

Cisco AON Installation and Administration Guide

AON Release 1.1
November 2005

Corporate 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: 408 526-4100



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This product includes software developed by the Apache Software Foundation <http://www.apache.org>

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Cisco AON Installation and Administration Guide
Copyright © 2005 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Introduction 1-1

- AON Devices 1-1
 - Management Tools 1-2
 - Nodes 1-2
 - Other Entities 1-2
- AON Features 1-3
- AON Setup Summary 1-4
- Advanced AON Configuration 1-4

CHAPTER 2

Configuring AON Devices 2-1

- Working with AMC 2-1
 - Generating a Java Keystore 2-1
 - Installing and Upgrading AMC 2-4
 - Stopping, Starting, and Restarting the AMC Daemon 2-6
- Working with Nodes 2-7
 - Configuration Prerequisites 2-7
 - Configuring a Cisco 8300 Series AON Appliance 2-8
 - Configuring Networking Parameters 2-8
 - Disabling Cisco Discovery Protocol 2-9
 - Configuring Networking Parameters on a Catalyst 6500 Series Switch 2-10
 - Configuring a VLAN under the Catalyst Operating System 2-10
 - Configuring a VLAN under Cisco IOS 2-11
 - Assigning IP Addresses to the AON-SM Interface 2-11
 - Configuring Network Parameters on a Cisco Modular Access Router 2-12
 - Configuring Nodes to Use SSH 2-13
 - Configuring Nodes to Register with the AMC 2-14
 - Upgrading Nodes 2-15
 - Upgrading an AON Appliance or AON-NM 2-15
 - Upgrading an AON-SM 2-18
 - Using Catalyst Operating System to Upgrade an AON-SM 2-18
 - Using Cisco IOS to Upgrade an AON-SM 2-21

CHAPTER 3

Working with Nodes 4-1

- Managing Nodes 4-1

- Creating Nodes 4-2
- Configuring WCCP for Traffic Redirection 4-4
- Editing Nodes 4-6
- Deleting Nodes 4-7
- Replacing Nodes 4-8
- Exporting Nodes 4-9
- Importing Nodes 4-10
- Managing WCCP Servers 4-11
 - Creating WCCP Servers 4-11
- Managing Virtual Clusters 4-12
 - Creating a Virtual Cluster 4-12
 - Changing Nodes Within a Virtual Cluster 4-14
 - Configuring WCCP for Cluster Management 4-14
 - Configuring WCCP for Traffic Redirection 4-17
- Configuring ACL/Classifiers 4-19
- Configuring Recovery 4-21
- Deploying to Nodes 4-22
- Viewing Logs 4-24
- Viewing Events 4-24

CHAPTER 4

Managing AON Properties 5-1

- Adapter Registry 5-2
- Adapter Listener Domain 5-3
- Adaptive Load Balancer 5-4
- Databases 5-5
- Reliable Messaging 5-6
- Caching 5-7
- Content Parser 5-9
- Content Validation 5-10
- Configuring Message Delivery Properties 5-11
 - Configuring Delivery Connection 5-11
 - Configuring Delivery Notification 5-12
 - Configuring Delivery Semantics 5-13
 - Binding Message Delivery Properties to a Message Type 5-14
- Encoding 5-15
- Message Log Domain 5-17
 - Create a Message Log Database 5-17
 - Configure Message Log Domain Property 5-18
- Next Hop Domain 5-20

Node Capabilities	5-21
Transformation	5-22
Configuring JMS Properties	5-23
JMS Destination Property	5-23
JMS Source Property	5-24
JMS Reply To	5-25
JMS Connections Property	5-26
JMS Naming Property	5-27
Bladelet Monitoring Property	5-29
Service Profiles	5-30

CHAPTER 5**Managing AON Security 6-1**

Managing AON Users	6-1
Managing Local Users	6-1
Creating New Users	6-3
Displaying Information on Users	6-4
Editing Users	6-5
Assigning Roles to Users	6-5
Managing External Users	6-6
Creating an LDAP Profile	6-6
Assigning Roles to External Users	6-8
Creating an Authentication Realm	6-9
Managing Keystores	6-10
Configuring a Keystore Passphrase	6-10
Managing Keypairs	6-10
Upload PKCS#12	6-11
Generate and Register a New Key	6-12
Generate a Self-Signed Keypair and Certificate	6-13
Generate an SSL Certificate	6-14
Import a Keypair or Keystore	6-17
Manage Public Certificates or Root Certificates	6-18
Add a Certificate	6-18
Configuring Security Properties	6-20
Endpoint SSLID Property	6-21
SSL Configuration Property	6-22
SSL Binding Property	6-23
Configuring Authentication and Authorization Properties	6-24
Configuring LDAP	6-24
Configuring Kerberos	6-26

APPENDIX A

Message Log Schemas 1

Oracle 1

Sybase 3



Introduction

Cisco Application-Oriented Network (AON) is a technology foundation for a new class of Cisco products that embed intelligence into the network to better meet the needs of application deployment. AON complements existing networking technologies by providing a greater degree of awareness of what information is flowing within the network and helping customers to:

- Integrate disparate applications by routing information to the appropriate destination, in the format expected by that destination
- Enforce security policies for information access and exchange
- Optimize the flow of application traffic, both in terms of network bandwidth and processing overheads
- Provide increased manageability of information flow, including monitoring and metering of information flow for both business and infrastructure purposes

AON provides this enhanced support by understanding more about the content and context of information flow. As such, AON works primarily at the message-level rather than at the packet level. Typically, an AON node terminates a TCP connection to inspect the full message, including the “payload” and all headers. AON also understands and assists with popular application-level protocols such as HTTP, JMS, and other de facto standards.

This chapter introduces the concepts necessary for configuring and administering an application-oriented network. It includes the following topics:

- [AON Devices, page 1-1](#)
- [AON Features, page 1-3](#)
- [AON Setup Summary, page 1-4](#)

AON Devices

An application-oriented network consists of the following devices:

- [Management Tools](#)
- [Nodes](#)
- [Other Entities](#)

Management Tools

AON Management Console (AMC)

AMC is the tool that enables centralized management of the application-oriented network. This includes:

- Configuring, managing, and monitoring AON nodes
- Deploying global and node-level properties
- Managing certificates and keypairs

AON Development Studio (ADS)

ADS is the tool for developers to create message-level logic using a graphical user interface (GUI). ADS provides a set of preconfigured functions, called Bladelets, that are used to construct Policy Execution Plans (PEP). Additionally, ADS includes functionality that enables developers to upload custom Bladelets to perform business functions unique to different environments.

Nodes

AON Services Modules on Catalyst 6500 Series Switches

This is the AON form factor available as a single-slot services module for the Catalyst 6500 Series Switches. Typically this node is used in a data center.

AON Network Modules on Cisco 2600, Cisco 2800, Cisco 3700, and Cisco 3800 Series Routers

This is the AON form factor available as a single-slot network module for several different Cisco modular access routers. Typically this type of node is used in a branch office. See *Release Notes for Cisco Application-Oriented Networking* for a detailed list of supported router platforms.

Other Entities

Depending on the configuration of your network and the needs of your business, your application-oriented network may include any of the following devices:

Database

When a database policy is configured, AON can store specified data in a Sybase or Oracle database.

LDAP server

Can be used to perform user authentication for both the AMC application and on individual messages traversing the application-oriented network.

Java Messaging Service (JMS)

AON devices can be configured to exchange messages between clients and JMS queues.

AON Features

Explicit and Transparent Interception

An AON node resides in the network as an inline application-aware device. The device acts as an intelligent intermediary gateway that can either be explicitly addressed by applications or as a passthrough proxy that is transparent to applications.

Access Methods and Adapters

AON understands various application access methods and provides adapters that can natively interface with the protocols. The key protocols that AON supports include:

- HTTP v1.0/ v1.1 and HTTPS
- MQ Native Adapter
- JMS

Additionally, custom protocols are supported through the AON software development kit (SDK).

Protocol Translation

AON nodes can act as protocol gateways between multiple applications — an example of this would be the node receiving an application message through JMS and sending the same message to another application as an HTTP post.

Transformation

AON supports both XML and non-XML transformation through an open transformation architecture. AON uses an XSLT based transformation engine. You can add your own Java transformation engine to execute custom transformations.

Security

AON provides a series of intelligent services which enable message-level access and control to meet application security needs within the network. These security services include authentication, authorization, nonrepudiation, data integrity, data confidentiality, and centralized key management.

Service Virtualization

AON has the capability to act as proxy to create an abstraction layer for endpoint applications and apply policies across all of these services—in a centralized configuration manner with distributed enforcement in the network. Service virtualization functionality enables customers to execute content-based routing, workload balancing, and message distribution operations.

Schema Validation

AON provides the ability to validate XML documents against schemas you create.

Reliable Messaging

AON provides a reliable delivery semantic across all supported protocols. Based on the level of support required, AON can ensure exactly once delivery, at least once delivery, or at most once delivery.

Optimization Services

AON has the capability to cache or compress messages to allow for optimization of message traffic, thus enabling reduced application response time and the conservation of network bandwidth.

External Data Access

AON provides the capabilities to access or notify other applications in parallel to handling the main message flow. External access is currently available using HTTP and Java Database Connectivity (JDBC).

Message Logging

AON can capture application messages for logging either synchronously for auditing purposes or asynchronously.

AON Setup Summary

The process for implementing an application-oriented network is divided into two chapters:

- [Chapter 2, “Configuring AON Devices”](#)
This chapter describes the procedures you need to perform when you add AON devices to your network. You will perform most of the procedures in this chapter the first time you implement application-oriented networking.
- [Chapter 3, “Validating an AON Installation”](#)
This chapter describes the procedures you need to perform when you are initially deploying AON. The procedures include steps that will help you ensure that your installation of AMC and AON devices is functioning properly.

This section summarizes the procedures detailed in these chapters:

1. Install all switches, routers, and related AON modules and ensure they are configured for basic IP networking. Refer to documentation related to your switch or router for detailed configuration instructions.
2. Establish a relationship with a well-known certificate authority and generate a Java keystore. See the [“Generating a Java Keystore”](#) section on page 2-1.
3. Install AMC on a Linux server. See the [“Working with AMC”](#) section on page 2-1.
4. Configure AON nodes to register with AMC. See the [“Working with Nodes”](#) section on page 2-7.
5. Install the AON Development Studio (ADS) on a Windows PC. See the *AON Development Studio User Guide* for detailed installation instructions.

Advanced AON Configuration

Depending on the requirements of your applications and network, you may need to:

- Configure nodes. See [Chapter 3, “Working with Nodes”](#) to create and configure nodes and to configure virtual clusters and WCCP. This chapter covers node deployment and node monitoring.
- Configure properties. See [Chapter 4, “Managing AON Properties”](#) to configure global- and node-level properties.
- Configure security. See [Chapter 5, “Managing AON Security”](#) to configure and manage security-related features in AON.



Configuring AON Devices

This chapter includes the following sections:

- [Working with AMC, page 2-1](#)
- [Working with Nodes, page 2-7](#)

Working with AMC

This section describes how to install the AON Management Console (AMC). It includes the following sections:

- [Generating a Java Keystore, page 2-1](#) (required)
- [Installing and Upgrading AMC, page 2-4](#) (required)
- [Stopping, Starting, and Restarting the AMC Daemon, page 2-6](#) (optional)

Generating a Java Keystore

Before installing or upgrading AMC, you must obtain a certificate. This certificate must be in the form of a Java Keystore (.jks) file and be compatible with JDK 1.4.2 or later release. Additionally, AMC accepts only the well-known certificate authorities included in the Java Runtime Environment (JRE) 1.4 truststore.

Prerequisite

- Install the Java Runtime Environment and add the **/bin** directory to your path.

Step 1 To generate the key type the following on the command line of a Linux workstation:

```
[root@linux opt]# keytool -genkey -alias <name> -keyalg <algorithm> -keysize <size> -validity <days> -keystore <filename> -storepass <password>
```

This command requires you to provide the following variables:

- *name* = Select an alias name for your keystore.
- *algorithm* = Specify either RSA or DSA. We recommend that you use RSA.
- *size* = Specify the size of the key in bits. This value must be a multiple of 64 between 512 and 1024.
- *days* = Specify the number of days your key will be valid.

- *filename* = Specify the location and filename where you want your keystore file to be generated.
- *password* = Specify the password used to protect your keystore file.

The following is a sample entry using the above variables:

```
[root@linux]# keytool -genkey -alias test -keyalg rsa -keysize 512 -validity 365
-keystore teststore -storepass password
```

- Step 2** After pressing RETURN, you are prompted for information related to your organization and location. Enter the appropriate data. The values that follow are for illustrative purposes only:



Note

When prompted for your first and last name, enter the hostname for the server on which AMC is to be installed.

```
What is your first and last name?
[Unknown]: aon.hostname.com
What is the name of your organizational unit?
[Unknown]: Application-Oriented Networking
What is the name of your organization?
[Unknown]: Cisco Systems
What is the name of your City or Locality?
[Unknown]: San Jose
What is the name of your State or Province?
[Unknown]: California
What is the two-letter country code for this unit?
[Unknown]: US
Is CN=aon.hostname.com, OU=Application-Oriented Networking, O=Cisco Systems, L=San Jose,
ST=CA, C=US correct?
[no]: yes
Enter key password for <test>
(RETURN if same as keystore password):
```

- Step 3** Enter the following command to view the details of your keypair.

```
[root@linux opt]# ./keytool -list -v -keystore teststore -storepass password
Keystore type: jks
Keystore provider: SUN
```

Your keystore contains 1 entry

```
Alias name: test
Creation date: April 20, 2005
Entry type: keyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=aon.hostname.com, OU=Application-Oriented Networking, O=Cisco Systems, L=San
Jose, ST=California, C=US
Issuer: CN=aon.hostname.com, OU=Application-Oriented Networking, O=Cisco Systems, L=San
Jose, ST=California, C=US
Serial number: 42768483
Valid from: Mon May 02 12:50:27 PDT 2005 until: Tue May 02 12:50:27 PDT 2006
Certificate fingerprints:
MD5: 8E:C8:62:5F:30:3F:DE:47:80:75:9A:84:6D:B6:0E:EF
SHA1: 28:0E:76:86:13:EC:B0:8D:B0:1E:73:A4:7D:87:D0:0F:55:81:E5:63
```



Note

At this point, you do not have a keystore file with your keypair. Your keypair contains a self-signed certificate, which cannot be used with AMC until it is registered with a certificate authority.

