

System 800xA

Post Installation

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/EEC and in Low Voltage Directive 2006/95/EEC.

TRADEMARKS

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

Copyright © 2003-2011 by ABB.
All rights reserved.

Release: August 2011
Document number: 3BUA000156-510 C

Table of Contents

About this User Manual

General	15
Version Described in this Document	15
Document Conventions	16
Feature Pack	16
Warning, Caution, Information, and Tip Icons	16
Terminology	17
Related Documentation	18

Section 1 - Post Installation Overview

Introduction	19
800xA 5.1 Revision A Installation	19
System Security	19
800xA Installing User.....	20
Supported Operating Systems	20
New Installations	20
Upgrades	21
System Configuration Console	21
Post Installation Sequence	22

Section 2 - System Level Tasks

Introduction	23
800xA 5.1 Revision A Installation	23
Configuring RNRP	23
Creating a System.....	23
Releasing All Reservations	26

Nonversioned System	26
Versioned System.....	26
Loading System Extensions	27
Adding Connectivity and Application Servers.....	33
Adding Clients	35
Redundancy	36
Redundant Aspect Servers	36
Redundant Connectivity Servers.....	38
Verifying the System and Servers	39
Affinity	40
Overview	40
Planning Load Balancing.....	41
Configuring Affinity	44
Creating the Affinity Objects	45
Configuring the Affinity Aspects.....	45
Applying Affinity Settings to the Services	46
Defining Users.....	47
Time Services	47
Disabling the Windows Time Service.....	47
Configuring the Time Service.....	48
Configuring the System Time Server.....	48
Configuring the Time Client	49
Base Function Setup for Scheduler and Calculations	49
Redundant Calculation Servers	51
Two Information Management Nodes	51
Two Nodes Where One is an Information Management Node.....	52
Two Non-Information Management Nodes	52
 Section 3 - SoftPoint Server	
Introduction	53
Configuring Softpoint Services	53
 Section 4 - Diagnostics Collection Tool	
Introduction	57

Changing the ABBResults Directory Share Location	57
Modifying the DCT Service Account for a Domain Controller	58

Section 5 - SMS and e-mail Messaging

Introduction	65
Configuring the Location of the Application Server	65
Restarting the Event Collector Service	66

Section 6 - Structured Data Logger (SDL)

Introduction	67
Configuring the SDL Collector Service	67
SDL Collector Service Group	67
SDL Collector Service Provider	69
Post Installation when Using SoftController	71
Installation Troubleshooting	71
System Synchronization Recommendations	73

Section 7 - 800xA for AC 800M

Introduction	75
Control Builder M	75
Planning	75
Defining the Number of OPC and Panel 800 Alarm and Event Subscriptions	77
AC 800M Controller	80
Downloading Controller Firmware via Serial Line	80
Setting IP Address for AC 800M Controllers	83
Setting IP Addresses on Redundant CPUs	85
Verification	86
Downloading Controller or Communication Interface Firmware Using Ethernet	87
OPC Server Configuration	88
Configuration Planning	88
Additional Parameters	90
Connecting to Controllers	91
Saving Cold Retain Values	93
Configuring OPC Data Access Connections	94
Configuring OPC Data Access Redundancy	96

Configuring the OPC Server for Alarm and Event Collection	96
Verifying the OPC Server Configuration	98
 Section 8 - 800xA for Advant Master	
Introduction	101
Connectivity Server Configuration.....	101
Assigning MB300 Network and RTA Board Objects to the Control Structure .	102
RTA Board Network Settings	103
Verifying the RTA Board Network Settings	105
Entering License Information for Connected Controllers.....	105
 Section 9 - 800xA for Harmony	
Introduction	107
Harmony Executive Service Provider Setup	107
Configure Access Rights	108
OPC Server Network Object Setup.....	110
Alarm and Event Service Provider Setup.....	111
Import the Harmony Configuration.....	112
New Installations	112
Reloading when a Backup Exists.....	113
Reloading when a Backup does not Exist.....	113
Synchronize the Aspect Directory.....	114
Harmony Communication Configuration.....	115
ICI Device Configuration.....	115
Replication Monitor Internet Explorer Security Settings.....	116
 Section 10 - 800xA for AC 870P/Melody	
Introduction	119
Melody Executive Service Provider Setup.....	119
 Section 11 - 800xA for MOD 300	
Introduction	121
Setting Up Time Synchronization	121

800xA System is Master Timekeeper	121
MOD 300 System is Master Timekeeper	122
Time Synchronization on the MOD 300 Connectivity Server	122
Time Synchronization on the Domain Controller	123
Time Synchronization on the MOD 300 Client	124
Time Synchronization on the Service Provider Definition Aspect	124
Process Administration Supervision (PAS) Account and Communication Settings	125
Redundancy	127
Setting Up the System Structure	128

Section 12 - PLC Connect

Introduction	129
Control Network Setup	130
Creating a New Control Network Object	130
Configuring PLC Connect Services	130
SoftPoint and PLC Connect Coexistence	132
IEC 60870 Licensing	133
Software Keys	133
Licensing Procedure	133
Enable Temporary Authorization	133
Completing and Sending the License Files	134
Completing Formal Licensing	135
Transferring the Software License	135
Other Licensing Options	136
PLC Server	136
Configuring PLC Server Processes	137
Service Structure Example	137

Section 13 - IEC 61850 Connect

Introduction	139
Replacing the XML Files	139

Section 14 - Asset Optimization

Introduction	141
AoWebServerNode.....	141
Asset Monitoring Service Provider Node	141
Adding Additional AO Servers to the System	142
Restarting the Event Collector Service	144
Web-Enabled Views on Non-Industrial IT Systems.....	145
cpmPlus Enterprise Connectivity (ECS 4.0 and 4.2)	145
Maximo Integration.....	146
Maximo Business Object (Maximo 6.2 and 7.1)	146
SAP/PM Integration	147
Internet Explorer Configuration	148
Excel Initialization	149
 Section 15 - PC, Network and Software Monitoring	
Introduction	151
Basic Computer Monitoring.....	151
 Section 16 - Device Library Wizard	
Introduction	153
Device Library Wizard Server Settings.....	153
Fieldbus Device Type Preparation (Optional).....	154
Installing Fieldbus Device Types	154
 Section 17 - Device Management FOUNDATION Fieldbus	
Introduction	157
General Settings	157
Time Synchronization	157
 Section 18 - Process Engineering Tool Integration	
Introduction	159
INtools Import Export Utility.....	159
Process Engineering Tool Integration	160
 Section 19 - Information Management	

Introduction	161
Information Management Setup	161
Referenced Post Installation Procedures	163
ActiveX Security Settings.....	164
Creating a History Database Instance.....	164
Creating a Secured Password for Oracle TNS Listener	169
Starting Process Administration Supervision (PAS)	169
Configuring the DBA (ADO) Data Provider for Oracle Data	171
Creating an ODBC Data Source for the Oracle Database.....	171
Editing the ADO Data Provider Configuration	173
Defining the Users	175
Configuring the Default ACC Users	175
Oracle Connection for Reports	176
Adding ABB Inc. as a Trusted Publisher in Excel	176
Troubleshooting Oracle	177
Database Instance Errors	178
Drive Space Configured Incorrectly.....	178
Available Diskspace Changes Before Running the Wizard	178
Insufficient Space for Oracle System Files	179
Verifying Oracle Service Names	179
Information Management Profiles Client Post Installation	181

Section 20 - Batch Management

Introduction	183
Batch Management System Service Definitions	183
Shutdown Script	186
Print BMA Report Configuration	187
Batch Management Toolbar.....	188
Using Batch Management Advanced Templates Only	188
Setting the Date Format for Batch Auto ID for Automatic Scheduling	188
Setting the SQL Server Maximum Server Memory Limit	189

Section 21 - TRIO Integration

Introduction	191
Install TRIO Integration Software.....	191
Loading the TRIO Integration System Extension	191
Inserting the Hardware Library	192
Adding a CI862 TRIO Interface.....	192
Loading Firmware	192

Section 22 - Multisystem Integration

Introduction	195
Remote Access Server.....	195
Creating a Remote Access Server.....	196
Node Configuration	197
Read-Only System	197
User Mapping	197
Password Configuration	199
Advanced Configuration	199
Remote Access Client	200
Creating a Remote Access Client	201
Advanced Configuration	202
Uploading a Configuration	203
Running Upload	206
Proxy Objects.....	209
Proxy Control Connection	210
Proxy Log Configuration	210
Proxy Log Template.....	210
Redundant Configurations.....	210
Redundant Remote Access Client.....	210
Redundant Remote Access Server.....	211
Dual Remote Access Redundancy	212
Redundant Remote History Service.....	212
Redundant Remote Alarm and Event Service	213

Section 23 - Windows Firewall Configuration

Introduction	215
Configuring Windows Firewall	216
Common Causes of Errors	217
Log File	217

Section 24 - Windows Services Configuration

Introduction	219
Configuring Windows Services	219
Common Causes of Errors	220
Log File	220

Index

Revision History

Introduction	225
Revision History	225
Updates in Revision Index A	226
Updates in Revision Index B	226
Updates in Revision Index C	227

About this User Manual

General



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

This User Manual describes how to manually perform post installation procedures for the 800xA Base System and Functional Area software. It does not include information on site planning, engineering planning, software configuration, network design, etc. that can be found in other 800xA User Manuals.

Unless otherwise noted, the version of all 800xA Base System and Functional Area software described in this instruction is the latest release of 800xA 5.1. The procedures described require Windows Administrator privileges.

This User Manual does not include information on site planning, engineering planning, software configuration, network design, security measures, tools, maintenance, etc. that can be found in other 800xA User Manuals.

Version Described in this Document

All information and procedures described in this document are specific to the latest release of 800xA 5.1.

Document 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

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 publication 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 instruction are listed in the following table.

Term/Acronym	Description
Backup	<p>800xA Backup: Backup using the 800xA Backup Definition aspect.</p> <p>Functional Area Backup: Backup via defined tools or copy of Functional Area configuration and/or data to a safe media for items not covered by 800xA Backup.</p> <p>The specific operations called out for the Functional Area within the Backup/Restore procedure in <i>System 800xA Maintenance (3BSE046784*)</i> for same version to same version backup and restore.</p>
Restore	<p>800xA Restore: Restore via Configuration Wizard.</p> <p>Functional Area Restore: Restore via defined tools or copy of Functional Area configuration and/or data from a safe media for items not covered by 800xA Backup.</p> <p>The specific operations called out for the Functional Area within the Backup/Restore procedure in <i>System 800xA Maintenance (3BSE046784*)</i> for same version to same version backup and restore.</p>

Term/Acronym	Description
Upgrade	Moving from one 800xA release to a later 800xA release, whether it be a major or minor release.
Update	Adding service packs, patches, hot fixes, or rollups to an existing 800xA System.

Related Documentation

A complete list of all documents applicable to the 800xA System is provided in *System 800xA Released User Documents (3BUA000263*)*. This document lists applicable Release Notes and User Instructions. It is provided in PDF format and is included on the Release Notes/Documentation media provided with your system. Released User Documents are updated with each release and a new file is provided that contains all user documents applicable for that release with their applicable document number. Whenever a reference to a specific instruction is made, the instruction number is included in the reference.

Section 1 Post Installation Overview

Introduction



This document reflects 800xA System and Functional Area software at the time of release. All 800xA System and Functional Area Release Notes must be read and understood before performing any automated or manual installation, post installation, or upgrade procedures. The Release Notes contain any last minute changes that must be performed when installing or upgrading the 800xA System. All Release Notes can be found on the CD labeled *System Version 5.1 Released Documents*.

Before performing the procedures in this instruction, refer to *System 800xA Installation (3BSE034678*)* for procedures on installing 800xA Base System and Functional Area software and the software keys. The software keys must be in place in order to complete some procedures in this instruction.

800xA 5.1 Revision A Installation

800xA 5.1 Rev A must be installed before performing the post installation procedures in this document.

System Security



It is very important to have a corporate security policy that is revised on a regular basis. This is the responsibility of the user of the 800xA System.

This document does not contain recommendations on system security, users, user groups, or user roles and permissions. Refer to *System 800xA Administration and*

Security (3BSE037410)*, *System 800xA Network Configuration (3BSE034463*)*, and *System 800xA System Planning (3BSE041389*)* for more information.



Windows Firewall must be turned off during all installation and post installation procedures. The Windows Firewall Configuration procedure must be performed after all new 800xA System software is added to the system and post installation procedures are complete.

800xA Installing User

Unless otherwise specified, perform all procedures in this instruction logged in as the 800xA Installing User.

When the system is created, the user currently logged in is added to the system as a member of the **Administrators**, **Everyone**, **System Engineer**, and **Application Engineer** IndustrialIT groups. The 800xA Installing User must not be a member of the Domain Administrators Group on the Domain Controller node. It is mandatory that the 800xA Installing User be a Local Administrator on every 800xA System node.

Supported Operating Systems

800xA System software may be installed on 32-bit (x86) US English version of Windows Server 2008 Standard or Enterprise edition with Service Pack 2, or the 32-bit (x86) US English version of Windows 7 Professional or Enterprise edition with SP1. Windows Server 2008 R2 is not supported.



Windows Server 2008 and Windows 7 will be used throughout the remainder of this document (service pack and edition info will not be repeated).

New Installations

If **not** starting with an 800xA System preinstalled by ABB, post installation procedures can be executed either semi-automatically using the System Installer as described in *System 800xA Automated Installation (3BSE034679*)*, or manually as described in this instruction.

If performing a manual post installation, read the rest of this section in its entirety for guidelines on how to proceed before beginning post installation procedures for 800xA Base System and Functional Area software.



800xA for DCI was not included with the initial release of 800xA 5.1 and thus 800xA for DCI post installation instructions are not documented in this user manual. Refer to *800xA for DCI 5.1 Installation - Post Installation - Upgrade Supplemental User Manual (3BUA001686*)* for Post installation of 800xA for DCI 5.1.

Upgrades

Upgrades can be executed either semi-automatically using the System Installer as described in *System 800xA Automated Installation (3BSE034679*)* or manually as described in *System 800xA Upgrade (3BSE036342*)*.

If an installed system exists and is being manually upgraded from System Version 4.1 to System Version 5.1 or from System Version 5.0 Service Pack 2 to System Version 5.1, refer to *System 800xA Upgrade (3BSE036342*)*.



Upgrades directly from System Baseline 2.1/2 and System Version 3.1 Service Pack 3 to System Version 5.1 are not supported. Refer to *System 800xA Upgrade (3BSE036342*)* for the supported upgrade paths.

System Configuration Console

Some procedures described in this instruction use the 800xA System Configuration Wizard. A new feature, the System Configuration Console, can also be used to perform many of these procedures. Refer to *System 800xA Tools (2PAA101088*)* for information and instructions on using the System Configuration Console.

Post Installation Sequence

Perform the procedures, applicable to the specific system, in the order presented in this instruction manual on a node by node basis, including [Windows Firewall Configuration](#) and [Windows Services Configuration](#).



The Windows Firewall Configuration procedure must be performed every time new 800xA System software is added to the system.

Section 2 System Level Tasks

Introduction

This section describes post installation tasks that must be done at the 800xA Base System level before proceeding with the post installation tasks for the individual Functional Areas.



This instruction does not contain information related to Environment setup and related functionality. Refer to the appropriate 800xA System documentation for more details.

800xA 5.1 Revision A Installation

800xA 5.1 Rev A must be installed before performing the post installation procedures in this document.

Configuring RNRP

Refer to *System 800xA Network Configuration (3BSE034463*)* for information about configuring Redundant Network Routing Protocol (RNRP).

Creating a System

Creating a system will create the first Aspect Server (the Primary Aspect Server). Perform this on the node designated to be the Primary Aspect Server.

When the system is created, the user currently logged in is added to the system as a member of the **Administrators**, **Everyone**, **System Engineer**, and **Application Engineer** IndustrialIT groups.

Use the 800xA Installing User account when creating the system.

1. Start the Configuration Wizard on the node designated to be the Primary Aspect Server. Select:
Start > All Programs > ABB Industrial IT 800xA > System > Configuration Wizard
2. The Select Type of Configuration dialog box appears. Select **Create System** and click **Next**.
3. The Define Name and Description of the System dialog box appears. Use [Table 1](#) to configure this dialog box.

Table 1. Create New System Dialog Box Settings

Field	Description/Setting
Name	Enter the system name. Do not use special characters, or characters specific to keyboard in languages other than English.
Description	Enter the system description (optional).
Server Node	The current node (not an editable field).
Server Type	Select Aspect Server if a dedicated node is used for the Primary Aspect Server (distributed configuration).
	Select Aspect Server and Connectivity Server for single-node or small system configurations, where the Aspect and Connectivity Servers are combined.
	Select Aspect Server and Connectivity Server for Information Management Consolidation nodes.

4. Click **Next**.
5. The Define Paths to Data Directories dialog box appears. Specify the paths to data directories (or accept the defaults) and click **Next**.



Use a local disk on the Aspect Server node. Using a network disk will severely decrease the performance of the Aspect Server and risk availability of the entire system.

6. The Configure System Network dialog box appears. It is used to tell the 800xA System the number of network areas where 800xA System nodes will communicate. This should be network areas where clients and servers communicate with each other. Network areas where only controllers and

Connectivity Servers are connected do not need to be counted here. The number is **1** in almost all systems.

7. The Configure Network Addresses dialog box appears. For a nonredundant network area the Secondary Network Address field can be left empty. There will be as many dialog boxes for network addresses as the Number of Areas specified in the Configure System Network dialog box. The order in which the areas are specified is not important. Fill in each dialog box with the proper information and click **Next**.
8. The Apply Settings dialog box appears. Click **Finish** to accept the settings and create the system, or click **Back** to make changes. System creation takes some time.

The System creation is finished when the Select Type of Configuration dialog box seen in [Step 2](#) reappears.

9. Exit the Configuration Wizard.
10. To verify the system is running, hover the cursor over the ABB System Supervisor symbol in the Windows Notification area shown in [Figure 1](#). The pop-up message should indicate that the system is **Enabled**.

ABB SYSTEM SUPERVISOR
SYMBOLS



Figure 1. ABB System Supervisor Symbol



Back up SMDData.dat in the ...\\OperateITData\\ServiceManager directory (the path to the OperateITData directory was configured in [Step 5](#)).



Check the Configuration Wizard log file for errors after creating the system.

Releasing All Reservations



If system extensions will be loaded as part of an upgrade procedure (going from one major system version to another; for example, 800xA 4.1 to 800xA 5.1 or 800xA 5.0 SP2 to 800xA 5.1) release all reservations before loading the system extensions.

Perform this procedure only if loading system extensions is part of an upgrade procedure (going from one major system version to another; for example 800xA 4.1 to 800xA 5.1).

Nonversioned System

Perform the following on a nonversioned system:

1. Open a Plant Explorer Workplace.
2. Launch the Find tool.
3. Select **Objects** and the **Reserved by** attribute.
4. Click **Search**.
5. Select all found Objects and release them using the context menu.

Versioned System

Perform the following on a versioned system:

1. Verify that the Engineering Environment does not contain any undeployed changes.
 - Deploy any undeployed changes or export them and import them after completing this procedure.
2. Verify that no entities or aspects are reserved in the Production Environment:
 - a. Open a Plant Explorer Workplace in the Production Environment.
 - b. Launch the Find tool.
 - c. Select **Objects** and the **Reserved by** attribute.
 - d. Click **Search**.
 - e. Select all found Objects and release them using the context menu.

- f. Select Aspects and the Reserved by attribute in the Find tool.
- g. Click **Search**.
- h. Select all found aspects and release them using the context menu.
- i. Refresh the Engineering Environment after loading the system extensions.

Loading System Extensions



If system extensions will be loaded as part of an upgrade procedure (going from one major system version to another; for example, 800xA 4.1 to 800xA 5.1 or 800xA 5.0 SP2 to 800xA 5.1), release all reservations before loading the system extensions. Refer to [Releasing All Reservations](#) on page 26.

System extensions provide the 800xA System with additional functionality.



Previous versions of the 800xA System (800xA 5.0 SP1 and earlier) included a system extension for 800xA Documentation. This system extension is no longer included.

Refer to [Table 2](#) for a list of system extensions available to be loaded for *new installations*.

Refer to [Table 3](#) for a list of VB Graphics system extensions available to be loaded *when upgrading* from a previous 800xA system version.

To load the system extensions:

1. Start the Configuration Wizard from the primary Aspect Server node. Select:
Start > All Programs > ABB Industrial IT 800xA > System > Configuration Wizard
2. Open the System Extension Load dialog box by going to:
System Administration > Select System > System Extension Load
3. A view appears with the available system extensions listed in the left pane. Select the system extension to load in the list in the left pane and move it to the list in the right pane by clicking >. To move all the system extensions from the left pane to the right pane, click >>.
4. The red cross, green check mark, and warning icons indicate the status of the dependency evaluation.

Table 2. System Extensions for New Installations

Application	System Extension
800xA for AC 800M	AC800M Connect
	<p>AC800M Classic</p> <p>This system extension contains <i>Classic</i> (i.e., older) versions of libraries that exist in more than one major version. These libraries have previously been included in the <i>base</i> system extension for AC 800M Connect.</p> <ul style="list-style-type: none"> This system extension should only be installed and loaded in case a needed backup file or Afw file has dependencies to this system extension or the libraries in it. This system extension is not available for loading unless it was enabled via the Custom installation option during AC 800M Connect installation. If it is needed but was not enabled, the AC 800M Connect installation must be modified via Programs and Features in Windows Control Panel. Select AC 800M Connect and choose Change.
	<p>AC 800M HI Extensions</p> <p>This system extension contains High Integrity versions of hardware libraries.</p> <ul style="list-style-type: none"> This system extension should only be installed and loaded in case High Integrity version is used. <p>NOTE:</p> <p>The version for PM865, SM810, and SM811 in AC 800M HI Extensions must be verified before operational use to be in conformance with the list of certified software combinations found in the Annex 2 of the TÜV Certificate Report (3BSE054960).</p>
Batch management	<p>Batch Management</p> <p>Batch Advanced Templates</p>
Information Management (IM)	<p>Industrial IT Archival</p> <p>Inform IT Calculations (load manually if not installing IM application)</p> <p>Inform IT History</p> <p>Inform IT ODA</p> <p>Inform IT Scheduler (load manually if not installing IM application)</p>
SoftPoint Server	ABB SoftPoint Server

Table 2. System Extensions for New Installations (Continued)

Application	System Extension
Asset Optimization	Asset Optimizer Server Asset Monitor Environment Maximo Connectivity or SAP Connect System Extension (choose only one) NOTE: If Device Management for Fieldbus will be used in conjunction with Asset Optimization, it is mandatory to load the Device Integration Library - Asset Monitoring system extensions described later in this table.
SMS and e-mail Messaging	SMS and e-mail Messaging
PC, Network and Software Monitoring	PC, Network and Software Monitoring
Engineering Studio	ABB Engineering Base ABB DM & PM Application ABB Function Designer ABB Topology Designer ABB Script Manager ABB Reuse Assistant
	ABB Signal Extension for AC800M Connect ABB Function Designer for AC800M Connect ABB Topology Designer for AC800M Connect ABB Topology Designer For AC800M High Integrity ABB CI Extension for AC800M Connect ABB Signal Extension for TRIO Connect
Engineering Studio (continued)	ABB Function Designer for AC 800M Classic ABB Topology Designer for AC800M Classic ABB Function Designer for Fieldbus Builder Profibus/Hart ABB AC 800MC Signal Extension Classic NOTE: These system extensions are optional and should only be loaded if AC 800M Classic has been loaded.

Table 2. System Extensions for New Installations (Continued)

Application	System Extension
Device Management PROFIBUS & HART and Device Management FOUNDATION Fieldbus NOTE: After loading the system extensions for Device Management, use the Device Library Wizard for adding separately delivered device types into the 800xA System. Refer to <i>System 800xA Device Management Device Library Wizard (2PAA102573*)</i> for details.	Fieldbus Builder PROFIBUS/HART HART Device Integration Library - Basics PROFIBUS Device Integration Library - Basics Load the following system extensions only if Asset Optimization system extensions have been loaded: <ul style="list-style-type: none"> • HART Device Integration Library - Asset Monitoring • PROFIBUS Device Integration Library - Asset Monitoring
	Load the following system extension only if the Fieldbus Builder PROFIBUS/HART, PROFIBUS & HART Device Integration Library - Basics, Engineering Base, and Function Designer system extensions have been loaded: <ul style="list-style-type: none"> • Function Designer for Fieldbus Builder PROFIBUS/HART
	Fieldbus Builder FF FF Device Integration Library - Basics Load the following system extension only if Asset Optimization system extensions have been loaded: <ul style="list-style-type: none"> • FF Device Integration Library - Asset Monitoring
800xA for Advant Master	800xA for Advant Master
800xA for Safeguard	800xA for Safeguard
800xA for MOD 300	MOD300 Connect MOD300 OPC Connect
PLC Connect	PLC Connect
IEC 61850 Connect	IEC 61850 Connect System Extension
800xA for Harmony	Harmony Connect Load the following system extension only if Asset Optimization system extensions have been loaded: <ul style="list-style-type: none"> • Harmony CNAM. Load the following system extension only if the Batch Management system extensions have been loaded: <ul style="list-style-type: none"> • Batch for Harmony.

Table 2. System Extensions for New Installations (Continued)

Application	System Extension
800xA for AC 870P/Melody	Melody Connect
Central Licensing System	Central Licensing System
Process Engineering Tool Integration	Process Engineering Tool Integration
SFC Viewer	ABB SFC Viewer
Structured Data Logger	SDL Extension
TRIO Integration	The TRIO Integration system extension must be loaded separately after the AC 800M system extensions are loaded. Refer to Section 21, TRIO Integration to install TRIO Integration and load its system extension after performing all other post installation procedures.

Table 3. VB Graphics System Extensions for Upgrades

Directory	Software
800xA Connectivities	AC 800M Connect VB Graphics Extension ABB 800xA for Advant Master VB Graphics Extension ABB 800xA for Safeguard VB Graphics Extension ABB 800xA for Harmony VB Graphics Extension 5.1.00 ABB 800xA for IEC61850 VB Graphics Extension ABB 800xA for MOD 300 VB Graphics Extension ABB PLC Connect VB Graphics Extension 5.1.00

Table 3. VB Graphics System Extensions for Upgrades (Continued)

Directory	Software
Device Management & Fieldbuses	ABB Device Management FOUNDATION Fieldbus VB Graphics Extension
Batch Management	Batch VB Graphics Extension Batch Advanced Templates VB Graphics Extension

- The green check mark indicates that the system extension must be loaded first.
 - The red cross icon indicates that the system extension can not be loaded until the one with the green check mark icon is loaded.
 - The warning icon indicates that the system extension can be loaded, but that there is additional information available in the Description frame in the lower part of the dialog box. The additional information can, for example, be that the system extension contains aspect types that are not environment aware.
5. If the list in the right pane contains more than one system extension, click **Press header to autosort** to sort the system extension load order with regard to dependencies.
 6. All system extensions in the right pane should be marked with the green check mark or the warning icon.
 7. Click **Next** and the Apply Settings dialog box appears.
 8. Click **Finish** to load all system extensions.

9. A progress dialog box is shown during the load. Click **View Log** to view log messages during load.



The load is aborted if:

- The user clicks **Abort**.
- An error occurs; for example, if the Configuration Wizard fails to load a file into the system.

An aborted system extension load can be resumed from the System Extension Maintenance dialog box.

10. When the load operation is finished, click **Finished** and view the Configuration Wizard log to verify that no errors occurred during the load.
11. Close the Configuration Wizard.

Adding Connectivity and Application Servers

This procedure is required for all Connectivity Servers, and for Application Servers (IM Servers, Batch Servers, and other applications such as AO Server, 800xA for Harmony Configuration Server, and 800xA for AC 870P/Melody Configuration Server) in a distributed (multinode) system.

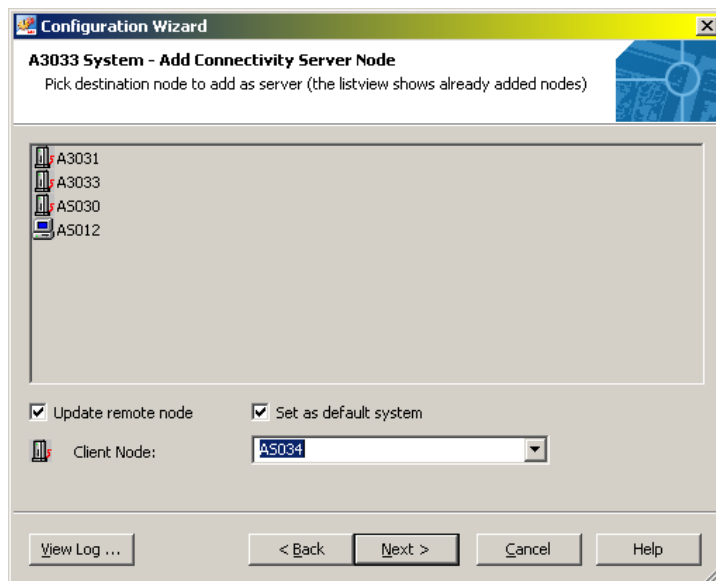
Before beginning the procedure, adhere to the following guidelines:

- Application Servers are added to the system as Connectivity Servers. There is not a separate option for adding Application Servers.
 - When a Secondary Batch Server is added, it must be added as a redundant Connectivity Server as described in [Redundancy](#) on page 36.
 - This procedure is not required when setting up a single node system.
 - Before adding any node, make sure that the node to be added has all required software installed. It must also have the same versions of system extension software installed as the Aspect Server.
1. Start the Configuration Wizard on the Primary Aspect Server.
 2. Select **System Administration** and click **Next**.
 3. Select the system and click **Next**.
 4. Select **Nodes** and click **Next**.
 5. Select **Add Connectivity Server** and click **Next**.

6. The Add Connectivity Server Node dialog box appears. Select the node from the drop-down list box as shown in [Figure 2](#) and click **Next**.



If a node is not present in the drop-down list box, it could be due to configuration issues with name lookup. The node name can be typed in manually.



TC05971A

Figure 2. Add Connectivity Server Node Dialog Box



Do not add the redundant Connectivity Server using this procedure. Refer to [Redundant Connectivity Servers](#) on page 38 when adding the redundant Connectivity Server.

7. Repeat [Step 5](#) and [Step 6](#) for all Primary Connectivity Servers (for example, one for the 800xA for Advant Master Connectivity Server and one for the AC 800M Connectivity Server), but not the (optional) redundant Connectivity Servers. Redundant servers will be added in [Redundancy](#) on page 36. When all Connectivity Servers have been added, proceed to [Step 8](#).
8. Verify that all Connectivity Servers are running after they are added.
 - a. Open a Plant Explorer Workplace.

- b. Use the Structure Selector to open the **Node Administration Structure**.
- c. Use the Object Browser to navigate to and select **All Nodes, Node Group** as shown in [Figure 3](#).

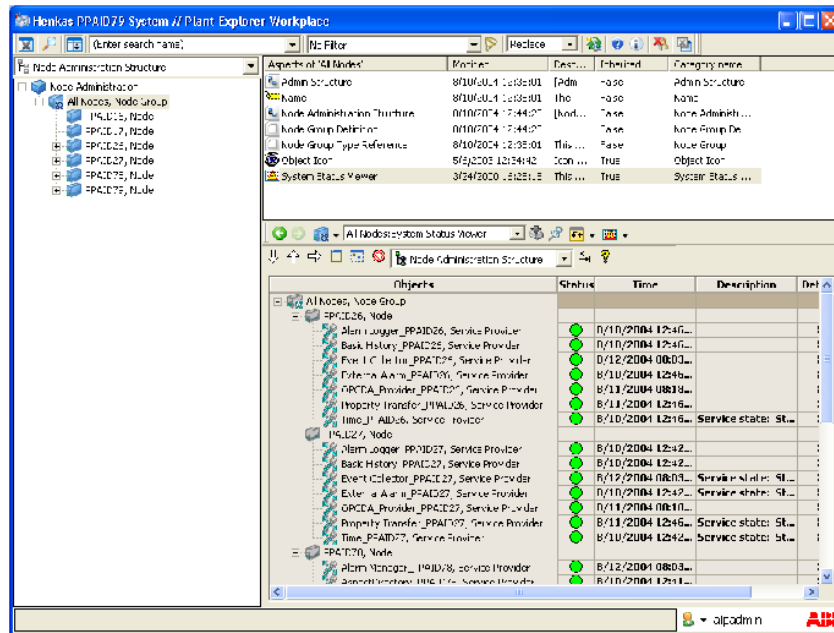


Figure 3. Verifying that Connectivity Servers and Services Are Running

- d. Select **System Status Viewer** in the Aspect List Area.
- e. The status is shown in the Preview Area.

Adding Clients

This procedure is required for all workplace client nodes including Operator Workplace Clients, Engineering Workplace Clients, IM Client Toolkit nodes, Batch Clients, and AO Clients.



Before adding any node, make sure that the node to be added has all required software installed. It must also have the same versions of system extension software installed as the Aspect Server.

To add a client follow the steps:

1. Start the Configuration Wizard on the Primary Aspect Server.
2. Select **System Administration** and click **Next**.
3. Select the system and click **Next**.
4. Select **Nodes** and click **Next**.
5. Select **Add Client** and click **Next**.
6. The Add Client Node dialog box appears. Select the node from the drop-down list box and click **Next**.
7. In the next dialog box, click **Finish**.
8. Repeat [Step 5](#) and [Step 7](#) for all clients.

Redundancy

To increase the uptime and eliminate loss of data, the 800xA System supports optional redundant server configurations. One of the key features of redundancy and parallel servers is the fail-over functionality from one Service Provider to another. If the Service Provider with which a client application is communicating fails, or if the whole server node where the Service Provider is running fails, the client node will perform a fail-over and connect to a redundant Service Provider on another server node. Future transactions will be transferred to the redundant Service Provider.



Performance can be increased by load balancing. Refer to [Affinity](#) on page 40.

Redundant Aspect Servers

This section provides guidelines for planning a redundant installation and instructions for configuring redundancy.

The redundant Aspect Server configuration is based on a *one-out-of-two (1oo2)* or *two-out-of-three (2oo3)* system.

The following base services are redundant in a redundant configuration of Aspect Servers:

- File Set Distribution (FSD) Service.

