Installation Guide for Cisco Unified Automated Administrator for Avaya Aura Contact Center

Release 10.0(x)

June 2014
CONTENTS

About This Guide i
Purpose i
Audience i
Organization i
Conventions ii

Obtaining Documentation, Obtaining Support, and Security Guidelines ii
Documentation Feedback iii

CHAPTER 1

About Automated Administrator for AACC 1-1
About Automated Administrator for AACC 1-1
AAS Architecture 1-1
AAS Performance and Scalability 1-3
   AAS Performance 1-3
   AAS Scalability 1-4
      Multiple AAS connecting to single Administration & Data Server 1-4
      Force Synchronization 1-5

CHAPTER 2

Installing and Configuring Automated Administrator for AACC 2-1
Installation 2-1
Supported Configurations 2-2
   Fully Redundant 2-2
   Partially Redundant 2-3
   Not Redundant 2-5
Supported Configurations with Firewall 2-6
   Fully Redundant 2-6
   Partially Redundant 2-7
   No Redundancy 2-8
   Firewall Usage and Configuration 2-8
Prerequisites for Installing AAS 2-9
   Minimum System Requirements 2-10
   Unified ICM Requirements 2-10
   Supported Unified ICM Versions 2-10
   Pre-installation Checklist 2-10
      Enabling the CMS Node Check box 2-11
   Installation Guidelines 2-11
      Order of Installation/Configuration 2-12
# About This Guide

## Purpose

This manual provides installation and troubleshooting information about Installation Guide for Cisco Unified Automated Administrator for Avaya Aura Contact Center, which is referred to as “AACC” 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](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.

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1</td>
<td>About Automated Administrator for AACC</td>
<td>Provides an overview of the functionality and performance of AAS.</td>
</tr>
<tr>
<td>Chapter 2</td>
<td>Installing and Configuring Automated Administrator for AACC</td>
<td>Provides prerequisites and installation instructions for installing AAS.</td>
</tr>
<tr>
<td>Chapter 3</td>
<td>Configuring the ICM ConAPI Connection</td>
<td>Describes how to configure the Unified ICM ConAPI connection.</td>
</tr>
<tr>
<td>Chapter 4</td>
<td>Debugging and Throttling</td>
<td>Provides information on debugging and troubleshooting AAS.</td>
</tr>
<tr>
<td>Chapter 5</td>
<td>Limitations of Automated Administrator for AACC</td>
<td>Describes the limitations of AAS.</td>
</tr>
<tr>
<td>Appendix A</td>
<td>Working with Registry Settings, page 1</td>
<td>Describes the configuration and dynamic registry settings in AAS.</td>
</tr>
</tbody>
</table>

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

This manual uses the following conventions:

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

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:

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

This chapter includes the following sections:
- About Automated Administrator for AACC, page 1-1
- AAS Architecture, page 1-1
- AAS Performance and Scalability, page 1-3

### About Automated Administrator for AACC

AAS is middleware software, which converts AACC 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 AACC system with the ICM database, thereby eliminating the need for a system administrator to execute changes twice (once in the AACC Administration and once in the ICM administration). All additions and updates to agents and their skill sets made using AACC administration are also dynamically made to the ICM database in real time. However, changes made in the system are not reflected in AACC.

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

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 an integrated installer from Unified ICM versions 7.1(3) or later.

**Note**

AACC is formerly known as Nortel SCCS.

### AAS Architecture

Following are the components of AAS:
- The AACC interface (SEI layer), which encapsulates the interface between AAS and AACC.
- The ICM interface (ConAPI layer), which encapsulates the interface between AAS and Administration & Data Server.
- Data Synchronizer, which compares the information from AACC 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 Avaya Aura Contact Center (AACC). SEI is a Avaya product that enables third-party products (such as AAS) to receive events from AACC.