Step 4 Generate a certificate signing request (CSR) for your keypair by entering the following command:

```
[root@linux]# keytool -certreq -v -alias <alias_name> -file <outputfile> -keystore
<keystore> -storepass <storepassword>
```

This command requires you to provide the following variables:

- <alias_name> = The alias you created in [Step 1](#).
- <file> = The name of the file where the CSR is to be stored.
- <keystore> = The name of the keystore file you created in [Step 1](#).
- <storepassword> = The password for the keystore file.

```
[root@linux]# keytool -certreq -v -alias test -file testcert -keystore teststore
-storepass password
Certification request stored in file <testcert>
Submit this to your CA
```

Step 5 Submit the CSR file (*testcert* in the above example) to your certificate authority. On successful submission, the CA will provide you with a .cer file that contains your production certificate.

Step 6 Import the .cer file from your CA into the keystore created in [Step 1](#).

```
[root@linux]# keytool -import -v -alias <alias> -file <cer_file> -keystore <keystore_file>
-storepass <keystore_password>
```

This command requires you to provide the following variables:

- <alias> = Alias created in [Step 1](#).
- <cer_file> = Path to the .cer file you received from CA.
- <keystore_file> = keystore file created in [Step 1](#).
- <keystore_password> = The keystore password.

After you enter this command, information similar to the following is displayed:

```
Owner: CN=aon.hostname.com, OU=Application-Oriented Networking, O=Cisco Systems, L=San
Jose, ST=California, C=US
Issuer: OU=Secure Server Certification Authority, O="RSA Data Security, Inc.", C=US
Serial number: 3a7a57a56046cce564ce7cc500995b21
Valid from: Sun Feb 06 16:00:00 PST 2005 until: Tue Feb 07 15:59:59 PST 2006
Certificate fingerprints:
MD5: 8E:C8:62:5F:30:3F:DE:47:80:75:9A:84:6D:B6:0E:EF
SHA1: 28:0E:76:86:13:EC:B0:8D:B0:1E:73:A4:7D:87:D0:0F:55:81:E5:63
Trust this certificate? [no]: yes
Certificate was added to keystore
[Saving ./CreateKeystore/teststore.jks]
```



Note

Note the name and location of the .jks file. You will need it each time you install or upgrade AMC.

Installing and Upgrading AMC

Cisco distributes the AMC application in two formats, a package that installs a fresh copy of AMC, and a package that upgrades an AMC but preserves the existing database of nodes, properties, logs, and other settings. The instructions that follow assume installation in the `/opt/amc` directory. However, you can install AMC in any directory of your choosing.

Requirements

- You must install AMC on a local disk. AMC cannot run on a network file system.
- You must obtain a certificate from a certificate authority before installing or upgrading AMC. The keystore information must be in the Java Keystore format with a `.jks` extension. See the “[Generating a Java Keystore](#)” section on page 2-1 for instructions. AMC accepts only the well-known certificate authorities included in the Java Runtime Environment (JRE) 1.4 truststore.
- It is possible to install multiple instances of AMC on a single server if each AMC uses a unique set of TCP ports. We recommend that this be done only in testing or training environments. A given node cannot be managed by more than one AMC, and we recommend that a production AON include no more than one AMC.
- If you are upgrading AMC, be sure to deactivate any active nodes.
- You must have root-level permission on the server on which AMC is to be installed.



Caution

If you are upgrading AMC, be sure to read the latest AON Release Note before running the upgrade package. The new release note may contain critical upgrade procedures beyond those described below. Failure to follow the procedure described in the release note may result in data loss or corruption.

Step 1 Download the installation file and use the `chmod` command to make it executable.

```
[root@linux opt]# chmod +x aon-amc_<version>_lnx.bin
```

Step 2 Execute the installer.

```
[root@linux opt]# ./aon-amc_<version>_lnx.bin
Preparing to install...
```

Step 3 Enter the directory in which AMC is to be installed. The `/opt/amc` directory is the default, although any directory is acceptable.

```
Enter the directory to install the AMC to [/opt/amc]:
Directory "/opt/amc" does not exist - create? [y/n]:y
Extracting archive.
Configuring paths.
Configuring the ports that the AMC will listen on
If you are installing more than one AMC, these values
must be unique to each installation.
```

Step 4 Enter the port on which AMC will listen for HTTP requests. 7015 is the default.

```
Enter a port for http [7015]:7015
```

Step 5 Enter the port on which AMC will listen for HTTPS requests. 7010 is the default.

```
Enter a port for https [7010]:7010
```

Step 6 Enter the port on which AMC will listen for traffic from nodes. 7011 is the default.

```
Enter a port for communication with AON nodes [7011]:7011
```

Step 7 Enter the port on which AMC will listen for shutdown signals. 7025 is the default.

```
Enter a port for server shutdown signals [7025]:7025
```

Step 8 Enter the port on which AMC will listen for database transactions. 2638 is the default.

```
Enter a port for the database [2638]:2638
```

Step 9 Enter the logging level to be used while AMC runs.

```
Enter AMC logging level (DEBUG|INFO|WARN|ERROR|FATAL) [INFO]:error
```

AMC can use one of the following log levels:

- DEBUG—Logs explicit debug messages, plus informational, warning, error, and fatal messages.
- INFO—Logs informational messages, plus warning, error, and fatal messages.
- WARN—Logs warning messages, plus error and fatal messages.
- ERROR—Logs error messages and fatal messages.
- FATAL—Logs only fatal messages.



Note In production environments, we recommend that only ERROR or FATAL log levels be used. More verbose log levels can have an adverse affect on the performance of AMC.

Step 10 Enter the size of the log file in kilobytes. When the log size is exceeded, AMC saves it as a backup and generates a new log file.

```
Enter log file rollover threshold size (KB) [1024]:1024
```

Step 11 Enter the number of backup logs to keep. When the number of backup logs is exceeded, AMC discards the oldest file.

```
Enter number of backup logs to keep [5]:5
```

Step 12 AMC uses a keystore file for communication with AON nodes. Enter the path and filename for this keystore.

The AMC requires a keystore file and password to communicate with the AON node.

```
Enter the path to the keystore file:/root/amcKeystore.test.cisco.com.jks
```



Note The path to amcKeystore shown above is for illustrative purposes. You must provide the path to an actual Java keystore in order to complete the installation.

Step 13 If the keystore file has multiple keypairs, enter the name for the pair you want to use.

You may optionally enter a keyname within the keystore.

```
Enter a keyname, otherwise enter none [none]:none
```

Step 14 Enter the password associated with the keystore.

```
Enter a password for this keystore:
AMC_HOME is /opt/amc and /opt/amc
Using existing ciscoamc group
Using existing ciscoamc user
Setting permissions for AMC installation
Configuring AMC service to start at boot...
```

Step 15 Enter **y** to start AMC now or **n** to start it later.

```
Would you like to run the AMC now? [y|n]:y
Starting AMC Database...Done.
Starting AMC...Done.
Installation successful.
To uninstall, run '/opt/amc/bin/amcSetup uninstall'.
```

Step 16 Use a Web browser to navigate to the AMC log-in page to confirm that the installation was successful. The URL is **https://hostname:7010/amc**. Replace *hostname* in this URL with the name or IP address for the server running AMC.



Note

For best results, we recommend you use Microsoft Internet Explorer 6 or later with AMC.

Figure 2-1 shows the AMC log-in page.

Figure 2-1 AON Management Console Log-on Screen



Note

The default user name and password are **aonsadmin**.

Stopping, Starting, and Restarting the AMC Daemon

During the installation process, the AMC daemon (`amcd`) is configured to run when the server on which it is installed starts up, and it stops when the server is shut down. You might, however, have need to stop, start or restart the AMC daemon independently of the server. The examples that follow show how to do this.

Example 2-1 Shutting Down AMC

```
[root@linux]# /opt/amc/bin/amcd stop
Stopping AMC...waiting for services to complete...Done.
Stopping AMC Database...Done.
```


Example 2-2 Starting AMC

```
[root@linux]# /opt/amc/bin/amcd start
Starting AMC Database...Done.
Starting AMC...Done.
```

Example 2-3 Restarting AMC

```
[root@linux]# /opt/amc/bin/amcd restart
Stopping AMC...waiting for services to complete...Done.
Stopping AMC Database...Done.
Starting AMC Database...Done.
Starting AMC...Done.
```

Working with Nodes

AON nodes have no direct console access, so the first configuration task for an AON service module (AON-SM) or AON network module (AON-NM) is to define IP address and subnet masks for the AON interface. See the following sections for configuration tasks for AON nodes. Each task in the list is identified as either required or optional.

- [Configuration Prerequisites, page 2-7](#) (required)
- [Configuring a Cisco 8300 Series AON Appliance, page 2-8](#) (required)
- [Configuring Networking Parameters on a Catalyst 6500 Series Switch, page 2-10](#) (required)
- [Configuring Network Parameters on a Cisco Modular Access Router, page 2-12](#) (required)
- [Configuring Nodes to Use SSH, page 2-13](#) (optional)
- [Configuring Nodes to Register with the AMC, page 2-14](#) (required)
- [Upgrading Nodes, page 2-15](#) (optional)

**Caution**

AON modules do not support online insertion and removal. Always power off the router or switch before inserting or removing a module.

Configuration Prerequisites

This guide assumes that your switch, router, or AON appliance is properly installed. Additionally, switches and routers that will house AON nodes must be configured for basic IP communications and have their AON modules installed. See the following platform documentation if necessary:

- Cisco 8300 Series AON Appliance Hardware Installation Guide
<http://lbj.cisco.com/targets/ucdit/cc/td/doc/product/aon/aonmod/8300/8300hig/index.htm>
- Catalyst 6500 Series Switch Installation Guide
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/6000hw/inst_aug/index.htm
- Catalyst 6500 Series Switch Module Installation Guide
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/6000hw/mod_inst/index.htm
- Cisco Modular Access Routers
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/index.htm

- Cisco Network Modules Hardware Installation Guide
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/nm_inst/nm-d oc/index.htm

Configuring a Cisco 8300 Series AON Appliance

A Cisco 8300 AON Appliance arrives from the factory with AON software preinstalled. In order to configure an appliance, you must connect a terminal server to the serial port on the rear of the appliance. For instructions on connecting a terminal server, see the *Cisco 8300 Series AON Appliance Hardware Installation Guide*. This section includes the following topics:

- [Configuring Networking Parameters, page 2-8](#)
- [Disabling Cisco Discovery Protocol, page 2-9](#)

Configuring Networking Parameters

Perform the following steps to configure networking parameters:

- Step 1** With your terminal server connected, power on the appliance and allow it to boot. When the appliance is ready for configuration, a **Password :** prompt is displayed. Enter the default password of **oonsadmin**.

```

Welcome to Cisco AON Engine
  (Version: 1.1.0.189)

Fri Nov  4 03:24:41 PST 2005
AON boot: hit RETURN to set boot flags: 0002

Available boot flags (enter the sum of the desired flags):
  0x0000 - exit this menu and continue booting normally
  0x2000 - disable login security

[AON boot - enter bootflags (type '-' to exit)]: 0x0000
You have entered boot flags = 0x0
Boot with these flags? [yes]: y
Boot with these flags? [yes]: yes

***** rc.aesop *****
Setting timezone: No timezone configured
Loading Tarari Drivers...
SUCCESS: Loaded Tarari Drivers
Loading Cisco WCCP module
wccp: v1.00 (20000327), debug=0
Kernel IP routing table
Destination      Gateway          Genmask         Flags   MSS Window  irtt Iface
Serial Number: 99C7523
Reading Manifest...done.
Doing Certificate Check
Certificate Check Done
INIT: Entering runlevel: 2
***** rc.post_install *****
INIT: Switching to runlevel: 4
INIT: Sending processes the TERM signal

waiting 51 ...
Password :

```

- Step 2** Enter configuration terminal mode.

```
defaulthost> configure terminal
Enter configuration commands, one per line. End with exit.
```

Step 3 Enter interface configuration mode for Gigabit Ethernet Interface 1

```
defaulthost(config)> interface gigabitethernet 1
```



Note The appliance includes three gigabit ethernet connectors, however, only Gigabit Ethernet 1 is supported in AON version 1.1.

Step 4 Enter the IP address and subnet mask to be used by the appliance, then exit interface configuration mode.

```
defaulthost(config-interface)> ip address 192.168.56.106 255.255.255.0
WARNING!!! Changing interface IP address will disrupt connectivity and traffic!
defaulthost(config-interface)> exit
SYSTEM ONLINE
```

Step 5 Configure the default gateway to be used by the appliance.

```
defaulthost(config)> ip default-gateway 192.168.56.1
```

Step 6 Configure the domain name to be used by the appliance.

```
defaulthost(config)> ip domain-name cisco.com
```

Step 7 Configure the domain name servers to be used by the appliance.

```
defaulthost(config)> ip name-server 192.168.168.183 192.168.226.120
```

Step 8 Configure the NTP server to be used by the appliance.

```
defaulthost(config)> ntp server 192.168.156.11
```

Step 9 Configure the hostname to be used by the appliance.

```
defaulthost(config)> hostname aon-appliance
```

Step 10 Enable secure shell (SSH) access for the appliance.

```
aon-appliance(config)> ssh enable
```

Step 11 Change the default password.

```
aon-appliance(config)> login password unencrypted mypassword
```



Note For a detailed description of SSH and login passwords, see the [“Configuring Nodes to Use SSH”](#) section on page 2-13.

Step 12 Exit configuration mode, and save the new configuration.

```
aon-appliance(config)> exit
aon-appliance> write memory
```

Disabling Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is primarily used to obtain protocol addresses of neighboring devices and discover the platform of those devices. CDP is enabled by default, and the appliance sends CDP Version-1 (CDPv1) advertisements. It receives both CDPv1 and CDPv2 advertisements. [Example 2-4](#) shows CDP being disabled.

If you do not need CDP, you should disable it.



Note

Only the Cisco 8300 Series AON Appliance supports CDP at this time.

Example 2-4 Disabling CDP

```
aon-appliance> configure terminal
Enter configuration commands, one per line. End with exit.
aon-appliance(config)> no cdp run
aon-appliance(config)> exit
aon-appliance> write memory
```



Note

You can use **cdp run** to enable CDP again if necessary.

