Installation Guide for Cisco Unified Automated Administrator for Symposium (AAS)

September 2011

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Installation Guide for Cisco Unified Automated Administrator for Symposium (AAS)

CONTENTS

About This Guide

Purpose

This manual provides installation and troubleshooting information about Cisco Automated Administrator for Symposium (AAS), which is referred to as “AAS” throughout this document. It also provides information about creating application instances using the Cisco Unified Intelligent Contact Management (Unified ICM) Configuration Manager and describes how to establish administration connections.

Note For information about Unified ICM, refer to http://www.cisco.com for the complete set of Unified ICM manuals.

Audience

This document is intended for contact center administrators and contact center technology experts, who will install and use AAS.

Organization

The following table describes the information contained in each chapter of this guide.

Chapter	Title	Description
Chapter 1	About Automated Administrator for Symposium	Provides an overview of the functionality and performance of AAS.
Chapter 2	Installing and Configuring Automated Administrator for Symposium	Provides prerequisites and installation instructions for installing AAS.
Chapter 3	Configuring the ICM ConAPI Connection	Describes how to configure the Unified ICM ConAPI connection.
Chapter 4	Debugging and Throttling	Provides information on debugging and troubleshooting AAS.

Chapter	Title	Description
Chapter 5	Limitations of Automated Administrator for Symposium	Describes the limitations of AAS.
Appendix A	Working with Registry Settings, page 1	Describes the configuration and dynamic registry settings in AAS.

For troubleshooting tips for Cisco Unified Contact Center Products, go to http://docwiki.cisco.com/wiki/Category:Troubleshooting, then click the product/option you are interested in.

Conventions

This manual uses the following conventions:

Format	Example
Boldface type is used for user entries, keys, buttons, and folder and submenu names.	Click **Logger**, then click the **Edit** button in the Instance Components section.
Italic type indicates one of the following: • A newly introduced term • For emphasis • A generic syntax item that you must replace with a specific value • A title of a publication	• A *skill group* is a collection of agents who share similar skills. • *Do not* use the numerical naming convention that is used in the predefined templates (for example, **persvc01**). • IF (*condition*, *true-value*, *false-value*) • For more information, see the *Database Schema Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* available at cisco.com.
An arrow (>) indicates an item from a pull-down menu.	The Save command from the File menu is referenced as **File > Save**.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Documentation Feedback

You can provide comments about this document by sending an email to the following address:

ccbu_docfeedback@cisco.com

We appreciate your comments.

CHAPTER 1

About Automated Administrator for Symposium

This chapter describes the Automated Administrator for Symposium (AAS), the prerequisites needed before installing AAS, and lists the procedure for installing AAS.

This chapter includes the following sections:

About Automated Administrator for Symposium

AAS is middleware software, which converts Nortel Symposium Event Interface (SEI) messages into Cisco Unified Intelligent Contact Management (Unified ICM) ConAPI messages. The purpose of this software is to synchronize administrative changes made on the Symposium system with the ICM database, thereby eliminating the need for a system administrator to execute changes twice (once in the Nortel Symposium Administration and once in the ICM administration). All additions and updates to agents and their skill sets made using Nortel Symposium administration are also dynamically made to the ICM database in real time. However, changes made in the system are not reflected in Nortel Symposium.

AAS is an optional software for Unified ICM. AAS is co-resident with Symposium PG and interacts only with ICM DB and SCCS SEI Server. AAS is controlled by the ICM Node Manager.

Prior to integration of AAS with Unified ICM, you would need to install AAS using a standalone installer. Patches of AAS were also available as a standalone installer.

After integration of AAS with Unified ICM, AAS patches are available as a part of the ICM installer. In addition, from Unified ICM 7.1(3), you can install AAS using the ICM installer.

The following points describe the packaging and bundling information of AAS:

- AAS can be installed on existing ICM PGs as well as new installations.
- AAS is available as a standalone installer up to Unified ICM 7.1(2).
- AAS is available as an integrated installer from Unified ICM versions 7.1(3) and later.

Note From 6.0(0) SR8, although AAS is installed using a standalone installer, AAS patches are integrated with the ICM installer. This is applicable to the 6.0(0) stream only.

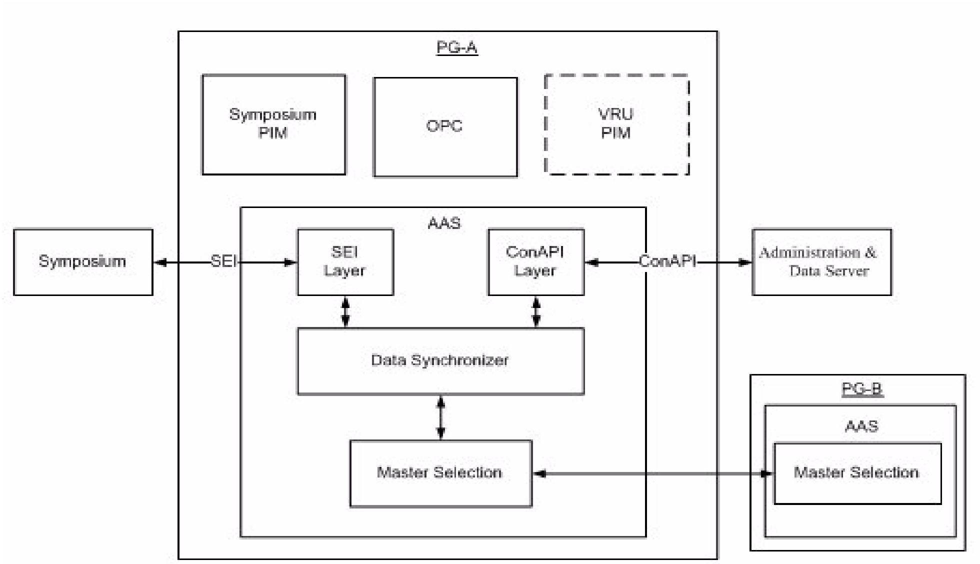
AAS Architecture

Following are the components of AAS:

- The Symposium interface (SEI layer), which encapsulates the interface between AAS and Nortel Symposium.
- The ICM interface (ConAPI layer), which encapsulates the interface between AAS and Administration & Data Server.
- Data Synchronizer, which compares the information from Symposium and Administration & Data Server to determine what information to send to Administration & Data Server.
- Master Selection, which determines the master AAS in a duplex environment.

Figure 1-1 illustrates the AAS components.

Figure 1-1 AAS Software Key Subsystem Components



SEI (also referred to as “SEI Lite”) is the connection between AAS and Symposium Call Center System (SCCS). SEI is a Nortel product that enables third-party products (such as AAS) to receive events from Nortel SCCS.

Refer to the *Cisco Unified ICM Software ACD Supplement for Nortel Symposium* for more details about the Nortel Symposium PG. The *Cisco Unified ICM Software Supported Switches (ACDs)* document lists the ACD supported switches. (All Cisco documentation is available on Cisco.com.) The Nortel SEI documentation set provides detailed information about SEI.

The following points describe the functionality of the AAS architecture:

- AAS is controlled by ICM Node Manager like other Unified ICM components. AAS can be started/stopped via ICM Service Control for PG.
- For duplex AAS systems, Master Selection will determine which AAS will be active (master) and which will be in warm standby mode (subscriber).
- SEI layer is responsible for managing connection with SCCS and requesting and getting SEI events from SCCS.

- ConAPI layer is responsible for managing connection with Administration & Data Server, requesting and updating agent, skill, and skill assignments information in ICM via ConAPI.
- Data synchronizer layer is responsible for converting and synchronizing the SEI and ConAPI data.
- After an AAS becomes active:
  - ConAPI layer will connect with Administration & Data Server.
  - SEI layer will connect to SCCS.
  - SEI layer will request synchronization from SCCS, and the SCCS begins to send a snapshot of its configuration.
  - SEI layer will pass data to Data synchronizer, which synchronizes the data from the Administration & Data Server and sends the changes back to the Administration & Data Server through the ConAPI layer.
  - After initial synchronization, SCCS sends any subsequent changes in SCCS administration as they occur to SEI layer where it goes through the above process again.
- AAS fault tolerance is not the same as regular Unified ICM. The master selection decides the active AAS (master) and the inactive AAS (slave).

AAS Performance and Scalability

This section provides information on AAS performance parameters and scalability.

AAS Performance

All messages sent to the ConAPI interface are "throttled" by AAS. This includes startup messages as well any messages sent at run time. Throttling will prevent flooding the ConAPI interface. Throttling parameters are controlled by the AAS registry. Refer Working with Registry Settings, page A-1 for more information on the throttling parameters.

The performance parameters of AAS are as follows:

- Runs as high priority like other ICM processes.
- Uses an average of < 10% CPU time on resynchronization.
- Uses < 5% CPU for normal changes in Symposium.
- Resynchronization for 1000 agents with 100 skill groups takes < 10 minutes.
- Normal changes in Symposium appear in the system within 5 seconds.
- Uses approximately 40 MB memory during resynchronization.
- Uses approximately 20 MB memory during normal operations.
- AAS supports a maximum of 600 configuration changes/hour.

The number of configuration transactions updated by AAS to Administration & Data Server depends on the number and type of configuration changes made on the Nortel SCCS.

For Unified ICM Releases earlier than Unified ICM 7.2.(3):

- Each configuration change reported by the SCCS to AAS will require AAS to make one configuration transaction from AAS to Administration & Data Server. For example, 100 configuration changes reported by SCCS to AAS will need 100 configuration transactions from AAS to the Administration & Data Server.

From Unified ICM Release 7.2.(3):

- Events for certain configuration changes (For example, Agent Skill Assignment and De-assignment) are combined by AAS as a single configuration transaction.
- Events for certain configuration changes (For example, Skillgroup Priority Change) cannot be combined by AAS as a single configuration transaction.

For example, 100 configuration changes reported by SCCS to AAS will get updated in less than 100 configuration transactions from AAS to the Administration & Data Server. The actual number will depend on the combination and interleaving of the various types of events from SCCS.

The number of records updated in each transaction depends on the following registry key: **AASConAPIThrottleMaxModificationsPerTrans**.

Note The CMS Node has a record retrieval limit of 1024 * 1024 characters. To ensure that this limit is not exceeded, AAS has a registry key (AASConAPIThrottleMaxResults) to control the number of records from Administration & Data Server . The default value of this registry key is 1500. This value can be increased up to 3500, which is the maximum recommended value. For more information on AAS Throttling Guidelines, refer AAS Throttling Guidelines, page 4-1.

AAS Analyzer

AAS Analyzer is a built-in feature of AAS used to determine AAS performance and is available from Unified ICM 7.2(3) and later versions. The purpose of the AAS Analyzer is to determine the number of events sent by the Nortel Symposium over the SEI link to AAS. AAS Analyzer logs the events received from the Symposium. The logs are captured on hourly basis.

AAS can be run in the following modes:

- Analyzer Mode: To run AAS in Analyzer mode, set AASAnalyseMode to 1
- Normal Mode: To run AS in Normal mode, set AASAnalyseMode to 0

The following registry controls the operation of AAS in the Analyzer and Normal modes:
Config registry "AASAnalyseMode" of type REG_DWORD

This is registry is available at:
My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<icm instance>\PGxx\PG\CurrentVersion\AASS\aas1\AASData\Config

Note

- AAS Analyzer does not modify the configuration changes to the system and has no adverse impact on your system.
- When AAS Analyzer is turned on, AAS does not send any configuration changes to the cmsjserve on AW.
- For additional information regarding the set up and operation of AAS in Analyzer mode, contact TAC.

AAS Scalability

The scalability features of AAS are described in this section.

Multiple AAS connecting to single Administration & Data Server

- During startup, you must start each instance of AAS one by one. A delay of 2 minutes before starting another instance is recommended.
- On reaching steady state, multiple AAS instances will remain connected to a Administration & Data Server and update the configuration changes to Administration & Data Server. A maximum of three concurrent AAS instances can connect to a single Administration & Data Server at a time.

Two AAS connecting to single Administration & Data Server

The following configurations are supported in a duplex AAS environment.

Both sides of AAS (A and B) are on two different machines and connect to Administration & Data Server on a different machine.

Case 1: AAS side A and side B use the same server name but different client names.

Configure the AAS config registries **AASConAPIRemoteServiceName1** and **AASConAPILocalServiceName1** as follows:

- AAS side A: AASServer1, AASClient1
- AAS side B: AASServer1, AASClient2

Configure the **Administration & Data Server link** and **Application link** parameters in CMS Control at Administration & Data Server as follows:

- AAS side A: AASServer1, AASClient1
- AAS side B: AASServer1, AASClient2

Case 2: AAS side A and side B use different server and client names.

Configure the AAS config registries **AASConAPIRemoteServiceName1** and **AASConAPILocalServiceName1** as follows:

- AAS side A: AASServer1, AASClient1
- AAS side B: AASServer2, AASClient2

Configure the **Administration & Data Server link** and **Application link** parameters in CMS Control at Administration & Data Server as follows:

- AAS side A: AASServer1, AASClient1
- AAS side B: AASServer2, AASClient2

Case 3: AAS side A and side B use the same server and client names.

Configure the AAS config registries **AASConAPIRemoteServiceName1** and **AASConAPILocalServiceName1** as follows:

- AAS side A: AASServer1, AASClient1
- AAS side B: AASServer1, AASClient1

Configure the **Administration & Data Server link** and **Application link** parameters in CMS Control at Administration & Data Server as follows:

- AAS side A: AASServer1, AASClient1
- AAS side B: AASServer1, AASClient1

Force Synchronization

AAS synchronization process gets triggered after AAS has become active. The synchronization can be forced by modifying the dynamic registry key given below:

HKEY_LOCAL_MACHINE/SOFTWARE/Cisco Systems, Inc./ICM/<ICMinstance>/PG<XX>/PG/CurrentVersion/AASS/aas<X>/AASData/Dynamic/AASForceResync.

CHAPTER 2

Installing and Configuring Automated Administrator for Symposium

This chapter describes Automated Administrator for Symposium (AAS), the prerequisites needed before installing AAS, and details the procedure for installing AAS.

This chapter includes the following sections:

Types of Installation

Standalone Installation

Standalone installation applies to the installation of AAS on Unified ICM releases 5.0(0), 6.0(0), and 7.0(0). Refer the Appendix 2, "How to Install AAS on Unified ICM Releases Earlier Than Unified ICM 7.1(3) (Standalone Installer)" section for more information on standalone installation.

Integrated Installation

Integrated installation applies to the installation of AAS on Unified ICM releases from 7.1(3). Refer the Appendix 2, "How to Install or Reinstall AAS on Unified ICM 7.1(3) (Integrated Installer)" section for more information on integrated installation.

Note Standalone installation of AAS is not supported if you are running Unified ICM version 7.1(3) and later. If you have AAS installed as a standalone installer with 7.1(2), you can upgrade to 7.1(3) and continue to run AAS without impacting your existing configuration.

Supported Configurations

The supported combination of single and dual redundant components is given in the Table 2-1 below:

Table 2-1 Supported Configurations

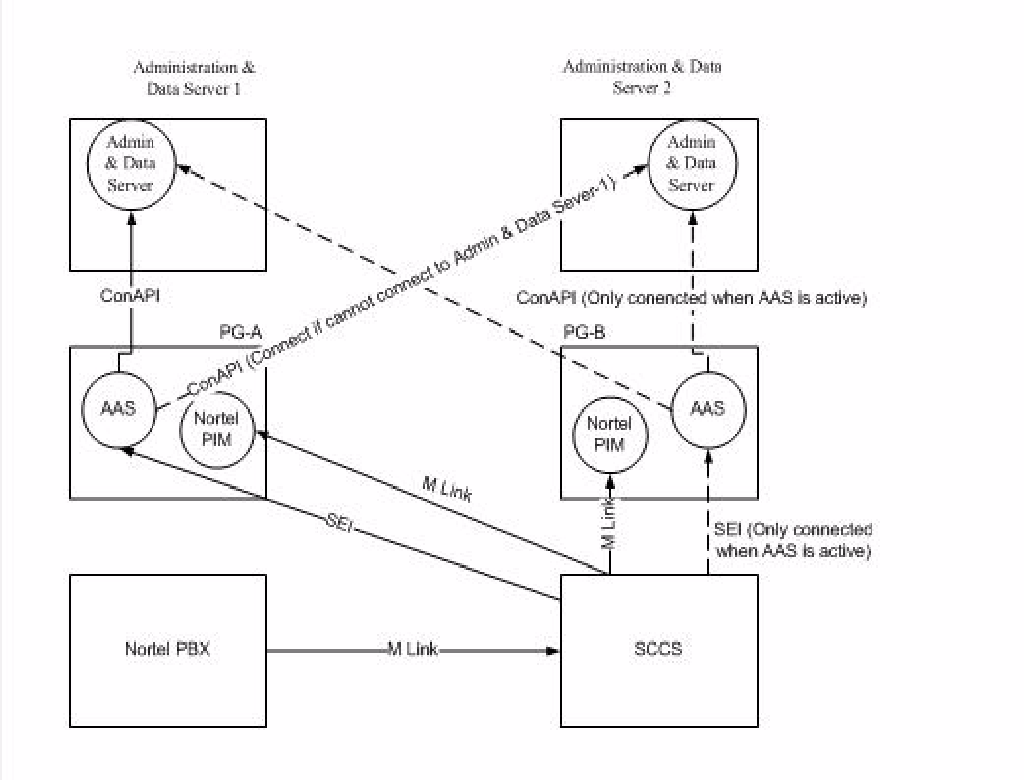
	PG (with AAS)	Administration & Data Server	SCCS
Fully redundant	Duplex	Connecting to primary and secondary Administration & Data Server	Single
Partially redundant	Duplex	Single	Single
No redundancy	Single	Single	Single

Fully Redundant

In a fully redundant configuration, there are two AAS servers: one is active and the other is in standby. The active AAS server is connected to SCCS and Administration & Data Server. The standby AAS server does not have a connection to SCCS or Administration & Data Server.

