



## Security Audit Config



From System Version 5.1 onwards, Audit can also be configured using the **System Configuration Console**. Refer to *System 800xA 5.1 Tools (2PAA101888\*)* for more information.

The procedure to audit the Security Definition aspect with the audit function is described below:

1. Click on the Security Definition aspects **Permissions** tab.
2. Click on the **Add** button, see [Figure 67](#).

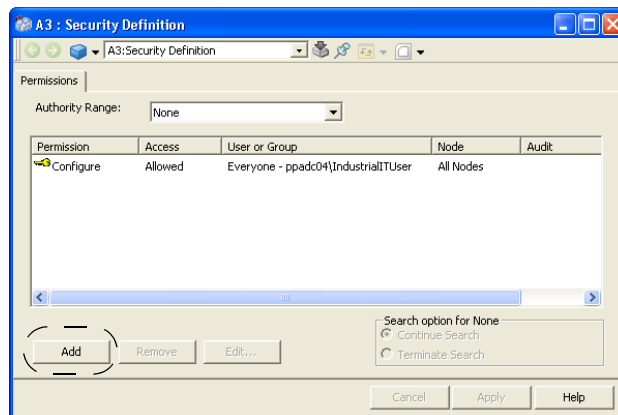


Figure 67. Security Definition Aspect Configuration View

3. Mark the **Audit** check box to set audit for the different permissions settings. See [Figure 68](#).

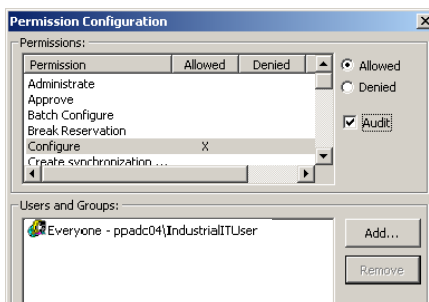


Figure 68. Audit Configuration

4. Click on the **OK** button.
5. Click the **Apply** button, and the line (since Full Audit was chosen by selecting both Allowed and Denied when configuring) is divided into two lines; one for Allowed and one for Denied. See [Figure 69](#).

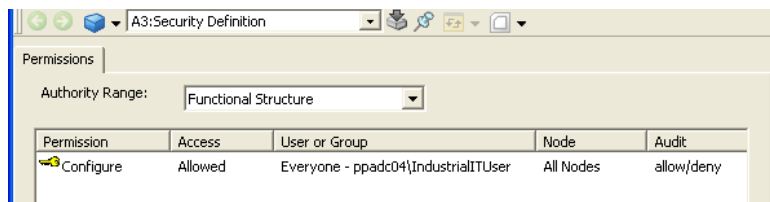
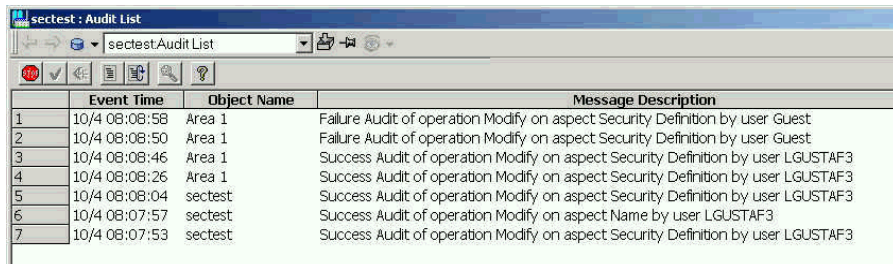


Figure 69. The Audit Configure

You have now set an audit for Configure on this object. See [Figure 70](#).



	Event Time	Object Name	Message Description
1	10/4 08:08:58	Area 1	Failure Audit of operation Modify on aspect Security Definition by user Guest
2	10/4 08:08:50	Area 1	Failure Audit of operation Modify on aspect Security Definition by user Guest
3	10/4 08:08:46	Area 1	Success Audit of operation Modify on aspect Security Definition by user LGUSTAF3
4	10/4 08:08:26	Area 1	Success Audit of operation Modify on aspect Security Definition by user LGUSTAF3
5	10/4 08:08:04	sectest	Success Audit of operation Modify on aspect Security Definition by user LGUSTAF3
6	10/4 08:07:57	sectest	Success Audit of operation Modify on aspect Name by user LGUSTAF3
7	10/4 08:07:53	sectest	Success Audit of operation Modify on aspect Security Definition by user LGUSTAF3

Figure 70. An Example of an Audit List



Refer to *System 800xA 5.1 Configuration (3BDS011222\*)* on how to change message description for a Generic OPC Property. Refer to *System 800xA Control 5.1 AC 800M Configuration (3BSE035980\*)* on how to change message description for 800xA for AC 800M properties.

### Audit List

The Audit List displays audit logs of operator actions and security. It can be a useful help to, for example, see what changes the last operator on shift made in the system.

**How to Create an Audit List.** To add an Audit List to an object follow the steps below:



Note that the Audit List audits the entire system, not one single object. The Audit List can be placed on any object, but it still shows activities for the whole system.



For the audit logging to work in the list, the audit trail must be activated. See [Audit Trail Configuration](#) on page 102.

1. Add an Alarm and Event List aspect to the object in the Plant Explorer.

2. Name it for example Operator Actions List, see [Figure 71](#).

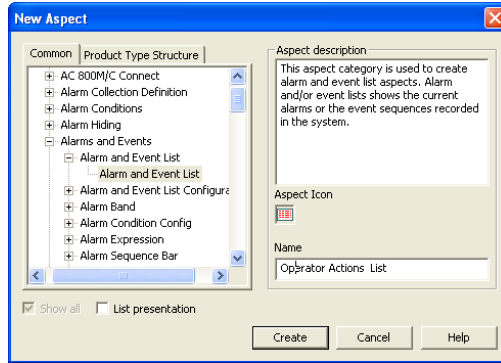


Figure 71. New Aspect - Operator Actions List

3. Right-click on the Operator Actions List in the aspect list and select **Config View**.
4. In the Configuration area select **Common Audit List**, see [Figure 72](#).

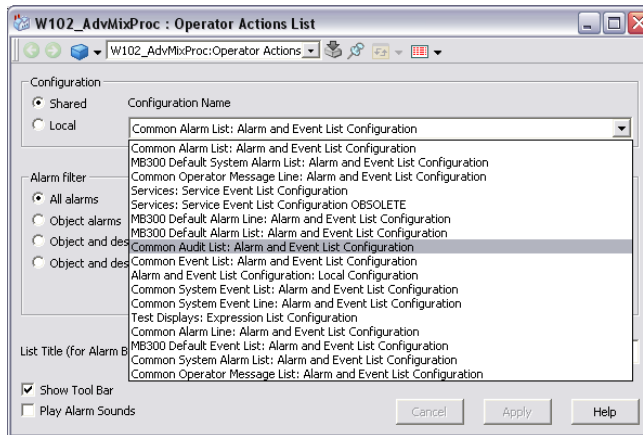


Figure 72. Select Configuration Name

5. Click **Apply**.

**Accessing the Audit List.** The Audit List is accessible through the context menu for the object, on which the list is placed. The name of the list may differ depending on configuration. In the example the list is named Operator Actions List, see [Figure 73](#).

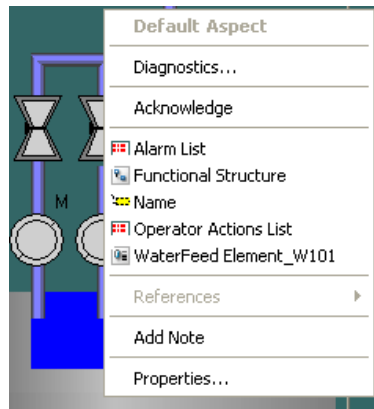


Figure 73. Context Menu

The audit logs are viewed in the Audit List. See [Figure 74](#)

	EventTime	AspectName	Category	MessageDescription	SourceName	UserFullName
5	04-09-16 15:53:47:664		AuditEvent_Acknowledge	Alarm on object AIC4_3 ackno AIC4_3		
6	04-09-16 15:53:47:367		AuditEvent_Acknowledge	Alarm on object AIC4_3 ackno AIC4_3		
7	04-09-16 15:53:43:196		AuditEvent_Acknowledge	Alarm on object MW STATUS a MW STATUS		
8	04-09-16 15:53:41:211		AuditEvent_Acknowledge	Alarm on object AIC4_4 ackno AIC4_4		
9	04-09-16 15:53:40:899		AuditEvent_Acknowledge	Alarm on object AIC4_5 ackno AIC4_5		
10	04-09-16 15:53:40:524		AuditEvent_Acknowledge	Alarm on object AIC4_4 ackno AIC4_4		
11	04-09-16 15:53:40:117		AuditEvent_Acknowledge	Alarm on object AIC4_5 ackno AIC4_5		
12	04-09-16 15:53:39:633		AuditEvent_Acknowledge	Alarm on object AIC4_4 ackno AIC4_4		
13	04-09-16 15:53:37:636		AuditEvent_Acknowledge	Alarm on object AIC4_5 ackno AIC4_5		
14	04-09-16 15:53:37:492		AuditEvent_Acknowledge	Alarm on object AIC4_4 ackno AIC4_4		
15	04-09-16 15:53:37:227		AuditEvent_Acknowledge	Alarm on object Alarm Manag Alarm Manager_Basic_PPaid11		
16	04-09-16 15:53:35:805		AuditEvent_Acknowledge	Alarm on object LAN acknowle LAN		
17	04-09-16 15:53:35:352		AuditEvent_Acknowledge	Alarm on object AIC4_5 ackno AIC4_5		
18	04-09-16 15:52:00:930	Audit Trail Config	AuditEvent_ConfigurationChange	Audit Trail message class filter w437a1 Production System		PPA Service 1
19	04-09-16 15:52:00:930	Audit Trail Config	AuditEvent_ConfigurationChange	Audit Trail message class filter w437a1 Production System		PPA Service 1
20	04-09-16 15:52:00:930	Audit Trail Config	AuditEvent_ConfigurationChange	Audit Trail message class filter w437a1 Production System		PPA Service 1

Figure 74. Example of an Operator Actions List

The list contains the following information:

- Date and time for the operation.
- Node from which the operation was performed.
- User name of the individual performing the operation.
- Type of operation.
- Object, property or aspect affected by the operation.
- Additional information from the involved aspect system.

## Windows Audit Function

In Windows you will find an audit function, which gives you the means to create reports regarding log-on, log-off and so on. As a Windows Domain Administrator you can set this function to support your security level.

The result of Windows audit is presented in the Event Viewer.

The settings are shown below:

1. Click **Start > Control Panel > Administrative Tools > Local Security Policy**.
2. Click **Audit Policy**, refer to [Figure 75](#).

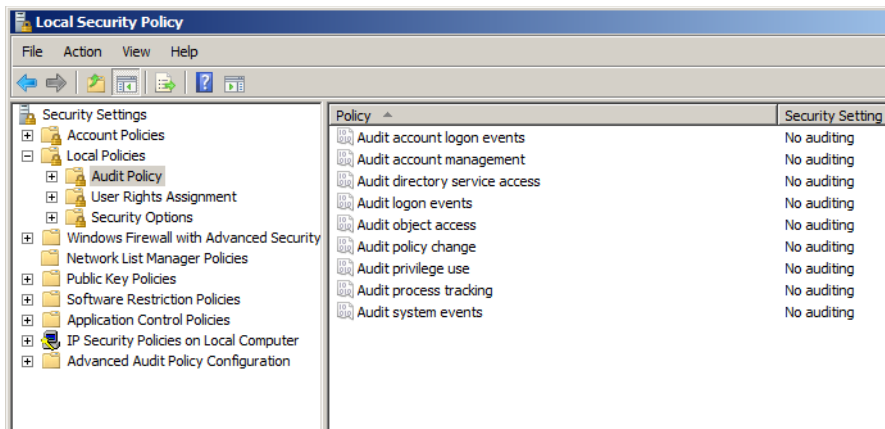
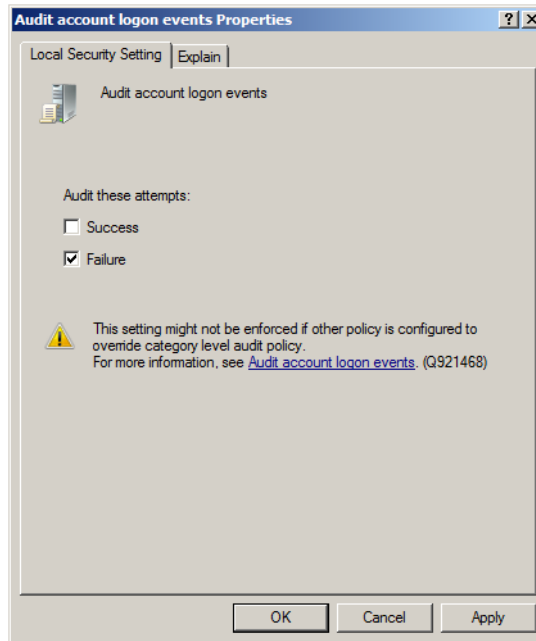


Figure 75. Audit Policy Settings

3. You now have the means to make a lot of settings.  
As an example, if you want to log all accesses to the system that Fail, double-click **Audit account logon events** as shown in [Figure 76](#) and the dialog box opens. In this dialog you can set that all connection attempts to the system that result in a **Failure** will be logged.



*Figure 76. Audit Account Logon Events*

- Further you can set the log size and other log declarations. Follow the path **Windows Settings > Security Settings > Event Log > Settings for Event Log** (see [Figure 77](#)).

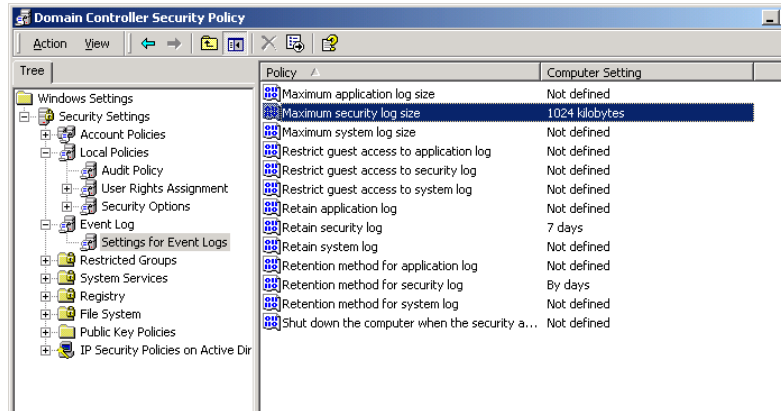


Figure 77. Settings for Event Log in Windows

- Double-click on the line “Maximum security log size” and a dialog box opens as shown in [Figure 78](#). In this dialog you can set how many kilobytes you want to allocate to the security log function.

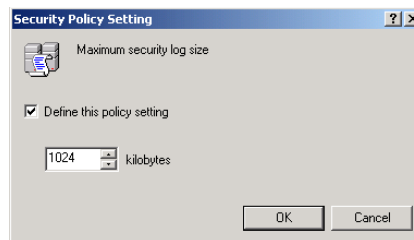
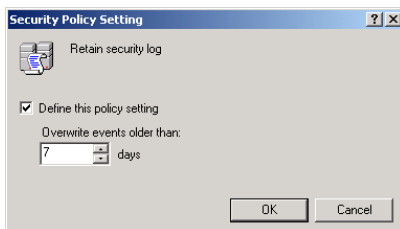


Figure 78. Maximum Security Log Size

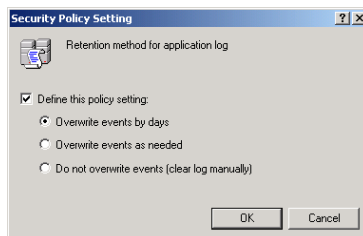


6. Double-click on the line “Retain security log”. This will bring up a dialog box as in [Figure 79](#). In this dialog you can set how many days a log must be stored in the log file, for example 7 days.



*Figure 79. Retain Security Log*

You can also give the retention methods for the log. If you, for example, double-click on the “Retention method for application log” line, a dialog box opens as in [Figure 80](#). In this dialog you can set the rules for the log according to the text in the dialog box.



*Figure 80. Retention Method for Application Log*



For further information about the Audit function in Windows, refer to the relevant Microsoft documentation.

## Critical Operation Authentication Support

For process critical operations, an aspect category may be configured to require an explicit authentication operation before the operation can be performed.

Two different authentication operations are supported:

- Re-authentication is used to guarantee that an operation is performed by the correct person. Requiring a re-authentication immediately before a change can be performed guarantees that no one can use a workplace if an operator temporarily leaves it.
- Double-authentication is used for operations critical to the quality of the product or required by regulation. It is used where the knowledge of an operator is limited or where it is required that another operator verifies the change before it is implemented.



From System Version 5.1 onwards, authentication operations can also be configured using the System Configuration Console. Refer to *System 800xA Tools (2PAA101888\*)* for more information.

### Re-authentication

The re-authentication dialog box is used to guarantee that the correct person performs each operation. When a change is made to an OPC property or aspect that requires a re-authentication, the dialog box pops up.

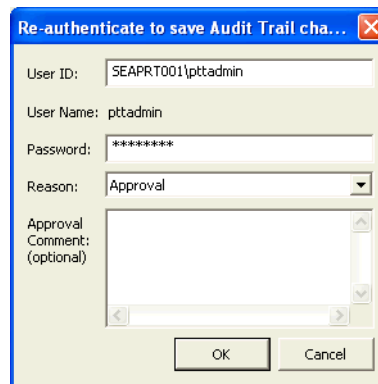
A screenshot of a Windows-style dialog box titled "Re-authenticate to save Audit Trail cha...". The dialog has a blue title bar with a close button (X) on the right. The main area is light green and contains several fields: "User ID:" with the text "SEAPRT001\pttadmin"; "User Name:" with the text "pttadmin"; "Password:" with a masked field of seven asterisks; "Reason:" with a dropdown menu showing "Approval"; and "Approval Comment: (optional)" with a large empty text area. At the bottom, there are two buttons: "OK" and "Cancel".

Figure 81. Approval Dialog

The user must type his/her User ID (with domain if it differs from the default domain) and password and select a reason from the **Reason** drop-down menu before pressing **OK**. Optionally, to type a comment in the **Approval Comment** text field.

If the provided information is accepted the dialog box disappears and the operation proceeds.

If authentication fails a pop-up error message appears which must be acknowledged before making a new attempt. If it fails three times in a row the dialog box will be terminated and the administrator will be notified about the failure with a system event.

### **Double-authentication**

The double-authentication dialog box is used to guarantee that the correct persons perform an operation. When a change is made to an OPC property that requires double-authentication, the dialog box pops up.

The user must type his/her User ID (with domain if it differs from the default domain) and password and select a reason from the **Reason** drop-down menu in the **First Approval** area before pressing **Apply**. It is optional to type a comment in the **Approval Comment** text field.

If the information provided by the user as the primary authenticator is accepted the **Second Approval** area is activated.

If it fails a pop-up error message is displayed which must be acknowledged before making a new attempt. If it fails three times in a row the dialog box will be terminated and you will be notified about the failure.

In the **Second Approval** area a secondary authenticator, which must have Approve permission granted on the object, shall type his/her User ID (with domain if it differs from the default domain) and password and reason before pressing **OK**. It is also here optional to type a comment in the **Approval Comment** text field.

If the provided information is accepted the dialog box disappears and the operation proceeds.

If it fails a pop-up error message appears which must be acknowledged before a new attempt can be made. If it fails three times in a row the dialog box will be terminated and you will be notified about the failure with a system event.

## How to Configure Authentication

To configure authentication for an aspect category follow the steps below:

1. Open the Aspect System Structure in the Plant Explorer.
2. Expand the Aspect System and Aspect Type of the aspect category to configure.
3. Select the aspect category for which authentication is to be configured.
4. Select the Aspect Category Definition aspect in the aspect list.
5. Select the **Configuration** tab in the configuration view.
6. Mark the **Single Authentication Required** check box if re-authentication for the aspect category. If double-authentication is required for the aspect category mark the **Double Authentication Required** check box.



The global System Setting for Advanced Access Control must be True for authentication to work. See [Configuration of Advanced Access Control](#) on page 116 for information about the global System Setting.



How to configure authentication for object properties is described in the *System 800xA 5.1 Configuration (3BDS011222\*)* instruction.

## Configuration of Advanced Access Control

Before re- or double authentication can be activated it must be configured by an overall system setting so that the activation can take affect.

You must hold the System Engineer role and have Security Configure permission to do this.



Note that the Advanced Access Control feature requires a license. If no license is obtained the value field will be disabled.

To do this follow the steps below:

1. Open the Admin Structure in the Plant Explorer and expand Administrative Objects.
2. Expand Domains and select the object with the name you gave to your system. By default this is <server node name>System.
3. Select the System Settings aspect in the aspect list.

- Change the value for the Advanced Access Control property to **True** in the **Value** drop-down menu.

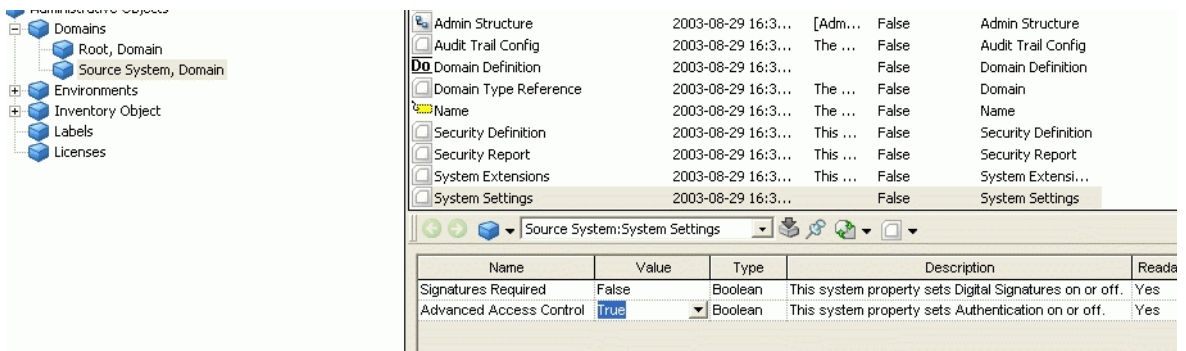


Figure 82. System Settings Aspect - Advanced Access Control

- Click **Apply**.

To activate authentication follow the steps below:

- Open the Admin Structure in the Plant Explorer and expand the Inventory Object.
- Open the object Aspect Category.
- Select the aspect category that you require authentication for.
- Select the Aspect Category Definition Settings aspect in the aspect list. See [Figure 83](#).

5. Select the **Configuration** tab in the configuration view to set re-and double authentication for the aspect category.

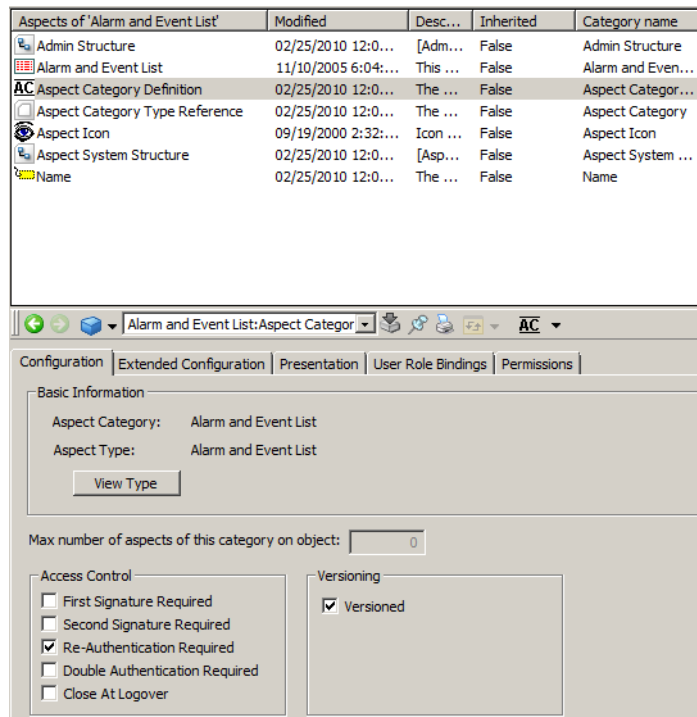


Figure 83. Aspect Category Definition Aspect - Configuration Tab

6. Click **Apply**.

### System Alarm

When a user fails to re-authenticate/log over, sign an aspect, or gets access denied there is a possibility to generate a system alarm. This is done by creating a System Alarm aspect and configure the message that should generate a system alarm. The recommendation is to place the System Alarm aspect on the Message object in the Library Structure.

The following messages can be set to generate system alarms:

*Table 8. System Alarm Messages*

LogoverFailure	When log over fails.
AspectReauthenticationFailure	When re-authentication of an aspect fails.
ReAuthenticationFailure	When re-authentication of an OPC property fails.
AuditEvent_AccessDenied	When a user gets access denied.
SignatureFailure	When a user fails to sign an aspect.

## Logover

The logover function enables a fast and temporary switch between users in a running workplace. It is designed to be used in a Operator environment, primarily to allow a user with more user rights than the logged in user. Users can log over and perform actions requiring privileges not possessed by the original user. Log over has the advantage that process supervision and control is not interrupted during the log over procedure compared to log out and logging in again as a different user. For example if an operation requires a permission not held by an operator, another user (e.g. an administrator) that holds the required permission, can log on to perform that operation. The logover changes the permissions and user roles but keeps all open windows with their present contents. The permitted actions in the open windows are controlled by the permissions of the logged over user.

It is also possible to configure an inactive user, that is a user with limited permission (read) that the system automatically will revert to after a certain amount of inactive time, see [Additional Logover Settings](#) on page 121.



The logover only affect the System permission. Windows security is still the same as the user logged in. This means that the access to files is still controlled by the user logged in.



If you have used display aspects as a substitute for faceplate aspects the logover function will not work.



The log over function is not intended to be used for engineering activities. The focus for the function is to enable operator related tasks to be performed during a log over. Restrictions in working with Import/Export tool, Control Builder, Graphic Builder or adding users to 800xA System limits its use.

### Configure Logover



From System Version 5.1 onwards, Logover settings can be configured using the System Configuration Console. Select System Configuration Console > Security > Logover.

To configure Logover follow the steps below:

1. Open the Admin Structure in the Plant Explorer and expand Administrative Objects.
2. Expand Domains and select the object with the name you gave to your system. By default this is <server node name>System.
3. Select the Logover Settings aspect in the aspect list.
4. Check the **Enable Logover** check box.

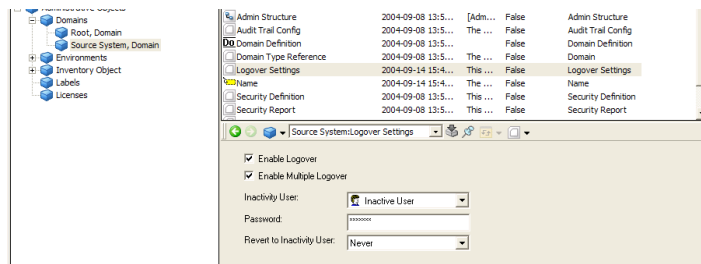


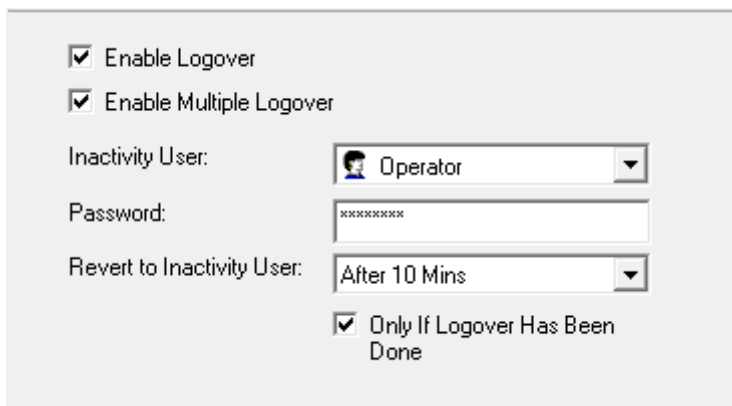
Figure 84. Logover Settings Aspect

5. Click **Apply**.



**Additional Logover Settings.** To configure the inactive user follow the steps below:

1. Add a user that must be the inactive user by using the Configuration Wizard or System Configuration Console.
2. Open the Admin Structure in the Plant Explorer and expand Administrative Objects.
3. Expand Domains and select the object with the name you gave to your system. By default this is <server node name> System.
4. Select the **Logover Settings** aspect in the aspect list, refer [Figure 84](#).
5. Check the **Enable Multiple Logover** check box, refer [Figure 85](#).



The screenshot shows a configuration window for Logover settings. It contains the following elements:

- Enable Logover
- Enable Multiple Logover
- Inactivity User: A dropdown menu with a user icon and the text "Operator".
- Password: A text field containing "\*\*\*\*\*".
- Revert to Inactivity User: A dropdown menu with the text "After 10 Mins".
- Only If Logover Has Been Done

*Figure 85. Logover Settings*

6. Select which user must be configured as an inactive user from the **Inactivity User** drop-down menu.
7. Set a password for the inactive user in the **Password** text field.
8. Set the time for automatic revert to inactive user in the **Revert to Inactivity User** drop-down menu.



If **Revert to Inactivity User** is enabled, a timer indicating the remaining time until revert is shown in the bottom-right corner of the screen, refer [Figure 86](#).

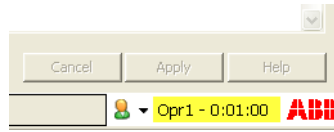


Figure 86. Timer - Revert To Inactive User

9. Check the **Only If Logover Has Been Done** check box.

The default setting is disabled. When enabled, the revert to the configured inactivity user is performed only if a manual logover has been done. In this case, the user that started the workplace never gets automatically logged out due to inactivity timeout.

10. Click **Apply**.

**Log Over Critical Aspect Views.** Aspect views that do not support log over can be configured so that they must be closed before the user is allowed to perform a log over operation. This is configured per aspect category.

To make this configuration follow the steps below:

1. Open the Admin Structure in the Plant Explorer and expand the Inventory Object.
2. Open the object Aspect Category.
3. Select the aspect type that you want to configure.
4. Select the Aspect Category Definition aspect in the aspect list.
5. Select the **Configuration** tab in the configuration view and mark the **Close At Logover** check box, refer [Figure 87](#).