- Aspect Directory Service.
- Cross Referencing Service.
- System Message Service.
- Time Service.
- Alarm Manager Service.
- Soft Alarms Service.
- External Alarm Service.
- FF DataStorageAndDistribution service - if Device Management FOUNDATION Fieldbus is installed.
- Event Storage.
- Event Collector (2 instances).



Delete the third Event Storage Service Provider in a two-out-of-three (2oo3) configuration. The Event Storage service only runs on two Aspect Servers.



The License Service is not redundant and will be running only on the Primary Aspect Server.

Aspect Servers are the central storage mechanism, so special rules for redundancy apply. These rules are based on a majority-minority scheme, where the minority always goes into read-only mode and no updates are accepted. For example, in a 2oo3 Aspect Server configuration, all updates are always replicated to all three servers. If one of the servers can not find its cooperating servers, regardless of the reason (node shutdown, network problems), it becomes the minority and goes into read-only mode. If the other two servers are still running and can communicate with each other, they become the majority and continue to accept updates.

If an even number of Aspect Servers are configured, they consider themselves to be in majority if they are in contact with at least half of the servers and continue to accept updates. This means that in a 1oo2 Aspect Server configuration, if one server can not find its cooperating server it will continue to accept updates.

Before adding a redundant Aspect Server, verify that:

- The system exists and that the Primary Aspect Server is up and running. This is the node where the system was created under [Creating a System](#) on page 23.
 - The node to be added has all required software installed. It must also have the same versions of system extension software installed as the Primary Aspect Server.
1. Start the Configuration Wizard on the Primary Aspect Server.

2. Select **System Administration** and click **Next**.
3. Select the system and click **Next**.
4. Select **Nodes** and click **Next**.
5. Select **Add Redundant Server** and click **Next**.
6. The Select Redundant Node dialog box appears showing all available server nodes (Aspect and Connectivity Server nodes). Select the ***Aspect Server node*** to be duplicated and click **Next**.
7. In the next dialog box, select the node that will function as the redundant Aspect Server from the **Server Node** drop-down list box.
8. Select the **Update remote node** check box to update and activate the remote server node.
9. Click **Next**.
10. In the next dialog box, click **Apply**.
11. For a 2003 system, repeat these steps to add a third Aspect Server node.

Redundant Connectivity Servers

The redundant Connectivity Server configuration is based on running two servers in parallel.

In a redundant configuration of Connectivity Servers, the following base services are in parallel:

- Event Collector Service.
- Basic History Service.
- OpcDA_Connector Service.
- Property Transfer Service.
- Time Service.
- Alarm Logger Service.



Connectivity Server services are not fully redundant, but they are in parallel. This means that they will not replicate data between Service Providers.

Applications can read/write process data as long as at least one Connectivity Server is available.

Use the procedure under [Redundant Aspect Servers](#) on page 36 to add redundant Connectivity Servers, except select the **Connectivity Server** to duplicate in Step 6.



When a redundant Connectivity Server is added, OPC Data Access redundancy must be configured manually. Refer to [Configuring OPC Data Access Redundancy](#) on page 96.

Verifying the System and Servers

To verify that the system is running, and that all servers are working as configured:

1. Open a Plant Explorer Workplace.
2. Use the Structure Selector to open the **Node Administration Structure**.
3. Use the Object Browser to select All Nodes, Node Group as shown in [Figure 4](#).

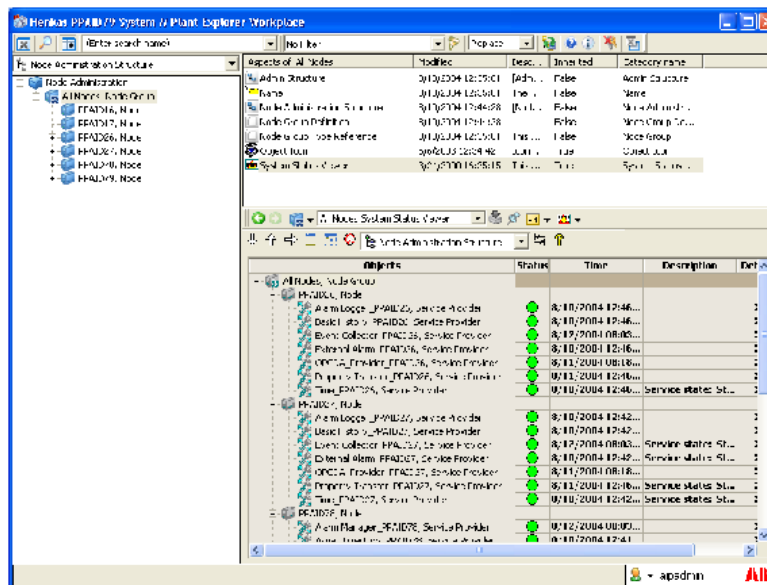


Figure 4. Verifying the System and Servers

4. Select `System Status Viewer` in the Aspect List Area.
5. The status is shown in the Preview Area.

Affinity



A new feature, the System Configuration Console, can be used to perform load balancing (affinity). Refer to *System 800xA Tools (2PAA101088*)* for information and instructions on using the System Configuration Console to configure load balancing.

Affinity is a means to ensure a predictable system configuration. To achieve predictable load balancing, affinity must be set up correctly. This section provides a brief overview of the affinity concept, guidelines for planning affinity, and instructions for configuring affinity in the system.



Configuring affinity is optional; however, if affinity is not configured, clients will randomly select providers for their services, which may lead to unpredictable performance.

Overview

Balancing the client load within a server group will achieve a predictable and stable running condition. This is especially important for Connectivity Servers, which handle large amounts of process data. Without load balancing, the problem can arise where one server node handles the larger part of the client node load, while the other server nodes are idling.

Affinity is also an important consideration with respect to Information Management. Clients should have affinity toward Information Management Servers with history configurations.

Affinity is configured using an affinity aspect placed in the **Administration Structure**. It specifies the order for which a client should pick servers for a certain service. For example, Client A must always connect to Connectivity Server A (when available) and Client B to Connectivity Server B. Refer to [Figure 5](#) for an example of load balancing.

Different services may use different affinity settings. Affinity settings for clients to services provided by Connectivity Servers differs from the settings for services provided by Aspects Servers.

The basic steps are:

- Create the Affinity aspect.
- Configure the Affinity aspect.
- Apply affinity settings to desired services.

These steps are described in detail in [Configuring Affinity](#) on page 44.

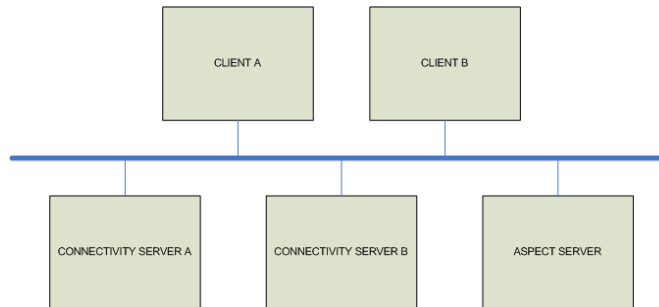


Figure 5. Configuration Example of Load Balancing

Planning Load Balancing

Affinity can be configured for redundant Aspect Servers as well as Connectivity Servers. Before configuring affinity, plan how to balance the client load between the redundant servers of the system.

When developing a new load balancing plan it is always recommended to maintain a triangle-relationship between a particular client, Aspect Server, and Connectivity Server as shown in [Figure 6](#). This is to minimize disturbance.

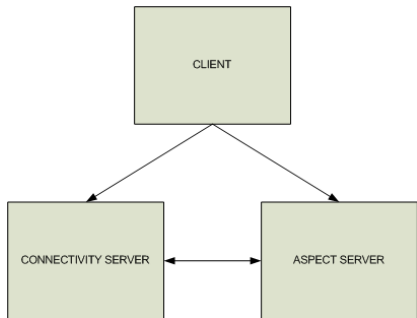


Figure 6. Triangle-Relationship for Planning Affinity

If Client 1 primarily accesses Aspect Server 3 and Connectivity Server 2, then Aspect Server 3 should also primarily access Connectivity Server 2, in order to maintain the triangle-relationship between Client 1, Aspect Server 3, and Connectivity Server 2.

Relationships are always planned and drawn from the client point of view. The relationship between the Aspect Server and the Connectivity Server is bidirectional, as both servers can act as clients and access the other one.



The triangle-relationship is kept only under normal running conditions of the system.

If one server of a triangle fails and the client fails over to the next server, the triangle-relationship is lost. There are no lower prioritized triangle-relationship setups for failure conditions.

The planned affinity settings are then transferred into a load balancing table. This table is later used as a base reference in the affinity configuration steps in [Configuring Affinity](#) on page 44. The numbers within the table indicate the order in which clients fail over to different servers. All triangle-relationships are entered into this table using the highest order number (1), indicating that this is the preferred access under normal running system conditions. The remaining cells are filled with lower order numbers, but they do not follow any triangle-relationships.

Figure 7 shows an example of a load balancing plan for a system with two clients, three Aspect Servers, and two Connectivity Servers. Bold numbers in Table 4 are results taken from the corresponding triangle-relationships.



It is not always possible to create triangle-relationships covering all servers without producing any conflicts in the load balancing table. The primary goal of planning load balancing is to define as many conflict free triangles as possible for the preferred client-server relationships, mainly for the operator stations, under a normal running system condition.

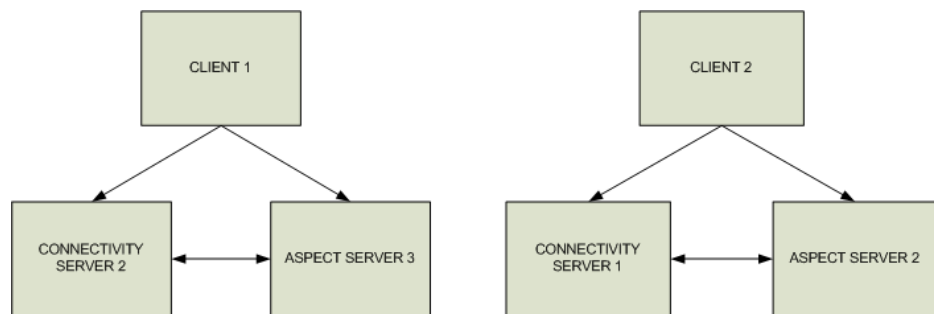


Figure 7. Load Balancing Plan Example

Table 4. Load Balancing Table for Load Balancing Plan in Figure 7

Affinity	Aspect Server 1	Aspect Server 2	Aspect Server 3	Connectivity Server 1	Connectivity Server 2
Client 1	3	2	1	2	1
Client 2	2	1	3	1	2
Aspect Server 1	1	2	3	2	1
Aspect Server 2	3	1	2	1	2
Aspect Server 3	2	3	1	2	1
Connectivity Server 1	3	1	2	1	2

Table 4. Load Balancing Table for Load Balancing Plan in [Figure 7](#) (Continued)

Affinity	Aspect Server 1	Aspect Server 2	Aspect Server 3	Connectivity Server 1	Connectivity Server 2
Connectivity Server 2	2	3	1	2	1

NOTE:
Bold entries are results taken from the corresponding triangle relationships.

Configuring Affinity

In this example, two Affinity objects are created: CS and AS. This is the recommendation for a redundant system.

Recommendations:

- Set up a redundant system and verify it before setting up the affinity.
- Use the following services when using affinity:
 - File Set Distribution (FSD) Service.
 - Aspect Directory Service.
 - Basic History Service.
 - Cross Referencing Service.
 - Opc_DA Connector Service.
 - Alarm Manager Service.
 - Event Storage.



For the client node, the affinity should be set in such a way that for all services running on an Aspect Server, the affinity is pointing to one (the same) Aspect Server in a 2oo3 setup. Do not point to different Aspect Servers for different services. This is also true for redundant (parallel) Connectivity Server pairs. The client should point to all services on one Connectivity Server, rather than mixing affinity settings.

The basic steps are:

- [Creating the Affinity Objects.](#)
- [Configuring the Affinity Aspects.](#)
- [Applying Affinity Settings to the Services.](#)

Creating the Affinity Objects

To create the Affinity objects:

1. Open a Plant Explorer Workplace.
2. Use the Structure Selector to open the **Admin Structure**.
3. Use the Object Browser to navigate to:
`Administrative Objects > Inventory Object> Affinity`
4. Right-click the **Affinity aspect type object** and select **New Object** from the context menu.
5. The New Object dialog box appears. Create a new object of type **Affinity**.
6. Specify a name (CS_Affinity) for the Affinity object in the **Name** field.
7. Repeat the procedure to create and name the AS Affinity object.

Configuring the Affinity Aspects

To configure the Affinity aspects:

1. Select the Affinity Definition aspect of an Affinity object in the Aspect List Area.
2. Select the **Configuration** tab in the Preview Area.
3. Click **Add** under the **Selection Group/Node** list to add clients to the list.
4. In the **Item Contents** list (to the right) specify the server nodes and server node groups and the order in which the client must connect to the servers. The client nodes select the server in order from top to bottom.
5. When defining CS_affinity, it is important to include every server that runs Basic History or OpcDA_Connector in **Item Contents** for every **Selection Group/Node**. This can be achieved by adding **All Nodes** to every **Selection Group/Node** as the last item.
6. Click **Apply**.

- 7. Verify the configuration in the **Affinity Summary** tab (Figure 8). The Affinity **Summary** tab lists the configuration performed for all nodes in the system.

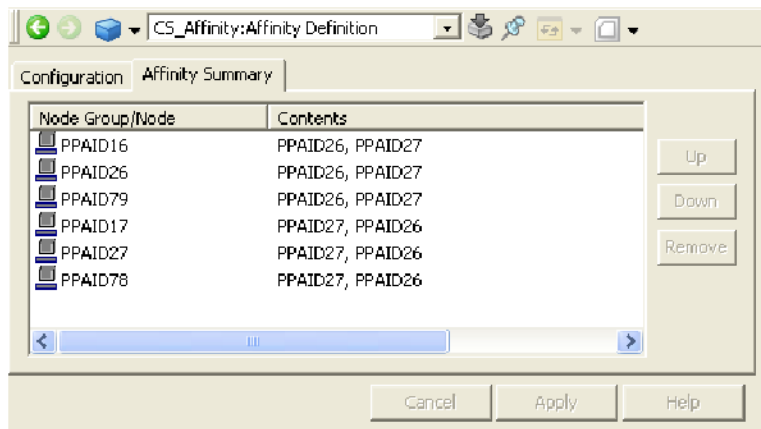


Figure 8. Affinity Summary Tab

- 8. Repeat this procedure for the AS affinity.

Applying Affinity Settings to the Services

ABB recommends setting up Affinity for services according to Table 5.

Table 5. Affinity Services

Affinity Objects	Services
AS_affinity	FSD, AspectDirectory, Cross Referencing Server, Alarm Manager, Event Storage
CS_affinity	Basic History, OpcDA_Connector

When the Affinity aspects have been configured, they must be set up to be used by the services in the system.

- 1. Use the Structure Selector to select the **Service Structure**.

2. Use the Object Browser to select the service to be load balanced.
3. Select `Service Definition` in the Aspect List Area.
4. Select the **Configuration** tab in the Preview Area.
5. Select the desired Affinity aspect from the **Affinity** drop-down list box and click **Apply**.

Defining Users

To define users and their roles and permissions, refer to *System 800xA Administration and Security (3BSE037410*)*.

Time Services

The following procedures must be performed to configure the Time Services:

- [Disabling the Windows Time Service](#).
- [Configuring the Time Service](#).
- [Configuring the System Time Server](#).
- [Configuring the Time Client](#).

Disabling the Windows Time Service

Perform this procedure on all nodes, except FOUNDATION Fieldbus Connectivity Servers nodes, Domain Controller nodes, and the designated Connectivity Time Servers.

1. Open Windows Control Panel.
2. Double-click `Administrative Tools` to open the Administrative Tools dialog box.
3. Double-click `Services` to open the Services dialog box.
4. Scroll down to and double-click `windows Time` to open the Windows Time Services (Local Computer) dialog box.
5. Click **Stop** in the Service Status field.
6. Select **Disabled** in the **Startup Type** drop-down list box.

7. Click **Apply** and then **OK**.

Configuring the Time Service

To configure the Time Service:

1. Open a Plant Explorer Workplace.
2. Use the Structure Selector to open the **Service Structure**.
3. Use the Object Browser to navigate to and select:
`Services > Time, Service`
4. Select `Service Definition` in the Aspect List Area.
5. Select the **Special Configuration** tab in the Preview Area.
6. Verify that the **Server Running** check box is selected. If it is not, select it.
7. Verify that the **Clients allowed to set time** check box is cleared. If it is not, clear it.
8. Verify that the **Enable external clock master function** check box is cleared. If it is not, clear it.
9. Click **Apply**.

Configuring the System Time Server

To configure the System Time Server:

1. Open a Plant Explorer Workplace.
2. Use the Structure Selector to open the **Service Structure**.
3. Use the Object Browser to navigate to and expand:
`Services > Time, Service > Basic, Service Group`
4. Select the Connectivity Server designated to act as the Time Server.
5. Select `Service Provider Definition` in the Aspect List Area.
6. Select the **Configuration** tab in the Preview Area.
7. For all nodes acting as a Time Server (primary or redundant):

- a. Verify that the **Enabled** check box is selected. If it is not, select it.
 - b. Click **Apply**.
8. For all other nodes not acting as a Time Server:
 - a. Disable the Service Provider by clearing the **Enabled** check box.
 - b. Click **Apply**.

-or-

Delete the Service Provider.

Configuring the Time Client

To configure the Time Client:

1. Open a Plant Explorer Workplace.
2. Use the Structure Selector to open the **Node Administration Structure**.
3. Use the Object Browser to navigate to and select a node in the list under:
Node Administration > All Nodes, Node Group
4. Select **Time Server Client Configuration** in the Aspect List Area.
5. Select the **Allowed to set time** check box, only if desired.
6. Select the **Time Sync Running** check box for all nodes.
7. Set the **Deviation Limit** to 1000 msec.
8. Click **Apply**.
9. Repeat [Step 3](#) through [Step 8](#) for every node in the system.

Base Function Setup for Scheduler and Calculations

Application Scheduler and Calculations may be installed and run on server nodes in the 800xA System that are not Information Management Servers. In this case, the service group/service provider objects for those services must be created manually for each of those non-Information Management Servers.

It is not possible to enable a calculation until it has been assigned to a specific service group or service provider. If a calculation is using a SoftPoint as an input or an output, it is recommended to have the Calculation aspect execute on the same node.

After manually adding the system extension, there are a number of configuration steps required in order to get the Scheduler and Calculations Services running.

1. Open a Plant Explorer Workplace.
2. Use the Structure Selector to open the **Service Structure**.
3. Create the Service Group object under the applicable service container in the **Service Structure**; for example, Calculation Server.
 - a. Select the service container, right-click and choose **New Object** from the context menu.
 - b. Assign a name to the new object. Typically, the name is based on the node, then select **Create**.
4. Create the service provider object under the new Service Group object.
 - a. Select the new Service Group object, right-click and choose **New Object** from the context menu.
 - b. Assign a name to the new Service Provider object. The name is typically based on the node, then select **Create**.
5. Configure the Service Provider object to point to the node where the service (in this case Calculations) must run.
 - a. Select the Service Provider object in the object browser.
 - b. Select `Service Provider Definition` in the Aspect List Area.
 - c. Select the **Configuration** tab in the Preview Area.
 - d. Use the **Node** drop-down list box to select the node where the service will run.
 - e. Select the **Enabled** check box.
 - f. Click **Apply**.

Redundant Calculation Servers

The redundant Calculation Server option allows for a primary Calculation Server running in Service mode and a redundant Calculation Server running in Standby mode during normal operation. When the primary Calculation Server is down, the redundant Calculation Server will become the primary and begin scheduling/executing the Calculations assigned to its Service Group. Calculations can only be assigned to Service Groups, not Service Providers.

Refer to the following as applicable to the system configuration:

- [Two Information Management Nodes](#) on page 51.
- [Two Nodes Where One is an Information Management Node](#) on page 52.
- [Two Non-Information Management Nodes](#) on page 52.

Two Information Management Nodes

After Installation of software on two Information Management nodes and the nodes have been added to the system, there should be a Calculation Service Group for each node with a Service Provider under each group. These will not be used with redundant Calculation Servers. To set up the redundant Calculation Servers, perform the following.

1. Disable the two Calculation Service Providers.
2. Create a third Calculation Service Group to be used for redundancy.
3. Add a Service Provider to the newly created Service Group.
4. Assign the newly added Service Provider to one of the two Information Management nodes.
5. Enable the Service Provider and it should go into Service mode and become the primary.
6. Add a second Service Provider to the newly created Service Group.
7. Assign the second newly added Service Provider to the other Information Management node.
8. Enable the Service Provider and it should go into Standby mode.
9. Delete the original two Calculation Service Groups.

Two Nodes Where One is an Information Management Node

To set up the redundant Calculation Servers where one of them is an Information Management node, perform the following:

1. Disable the Service Provider on the Calculation Service Group that was created by the Information Management node.
2. Create a Calculation Service Group to be used for redundancy.
3. Add a Service Provider to the redundant Calculation Service Group.
4. Assign its node and enable the Service Provider. It should go into Service mode and become the primary.
5. Add a second Service Provider on the Calculation Service Group to be used for redundancy.
6. Assign its node and enable the Service Provider. It should go into Standby mode.
7. Delete the original Calculation Service Group that was created by the Information Management node.

Two Non-Information Management Nodes

To set up the redundant Calculation Servers when neither of them is an Information Management node, perform the following:

1. Create a Calculation Service Group to be used for redundancy.
2. Add a Service Provider to the newly created Service Group.
3. Assign the newly added Service Provider to one of the two nodes.
4. Enable the Service Provider and it should go into Service mode and become the primary.
5. Add a second Service Provider to the newly created Service Group.
6. Assign the second newly added Service Provider to the node.
7. Enable the Service Provider and it should go into Standby mode.

Section 3 SoftPoint Server

Introduction

The SoftPoint Server can be configured to run on any type of 800xA System server node. The section describes how to configure the installed SoftPoint Server software using the Softpoint Generic Control Network Configuration Wizard. This will automatically:

- Configure the SoftPoint Service Group object and Service Provider objects.
- Configure the Virtual Control Network by which other system applications (History, desktop applications, etc.) can access the SoftPoint data on that node.
- Configure the Source Definition aspect for each network. This is used to deploy the SoftPoints on their respective nodes.
- Integrate the SoftPoint Alarm and Event messages into the 800xA System Event Collector Service.

SoftPoint redundancy is supported on an Information Manager Server pair (these are Connectivity Servers). When installed on a redundant Connectivity Server, it should follow the rules as established in the connectivity for configuration. For greatest efficiency between Calculations and SoftPoints, put the Primary Calculation Server on the same node as the Primary SoftPoint Server.

Configuring Softpoint Services

1. Open a Plant Explorer Workplace.
2. Use the Object Browser to navigate to and right-click:
 Root, Domain
3. Select **New Object** from the context menu.

4. This displays the New Object dialog box. Expand the Object Types category, and select:
Softpoint Generic Control Network (under Softpoint Basic Object Types).
5. Enter a name to identify the network (for example: *Network1*) and then click **Create**.
6. Select the Generic Control Network Configuration aspect of the new object in the Aspect List Area.
7. Click the **Configure** tab in the Preview Area to produce the view shown in [Figure 9](#).

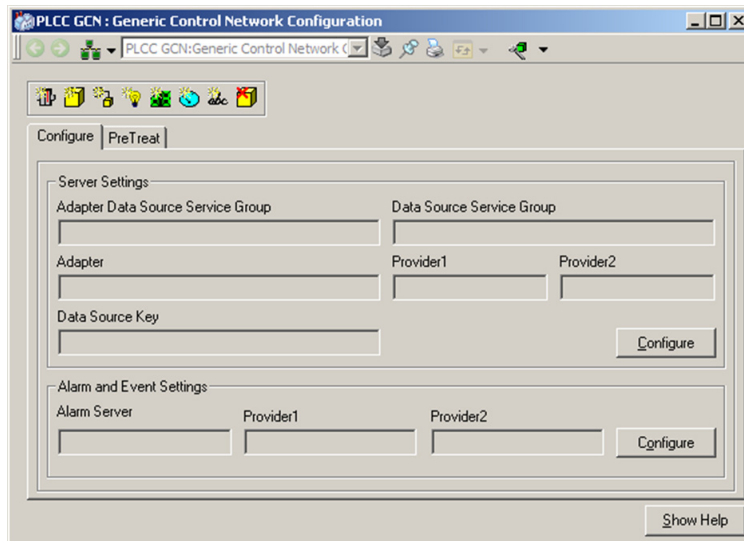


Figure 9. Generic Control Network Configuration Aspect

8. Click **Configure** in the Server Settings Frame. This launches the Choose Connectivity Server Node dialog box.
9. Select the primary Connectivity Server Node and click **OK**.
10. Click **OK** at the configuration completed message.

11. Click **Configure** in the Server Settings frame again if redundant Connectivity Servers were created. This launches the Choose Connectivity Server Node dialog box again.
 - a. Select the **Node is redundant provider** check box.
 - b. Select the redundant Connectivity Server Node where the SoftPoint Server software is installed and click **OK**.
12. Click **OK** at the configuration completed message.
13. In order for the System Message Service to collect alarms and events from the SoftPoints on this network, the OPC Alarm Server for SoftPoint messages must be added to an Event Collector Service Group. This is done automatically when the Alarm and Event Settings portion of the **Generic Control Network Configuration** aspect is configured.
 - a. Click **Configure** in the Alarm and Event Settings frame of the Generic Control Network Configuration aspect.
 - b. Add providers in the same way as for the Server Settings.

Section 4 Diagnostics Collection Tool

Introduction

This section contains post installation procedures for the Diagnostics Collection Tool (DCT) software.



DCT software must be run under a user account with Administrative privileges.

Changing the ABBResults Directory Share Location

The default path for the folder created for ABBResults is:

`... \ABBResults`

It is set to be shared with full access rights for the 800xA Service User account.

The location of the ABBResults directory share can be changed. The ABBResults directory share is where the Diagnostics Collection Tool stores previously generated cabinet (cab) files. To change the location of the ABBResults directory share:

1. Launch the Diagnostics Collection Tool.
2. Select the **Collect Data** option in the ABB DCT dialog box and click **OK**. This launches the Collection Tools dialog box.
3. Select

Tools > Options

to launch the DCT Options dialog box.

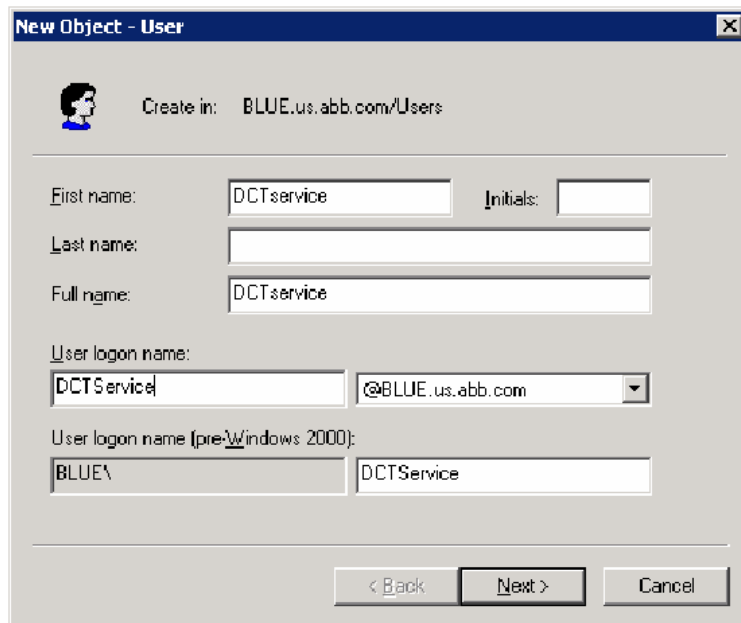
4. Select the **Collecting Data** tab and click **Browse**.
5. Select the desired folder for the ABBResults directory share and click **OK**.
6. Restart the Diagnostics Collection Tool.

Modifying the DCT Service Account for a Domain Controller

The DCT Service Account must be modified after the DCT software is installed on a Domain Server node.

1. Add the DCTService User to the Domain Server.
 - a. To launch the Active Directory of Computers and Users dialog box, select:
Start > All Programs > Administrative Tools > Active Directory of Computers and Users
 - b. In the left pane of the Active Directory of Computers and Users dialog box, navigate to:
Domain Name > Users
 - c. Select:
New > User
from the context menu to launch the New Object - User Wizard.
 - d. Fill in the fields as shown in [Figure 10](#) and **click** Next.
 - e. Fill in the password in the Password and Confirm Password fields and **click** Next. Select a password that conforms to the system password policy settings.
 - f. Click **Finish** in the next dialog box to exit the wizard.
2. Add the DCTService User to the Administrators Group.
 - a. In the right pane of the Active Directory Users and Computers dialog box, right-click DCTService and select **Properties** from the context menu to launch the DCTService Properties dialog box.
 - b. Select the **Member Of** tab.

- c. Click **Add** to launch the Select Groups dialog box.



The screenshot shows the 'New Object - User' dialog box. At the top, it says 'Create in: BLUE.us.abb.com/Users'. Below this, there are several input fields: 'First name' with 'DCTservice', 'Last name' (empty), 'Full name' with 'DCTservice', 'User logon name' with 'DCTService' and a dropdown menu showing '@BLUE.us.abb.com', and 'User logon name (pre-Windows 2000)' with 'BLUE\'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Figure 10. New Object - User Wizard

- d. Click **Advanced** to launch the dialog box shown in [Figure 11](#).
 - e. Click **Find New** and select `Administrators` in the Search Results frame.
 - f. Click **OK** until all dialog boxes are closed.
3. Grant the DCTService log on as a service right.
 - a. Select:
Start > All Programs > Administrative Tools > Domain Controller Security Policy

to launch the Default Domain Controller Security Settings dialog box.

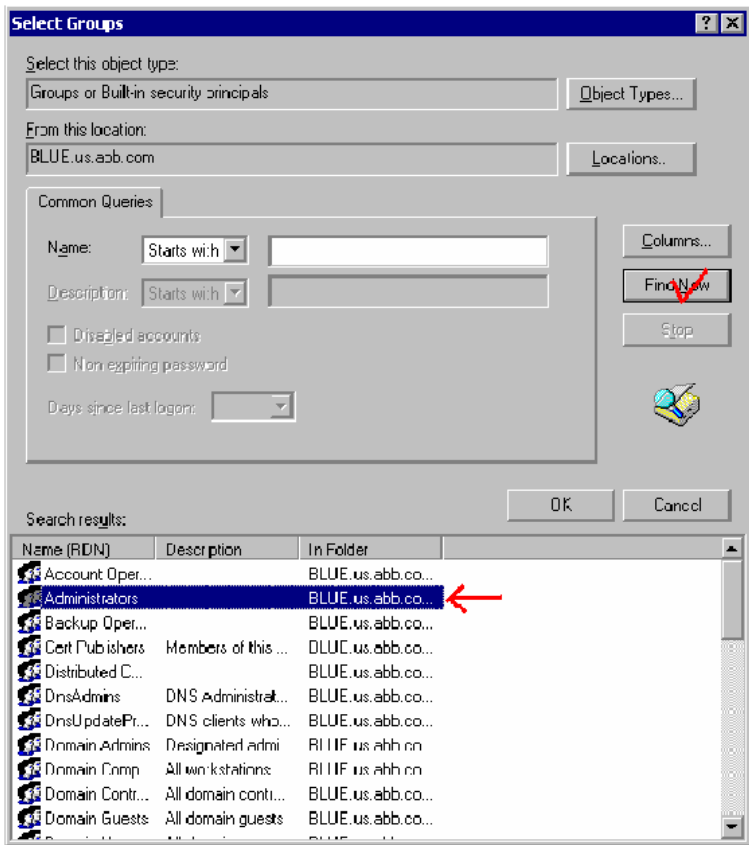


Figure 11. Adding the DCTService User to Administrators Group

- b. Navigate to:
Local Policies > User Rights Assignments
in the left pane of the Default Domain Controller Security Settings dialog box.
- c. Right-click Log on as a service user in the right pane and select **Properties** from the context menu to launch the Log on as a Service Properties dialog box.

- d. Click **Add User or Group** to open the Add User or Group dialog box.
- e. Click **Browse** to open the Select Users, Computers, or Groups dialog box.
- f. Click **Advanced** to open the dialog box shown in [Figure 12](#).

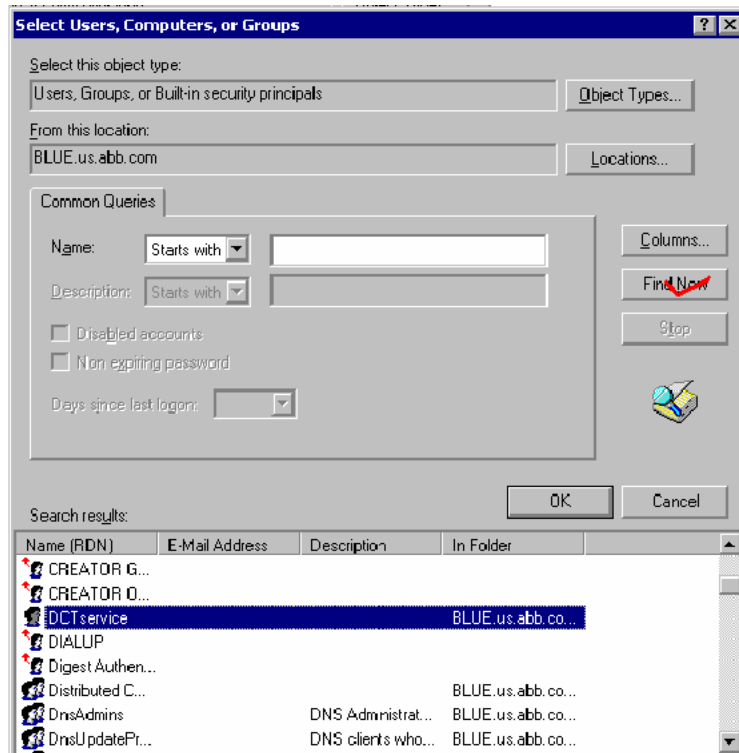


Figure 12. Granting the DCTService User Log On as a Service Rights

- g. Click **Find** and select DCTService from the list.
 - h. Click **OK** until all dialog boxes are closed.
4. Modify the ABBResults folder security so that the DCTService can write the results.
 - a. Open My Computer from the desktop.
 - b. Navigate to and right-click on:

Drive:\ABResults

to open the ABResults Properties dialog box.

