System 800xA

Multisystem Integration

Power and productivity
for a better world ™ **ABB**

System 800xA

Multisystem Integration

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.

Release: April 2016
Document number: 3BSE037076-510 D

Table of Contents

Section 4 - Operation

Section 5 - Maintenance

Appendix A - Error Messages

Appendix B - Fault Tracing

Index

Revision History

About This User Manual

General

Any security measures described in this User Manual, 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 user manual describes the 800xA Multisystem Integration system extension. 800xA Multisystem Integration makes it possible to connect to one or more 800xA systems and operate them from one single place, as if they where one system.

The user manual consists of the following sections:

• Introduction - describes the functionality of 800xA Multisystem Integration.

• Installation - describes the installation of 800xA Multisystem Integration and some typical hardware configurations.

• Configuration - describes of how to configure 800xA Multisystem Integration.

• Operation - provides information for the operators and engineers on how to operate and supervise a system using 800xA Multisystem Integration.

• Maintenance - provides information on how to maintain Multisystem Integration, backup/restore a configuration, System Alarm and Events, Audit Events, and System Status.

• Error Messages - describes error messages for the system with explanations.

• Fault Tracing - provides instruction to use when the system malfunction.

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.

Feature Pack

The Feature Pack content (including text, tables, and figures) included in this User Manual is distinguished from the existing content using the following two separators:

Feature Pack Functionality_____

<Feature Pack Content>

_____

Feature Pack functionality included in an existing table is indicated using a table footnote (*) :
*Feature Pack Functionality

Feature Pack functionality in an existing figure is indicated using callouts.

Unless noted, all other information in this User Manual applies to 800xA Systems with or without a Feature Pack installed.

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. Terms that uniquely apply to this User Manual are listed in the following table.

Term/Acronym	Description
Provider	The 800xA system running the Remote Access Server
RAC	Remote Access Client
RAS	Remote Access Server
Remote system	The system you communicate to, that is, reverse of local system
Subscriber	The 800xA system running the Remote Access Client
VBPG	Visual Basic based Process Graphics
Provider	The 800xA system running the Remote Access Server

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

Product Overview

Product Scope

800xA Multisystem Integration makes it possible to supervise and operate several 800xA systems from one central operating room. The 800xA subscriber and provider systems can be in the same Windows domain, different Windows domain, or different workgroups. The supervised system can be without any local workgroups or be a complete system with its own local operator room.

The supervising system is called the *Subscriber* and the supervised system is called *Provider*. Two services implement the communication, the Remote Access Server running in the provider system, and the Remote Access Client running in the subscriber system.

For detailed information about supported products, refer to *System 800xA, System Guide, Technical Data and Configuration (3BSE041434*)*.

Remote Access Client   Remote Access Server
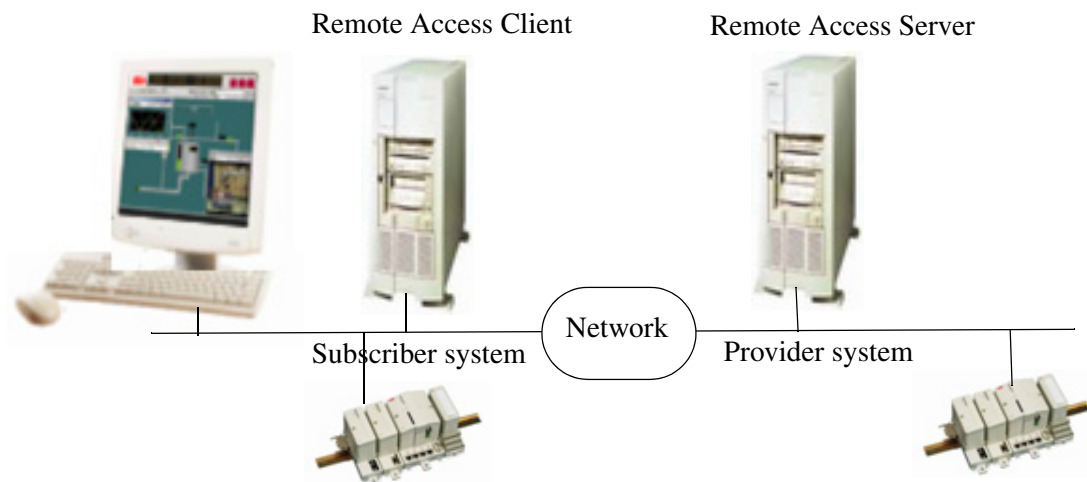
Figure 1. Subscriber and Provider Configuration

The network between the subscribers and the providers can be anything from a high speed LAN 100 MBit/s down to modem connection with a speed of 128 kBit/s.

A password and encryption can be used to secure the connection between the provider and the subscriber.

Figure 2. One subscriber Supervising two Providers

For more information about network configurations refer to *System 800xA, Network, Configuration (3BSE034463*).*

New in This Release

Feature Pack Functionality_____

Asset Optimization with Multisystem Integration

Using Asset Optimization with Multisystem Integration, the Condition Reporting and Monitoring, and Work Order Management functions can be performed remotely from the subscriber system.
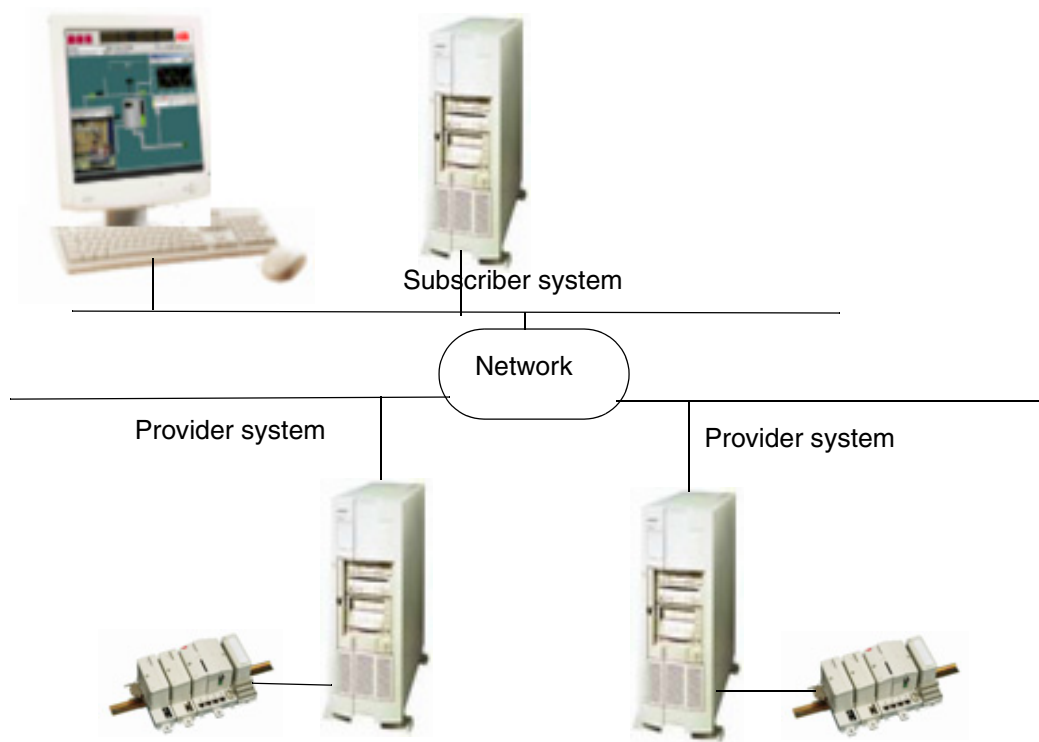
Multisystem Integration with Point of Control support

System 800xA Multisystem Integration now supports Point of Control. Using Point of Control with Multisystem Integration, the responsibility can be taken locally on the provider system, and remote on the subscriber system. For more information on the Point of Control function, refer to *Point of Control* section in *System 800xA Administration and Security (3BSE037410*).*

_____

Connect Method for Multisystem Integration

Connection between provider system and subscriber is not possible with unknown user account. The connection is possible from the subscriber system to the provider system only when user account is known in the provider system.

> If the provider and subscriber belongs to the same Windows domain, a domain user account can be used. If the provider and subscriber belongs to different Windows domains, or workgroups a node local account has to be used.

Prerequisites and Requirements. Local user account in both provider system and subscriber system should have the same account name and password.

The user should be an ordinary Windows domain user.

800xA Multisystem Integration with object locking for AC400 controller.

800xA Multisystem Integration now supports object locking for AC400 controller.

Prerequisites and Requirements

800xA Multisystem Integration must be installed on all 800xA nodes of the provider and subscriber. To be able to install 800xA Multisystem Integration, the 800xA Core system must be of SV 5.0 SP2 or latest version.

The version of the Multisystem Integration must belong to the same system version as Process Portal A and the other used system extensions.

To be able to use 800xA Multisystem Integration a separate license has to be purchased.

Section 2 Installation

800xA Multisystem Integration Installation

The 800xA Multisystem Integration wizard is used to install the 800xA Multisystem Integration. Perform the following steps:

1. Select Installation media.

2. Double-click on the Setup.exe program.

3. Select 800xA Multisystem Integration product, click **Install**.

   The 800xA Multisystem Integration installation startup dialog is displayed, see Figure 3.
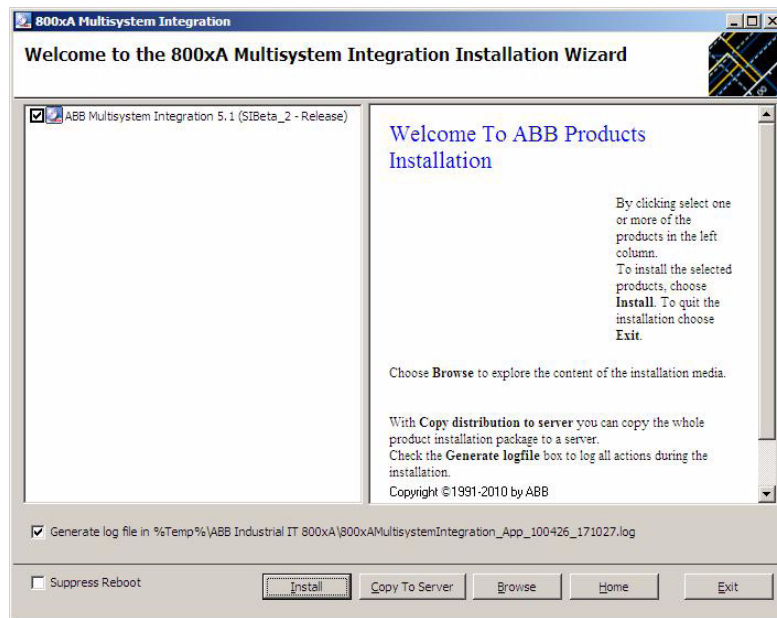
Figure 3. Installation Startup Display

Continue the installation and fill in the requested information. You can change the path of installation directory.

4.   Click **Browse** to change the path of installation directory, see Figure 4.

Figure 4. Installation Path

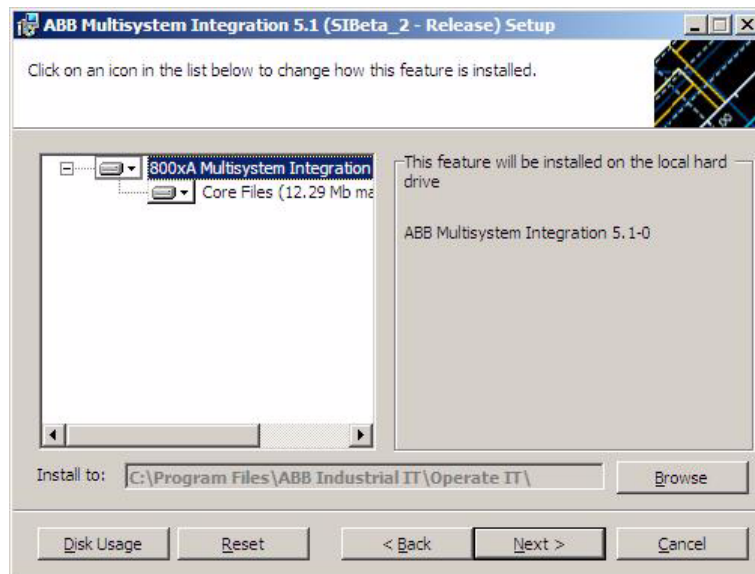> After the installation of 800xA Multisystem Integration the system extension must be loaded. The Configuration Wizard is used to install 800xA Multisystem Integration System Extensions.

5. Select **System Administration**.

6. Select system > **System Extensions**.

7. Select **800xA Multisystem Integration** and click **Finish**.

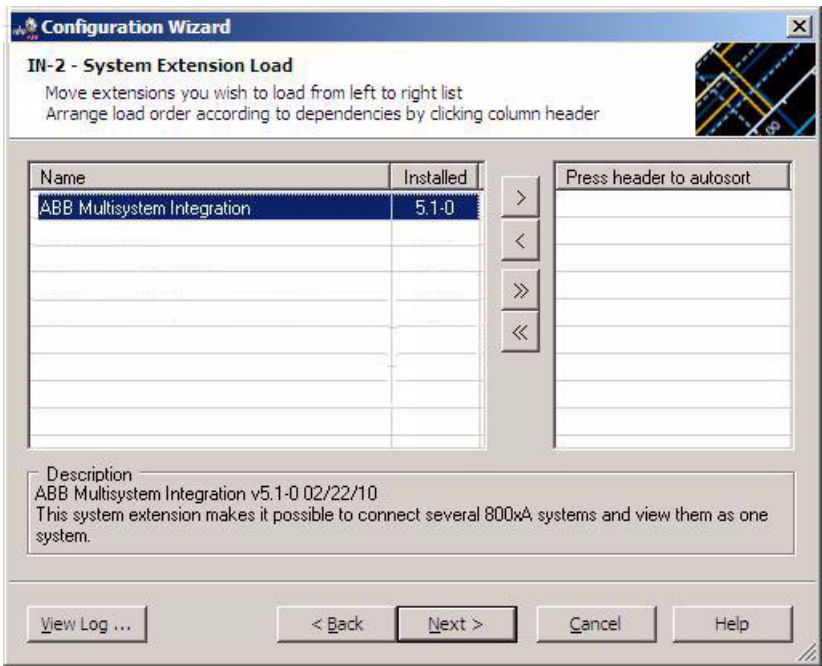> The Installation System Extensions list is displayed, see Figure 5.

Figure 5. Installation System Extension

8. Click **Next** and then **Finish**.

    The loading of the 800xA Multisystem Integration system extension is
    finished.

After loading the 800xA Multisystem Integration re-boot the machine; otherwise
the Remote Access Server and Remote Access Client fails to start.

If Visual Basic based Process Graphics (VBPG) is used with Multisystem
Integration, install Visual Basic as a prerequisite on all the nodes running the
Remote Access Client in order to deploy all the uploaded displays.

If only graphics built on Process Graphics 2 is used, installing Visual Basic is not
mandatory.

Depending on the system extensions used in the provider may more system
extensions can to be installed on the subscriber system. See documentation for the
system extension for information if they need to be installed on the subscriber

system or not. The general rule is that a system extension should be installed on the subscriber system if aspects from the system extension is uploaded.

Recommended Hardware Configurations

This chapter describes different configurations, used for a small and medium/large systems.

There are no special hardware requirements for 800xA Multisystem Integration, except the requirements for the 800xA Core system software.

The time difference between a Remote Access Client and a remote Access Server should be reasonable, normally less than a minute. To achieve this time synchronization additional external equipment may be needed.

The recommended hardware configurations are:

• Small Configuration

• Medium/Large Configuration

Small Configuration

For a small configuration, some few hundreds of I/O-signals, the Remote Access Server can run in the same node as the Connectivity and Aspect Directory servers. It is not recommended to run on an operative workplace on the same node.

Aspect Directory Server
Connectivity Server
Remote Access Client

Aspect Directory Server
Connectivity Server
Remote Access Server

< 1000 I/O

Network

Figure 6. Small Configuration

Aspect Directory   Connectivity Remote Access Client

Aspect Directory Server   Connectivity Remote Access Server

Network

< 5000 I/O
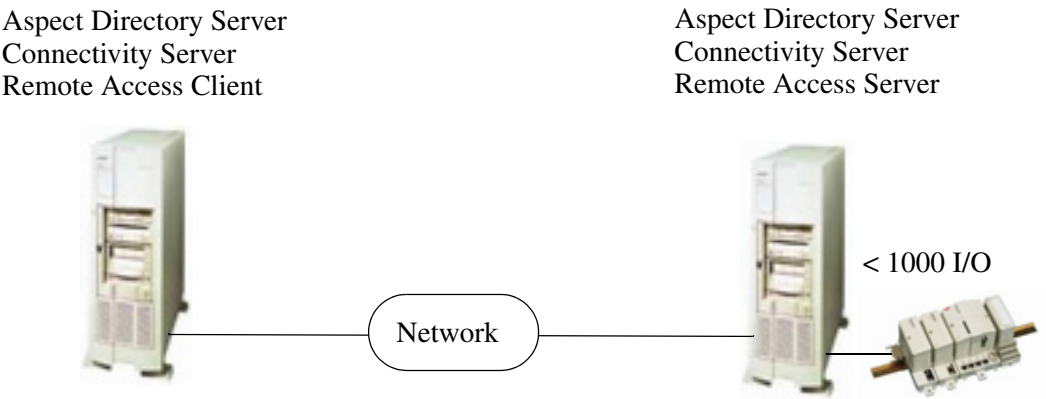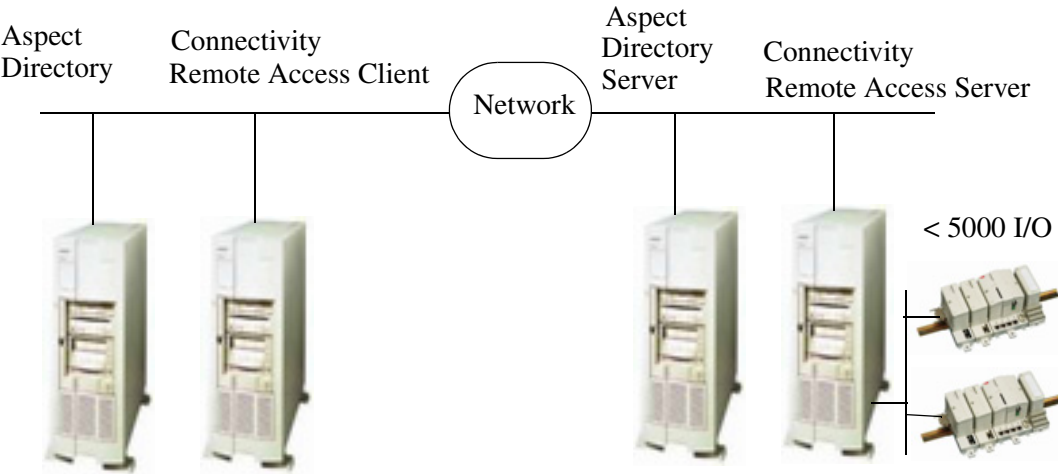
Figure 7. Medium Size Configuration

Medium/Large Configuration

For a medium/large configuration, it is recommended to run the Remote Access Server in the connectivity server node.