Refer to the *Cisco Unified ICM Software ACD Supplement for Nortel Symposium* for more details about the AACC PG. The *Cisco Unified ICM Software Supported Switches (ACDs)* document lists the ACD supported switches. (All Cisco documentation is available on Cisco.com.) The Avaya 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 AACC and requesting and getting SEI events from AACC.
- 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 AACC.
  - SEI layer will request synchronization from AACC, and the AACC 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.
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 AACC.
- Resynchronization for 1000 agents with 100 skill groups takes < 10 minutes.
- Normal changes in AACC 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 AACC.

From Unified ICM Release 7.2.(3) or later:

- 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 AACC 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 AACC.

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

Note: For more information on AAS Throttling Guidelines, refer AAS Throttling Guidelines, page 4-1.
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:

2
Installing and Configuring Automated Administrator for AACC

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

This chapter includes the following sections:

- Installation, page 2-1
- Supported Configurations, page 2-2
- Supported Configurations with Firewall, page 2-6
- Prerequisites for Installing AAS, page 2-9
- Installing AAS, page 2-13

Installation

Refer the Appendix 2, “How to Install or Reinstall AAS on Unified ICM 7.2(7) or later” section for more information on installation.
Supported Configurations

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

<table>
<thead>
<tr>
<th>Supported Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>PG (with AAS)</td>
</tr>
<tr>
<td>Fully redundant</td>
</tr>
<tr>
<td>Partially redundant</td>
</tr>
<tr>
<td>No redundancy</td>
</tr>
</tbody>
</table>

**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 AACC and Administration & Data Server. The standby AAS server does not have a connection to AACC 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 AACC and/or both Administration & Data Server, it will failover to the other AAS server. **Figure 2-1** shows the fully redundant configuration.
**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
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 AACC is not supported because the AACC port is dynamic.

Fully Redundant

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

*Figure 2-4  Fully Redundant Configuration with Firewall*
Partially Redundant

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

**Figure 2-5  Partially Redundant Configuration with Firewall**
No Redundancy

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

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.
AACCAAS 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 AACC is not supported because the AACC port is dynamic.

Prerequisites for Installing AAS

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

You must install ICM PG on the system before AAS installation. Before installation, ensure the following registry is set to 60:

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

Minimum System Requirements

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

<table>
<thead>
<tr>
<th>Product</th>
<th>Required Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya Aura Contact Center (AACC)</td>
<td>AACC 6.0</td>
</tr>
<tr>
<td>AACC Event Interface</td>
<td>No separate versioning required</td>
</tr>
<tr>
<td>Unified ICM</td>
<td>Unified ICM Releases 7.2(7) or later</td>
</tr>
</tbody>
</table>

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 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 AACC. (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 AACC” 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 AACC Event Server (SEI CORBA) is installed
- AACC site name
- SEI user name and password
- ICM peripheral ID for the AACC 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

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 AACC PG installation component matrix. AAS is an optional additional component of the AACC 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.
Chapter 2 Installing and Configuring Automated Administrator for AACC

Prerequisites for Installing AAS

- 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 AACC 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 Avaya Symposium* available at cisco.com.

- Set the default sub skill group mask for the AACC 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 AACC 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 AACC 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.

**Caution** You must install the AAS and PG on the same computer. Do not install the AACC 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.
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 or Reinstall AAS on Unified ICM 7.2(7) or later

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From the ICM Installer, run the PG setup.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>At the PG setup screen:</td>
</tr>
<tr>
<td></td>
<td>a. Select the AACC Version 6.0.</td>
</tr>
<tr>
<td></td>
<td>b. Check <strong>Install AAS</strong>.</td>
</tr>
<tr>
<td></td>
<td>c. Select <strong>Yes</strong> at the prompt to confirm the installation.</td>
</tr>
<tr>
<td></td>
<td>d. Click <strong>OK</strong> to open the AAS Configuration screen.</td>
</tr>
</tbody>
</table>
Figure 2-8  AACC Configuration

Step 3  At the AAS Configuration screen (Figure 3-5 shows the AAS Configuration screen):

a. Enter the AACC Site Name.