- c. Select Administrators and click **Add** to launch the Select Users, Computers, or Groups dialog box.
- d. Click **Advanced** to launch the next dialog box.
- e. Click **Find** and select DCTService in the Search results frame.
- f. Upon return to the ABResults Properties dialog box, configure it according to [Figure 13](#).

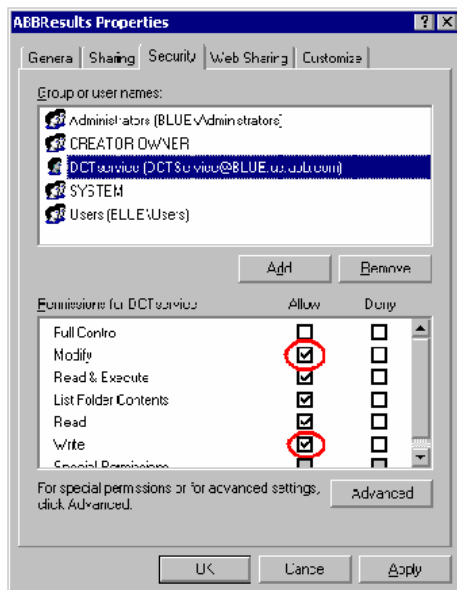


Figure 13. Modifying the ABResults Security Folder

- g. Click **OK** until all dialog boxes are closed.
5. Modify the ABB Node Interrogator Service log in to use the DCTService User account.
 - a. Select:

Start > Administrative Tools > Services

to launch the Services dialog box.

- b. Navigate to and right-click on ABB Node Interrogator.
- c. Select **Properties** from the context menu to open the ABB Node Interrogator Service Properties dialog box.
- d. Select the **Log On** tab to produce the view shown in [Figure 14](#).

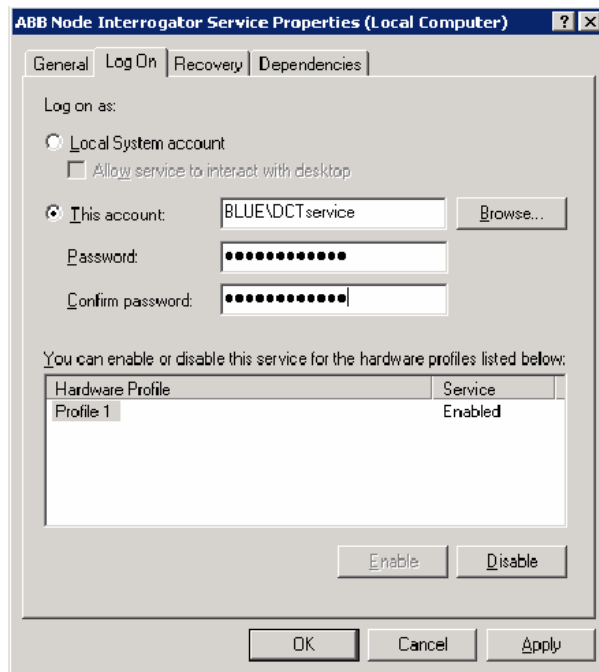


Figure 14. Modifying the ABB Node Interrogator Service

- e. Fill in the information as shown in [Figure 14](#) and click **Apply**.
- f. Select the **General** tab.
- g. Click **Stop** and then **Start** to stop and restart the service. This allows the new user settings to take effect.

Section 5 SMS and e-mail Messaging

Introduction

The procedure in this section is required to correctly configure the location of an Application Server for SMS and e-mail Messaging in the **Service Structure**.

Configuring the Location of the Application Server

Perform the following steps to configure the location of the Application Server for SMS and e-mail Messaging.

1. Open a Plant Explorer Workplace.
2. Use the Structure Selector to open the **Service Structure**.
3. Use the Object Browser to navigate to:
`Services > Messenger Server, Service > Messenger SG_1,
Service Group > Messenger SP_1, Service Provider`
4. Select `Service Provider Definition` in the Aspect List Area.
5. Select the **Configuration** tab in the Preview Area:
 - a. Select the node designated to run the Messenger Service in the **Node:** drop-down list box.
 - b. Select the **Enabled** check box and click **Apply**.
 - c. Verify that the Current field (below the **Enabled** check box) changes from `Undefined` to `Service`.

Restarting the Event Collector Service

Perform the following steps to see events in the Messenger Event Log:

1. Use the Structure Selector to open the **Service Structure**.
2. Use the Object Browser to navigate to:

```
Event Collector,Service > ABB 800xA System Message  
Server,Service Group > Event Collector_ABB 800xA  
System Message Server_NodeName, Service Provider
```

where NodeName is the node where the service is registered which is generally the Aspect Server node.

3. Select `Service Provider Definition` in the Aspect List Area.
4. Clear the **Enabled** check box and click **Apply**.
5. Select the **Enabled** check box and click **Apply**.
6. This will restart the `Event Collector_ABB 800xA System Message Server_NodeName` service and the Messenger Event Log will display all events.

Section 6 Structured Data Logger (SDL)

Introduction

This section provides post installation procedures for the Structured Data Logger (SDL).

Configuring the SDL Collector Service

The SDL Collector service is configured via the standard Service Group aspect. The Service Group aspect defines one SDL Collector service with one connection to a database. More Service Group objects may be added for connection to more database instances.



The SDL Collector Service reads data from SDL Log Aspects and the SDL Log Aspects read the configuration from the database for the configured properties. Therefore, connecting and reconnecting to a database with a high amount of logs can take some time. For example, a database with 1,000 logs may take up to 20 minutes.

SDL Collector Service Group



If more than one SQL Server 2008 SP2 instance is used a SDLCollector Service Group object with a Service Group Definition aspect must be assigned to each.

1. Open a Plant Explorer workplace.
2. Use the Structure Selector to open the **Service Structure**.
3. Use the Object Browser to navigate to and select:
`Services > SDLCollector, Service > SDLCollector,
Service Group`
4. Select Service Group Definition in the Aspect List Area.

5. Select the **Special Configuration** tab in the Preview Area.
6. The **Special Configuration** tab is divided into three sections:
 - **SQL Database Connect:** This section specifies:
 - **DB Instance field:** The SQL Server instance with the SDL database.
 - **Number of connections field:** The SDL Collector may use more parallel connections to the SQL Server database.
 - **Trusted Connection check box:** Select so that Windows Login credentials are used.
 - **Protocol timers:** This section specifies:



The value of the Read timer protocol timer must be greater than the OPC read cycle for the communication channel used. Failure to comply with this may cause the SDL Collector to abort a previous read request and reread properties before a result can be returned, forcing it into an endless loop.

- **Read timer field (value in ms):** An SDL Collector waiting period before rereading OPC data that had bad status. The recommended value is 10,000. Refer to **SDL Collector Functions** in *System 800xA Configuration (3BDS011222*)*.
- **ADO timer field (value in ms):** An SDL Collector waiting period before reconnecting to the database after a failed call to the database. The recommended value is 60,000.
- **DB maintenance:** This section specifies:
 - **Delete data older than field:** The retention period of the collected data in terms of days. Data older than the specified number of days is deleted.



The minimum retention period must be longer than 35 days to avoid unintended deletion of data.

- **days every and at fields:** Day of the week and time of day that the data will be deleted.



DB maintenance that requires the Structured Data Logger database to be taken offline requires that the database be detached and then attached in order to close any open connections.

Figure 15 shows a typical SDL Collector Service Group configuration. The values will vary depending on the installation.

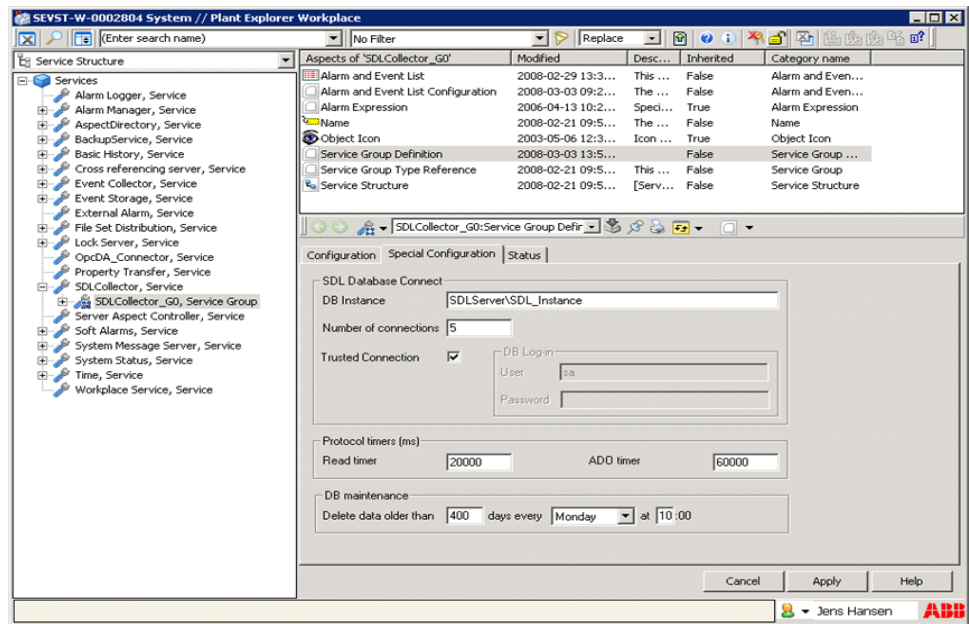


Figure 15. SDL Collector Service Group

SDL Collector Service Provider



The node assigned to run the SDL Collector Service must be a nonredundant Application Server node or the service must reside on the Database Server node.



Multiple SDL Collector Service Providers are not supported.

The SDL Collector service is run by a Service Provider. The Service Provider is a server node assigned to run the service. This assignment is made via the Service Provider Definition aspect on the SDL Service Provider object under the SDL Service Group object:

1. Open a Plant Explorer workplace.

2. Use the Structure Selector to open the **Service Structure**.
3. Use the Object Browser to navigate to and select:
 Services > SDLCollector, Service > SDLCollector,
 Service Group > SDLCollector_<Server>, Service
 Provider
4. Select Service Group Definition in the Aspect List Area.
5. Select the **Configuration** tab in the Preview Area (if not already selected).
6. Select the **Enabled** check box.
7. Select the Service Provider in the Node field.

Figure 16 shows a typical SDL Collector Service Provider configuration. The values will vary depending on the installation.

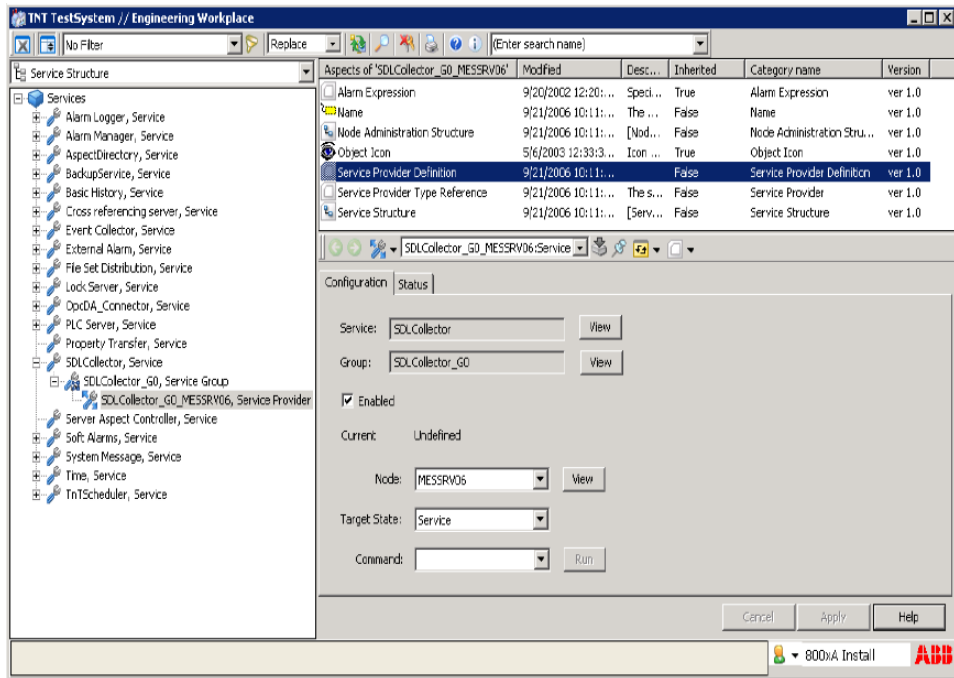


Figure 16. SDL Collector Service Provider

Post Installation when Using SoftController

Perform the following only if using SoftController.

1. Start the SoftController.
2. Start the OPC Server.
3. Download the applications.
4. Restart the SDL Collector Service.
 - a. Open a Plant Explorer workplace.
 - b. Use the Structure Selector to open the **Service Structure**.
 - c. Use the Object Browser to navigate to and select:
`Services > SDLCollector, Service > SDLCollector,
Service Group > SDLCollector_<Server>, Service
Provider`
 - d. Select Service Group Definition in the Aspect List Area.
 - e. Select the **Configuration** tab in the Preview Area (if not already selected).
 - f. Clear the **Enabled** check box and click **Apply**.
 - g. Select the **Enabled** check box and click **Apply**.

Installation Troubleshooting

It may be necessary to install Structured Data Logger software again in some circumstances.

The following scenarios outline corrective actions. They are presented in order from least to most serious. It is assumed for all scenarios that the 800xA System itself is intact.

1. **A specific 800xA Client with SDL does not function but other 800xA Clients and Servers do.**
 - a. Use Add/Remove Programs in Windows Control Panel to uninstall the SDL software.

- b. Refer to *System 800xA Installation (3BSE034678*)* and install the SDL software, but do not select Database Components in the Installed Features Selection dialog box.
- 2. **A specific 800xA Application Server with SDL, including SDL the database, does not function. The database and the installation files are intact.**
 - a. Use Add/Remove Programs in Windows Control Panel to uninstall the SDL software.
 - b. Refer to *System 800xA Installation (3BSE034678*)* and install the SDL software, but do not select Database Components in the Installed Features Selection dialog box.
 - c. Use the System Extension Maintenance feature in the Configuration Wizard to update the SDL system extension (refer to **System Extension Maintenance** in *System 800xA Tools (2PAA101888*)*).
- 3. **A specific 800xA Application Server with SDL including the SDL database, does not function. The database is intact, but the installation files are lost.**
 - a. Use Add/Remove Programs in Windows Control Panel to uninstall the SDL software.
 - b. Refer to *System 800xA Installation (3BSE034678*)* and install the SDL software, but do not select Database Components in the Installed Features Selection dialog box.
 - c. Use the System Extension Maintenance feature in the Configuration Wizard to update the SDL system extension (refer to **System Extension Maintenance** in *System 800xA Tools (2PAA101888*)*).
- 4. **A specific 800xA Application Server with SDL, including SDL database, does not function. The database data storage is intact, but the stored procedures and the installation files are outdated, corrupt, or lost.**
 - a. Use Add/Remove Programs in Windows Control Panel to uninstall the SDL software.
 - b. Refer to *System 800xA Installation (3BSE034678*)* and install the SDL software.

- c. Use the System Extension Maintenance feature in the Configuration Wizard to update the SDL system extension (refer to **System Extension Maintenance** in *System 800xA Tools (2PAA101888*)*).
- 5. **A specific 800xA Application Server with SDL, including SDL database, does not function. The database and the installation files are lost.**
 - a. Perform a complete new installation as described in *System 800xA Installation (3BSE034678*)* with one exception: instead of the action in Create the SDL Database perform a restore of the latest backup of the SDL database as described in *System 800xA Maintenance (3BSE046784*)*.



If the SDL database resides on a separate database server the actions in scenario 4 and 5 concerning the database can be applied.

System Synchronization Recommendations

Consider how the engineering and production system are connected to the databases if using System Synchronization. The SDL Collector service object holds the specification of the connections to the databases.

After a restore of a system or synchronization of the services, perform the following:

- The DB Instance field must be amended to hold the correct instance reference in the **Special Configuration** tab of every SDL Collector Service Group.
- The Node field must be amended to hold the correct node name in the **Configuration** tab of the SDLCollector Service Provider.

Section 7 800xA for AC 800M

Introduction

This section contains procedures for:

- [Control Builder M.](#)
- [AC 800M Controller.](#)
- [OPC Server Configuration.](#)

Control Builder M

Setting up the Control Builder M includes planning and defining the number of OPC and Panel 800 Alarm and Event Subscriptions.

Planning

The Control Builder M software needs to be configured by setting a number of parameters. The following is a summary of the most important ones:

- **File locations:** Control Builder M installations on separate nodes must never point to the same Working Folder on a shared disk; however, it is permissible for the Working Folder to be in the same relative location on the local disk of each node.

If changes are needed to the Control Builder M default settings:



Windows Administrator privileges are required to change the settings.

1. Run the Setup Wizard ([Figure 17](#)) on the Engineering Station and other nodes where the Control Builder M is installed. Select:

Start > All Programs > ABB Industrial IT 800xA > Engineering > Utilities > Setup Wizard

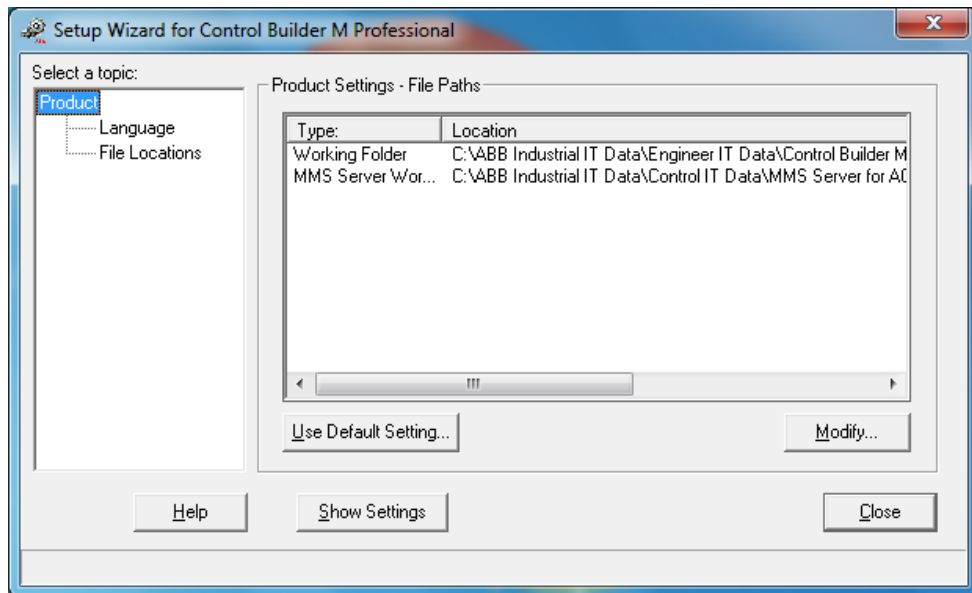


Figure 17. Control Builder M Setup Wizard

2. Enter the required configuration parameters under **Product**.
3. Click **Show Settings** and check the settings (summary of all configuration parameters).
4. To make additional changes, refer to the other items in the Control Builder M under:

Tools > Setup > Station

Refer to the Online Help for detailed information on these items.

Defining the Number of OPC and Panel 800 Alarm and Event Subscriptions



Return to this procedure at a later time if no controller applications are created at this point.

The controllers are set to deliver Alarm and Event data to only one OPC Server or Panel 800 by default. If there is more than one OPC Server and/or Panel 800 connected to a given controller, as is typically the case in redundant configurations, then adjust this setting. It should not be larger than the number of connected OPC Servers and Panel 800s, as this will increase the memory load in the controller.

The following procedure describes how to define the number of OPC and Panel 800 Alarm and Event subscriptions. Perform the procedure for each of the controllers in the network.

1. Open Control Builder M (on the Engineering Station). Select:
Start > All Programs > ABB Industrial IT 800xA > Engineering > Control Builder M
2. Control Builder M must be in Offline mode. If it is not, click the **Offline** icon in the Control Builder M.

3. Double click to open the 0 item for the controller as shown in Figure 18.

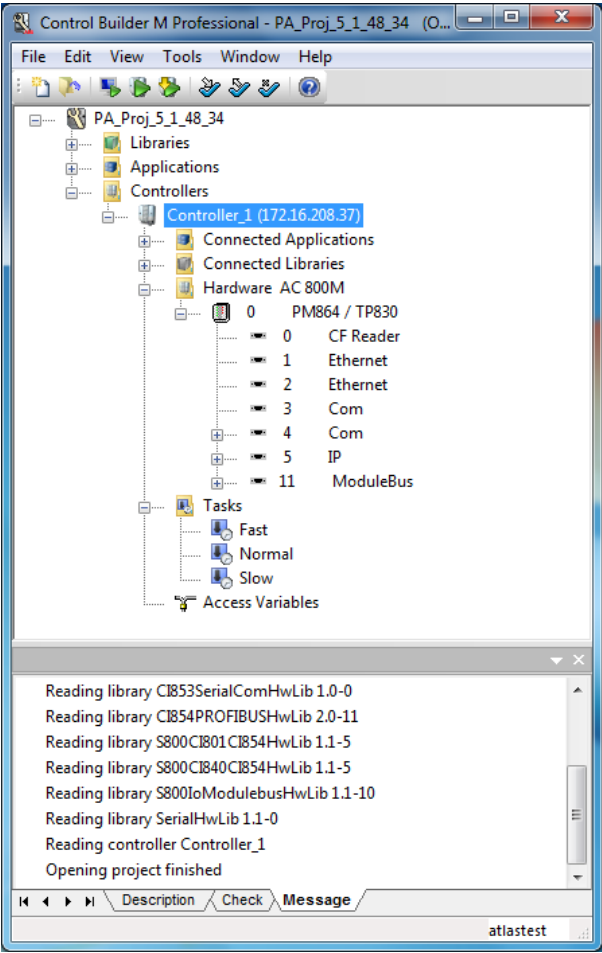
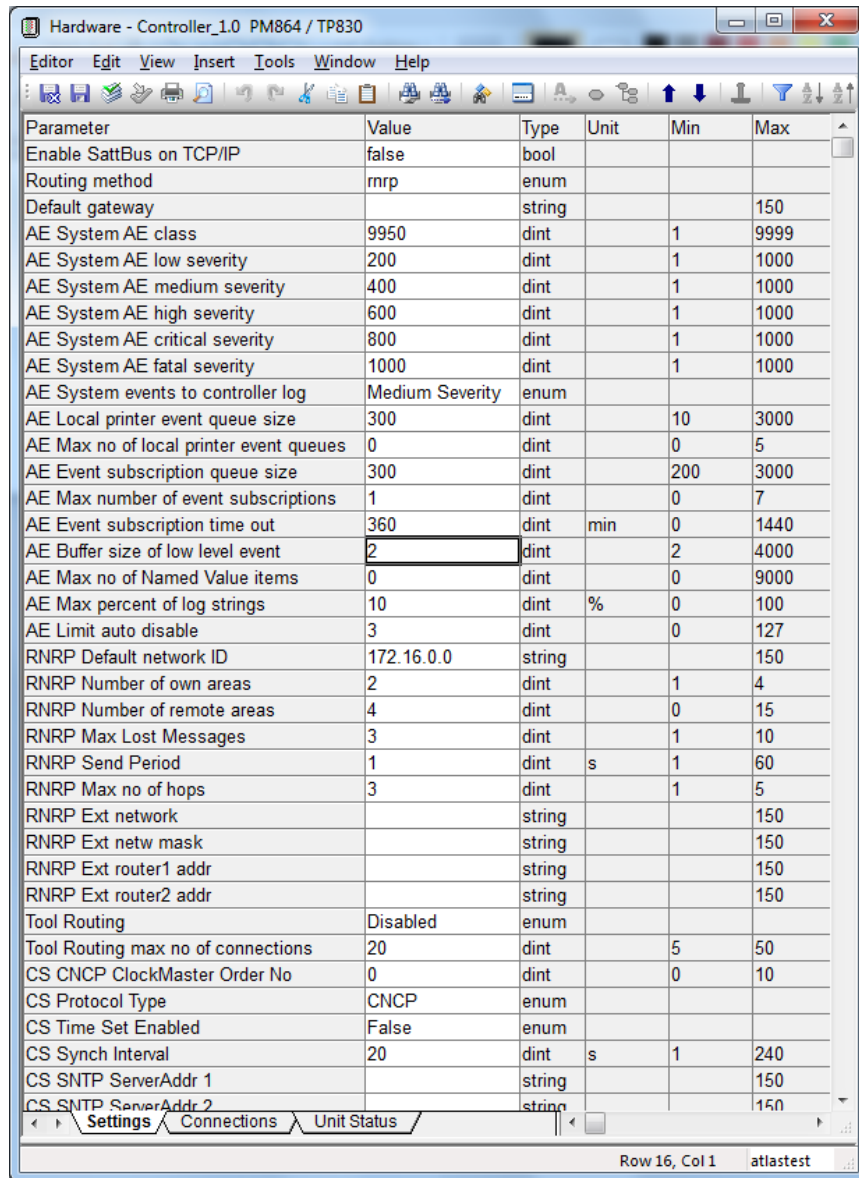


Figure 18. Control Builder M

4. Select the **Settings** tab to view the parameters as shown in Figure 19.



Parameter	Value	Type	Unit	Min	Max
Enable SattBus on TCP/IP	false	bool			
Routing method	mrp	enum			
Default gateway		string			
AE System AE class	9950	dint		1	9999
AE System AE low severity	200	dint		1	1000
AE System AE medium severity	400	dint		1	1000
AE System AE high severity	600	dint		1	1000
AE System AE critical severity	800	dint		1	1000
AE System AE fatal severity	1000	dint		1	1000
AE System events to controller log	Medium Severity	enum			
AE Local printer event queue size	300	dint		10	3000
AE Max no of local printer event queues	0	dint		0	5
AE Event subscription queue size	300	dint		200	3000
AE Max number of event subscriptions	1	dint		0	7
AE Event subscription time out	360	dint	min	0	1440
AE Buffer size of low level event	2	dint		2	4000
AE Max no of Named Value items	0	dint		0	9000
AE Max percent of log strings	10	dint	%	0	100
AE Limit auto disable	3	dint		0	127
RNRP Default network ID	172.16.0.0	string			150
RNRP Number of own areas	2	dint		1	4
RNRP Number of remote areas	4	dint		0	15
RNRP Max Lost Messages	3	dint		1	10
RNRP Send Period	1	dint	s	1	60
RNRP Max no of hops	3	dint		1	5
RNRP Ext network		string			150
RNRP Ext netw mask		string			150
RNRP Ext router1 addr		string			150
RNRP Ext router2 addr		string			150
Tool Routing	Disabled	enum			
Tool Routing max no of connections	20	dint		5	50
CS CNCP ClockMaster Order No	0	dint		0	10
CS Protocol Type	CNCP	enum			
CS Time Set Enabled	False	enum			
CS Synch Interval	20	dint	s	1	240
CS SNTP ServerAddr 1		string			150
CS SNTP ServerAddr 2		string			150

Row 16, Col 1 atlastest

Figure 19. Parameters Under the Settings Tab

5. Change AE Max number of event subscriptions to the sum of the OPC Servers and Panel 800s connected to this controller.
6. Click the **Save and Close** icon when finished.
7. Repeat [Step 3](#) through [Step 6](#) for each of the controllers in the network.
8. Click the **Download Project and Go Online** icon in the Control Builder M Toolbar when finished.

AC 800M Controller

This section describes how to download firmware for AC 800M Controllers. The firmware is the basic runtime software in the controllers and its (optional) communication interfaces. It also describes how to initially set the IP address in the controllers.

Downloading Controller Firmware via Serial Line



The initial firmware upgrade can also be made using a Compact Flash image. A serial RS-232 tool cable is then not needed. Refer to **Loading System Firmware on PM86X CPU using Compact Flash Card** in *System 800xA Control AC 800M Configuration (3BSE035980*)*.

The AC 800M firmware must be downloaded to each AC 800M Controller before it can be used. The factory supplied firmware needs to be replaced by a firmware version that matches the version of the Control Builder M.

At the first download of the firmware, a serial RS-232 tool cable (TK212 or TK212A) is needed to connect the controller and the Control Builder M node, as well as the Control Builder M software installed on the node.

To download the firmware:

1. Connect the serial RS-232 tool cable between the Control Builder M node and the tool port of the controller, as specified in [Table 6](#).

Table 6. Cable Connection

Controller	Tool Port	Connector	Cable Name
AC 800M	COM 4	RJ 45	TK212 or TK212A

2. Select the appropriate COM port for the Control Builder M node (default COM 1).



No program capable of blocking the selected COM port must be running during the upgrade procedure.

3. Power up the controller.
4. Select:
Start > All Programs > ABB Industrial IT 800xA > Engineering > Utilities > Serial Firmware Upgrade
5. Select **Settings** from the dialog box, followed by the COM port selected for the Control Builder M node.
6. Click **Connect**.
7. Hold down the **Init/Reset** button on the controller for at least 3 seconds until the green **R** LED starts to blink.
8. Release the **Init/Reset** button and the controller will perform a cold test. Wait about a minute until a message appears.

- a. If the connection is correct, then the Serial Firmware Upgrade dialog box appears as shown in [Figure 20](#).

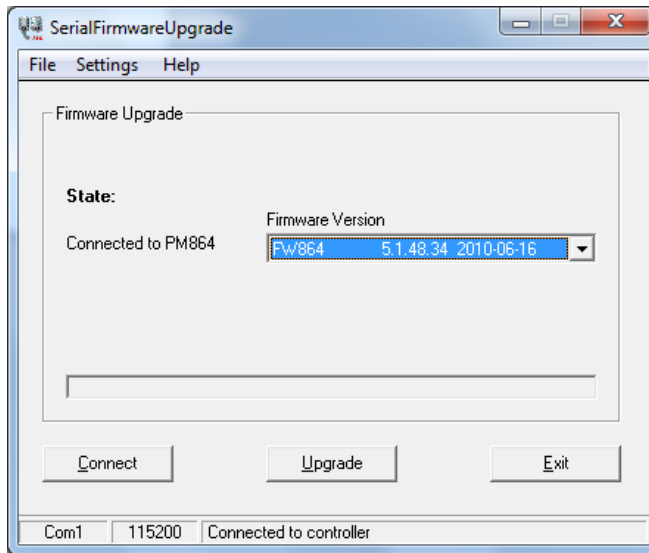


Figure 20. Serial Firmware Upgrade Dialog Box

- b. If the `Connect` failed error message appears, check the cables and repeat the steps thus far in this procedure (refer to the Serial Firmware Upgrade Online Help).
9. Select the firmware version in the **Firmware Version** drop-down list box.
10. Click **Upgrade** and wait five to ten minutes. The LED behavior during the upgrade procedure is described in the Serial Firmware Upgrade Online Help.
11. Hold down the **Init/Reset** button on the controller for at least three seconds. For redundant controllers, repeat this procedure for both CPUs.
12. Before checking the firmware download, or connecting an AC 800M Controller to a Control Network, its IP address must be set. Refer to [Setting IP Address for AC 800M Controllers](#).

Setting IP Address for AC 800M Controllers

Each AC 800M Controller must have a unique IP address and associated subnet mask before it can be used in a Control Network. The IP address can be initially set after the firmware for the controller has been installed. The IP address can be changed via the Control Network once it has been initially set.

At the first setting of an IP address in a controller, a serial RS-232 tool cable (TK212 or TK212A) is needed to connect the controller and the Control Builder M node. The Control Builder M software must be installed on the node.



Check that the Serial Firmware Upgrade tool is not running. If it is, that application will allocate the COM port.

1. Connect the serial RS-232 tool cable between the Control Builder M node and the tool port of the controller, as specified in [Table 6](#).



If the controller is redundant, the serial line should be connected to the primary CPU and the power on the backup CPU should be off.

2. Select the appropriate COM port for the Control Builder M node (default COM 1).



No program capable of blocking the selected COM port must be running during the upgrade procedure.

3. Select:

Start > All Programs > ABB Industrial IT 800xA > Engineering > Utilities > IPConfig

4. In the IP Config dialog box (Figure 21), select:

Settings > Advanced mode

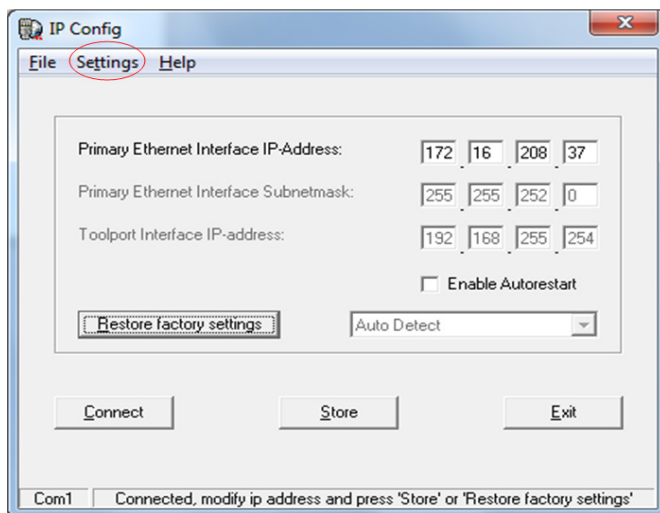


Figure 21. IPConfig Dialog Box

5. Click **Connect**.
6. Hold down the **Init/Reset** button on the controller for at least three seconds and wait up to one minute.
 - a. If the connection procedure passes, the current IP settings (the IP Ethernet address and its associated Subnet mask) will be displayed in the IP Config dialog box shown in Figure 21 (settings not shown in figure).
 - b. If the connection procedure fails, a time out message will appear. Check the cables and repeat the steps in this procedure up to this point. To connect to a redundant controller, refer to [Setting IP Addresses on Redundant CPUs](#) on page 85.



The **Enable Autostart** check box is normally cleared. Refer to the IPConfig Online Help for more information.

7. Enter a unique Primary Ethernet Interface IP Address and Subnet mask according to the **Acquiring Installation and Configuration Parameters** topic in *System 800xA Installation (3BSE034678*)*.

Example: IP address 172.16.0.201, Subnet mask, 255.255.252.0.

8. Click **Set IP** in the IPConfig dialog box to send the new address to the controller.
9. If using a redundant CPU, set the addresses as described in [Setting IP Addresses on Redundant CPUs](#).
10. Restart the controller with the **Init/Reset** button.