The active server will have the word **Active** in its console window. The standby server will have the word **Idle** in its console window. If the active AAS server cannot connect to one Administration & Data Server, it will try the other Administration & Data Server. If the active AAS server cannot connect to SCCS and/or both Administration & Data Server, it will failover to the other AAS server. Figure 2-1 shows the fully redundant configuration.

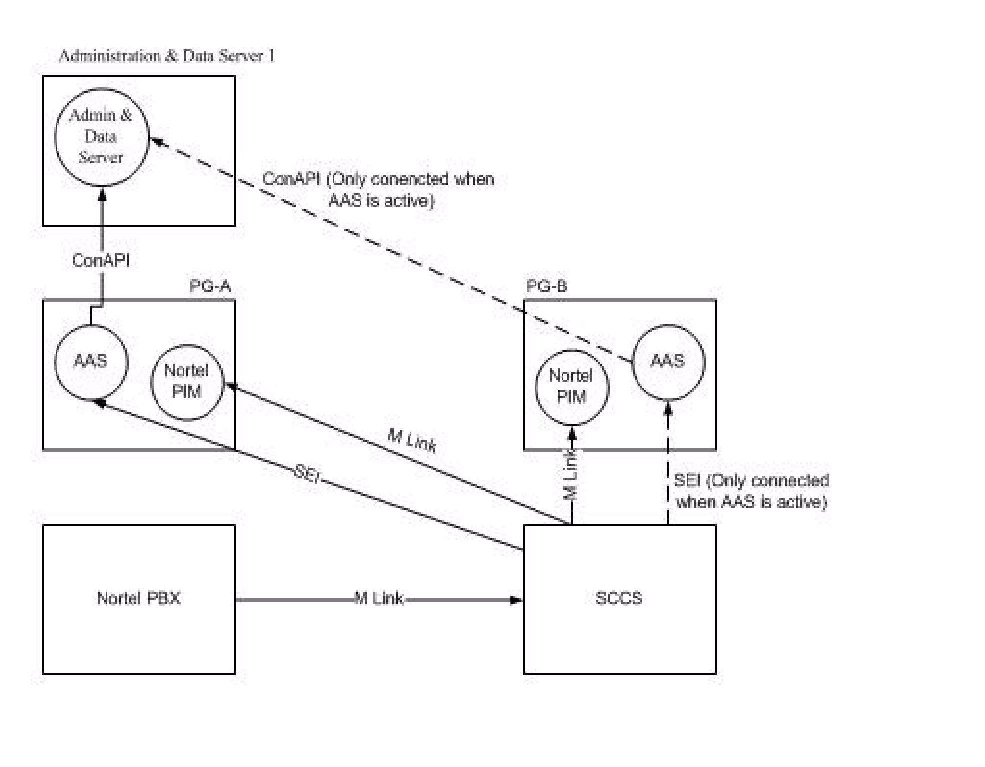
Figure 2-1 Fully Redundant Configuration


Administration & Data Server 1
Administration & Data Server 2
Admin & Data Server
Admin & Data Server
ConAPI
ConAPI (Connect if cannot connect to Admin & Data Sever-1)
ConAPI (Only conencted when AAS is active)
PG-A
PG-B
AAS
Nortel PIM
Nortel PIM
AAS
M Link
SEI
M Link
SEI (Only connected when AAS is active)
Nortel PBX
M Link
SCCS

Partially Redundant

In a partially redundant configuration, there is only one Administration & Data Server. The AAS server will only connect to this Administration & Data Server. The AAS server can failover to the other AAS server if it has problems. Figure 2-2 shows the partially redundant configuration.

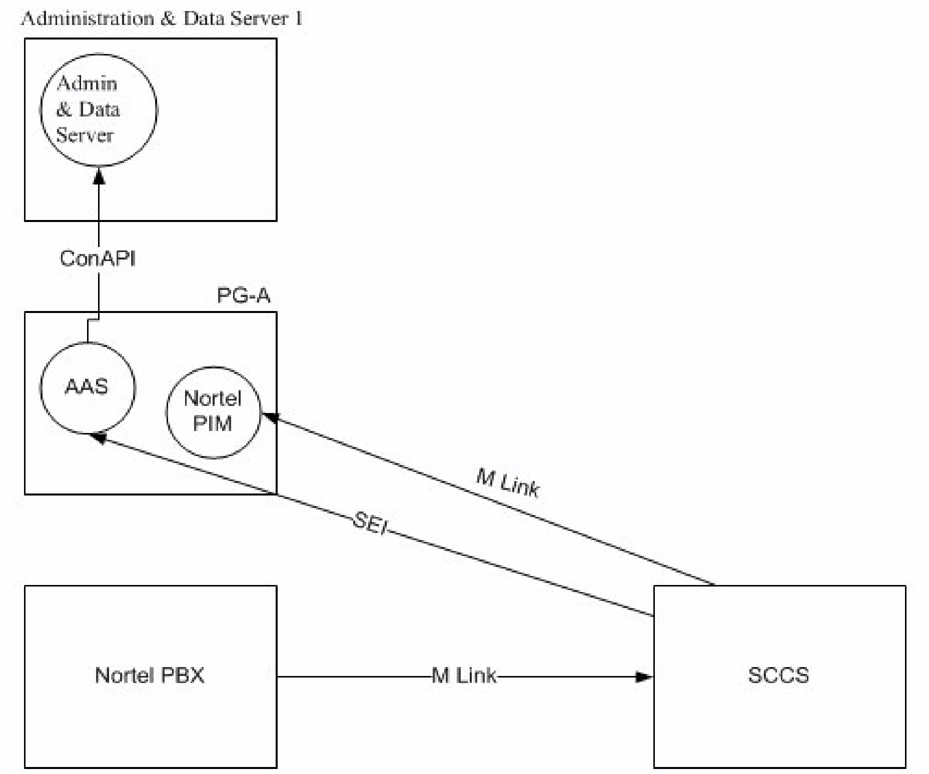
Figure 2-2 Partially Redundant Configuration


Administration & Data Server 1
Admin & Data Server
ConAPI (Only conencted when AAS is active)
ConAPI
PG-A
PG-B
AAS
Nortel PIM
Nortel PIM
AAS
M Link
SEI
M Link
SEI (Only connected when AAS is active)
Nortel PBX
M Link
SCCS

Not Redundant

In the absence of redundancy, there is only one Administration & Data Server and one AAS. In case of Administration & Data Server failure, AAS will continue trying to connect to Administration & Data Server until the connection is established. Figure 2-3 shows the non-redundant configuration.

Figure 2-3 Configuration without Redundancy



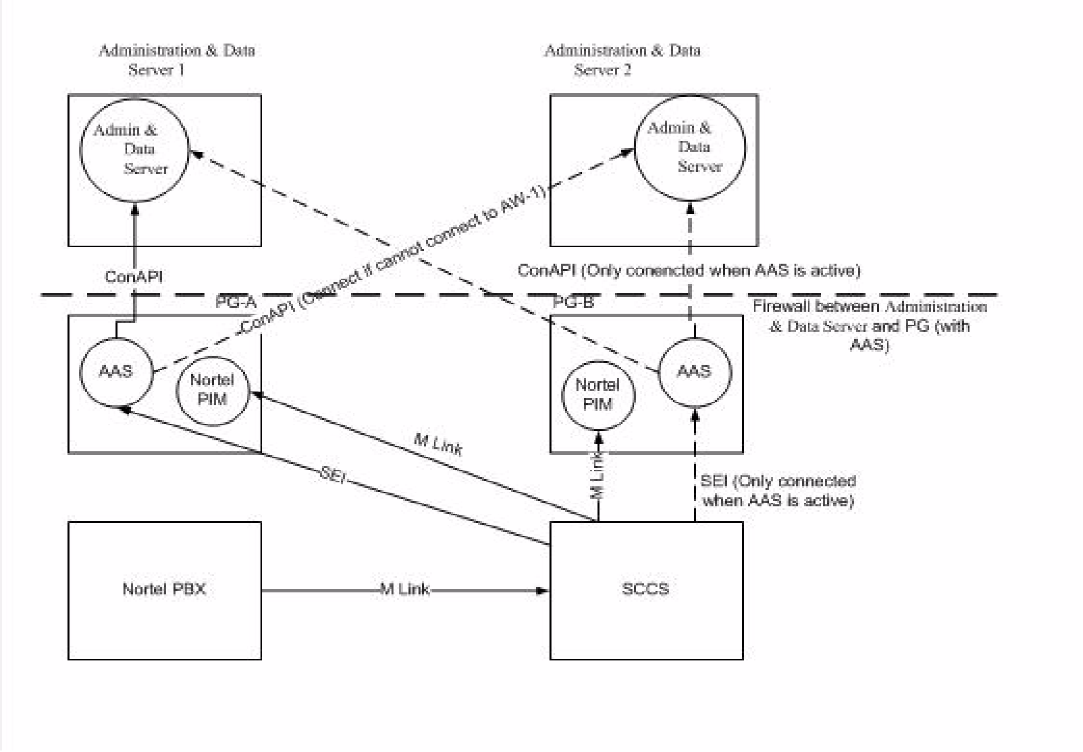
Supported Configurations with Firewall

The below diagrams depict the firewall configurations supported between AAS and Administration & Data Server. Firewall between AAS and SCCS is not supported because the Nortel SCCS port is dynamic.

Fully Redundant

Figure 2-4 shows the fully redundant configuration with firewall.

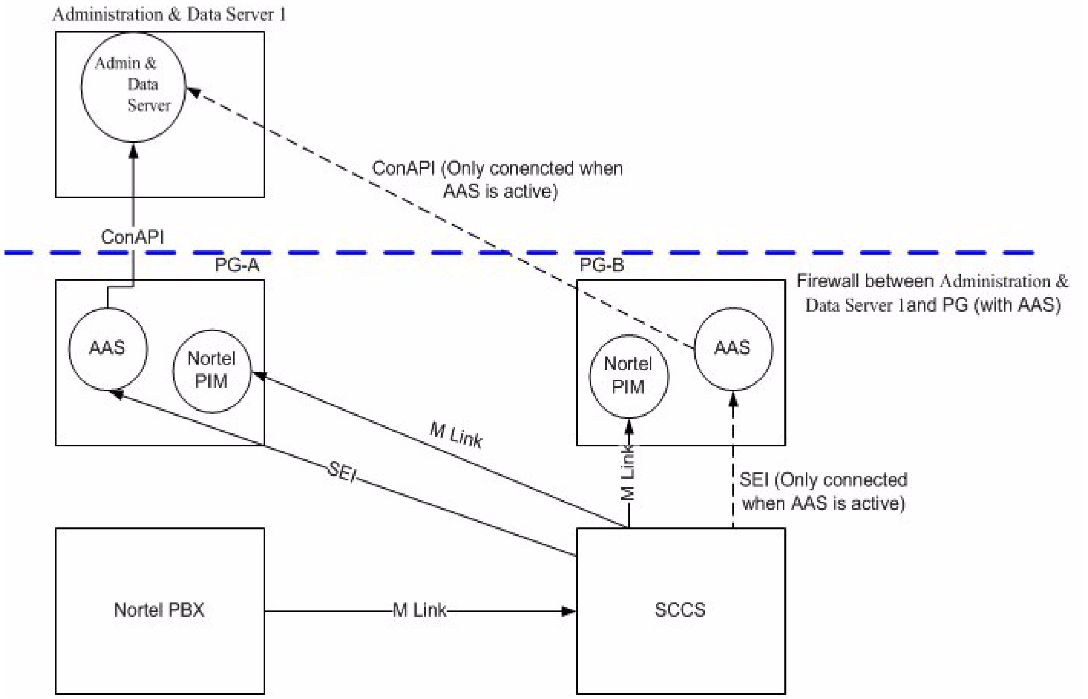
Figure 2-4 Fully Redundant Configuration with Firewall


Administration & Data Server 1
Administration & Data Server 2
Admin & Data Server
Admin & Data Server
ConAPI (Connect if cannot connect to AW-1)
ConAPI
ConAPI (Only conencted when AAS is active)
PG-A
PG-B
Firewall between Administration & Data Server and PG (with AAS)
AAS
Nortel PIM
Nortel PIM
AAS
M Link
SEI
M Link
SEI (Only connected when AAS is active)
Nortel PBX
M Link
SCCS

Partially Redundant

Figure 2-5 shows the partially redundant configuration with firewall.

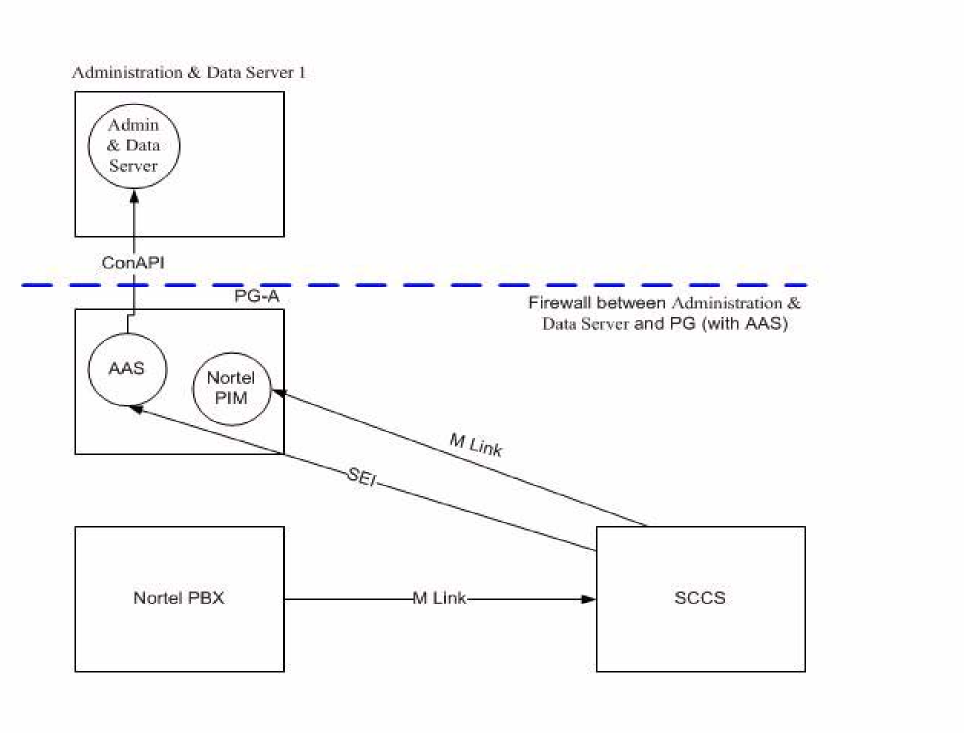
Figure 2-5 Partially Redundant Configuration with Firewall


Administration & Data Server 1
Admin & Data Server
ConAPI (Only conencted when AAS is active)
ConAPI
PG-A
PG-B
Firewall between Administration & Data Server 1and PG (with AAS)
AAS
Nortel PIM
Nortel PIM
AAS
M Link
SEI
M Link
SEI (Only connected when AAS is active)
Nortel PBX
M Link
SCCS

No Redundancy

Figure 2-6 shows the non-redundant configuration with firewall.

Figure 2-6 Non-redundant Configuration with Firewall


Administration & Data Server 1
Admin & Data Server
ConAPI
PG-A
Firewall between Administration & Data Server and PG (with AAS)
AAS
Nortel PIM
M Link
SEI
Nortel PBX
M Link
SCCS

Firewall Usage and Configuration

This section has information on firewall usage and configuration between AAS and Administration & Data Server. This section is applicable if you are using a firewall between AAS and Administration & Data Server. If you are not using firewall between AAS and Administration & Data Server, you can ignore this section.