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 Avaya Aura Contact Center machine ("SEI CORBA" refers to the Avaya Aura Contact Center.)
   - **SEI CORBA Port**: The Port of the Avaya Aura Contact Center machine ("SEI CORBA" refers to the Avaya Aura Contact Center.)

Note
SEI CORBA software is the CORBA naming service used by SEI. This information can be found in the SEI.properties file on the AACC 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 7.2(7) or later

Step 1  From the ICM Installer, run the PG setup.
Step 2  At the PG setup screen:
   a. Select the AACC Version 6.0.
   b. Deselect Install AAS.

Figure 2-9  AACC Configuration

Note  If you are using AACC versions higher than 6.0, select 6.0.

Step 3  Click OK.
Step 4  Click Next to finish PG Setup.
3

Configuring the ICM ConAPI Connection

This chapter includes the following sections:

- About Unified ICM Application Instances, page 3-1
- About Configuring Application Instances, page 3-1
- About Establishing Administration Connections, page 3-2

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**

![Application Instance List](image)

**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**

---

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

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

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

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

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

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

- **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.)

---

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

<table>
<thead>
<tr>
<th>Application connection details</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICM Distributor AV Link:</td>
</tr>
<tr>
<td>ICM Distributor AV RMI registry port:</td>
</tr>
<tr>
<td>Application Link:</td>
</tr>
<tr>
<td>Application RMI registry port:</td>
</tr>
<tr>
<td>Application host name:</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Application connection details</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICM Distributor AV Link:</td>
</tr>
<tr>
<td>ICM Distributor AV RMI registry port:</td>
</tr>
<tr>
<td>Application Link:</td>
</tr>
<tr>
<td>Application RMI registry port:</td>
</tr>
<tr>
<td>Application host name:</td>
</tr>
</tbody>
</table>
Figure 3-5 illustrates the window for AAS configuration when "Install AAS" checkbox is selected in PG setup.
4
Debugging and Throttling

This chapter includes the following sections:

- AAS Throttling Guidelines, page 4-1
- Debugging, page 4-2

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 AACC 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 Avaya Aura Contact Center 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/AASSEIThrottleSetEventQueueDelay`. 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.” 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.
Chapter 4 Debugging and Throttling

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

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.
Limitations of Automated Administrator for AACC

This chapter includes the following sections:

- Limitations of AAS, page 5-1
- AACC Limitations, page 5-1

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 AACC 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 AACC 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 AACC 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 AACC SEI interface.

- Agents in standby mode on the AACC will not be updated by AAS onto ICM.

- The only way to determine the status of AAS is via logs.

- AAS does not filter any events for agents and skill groups from AACC; hence, all events of AACC 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 AACC, 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 AACC, and the second is for connection between the duplex (A/B) PG pair.

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

AACC Limitations

The following are the limitations in AAS caused due to AACC limitations:
• AACC 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 AACC.
• Changes to agents skill sets made in ICM are not automatically reflected onto the AACC.
• Deleting an agent or skill group from AACC in the AACC Administration does not unassign the agent from all the skill groups in ICM. The AACC 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 AACC is not supported because the AACC port is dynamic.
Appendix A      Working with Registry Settings