Configuring Networking Parameters on a Catalyst 6500 Series Switch

You must configure a VLAN for the AON-SM, then assign an IP address to it. These tasks are covered in the following sections:

- [Configuring a VLAN under the Catalyst Operating System, page 2-10](#) (required for Catalyst operating system)
- [Configuring a VLAN under Cisco IOS, page 2-11](#) (required for Cisco IOS)
- [Assigning IP Addresses to the AON-SM Interface, page 2-11](#) (required)

Configuring a VLAN under the Catalyst Operating System

You must configure a VLAN for the AON-SM by completing the following steps:

Step 1 Create a VLAN to be used by the AON node.

```
Router> (enable) set vlan 100
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 100 configuration successful
```

Step 2 Assign the VLAN to the AON node.

```
Router> (enable) set vlan 100 5/2
VLAN 100 modified.
VLAN 1 modified.
VLAN Mod/Ports
-----
100 5/2

Vlan 100 is active.
Router> (enable)
```

Configuring a VLAN under Cisco IOS

You must configure a VLAN for the AON-SM by completing the following steps:

- Step 1** Enter configuration terminal mode.

```
MSFC# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

- Step 2** Create a VLAN to be used by the AON node.

```
MSFC(config)# vlan 100
```

- Step 3** Make the VLAN active, then exit configuration terminal mode.

```
MSFC(config-vlan)#state active  
MSFC(config)# exit
```

- Step 4** Assign the VLAN to the AON-SM.

```
MSFC(config)# AON module 6 vlan 100
```

- Step 5** Enter interface configuration mode for the VLAN.

```
MSFC(config)# interface vlan 100
```

- Step 6** Assign an IP address and subnet mask to the VLAN.

```
MSFC(config-if)# ip address 192.168.22.36 255.255.255.0
```

Assigning IP Addresses to the AON-SM Interface

To assign IP addresses to the AON service module running in a Catalyst 6500 series switch, perform the following steps:

- Step 1** If this is an active node for which you are assigning a new IP address, use AMC to deactivate it.

- Step 2** Open a session to the AON-SM, then enter configuration terminal mode.

```
Router# session slot number processor number  
The default escape character is Ctrl-^, then x.  
You can also type 'exit' at the remote prompt to end the session  
Trying 127.0.0.31 ... Open
```

```
Welcome To Cisco AON Engine
```

```
aon-node> enable  
aon-node# configure terminal
```

- Step 3** Select an interface to configure.

```
aon-node(config)# interface GigabitEthernet 2
```



Note

At this time, AON supports only the GigabitEthernet 2 interface.

- Step 4** Specify the IP address for the interface, then exit interface configuration mode.
- ```
aon-node(config-interface)#ip address 192.168.3.11 255.255.255.0
aon-node(config-interface)#end
```
- Step 5** Specify the IP address for the default gateway, then exit configuration terminal mode.
- ```
aon-node(config)#ip default-gateway 192.168.3.1
aon-node(config)#end
```
- Step 6** Save the configuration in NVRAM.
- ```
aon-node# write memory
```
- Step 7** Proceed to the “[Configuring Nodes to Register with the AMC](#)” section on page 2-14 to continue configuring the AON-SM.
- 

## Configuring Network Parameters on a Cisco Modular Access Router

To assign IP addresses to the AON network module running in a router, perform the following steps:

- Step 1** If this is an active node for which you are assigning a new IP address, use AMC to deactivate it.
- Step 2** Enter configuration mode for the AON network module interface.
- ```
Router(config)# interface AONS-engine 1/0
```
- Step 3** Specify that FastEthernet 0/0 interface is unnumbered.
- ```
Router(config-if)# ip unnumbered FastEthernet 0/0
```
- Step 4** Configure an IP address for the interface used by the AON network module.
- ```
Router(config-if)# service-module ip address 10.4.1.184 255.255.255.0
```
- Step 5** Specify the default gateway used by the AON network module.
- ```
Router(config-if)# service-module ip default-gateway 10.4.1.183
```
- Step 6** Bring up the AON network module interface.
- ```
Router(config-if)# no shutdown
```
- Step 7** Exit configuration mode.
- ```
Router(config-if)# exit
```
- Step 8** Configure IP routing on the router.
- ```
Router(config)# ip routing
```
- Step 9** Define a static IP route to the AON network module.
- ```
Router(config)# ip route 10.4.1.184 255.255.255.255 AONS-Engine1/0
```
- Step 10** Define a static IP route to the default gateway.
- ```
Router(config)# ip route 0.0.0.0 0.0.0.0 10.4.1.1
```
- Step 11** Exit configuration mode.
- ```
Router(config)# exit
```

**Step 12** Save the configuration in NVRAM.

```
Router# write memory
```

---

## Configuring Nodes to Use SSH

Using the default configuration, you connect to a node's command-line interface using telnet or a serial interface. AON nodes running release 1.1 and later versions can be configured to use secure shell (SSH). When SSH is used, all traffic between the node and your SSH client is encrypted. Additionally, SSH enables users to configure a node without providing access to the switch or router command-line interface. To configure a node to use SSH, perform the following steps:

**Step 1** In the node's configuration terminal mode, use the **ssh enable** command to enable ssh.

```
aon-node(config)> ssh enable
```



**Note** Until you complete [Step 2](#), the default password to gain secure access to a node is **aonsadmin**.

---

**Step 2** Use the login password command to configure a password for SSH access. This command accepts either encrypted or plaintext passwords.

- To enter a plain text password:

```
aon-node(config)> login password unencrypted cisco
```

- To enter an MD5 encrypted password

```
aon-node(config)> login password encrypted $1$7v.O130F$xGo.LUNGt0eYxWTCZ/McQ
```

**Step 3** Exit configuration terminal mode and save the configuration.

```
aon-node(config)> exit
aon-node> write memory
```

**Step 4** Verify the configuration by using an SSH client to connect to the IP address assigned to the node.

```
[root@linux root]# ssh admin@10.4.1.92
The authenticity of host '10.4.1.92 (10.4.1.92)' can't be established.
RSA key fingerprint is 50:fa:d4:7e:46:e3:7b:2f:17:0d:e6:9f:d0:b4:1e:d5.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.4.1.92' (RSA) to the list of known hosts.
admin@10.4.1.92's password:
```



**Note** The only username permitted to connect to an AON node is **admin**.

---

## Configuring Nodes to Register with the AMC

In order to register with the AMC, the AON node must be configured with connection details for both itself and the AMC. To complete this task, perform the following steps:

- 
- Step 1** Enter configuration terminal mode on the AON node, then create an AON configuration ID. A configuration ID can be any combination of letters and numbers.
- ```
AON-node (config)# AON config abc create
```
- Step 2** Configure the hostname or IP address of AMC. This is used by the AON node to communicate with AMC.
- ```
AON-node (config)# AON config abc amc host 10.1.1.1
```
- Step 3** Assign an IP address to the AON management agent.
- ```
AON-node (config)# AON config abc ama host 10.1.1.2
```
- Step 4** Activate the AON configuration.
- ```
AON-node (config)# AON config abc activate
```
- Step 5** Specify a network time protocol (NTP) server that the node can use to maintain accurate time.
- ```
AON-node (config)# ntp server 10.1.1.10
```
- Step 6** Specify the domain name of the node.
- ```
AON-node (config)# ip domain-name cisco.com
```
- Step 7** Specify the DNS server to be used by the node.
- ```
AON-node (config)# ip name-server 10.1.10.10
```
- Step 8** Exit configuration terminal mode. When AON asks to restart, enter **n**.
- ```
AON-node (config)# exit
CAUTION!! Configuration changed. Need to restart AON.
Confirm restart[y]? n
```
- Step 9** Use the **write memory** command to save the AON configuration to nonvolatile memory, then restart AON.
- ```
AON-node> write memory
AON-node> AON restart force
!!CAUTION!! Restarting all processes right away.
Are you sure[n]? y
Start counting down before restart
```

This may take a while longer...

After the AON restart is complete, the node attempts to register with the AMC. The AMC ignores these attempts until a node with the proper credentials has been added.

- Step 10** Use the **show version** command to obtain the module serial number (highlighted below). You need this information when you create a new node in AMC.

```
AON-node> show version
CPU Model:                Pentium III (Coppermine)
CPU Speed (MHz):          498.675
CPU Cache (KByte):        256
Chassis Type:              C2691
Chassis Serial:           12345678901
Module Type:               NM-AON-K9
Module Serial:             FOC082313YY
AON:                       0.0.0.409
AMA:                       0.0.0.409
```

- Step 11** Use the **write memory** command to save the configuration

```
AON-node> write memory
```

Upgrading Nodes

Cisco periodically releases new versions of AON software to add features and to correct defects. Included in these releases is a package that upgrades your AMC installation and nodes while preserving your existing databases and Policy Execution Plans (PEPs). This section covers the following topics:

- [Upgrading an AON Appliance or AON-NM, page 2-15](#)
- [Upgrading an AON-SM, page 2-18](#)

Prerequisites

- Obtain the upgrade software from the Software Center on Cisco.com. Copy the software for upgrading nodes to a Web or FTP server that is accessible to the nodes.
- See the release note for the AON software release. It includes important information about the new software release. It may also contain critical upgrade instructions that apply only to a specific AON release.
- Upgrade AMC before you upgrade AON nodes. See the “[Installing and Upgrading AMC](#)” section on page 2-4.



Caution

Be sure to read the latest AON release note before starting an upgrade. The new release note may contain critical upgrade procedures beyond those described below. Failure to follow the procedure described in the release note may result in data loss or corruption.

Upgrading an AON Appliance or AON-NM

The Cisco 8300 Series AON Appliance and the AON networking module have very similar upgrade procedures. To upgrade the software on these devices, perform the following steps:

- Step 1** Obtain the new software from Cisco. Copy the helper image to a TFTP server; copy the other upgrade files to an FTP or Web server.
- Step 2** If the node you are upgrading is active, use AMC to deactivate it.

Step 3 Use a terminal server to connect to the node, enter configuration terminal mode, and reload the software.

```
aon-appliance> reload
Are you sure you want to reload?
Doing a reload will cause any unsaved configuration data to be lost.
Continue[y]? : y
Allow graceful shutdown of aons processes[y]? : y
Timeout after (seconds)[300]? :
INIT: Remounting device 08:01 ... OK
Done.
Restarting system.
```

Step 4 Perform the following steps to enter the bootloader and boot the helper image from a TFTP server.

- a. While the node reboots, watch for the prompt shown below in bold text, then enter ******* to enter the bootloader.

Please enter '*' to change boot configuration: *****

- b. Use the **config** command to enter the node's networking parameters. When you boot from the network, the node uses this configuration information to download new software from the TFTP server.

```
Cisco Bootloader> config
IP Address > 10.4.1.184
IP Netmask > 255.255.255.0
TFTP Server > 10.69.23.173
Gateway IP Address > 10.4.1.183
Default Helper-file > package_name
```



Note

The package name varies depending on the type of software being upgraded. Valid package names include the following:

- **aon-apl-8340_1.1.0.189_k9_helper_lnx**—helper image for appliance.
- **aon-nm_1.1.0.189_k9_helper_lnx**—helper image for AON-NM.

Do not attempt to load any other software packages.

```
Ethernet interface [internal] > internal
Default Boot [none|disk] [disk] > disk
Default bootloader [primary|secondary] primary >
Updating flash with bootloader configuration
```

- c. Use the **boot network** command to load the new helper from the TFTP server.

```
Cisco Bootloader> boot network
Me: 10.4.1.184, Server: 10.69.23.173, Gateway: 10.4.1.183
Netbooting package_name (CTRL-C aborts)
```



Note

The output produced by booting from the helper image is extensive. It has been omitted here for brevity.

```
***** rc.post_install *****
INIT: Switching to runlevel: 4
INIT: Sending processes the TERM signal
monitor: INFO monitor output log START

monitor: INFO monitor output log STARTED: CLIFrontEnd
```

Step 5 If you are upgrading the bootloader, use the **software install package url** command to retrieve and install this software. The helper cannot resolve domain names, so be sure to use only an IP address when you enter a URL. If you are not upgrading the bootloader, skip to [Step 6](#).

- For FTP:

```
AONinstaller#> software install package url ftp://ip_address/package-name user username
password password
```

- For HTTP:

```
AONinstaller#> software install package url http://ip_address/package-name
```

```
Connecting to host...
```

% Total	% Received	% Xferd	Average Speed		Time	Curr.
			Dload	Upload	Total	Current
100	63865	100	63865	0	0	903k
						0 0:00:00
						0:00:00 0:00:00
						1003k

Which Bootloader would you like to update primary or secondary (p,s) [p] p

```
WARNING: DO NOT POWER OFF ROUTER DURING UPDATE!
```

```
Updating...complete.
```

```
Cleaning up...complete.
```



Note

The package name varies depending on the type of software being upgraded. Valid package names include the following:

- aon-apl-8340_version_bl.pkg—bootloader for the appliance.
- aon-nm_version_bl.pkg—bootloader for the AON-NM.
- aon-apl-8340_version_k9_lnx.pkg—AON software for the appliance.
- aon-nm_version_k9_lnx.pkg—AON software for the AON-NM.

Do not attempt to load any other software packages.

Step 6 Use the **software install package url** command to retrieve and install the upgrade package. The helper cannot resolve domain names, so be sure to use only an IP address when you enter a URL.

- For FTP:

```
AONinstaller#> software install package url ftp://ip_address/package-name user username
password password
```

- For HTTP:

```
AONinstaller#> software install package url http://ip_address/package-name
```

```
Connecting to host...
```

% Total	% Received	% Xferd	Average Speed		Time	Curr.
			Dload	Upload	Total	Current
100	81915	100	81915	0	0	727k
						0 0:00:00
						0:00:00 0:00:00
						961k

```
File listing is signed
```

```
Retrieving aon-nm_1.1.0.185_k9_lnx.manifest from 171.71.46.117
```

```
Manifest Version retrieved is 1.0
```

```
Manifest Version matches package version
```

```
WARNING: This is an unrecoverable operation!
```

```
WARNING: This will completely replace existing AON software.
```

```
Do you wish to continue (y,n) [n] y
```

```
Scanning filesystem for errors (this may take a minute)
```

```

No errors found on filesystem (/dev/hda1)

Removing old installation...done.
Retrieving aon-nm_1.1.0.185_k9_lnx.prt1 from 171.71.46.117
Connecting to host...
  % Total    % Received % Xferd  Average Speed          Time      Curr.
  Dload  Upload  Total    Current  Left      Speed
100 106M 100 106M    0     0  835k      0  0:02:10  0:02:10  0:00:00  867k
complete.
Validating security header...done
Extracting files from package...done
Installing software onto the system...
Mon Oct 17 09:58:22 UTC 2005
100% complete.
Done.
Applying image signature...complete.
Cleaning up...complete.
AONinstaller#>

```

Step 7 Use the **reboot** command to reset the node and boot the new software image.