Firewall between AAS and Administration & Data Server

If you are using firewall between AAS and Administration & Data Server, you will need to open the ports used between AAS and Administration & Data Server in the firewall. This ensures that these ports are not blocked by firewall and facilitates proper communication between AAS and Administration & Data Server.

The following ports are used for firewall configuration between AAS and Administration & Data Server:

1. AAS uses a static port (which can be configured) on AAS for RMI connection from Administration & Data Server.
2. AAS uses two dynamic ports on AAS for communication with Administration & Data Server.

AAS Registry values:

To configure the firewall between AAS and Administration & Data Server, define the following registry values:

1. The below registry value should be set to "true"

HKEY_LOCAL_MACHINE/SOFTWARE/Cisco Systems, Inc./ICM/<ICMinstance>/PG<XX>/PG/CurrentVersion/AASS/aas<X>/AASData/Config/AASConAPI DisableAutoConnect

2. The below registry value is used as the local RMI port by AAS. Open this port in the firewall.

HKEY_LOCAL_MACHINE/SOFTWARE/Cisco Systems, Inc./ICM/<ICMinstance>/PG<XX>/PG/CurrentVersion/AASS/aas<X>/AASData/Config/AASConAPI LocalRegistryPort

For ex: 1099

3. The following registry value is used as the local communication port by AAS. Open this port in the firewall.

HKEY_LOCAL_MACHINE/SOFTWARE/Cisco Systems, Inc./ICM/<ICMinstance>/PG<XX>/PG/CurrentVersion/AASS/aas<X>/AASData/Config/AASConAPI LocalPort

Example Port Usage

Ports used between AAS and Administration & Data Server with the above registry values:

For example, 5555 is the AASConAPILocalPort

Ports usage between AAS and Administration & Data Server with the above registry settings:

1. Port 1099 is used on AAS for RMI connection from Administration & Data Server.
2. Port 5555 is used on AAS for communication with Administration & Data Server.

Guidelines for Firewall configuration between AAS and Administration & Data Server

Refer the above example for this section.

1. If firewall is installed in the network that AAS is part of:

Open ports 1099 and 5555 in the firewall for incoming connections from Administration & Data Server towards AAS.

2. If firewall is installed in the network that Administration & Data Server is part of:

Open ports 1099 and 5555 in the firewall for outgoing connections from Administration & Data Server towards AAS.

Note Firewall between AAS and SCCS is not supported because the Nortel SCCS port is dynamic.

Prerequisites for Installing AAS

This section gives information on the hardware and software supported, information needed, and guidelines for installing AAS.

You must install ICM PG on the system before AAS installation. Before installation, ensure the following registry is set to 50:

HKEY_LOCAL_MACHINE/SOFTWARE/Cisco Systems, Inc./ICM/<ICM instance>/PG<XX>/SymposiumVersion

Minimum System Requirements

Table 2-2 lists the minimum system requirements for installing AAS.

Table 2-2 Minimum System Requirements

Product	Required Version
Symposium Call Center Server (SCCS)	5.0 SU03 with Designer Patch NN_SCCS_5.0_DP_03_S or 5.0 SU06 or NCCM 6.0
Symposium Event Interface	No separate versioning required
Unified ICM	Unified ICM Releases 5.0(0) SR10 and later, 6.0(0) SR3 and later, and 7.0 (0) SR2 and later (with any appropriate patches)

Unified ICM Requirements

The Administration & Data Server must be installed to support use of the ConAPI interface. (See "Configuring the ICM ConAPI Connection" for more information.) The Administration & Data Server can either be installed as co-resident with the PG or installed on a separate machine.

See the Unified ICM documentation set for detailed information about installing and configuring Unified ICM and to the *Hardware & System Software Specification (Bill of Materials) for Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 8.0(1)* for information about Unified ICM hardware and software requirements. See the *Cisco Unified ICM Enterprise Software ACD Supplement for Nortel Symposium* for detailed information about the SEI Lite interface with Nortel Symposium. (All documentation is located on the Cisco web site.)

Note The minimum bandwidth required between AAS and Administration & Data Server is 128 Kbps.

Supported Unified ICM Versions

Refer Appendix 1, "About Automated Administrator for Symposium" for supported Unified ICM versions.

Pre-installation Checklist

Ensure that you have the following information before installation:

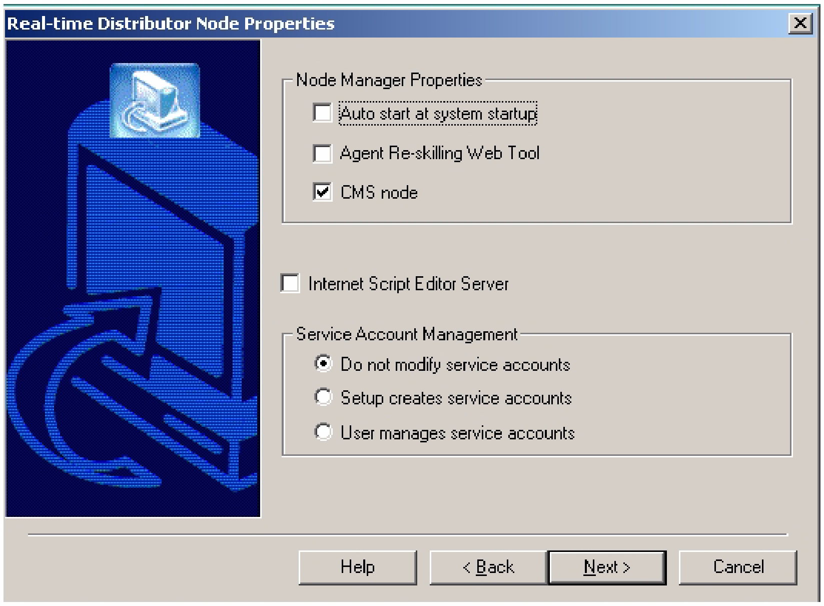
- ICM instance name, PG instance name, and AAS name
- RMI port number
- The IP address of the Administration & Data Server machine
- The IP address/host and port number of the AAS machine
- IP address and port number of the machine where the SCCS Event Server (SEI CORBA) is installed
- Symposium site name (this name is found in the Start\Programs\Symposium Call Center Server\System Information - Site Name directory)
- SEI user name and password
- ICM peripheral ID for the Symposium PG

Enabling the CMS Node Check box

Before installing AAS, the **CMS Node** check box in the Real-time Distributor Node Properties window must be enabled on the Administration & Data Server component. You need to run the ICM Local Setup for this.

Figure 2-7 figure shows the Real-time Distributor Node Properties dialog box with the CMS node check box enabled.

Figure 2-7 CMS Node Check box



Real-time Distributor Node Properties

Node Manager Properties

□ Auto start at system startup

□ Agent Re-skilling Web Tool

☑ CMS node

□ Internet Script Editor Server

Service Account Management

● Do not modify service accounts

○ Setup creates service accounts

○ User manages service accounts

For more information, see the *Configuration Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* available at cisco.com.

Installation Guidelines

Follow these guidelines *before* installing AAS:

- Follow the guidelines as documented in the Symposium PG installation component matrix. AAS is an optional additional component of the Symposium PG.
- The ICM ConAPI connection must be configured *before* installing the AAS software. (See "Configuring the ICM ConAPI Connection" for detailed instructions.)
- If you configure primary and secondary PGs, AAS can be installed on both the Side A and Side B PGs.
- You can install only one AAS instance for one PG.
- Remove all skill groups from ICM before installing and running AAS. This has to be done to avoid any conflicts between the ICM PeripheralNumber and the Symposium skillset ID. When deleting skill groups, persons, or agents in ICM, delete them permanently.

Note For more information, see the Unified ICM Software Setup and Configuration section in the *Cisco Unified ICM Enterprise Software ACD Supplement for Nortel Symposium* available at cisco.com.

- Set the default sub skill group mask for the Symposium Peripheral to **None** by deselecting all skill groups on the Skill Group Mask tab for the peripheral.
- Make sure the PG name in ICM and the skill group name in Symposium are kept short; otherwise, AAS will not be able to generate a unique Enterprise name for the skill group in ICM. The total length of the PG name and the skill group name *combined* cannot be more than 28 characters.
- The Symposium skillset name cannot be longer than 29 characters; otherwise, AAS will not be able to generate a unique peripheral name for the skill group in ICM application.
- If you are using the SU05 version of SCCS, perform the following steps on the Symposium system before installing AAS:
  - Change the HKLM/SOFTWARE/ACE/TAO/TaoNamingServiceOptions registry key to the value: -m 1 -OrbEndPoint iiop://<*hostname*>:4422 -o tao_name_service.ior (where <*hostname*> indicates the machine's hostname).
  - Stop the following services: RSM, ES, TFA, and TAO_Naming_Service.
  - When the above services are stopped, delete the "tao_naming_service.ior" and "tao_naming_service.dat" files located in the 'system32' folder. After these files are deleted, restart the services starting with the TAO_Naming_Service.

Caution You must install the AAS and PG on the same computer. *Do not* install the Symposium software on the same computer as ICM software since this may cause performance issues.

Order of Installation/Configuration

You must install/configure AAS in the following order:

1. Configure Application Instance in ICM Configuration Manager. Refer Appendix 3, "How to configure an application instance" for detailed instructions.
2. Establish administration connection using CMS Control Application. Refer Appendix 3, "How to establish an administration connection" for detailed instructions.

3. Configure the application details. Refer Appendix 3, “About Establishing Administration Connections” for further information.
4. Permanently delete all agents and skill groups from Unified ICM before installing AAS, using ICM Agent Explorer and ICM Skill Group Explorer. Then use ICM Deleted Object tool to delete them permanently from ICM DB.
5. Install and configure AAS.

Installing AAS

This section describes how to install AAS.

Caution You must stop the PG *before* installing or reinstalling AAS software, and restart it once AAS has been installed. Otherwise, AAS will remain in an undefined state or will require a system reboot. If you need to remove AAS, you must remove AAS before removing the PG or AAS will have problems removing.

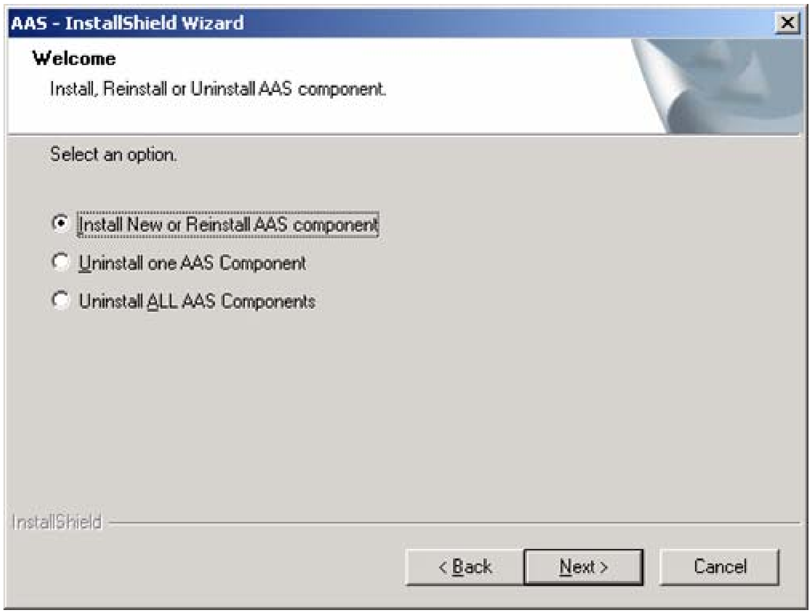
How to Install AAS on Unified ICM Releases Earlier Than Unified ICM 7.1(3) (Standalone Installer)

Before installing AAS, observe the following guidelines:

- For a simplex system (one PG/AAS), enter the local IP address and other required information.
- For a duplex system (two PGs/AASs), enter the IP for each host on Administration & Data Server Sides A and B.

Step 1 Run the **aas_setup.exe** file on the CD. The AAS InstallShield Wizard displays.

Figure 2-8 AAS InstallShield Wizard - Welcome Screen



AAS - InstallShield Wizard

Welcome

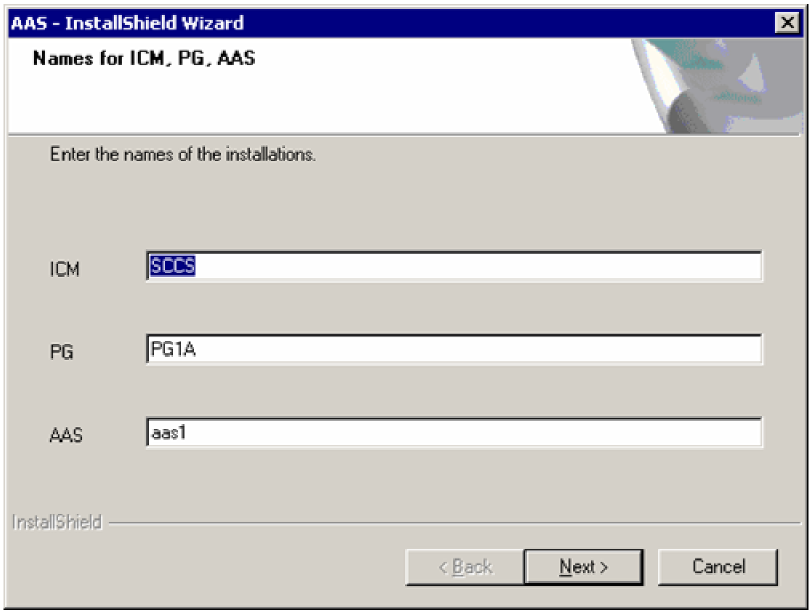
Install, Reinstall or Uninstall AAS component.

Select an option.

● Install New or Reinstall AAS component
○ Uninstall one AAS Component
○ Uninstall ALL AAS Components

Step 2 Enter the name of the ICM instance, the PG name, and the AAS name; then click **Next**. For the AAS name, use the format “aas” and the number; for example, aas1, aas2, etc. (all entries are case-sensitive).

Figure 2-9 AAS InstallShield Wizard - Names of ICM, PG, AAS



AAS - InstallShield Wizard

Names for ICM, PG, AAS

Enter the names of the installations.

ICM: SCCS

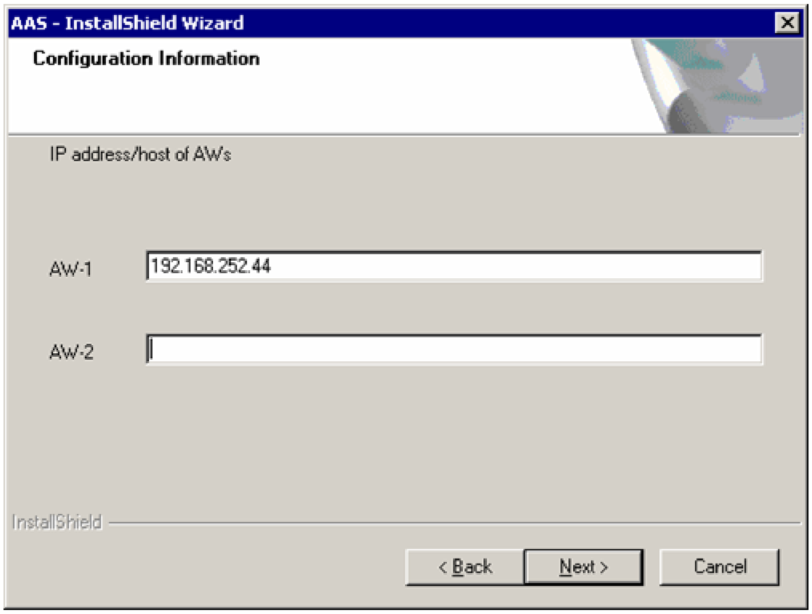
PG: PG1A

AAS: aas1

Note The PG name and the AAS name are each combinations of the node and the side.