Setting IP Addresses on Redundant CPUs

For an AC 800M Controller with redundant CPUs (e.g. PM861) four Ethernet IP addresses need to be entered:

- Primary Ethernet port on the Primary CPU.
- Secondary Ethernet port on the Primary CPU.
- Primary Ethernet port on the Backup CPU.
- Secondary Ethernet port on the Backup CPU.

These four addresses must be known by both the primary and backup CPU; however, it is only necessary to set the IP addresses in the primary CPU. The backup CPU will automatically be configured by the primary.

When connecting with IPConfig in [Step 5](#) under [Setting IP Address for AC 800M Controllers](#) on page 83, first power off the backup CPU and connect the serial line to the primary, and connect the RCU link.

To set the two backup IP addresses with IPConfig:

1. Make sure that the Primary Ethernet Interface IP address is correct (as set in [Step 7](#) under [Setting IP Address for AC 800M Controllers](#) on page 83).

2. Select

Settings > Set Backup IP Addresses

3. Select:

Ethernet 1

4. Select the **Obtain an IP address by using default rule** check box.
5. Click **Store Interface Settings**.
6. Click **OK** when the dialog box appears stating:
`This will update the IP settings for the Backup CPU's Ethernet interface 1. Continue?`
7. Click **OK** when the dialog box appears stating:
`Backup CPU's Ethernet interface 1 stored successfully.`
8. Select **Ethernet 2**.
9. Select the **Obtain an IP address by using default rule** check box.
10. Click **Store Interface Settings**.
11. Click **OK** when the dialog box appears stating:
`This will update the IP settings for the Backup CPU's Ethernet interface 2. Continue?`
12. Click **OK** when the dialog box appears stating:
`Backup CPU's Ethernet interface 2 stored successfully.`

When powering up the backup CPU, its IP addresses will be assigned. All addresses except the one for the secondary Ethernet port on the Primary can be set with IPConfig. That address is set in the project created with the Control Builder M.

Verification

Before connecting an AC 800M Controller to a Control Network, its IP address can be checked by connecting to the controller again via the IPConfig tool.

Connect the network cable between CN1 on the controller CPU and the Control Network.

The controller IP address and connect status can be checked by opening a Command Prompt window on a node connected to the network, and entering:

ping <IP-address>

The controller should properly answer the ping command.

Downloading Controller or Communication Interface Firmware Using Ethernet

After the initial download of the controller firmware and setting of the IP address in the controller, further upgrades can be done via Ethernet (the Control Network). This also includes downloading or upgrading the firmware in communication interfaces connected to the controller (e.g. PROFIBUS DP - CI854).

The download is done via the Control Builder M running on a node connected to the same Ethernet network as the controller. Firmware can only be upgraded when the controller has no application program.

Download procedure:

1. In Control Builder M, open a project containing the controller. Alternatively, create a new AC 800M project and enter the correct system identity (IP address) for the controller.
2. Make sure the relevant libraries are connected under **Libraries > Hardware**, and also that they are connected to the controller.
3. Select **Show Remote System** in the controller context menu.
4. Select **Show Firmware Information**.
5. Evaluate the information for the current firmware in the controller CPU and other units. Firmware available in libraries is presented in the combo boxes.



Update each controller in a redundant pair individually (power up one and power down the other).

6. Choose the new alternative (or the same) firmware for each unit and select the corresponding **Download** check box to the right.
7. Click **Download Firmware for selected units** to start downloading.
8. The new firmware is downloaded after the old version has been removed from the controller CPU. When the upgrade is complete, the controller restarts automatically. During this sequence it is not possible to communicate with the controller.
9. To verify, confirm that the upgrade is complete by testing the firmware, or by reading the controller system log. If the upgrade program in the controller

detects any errors while performing the upgrade, they are written to the controller system log.

OPC Server Configuration

It is important to plan the OPC Server configuration before performing the OPC Server configuration procedures.

Configuration Planning

The OPC Server must be configured to specify which controllers will provide the OPC Data Access Server and the OPC Alarm and Event Server with data, and make other settings necessary for the operation of the OPC Server. The OPC Server is set up via an OPC Server Configuration panel.

When connected, the OPC Server has access to all relevant data in the controllers. The panel has two controller specification tabs, one for data access and one for alarms and events.

- **OPC Server Data Access tab:** Add IP address and connect all controllers that the OPC Data Access Server must provide data from/to.
- **OPC Server Alarm and Event tab:** The OPC Alarm and Event Server gets data from controllers via subscription. The subscription is made by using the controller IP address. When the Alarm and Event subscription is added to a controller, the address of the OPC Server will be stored in the controller. All event notifications from the controller will be transferred to the OPC Server.

There are a number of alternatives: in the OPC Server Panel Settings menu:

- **Autoload Configuration setting:** The configuration settings are saved in a file. Automatic load (autoload) can be enabled or disabled when the OPC Server starts up using the **Enable Autoload Configuration** check box. A cleared check box is the default.
- **Time Synchronization setting:** The time synchronization setting is disabled by default. Do not change the default setting in an 800xA System.



Do not enable the time synchronization setting in an 800xA System. Enabling the time synchronization setting will cause the OPC Server to time synchronize all connected controllers at a certain interval.

- **Update Rate setting:** The cache update rate, set in milliseconds, controls how often the OPC Data Access Server updates its internal cache with data from a certain controller. To distinguish between fast and slow update rates there are five categories for simple values (integer, real, bool) and a separate category for strings.



When the OPC Server is started, the values are set to their defaults. The rule to adhere to is that the OPC Server must fetch the data twice as fast as the clients request it.

- **Max. Number of Alarms:** This setting can be found under AE Settings (Figure 22). To access AE Settings, select:

Settings > AE Settings

Figure 22. AE Settings

The OPC Server contains a list of all alarms that are not idle in the connected controllers. The **Max. Number of Alarms** system variable defines the maximum number of alarms in the list. If there is an overflow, the latest alarm

is deleted and a system simple event is generated to announce the overflow. The list must be filled with less than 90 percent of the **Max. Number of Alarms** value before a new system simple event can be generated. The range of values for **Max. Number of Alarms** is **100 to 10,000**. The default value is **5,000**.

- **Client Queue Size:** This setting can be found under:

Settings > AE Settings

Every OPC Alarm and Event client holds a queue in this gateway to buffer event notifications. This number specifies the maximum number of items in every queue. Each queue has the same limitations. The range of values is 1,500 to 5,000. The default value is **2,000**.

- **Other AE Settings:** Refer to the OPC Server Online Help for more information.

The **Tools > Save cold retain values...** menu in the OPC Server Panel displays the dialog box for setting save cold retain values using the OPC Server. Cold retain values are values from control applications needed at a cold restart of a controller. Saving via the OPC Server can be done manually or periodically.

The **Save cold retain values** option is only available if the data access view is active and a controller is successfully connected. Refer to [Saving Cold Retain Values](#) on page 93.

Additional Parameters

If changes are required to the OPC Server default settings as described in [Configuration Planning](#) on page 88:

1. Open the Configuration dialog box (normally on the Connectivity Servers).
Select:
Start > All Programs > ABB Industrial IT 800xA > Control and I/O > OPC Server for AC 800M 5.1 > OPC Server for AC 800M 5.1
2. Select **Settings** and select the menu item to change.
3. Make the desired changes.
4. Click **File > Save Configuration...**

5. Select the file name of the OPC Server configuration, and save the file.
6. If additional parameters require changes:
 - a. Run the Setup Wizard (on the Engineering Station). Select:
Start > All Programs > ABB Industrial IT 800xA > Control and I/O > OPC Server for AC 800M 5.1 > SetupWizard

Enter the required configuration parameters under **Product**.



If the Service Account (800xA Service User as entered in the System Software User Settings dialog box) has not been specified, do this now. To get the Service Account information, launch the Configuration Wizard:

Start > All Programs > ABB Industrial IT 800xA > System > Configuration Wizard, then select the **System Software User Settings** dialog box.

Connecting to Controllers

To connect to controllers:

1. Open the configuration dialog box (on Connectivity Servers and other nodes where the OPC Server is installed). Select:
Start > All Programs > ABB Industrial IT 800xA > Control and I/O > OPC Server for AC 800M 5.1 > OPC Server for AC 800M 5.1
2. Select the **Data Access** tab.
3. Select:
View > Available Controllers

4. Drag the IP address of the requested controllers to the Controller Identity field in the OPC Server Configuration dialog box (clear old contents first) and click **Connect**. Refer to [Figure 23](#).

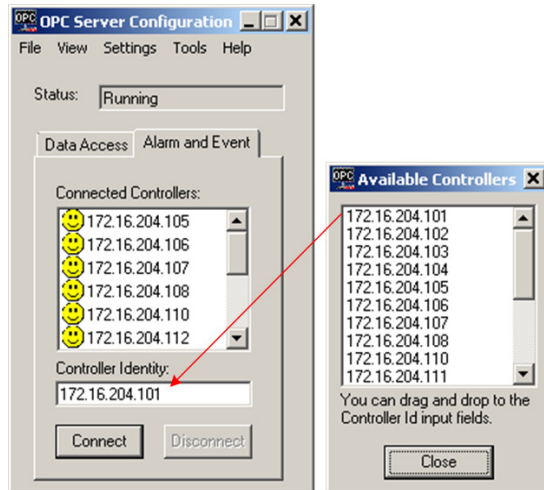


Figure 23. Connect to Controllers

5. Repeat for the Alarm and Event Server (the **Alarm and Event** tab in the OPC Server Configuration dialog box).
6. If the OPC Server asks to browse needed files when trying to connect, select **NO**.



If CNCP or SNTP is used on the Control Network, the MMS Time Synchronization from the OPC Server must be disabled.

7. Select:

Settings > Time Synchronization

8. The Time Synchronization dialog box appears. Deselect **Enable** and click **OK**.
9. Click **File > Save Configuration....**
10. Enter a name for the configuration file and save the file.

11. Select:
Settings > Autoload Configuration
to open the Autoload Configuration dialog box.
12. Select the **Enable Autoload Configuration** check box.
13. Enter the name of the configuration file saved in [Step 10](#).
14. Click **Apply** and **Close**.
15. Click **File > Save Configuration...**
16. Select the file name chosen in [Step 10](#), and save the file.

Saving Cold Retain Values

The OPC Server for AC 800M can periodically save the Cold Retain values of the controllers. It will transfer them from the controllers and save the values into the Aspect Directory. This is configured in the OPC Server.

1. Open the configuration dialog box (normally on one of the Connectivity Servers). Select:
Start > All Programs > ABB Industrial IT 800xA > Control and I/O > OPC Server for AC 800M 5.1 > OPC Server for AC 800M 5.1
2. Select the **Data Access** tab.
3. Select:
Tools > Save cold retain values
4. Select the **Automatically** check box.

5. The Save Cold Retain Values dialog box appears as shown in [Figure 24](#). Enter a suitable period time.

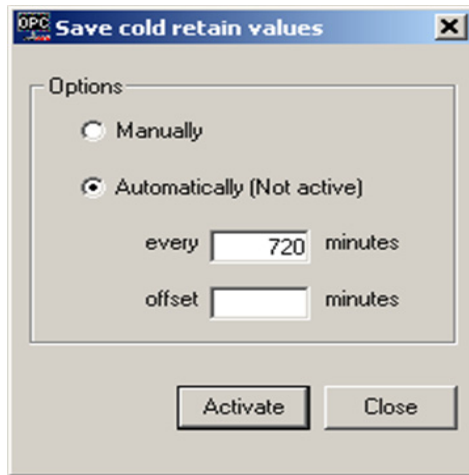


Figure 24. Save Cold Retain Values Dialog Box

6. To start the saving of Cold Retain values, click **Activate** in the Save Cold Retain Values dialog box. This can also be done at a later time. Click **Close**.
7. Click **File > Save Configuration....**
8. Select the file name of the OPC Server configuration, and save the file.

Configuring OPC Data Access Connections

An OPC Data Access connection can be located, established, and verified with the OPC Connector in the Connectivity Server.

1. Open a Plant Explorer workplace on the Connectivity Server.
2. Use the Structure Selector to open the **Control Structure**.
3. Create a Control Network object under the root object:
 - a. Select the root object.
 - b. Right-click and choose **New Object** from the context menu.

- c. The New Object dialog box appears. Select **Control Network** and click **Create**.
4. Select **OPC Data Source Definition** for the **Control Network** object in the **Aspect List Area**.
5. Select the **Connectivity** tab in the **Preview Area** as shown in [Figure 25](#).

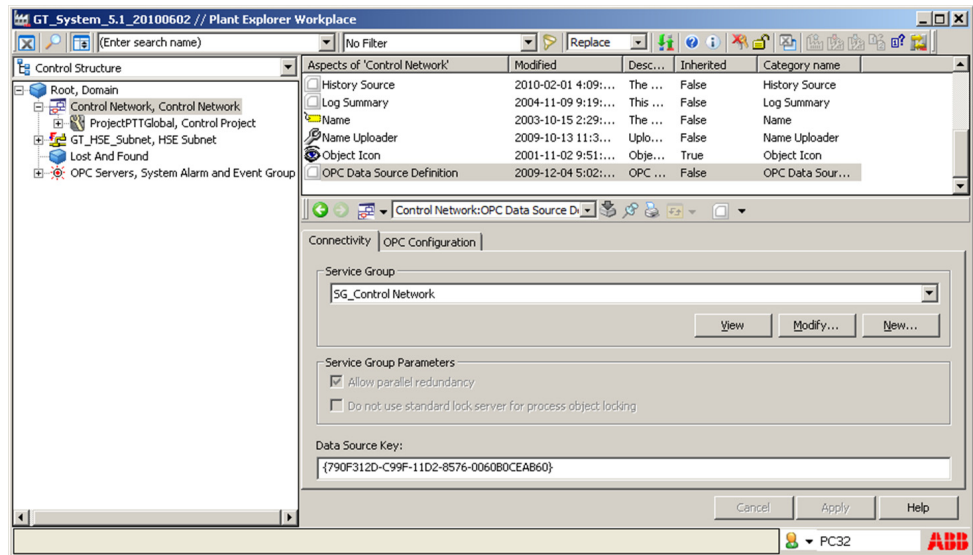


Figure 25. Data Source Definition Aspect

6. Click **New**. The New Service Group dialog box appears.
7. Click **Add**. The Add Service Provider dialog box appears.
8. Select the node name of the Connectivity Server as the OPC Server Provider and click **OK**.
9. Repeat [Step 7](#) and [Step 8](#) for an optional redundant Connectivity Server.
10. Click **OK** in the New Service Group dialog box.
11. Click **Apply** in the Data Source Definition aspect.

Configuring OPC Data Access Redundancy

After a redundant Connectivity Server has been added, OPC Data Access redundancy must be manually configured. The Data Source Definition aspects (OPC Data, Adapter Data, and Generic Data) that point to Service Groups that run on the redundant Connectivity Server must be configured. If several Data Source Definition aspects point to the same Service Group, it is sufficient to add redundant providers for one of them.

1. Go to the Data Source Definition aspect as shown in [Figure 25](#).
2. Select the **Connectivity** tab in the aspect config view of the aspect.
3. Click **Modify**. The Modify Service Group dialog box appears.
4. Click **Add**. The Add Service Provider dialog box appears.
5. Select the node name of the redundant Connectivity Server and click **OK**.
6. Click **OK** in the Modify Service Group dialog box.
7. Click **Apply** in the Data Source Definition aspect.

Configuring the OPC Server for Alarm and Event Collection

In order for alarms and events to propagate to the 800xA System, the Event Collector Service must be configured on the AC 800M OPC Server node.

Set up this collector connection as follows:

1. Make sure that the OPC Server is running with the controllers connected and configured.
2. Open a Plant Explorer Workplace.
3. Use the Structure Selector to select the **Service Structure**.
4. Use the Object Browser to navigate to:
`Services > EventCollector, Service`
5. Create the Service Group and Service Provider objects in [Step 6](#) through [Step 14](#), if they do not already exist.
6. Right-click on `EventCollector, Service` and select **New Object** from the context menu.

7. The New Object dialog box appears. Select **Service Group** and enter a name, such as **AC800SG_x** (where **x** is a running number) and click **Create**.
8. Right-click on the newly created Service Group object and select **New Object** from the context menu.
9. The New Object dialog box appears. Select **Service Provider** and enter a name, such as **AC800SP_nodename** (where **nodename** is a Connectivity Server name) and click **Create**.
10. Select the Service Provider Definition aspect for the AC800SP_nodename Service Provider object in the Aspect List Area.
11. Select the **Configuration** tab in the Preview Area as shown in [Figure 26](#).

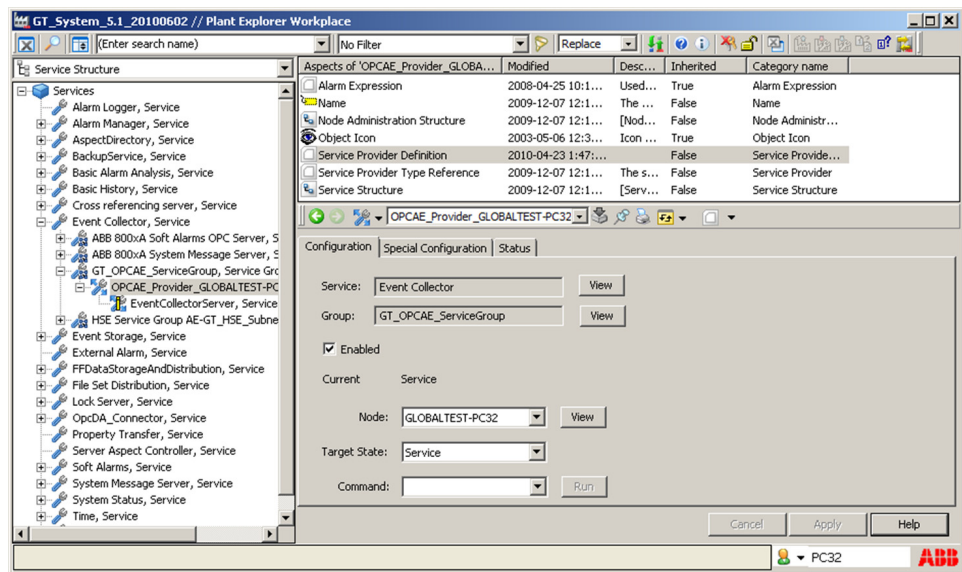


Figure 26. Node Settings for the Event Collector Service Provider

12. Select the name of the AC 800M Connectivity Server in the **Node** drop-down list box.
13. Click **Apply**.
14. Repeat [Step 8](#) through [Step 13](#) for a redundant Connectivity Server.

15. Use the Object Browser to navigate to the Event Collector Service Group previously created.
16. Select the Service Group Definition aspect in the Aspect List Area.
17. Select the **Special Configuration** tab in the Preview Area.
18. Select **OPC AE Server for AC 800M** in the **Alarm Server** drop-down list box.
19. Click **Apply**.
20. Verify that **OPC AE Server for AC 800M** is set in the **Collection Definition** drop-down list box.



Additional settings can be made from the Alarm Manager object in the **Service Structure**.

21. Verify the connection by checking the status.
 - a. Click on the **Status** tab on the Event Collector object.
 - b. Verify that the state is *Service*, as shown in [Figure 27](#).

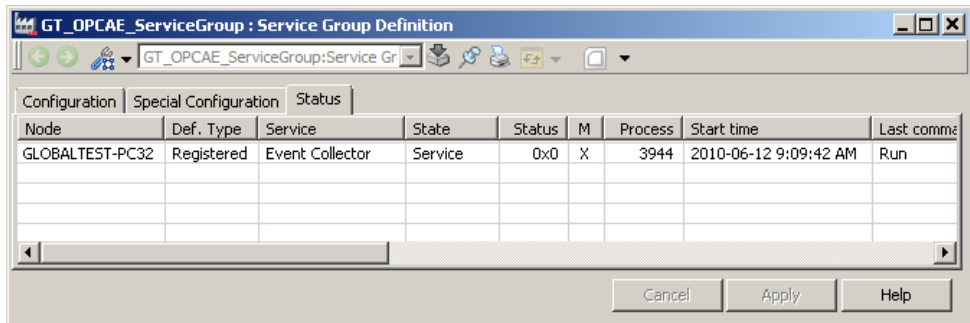


Figure 27. Verify the Connection

Verifying the OPC Server Configuration

Refer to [Figure 23](#) and verify that the OPC Server is running, and its connection status for the controllers can be viewed in the OPC Server panel.

If the connection to controllers has been done in the OPC Server, and there is a valid control application downloaded to one or more of the controllers, the OPC Server will start transferring values and events from the controllers to any OPC client requesting such values. OPC clients are, for example, the Operator Workplace displays and Event Lists. The statistics of the current OPC Server traffic can be viewed as follows:

1. Open the configuration dialog box (normally on the Connectivity Servers).
Select:

Start > All Programs > ABB Industrial IT 800xA > Control and I/O > OPC Server for AC 800M 5.1 > OPC Server for AC 800M 5.1

2. To open the OPC Statistics - Data Access dialog box shown in [Figure 28](#), select:

Tools > Display OPC statistics > Data Access

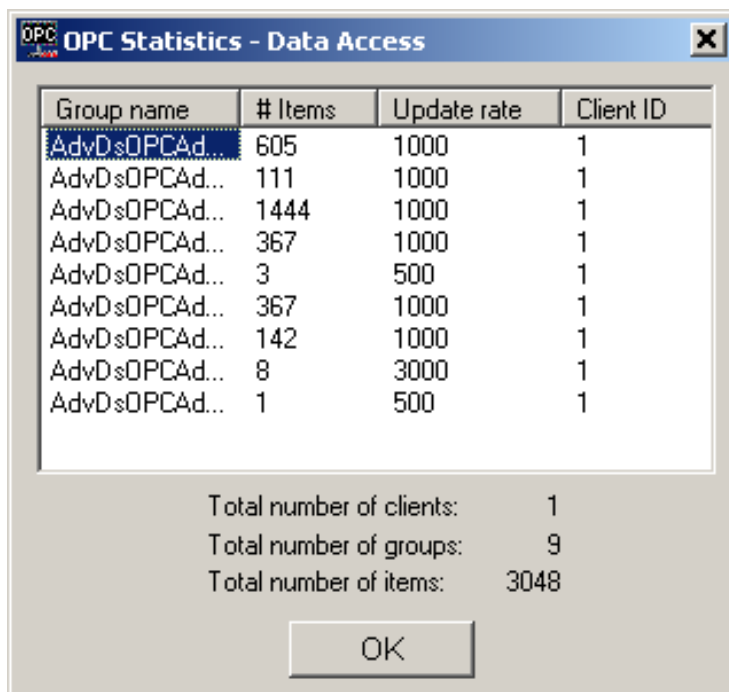


Figure 28. View OPC Server Statistics

Section 8 800xA for Advant Master

Introduction

This section describes post installation procedures for 800xA for Advant Master. Refer to *800xA for Advant Master Configuration (3BSE030340*)* for more information on configuration issues.

Connectivity Server Configuration

To communicate with Advant Controller 400 Series (with Master software) on MasterBus 300, each 800xA for Advant Master Connectivity Server is equipped with a hardware device called a Real Time Accelerator (RTA). Two different types of RTA can be used:

- **PU410:** An external unit connected to Connectivity Server via TCP/IP.
- **PU515A:** An internal board with PCI connection.

The following configuration steps are identical for both RTA types.

Configuring the Connectivity Server consists of the following steps:

1. [Assigning MB300 Network and RTA Board Objects to the Control Structure.](#)
2. [RTA Board Network Settings.](#)
3. [Verifying the RTA Board Network Settings.](#)



The Application Engineer or System Engineer must be a member of the Administrators group to be able to perform the configurations.



Alarms that are received from the controllers before an upload is performed will be created as objects in Lost and Found in the **Control Structure**. To minimize the risk of this happening, it is recommended to not connect the Connectivity Server to the MB300 Network until an upload is performed.

Assigning MB300 Network and RTA Board Objects to the Control Structure

Perform the following steps. This will also create and configure the necessary objects in the **Service Structure**. The default settings for these objects should generally not be modified.

1. Start the Configuration Wizard on the Aspect Server. Select:
Start > All Programs > ABB Industrial IT 800xA > System > Configuration Wizard
2. The Select Type of Configuration dialog box appears. Select **System Administration** and click **Next**.
3. The Select System dialog box appears. Select the system and click **Next**.
4. The Select Type of Configuration for System dialog box appears. Select **Add RTA** and click **Next**.
5. The Add RTA dialog box shown in [Figure 29](#) appears. Select the primary network number from the **Network** drop-down list box, or enter it manually.
6. Select the server node from the **Server node** drop-down list box and click **Next**.

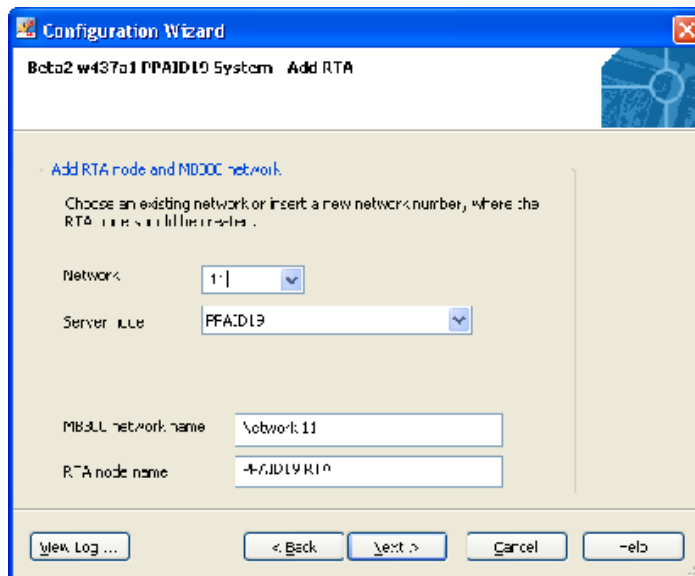


Figure 29. Add RTA Dialog Box

7. When the Apply Settings dialog box appears, click **Apply**.
8. Repeat the procedure for all 800xA for Advant Master Connectivity Servers (i.e. the redundant servers), except in [Step 5](#), and select the same network number as entered for the Primary Connectivity Server in the **Network** drop-down list box.

RTA Board Network Settings

To configure the RTA Board network settings:

1. Start the Configuration Wizard on the Aspect Server. Select:
Start > All Programs > ABB Industrial IT 800xA > System > Configuration Wizard
2. The Select Type of Configuration dialog box appears. Select **System Administration** and click **Next**.
3. The Select System dialog box appears. Select the system and click **Next**.
4. The Select Type of Configuration for System dialog box appears. Select **MB300 RTA Settings** and click **Next**.
5. The MB300 RTA Network Settings dialog box shown in [Figure 30](#) appears. Select the name of the 800xA for Advant Master Connectivity Server in the **AC 400 Server** drop-down list box.
6. Fill in the appropriate values in the Network Number 1, Network Number 2, and Node Number fields and click **Next**.
7. When the Apply Settings dialog box appears, click **Apply**.

- 8. Repeat the procedure for all 800xA for Advant Master Connectivity Servers.

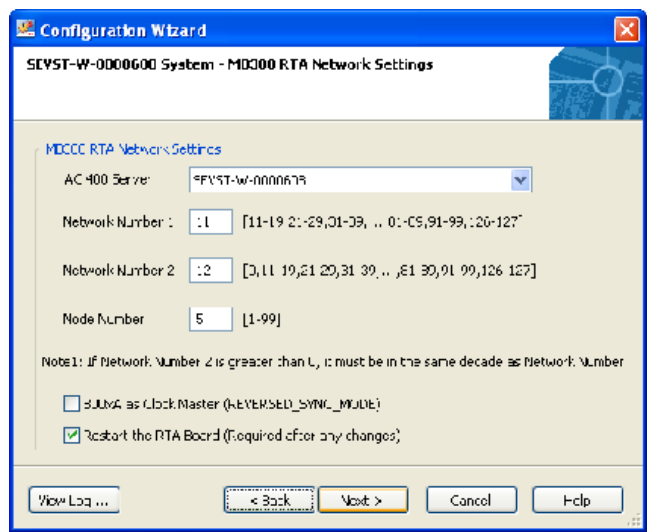


Figure 30. MB300 RTA Network Settings Dialog Box

Verifying the RTA Board Network Settings

Verify that the RTA Boards are running by inspecting the RTA Board Control aspect on the MB300 RTA Board objects in the **Control Structure** as shown in [Figure 31](#).

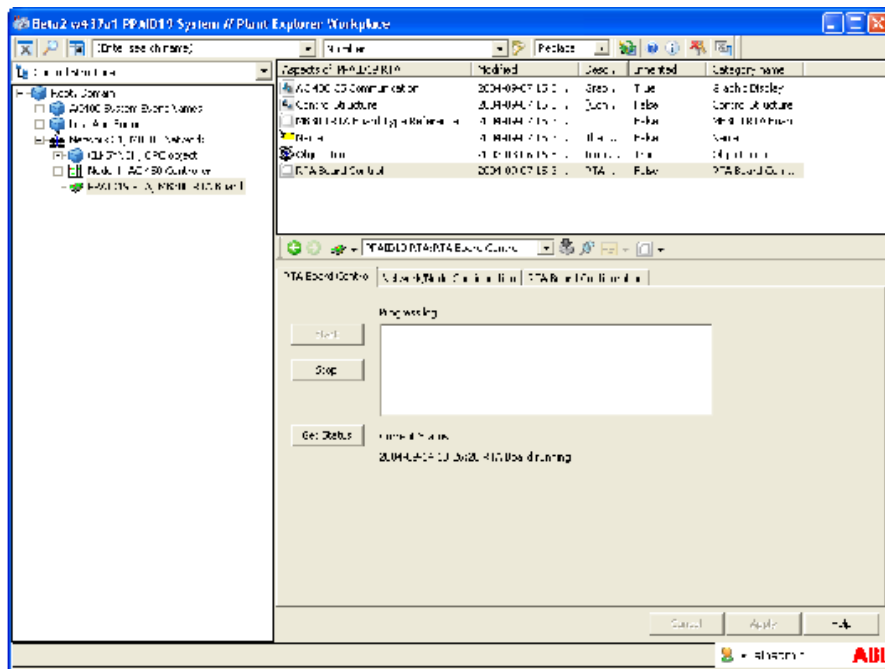


Figure 31. Verifying the RTA Board Status

Entering License Information for Connected Controllers

All controllers, such as MasterPiece 200/1, Advant Controller 410, Advant Controller 450, Advant Controller 450RMC, and Safeguard 410, connected to the 800xA System should be documented in the Advant Master Controller Licenses.txt file.

The Licenses .txt (Figure 32) file can be opened using Notepad and is found in the following directory on the Primary Aspect Server after installation of 800xA for Advant Master:

```
<Installation path>\ABB Industrial IT\Operate IT\  
AC 400 Connect\Licenses\Advant Master Controller  
Licenses.txt
```

The installation path is typically C:\Program Files.

Enter License information, network, and node numbers, and the Product being used in the respective column. Repeat this for all Controllers being connected to the 800xA System.

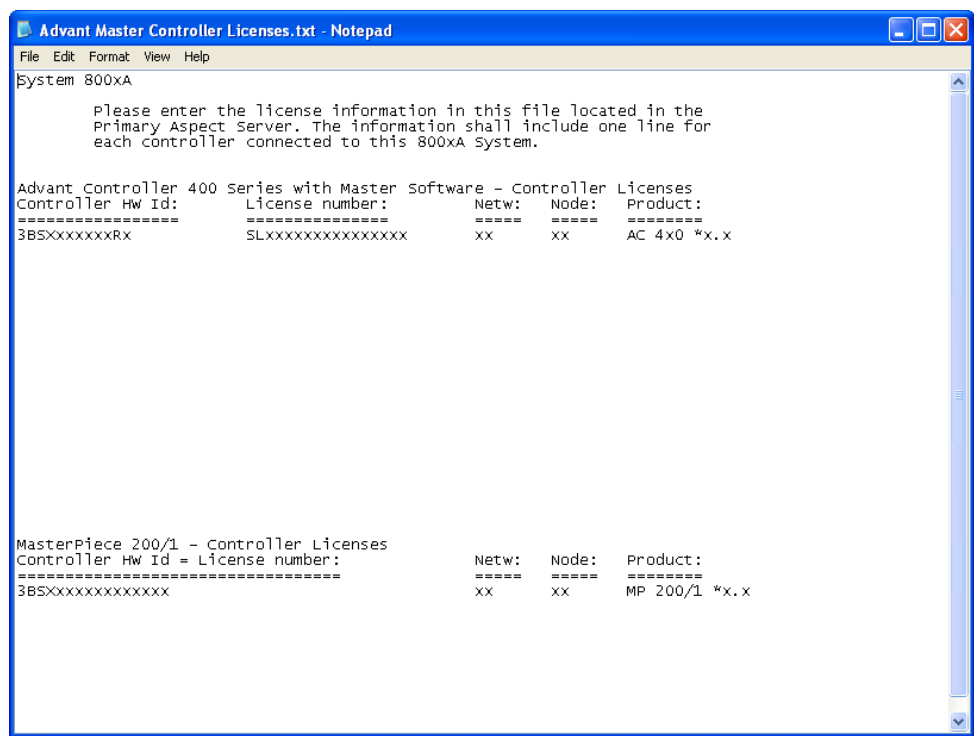


Figure 32. Advant Master Controller Licenses Text File

Section 9 800xA for Harmony

Introduction

This section describes post installation procedures for 800xA for Harmony.

Harmony Executive Service Provider Setup

Perform the following procedure on every Harmony Connectivity Server, Harmony Configuration Server, and Harmony Configuration Server with Connectivity Server node in the 800xA System.

1. Use the Structure Selector to open the **Service Structure**.
2. Use the Object Browser to navigate to and select:
`Services > Harmony Executive, Service > Basic, Service Group`
3. Select `Service Group Definition` in the Aspect List Area.
4. Select the **Configuration** tab in the Preview Area (if not already selected).
5. Click **Add** to open the New Service Provider Name dialog box.
6. Enter the Service Provider name, such as `HarmonyExecutive_XXXX` (where `XXXX` is the node name of the current node).
7. Click **OK** to accept the addition and close the New Service Provider Name dialog box.
8. Use the Object Browser to select the newly created Harmony Executive Service Provider.
9. Select `Service Provider Definition` in the Aspect List Area.