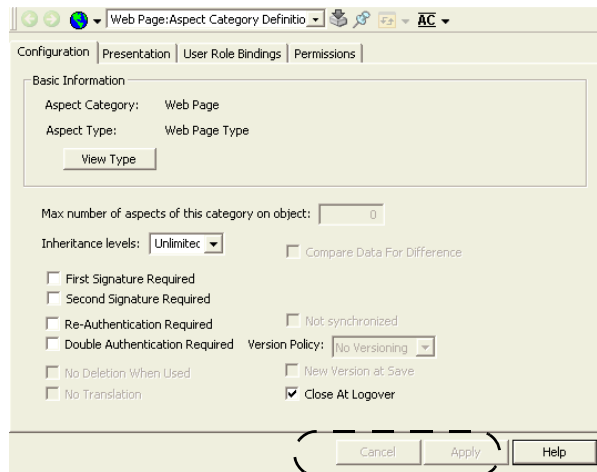


Figure 87. Configure Critical Aspect Views

6. Click **Apply**.

### How to use Log over

To change user right-click on the user name and select **Change User**. See [Figure 88](#).

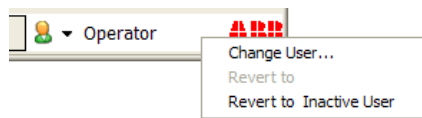
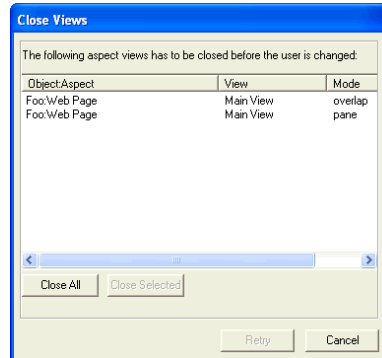


Figure 88. Change User

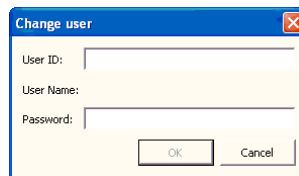
If a log over critical aspect view is open when the user selects **Change User**, a Close Views dialog box appears. See [Figure 89](#). In this dialog box the user can close the log over critical views.



*Figure 89. Close Views Dialog Box*

When the views are closed click **Retry** to proceed with the log over operation.

A Change-user authentication dialog box appears and the new user must enter his/her User ID (with domain if it differs from the default domain) and password. See [Figure 90](#).



*Figure 90. Change User Authentication Dialog Box*

If the User ID with domain and password are accepted the dialog box disappears and the new user can operate the workplace.

If the User ID with domain and password fail, a pop-up error message appears which must be acknowledged before a new attempt can be made. After three failed

attempts in a row the dialog box will be terminated and you will be notified about the failure. A system event is also created.

To return to the first user right-click on the user name again and select **Revert User**, see [Figure 90](#). The revert user operation requires authentication in order to change back to the original user.

Some applications will start and run as the logged on user, even if a log over is done. The following applications do not support log-over:

- AfwImportExport.exe
- AfwConfigWizard.exe
- Afw.NLS.TranslationTool.exe
- AfwSetVariable.exe
- AfwUhOp.exe
- PgDisplayTool.exe
- AfwWorkplaceApplication.exe



Use Windows File security to protect the applications above from being launched by unauthorized users.

### Windows Settings for Log over

The **Log Over** function will not work properly for other users than those with Windows administrator rights.

To resolve the problem assign the “Impersonate a client after authentication” user right to the user or user group that should use the logover function. To do this, follow the steps below:

1. Go to **Start > Control Panel > Administrative Tools** and then select **Local Security Policy**.
2. Expand **Local Policy**, and click **User Rights Assignment**.
3. In the right panel, double-click **Impersonate a client after authentication**.
4. In the Local Security Policy Setting dialog box, click **Add**.

5. In the Select Users or Group dialog box, click the user account the you want to add, click **Add** and then **OK**.
6. Click **OK**.

## Digital Signature



The Digital Signature function requires a license.

The digital signature function allows a user to electronically sign an aspect (a requirement for some industries and /or countries).

The Digital Signature Server is also used to verify the identity of signed aspects, when it was signed, and if the aspect is unchanged since it was signed.

The global System Setting for Signatures Required must be set to **True** for the Digital Signature to work. Refer to [Finding signed and unsigned aspects](#) on page 133 for information about the global System Setting.

To be able to sign an aspect the user must have the permission configured for the First and/or Second Signature operations.



From System Version 5.1 onwards, it is possible to configure the Digital Signatures using the System Configuration Console. Refer to *System 800xA 5.1 Tools (2PAA101888\*)* for more information.

To sign an aspect follow the steps below:

1. Select the aspect to be signed.
2. Open the context menu and select **Add Signature**.
3. The authentication dialog appears, see [Figure 91](#). Type a User ID with domain and a password and select a reason from the **Reason** drop-down menu before you press **OK**. It is optional to type a comment in the **Approval Comment** text field.



Figure 91. Authentication Dialog for Digital Signature

4. Click **OK**. This will create a Signatures aspect containing the signature. See Figure 92. An audit trail will also be generated if the audit function is active.
5. To verify the signature double click on the Signatures aspect.
6. Click **Verify** in the Signatures dialog box.

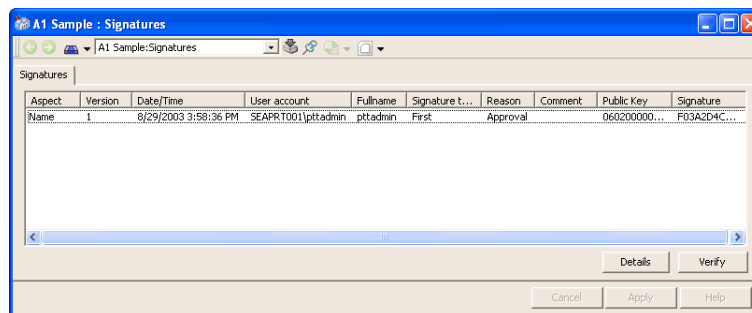


Figure 92. Signatures

7. A Signatures Verification dialog appears, click **OK**.

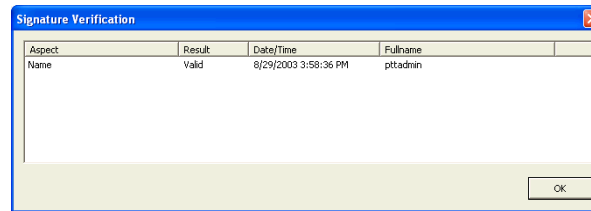


Figure 93. Signature verification

8. The column **Result** shows if the signature is valid. The signature is Invalid if the signed aspect is changed in any way since its signing.
9. If you click on the **Details** button (see [Figure 92](#)) a dialog box appears with detailed information about the signature, you also have the possibility to copy information from this dialog box, such as the Public Key and Signature.

### Adding a new Reason

You can add a new Reason for the Authentication Dialog if you feel that the default reasons not are adequate.

The default Reasons are:

Table 9. Authentication Reasons

Reason	Description
Approval	Approval of action or document.
Danger	Danger to personal or machinery.
Disturbance	Process disturbance.
Maintenance	Equipment maintenance.
Optimization	Process optimization.
Order	Supervising order.

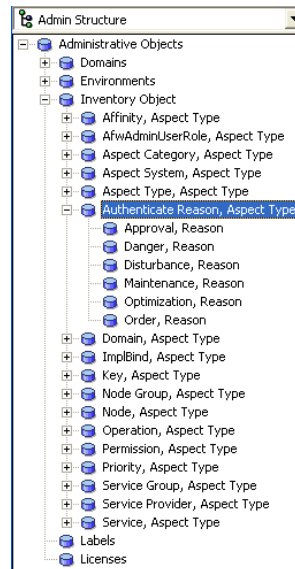




There may be more reasons depending on installed system extensions.

To add a new Reason follow the steps below:

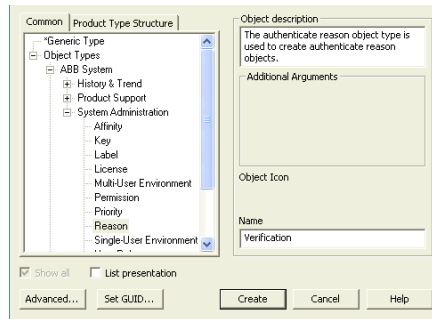
1. Go to the Admin Structure and expand the Inventory Object.
2. Expand the Authenticate Reason object. All default Reason objects are listed below. See [Figure 94](#).



*Figure 94. Authenticate Reason Object*

3. Right-click on the Authenticate Reason object and select **New Object** from the context menu.

4. Select the Reason object according to [Figure 95](#), and give it a proper name. Click **Create**.



*Figure 95. Reason Object*

5. Select the Name aspect in the aspect list.
6. Type a description in the **Description** text field. This text will appear as tool tip when placing the cursor over the Reason in the Authentication Dialog. See [Figure 96](#).



To change the description for a default Reason, change it in the Name aspect of the Reason object that is to be changed.

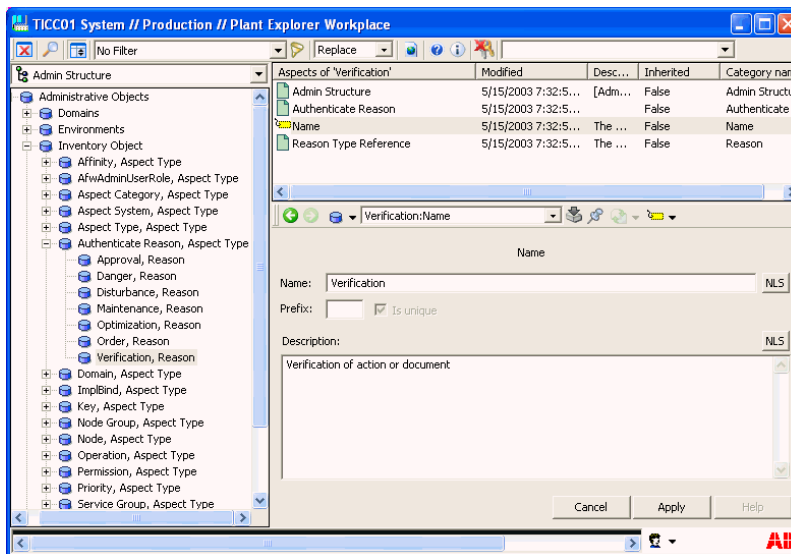


Figure 96. Name Aspect of Verification Object

7. Click **Apply**.

### Finding Signature Aspect

The Find Tool can be used for finding signed and unsigned aspects. For example, an object for which you want to sign all the unsigned aspects, do this by running a search of all unsigned aspects for that specific object.

### Finding signed and unsigned aspects

1. Click on the Find Tool icon in the Plant Explorer, see [Figure 97](#).

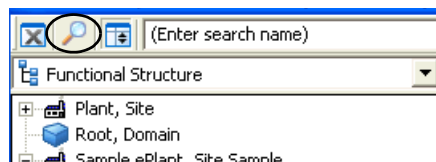


Figure 97. Find Tool Icon

2. Select the Aspect Signature in the **Add attribute** drop-down menu, see [Figure 98](#).

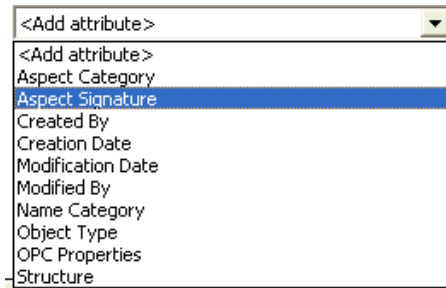


Figure 98. Add Attribute

3. Select **Objects** or **Aspects** depending on search, see [Figure 99](#). If you select **Objects** you will find all objects which have signed/unsigned aspects. If you want to make a search for signed/unsigned aspects of a certain object, you must type the name of the object in the **Name** text field. If you select **Aspects** you will find all signed/unsigned aspects.

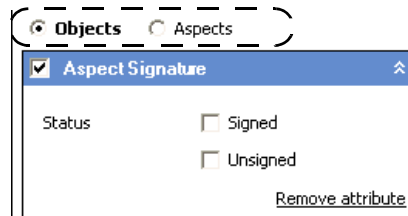


Figure 99. Objects/Aspects

- You can search for signed aspects, unsigned aspects, or both by checking the check boxes in the status field, see [Figure 100](#)



Figure 100. Status Field - Signed/Unsigned

- When your selections are made click the **Search** button to begin the search. The result is displayed in the right pane, see [Figure 101](#).

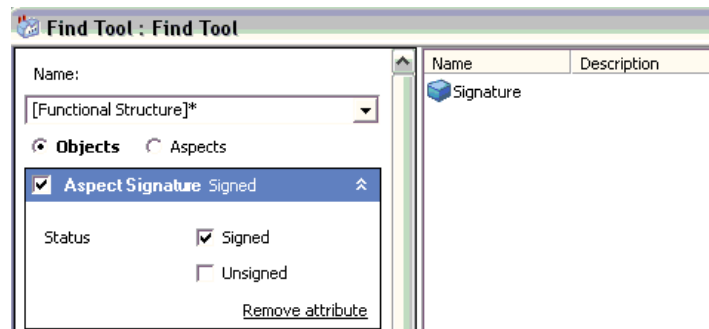


Figure 101. Search Result

### Configuration of Digital Signature

The first signature is given to aspect types that hold important information and therefore need to be digitally signed. The second signature is given to aspect types that also hold important information but need an additional authentication, i.e. two digital signatures.

Before you can activate the first and second signatures you have to configure an overall system setting so that the activation can take affect.

You must hold the System Engineer role and have Security Configure permission to do this.



Note that the Digital Signature feature requires a license. If no license is obtained the value field will be disabled.

To do this follow the steps below:

1. Open the Admin Structure in the Plant Explorer and expand Administrative Objects.
2. Expand Domains and select the object with the name you gave to your system. By default this is <server node name> System.
3. Select the System Settings aspect in the aspect list.
4. Change the value to **True** in the **Value** drop-down menu. See [Figure 102](#).

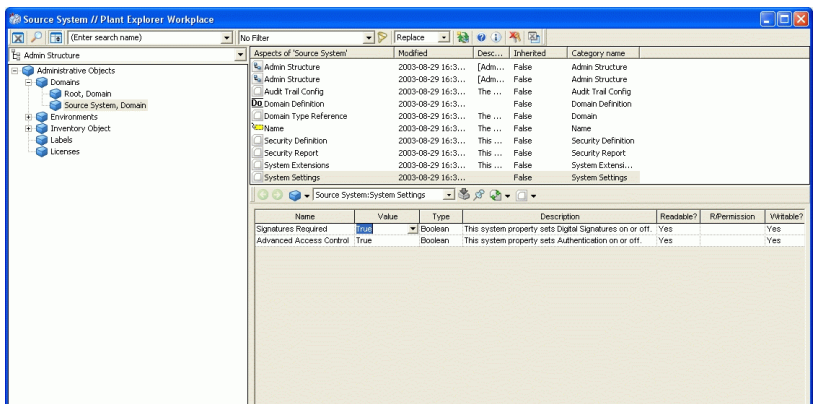


Figure 102. System Settings Aspect - Signatures Required

5. Click **Apply**.
6. Re-authentication is required to apply this change, given that Advanced Access Control is set to True.

To activate the first/second signature follow the steps below:

1. Open the Aspect System Structure in the Plant Explorer and expand the Aspect Directory Aspects, Aspect Systems.

2. Open the object Aspect Category.
3. Select the aspect type that you require digital signature for.
4. Select the Aspect Category Definition aspect in the aspect list. See [Figure 103](#).
5. Select the **Configuration** tab in the configuration view to set first/second signature for the aspect category.

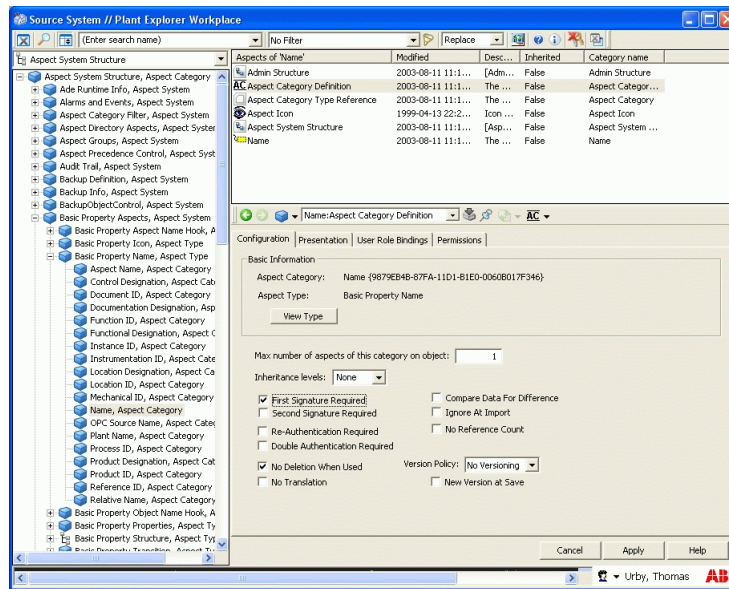


Figure 103. Aspect Category Definition Aspect - Configuration Tab

6. Click **Apply**.

**Required Permission for Signing.** The default setting in the system is that everyone with configure permission can sign an aspect. You can easily change that by configuring the required permission for the first and second signature. Follow the steps below:

1. Open the Aspect System Structure in the Plant Explorer.
2. Expand the Basic Property Aspects object.

3. Select the aspect category that you want to configure the required permission to do a first/second signature for.
4. Select the Aspect Category Definition aspect in the aspect list.
5. Select the **Permissions** tab in the configuration view and select the operation that you want to set permission for.
6. Select permission for the operation in the **Permission** drop-down menu, see [Figure 104](#). Click **Apply**.

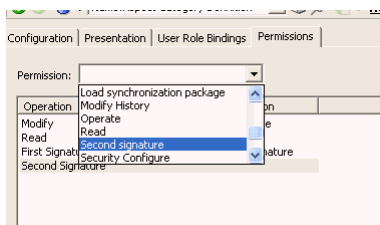


Figure 104. Permission for Signing

## Confirmed Write

When operating a SIL application, all operations on writable OPC properties must be confirmed by the operator. The operator is responsible for checking that the operation performed in, for example, a faceplate, corresponds to the operation indicated in the Confirm Operation dialog. The content of the Confirm Operation dialog is the system's interpretation of the operation. To be able to do this, the texts displayed in the Confirm Operation dialog must uniquely identify the operation performed, see [Figure 105](#).



Please note that the Confirmed Write function only can be used for properties in SIL application in an AC 800M High Integrity controller.

Confirmed Write also enables two-step operations for faceplates. In this case the Confirm Operation dialog gives the operator the possibility to verify that the initiated operation is the wanted operation.



To execute a Confirmed Write operation it requires the operator to have the Safety Operator Role in PPA.





The timeout dialog of the Confirmed Online Write has to be acknowledged within 90 seconds otherwise the confirm button is dimmed and its only possible to cancel the write operation.

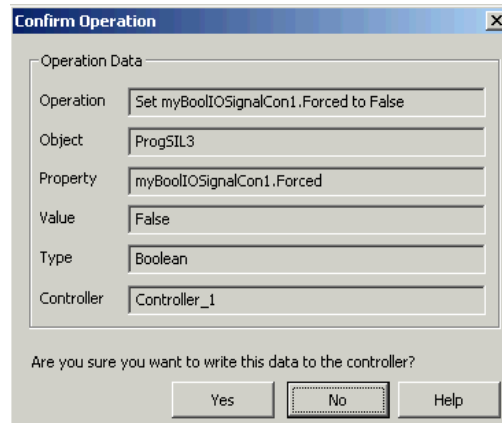


Figure 105. Confirmed Write Support Configuration

Property Name column shows to the addressed property, and the Value column shows the value to be written to this property. Each property that is enabled for writing in SIL applications must be configured to identify corresponding faceplate operations.

### Confirmed Write Support Configuration

Confirmed Write is preconfigured for all SIL classified control module types and function block types in AC 800M. It can also be configured manually for other control module types and function block types. This is described below.

#### Adding a Confirmed Write Support Aspect

1. Right-click the type and select **New Aspect**. A New Aspect window opens.
2. Click the **Common** tab in the New Aspect window, then check **Show all** and **List presentation**.
3. Scroll down the aspect list and select **Confirmed Write Support**.

- Click **Create**. A Confirmed Write Support aspect has been created (located at the top of the aspect pane).

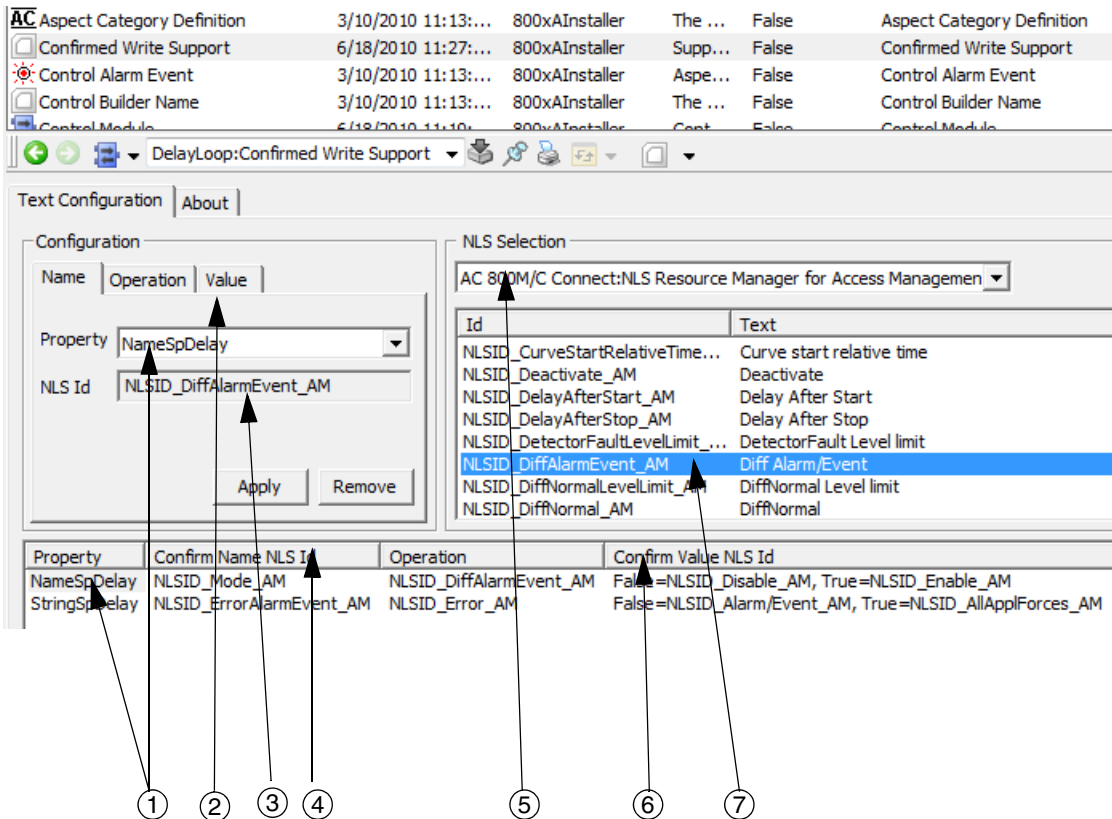


Figure 106. Configuration of the Confirmed Write Support Aspect

### Confirmed Write Support Aspect Description

The following numbers correspond to the balloon marks in [Figure 106](#):

- Property Select.** The property to be configured is selected either in the **Property** drop-down menu, or by selecting a property in the **Property** column.
- Operation.**

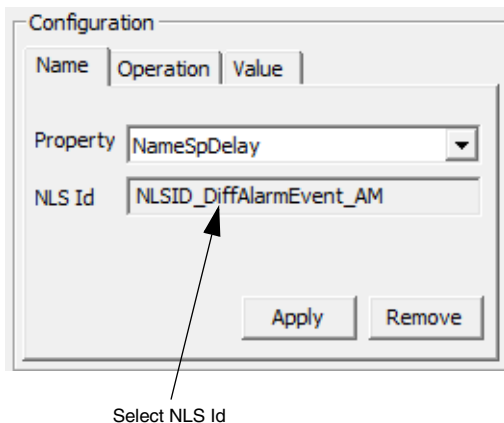
3. **Value Configuration.** Operation controls in a faceplate. For example pressing the **Start** button which writes a Boolean value *true* to the controller, the Confirm Operation dialog should show the text **Start** in the Value column, not the Boolean value *true*. See also [Value Configuration](#) on page 140.
4. **Select NLS Id.** The **NLS Id** text field shows the selected NLS ID, which will be associated with the selected property if the **Apply** button is pressed.
5. **Configured Property Name.** The **Confirm Name NLS Id** column displays the configured NLS Id for each property.
6. **NLS Resource Manager Select.** The NLS Resource Manager to be used for text that has been selected in the **NLS Selection** drop-down menu.
7. **Configured Value.** The **Confirm Value NLS Id** column displays the NLS Id for any values that have been assigned texts (see Value Configuration No. 2).
8. **NLS Id Select.** The NLS Selection list displays all NLS identities defined in the selected NLS Resource Manager. The text to be assigned to the selected property is selected in the **NLS Selection** list.



Please note that when renaming a variable the configured values will be lost. The system does not have an automatic consistency check, so it will not give you notification or warning during download saying that the values are lost. It is however possible to make a manual consistency check.

It is recommended to configure the Confirmed Write Support texts late in a commissioning phase, when the need for renaming variables is low.

**Value Configuration.** The association between the value written to the controller, and the text shown in the Value column is configured under the **Confirm Value** tab, see [Figure 107](#).



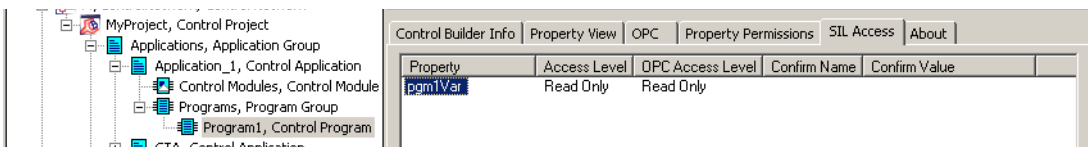
*Figure 107. Value Configuration Dialog under the Confirm Value Tab.*

1. **Value Select.** The value to be configured is selected from the **Property** drop-down menu.
2. **Select NLS Id.** The **NLS Id** text field shows the selected NLS id, which will be associated with the selected property/value.

**Confirm Online Write Example.** This small example illustrates how to configure Access levels in a SIL application. It starts by applying an access level on a property, and describes how different settings may affect other settings. At the end of the example you will learn how to configure a property with NLS strings and to make the strings appear in a Confirm Operation dialog box.

### Applying Access Level on a Property

Assume the following; a small project called MyProject with a local variable *pgm1Var* **integer** declared in *Program1*. The Property *pgm1Var* will be displayed in the Program's control aspect, as in [Figure 108](#).



*Figure 108. The variable *pgm1Var* displayed as a Property under the SIL Access tab in the Plant Explorer.*

As you can see in [Figure 108](#), the variable *pgm1Var* has both the Access Level and the OPC Access Level configured to Read Only. Properties are always configured to Read Only the first time (default). If an operator should write to *pgm1Var* online, you must change the access level to *Confirm* or *Confirm and Access Enable*.

However, by changing the access level on *pgm1Var* to *Confirm* will only result in an apparent change on the variable *pgm1Var*, the OPC Access Level will at this point still be *Read Only*, see [Figure 109](#).

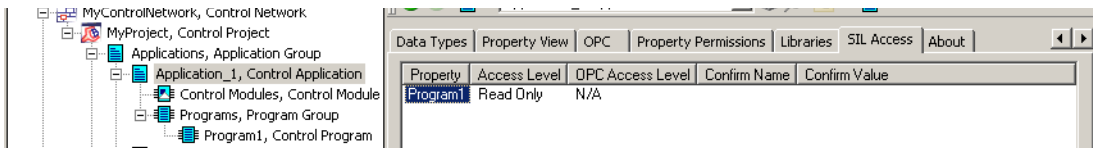


*Figure 109. The Access Level and the OPC Access Level for the variable *pgm1Var*.*

This means that an operator cannot write to *pgm1Var* online, even though the access level has been changed to *Confirm*. The reason is because of *Program1*. The variable *pgm1Var* was declared as a local variable inside *Program1* in the Project Explorer. *Program1* has not yet been configured in Plant Explorer, thus still got Access Level *Read Only*, which overrides *Confirm* on *pgm1Var*.

You must set Access level on *Program1* to *Confirm* before the OPC Access level on *pgm1Var* can be *Confirm*.

The Access Level for *Program1* can be reached by selecting the SIL Access tab from the Application's control aspect, according to [Figure 110](#).



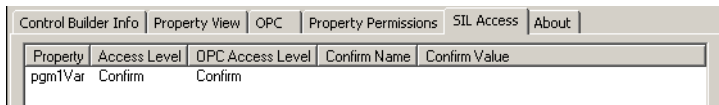
*Figure 110. The Application's control aspect displaying the Access level for Program1.*

The Access level for *Program1* decides the OPC Access Level for *pgm1Var*, and in the end possibilities to write to *pgm1Var* online. To get the OPC Access level for *pgm1Var* to *Confirm*, first set *Program1* to *Confirm* according to [Figure 111](#).



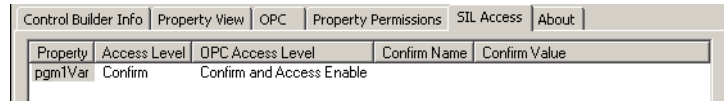
*Figure 111. The Program1 has changed the Access Level to Confirm.*

This will result in OPC Access Level *Confirm* for *pgm1Var*, see [Figure 112](#). The variable *pgm1Var* has got OPC Access Level changed to *Confirm*, which means that an operator can write to the *pgm1Var* online.



*Figure 112. Variable pgm1Var with the new OPC Access Level Confirm.*

Similar, by changing the Access level on *Program1* to *Confirm and Access Enable*, will instead result in an OPC Access Level *Confirm and Access Enable* for *pgm1Var*. See [Figure 113](#).



Property	Access Level	OPC Access Level	Confirm Name	Confirm Value
pgm1Var	Confirm	Confirm and Access Enable		

Figure 113. The OPC Access Enable for *pgm1Var* if the *Program1* was instead changed to (*Confirm and Access Enable*).

### Changing the SIL Access on Structured Data Types

This subsection describes how to apply a new Access Level on a structured data type and its components.

Assume that *MyProject* has been extended with a structured data type ‘*MyDataType*’ inside the *Application\_1*, according to [Figure 114](#).