Remote Access Client   Remote Access Server
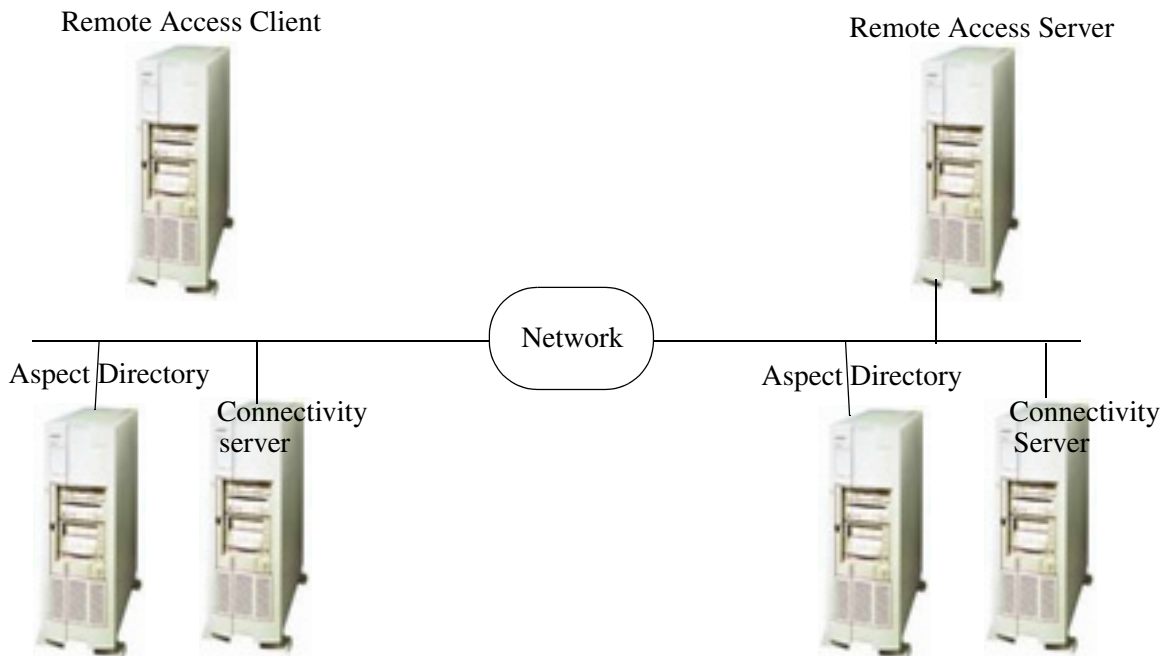

Figure 8. Medium/Large Scale Configuration

Some combinations of these three basic configurations can also be used.
For example if the provider system is small, but the subscriber system is connected to a lot of provider systems, the configuration for a small system may be used on the provider side, and a medium/large configuration may be used on the subscriber side.

For larger systems and to minimize impact on the provider and subscriber system may a separate node be used for the Remote Access Server and Remote Access Client.

For more information about Multisystem Integration network configuration refer to *System 800xA, Network, Configuration (3BSE034463*).*

Section 3 Configuration

Introduction

Before the 800xA Multisystem Integration can be used, it must be configured both in the provider and the subscriber systems. The configuration is done in three steps:

1. Create and configure the provider (Remote Access Server).

2. Create and configure the subscriber (Remote Access Client).

3. Configure and upload the provider objects and structures.

The configuration of the *Remote Access Server* in the provider must match the configuration of the *Remote Access Client* in the subscriber system.

The information to configure is:

• TCP/IP-addresses for all nodes, mandatory.

• Password, strongly recommended but not mandatory.

• Windows domain users or user mapping, mandatory.

Remote Access Server

Overview

The 800xA system to be supervised is called the *Provider* system, since it provides the supervising system with data. The supervisor system is called the *Subscriber*, since it subscribes to values from the provider.

All engineering and configuration of the provider system is done locally in the provider system.

Creation of a Remote Access Server

The Configuration Wizard is used to create the Remote Access Server in the provider system. Perform the following steps:

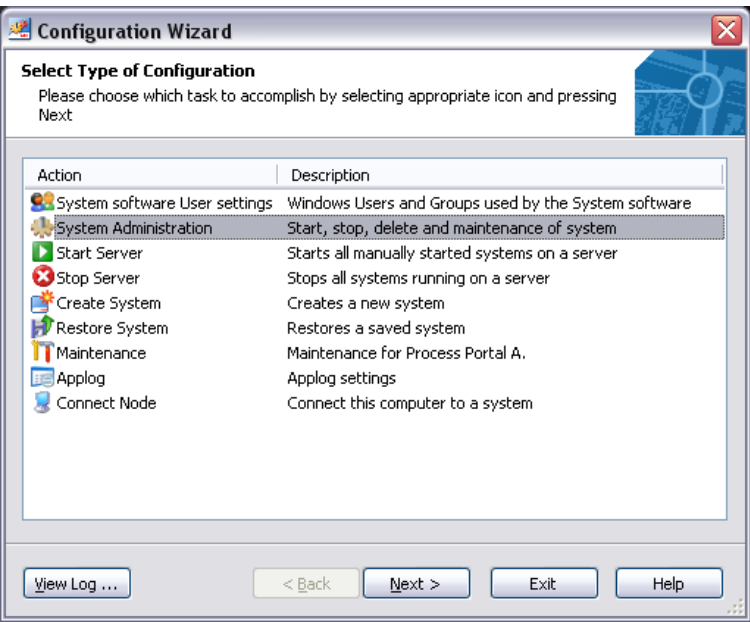1.   Select the **System Administration** option, click **Next**, see Figure 9.

Figure 9. Create Remote Access Server

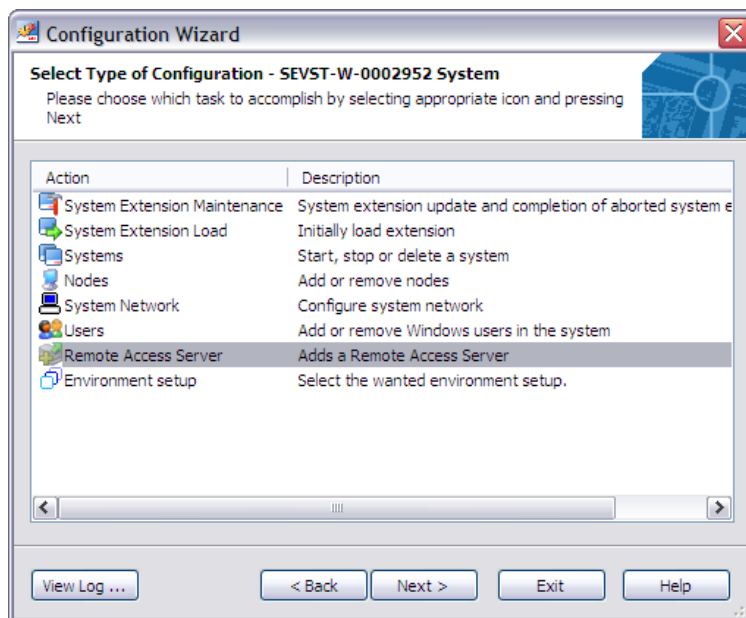2.   Select **Remote Access Server** option, click **Next**, see Figure 10.

Figure 10. Create Remote Access Server

The Add a Remote Access Server dialog box is displayed, see Figure 11.
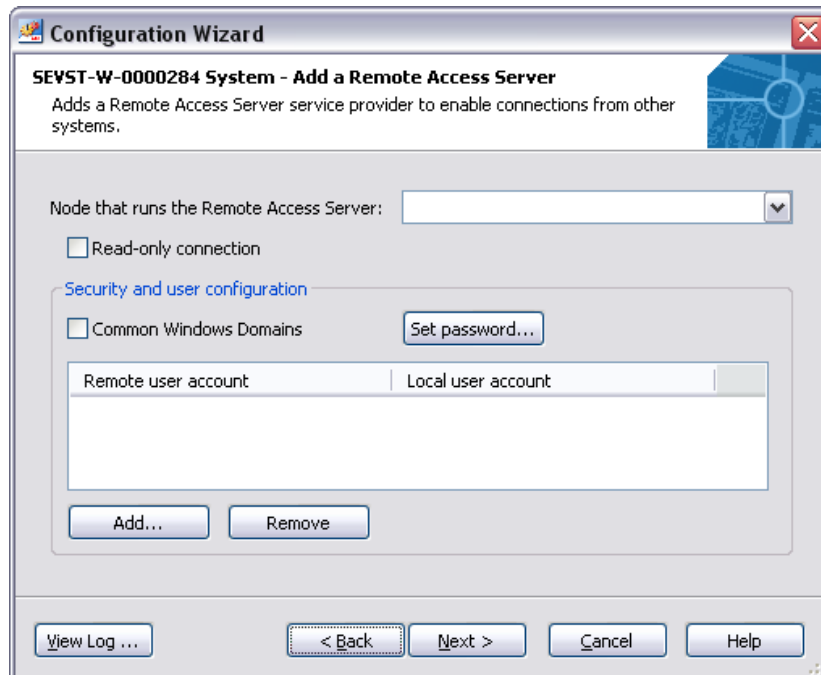
Figure 11. Add Remote Access Server

The following are configured in this dialog:

*   Node to run the Remote Access Server service provider.

*   If the connected clients will get a read-only connection.

*   If the Remote Access Server and Client is running in the same Windows domain.

*   If the provider and subscriber are running in different Windows domains a user mapping must be set up.

*   A password to connect to the Remote Access Server.

Select a password with at least 8 character, mixed lower- and uppercase letters, and also add some special characters.

3.   Click **Next**, see Figure 11 and then in new screen click **Finish**.

Node Configuration

The recommended node to run the Remote Access Server service differs depending on the size of the system. See section Recommended Hardware Configurations on page 23. Select the desired node from the drop-down menu.

Read-only System

If the **Read-only connection** check box is selected all clients connected to this provider can only read the values. This means that OPC writes from faceplates, history data updates and alarm acknowledge will be prohibited for all connected clients.

Read-only connection is a good choice if the system is to be supervised only, and it should not be possible to control anything from a remote client.

User Mapping

There are two ways to configure the users depending if the users in the subscriber and the provider systems belong to the same Windows domain or not.

If the users in the subscriber system and provider system belong to the same Windows domain the **Common Windows domain** check box should be selected.

> Usage of "Common Windows Domains" requires the user in the subscriber system to also exist in the provider system.

If the Remote Access Server and Client are in different Windows domains a user mapping between a user in the subscriber system (Remote Access Client) and a user in the provider system (Remote Access Server) must be set up. This is done by clicking the **Add** button.

Input the Windows account name, including the domain, for the subscriber system and select a Windows account to map to on the provider system.

If the remote user is a node local user, i.e. not a domain user, on the subscriber node the Remote Access Client node name must be inserted before the user account. For example: the local user Operator with the Remote Access Client running on node N124 should be written as "N124\Operator" in the user mapping for the Remote Access Server.

The wildcard character '*' can be used instead of a Windows account name in the subscriber system. Use this method only to map to a read-only or Guest user in the provider system, since it opens up a system for write from all accounts in the subscriber system.

The Security Report in the provider system is extended with a part that documents the user mapping for the Remote Access Server.

Password Configuration

It is recommended to configure a password for the Remote Access Server. The selected password must also be given when the Remote Access Client is configured. See section Remote Access Client Advanced Configuration on page 38. To configure the password, click the **Set Password** button.

> Setting a password is highly recommended but not mandatory. A password check is not made during a client-server connection. Clients can connect to the server without a password.

Figure 12. Set Password Dialog Box

Remote Access Server Advanced Configuration

There are two more configurations possible for the Remote Access Server. They are configured directly in the Special Configuration tab on the Service Group object.

These configurations are:

- Port number to use for the connection

- Usage of encryption for the connection

To configure port number and encryption usage for a connection, select the Service Structure and select the object Services/Remote Access Server/Basic, Service Group. Select the Service Group Definition aspect and the Special Configuration tab.
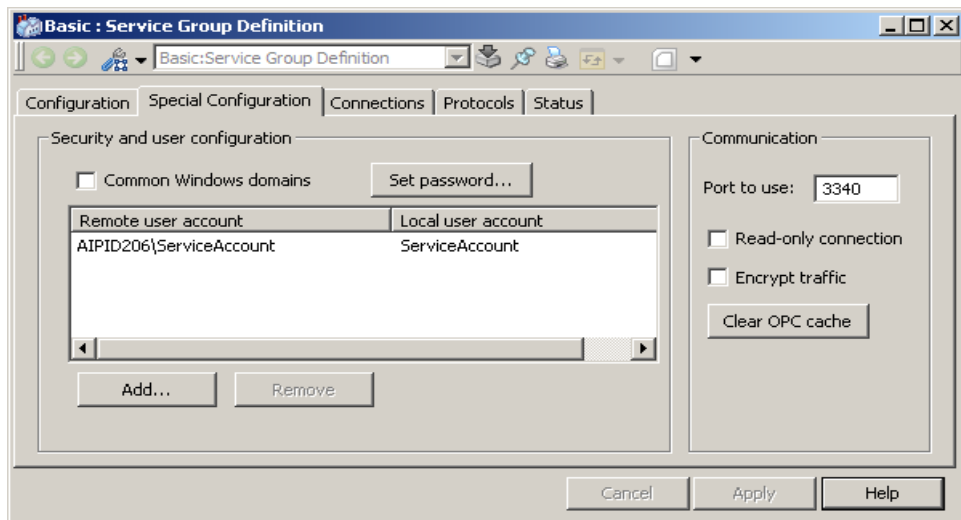

Figure 13. Remote Access Service, Special Configuration Tab

To specify the port number to use, enter the port number in the **Port to use** field. Default port is 3340.

Ensure the port selected is free to use. Consult your network responsible for information.

> If the Remote Access Server is protected by a firewall, make sure the selected port is open in the firewall.

It is possible to encrypt all messages between the Remote Access Server and the Remote Access Client if a password is set. Checking the **Encrypt traffic** check box specifies that encryption will be used. Encryption makes it more difficult to act as a

client against the provider, even if an unauthorized user gets physical access to the network.

> Encrypting the traffic between the Remote Access Server and Remote Access Client will result in a not noticeable performance decrease.

If a user wants to change the password, the old password must be given before a new password is accepted. A user with administrative rights can change the password.

Figure 14. Change Password Dialog Box

The remote access server caches information about OPC properties to speed up data subscription setup. If the set of uploaded object changes will this cache still contain information about the previous set of object. To optimize the data subscription time may the OPC property cache be cleaned by pressing the Clear OPC cache button.

> The time to get OPC properties data is longer the first time a display is brought up after a clean-up of the OPC property cache, but will be optimized the next time the same display is brought up.

Remote Access Client

Overview

The Remote Access Client service communicates with the Remote Access Server, but resides on the subscriber system. There is always a one-to-one relation between one Remote Access Client and one Remote Access Server, i.e. it only communicates with one Remote Access Server.

The Remote Access Client service is automatically created when the Remote System object is created.

Remote Access Client requires one license per provider to run without warnings.

Creation of a Remote Access Client

The Remote System object represents the provider system in the subscriber system. It also holds the information about the upload configuration, and upload history logs.