```

AONinstaller#> reboot
WARNING: This will reboot the AON Engine!
Do you wish to continue (y,n) [n] y
INIT: monitor:      INFO monitor output log END
Remounting device 01:00 ... OK
Done.
Restarting system.

```

Upgrading an AON-SM

How you upgrade an AON-SM depends on whether the switch is running Cisco IOS or the Catalyst operating system. The following sections describe how to upgrade the AON-SM for each switch operating system:

- [Using Catalyst Operating System to Upgrade an AON-SM, page 2-18](#)
- [Using Cisco IOS to Upgrade an AON-SM, page 2-21](#)

Using Catalyst Operating System to Upgrade an AON-SM

To upgrade the AON software on an AON service module running under Catalyst operating system, perform the following steps.

- Step 1** Obtain the new software from Cisco and copy it to an FTP or Web server.
- Step 2** If the node is active, use AMC to deactivate it.
- Step 3** Set the default boot partition to boot the AON-SM with the helper image contained on partition 4 of the compact flash.

```

Router> (enable) set boot device cf:4 module_number
Device BOOT variable = cf:4
Memory-test set to PARTIAL
Warning: Device list is not verified but still set in the boot string.

```

Step 4 Reload the AON-SM

```
Router> (enable) reset 5
This command will reset module 5.
Unsaved configuration on module 5 will be lost
Do you want to continue (y/n) [n]? y
```

Step 5 Open a session to the node.

```
Router# (enable) session slot <slot number>
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.31 ... Open
Starting Config
```

```
Welcome To Cisco AON Installer
          (Version: version_number)
```

```
*****
* AONS Installer IP Configuration *
*****
```

```
Please enter the IP address of your module: 10.45.0.1
Please enter the netmask of your module: 255.255.0.0
Please enter the default gateway for your module: 10.45.0.2
```

The following IP configuration is set:

```
IP       : 10.45.0.1
NETMASK: 255.255.0.0
GATEWAY: 10.45.0.2
```

Do you wish to use this configuration (y,n) [n] **y**

Step 6 Load the new helper image into compact flash.

- For FTP:

```
AONinstaller#> software install package url ftp://ftp_server_ip_address/helper-image-name
user username password password
```

- For HTTP:

```
AONinstaller#> software install package url
http://http_server_ip_address/helper-image-name
```



Note

The installer cannot resolve domain names. Be sure to use only an IP address when you enter a URL.

```
Connecting to host...
  % Total    % Received % Xferd  Average Speed          Time      Curr.
 100 30803  100 30803    0     0  859k      0  0:00:00  0:00:00  0:00:00 6879k
File listing is signed
Retrieving aon-svc_version_helper_lnx.manifest from 10.47.0.2
Manifest Version retrieved is 1.0
Manifest Version matches package version
WARNING: This is an unrecoverable operation!
WARNING: This will erase all data on the AONS Engine and install new software.
WARNING: Configuration and user data must be restored after the system restarts.
```

```
Do you wish to continue (y,n) [n] y
Which Helper would you like to update primary or secondary (p,s) [p]
```

Step 7 Reset the AON-SM to load the new helper image.

```
cat6K# reset 5
```

Step 8 Open a session to the module.

```
cat6k# session 5
```

Step 9 Use the **software install package url** command to retrieve and install the upgrade package.

```
AONinstaller#> software install package url ftp://ftp_server_ip_address/package-name
Connecting to host...
  % Total    % Received % Xferd  Average Speed          Time              Curr.
                Dload Upload Total    Current  Left      Speed
100 146k 100 146k    0      0 1540k      0 0:00:00 0:00:00 0:00:00 3164k
File listing is signed
Retrieving aon-svc_version_helper_lnx.manifest from 10.47.0.2
Manifest Version retrieved is 1.0
Manifest Version matches package version
WARNING: This is an unrecoverable operation!
WARNING: This will erase all data on the AON Engine and install new software.
WARNING: Configuration and user data must be restored after the system restarts.

Do you wish to continue (y,n) [n] y
prepfs kplus reiser
umount: /dev/hdc1: not mounted

*****
* Warning: The dma on your hard drive is turned off. *
* This may really slow down the fsck process.         *
*****
Reiserfs super block in block 16 on 0x1601 of format 3.6 with standard journal
Blocks (total/free): 4883752/4822276 by 4096 bytes
Filesystem is cleanly umounted
Replaying journal..
0 transactions replayed
Checking internal tree..finished
Removing old installation...done.
Retrieving aon-svc_version_helper_lnx.prt1 from 10.47.0.2
Connecting to host...
  % Total    % Received % Xferd  Average Speed          Time              Curr.
                Dload Upload Total    Current  Left      Speed
100 89.9M 100 89.9M    0      0 4332k      0 0:00:21 0:00:21 0:00:00 2638k
complete.
Validating security header...done
Extracting files from package...done
Installing software onto the system...
100% complete.
Done.
```

Step 10 Set the device from which the module will boot when it is reset.

```
cat6K# (enable) set boot device hdd:1 5
```

Step 11 Reset the AON-SM to load the new image from the hard drive.

```
cat6k# (enable) reset 5
```

Using Cisco IOS to Upgrade an AON-SM

To upgrade the AON software on an AON service module running under the Cisco IOS, perform the following steps.

Step 1 Obtain the new software from Cisco and copy it to an FTP or Web server.

Step 2 If the node is active, use AMC to deactivate it.

Step 3 Boot the AON-SM to the helper image contained on the compact flash.

```
Router# hw-module module 3 reset cf:4
Device BOOT variable for reset = <cf:4>
Warning: Device list is not verified.
```

```
Proceed with reload of module? [confirm]
```

Step 4 Open a session to the module.

```
Router# session slot <slot number> processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.31 ... Open
Starting Config
```

```
Welcome To Cisco AON Installer
                (Version: version_number)
```

```
*****
* AONS Installer IP Configuration *
*****
```

```
Please enter the IP address of your module: 10.45.0.1
Please enter the netmask of your module: 255.255.0.0
Please enter the default gateway for your module: 10.45.0.2
```

```
The following IP configuration is set:
```

```
IP       : 10.45.0.1
NETMASK: 255.255.0.0
GATEWAY: 10.45.0.2
```

```
Do you wish to use this configuration (y,n) [n] y
```

Step 5 Load the new helper image into compact flash.

- For FTP:

```
installer#> software install package url ftp://ftp_server_ip_address/helper-image-name
user username password password
```

- For HTTP:

```
installer#> software install package url http://http_server_ip_address/helper-image-name
```



Note

The installer cannot resolve domain names. Be sure to use only an IP address when you enter a URL.

```
Connecting to host...
  % Total    % Received % Xferd  Average Speed          Time          Curr.
                                Dload Upload Total      Current Left      Speed
100 30803  100 30803    0     0  859k      0  0:00:00  0:00:00  0:00:00  6879k
File listing is signed
Retrieving aon-svc_version_helper_lnx.manifest from 10.47.0.2
```

```
Manifest Version retrieved is 1.0
Manifest Version matches package version
WARNING: This is an unrecoverable operation!
WARNING: This will erase all data on the AONS Engine and install new software.
WARNING: Configuration and user data must be restored after the system restarts.
```

```
Do you wish to continue (y,n) [n] y
Which Helper would you like to update primary or secondary (p,s) [p]
```

Step 6 Reset the AON-SM to load the new helper image.

```
cat6K# hw-module module slot number reset cf:4
```

Step 7 Open a session to the module.

```
cat6k# session slot slot number processor 1
```

Step 8 Use the **software install package url** command to retrieve and install the upgrade package.

```
AONinstaller#> software install package url ftp://ftp_server_ip_address/package-name
Connecting to host...
```

% Total	% Received	% Xferd	Average Speed	Time	Curr.
			Dload Upload Total	Current	Left Speed
100	146k	100	146k	0	0
			1540k	0	0
				0:00:00	0:00:00
				0:00:00	0:00:00
					3164k

File listing is signed

Retrieving aon-svc_version_helper_lnx.manifest from 10.47.0.2

Manifest Version retrieved is 1.0

Manifest Version matches package version

WARNING: This is an unrecoverable operation!

WARNING: This will erase all data on the AON Engine and install new software.

WARNING: Configuration and user data must be restored after the system restarts.

Do you wish to continue (y,n) [n] **y**

prepfs kplus reiser

umount: /dev/hdc1: not mounted

```
*****
* Warning: The dma on your hard drive is turned off. *
* This may really slow down the fsck process. *
*****
```

Reiserfs super block in block 16 on 0x1601 of format 3.6 with standard journal

Blocks (total/free): 4883752/4822276 by 4096 bytes

Filesystem is cleanly unmounted

Replaying journal..

0 transactions replayed

Checking internal tree..finished

Removing old installation...done.

Retrieving aon-svc_version_helper_lnx.pt1 from 10.47.0.2

Connecting to host...

% Total	% Received	% Xferd	Average Speed	Time	Curr.
			Dload Upload Total	Current	Left Speed
100	89.9M	100	89.9M	0	0
			4332k	0	0
				0:00:21	0:00:21
				0:00:21	0:00:00
					2638k

complete.

Validating security header...done

Extracting files from package...done

Installing software onto the system...

100% complete.

Done.

Step 9 Reset the AON-SM to load the new image from the hard drive.

```
cat6K# hw-module module slot number reset hdd:1
```




Working with Nodes

This chapter includes the following topics

- [Managing Nodes, page 3-1](#)
- [Managing Virtual Clusters, page 3-12](#)
- [Managing WCCP Servers, page 3-11](#)
- [Configuring Recovery, page 3-21](#)
- [Deploying to Nodes, page 3-22](#)
- [Viewing Logs, page 3-24](#)
- [Viewing Events, page 3-24](#)

Managing Nodes

Nodes are the individual devices that process messages in an AON environment. After being configured for basic network connectivity, a node must be configured to register with an AMC. On receipt of proper credentials, the AMC assumes control of the node.

From the perspective of the AMC, nodes exist in one of the following states.

- **Unregistered**—Node created in the AMC, but no successful establishment of a trust relationship with AMC.
- **Registered**—Node successfully established a trust relationship with AMC.
- **Active**—Node activated by the administrator. Active nodes are able to receive deployment requests and process messages.
- **Inactive**—Formerly active node that has gone offline.
- **Replaced**—Node replaced by another node. During replacement, the new node assumes all processing responsibilities of the node being replaced. Replaced nodes cannot be activated again, nor can they be further configured by an administrator.

This section covers the following topics:

- [Creating Nodes, page 3-2](#)
- [Configuring WCCP for Traffic Redirection, page 3-4](#)
- [Editing Nodes, page 3-6](#)
- [Deleting Nodes, page 3-7](#)

- [Replacing Nodes, page 3-8](#)
- [Exporting Nodes, page 3-9](#)

Creating Nodes

This section describes the procedure for creating a new AON node. To complete this procedure, you need access to the command-line interface of the node you are adding, and you need administrator access to AMC.

Prerequisites

- AMC must be installed and running, and you must have appropriate privileges to create network nodes.
- Your node must be configured for basic IP network connectivity.

Step 1 Connect to the command-line interface of the AON node. Use the **show version** command to obtain the module serial number (highlighted below).

```
aon-node> show version
CPU Model:           Pentium III (Coppermine)
CPU Speed (MHz):    498.675
CPU Cache (KByte):  256
Chassis Type:       C2691
Chassis Serial:     12345678901
Module Type:        NM-AON-K9
Module Serial:      FOC082313YY
AONS:               0.0.0.409
AMA:                0.0.0.409
```

Note the module serial number highlighted above. You will need this number to complete [Step 3](#).

Step 2 Log in to AMC and go to **Network > Network Nodes > Manage** to load the Manage Network Nodes page. Click the **New** button to load the New Network Node page, shown in [Figure 3-1](#).

Figure 3-1 Create a Network Node

The screenshot shows the AMC web interface. On the left is a navigation menu with 'Network Nodes' expanded, showing 'Manage', 'Configure', and 'Activate/Deactivate'. The main content area has a breadcrumb path 'Network > Network Nodes > Manage > New' and a title 'New Network Node'. Below the title are three input fields: '* Name:', '* Serial Number:', and 'Description:'. At the bottom right are 'Save' and 'Cancel' buttons.

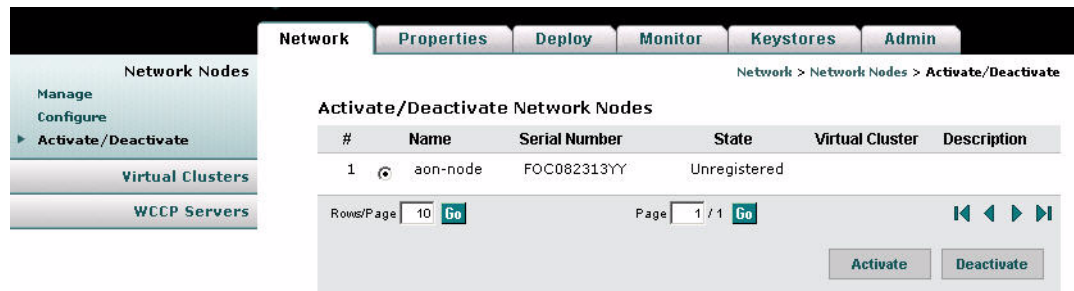
Step 3 Complete the entries on this page as described in [Table 3-1](#).

Table 3-1 New Network Node Entries

Entry	Description
Name	Name of your choosing for this node.
Serial Number	Enter the serial number obtained in Step 1 .
Description	Optional entry.

Step 4 Click Save to create the network node. [Figure 3-2](#) shows the Manage Network Nodes page with the new node in the Unregistered state. The node remains in this state until you configure the AON module to communicate with the AMC in the next step.

Figure 3-2 Unregistered Network Node



Step 5 In Configuration Terminal mode on the AON module, create an AON configuration. This configuration enables the AON node to register with the AMC.

```
aon-node> configure terminal
Enter configuration commands, one per line. End with exit.
aon-node(config)> aon config configuration_id create
aon-node(config)> aon config configuration_id ama host module_IP_address
aon-node(config)> aon config configuration_id amc host AMC_IP_address
aon-node(config)> aon config configuration_id activate
aon-node(config)> exit
CAUTION!! Configuration changed. Need to restart AONS.
Confirm restart[y]? y
graceful restart[y]? n
Start counting down before restart
```

This may take a while longer...

Step 6 After the module restarts, use the **write memory** command to save the configuration.