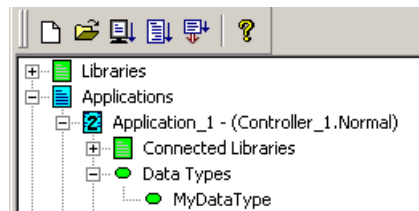


Figure 114. The structured data type *MyDataType* has been created inside *Application\_1*.

A new variable has also been declared in *Program1* called *pgm1Struct* and is of *MyDataType*. The *pgm1Struct* contains three components; *Comp1*, *Comp2*, and *Comp3*. After creating a structured data type and declaring a new variable in Project

Explorer, the SIL Access tab in Plant Explorer will display the properties, according to [Figure 115](#).

Property	Access Level	OPC Access Level	Confirm Name	Confirm Value
pgm1Var	Confirm	Confirm and Access Enable		
pgm1Struct.Comp1	N/A	Read Only		
pgm1Struct.Comp2	N/A	Read Only		
pgm1Struct.Comp3	N/A	Read Only		
pgm1Struct	Read Only	N/A		

*Figure 115. The new variable pgm1Struct and its components displayed inside Program\_1.*

The new variable *pgm1Struct* has Access Level (Read Only) as default, and the OPC Access Level (N/A=not applicable). This means that you cannot operate on the components (*Comp1*, *Comp2* and *Comp3*) from the current location (*Program\_1*).

To learn how the *pgm1Struct* is configured, you must shift to the Object Type Structure and look inside MyDataType. [Figure 116](#) is showing the type definition with the default configuration.

Property	Access Level	OPC Access Level	Confirm Name	Confirm Value
Comp1	Read Only	Read Only		
Comp2	Read Only	Read Only		
Comp3	Read Only	Read Only		

*Figure 116. The three new components displayed under the SIL Access tab inside the control aspect for Data Types.*



In order to study how different Access Level settings will behave, each component is configured to have a higher access level than it's previous. See [Figure 117](#).

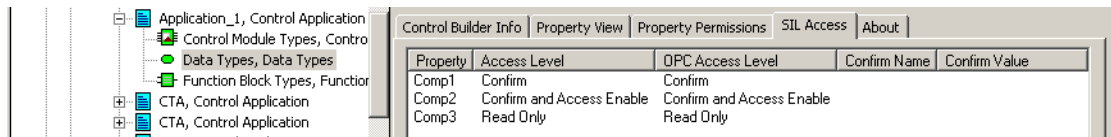


Figure 117. The three components with different Access Level.

The *Comp1* and *Comp2* have been given new access levels, whereas *Comp3* still got (Read Only). According to the new configuration displayed in the Control Structure (see [Figure 118](#)), none of the Access level settings has been executed. In this case the problem is the settings on *pgm1Struct* and *Program1*.

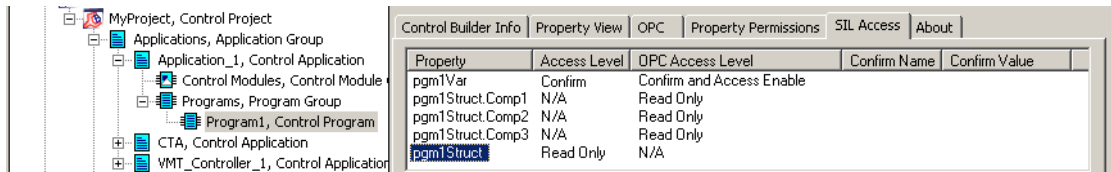


Figure 118. None of the settings on the components have been executed

By changing the *pgm1Struct* to *Confirm* should change the OPC Access Level status for the components. But, according to [Figure 119](#), is the OPC Access Level for *Comp1* *Confirm and Access Enable*, even though it should be *Confirm*. Why?

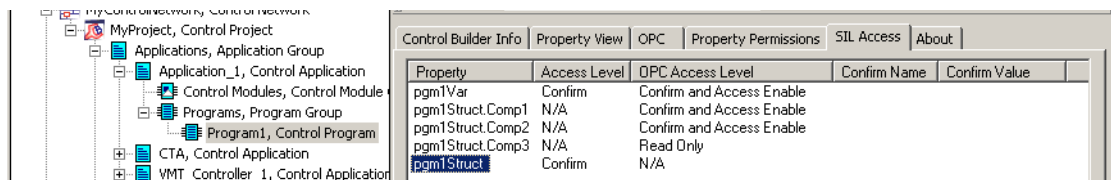


Figure 119. Comp1 still got the OPC Access Level Confirm and Access Enable.

The reason *Comp1* does not have *Confirm* is because of the setting on *Program1*.

According to the example illustrated in Figure 113, was the *Program1* changed to *Confirm and Access Enable* to show how that would affect the OPC Access level for *pgm1Var*. Because of the present Access level on *Program1*, apparently *Confirm and Access Enable*, it overrides *Comp1*'s Access Level *Confirm* but accepts *Comp2*'s Access level *Confirm and Access Enable*.

If the Access level for *Program\_1* is changed to *Confirm*, according to Figure 120, the OPC Access level for *Comp1* will be *Confirm*. See Figure 121.

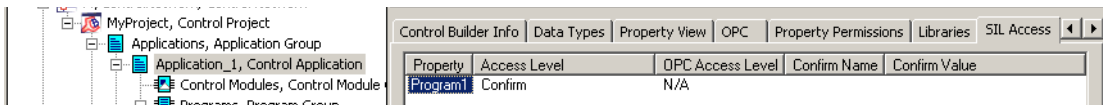


Figure 120. Program1 is changed to (Confirm).

By changing *Program1* to *Confirm*, will enable the OPC Access Level on *Comp1* to be *Confirm*. Note, that *pgm1Var* also got OPC Access level *Confirm*.

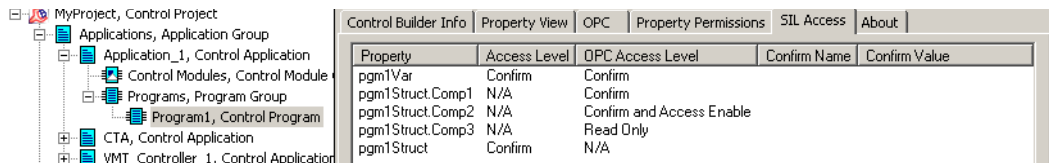


Figure 121. Comp1 with OPC Access Level (Confirm).



For more information about Confirmed Online Write see *System 800xA Control 5.1 AC 800M Configuration (3BSE035980\*)*.

## Memory Swapping

When running Operator Workplace in full screen mode and leaving the Workplace for some time, the system memory will be swapped out to the hardware. To resolve this problem assign the “Increase Scheduling Priority” user right to the user or user group. To do this, follow the steps below:

1. Go to **Start > Control Panel > System and Security > Administrative Tools** and then select **Local Security Policy**.
2. Expand **Local Policy**, and click **User Rights Assignment**.

3. In the right panel, double-click **Increase scheduling priority**.
4. In the **Local Security Policy Setting** dialog box, click **Add**.
5. In the **Select Users or Group** dialog box, click the user account the you want to add, click **Add** and then **OK**.
6. Click **OK**.

## Security of External Data

### Bulk Data Manager / Document Manager / Engineering Templates

Bulk Data Manager is an Engineering Studio feature consisting of Microsoft Excel enhanced by AddIn LBEMacros.

Document Manager is - together with Parameter Manager - an Engineering Studio feature using Microsoft Word.

Engineering Templates are predefined workbooks for Bulk Data Manager.

It is possible to read information from an 800xA System and to save it to the Windows file system using BDM and DM/PM. To avoid undermining the security policy set up for an 800xA System, users should save the contents of Bulk Data Manager sheets, Document Aspects or Engineering Templates in secure folders only.



A secured folder for example is the login user's folder "C:\Documents and Settings\User" (User: Logged in user name).

The Bulk Data Manager (Microsoft Excel) as well as Document Manager (Microsoft Word) can be used to write values through OPC properties to running controllers. Ensure that the required permissions for these properties are defined according to the security policy.

## Parameter Manager

Parameter Manager stores the parameter aspect property data and the parameter aspect category definitions in an aspect blob. For more information, refer to *System 800xA Engineering 5.1 Engineering Studio (3BDS011223\*)*.

## Reuse Assistant

### Saving Reuse Instruction

In build mode, it is possible to save the Reuse Instruction in the form of an xml file, see [Figure 122](#). The saved file is mainly used for instruction comparison.

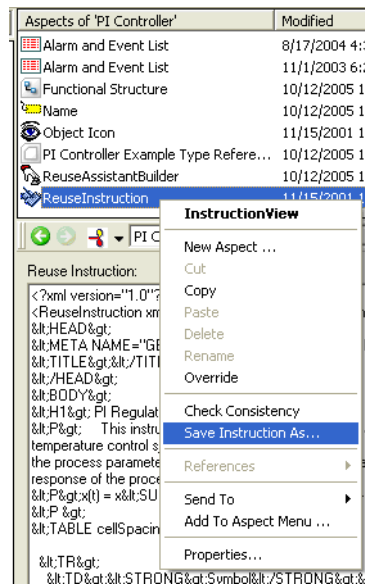


Figure 122. Save Reuse Instruction

The file should be saved in a secured folder such as login user's folder "C:\Documents and Settings\User". Where "User": Logged in user name.

### Saving Reuse Instruction State

The Reuse Instruction state can be saved in form of xml file, see [Figure 123](#).

The saved file is mainly used for instruction state comparison.

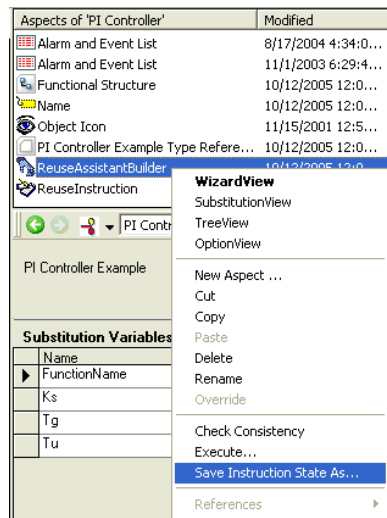


Figure 123. Save Instruction State

The file should be saved in a secured folder such as login user's folder "C:\Documents and Settings\User". User: Logged in user name.

### Export / Import of Reuse Instruction AFW file

The Reuse Instruction generated in the architect mode can be shipped to customer in form of AFW file.

The creation of Reuse Instruction AFW file is provided in the Section 8 - Reuse Assistant, Architect - Shipping the Reuse Instruction of user guide *System 800xA Engineering 5.1 Engineering Studio (3BDS011223\*)*.

The file should be saved in a secured folder such as login user's folder "C:\Documents and Settings\User".

User: Logged in user name

Before exporting/importing the Reuse Instruction AFW files to/from a floppy disk, it should be scanned for virus.

## Secure Remote Connections using VPN

Virtual private network (VPN) is a general notion for a connection that is created over an existing public or shared infrastructure using encryption and/or authentication technologies to protect its payload. A VPN Connection may be established between two nodes or between a node and a firewall. There are different protocols that can be used to create VPN connections. One example is to use L2TP over an underlying IPsec tunnel.

If a remote node is connected as a client to an 800xA system through a VPN connection it is very important to notice that the same care must be taken regarding the security handling of the remote node as for the 800xA nodes since the VPN connection may make the remote node a member of the 800xA system and if the remote node is unsecure the whole system may be unsecure.

See the *System 800xA 5.1 Network Configuration (3BSE034463\*)* for more information.

---

# Section 5 Process Sectioning

## Security Setting by Structuring in Plant Explorer



A member of the System Engineer group must set the security described in this section.

A very useful method to set security is to build structures for the plant, and set Security Definition aspects with Structure range. Create typical structures in the Location Structure by putting process equipment in buildings and rooms, or dividing the Functional Structure into process sections.

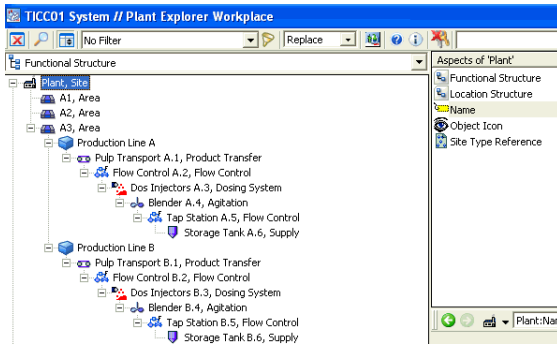


Figure 124. Production Procedure Structuring in Plant Explorer

We have a production process in the A3, Area which produces in two similar production lines - Line A and Line B. In the Plant Explorer, each line includes separate production steps according to Figure 124.

Basically each line has its own operator (operator Opr1 for Line A and operator Opr2 for line B). The security must be set in such a way that the operators are only able to operate their “own” line. We set a System Engineer as an Operator for both lines.

This is easily done by using the structure settings and three Security Definition aspects. We add one Security Definition aspect to the “top” Aspect Object A3, Area and one each to the objects “Production Line A” and “Production Line B”.

## Setting the Security Definition Aspects in the Example

### Security Definition Aspect for the A3, Area Aspect Object

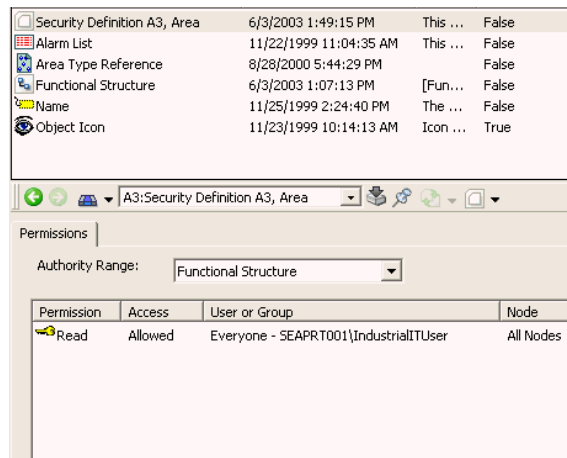


Figure 125. Security Definition Aspect Setting in the “top” Object A3,Area?

On the “top” object for the two production lines, the A3, Area object, we configure the security setting so the System Engineers can operate both lines.

We terminate search, because we do not want the default settings to be valid.

Ending the Terminate Search means that access is denied to anyone not specified in this Security Definition aspect.



## Security Definition Aspect for the Production Line A Object

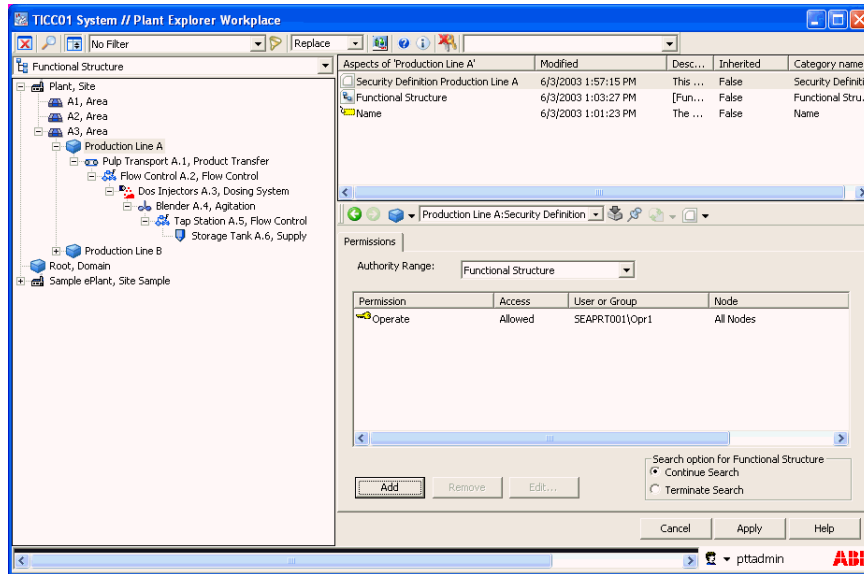


Figure 126. Security Definition Aspect Setting in Production Line A Object

In each structure we set a Security Definition aspect that defines persons/groups that must have a permission in one structure but not in the other.

For example, in a security aspect added to the Production Line A object we define the permissions in that structure. In this case we give operator Opr1 the permission to operate the objects in this structure.

By setting **Continue Search**, the security search goes upwards in the structure.

### Security Definition Aspect for the Production Line B Object

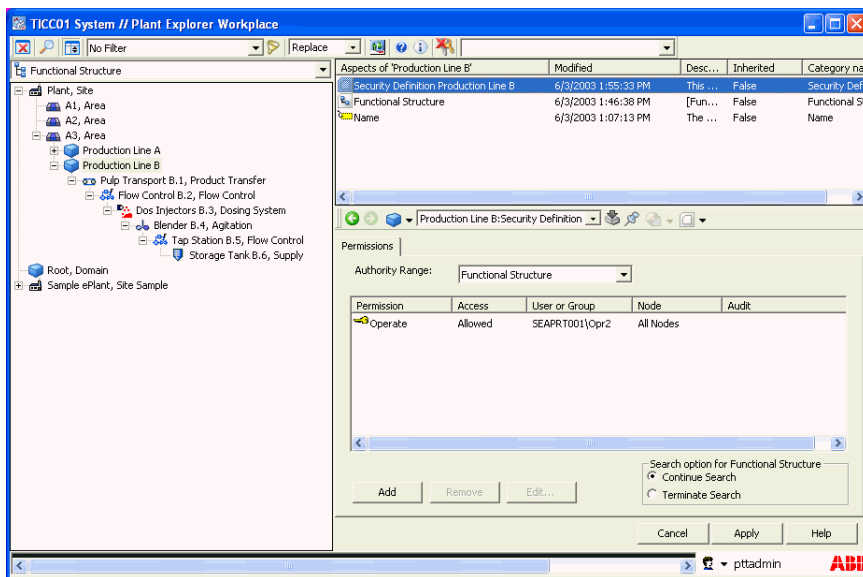


Figure 127. Security Definition Aspect Setting in Production Line B Object

The security aspect added to the Production Line B object defines the permissions in this structure. In this case we give operator Opr2 the permission to operate the objects in this structure.

By setting **Continue Search**, the security search goes upwards in the structure.

---

# Section 6 Point of Control

## Introduction

A plant structure is often divided into logical sections that can be operated individually by a set of designated users. In a distributed system, multiple users operating from different geographical locations can be responsible for different sections of the plant. In such situations, to avoid the risk of more than one user operating a section simultaneously, a strict security can be applied. Setting up a strict security can be challenging and a number of scenarios must be taken into consideration. The feature Point of Control is provided to simplify this process.

Point of Control is a concept that allows dividing the plant into sections. The Operator that is in control over a section is called the Responsible User. The Responsible User has security right granted that other users in the system lack for the same section. A typical scenario is that only the Responsible User will be able to control the process in this section.

## Point of Control Features

The key features of the Point of Control functionality are:

- Improved System Security  
The Point of Control functionality enforces a strict security on the system to avoid the risk of many users operating a section at the same time.
- Transfer of responsibility between the users:
  - Request Responsibility
  - Grab Responsibility
  - Release Responsibility

- Alarm List Responsibility Filter  
Alarms can be filtered based on the current responsibility. The same filter will hide these alarms for other users.
- Audit Logging  
If audit is enabled for AuditEvent\_OperatorAction, the responsibility transfer between different users and nodes will be logged.
- Point of Control Summary  
Displays an overview of the current status of each section. For more information about the Point of Control Summary, refer to *System 800xA Operations 5.1 (3BSE036904\*)*.
- Security Report  
The Section Definition aspect and Security Definition aspect configurations are included in the Security Report.
- OPC Properties for Status  
The Point of Control status for a section is exposed as standard OPC properties. This makes it possible to create overview graphics that displays the Point of Control status for example, the currently responsible user for a section.
- Bulk Data Manager Support  
The Section Definition aspects supports configuration using the Bulk Data Manager. For more information about Bulk Data Manager, refer to *System 800xA Engineering 5.1 Engineering Studio Function Designer (3BDS011224\*)*.



Point of Control is designed to be used by Operators. Use Reserve for Engineering tasks. Refer to *System 800xA Engineering 5.1 Engineering Studio Function Designer (3BDS011224\*)* for more information.



Point of Control is supported only in the Production Environment. Refer to *System 800xA Engineering 5.1 Engineering and Production Environments (3BSE045030\*)* for more information about the environments supported.

## Enabling Point of Control

The Point of Control functionality is a licensed feature in the 800xA system and must be enabled before it can be used.

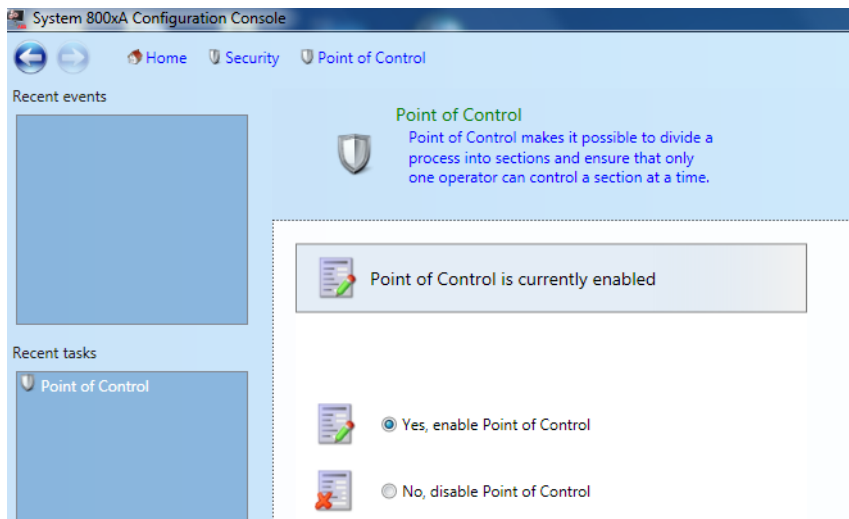


Figure 128. Enabling Point of Control

To enable the functionality using System Configuration Console, select **Start > All Programs > ABB Industrial IT 800xA > System > System Configuration Console > Security > Point of Control**, refer to [Figure 128](#).

By default, the Point of Control functionality is disabled.



Point of Control can be configured only by users that belong to both the System Engineer and the Application Engineer groups.

## Configuring Point of Control

The following configuration steps are required to use the Point of Control functionality:

1. Responsibility Configuration.

This configuration is used to decide the permissions that will be handled using the Point of Control functionality. The system is delivered with a default responsibility, which is the Operation responsibility, refer to [Figure 129](#).

It is recommended to use the default responsibility. For more information, refer to [Responsibility Configuration](#) on page 159.

It is required to understand the standard security features prior to configuring the Point of Control functionality, refer to [Section 4, Security Configurations](#).

2. Section Configuration.

Configuring a section includes the following steps:

- a. Creating a section

In this step, the Process Objects are organized in hierarchies to create sections. It is important to include all relevant objects in the section to ensure proper security settings. The key point is to group all the objects that are needed for one section into one place. The sections are created directly in the existing structure by adding Section Definition aspects or by building up a hierarchy in a different structure and inserting the objects into each section. For more information about defining a section, refer to [Creating a Section](#) on page 164.

- b. Configuring the section

In this step, it is configured which users are allowed to request responsibility for a section and from which nodes. For information about configuring the Section Definition aspect, refer to [Configuring a Section](#) on page 166.

3. Set up required permissions for Release and Grab responsibility

Assign the Release and Grab permissions to the required groups or users. This setting is configured using the relevant Security Definition aspect.

It is recommended to provide the Release permission to all users and the Grab permission only to selected operators. For information about transferring responsibility of a section, refer to *System 800xA Operations 5.1 (3BSE036904\*)*.

4. Alarm List Responsibility Filter Configuration (Optional)

In this step, the Alarm and Event Lists are configured to enable filtering of alarms based on the responsibility.

For more information about the Responsibility filter configuration, refer to [Alarm List Responsibility Filter Configuration](#) on page 171.

5. Alarm Mapping Configuration (Optional)

All alarms are by default mapped to the Operation responsibility. For information on how to modify the default setting, refer to [Alarm Mapping](#) on page 173.

## Responsibility Configuration

The Responsibility Configuration aspects are located in the Admin structure under **Administrative Objects > Inventory Objects > Responsibility**. This aspect is used to modify or create Permission Sets. A Permission Set contains the Permissions that are granted to the Responsible User. These permissions are at the same time denied to all other users within the section.

In this configuration, security audit for a permission can also be enabled. For more information about audit, refer to [Section 4, Security Configurations](#).

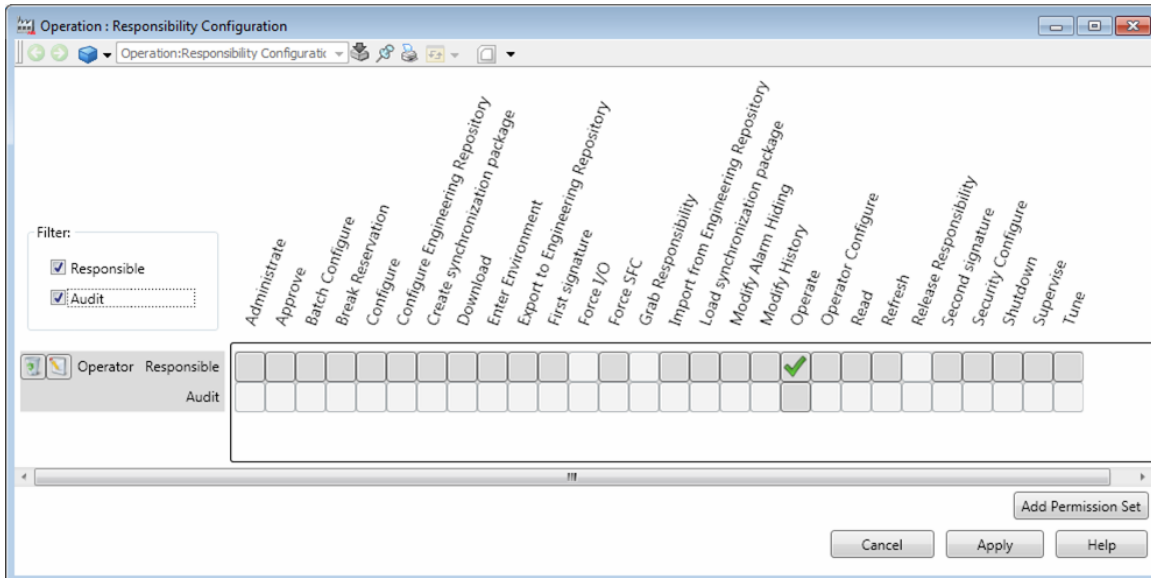


Figure 129. Default Responsibility Configuration

### Modify a Permission Set

The default Operation responsibility has an Operator Permission Set with only the Operate permission configured. This default can be modified to include additional permissions required by the operator. For example, the Tune permission can be given to the operators, refer to [Figure 130](#).

The effect of this configuration is that the Responsible User will be granted the Operate and Tune permissions while all other users will be denied on these permissions.



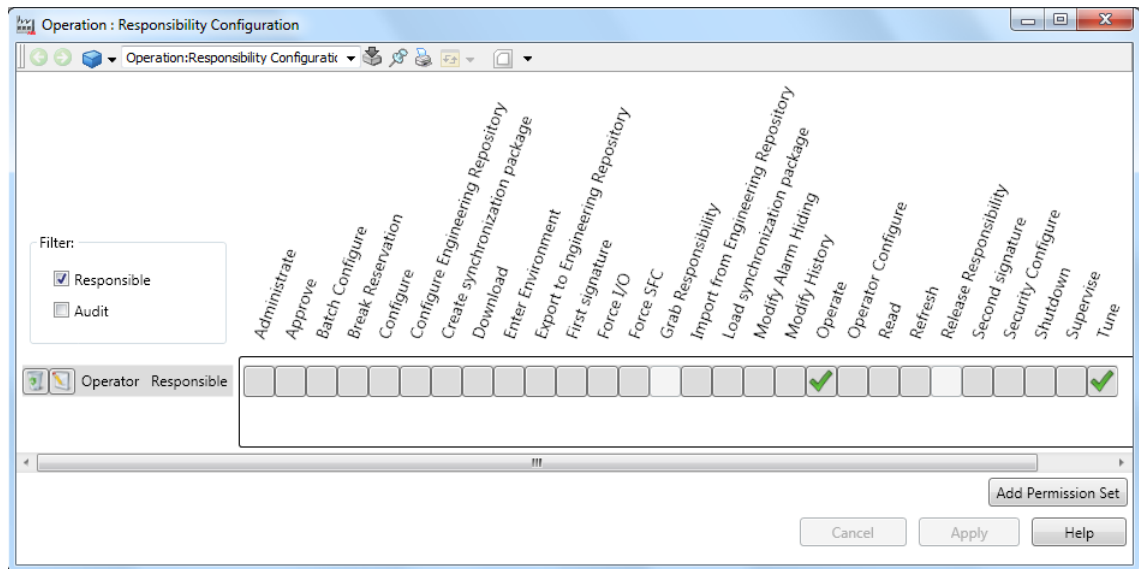


Figure 130. Additional Permissions

### Add a Permission Set

In certain situations, when there is a need for some of the operators (such as Maintenance Operator) to have more permissions to operate the section, an additional Permission Set can be created.

The following procedure gives a workflow for creating a new Permission Set with the additional permissions:

1. Select the **Responsibility Configuration** aspect on the Operation object.
2. Select the **Responsible** check box in the Filter to configure the permissions.
3. Click **Add Permission Set**.
4. Enter a **Permission Set Name** and **Permission Set Description** in the pop-up window, and then click **OK**.

- To configure the Permission Set, select the necessary permissions from the grid, for example, select **Operate** and **Tune**, refer to [Figure 131](#).

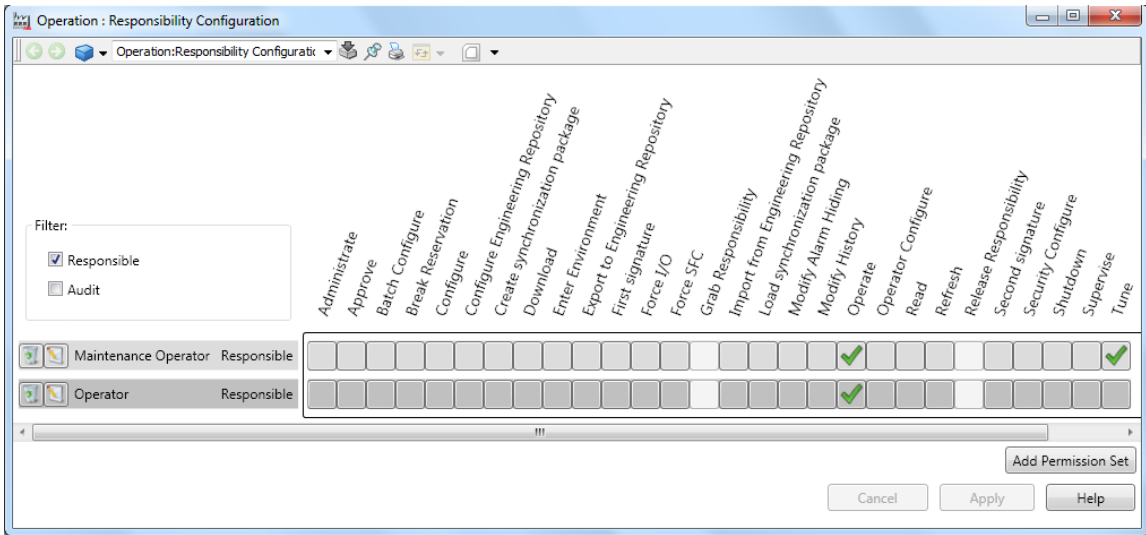


Figure 131. Modifying Responsibility

- Click **Apply**.