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

<table>
<thead>
<tr>
<th>Registry Value</th>
<th>Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>AASPGHostA</td>
<td>String</td>
<td>IP address/Host of AAS Server A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: &lt;blank&gt;</td>
</tr>
<tr>
<td>AASPGPortA</td>
<td>DWORD</td>
<td>MSL Port of AAS Server A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 42034</td>
</tr>
<tr>
<td>AASPGHostB</td>
<td>String</td>
<td>IP address/Host of AAS Server B</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: &lt;blank&gt;</td>
</tr>
<tr>
<td>AASPGPortB</td>
<td>DWORD</td>
<td>MSL Port of AAS Server B</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 43034</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Registry Value</th>
<th>Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>AASConAPILocalServiceName1</td>
<td>String</td>
<td>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.</td>
</tr>
<tr>
<td>AASConAPILocalServiceName2</td>
<td>String</td>
<td>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.</td>
</tr>
<tr>
<td>AASConAPILocalRegistryPort</td>
<td>DWORD</td>
<td>The local port for RMI register. Default: 2099</td>
</tr>
<tr>
<td>AASConAPIRemoteServiceName1</td>
<td>String</td>
<td>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.</td>
</tr>
<tr>
<td>AASConAPIRemoteServiceName2</td>
<td>String</td>
<td>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.</td>
</tr>
<tr>
<td>AASConAPIRemoteRegistryPort</td>
<td>DWORD</td>
<td>The port for RMI register at the remote computer. Default: 2099</td>
</tr>
<tr>
<td>AASConAPIDisableAutoConnect</td>
<td>DWORD</td>
<td>Default: false</td>
</tr>
<tr>
<td>AASConAPIRemoteHost1</td>
<td>String</td>
<td>Location of the Administration &amp; Data Server-1. Default: 127.0.0.1 (localhost) The value is case-sensitive.</td>
</tr>
<tr>
<td>AASConAPIRemoteHost2</td>
<td>String</td>
<td>Location of the Administration &amp; Data Server-2. Default: &lt;blank&gt; The value is case-sensitive.</td>
</tr>
<tr>
<td>AASConAPITransportType</td>
<td>String</td>
<td>The type of network layer implementation. Default: RmiDriver The value is case-sensitive.</td>
</tr>
</tbody>
</table>
## Working with Registry Settings

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

<table>
<thead>
<tr>
<th>Registry Value</th>
<th>Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>AASConAPIConnectionAttempts</td>
<td>DWORD</td>
<td>The number of times the AAS application attempts to find the distributor. Default: 1 Maximum: 10</td>
</tr>
<tr>
<td>AASConAPILocalPort</td>
<td>DWORD</td>
<td>The Administration &amp; Data Server RMI Registry Port (as shown on CMS Control). Default: 0</td>
</tr>
<tr>
<td>AASConAPIType</td>
<td>String</td>
<td>The type of the ConAPI implementation. Default: Remote The value is case-sensitive.</td>
</tr>
<tr>
<td>AASConAPIDefaultTimeout</td>
<td>DWORD</td>
<td>The time in msec a thread will block waiting for a reply. Default: 30000 Maximum: 300000</td>
</tr>
<tr>
<td>AASConAPINumRetryAttempts</td>
<td>DWORD</td>
<td>Number of times to retry a ConAPI operation. Default: 2 Maximum: 10</td>
</tr>
<tr>
<td>AASConAPIUserName</td>
<td>String</td>
<td>Application name to connect to Administration &amp; Data Server via ConAPI. Default: AAS The value is case-sensitive.</td>
</tr>
<tr>
<td>AASConAPIUserPassword</td>
<td>DWORD</td>
<td>Application password to connect to Administration &amp; Data Server via ConAPI. The password is NOT encrypted. Default: AAS The value is case-sensitive.</td>
</tr>
<tr>
<td>AASConAPIMaxConnTries</td>
<td>DWORD</td>
<td>Maximum number of tries to connect to an Administration &amp; Data Server before trying the other Administration &amp; Data Server. Default: 2 Maximum: 10</td>
</tr>
<tr>
<td>AASPeripheralID</td>
<td>DWORD</td>
<td>Peripheral ID for AACC. Default: 0</td>
</tr>
</tbody>
</table>
### Working with Registry Settings

Base: HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<ICM instance>\PG<XX>\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