```
aon-node> write memory
```

- Step 7** In your browser window, click the browser's **Reload** button to refresh the Manage Network Nodes page. The new node should now be registered, as shown in [Figure 3-3](#).

Figure 3-3 Registered Network Node

The screenshot shows the 'Network Nodes' management page. The breadcrumb trail is 'Network > Network Nodes > Activate/Deactivate'. The page title is 'Activate/Deactivate Network Nodes'. A table lists one node with the following details:

#	Name	Serial Number	State	Virtual Cluster	Description
1	aon-node	FOC082313YY	Registered		

Below the table, there are pagination controls: 'Rows/Page' set to 10, 'Page' 1 of 1, and navigation arrows. There are also 'Activate' and 'Deactivate' buttons.



Tip

If your network node remains unregistered, verify that the serial number is entered exactly as described in [Step 3](#). The AMC will not establish trust with a node if this information is incorrect.

- Step 8** Click the Activate/Deactivate link to load the Activate/Deactivate Network Nodes page, then click the radio button for the registered node. Click the **Activate** button.

When the state changes to Active, as shown in [Figure 3-4](#), the node is ready for configuration deployment.

Figure 3-4 Activate a Network Node

The screenshot shows the 'Network Nodes' management page. The breadcrumb trail is 'Network > Network Nodes > Manage'. The page title is 'Manage Network Nodes'. A table lists one node with the following details:

#	Name	Serial Number	State	Description
1	aon-node	FOC082313YY	Active	

Below the table, there are pagination controls: 'Rows/Page' set to 10, 'Page' 1 of 1, and navigation arrows. There are also 'New', 'Show', 'Edit', 'Replace', and 'Delete' buttons.



Note

You can make configuration changes to a node in the registered or unregistered state, however, you cannot deploy those configuration changes until the node becomes active.

Configuring WCCP for Traffic Redirection

AON nodes can be configured to use WCCP for traffic redirection. When this feature is configured, a node can intercept messages using a specific port, then redirect them to another destination for further processing.

How to Get There

- Go to **Network > Network Nodes > Configure**. Select a node, then click the **WCCP for Traffic Redirection** button and click **New**.

Figure 3-5 shows the New WCCP Service Group page.

Figure 3-5 New WCCP Service Group

The screenshot shows the 'New WCCP Service Group' configuration page. The left sidebar has 'Network Nodes' selected, with sub-options 'Manage', 'Configure', and 'Activate/Deactivate'. The main content area has a breadcrumb trail: 'Network > Network Nodes > Configure > WCCP for Traffic Redirection'. The form fields are as follows:

- * Service Group ID: 51
- * Multicast Address: 10 . 0 . 13 . 2
- Authentication Password: [masked]
- Confirm Authentication Password: [masked]
- * Port Map: 80
- * Listener Port: 8080

Buttons at the bottom: Add Servers, ACL/Classifier, Save, Cancel.

Table 3-6 shows the entries available on the New WCCP Service Group page.

Table 3-2 New WCCP Service Group Entries

Entry	Description
Service Group ID	Unique number for each service group. Range is 51 – 99.
Multicast address	IP address to be used by members of this service group.
Authentication password	Password by members of this service group for authentication.
Port map	Comma-delimited string of destination ports to be redirected.
Listener port	Comma-delimited string of ports at which an adapter is listening for traffic.

Editing Nodes

The AMC enables you to edit the name and description of any node. If a node is unregistered, you can also change the serial number.

How to Get There

Go to **Network Nodes > Manage** then select a node and click the **Edit** button. See [Figure 3-6](#).

Figure 3-6 Edit a Network Node

The screenshot displays the 'Edit Network Node' page in a web application. On the left is a navigation sidebar with 'Network Nodes' selected, showing sub-options: 'Manage', 'Configure', and 'Activate/Deactivate'. Below these are 'Virtual Clusters' and 'WCCP Servers'. The main area has a breadcrumb trail: 'Network > Network Nodes > Manage > Edit'. At the top of the main area are tabs: 'Network', 'Properties', 'Deploy', 'Monitor', 'Keystores', and 'Admin'. The 'Edit Network Node' form includes:

- * Name:
- * Serial Number:
- Description:

 At the bottom right of the form are 'Save' and 'Cancel' buttons.

Actions to Take

You can take one of the following actions:

- Make changes to the Name or Description. If a node is unregistered, you can also make changes to the serial number.
- Click the **Save** button to preserve your changes.
- Click the **Cancel** button to return to the Manage Network Nodes page.

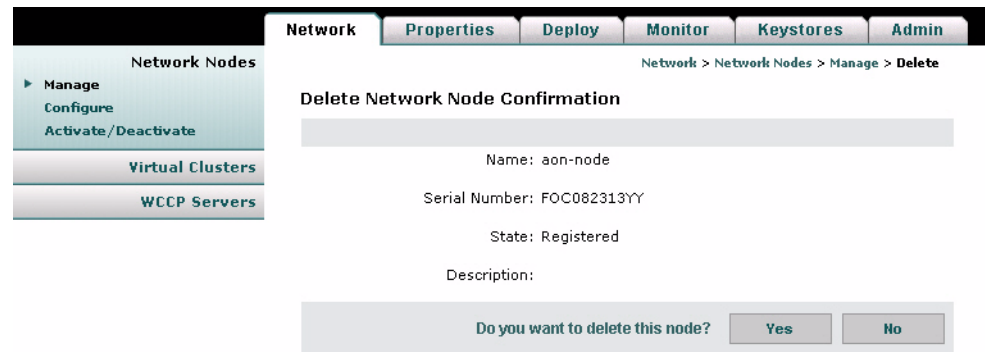
Deleting Nodes

You can delete any node, regardless of its state. If a node is active, the AMC instructs the node to stop message processing before it is deleted.

How to Get There

Go to **Network Nodes > Manage**, then select a node and click the **Delete** button. See [Figure 3-7](#).

Figure 3-7 Delete a Network Node



Actions to Take

You can take one of the following actions:

- Click the **Yes** button to delete the node.
- Click the **No** button to cancel deletion and return to the Manage Network Nodes page.

Replacing Nodes

You can replace a registered node with another registered node. Active and unregistered nodes cannot be replaced, nor can they serve as replacements. After a node has been replaced, you can no longer change its configuration in the AMC, nor can you activate it for message processing. The replacement node inherits the exact configuration of the node being replaced, and you are then able to activate it for message processing.

How to Get There

Go to **Network Nodes > Manage**. Click the radio button for the node you want to replace, then click the **Replace** button. See [Figure 3-8](#).

Figure 3-8 Replace a Network Node

The screenshot shows the 'Network Nodes' management interface. The 'Network Nodes' menu is open, showing 'Manage', 'Configure', and 'Activate/Deactivate' options. The 'Manage' option is selected, leading to the 'Replace Node' dialog. The dialog has tabs for 'Network', 'Properties', 'Deploy', 'Monitor', 'Keystores', and 'Admin'. The 'Network' tab is active. The dialog title is 'Replace Node' and it contains the instruction 'Select the node that should replace NodeA'. Below this is a table with the following data:

#	Name	Serial Number	State	Virtual Cluster	Description
1	<input checked="" type="radio"/> aon-node	FOC082313YY	Registered		

Below the table are pagination controls: 'Rows/Page' set to 10, 'Page' set to 1 / 1, and navigation arrows. At the bottom right are 'Activate' and 'Deactivate' buttons.

Actions to Take

You can take one of the following actions:

- Click the radio button for the node that is to serve as the replacement, then click the **Submit** button to save your change.
- Click the **Cancel** button to discard your change and return to the Manage Network Nodes page.

Exporting Nodes

AMC provides the ability to export the configuration data from a node so that it can be imported by another AMC. Enter a unique name for the checkpoint label.



Note

AMCs involved in exporting and importing nodes must be running the same version of software.

How to Get There

Go to **Admin > Node Migration**, then click **Export**. See [Figure 3-9](#).

Figure 3-9 Export a Network Node

The screenshot shows the 'Export Nodes' page in the AMC interface. The breadcrumb trail is 'Admin > Node Migration > Export'. The page title is 'Export Nodes'. Below the title is a table with the following data:

#	Name	Type	Status
1	aon-node	Network Node	

Below the table, there is a 'Rows/Page' dropdown set to '10' and a 'Go' button. To the right, there is a 'Page' dropdown set to '1 / 1' and another 'Go' button. Below these are navigation arrows. A text input field labeled 'Specify a Checkpoint Label:' contains the text 'aon-node-export'. At the bottom right, there are two buttons: 'Export' (which is active) and 'Download File' (which is disabled).

Actions to Take

You can take the following action:

- Select a node, enter a checkpoint label, and click the **Export** button to prepare the file for download.



Note

The export process takes several seconds to complete. On completion, the **Export** button is grayed out, and the **Download File** button is active.

[Figure 3-10](#) shows the Export Node page after the file has been prepared and is ready for download.

Figure 3-10 Download File for Exported Network Node

The screenshot shows the 'Export Nodes' page in the AMC interface after the export process is complete. The breadcrumb trail is 'Admin > Node Migration > Export'. The page title is 'Export Nodes'. Below the title is a table with the following data:

#	Name	Type	Status
1	aon-node	Network Node	Exported

Below the table, there is a 'Rows/Page' dropdown set to '10' and a 'Go' button. To the right, there is a 'Page' dropdown set to '1 / 1' and another 'Go' button. Below these are navigation arrows. At the bottom right, there are two buttons: 'Export' (which is grayed out) and 'Download File' (which is active).

Actions to Take

You can take the following action:

- Click the **Download File** button to begin the download.

Importing Nodes

After a node has been exported, you can import it to another AMC. [Figure 3-11](#) shows the Import Network Node page.

Figure 3-11 Import a Network Node

Actions to Take

You can take the following action:

- Enter the location and name of the configuration file, then click the **Upload** button.
- Click the **Browse** button to navigate to the appropriate file, then click the **Upload** button.

After the file has been uploaded, you can apply the configuration to an existing network node, as shown in [Figure 3-12](#).

Figure 3-12 Apply an Imported Configuration

#	Name	Type	Status
1	aon-node	Network Node	

Actions to Take

You can take the following actions:

- Select source node from the drop-down list.
- Select a destination node.
- Select how to resolve any conflicts.
- Click the **Import** button to apply the configuration to the destination node.

Managing WCCP Servers

A WCCP server is a router that redirects traffic to an AON node. A WCCP Server can also be used for load balancing. By configuring a WCCP server, you provide the AMC with the information that it uses to contact the server and configure it for traffic redirection or load balancing.

This section covers the following topics

- [Creating WCCP Servers, page 3-11](#)

Creating WCCP Servers

How to Get There

Go to Network > **WCCP Servers** > **Define WCCP Servers**, then click the **New** button. [Figure 3-13](#) shows the New WCCP Server page.

Figure 3-13 New WCCP Server

The screenshot displays the 'New WCCP Server' configuration page. The interface includes a navigation menu on the left with options like 'Network Nodes', 'Virtual Clusters', and 'WCCP Servers'. The main content area has tabs for 'Network', 'Properties', 'Deploy', 'Monitor', 'Keystores', and 'Admin'. The breadcrumb path is 'Network > WCCP Servers > Define WCCP Servers > New'. The form fields are as follows:

- * IP address: 10 . 0 . 10 . 13
- User name: admin
- * Password: [masked]
- * Confirm password: [masked]
- * Enable password: [masked]
- * Confirm enable password: [masked]
- * Access method: Secure Shell

Buttons for 'Save' and 'Cancel' are located at the bottom right of the form.

Table 3-3. shows the entries available on the New WCCP Server page.

Table 3-3 New WCCP Server Entries

Entry	Description
IP Address	IP address of the device being configured.
User name	Username required to configure device.
Password	Password required to gain access to device.
Enable password	Enable password required to access privileged EXEC mode.
Access method	If the device is configured for SSH, select secure shell. Otherwise select telnet.

Managing Virtual Clusters

A virtual cluster is a set of identically configured network nodes. After nodes are added to a virtual cluster, you can update the entire clustered group by changing a single set of configuration parameters. Virtual clusters can be configured for the following:

- High availability—Nodes in a cluster can function as a single node. When a node is taken out of service, the other nodes in that virtual cluster assume the messaging processing responsibilities of the missing node.
- Load balancing—Nodes in a cluster can share workload, meaning no single node becomes overloaded with network traffic.

This section covers the following topics:

- [Creating a Virtual Cluster, page 3-12](#)
- [Changing Nodes Within a Virtual Cluster, page 3-14](#)
- [Configuring WCCP for Cluster Management, page 3-14](#)

Creating a Virtual Cluster

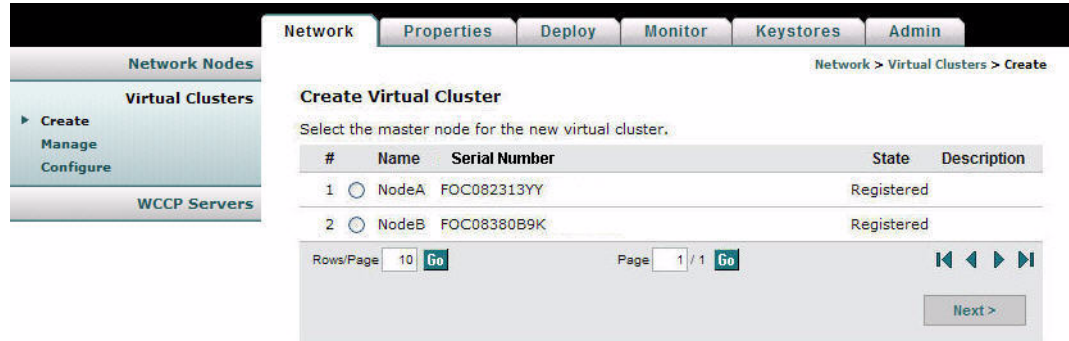
A virtual cluster consists of two or more AON nodes that are configured to share workload and ensure redundancy. The first node you choose for a cluster is called the master node. Other nodes that you add to the cluster will receive duplicate configurations to that of the master node. After the virtual cluster has been created, all nodes are equal, meaning no node is a master node.

Prerequisites

- You need at least two registered nodes. Nodes cannot be unregistered while they are being added to a virtual cluster. The master node can be active, however, the nodes being added must be in the registered state.