The Remote System object can only be created in the Control Structure:

1. To create a Remote System object, select Control Structure and select **New object** from the context menu. Select the object type **Remote System** in the **New Object dialog**, see Figure 15.
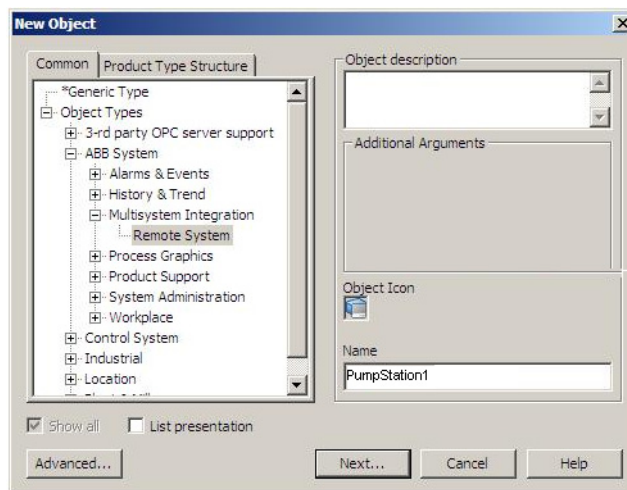
Figure 15. New Object Dialog Box for Remote System Object

2.   Enter the Name, and click **Next,** the system displays Additional Arguments
     dialog, see Figure 16. The name given for the Remote System object will be
     presented in faceplates, process displays, alarm lists, trends, and history logs.
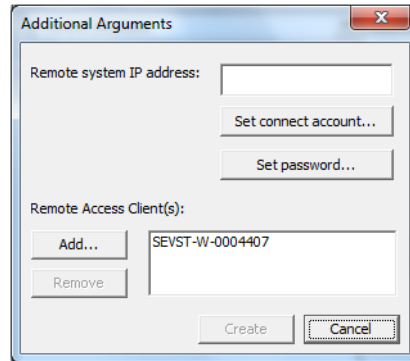
Figure 16. Configuring the Connect Account

3.   Enter the Remote system IP address, and click **Set Connect Account** to configure the Connect Account. The user specified should be a local user, or a domain user. Domain user can be used when the provider and subscriber system belongs to the same Windows domain. The provider and subscriber belongs to different Windows domains, or workgroups, then a local user is specified. The local user should exists both in the provider and subscriber system with the same user name and password, see Figure 16 and Figure 17.
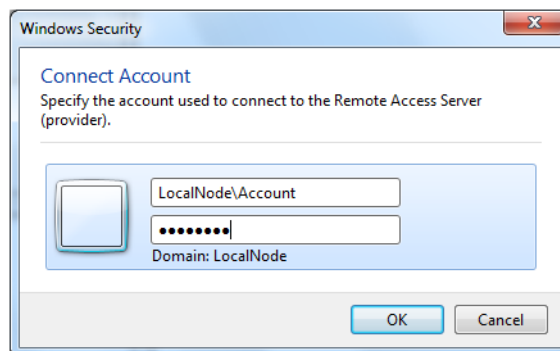

Figure 17. Connect Account

4.   Click **OK**.

5.   Click **Set Password**, see Figure 16. Password only have to be set if encryption is used.

Figure 18. Set Password

6.   Enter the password as specified in the Provider System (Remote Access Server), and click **OK**.

7.   Click **Add** (Remote Access Clients), and click **Create**, see Figure 16.

The Remote System Object is created.

Remote Access Client Advanced Configuration

The configuration of the Remote Access Client can be changed after the Remote System object is created. Select **Service Structure** and open the Services/Remote Access Client/Service Group. Select the **Service Group Definition** aspect, the **Service Group Definition** dialog is displayed, see Figure 19.
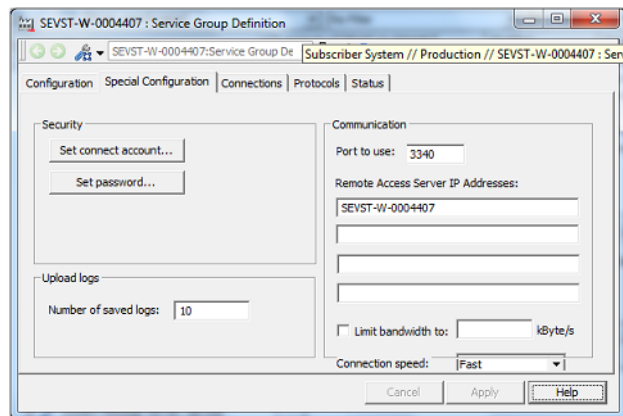
Figure 19. Remote Access Client, Special Configuration Tab

To configure the Remote Access Client, execute the following steps:

ℹ️ The Connect account must be configured on the node that executes the Remote Access Client (*AfwRAC.exe*).

If the system is redundant, the Connect account must be configured twice. The password must be configured on the Remote Access Client nodes, and the Remote Access Service (*AfwRAS.exe*) node.

For a redundant system, the password must be set four times, that is, twice for the Remote Access Client and twice for the Remote Access Service.

1. Select **Special Configuration** tab, and click **Set Connect Account**. The connect account dialog is displayed.
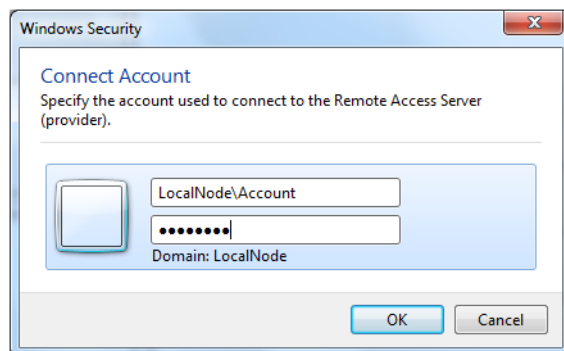
Figure 20. Connect Account

> **i**   The Remote Access Client (RAC) must be restarted after applying the Connect Method.

2. Specify the Account used to connect to the Remote Access Server (Provider) and click **OK**. See Figure 20.

3. Click **Set Password**, see Figure 19. Password only have to be set if encryption is used.
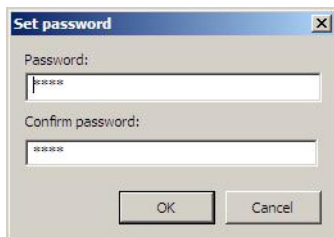

Figure 21. Set Password

4. Enter the password as specified in the Provider System (Remote Access Server) and click **OK**.

Upload Configuration

Before any objects in the provider system can be used in the subscriber system, proxy objects for the remote objects must be created in the subscriber system. This is done through an upload operation. Refer to the *System 800xA, Tools (2PAA101888*)* instruction for details.

Before the upload operation can start, you must specify what part of the provider system that should be uploaded. This configuration is done in the Upload Configuration tab of the Remote System object. Select the System Connection aspect of the previously created Remote System object. Click Upload Configuration tab.
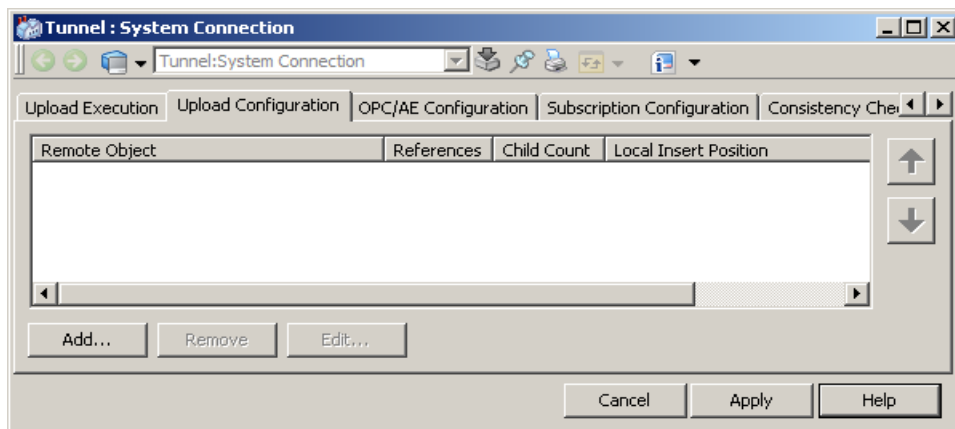

Figure 22. System Connection Aspect, Upload Configuration Aspect

If an upload is done, this view shows the number of children for this entry in the provider and subscriber system. If the count differs, the systems are not in sync and a new upload is needed. If the communication towards the provider is down <No data> is shown.

To add a new object or structure from the provider, click the **Add** button.

Try to limit the upload to the objects needed to supervise and operate the provider system only.
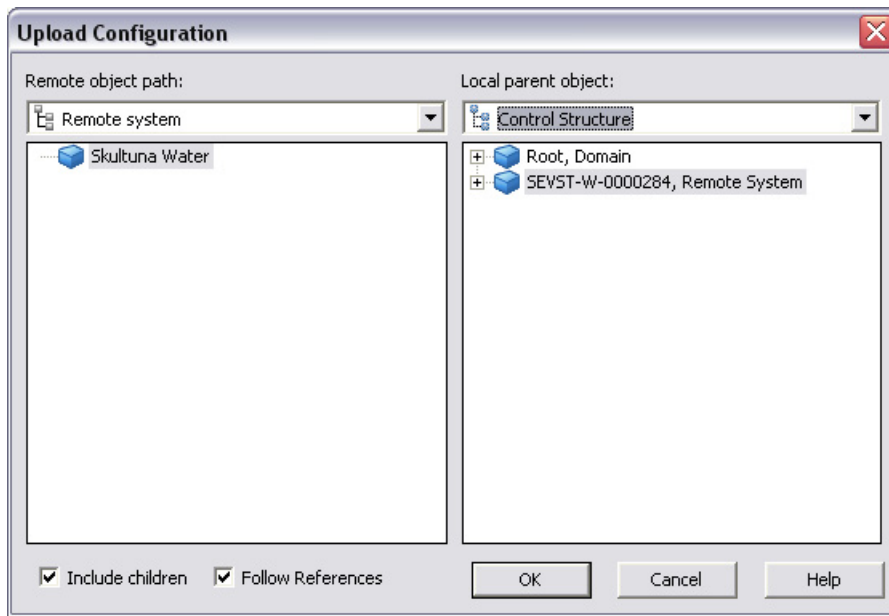
Figure 23. Upload Configuration Dialog Box

Select the desired structure/object from the provider system in the left structure selector (Remote object path). To include or remove the child objects of the selected object, select or deselect the **Include children** check box appropriately.

The **Follow references** check box controls if objects needed by an uploaded aspect should be included in the upload as well. If this check box is selected Faceplate Elements and Display Elements will be included when Faceplates respectively Graphic Displays are uploaded.

> Since all referenced objects will be uploaded, it is possible to limit the upload to only the objects with displays used for the operation of the provider system.

The right structure selector (Local parent object) makes it possible to upload to a structure other than the structure selected in the provider system. If structure selected in the subscriber system is not the Control Structure, the proxy objects for

the remote system will be uploaded below the Remote System/Inventory object in the Control Structure, in addition to the selected structure.
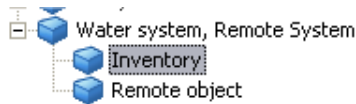

Figure 24. Inventory Object

The "Include children" and "Follow References" configuration are shown in the Upload Configuration tab in the columns References and Child Count after an upload.
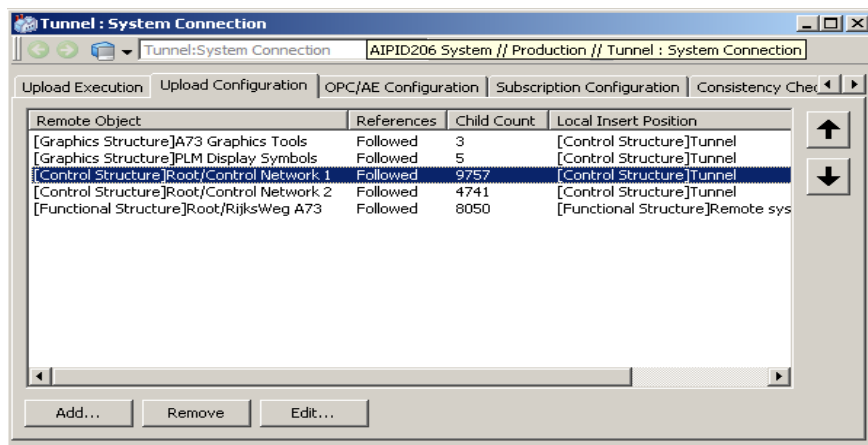
Figure 25. Upload Configuration after an Upload

The order in which structures are uploaded is significant for the VBPG if any of the graphics or references uploaded have a composite structure. Any structures containing composite structures used for graphics must be uploaded before structures using the aspects. Generally this means that the control structures, or part of the control structure, should be uploaded before the functional structure. Use the up/down button in the upload tab to change the upload order.

The aspect categories to upload are specified in the Aspect Category Definition
aspect. Select the Aspect System Structure and select the aspect category you want
to see the configuration. Figure 26 shows the Faceplate aspect category.

It is possible to incrementally add more and more objects/structures to an upload
configuration and run an upload several times. Do not delete the configuration of
the previously uploaded structures/objects when adding new ones. The upload
function compares the objects in the subscriber with the objects in the provider
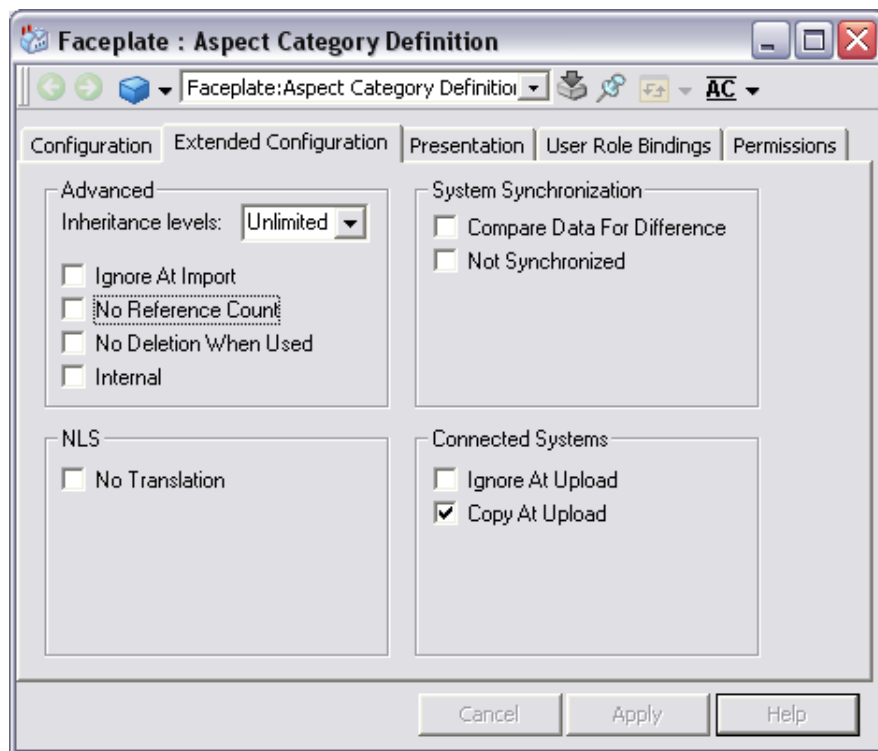and does not update the same objects or aspects twice.

Figure 26. Aspect Category Definition, Extended Configuration Tab

There are three ways to treat an aspect category when it is uploaded by 800xA
Multisystem Integration. 800xA system extensions have predefined this setting, so it
is very rare that this setting has to be changed.

- Ignore at upload
  The aspect is not uploaded to the subscriber system. Useful when an aspect category defines OPC properties that should be excluded when creating proxy aspects.

- Copy at upload
  The aspect is copied from the provider to the subscriber system.

- Create a proxy aspect
  A control connection, log configuration, or log template proxy is created.

When an aspect is copied from the provider system to the subscriber system, references to other uploaded objects and aspects are also changed. This means that an uploaded aspect is not a binary copy of the original aspect. The aspect system for the copied aspect must be installed both on the provider and the subscriber system and support the 800xA Multisystem Integration System Extension.

If structures are added and uploaded but later removed from the upload configuration, in some cases, objects will be left in the subscriber. These objects will not work correctly. To get a correct set of uploaded objects, run Clean and make a new upload before going into operation with the subscriber.

Clean command will not remove the object ID mappings for the uploaded objects. A new upload will continue to have the same object ID as the previous upload, so the displays in the subscriber system that has references to the provider objects will be valid after a clean and a new upload.

Provider Services

If a more detailed system status for the provider system is needed in the subscriber the complete service structure in the provider should be uploaded. Navigate to the Service Structure in the upload browser and select the "Services" object. Include children and references and upload to the Control Structure in the subscriber. The system status can be viewed in the system status viewer aspect also uploaded from the provider.

Node Structure

Alarm and events for objects not uploaded will be discarded in the subscriber
system. If alarms and events for actions related to nodes in the provider are wanted
the Node Administration structure should be uploaded to the subscriber. Navigate to
the Node Administration structure in the upload browser and select the node group
"All Nodes" in the provider. Include children and references and upload to the
Control Structure in the subscriber.

Composite Graphic

When uploading composite VBPG with references to instances in the Control
Structure, the objects must be uploaded explicitly to the control structure.

A large upload that involves deploy of several Visual Basic graphic aspects
continuously may cause a large memory usage, to avoid large memory usage, a
large upload should be divided into smaller parts; each part should not exceed
more than 4,000 graphic aspects.

Running Upload

Before an upload is started a complete consistency check should be performed in the
provider system on the objects configured to be uploaded. Consistency problem
may prevent a correct upload operation.

The performance of the provider and subscriber system will be affected during an
upload.

The upload reads the upload configuration and creates proxy objects in the
subscriber system for the objects and structures selected from the provider system.

The proxy objects are placed in the subscriber according to the specification in the
upload configuration.

The proxy objects created in the subscriber will get a new object identity (GUID).
This allows upload from several provider systems containing exactly the same
configuration. Aspects categories configured to be copied at upload, and all aspects
having OPC properties, Log configurations, and Log templates, not configured to be
ignored at upload, will be uploaded to the proxy objects.

Activation of an upload is done from the Upload Execution tab on the System
Connection aspect found on the Remote System object.