<table>
<thead>
<tr>
<th>Registry Value</th>
<th>Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>AASConAPIRenameSubSkillGroups</td>
<td>String</td>
<td>Indicates whether AAS will manually rename subskill groups when a base skill group is renamed. Default False.</td>
</tr>
<tr>
<td>AASRetriesToRestart</td>
<td>DWORD</td>
<td>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</td>
</tr>
</tbody>
</table>

**Table A-3**  Configuration Information Used by AAS – SEI

<table>
<thead>
<tr>
<th>Registry Value</th>
<th>Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>AASSEISiteName</td>
<td>String</td>
<td>SEI site name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: &lt;blank&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The value is case-sensitive.</td>
</tr>
<tr>
<td>AASSEIUserName</td>
<td>String</td>
<td>SEI user name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: nortel</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The value is case-sensitive.</td>
</tr>
<tr>
<td>AASSEIUserPassword</td>
<td>String</td>
<td>SEI password</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The password is NOT encrypted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: nortel</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The value is case-sensitive.</td>
</tr>
<tr>
<td>AASSEINamingServiceIP</td>
<td>String</td>
<td>SEI CORBA Naming Service IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This information is contained on the SEI server in the configuration file SEI.properties. Default: 127.0.0.1 (localhost)</td>
</tr>
<tr>
<td>AASSEINamingServicePort</td>
<td>DWORD</td>
<td>SEI CORBA Naming Service Port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This information is contained on the SEI server in the configuration file SEI.properties. Default: 4422</td>
</tr>
</tbody>
</table>
## Working with Registry Settings

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

<table>
<thead>
<tr>
<th>Registry Value</th>
<th>Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>AASSEIUpdateFrequency</td>
<td>DWORD</td>
<td>The interval of time (in msec) between pushed events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maximum: 60000</td>
</tr>
<tr>
<td>AASSEIMaxConnTries</td>
<td>DWORD</td>
<td>Maximum # of tries to connect to a SEI server before failing over to other AAS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maximum: 10</td>
</tr>
<tr>
<td>AASSEIMaxEventQueueSize</td>
<td>DWORD</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 3000</td>
</tr>
<tr>
<td>AASSEIUseBulkProcessing</td>
<td>String</td>
<td>Indicates whether AAS will process events passed to it during resync in bulk. Bulk processing is significantly faster than processing events one by one.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: True</td>
</tr>
<tr>
<td>JavaRuntimeComponent</td>
<td>String</td>
<td>List of jar files to include in the classpath when running AAS. The base directory is /icm/bin.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: aas;aas\aas.jar;aas\backport-util-concurrent.jar;aas\cci\sCommon.jar;aas\conapi.jar;aas\icmJavaLib.jar;aas\log4j-1.2.9.jar;aas\nortelSei.jar;aas\SplkStd4J.jar</td>
</tr>
<tr>
<td>JavaRuntimeOptions</td>
<td>String</td>
<td>Java runtime options to pass to the jvm.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: &lt;blank&gt;</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Registry Value</th>
<th>Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMSAllLogFilesMax</td>
<td>DWORD</td>
<td>Default: 0x5b8d80 (6000000 dec)</td>
</tr>
<tr>
<td>EMSBreakOnExit</td>
<td>DWORD</td>
<td>Default: 0</td>
</tr>
<tr>
<td>EMSBreakOnInit</td>
<td>DWORD</td>
<td>Default: 0</td>
</tr>
<tr>
<td>EMSDebugBreak</td>
<td>DWORD</td>
<td>Default: 1</td>
</tr>
<tr>
<td>EMSDisplayToScreen</td>
<td>DWORD</td>
<td>Default: 1</td>
</tr>
</tbody>
</table>
## Appendix A
### Working with Registry Settings