Step 3 In the Configuration Information window for the IP address/host of Administration & Data Server s, enter the Administration & Data Server machine IP address for ICM Primary Administration & Data Server and for Unified ICM Secondary Administration & Data Server (if you are using a secondary distributor); then click **Next.**

Figure 2-10 .AAS InstallShield Wizard - Configuration Information

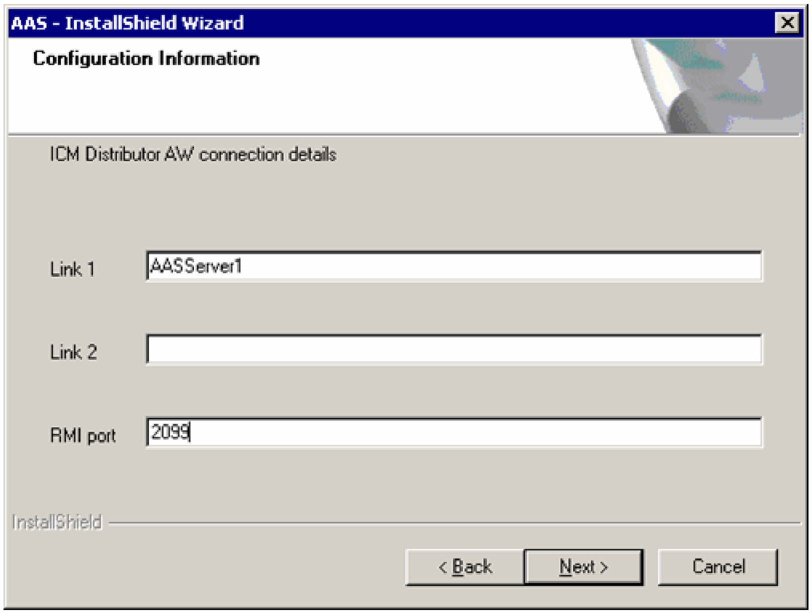


AW-1 192.168.252.44

AW-2

Step 4 In the Configuration Information window for the Administration & Data Server connection, enter the Administration & Data Server Link 1 name, the Administration & Data Server Link 2 name (if using a secondary distributor), and the Administration & Data Server RMI registry port number using the same values used in Step 4 in "How to establish an administration connection" section on page 3-3; then click **Next**.

Figure 2-11 AAS InstallShield Wizard - Configuration Information



AAS - InstallShield Wizard

Configuration Information

ICM Distributor AW connection details

Link 1: AASServer1

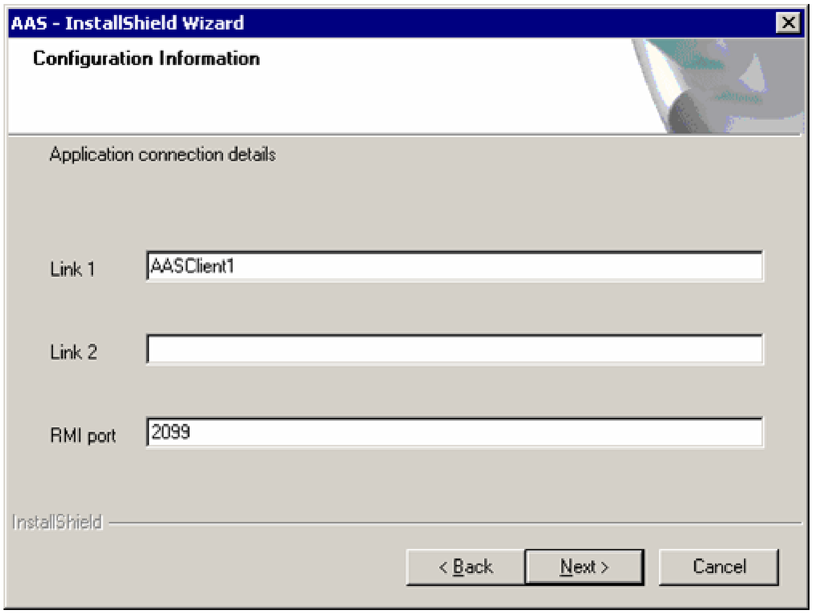
Link 2:

RMI port: 2099

Caution If you are using a secondary distributor, the names of the AAS servers *must* be different; for example, "AASServer1" cannot be the name of the Administration & Data Server link on both computers. If you have multiple AAS servers on your network, each one must have unique entries due to RMI requirements.

Step 5 In the Configuration Information window for the application connection details, enter the Application Link 1 name, the Application Link 2 name (if using a secondary distributor), and the Application RMI registry port number; then click **Next**.

Figure 2-12 AAS InstallShield Wizard - Configuration Information


AAS - InstallShield Wizard
Configuration Information
Application connection details
InstallShield
< Back
Next >
Cancel

Link 1: AASClient1

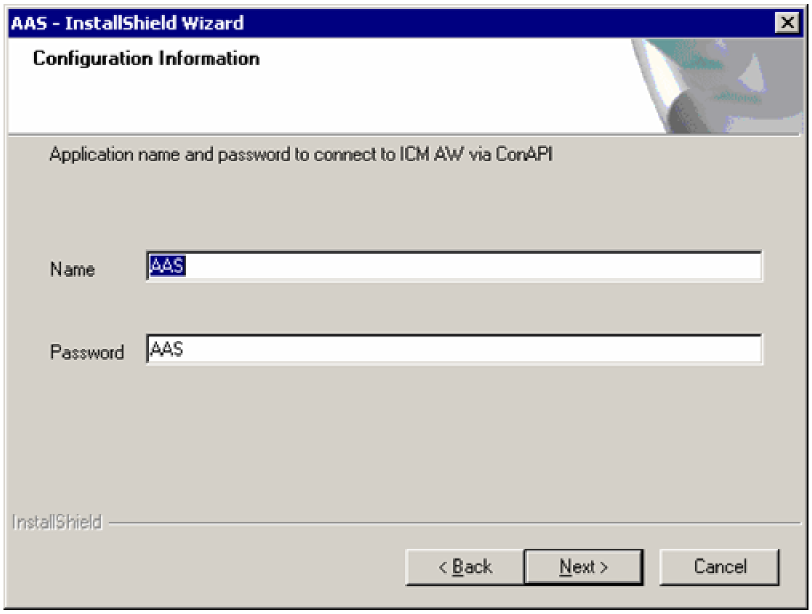
Link 2:

RMI port: 2099

Caution f you are using a secondary distributor, the names of the AAS clients *must* be different; for example, "AASClient1" cannot be the name of the Application link on both computers. If you have multiple AAS servers on your network, each one must have unique entries due to RMI requirements.

Step 6 Enter the application instance name and password/application key (if applicable) to connect to the Administration & Data Server; then click **Next**.

Figure 2-13 AAS InstallShield Wizard - Configuration Information



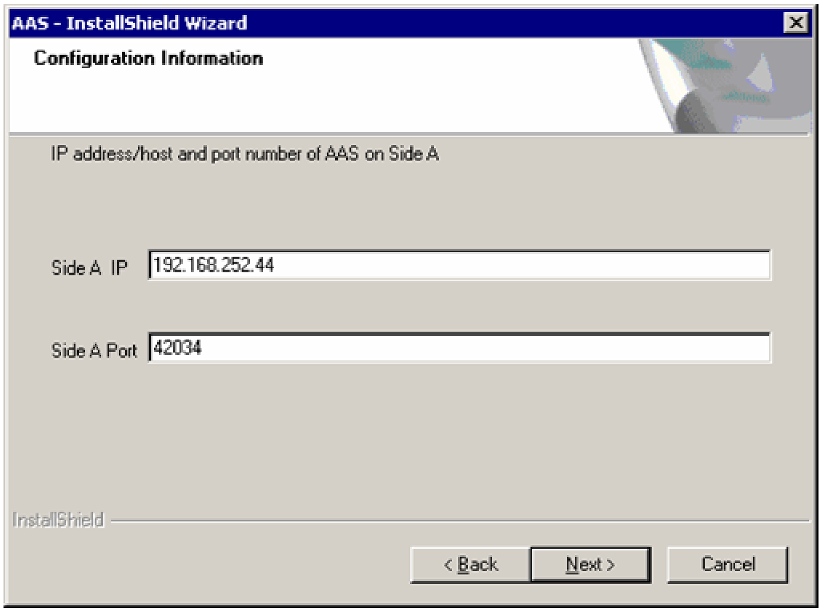
Application name and password to connect to ICM AW via ConAPI

Name: AAS

Password: AAS

Step 7 Enter the AAS machine IP address/host and port number (default displays) for Side A; then click **Next**.

Figure 2-14 AAS InstallShield Wizard - Configuration Information



AAS - InstallShield Wizard

Configuration Information

IP address/host and port number of AAS on Side A

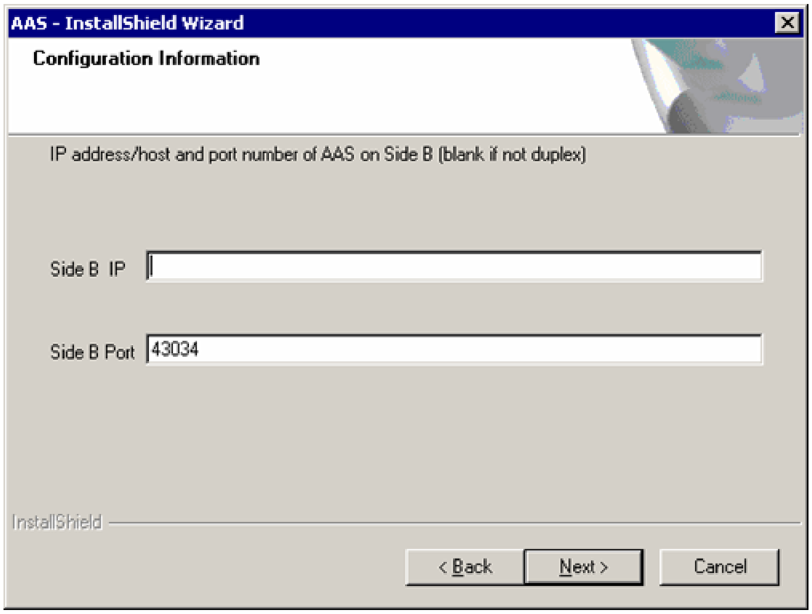
Side A IP: 192.168.252.44

Side A Port: 42034

Note *Do not* use the loopback IP address (127.0.0.1). Instead, use the *machine's* actual IP address.

Step 8 Enter the AAS machine IP address/host and port number (default displays) for Side B (if using a duplex system); then click **Next**.

Figure 2-15 AAS InstallShield Wizard - Configuration Information


AAS - InstallShield Wizard

Configuration Information

IP address/host and port number of AAS on Side B (blank if not duplex)

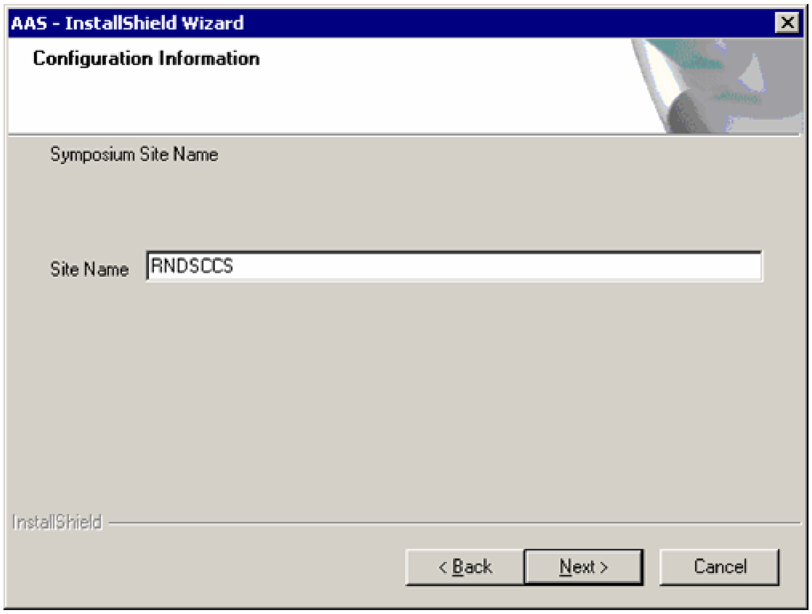
Side B IP

Side B Port 43034

Note *Do not* use the loopback IP address (127.0.0.1). Instead, use the *machine's* actual IP address.

Step 9 Enter the Symposium Site name and click **Next**. (This name is found in the Start\Programs\Symposium Call Center Server\System Information - Site Name directory.)

Figure 2-16 AAS InstallShield Wizard - Configuration Information



AAS - InstallShield Wizard

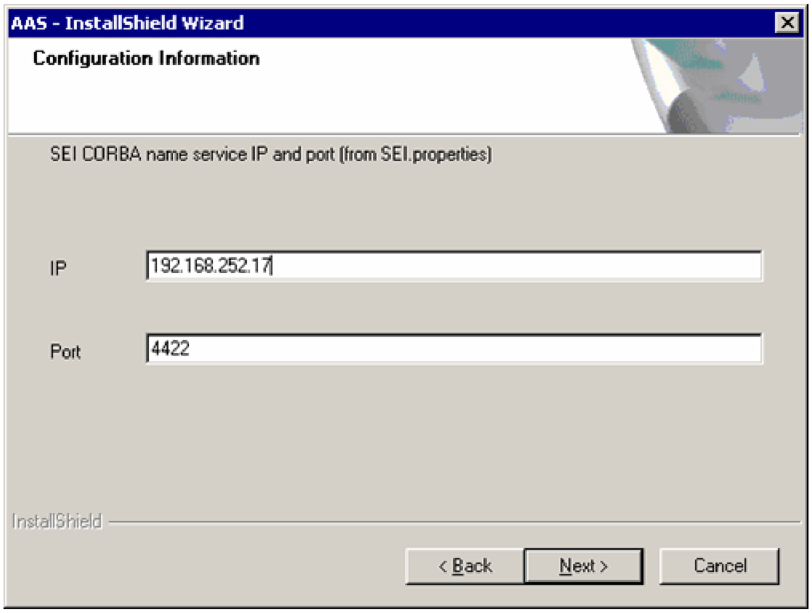
Configuration Information

Symposium Site Name

Site Name: RNDSCCS

Step 10 Enter the IP address and port number of the Symposium Call Center Server machine ("SEI CORBA" refers to the Symposium Call Center Server); then click **Next**.

Figure 2-17 AAS InstallShield Wizard - Configuration Information



AAS - InstallShield Wizard

Configuration Information

SEI CORBA name service IP and port (from SEI.properties)

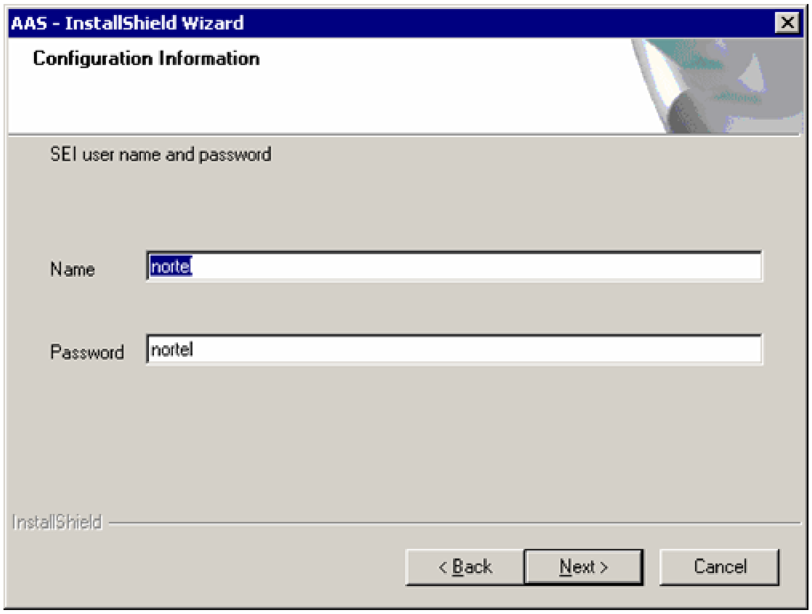
IP: 192.168.252.17

Port: 4422

Note SEI CORBA software is the CORBA naming service used by SEI. This information can be found in the SEI.properties file on the SCCS computer.

Step 11 Enter the SEI user name and password; then click **Next**.

Figure 2-18 AAS InstallShield Wizard - Configuration Information



AAS - InstallShield Wizard

Configuration Information

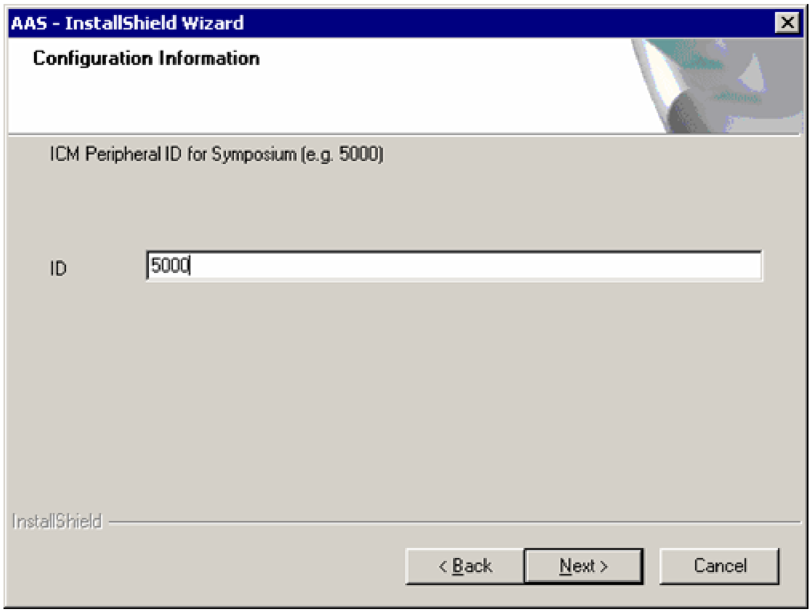
SEI user name and password

Name: nortel

Password: nortel

Step 12 Enter the ICM Peripheral ID for Symposium; then click **Next**.