10. Select the current node from the **Node** drop-down list box in the Preview Area and click **Apply**.
11. Repeat the procedure on every Harmony Connectivity Server, Harmony Configuration Server, and Harmony Configuration Server with Connectivity Server node in the 800xA System.

Configure Access Rights



If the Client Setup Type was installed, there is no need to configure access rights.

All Industrial IT users require read access to the Configuration Server and SQL Server databases for 800xA for Harmony. To configure access rights for read access, perform the following steps on all 800xA for Harmony Configuration and Connectivity servers:

1. Open the SQL Server Enterprise Manager. Select:
Start > Programs > Microsoft SQL Server 2008 > SQL Server Management Studio
2. Select the *node_name*\HARMONY_INSTANCE in the Server Name field and click **Connect**.
3. Expand the listing to the view the following directory (Figure 33):
Security\Logins
4. Right-click **Logins** and select **New Login** from the context menu.
5. Click **Search** next to the Login Name field on the General page.
6. Click **Object Types** in the Select User Group window.
7. Select the **Groups** option in the Object Types dialog box and click **OK**.
8. Ensure the domain or Workgroup name is displayed in the From This Location field and click **Advanced**.
9. Click **Find Now**.



Log into the Administrator account if prompted to do so.

10. From the search results, select **IndustrialITUser** and click **OK**, and **OK** again.

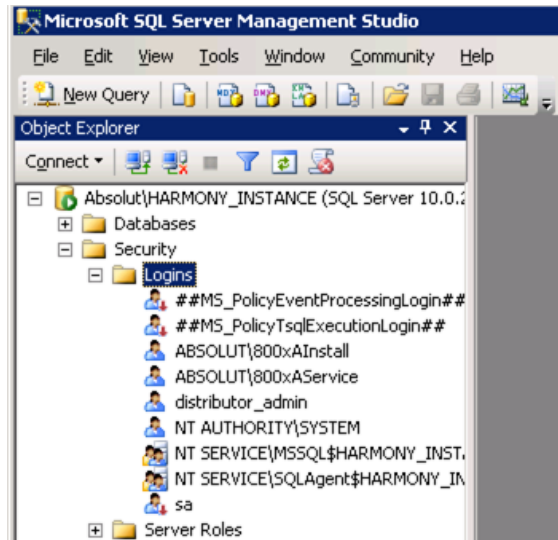


Figure 33. SQL Server Management Suite

11. Select the **Windows Authentication** option.
12. Select **ConfigServer** in the Default Database field.
13. Select the **Map** check box for the ConfigServer database on the User Mapping page.
14. Select the **db_datareader** check box in the Database Role Membership for: ConfigServer area.
15. Select the **Grant** option for the Permission to connect to database engine setting on the Status page.
16. Select the **Enabled** option for the Login setting and click **OK**.

OPC Server Network Object Setup

Create the OPC Server Network object on each Primary Harmony Connectivity Server, or Harmony Configuration Server with Connectivity Server node.

1. Open a Plant Explorer Workplace.
2. Use the Structure Selector to open the **Control Structure**.
3. Right-click on `Root, Domain`.
4. Select **New Object** from the context menu.
5. Select the **List Presentation** check box.
6. Select `Harmony OPC Server Network` from the list of objects.
7. Enter a name and click **Next**.
8. Click **Add**.
9. Select the node that contains the Connectivity Server and click **OK**.



Redundant Connectivity Server nodes are listed in addition to Primary Connectivity Server nodes. Select both Primary and Redundant Connectivity Server nodes.

10. In the Harmony OPC Server, ProgID field, select **ABBMaestroNT.OPCServer.1** from the drop-down list box.
11. Click **Create**. The new OPC Server Network object is created and appears under `Root, Domain` in the Control Structure.
12. Right-click on the new OPC Server Network object and select **NetConfig**.
13. Select the domain or workgroup name that the Configuration Server is located on from the **Configuration Server Domain Name** drop-down list box.
14. Select the Configuration Server node name from the **Configuration Server Machine Name** drop-down list box.
15. Select the Database name from the **Database Name** drop-down list box.

16. Select the Harmony Server tag name of the Primary Harmony Connectivity Server node from the **Tag Server Name** drop-down list box.



If a Redundant Connectivity Server node is present, verify that the Primary Harmony Server tag name is selected in the **Tag Server Name** drop-down list box.

17. Click **Apply**.

Alarm and Event Service Provider Setup

Create the Alarm and Event Service Provider on a Connectivity Server node.

1. Use the Structure Selector to select the **Service Structure**.
2. Select:
`Services > Event Collector, Service`
3. If it does not already exist, create the Service Group object.
 - a. Right-click on `Event Collector, Service` and select **New Object** from the context menu.
 - b. Select **Service Group** and enter a name such as `Harmony_AE_SGx` (where *x* is a running number).
 - c. Click **Create**.
4. Right-click on the Service Group object and select **New Object**.
5. Select **Service Provider** and enter a name, such as `Harmony_AE_SP_nodename` (where *nodename* is the Connectivity Server name).
6. Click **Create**.
7. Select the Service Group Definition aspect for the `Harmony_AE_SP_nodename` object.
8. Select the name of the Connectivity Server in the drop-down list box in the **Configuration** tab, and click **Apply**.
9. Repeat [Step 4](#) through [Step 8](#) for redundant Connectivity Servers.
10. Select `Service Group Definition` in the Aspect List Area.

11. Select the **Special Configuration** tab in the Preview Area.
12. Select **Maestro/OPC Event Server [InProc]** from the **Alarm Server** drop-down list box.
13. Select **Harmony AE Server** from the **Collection Definition** drop-down list box.
14. Select **Tracking Source Object Interceptor** from the **Object Handler** drop-down list box and click **Apply**.
15. Use the Object Browser to navigate to:
`Services > Alarm Manager, Basic, Service Group`
16. Select the **Special Configuration** tab in the Preview Area.
17. Clear the **Make new alarm entry each time a condition gets active** check box and click **Apply**.



Clearing the **Make new alarm entry each time a condition gets active** is a system wide setting. This is only a recommendation for 800xA for Harmony. It may conflict with other applications.

Import the Harmony Configuration

The following scenarios cover importing the Harmony configuration. Perform the one that applies to the system.

- [New Installations.](#)
- [Reloading when a Backup Exists.](#)
- [Reloading when a Backup does not Exist.](#)

New Installations

Use the tag importer utility to import the Harmony Configuration by performing the following steps:

1. Select the following on the Configuration Server node, or Configuration Server with Connectivity Server node:

**Start > All Programs > ABB Industrial IT 800xA >
800xA for OCS Systems > Harmony > Configuration >
Tag Importer Exporter**

2. Select **Import Existing Configuration Data**.
3. Select the appropriate import options and click **Next** to continue.



Refer to *800xA for Harmony Configuration (3BUA000157*)* for more information.

4. Select the file to be imported and click **Next** to continue.

Reloading when a Backup Exists

If the Harmony tag objects already exist in the Aspect Directory (due to a reload of the Harmony Configuration Server node), and a backup exists, perform the following steps:

1. On the Configuration Server node or Configuration Server with Connectivity Server node select:

**Start > All Programs > ABB Industrial IT 800xA >
800xA for OCS Systems > Harmony > Configuration >
Restore Configuration**


2. Click **Connect**.
3. Choose the backup file name to restore.
4. Click **Restore**.

Reloading when a Backup does not Exist

If the Harmony tag objects already exist in the Aspect Directory (due to a reload of the Harmony Configuration Server node), and a backup does not exist, perform the following steps.

1. Open a Plant Explorer Workplace.
2. Use the Structure Selector to select the **Control Structure**.
3. Use the Object Browser to select the OPC Server Network object.
4. Select the Harmony Synchronizer aspect in the Aspect List Area.

5. In the Preview Area:
 - a. Clear all **Import from Configuration Server** options.
 - b. Select all **Export to Configuration Server** options.
 - c. Select the **Advanced** tab.
 - d. Select the **Export** option under **Disconnected Tag Options**.
 - e. Select the **General** tab and select **Synchronize**.
 6. On the Configuration Server node or Configuration Server with Connectivity Server node select:

**Start > All Programs > ABB Industrial IT 800xA >
800xA for OCS Systems > Harmony > Configuration >
Tag Importer Exporter**
 7. Select **Import Existing Configuration Data**.
 8. Select the appropriate import options and click **Next** to continue.
-  Refer to *800xA for Harmony Configuration (3BUA000157*)* for more information.
9. Select the file to be imported and click **Next** to continue.

Synchronize the Aspect Directory

Synchronize the Aspect Directory with the Harmony Configuration Server using the Harmony Synchronizer aspect (if it has not been performed in previous procedures).

1. Open a Plant Explorer Workplace.
2. Use the Structure Selector to select the **Control Structure**.
3. Use the Object Browser to select the OPC Server Network object.
4. Select the Harmony Synchronizer aspect in the Aspect List Area.
5. Select **Synchronize**.



Refer to *800xA for Harmony Configuration (3BUA000157*)* for more information.

Harmony Communication Configuration

ICI Device Configuration

Run the ABB Harmony System Configuration utility on each Harmony Connectivity Server node.

1. Double-click the shortcut on the desktop created during installation.
2. Click **Help** to view the configuration guide provided with the HarmonyAPI.

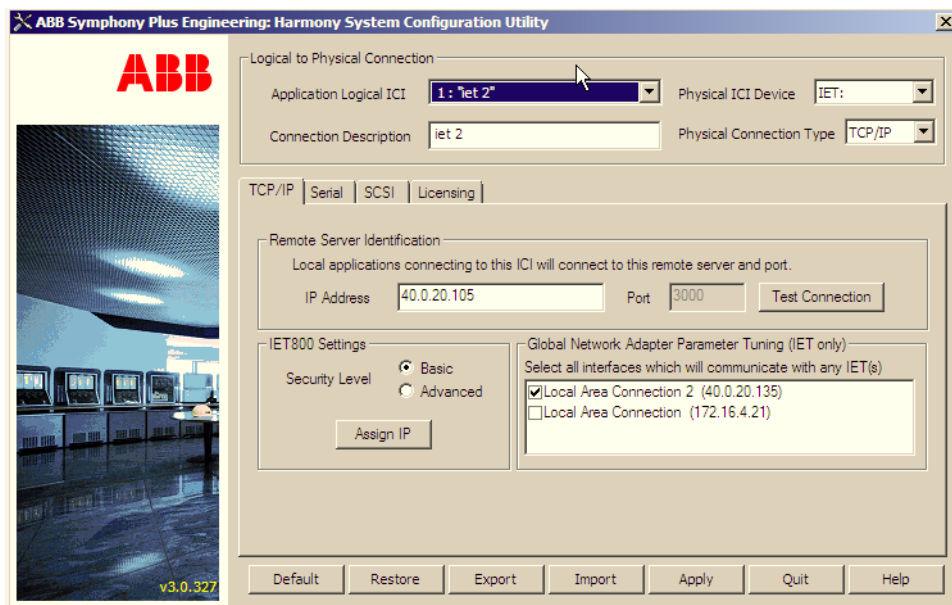


Figure 34. hAPI Application Logical ICI Definition Dialog Box

3. Select:

Start > Run

from the Windows Taskbar.

4. Enter:

```
... \Program Files\ABB Symphony
Plus\Engineering\HarmonyAPI\EXE\DeviceAsServiceU.exe '
-i dd_XXXX
```

(where `XXXX` is `com1` or `com2` for serial ports, or `_s00y` for SCSI (where `y` is the SCSI address number)) in the Run dialog box and click **OK**.

5. Select:

Start > Control Panel > Administrative Tools > Services

6. Right-click the `dd_XXXX` service entered in [Step 4](#) and select **Properties** from the context menu.
7. Change the value in the **Startup type** drop-down list box under the **General** tab to **Automatic** and click **OK**.



Refer to the **NIC Time Synchronization** section of *800xA for Harmony Operation (3BUA00158*)* to select the Time Sync Network and its network priority.

8. Restart the node.

Replication Monitor Internet Explorer Security Settings

If using the Replication Monitor, the Internet Explorer Security Settings for the Local Intranet must be configured.

Perform this procedure on all 800xA for Harmony Connectivity, Configuration, and Configuration with Connectivity Server nodes.

1. Launch Internet Explorer.

2. Select:

Tools > Internet Options

to launch the Internet Options dialog box.

3. Select the **Security** tab.
4. Select `Local intranet` and click **Custom level...**
5. Scroll down to the `Access data sources across domains` entry under `Miscellaneous`.

6. Select **Enable**.
7. Click **OK** until all dialog boxes are closed.

Section 10 800xA for AC 870P/Melody

Introduction

This section describes post installation procedures for 800xA for AC 870P/Melody (this product was referred to as 800xA for Melody prior to 800xA 5.1).

For further post installation issues refer to Section 2, Base Configuration in *800xA for AC 870P/Melody Configuration (3BDD011741*)*.

Melody Executive Service Provider Setup

The Melody Executive Service is an 800xA System service that controls underlying 800xA for AC 870P/Melody services running on the Melody Configuration Server and Connectivity Servers (it starts and stops Config Server database replication and Melody OPC Servers). Once configured, it requires no further user interaction.



Log on once with the 800xA Service Account before configuring the Melody Executive Service Provider for a node.

1. Use the Structure Selector to open the **Service Structure**.
2. Use the Object Browser to navigate to and select:
`Services > Melody Executive, Service`
3. Right-click `Melody Executive, Service` and select **New Object** from the context menu.
4. Select **Service Group** and enter a name such as **Basic**.



Perform the remainder of this procedure on every Melody Connectivity Server and Melody Configuration Server node in the 800xA System.

5. Use the Object Browser to select the newly created Service Group.
6. Select `Service Group Definition` in the Aspect List Area.

7. Select the **Configuration** tab in the Preview Area (if not already selected).
8. Click **Add** to open the New Service Provider Name dialog box.
9. Enter the Service Provider name, such as:
`MelodyExecutive_XXXX`
(where `XXXX` is the node name of the current node).
10. Click **OK** to accept the addition and close the New Service Provider Name dialog box.
11. Use the Object Browser to select the newly created Melody Executive Service Provider.
12. Select `Service Provider Definition` in the Aspect List Area.
13. Select the current node from the **Node** drop-down list box in the Preview Area and click **Apply**.
14. Repeat the procedure on every Melody Connectivity Server and Melody Configuration Server node in the 800xA System.

Section 11 800xA for MOD 300

Introduction

This section provides post installation procedures for 800xA for MOD 300.

Setting Up Time Synchronization

Perform the following to set up time synchronization:

- [800xA System is Master Timekeeper](#) on page 121.
- [MOD 300 System is Master Timekeeper](#) on page 122.
- [Time Synchronization on the Service Provider Definition Aspect](#) on page 124.

800xA System is Master Timekeeper

When the 800xA System is the master timekeeper, follow the instructions for setting up time on the 800xA System and then set the 800xA for MOD 300 Connectivity Server so reverse time synchronization is enabled. This will allow Windows clock to set the Real-Time Accelerator (RTA) clock and give the RTA the ability to update the MOD 300 system if it is made the master timekeeper (refer to the *Advant Station 500 Series with Advacommand / Advabuild User Guide* for additional information).



Be extremely careful when making changes in the registry. Do not make any changes in the registry without first making a backup copy of the registry. Refer to the online help for the registry editor on how to create a backup.

Set the following:

- Enable Reverse Time Synchronization: **REVERSED_SYNC_MODE = 1**

Registry Location:

HKEY_LOCAL_MACHINE\Software\ABB\SystemServices\DxBASE\dxTimeSync

MOD 300 System is Master Timekeeper

Time Synchronization on the Windows side of a Connectivity Server node can be set so Reverse Time Synchronization (RTS) is disabled. This allows the host Connectivity Server to constantly be updated by the RTA clock which gets its time from the MOD 300 System Master Timekeeper over the Distributed Communications Network (DCN). The host node then broadcasts this time to the other MOD 300 nodes on the 800xA System as well as the domain controller.

MOD 300 Connectivity Servers, Clients, and the associated Domain Controller all need to be set up to handle getting time from the MOD 300 system through the RTA on the Connectivity Servers.

Time Synchronization on the MOD 300 Connectivity Server

Reverse time synchronization is disabled on these nodes to allow the MOD 300 system to update the RTA clock on the Connectivity Server. In addition, these servers act as a Simple Network Time Protocol (SNTP) server for the Domain Controller.



Be extremely careful when making changes in the registry. Do not make any changes in the registry without first making a backup copy of the registry. Refer to the online help for the registry editor on how to create a backup.

Set the following:

- Disable Reverse Time Synchronization: **REVERSED_SYNC_MODE = 0**

Registry Location:

HKEY_LOCAL_MACHINE\Software\ABB\SystemServices\DxBASE\dxTimeSync

- SNTP Registry parameter NtpServer = time.windows.com,0x1

Registry Location:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters

- Set the **Windows Time** (W32Time) in the Services window via:
Start > Control Panel > Administrative Tools > Services
as follows:
 - **Startup Type** is Automatic.
 - **Status** is Started.
- Set the SNTP to fetch the time from itself. From the command prompt enter:

```
net time /setsntp:a.b.c.d
```

where *a.b.c.d* is the IP address of the Connectivity Server itself.

Time Synchronization on the Domain Controller

The Connectivity Servers act as a SNTP server for the Domain Controller that then distributes time to all nodes in the domain. This is handled with the default settings for W32Time.

Set the following:

- Set the **Windows Time** (W32Time) in the Services window as follows:
 - **Startup Type** is Automatic.
 - **Status** is Started.
- SNTP Registry parameter:



Be extremely careful when making changes in the registry. Do not make any changes in the registry without first making a backup copy of the registry. Refer to the online help for the registry editor on how to create a backup.

NtpServer = time.windows.com,0x1

Registry Location:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
W32Time\Parameters

- SNTP Configuration, from the command prompt enter:
 - If there is a single time server:

```
net time /setsntp:a1.b1.c1.d1 a2.b2.c2.d2
```
 - If there are multiple time servers:

```
net time /setsntp:"a1.b1.c1.d1 a2.b2.c2.d2 "
```

where *a1.b1.c1.d1* and *a2.b2.c2.d2* are the IP addresses of the Connectivity Servers.

Time Synchronization on the MOD 300 Client

Client nodes get their time from the Domain Controller and are set up as SNTP clients.

Set the following:

- Set the **Windows Time** (W32Time) in the Services window as follows:
 - **Startup Type** is Disabled.
 - **Status** is Stopped.
- SNTP Registry parameter default:



Be extremely careful when making changes in the registry. Do not make any changes in the registry without first making a backup copy of the registry. Refer to the online help for the registry editor on how to create a backup.

NtpServer = time.windows.com,0x1

Registry Location:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
W32Time\Parameters

Time Synchronization on the Service Provider Definition Aspect

To complete time synchronization setup, the Service Provider Definition aspect must be set up as described in the Set Up System Structure section of *800xA for MOD 300 Configuration (3BUR002417*)*. At that time, set up the Service Provider Definition aspect (located in the **Service Structure** as part of the Time Service object) for client nodes by clearing the **Enabled** check box in the **Configuration** tab and applying. This function is selected by default and must be left selected on the Connectivity Servers.

Process Administration Supervision (PAS) Account and Communication Settings

After the node is restarted, set the PAS account and initialize the OMF settings to start system services. The PAS services will not start until the PAS account and communications settings are initialized as described in the following steps.

1. Use Administrative Tools in Windows Control Panel to select:

PAS > Process Administration

2. A dialog box will appear. Enter the Service Account and password used to install 800xA for MOD 300.
3. Close the Process Administration.
4. Select:

PAS > Settings

to open the Communications Configuration Tool.



The message:

Would you like to revert back to saved settings?

appears if settings were previously saved. To restore the previous settings, perform [Step a](#) through [Step d](#) as follows.

- a. Select **Yes** at the message

Would you like to revert back to saved settings?

This opens the Communication Settings dialog box.

- b. Select **OK** on the Communication Settings dialog box to save the settings and close the dialog box.

- c. Select **OK** at the message:

Settings have been saved . . .

- d. Proceed to [Step 10](#) and restart the node.

5. Configure the **Control Network** section. Select **MOD300** to connect this node to a MOD 300 DCN. The network address parameters are displayed in the Network Address frame.

6. Configure the Network Address section:



The DCN Address and the E-DCN Network Addresses (1 and 2) must be set to valid values whether connecting to the DCN or E-DCN.

The DCN Address is required for both DCN and E-DCN connections. This is the device number on the DCN. Set the DCN address to the same decimal value as the Physical Device number specified on the GENERICD object of the node in the ABB OCS database (refer to *800xA for MOD 300 Configuration (3BUR002417*)* for guidelines). Valid entries are 2 through 255 decimal that represent the hexadecimal address (1 is reserved for the MOD engineering station).



When connecting to the standard DCN, leave the E-DCN addresses at their default values.

For E-DCN connection, follow these guidelines to configure the E-DCN addresses:

- **E-DCN Network Address 1** must be set to match the E-DCN Network Address 1 value for all other nodes connecting to that media. E-DCN Network Address 1 must be an even number, for example **6**.
- **E-DCN Network Address 2** must be set to match the E-DCN Network Address 2 value for all other nodes connecting to that media. E-DCN Network Address 2 must be an odd number, for example **7**.

7. Set OMF Shared Memory Size to **32** MByte if not already set.
8. Select **OK** to apply the changes. There is no need to change the other settings (your displayed settings may be different and may show TCP/IP not checked for example).
9. Select **OK** at the informational message that the settings have been changed. A restart is always required if the Control Network Setting, OMF Memory, or TCP/IP enabled setting has been changed.
10. Restart the node.

Redundancy

Perform the following to set redundancy:

1. Set redundancy in the registry as follows:



Be extremely careful when making changes in the registry. Do not make any changes in the registry without first making a backup copy of the registry. Refer to the online help for the registry editor on how to create a backup.

Redundant Partner = *computer name of other connectivity server.*

Registry Location:

HKEY_LOCAL_MACHINE\Software\ABB\AdvOPCAEServer\config

- a. Enter the name of the redundant partner Connectivity Server if the two servers are redundant. Perform this step for both servers. Leave the setting blank if no redundancy is required.

2. The **Require Dual Acknowledge (both servers in a redundant pair get acknowledge requests)** check box is selected by default.

To verify the setting:

- a. Use the Object Browser to navigate to the following:
[Library Structure]:Alarm & Event\Alarm Connection Definitions\MOD300Alarms
- b. Select the Alarm Collection Definition aspect (the Main View shows by default).
- c. Switch to the Config View.
- d. Select the **Configuration** tab.
- e. Verify that the **Require Dual Acknowledge (both servers in a redundant pair get acknowledge requests)** check box is selected.
- f. Click **OK**.

3. Clear the **Make new alarm entry each time a condition gets active** check box:



Clearing the **Make new alarm entry each time a condition gets active** check box is a system wide setting. This is only a recommendation for 800xA for MOD 300. It may conflict with other applications.

- a. Use the Structure Selector to open the **Service Structure**.
- b. Use the Object Browser to navigate to:
Services > Alarm Manager, Basic, Service Group
 - a. Select the **Special Configuration** tab in the Preview Area.
 - a. Clear the **Make new alarm entry each time a condition gets active** check box and click **Apply**.

Setting Up the System Structure

Refer to the **Set Up System Structure** topic in **Section 2 - Administration of 800xA for MOD 300 Configuration (3BUR002417*)** to set up the System Structure.

Section 12 PLC Connect

Introduction

This section provides post installation procedures for PLC Connect.

The SoftPoint Server is a subset of PLC Connect. Both use the same server processes and share a common real-time database (RTDB). PLC Connect and the SoftPoint Server can coexist in the same system, but the setup differs depending on whether PLC Connect and the SoftPoint Server are installed on the same node, or on separate nodes. Refer to [Figure 35](#) for an example.

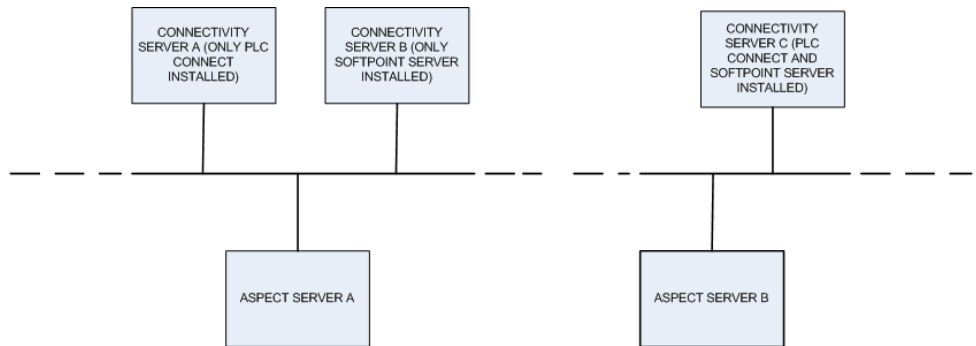


Figure 35. PLC Connect and SoftPoint Server Coexistence



Refer to [PLC Server](#) on page 136 (only if needed) for information on how to configure PLC Connect specific server processes. For example, to use a customer generated program with the 800xA System.

Control Network Setup

For each control network, a connection between the control network and its PLC Connect Connectivity Server must be established (a Connectivity Server node with the PLC Connect system extension). This is necessary in order to gain access to the dynamic process data that the Connectivity Servers provide.

Perform the procedures outlined in the following to set up the control network:

- [Creating a New Control Network Object](#) on page 130.
- [Configuring PLC Connect Services](#) on page 130.
- [SoftPoint and PLC Connect Coexistence](#) on page 132.

Creating a New Control Network Object

To create a new Control Network Object:

1. Open a Plant Explorer Workplace.
2. Use the Structure Selector to open the **Control Structure**.
3. Use the Object Browser to select `Root, Domain`.
4. Right-click `Root, Domain`, and select **New Object** from the context menu.
5. The New Object dialog box appears. Select the **List Presentation** check box.
6. From the left-hand list, select `PLC Generic Control Network`.
7. In the Name field, enter the name of the control network the object will represent.



For example, include the node name as part of the control network name.

8. Click **Create**.

Configuring PLC Connect Services

To configure PLC Connect services:

1. Select `Generic Control Network Configuration` in the Aspect List Area for the new PLC Generic Control Network object.

- Click the **Configure** tab in the Preview Area to produce the view shown in Figure 36.

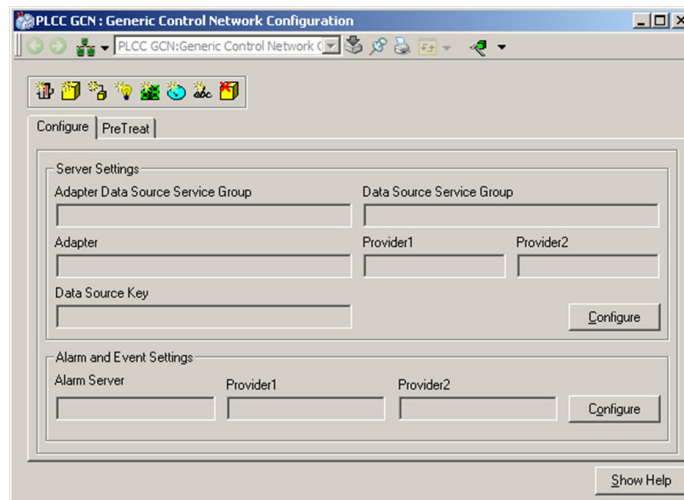


Figure 36. Generic Control Network Configuration Aspect

- Click **Configure** in the Server Settings Frame. This launches the Choose Connectivity Server Node dialog box.
- Select the primary Connectivity Server Node where the PLC Connect Server software is installed and click **OK**.
- Click **OK** at the configuration completed message.
- Click **Configure** in the Server Settings frame again if redundant Connectivity Servers were created. This launches the Choose Connectivity Server Node dialog box.
 - Select the **Node is redundant provider** check box.
 - Select the redundant Connectivity Server Node where the PLC Connect Server software is installed and click **OK**.
- Click **OK** at the configuration completed message.

8. The OPC Alarm Server for PLC Connect messages must be added to an Event Collector Service Group so that the System Message Service will collect alarms and events from PLC Connect on this network. This is done automatically when the Alarm and Event Settings portion of the **Generic Control Network Configuration** aspect is configured.
 - a. Click **Configure** in the Alarm and Event Settings frame of the Generic Control Network Configuration aspect.
 - b. Add providers in the same way as for the Server Settings.

SoftPoint and PLC Connect Coexistence

1. Use the Structure Selector to select the **Control Structure**.
2. Use the Object Browser to drag the `SoftPoints`, `SoftPoints Type` object from a SoftPoint Generic control network to the corresponding PLC Generic control network. Place the object at the same level as the `Controllers`, `PLC Controller Type` object as shown in [Figure 37](#).

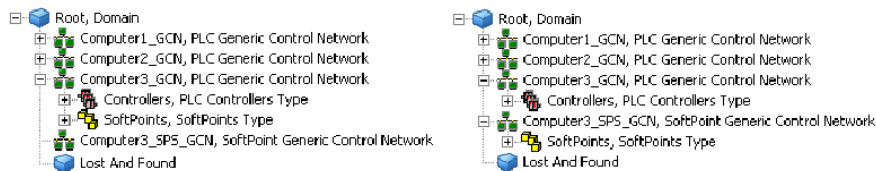


Figure 37. Dragged Object

3. Use the Object Browser to select the PLC Generic control network containing the dragged object.
4. Select `Deploy` in the Aspect List Area.
5. Click **Deploy** in the Preview Area.
6. Repeat this procedure for any other SoftPoint Generic control networks.

IEC 60870 Licensing

The IEC driver provides communication with controllers by the IEC60870-5 protocol suite. This is a licensed option.

Software Keys

The software key for the IEC 60870 driver is specific to the node on which it is installed. A new software key may also be required if the configuration of the node is changed. The licensing procedure for a node is described in the following subsections.

If necessary a license can be transferred from one node to another. Refer to [Transferring the Software License](#) on page 135. Other licensing options are described in [Other Licensing Options](#) on page 136.

Licensing Procedure

Perform the following procedures to license the IEC 60870 driver for a node:

- [Enable Temporary Authorization](#) on page 133.
- [Completing and Sending the License Files](#) on page 134.
- [Completing Formal Licensing](#) on page 135.

Enable Temporary Authorization

A temporary key allows the IEC 60870 driver to run in fully functional mode for 30 days from the installation date.

1. Log on with Administrator privileges to a node with the IEC 60870 driver option installed.
2. Start the software authorization licensing program:

**Start > All Programs > ABB Industrial IT 800xA > PLC Connect >
IEC60870 > License Utility**

The MTK Software Authorization dialog box appears (Figure 38).

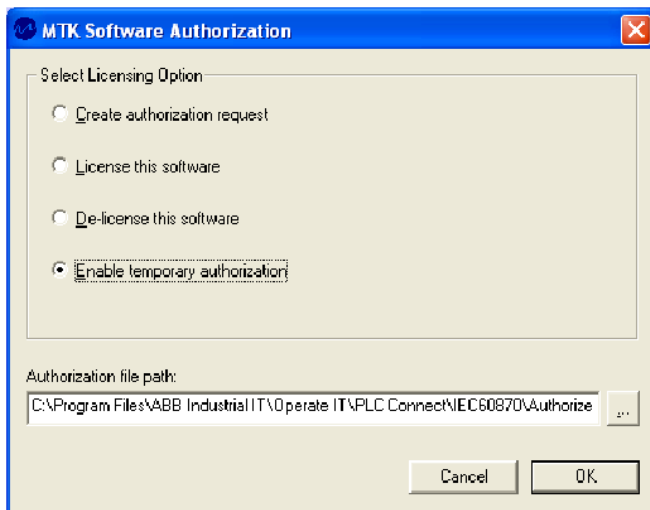


Figure 38. MTK Software Authorization Dialog Box

3. Select the **Enable temporary authorization** option.
4. Make sure the path is correct. (... \ABB Industrial IT\Operate IT\PLC Connect\IEC60870). If necessary, click ... to locate the file.
5. Click **OK**.

The application processes the key file and a confirmation message verifies that the software has been successfully licensed. If an error occurs, note the error information carefully, and contact ABB Customer Service.

Completing and Sending the License Files

During installation of PLC Connect with the IEC 60870 driver option on a node, all license related data is stored in two files: Software Key Request.doc and AuthorizeRequest.MTK. The two files are created in the following folder:

... \ABB Industrial IT\Operate IT\PLC Connect\IEC60870.

1. Fill out the Software Key Request file. (The file `AuthorizeRequest.MTK` is automatically generated.)
2. Send the two files by e-mail to `software_prod.seapr@se.abb.com`.

Completing Formal Licensing

Within a week from a request ABB will issue a software license key file named `Authorize.MTK` and send it to your e-mail address.

1. Log on with Administrator privileges to the node for which the license was requested.
2. Copy the `Authorize.MTK` file to the following folder:
`...\ABB Industrial IT\Operate IT\PLC Connect\IEC60870.`
3. Start the software authorization licensing program:
Start > All Programs > ABB Industrial IT 800xA > PLC Connect > IEC60870 > License Utility

4. The MTK Software Authorization dialog box appears ([Figure 38](#)).
5. Select the **License this software** option.

6. Click **...** to locate the authorization file. Make sure the path is correct:

`...\ABB Industrial IT\Operate IT\PLC Connect\IEC60870.`

7. Click **OK**.

The application processes the key file and a confirmation message verifies that the software has been successfully licensed. If an error occurs, record the error information exactly as it appears, and contact ABB Customer Service.

8. Back up all licensing files, `*.MTK`, from the following folder:

`...\ABB Industrial IT\Operate IT\PLC Connect\IEC60870.`

to removable media.

Transferring the Software License

If it is necessary to transfer a license from one node to another node, perform the following:

1. Locate the file REMOVEREQUEST.MTK on the previously used node. This file was generated during the authorization process, and is located in the following folder:

... \ABB Industrial IT\Operate IT\PLC Connect\IEC60870.

Send the file to ABB together with the two files generated on the new node.

2. When entering information onto the Software Key Request form, specify **Transfer of software** and state the reason for the transfer.

If transferring the software to another node, install it there first, and send the new authorization request file along with the remove request file at the same time. ABB will then issue a license authorization file for the new node.

Other Licensing Options

The rest of the licensing options in the MTK Software Authorization dialog box (Figure 38), are described in Table 7. When an action is selected, the corresponding default path and file name are displayed. Click ... to locate a file.