- All nodes in a cluster must be running on the same type of hardware. You cannot combine an AON-SM and AON-NM into a virtual cluster.

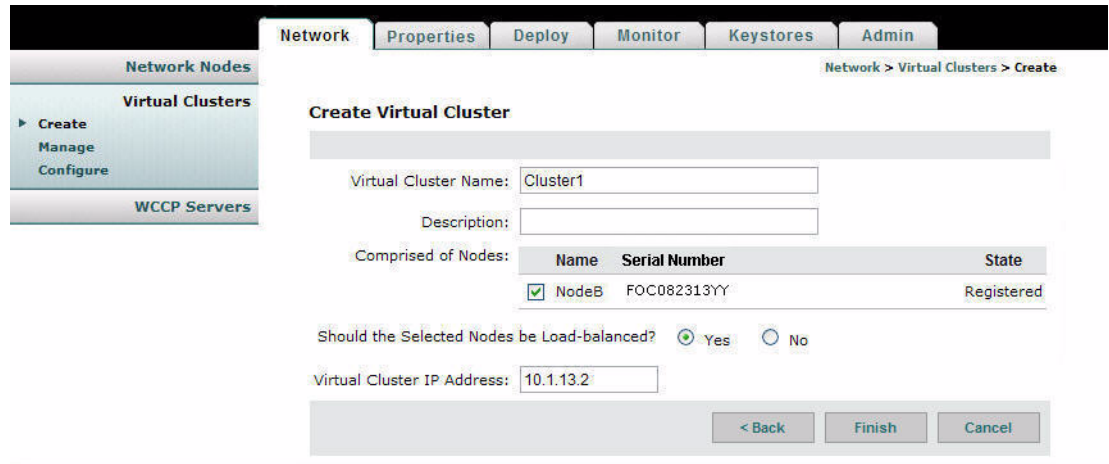
Step 1 Go to **Network > Virtual Clusters > Create**. This loads the Create Virtual Cluster page, as shown in [Figure 3-14](#).

Figure 3-14 Create a Virtual Cluster



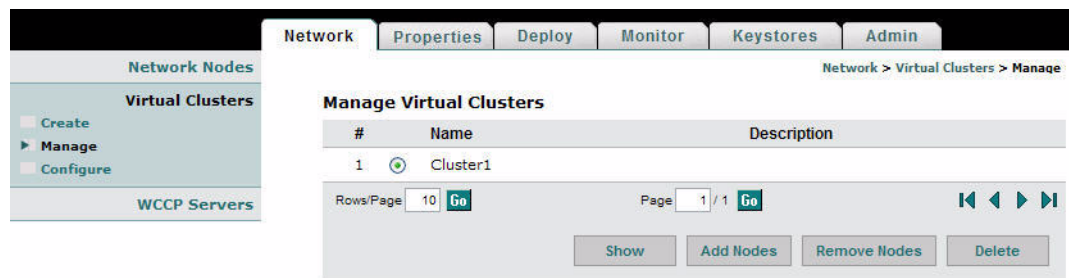
Step 2 Select a master node (the node whose configuration will be duplicated on the other nodes in the cluster) and click the **Next** button. This loads the Create Virtual Cluster page, as shown in Figure 3-15.

Figure 3-15 Create a Virtual Cluster



Step 3 Complete the entries as appropriate for your network and select the other nodes to be added to the cluster.
Step 4 Click the **Finish** button to save your changes, then go to **Network > Virtual Clusters > Manage** to verify that the cluster was configured. Figure 3-16 shows the Manage Virtual Clusters page.

Figure 3-16 Manage Virtual Clusters



- Step 5** Go to **Network Nodes > Activate/Deactivate** to make the nodes in the cluster Active. [Figure 3-16](#) shows the Activate / Deactivate Network Nodes page after the nodes in the virtual cluster have been activated.

Figure 3-17 Activate/Deactivate Network Nodes

The screenshot shows the 'Activate/Deactivate Network Nodes' page. The breadcrumb trail is 'Network > Network Nodes > Activate/Deactivate'. The page title is 'Activate/Deactivate Network Nodes'. Below the title is a table with the following data:

#	Name	Serial Number	State	Virtual Cluster	Description
1	NodeA	FOC082313YY	Active	Cluster1	
2	NodeB	FOC08380B9K	Active	Cluster1	

Below the table, there are controls for 'Rows/Page' (set to 10) and 'Page' (set to 1 / 1). There are also 'Activate' and 'Deactivate' buttons.

Changing Nodes Within a Virtual Cluster

After a virtual cluster is configured, you can perform any of the following actions:

- **Add Nodes**—When you add additional nodes, the new nodes receive identical configuration to that of the existing nodes in the cluster.
- **Remove Nodes**—If you remove a node from a cluster, it is returned to the registered state. Remaining nodes in the cluster continue to operate in the absence of the removed node. The configuration of a node that is removed from a cluster is restored to the factory default when that node is activated outside of the cluster.
- **Delete**—If you delete a cluster, all member nodes are returned to the registered state, and their configurations are restored to the factory default. **Network > Network Nodes**.

Configuring WCCP for Cluster Management

Virtual clusters use WCCP to detect when a member of a cluster goes offline. If this happens, other members of the cluster assume the missing node's message processing workload.

Prerequisites

- You must have a WCCP server available to add to the virtual cluster before beginning this configuration. See the [“Managing WCCP Servers”](#) section on page 3-11 to configure a WCCP server.

- Step 1** Go to **Virtual Clusters > Configure**. Select a cluster and click the **WCCP for Cluster Management** button, then click the **New** button.

Figure 3-18 shows the New WCCP Service Group page.

Figure 3-18 New WCCP Service Group

Table 3-6 shows the entries available on the New WCCP Service Group page.

Table 3-4 New WCCP Service Group Entries

Entry	Description
Service group ID	Unique number for each service group. Range is 51 – 99.
Multicast address	IP address to be used by members of this service group.
Authentication password	Password by members of this service group for authentication.

Step 2 After completing the entries, click the **Add Servers** button. This loads the a page that lists available WCCP servers, as shown in Figure 3-19.

Figure 3-19 Add WCCP Servers

Step 3 Choose one or more servers, then click the **Add** button. The servers are added to the WCCP service group, as shown in Figure 3-20.

Figure 3-20 New WCCP Service Group

- Step 4** Click the **Configure Interfaces** button to specify the interface to be used by the WCCP server. This loads the Server Interfaces page, as shown in [Figure 3-19](#).

Figure 3-21 Server Interfaces

- Step 5** Enter the names, such as Service-Engine1/0, of the interfaces to be used by members of the service group, then click the **Save** button. After you are returned to the New WCCP Service Group page, click the **Save** button to save the entire service group configuration.

Configuring WCCP for Traffic Redirection

Virtual clusters use WCCP to for traffic redirection and load balancing. You can configure nodes to redirect messages based on the IP address or port.

Prerequisite

- If traffic redirection is to be based on source or destination IP addresses, you must configure an ACL/Classifier for the cluster. See the “[Configuring ACL/Classifiers](#)” section on page 3-19 to specify IP address parameters for traffic redirection.

Step 1 Go to **Virtual Clusters > Configure**. Select a cluster and click the **WCCP for Traffic Redirection** button, then click the **New** button.

[Figure 3-22](#) shows the New WCCP Service Group page.

Figure 3-22 New WCCP Service Group

[Table 3-5](#). shows the entries available on the New WCCP Service Group page.

Table 3-5 New WCCP Service Group Entries

Entry	Description
Service group ID	Unique number for each service group. Range is 51 – 99.
Multicast address	IP address to be used by members of this service group.
Authentication password	Password by members of this service group for authentication.
Port map	Comma-delimited string of destination ports to be redirected.
Listener port	Comma-delimited string of ports at which an adapter is listening for traffic.

- Step 2** Complete the entries as appropriate for your network, then click the **Add Servers** button. This loads a page that lists available WCCP servers, as shown in [Figure 3-23](#).

Figure 3-23 Add WCCP Servers

#	IP Address
1	<input type="checkbox"/> 10.0.0.45
2	<input checked="" type="checkbox"/> 10.0.0.46

- Step 3** Choose one or more servers, then click the **Add** button. The servers are added to the WCCP service group, as shown in [Figure 3-24](#).

Figure 3-24 New WCCP Service Group

New WCCP Service Group

* Service Group ID:

* Multicast Address: . . .

Authentication Password:

Confirm Authentication Password:

* Port Map:

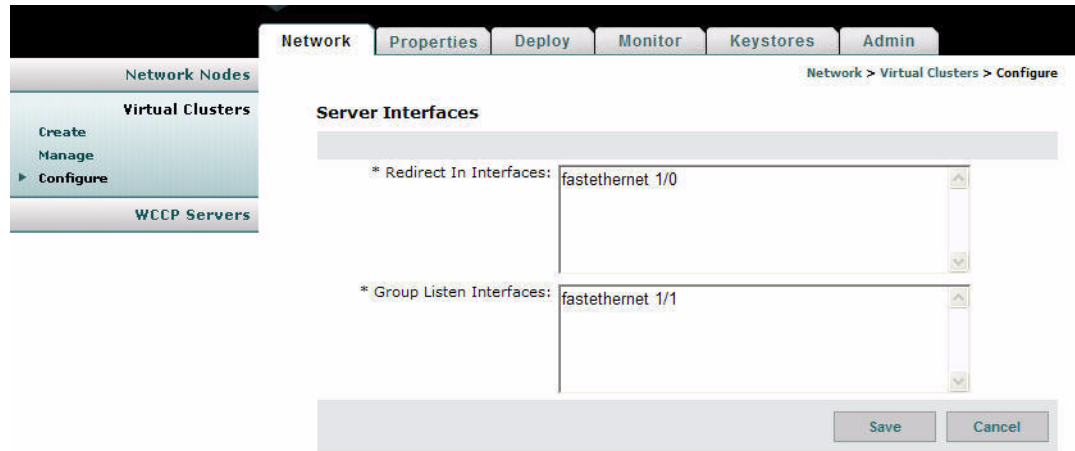
* Listener Port:

Server List

Select	IP Address
<input checked="" type="radio"/>	10.0.0.46

- Step 4** Click the **Configure Interfaces** button to specify the interface to be used by the WCCP server. This loads the Server Interfaces page, as shown in [Figure 3-25](#).

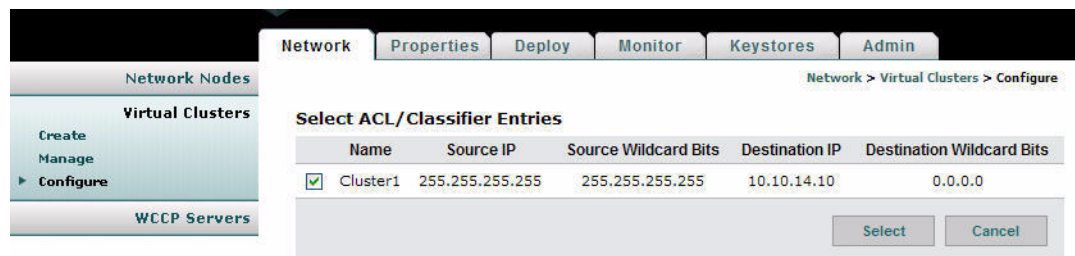
Figure 3-25 Server Interfaces



Step 5 Enter the name of the interfaces to be used by members of the service group, then click the **Save** button.

Step 6 After you are returned to the New WCCP Service Group page, click the **ACL/Classifier** button. On the next page, click the **Add Entries** button to load the page that lists the available ACL/Classifiers, as shown in Figure 3-26.

Figure 3-26 Select ACL/Classifier Entries



Step 7 Choose an ACL/Classifier, then click the **Select** button to associate it with the WCCP service group.

Step 8 Click the **Save** button to save your changes and return to the New Service Group page. From there click the **Save** button to complete the configuration.

Configuring ACL/Classifiers

An ACL/Classifier contains an ordered list of access control entries. Each entry contains a source and destination IP address that are matched against the contents of a packet to determine if messages are to be redirected by WCCP. ACL/Classifiers are also used for message classification.

Step 1 Use one of the following navigation paths:

- For network nodes; **Network > Network Nodes > Configure**. Select a node, then click the **ACL/Classifier** button.
- For virtual clusters: **Network > Virtual Clusters > Configure**. Select a cluster, then click the **ACL/Classifier** button.

This loads the New ACL/Classifier Entry page, as shown in [Figure 3-27](#).

Figure 3-27 New ACL/Classifier

The screenshot shows the 'New ACL/Classifier Entry' configuration page. The navigation menu on the left includes 'Network Nodes', 'Virtual Clusters', and 'WCCP Servers'. The 'Configure' option is selected. The main configuration area contains the following fields:

- * Name: Test
- * Source IP: 10 . 22 . 47 . 10 Port
- * Source Wildcard Bits: 255 . 255 . 255 . 0
- * Destination IP: 10 . 22 . 48 . 99 Port
- * Destination Wildcard Bits: 0 . 0 . 0 . 0

At the bottom right, there are 'Save' and 'Cancel' buttons.

Step 2 Complete the entries as required by your environment, taking the following into consideration:

- A 0 (zero) wildcard bit equates to “only”
- A 255 wildcard bit equates to “any”

For the configuration depicted in [Figure 3-27](#), a match is found for any traffic that has source IP 10.22.47.* and a destination 10.22.48.99.

Step 3 Click the **Save** button to save your changes.

Configuring Recovery

The AMC enables you to control the recovery parameters of network nodes and virtual clusters. Watchdog is a process that runs on an AON node and verifies that the AON application on that node is operating normally. When watchdog detects a failure, it can attempt to restart AON and WCCP.

How to Get There

- Network node: Go to **Network Nodes > Configure**. Select a node and click the **Recovery** button.
- Virtual cluster: Go to **Virtual Clusters > Configure**. Select a node and click the **Recovery** button.

Figure 3-6 shows the Recovery Properties page.

Figure 3-28 Recovery Properties

The screenshot shows the 'Recovery Properties: AONSNODEFORKPLUS' configuration page. The left sidebar contains navigation options: Network Nodes (Manage, Configure, Activate/Deactivate), Virtual Clusters, and WCCP Servers. The main content area has tabs for Network, Properties, Deploy, Monitor, Keystores, and Admin. The breadcrumb trail is 'Network > Network Nodes > Configure > Recovery'. The configuration fields are as follows:

- AON Heartbeat Interval (Seconds): 6
- AON Startup Delay (Seconds): 120
- Watchdog Recovery Action: Restart Aons and WCCP
- WCCP "Here I Am" Interval (Seconds): 10
- Enable Watchdog: true
- Watchdog Failure Detection Interval (Seconds): 30

Buttons for Save, Cancel, and < Back are located at the bottom right.

Table 3-6. shows the entries available on the Recovery page.

Table 3-6 Recovery Entries

Entry	Description
AON Heartbeat Interval	Rate at which the AON process sends heartbeats to the watchdog process.
AON Startup Delay	Number of seconds watchdog waits for the AON process to start up before attempting to restart.
Watchdog Recovery Action	Action to be taken when a watchdog timer expires.
WCCP "Here I Am" Interval	Interval at which WCCP clients send the "Here I Am" message.
Enable Watchdog	Drop-down list to select if watchdog is enabled or disabled.
Watchdog Failure Detection Interval	Time that will elapse before watchdog detects that AON is down.

Deploying to Nodes

When a configuration is changed within the AON network, usually this change requires deployment to AON nodes. Deployment requests consist of two types:

- Global Deployment Request—A change, such as a global policy, that applies to all nodes in the AON network.
- Node Deployment Request—A change, such as a new PEP or message type, that applies only to an individual node.
-

Changes made to the configuration of an AON node must be explicitly deployed to the node. These include those made in AMC those uploaded from the AON Development Studio. Whenever a configuration change is made, it appears in a deployment request (DR). There are two types of deployment requests:

- Global Deployment Request—contains changes, such as a global properties, that apply to all nodes in the AON network.
- Node Deployment Request—contains changes, such as a new PEPs or message types, that apply to an individual node.

Step 1 Go to **Deployment > Manage Staging** to view the deployment requests waiting in the Open and Staged state. [Figure 3-29](#) shows the Manage Staging page.

Figure 3-29 Manage Staging

Deployment Requests

- Manage Staging
- Manage Deployment
- Summary

Network Properties Deploy Monitor Keystores Admin

Deploy > Deployment Requests > Manage Staging

Manage Staging

Open Global Deployment Requests

#	Name	State	Deployment Error
1	<input type="radio"/> Global Deployment Request: Jun 16, 2005 21:31:07	Open	

Rows/Page: 10 Go Page: 1 / 1 Go

Details Stage Unstage Delete

No Node Deployment Requests Available

Step 2 Click the radio button for the deployment request, then click the **Stage** button. This changes the state to Staged, which is the last stop before deployment.

Step 3 Click the Manage Deployment link, which loads the Manage Deployment page, as shown in [Figure 3-30](#).

Figure 3-30 Manage Deployment

Deployment Requests
 Manage Staging
 Manage Deployment
 Summary

Network Properties **Deploy** Monitor Keystores Admin
 Deploy > Deployment Requests > Manage Deployment

Manage Deployment

Staged Global Deployment Requests

#	Name	State	Deployment Error
1	Global Deployment Request: Jun 16, 2005 21: 31:07	Staged	

Rows/Page: 10 Go Page: 1 / 1 Go

Details Unstage Deploy

No Node Deployment Requests Available

Step 4 Click the radio button for the deployment request, then click the **Deploy** button. The AMC deploys the request to the AON node.