Figure 2-19 AAS InstallShield Wizard - Configuration Information



AAS - InstallShield Wizard

Configuration Information

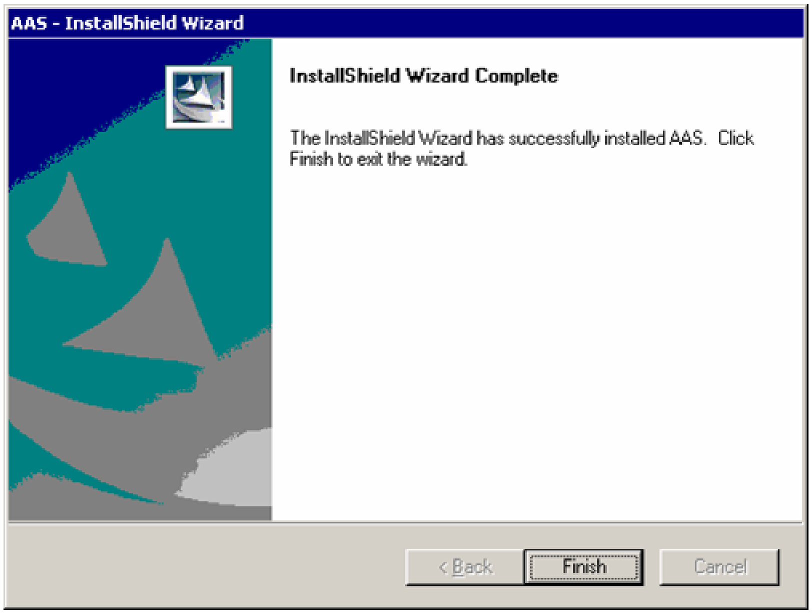
ICM Peripheral ID for Symposium (e.g. 5000)

ID: 5000

Step 13 The install program runs. When finished, the InstallShield Wizard Complete window displays stating that AAS has been successfully installed.

Step 14 Click **Finish**.

Figure 2-20 InstallShield Wizard Complete



InstallShield Wizard Complete

The InstallShield Wizard has successfully installed AAS. Click Finish to exit the wizard.

Step 15 If you are using ICM Release 5.0(0) SR10 or Release 6.0(0) SR3, you need to change the value of the following registry variable:

HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/EventLog/Application/Cisco Systems, Inc./ICM/CategoryCount

from **0x52** to **0x53**, if you want the Windows Event Log **Category** field to contain a symbolic name rather than a number for AAS messages.

Caution If you do not make this change, the **Category** field for AAS messages will contain the number 83.

Note You do not need to perform step 15 if you are running an SR beyond 5.0 SR10 and 6.0 SR3.

How to reinstall AAS on Unified ICM Releases Earlier Than ICM 7.1(3)

Step 1 Double-click the **aas_setup.exe** file on the CD. The AAS InstallShield Wizard displays.

Step 2 Select the **Install New or Reinstall AAS component** option; then click **Next**.

Step 3 Enter the name of the ICM instance, the PG name, and the AAS name that was entered for the original install; then click **Next**. By specifying the same information used for the original install, the process reinstalls over the top of the existing installation.

Step 4 Click **Yes** in the Question dialog box that asks for confirmation to reinstall.

Step 5 The next set of windows that display are the same as those shown for a new install. (See "How to Install AAS on Unified ICM Releases Earlier Than Unified ICM 7.1(3) (Standalone Installer)" section on page 2-15 for more information.)

Note Only the prompted information is overwritten during the reinstallation. Non-prompted settings (including tuning) in the registry are preserved.

How to remove AAS on Unified ICM Releases Earlier Than Unified ICM 7.1(3)

Step 1 Double-click the **aas_setup.exe** file on the CD. The AAS InstallShield Wizard displays.

Step 2 To remove one AAS instance, select the **Uninstall one AAS component** option; then click **Next**.

Step 3 Enter the name of the ICM instance, the PG name, and the AAS name that was entered for the original install; then click **Next**. (The process removes this AAS instance even if there are multiple AAS instances installed.)

Step 4 To remove all AAS instances on the computer, select the **Uninstall ALL AAS components** option; then click **Next**. (The process does not prompt for the instance names.)

How to Install or Reinstall AAS on Unified ICM 7.1(3) (Integrated Installer)

Step 1 From the ICM Installer, run the PG setup.

Step 2 At the PG setup screen:

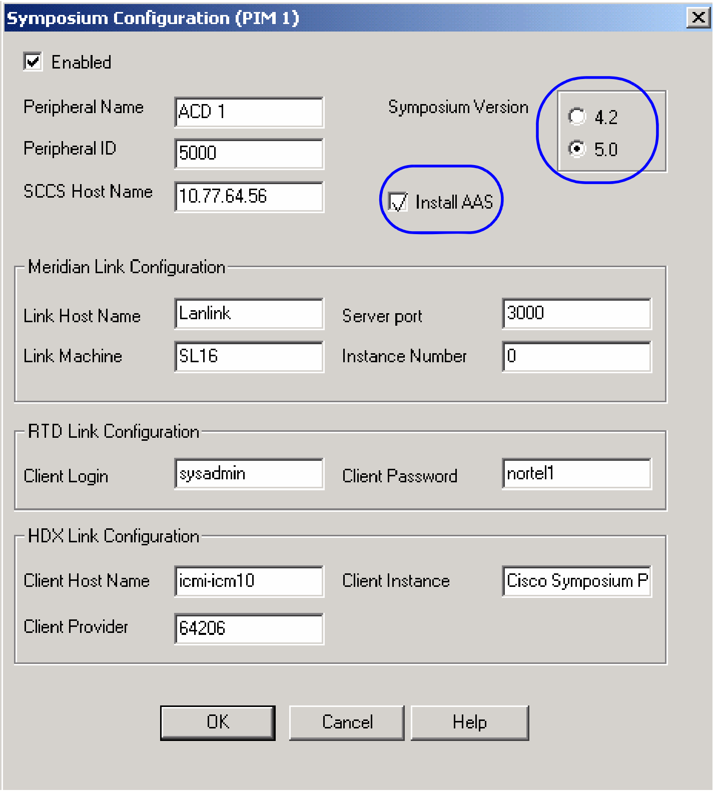
a. Select the Symposium Version **5.0**.

b. Check **Install AAS.**

c. Select **Yes** at the prompt to confirm the installation.

d. Click **OK** to open the AAS Configuration screen.

Figure 2-21 Symposium Configuration



Symposium Configuration (PIM 1)

☑ Enabled

Peripheral Name: ACD 1
Peripheral ID: 5000
SCCS Host Name: 10.77.64.56

Symposium Version: ○ 4.2 ● 5.0

☑ Install AAS

Meridian Link Configuration
Link Host Name: Lanlink
Server port: 3000
Link Machine: SL16
Instance Number: 0

RTD Link Configuration
Client Login: sysadmin
Client Password: nortel1

HDX Link Configuration
Client Host Name: icmi-icm10
Client Instance: Cisco Symposium P
Client Provider: 64206

Step 3 At the AAS Configuration screen (Figure 3-7 shows the AAS Configuration screen):

a. Enter the Symposium Site Name. (You will find this name in the Start\Programs\Symposium Call Center Server\System Information - Site Name directory.)

b. Enter the details of the Administration & Data Server machine of primary distributor under **Administration & Data Server-1 Information**:

- **Host Name:** The Administration & Data Server machine IP address for ICM Primary Administration & Data Server.
- **Administration & Data Server Link1:** The ICM Administration & Data Server Link 1 name for the Primary Distributor. (The Administration & Data Server Link 1 name should be the same as used in Step 4 in "How to establish an administration connection" section on page 3-3.)
- **Application Link1:** The Application Link 1 name for the Primary Distributor.

c. Enter the details of the Administration & Data Server machine of secondary distributor (if used) under **Administration & Data Server-2 Information**:

- **Host Name:** The Administration & Data Server machine IP address for ICM Secondary Administration & Data Server.
- **Administration & Data Server Link2:** The Administration & Data Server Link 2 name for the Secondary Distributor. (The Administration & Data Server Link 2 name should be the same as used in Step 4 in the "How to establish an administration connection" section on page 3-3.)

Caution If you are using a secondary distributor, the names of the AAS servers must be different; for example, "AASServer1" cannot be the name of the Administration & Data Server link on both computers. If you have multiple AAS servers on your network, each one must have unique entries due to RMI requirements.

- **Application Link2:** The Application Link 2 name for the Secondary Distributor.

Caution If you are using a secondary distributor, the names of the AAS servers must be different; for example, "AASClient1" cannot be the name of the Application link on both computers. If you have multiple AAS servers on your network, each one must have unique entries due to RMI requirements.

d. Enter the details of the AAS host under **AAS Host Information**:

- **Application User ID:** The Application Instance name
- **Application Password:** The Application password

Note For the application instance name, use the same name entered in Step 3a. in "How to configure an application instance" section on page 3-2. The password/application key is the same number used in Step 3b.

- **SideA Host Name:** The AAS machine IP address/host for Side A

Note **SideB Host Name:** The AAS machine IP address/host for Side B. *Do not* use the loopback IP address (127.0.0.1). Instead, use the *machine's* actual IP address.

- **Local RMI Port:** The local RMI registry port number
- **Remote RMI Port:** The remote RMI registry port number

Note The RMI port should be the same as used in Step 4 in the "How to establish an administration connection" section on page 3-3.)

- **SideA Port:** The AAS machine's Port for Side A
- **SideB Port:** The AAS machine's Port for Side B

e. Enter the details of the SEI CORBA host under **SEI CORBA Information**:

- **SEI CORBA Hostname:** The IP address of the Symposium Call Center Server machine ("SEI CORBA" refers to the Symposium Call Center Server.)
- **SEI CORBA Port:** The Port of the Symposium Call Center Server machine ("SEI CORBA" refers to the Symposium Call Center Server.)

Note SEI CORBA software is the CORBA naming service used by SEI. This information can be found in the SEI.properties file on the SCCS computer.

f. Enter the details of the SEI User under **SEI User Information**:

- **Name:** The SEI User Name
- **Password:** The SEI Password

Step 4 Click **OK**.

Step 5 Click **Next** to finish the PG setup.

How to remove AAS for Unified ICM 7.1(3)

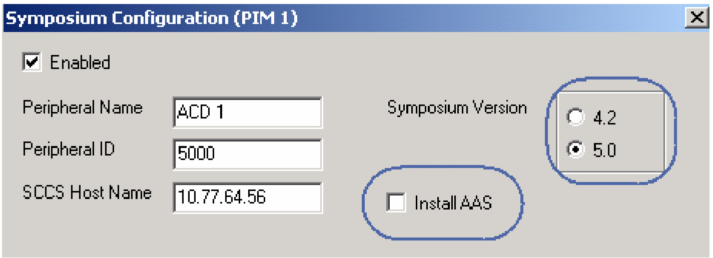
Step 1 From the ICM Installer, run the PG setup.

Step 2 At the PG setup screen:

a. Select the Symposium Version **5.0**.

b. Deselect **Install AAS**.

Figure 2-22 Symposium Configuration



Symposium Configuration (PIM 1)

☑ Enabled

Peripheral Name: ACD 1

Peripheral ID: 5000

SCCS Host Name: 10.77.64.56

Symposium Version: ○ 4.2 ● 5.0

□ Install AAS

Note If you are using Symposium versions higher than 5.0, select **5.0**.

Step 3 Click **OK**.

Step 4 Click **Next** to finish PG Setup.

Real-time Monitoring of AAS

Real-time monitoring of AAS is supported from Unified ICM 8.0(1) onwards. Real-time monitoring is a supervision mechanism to monitor AAS using Simple Network Management Protocol (SNMP) traps.

This feature helps you to:

- Determine the status (active or inactive) of AAS
- Receive status notifications/alerts

Configuring the SNMP Service

The SNMP Service should be configured on the Logger machine. Follow these steps to configure the SNMP service for Windows 2003 and Windows XP:

Step 1 Go to **Start** > **Control Panel** > **Add or Remove Programs**.

Step 2 In the Add or Remove Programs window, click the **Add or Remove Windows Components** icon. The Windows Components Wizard window appears.

Step 3 Select the **Management and Monitoring Tools** check box and click the **Details** button. The Management and Monitoring Tools window appears.

Step 4 In the Management and Monitoring Tools window, select the **Simple Network Management Protocol** check box.

Step 5 Click **OK**.

Step 6 Click **Next** in the Windows Components Wizard window. SNMP services will be installed on your system.

Note

- If you are prompted, insert the Windows setup CD/DVD disc into your optical drive. The SNMP services will start automatically.
- It is recommended to verify the service status from **Start** > **Control Panel** > **Administrative Tools** > **Component Services** > **Services**. If the service has stopped, you must start the SNMP service from the above location.

The following services are available after the SNMP service configuration:

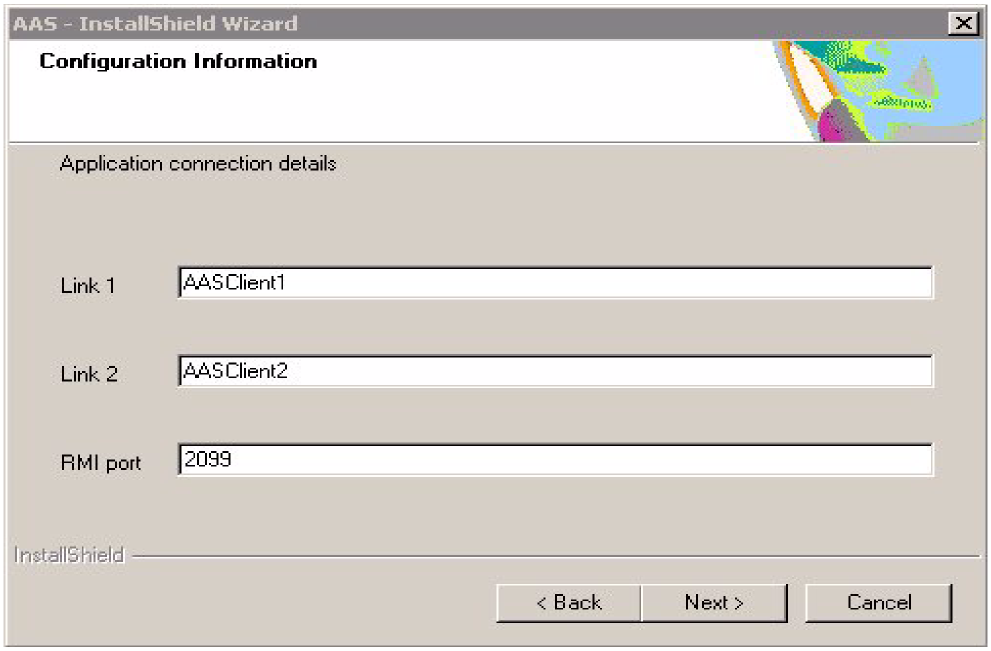
- SNMP Service: The main engine which monitors the network device activities, and sends the monitoring data to the monitoring console workstation.
- SNMP Trap Service: Receives trap messages generated by local or remote SNMP agents and forwards the messages to the SNMP management programs running on your computer.

Registering a Remote Machine with the Logger Machine

Steps to register a Remote machine with the Logger machine:

Step 1 From the command-line interface of your Logger machine, type the “mmc” command. The Console1 window appears.

Figure 2-23 Console1 Window



AAS - InstallShield Wizard

Configuration Information

Application connection details

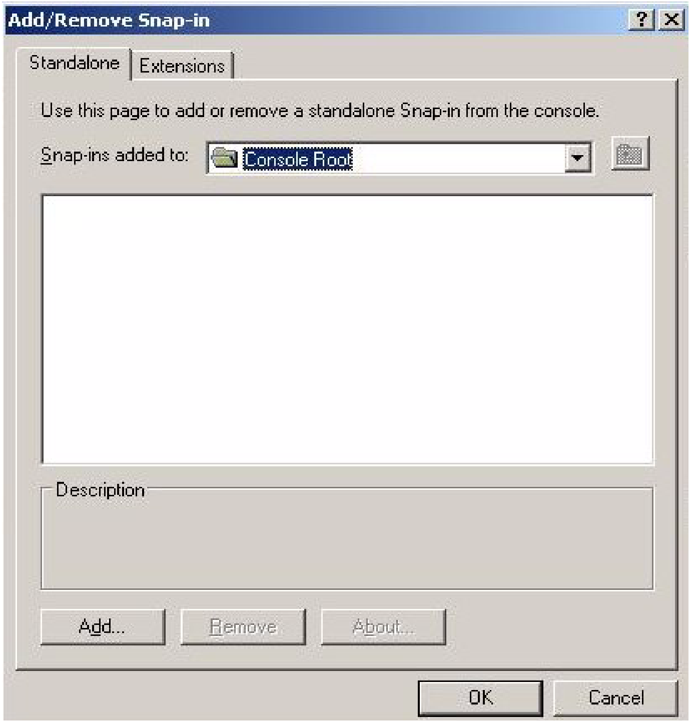
Link 1: AASClient1

Link 2: AASClient2

RMI port: 2099

Step 2 Choose **File** > **Add/Remove Snap-in**. The Add/Remove window appears.