#### EMSForwardLevel
- **Type:** DWORD
- **Default:** 1

#### EMSLogFileCountMax
- **Type:** DWORD
- **Default:** 0x3e8 (1000 dec)

#### EMSLogFileLocation
- **Type:** String
- **Default:** logfiles

#### EMSLogFileMax
- **Type:** DWORD
- **Default:** 0x000f4240 (1000000 dec)

#### EMSNTEventLogLevel
- **Type:** DWORD
- **Default:** 2

#### EMSTraceMask
- **Type:** DWORD
- **Default:** 0

#### EMSUserData
- **Type:** Binary
- **Default:** 30 30 30 30 (bin)

<table>
<thead>
<tr>
<th>Registry Value</th>
<th>Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMSForwardLevel</td>
<td>DWORD</td>
<td>Default: 1</td>
</tr>
<tr>
<td>EMSLogFileCountMax</td>
<td>DWORD</td>
<td>Default: 0x3e8 (1000 dec)</td>
</tr>
<tr>
<td>EMSLogFileLocation</td>
<td>String</td>
<td>Default: logfiles</td>
</tr>
<tr>
<td>EMSLogFileMax</td>
<td>DWORD</td>
<td>Default: 0x000f4240 (1000000 dec)</td>
</tr>
<tr>
<td>EMSNTEventLogLevel</td>
<td>DWORD</td>
<td>Default: 2</td>
</tr>
<tr>
<td>EMSTraceMask</td>
<td>DWORD</td>
<td>Default: 0</td>
</tr>
<tr>
<td>EMSUserData</td>
<td>Binary</td>
<td>Default: 30 30 30 30 (bin)</td>
</tr>
</tbody>
</table>

#### Table A-4
#### Configuration Information Used by AAS – Ems (continued)

<table>
<thead>
<tr>
<th>Registry Value</th>
<th>Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateProcHighPriority</td>
<td>DWORD</td>
<td>Default: 0</td>
</tr>
<tr>
<td>CreateProcNonDetached</td>
<td>DWORD</td>
<td>Default: 0</td>
</tr>
<tr>
<td>DbgDieOnPing</td>
<td>DWORD</td>
<td>Default: 0</td>
</tr>
<tr>
<td>DbgDieOnShutdown</td>
<td>DWORD</td>
<td>Default: 0</td>
</tr>
<tr>
<td>DbgIgnoreDbgIfDirty</td>
<td>DWORD</td>
<td>Default: 0</td>
</tr>
<tr>
<td>DbgNackPing</td>
<td>DWORD</td>
<td>Default: 0</td>
</tr>
<tr>
<td>DbgNackShutdown</td>
<td>DWORD</td>
<td>Default: 0</td>
</tr>
<tr>
<td>DbgPingDelay</td>
<td>DWORD</td>
<td>Default: 0</td>
</tr>
<tr>
<td>DbgShutdownDelay</td>
<td>DWORD</td>
<td>Default: 0</td>
</tr>
<tr>
<td>ImageArgs</td>
<td>String</td>
<td>Default: &lt;blank&gt;</td>
</tr>
<tr>
<td>ProcDelayRestartSecs1</td>
<td>DWORD</td>
<td>Default: 10</td>
</tr>
<tr>
<td>ProcDelayRestartSecs2</td>
<td>DWORD</td>
<td>Default: 0</td>
</tr>
<tr>
<td>ProcDisabled</td>
<td>DWORD</td>
<td>Default: 0</td>
</tr>
<tr>
<td>ProcMinUpSecs</td>
<td>DWORD</td>
<td>Default: 0</td>
</tr>
<tr>
<td>ProcPingInterval</td>
<td>DWORD</td>
<td>Default: 0</td>
</tr>
<tr>
<td>ProcPingTimeout</td>
<td>DWORD</td>
<td>Default: 0</td>
</tr>
<tr>
<td>ProcShutdownTimeout</td>
<td>DWORD</td>
<td>Default: 0</td>
</tr>
<tr>
<td>ProcStartupTimeout</td>
<td>DWORD</td>
<td>Default: 0</td>
</tr>
<tr>
<td>RebootOnFailOnce</td>
<td>DWORD</td>
<td>Default: 0</td>
</tr>
<tr>
<td>RebootOnFailTwice</td>
<td>DWORD</td>
<td>Default: 0</td>
</tr>
<tr>
<td>ShutdownDirty</td>
<td>DWORD</td>
<td>Default: 0</td>
</tr>
</tbody>
</table>
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 effect.