The Point of Control functionality will now deny the **Tune** permission for all other users that are not Maintenance Operators. The Section Definition aspect configures the Permission Sets to use for that section. For more information, refer to [Section Configuration](#) on page 164.

### Advanced Configuration

When there is a need for different users with varied permissions to simultaneously work on a section, multiple responsibilities must be configured for that section. These responsibilities can then be held at the same time by different users. For example, to create a System responsibility, perform the following steps:

- Navigate to the **Admin Structure > Administrative Objects > Inventory Objects > Responsibility**.

2. Create a new object of the type Responsibility. Enter a name for the object for example, System.
3. Select the **Responsibility Configuration** aspect on the System object.
4. Select the **Responsible** check box in the Filter to configure the permissions.
5. Click **Add Permission Set**.
6. Enter a **Permission Set Name** and **Permission Set Description** in the pop-up window, and then click **OK**.
7. To configure the Permission Set, select the necessary permissions from the grid, for example, select **Shutdown**, refer to [Figure 132](#).
8. Click **Apply**.

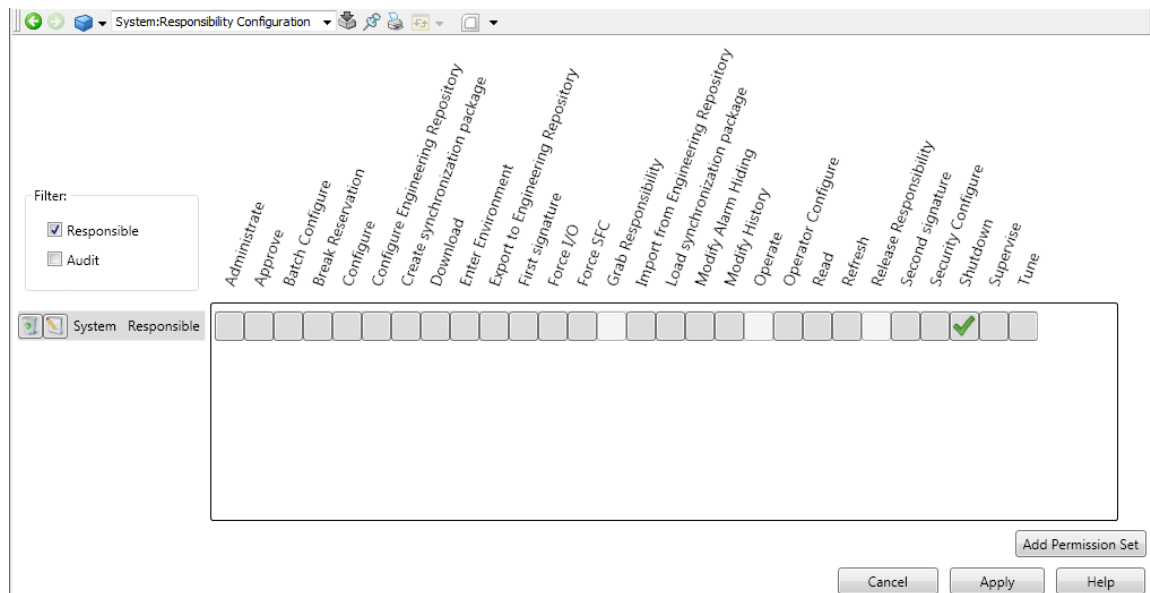



Figure 132. Configure Permissions




Two Responsibilities cannot control the same permissions, that is, an overlap of a permission is not allowed.

### Edit or Delete a Permission Set

To edit or delete any Permission Set configured in the system:

1. Navigate to the Responsibility object in the Admin Structure and open the **Responsibility Configuration** aspect.
2. Select the Permission Set to edit or delete.
3. Click the **Edit** button  next to the Permission Set name to make any changes to the Permission Set name or description.

or

Click the **Trashcan** button  next to the Permission Set name to delete the Permission Set.

4. Confirm the changes to the Responsibility in the Confirmation dialog box.

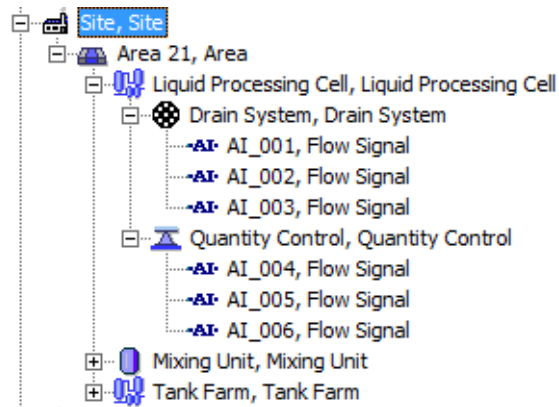
## Section Configuration

The Section Configuration includes the following steps:

### Creating a Section

Group the objects that should be part of the section in a hierarchy, ensuring that all the relevant process objects are included. Create a Section Definition aspect on the root object of the hierarchy.

The aspect objects under the section definition aspect are part of the section, refer to [Figure 133](#).

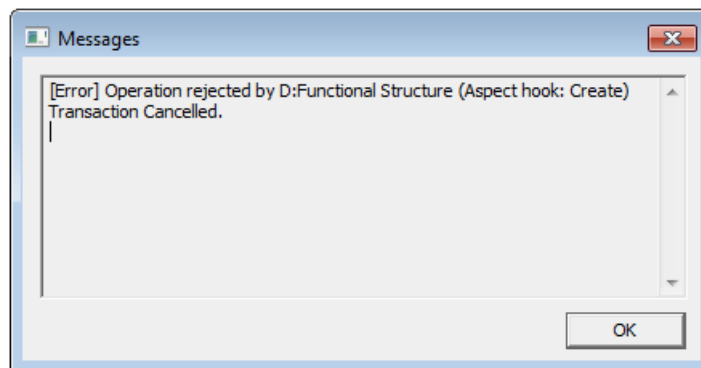


*Figure 133. Sections Defined in the Functional Structure*

It is also possible to add Section Definition aspects to objects that are part of this section, this will then create new sections within the section, refer to [Figure 133](#). Different users can be responsible for different sections.



An object can belong to only one section. An attempt to insert an object into two sections will throw an error message as in [Figure 134](#).



*Figure 134. Error Message*

## Configuring a Section

To configure a section:

1. Create a Section Definition aspect on the top object of a section (refer to [Figure 135](#)).



A Point of Control Security aspect is automatically created with the Section Definition aspect. This aspect works as a standard Security Definition aspect and defines the permissions for the section. It dynamically changes the permission of the section when the responsibility changes and can be used to verify the configuration of the section. For information about the standard Security Definition aspect, refer to [Section 4, Security Configurations](#).

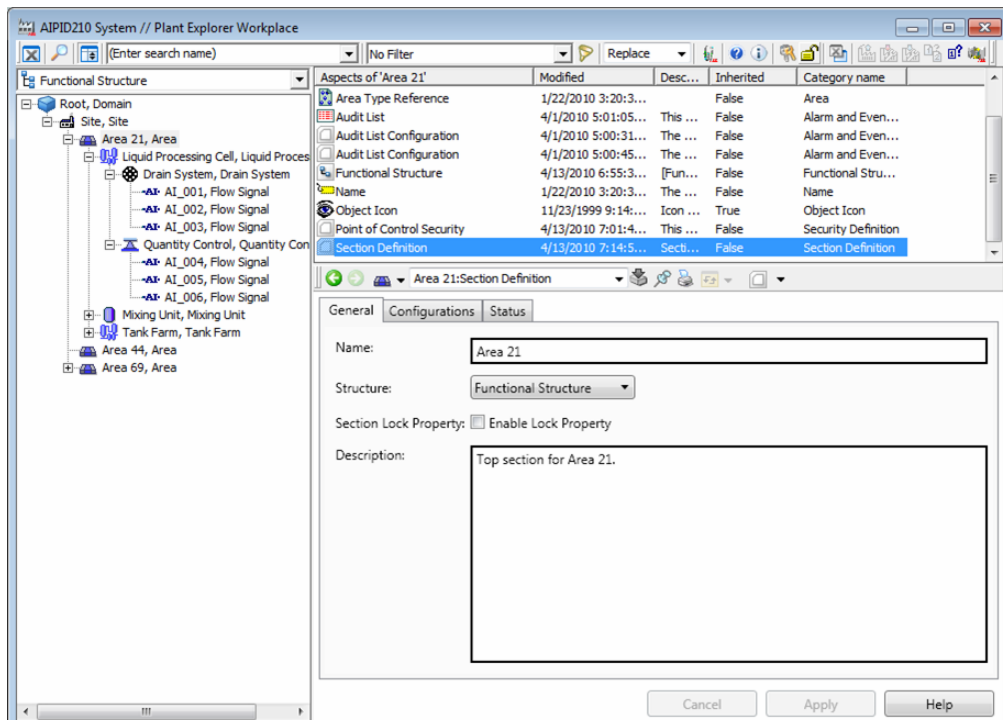


Figure 135. Section Definition Configuration



If a section is defined above an object in another structure that is already within a section, an error message as in [Figure 136](#) is displayed.

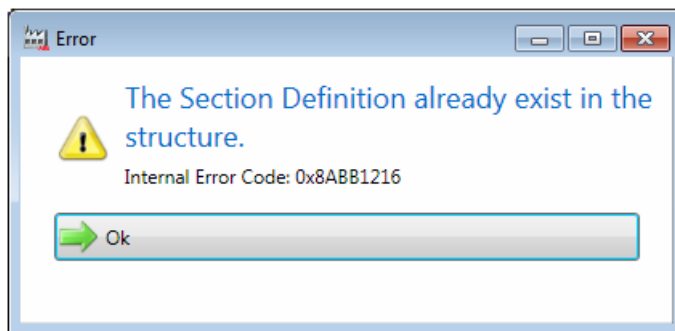


Figure 136. Error Message - Section Definition

2. Select the **Section Definition** aspect.

### Basic Configuration

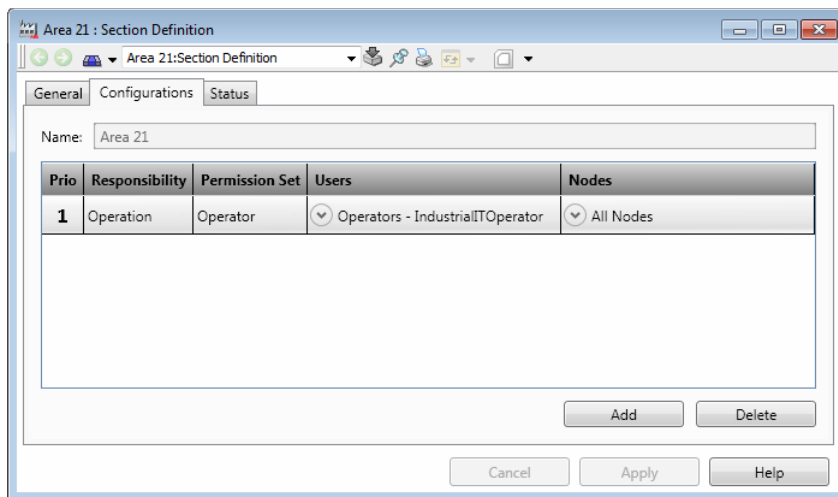
The **General** tab includes the basic configuration of the section.

- a. Enter a **Name** and **Description** for the section (refer to [Figure 135](#)).  
The name of the section is by default the name of the object on which the aspect is created.
- b. If the object exists in multiple structures, select the structure the section should be part of.
- c. Optionally, select the **Section Lock Property** check box. Click **Browse** to select the OPC property that will be used to lock the section. For more information about section lock, refer to [Section Lock](#) on page 175.

### Section Responsibility Configurations

The **Configurations** tab on the Section Definition aspect is used to configure the possible responsibilities for the section. Each configuration row holds a

Priority, Responsibility, a Permission Set, a set of Users, and Nodes, refer to [Figure 137](#).



*Figure 137. Section Definition Configurations Tab*

When a user requests responsibility of a section, the Point of Control functionality finds the first configuration that matches the user and the node.

- a. Click **Add** to include a new configuration.
- b. In the **Responsibility** column, select the responsibility. The Operation responsibility is selected by default.
- c. In the **Permission Set** column, select the required permission set. The Operator permission set is selected by default.
- d. In the **Users** column, the users that are allowed to take the responsibility for the section is configured.
- e. In the **Nodes** column, the nodes from which the responsibility can be taken and the nodes where the responsible user can operate from is configured.
- f. Click **Apply**.



Figure 138 shows an example of an advanced configuration of the Section Definition aspect with multiple responsibilities. If Operator 1 requests the Operation responsibility, the user will be assigned an **Allow** on all permissions in the Maintenance Operator Permission Set for all nodes in the Control Room and Pump Station node groups. All other users will have **Deny** on all permissions in the Maintenance Operator permission set for all nodes.

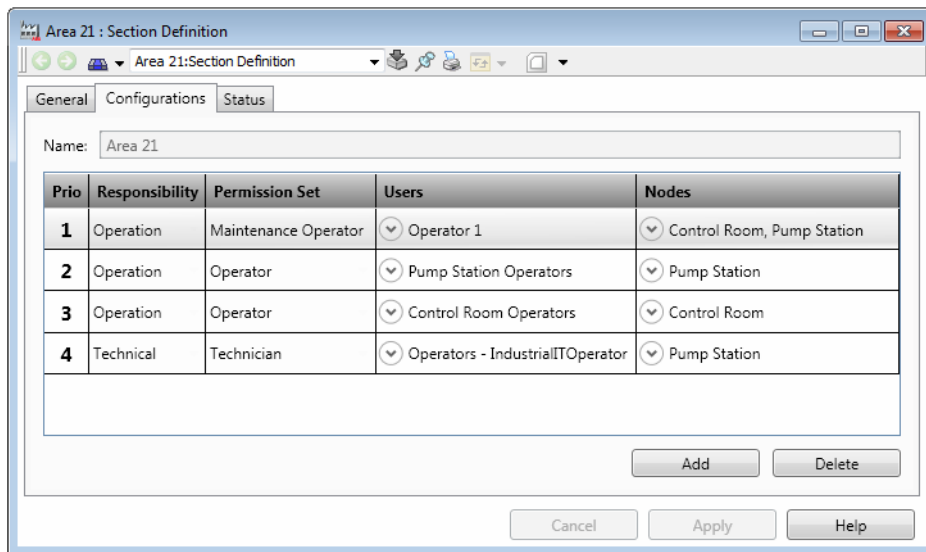


Figure 138. Section Definition with Multiple Responsibilities

The **Prio** column decides in which order each row will be evaluated during a request for responsibility. It is used to affect which permission set is assigned to the requesting user. The priority can be changed by a drag and drop in the **Prio** column.

### Section Status

The **Status** tab displays information about the responsibilities taken on the section, refer to [Figure 139](#). It displays the information about the responsible user that took the responsibility and the node it was taken from.



The **Responsible Node** column indicates the node from where the responsibility was taken and not from where the Responsible User can operate. To see this, refer to the **Nodes** column on the **Configurations** tab.

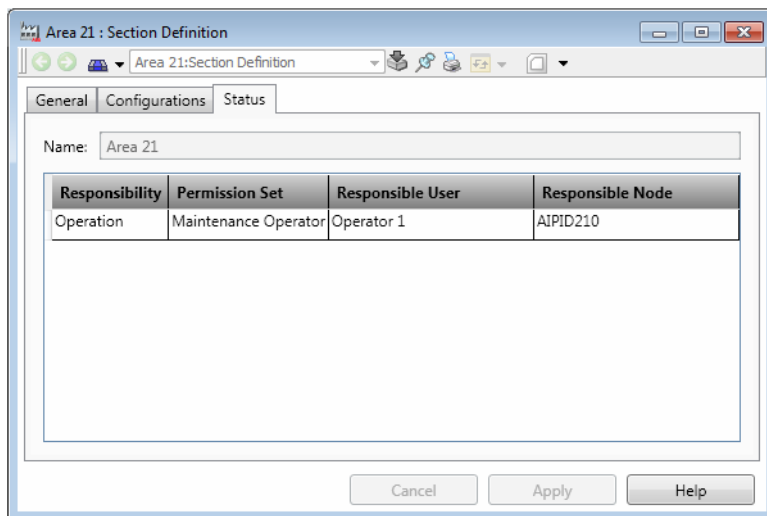


Figure 139. Section Definition Status Tab

## Alarm List Responsibility Filter Configuration

An alarm list can be configured so that only the Responsible User can view the alarms.



The default Alarm and Event List must not be modified. Create a copy of the Alarm and Event list and modify the copy to include the Responsibility filter.



If the Responsibility filter is used, it is recommended to configure an Alarm List with the Responsibility filter disabled, which can be used in any emergency situation.

To configure the responsibility filtering:

1. Select **Filter > Area** on the Main View of the aspect, refer to [Figure 140](#).

The following Responsibility filters are provided:

- a. Responsible.

When this filter is selected, the alarm list shows the alarms that the operator is responsible for.

- b. Responsible and not responsible by anyone.

When this filter is selected, the alarms list shows the alarms that the operator is responsible for (as in [Step a](#)) and the alarms that no user is responsible for.

- c. All.

The Responsibility filter is disabled, that is, all the alarms are displayed.

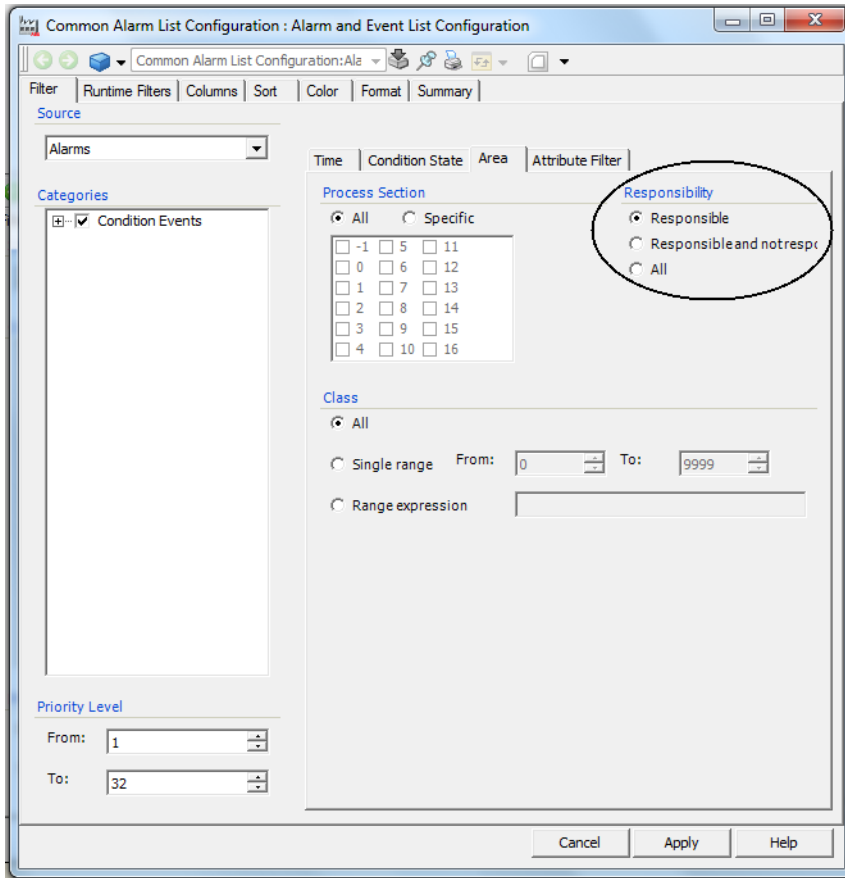


Figure 140. Alarm List Configuration

The following alarm attributes are related to Point of Control:

- Responsibility
- ResponsibilityID
- ResponsibilitySection
- ResponsibleNode

- ResponsibleUser
- ResponsibleUserID

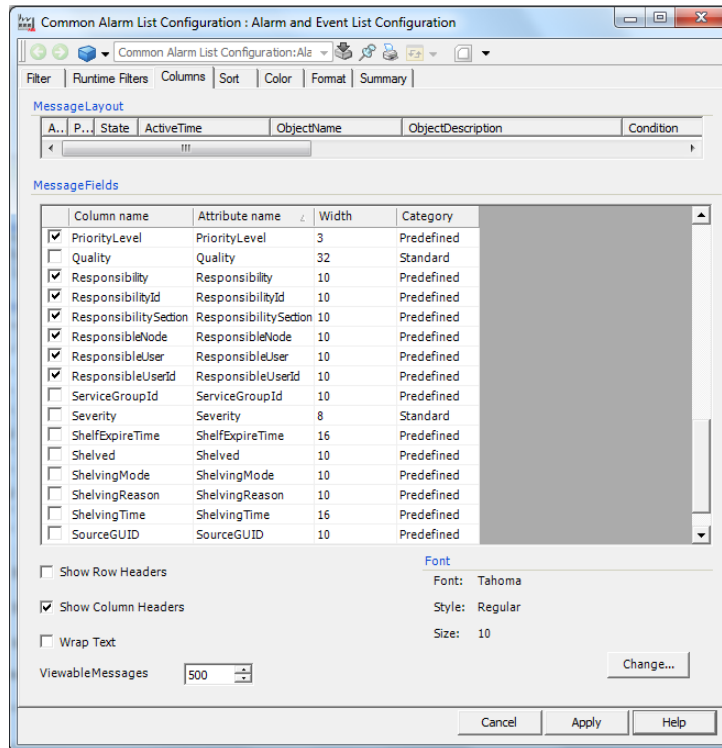


Figure 141. Point of Control related Alarm Attributes

## Alarm Mapping

All the alarms for a section are by default mapped to the Operation responsibility.

For advanced configurations, when more than one responsibility is configured in the system, all alarms needs to be mapped to the correct responsibility.

To map the alarms to different responsibilities:

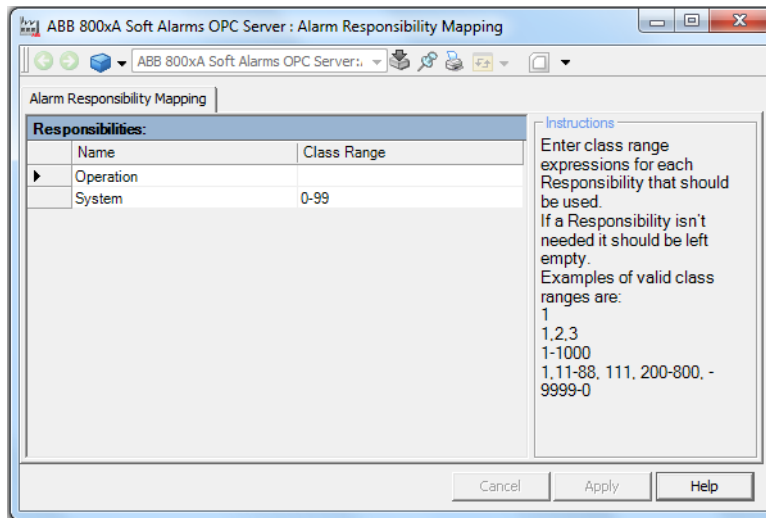
1. In the Plant Explorer, navigate to the **Library Structure > Alarm & Event > Alarm Collection Definitions > [Alarm Server object]**.

2. Select the **Alarm Responsibility Mapping** aspect.

The Alarm Responsibility Mapping aspect displays the responsibilities in the system. If more than one responsibility is configured, the alarms can be mapped to different responsibilities using the Class attribute.

For example, to map alarms to the System responsibility, in the Alarm Responsibility Mapping aspect (refer to [Figure 142](#)), for the System responsibility, enter a Class Range of **0-99**.

All the alarms for the selected section with a class range value between 0 and 99 will be displayed for the user having the System responsibility.



*Figure 142. Responsibility Mapping*

Alarms that are not mapped to any responsibility will be, by default, mapped to the Operation responsibility.

## Section Lock

The Section Lock functionality temporarily disables the transfer of responsibility. For information about transfer of responsibility, refer to *System 800xA Operations 5.1 (3BSE036904\*)*. This is useful when performing certain important tasks that must not be interrupted by a request for responsibility or an accidental release.

In the **General** tab, it is possible to specify the section lock property (Figure 143). If the **Enable Lock Property** check box is selected, the user can configure what property to use to lock the section in the Section Definition aspect.

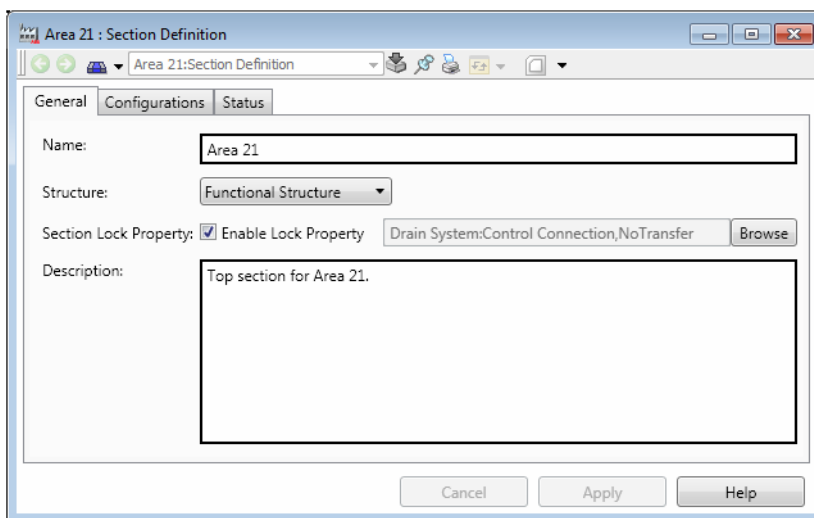


Figure 143. Section Lock

The section is locked when the boolean property is true. When a section is locked, other users will not be allowed to request responsibility of the section.



The OPC property is normally defined and set by the control application. Section lock is different from process object lock.

The Grab responsibility protocol overrides the section lock functionality, that is, a user with the Grab permission can take over the responsibility of a locked section. For information about the Grab responsibility, refer to *System 800xA Operations 5.1 (3BSE036904\*)*.

## OPC Properties

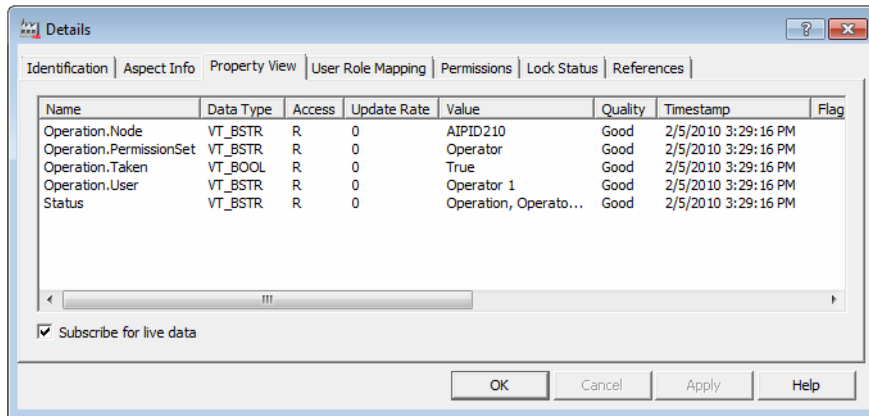
The OPC properties available on the Section Definition aspect can be used to create graphic displays showing the responsibility status of a section.

There are five OPC properties available on the Section Definition aspect as shown in [Table 10](#).

*Table 10. OPC Properties on the Section Definition Aspect*

OPC Property	Description
Operation.PermissionSet	This string property holds the information about what Permission Set is currently used for the Operation responsibility on the selected section.
Operation.Node	This string property holds the name of the node from which the Operation responsibility was taken for the section.
Operation.User	This string property holds the name of the user that currently has the Operation responsibility for the section.
Operation.Taken	This Boolean property is set to true if the Operation responsibility is taken for this section.
Status	This string property holds the information about the different responsibilities taken. It contains the same information that is visible on the Status tab on the Section Definition aspect. It is a long string with semicolon used as a delimiter between responsibilities and comma as a delimiter between fields. The information is presented in the following order: Responsibility, Responsible User, Responsible Node; Responsibility, Responsible User, Responsible Node; and so on.





Name	Data Type	Access	Update Rate	Value	Quality	Timestamp	Flag
Operation.Node	VT_BSTR	R	0	AIPID210	Good	2/5/2010 3:29:16 PM	
Operation.PermissionSet	VT_BSTR	R	0	Operator	Good	2/5/2010 3:29:16 PM	
Operation.Taken	VT_BOOL	R	0	True	Good	2/5/2010 3:29:16 PM	
Operation.User	VT_BSTR	R	0	Operator 1	Good	2/5/2010 3:29:16 PM	
Status	VT_BSTR	R	0	Operation, Operato...	Good	2/5/2010 3:29:16 PM	

Figure 144. OPC Property View

The Details view (Figure 144) of the Section Definition aspect shows the OPC properties and the corresponding values.








---

## Section 7 Security Examples

### Default Security Setting of the Admin Structure

The Admin Structure is protected by a Security Definition aspect added to the root object “Administrative Objects”. **The settings in this aspect are done to protect the Admin Structure.** See the settings on delivery in [Figure 145](#). For example all members of the IndustrialITUser group defined in Windows are by default given the permission to Read.

Permission	Access	User or Group	Node
 Read	Allowed	Everyone - PPADC04\Ind...	All Nodes
 Configure	Allowed	Application Engineers - PP...	All Nodes
 Enter Environment	Allowed	Everyone - PPADC04\Ind...	All Nodes
 Administrate	Allowed	System Engineers - PPAD...	All Nodes
 Security Configure	Allowed	System Engineers - PPAD...	All Nodes

*Figure 145. The Security Definition Aspect for the Admin Structure*

As a member of the Administrators group in 800xA System you can change the default settings in the Admin Structure.