> ℹ It is not possible to abort an upload when the finalization of the VBPG has
> started. Finalization is when the message "Finalize of graphics started." is shown
> in the System Connection aspect. Abort can take long time if the provider has
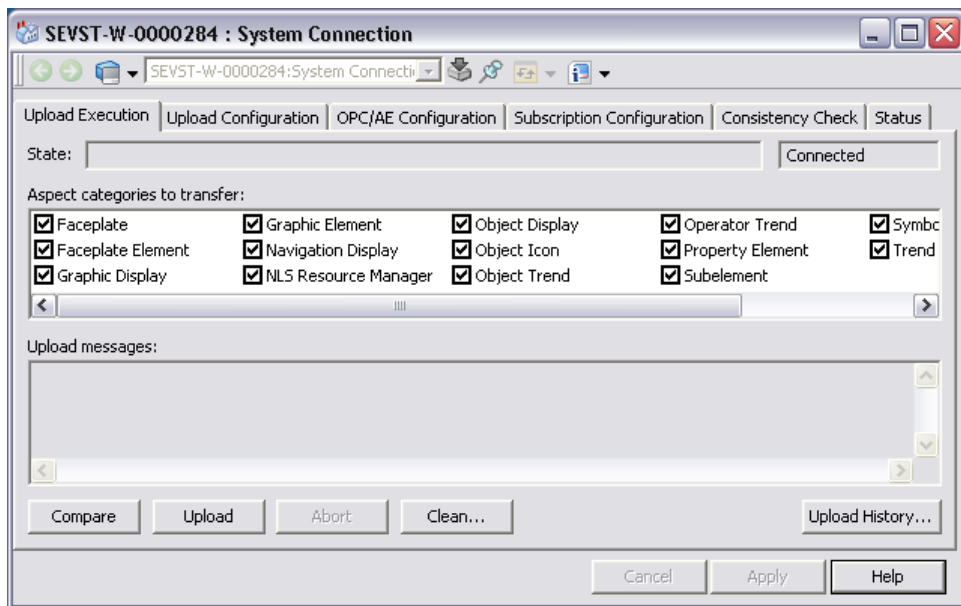> started an OPC-property scan.

Figure 27. System Connection, Upload Execution Tab

If the second State field shows "Connected" it is possible to start an upload by
pressing the "Upload" button. The first State will then show that an upload is
running. The progress of the upload can be followed in the upload messages
window.

> ℹ It is not possible to execute several uploads in parallel. Always finish an upload
> before a new one is started.

The list of aspect categories shown in the Upload Execution tab is the aspects with
the **Copy at upload** check box selected. However, it is possible to override the

configuration by un-checking the aspect category in the list above. Unchecking means the aspect category will not be uploaded.

All aspects with OPC properties, Log configurations, and Log templates will also be uploaded unless "Ignore at upload" is checked on the aspect category.

The upload execution running in the Remote Access Client and will continue even if the Plant Explorer is closed. To abort an on-going upload click the **Abort** button.

Interrupting an upload can make the uploaded proxies inconsistent and thus not working properly.

After an upload is complete, the result can be viewed either in the Upload messages window or in the Upload History viewer.

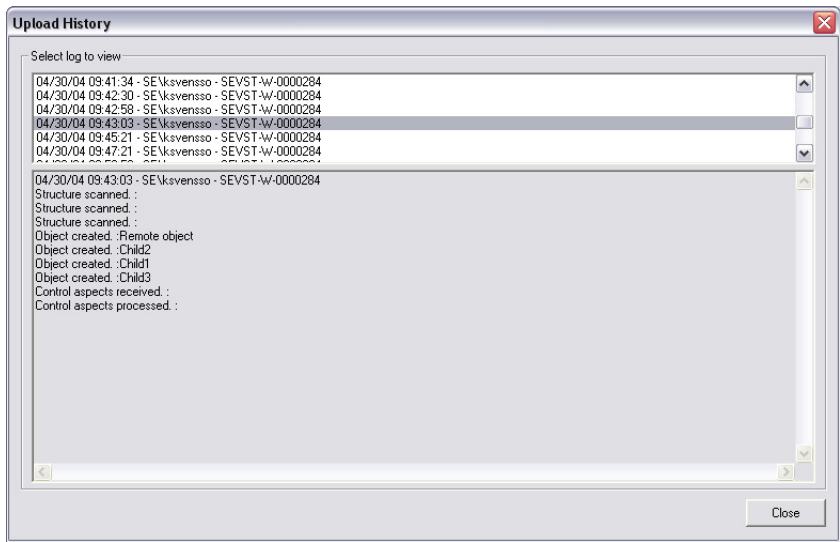To see a saved upload log, click the **Upload History** button. An upload history viewer will open.

Figure 28. Upload History Viewer

Select the upload log to view the desired log. The log will then be shown in the lower window. The number of logs stored is configured in the Remote Access

Client, Special Configuration tab. See section Remote Access Client Advanced
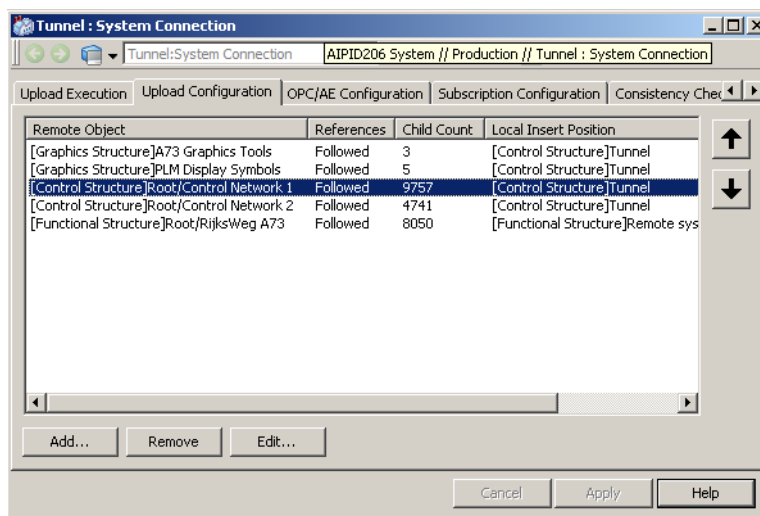Configuration on page 38.

Figure 29. Upload Configuration after Upload

The Upload Configuration tab shows how the upload is configured. The **References**
field will show Followed if the **Follow references** check box was selected. The
Child Count will show number of children uploaded. If **Include children** check box
was deselected will this field only show a "-" character.

Changes in the provider system will not automatically be uploaded to the subscriber
system. However, there is a way to see if there are any changes in the provider
compared to the state in the subscriber, and it is to use the compare function.

The compare function compares the configuration from the provider system with
the currently uploaded configuration in the subscriber. Clicking the **Compare**
button starts a comparison, and creates a compare log that is viewable in the Upload
messages window and the Upload History viewer.

The compare messages tell what will happen if an upload is performed. The
message "*Object not created.   Added object   [Control Structure]RemotePlant*"
says the object "*RemotePlant*" will be created when uploading. The same with the
messages "*Aspect not updated*" and "*Aspect not created*".

Clicking the **Clean** button removes all proxy objects and aspects uploaded for the system represented by the Remote System object. After clicking the **Clean** button confirm the clean function by selecting **Yes** in the dialog shown below.
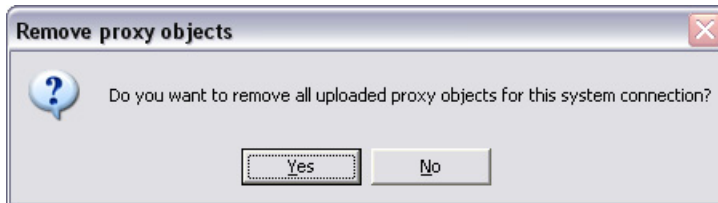

Figure 30. Clean Verification Dialog Box

Clean should be used if structures has been removed in the upload configuration between different uploads.

A new upload has to be performed to be able to operate the provider system from the subscriber system after a clean has been done.

The System Connection aspect also has a Consistency Check tab. The consistency check can detect problems, such as dangling references in object types, process displays and faceplates.
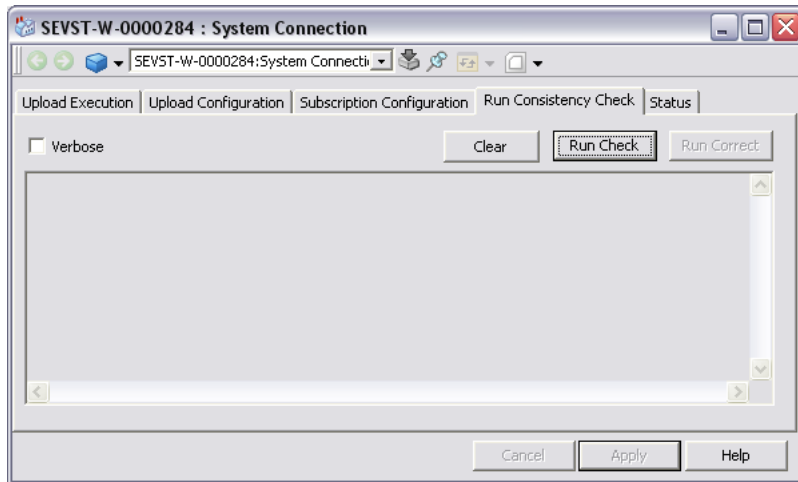
Figure 31. System Connection, Run Consistency Tab

If any inconsistencies are found during the check, the **Run Correct** button is enabled. When clicked it will try to correct the inconsistencies. If it fails, a new upload must be performed.

Proxy Objects

The proxy objects created in the subscriber system are mirrors of the objects uploaded from the provider system. Aspect having OPC properties, such as Control Modules, Function Blocks or Signals, are replaced with a proxy control connection aspect and a Remote Object Info aspect is added.
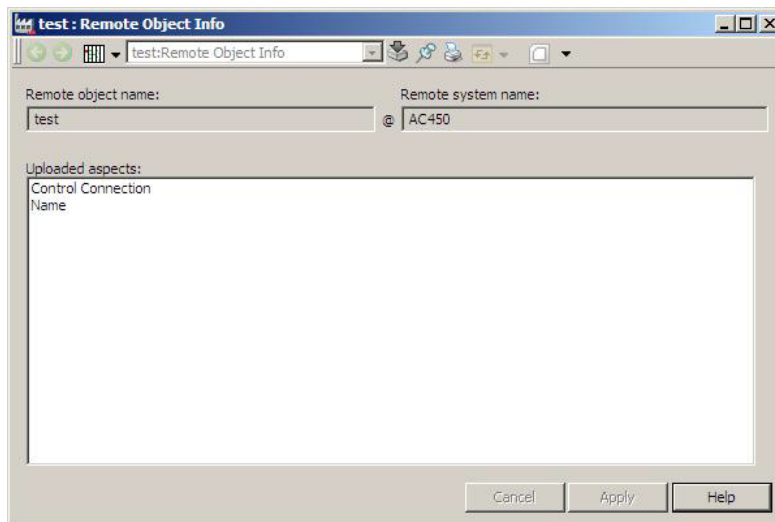
Remote Object Info Aspect

Figure 32. Remote Object Info Aspect

The Remote Object Info aspect shows the object name, the remote system name, and a list of uploaded aspects.

The remote system name is the name of the Remote System object in the subscriber system, and may differ from the real provider system name.

The Remote Object Info is used to compose the name shown in the plant explorer and aspect objects in trends and faceplates. For example, the definition of the name format is found as aspects Object Handling Profile Values, variable Name Format and Workplace Profile Values, variable Plant Explorer Settings/tab Name Composer. These aspects are available on the User object in the User Structure.

For Object Handling Profile Values the value is:

```
%Name:Plant Name:Relative Name%[%Remote Object Info%@%%]
```

For Workplace Profile Values the value is:

```
%Name:Relative Name%[%Remote Object Info%@%%][%Type Name%,%%]
```

Proxy Control Connection

A Proxy Control Connection aspect is created on the Proxy object for all aspects that defines OPC properties not marked as "Ignore at upload" in the remote system. The Proxy Control Connection shows the information for all properties, and can be used when building faceplates and displays like any other control connection aspects. It is also possible to subscribe for OPC properties values from this aspect.

It is not possible to make any configuration changes in those aspects. All changes should be done in the provider system, and uploaded again.

One optimization, to hide the properties in the control programs not necessary to have as OPC properties, affects the size of the uploaded information.

Proxy Log Configuration

A Proxy Log Configuration aspect represents a log configuration in the provider system. It has the same behavior as a log configuration in the subscriber system, but it is read-only.

Proxy Log Template

A Proxy Log Template aspect represents a log template in the provider system. It has the same behavior as a log template in the subscriber system, but it is read-only.

Miscellaneous Configuration

Security Configuration

Security for the OPC properties in the provider system is controlled by the provider system only. The domain user or the user mapped in the provider is used to evaluate the access rights. The major difference between remote user and local user evaluation of security is that the node used for the evaluation is the node where the Remote Access Server is running, not the node the user in the subscriber system is using.

The security configuration does not only affect the access rights, it also effects the user interface. If an operation is denied by the security, the user interface is dimmed. This does not work for uploaded objects and structures, since the security settings are not uploaded. To make the user interface act the same way in the subscriber as it does in the provider, the security in the subscriber node must be configured the same way as it is in the provider node, with the difference that the subscriber user/group must be used instead of the provider user/group. For details about security configuration, see *System 800xA, Administration and Security (3BSE037410*).*

Advanced Access Control

If the advanced access control functions, re-authentication and double-authentication, are used in the provider system it must also be activated in the subscriber system. If it is not activated it will be possible to write to an OPC property in the provider system without any re- or double-authentication dialog is shown in the subscriber system.

Confirm write is not supported in the subscriber system. An OPC property that requires confirm write will be changed to be read-only in the subscriber system.

Data Subscription

If the bandwidth of the connections between the subscriber system and the provider system is low it can be useful to lower the subscription times for OPC data. The System Connection aspect on the Remote System object has a configuration tab to map the original subscription times for OPC properties to new values when a remote connection is used.

The lower subscription rate can be useful if the subscriber is only used to present an overview of the providers state.
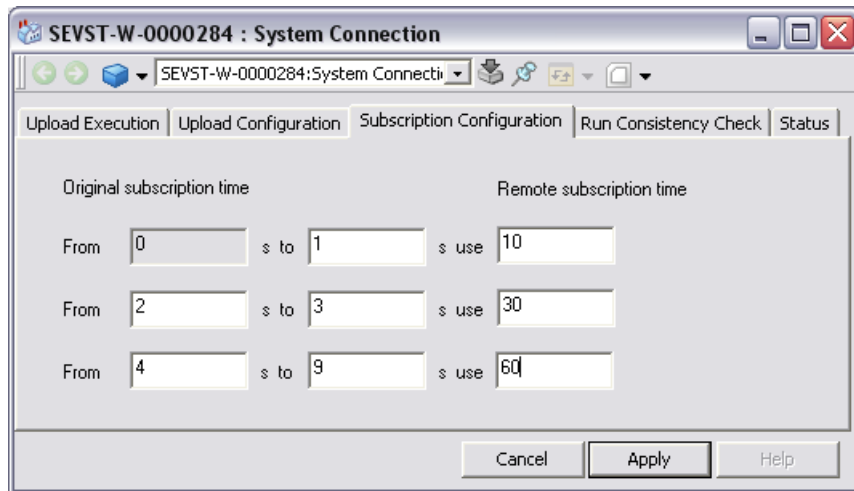

Figure 33. System Connection, Subscription Configuration

The configuration above specifies that properties with update rates 0-1 seconds will get 10 seconds, 2-3 seconds will get 30 seconds and 4-9 second will get 60 seconds.

The delay is only affecting the cyclic data, i.e a faceplate will get data directly when it is brought up.

These values must not overlap, i.e 0-10, 5-20 is not allowed, and only whole seconds can be specified.

For Advant Master controllers the fixed cyclic rates (1s, 3s, or 9s) should be used as subscription values freely selected may give a significant higher load in the controller. See *System 800xA for Advant Master, Configuration (3BSE030340*)* for more guidelines regarding Advant Master data subscription.

Process Displays

During an upload the process displays and display elements are transferred from the provider system to the subscriber. The references to the provider objects are changed to references to the proxy objects.

> Process Graphics will resolve the late binding references such as, LateBoundPropertyRef function only on the subscriber system. Ensure to include the referenced objects during an upload to the subscriber system as they are not automatically uploaded.

In some applications it is useful to have process displays that show values from more than one provider. With 800xA Multisystem Integration this is easily achieved, since the uploaded proxy aspect works identically with all other aspects with OPC data.

This means that to create a new process display with values from any connected provider system is exactly the same way as to create process displays for a single system.

> It is recommended that the additional process displays are not placed within an uploaded object, as that they will be removed when a **Clean** operation is performed.

If there are displays in the provider system using new Logical Color definition aspects, or if the default one is changed, these must be exported from the provider system and imported to the subscriber system using the Import/Export tool.

> Do not upload the Graphics Structure to the subscriber if PG2 is used. Instead, export the used generic elements and solution libraries from the provider system and import them to the subscriber system using the Import/Export tool.

Faceplates

During an upload, faceplates are transferred from the provider to the subscriber system and their references are automatically changed to the uploaded proxy objects.

> As operator notes are not uploaded, the diagnostics information for faceplates will show that the property *HoldsData* is invalid. This does not affect the functionality of the faceplate, except for the operator note.

Adding new faceplates for a proxy object is done the same way as building faceplates for a single system. It is also possible to build faceplates that work against more than one provider system.

History and Trends

The trend displays are also transferred with their log configuration during an upload, the references are changed to the uploaded proxy objects.

Building a new trend or log configuration is done in the same way as for a single system, but using the proxy objects instead of local objects.

Avoid logs of provider values in the subscriber. It is more efficient to create the logs in the provider and only view them in the subscriber.

There is one history service that connects to the provider system(s). It can be configured in the RAC history service group Special Configuration tab.
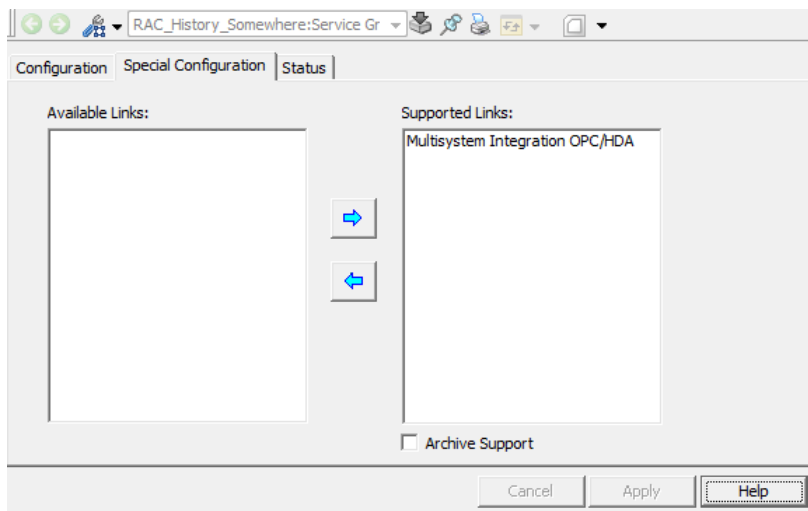

Figure 34. Remote History Service Group Configuration

The Multisystem Integration OPC/HDA link should be added to Supported Links if the creation of the History group is done manually. If no History group with this

supported link is found during the first upload, the upload will automatically create a History Group with the supported link configured.