<table>
<thead>
<tr>
<th>Registry Value</th>
<th>Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>AASConAPIThrottleMaxModificationsPerTrans</td>
<td>DWORD</td>
<td>Default is 100.</td>
</tr>
<tr>
<td>AASMslHeartbeatInterval</td>
<td>DWORD</td>
<td>Master Selection heartbeat interval in msec. Default: 5000</td>
</tr>
<tr>
<td>AASSEILostMessageResyncTimeThreshold</td>
<td>DWORD</td>
<td>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. This value has no impact on resynchronizations triggered by AAS for other reasons. Default: 60000</td>
</tr>
<tr>
<td>AASSEILostMessageThreshold</td>
<td>DWORD</td>
<td>Indicates how many “lost messages” SEI can tell AAS about before AAS starts a resync process. Default: 5</td>
</tr>
<tr>
<td>AASSEIThrottleSeiEventQueueDelay</td>
<td>DWORD</td>
<td>Throttles the speed in the form of a delay (in milliseconds) at which events are processed as they come in from AACC. Important! This setting has the most dramatic impact on CPU utilization by AAS. Default: 30 Maximum: 1000</td>
</tr>
</tbody>
</table>

Note: <ICM instance> and PG<XX> values are obtained from NodeManager.
### Working with Registry Settings

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

<table>
<thead>
<tr>
<th>Registry Value</th>
<th>Type</th>
<th>Comments</th>
</tr>
</thead>
</table>
| AASForceResync                  | DWORD    | This setting allows the user to force AAS to do a resync with AACC. 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 |
| AASQueueArrivalRateTrailOff     | DWORD    | Indicates the maximum inflow of events that can occur in AASQueueArrivalRateDuration time before the resync trigger can enable.  
Default: 3 |
### Working with Registry Settings

#### AASQueueArrivalRateDuration
- **Type:** DWORD
- **Comments:** 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
- **Type:** String
- **Comments:** 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

A
AAS 1-1
components 1-1
installing, configurations available 2-11
throttling guidelines 4-1
Administration connection, configuring 3-3
Application instance, configuring 3-2
Architecture 1-1

C
CMS Control, configuring an administration connection 3-3
CMS Node check box, enabling 2-11
components 1-1
Components, AAS 1-1
ConAPI layer 1-1
Configuration 2-14
Configuration registry settings A-1
Configurations 2-2
Configuring
administration connection 3-3
application instance 3-2

D
Data Synchronizer 1-1
Debugging 4-2
Debug trace levels for AAS 4-2
Dynamic Registry Settings A-7
Dynamic registry settings A-7

E
Establishing Administration Connections 3-2

F
Firewall 2-6
Force Synchronization 1-5
Fully Redundant 2-2

I
ICM Application Instances 3-1
ICM peripheral ID 2-11
ICM software requirements 2-10
ICM Versions 2-10
Installing
AAS 2-13
AAS, configurations available 2-11
IP address 2-10

L
limitations 5-1

M
Multiple AAS connecting to single AW 1-4

N
Nortel SCCS 5-1
Not Redundant 2-5

P
packaging and bundling 1-1
Partially Redundant 2-3
Performance and Scalability 1-3
Port 2-9
Pre-installation Checklist 2-10
Prerequisites 2-9
R

Registry Settings  A-1
Registry settings
  configuration  A-1
  dynamic  A-7

S

SEI events  5-2
SEI Lite  1-2
skill groups  5-1
Software requirements, ICM  2-10
support  5-1
System Requirements  2-10
System requirements, minimum  2-10

T

Throttling guidelines  4-1
Trace Levels  4-2

U

uninstall  2-16