Table 7. Other PLC Connect Licensing Options

Function	Description
Create authorization request	Creates a software license request file. It is normally not necessary to use this function, since a request file is generated automatically during installation.
De-license this software	Removes the licensing. Use this function if requested by ABB to do so, for example to return the software after an evaluation period.

PLC Server

The PLC Server manages all PLC Connect specific server processes. It is configured automatically during the software installation. However, it may be necessary to configure PLC Server processes manually for a specific control network, for example, to:

- Restart a server process for the control network.
- Add a program as a server process for the control network; for example, to use a customer generated program with the 800xA System.

Configuring PLC Server Processes

To configure PLC Server processes for a specific control network:

1. Open a Plant Explorer Workplace.
2. Use the Structure Selector to select the **Service Structure**.
3. Use the Object Browser to select PLC Server, Service.
4. Select the Service Group object for the desired control network (the Service Group object representing the node with the Connectivity Server that is connected to the desired control network). An example is presented in [Service Structure Example](#) on page 137.
5. Select Service Group Definition in the Aspect List Area.
6. Select the **Special Configuration** tab in the Preview Area to view the server processes for the control network.
7. Click **Help** for more information on how to use the tab.
8. To configure the same server processes for other control networks, repeat [Step 4](#) to [Step 7](#) for each one.

Service Structure Example

The names of the Service Group objects are typically the same as the respective node name. In the example in [Figure 39](#), they are Computer1, Computer2, and Computer3.



Figure 39. Service Structure Example

Section 13 IEC 61850 Connect

Introduction

This section provides post installation procedures for IEC 61850 Connect.

Replacing the XML Files

Perform this procedure on all IEC 61850 Connectivity Servers. XML files must be copied from one location to another.



Perform this procedure before configuring the OPC Server.

1. Use Windows Explorer to navigate to the following folder:
 ...:\Install folder\ABB Industrial IT\Operate
 IT\IEC61850 Connect\opcconfig
2. Copy all XML files in this folder.
3. Use Windows Explorer to navigate to the following folder:
 ...:\Install folder\ABB\61850 OPC
 Server\CET\bin\Object Types\xml
4. Paste the files copied in [Step 1](#).
5. Click **Yes** in the Confirm File Replace dialog box.

Section 14 Asset Optimization

Introduction

This section describes post installation procedures for Asset Optimization.

AoWebServerNode

Perform the following steps to set the AO Web Server Node.

1. Open a Plant Explorer Workplace.
2. Use the Structure Selector to open the **Control Structure**.
3. Use the Object Browser to navigate to:
Root, Domain > Asset Optimization, Asset Optimization
4. Select Asset Optimization Configuration Properties in the Aspect List Area.
5. In the Preview Area, set the AOWebServerNode property to the AO server node designated as the AO Web Server.



The AO Server node designated as the AO Web Server in a multinode system must be a node using Windows Server 2008 as the operating system.

Asset Monitoring Service Provider Node

Perform the following steps to set the Asset Monitoring Service Provider Node:

1. Open a Plant Explorer Workplace.
2. Use the Structure Selector to open the **Service Structure**.
3. Use the Object Browser to navigate to:

Services > Asset Monitoring, Service > AssetMonitoring
SG_1, Service Group > AssetMonitoring SP_1, Service
Provider

4. Select `Service Provider Definition` in the Aspect List Area.
5. Set the Asset Optimization Service Provider node to the node designated to run the default AssetMonitoring Service and related AO Engine in the **Node:** drop-down list box. This node name is usually the same as `AoWebServerNode`.
6. Select the **Enabled** check box and click **Apply**. This will set the Service Provider hostname.
7. Use the Structure Selector to open the **Control Structure**.
8. Use the Object Browser to navigate to:

Root, Domain > Asset Optimization, Asset Optimization >
AO Server 1, AO Server 1
9. Select `Asset Optimization Server` in the Aspect List Area.
10. Verify that Service Status is Service, and the Asset Monitoring Engine is running.

Refer to the **Loading Asset Monitor Configurations to an AO Server** topic in **Section 2 - System Setup** of *System 800xA Asset Optimization Configuration (3BUA000118*)* for information on how to load the AO Server configuration.

Adding Additional AO Servers to the System

Asset Monitoring supports a maximum number of four AO Servers running on Application Server Nodes or four AO Servers if the AO Server is combined with a Connectivity Server (such as HART Connectivity Server or FOUNDATION Fieldbus Connectivity Server). Each AO Server can support a maximum number of 30,000 asset conditions. The maximum supported asset monitors is 10,000 per server or 20,000 per 800xA System.

The Asset Optimizer Server System Extension provides the configuration for one AO Server. An AO Server is represented by:

- An AO Server object located in the **Control Structure** under the Asset Optimization parent node.

- An AssetMonitoring Service Group and related Service Provider in the **Service Structure**.



Never move/delete the Asset Optimization object in the **Control Structure** since this object has a specific ID.

To add an additional AO Server node in an 800xA System:

1. Open a Plant Explorer Workplace.
2. Use the Structure Selector to open the **Service Structure**.
3. Use the Object Browser to navigate to and right-click on:
`Services > AssetMonitoring, Service`
4. Select **New Object** from the context menu. This opens the New Object dialog box.
5. Select `Service Group` from the list on the left.
6. Type a name in the Name field and click **Create**.
7. Use the Object Browser to navigate to and right-click on the newly created Service Group.
8. Select **New Object** from the context menu. This opens the New Object dialog box.
9. Select `Service Provider` from the list on the left.
10. Type a name in the Name field and click **Create**.
11. Select `Service Provider Definition` in the Aspect List Area for the newly created Service Provider.
12. Select the node identified to host this AO Server from the **Node:** drop-down list box. There can only be one AssetMonitoring Service per node.
13. Click **Apply**. This will set the Service Provider hostname for this AO Server.
14. Use the Structure Selector to open the **Control Structure**.
15. Use the Object Browser to navigate to and right-click on:
`Root > Asset Optimization`

16. Select **New Object** from the context menu. This opens the New Object dialog box.
17. Select `AO Server` from the list on the left.
18. Type a name in the Name field and click **Create**.
19. Use the Object Browser to select the newly created object.
20. Select `Asset Optimization Server` in the Aspect List Area.
21. In the Preview Area, select the newly created Service Group from the **Service Group** drop-down list box and click **Apply**.
22. Navigate to this Asset Optimization Server default view and verify that Service Status is Service, and AssetMonitoring Engine is running.



It is possible to designate a different AO Server as the default AO Server by navigating to the AO Server, Asset Optimization Server aspect Config View and selecting the default **Asset Optimization Server** check box and clicking **Apply**.

Refer to the **Loading Asset Monitor Configurations to an AO Server** topic in **Section 2 - System Setup** of *System 800xA Asset Optimization Configuration (3BUA000118*)* for information on how to load the AO Server configuration.

Restarting the Event Collector Service

Perform the following steps to see events in Asset Optimization Event Log:

1. Open a Plant Explorer Workplace.
2. Use the Structure Selector to open the **Service Structure**.
3. Use the Object Browser to navigate to:

```
Event Collector,Service > ABB 800xA System Message  
Server,Service Group > Event Collector_ABB 800xA  
System Message Server_NodeName, Service Provider
```

where *NodeName* is the node where the service is registered which is generally the Aspect Server node.

4. Select `Service Provider Definition` in the Aspect List Area.
5. Clear the **Enabled** check box and click **Apply**.

6. Select the **Enabled** check box and click **Apply**.
7. Repeat [Step 4](#) through [Step 6](#) for:

```
Event Collector,Service > ABB 800xA Soft Alarm OPC  
Server,Service Group > Event Collector_ABB 800xA Soft  
Alarm OPC Server_NodeName, Service Provider.
```
8. This will restart the Event Collector_ABB 800xA System Message
Server_NodeName and Event Collector_ABB 800xA Soft Alarm OPC
Server_NodeName services and the Asset Optimization Event Log will display
all events.

Web-Enabled Views on Non-Industrial IT Systems

The software requirements on non-Industrial IT systems required to support web-enabled Asset Optimization views are:

- Internet Explorer 6 or later.
- MS XML 3.0 with Service Pack 2 or later.
- Microsoft Visual C++ 2008 SP1 Redistributable Package (x86).
(vcredist_x86.exe available for download from Microsoft).

The maximum security settings on non-Industrial IT systems required to support web-enabled Asset Optimization views are:

- Set Local Intranet security to High.
- Select Custom Level and set the following:
 - Download signed ActiveX[®] controls: Prompt.
 - Run ActiveX controls and plug-ins: Enable.
 - Script ActiveX controls marked for safe scripting: Enable.
 - Active scripting: Enable.



Accessing the Asset Optimization thin client interface always requires user authentication for Asset Optimization web pages.

cpmPlus Enterprise Connectivity (ECS 4.0 and 4.2)

The Maximo Server name and IP address must be entered in the Window hostfile on the node where ECS is installed.

Maximo Integration

This section describes the configuration and setup information required for Maximo Server.

Maximo Business Object (Maximo 6.2 and 7.1)

The [Table 8](#) and [Table 9](#) displays the web services that needs to be configured on the Maximo Server.

Configure the following web services on the Maximo Server. Contact Maximo technical support for detailed procedure.

Table 8. Maximo Business Object (Maximo 6.2)

Integration Object Name	AO Function	Interface
MXWO	Submit Work Order	MXWOInterface
MXWO	View Active Work Order, Work Order History	MXWorkOrderQuery
MXASSET	View Equipment Status	MXASSETQInterface
SPAREPART	View Spare Parts	MXSparePartQInterface
PM	Vier Prev Maint Schedule	MXPMQInterface
MXINVENTORY	Spare Part Availability (This function is called from View Spare Part aspect)	SPAVAILQ

Table 9. Maximo Business Object (Maximo 7.1)

Integration Object Name	Object Structure	AO Function	Interface
WORKORDER	MXWO	Submit Work Order, View Active Work Order, Work Order History	MXWO
ASSET	MXASSET	View Equipment Status	MXASSET
SPAREPART	MXSPAREPART	View Spare Part	MXSPAREPART
PM	MXPM	View Preventive Maintenance	MXPM
INVENTORY	MXINVENTORY	View Spare Part Availability (This function is called from View Spare Part aspect)	MXINVENTORY



Do not change the interface name in the [Table 8](#) and [Table 9](#). Modifying the interface name involves additional engineering effort.

SAP/PM Integration

The Asset Optimization integration with the SAP/PM module requires that the SAP administrator install ABAP code on the SAP/PM production server where the PM module is installed.

1. Navigate to the directory where Asset Optimization software is installed.
2. Use Windows Explorer to locate the following directory:

```
... \Asset Optimization \SAPConnectivity \SAP-ABAP
```
3. This directory contains the source for the ABB ABAP integration code and documentation that describes the ABAP code integration.

The ABB ABAP integration code source files are:

- Z_ABB_EQUIPMENT_DETAIL.ABAP.doc
- Z_ABB_MS_LIST.ABAP.doc
- Z_ABB_NOTIFICATION_CREATE.ABAP.doc
- Z_ABB_NOTIFICATION_LIST.ABAP.doc
- Z_ABB_OBJECTSTATUS_LIST.ABAP.doc
- Z_ABB_WORKORDER_LIST.ABAP.doc
- Z_ABB_WORKORDER_HIST1.ABAP.DOC

Reference documents include the following:

- SAP RTAO Development.doc
- - Z_ABB_PM_FunctionGroup-Modules.doc

Refer to the SAP/PM Basis and ABAP integration personnel for details involving the addition of ABAP-enabled interfaces in SAP.

Feature Pack Functionality

ECS SAP Plugin uses the `Librfc32.dll` to communicate with the SAP System. This version of the dll is specific to SAP Server.

Copy the dll from SAP Server to the following folder:

```
<InstallDirectory>\Program Files\ABB Industrial IT\cpmPlus  
Enterprise Connectivity\Service
```

Internet Explorer Configuration

To configure Internet Explorer for use with Asset Optimization:

1. Use standard Windows procedures to access the Local Area Network (LAN) Settings dialog box.
2. If proxy configuration is selected, select the **Automatically detect settings** check box.

Excel Initialization

The following procedure is necessary if using the XY Profile Deviation Asset Monitor.



Failure to perform the required Microsoft Excel user setup when using the XY Profile Deviation Asset Monitor may cause the AO Server startup to fail.

1. Use the 800xA Service User account to open Microsoft Excel at least once.
2. Perform the required user setup (first time execution installation user initials).

Section 15 PC, Network and Software Monitoring

Introduction

This section describes the actions necessary to set up the Basic Computer Monitoring functionality of PC, Network and Software Monitoring.

Basic Computer Monitoring

Set up Basic Computer Monitoring according to the information provided in Section 2 of *System 800xA PC, Network and Software Monitoring Configuration* (3BUA000447*).

The OPC Data Source Definition aspect must be set up in order to have the Basic Computer Monitoring functionality.

Perform the following to set up the OPC Data Source Definition aspect:

1. Open a Plant Explorer Workplace.
2. Use the Structure Selector to open the **Control Structure**.
3. Use the Object Browser to navigate to and select IT OPC Server Network.
4. Right-click on OPC Data Source Definition in the Aspect List Area and select **Config View** from the context menu.
5. Click **New** in the Preview Area.
6. Click **Add** and select the appropriate service provider from the list.
7. Click **OK** twice.
8. Click **Apply**.

In order to create and configure the Basic Computer Monitoring functionality the Basic Computer Monitoring Configuration Tool must be run.



Run the Basic Computer Monitoring Configuration Tool once all nodes that will form the 800xA System have been added and identified to the 800xA System (added as Aspect Servers, Connectivity Servers, or Clients). If new 800xA System nodes are added or removed after the Basic Computer Monitoring Configuration Tool has been run, then it will be necessary to run the Basic Computer Monitoring Configuration Tool to ensure that the correct assets are being monitored.

- 1. Select:
Start > All Programs > ABB Industrial IT 800xA > Asset Optimization > PC, Network and Software Monitoring > Basic Computer Monitoring Configuration Tool
to launch the Basic Computer Monitoring Configuration Tool.
- 2. Click **Start**. The application will automatically close when it is completed.

Minor configuration changes are normally required after the software is installed and the Basic Computer Monitoring Configuration Tool is run. The default alarm limits are expected to be suitable in most situations. In some cases it may be necessary to modify the hard drives that require monitoring.

Changing the alarm limits and the hard drives being monitored is done in the Basic Computer Device aspect shown in [Figure 40](#).

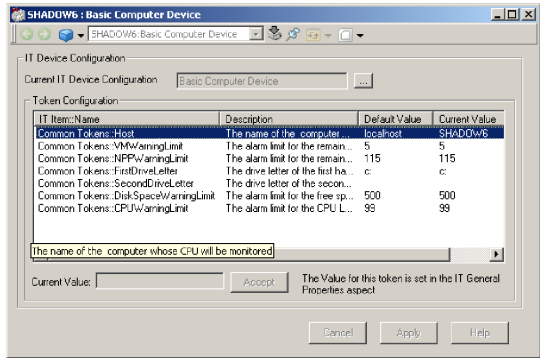


Figure 40. Basic Computer Device Aspect

Section 16 Device Library Wizard

Introduction

This section describes post installation procedures for the Device Library Wizard.

Device Library Wizard Server Settings

Perform the following procedure on all 800xA System nodes where the Device Library Wizard - Client component is installed.

1. Open the Device Library Wizard:

Start > All Programs > ABB Industrial IT 800xA > Device Mgmt > ABB Device Library Wizard

-or -

double-click the *ABB Device Library Wizard* shortcut on the Desktop.

2. When the Device Library Wizard main dialog box opens, select **Device Library Wizard Administration** and click **Next**.



The following can be skipped on the system node where the Device Library Wizard - Server and the Device Library Wizard - Client are installed, as the **Connect Client** function is performed automatically.

3. Select **Connect Client** and click **Next**.
4. Enter the name or IP address for the Primary Aspect Server in the Name/IP field and click **Next**.
5. Click **Finish** to confirm the Server setting.
6. Successful connection is indicated by the *Configuring server settings is completed!* entry in the logger area of the Finish Operation dialog box. Click **Main Menu** to complete and exit from the configuration process.

7. Close the Device Library Wizard by clicking **Exit**.



It is only possible to work with Device Types using the Device Library Wizard after successfully completing the server node settings configuration.

Fieldbus Device Type Preparation (Optional)

Perform the following steps at the point of time the Device Types to be used in the 800xA System are known.



If performing a system upgrade from a previous 800xA System version, it is mandatory to follow the procedure described in *System 800xA Upgrade (3BSE036342*)*.

Installing Fieldbus Device Types



The following steps for Device Types need to be carried out on every system node, except thin client nodes and separate Domain Controller nodes. Perform the install Device Types procedure on the nodes in the following sequence:

Aspect Servers (including redundant Aspect Servers). Install the Device Types on the Primary Aspect Server node before starting to install them on other system nodes. Do not run parallel installations of Device Types on other system nodes unless all Device Types are installed on the Primary Aspect Server node. Installation of Device Types on other system nodes can be done in parallel after they are installed on the Primary Aspect Server node.

- Connectivity Servers (including redundant Connectivity Servers).
 - Application Servers.
 - Clients.
1. Insert the 800xA System DVD for the required Fieldbus Device Types into the DVD drive (FOUNDATION Fieldbus, HART, or PROFIBUS).
 2. Start the Device Library Wizard:

Start > All Programs > ABB Industrial IT 800xA > Device Mgmt > Device Library Wizard

-or-

double click the *Device Library Wizard* icon on the desktop.

3. Navigate to the Device Library Wizard main dialog box and select:
Extract Device Types > Extract Device Types via Manual Selection.

4. Click **Browse** and navigate to the DVD drive.
5. In the Browse dialog box, select all Device Types required for system engineering and start extracting.



If the installation DVD does not contain all Device Types, the missing Device Types may be available for download from ABB SolutionsBank.

Continue with this procedure after all required Device Types are extracted.

6. Navigate back to the Device Library Wizard main dialog box after a successful extraction.
7. Select:
Device Type Administration > Install Device Types > (required protocol (FOUNDATION Fieldbus, HART or PROFIBUS))
8. Each listed Device Type includes a Release Note for the corresponding Device Type object. Right-click on the listed Device Type to open the Release Note. Read the Release Note carefully for detailed installation and engineering information or limitations.
9. Select the Device Types required for engineering in the system and follow the install procedure.
10. Exit the Device Library Wizard.

Section 17 Device Management FOUNDATION Fieldbus

Introduction

This section describes post installation procedures for Device Management FOUNDATION Fieldbus.

General Settings

During Device Management FOUNDATION Fieldbus installation a dialog box for entering hardware and software settings was displayed. If those settings were not entered during the installation process, they should be entered now.

1. Select:
Start > All Programs > ABB Industrial IT 800xA > Device Mgmt > FF > Configure
2. Refer to the General Settings topics in the Device Management FOUNDATION Fieldbus section of *System 800xA Installation (3BSE034678*)* for a detailed description.

Time Synchronization

Device Management FOUNDATION Fieldbus requires active time synchronization on HSE net for appropriate alarm time stamping. Windows Time Service (W32Time) must be activated on each FOUNDATION Fieldbus Connectivity Server. Refer to the **Time Synchronization** section in *System 800xA Network Configuration (3BSE034463*)*.

Section 18 Process Engineering Tool Integration

Introduction

This section describes post installation procedures for Process Engineering Tool Integration.

INtools Import Export Utility

Perform the following steps on the node that contains INtools 6.0 or SmartPlant Implementation 7.0 (INtools/SPI) software.

1. Select the following:

Start > Programs > ABB Industrial IT > Engineering > Process Engineering Tool Integration > INtools Import Export Utility

2. Click **Load INtools.ini File** and select the desired .ini file.



The status button will turn green indicating the INtools Import Export utility connected to the INtools/SPI database successfully.

3. Click the **Administrator** tab.

4. Click **Install INtools Connector**.



INtools/SPI data can not be read using Web Services or the CAEX file without successful installation of the connector.

Process Engineering Tool Integration

Perform this procedure when Process Engineering Tool Integration is installed on:

- The Primary Aspect Server node (containing Control Builder M and Engineering Studio).
- Engineering Workplace nodes with Control Builder M installed.



The Process Engineering Tool Integration system extension should have been added on the Primary Aspect Server node as described in [Loading System Extensions](#) on page 27.

1. Select:
Start > All Programs > ABB Industrial IT 800xA > Engineering > Process Engineering Tool Integration
2. Click **Set** in the Start dialog box.
3. Select the desired Workflow from the drop-down list box and click **Apply**.
4. Select **Transfer Data** in the Start dialog box and click **Set Server Name**.
5. Enter the name of the node that contains INtools/SPI and Web Services software and click **Apply**.

Section 19 Information Management

Introduction

This section describes post installation procedures for Information Management.



Some procedures in this section require administrator-level user privileges. The user must be a domain user with Administrator privileges if the IM Server resides in a domain. Use the 800xA Installing User account.

Information Management Setup

Use the post installation configuration assistant installed with the Information Management software to ensure that installation and post installation procedures are completed in the correct sequence.

To launch the configuration assistant, select:

**Start > All Programs > ABB Industrial IT 800xA >
Information Mgmt > Configuration Assistant**

The Configuration Assistant, [Figure 41](#), lists the installation and post installation requirements in the order in which they must be completed.

Each procedure has a dedicated row. The row indicates whether the procedure is required or optional, whether or not the procedure has been completed, the action to be performed when the procedure is launched from the assistant, and any special considerations and guidelines that apply to the procedure.

The rows are also color-coded. Procedures that have been completed are black. Uncompleted required procedures are red, and uncompleted optional procedures are brown. Some rows are headings for multistep procedures; for example, step 4.0 Configuring the DBA (ADO) Data Provider for Oracle. These rows do not have an associated action, since the actions are performed in the steps following

them. The associated steps are sequentially numbered, for example 4.1, 4.2, etc. Instructions for the selected procedure (or step) are indicated in the Instructions box in the upper right corner of the display.

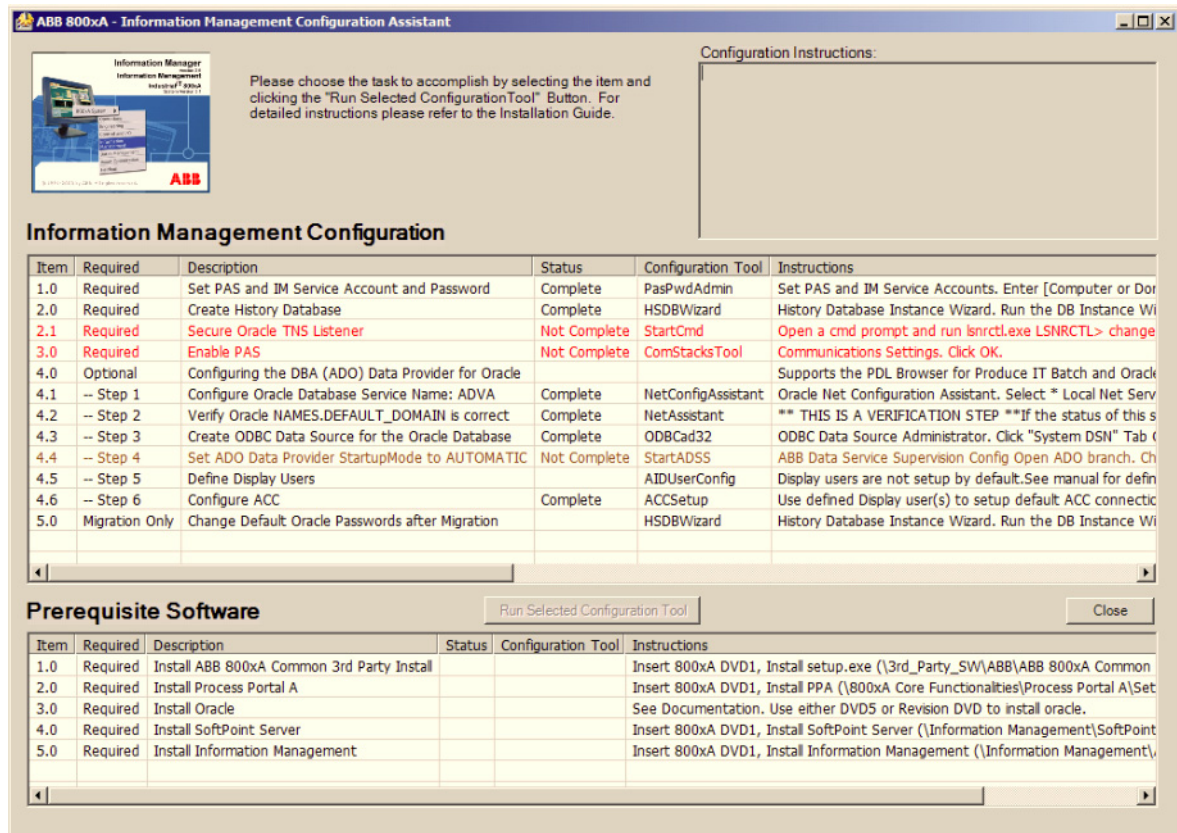


Figure 41. Information Management Configuration Assistant

For confirmation purposes, all installed software components are listed in the Prerequisite Software list in the lower pane. After confirming that all of the necessary software is installed, use the procedures in this section and the Configuration Assistant for:

- [Creating a History Database Instance](#) (required).

- [Creating a Secured Password for Oracle TNS Listener](#) (required) Follow the instructions to create a password for the oracle listener.
- Initializing communication settings and [Starting Process Administration Supervision \(PAS\)](#)(required).
- [Configuring the DBA \(ADO\) Data Provider for Oracle Data](#) (optional) If Oracle data access is required for PDL access for Batch management, and/or history message log access). It is also required for general SQL functionality offered in DataDirect and SQLBrowser. In this revision, the user must create the display users, refer to the *System 800xA Information Management Configuration (3BUF001092*)*. Once the user is created, run the ACC setup to map the defined users.

Referenced Post Installation Procedures

When completed with the configuration assistant, refer to the following list to determine whether any other post installation is required to set up the system and make it ready for application building. These procedures are covered in the referenced instructions.

- One or more History Source aspects must be configured to support operator trend and historical data collection. Refer to **Section 5 - Configuring History Database** in *System 800xA Information Management Configuration (3BUF001092*)*.
- Add-in tools for DataDirect and Information Management History Bulk Configuration are added into Microsoft Excel on a user basis. These add-ins are added by default for the Installing User. To use these applications as any other user, the corresponding add-ins must be installed in Microsoft Excel for that user. Refer **Section 5 - Configuring History Database** in *System 800xA Information Management Configuration (3BUF001092*)*, or **Section 3 - DataDirect - Excel Data Access Functions** in *System 800xA Information Management Data Access and Reports (3BUF001094*)*.



If it is intended to use the 800xA Application Scheduler to run reports created with DataDirect (Excel Data Access), the add-in tools must be added for the 800xA Service User account. This is the account used by the Application Scheduler.

- Change the default password to secure the Information Management database from unauthorized access. Refer to the **Managing Users** topic in **Section 17 - System Administration** of *System 800xA Information Management Configuration (3BUF001092*)*.

ActiveX Security Settings

If the default security ActiveX settings are not changed, a prompt appears asking whether or not to allow access of blocked controls every time an attempt is made to use a tool that includes an ActiveX control. This affects the Desktop tools and the Profile client applications.

To allow the controls to load without intervention, perform the following steps:

1. Launch Internet Explorer.
2. Select: **Tools > Internet Options**.
3. Select the **Advanced** tab.
4. In the Security section, enable the following check boxes:
 - **Allow active content from CDs to run on My Computer.**
 - **Allow active content to run in files on My Computer.**

Creating a History Database Instance

Use the DB Instance wizard to create a History database instance. This will determine the Oracle tablespace and disk space requirements and where History related files will be stored. If installing Information Management software for an end user, the History database requirements may not be known at this time. In this case, the wizard default values can be used to create a default instance sized to fit most History applications. If it is determined later that the default instance is not large enough, the end user can drop this instance and create a new one.

To create the default database instance:

1. Launch the History Database Maintenance wizard by selecting:
Start > Programs > ABB Industrial IT 800xA > Information Mgmt > History > Oracle Instance Wizard

2. Click **Next** in the Welcome dialog box.
3. Select the **I will enter the information manually and save it to a new configuration file** option and click **Next** in the Configure File Options dialog box.



Perform only the following procedures applicable to the needs of the installed 800xA System.

4. Message Logs.

- a. Determine if message logs will be used, select the appropriate option, and click **Next**.
- b. Enter the required OPC and DCS message log information ([Figure 42](#)).

Figure 42. Message Logs Information

5. Numeric Logs.

- a. Determine if numeric logs will be used, select the appropriate option, and click **Next**.
- b. Enter the required numeric log information ([Figure 43](#)). Click + or - (not shown in [Figure 43](#)) to add or remove a group of logs.

Expected Numeric Log Configuration					
Number Of Logs	Rate	Unit	Duration	Unit	Storage Type
10	1	Second(s)	3	Month(s)	TYPE5

Figure 43. Numeric Logs Information

6. Profile Logs.

- a. Determine if profile logs will be used, select the appropriate option, and click **Next**.
- b. Enter the required profile log information (Figure 44). Click + or - (not shown in Figure 44) to add or remove a group of logs.

☒ Yes. I will be using profile logs.

Expected Profile Log Configuration					
Number Of Logs	Rate	Unit	Duration	Unit	Array Size
10	1	Second(s)	3	Week(s)	100

Figure 44. Profile Logs Information

- c. Determine if profile PDL logs will be used, select the appropriate option, and click **Next**.
- d. Enter the required profile PDL log information (Figure 45).

☒ Yes. I will be using profile PDL.

Storage Duration

3

Month(s)

Reels and Grades Per Day

20

Per Reel/Grade

Variables

5

History Associations

5

Figure 45. Profile PDL Logs Information

7. Batch Management PDL Logs.

- a. Determine if a Batch Management PDL log will be used, select the appropriate option, and click **Next**.

- b. Enter the required Batch Management PDL log information (Figure 46).

☒ Yes, I will be using Batch Management PDL.

Storage Duration: Month(s)

Batches Per Day:

Procedures Per Batch:

PDL Message Log Capacity:

Per Procedure:

Variables:

History Associations:

Equipment Transactions:

Space Required: 1795 MB

Figure 46. Batch Management PDL Log Information

8. Unarchived Reports.

- a. Determine if reports will be stored online (unarchived reports), select the appropriate option, and click **Next**.
- b. Enter the number of reports to be stored online.
9. Specify the disk drives that will contain the Oracle system files, history data files, and history indexes, and click **Next**.
10. Click **Advanced** to access the advanced version of this dialog box (Figure 47) that allows the disk drive, initial memory size, and maximum memory size of each type of file to be specified.
11. Specify the amount of flat file space to allocate and on which disk drives it should be allocated (Figure 48) and click **Next**. Be sure to allocate enough memory space so that the Flat File Space Left To Reserve number is equal to zero.
12. Click **Next** when notified that the Oracle Instance Wizard has all the information it needs to configure the history Oracle instance.
13. Click **OK** when notified that the Oracle instance has been successfully created.
14. Click **Next** in the Configuring Oracle window.

- 15. Determine if the accounts of Oracle system users are allowed to use the default passwords or they all should use the same new password and click **Next**.
- 16. If all the accounts are to use the same new password, enter and then re-enter the new password.
- 17. Click **Finish** when notified that the Oracle configuration process is complete.

Information Management: Oracle Instance Wizard

Choose Database File Locations

Below is a list of all of the files that History's Oracle instance will need as well as the amount of disk space that each file will require. Please indicate on which disk drive you would like to store each file. It is recommended, but not necessary, that you store the Oracle system files on one disk, the History data files on a second disk and the History index files on a third disk.

File Description	File Type	Initial Size (MB)	Auto Extend	Maximum Size (MB)	Disk Drive	Disk Drive	Free Space (MB)
History Runtime Data	Data	640	<input checked="" type="checkbox"/>	768	C:\	C:\	176105 MB
History Configuration Data	Data	64	<input checked="" type="checkbox"/>	192	C:\	D:\	153264 MB
History PDL Data	Data	64	<input checked="" type="checkbox"/>	192	C:\		
History Restored Logs	Data	64	<input checked="" type="checkbox"/>	192	C:\		
History Reports	Data	64	<input checked="" type="checkbox"/>	192	C:\		
History Runtime Indexes	Indexes	640	<input checked="" type="checkbox"/>	768	C:\		
History Configuration Indexes	Indexes	64	<input checked="" type="checkbox"/>	192	C:\		
History PDL Indexes	Indexes	64	<input checked="" type="checkbox"/>	192	C:\		
Oracle System Files	System	256	<input checked="" type="checkbox"/>	384	C:\		
Oracle System Aux Files	System	256	<input checked="" type="checkbox"/>	384	C:\		
Oracle Temp Files	System	512	<input checked="" type="checkbox"/>	640	C:\		
Oracle Undo Files	System	128	<input checked="" type="checkbox"/>	256	C:\		
Oracle Redo Log	System	256	<input checked="" type="checkbox"/>		C:\		

Basic

Help

Back

Next

Figure 47. Advanced Database File Locations Information

Flat File Space Left To Reserve: 8830 MB

Flat File Locations		
Disk Drive	Free Space (MB)	Flat File Space Allocated (MB)
C:\	137468	0
E:\	84954	0
F:\	476812	0

Figure 48. Flat File Space Allocation Information

To secure the Information Management database, ensure to set the oracle instance users password once the database is created. Refer to the *System 800xA Information Management Configuration (3BUF001092*)* for more details to set the oracle instance users password.

Creating a Secured Password for Oracle TNS Listener

Perform the following steps to create a secured password for Oracle TNS listener from the configuration assistant. Follow the instructions from the Configuration Instructions: for the Item selected from configuration assistant window.

1. Click **Run Selected Configuration tool**, the command prompt appears.
2. Enter a password from the command prompt for the Oracle TNS Listener.



It is recommended to use the same password that is used for the oracle administrator.

Starting Process Administration Supervision (PAS)

PAS manages all Information Management services. PAS must be started after the software has been installed. When PAS is started for the first time the communication settings must be initialized. This is required for History Services to run. These settings only need to be initialized at this time. They do not need to be configured to their final values.

When the History Service is started under PAS, the following History setup occurs:

- The Service Group/Service Provider structure for the Information Management node will be created in the **Service Structure**.

- The OPC Alarm Server for History will be added in the Alarm and Event Service Group under the Alarm and Event Services category for this node in the **Service Structure**.
- The IM History, IM Archive, and IM Importer links will be added to the Basic History Service Group for this node in the **Service Structure**.