It is recommended to use a separate History service for communication with provider system(s).

Alarm and Events

When the Remote System object is created, one event collector service is created automatically and assigned to handle subscription for the remote system. A collection definition object is also created for each remote system that is added to the subscriber system. When an upload is performed event categories are uploaded to this collection definition object.

> Before the first upload the event collector will indicate an error, OPCAE_STATUS_NOCONFIG. After the first upload the status will be good.

Alarms from the provider system will be collected for objects that have been uploaded only. Alarm and Event lists on proxy objects will be uploaded together with their List Configuration and Color Definition aspects.

For large configurations with many provider systems it is possible to add more collector services and change the default assignment. The event collector group assignment is changed in the OPC/AE Configuration tab of the System Connection aspect in the Remote System object.
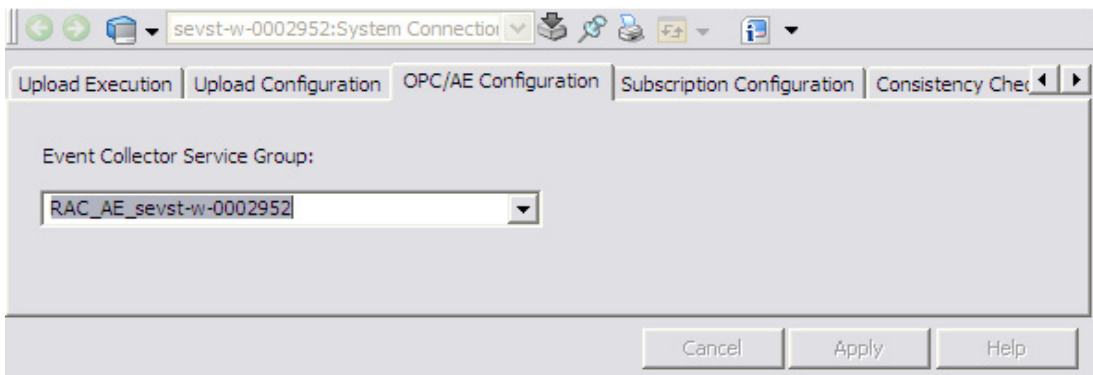

Figure 35. System Connection, OPC/AE Configuration

The Alarm and Event List configured on the subscriber to show the alarms from the provider systems must be reconfigured to show the column SystemName. The SystemName column shows the name of the provider system, i.e the name of the Remote system object.

Alarm Manager Configuration

For consistent and correct behavior in the connected systems it is important that the Alarm Manager configuration is properly configured. The following recommendation for the Special Configuration must be followed:

1. Use the same settings for Alarm Handling in the provider and the subscriber system.

2. Also use the same setting for Event Logging in the provider and the subscriber system.

3. Make sure that Alarm Storage in the subscriber system is large enough to hold both the local alarms and the remote alarms. If for example the subscriber system is connected to one provider system, the size should be double and so on.
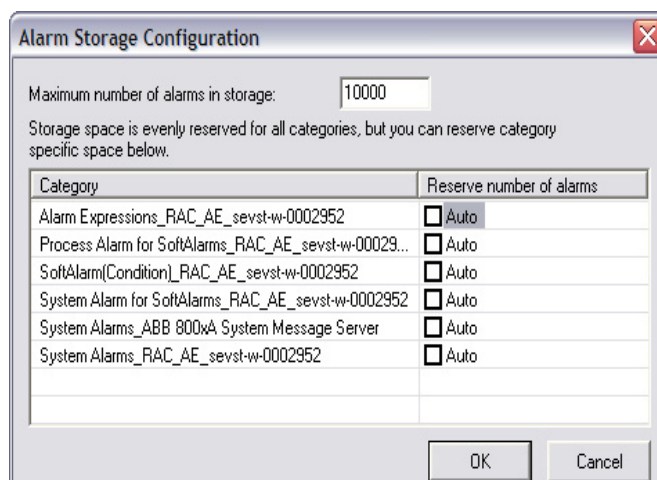

Figure 36. Alarm Storage Configuration

Alarm Hiding

Alarm hiding should be configured in the provider system. Alarms hidden in the provider will show up in a hidden alarm list in the subscriber system. It is however not possible to show the corresponding hiding rule in the subscriber for a hidden alarm, since the hiding rule only exists in the provider.

Alarm Shelving

Alarm shelving configuration is done in library structure in both provider and subscriber systems. For a consistency behavior it is recommended that shelving configuration conforms for provider and subscriber.

Audible Alarms/Global Silence

Global silence is a function which allows an operator on one workplace to silence an alarm on all workplaces. If global silence is used with Multisystem Integration, a silence operation made in the provider will also affect the subscriber and vice versa.

Feature Pack Functionality_____

Point of Control Support

This section applies to the System 800xA 5.1 Feature Pack release only.

Point of Control is a concept that allows division of the plant into sections. The operator controlling a section is called the Responsible User. The Responsible User has all access rights for the section. A typical scenario is that only the Responsible User will be able to control the process in this section.

Using Point of Control with Multisystem Integration, the responsibility can be taken locally on the provider system, and remotely on the subscriber system. For more information on the Point of Control function, refer to *Point of Control* section in *System 800xA Administration and Security (3BSE037410*)*.

The responsibility can be transferred between the provider systems located within the plant area and also between the provider system and the subscriber system.

Enabling Point of Control

To use Point of Control in the subscriber system, a valid license key is required and the Point of Control must be enabled. For more information on Enabling Point of Control, refer to *Enabling Point of Control* section in *System 800xA Administration and Security (3BSE037410*)*.

Execute one of the following methods to enable the Point of Control:

1. Select **Point of Control** from **Start > ABB Industrial IT 800xA > System > System Configuration Console > Security.**

    In the **System 800xA Configuration Console** dialog, select **Yes, enable Point of Control**, and click **Apply** (see Figure 37)**.** By default, the Point of Control functionality is disabled.
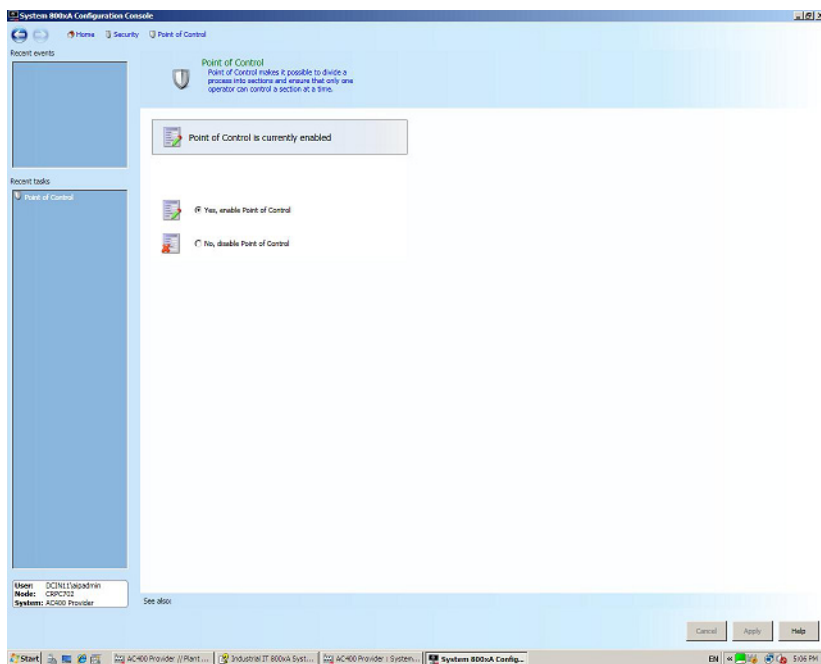

Figure 37. Enabling the Point of Control thru SCC

2.   Select **System Setting** aspect from **Admin Structure** > **Subscriber2, Domain** (System Name).

In this aspect, select *True* in the **Values** column for *Point of Control* (see Figure 38).
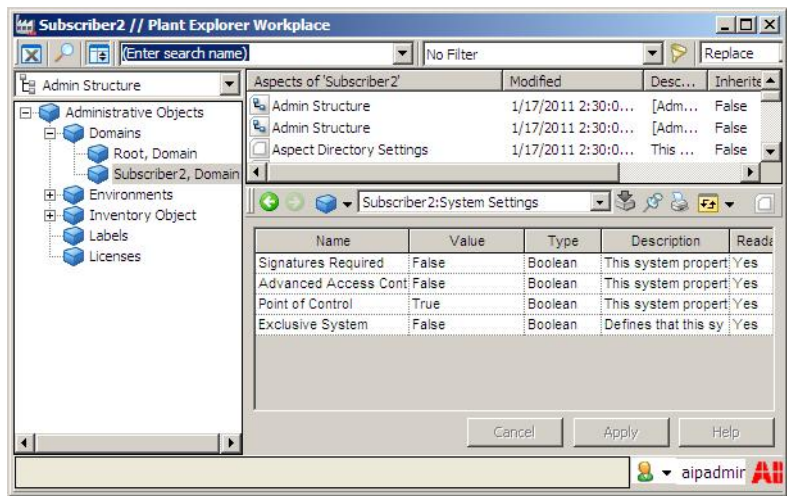

Figure 38. Enabling the Point of Control through System Setting Aspect

The Point of Control feature is configured by a System Engineer.

Configure permission is required to configure the **Section Definition** aspects. Add the System Engineer to the Application Engineer group or explicitly provide the Configure permission to the System Engineer.

Upload Configuration

Ensure that when configuring the *Upload*, the complete section is uploaded. It is not possible to upload a subsection or a single object that belongs to a complete section. During upload, the used responsibility configurations are uploaded to the subscriber system. For more information refer to Upload Configuration on page 41.

User Mapping

Ensure that the mapped users belong to the same user group in the provider, similar to that in the subscriber. If the user groups other than the default groups are used, they must be exported from the provider and imported to the subscriber.

Node Configuration

To take the responsibility in the subscriber system, **All Nodes** must be used as node configuration in the provider system. See Figure 39.
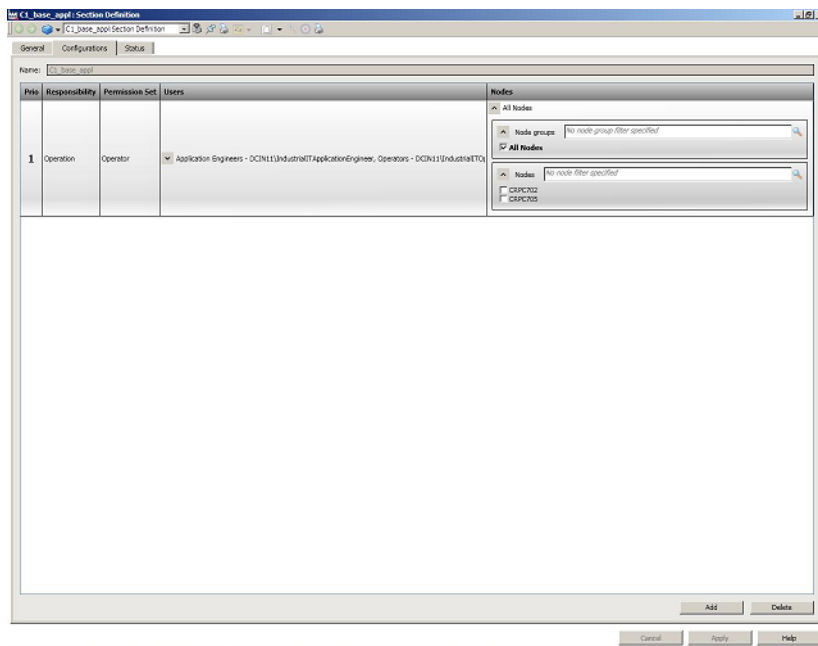

Figure 39. Node Configuration

Before uploading the **Section Definition** aspect to the subscriber, all nodes should be configured in the **Section Definition** aspect of the provider.

_____

Asset Optimization

This section applies to the System 800xA 5.1 Feature Pack release only.

Asset Optimization brings maintenance management to the operator environment to provide a single window interface for all Asset Management related operations. This allows the plant personnel to collect, compare, and monitor asset data to accurately assess equipment conditions in real time.

For maintenance personnel, Asset Optimization provides a default Maintenance Workplace that supports daily maintenance activities in a most efficient way.

Using Asset Optimization with Multisystem Integration, the Condition Reporting and Monitoring, and Work Order Management functions can be performed remotely from the subscriber system. For more information on the Asset Optimization, refer to *System 800xA Asset Optimization Configuration (3BUA000118*)* and *System 800xA Asset Optimization Operation (3BUA000150*)*.

Asset Optimization Aspects

During the upload operation, Asset Optimization aspects are replaced on the proxy object, with the **Web View** aspect that provides the similar functionality in the subscriber system.

Table 1 provides the mapping for Asset Optimization aspects and the aspects of the category **Web View**.

Table 1. Mapping for Asset Optimization aspects and Web View aspect

Provider System	Subscriber System
Asset Viewer	Asset Viewer Web View
Asset Reporter	Asset Reporter Web View
Asset Reporter with System Status	Asset Reporter Web View

Table 1. Mapping for Asset Optimization aspects and Web View aspect

Provider System	Subscriber System
Fault Report Submitter	Fault Report Submitter Web View
CMMS View(s)	CMMS Web View(s)

Configuration

The **Web View** aspects communicate with the **AOWebServerNode** in the provider system using the Hypertext Transfer Protocol Secure (HTTPS) / Hypertext Transfer Protocol (HTTP) communication protocol.

During upload, the default configuration is to use the **AOWebServerNode** host name and **HTTPS** protocol. The default configuration can be changed using the **Asset Optimization Configuration** aspect.

> If the **AoWebServerNode** is protected with firewall, ensure that the ports **443** (HTTPS) or **80** (HTTP) is open in the firewall based on the communication protocol selected in the **Asset Optimization Configuration** aspect.

Asset Optimization Configuration Aspect

The **Asset Optimization Configuration** aspect is added to the **Remote System Object** that represents the provider system in the subscriber system, when the **Remote Access Service** is started. This aspect controls the communication parameters that are used by the Asset Optimization **Web View** aspects.

The main view of this aspect (see Figure 40) shows the current configuration parameters for the Communication Protocol and the AoWebServerNode Host Name or IP Address that are used in the communication.
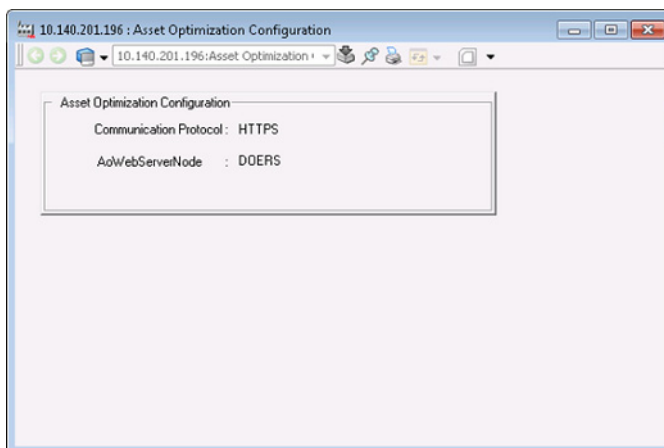
Figure 40. Asset Optimization Configuration Aspect-Main View

Communication Protocol. The default communication protocol is **HTTPS**. It is also possible to use the **HTTP** protocol.

When HTTP protocol is used, the data passed between Subscriber and Provider is not encrypted. The HTTP Communication Protocol must be selected only after assessing the security requirements.

To change the Communication Protocol settings:

1. Go to the **Config View** of the **Asset Optimization Configuration** aspect and select **HTTP**.

Figure 41. Changing the Communication Protocol

2. Click **Apply** to save the settings.

AOWebServerNode. The default configuration is to use the **AOWebServerNode** host name for the communicating with the Provider Asset Optimization Server. It is possible to use the IP address of **AOWebServerNode** for communication instead of the host name.

To change the host name or IP address settings:

1. Go to the **Config View** of the **Asset Optimization Configuration** aspect and select **IP**.
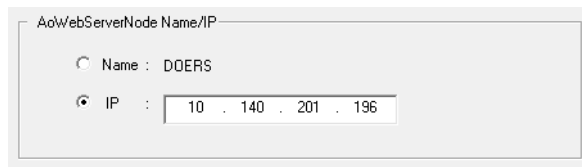
2. Enter the IP address of the **AOWebServerNode**.

Figure 42. Changing the IP address

3. Click **Apply** to save the settings.

This configuration change does not require an upload of objects.

HTTPS Communication Protocol

This section describes the steps to be performed when using **HTTPS** as the Communication Protocol.

Secure Socket Layer (SSL) Certificates

The Asset Optimization data communication between the subscriber and provider system is secured and encrypted using the SSL Certificate. The SSL certificate must be installed and configured on the **AOWebServerNode** in the Provider system.

The following are the requirements for the SSL Certificate:

1. The Common Name (CN) must be the host name of the **AOWebServerNode**.

2. The recommended validity of the certificate is up to 4 years.

3. The recommendation for RSA Key Size is 1024 bits.

ℹ️ For information on generating certificate request, installing the certificate, and renewing the certificate, refer to the Microsoft Internet Information Server documentation.

IIS Site Bindings

After installing the SSL certificate, the HTTPS binding must be added to the Internet Information Server running on the **AOWebServerNode** to allow the HTTPS communication in the Provider system.