Changes in the Admin Structure affect the security. Allow only a limited number of people permission to change this structure.

### The Default Security Setting of a System Object

For each created system there is a system object. Its name is by default **<nodename> system**, but the name can be freely chosen when the system is created.

In the Security Definition aspect for this object, **default security** is set for the created system. After creation of a system the default settings are as shown in Figure 146.

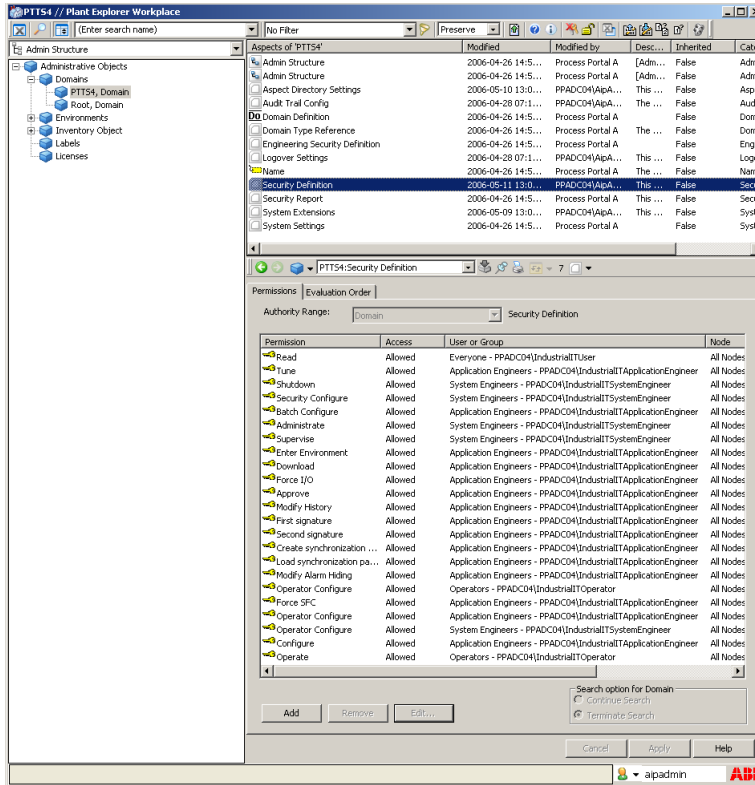


Figure 146. The Default Security Settings in the System Root Object in the Admin Structure

Below is an example of how to reconfigure the Default Security Settings. According to this example you can redefine the Default Security aspect setting in such a way, that your basic demands on security are met.



You need Security Configuration permission to be allowed to change the Default Security Settings.

First access the system's security definition aspect and reconfigure it:

1. Go to the Admin Structure in Plant Explorer and select the created system. Its name is the name of the server node, or the name given when the system was created.
2. Select the Security Definition aspect and its **Permissions** tab.
3. The next step is to set Allowed only for personnel that must perform that type of operation. In this system only two persons must have Operate permission, so delete the Operate line by selecting it and clicking on the **Remove** button. Then you click **Add** and insert the group of persons, that are allowed to Operate the system.

Permission	Access	User or Group	Node
Read	Allowed	Everyone - PPADC04\IndustrialITUser	All Nodes
Tune	Allowed	Application Engineers - PPADC04\IndustrialITApplicationEngineer	All Nodes
Shutdown	Allowed	System Engineers - PPADC04\IndustrialITSystemEngineer	All Nodes
Security Configure	Allowed	System Engineers - PPADC04\IndustrialITSystemEngineer	All Nodes
Batch Configure	Allowed	Application Engineers - PPADC04\IndustrialITApplicationEngineer	All Nodes
Administrate	Allowed	System Engineers - PPADC04\IndustrialITSystemEngineer	All Nodes
Supervise	Allowed	System Engineers - PPADC04\IndustrialITSystemEngineer	All Nodes
Enter Environment	Allowed	Application Engineers - PPADC04\IndustrialITApplicationEngineer	All Nodes
Download	Allowed	Application Engineers - PPADC04\IndustrialITApplicationEngineer	All Nodes
Force I/O	Allowed	Application Engineers - PPADC04\IndustrialITApplicationEngineer	All Nodes
Approve	Allowed	Application Engineers - PPADC04\IndustrialITApplicationEngineer	All Nodes
Modify History	Allowed	Application Engineers - PPADC04\IndustrialITApplicationEngineer	All Nodes
First signature	Allowed	Application Engineers - PPADC04\IndustrialITApplicationEngineer	All Nodes
Second signature	Allowed	Application Engineers - PPADC04\IndustrialITApplicationEngineer	All Nodes
Create synchronization ...	Allowed	Application Engineers - PPADC04\IndustrialITApplicationEngineer	All Nodes
Load synchronization pa...	Allowed	Application Engineers - PPADC04\IndustrialITApplicationEngineer	All Nodes
Modify Alarm Hiding	Allowed	Application Engineers - PPADC04\IndustrialITApplicationEngineer	All Nodes
Operator Configure	Allowed	Operators - PPADC04\IndustrialITOperator	All Nodes
Force SFC	Allowed	Application Engineers - PPADC04\IndustrialITApplicationEngineer	All Nodes
Operator Configure	Allowed	Application Engineers - PPADC04\IndustrialITApplicationEngineer	All Nodes
Operator Configure	Allowed	System Engineers - PPADC04\IndustrialITSystemEngineer	All Nodes
Configure	Allowed	Application Engineers - PPADC04\IndustrialITApplicationEngineer	All Nodes
Operate	Allowed	PPADC04\opr1	PTT54ID1
Operate	Allowed	PPADC04\opr2	PTT54ID1

Figure 147. Changed Default Security Definition Setting

As you can see from there are two groups that have Operate permission from a specific node (Workstation).

## Security Setting on an Aspect Object Basis

You can very easily set protection for a specific Aspect object in 800xA. You only have to add a Security Definition aspect to the object and set Authority Range to Object. This means that this aspect setting is valid only for the object. Every setting of permission will be valid only for the object.

If you then set the Search Option for Object to:

- Continue Search**  
 For groups of persons and persons that have no setting for the permission checked, the search will go on in other structures according to the Evaluation Order setting.
- Terminate Search** (as shown in the image)  
 For groups of persons and persons that have no setting for the checked permission, everything is **denied** regarding this object.

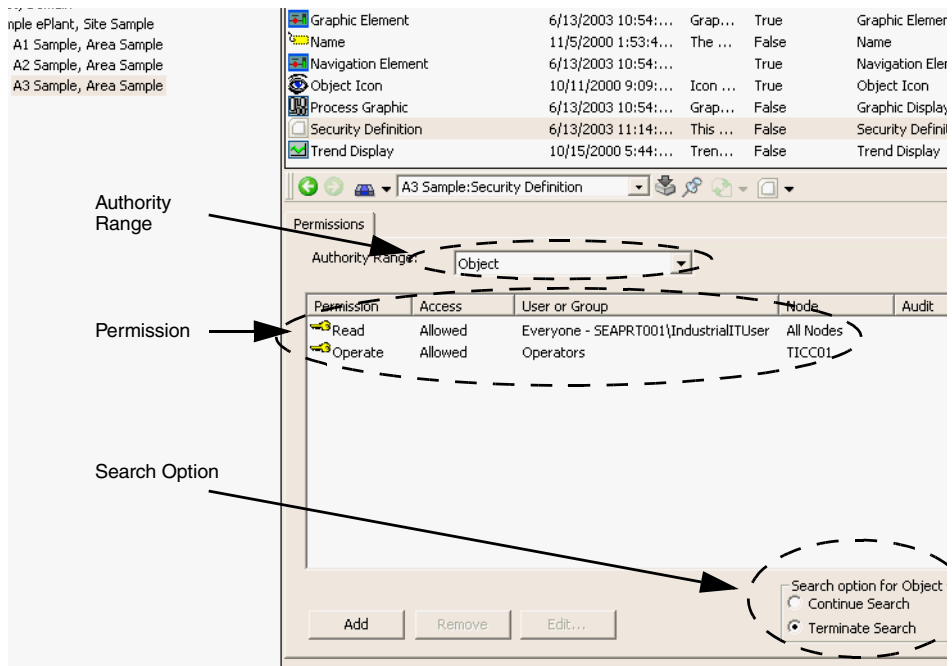


Figure 148. Security Definition Aspect Setting for an Aspect Object



If Read permission is omitted in this security definition everyone is denied access by the implicit deny rule.

### Different Settings of Structure in Authority Range

If an object is inserted twice in a structure, ensure that the structure setting is valid for each insertion and has different security and settings.

Observe that you must select the right Functional Structure object in the Authority Range to get the desired function. If you select the one according to [Figure 149](#), you set the “other” users permissions to the Emergency Valve. “Other” users are those users not explicitly granted permissions in the Security Definition.

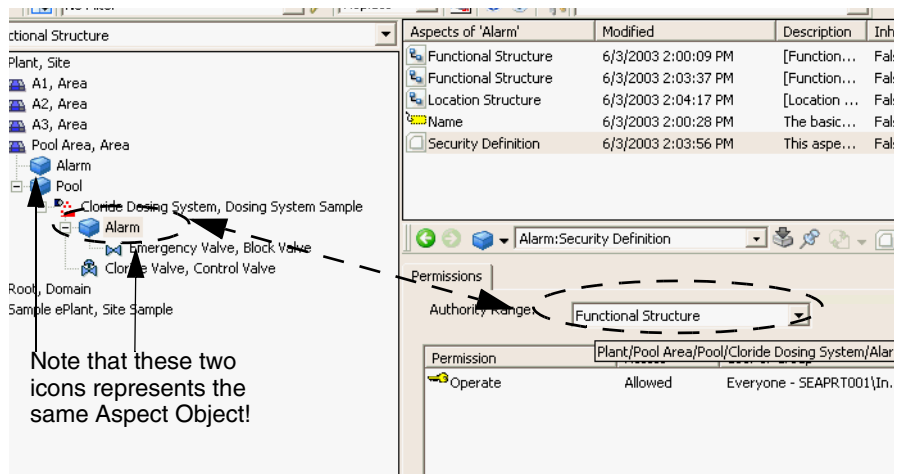


Figure 149. Functional Structure - Authority Range



If a path gives a denied permission, then the object will have denied permission.

Administrate	Denied
Read	Allowed
Operate	Allowed
Shutdown	Denied
Security Configure	Denied
Configure	Denied
Tune	Denied

Figure 150. Permission for Guest Users



Observe that the two Alarm Aspect Objects shown in the Functional Structure are the **SAME OBJECT** inserted twice in the structure!

If choosing the upper Alarm object instead, according to [Figure 151](#), other users' permissions to the Emergency Valve will be as shown in [Figure 152](#).

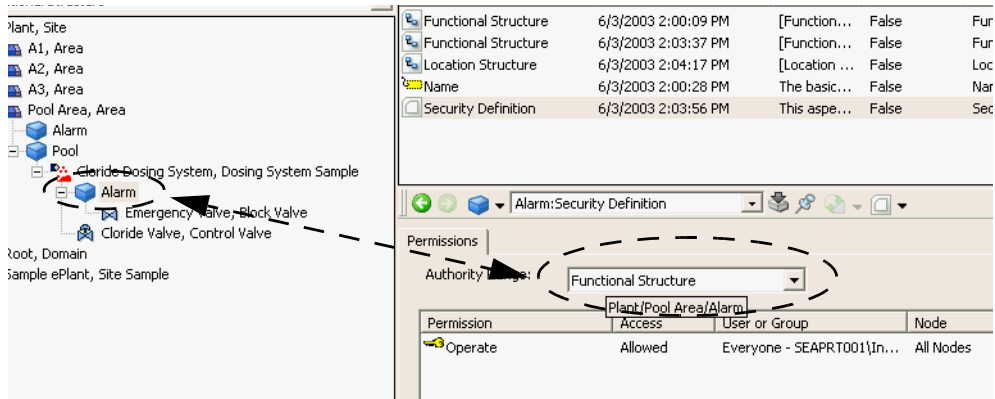


Figure 151. Functional Structure - Authority Range

Security settings for SEABBVSTW5848\Guest:

Permission	Type
✗ Administrate	Denied
🔑 Read	Allowed
✗ Operate	Denied
✗ Shutdown	Denied
✗ Security Configure	Denied
✗ Configure	Denied
✗ Tune	Denied
✗ Batch Configure	Denied

Figure 152. Permission for Guest Users

As you can see changing the position of the object in the Functional Structure within the Authority Range completely changes the authority.

When the Functional Structure object for the upper object is set, the Operator permission is denied to other users. When the lower is selected, the Operator permission is allowed.



---

## Section 8 System Services



Note that a member of the System Engineer group must configure the system services.

A service provides a function in the system, for example, the Aspect Directory service and the Alarm and Event service. One or more services can run on a server node.

A service consists of one or more non-overlapping service groups. Each service group is further divided into service providers that is, the server nodes. Each provider in a group provides exactly the same function, that is, if there is more than one service provider in a service group the service is redundant or parallel. Redundant or parallel service providers always run on different server nodes.

A client of a service does not see the service as a division of groups and providers but one uniform function to which its addresses its request.

### Unique Naming of Service Groups

If several Service Groups belonging to the same Service Type are used, ensure that each Service Group has a unique name. This simplifies troubleshooting in the System Status Viewer and during configuration.

### History

The History Source aspect is used to define the service group that shall handle a subset of logs, that is, the Log Configurations on all child objects. This functionality enables distribution of the History Service among the service group in the system. It is possible to have one group handling one control network and another handling another control network.

In the History Source aspect view it is permissible to select one of the configured service groups.

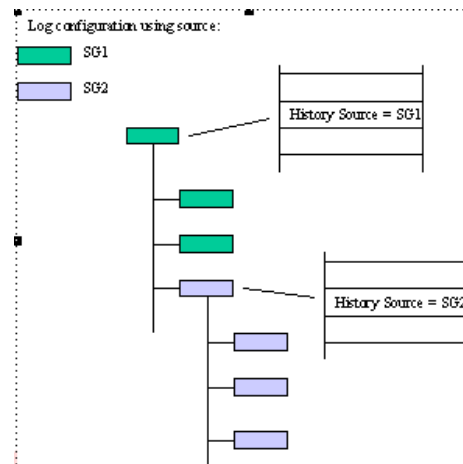


Figure 153. History Source for Different Log Configurations

The history source will impact logs that are configured as child objects of the parent log as described in [Figure 153](#).



Note that if no history source has been defined no logging will occur.



It is recommended to include the History Source aspect and choose Service Group as early as possible in the engineering process.

Updating the History Server for a Service Group change can take long time for large configurations. All logged data will be lost during change of Service Group for associated log configurations.

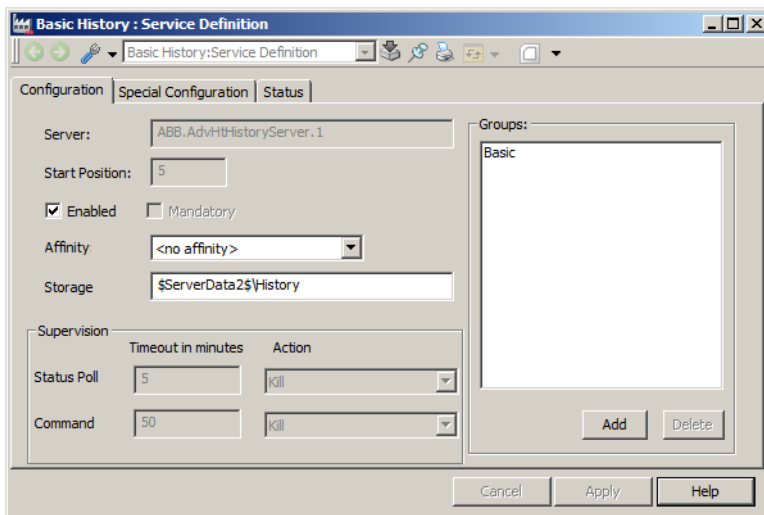


Figure 154. History Source dialog box

The special configuration (**Service Structure > Basic History, Service > Service Definition > Special Configuration tab**) of the History Service is used to specify in which structures objects shall be logged. A History Source aspect can be placed in any structure that has been defined to support log configuration. It is also possible to specify the priority order for the different structures.

If an object exists in several structures, the priority order specified in the special configuration of the History Service will be used to locate the History Source aspect.



It is recommended to specify history sources in the control structure if the objects exist in that structure.

## History Server Provider Metrics

The list of History Server provider metrics can be found at the following location:

**Service Structure > Basic History, Service > Basic, Service Group > Basic History\_Basic\_<ABC>, Service Provider > Provider Metrics, Service Status Object > Service Provider Status > Property View**

Table 11 provides the list of provider metrics and the description of each metric.

Table 11. History Server Provider Metrics

Metric	Description
ActiveAdviseRequests	Shows the number of active advised read requests. An advise request makes a subscription for the new data from the OPC HDA server and notifies the History Server when it has been terminated by a client. This count will be decremented when a client terminates the read request.
AdvisePoints	Shows the number of new data points sent by the History Server from the start time to the current time.
AdvisePointsPerSecond	Shows the number of new data points sent per second by the History Server from the start time to the current time.
AverageReadRequestTime	Shows the average time it takes to handle read requests for a log, in milliseconds. It includes the deleted read requests also.
CurrentAverageReadRequestTime	Shows the average time it takes to handle read requests for a log, in milliseconds, for the last hundred read requests.
Logs	Shows the number of logs (both enabled and disabled logs) referring to the current History Server.
DirectLogs	Shows the number of property logs referring to the current History Server.
ElapsedTime	Shows the elapsed time in seconds, from the start of taking the log read statistics.
EnabledDirectLogs	Shows the number of enabled property logs referring to the current History Server.
EnabledLogs	Shows the number of enabled logs referring to the current History Server.
EnterServiceTime	Shows the date and time when the History Server has entered the Service State.

Table 11. History Server Provider Metrics (Continued)

<b>Metric</b>	<b>Description</b>
FlushedCycles	Shows the number of times the logs have been flushed.
ItemReadRequests	Represents the number of items requested for reading.
ItemReadRequestsPerSecond	Represents the number of item read requests per second from the History Server from the start time to the current time.
LogMgrQueueLength	Represents the collective size of the backup restore, collection, configuration object, History Server, and synchronizer message queues.
LogsLoadedTime	Shows the end time of loading of all the log files found in the History Server log directory.
MaxReadRequestTime	Shows the maximum time taken, in milliseconds, to handle a read request.
PercentSynchronized	Shows the percentage of synchronization between the redundant History Servers.
ReadFromFileCount	Shows the number of times the log file read operation is performed.
ReadPoints	Shows the number of points read from the History Server.
ReadPointsPerRequest	Shows the average number of points read for a request.
ReadPointsPerSecond	Shows the number of points read per second from the History Server from the start time to the current time.
ReadRequests	Shows the number of read requests received.
ReadRequestsPerSecond	Shows the number of read requests received per second from the History Server from the start time to the current time.
ReadWritePerSecond	Shows the number of read and write operations performed for history logs per second.
RemainingChangedLogs	Shows the number of deleted logs plus the number of changed logs by the log manager.

Table 11. History Server Provider Metrics (Continued)

Metric	Description
StoredExtendedPoints	Shows the number of times at least one point has been extrapolated to a log.
StoredHierarchicalPoints	Shows the number of stored points to the Basic History Hierarchical logs from the start time to the current time.
StoredRawPoints	Shows the number of stored points to Basic History Direct logs from start time to current time.
StoredRawPointsPerSecond	Shows the number of stored points to Basic History Direct logs per second from start time to current time.
WriteToFileCount	Shows the number of times the log file write operation is performed.

### Examples

The following examples provide a description of how to utilize the provider metrics for the Basic History Server.

#### Example 1

A value continuously a bit over zero for *LogMgrQueueLength* indicates that the Log Manager handling the read and write operations of the Basic History log files may encounter a performance problem.

The corrective actions can be to check if any antivirus program is scanning the log files that can decrease the performance of the system or if a faster disk can be used.

#### Example 2

If *ItemReadRequest* is higher than *ReadRequest*, each read request will contain many items such as, log files. Reading data for many items in a read request will cause a lot of reads to the disk during a short time.

To spread the reads from the disk, it is good to split each read request into more requests with less number of items in each request.

**Example 3**

Having a high value for *CurrentAverageReadRequestTime* indicates that the Basic History server has some performance problem.

## Lock Server

The Lock Server Service (found in the Service Structure) is used for handling of locks (for example, Process Object Locking) in the system.

### Process Object Locking Aspect

The Process Object Locking aspect ([Figure 155](#)) is used for configuring the Object Locking function. By default the function is disabled.

For information about the Object Locking function, refer to the *System 800xA Engineering 5.1 Process Graphics based on Visual Basic (3BSE030335\*)* instruction. The Process Object Locking aspect consist of two tabs which are described as follows:



From System Version 5.1 onwards, the System Configuration Console is available that can be used for a simplified configuration of the Process Object Lock functionality. Refer to *System 800xA 5.1 Tools (2PAA101888\*)* for more information.

## Configuration Tab

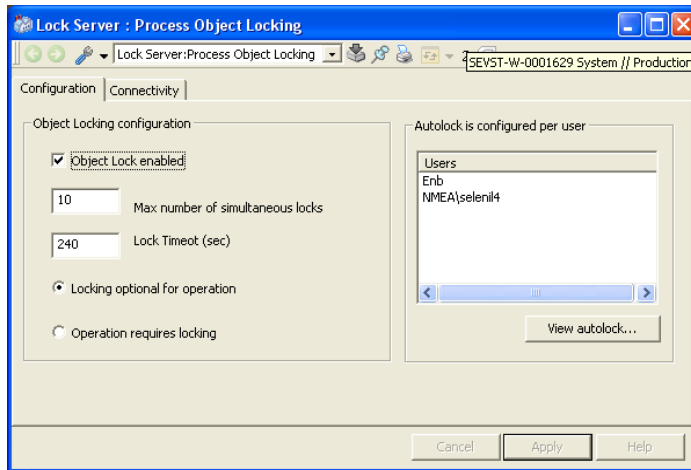


Figure 155. Lock Server Service - Process Object Locking Aspect, Configuration Tab

- Select the **Object Lock enabled** check box to enable the Object Lock function.
- Type number of locks that can be held by one user on one node at the same time in the **Max number of simultaneous locks** field. -1 specifies infinite number of locks.
- **Lock Timeout** controls how long a lock should be held. When the timeout is reached the lock will be broken. (Same value as the **Hold Timeout** in the Special Configuration tab of the Service Definition aspect)



The time specified below as one minute is not relevant.

- If the **Locking optional for operation radio button** is selected it is possible to operate without locking the object first.
- If the **Operation requires locking** radio button is selected it is required to lock the object before it is possible to operate on it.



- Autolock is configured per user. You can view and configure the settings for each user by selecting the user from the list and then click the **View Autolock** button. Refer to *System 800xA Engineering 5.1 Process Graphics based on Visual Basic (3BSE030335\*)* instruction for more information about autolock.

## Connectivity Tab

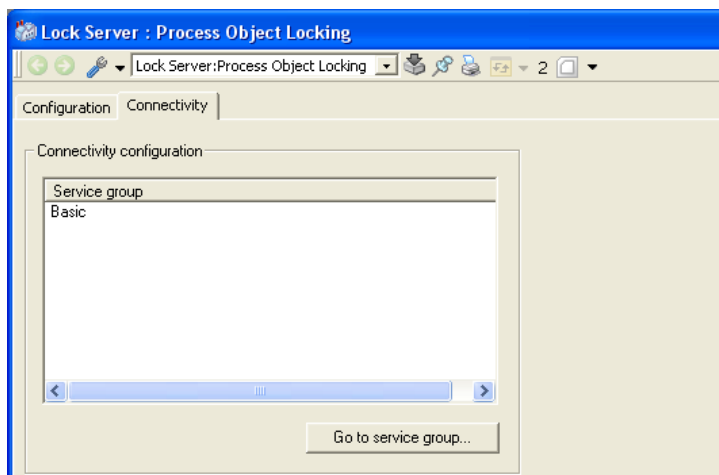


Figure 156. Lock Server Service - Process Object Locking Aspect, Connectivity Tab

It is possible to configure if the Lock Server should be used for process object locking for each connectivity in the system. The tab contains a list of the OPCDA\_Connector services' service groups. Select a service group and click the **Go to service group** button. The Service Group Definition aspect of the selected service group will open, and in the Special Configuration Tab user configures if Lock Server should be used or not. Refer to *System 800xA 5.1 Configuration (3BDS011222\*)* for more information.

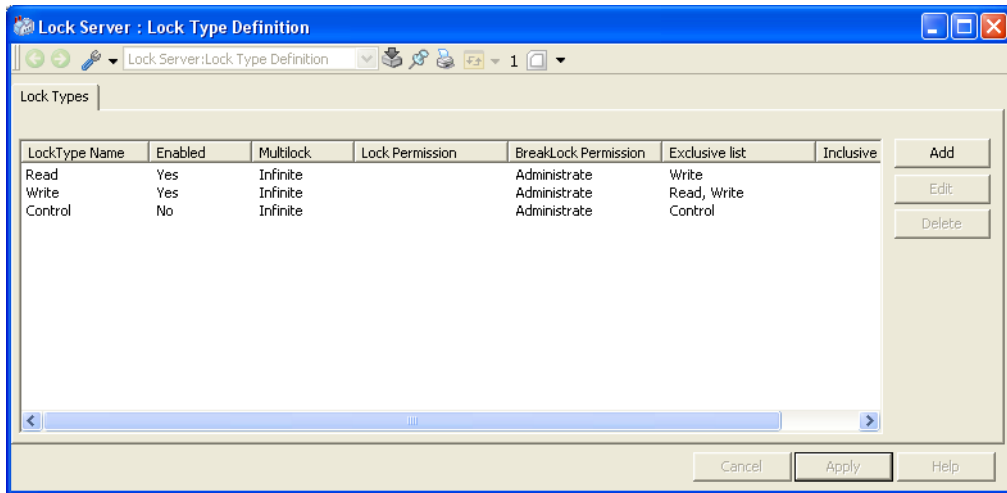


Some connectivities implements process object locking without using the Lock Server. Before changing any settings read the respective connectivity instruction.

## Lock Type Definition Aspect

There are three pre-defined lock types in the system; Read, Write and Control. The Control lock type is used for process object locking.

In the Lock Type Definition aspect, configure the lock types, refer to [Figure 157](#).



*Figure 157. Lock Server Service - Lock Type Definition Aspect*

Select a lock type and click **Edit**. In the Lock Type Configuration dialog (see [Figure 158](#)) you can configure permission to break a lock, enable/disable the lock type, set maximum numbers of simultaneous locks (-1 is infinite). For the Control lock type the enabled and multi lock settings are the same as the settings in the Process Object Locking aspect.

The Inclusive, Available and Exclusive lists should not be modified.

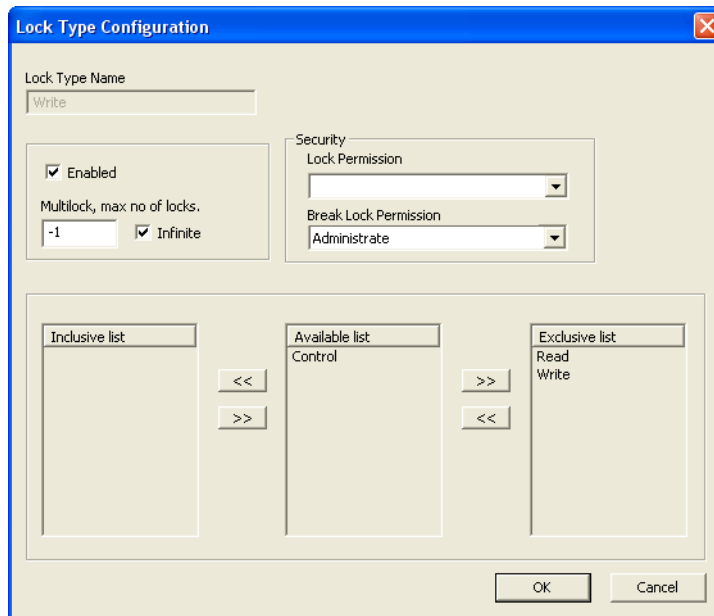


Figure 158. Lock Type Configuration Dialog Box

## Service Definition Aspect

The Special Configuration tab (see [Figure 159](#)), in the Service Definition aspect of the Lock Server object, is used for defining various timeouts.



Change the parameters in this section only when it is found absolutely necessary after an evaluation.

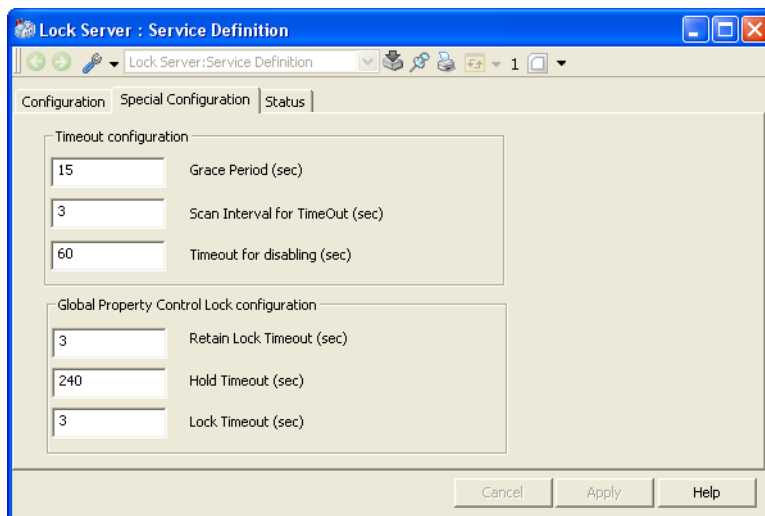


Figure 159. Lock Server Service - Service Definition Aspect, Special Configuration Tab

In the **Timeout Configuration** area you can configure timeouts in the server for:

- **Grace Period** - A grace period takes place when the server starts. Only saved locks are allowed to be sent to the server during this period. This to make sure that no new client locks a resource before all existing clients have re-entered their saved locks. It also gives the Resource Managers time to re-register themselves.
- **Scan Interval for TimeOut** - For each lock the client specifies how long it wants to wait for the lock to be granted. When this time has passed, the Lock Server will remove the lock. The **Scan Interval for timeout** value specifies how often the Lock Server will scan for timeout locks.
- **Timeout for disabling** - If the server, or connection to the server, goes down the disable timeout is started. When the timeout is reached all locks that the client holds will be broken.