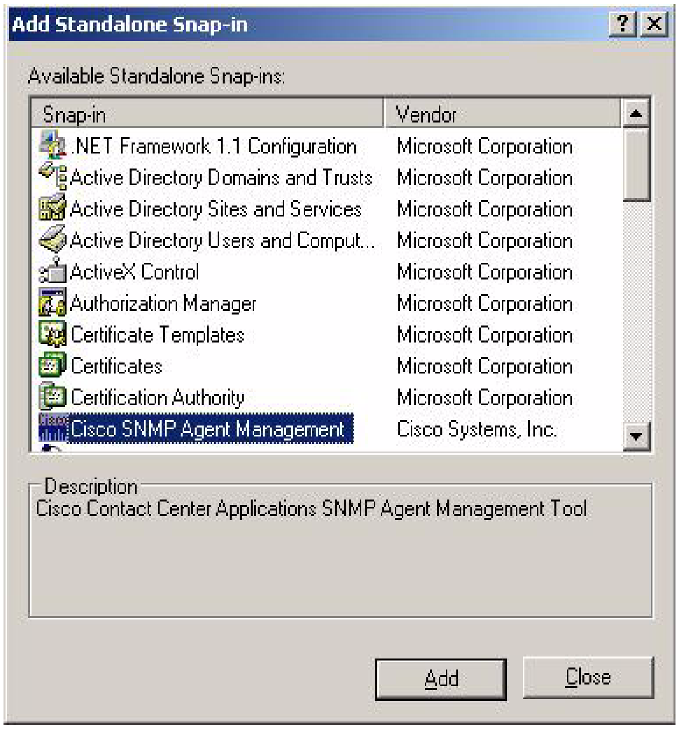
Figure 2-24 Add/Remove Snap-in



Snap-ins added to: Console Root

Step 3 In the **Add/Remove** window (Figure 2-24), click **Add**. The Add Standalone snap-in window appears.

Figure 2-25 Add Standalone Snap-in



Snap-in	Vendor
.NET Framework 1.1 Configuration	Microsoft Corporation
Active Directory Domains and Trusts	Microsoft Corporation
Active Directory Sites and Services	Microsoft Corporation
Active Directory Users and Comput...	Microsoft Corporation
ActiveX Control	Microsoft Corporation
Authorization Manager	Microsoft Corporation
Certificate Templates	Microsoft Corporation
Certificates	Microsoft Corporation
Certification Authority	Microsoft Corporation
Cisco SNMP Agent Management	Cisco Systems, Inc.

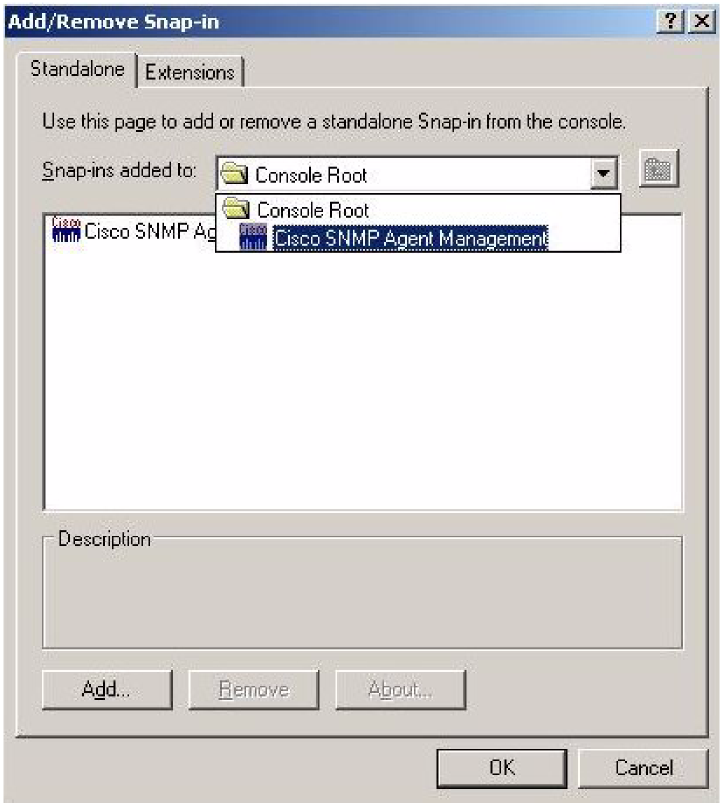
Description: Cisco Contact Center Applications SNMP Agent Management Tool

Step 4 Choose **Cisco SNMP Agent Management** snap-in list and click **Add**.

Step 5 Click **Close** to exit the Add Standalone snap-in window.

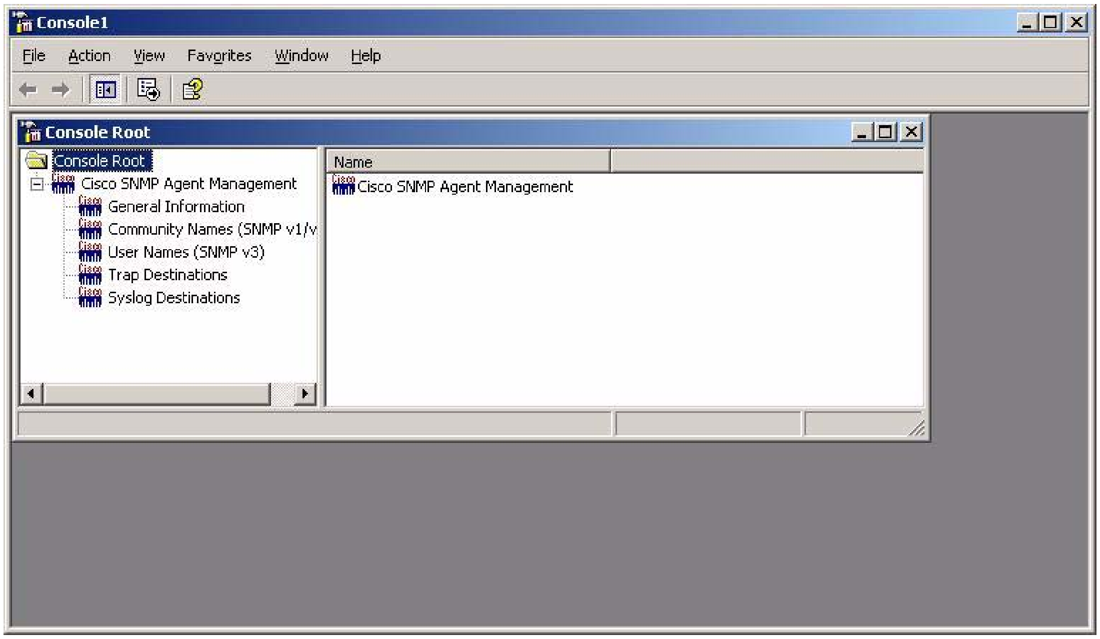
Step 6 In the Add/Remove window, select **Cisco SNMP Agent Management** from the **Snap-ins added to** drop-down list.

Figure 2-26 Add/Remove Snap-in Window



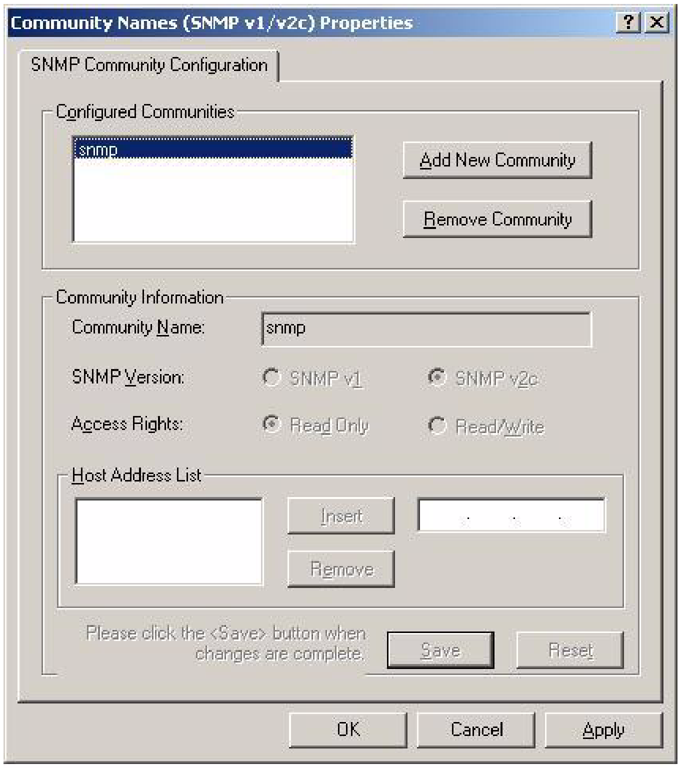
Step 7 Expand the Cisco SNMP Agent Management option.

Figure 2-27 Cisco SNMP Agent Management



Step 8 Right click Community Names (SNMP v1/v2c) and choose **Properties**. The Community Names (SNMP v1/v2c) Properties window appears.

Figure 2-28 Community Names (SNMP v1/v2c) Properties



Configured Communities: snmp

Community Name: snmp

SNMP Version: ○ SNMP v1 ● SNMP v2c

Access Rights: ● Read Only ○ Read/Write

Please click the <Save> button when changes are complete.

Step 9 Enter the community name in **Community Name** text box and choose the appropriate SNMP version.

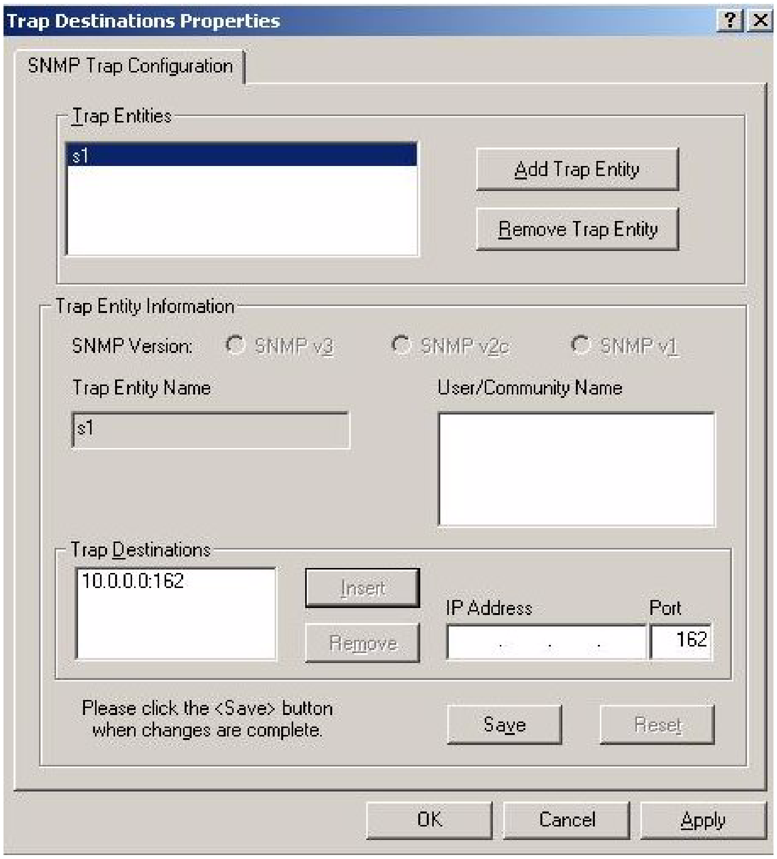
Step 10 Click **Add Community**. The new community is displayed in the Configured Communities text box.

Step 11 Click **Apply** to apply the changes.

Step 12 Click **OK** to exit the Community Names (SNMP v1/v2c) Properties window.

Step 13 In the Cisco SNMP Agent Management (Figure 2-27), right click Trap Destination and choose **Properties**. The Trap Destination Properties window appears.

Figure 2-29 Trap Destinations Properties



Trap Entities: s1

Trap Entity Name: s1

Trap Destinations: 10.0.0.0:162

Port: 162

Please click the <Save> button when changes are complete.

Step 14 Select the appropriate trap entry and enter the IP address of the Remote machine.

Step 15 Click **Insert**. The IP address of the Remote machine is updated in the **Trap Destinations** text box of the Logger machine.

Step 16 Click **Save**.

Step 17 Click **Apply** to apply the changes.

Step 18 Click **OK** to exit the Trap Destination Properties window.

Note Do not configure a firewall for AAS.

CHAPTER 3

Configuring the ICM ConAPI Connection

This chapter includes the following sections:

About Unified ICM Application Instances

ICM application instances allow identification and access to the Unified ICM Configuration Management System (CMS). The application instance basically provides the authentication for that connection.

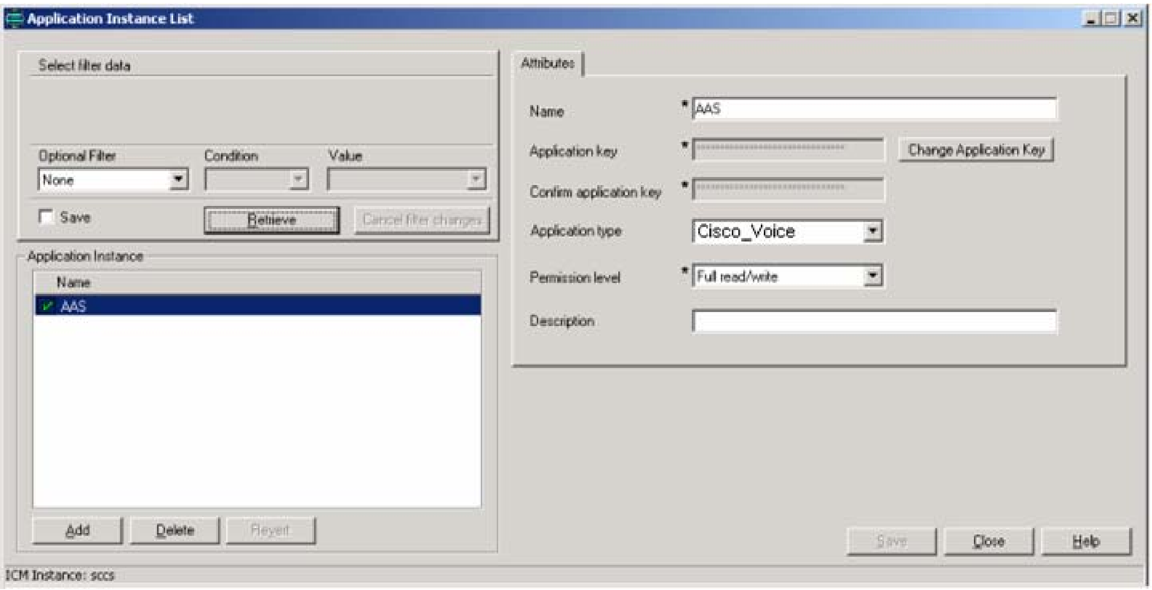
About Configuring Application Instances

You must configure a single application instance to support one or more AAS servers. One application connection is required for each AAS Server.

How to configure an application instance

Step 1 From the Unified ICM Configuration Manager, select **Tools > List Tools > Application Instance List**. The Application Instance List window displays.

Figure 3-1 Application Instance List



Optional Filter: None
Condition:
Value:
□ Save

Name
✓ AAS

Name * AAS
Application key * ****************************
Confirm application key * ****************************
Application type Cisco_Voice
Permission level * Full read/write
Description

ICM Instance: sccs

Step 2 Click **Retrieve** and then **Add** to display the Attributes tab.

Step 3 Enter the following information:

a. **Name.** The enterprise name for the application instance. (This is the same name you entered to connect to the Administration & Data Server while installing AAS.)

b. **Application key.** This is the password that the integrated application will use to be identified by the Unified ICM.

c. **Application type.** Select **Cisco_Voice**.

d. **Permission level.** Select the **Full read/write** level from the drop-down list. This level must be selected; otherwise, AAS will not be able to save configuration changes.

Step 4 After entering the required fields, save the configuration and close the window.