Execute the following to configure the HTTPS binding using the SSL certificate with the CN **WD-03-AO**:

1. Open the **Internet Information Services** (IIS) **Manager** on the **AOWebserverNode** in the Provider system.

2. Select **Sites > Default Web Site**.

3. Click **Bindings** in **Actions > Edit Site**.

4. Click **Add** and select **Type** as **https** and enter the **Port** as **443**. See Figure 43.

    The **SSL certificate** lists the installed SSL certificates. Select the certificate that is installed to be used for securing AO communication.
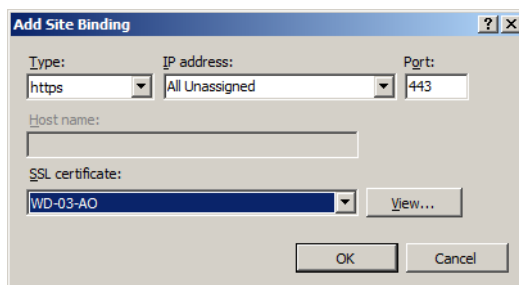

Figure 43. Changing the values in Bindings

5. Click **OK** to save the changes, and then click **Close**.

Importing Root Certificates

The certificate of the issuing Certificate Authority must be added to the **Trusted Root Certification Authorities** store on the Asset Optimization Client and Server Nodes in the Subscriber system.

Execute the following steps to import the certificate:

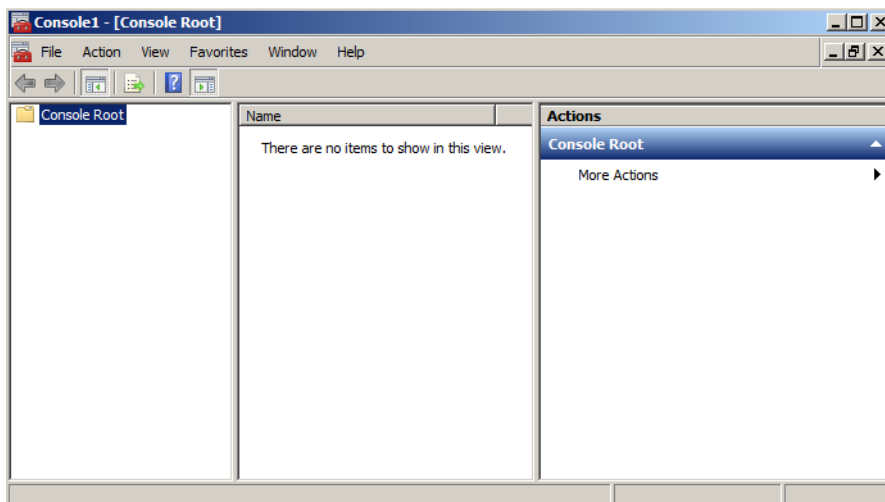1.   Select Start and enter **mmc** in the Search field. The **Console 1** dialog appears.

Figure 44. Console 1

2.   Select **File > Add/Remove Snap-in**. The **Add or Remove Snap-ins** dialog appears.
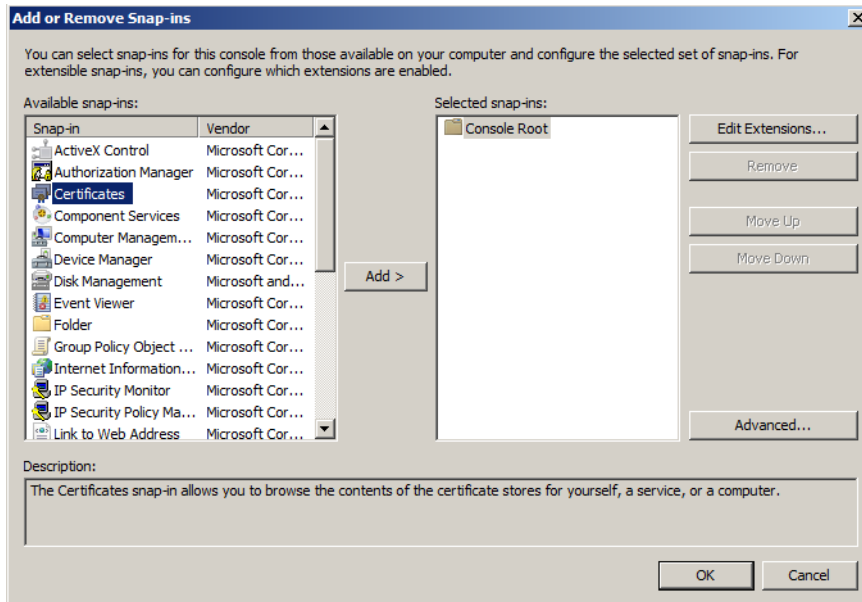

Figure 45. Add or Remove Snap-ins

3.   Select **Certificates** and click **Add**. The **Certificates snap-in** dialog appears.
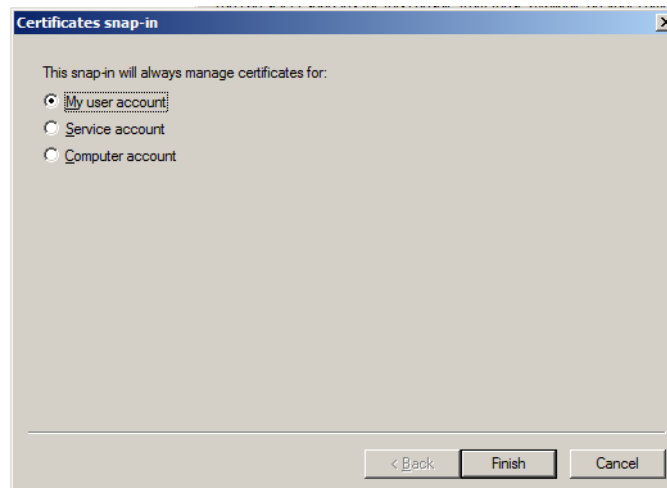
Figure 46. Add or Remove Snap-ins

4. Select an account and click **Finish**.

5. Right-click **Trusted Root Certification Authorities** and select **All Tasks >
    Import** from the context menu.

Figure 47. Importing Trusted Root Certification Authorities

Limitations

Export/Import

Export/Import is not possible to use with uploaded objects or structures since part of the information for the proxy objects is stored in the Remote Access Client service.

Logical Colors

User defined logical colors used in graphic displays must be moved from the provider to the subscriber by exporting and importing them.

Composite Graphic

Composite VBPG displays with references to instances in the control structure must explicitly be uploaded to the control structure. If an old composite display resides both in the functional structure and the control structure, the control structure should be uploaded before the functional structure.

Aspect Link Control

Aspect link control dynamically programmed from Visual Basic can not be uploaded from the provider and used in the subscriber system. Only use statically configured aspect links.

Confirmed Write

Properties using confirm write is not supported by Multisystem Integration. OPC properties using confirm write will be uploaded as read-only properties. Confirmed write is used to write SIL-data to High Integrity (HI) controllers.

Object Lock

Object lock for systems with mixed AC800M controller and 800xA for Advant Master controllers are supported. The only lock policy supported is *Lock Optional for Operation*.

Object lock policy must be the same for the subscriber and all providers. It is not possible to have different lock policies on different systems.

The Power Plant libraries for PI and PT cannot be used together.

Section 4 Operation

Overview

Operation of a remote provider system is done the same way as operation of a local system, with the exception that the speed of operation may be slower if the connection towards the remote system is slow. With a connection speed of 10 MBit/s or higher the delay is hardly noticeable. This section shows additions and deviations in operation for Multisystem Integration compared to ordinary operation. See *System 800xA, Operations (3BSE036904*).*

Process Displays

Process displays with process provider system work the same way as local process displays, with the addition that the name and tool-tip for objects include the system name. For example, the tool-tip for the object Remote object at provider system Water system will be Remote object@Water system.
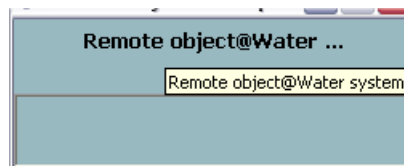

Figure 48. Remote Object Tooltip

Object Displays for Advant Master only shows the object name.

In order to show System Alarms from Advant Master Controllers, an additional upload of AC 400 System Event Names and descendant objects in the Control Structure needs to be performed.

Faceplates

Faceplates for a remote provider system work in the same way as a faceplate for a local object. The name and the tool-tip will show the object name with the provider system name.

Trends

Trends for a remote provider system work in the same way as a trend for local objects, but with the name and the tool-tip changed the same way as for faceplates and process displays.

If a trim curve from a remote system displays values in the past or in the future there probably is a problem with the time synchronization between the subscriber and provider. See Appendix B, Fault Tracing for details of how to check the difference.

Object Trends for Advant Master only shows the object name.

Alarm and Events

Alarm operations can be performed from the subscriber system, or the provider system. Operations done in the provider system will also affect the subscriber system.

Alarm operations include:

- Acknowledge

- Alarm comments

- Enable/disable conditions

- Global silence

- Remove alarm (used with the "Keep inactive-acknowledged alarms" feature)

- Delete alarm

- Alarm hiding

- Alarm shelving

Alarm and event lists for a remote provider system works the same way as an alarm and event lists for a local object/structure, except that "Delete" of an alarm is only local to the provider and subscriber i.e. an alarm is not deleted in the subscriber when deleted in the provider.

The system name column shows the name of the system from which the alarms are emitted. This is typically useful when configuring alarm and event lists in the subscriber system that shows both local and remote alarms.

The column "SystemName" must be added manually.

If the time stamp for an alarm or event shows up too long in the past or in the future there probably is a problem with the time synchronization between the subscriber and provider. See Appendix B, Fault Tracing for details of how to check the difference.

History Log Updates

History Log updates for a remote provider system work the same way as for local objects. Security checks are done both in the provider and subscriber system but audit events are generated and logged in the provider system only.

Feature Pack Functionality_____

Operating the Point of Control

This section applies to the System 800xA 5.1 Feature Pack release only.

This section describes the procedure to use the Point of Control feature for Multisystem Integration,

For more information on using the Point of Control feature, refer to the *Point of Control* section in *System 800xA, Operations (3BSE036904*).*

Point of Control Summary Aspect

The **Point of Control Summary** aspect displays the responsibility status of all configured sections. Select the **Filtered mode** check box, to display current objects (see Figure 49 and Figure 50).
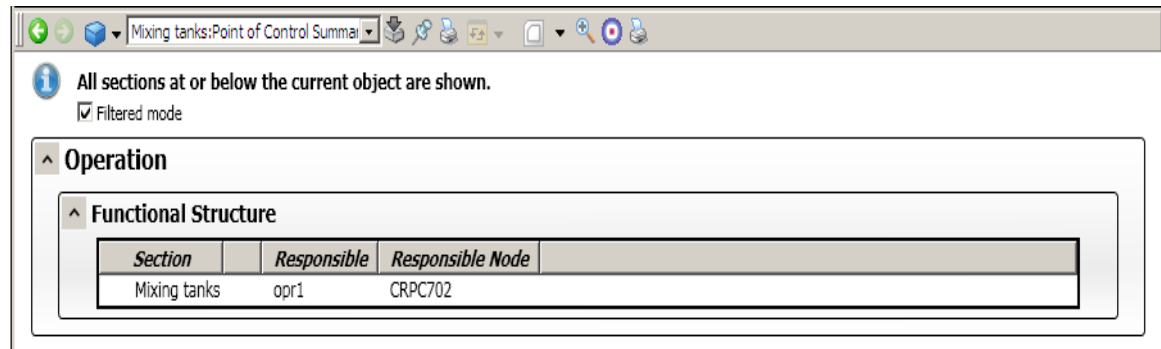

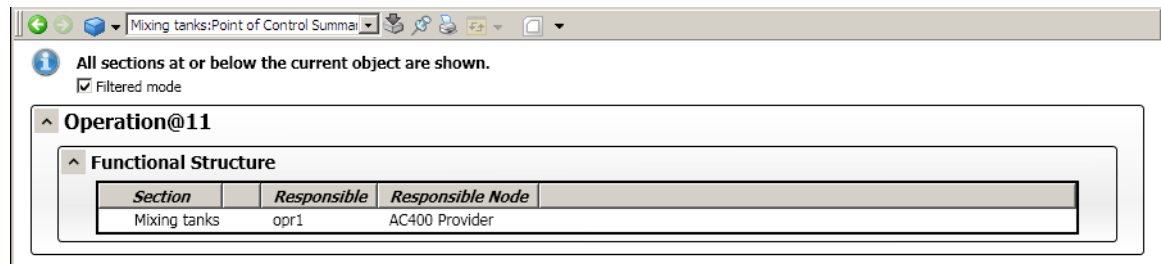*Figure 49. Point of Control Summary Aspect in the Provider System*

Figure 50. Point of Control Summary Aspect in the Subscriber System

The name of the provider or subscriber system is displayed in the **Responsible Node** field. If the connection between the subscriber and provider system is lost, the

Point of Control Summary dialog displayed in both the subscriber and provider system displays that the subscriber system has responsibility instead of the subscriber node.

If the responsible user in the provider system is not mapped to a subscriber user the responsibility status will display *Remote User* in the subscriber.

Transfer of Responsibility

The Point of Control functionality allows responsibility interaction from any object that belongs to a section based on the following three protocols:

- Request Responsibility

- Grab Responsibility

- Release Responsibility

For more information, refer to *Transfer of Responsibility* section in *System 800xA, Operations (3BSE036904*)*.

Request Responsibility

The responsibility of a section can be requested using the object context menu. When a user requests the responsibility of a section, a tree structure including the section with subsections is displayed.
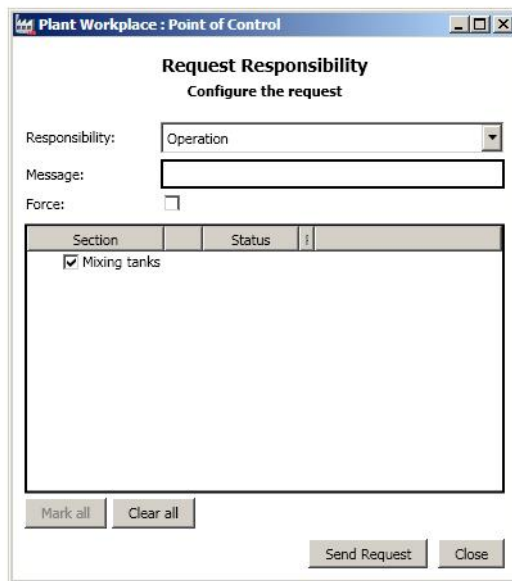
The user can select the required sections and subsections to take the responsibility. The currently responsible user can allow or deny the request for responsibility (see Figure 51).

Execute following steps to request a Request Responsibility:

1. In the **Request Responsibility** dialog, select the responsibility type in **Responsibility**. For example, if the user has only the operation responsibility configured, it is selected by default.

When the responsibility for a section is requested, the subsections are automatically included.

Figure 51. Request Responsibility Dialog

2. Type the message in the **Message**, describing the reason for the responsibility request. The message will be shown to the responsible user and stored in the audit list.

3. Select the sections to take over the responsibility and click **Send Request**.

After the request for the section is sent, the **Handover Responsibility** dialog appears to the current responsible user in the corresponding node. The current responsible user can select **Accept all**, **Deny all**, or **Accept Selected** sections (see Figure 52).
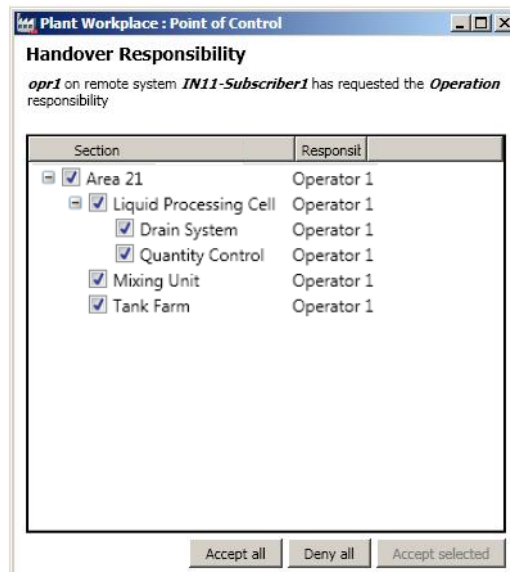

Figure 52. Handover Responsibility

> The users displayed in the Point of Control dialogs of the subscriber system are modified through the user mapping done on a Remote Access Service (RAS).

If the responsible user accepts the request, the responsibility is immediately transferred and a confirmation is sent to the new responsible user (see Figure 53).

Figure 53. Request Responsibility after the Request is Taken

If the user in the subscriber system is not mapped in the provider system, the error message will be displayed in the **Status** column (see Figure 54).

⚠ The responsibility is kept in the subscriber system when the connection is broken. The provider must use the grab responsibility to take the responsibility from a disconnected subscriber.

Figure 54. Request Responsibility after the Request is Denied.

_____

Asset Optimization

This section applies to the System 800xA 5.1 Feature Pack release only.

This section describes the usage of Asset Optimization with Multisystem Integration.

Condition Reporting and Monitoring, and Work Order Management

During the upload operation, Asset Optimization aspects that provide Asset Condition Reporting and Monitoring, and Work Order Management capability are replaced on the proxy object, with the **Web View** aspects that provide the similar functionality in the Subscriber system.

When these aspects are called-up, the aspect will communicate with the **AOWebServerNode** on the Provider system and display the information and status values of the remote object in the Subscriber system. A refresh operation is required to view the dynamic status changes.

Table 2 provides the mapping for Asset Optimization aspects and the aspects of the category **Web View**.

Table 2. Mapping for Asset Optimization aspects and Web View aspect

Provider System	Subscriber System
Asset Viewer	Asset Viewer Web View
Asset Reporter	Asset Reporter Web View
Asset Reporter with System Status	Asset Reporter Web View
Fault Report Submitter	Fault Report Submitter Web View
CMMS View(s)	CMMS Web View(s)

> **i** If the **Read-only connection** check box is selected while configuring the Remote
> Access Server, it shall not be possible to Dismiss the fault report, Submit, or
> Create a new Work Order using the **Fault Reporter Submitter Web View** in the
> Subscriber system.