In the **Global Property Control Lock configuration** area you can configure timeouts for locks that are written to the Global Properties of the Lock Server.

The Global Properties are used for process object locking (refer to [Process Object Locking Aspect](#) on page 191)

- **Retain Lock Timeout** - Sets the time for how long a lock should be held after a server failure.
- **Hold Timeout** - Sets the time for how long a lock should be held. When the timeout is reached the lock will be broken.
- **Lock Timeout** - Sets the time for how long the client will wait before the lock is granted. If the timeout is reached the lock request will be cancelled.

## Workplace Service

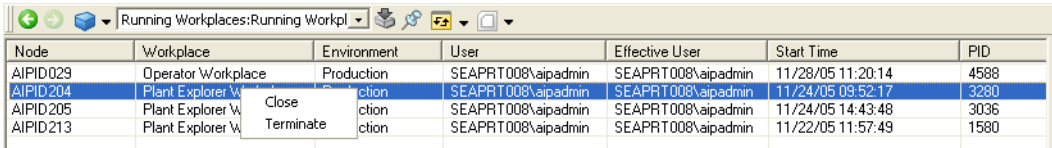
The remote navigation function makes it possible to interact remotely with other workplaces. It also provides a tracking function of running workplaces in the system.

### Tracking Function

The workplace service keeps track of all running workplaces in the system. When a workplace is started it is registered in the workplace service.

The Config View of the Running Workplace Overview aspect lists all the running workplaces in the system, where they are running and who is running them etc.

From this aspect you can close or terminate a workplace. Right-click on the workplace in the list and select **Close** or **Terminate**. Close is equivalent to clicking the **Close Workplace** button and are the preferred way to close a workplace, while Terminate kills the workplace unconditionally.



Node	Workplace	Environment	User	Effective User	Start Time	PID
AIPID029	Operator Workplace	Production	SEAPRT008\ajpadmin	SEAPRT008\ajpadmin	11/28/05 11:20:14	4588
AIPID204	Plant Explorer V	Production	SEAPRT008\ajpadmin	SEAPRT008\ajpadmin	11/24/05 09:52:17	3280
AIPID205	Plant Explorer V		SEAPRT008\ajpadmin	SEAPRT008\ajpadmin	11/24/05 14:43:48	3036
AIPID213	Plant Explorer V		SEAPRT008\ajpadmin	SEAPRT008\ajpadmin	11/22/05 11:57:49	1580

Figure 160. Running Workplace Overview Aspect - Config View

## Enable Workplace Service

Follow the steps below to enable the Workplace Service.

1. Start Plant Explorer Workplace by selecting **Start > All Programs > Industrial IT 800xA > System > Workplace**. Select Plant Explorer.
2. Go to the Service Structure.
3. Right click on the Workplace Service object and select **New Object** from the context menu.
4. Create a new object under the new Service Group object.
5. Right click on the new Basic object and select **New Object** from the context menu.
6. Create a new object of the new Service Provider.



Ensure that Service Definition aspect on the Workplace Service object is enabled.

## Remote Interaction Function



Workplace Service must be running for the Remote Interaction Function to be enabled.

With the remote interaction function you can interact remotely with the other running workplaces in the system. There are three ways to interact with another workplace remotely:

- Open an aspect view.
- Execute a verb.
- Close the workplace.



Select **Send To** from the drop-down menu to display the aspect view on another workplace. Refer to *System 800xA Operations 5.1 (3BSE036904\*)* for more information.

## Security Settings

To close a workplace remotely requires the Administrator user role.

A node can be configured to allow or disallow access from other nodes by using the security function. The default setting is disallowed.

Two operations, RemoteExecution and RemoteNavigation, are available for configuring security of Workplace Services. The default required permission for RemoteExecution is Configure, and Operate for RemoteNavigation.

Permission for these operations is given to the node in the Node Administration structure. Modification of the two default required permissions for the operations is done on the Node Definition aspect category in the Aspect System Structure.

## Alarm and Event

### Alarm Services

The services for Alarm and Event are found in the Service Structure, refer to [Figure 161](#).

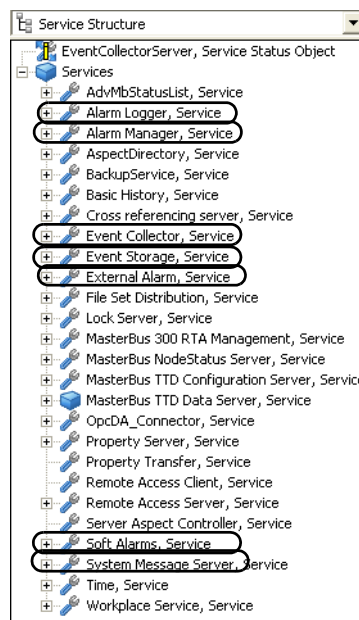


Figure 161. Service Structure

### Alarm Manager Service

Under the **Special Configuration** tab (found in the Service Structure, refer to [Figure 162](#)) configure alarm handling settings, event logging settings, and alarm storage size.

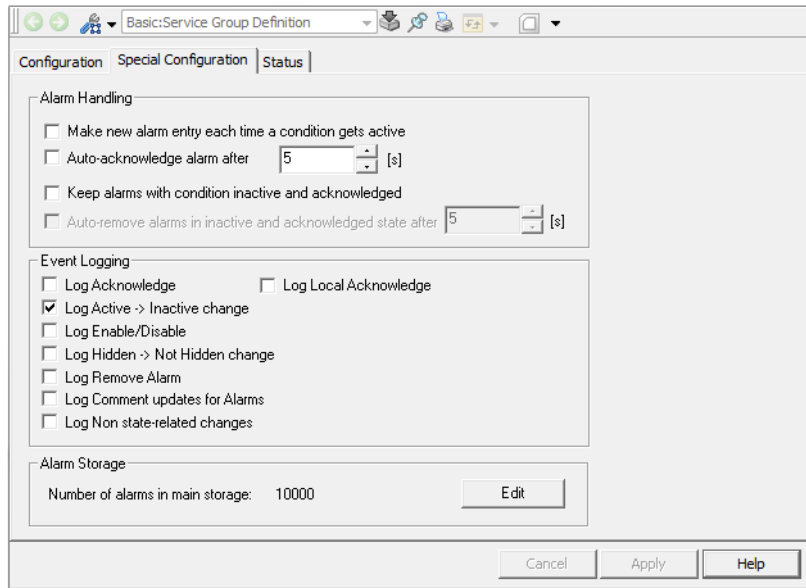


Figure 162. Alarm Manager - Special Configuration Tab

### Alarm Handling.

You have four options:

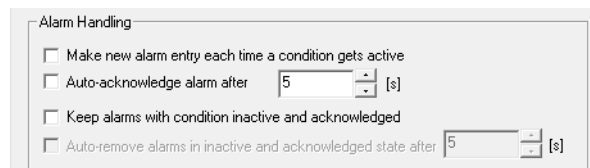


Figure 163. Alarm Handling



- **Make new alarm entry each time a condition gets active**  
If this check box is not selected, the previous condition will be replaced when the condition gets reactivated, that is, there is only one entry for each condition.  
If this check box is selected, an additional entry will be added each time the condition gets active and will not be removed until the alarm is acknowledged.



It is not recommended to select this check box. Default behavior for 800xA System Version 5.1 is to only display the present conditions in the alarm list.

- **Auto-Acknowledge alarms**  
If marked - alarms is autoacknowledged after the specified time interval.
- **Keep alarms with condition inactive and acknowledged**  
If marked - inactive and acknowledged alarms needs to be removed before disappearing. Removal can be done either manually or automatically.
- **Auto-remove alarms with condition inactive and acknowledged**  
If marked - alarms that becomes inactive and acknowledged will be automatically removed after the specified time interval. This setting is only possible when the Keep alarms with condition inactive and acknowledged check box is checked.

**Event Logging.** In the **Event Logging** area, you can specify the type of condition related events that's gets stored to the Event Storage, refer to [Figure 164](#).

You have eight options:

- **Log Acknowledge**  
If marked - the acknowledgement of alarms will be logged to the Event Storage Server as an event.
- **Log Local Acknowledge**  
If marked - the event storage will contain entries for alarm acknowledgements of non-present conditions. Note that such alarms only exists if the Make new alarm entry each time a condition gets active check box is checked.
- **Log Active -> Inactive Change**  
If marked - the active to inactive state changes of alarms will be logged to the Event Storage Server as an event.

- **Log Enable/Disable**  
If marked - the enabling and disabling of alarms will be logged to the Event Storage Server as an event.
- **Log Hidden -> Not Hidden change**  
If marked - the hidden status for an alarm from hidden to not hidden will be logged to the Event Storage Server as an event.
- **Log Remove Alarm change**  
If marked - the event storage log will contain entries of when alarms are removed (either manually or automatically depending of alarm handlings settings).
- **Log Comment Updates**  
If marked - the event storage log will contain entries of when comments are added to and alarm.
- **Log Non-state related changes**  
If marked - the event storage log will contain entries of when non-state related changes occurs for condition, such as attribute value changes or other changes that does not occur in conjunction with a state change.



If all check boxes have been checked, the event notifications will be stored in the event storage.

A screenshot of a configuration window titled "Event Logging". It contains a list of checkboxes for logging various events. The "Log Active -> Inactive change" checkbox is checked, while all other checkboxes are unchecked.

Event Logging	
<input type="checkbox"/>	Log Acknowledge
<input type="checkbox"/>	Log Local Acknowledge
<input checked="" type="checkbox"/>	Log Active -> Inactive change
<input type="checkbox"/>	Log Enable/Disable
<input type="checkbox"/>	Log Hidden -> Not Hidden change
<input type="checkbox"/>	Log Remove Alarm
<input type="checkbox"/>	Log Comment updates for Alarms
<input type="checkbox"/>	Log Non state-related changes

Figure 164. Event Logging

### Alarm Storage.



All alarms are stored, by default, in the main storage. The Alarm Server is capable to save the 10000 (default) most recent alarms. Alarms belong to different categories, and some categories are more important than others. Less important alarms are therefore capable to cut out the more important ones. It is possible to define the most important alarms (of a certain category) to be excluded from the main storage and to be stored in a special storage instead.

Click the **Edit** button in the **Alarm Storage** area to configure the alarm storage.

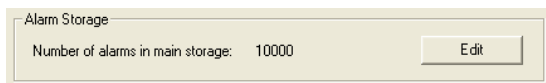


Figure 165. Alarm Storage

Set the following:

- **Maximum number of alarms in storage**  
Gives the maximum number of alarms which can be stored in the Alarm Manager.
- **Reserve number of alarms**  
Gives the number of alarms that are stored for each category. When the check box is unchecked and *Auto* is indicated, the alarms of that category are stored in the main storage.  
It is possible to give the maximum number of alarms that are stored for each category by marking the check box and type the number in the edit field. The sum of all maximum alarms for the categories cannot exceed the maximum number of alarms in the Alarm Manager.

### Event Collector Service

The Event Collector service handles the connected OPC Alarm & Event Servers.

Follow the steps below to connect to an Alarm and Event Server:

1. Locate the Event Collector service in the Service Structure.
2. Create a new service group and give the group a meaningful name (e.g. the name of the Connect).

3. Create a new service provider and select which node it shall run on (same as the connect product).
4. From the Special Configuration tab of the service group definition:
  - a. Select the OPC Alarm & Event server to connect to.
  - b. Select the Collection definition to use 2).
  - c. Press Apply.
5. For a redundant configuration create a service provider for the secondary server as well.



These steps can also be described in the User Guide for each connect, along with other important information on how to retrieve alarm and events for that product.



If connecting to a Third Party OPC server, there may not be a collection definition, follow the guidelines integration a Third party OPC in the *System 800xA 5.1 Configuration (3BDS011222\*)* instruction.

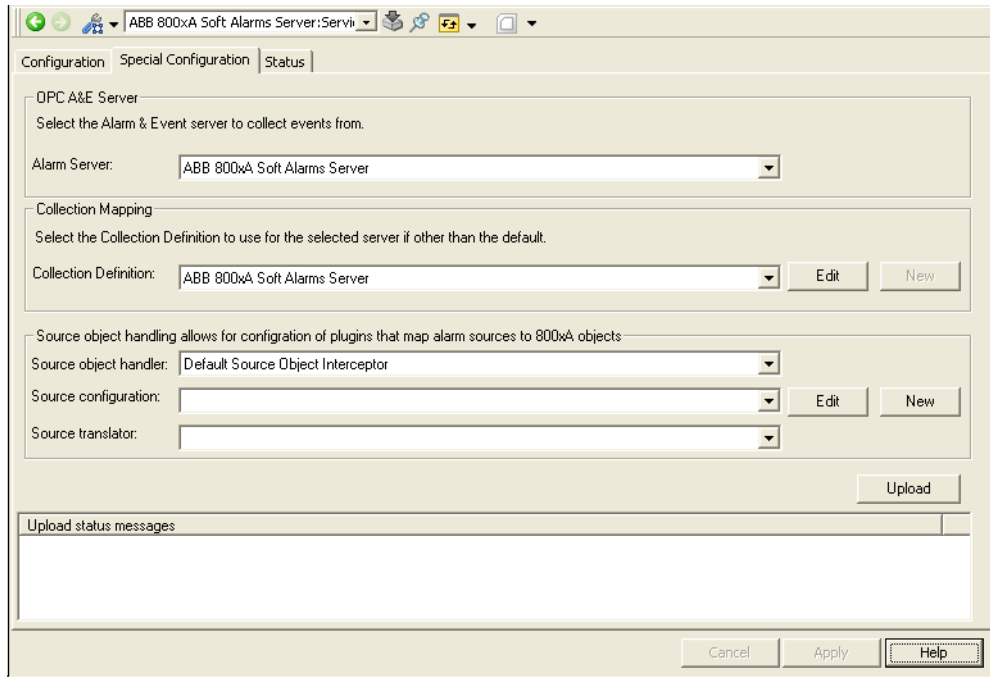


Figure 166. Event Collector Service - Special Configuration Tab

### OPC A&E Server.

- **Alarm Server**  
Here you select to which OPC Alarm & Event Server the Event Collector group will collect events from.

### Collection Mapping.

- **Collection Definition**  
Here you select which Collection Definition to use for the selected OPC Alarm & Event Server.



The collection definition is predefined for all connects and should not be modified.



For more information about Collection Mapping see the manual *System 800xA 5.1 Configuration (3BDS011222\*)*.

### Source Object Handling.

The Source Object Handling section allows to specify how events are related to aspect objects. There is usually no need to change the default settings.

- Object Handler

A source Object Handler is a software that translates the alarm source to an aspect object. Two types of object source handlers are available:

- Default Object Handler Interceptor
- Tracking Object Handler Interceptor

Technical Details:

- The Default Source Object Handler supports both alarm sources with:

1. Source Name specifying the name of the associated aspect object.
2. Source GUID attribute specifying the object ID for the associated aspect object.

For connects that does not support the "SourceGUID" attribute:

If an object with a specified name does not exist a new object will be created, by default under the "Lost and Found" object in the control structure. To configure an alternative location for creating objects see Source Configuration below.

- The Tracking Source Object Handler works as the Default Source Object Handler with one addition. It tracks and updates aspect object cache. This is common during upload from a controller.

- Source Configuration

A Source Configuration is an aspect that defines the Aspect Objects that corresponds to the connected OPC Alarm & Event server. The Object Handler will only look among these objects when finding the object that corresponds to an event.

A default root object can also be configured, under which new object will be created if an associated object cannot be found.

When to use:

#### Preload Descendents

If checked the Source Object Handler caches all the children of the specified root nodes. This will give better performance if the number of objects associated with the connected OPC A&E server is relatively small.

#### Default Root Node

Specifies the default root node that the Object Handler will use to find objects associated with the events. New object created by the Alarm system will be created under this node (instead of under the "Lost and Found" object) if specified. Press the Browse button to browse for and to select the default root node.

#### Additional root nodes

The additional root nodes is an ordered list for additional nodes to use when searching for objects.

Here you select the configuration aspect that defines how the source object interceptor should behave. This is an optional selection.

To bring up the Source Configuration aspect, click the **Edit** button. To create a new source interceptor, click the **New** button.

#### **Preload all descendants**

If marked - the source object interceptor caches the object name and object id of the root nodes child nodes.

The **Browse button** allows you to select a default root node, object and structure. This node is the one where new objects are created.

The Additional nodes list is an ordered list for additional nodes to use when searching for objects.

- Source Translator

Here you select which Source Translator to use.

A Source Translator is a software component that translates an alarm source into a corresponding aspect object name. The Source Translator function allows for plug-in source name translators which can be used when integrating 3:rd party OPC servers (see *System 800xA 5.1 Configuration, 3BDS011222\* instruction.*) By default there are no source name interceptors installed with the product.

The **Upload** button lets you create attribute definition aspects for all categories and attributes exposed by the server, and then restart the event collector service.



The **Upload** button is only visible when the service is configured and running.

### **Alarm Logger Service.**

Refer to the *System 800xA 5.1 Configuration (3BDS011222\*)* instruction for information about the Alarm Logger Service.

### **External Alarm Service**

Refer to the *System 800xA 5.1 Configuration (3BDS011222\*)* instruction.

### **Soft Alarm Service**

No configuration is needed for the Soft Alarms Service.

### **Alarm Analysis Service**

The Alarm Analysis function uses alarm key performance indicators (KPIs) to monitor and analyze the alarms generated in the system. Refer to the *System 800xA 5.1 Configuration (3BDS011222\*)* for more information. Perform the following procedure to configure the Alarm Analysis service:


1. Locate the Alarm Analysis service in the Service Structure.
2. Create a new service group under the Alarm Analysis service.



Basic:Service Group Definition

Configuration | **Special Configuration** | Status

**Time & Date**

 Enter the short term interval (typically 10 minutes) and the reporting period (typically a shift or a week) to be used in KPI calculations. The reporting period must be a multiple of the short term interval.


Short term interval:  [minutes]

Reporting period:  [minutes]

The first reporting period will start at the selected start time. If the selected start time is in the past a new start time will be calculated using the selected start time plus a multiple of the reporting period.

Start reporting at:  [Time]

**Level**

 Configure levels for acceptable alarm flow and alarm bursts.

Performance acceptability level specifies what is considered as good alarm system performance. Intense alarm activity level specifies what is considered to be an alarm burst.

Performance acceptability level:  [events per short term interval]

Intense alarm activity level:  [events per short term interval]

Cancel Apply Help

Figure 167. Alarm Analysis Configuration

3. Create a new service provider and select the node the provider will connect to. It is recommended to select the Aspect Server node.
4. On the **Special Configuration** tab of the service group definition (Figure 167), configure the following settings:
  - a. **Short term interval.** Alarm Analysis calculates some of the KPIs once in every short term interval set. The default value is 10 minutes.

- b. **Reporting period.** Specifies a reporting period such as, one shift, one week, or one month. The KPIs calculated are reset for every reporting period.



When creating a new Alarm Analysis object, a complete reporting period needs to be collected, before any data is presented for that period. In this case the Alarm Analysis display and elements may indicate bad data quality (that is, no initial data) for up to 2 reporting periods. This also occurs when the Alarm Analysis service group is started.

- c. **Start time for reporting.** Typically specifies the start of a shift, for example, 6:00 AM.



If this value is set to some past date, the new start time will be calculated using the specified start time plus a multiple of the reporting period.

- d. **Performance acceptability level.** Specifies the acceptable level of alarm flow per short term interval. The default recommendation is 1 alarm per 10 minutes.
- e. **Intense alarm activity level.** Specifies the value of alarm activity that is considered to be an alarm burst.

### Redundant Service Providers

In case of a redundant configuration, create and configure a service provider for the secondary server.

When the first service provider in the Service Structure goes down, the second provider continues to report the KPI values correctly.

At startup, the redundant service provider synchronizes with the running provider to collect the data. The synchronization of data allows both the providers to report the same KPI values at the end of the reporting period.

### Event Storage

The Event Storage server handles messages from the services, connected systems, and workplace clients.

Normally you do not need to alter the defaults of the Event Storage Server. However, this section describes how to do it.

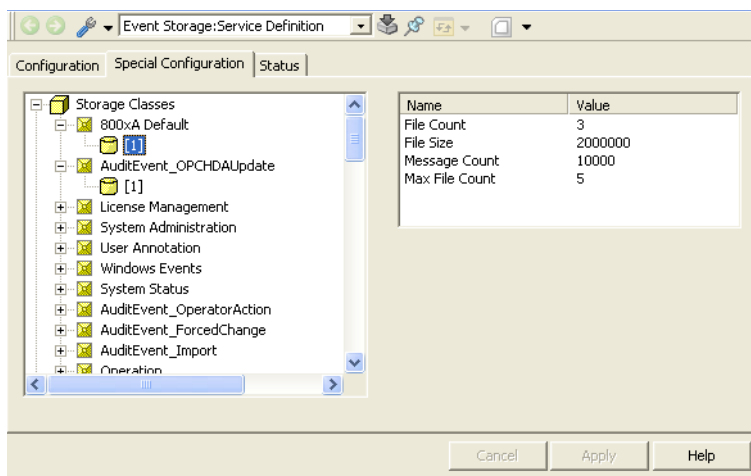
Configuration data is stored in the Service Definition aspect of the Event Storage Service object in the Service Structure, that is **Service Structure > Services > EventStorage, Service > Service Definition** aspect. The Event Storage Configuration appears on the **Special Configuration** tab for Service Definition aspect.

**Special Configuration.** Each priority within a message class has its own storage.

The **Special Configuration** tab shows a tree with two root folders, refer to [Figure 168](#):

- [Storage Classes](#)
- [Default Sizes](#)

You can also manipulate storage information for different message classes through Edit String dialog.



*Figure 168. Event Storage Configuration - Special Configuration*

- [Storage Classes](#)

Under the **Storage Classes** folder, each defined **Event Category class** is listed. In [Figure 168](#), the 800xA Default class has storage for messages with priority 1. The list to the right shows the storage information for this storage.

- Default Sizes

The **Default Sizes** folder defines the storage information for storages that have not been defined. By default, those storages will get the size specified under this folder. See [Figure 168](#).

**Edit String.** The list to the right shows the storage information for different storages. The values can be modified by double clicking the **Name** field. A dialog will be displayed. Make changes in the **Value Data** field and then click **OK**.

Click the **Apply** button on the **Special Configuration** tab to save the changes.

**Values.** The special configuration for Event Storage is shown in [Figure 168](#). Select the **800xA Default** storage class in the tree view. The priority level associated with this class indicates that messages with a priority 1 are included in the selected storage class. The list view, to the right, shows the configuration settings for the selected storage.

The following values for every priority are specified under the **Special Configuration** tab:

- File Count
- File Size
- Message Count
- Max File Count

File Size and File Count specify the storage size on the disk that is pre-allocated for the storage. Message Count specifies the number of messages that the message server tries to hold.

If the specified storage size (*File Size \* File Count*) is too small to hold the specified number of messages, the message server will allocate more files on the disk.

Max File Count is the maximum limit of the number of files that can be stored. The number of files allocated on disk will not exceed Max File Count.



Message sizes may vary, which means that the number of messages that can be stored is not guaranteed by a certain amount of allocated disk space.

The values that can be configured for each storage are listed in [Table 12](#).

*Table 12. Values that can be configured on the Special Configuration Tab*

<b>File Count</b>	Number of files that are pre-allocated on disk for the selected storage.
<b>File Size</b>	The size of the files that are pre-allocated on disk for the selected storage.
<b>Message Count</b>	The number of messages that the selected storage should hold.
<b>Max File Count</b>	The maximum number of files that are allocated on disk for the selected storage.

The two reasons to change the default values for the Event Storage configuration are to increase/decrease the number of stored messages, or make sure the messages do not overflow the disc.

By increasing the Message Count together with the Max File Count the total number of stored messages increase. The File Size and File Count should be adapted to the Message Count set.

A mean sized message is 150 bytes. This means that the File Size \* File Count should be close to Message Count \* 150. Max File Count larger than File Count means that more files can be allocated. The recommendation is to keep the default File Count and instead change the File Size.



The Message Count is a hard limit. Independent of the size and number of files used Message Count is the upper limit for number of messages stored.

You can set the Max File Count to the same value as the File Count to be sure that no extra disc space is allocated by the Event Storage after creation of the system.

- Setting FileCount

These settings are made by bringing up the Edit String dialog, by double clicking the configuration settings for the selected storage in the list view to the right.

*Table 13. File Count Settings*

<b>Increase</b>	<p><math>\text{NewFileCount} &gt; \text{FileCount}</math>                  New files will be allocated if the actual number of files is less than the new FileCount so that the actual number of files will be NewFileCount.</p>
<b>Decrease</b>	<p><math>\text{NewFileCount} &lt; \text{File Count}</math>                  The oldest files will be deleted if they are not needed to hold MessageCount number of messages. Otherwise the files remain.                  This is due to the fact that the MessageCount has higher precedence than FileCount.</p>

- Setting the File Size

These settings are made by bringing up the Edit String dialog, by double clicking the configuration settings for the selected storage in the list view to the right.

*Table 14. File Size Settings*

<b>Increase</b>	<p><math>\text{newFileSize} &gt; \text{FileSize}</math>                  All files will be resized to the new size.</p>
<b>Decrease</b>	<p><math>\text{newFileSize} &lt; \text{FileSize}</math>                  Files with no message data at a position greater than the new size will be resized to the new file size. Other files will be resized as messages are written to them.</p>

- Setting MessageCount

These settings are made by bringing up the Edit String dialog, by double clicking the configuration settings for the selected storage in the list view to the right.

*Table 15. Message Count Settings*

<b>Increase</b>	NewMessageCount > MessageCount Sets the MessageCount to the new value.
<b>Decrease</b>	NewMessageCount < MessageCount Sets the MessageCount to the new value.

- Setting MaxFileCount

These settings are made by bringing up the Edit String dialog, by double clicking the configuration settings for the selected storage in the list view to the right.

*Table 16. Max File Count Settings*

<b>Increase</b>	NewMaxFileCount > MaxFileCount The new MaxFileCount will allow the storage to grow to the new value of MaxFileCount.
<b>Decrease</b>	NewMaxFileCount < MaxFileCount If the actual number of files is larger than maxFileCount, the number of files will be reduced to MaxFileCount files.

**Recovering from Disconnected Mode to Connected Mode.** In disconnected mode data between the servers are not replicated. When the servers are back in connected mode the servers might not contain the same data. For the servers to be identical again you must decide which of the servers that has the best database. You can do this by comparing event lists connected to the different servers. Restart the server which contain the least accurate database.

### Priority Level Mapping

The Collection Definition object type has an Alarm Priority Mapping aspect, which indicates how AE OPC server severities should map to 800xA. The maximum number of priority levels is 32 in 800xA.

Each connectivity package provides a preconfigured priority mapping aspect.

By default the Alarm Priority Level aspect is configured for 4 levels, see [Figure 169](#).

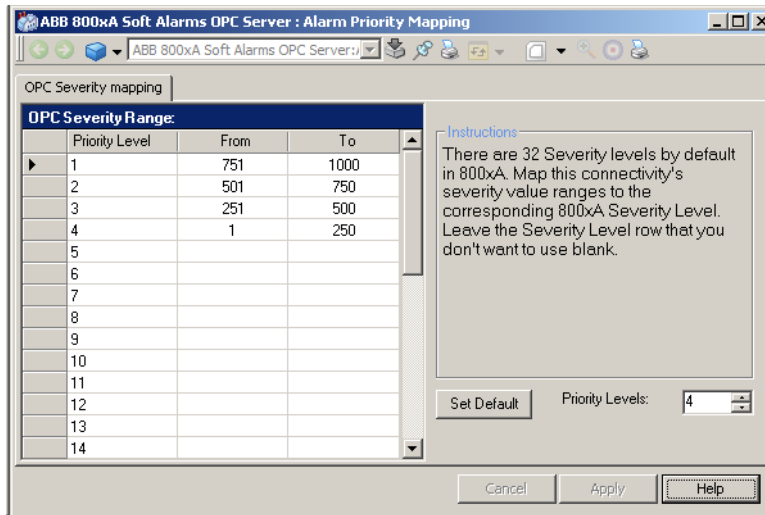


Figure 169. The Severity Level Mapping

### Category and Attribute Mapping

OPC Event category and attribute information is stored in attribute definition aspects for each event collector definition (in library structure).

There is one Event Attributes definition aspect for each of the OPC AE server's categories.

**Collect Events from this category.** If the Collect events from this category check box is unchecked, all events of this category will be ignored by the alarm system,



that is not collected shown in lists or stored in event storage. Figure 170 shows the category and attribute mapping aspect.

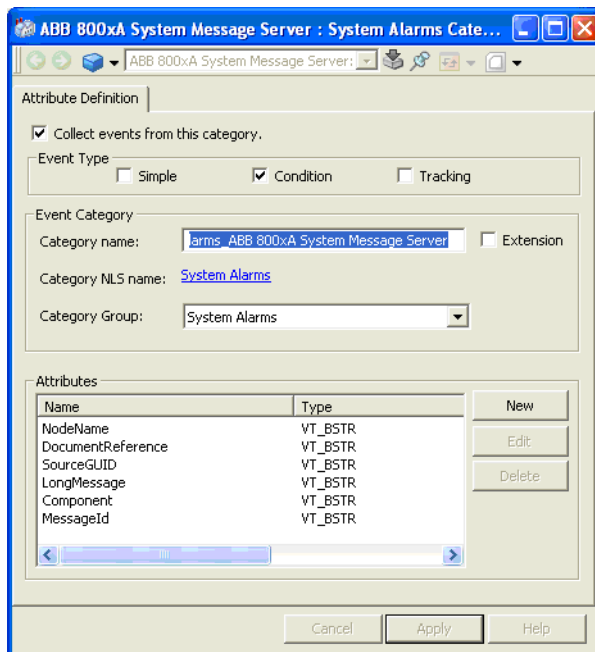


Figure 170. The Category and Attribute Mapping

**Event Type.** The check boxes (Simple, Condition, and Tracking) in this category indicate the type of event(s) and must not be changed.

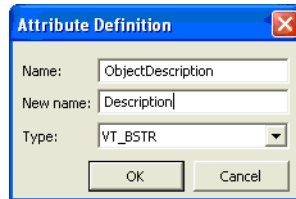
#### Event Category.

- **Category Name**  
The Event Category name is defined by the OPC AE server, and exposed by the Alarm manager as an 800xA category name. This name is NLS handled, and the translations are defined in an aspect named Category translations (located on event collector definition object). The category name is used as a resource id, and should not be changed.

- **Category NLS name**  
The NLS texts may be changed and new languages may be added.
- **Category Group**  
Displays which category this category belongs to. This should not be changed. The settings only applies when connecting 3rd party OPC with different specifications.