To start PAS and initialize the communication settings, from the configuration assistant, select **Enable PAS**, then click **Run Selected Configuration Tool**. This launches the Communication Settings dialog box shown in [Figure 49](#).

These settings can be configured to their final values at this time if the required information is available, or they can be initialized now, and configured later. This section describes how to initialize the settings. For further guidelines on configuring the settings, refer to **Appendix A - Extending OMF Domain to TCP/IP** in *System 800xA Information Management Configuration (3BUF001092*)*.

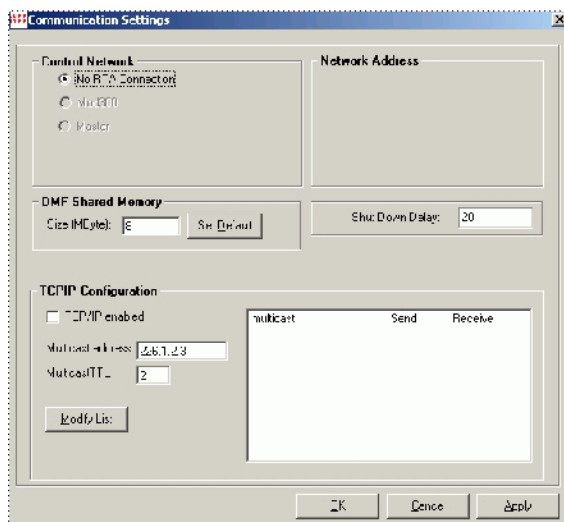


Figure 49. Communication Settings Dialog Box

1. To initialize the current settings, click **OK** in the Communication Settings dialog box.

2. A prompt appears asking whether or not to restart the computer. A restart is not required at this time. A restart is only required when the OMF Memory or TCP/IP enabled setting is changed. After responding to the Restart Inquiry prompt, the processes will automatically be restarted by PAS and the Communication Settings dialog box will close.

Configuring the DBA (ADO) Data Provider for Oracle Data

The Information Management installation provides two default ADO data providers.

The second ADO data provider supports the PDL browser for Batch Management, and Oracle data access via DataDirect, Display Services, and Desktop Trends.

The first data provider is configured to support data access for the demonstration displays provided with Display Services. Refer to **Appendix A - A Demonstration of Display Services** in *System 800xA Information Management Configuration for Display Services, (3BUF001093*)* for more information. This data provider does not require any further configuration.

The second ADO data provider supports the PDL browser for Batch Management, and Oracle data access via DataDirect, Display Services, and Desktop Trends.

This data provider requires some configuration to make it operational at the site. Specifically, a local Net service name must be configured and an ODBC data source must be created for the Oracle database. The StartUpMode of the ADO data provider must then be changed. Follow these basic steps and refer to the referenced pages for details:

- [Creating an ODBC Data Source for the Oracle Database](#) on page 171.
- [Editing the ADO Data Provider Configuration](#) on page 173.

Creating an ODBC Data Source for the Oracle Database

This procedure explains how to install and configure an Oracle ODBC driver for the Information Management Oracle database.

1. From the configuration assistant, select **Create ODBC Data Source for the Oracle Database**, then click **Run Selected Configuration Tool**. This displays the ODBC Data Source Administrator dialog box shown in [Figure 50](#).

- 2. Select the **System DSN** tab.

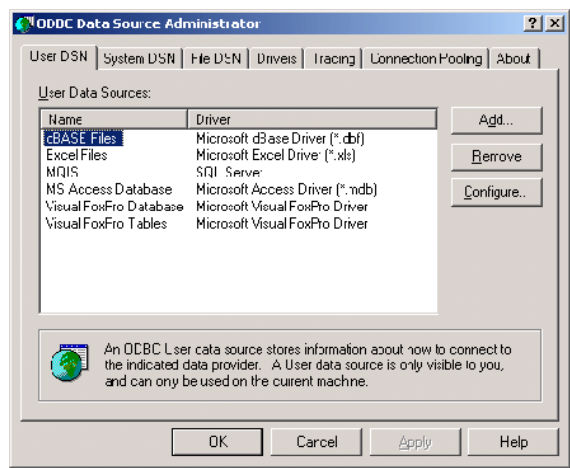


Figure 50. ODBC Data Source Administrator Dialog Box

- 3. Click **Add** to display the Create New Data Source dialog box shown in [Figure 51](#).

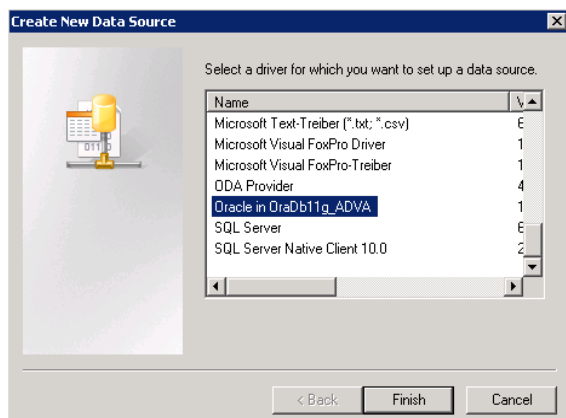


Figure 51. Create New Data Source Dialog Box

4. Select `Oracle` in `OraDb11g_ADVA` and click **Finish**. This launches the Oracle ODBC Driver Configuration dialog box (Figure 52).
5. Set the Data Source Name and TNS Service Name fields to `localhost`, as shown in Figure 52.

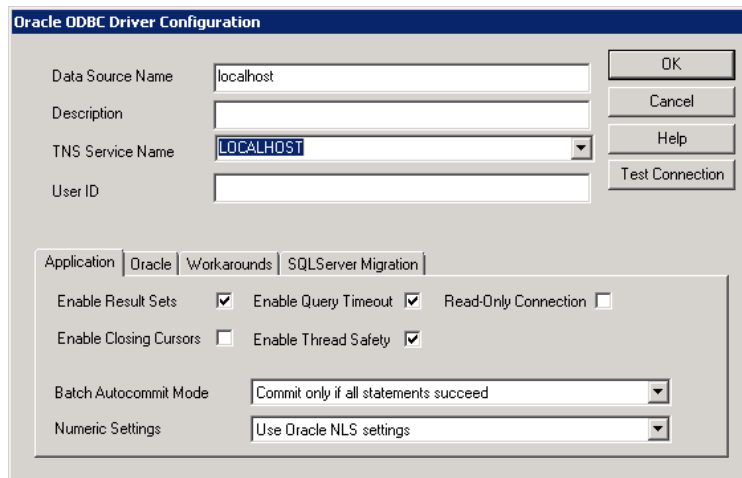


Figure 52. Oracle ODBC Driver Configuration Dialog Box

6. Click **OK** when finished to return to the **System DSN** tab on the ODBC Data Source Administrator dialog box. The new driver will be added to the System Data Source list.



If a `tnsnames.ora` error message appears when attempting to apply these configuration settings, refer to [Verifying Oracle Service Names](#) on page 179.

7. Click **OK** to exit the ODBC Data Source Administrator dialog box.

Editing the ADO Data Provider Configuration

This procedure describes how to change the `StartupMode` for the ADO data provider from `MANUAL` to `AUTOMATIC`. To edit the ADO data provider:

1. From the configuration assistant, select **Configure ADO Data Provider**, then click **Run Selected Configuration Tool**. This displays the ABB Data Service Supervision dialog box.
2. Click the plus (+) symbol next to Supervision to expand the navigation tree and show the available data providers.
3. Select the ADO data provider as shown in [Figure 53](#).

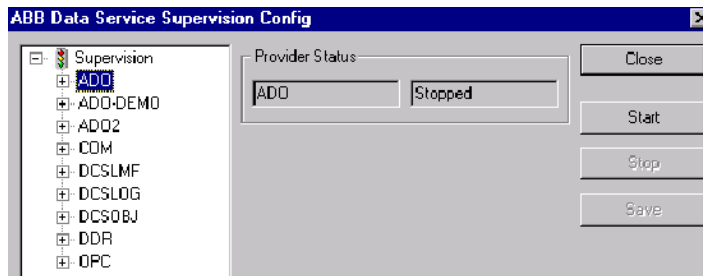


Figure 53. Selecting the Existing ADO Data Provider



The data provider must be stopped to configure its attributes. This is the default state. If the data provider is started, click **Stop** to stop the data provider.

4. Click the plus (+) symbol next to the ADO data provider to show the data provider attributes.
5. Select the `StartupMode` for this data provider.

- Set the Argument Value field to **AUTOMATIC**, as shown in Figure 54.

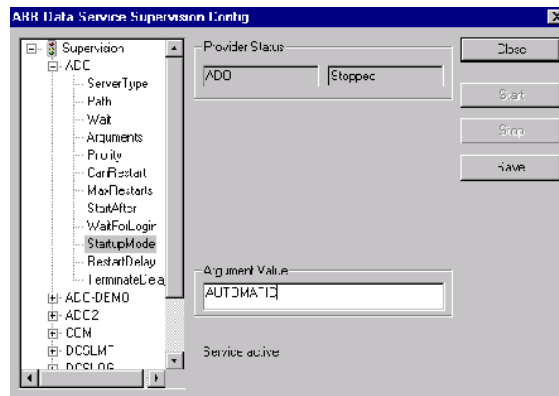


Figure 54. Changing StartupMode to Automatic

- Click **Save** to save the changes.
- To start the ADO data provider, select it and click **Start**.
- Click **Close** to exit this dialog box.



The ADO-DEMO data provider supports demonstration displays. This data provider may be stopped, and its StartupMode may be changed to **MANUAL**, if the demonstration displays are not being used.

Defining the Users

Click **Run Selected Configuration Tool**, the two windows are displayed. Use the windows explorer to locate the default users profiles folder (UserExamples) and the folder to define the users (Data). CreatePassword window is used to encrypt the password for the new users. Refer to the *System 800xA Information Management Configuration (3BUF001092*)* for the information about creating the correct types of users.

Configuring the Default ACC Users

Select a AID user and configure the default user for ACC.

Oracle Connection for Reports

Reports should use a connection to Oracle using a remote ODBC connection in the Oracle database. The numericlog and genericda public synonyms within the Oracle instance can then be used to access the ODA software. This is done by creating a new ODBC data source on the **System DSN** tab of the ODBC Data Source Administrator (in the Administrative Tools). The report will then use this data source instead of connecting to the Database1 source on the Information Management node.

Adding ABB Inc. as a Trusted Publisher in Excel

ABB Inc. must be added as a Trusted Publisher in Microsoft Excel the first time an Information Management application that runs in Excel is used. This includes DataDirect, the Archive Import Tool, and all Bulk Data Tools.

When a Macro Security Alert appears in the Excel bar:

1. Use the Macro Security Alert to launch the Microsoft Office Security Options dialog box (Figure 55).

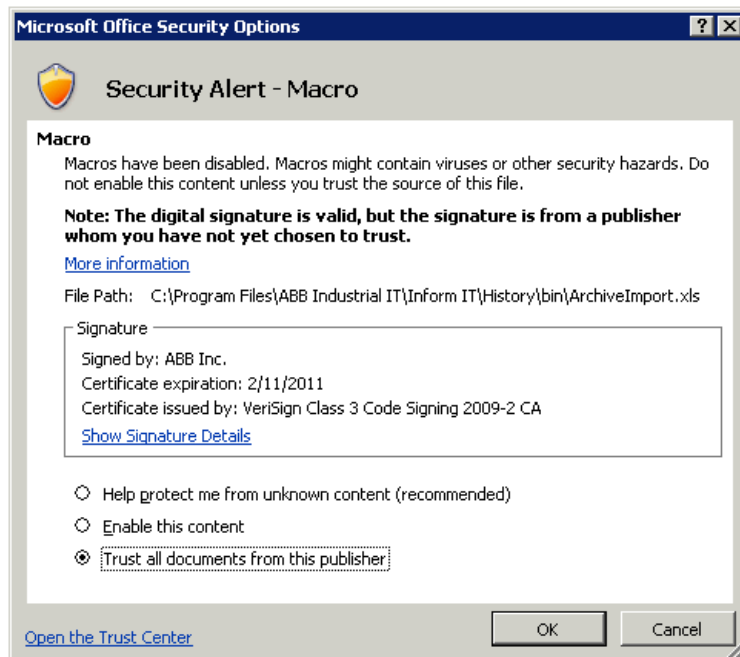


Figure 55. Accepting ABB Inc. as a Trusted Publisher

2. Select **Trust all documents from this publisher** and click **OK**.
3. After making this setting, any other documents digitally signed by ABB Inc. will run without the Macro Security Alert appearing in the Excel bar.

Troubleshooting Oracle

The following information addresses errors that may occur while setting up Oracle.

Database Instance Errors

This section describes the error messages that may be encountered while creating a History database instance, and provides guidelines for correcting the error.

Drive Space Configured Incorrectly

If the message shown in [Figure 56](#) appears, the current drive space configuration can not support the tablespace required by the database instance. This may occur even though the total space allocated exceeds the minimum disk space requirement. This is because one or more tablespaces are too large to fit on any of the drives where space is allocated.

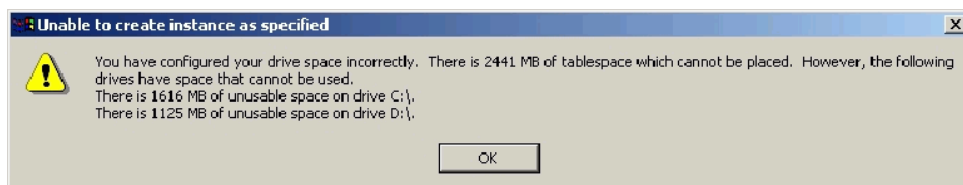


Figure 56. Drive Space Configured Incorrectly Message

When this occurs, first try to change the disk space configuration. If this is not possible, go back to the Instance Sizing dialog box, and change one or more log specifications to reduce the disk space requirements.

Available Diskspace Changes Before Running the Wizard

If the message shown in [Figure 57](#) appears, it is probable that the available disk space changed between the time when it was configured, and the time an attempt was made to run the wizard. For example, a file may have been unzipped that

consumed a large amount of disk space. When this occurs, return to the wizard, drop the current database instance, and create a new instance.

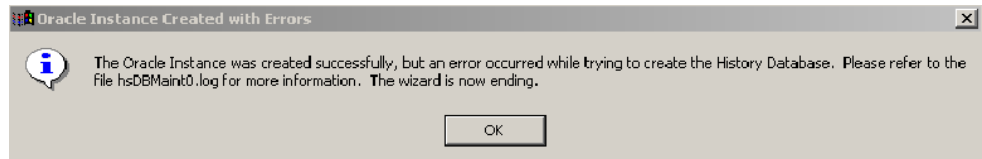


Figure 57. Available Disk Space Changed Message

Insufficient Space for Oracle System Files

The drive where the Oracle software is installed requires a certain amount of disk space for system files. The message shown in [Figure 58](#) appears when the drive where Oracle is installed does not have enough disk space allocated (311 MB minimum is required). When this occurs, re-allocate disk space to support the system files on that drive.

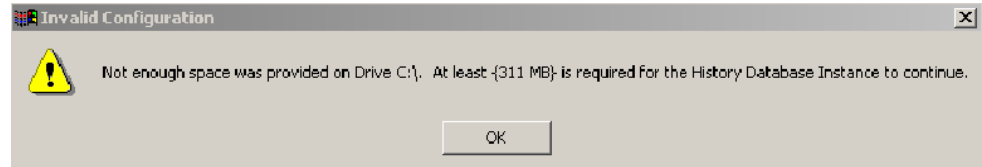


Figure 58. Insufficient Space For Oracle System Files

Verifying Oracle Service Names

Under normal circumstances, Oracle software is installed after the Information Management Server has been added to a domain. Oracle detects that the node belongs to a domain, adds a line with the domain name to the sqlnet.ora file, and appends the domain name to all service names defined in the tnsnames.ora file.

If for some reason Oracle is installed before the node is added to a domain, the domain name will not be entered into the sqlnet.ora file. The HSEH service name (created during Information Management software installation), and the LOCALHOST service name (created as a post installation step) will have the

domain name appended. This will create a mismatch between these service names and sqlnet.ora file, and cause these service names to fail.

To correct this condition, enter the domain name in the sqlnet.ora file and update any names in the tnsnames.ora file that do not have the domain name extension.

1. Use Windows Explorer to locate and open the sqlnet.ora file. The path is:

C:\oracle\product\11.2.0\db_1\NETWORK\ADMIN

2. Open the sqlnet.ora file with a text editor and add the following line (Figure 59):

NAMES.DEFAULT_DOMAIN = domainName

for example:

NAMES.DEFAULT_DOMAIN = pttdomain.us.abb.com

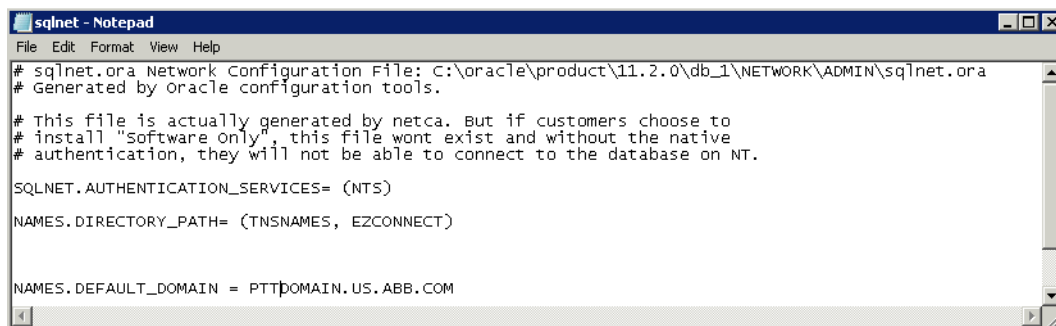
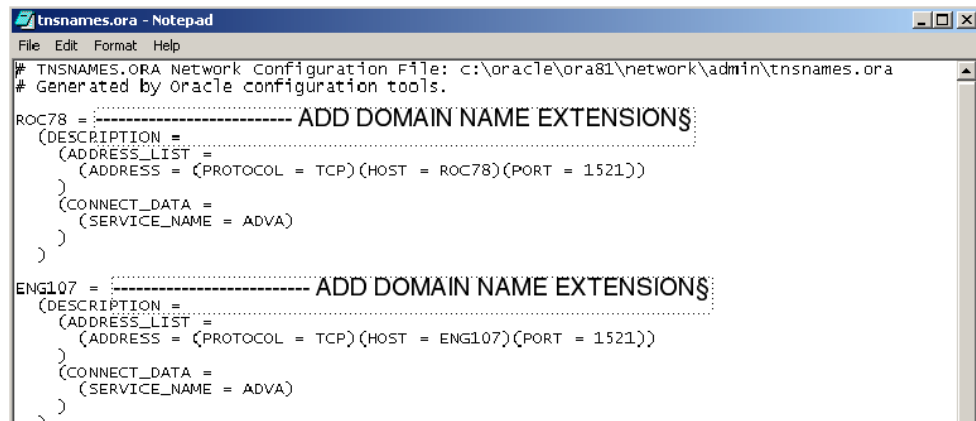


Figure 59. Editing the sqlnet.ora File

3. Save the file when complete.

4. Open the tnsnames.ora file with the text editor and add the domain name extension to all service names (Figure 60).



```
tnsnames.ora - Notepad
File Edit Format Help
# TNSNAMES.ORA Network Configuration File: c:\oracle\ora81\network\admin\tnsnames.ora
# Generated by Oracle configuration tools.

ROC78 = ----- ADD DOMAIN NAME EXTENSIONS:
(DESCRIPTION =
  (ADDRESS_LIST =
    (ADDRESS = (PROTOCOL = TCP)(HOST = ROC78)(PORT = 1521))
  )
  (CONNECT_DATA =
    (SERVICE_NAME = ADVA)
  )
)

ENGL07 = ----- ADD DOMAIN NAME EXTENSIONS:
(DESCRIPTION =
  (ADDRESS_LIST =
    (ADDRESS = (PROTOCOL = TCP)(HOST = ENGL07)(PORT = 1521))
  )
  (CONNECT_DATA =
    (SERVICE_NAME = ADVA)
  )
)
```

Figure 60. Editing the tnsnames.ora File

5. Save the file when complete.



If using a workgroup rather than a domain, do not add the domain name where indicated in Figure 60. Also, the domain following localhost (PTTDOMAIN.US.ABB.COM) in Figure 60 will not appear.

Information Management Profiles Client Post Installation

The Profiles Client application runs independent of the Information Management System Services or 800xA System software. To access the Information Management Server, all profile clients nodes can be in the same domain as the Information Management Server and then no post installation changes are required. However, to access the Information Management Server from a node outside the domain/workgroup that the Information Management Server is part of, the following steps must be performed (Windows Server 2008 and Windows 7 have the same dcomcnfg views):

1. Start dcomcnfg. Use **Start > Run** and enter **dcomcnfg**.
2. Go to and expand Windows Component Services.

3. Right-click **My Computer** and select **Properties** from the context menu.
4. Select the **COM Security** tab.
5. Select **Edit Limits for Launch and Activation Permissions**.
6. Set the **Remote Activation Permissions for the Everyone user** to **Allow** and then select **OK** as required to close the setup windows.

It is also necessary to create the 800xA Service User account on the Profiles Client. The 800xA Service User account name can be found on the Domain controller. Verify that the name is the same case and the passwords are identical.

Section 20 Batch Management

Introduction

This section provides post installation procedures for Batch Management.

Batch Management System Service Definitions

To define the Primary Batch Server to the Batch service:

1. Open a Plant Explorer Workplace on any Batch node.
2. Use the Structure Selector to open the **Service Structure**.
3. Use the Object Browser to navigate to and select:
`Services > Batch Service, Service`
4. Right-click `Batch Service, Service` and select **New Object** from the context menu.
5. The New Object dialog box appears. Select `Service Group`, enter a name, and click **Create**.
6. Right-click the newly created Service Group object and select **New Object** from the context menu.
7. The New Object dialog box appears. Select `Service Provider`, enter a name, and click **Create**.



Use a unique name (Batch Primary for example) for this Service Provider so that it can be easily recognized in the System Status Viewer dialog box.

8. Select the **Configuration** tab of the Service Provider Definition aspect.

9. Select the name of the Primary Batch Server node in the Node field and click **Apply**. Refer to [Figure 61](#).

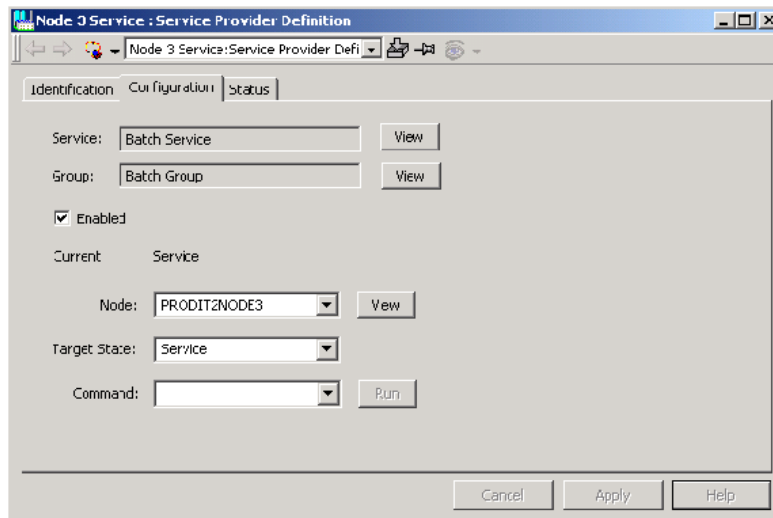


Figure 61. Service Provider Definition Dialog Box

10. Wait until the Primary Batch Server node is in primary mode by viewing a P in the Windows Taskbar of the selected Primary Batch Server. The length of time for the P icon to appear depends on the size of configuration (number of batch units) and the number of nodes in a system. There is generally no configuration in the system at this point, so the P icon should appear in under three minutes.



This step will normally complete in less than three minutes; however, it may take up to 10 minutes when restoring or upgrading a large system.

11. Use the Object Browser to navigate to and select:
 Services > EventCollector, Service
12. Right-click EventCollector, Service and select **New Object** from the context menu.
13. The New Object dialog box appears. Select Service Group, enter a name, and click **Create**.

14. Right-click the newly created Service Group object and select **New Object** from the context menu.

15. The New Object dialog box appears. Select `Service Provider`, enter a name, and click **Create**.



Use a unique name (Batch EC Primary for example) for this Service Provider so that it can be easily recognized in the System Status Viewer window.

16. Select `Service Group Provider` in the Aspect List Area for the Service Provider object.

17. Select the name of the Primary Batch Server node in the Node field and click **Apply**.

18. Select the EventCollector Service Group object created in [Step 12](#) and [Step 13](#).

19. Select `Service Group Definition` in the Aspect List Area for the EventCollector Service Group object.

20. Select the **Special Configuration** tab in the Preview Area.

21. Select `Produce IT Batch OPC AE Server` in the OPC A&E Server area of the dialog box. This will insert Produce IT Batch OPC AE Server in the Collection Definition field.

22. Click **Apply and Upload**.

To define the Secondary Batch Servers to the Batch service:

1. Navigate to the Batch Service group object (created when defining the Primary Batch Server to the Batch service).

2. Right-click and select **New Object** from the context menu.

3. The New Object dialog box appears. Select `Service Provider` and enter a name.



Use a unique name (Batch Secondary for example) for this Service Provider so that it can be easily recognized in the System Status Viewer window.

4. Select `Service Provider Definition` in the Aspect List Area for the Service Provider object.

5. Select the **Configuration** tab in the Preview Area.

6. Select the name of the Secondary Batch Server node in the Node field and click **Apply**.
7. Wait until the Secondary Batch Server node is in secondary mode by viewing an S in the Windows Taskbar of the selected Secondary Batch Server. The length of time for the S icon to appear depends on the size of configuration (number of batch units) and the number of nodes in a system. There is generally no configuration in the system at this point, so the S icon should appear in under five minutes.



This step will normally complete in less than five minutes; however, it may take up to 15 minutes when restoring or upgrading a large system.

8. Navigate to the EventCollector Service group object created when defining the Primary Alarm and Event Server to the Batch service.
9. Right-click and select **New Object** from the context menu.
10. The New Object dialog box appears. Select `Service Provider` and enter a name.



Use a unique name (Batch EC Secondary for example) for this Service Provider so that it can be easily recognized in the System Status Viewer window.

11. Select `Service Provider Definition` in the Aspect List Area for the Service Provider object.
12. Select the **Configuration** tab in the Preview Area.
13. Select the name of the Secondary Batch Server node in the Node field and click **Apply**.

Shutdown Script

The batch_shutdown.bat script shuts down the Batch application properly and must be installed on all Batch Servers. To install this script:

1. Select:

Start > Run

from the Windows Taskbar.

2. Enter:

`gpedit.msc`

in the Run dialog box and click **OK**.

3. Select:

Computer Configuration > Windows Settings > Scripts
(Startup/Shutdown).

4. Double-click Shutdown.
5. Click **Add** and then **Browse**.
6. Select:

...\Program Files\ABB Industrial IT\Produce
IT\Batch\bin\batch_shutdown.bat

in the Script Name field and click **Open**.

7. Click **OK** twice to complete the installation and close the Group Policy dialog box.

Print BMA Report Configuration

In order to print a BMA report, the Batch application must be configured (refer to *System 800xA Batch Management Configuration (3BUA000146*)*) and the AT Service Account must be configured to use the settings of a certain account. All print requests for a BMA report from any user will use the settings from this account to print the report.

To configure the AT Service Account:

1. Select:

Start > All Programs > ABB Industrial IT 800xA > System > Configuration Wizard.

2. Double-click Systems Software User Settings.
3. Record the user account name listed in the Service Account, Used by System Software field and exit the Configuration Wizard.
4. Use standard Windows procedures to access Task Scheduler via Windows Control Panel > Administrative Tools.

5. Select **Action > AT Service Account Configuration** from the menu bar.
6. Select **Another User Account:** and click **Change User...**
7. Enter the user account name recorded earlier in this procedure.
8. Enter the password for the account in the Password field and click **OK** twice.
9. Log in as the user recorded earlier in this procedure and configure a default printer.
10. Create the following folder on all Batch Server nodes:

C:\Windows\System32\config\systemprofile\Desktop

Batch Management Toolbar

Batch Management provides a Toolbar that contains buttons for the Batch Overview, Batch History Overview, and Equipment Overview dialog boxes. If desired, refer to *System 800xA Batch Management Configuration (3BUA000146*)* for information about enabling this Toolbar.

Using Batch Management Advanced Templates Only

In some scenarios, it may be a requirement to use the advanced control modules provided by Batch Management without running Batch procedures from a Batch Server. To use the advanced control modules in this way:

1. Install a Batch Client on all nodes.
2. Load the Batch and Batch Advanced Templates extensions on the Primary Aspect Server using the 800xA System Configuration Wizard.

Setting the Date Format for Batch Auto ID for Automatic Scheduling

Perform the following procedure on all Batch Server nodes if using Batch Auto ID for Automatic Scheduling. Do not change any of the settings that were made while setting up Windows before installing the 800xA System.

1. Log off the 800xA Installing User account.

2. Log into the 800xA Service account.
3. Open Windows Control Panel.
4. Double-click **Regional and Language Options** to launch the Regional and Language Options dialog box.
5. Click **Customize this format** to launch the Customize Regional Options dialog box.
6. Click the **Date** tab.
7. Change the value in the **Short date** drop-down list to `MM/dd/yyyy` and click **Apply**.
8. Log off of the 800xA Service User account.
9. Log onto the 800xA Installing User account.

Setting the SQL Server Maximum Server Memory Limit

Perform the following procedure on all Batch Servers in the 800xA System.

1. Use the SQL Server Management Studio to connect to the `BATCH_INSTANCE`.
2. Right-click **BATCH_INSTANCE** and select **Properties** from the context menu.
3. Select the Memory Settings in the Server Properties dialog.
4. Change the Maximum Server Memory (in MB) field to be equal to 25 percent of the physical RAM of the Batch Server.

Section 21 TRIO Integration

Introduction

This section describes procedures related to TRIO Integration.



The AC 800M software must be installed and the AC 800M Connect system extension must be loaded prior to loading the TRIO Integration system extension.

Install TRIO Integration Software

Run the Installation Wizard for TRIO Integration on all nodes that have Control Builder M installed as follows:

1. Insert System Installation DVD 1 into the drive. The Installation AUTORUN screen will appear.
2. Select:

Manual Installation > Additional Products > TRIO Select Additional Products > TRIO

3. Follow the Installation Wizard to complete the installation.

Loading the TRIO Integration System Extension



Hardware definition files for TRIO Integration are loaded with its system extension. The CI862 TRIO Interface will be present if it is properly loaded.

Refer to [Loading System Extensions](#) on page 27 and follow the procedure for using the Configuration Wizard to load the TRIO Integration system extension.

Inserting the Hardware Library

The hardware library for TRIO Integration must be manually inserted onto each Control Builder project that uses TRIO Integration.

Use Control Builder to install the hardware library for TRIO Integration as follows:

1. Open a Plant Explorer Workplace.
2. Open or create a Control Builder project.
3. Select **Library > Hardware**.
4. Right-click **Hardware > Insert Library** and select the **CI862TRIOHwLib** library from the context menu.
5. Click **Insert**.
6. Select **OK** to insert the hardware definition files. Control Builder will read the files.

Adding a CI862 TRIO Interface

Use Control Builder to add a CI862 TRIO Interface to the AC 800M hardware tree as follows:

1. Open a Plant Explorer Workplace.
2. Open or create a Control Builder project.
3. Open the associated controller and select **Hardware, AC 800M**.
4. Right-click and select **New Unit > CI862** from the context menu.
5. Use the hardware editor and add I/O units after adding the CI862 TRIO Interface (if required).

Loading Firmware

Use Control Builder to ensure that the latest firmware is installed on the controller and the CI862 TRIO Interface as follows:

1. Open a Plant Explorer Workplace.

2. Open or create a Control Builder project.
3. Select **Tools > Maintenance > Remote System**.
4. Click **Show Remote Systems**.
5. Select the remote system IP address for the selected controller and click **OK**.
6. Click **Show Firmware Information**. The dialog box will show the current version and what is available on disk.
7. Select the **download** check box for the new version of hardware.
8. Click **Download Firmware for selected Units** and click **Continue** when prompted.
9. Click **OK**.

Section 22 Multisystem Integration

Introduction

This section describes post installation procedures for the Multisystem Integration software. Before the Multisystem Integration functionality can be used, it must be configured both in the Provider and the Subscriber Systems. The configuration is performed in three steps:

1. Creation and configuration of the [Remote Access Server](#).
2. Creation and configuration of the [Remote Access Client](#).
3. Upload of the Provider objects and structures via the [Uploading a Configuration](#) aspect.

The configuration of the Remote Access Server in the Provider System must match the configuration of the Remote Access Client in the Subscriber System.

The information to configure includes:

- **TCP/IP addresses for all nodes:** mandatory.
- **Password:** recommended but not mandatory.
- **Windows domain users or user mapping:** mandatory.

It is possible to use redundant configurations for the Remote Access Server and the Remote Access Client. Refer to [Redundant Configurations](#) on page 210.

Remote Access Server

The 800xA System to be supervised is called the Provider System, since it provides the Supervisor System with data. The Supervisor System is called the Subscriber, since it subscribes to values from the Provider System.

All engineering and configuration of the Provider System is done locally in the Provider System.

Creating a Remote Access Server

1. Start the Configuration Wizard.
2. Select:
Start > All Programs > ABB Industrial IT 800xA > System > Configuration Wizard
3. Open the Add Remote Access Server dialog box (Figure 62) by going to:
System Administration > Select System > Remote Access Server

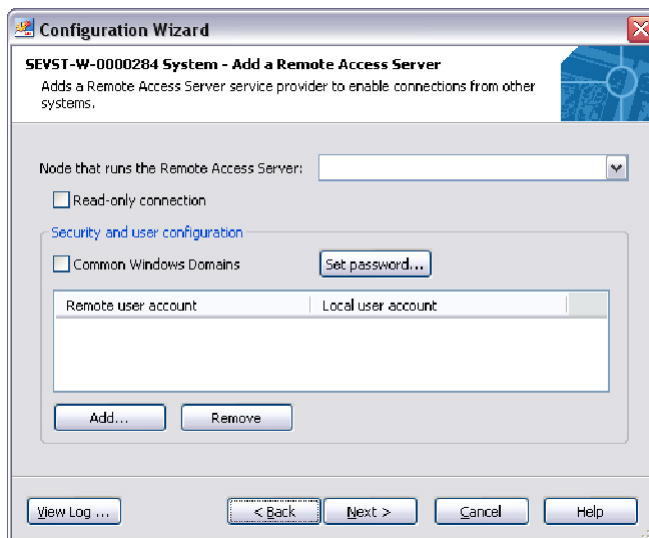


Figure 62. Remote Access Server Dialog Box

4. Use this dialog box to configure the following:
 - Node to run the Remote Access Server Service Provider.
 - Whether or not the connected clients will get a read-only connection.