About Establishing Administration Connections

You must configure a communications path between the Unified ICM and the AAS application using the CMS Control application.

Note **Important!** The **CMS Node** check box in the Real-time Distributor Node Properties window must be enabled on the Administration & Data Server component in Unified ICM Setup to successfully configure a communications path. For more details, see the *Configuration Guide for Cisco Unified ICM Enterprise* available at Cisco.com.

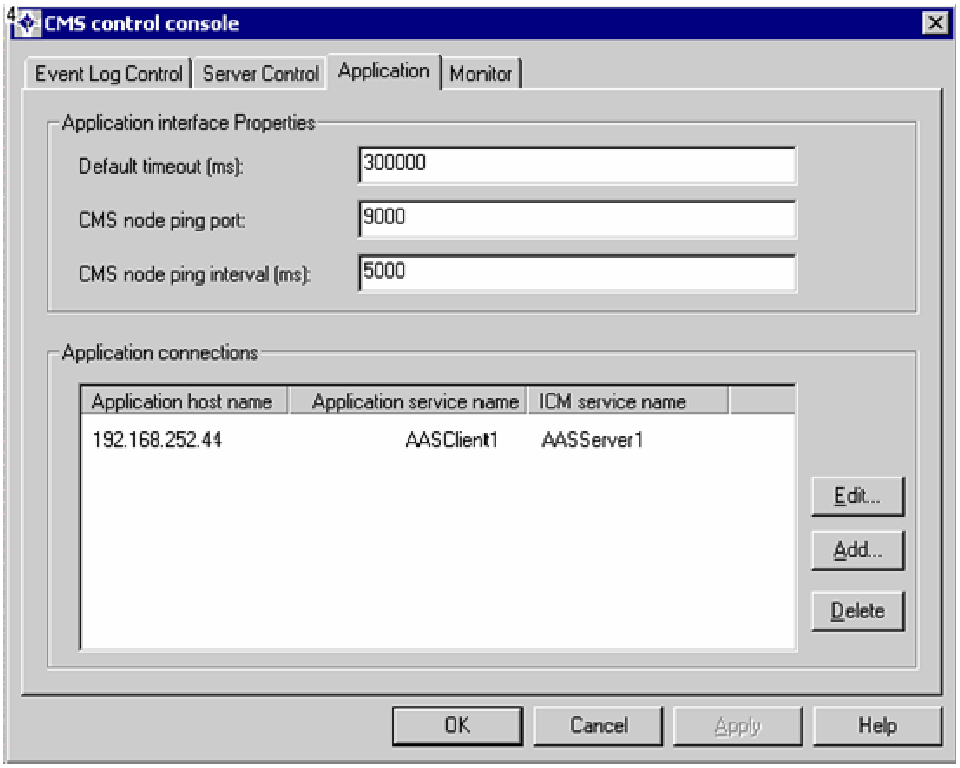
How to establish an administration connection

Perform the following steps for each AAS application you are setting up.

Step 1 Select **Start > Programs > Administration & Data Server > CMS Control**.

Step 2 Select the **Application** tab.

Figure 3-2 CMS control console



Default timeout (ms): 300000

CMS node ping port: 9000

CMS node ping interval (ms): 5000

Application host name	Application service name	ICM service name
192.168.252.44	AASClient1	AASServer1

Step 3 Click **Add**. The Application Connection Details dialog box displays.

Step 4 Enter the application connection properties. Complete this window as follows:

a. **Administration & Data Server link**. Enter the link name on ICM; for example, enter "AASServer" followed by a unique identifier such as "AASServer1" or "AASServer2".

b. **Administration & Data Server RMI registry port**. Enter the RMI registry port for ICM.

Note The **Administration & Data Server RMI registry port** number and the **Application RMI registry port** number must be the same.

c. **Application link**. Enter the link name for the application; for example, use "AASClient" followed by a unique identifier such as "AASClient1".

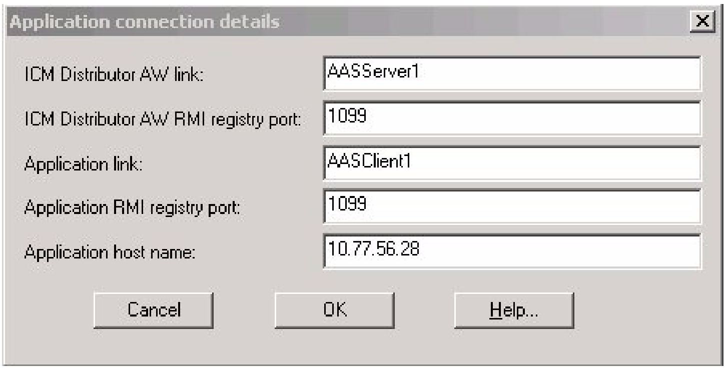
d. **Application RMI registry port**. Enter the RMI registry port for the application.

e. **Application host name**. Enter the host name or IP address of the application. (This is the host name/IP address of the computer where AAS is running.)

Step 5 Click **OK** twice. This restarts the Cms_Jserver on the Administration & Data Server.

Figure 3-3 and Figure 3-4 illustrate the windows in the Administration & Data Server where you must enter the RMI connection details.

Figure 3-3 ICM Application Connection Details Window for Side A



Application connection details

ICM Distributor AW link: AASServer1

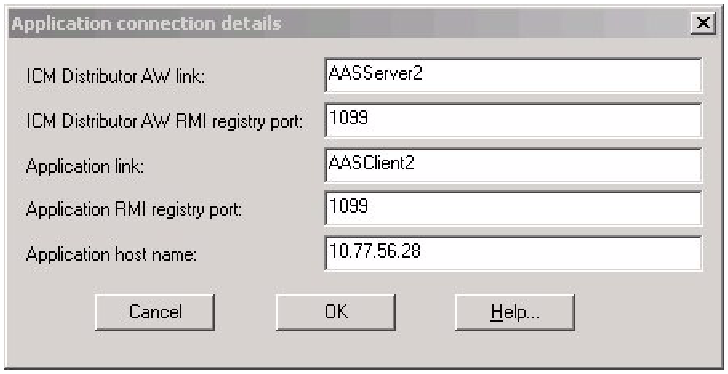
ICM Distributor AW RMI registry port: 1099

Application link: AASClient1

Application RMI registry port: 1099

Application host name: 10.77.56.28

Figure 3-4 ICM Application Connection Details Window for Side B



Application connection details

ICM Distributor AW link: AASServer2

ICM Distributor AW RMI registry port: 1099

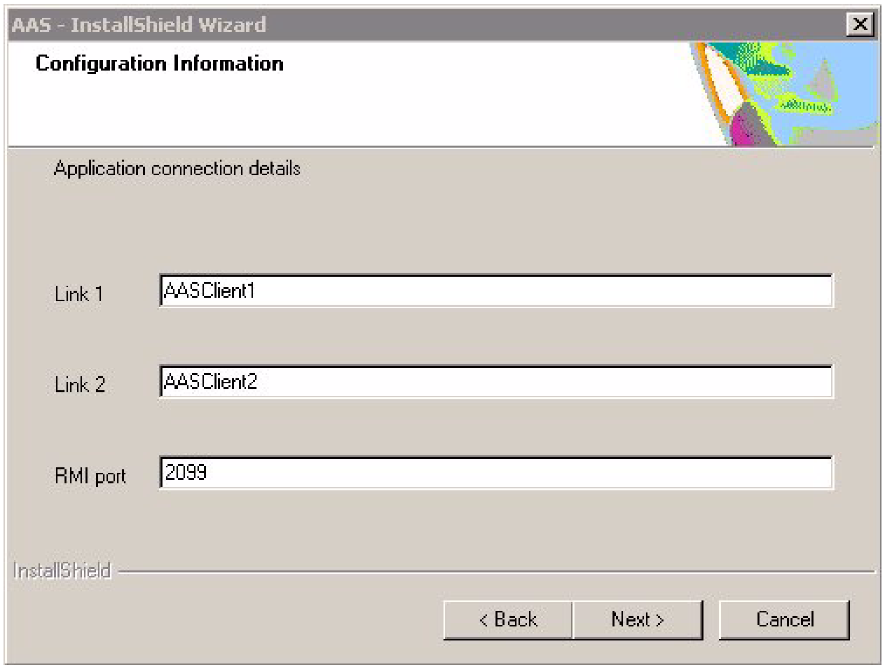
Application link: AASClient2

Application RMI registry port: 1099

Application host name: 10.77.56.28

Figure 3-5 illustrates the window in the AAS installation program where you must enter the Administration & Data Server connection details. (See Installing AAS, page 2-14 for more details about the AAS installation program.)

Figure 3-5 AAS Application Connection Details Window for Administration & Data Server (Standalone Installer)



AAS - InstallShield Wizard

Configuration Information

Application connection details

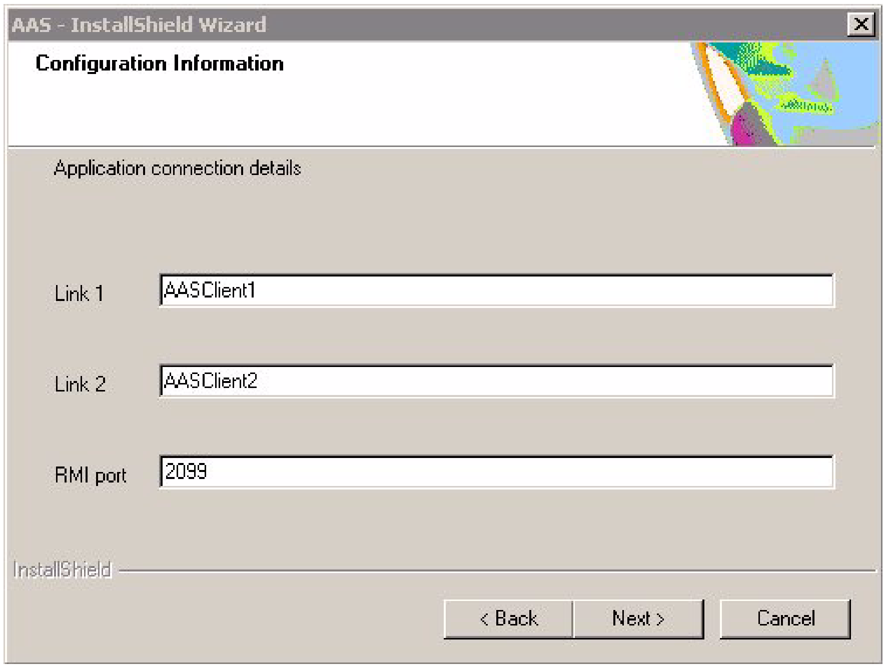
Link 1: AASClient1

Link 2: AASClient2

RMI port: 2099

Figure 3-6 illustrates the window in the AAS installation program where you must enter the application connection details. (See Installing AAS, page 2-14 for more details about the AAS installation program.)

Figure 3-6 AAS Application Connection Details Window (Standalone Installer)



AAS - InstallShield Wizard

Configuration Information

Application connection details

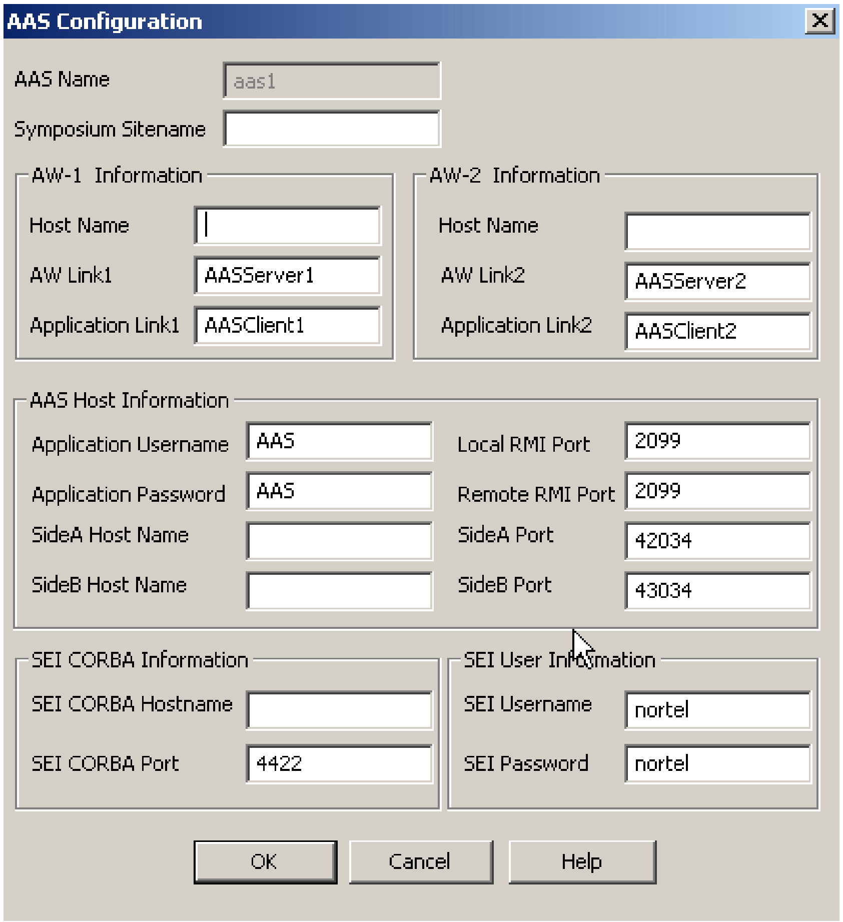
Link 1: AASClient1

Link 2: AASClient2

RMI port: 2099

Note **Important!** You must ensure that the values entered on the AAS application match those entered on the Administration & Data Server because ICM must be configured before AAS is installed.

Figure 3-7 AAS Configuration and Application Connection Details (Integrated Installer)



AAS Configuration

AAS Name: aas1
Symposium Sitename:

AW-1 Information
Host Name:
AW Link1: AASServer1
Application Link1: AASClient1

AW-2 Information
Host Name:
AW Link2: AASServer2
Application Link2: AASClient2

AAS Host Information
Application Username: AAS
Application Password: AAS
SideA Host Name:
SideB Host Name:
Local RMI Port: 2099
Remote RMI Port: 2099
SideA Port: 42034
SideB Port: 43034

SEI CORBA Information
SEI CORBA Hostname:
SEI CORBA Port: 4422

SEI User Information
SEI Username: nortel
SEI Password: nortel

CHAPTER 4

Debugging and Throttling

This chapter includes the following sections:

AAS Throttling Guidelines

The AAS throttling mechanism depends on the following parameters:

- Number of records being updated in a single transaction
- Throttling delay in processing events from Nortel Symposium ACD

The above mentioned parameters are controlled by the registry. Tuning the registry keys for these parameters will help you resolve the following errors:

1. Changes in the Symposium Contact Center Manager are taking too long to propagate to Unified ICM. This problem can be the result of an overtaxed machine or:

   a. It could be that the queueing delay is set too high in the registry. To fix the latter, look at the registry value HKEY_LOCAL_MACHINE/SOFTWARE/Cisco Systems, Inc./ICM/<*ICM instance*>/PG<*XX*>/PG/CurrentVersion/AASS/aas<*X*>/AASData/Dynamic/AASSEIThrottleSeiEventQueueDelay. Reduce the value in increments of 25 (down to a minimum of 0) until throughput increases to the desired rate.

      Note This value can be changed without restarting AAS.

   b. Check HKEY_LOCAL_MACHINE/SOFTWARE/Cisco Systems, Inc./ICM/<*ICM instance*>/PG<*XX*>/PG/CurrentVersion/AASS/aas<*X*>/AASData/Dynamic/AASConAPIThrottleMaxModificationsPerTrans to see if it is too low. Changing this value primarily affects resynchronizations, shift changes, and imports. Try increasing this value in increments of 50 until the desired performance is achieved. This setting requires the value mentioned in Option c. below to be set to "true." The maximum value supported under Unified ICM Release 5.0(0) is 100. Using a value higher than 100 will most likely break the bulk processing AAS does during a resync. In Unified ICM Release 6.0(0), do not use a value greater than 200.

      Note This value can be changed without restarting AAS.

c. Check HKEY_LOCAL_MACHINE/SOFTWARE/Cisco Systems, Inc./ICM/<*ICM instance*>/PG<*XX*>/PG/CurrentVersion/AASS/aas<*X*>/AASData/Config/AASSEIUseBulkProcessing. This allows AAS to process bulk database transactions on ICM, which is significantly quicker than processing them one-by-one. Make sure this value is set to “true.” You must restart AAS if you change this setting.

Note If none of these solutions resolve the problem, there may be other applications drawing too much attention from the CPU or network traffic might be too slow.