CMMS Views (Maximo, SAP/PM)

The **CMMS View** aspects for the Maximo and SAP/Integration are replaced with
the **CMMS Web View** aspect on the proxy object that is uploaded to the Subscriber
system. These aspects provide the similar functionality and communicate with AO
Web Server node in the Provider system.

Table 3 and Table 4 provides the mapping for the **CMMS Views** aspects and the
aspects of the category **Web View**.

Table 3. Maximo Integration

Provider System	Subscriber System
View Active Work Orders	CMMS Web View
View Equipment Status	CMMS Web View
View Prev Maint Schedule	CMMS Web View
View Spare Parts	CMMS Web View
View Work Order History	CMMS Web View

Table 4. SAP Integration

Provider System	Subscriber System
SAP View Active Work Orders	CMMS Web View
SAP View Equipment Status	CMMS Web View
SAP View Prev Maint Schedule	CMMS Web View
SAP View Work Order History	CMMS Web View

The highlighted hyperlink in the **CMMS Web View** aspects opens the corresponding CMMS system web portal pages. Connectivity to the CMMS Web Portal from the Asset Optimization nodes is required in the Subscriber system.

Authentication

The access to the **Web View** aspects is restricted using the Windows Integrated Authentication on the Provider system. The Windows authentication credentials of the user in the Provider system that is mapped to the current user in the Subscriber system, must be provided when calling up the **Web View** aspect in the Subscriber system.

This is required in the following scenarios:

•   When the Provider and Subscriber system are in different domain.

•   If a different set of user name or password is used in the Provider and Subscriber system in a workgroup environment

•   When the IP address is used to communicate with the **AOWebServerNode** in Provider system.

The credential must be provided once per session and will remain valid till the time-out of the current session. A session is created when the **Web View** aspect is called with in the Workplace or when a new floating Internet Explorer window is launched from the **Web View** aspect.

_____

Section 5 Maintenance

Backup and Restore

The configuration data for the proxy objects has to be included in the Backup and Restore. The backup configuration is done in the Maintenance structure. Select the Backup Definition object, and create an object below it of type Full Backup. A recommendation is to include the remote system name and current date in its name.

Select the Backup Definition aspect, change backup type to External Services and check the Remote Access Client service.
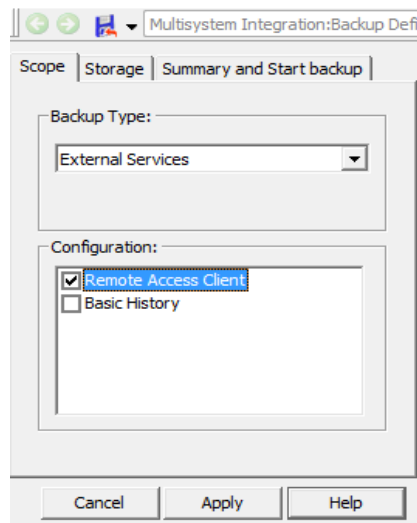

Figure 55. Backup Definition for Remote Access Client

Select the **Summary** and Start Backup tab and click the **Start Backup** button to make a backup of the Remote Access Client service.

When the Remote Access Client is backed up a full backup of the aspect directory should be done.

> If there are problem with deploy of the uploaded graphics the backup will also contain the same warnings. Try to make all uploaded graphics correct before it is backup.

Restore procedure

Restore must be done both of the Aspect Directory data and the additional Remote Access Client service proxy object data.

For a description about how to make a restore of the Aspect Directory data, refer to *System 800xA, Administration and Security (3BSE037410*).*

When a provider system is restored, the Aspect Directory and the file set distribution services obtain new service identities.

If the service structure was uploaded from a provider to a subscriber, the system status information will be down for these two services. To correct this problem, make a new upload from the provider after a restore.

> A *Clean* operation is not required before the upload.

> If a provider system is upgraded to System Version 5.1 a new upload to the subscriber system is done to correct the service IDs if uploaded from the provider.

To restore the proxy objects for the Remote Access Client, follow the following procedure.

> Ensure that the Remote Access Client service has entered the **Service State** before starting the restore of it.

1. Select the Maintenance Structure and select the Remote Access Client backup object created when the backup was done.

2. Select the Backup Info aspect on the object.

3.   Select the **Restore** tab and check the **Remote Access Client** check box and Unit 0; click **Apply**.

4.   Click the **Restore** button to finish the restore.

After the restore of the subscriber node, restart the Remote Access Client. You can perform this task by killing the AfwRAC process from the task manager.

> A restore of the Remote Access Client service is necessary for the uploaded objects to work. Without a valid backup of the Remote Access Client, the provider system must be uploaded again to the subscriber system.

System Alarms and Events

800xA generates a number of system alarms and events. Table 5 shows under what conditions they are generated.

Table 5. System Messages

Message Description	Extended Description
Host '%HOST%' disconnected.	Connection from the RAC to the RAS broken. This alarm is generated both in the subscriber and provider end.
Connection to '%HOST%' accepted.	Connection established from the RAC to the RAS. This event is generated in the subscriber and provider end.
The node '%HOST%' could not be accepted (incorrect password).	Connection refused due to wrong password. This event is generated in both ends.
No user mapping for remote user '%USER	No user mapping found when an attempt to perform an operation was done. This event is generated in both ends.

Table 5. System Messages (Continued)

Message Description	Extended Description
The protocol '%PROTOCOL%' was not found (%APPL%:%NODE%)	Failed to load a protocol. This message is generated for the system that fails to load.
Time difference between systems exceeds limit, time difference=%Diff%	Time differs between the subscriber and provider. This event is generated every hour in both ends if the time difference is more than 5 minutes.
Unknown tcp/ip address in use ('%IPADDR%)	An symbolic IP-address can not be resolved by the DNS service. This event is generated every hour in the subscriber end.

It is possible to turn all system events into a system alarm with help of the System Alarm function. Refer to the *System 800xA, Configuration (3BDS011222*)* instruction for details.

Audit Events

Audit events are generated both in the subscriber and provider, but for different activities. All process related activities, like OPC property writes, history log updates and alarm acknowledgement are stored in provider and also viewed in subscribers audit list. Some activities like starting, aborting or finishing an upload, or compare, will generate an audit trail both in the provider and the subscriber. The audit events configurable as system alarms are:.

Table 6. Audit Events

Name	Description
OPCItemWritten	OPC property written. Generated in the provider.
AuditEvent_Acknowledge	Alarm acknowledged. Generated in the provider.

Table 6. Audit Events (Continued)

Name	Description
OPCHDASingleUpdates	A single historian value has changed. Generated in the provider.
OPCHDAMultipleUpdate	Multiple historian values have been changed. Generated in the provider.
UploadStarted	Upload started. Generated in both provider and subscriber.
UploadStopped.	Upload finished. Generated both in provider and subscriber.

The user account and full name shown in the audit list in the provider system will be the user in the provider. When subscriber and provider is running in different Windows domains, the user mapping table, configured for the Remote Access Server, will be used to look up the user in the provider system to use when the audit trail is generated.

> When it is essential to comply with Food and Drug Administrations (FDA) regulations a one-to-one mapping between a user in the provider system and a user in the subscriber system should be used.

System Status
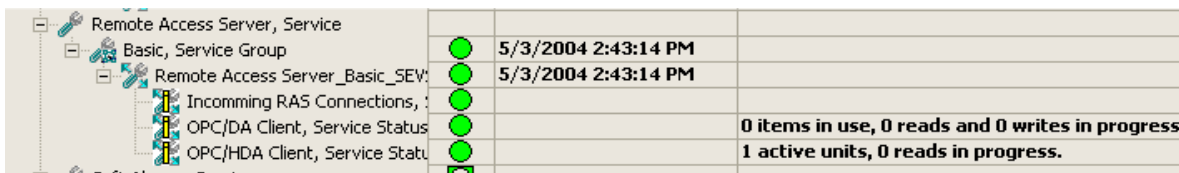
The system status function is extended to facilitate fault tracing of a remote system connection. The overview part is the same as in a regular 800xA system, but the service provider object can be opened to show more details about the connection between the Remote Access Server and Remote Access Client.

Figure 56. System Status Overview

The Remote Access Server and Remote Access Client show up in the system status viewer like all other services, using the same color scheme to indicate if there are any problems with the services.

A difference between the Remote Access Server/Remote Access Client and other services is that the service can work correctly, but still fail to fulfill its duties because the other part, the subscriber/provider, is not working correctly. This type of failure can be detected if the service providers are expanded in the system status viewer.
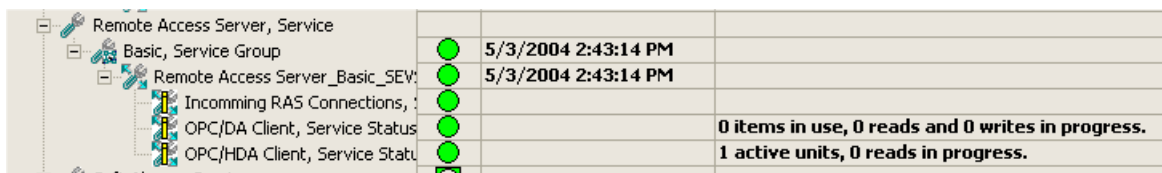
Figure 57. System Status Details, Remote Access Server

The system status details for the Remote Access Server shows incoming connections for Remote Access Clients to the Remote Access Server, OPC Data Access clients, Alarm and Event clients, and OPC History Data Access clients.

Similar information can be viewed on the Remote Access Client.

Figure 58. System Status details, Remote Access Client

Detailed information about the communication between the Remote Access Client and the Remote Access Server is available in the Connection and Protocols tab for the service group and service provider objects.

If the Service Structure of the provider has been uploaded, details about the services can be viewed in the System Status Viewer.

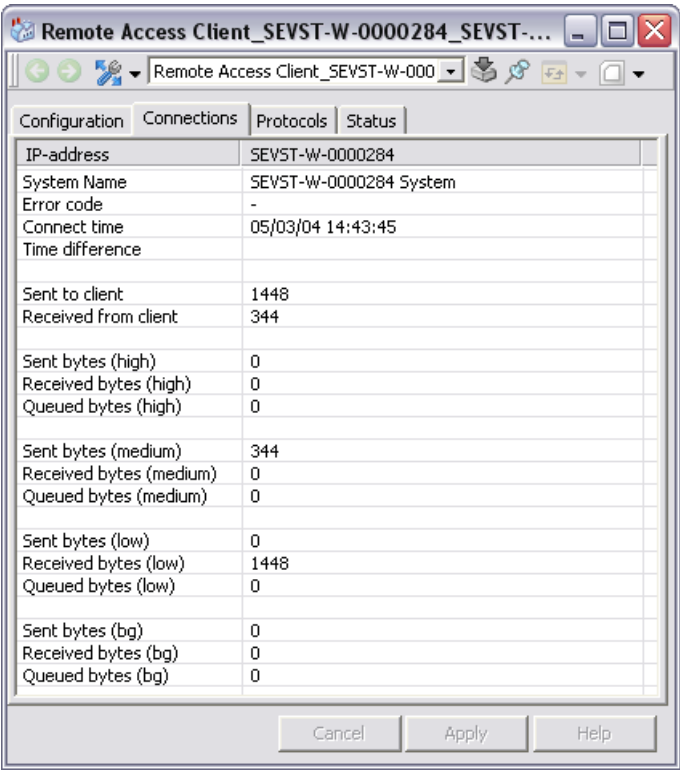Figure 59 shows the connection tab of the Remote Access Client provider.

Figure 59. Remote Access Client, Connection Tab

Table 7 describes each field.

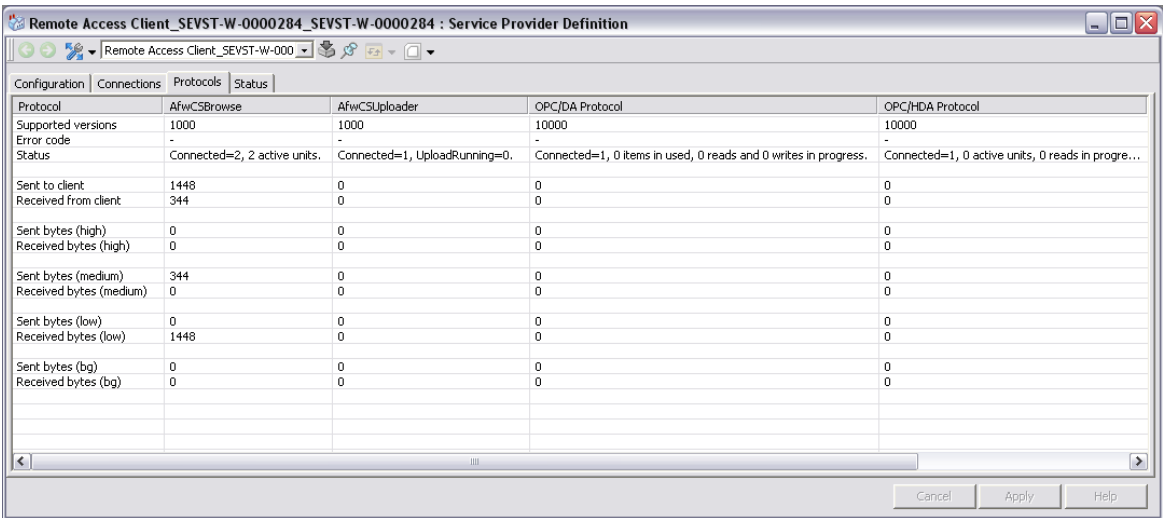*Table 7. Remote Access Client, Connection Tab Description*

Item	Description
IP-Address	Numeric or symbolic IP-Address of the Remote Access Server
System Name	Provider system name, i.e the Remote System object name

Table 7. Remote Access Client, Connection Tab Description

Item	Description
Error code	Error code if there is any problem with the connection, see Appendix A for details
Connect time	Time when the connection was established
Time difference	Difference between the system clocks in the subscriber and provider
Sent to client	Number of bytes sent from a local client to the Remote Access Client service
Received from client	Number of bytes received from a local client to the Remote Access Client service
Sent bytes	Number of bytes sent to the Remote Access Server with high priority (high, medium, low priority)
Received bytes	Number of bytes received from the Remote Access Server with high priority (high, medium, low priority)
Queued bytes	Number of bytes queued to be sent to the Remote Access Server (high, medium, low priority)

More information is available in the Protocol tab.

Figure 60. Remote Access Client, Protocol Tab

The information in the Protocols tab is similar to the Connections tab information, but the information is separated for the different protocols used between the Remote Access Client and Remote Access Server.

The same tabs, with the same information, are also available for the Remote Access Server.

Upgrade Procedure

When you upgrade the software for the Multisystem Integration to a new release or new service pack, perform the following steps:

1.   Stop the subscriber server. Install the new service pack or new release.

2.   Start the subscriber server.

3.   Stop the provider server. Install the new service pack or new release.

4.   Start the provider server.

When upgrading the Multisystem Integration, also Process Portal A and all used system extensions should be upgraded to the same service pack or release.

Appendix A Error Messages

The 800xA Multisystem Integration extends the error messages, shown in upload logs or as message boxes, possible to receive from the 800xA system with its own set of messages. The table below lists the error messages, and a short explanation of the cause. All error messages start with the string "E_AFW_CONSYS_". The table below shows the messages without this prefix string.

Table 8. 800xA Multisystem Integration Error Messages

Error Messages	Description
ABORTED	An upload was aborted by the user.
ACCOUNT_PROMPT_FAILED*	Internal error. Failed to activate the dialog to input the connect account. Try to repair the windows installation.
AE_REFERENCE_NOT_FOUND*	A referenced aspect in the alarm and event system is not found in the provider.
ASPDIR_DOWN*	The aspect directory is down on the provider side. Check the status of the provider.
ASPECT_NOT_FOUND	Internal error. No subscribe information was found for the proxy aspect. Try to upload all proxy objects again to regain internal table consistency.
BAD_ID	Internal error. Bad identifier (used in multiple places).
BAD_PASSWORD	The passwords defined for the Remote Access Server and Client pair do not match each other. Define the password again both on the provider and subscriber side.
BAD_UNIT_ID	Internal error. Remote Access Server/Client unit did not exist.
BAD_VERSION	The version of the Remote Access Server and Client is different and no common version can be found. Installation of the same version of 800xA Multisystem Integration on both the provider and subscriber solves the problem.
CONSYS_INVALIDACCOUNT*	The account name or password is wrong for the connect account. The account name must exists as a local user in the node, or as a domain user.
FILE_ERROR	File error when reading or writing data related to the Remote Access Client service. Check access to disc and if the disc is full.

Table 8. 800xA Multisystem Integration Error Messages (Continued)

Error Messages	Description
FILE_FORMAT	File format error in Remote Access Client service data. This may happen if a newer version of the Multisystem Integration function is installed and will require a full new upload to get correct data.
FILE_VERSION	File version error in Remote Access Client service data. This may happen if a newer version of the Multisystem Integration function is installed and will require a full new upload to get correct data.
HDA_BAD_HANDLE	Internal error. History server encountered a bad (unknown) handle.
HDA_BAD_ITEMID	Internal error. History server address with malformed item identifier.
HDA_NOT_INITED	Internal error. History server linked adaptor not initialized before use.
HDA_REFERENCE_NOT_FOUND*	A referenced aspect in a history log configuration is not found in the provider.
INITED	Internal error. Object is re-initialized after first use.
ID_USED	The user mapping is already used.
ID_IN_USE	Internal error. Identifier already in use.
INVALID_SECTION*	A section is uploaded through a reference without being explicitly uploaded. Upload the section before any objects referencing the section.
MANAGED_READONLY	Internal error. A read-only property table was the target for an update.
NODE_ADMIN_ERROR *	Internal error. Handling of the pseudo nodes representing the remote system failed.
NO_CONNECTION	Currently no connection open to the provider system. Check the connection status to pinpoint the problem.