- Whether or not the Remote Access Server and Client are running in the same Windows domain.
- If the Provider and Subscriber are running in different Windows domains user mapping must be set up.
- A password required to connect to the Remote Access Server is highly recommended.

Node Configuration

The recommendation of the node to run the Remote Access Server service differs depending on the size of the system.

The Remote Access Server can run in the same node as the Connectivity and Aspect Servers for a small configuration with a few hundred I/O signals. It is recommended to not run a Workplace on the same node.

It is recommended to run the Remote Access Server in the Connectivity Server node for a medium/large configuration.

Combinations of these 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.

Select the desired node from the drop-down list box in the Remote Access Server dialog box.

Read-Only System

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

A read-only connection is a good choice if the system will only be supervised and it will not be possible to control anything from a remote client.

User Mapping

There are two choices to configure the users depending on whether or not the users in the Subscriber and the Provider Systems belong to the same Windows domain.

If the users in the Subscriber System and Provider System belong to the same Windows domain, select the **Common Windows Domains** check box.



Selecting the **Common Windows Domains** check box requires that the users in the Subscriber System also exist in the Provider System.

User mapping must be performed between users in the Subscriber System (Remote Access Client) and users in the Provider System (Remote Access Server if the Remote Access Server and Client are in different domains).

1. Click **Add...** in the Remote Access Server dialog box and the Set user mapping dialog box appears as shown in [Figure 63](#).



Figure 63. Set User Mapping Dialog Box

2. Input the Windows account name, including the domain, for the Subscriber System in the Remote user account field.
3. Select a Windows account to map to on the Provider System in the Local user account field.

If the remote user is a node local user (not a domain user), the Remote Access Client node IP address must be inserted before the user account on the Subscriber node. For example, the local user **Operator** on the Subscriber 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 the 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 otherwise opens up a system for writing from all accounts in the Subscriber System.

The Security Report in the Provider System is extended to document the user mapping performed for the Remote Access Server.

Password Configuration

It is recommended, but not mandatory, to configure a password for the Remote Access Server. The selected password must also be provided when the Remote Access Client is configured. Refer to [Advanced Configuration](#) on page 199.

1. To configure the password, click **Set Password....** The Set password dialog box appears.
2. Enter the password in the Password field.
3. Enter the password again in the Confirm Password field and click **OK**.

Advanced Configuration

There are two more configurations that can be performed for the Remote Access Server, but they must be performed from 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.
1. Open a Plant Explorer Workplace.
 2. Use the Structure Selector to open the **Service Structure**.
 3. Use the Object Browser to navigate to:
Services/Remote Access Server/Basic, Service Group
 4. Select Service Group Definition in the Aspect List Area.
 5. Select the **Special Configuration** tab in the Preview Area.

6. To specify the port number to use, enter the port number in the Port to use: field. The default port, if not specified, is 3340.



Be sure the port selected is free to use. Consult the TCP/IP documentation for details.



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

7. To encrypt all messages between the Remote Access Server and the Remote Access Client select the **Encrypt traffic** check box.



Selecting the **Encrypt traffic** check box will result in a small performance decrease. The encryption function is available only if a password is set for the Remote Access Server.

8. If a user who does not belong to the Administrators user group wants to change the password (via **Set Password...**), the old password must be entered before a new password is accepted.
 - a. Enter the old password in the Current password field.
 - b. Enter the new password in the New password field.
 - c. Enter the new password again in the Confirm new password field and click **OK**.

Remote Access Client

The Remote Access Client service communicates with the Remote Access Server, but resides on the Subscriber System. There is always a one-to-one relationship 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.



Each Remote Access Client requires one license to run without warnings.

Creating 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**.

To create a Remote System object:

1. Open a Plant Explorer Workplace.
2. Use the Structure Selector to select the **Control Structure**.
3. Use the Object Browser to navigate to and right-click `Root Domain` and select **New Object** from the context menu.
4. Select `Remote System` in the list on the left.
5. Enter a name in the Name field. This name will be presented in proxy objects, faceplates, process displays, alarm lists, trends, and history logs.
6. Click **Next** and the Additional Arguments dialog box shown in [Figure 64](#) appears.

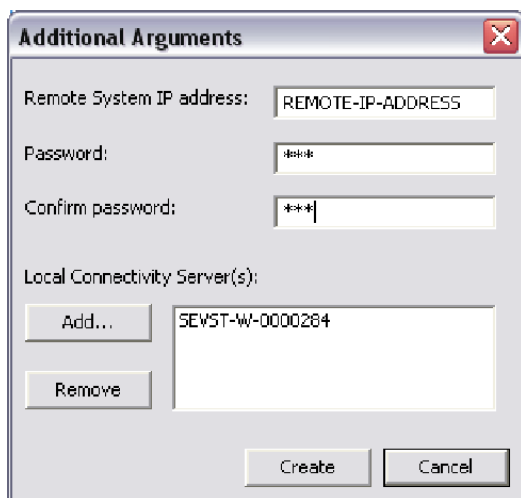


Figure 64. Additional Arguments Dialog Box

7. Enter the Remote System IP address. This can be either a name of the node running the Remote Access Server, or a numeric IP address.



The node name can only be used if the Provider and Subscriber System share a common DNS Server.

8. Enter and confirm the password in the Password and Confirm Password fields.



The password specified must match the password given for the Remote Access Server of the Provider configured with the Configuration Wizard. The password is case sensitive.

9. Configure the node where the service should be running in the Local Connectivity Server(s) field. It is possible to add more than one node if a redundant solution is desired.
10. Click **Create** when complete.

Advanced Configuration

The configuration of the Remote Access Client can be changed after the Remote System object is created.

1. Open a Plant Explorer Workplace.
2. Use the Structure Selector to select the **Service Structure**.
3. Use the Object Browser to navigate to:
`Services/Remote Access Client/Basic, Service Group`
4. Select `Service Group Definition` in the Aspect List Area.
5. Select the **Special Configuration** tab in the Preview Area. This dialog box makes it possible to change the password, number of stored upload logs, port number to use when connecting to the Remote Access Server, and limit the bandwidth allowed to be used for the Provider System.
6. Make sure that the port used for the Remote Access Client matches the port specified for the Remote Access Server, and that all firewalls are configured to open the selected port. The default port number is 3340.
7. The bandwidth limitation can be very useful, if the physical connection to a Remote Access Server has high bandwidth, but the Subscriber System should have limited impact on the load of the Provider System. An example of usage is

information presentation where update rates can be low. Bandwidth limitation should be combined with Subscription control. Refer to *Industrial IT, 800xA - System, Administration and Security (3BSE037410Rxxx)* for more information.

Uploading a 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 performed through an upload operation.

Before the upload operation can start, the part of the Provider System to be uploaded must be specified. This configuration is performed in the **Upload Configuration** tab of the Remote System object.

1. Select the System Connection aspect of the previously created Remote System object in the Aspect List Area.
2. Select the **Upload Configuration** tab in the Preview Area to produce the view shown in [Figure 65](#). After an upload is performed, this view will show 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 <No data> is shown the communication towards the Provider is down.

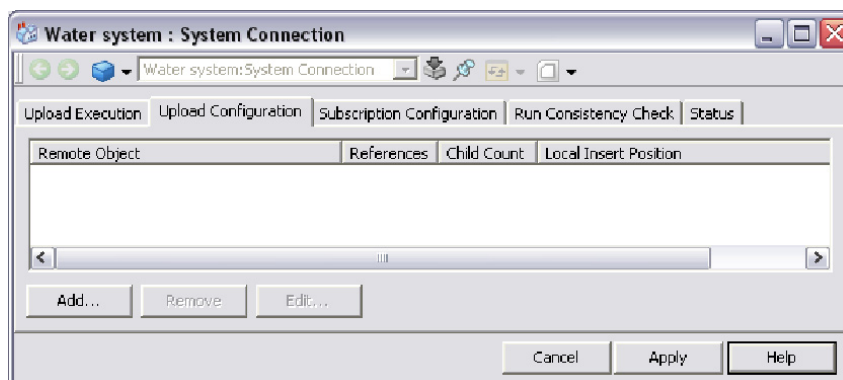


Figure 65. Upload Configuration Tab Before Upload

3. Click **Add...** to add a new object or structure from the Provider. This produces an Upload Configuration dialog box similar to the one shown in [Figure 66](#).



Try to limit the upload to the objects needed to supervise and operate the Provider System.

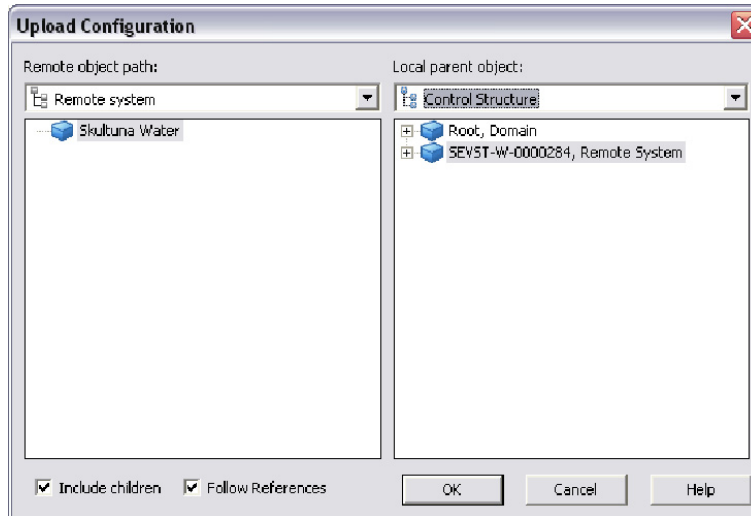


Figure 66. Upload Configuration Dialog Box

- a. Select the desired structure/object from the Provider System in the Remote object path pane.
- b. To include the children of the selected object in the upload, select the **Include Children** check box. If not, clear the check box.
- c. To include objects needed by an uploaded aspect in the upload, select the **Follow References** check box. If not, clear the check box. Selecting the check box means that faceplate elements and Display Elements will be included when Faceplates and Graphic Displays are uploaded.

- d. The Include Children and Follow References configuration is shown in the **Upload Configuration** tab after an upload (Figure 67).

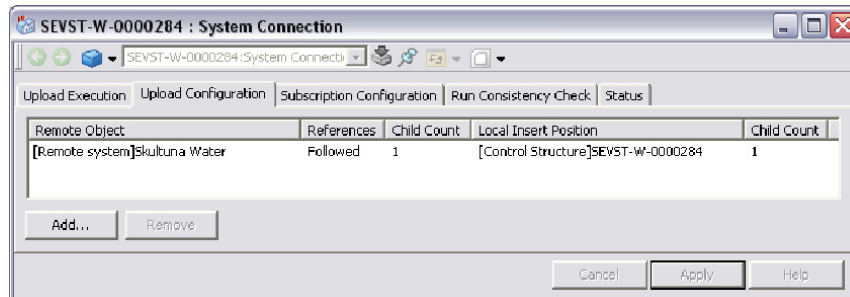


Figure 67. Upload Configuration Tab After Upload

4. The Local parent object pane makes it possible to upload to a structure other than the structure selected in the Provider System. If the 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.
5. The aspect categories to upload are specified in the Aspect Category Definition aspect. Use the Structure Selector to open the **Aspect System Structure** and select the desired aspect category.



It is possible to incrementally add more and more objects/structures to an upload configuration and run upload several times.

6. There are two ways to treat an aspect category when it is uploaded:
 - **Ignore at upload:** The aspect is not uploaded to the Subscriber System. This is 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.



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.

Running Upload

An 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 will get a new object identity. This allows upload from several Provider Systems containing exactly the same configuration. Aspect 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 performed from the **Upload Execution** tab on the System Connection aspect found on the Remote System object (Figure 68).

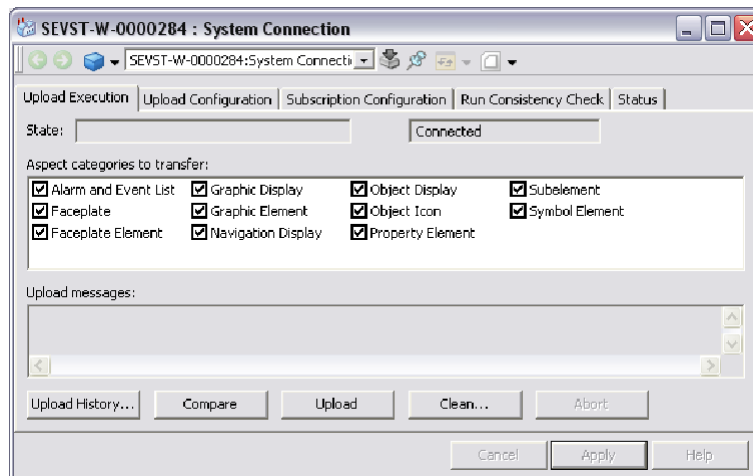


Figure 68. Upload Execution Tab

1. If the State field on the right shows **Connected** it is possible to start an upload by clicking **Upload**. The State field on the left will then show that an upload is running. The progress of the upload can be followed in the upload messages frame.
2. The list of aspect categories shown in the Aspect Categories to transfer frame are aspects with the **Copy at upload** check box selected. However, it is possible to override the configuration by clearing the aspect category in the list. Clearing an aspect category means it will not be uploaded.

All aspects with OPC properties, log configurations, and log templates will also be uploaded unless the **Ignore at upload** check box is selected on the aspect category.

3. The upload execution is running in the Remote Access Client and will continue even if the Plant Explorer Workplace is closed. To abort an ongoing upload, click **Abort**.



Interrupting an upload can make the uploaded proxies inconsistent and as a result, they will not work properly.

4. After an upload is complete the result can be viewed either in the Upload Messages dialog box or in the Upload History Viewer. To view a saved upload log, click **Upload History**. An Upload History Viewer will open.
5. Click on the desired log in the Select log to view frame. The log will then be shown in the lower portion of the frame. The number of logs stored is configured in the Remote Access Client, **Special Configuration** tab (refer to [Advanced Configuration](#) on page 202).
6. The **Upload Configuration** tab ([Figure 67](#)) shows how the upload is configured. The References field will show `Followed` if the **Follow References** check box was selected in the Upload Configuration dialog box ([Figure 66](#)). The Child Count will show the number of children uploaded if the **Include Children** check box was selected in the Upload Configuration dialog box. If it was cleared, this field shows a dash.
7. Changes in the Provider System will not automatically be uploaded to the Subscriber System. However, the Compare function makes it possible to see if there are any changes in the Provider compared to the state in the Subscriber. Clicking **Compare** (under the **Upload Execution** tab) starts a comparison and creates a compare log that is viewable in the Upload Messages dialog box and the Upload History Viewer.
8. Clicking **Clean** (under the **Upload Execution** tab) removes all proxy objects and aspects uploaded for the system represented by the Remote System object. After clicking **Clean**, a dialog box appears asking:

Do you want to remove all uploaded proxy objects for this system connection?

Click **Yes** to confirm the cleaning or **No** to abort.



A new upload must be performed in order to be able to control the Provider System after a clean has been performed.

9. The System Connection aspect also has a **Run Consistency Check** tab (Figure 69). The consistency check can detect problems, like dangling references in object types, process displays and faceplates, etc.

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

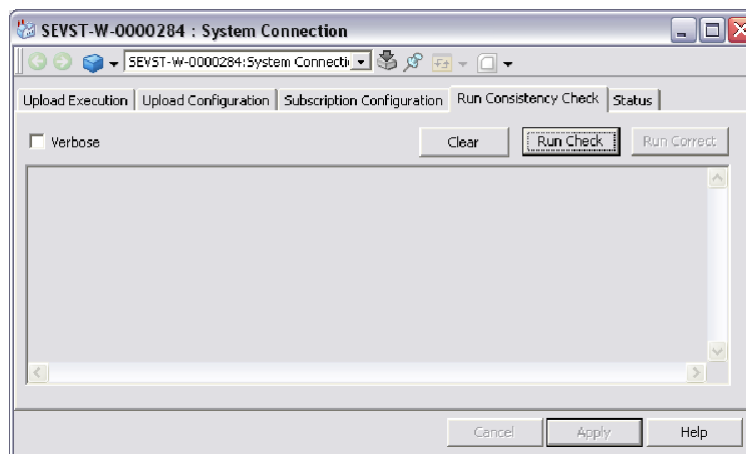


Figure 69. Run Consistency Check Tab

Proxy Objects

The Proxy objects created in the Subscriber System are not copies of the objects uploaded from the Provider System. Aspects presenting OPC properties are replaced with a Proxy aspect, and a Remote Object Info aspect is added.

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.

Proxy Control Connection

A Proxy Control Connection aspect is created on the Proxy object for all aspects, not marked as Ignore at upload in the Aspect Category Definition aspect, in the remote system that defines OPC properties. 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 these aspects. All changes have to be performed in the Provider System, and uploaded again.

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.

Redundant Configurations

It is possible to use redundant configurations for the Remote Access Server and the Remote Access Client. There may be redundancy in one of the ends or in both ends, depending on the desired availability.

A redundant solution, independent of where it is (Server or Client), should use a redundant communication network, since communication failure is probably the most common cause of a failure.

Redundant Remote Access Client

A redundant Remote Access Client can be created directly when the Remote System object is created, or it can be added later from the **Service Structure**.

1. To configure the Remote Access Client services to be redundant when the Remote System object is created, add more than one node in the Additional

Arguments dialog box (Figure 64). Up to three Remote Access Clients can be configured.

2. To configure the Remote Access Client services to be redundant after the Remote System object has been created:
 - a. Open a Plant Explorer Workplace.
 - b. Use the Structure Selector to open the **Service Structure**.
 - c. Use the Object Browser to navigate to the Remote Access Client Service Group object.
 - d. Create a new Service Provider and let it execute on a different node than the Provider created when the Remote Access object was created.
 - e. This new Service Provider will use the configuration in the **Special Configuration** tab on the Remote Access Client Service Group.

Redundant Remote Access Server

Redundant Remote Access Server services can only be configured after the first Remote Access Server is created using the Configuration Wizard.

To create a redundant Remote Access Server:

1. Open a Plant Explorer Workplace.
2. Use the Structure Selector to open the **Service Structure**.
3. Use the Object Browser to navigate to the Remote Access Server Service Group object.
4. Create a new Service Provider and configure it to run on a different node than the Provider created when the Remote Access object was created.
5. Verify that the nodes running the Remote Access Services use different or redundant communication lines towards the Remote Access Clients.
6. The Remote Access Client must also be configured in order to use the redundant services. On the system running the Remote Access Client:
 - a. Open a Plant Explorer Workplace.
 - b. Use the Structure Selector to open the **Service Structure**.

- c. Use the Object Browser to select the Remote System object representing the remote system.
- d. Select the System Connection aspect in the Aspect List Area.
- e. Select the **Status** tab in the Preview Area.



It is also possible to go to the **Service Structure** and select the Services/Remote Access Client/Service Group object, but it may be harder to find the correct Service Group if there are several Remote Access Client Groups.

- f. Click **View Group** to launch the Remote Access Client service group configuration aspect.
- g. Select the **Special Configuration** tab.
- h. The redundant Remote Access Server nodes should be listed in the Communication frame. Up to three redundant nodes can be specified.



All Remote Access Server services must have the same password configured.

Dual Remote Access Redundancy

It is possible to use redundancy on both the client and the server side, by combining the Remote Access Client and Remote Access Server configurations described in the previous two topics.

Redundant Remote History Service

Configuration of a redundant remote history service must be performed manually.

1. Open a Plant Explorer Workplace.
2. Use the Structure Selector to open the **Service Structure**.
3. Create a new history Service Provider object under the service group assigned for the Provider System.
4. Set the execution node to the redundant node.

Redundant Remote Alarm and Event Service

The Event Collector Service that handles alarm subscription from the Provider System can be redundant. A redundant Event Collector Service is created automatically when a redundant node is added; however, if a Remote System object is added afterwards, this configuration must be made manually.

1. Open a Plant Explorer Workplace.
2. Use the Structure Selector to open the **Service Structure**.
3. Create a new Service Provider object under the Service Group assigned for the Provider System.
4. Set the execution node to the redundant node.

Section 23 Windows Firewall Configuration

Introduction



The Windows Firewall Configuration procedure must be performed every time new 800xA System software is added to the system.



This section is only to be used when using this tool as a stand-alone application. For instance, to configure Windows Firewall after manually installing the 800xA System. This tool is integrated in the System Installer and Windows Firewall will be configured as part of 800xA System automated installation.



The System Installer tools must be launched using the Automated Installation selection from the Installation AUTORUN screen. This can be done via the following:

- With System Installation DVD 1 in the drive of the node where the tools are being run.
- With the contents of System Installation DVD 1 copied locally to the node where the tools are being run.

The tools can not be run from a file server.

Windows Firewall is a protective boundary that monitors and restricts information that travels between a server or client and a network or the Internet. Therefore, some settings may need to be adjusted for some applications that need an open connection. Exceptions can be made for these applications so that they can communicate through Windows Firewall, or a port can be opened instead. A port is like a small door in the firewall that allows communications to pass through.

Configuring Windows Firewall

The Windows Firewall settings are contained in firewall configuration files (fwc). By default, programs and ports mentioned in ppa.fwc are always configured. Run the Windows Firewall Configuration Tool on every node in the 800xA System.

To configure Windows Firewall:

1. Insert System Installation DVD 1 into the drive.
2. Wait for the Installation AUTORUN screen to appear.
3. Select:

Automated Installation > System Setup Tools > Configure Windows Firewall

4. The Firewall Configuration Files Selection dialog box appears.
5. Select the check boxes for the 800xA Base System and Functional Area software that is installed on the current node and require ports to be opened and/or Windows Firewall exceptions. Click **Check All** to select all check boxes and **Uncheck All** to clear all check boxes.



Selecting check boxes for applications that are not installed on the current node will result in an error message stating that some applications are not installed on the node, and an entry will be made in the log file. This will not result in improper configuration of Windows Firewall, as long as the check boxes for the applications that are installed on the node are selected. If there is any question as to what applications are installed on the node, select **Check All** and dismiss the error message when it appears.

6. When the desired check boxes are selected, click **OK**.
7. A Windows Firewall Configuration dialog box will appear notifying whether or not the configuration succeeded or failed. When the dialog box appears, click **OK**. If the configuration failed, refer to [Common Causes of Errors](#).
8. To verify the list of applications and ports added to the firewall exception list, select:

Start > Control Panel > Windows Firewall > Exceptions

Common Causes of Errors

The most common causes of errors when configuring the Windows Firewall are:

- The Windows Firewall Service is not running on the target system. The service name is Windows Firewall/Internet Connection Sharing (ICS). Make sure this service is running on the target system and try again.
- The programs mentioned in the respective fwc files are not installed on the system. Clear the check boxes for those programs and try again.
- The fwc files provided as input to the Windows Configuration Tool are not present in the exe directory (the folder from which the exe is launched). Make sure the fwc files are in the proper directory and try again.

Log File

The Windows Configuration Tool will create a log file of the Windows Firewall configuration in a temp folder (%temp%\ ABB Industrial IT 800xA). The name of the log file is:

```
windows.config + date + time + .log.
```

Section 24 Windows Services Configuration

Introduction



This appendix is only to be used when using this tool as a stand-alone application. For instance, to configure Windows services after manually installing the 800xA System. This tool is integrated in the System Installer and Windows services will be configured as part of 800xA System automated installation.



The System Installer tools must be launched using the Automated Installation selection on the Installation AUTORUN screen. This can be done via the following:

- With System Installation DVD 1 in the drive of the node where the tools are being run.
- With the contents of System Installation DVD 1 copied locally to the node where the tools are being run.

The tools can not be run from a file server.

Configuring Windows Services hardens Windows by disabling/removing/not installing components and services that are not explicitly required by 800xA System products. It configures Windows as securely as possible while still allowing for the 800xA System software to function. Some of the services that are typically installed but not used are FTP and Telnet.

Configuring Windows Services

The Windows Services settings are contained in Windows services configuration files (swc).

To configure Windows services:

1. Insert System Installation DVD 1 into the drive.

2. Wait for the Installation AUTORUN screen to appear.
3. Select:
Automated Installation > System Setup Tools > Configure Windows Services
4. Follow the wizard to complete the configuration of Windows services.
5. A Windows Service Configuration dialog box will appear notifying whether or not the configuration succeeded or failed. When the dialog box appears, click **OK**. If the configuration failed, refer to [Common Causes of Errors](#).
6. To verify the list of services enabled and disabled by the Windows Configuration Tool, select:

Start > Control Panel > Administrative Tools > Services

Common Causes of Errors

The most common causes of errors when configuring the Windows services are:

- The services mentioned in the respective .swc files are not present on the system. Resolve the differences between the services mentioned in the .swc files and those present on the system and try again.
- The swc files provided as input to the Windows Configuration Tool are not present in the exe directory (the folder from which the exe is launched). Make sure the swc files are in the proper directory and try again.

Log File

The Windows Configuration Tool will create a log file of the Windows services configuration in a temp folder (%temp%\ ABB Industrial IT 800xA). The name of the log file is:

`windows.config + date + time + .log.`

Index

Numerics

- 800xA for AC 800M 75
 - Control Builder configuration 75
- 800xA for AC 870P/Melody 119
- 800xA for Advant Master 101
 - RTAB network settings 103
- 800xA for Harmony 107, 112, 113, 114
- 800xA for MOD 300
 - Communications settings 125

A

- ABBResults directory share 57
- About this book 15
- AC 800M 75
 - Control Builder configuration 75
 - Downloading AC 800M controller firmware 80
 - OPC server configuration 88
 - Setting IP address 80
- Adding additional AO servers 142
- Adding clients 35
- Adding connectivity and application servers 33
- ADO provider 173
- Advanced templates 188
- Affinity 40
 - Configuration 44
 - Load balancing and system performance 40
 - Planning load balancing 41
- AoWebServerNode 141
- Application server
 - Adding 33
- Aspect directory 114
- Aspect directory synchronization for 800xA for Harmony 114
- Aspect server
 - Redundancy 37

Redundant 36

- Asset Optimization
 - Adding additional AO servers 142
 - AoWebServerNode 141
 - AssetMonitoring service provider node 141
 - SAP/PM Integration 147
 - Web-enabled views 145
- Asset optimization
 - Restarting event collector service 144
- AssetMonitoring service provider node 141

B

- Basic Computer Monitoring 151
- Batch Management 183
 - Advanced templates 188
 - Print BMS report configuration 187
 - Shutdown script 186
 - System service definitions 183
 - Toolbar 188

C

- CI862 TRIO interface 192
- Client
 - Adding 35
- Communications settings 125
- Compact flash 80
- Configuration
 - Affinity 44
 - OPC server for AC 800M 88
 - Print BMA report for Batch Management 187
 - Scheduler 50
 - Windows services 219
- Configuring redundancy 37
- Connectivity server
 - Adding 33

- Redundant 38
- Control Builder configuration 75
- Control network setup 130
- Creating the system 23

D

- Database 164
- DBA (ADO) data provider 171
- Defining users 47
- Device library wizard 153, 154
- Device management and fieldbuses
 - Device library wizard 154
- Device management FOUNDATION Fieldbus 157
 - General settings 157
 - Time synchronization 157
- Diagnostics Collection Tool 57
 - ABBRResults directory share 57

E

- Event collector service 66, 144

F

- FOUNDATION Fieldbus 157
 - General settings 157
 - Time synchronization 157

H

- Hardening 219
- Harmony configuration 112, 113

I

- IEC 60870 licensing 133
- Import Harmony configuration 112, 113
- Information Management 161
 - Creating database instance 164
 - DBA (ADO) data provider 171
 - Edit ADO data provider configuration 173
 - ODBC data source 171
 - Setup 161

- Starting PAS 169
- Troubleshooting 178

L

- Load balancing 41
- Load balancing and system performance 40
- Loading system extensions 27

M

- Multisystem integration 195
 - Remote access client 200
 - Remote access server 195
 - Upload configuration 203

N

- New installations 20

O

- OPC server configuration 88
- Oracle 171

P

- PAS 169
- PC, Network and Software Monitoring 151
- PLC Connect 129
 - IEC 60870 licensing 133
 - PLC server 136
- PLC connect
 - Control network setup 130
- PLC server 136
- Print BMA report configuration 187

R

- Redundancy 36
 - Adding aspect servers 37
 - Configuring 37
 - Redundant aspect servers 36
 - Redundant connectivity servers 38
 - Service providers for SoftPoint Server 53

- Redundant Connectivity Servers 127
- Redundant Partner 127
- Remote access client 200
- Remote access server 195
- Restarting event collector service 66, 144
- Reverse Time Synchronization Mode 121
- REVERSED_SYNC_MODE 121
- RTAB network settings 103

S

- SAP/PM Integration 147
- Scheduler
 - Configuration 50
- SDL Collector
 - SDL Collector Configuration 67, 69
- Setting IP address 80
- Shutdown script 186
- SMS and e-mail Messaging 65
 - Location of application server 65
- SMS and e-mail messaging
 - Restarting event collector service 66
- SoftPoint Server 53
 - Redundant service providers 53
- System configuration console 21
- System extensions 27
- System installer 20, 21
- System level tasks 23
 - Adding clients 35
 - Adding connectivity and applications servers 33
 - Affinity 40
 - Configuration 44
 - Configuring the time client 49
 - Configuring the time server 48
 - Creating the system 23
 - Defining users 47
 - Loading system extensions 27
 - Redundancy 36
 - Time services 47
 - Configuring 48

- Disable Windows time service 47
 - Verifying system and servers 39
- System service definitions 183

T

- Time client
 - Configuring 49
- Time server
 - Configuring 48
- Time services 47
 - Configuring 48
 - Disable Windows time service 47
- Time Synchronization 122
- Time synchronization 157
- TK212 80
- TK212A 80
- Toolbar 188
- TRIO integration 191
 - CI862 TRIO interface 192
 - Firmware 192
 - Hardware library 192
 - System extension 191
- Trio integration
 - Installation 191

U

- Upgrades 21
- Upload configuration 203
- Users
 - Defining 47

V

- Verifying system and servers 39

W

- Web-enabled views on non-Industrial IT systems 145
- Windows hardening 219
- Windows services 219
- Windows time service 47

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 Windows 7 Versions	Feb 2011
B	Updated for 800xA 5.1 Rev A	May 2011
C	Updated for 800xA 5.1 Feature Pack	Aug 2011

Updates in Revision Index A

The following table shows the updates made in this User Manual that were made to correct supported versions of Windows 7.

Updated Section/Sub-section	Description of Update
Section 2, Selecting the Windows Operating System	<p>Changed the following statement</p> <p>from:</p> <p>800xA System software may be installed on the 32-bit (x86) US English version of Windows Server 2008 Standard edition with Service Pack 2, or 32-bit (x86) US English version of Windows 7 Business or Enterprise edition.</p> <p>to:</p> <p>800xA 5.1 System software may be installed on the 32-bit (x86) US English version of Windows Server 2008 Standard or Enterprise edition with Service Pack 2, or the 32-bit (x86) US English version of Windows 7 Professional or Enterprise edition. Windows Server 2008 R2 is not supported.</p>

Updates in Revision Index B

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

Updated Section/Sub-section	Description of Update
About this User Manual	Added the Password Caution in the sub-section <i>General</i> .
Section 1 Post Installation Overview	Added a new sub-section <i>800xA 5.1 Rev A Installation</i> .
Section 2 System Level Tasks	Added a new sub-section <i>800xA 5.1 Rev A Installation</i> .

Updated Section/Sub-section	Description of Update
Section 2 System Level Tasks	Changes updated in the sub-section <i>Loading System Extensions</i> .
Section 9 800xA for Harmony	Changes done for the sub-section <i>ICI Device Configuration</i> .
Section 19 Information Management	Changes updated in the sub-section <i>Information Management Setup, ActiveX Security Settings and Creating a History Database Instance</i> .
Section 19 Information Management	Added new sub-section <i>Creating a Secured Password for Oracle TNS Listener</i> .
Section 19 Information Management	Added new sub-section <i>Defining the Users</i> .
Section 19 Information Management	Changes updated in the sub-section <i>Verifying Oracle Service Names</i> . Changes updated in the sub-section <i>Information Management Profiles Client Post Installation</i>
Section 20 Batch Management	Changes updated in the sub-section <i>Setting the SQL Server Maximum Server Memory Limit</i> .
Section 22 Multisystem Integration	Changes updated in the sub-section <i>Creating a Remote Access Server</i> .

Updates in Revision Index C

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

Updated Section/Sub-section	Description of Update
About this User Manual	Added a new section <i>Feature Pack</i> describing the user manual conventions used for indicating the Feature Pack content. Minor changes are made in the section.
Section 14 Asset Optimization	Added information in Configuring Maximo and ECS, and SAP/PM Integration. Feature Pack Icon added.

Contact us

ABB AB

Control Systems

Västerås, Sweden

Phone: +46 (0) 21 32 50 00

Fax: +46 (0) 21 13 78 45

E-Mail: processautomation@se.abb.com

www.abb.com/controlsystems

Copyright © 2003-2011 by ABB.

All Rights Reserved

3BUA000156-510 C

ABB Inc.

Control Systems

Wickliffe, Ohio, USA

Phone: +1 440 585 8500

Fax: +1 440 585 8756

E-Mail: industrialitsolutions@us.abb.com

www.abb.com/controlsystems

ABB Industry Pte Ltd

Control Systems

Singapore

Phone: +65 6776 5711

Fax: +65 6778 0222

E-Mail: processautomation@sg.abb.com

www.abb.com/controlsystems

ABB Automation GmbH

Control Systems

Mannheim, Germany

Phone: +49 1805 26 67 76

Fax: +49 1805 77 63 29

E-Mail: marketing.control-products@de.abb.com

www.abb.de/controlsystems

Power and productivity
for a better world™