**Attributes.** The attributes list contains all defined attribute name and types for this event category.

To make a new attribute name or map one of the OPC AE server existing attribute names to one that should be used in event lists and so on, click the **Edit** button to create a new name to use for this attribute, refer to [Figure 171](#) for the Attribute Definition edit dialog.



*Figure 171. The Attribute Definition Edit Dialog Box*

A new feature enables the value of a custom attribute to be mapped to the standard attribute called Message. To map a vendor-specific attribute to the standard Message attribute, enter *@Message* in the **New name** field.



Restart the corresponding Event Collector group(s) for the changes to take effect.

**Attribute Extensions.** Attribute extensions are defined with Event Attributes Definitions aspects. The Event Attributes Definitions aspect defines one or several custom attributes for a specific event category or for all the event categories.

To add a custom attribute to an aspect:

1. Navigate to the **Alarm Collection Definition** object of the OPC AE server to which the custom attribute is added.
2. Create an Event Attributes Definitions aspect, refer to [Figure 170](#).
3. Select the **Extension** check box, refer to [Figure 172](#).

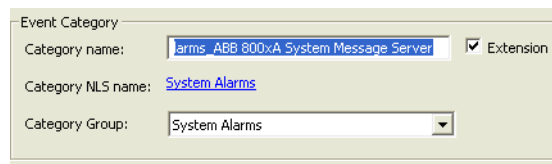


Figure 172. Category Mapping - Attribute Extension

4. Select the event category from the **Category name** drop-down list to add the custom attribute.
5. Click **New** in the Attributes section to add a new attribute.
6. Specify the **Name** and **Type** for the new attribute and click **Ok**, refer to [Figure 173](#).

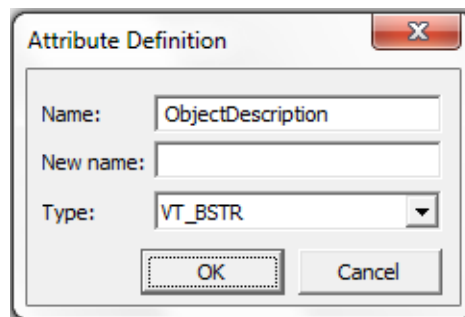


Figure 173. Attribute Definition Dialog Box

7. Click **Apply**.

To use the custom attribute:

1. Navigate to the object to which the custom attribute is added.
2. Create an **Event Attribute Object Extension** aspect.
3. On the **Object** tab, select if the attribute is extended to only the specific object and the descendants of the object or another object, refer to [Figure 174](#).

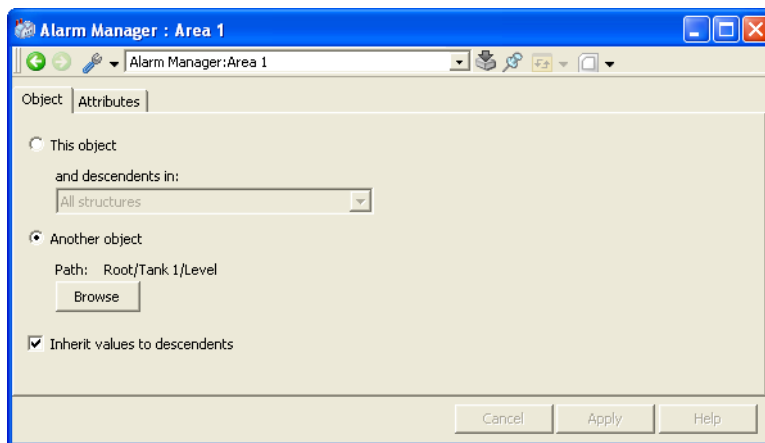


Figure 174. Object Tab Definition

- On the **Attributes** tab, select the category to which the extension is applied and set the attribute to the required value, refer to [Figure 175](#).

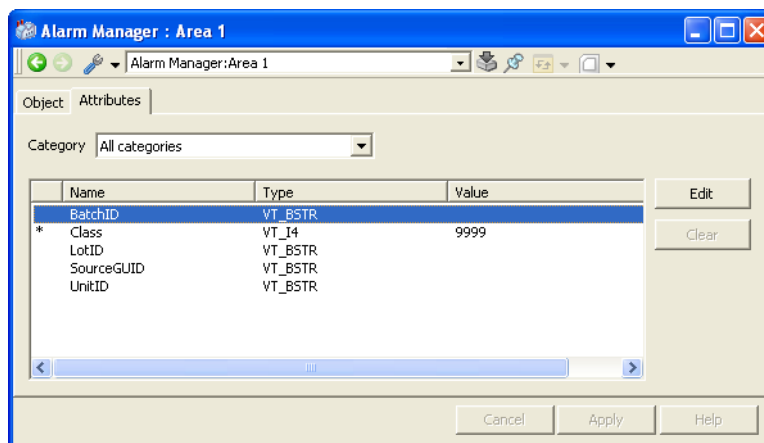


Figure 175. Attributes Tab Definition

- Click **Apply**.

The Alarm and Event List will display the attribute if the Alarm and Event List configuration is configured to include the corresponding column.



The Alarm and Event Lists already open will have to be closed and reopened to display the custom attribute.

### Supported Data Types

System 800xA supports the data types defined in [Table 17](#):

Table 17. Supported Data Types

Data Types
VT_BOOL
VT_BSTR

Table 17. Supported Data Types (Continued)

<b>Data Types</b>
VT_DATE
VT_DECIMAL
VT_I1
VT_I2
VT_I4
VT_I8
VT_INT
VT_R4
VT_R8
VT_UI1
VT_UI2
VT_UI4
VT_UI8
VT_UINT

## Redundant Services

This section describes how to handle problems that might occur when running redundant systems. For more information about configuration of redundant services, refer to *System 800xA 5.1, Post Installation (3BUA000156\*)*.

### Configuration of Redundant Services

At least two servers are required in order to be able to configure a redundant service. The set up of all redundant services is done automatically by the Configuration Wizard when adding a redundant server.

If a service has to be set up and configured manually, it should be done in the Service Structure. Open the service that should be redundant and select the Service Group. The **Configuration** tab of the Service Group Definition aspect shows the list of Service Providers. See [Figure 176](#).

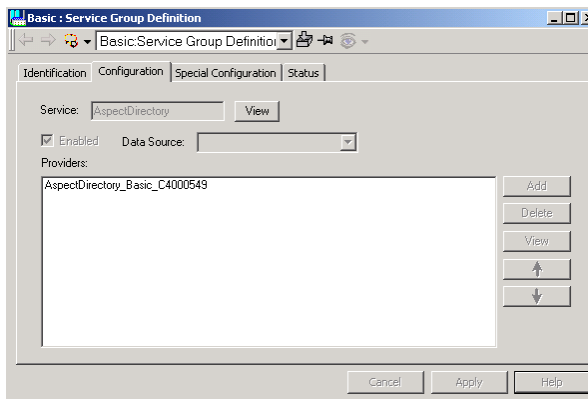


Figure 176. Configuration of Service Providers

Click **Add** to add a new service provider to the service group. The order determines which node will be the master.

### Redundant Aspect Servers

For aspect directories, being the central storage mechanism, special rules for redundancy apply. These rules are based on a majority-minority scheme where the

minority always goes to a read-only mode, e.g. no updates are accepted. For example if three redundant aspect servers are configured all updates are always replicated to all three servers. If one of these servers at any time cannot find its cooperating servers, regardless of reason (node shutdown, network problems), it finds itself being in minority and goes to read-only mode.

If the other two servers still are up and can communicate with each other they find themselves being in majority and continue accept updates. If an even number of aspect directory servers is configured they consider themselves to be in majority if they are in contact with at least half of the servers and continue to accept updates. This mean that in a configuration of two redundant aspect servers any of the servers that cannot find its cooperating server will continue to accept updates anyhow.

## Change from Redundant to Single Configuration

The following steps shows how to go from a redundant Aspect Directory configuration of three servers, to a single Aspect Directory Configuration.

1. Stop the third Aspect Server using the Configuration Wizard.
2. Remove the third Aspect Server using the Configuration Wizard.
3. Repeat step 1 and 2 for the second Aspect Server.

## Restart Redundant Configuration

Follow the steps below to return from single Aspect Directory to redundant Aspect Directory of three servers.



When a new system is created and large import-files will be loaded, it is recommended to import before redundant aspect directories are created.

1. Use the Configuration Wizard to start the Service Provider again. Select **Start Server**.  
The Aspect Directory service will go into an error state when trying to start up.
2. Start Plant Explorer Workplace by selecting **Start > All Programs > Industrial IT 800xA > System > Workplace**. Select Plant Explorer.
3. Go to the **Service Structure**, select the Aspect Directory and the third service provider.



4. Select the Service Provider Definition aspect and **Configuration** tab. Give the command **Cold Reset**. Wait until the Aspect Directory service has come into service state. (Can take some time depending on size of the system.)
5. Repeat the previous step to start the Aspect Directory service on the second service provider.

## Recovering from Read-only Mode

If there are not enough Aspect Directory servers running (that is only one in a 2 out of 3 redundancy network) the Aspect Directory will enter read-only mode.

The first step to recover from read-only mode is to start up the remaining servers and everything should work properly again.

However, in some cases this may not be possible (for example permanent loss of a redundant server).

The solution is to run a `NewSession` command on the Aspect Directory service provider of the only remaining aspect server node.

Locate the Service Provider object in the Service Structure (**Service Structure > Services > Aspect Directory > Basic > AspectDirectory\_Basic\_NodeName**).

Open the Service Provider Definition aspect and select **NewSession** in the **Command** drop-down menu and click **Run**. See Figure 177. This will change the node to run as a single Aspect Server node.

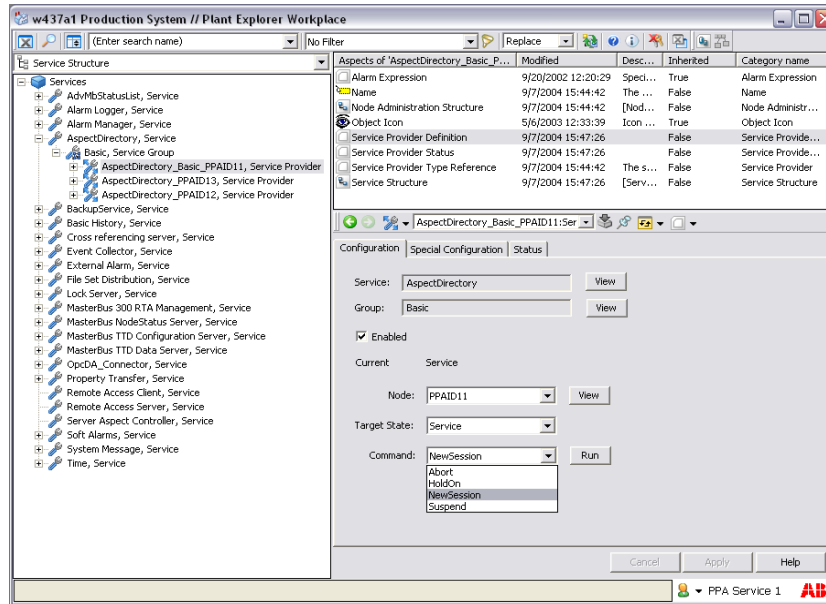


Figure 177. NewSession Command



If the previous lost redundant Aspect Servers would recover and start up again, their Aspect Directory Service Provider must then be forced to resynchronize (Cold Reset) to join the new single Aspect Server again.

To Cold Reset, run the following commands (in sequence): **Suspend**, **Cold Reset** **Run**.

## Aspect Server Automatic Recovery

The **Aspect Servers Automatic Recovery** option is available in the Aspect Directory **Special Configuration** tab, refer to Figure 178. When an Aspect Server, implemented in a 1oo2 redundant configuration fails, the Aspect Server Automatic Recovery option synchronizes the master and slave databases at the time of

reconnect. This synchronization takes place even if both the servers have modified their databases during the double network error.

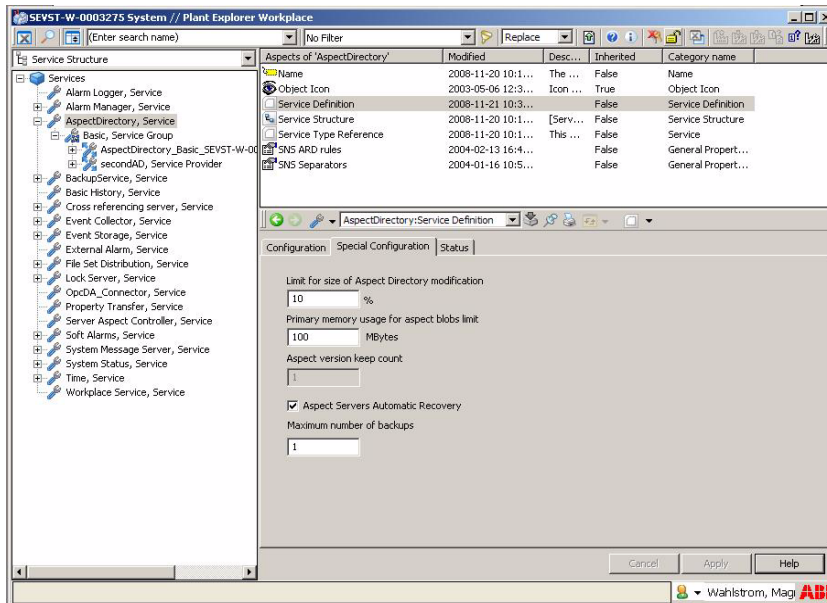


Figure 178. Aspect Directory Special Configuration tab

There are different risks and rewards with the Aspect Servers Automatic Recovery option.

At the time of a double network error:

- When the **Aspect Servers Automatic Recovery** option is enabled (default), the slave automatically performs a cold reset and synchronizes with the master.

This event results in losing the updates performed on the slave during the time of error. However, a cold reset creates a backup of the slave database before synchronizing with the master database and saves the backup folder with the original name followed by an index number such as, "...\\OperateITData\\AspDir.1"

The index number in the backup folder name is incremented with every backup that the cold reset creates. To ensure that the disk is not flooded with backups, configure the maximum number of backups in the **Special Configuration** tab, refer to [Figure 178](#). The default value is 1. When the number of backups reaches the specified threshold, the oldest backup is deleted to accommodate the new backup.

- When the Aspect Servers Automatic Recovery option is disabled, one of the Aspect Servers will go into Error state. The user manually needs to perform a cold reset to synchronize the databases.



Manually performed backups must not be placed in folders with names including the '.' character. This may cause erroneous behavior with the Aspect Server Automatic Recovery backup functionality.

---

## Section 9 Scheduling Reports

With the Scheduler it is possible to schedule and run jobs for Industrial<sup>IT</sup> 800xA System applications. For example, you can run reports, event-driven data collection, and consolidation of Production Data Logs (PDLs) and message logs. In this section scheduling of reports are described. Jobs can be scheduled and run at different times and under different conditions as specified through aspects related to a job definition object.

### Prerequisites

As a prerequisite a Report must have been created. How to create a report are described in *System 800xA Operations 5.1 Operator Workplace Configuration (3BSE030322\*)*.



To be able to run this function make sure that the Application Scheduler system extension is installed.

### Scheduling

Setup of scheduling is done in two steps:

- Creation of Service Group and Service Provider  
and
- Scheduling of the report.

## Creating Service Group/Service Provider Objects

The first step is to create a Service Group and a Service Provider for the Scheduler. To do this follow the steps below:

1. Create the Service Group object under the applicable service container in the Service Structure, in this case Scheduler, Service.
  - a. Select Scheduler, Service, open the context menu and select **New Object...** See [Figure 179](#).

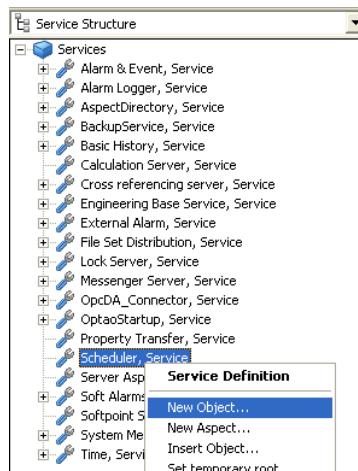
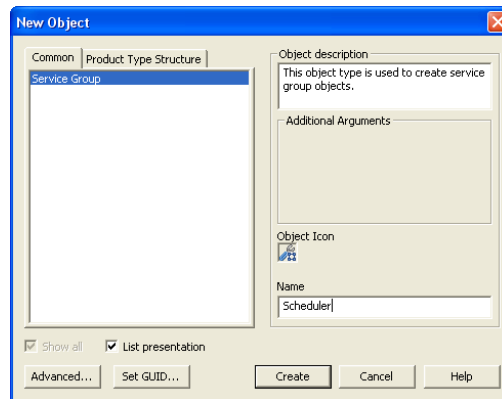


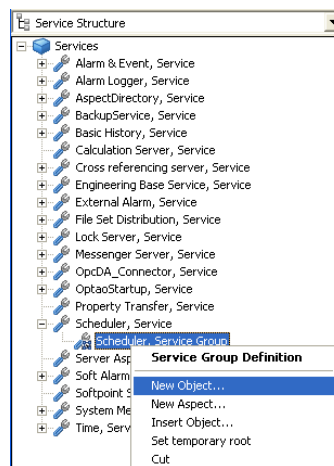
Figure 179. Creating a new Service Group Object for Scheduler

- b. Assign a name to the new Service Group object, see [Figure 180](#). Click **Create**.



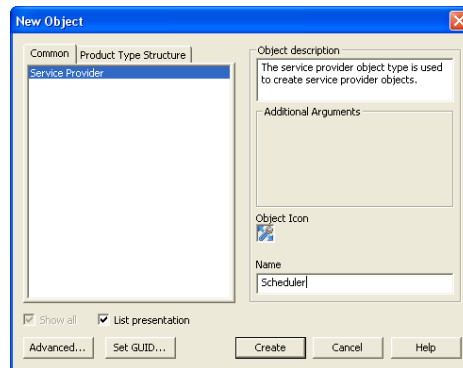
*Figure 180. Naming the Service Group Object*

2. Create the Service Provider object under the new Service Group object.
  - a. Select the new Service Group object, open the context menu and select **New Object...**, see [Figure 181](#).



*Figure 181. Creating a New Service Provider Object*

- b. Assign a name to the new Service Provider object, see [Figure 182](#). Click **Create**.



*Figure 182. Naming the Service Provider Object*

3. Configure the Service Provider object to point out the node where the service (in this case Scheduler) must run (see [Figure 183](#)).
  - a. Select the Service Provider object.
  - b. Select the Service Provider Definition aspect in the aspect list.
  - c. Select the **Configuration** tab.
  - d. Select the node where the service will run in the **Node** drop-down menu.
  - e. Check the **Enabled** check box.



f. Click **Apply**.

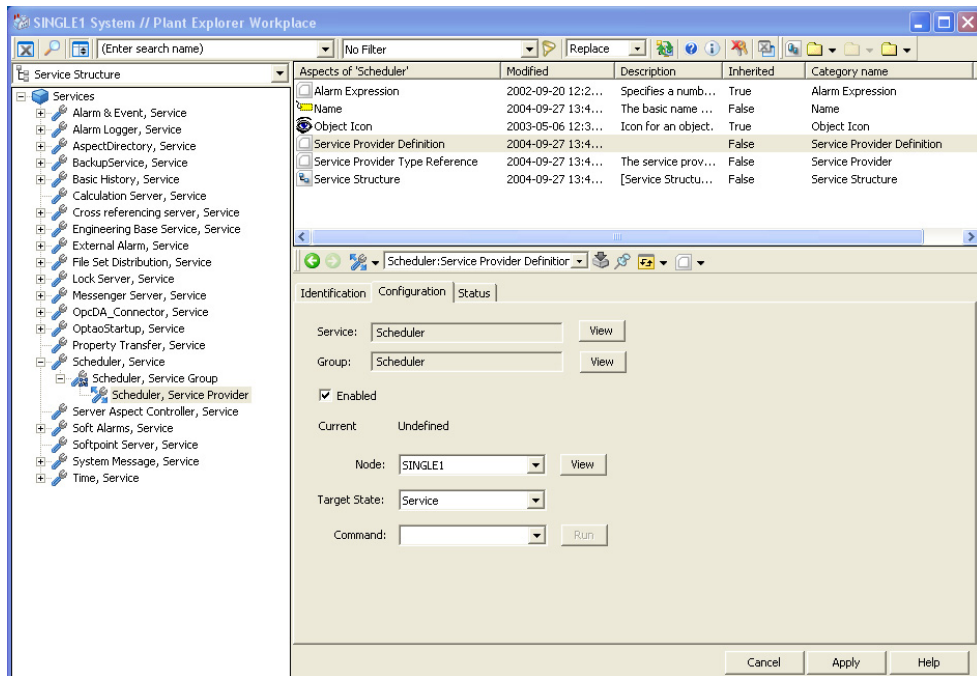


Figure 183. Service Provider Definition - Configuration Tab

## Scheduling Reports via the Application Scheduler

### Adding a Job and Specifying the Schedule

To add a job follow the steps below:

1. Select the Scheduling Structure in the Plant Explorer, and expand Schedules and Jobs.
2. Select the Job Descriptions object and open the context menu. See [Figure 184](#).

3. Select **New Object....**

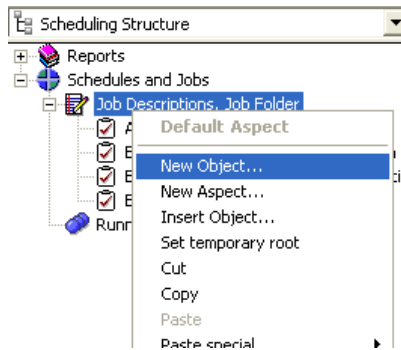


Figure 184. Creating a New Job Description Object

4. Select **Job Description** and assign the new Job Description object a name. See [Figure 185](#).

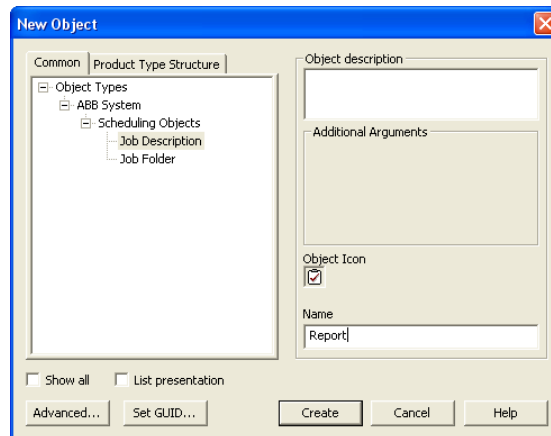


Figure 185. Naming of the Job Description Object

5. Click **Create**. This creates the new job under the Job Description branch, and adds the Schedule Definition aspect to the aspect list.

6. Click on the **Scheduling Definition** aspect in the aspect list to display the configuration view. Choose schedule alternative by clicking on the **Schedule** drop-down menu. There are six scheduling alternatives. For all alternatives the Service Group must be chosen in the **Service Group** drop-down menu.
  - **Cyclic Schedule** - a specific time interval.

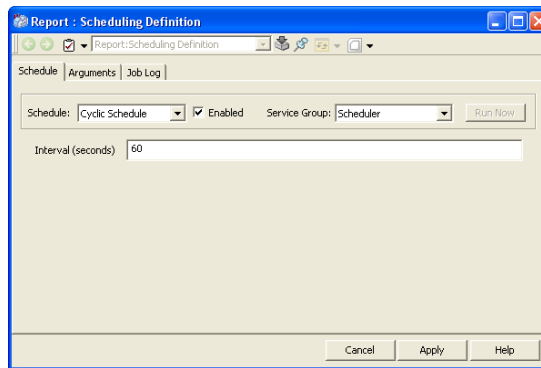


Figure 186. Cyclic Schedule

- **Periodic Schedule** - a specific time interval between two specific dates.

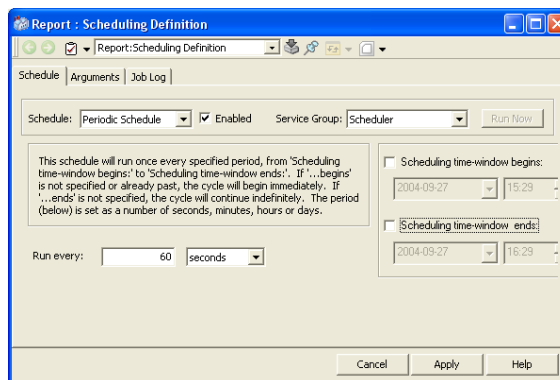


Figure 187. Periodic Schedule

- **Weekly Schedule** - a specific day of the week at a specific time.

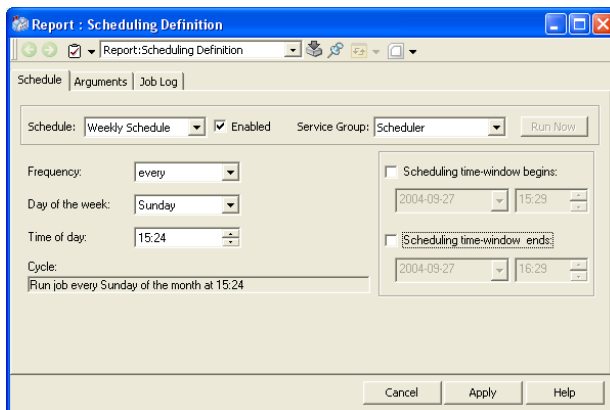


Figure 188. Weekly Schedule

- **Monthly Schedule** - a specific day of the month (for example 1st, 12th 31st, or every day) at a specific time.

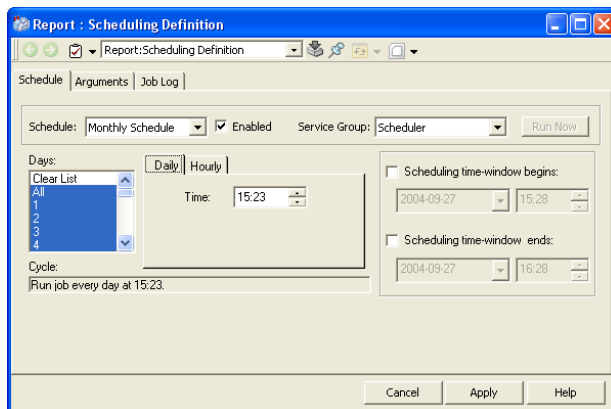


Figure 189. Monthly Schedule

- **List Schedule** - a list of scheduled date and times.

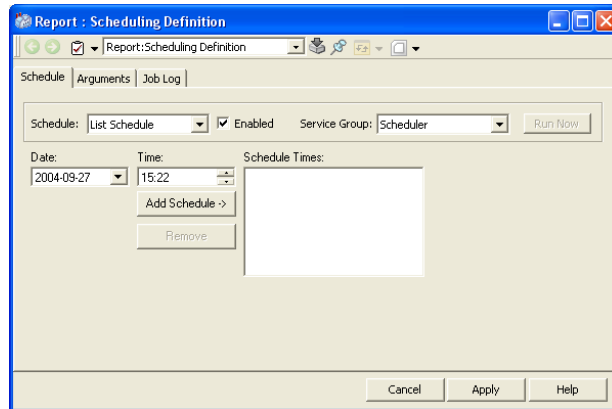


Figure 190. List Schedule

- **Expression Schedule** - the evaluation of an expression.

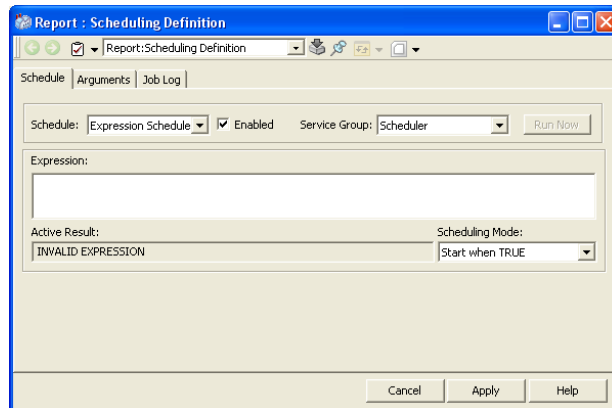


Figure 191. Expression Schedule

7. In this example (Figure 192) the scheduling is configured to run as a periodic schedule. Executed every hour starting July 2nd at 17:00 (5:00PM), and continuing until July 9th at 17:00.

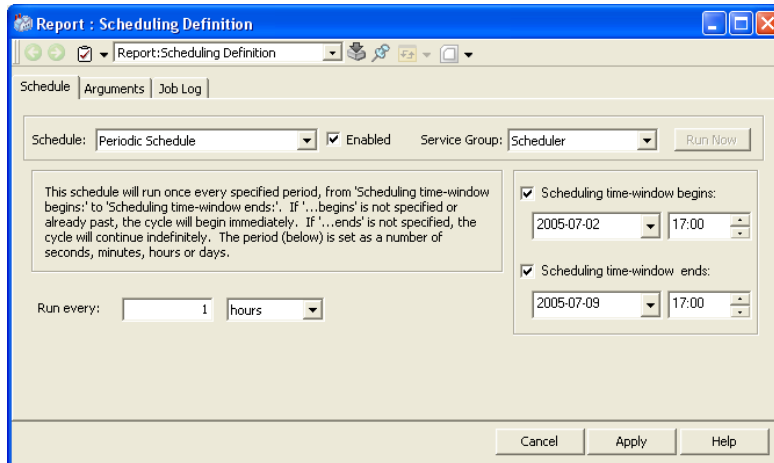


Figure 192. Scheduling Definition Aspect Configuration View - Periodic Schedule

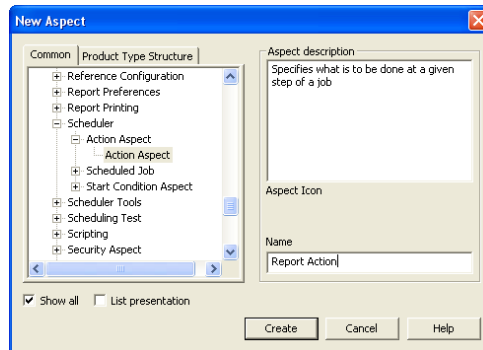
### Adding and Configuring the Report Action

Actions are implemented as aspects on an object which is on or under a Job Description in the Scheduling Structure.