Step 5 Click the Summary Link to verify that the request was successfully deployed. [Figure 3-30](#) shows the Deployment Summary page.

Figure 3-31 Deployment Summary

Deployment Requests
 Manage Staging
 Manage Deployment
 Summary

Network Properties **Deploy** Monitor Keystores Admin
 Deploy > Deployment Requests > Summary

Summary

All Global Deployment Requests

#	Name	State	Deployment Error
1	Global Deployment Request: Jun 16, 2005 21: 31:07	Deployed	

Rows/Page: 10 Go Page: 1 / 1 Go

Details

No Node Deployment Requests Available

Viewing Logs

After configuring the Message Log Domain Policy at **Properties > Application > Node > Message Log Domain**, you can retrieve these logs with the page shown in [Figure 3-32](#).

How to Get There

Go to **Monitor > Logs**, then select a node and click the **View Logs** button.

Figure 3-32 View Logs

Viewing Events

After configuring the Monitoring Policy at **Properties > Monitoring**, you can retrieve these events with the page shown in [Figure 3-33](#).

How to Get There

Go to **Monitor > Events**, then select a node and click the **View Events** button. See [Figure 3-33](#)

Figure 3-33 View Events

#	Name	Serial Number	State	Description
1	aon-node	SAD08320738	Active	



Managing AON Properties

Properties control how messages are processed in an Application-Oriented Network. Properties can be applied globally to the entire AON installation, or they can be applied only to individual nodes.



Note

This chapter covers most properties that appear on the Properties tab of the AMC. Properties related to security, authentication, and authorization are in [Chapter 5, “Managing AON Security.”](#)

This chapter includes the following sections:

- [Adapter Listener Domain, page 4-3](#)
- [Adapter Registry, page 4-2](#)
- [Adaptive Load Balancer, page 4-4](#)
- [Databases, page 4-5](#)
- [Reliable Messaging, page 4-6](#)
- [Caching, page 4-7](#)
- [Content Parser, page 4-9](#)
- [Content Validation, page 4-10](#)
- [Configuring Message Delivery Properties, page 4-11](#)
- [Encoding, page 4-15](#)
- [Message Log Domain, page 4-17](#)
- [Next Hop Domain, page 4-20](#)
- [Node Capabilities, page 4-21](#)
- [Transformation, page 4-22](#)
- [Configuring JMS Properties, page 4-23](#)
- [Bladelet Monitoring Property, page 4-29](#)
- [Service Profiles, page 4-30](#)

Adapter Registry

The Adapter Registry page enables you to manage the properties of both built-in and custom adapters. You can activate or deactivate an adapter, change the start-up mode, and change the protocol to be used by the adapter.

You can also configure additional properties and extensions for each adapter.

For more details about adapters, properties, and extensions, see the *AON Programming Guide*.

How to Get There

Go to **Properties > Adapter**.

Figure 4-1 shows the Adapter Registry page.

Figure 4-1 Adapter Registry

The screenshot displays the 'Adapter Registry: Edit Property Set' page. The navigation tabs at the top are Network, Properties, Deploy, Monitor, Keystores, and Admin. The breadcrumb trail is Properties > Adapter > Global > Edit. The left sidebar shows a tree view with 'Adapter' expanded to 'Global Node'. The main content area contains the following configuration fields:

- * Name: aonp
- Class: com.cisco.aons.adapter.stream.aonp.AONPAdapter
- Protocol: aonp
- Description:
- Bundle:
- Type: Embedded
- Is Active:
- Startup Mode:
- Origin: Built-in
- Receiver Handler Class: com.cisco.aons.adapter.stream.aonp.AONPReceiveHandler
- Send Handler Class: com.cisco.aons.adapter.stream.aonp.AONPSendHandler
- Outbox Handler Class:
- Configuration File:
- Attribute Domains:
- Native Libraries:
- Listener Info: aonp
- Protocol Aliases:
- Extension Types:
- Extension Info:

At the bottom right, there are and buttons.

Adapter Listener Domain

Adapter Listener Domain enables you to configure the listening parameters of an adapter. You can specify the port on which the adapter listens, and you can choose either clear or secure communication.

How to Get There

Go to **Properties > Application > Adapter Listener Domain**.

Figure 4-2 shows the Adapter Listener Domain page. For more information about adapters, see the *AON Programming Guide*.

Figure 4-2 Adapter Listener Domain

The screenshot displays the 'Adapter Listener Domain: Edit Property Set' configuration page. The left-hand navigation pane includes the following sections: Adapter, Application (with a sub-item 'Global Node'), Authentication & Authorization, JMS, Monitoring, AON Security, Node Management Security, and Service Profiles. The top navigation bar contains tabs for Network, Properties (which is active), Deploy, Monitor, Keystores, and Admin. The breadcrumb trail at the top right reads 'Properties > Application > Global > Edit'. The main form area contains the following elements:

- A header bar with the title 'Adapter Listener Domain: Edit Property Set'.
- A text input field for 'Name' with the value 'aonp'.
- A text input field for 'Port' with the value '7777'.
- A dropdown menu for 'Mode' with 'clear' selected.
- Two buttons at the bottom right: 'Submit' and 'Cancel'.

Adaptive Load Balancer

Adaptive Load Balancer is used to change the adaptive load balancing algorithm used by AON. [Figure 4-3](#) shows the Adaptive Load Balancer Property page.

Figure 4-3 Adaptive Load Balancer Property

Data to Enter

The Adaptive Load Balancing property page includes the entries described in [Table 4-1](#).

Table 4-1 Entries on Adaptive Load Balancer Property

Entry	Description
Name	Name of your choosing for this property.
Maximum Request Discard	Number of requests to wait before discarding a server's average response time data.
Maximum Response Samples	Number of samples used for determining the most responsive server.
Retry Interval	Time in seconds to wait before retrying a server that was deemed to be inaccessible.

Databases

Database properties enable AON to read and write to databases. For example, PEPs that use the Log bladelet need a database property that tells AON where to write log data. This is a global property. [Figure 4-4](#) shows the Database Property page.

Figure 4-4 Database Property

Data to Enter

The Database Property page includes the entries described in [Table 4-2](#).

Table 4-2 Entries on Database Property

Entry	Description
Name	Name of your choosing for this database property
User ID	User ID required to log on to the database. The user must have permission to create, read, write, update, and query the database.
Password	Password required to log on to the database
JDBC URL	Location of database. This entry must use one of the following formats:\n\nOracle: jdbc:oracle:thin: <i>@ip_address:port:database_name</i> \n\nSybase: jdbc:sybase:Tds: <i>ip_address:port/database_name</i>
Database name	One of the following: <ul style="list-style-type: none"> • Oracle • Sybase

Actions to Take

After completing the entries, you can take one of the following actions:

- Click **Submit** to save your changes.
- Click **Cancel** to discard your changes and return to the previous screen.

Reliable Messaging

The Reliable Messaging property is used to configure the parameters that control reliable messaging. Reliable messaging enables an AON device to ensure that messages are delivered to their destination regardless of how many hops are involved. Reliable Messaging is a Global property. [Figure 4-5](#) shows the Reliable Messaging Property page.

Figure 4-5 Reliable Messaging Property

The screenshot shows the 'Reliable Messaging: Edit Property Set' configuration page. The left sidebar contains a navigation menu with the following items: Adapter, Application, Global Node, Authentication & Authorization, JMS, Monitoring, AON Security, Node Management Security, and Service Profiles. The main content area has a breadcrumb trail: Properties > Application > Global > Edit. The title is 'Reliable Messaging: Edit Property Set'. Below the title, there is a text input field with the value '* Name: default'. There are three numeric input fields: 'Resend Check Period' with the value 10000, 'Time To Abort' with the value 120000, and 'Time To Resend' with the value 20000. At the bottom right, there are 'Submit' and 'Cancel' buttons.

Data to Enter

The Reliable Messaging Property page includes the entries described in [Table 4-3](#).

Table 4-3 Entries on Reliable Messaging Property

Entry	Description
Property Name	Name of your choosing for this property.
Resend Check Period	Number of milliseconds to wait before checking whether the end point received the message.
Time To Abort	Number of milliseconds to wait before aborting sending of message.
Time To Resend	Number of milliseconds to wait before resending a message.

Caching

AON includes a built-in cache engine that can be used as a proxy cache or reverse proxy cache depending on where and in which administrative domain the cache is placed. Use the Caching Property to configure how the AON cache engine operates. This is a device-level property, and it is used in conjunction with PEPs that include the CacheData and RetrieveCache bladelets. [Figure 4-6](#) shows the Caching Property page.

Figure 4-6 Caching Property

The screenshot displays the 'Caching: Edit Property Set' configuration page. The left sidebar shows a navigation tree with 'Node' selected under 'Application'. The main content area contains the following settings:

- Name:** caching
- Override no-cache Response Directive:** false
- Override no-store Response Directive:** false
- Override private Response Directive:** false
- Override no-cache Request Directive:** false
- Override no-store Request Directive:** false
- Override Pragma:no-cache Request Directive:** false
- Response Cache Default TTL:** 86400
- Variable Cache Default TTL:** 86400
- Max Objects Variable Cache:** 1000
- Max Objects Security Cache:** 100
- Response Cache Replacement Algorithm:** LRU
- Variable Cache Replacement Algorithm:** LRU
- Security Cache Replacement Algorithm:** LRU
- Loadbalancing Cache Replacement Algorithm:** LRU
- Cache Server:** localhost
- Cache Server Port:** 60606
- Connection Timeout:** 5
- Queue Size:** 1000
- Polling Interval:** 60
- Pending Message Queue Timeout:** 20
- Timed-out Message Count:** 500

At the bottom right, there are 'Submit' and 'Cancel' buttons.

Data to Enter

The Caching Property page includes the entries described in [Table 4-2](#).

Table 4-4 Entries on Caching Property

Entry	Description
Override no-cache Response Directive	If this value is set to true , the HTTP “no-cache” response directive is ignored.
Override no-store Response Directive	If this value is set to true , the HTTP “no-store” response directive is ignored.
Override private Response Directive	If this value is set to true , the HTTP “private” response directive is ignored.
Override no-cache Request Directive	If this value is set to true , the HTTP “no-cache” request directive is ignored.
Override no-store Request Directive	If this value is set to true , the HTTP “no-store” request directive is ignored.
Override Pragma:no-cache Request Directive	If this value is set to true , the HTTP “Pragma:no-cache” request directive is ignored.
Response Cache Default TTL	Default time to live (TTL) to be used for response caching.
Variable Cache Default TTL	Default TTL to be used for variable caching.
Max Objects Variable Cache	Determines the number of objects to store in the variable cache before replacement algorithms are activated.
Max Objects Security Cache	Maximum number of objects to be cached in the security cache before replacement algorithms are activated.
Response cache replacement Algorithm	This value must be set to LRU . This is the replacement algorithm to be used for response caching.
Variable Cache Replacement Algorithm	This value must be set to LRU . This is the replacement algorithm to be used for variable caching.
Security Cache Replacement Algorithm	Must be set to LRU . This is the replacement algorithm to be used for security caching.
Cache Server	Host name or IP address of the caching server. Must be set to localhost.
Cache Server Port	Port on which the caching server listens. Must be set to 60606.
Connection Timeout	Determines how long a request will wait for a response
Queue Size	The pending message queue contains references to messages that are awaiting response from the server. If a message remain in this queue beyond the timeout value, the server is assumed to be down. Typically set for 20–30 seconds.
Polling Interval	Determines the number of seconds the client will wait before checking if a failed server has returned to service.
Pending Message Queue Timeout	Determines the size of the client’s sending queue.
Timed-out Message Count	Determines how many failed messages are required for a server to be considered down.

Content Parser

The content parser property specifies a Java class that implements a content parser to use for reading an input content and converting it to an equivalent XML content. This property can also specify a Java class to use to perform the transformation instead of using XSLT-based transformation. [Figure 4-7](#) shows the Content Parser Property page.

Figure 4-7 Content Parser Property