Table 8. 800xA Multisystem Integration Error Messages (Continued)

Error Messages	Description
NO_LICENSE*	There is no enough number of licenses for Multisystem Integration
NO_LOCAL_INSERT_POSITION *	The object configured as parent to the uploaded objects do not exists. Check the upload configuration.
NO_DATA	Internal error. No subscribe table data for object proxy.
NO_REMOTE	Internal error. The referenced Remote System object does not exist.
NO_RAC_UNIT	Internal error. No Remote Access Client unit to address. Try to restart the Remote Access Client service.
NO_SUBSCRIBEINFO	No property information was found for a remote object proxy. This is an indication of an internal error but may be overcome by redoing the upload of the full structure specified for the remote object connection.
NO_PROXY	No proxy found when expected. Run 'upload clean' and then upload everything to rebuild consistent memory tables.
NO_PROXY_TEMPLATE	No log template was found for the log during upload. Run 'upload clean' and then upload everything to rebuild consistent memory tables.
NO_REMOTE_SYSTEM	No connection to the remote system. Check the status to see what is wrong.
NO_PROVIDER_OBJECT	Internal error. No remote object connection object was found for the specified item.
NO_TEMPLATE	No log template was found for the log. Rerun the upload to rebuild the internal tables.
NO_LOGCFG	No log configuration was found for the log. Rerun the upload to rebuild the internal tables.

Table 8. 800xA Multisystem Integration Error Messages (Continued)

Error Messages	Description
NOHOST	No valid host definition for Remote Access Client. Check the configuration of the Remote Access client.
NOT_INITED	Internal error. Object used without being initialized.
NOT_INITIALIZED	Internal error. Object not initialized before use.
NOT_COMPLETE_SECTION *	Tried to upload a subsection without uploading the top section. Can be caused by a reference to a subsection before the top section is uploaded.
OBJECTID_IN_USE	Internal error. Object identifier was already used by another object. Try to upload all proxy objects again to regain internal table consistency.
OBJECT_NOT_LOCKED*	The object to write to is not locked by the current user.
PERMISSION_MISSING*	A permission used in a section definition do not exist in the subscriber system. Use Import/Export to move the permission from the provider to the subscriber.
PROTOCOL_NOT_FOUND	One of the protocols used to communicate between the Remote Access Server and Remote Access Client can not be found. This may if different versions of the Multisystem Integration function is installed in the subscriber and provider or if some DLL-s are lost on the Remote Access Server/Client side. Re-install the 800xA to correct the problem.
PROTOCOL_VERSION	The version of one of the protocols used by the Remote Access Server and Remote Access Client to communicate do not match. Install the same version of 800xA Multisystem Integration on both provider and subscriber to correct this problem.
PORT_IN_USE	The port selected for the Remote Access Server or Client is already in use by another application. Can only be solved by removing the other application or selecting another port to use.

Table 8. 800xA Multisystem Integration Error Messages (Continued)

Error Messages	Description
RAC_HAS_BEEN_DELETED*	Internal error. Failed to upload event categories.
RAS_UNIT_NOT_OPEN	Internal error. Data received to non-existing RAS unit.
RAC_UNIT_NOT_OPEN	Internal error. No Remote Access Client unit to send data to. Try to restart the Remote Access Client service.
READONLY_CONNECTION	The connection is configured to be read-only, so all OPC writes, History logs update and alarm acknowledge are prohibited.
REGREAD_FAILED*	Failed to read the connect account or password information from the registry.
REGSAVE_FAILED*	Failed to save the connect account or password information to the registry. Check that you are local administrator on the current node.
SG_NOT_CONNECTED	No service group associated with the remote system connection object. This can be possibly be corrected through the consistency checker/auto correction function.
UPDATE_RUNNING	A new update operation can not be started as one is already being performed by the Remote Access Client. Abort can be used to terminate the running upload.
UPDATE_NOT_RUNNING	Internal error. An update operation was attempted by a Remote Access Client protocol object but no upload was in progress.
UNIT_CLOSED	Internal error. Unit was closed.
UNKNOWN_USER	The remote user account is not recognized by the Remote Access Server. If common Windows domain is used, check that the user is present in the provider system. If user mapping is used, check the user mapping table on the Remote Access Server, service group.
UPLOAD_RUNNING	An upload is already running. Wait until it terminates before a new upload is started.

Table 8. 800xA Multisystem Integration Error Messages (Continued)

Error Messages	Description
USER_MAPPING_MISSING*	A user in a section definition in the provider do not have any mapping to a user in the subscriber. Add a user mapping for all users in all section definitions to succeed with the upload.
USER_MISSING*	A user in a section definition is not found in the subscriber.
WRONG_ENVIRONMENT*	The system connection aspect can only be used and created in the production environment.

*   Feature Pack Functionality

The following error message indicates that there is an aspect link pointing to an aspect in a composite object type.

```
Can not "copy import" composite object type containing nested
graphic aspects (Aspect = Object:Aspect Name)
```

This error message can be ignored as the construction will work for an instance in the Control Structure.

If the suggested action does not solve the problem or, if the error is internal without suggestion for correction, collect the error information and contact the ABB support organization.

In case the error is presented as a hexadecimal figure, like 8ABB0091, the program AfwErrorLookup.exe could often be used to get a description of the error. AfwErrorLookup.exe is found in the "bin"-directory of the Process Portal A installation.

Appendix B Fault Tracing

Complex distributed systems also make fault tracing a rather complicated task. This appendix gives a step-by-step description of how to isolate a problem in the communication and functionality of the Remote Access Client and Remote Access Server.

Physical Connection and Network Configuration

For the 800xA Multisystem Integration to work the physical and logical network connections must be configured correctly. To check this make the following steps from the subscriber system:

1. In a Windows command window run: **ping <provider IP-address>**
    If there is a time-out check both with numeric address and symbolic address. If no connection can be established with ping, there is a network problem that needs to be fixed before 800xA Multisystem Integration can work.

2. In a Windows command window run: **ipconfig /all**
    Check that the configuration is correct for the network.

3. In a Windows command window run: **route print**
    Check that the routing configuration is correct for the network.

4. In a Windows command window run: **tracert <node>**
    Check the path the routing takes and where it fails.
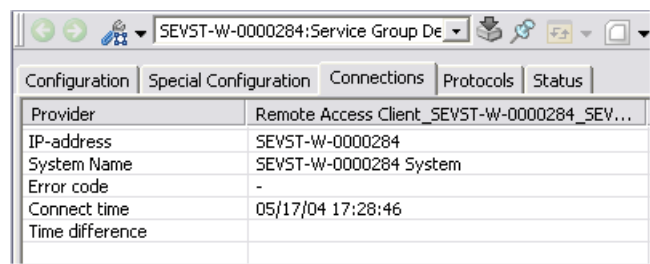
800xA Multisystem Integration Installation

Check that 800xA Multisystem Integration is installed on both the Remote Access Client Node and the Remote Access Server Node.

Protocol Status and Versions

Check protocol status and versions in the Service Structure, Service Provider Definition aspect, Protocols tab.

Trends, Alarms and Events Time Synchronization

For a remote connection to work properly, check the time difference between the subscriber and provider. If the time difference is more than 5 minutes a system event will be generated once every hour. To check the time difference between the subscriber and the provider, select the Remote Access Client, Connection tab, and check the row Time difference. This row will show the time difference between the subscriber and provider.

Figure 61. Presentation of Time Differences

To perform time synchronization between the subscriber and provider, an internet time synchronization protocol or external time synchronization equipment can be used.

Process Graphics Color

If the color of an uploaded display is different from than the original colors of the display in the provider system this could be caused by missing Logical Color aspects in the subscriber system. Use the Import/Export tool to copy them from the provider to the subscriber system.

No Alarm and Event in the Subscriber System

If there are no Alarm and Event from the provider system in the subscriber, check the following:

1. Is the connection to the provider up and running?

2. Is the object generating the alarm uploaded to the subscriber system? If not, make sure to upload it, because alarms from objects not uploaded will not be shown in the alarm list.

3. Check the service providers for the Alarm Manager, and Event Collector in the Service structure on the subscriber node. Are they all working correct?

4. Check the service providers for the Alarm Manager and Event Collector in the Service structure on the provider node. Are they all working correct?

Alarm with Object GUID Instead of Object Name

Alarms from objects that has been uploaded, but later not uploaded will be presented as object GUID instead of the object name. To correct this the Remote System object representing the provider has to be deleted and a new configuration and upload to be executed.

Failed to Deploy Graphic Display

If a graphic display is failing when doing deploy (finalize) check the following things:

1. Is it possible to deploy the graphic display in the provider?

2. Are all referenced graphic elements uploaded?

3. If the graphic display contains composite display elements, are they explicitly uploaded to the control structure?

4. Does the display or display element contain user written Visual Basic code that requires a specific environment to work.

No System Alarm in the Provider System

If there is no System Alarm when the connection to the provider system is broken, check the following to configure the System Alarm:

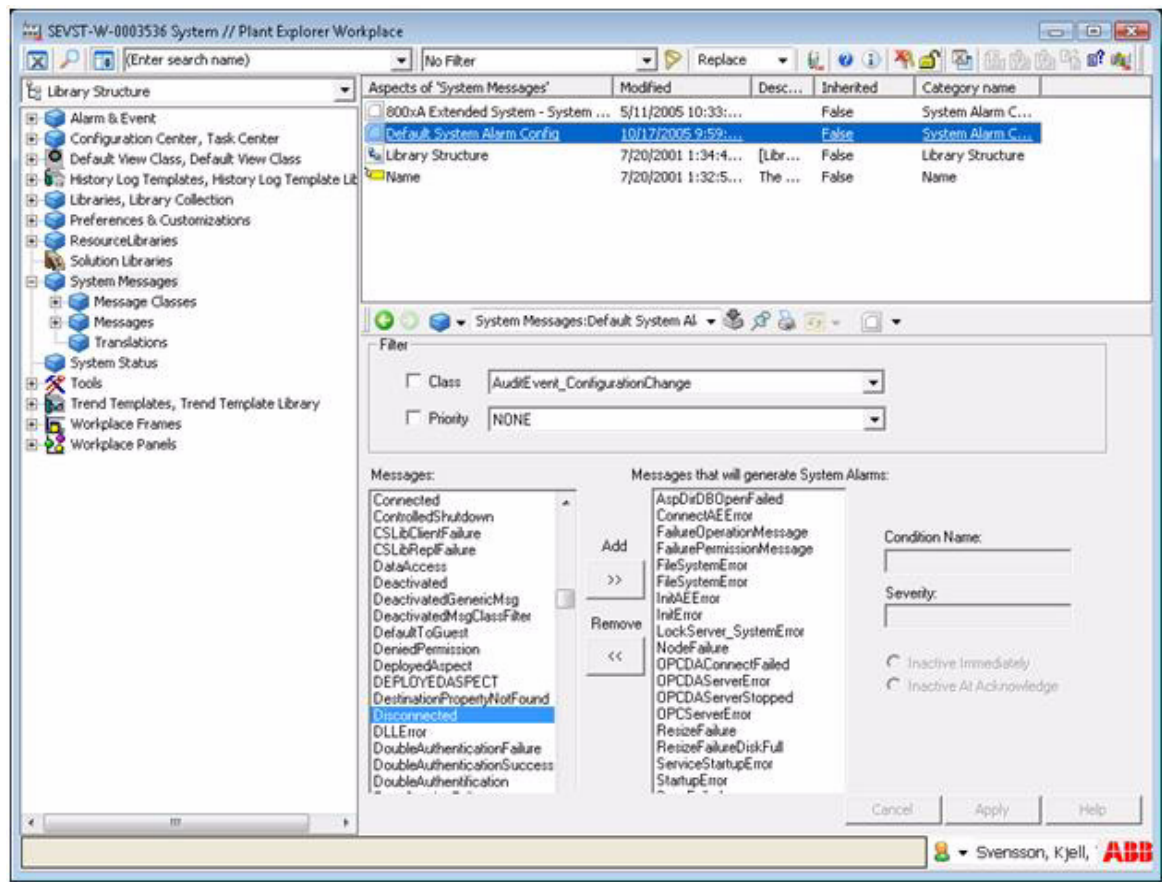1. In the Library Structure, select System Messages object, see Figure 62.

Figure 62. System Alarm

2. Select Default System Config aspect from the Aspects of 'System Messages' list.

3. Select Disconnected from the Messages list. Click **>>** to include the Disconnected message in the Messages that will generate System Alarms list.

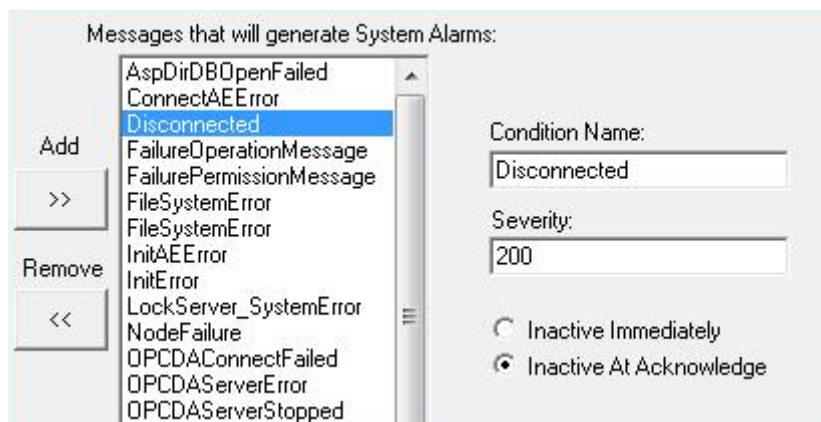4. Select Disconnected in the Message that will generate System Alarms list, see Figure 63.

Figure 63. Messages that will generate System Alarms

5.   Select Inactive At Acknowledge option.

6.   Click Apply, see Figure 62.

Index

Numerics

800xA Extended System 9

A

Abort 48
Acknowledge alarm 76
Advanced Access Control 54
Alarm and Event List 59
Alarm and Event list configuration 58
Alarm comments 76
Alarm Filtering 60
Alarm Hiding 60
Alarm Manager 59
Alarm shelving 77
AO-Authentication 86
AO-CMMS Views 85
AO-HTTPS Communication Protocol 67
Aspect Link Control 72
Aspects
    Proxy Control Connection 53
    Remote Object Info 52
    System Connection 41
Asset Optimization Aspect Configuration 64
Asset Optimization-Operation 84
Audible Alarms 60

B

Backup 87

C

Common Windows domain 31
Compare 49
Composite Graphics 72
Configuration
    Alarm and Event 58

Faceplates 56
Process Displays 56
Trends 57
Configuration Wizard 28
Configuring the Connect Account 37
Confirm write 54
    see Safety write 72
Confirmed write 72
Connect Account 37
Connect Method 16
Connection and Protocols tab 93
Consistency check 50
Control Structure 35
Copy at upload 45

D

Default port 33
Delete alarm 77
Domain 27
Double-authentication 54

E

E_AFW_CONSYS 99
Enable/disable conditions 76
Encrypt traffic 33
Error messages 99
Export/Import 72

F

Faceplate configuration 56
Fault tracing 107
Fire-wall 33
Follow references 42
Food and Drug Administration 91

3BSE037076-510 D

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.

Revision Index	Description	Date
-	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 Feature Pack 3	August 2012
D	Removed restrictions on Object locking in Section 1 Introduction	March 2016

Updates in Revision Index A

The following table shows the updates made in this User Manual for 800xA 5.1 Rev A.

Updated Section/Sub-section	Description of Update
Section 1, New in This Release	Added a new subsection *Connect Method for Multisystem Integration*.
Section 3, Remote Access Client	Added the procedure for configuring the Connect Method for Multisystem Integration.
Section 3, Composite Graphic	Added information note on large uploads should be divided into smaller parts.

Updates in Revision Index B

The following table shows the updates made in this User Manual for 800xA 5.1 Feature Pack 1.

Updated Section/Sub-section	Description of Update
About this User Manual	Added a section *Feature Pack* describing the user manual conventions used for indicating the Feature Pack content.
Section 1, Introduction	Added a subsection *Multisystem Integration with Point of Control support* in the section *New in this Release*.
Section 3, Configuration	Added a section *Point of Control Support.*
Section 4, Operation	Added a section *Operating the Point of Control.*

Updates in Revision Index C

The following table shows the updates made in this User Manual for 800xA 5.1 Feature Pack 3.

Updated Section/Sub-section	Description of Update
Section 1, New in This Release	Added a new subsection *Asset Optimization with Multisystem Integration*.
Section 3, Configuration	Added a section *Asset Optimization*.
Section 4, Operation	Added a section *Asset Optimization*.

Updates in Revision Index D

The following table shows the updates made in this User Manual for 800xA 5.1 Feature Pack 4.

Updated Section/Sub-section	Description of Update
Section 1, New in This Release	Removed restrictions on Object locking in Section 1 Introduction.

Contact us

ABB AB
Control Technologies
Västerås, Sweden
Phone: +46 (0) 21 32 50 00
e-mail: processautomation@se.abb.com
www.abb.com/controlsystems

ABB Automation GmbH
Control Technologies
Mannheim, Germany
Phone: +49 1805 26 67 76
e-mail: marketing.control-proucts@de.abb.com
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
www.abb.it/controlsystems

ABB Inc.
Control Technologies
Wickliffe, Ohio, USA
Phone: +1 440 585 8500
e-mail: industrialitsolutions@us.abb.com
www.abb.com/controlsystems

ABB Pte Ltd
Control Technologies
Singapore
Phone: +65 6776 5711
e-mail: processautomation@sg.abb.com
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
www.abb.com/controlsystems

ABB China Ltd
Control Technologies
Beijing, China
Phone: +86 (0) 10 84566688-2193
www.abb.com/controlsystems

Power and productivity
for a better world™

ABB