To add an action follow the steps below:

1. Select the newly created job (in this case Report) and open the context menu. Select **New Aspect**.

2. Select **Action Aspect** and assign the new Action aspect a name. See [Figure 193](#). Click **Create**.



*Figure 193. Naming of the Action Aspect*

3. Click on the Report Action aspect in the aspect list to display the configuration view.

4. Select **Report Action** in the **Action** drop-down menu. See Figure 194.

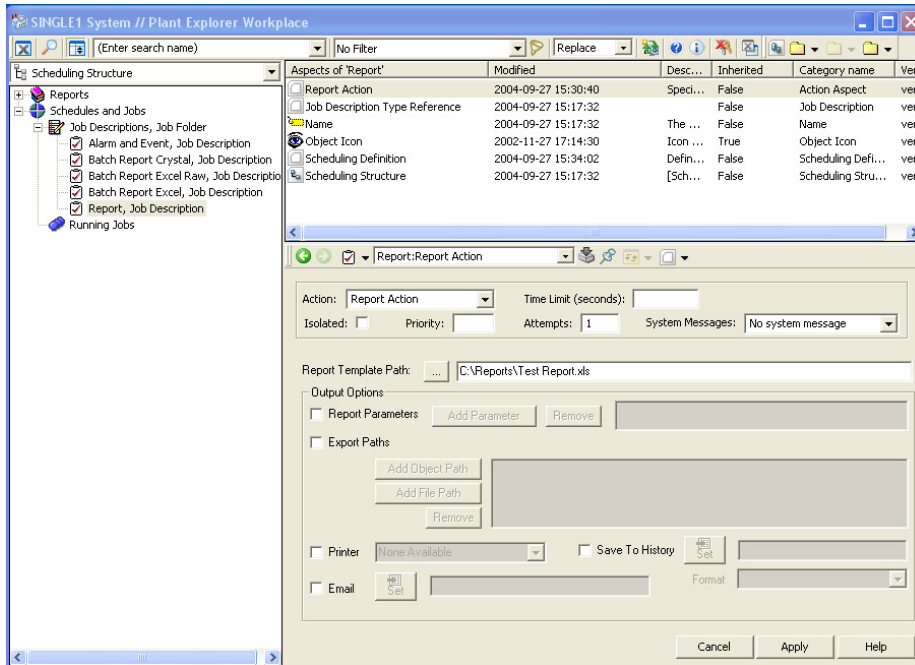


Figure 194. Report Action Aspect - Configuration View

5. Select your template report in the **Report Template Path** text field. Browse to it by clicking the button with three dots.
6. Select in what way you want to have the output of the report, for example printed or in a log file, in the **Output Options** area.
7. Click **Apply**. The referenced report will execute according to the schedule defined in the associated job description object.



For more information on how to use the Scheduler, see *System 800xA Information Management Data Access and Reports (3BUF001094\*)*.



---

# Appendix A Default Security Settings for Process Objects

AC 800M standard objects uses two default permissions as follows:

- **Operate**  
is used for settings which are expected to be used in the daily running of a plant. Examples are mode changes such as start, stop, go to auto mode, and go to manual mode. This also applies to parameters that are changed often such as a PID manual output value or a PID set point.
- **Tune**  
is used for tuning parameters. Examples are PID parameters (gain, offset) filter time, and alarm levels.

Note, however, that the default behavior could have been changed by an engineer using the Property Attribute Aspect.

This is an aspect that makes it possible to override existing permissions.

The property Attribute Aspect can be placed on an Aspect Object Type; thus affecting all Objects of that type. It can also be placed on a single Aspect Object; thus only affecting that particular object. See [Modification of 800xA Permissions for Process Objects](#) on page 54 for further information.



---

# Appendix B Security Checklists and Fault Search

## Security Checklists

Use the checklist below to make a major security check of your plant.  
Make sure that:

- All users have individual password protected accounts.
- All users of 800xA are members of Windows IndustrialITUser group.
- Only a few are members of the IndustrialITAdmin and Administrators groups.
- Default security on the system is changed to deny the Everyone group all permissions except **Read**.
- Security definitions setup on structures are correct.
- Backup routines are in place and checked.
- Firewall correctly configured.
- All ABB approved security updates installed.

## Fault Search of 800xA Security

In this section you will find questions and answers to guide you to find common problems in the 800xA Security system.

### Fault - Configuration Wizard only shows System Software Icon

If the Configuration Wizard is activated and only the “System Software and user settings” icon is visible, check the following:

Question:	Is the current user member of Industrial <sup>IT</sup> User group in the domain?
Answer:	Add the current user to the group.
Question:	Is the current user member of Industrial <sup>IT</sup> Admin group in the domain?
Answer:	Add the current user to the group.
Question:	Is there a local Industrial <sup>IT</sup> User or Industrial <sup>IT</sup> Admin group defined on the node?
Answer:	Remove the local groups.
Question:	Is the password of the Service Account correct?
Answer:	Redo the user settings.
Question:	Is the current user member of Local Admin or Domain Admin group?
Answer:	Add the current user to one of the groups.

## Fault - Permission granted for modify

When an operation is granted even when the configuration of security should deny this operation, check the following:

Question:	Is current user member of the Administrators group?
Answer:	All members of the Administrators group have full access to the system. Log in as another user.
Question:	What is the required permission?
Answer:	Check the Category definition aspect of the aspect involved in the Aspect System Structure, or look in the permission tab of aspect property.
Question:	What is the granted permission for the current user?
Answer:	Check granted permissions on the object with the Object Property dialog Permission tab. Then check all security definitions in all structures where the object is placed. End the check by checking the default security in the Admin Structure domain object.

## Fault - Permission not granted for modify

When an operation is denied even if the security configuration should allow it:

Question:	Is current user member of the Industrial <sup>IT</sup> User and Everyone groups?
Answer:	Add the user to the groups.
Question:	Does the current user have the correct role?
Answer:	Check the role of the current user in the User Structure, User Definition aspect.
Question:	What is the required permission for the operation?

Answer:	Check the Category Definition aspect of the aspect involved in the Aspect System Structure.
Question:	What is the granted permission for the current user?
Answer:	Check granted permissions on the object with the Object Property dialog Permission tab. Then check all Security Definitions in all structures where the object is placed. End the check by checking the default security in the Admin Structure domain object.

### Fault - Permission not granted for OPC Write

When an OPC write operation on a property is denied even if the security configuration should allow it, check the following:

Question:	Is current user member of the Industrial <sup>IT</sup> User and Everyone groups?
Answer:	Add the user to the groups.
Question:	Does the current user have the correct role?
Answer:	Check the role of the current user in the User Structure, User Definition aspect.
Question:	What is the required permission for the OPC property?
Answer:	Check the required permission in the Object Type Structure for the involved OPC property.
Question:	What is the granted permission for the current user?
Answer:	Check granted permission on the object with Object Property dialog Permission tab. Then check all Security Definitions in all structures where the object is placed. End the check by checking the default security in the Admin Structure domain object.

### Fault - The default permission does not apply to the wanted behavior

Question:	Is it possible to define your own permissions for groups of operators?
Answer:	Yes. Add your own permission, according to <a href="#">How to Add Your Own Permissions</a> on page 57. Then use the Property Attribute Override aspect for the Function block type or Control Module type and then you configure the default system security to include the new permission.

### Fault - A user is not possible to delete

Question:	Is all users possible to delete?
Answer:	No. The service account user and the user that created the system are protected from deletion.
Question:	Is it possible to delete a protected user?
Answer:	Yes. Select the User Definition aspect, then right-click and select Details...in the context menu.Go to the Aspect Info tab and remove the Service Account Key.



Removing the service account without having a new service account will make the system impossible to use.





---

## Appendix C Secured Server Configuration

Virus attacks are a real threat for networks connected to the Internet. However, there are some changes that can be done to make it harder for an intruder to get access to your servers. In the table below are some suggestions.



Do not apply any changes to your servers before confirming the changes with your IT department. Some suggestions may contradict your company's IT policy.

*Table 18. Network Settings*

Setting	Description
All partitions formatted to NTFS	NTFS partitions offer access controls and protections that are not available with the FAT, FAT32 or FAT32x file systems.
Install anti-virus software	Install latest anti-virus engine and make sure you are using the latest virus definition file. Refer <i>System 800xA Manual Installation (3BSE034678*)</i> instruction for restriction in usage.
Install latest approved service pack	Note. Approved means assessed and tested outside the production environment.
Remove additional OS installation if present	Remove other installed operating system except Windows NT Server.
Disable all unnecessary services	Review Services and disable those that are not used by the server's function.

Table 18. Network Settings (Continued)

Setting	Description
Unbind unnecessary protocols	If you are not using a particular protocol on a server, like IPX/SPX or NetBIOS, unbind it from the network adapter's it's bound to. This prevents denial-of-service attacks against that protocol, improves your overall server performance, and safe-guard you against protocol-specific exploits.
Change "Access this computer from Network" from Everyone to Authenticated users.	This only allows users having an account in the domain or on the machine to access shares on the server.
Disable IP-routing	If routing is enabled, you run the risk of passing data between the Intranet and the Internet.
Disable/delete all unnecessary accounts	Disable any non-active accounts and delete accounts that are no longer required.
Rename Administrator account	Rename the account to a non-obvious name.
Disable Guest account	Make sure Guest account is disabled.
Create a "decoy" account with no privileges and name it Administrator	Scan the event log regularly looking for evidence looking for evidence of attempts to use this account.
Enable auditing	Make sure to turn on auditing on these events: Logon and Logoff: Success, Failure User of User Rights: Failure Security Policy Changes: Success, Failure Restart, Shutdown, and System: Success, Failure
Remove all unnecessary file shares	All unnecessary file shares on the server should be removed to prevent possible information disclosure.
Set appropriate Access Control Lists (ACL's) on files, directories and shares	See Windows documentation.

Table 18. Network Settings (Continued)

Setting	Description
Hide last logon user name	To enable this, edit these registry setting: Hive: HKEY_LOCAL_MACHINE_SOFTWARE Key: Microsoft\WindowsNT\CurrentVersion\ Winlogon Value: DontDisplayLastUserName
Protect registry from unauthorized access	To restrict network access to the registry, make sure this entry exists: Hive: HKEY_LOCAL_MACHINE\SYSTEM Key: CurrentControlSet\Control\ SecurityPipeServers Value: RestrictAnonymous



---

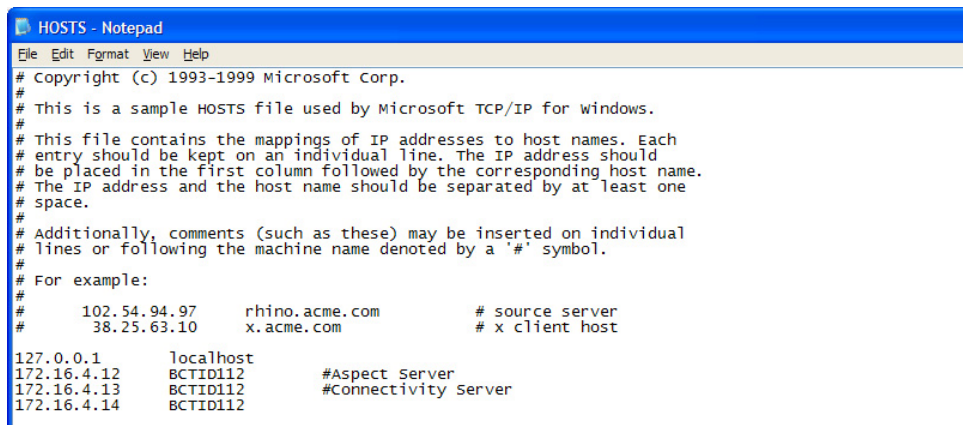
# Appendix D Troubleshooting in 800xA Workgroups

## Problem with Hostname Lookup

There may be a problem with getting the IP address for other hosts at boot time or when the primary connection of a redundant network fails. As a workaround to this problem, enter the addresses into the hostfile:

Install Drive:\Windows\system32\drivers\etc\hosts

for all hosts. [Figure 195](#) shows an example of the hosts file with the addresses entered.



```
HOSTS - Notepad
File Edit Format View Help
# Copyright (c) 1993-1999 Microsoft corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10      x.acme.com            # x client host

127.0.0.1       localhost
172.16.4.12     BCTID112          #Aspect Server
172.16.4.13     BCTID112          #Connectivity Server
172.16.4.14     BCTID112
```

*Figure 195. Host File*

## Fail to add Client or Server to a 800xA System

If there is a problem with adding a node when configuring the 800xA System and the node is using Windows Operating System (Windows 7 or Windows 2008), disable Sharing Wizard.

1. Select:

**Start > Control Panel > Folder Options**

The Folder Options dialog appears.

2. Select the **View** tab and configure it according to [Figure 196](#).
3. Clear the **Use Sharing Wizard (Recommended)** check box.

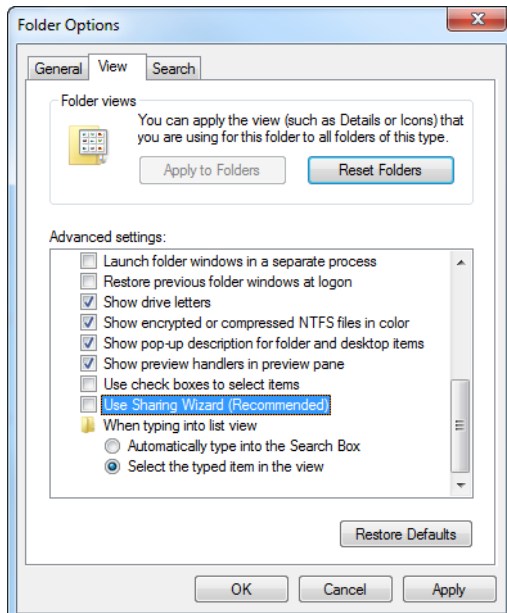


Figure 196. Folder Options Dialog - View Tab

---

## Invalid Account encountered during System Software User Settings

Under some conditions the default DCOM Security might not be properly set. It is then necessary to set it manually.

1. Select:

**Start > Run**

2. Type **dcomcnfg** in the Open field and click **OK**, **Yes**, and **Yes**.
3. Expand the tree in the left frame to:

**Component Services > Computers**

4. Right-click **My Computer** in the right frame and select **Properties** from the context menu that appears.
5. Select the **COM Security** tab.
6. Click **Edit Default** in the Access Permissions frame.
7. Give the IndustrialITAdmin and IndustrialITUser access permissions.
8. Click **OK**.
9. Click **Edit Default** in the Launch and Activate Permissions frame.
10. Give the IndustrialITAdmin and the IndustrialITUser launch permissions.
11. Click **OK**.
12. Click **Apply** and then **OK**.

## HTTP 500 - Internal Server Error Message

The following error message may appear in the Web Browser window when trying to view an ASP page after installing Microsoft Visual Studio 6.0 SP6:

```
HTTP 500 - Internal server error
```

Additionally, the following warning message may be logged in the system event log:

```
The server failed to load application  
'/LM/W3SVC/1/ROOT'. The error was 'General access  
denied error'.
```

To resolve this problem, grant the IWAM\_ComputerName user account the Read and Execute permission for the Mfc42.dll file. The Mfc42.dll file is located in the following folder:

`%WINDIR%\System32`

To grant the Read & Execute permission, follow these steps:

1. Use Windows Explorer to locate `Mfc42.dll`.
2. Right-click the `Mfc42.dll` file and select **Properties** from the context menu that appears. The Properties dialog appears.
3. Click the **Security** tab, and then click **Add**. The Select Users or Groups dialog appears.
4. In the Name field, locate and then click `IWAM_ComputerName`.
5. Click **Add**, and then **OK**.
6. Make sure that the **Allow** check box is selected for the Read and Execute permission, and then click **OK**.



---

# Appendix E System Alarm and Event Messages

## System Alarm Message Descriptions

The most important system alarms are described in the table below:

- The Component column lists from where the system alarm originates. (The corresponding function area is listed within parenthesis).
- The Message Description column lists short descriptions of system alarms. Text within % signs is replaced with the current data at run-time.
- The Extended description column explains system alarms further.

*Table 19. System Alarm Message Descriptions*

<b>Component</b>	<b>Message Description</b>	<b>Extended Description</b>
AdvDsOPCServerAdapter (Data Subscription)	OPC DA Connect Failed	The Data Subscription service failed to connect to an OPC Data Access Server. This indicates that no OPC Data will be available from this node.
AdvDsOPCServerAdapter (Data Subscription)	OPC DA Server Stopped	The Data Subscription service has lost contact with an OPC Data Access Server. This indicates that no OPC Data will be available from this node.
AdvDsOPCServerAdapter (Data Subscription)	OPC DA Server Error	The Data Subscription service has received a message from an OPC Data Access Server that it is in error. This indicate that no OPC Data will be available from this node.

Table 19. System Alarm Message Descriptions (Continued)

Component	Message Description	Extended Description
AfwAlarmEvent (Alarm and Event)	Connection to OPC AE Server lost	The Alarm and Event service has lost contact with an OPC Alarm and Event Server in the specified node.
AdvExtAlarm, AdvExtAIEngine (External Alarm)	Init of AE subscr. failed	The External Alarm service failed to connect to an OPC Alarm&Event Server. This indicates that the External Alarm function in this node is not working.
AdvExtAlarm, AdvExtAIEngine (External Alarm)	Connection of AE subscr. failed	The External Alarm service failed to connect to an OPC Alarm&Event Server. This indicates that the External Alarm function in this node is not working.
AdvExtAlarm, AdvExtAIEngine (External Alarm)	Initiation failed	Could not start the External Alarm Server due to severe problems in the system. This indicates that the External Alarm function in this node is not working.
AdvHtHistorySrv (Historian)	Exception caught in %APARTMENT% apartment object	An unexpected error has occurred in the specified function (APARTMENT). The History Server consists of several functions that run individually. Contact maintenance personnel for further investigations if this problem is indicated.
AfwAspDirSrv (Aspect Server/Aspect Directory)	Failed to open the aspect directory database files in %WORKDIR%.	Could not open the aspect directory database files. This indicates that the Aspect Directory in this node is not working.

Table 19. System Alarm Message Descriptions (Continued)

Component	Message Description	Extended Description
AfwAspDirSrv (Aspect Server/Aspect Directory)	Failed to synchronize database, reason=%HRESULT%	Failed to synchronize a backup Aspect Directory to the master Aspect Server. This indicates that the Aspect Directory in this node is not working.
AfwFsdServer (File Set Distribution) <sup>(1)</sup>	FileSystemError	A file system operation failed. The operations could be open, remove, find, create and rename. The files involved are fileset files either on the client (in the FSD cache) or on the server.
AfwFsdServer (File Set Distribution) <sup>(2)</sup>	ServiceStartupError	Unable to start up the File Set Distribution Service. This can be caused by a file system error.
AfwPropertyTransfer (Property Transfer)	Write to property %PROPERTY% failed	The data point (PROPERTY) will not be updated
AfwServiceManager (Service Manager)	Service provider stopped	This indicates that the service provider on the specified node is not working
AfwServiceManager (Service Manager)	Service provider entered error state	This indicates that the service provider on the specified node is not working.
AfwServiceManager (Service Manager)	Failed to update registry in client node %NODENAME%	This indicates that it will be problems for the specified client node to get in contact to a service provider.
AfwSMClient (RNRP)	RNRP connection down to %NodeName% path %NetworkPath%	This indicates that the RNRP connection to the specified node is down.
AfwSMClient (RNRP)	RNRP connection up node %NodeName% path %NetworkPath%	This indicates that the RNRP connection to the specified node is up.
AfwSMClient (RNRP)	RNRP node %Nodename% unreachable	This indicates that the specified node is unreachable.

Table 19. System Alarm Message Descriptions (Continued)

Component	Message Description	Extended Description
EventStorage	Resize failed: Unknown Error	The Event Storage Server has failed to resize a storage. This indicates that no more events will be stored.
EventStorage	Resize failed: Disk Full	The Event Storage Server has failed to resize a storage, because there was not enough space on disk. This indicates that no more events will be stored.

- (1) File set distribution (FSD) is typically used for distribution of Graphic Displays and Graphic Elements to all 800xA nodes. Problems with FSD will in some cases result in that Graphic Displays (or the latest version of these) are not available as expected on client nodes.
- (2) See footnote (1).

## System Events for Data Access Functions

This appendix describes System Events for Data Access functions. The messages are sectioned in function areas and submitting component.

### OPC DA Client - AdvDsOPCHandler

#### Write failed <Error>

A write operation to an OPC Item failed. The error description is included in the event text. The property name can be found in the long description of the event.

#### Invalid OPC DA Data Source configuration

The service group in the data source aspect is invalid. Check the configuration of the data source aspect and that the service group exists.

#### No OPC DA Data Source for OPC DA Item

No data source could be found for an OPC Item that was added. Check that there is a data source aspect in the tree above that object that defines the OPC Item and that the data key is correct.

**AddItems failed in 800xA OPC DA server**

AddItems in the 800xA OPC DA Server towards a connector service failed, the reason can be found in the long message. The client has received a failure code for the failing items. The connector service group or provider can be found in the long message.

**AddItems timed out in 800xA OPC DA Server**

AddItems in the 800xA OPC DA Server towards a connector service did not complete within the timeout. The client received bad quality for the items in this request. The connector service group or provider can be found in the long message.

**AddItems completed in 800xA OPC DA Server after a previous timeout**

AddItems in the 800xA OPC DA Server towards a connector service completed after a previous time out. The connector service group or provider can be found in the long message. This message is sent only as information.

## OPC DA Client - AdvDsOPCServerAdapter

**OPC DA Connect Failed <reason>**

Failed to connect to a remote OPC DA server. Check that the remote computer is reachable from the Connectivity Server and that it is possible to connect to the remote OPC DA server with a stand-alone OPC DA client.

**OPC DA server shutdown <reason>**

The target OPC DA server was stopped by manual shutdown.

**OPC DA server stopped <reason>**

The target OPC DA server has stopped unexpectedly or failed to respond within the supervision timeout. Check any error logs for the target OPC DA server.

**OPC Server Error <reason>**

An internal error occurred in the target OPC DA Server. The error code is included in the long description of the event. Check error logs for the target OPC DA server.

**OPC Server prog id is not valid.**

The OPC DA server id configured for the OPC DA Connector service provider is invalid. Check the configuration and that the OPC DA server is properly installed.

## Upload - AfwUploadServer

**Upload operation started**

An upload operation, retrieve or append was started.

**Upload operation completed successfully (Append/Retrieve)**

An upload operation, retrieve or append completed successfully ended.

**Upload operation was aborted by the user**

An upload operation was aborted by request of user.

**Upload operation failed**

An upload operation failed due to an internal error. The error code is included in the event text.

## Property Transfer - AfwPropertyTransfer

**Bad Property Transfer definition...**

The Property Transfer Service discovered a bad configuration in a Property Transfer Definition aspect.

**Write to property <name> failed...**

An error occurred when writing to the property <name>. A reason could be that the destination OPC server received too many write requests. Check error logs for the destination OPC DA server.

**Transaction overrun for property <name>...**

A write to property <name> was not completed before a new write was started. Reasons could be that the load in the Connectivity Server, destination OPC server or controller is too high. Try to change the update rate in the Property Transfer Definition aspect.





---

# Appendix F Additions in Windows added by 800xA

## Recommended Windows Configuration

Windows User Groups:

- **Everyone**  
a global user group for All Users.
- **Administrators**  
users with complete and unrestricted access to the node/domain.

### Power Users

users with the authority to add and delete programs as well as run all programs, but they are restricted from making any system changes.



Power User authority is required to build graphics.

When installing an 800xA product, the following user groups are added to the Windows user groups *if the installer is a member of Windows Administrator's group* (if the installer is NOT a Windows Administrator, see [Windows User Groups in Domain Controller](#) on page 36:

- **IndustrialITAdmin** (may be renamed during installation in the installation wizard). A member of this group runs all the services and has full access to the system. Restrict the number of users in this group.
- **IndustrialITUser** (may be renamed during installation in the installation wizard, (all 800xA users)).



---

# Index

## Numerics

800xA  
User groups 85

## A

Access evaluation algorithm 95  
Alarm Mapping 159  
Aspect Category Definition 51  
Aspect Category OPC property  
Required permission 51  
Assigning Permissions 25  
Associate Windows Group button 40  
Audit Trail Configuration 102  
Authority range 43 to 44

## B

Backup 24

## C

Cables 24  
Computer Room 24  
Confirmed Write 136  
Continue search  
Search option 45, 182  
Contractors 28

## D

Destruction of Data Media and Computers 24  
Digital Signature 126  
Double-authentication 114

## E

Evaluation search order 95  
An example 98

Event Storage  
Default Sizes 212  
Edit String 212  
File Count 214  
File Size 214  
Max File Count 215  
Message Count 215  
Storage Classes 211

## F

Firewall 25  
FSD 260

## G

Grab Responsibility 155  
Granted permission 52

## H

History Source 185

## I

IndustrialITAdmin  
Windows 2000 User Groups 36  
IndustrialITUser  
Windows 2000 User Groups 36  
Interface  
Role 85  
Inventory Spare Parts 25

## L

Log over 119

## M

Maximum security log size 112

**P**

Password Security 26  
Permission 43 to 44  
    Granted 52  
    Required 52  
Permission Set 160  
Permission tab 92  
Point of Control 155  
Point of Control Summary 156  
Process Equipment 24  
Property Attribute Override Aspect 56  
Protection of Admin Structure 179

**R**

Reason 128  
Re-authentication 114  
Release Responsibility 155  
Removing Users 32  
Request Responsibility 155  
Required permission 52  
    for Aspect Category OPC property 51  
Responsibility 158  
Responsible User 155  
Retain security log 113  
Retention method for application log 113  
Role 85  
    Interface 85  
Root Accounts 27

**S**

Scheduling Reports 229  
Search option 44 to 45  
    Continue search 45, 182  
    Terminate search 45, 182  
Section Definition 162  
Section Lock 175  
Sections 155  
Security  
    Report 88  
    testing 27

Security Definition aspect 30, 51  
Servers 25  
Services 25  
Special Configuration tab 211

**T**

Terminate search  
    Search option 45, 182  
The 210  
Training Program 28

**U**

UPS 24  
User Accounts 27  
User groups  
    800xA 85  
    Windows 2000 265

**V**

View of Audit Logs 101  
Virus Check 25

**W**

Windows 2000  
    User groups 265  
Windows 2000 audit  
    Presentation in the Event Viewer 110

---

# Revision History

## Introduction

This section provides information on the revision history of this User Manual.



The revision index of this User Manual is not related to the 800xA 5.1 System Revision.

## Revision History

The following table lists the revision history of this User Manual.

<b>Revision Index</b>	<b>Description</b>	<b>Date</b>
-	First version published for 800xA 5.1	June 2010
A	Updated for 800xA 5.1 Rev A	May 2011
B	Updated for 800xA 5.1 Feature Pack 1	August 2011
C	Updated for 800xA 5.1 Rev B	June 2012
D	Updated for 800xA 5.1 Feature Pack 4	February 2013

## Updates in Revision Index A

The following table shows the updates made in this User Manual for 800xA 5.1 Rev A.

<b>Updated Section/Subsection</b>	<b>Description of Update</b>
Section 3, Security Planning	Updated the Password Security subsection.
Section 4, Security Configurations	Updated the Configuring Access on Domain Servers subsection.
Section 8, System Services	Updated the Attributes Extension subsection.

## Updates in Revision Index B

The following table shows the updates made in this User Manual for 800xA 5.1 Feature Pack 1.

<b>Updated Section/Subsection</b>	<b>Description of Update</b>
Section 3, Security Planning	Updated the Password Security subsection.

## Updates in Revision Index C

The following table shows the updates made in this User Manual for 800xA 5.1 Rev B.

Updated Section/Subsection	Description of Update
Appendix D. Troubleshooting in 800xA Workgroups	Updated the Fail to add Client or Server to a 800xA System subsection with the screenshot.
Section 4. Security Configurations	<p>Changes done in the following subsection along with the Figures:</p> <p>Preparation and Configuration</p> <p>Associating a Windows Group to an 800xA Group</p> <p>Security Definition Aspect</p> <p>Windows Restrictions for Operators</p> <p>Minor updates in the steps also for creating the Group Policy.</p>
All Sections	<p>Renamed System 800xA 5.1 Installation to System 800xA 5.1 Manual Installation.</p> <p>The names of the Documents are corrected. It is observed that the names were given:</p> <p><b>Example:</b></p> <p><i>IndustrialIT 800xA, System, System Installation (3BSE034678*)</i> to</p> <p><i>System 800xA 5.1 Manual Installation (3BSE034678*)</i></p>

## Updates in Revision Index D

The following table shows the updates made in this User Manual for 800xA 5.1 Feature Pack 4.

<b>Updated Section/Subsection</b>	<b>Description of Update</b>
Section 4. Security Configurations	Changes updated in Audit Trail Configuration subsection.





# Contact us

## **ABB AB**

### **Control Technologies**

Västerås, Sweden

Phone: +46 (0) 21 32 50 00

e-mail: [processautomation@se.abb.com](mailto:processautomation@se.abb.com)

[www.abb.com/controlsystems](http://www.abb.com/controlsystems)

## **ABB Automation GmbH**

### **Control Technologies**

Mannheim, Germany

Phone: +49 1805 26 67 76

e-mail: [marketing.control-products@de.abb.com](mailto:marketing.control-products@de.abb.com)

[www.abb.de/controlsystems](http://www.abb.de/controlsystems)

## **ABB S.P.A.**

### **Control Technologies**

Sesto San Giovanni (MI), Italy

Phone: +39 02 24147 555

e-mail: [controlsystems@it.abb.com](mailto:controlsystems@it.abb.com)

[www.abb.it/controlsystems](http://www.abb.it/controlsystems)

## **ABB Inc.**

### **Control Technologies**

Wickliffe, Ohio, USA

Phone: +1 440 585 8500

e-mail: [industrialitsolutions@us.abb.com](mailto:industrialitsolutions@us.abb.com)

[www.abb.com/controlsystems](http://www.abb.com/controlsystems)

## **ABB Pte Ltd**

### **Control Technologies**

Singapore

Phone: +65 6776 5711

e-mail: [processautomation@sg.abb.com](mailto:processautomation@sg.abb.com)

[www.abb.com/controlsystems](http://www.abb.com/controlsystems)

## **ABB Automation LLC**

### **Control Technologies**

Abu Dhabi, United Arab Emirates

Phone: +971 (0) 2 4938 000

e-mail: [processautomation@ae.abb.com](mailto:processautomation@ae.abb.com)

[www.abb.com/controlsystems](http://www.abb.com/controlsystems)

## **ABB China Ltd**

### **Control Technologies**

Beijing, China

Phone: +86 (0) 10 84566688-2193

[www.abb.com/controlsystems](http://www.abb.com/controlsystems)

Copyright © 2003-2013 by ABB.

All rights reserved.

3BSE037410-510 D

Power and productivity  
for a better world™