2. AAS is using too much CPU. You can tune this by increasing the AASSEIThrottlingSeiEventQueueDelay value in the registry (found at HKEY_LOCAL_MACHINE/SOFTWARE/Cisco Systems, Inc./ICM/<*ICM instance*>/PG<*XX*>/PG/CurrentVersion/AASS/aas<*X*>/AASData/Dynamic/). Increase the value in increments of 25 until the CPU usage drops to an acceptable level.

Note This value can be changed without restarting AAS.

Debugging

For troubleshooting AAS, you may need to increase the AAS log level. While troubleshooting the CMS Node and CMS JServer logs may also need to be captured.The maximum trace level that can be set for AAS, CMS Node, and CMS Jserver is 0xffffffff (Hex).

The following section gives more information on the debug trace levels for AAS.

Debug Trace Levels for AAS

AAS uses EMS for logging. EMS outputs to Event Viewer, log file, screen, and SNMP. You can use Cisco’s Dumplog application to view the AAS logs.

The following debug trace levels are defined for AAS. You can turn on these debug trace levels to provide more tracing details in AAS logs, which can be useful for troubleshooting:

- EMS_TRACE_GENERAL = 0x1
- EMS_TRACE_CONAPI = 0x2
- EMS_TRACE_SEI = 0x4
- EMS_TRACE_AASDRIVER = 0x8
- EMS_TRACE_MSL = 0x10

CHAPTER 5

Limitations of Automated Administrator for Symposium

This chapter includes the following sections:

Limitations of AAS

The following are the known limitations of AAS:

- Remove all skill groups from ICM before installing and running AAS; otherwise, there could be a conflict between the ICM PeripheralNumber and the Symposium Skillset ID. When deleting skill groups, persons, or agents in ICM, delete them permanently.
- Make sure the PG name in ICM and the skill group name in Symposium are kept short; otherwise, AAS will not be able to generate a unique Enterprise name for the skill group in ICM. The total length of the PG name and the skill group name *combined* cannot be more than 28 characters.
- The Symposium Skillset name cannot be longer than 29 characters; otherwise, AAS will not be able to generate a unique peripheral name for the skill group in ICM.
- AAS does not support redundant connection to the Symposium SEI interface.
- Agents in standby mode on the SCCS will not be updated by AAS onto ICM.
- AAS does not have WebView supervision – the only way to determine the status of AAS is via the console window and logs.
- AAS does not filter any events for agents and skill groups from SCCS; hence, all events of Symposium related to non- monitored ICM agents are processed by AAS.
- While AAS is updating records in the steady state, opening and saving of scripts in the Script Editor may be impacted by the rate of the configuration changes.
- AAS supports up to 600 configuration changes/hour. If you are performing automated configuration changes on SCCS, ensure that the number of changes/hour do not exceed this limit. Exceeding this limit can make the Script Editor unusable.
- You cannot make the configuration changes when the preferred side of the Router is down.

- AAS supports a maximum of two Network Interface Controllers (NICs) - One is for connection between the PG/AAS and the Nortel SCCS, and the second is for connection between the duplex (A/B) PG pair.

Nortel SCCS Limitations

The following are the limitations in AAS caused due to Nortel SCCS limitations:

- Symposium does not expose the names of the agents in the SEI events. Therefore, AAS uses the agent ID to populate the First/Last Name in the Person table.
- AAS does not synchronize data from ICM to SCCS.
- Changes to agents skill sets made in ICM are not automatically reflected onto the SCCS.
- Deleting an agent or skill group from SCCS in the Nortel Symposium Administration does not unassign the agent from all the skill groups in ICM. The Symposium PG does not send any event to ICM on agent deletion. Due to this limitation, the agent will not get deleted in ICM and will remain assigned to the associated skill groups. This may lead to increase in the size of the database. To avoid this, agents and skillsets need to be deleted manually in ICM.
- Firewall between AAS and SCCS is not supported because the Nortel SCCS port is dynamic.

Limitations of Standalone Installer

- After AAS installation, if the ICM PG setup is run again, all the AAS registry keys are deleted. In this case, AAS setup needs to be re-run after the PG setup.

Limitations of Integrated Installer

- There can be only one AAS instance installed for each Symposium PIM.

APPENDIX A

Working with Registry Settings

This appendix includes the following topics:

- Working with Registry Settings, page A-1

Working with Registry Settings

AAS saves all of its configuration information in the registry. The following sections describe the configuration registry settings and the dynamic registry settings.

⚠ **Caution** Make changes in the registry entries only if you are familiar with working with the registry, or with the guidance of technical support.

Configuration Registry Settings

The following tables describe the configuration registry entries located under the configuration tree.

After changing these registry entries, you *must* restart the AAS server for changes to take effect.

Table A-1 Configuration information used by AAS – Duplex AAS Systems

Registry Value	Type	Comments
AASPGHostA	String	IP address/Host of AAS Server A Default: <blank>
AASPGPortA	DWORD	MSL Port of AAS Server A Default: 42034
AASPGHostB	String	IP address/Host of AAS Server B Default: <blank>
AASPGPortB	DWORD	MSL Port of AAS Server B Default: 43034

Base: HKEY_LOCAL_MACHINE/SOFTWARE/Cisco Systems, Inc./ICM/<*ICM instance*>/PG<*XX*>/PG/CurrentVersion/AASS/aas<*X*>/AASData/Config

Note <*ICM instance*> and PG<*XX*> values are obtained from NodeManager.

Table A-2 Configuration Information Used by AAS – ConAPI

Registry Value	Type	Comments
AASConAPILocalServiceName1	String	The local RMIDriver connection end-point identity. Value will be “AASClient” followed by AAS instance; for example, AASClient1. Default: AASClient1 The value is case-sensitive
AASConAPILocalServiceName2	String	The local RMIDriver connection end-point identity for the second remote host (if configured). Value will be “AASClient” followed by AAS instance; for example, AASClient2. This service name is only used when attaching to RemoteHost2. Default: AASClient2 The value is case-sensitive.
AASConAPILocalRegistryPort	DWORD	The local port for RMI register. Default: 2099

Table A-2 Configuration Information Used by AAS – ConAPI (continued)

Registry Value	Type	Comments
AASConAPIRemoteServiceName 1	String	The remote RMIDriver connection end point identity. Value will be "AASServer" followed by AAS instance; for example, AASServer1. Default: AASServer1 The value is case-sensitive.
AASConAPIRemoteServiceName 2	String	The remote RMIDriver connection end point identity for the second remote host (if configured). Value will be "AASServer" followed by AAS instance; for example, AASServer2. This service name is only used when attaching to RemoteHost2. Default: AASServer2 The value is case-sensitive.
AASConAPIRemoteRegistryPort	DWORD	The port for RMI register at the remote computer. Default: 2099
AASConAPIDisableAutoConnect	DWORD	Default: false
AASConAPIRemoteHost1	String	Location of the Administration & Data Server-1. Default: 127.0.0.1 (localhost) The value is case-sensitive.
AASConAPIRemoteHost2	String	Location of the Administration & Data Server-2. Default: <blank> The value is case-sensitive.
AASConAPITransportType	String	The type of network layer implementation. Default: RmiDriver The value is case-sensitive.
AASConAPIConnectionAttempts	DWORD	The number of times the AAS application attempts to find the distributor. Default: 1 Maximum: 10
AASConAPILocalPort	DWORD	The Administration & Data Server RMI Registry Port (as shown on CMS Control). Default: 0
AASConAPIType	String	The type of the ConAPI implementation. Default: Remote The value is case-sensitive.
AASConAPIDefaultTimeout	DWORD	The time in msec a thread will block waiting for a reply. Default: 30000 Maximum: 300000

Table A-2 Configuration Information Used by AAS – ConAPI (continued)

Registry Value	Type	Comments
AASConAPINumRetryAttempts	DWORD	Number of times to retry a ConAPI operation. Default: 2 Maximum: 10
AASConAPIUserName	String	Application name to connect to Administration & Data Server via ConAPI. Default: AAS The value is case-sensitive.
AASConAPIUserPassword	DWORD	Application password to connect to Administration & Data Server via ConAPI. The password is NOT encrypted. Default: AAS The value is case-sensitive.
AASConAPIMaxConnTries	DWORD	Maximum number of tries to connect to an Administration & Data Server before trying the other Administration & Data Server . Default: 2 Maximum: 10
AASPeripheralID	DWORD	Peripheral ID for Symposium. Default: 0
AASConAPIRenameSubSkillGroups	String	Indicates whether AAS will manually rename sub skill groups when a base skill group is renamed. This corrects a problem in Unified ICM releases prior to Release 7.0(0). Default (releases prior to Unified ICM Release 7.0(0)): True, else False.
AASRetriesToRestart	DWORD	Number of attempts AAS tries to get all of its services working before terminating itself, so that it can be restarted by the PIM. Default: 3 Minimum: 1 Maximum: 0x7fffffff

Base: HKEY_LOCAL_MACHINE/SOFTWARE/Cisco Systems, Inc./ICM/<*ICM instance*>/PG<*XX*>/PG/CurrentVersion/AASS/aas<*X*>/AASData/Config

Note <*ICM instance*> and PG<*XX*> values are obtained from NodeManager.

Table A-3 Configuration Information Used by AAS – SEI

Registry Value	Type	Comments
AASSEISiteName	String	SEI site name Default: <blank> The value is case-sensitive.
AASSEIUserName	String	SEI user name Default: nortel The value is case-sensitive.
AASSEIUserPassword	String	SEI password The password is NOT encrypted. Default: nortel The value is case-sensitive.
AASSEINamingServiceIP	String	SEI CORBA Naming Service IP This information is contained on the SEI server in the configuration file SEI.properties. Default: 127.0.0.1 (localhost)
AASSEINamingServicePort	DWORD	SEI CORBA Naming Service Port This information is contained on the SEI server in the configuration file SEI.properties. Default: 4422
AASSEIUpdateFrequency	DWORD	The interval of time (in msec) between pushed events Default: 2000 Maximum: 60000
AASSEIMaxConnTries	DWORD	Maximum # of tries to connect to a SEI server before failing over to other AAS. Default: 3 Maximum: 10
AASSEIMaxEventQueueSize	DWORD	Maximum event queue size. This value must be large enough to handle a full resync of SEI. If not, AAS will be unable to properly sync SEI with ICM. Each message queued by AAS requires approximately 1KB of space. Default: 3000
AASSEIUseBulkProcessing	String	Indicates whether AAS will process events passed to it during resync in bulk. Bulk processing is significantly faster than processing events one by one. Default: True

Table A-3 Configuration Information Used by AAS – SEI (continued)

Registry Value	Type	Comments
JavaRuntimeComponent	String	List of jar files to include in the classpath when running AAS. The base directory is /icm/bin. Default: aas;aas\aas.jar;aas\backport-util-concurrent.jar;aas\ccisCommon.jar;aas\conapi.jar;aas\icmJavaLib.jar;aas\log4j-1.2.9.jar;aas\nortelSei.jar;aas\SplkStd4J.jar
JavaRuntimeOptions	String	Java runtime options to pass to the jvm. Default: <blank>

Base: HKEY_LOCAL_MACHINE/SOFTWARE/Cisco Systems, Inc./ICM/<*ICM instance*>/PG<*XX*>/PG/CurrentVersion/Library/Processes/aas<*X*>

Note <*ICM instance*> and PG<*XX*> values are obtained from NodeManager. These are standard ICM registry entries for AAS. aas<*X*> indicates the AAS name.

Table A-4 Configuration Information Used by AAS – Ems

Registry Value	Type	Comments
EMSAllLogFilesMax	DWORD	Default: 0x5b8d80 (6000000 dec)
EMSBreakOnExit	DWORD	Default: 0
EMSBreakOnInit	DWORD	Default: 0
EMSDebugBreak	DWORD	Default: 1
EMSDisplayToScreen	DWORD	Default: 1
EMSForwardLevel	DWORD	Default: 1
EMSLogFileCountMax	DWORD	Default: 0x3e8 (1000 dec)
EMSLogFileLocation	String	Default: logfiles
EMSLogFileMax	DWORD	Default: 0x000f4240 (1000000 dec)
EMSNTEventLogLevel	DWORD	Default: 2
EMSTraceMask	DWORD	Default: 0
EMSUserData	Binary	Default: 30 30 30 30 (bin)

Table A-5 Configuration Information Used by AAS – NodeManager

Registry Value	Type	Comments
CreateProcHighPriority	DWORD	Default: 0
CreateProcNonDetached	DWORD	Default: 0
DbgDieOnPing	DWORD	Default: 0
DbgDieOnShutdown	DWORD	Default: 0
DbgIgnoreDbgIfDirty	DWORD	Default: 0

Table A-5 Configuration Information Used by AAS – NodeManager (continued)

Registry Value	Type	Comments
DbgNackPing	DWORD	Default: 0
DbgNackShutdown	DWORD	Default: 0
DbgPingDelay	DWORD	Default: 0
DbgShutdownDelay	DWORD	Default: 0
DbgStartupDelay	DWORD	Default: 0
ImageArgs	String	Default: <blank> AAS install will populate with <*ICM instance*> PG<*XX*>; for example, sccs pg1a.
ImageName	String	Default: aas\aas
ProcDelayRestartSecs1	DWORD	Default: 10
ProcDelayrestartSecs2	DWORD	Default: 0
ProcDisabled	DWORD	Default: 0
ProcMinUpSecs	DWORD	Default: 0
ProcPingInterval	DWORD	Default: 0
ProcPingTimeout	DWORD	Default: 0
ProcShutdownTimeout	DWORD	Default: 0
ProcStartupTimeout	DWORD	Default: 0
RebootOnFailOnce	DWORD	Default: 0
RebootOnFailTwice	DWORD	Default: 0
ShutdownDirty	DWORD	Default: 0

Dynamic Registry Settings

The following table includes registry settings for throttling parameters and heartbeat intervals. Throttling parameters are used to control load on the Administration & Data Server exerted by AAS. These settings also control the performance of AAS.

After changing these registry entries, you *do not* need to restart the AAS server in order for changes to take affect.

Base: HKEY_LOCAL_MACHINE/SOFTWARE/Cisco Systems, Inc./ICM/<*ICM instance*>/PG<*XX*>/PG/CurrentVersion/AASS/aas<*X*>/AASData/Dynamic

Note <*ICM instance*> and PG<*XX*> values are obtained from NodeManager.

Table A-6 Dynamic Registry Settings for AAS

Registry Value	Type	Comments
AASConAPIThrottleMaxModificationsPerTrans	DWORD	ICM Release 5.0(0): Default is 100. ICM Release 6.0(0): Default is 100.
AASMslHeartbeatInterval	DWORD	Master Selection heartbeat interval in msec. Default: 5000
AASSEILostMessageResyncTimeThreshold	DWORD	Indicates the minimum wait value in msec before one "lost message" resync can follow another lost message resync. This is done to prevent infinite resynchronizations in the case where SEI is consistently reporting lost messages. **Note** This value has no impact on resynchronizations triggered by AAS for other reasons. Default: 60000
AASSEILostMessageThreshold	DWORD	Indicates how many "lost messages" SEI can tell AAS about before AAS starts a resync process. Default: 5
AASSEIThrottleSeiEventQueueDelay	DWORD	Throttles the speed in the form of a delay (in milliseconds) at which events are processed as they come in from Symposium. **Note** **Important!** This setting has the most dramatic impact on CPU utilization by AAS. Default: 30 Maximum: 1000
AASForceResync	DWORD	This setting allows the user to force AAS to do a resync with Symposium. Simply change this value to something other than what it currently is, and the resync will be requested. **Note** If a resync occurred quite recently, this request might be ignored since AAS does not allow chain resynchronizations.
AASQueueSizeResyncThreshold	DWORD	Indicates the minimum queue size of backed-up events that will occur before the resync trigger can enable. Default: 20 Minimum: 10

Table A-6 Dynamic Registry Settings for AAS (continued)

Registry Value	Type	Comments
AASQueueArrivalRateTrailOff	DWORD	Indicates the maximum inflow of events that can occur in AASQueueArrivalRateDuration time before the resync trigger can enable. Default: 3
AASQueueArrivalRateDuration	DWORD	Indicates the maximum inflow of events that can occur in AASQueueArrivalRateTrailOff time before the resync trigger can enable. Default: 60 **Note** Value is in seconds.
AASIntelliSync	String	Indicates whether the IntelliSync feature is active. IntelliSync feature controls whether AASQueueSizeResyncThreshold, AASQueueArrivalRateTrailOff, and AASQueueArrivalRateDuration are used. Default: True **Note** IntelliSync is a feature that improves performance for large amounts of data synchronization after the startup resync has been performed. Post resync processing is usually processed one update at a time. However, when there is a series of these updates (for example, on a shift change), it is more efficient to process these in a bulk resynchronization. IntelliSync detects when there is a significant trail-off of events (for example, shift change processing completed) and looks at the size of the queue to determine if it is large enough to justify performing a resync. If not, the events will be processed one by one as usual. (This feature can be disabled.)

INDEX