The screenshot shows a web application interface for configuring a Content Parser property. The top navigation bar includes tabs for Network, Properties, Deploy, Monitor, Keystores, and Admin. The left sidebar lists various system components, with 'Node' selected under the 'Application' category. The main content area is titled 'Content Parser: Add New Property Set' and contains the following fields:

- * Name:
- Transformation Factory:
- Parser Class Name:
- Name of Package:

At the bottom right of the form are 'Submit' and 'Cancel' buttons.

Data to Enter

The Content Parser Property page includes the entries described in [Table 4-5](#).

Table 4-5 Entries on Content Parser Property

Entry	Description
Name	Name of the Content Parser property.
Transformation Factory	This parameter specifies the class name that implements a custom transformer.
Parser Class Name	This parameter specifies the name of Java class that is used to parse the input message content and convert it to equivalent XML content.
Name of Package	Specifies the name of the transform package.

Content Validation

A Content Validation application property imposes an external schema on an XML message that contains no predefined grammar declarations. This property is used when input XML does not contain any grammar declaration (XSD or DTD) but is expected to conform to a receiver point schema. It is also used when Input XML is transformed within AON and is expected to conform to a target schema. [Figure 4-7](#) shows the Content Validation Property page.

Figure 4-8 Content Validation Property

The screenshot displays the 'Content Validation: Add New Property Set' form. The left sidebar contains a tree view with 'Application' selected. The main area has a breadcrumb trail: 'Properties > Application > Node > Edit Properties > New'. The form fields are:

- * Name: [Text Input]
- Target Schema Name: [Text Input]
- Target Namespace: [Text Input]

 At the bottom right of the form are 'Submit' and 'Cancel' buttons.

Data to Enter

The Content Validation property page includes the entries described in [Table 4-6](#).

Table 4-6 Entries on Content Validation Property

Entry	Description
Name	Name of the Content Validation property.
Target Schema Name	Target schema to be imposed on XML messages running a particular PEP.
Target Namespace	Namespace for the target schema named above.

Configuring Message Delivery Properties

Message delivery properties define the delivery characteristics associated with a message type. All message types have a default delivery property, which is specified when you create the message type in the ADS. After a message is classified, the delivery properties of that message are dictated by the delivery property associated with that message type. Message delivery properties must be configured in the following order:

1. [Configuring Delivery Connection.](#)
2. [Configuring Delivery Notification.](#)
3. [Configuring Delivery Semantics.](#)
4. [Binding Message Delivery Properties to a Message Type.](#)

After you configure delivery properties, synchronize the ADS with the AMC to begin using the new delivery properties with message types.

Configuring Delivery Connection

The Delivery Connection property specifies how long a message type should wait for a timeout.

How to Get There

- Go to **Properties > Application > Node**. Select a node, then click the **Edit Properties** button.

Figure 4-9 shows the Delivery Connection Property page.

Figure 4-9 Delivery Connection Property

Data to Enter

The Delivery Notification property page includes the entries described in [Table 4-7](#).

Table 4-7 Delivery Connection Property Entries

Entry	Description
Name	Name of the Delivery Connection property.
Request Timeout	Length of time to wait for a response from the endpoint for a timeout, measured in milliseconds.

Configuring Delivery Notification

The Delivery Notification property defines how to handle delivery failure notification.



Note

You must configure [Configuring Delivery Connection](#) before configuring this property.

How to Get There

- Go to **Properties > Application > Node**. Select a node, then click the **Edit Properties** button.

[Figure 4-10](#) shows the Delivery Notification property.

Figure 4-10 Delivery Notification Property

Data to Enter

The Content Validation property page includes the entries described in [Table 4-8](#).

Table 4-8 Delivery Notification Property Entries

Entry	Description
Name	Name of the Delivery Notification property.
Delivery Notification Type	Log is the only supported option.

Configuring Delivery Semantics

The Delivery Semantics property specifies delivery properties for a message type. Use this property, in conjunction with the Delivery Connection and Delivery Notification properties, to configure the reliable and ordered delivery of messages.



Note

You must configure [Configuring Delivery Connection](#) and [Configuring Delivery Notification](#) before configuring this property.

How to Get There

- Go to **Properties > Application > Node**. Select a node, then click the **Edit Properties** button.

[Figure 4-11](#) shows the Delivery Semantics property.

Figure 4-11 Delivery Semantics Property

Data to Enter

The Delivery Semantics page includes the entries described in [Table 4-9](#).

Table 4-9 Delivery Semantics Property Entries

Entry	Description
Name	Name of your choosing for this property.
Is reliable delivery	Choose true or false to enable reliable delivery.
Is ordered delivery	Choose true or false to enable ordered delivery. Ordered message delivery is guaranteed to a single destination, not multiple destinations.
Time to live	How long either request message or response message can stay in the system Specified in milliseconds.
Expire treatment	Specify what is to happen if TTL expires. reliable messaging global ttl. time to abort
Retry timeout	Specified in milliseconds. takes precedence over global timeout
Delivery Notification	Select an available Delivery Notification Property.

Table 4-9 Delivery Semantics Property Entries (continued)

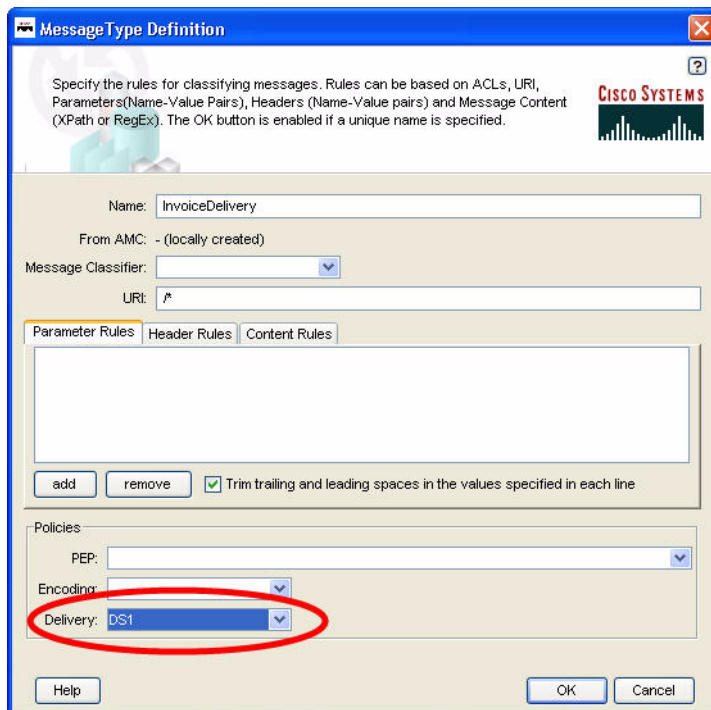
Entry	Description
Connection Property	Select an available Delivery Connection Property.

Actions to Take

Use the **Edit List** button to choose a delivery notification and connection property.

Binding Message Delivery Properties to a Message Type

After you configure message delivery properties in the AMC, the property is available to ADS users when they configure message types. [Figure 4-12](#) shows the ADS Message Type Properties window with the Delivery Properties drop-down list highlighted.

Figure 4-12 MDS Drop-Down List

Encoding

The Encoding property enables you to configure AON nodes to compress outgoing traffic. [Figure 4-13](#) shows the Encoding property page. After you configure an encoding property, that property is available to ADS users. When message types are configured, each message type can be associated with an encoding property.

Figure 4-13 Encoding Property

The screenshot shows a web interface for configuring encoding properties. On the left is a navigation tree with 'Application' selected and 'Node' expanded. The main area is titled 'Encoding: Edit Property Set' and contains the following elements:

- A breadcrumb trail: Properties > Application > Node > Edit Properties > Edit
- A label: * Name: EncodingPolicy
- A 'Request Encoding' dropdown menu with 'no gzip' selected.
- A 'Response Encoding' dropdown menu with 'gzip' selected.
- 'Submit' and 'Cancel' buttons at the bottom right.

Data to Enter

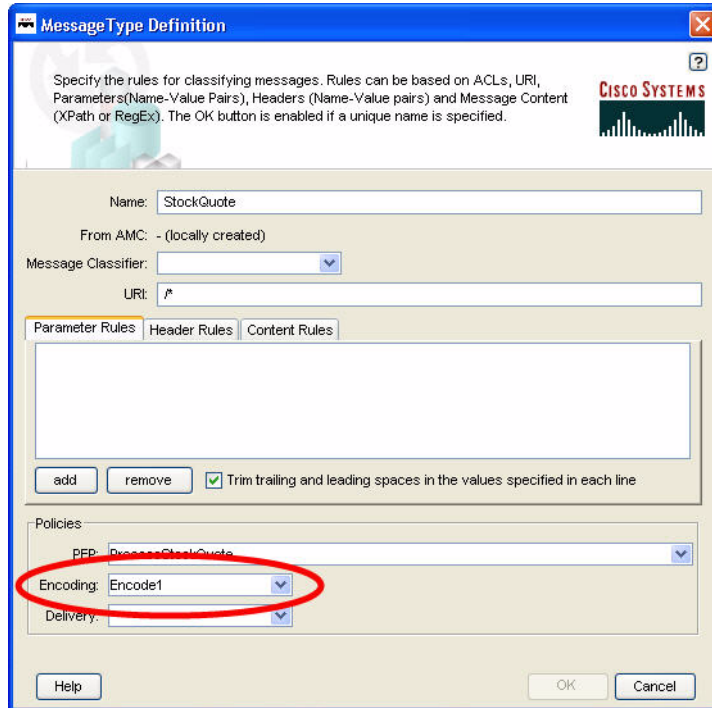
The Encoding property page includes the entries described in [Table 4-10](#).

Table 4-10 Encoding Property Entries

Entry	Description
Name	Name of your choosing for this property.
Request Encoding	Choose the encoding for the request portion of the PEP.
Response Encoding	Choose the encoding for the response portion of the PEP.

After you configure an Encoding profile, it is available to ADS users when they configure a message type. See [Figure 4-14](#).

Figure 4-14 Binding an Encoding Property to a Message Type



Message Log Domain

AON nodes are able to capture application log messages and store them in a database for later retrieval. This functionality requires you to complete the following tasks:

1. **Create a Message Log Database**—This is the Oracle or Sybase database in which log messages are to be stored.
 - **Configure Message Log Domain Property**—This defines within AMC the database configuration details to be used to store log messages.

Upon completion of these steps, ADS users will be able to use the Log Bladelet to store messages in the database.

Create a Message Log Database

If you enable AON message logging, you can configure an external Oracle or Sybase database to store log messages. An existing Oracle database can be used for message logging. However, a Sybase database must have a specific configuration to be compatible with AON. For this reason, we recommend that you create a new database.

-
- Step 1** Create a database and a user (for logins). Grant the user database privileges to create, query, delete, update, and insert.

Use one of the following for the Message Log Database:

- Oracle 9i (9.2)
 - You can create a separate Oracle 9i database for AON Message Logging.
- Sybase 12.5.1
 - You should create a separate Sybase 12.5.1 Adaptive Server (database) for AON message logging. The requirements for this external database are summarized below.
 - Page size $\geq 8K$
 - Procedure cache size - 100000
 - Max memory 131072 (in 2k units, i.e. $131072 * 2k = 256MB$)



Note See Oracle or Sybase documentation for specific database configuration instructions.

- Step 2** Run the appropriate script to create the Message Log schema in your database. See [Appendix A, “Message Log Schemas”](#) for Sybase and Oracle scripts.
-

Configure Message Log Domain Property

After a database as been configured, you can configure Message Log Domain Property. This is a device level property.

How to Get There

- Go to **Properties > Application > Node**. Select a node, then click the **Edit Properties** button.

Figure 4-15 shows the Message Log Domain Property page.

Figure 4-15 Message Log Domain Property

The screenshot displays the 'Message Log Domain: Edit Property Set' configuration page. The left sidebar contains a navigation menu with the following items: Adapter, Application, Authentication & Authorization, JMS, Monitoring, AON Security, Node Management Security, and Service Profiles. The main content area is titled 'Message Log Domain: Edit Property Set' and includes the following fields and values:

- * Name: mklog
- Enabled: true
- Sub-protocol: oracle.thin
- User ID: beta
- Password: ●●●●
- Database Alias: @jdgou-u5:1521:aonsmlog
- Driver: oracle.jdbc.OracleDriver
- Max Queue Size: 10000

At the bottom right of the form, there are 'Submit' and 'Cancel' buttons.

Data to Enter

The Message Log Domain Property page includes the entries described in Table 4-11.

Table 4-11 Message Log Domain Property Entries

Entry	Description
Name	Name of your choosing for this property.
Enabled	Select true to enable, false to disable.
Sub-protocol	oracle.thin for Oracle. sybase.Tds for Sybase.
User ID	User ID required to log on to the database. The user must have permission to create, read, write, update, and query the database.
Password	The password to gain access to the database.

Table 4-11 Message Log Domain Property Entries (continued)

Entry	Description
Database alias	<p>Alias pointing to the database. This value depends on the configuration of the database. The format for this entry is <i><IP address> : <port> : <name of database></i></p> <p>The following are examples:</p> <ul style="list-style-type: none"> • Oracle—@10.1.1.1:1521:aonmlog • Sybase—10.1.1.2:5000/aonmlog <p>The last part in the alias is the name of the database instance. The message log schema should be provided by your database administrator.</p>
Driver	<p>The JDBC driver name. AON supports the following two drivers:</p> <ul style="list-style-type: none"> • Oracle—oracle.jdbc.OracleDriver • Sybase—com.sybase.jdbc2.jdbc.SybDriver
Max Queue Size	Maximum size of the Message Log queue.

Next Hop Domain

Next Hop Domain Property enables a device to forward all traffic using a specified protocol to a designated AON node. Next Hop Domain is a device-level property.



Note

In a two-node scenario, configure this property on the client proxy with the configuration details necessary to route messages to the server proxy.

How to Get There

- Go to **Properties > Application > Node**. Select a node, then click the Edit Properties button.

Figure 4-16 shows the Next Hop Domain Property page.

Figure 4-16 Next Hop Domain Property Entries

Data to Enter

The Next Hop Domain Property page includes the entries described in Table 4-12.

Table 4-12 Entries on Next Hop Domain Property

Entry	Description
Name	Use the hostname or IP address of the destination and the port on which the host is listening for messages. <i>ip_address:port</i> or <i>hostname:port</i>
Address	IP address or hostname for next hop device.
Port	Port on which device is listening for next hop traffic.
Protocol	One of the following protocols: <ul style="list-style-type: none"> http aonp
Mode	Choose secure for encrypted or clear for unencrypted.

Node Capabilities

The Node Capabilities property enables you to configure reliable messaging on a node. Node Capabilities is a device level property.



Note

If message delivery persistence is to be stored in a database, you must configure two databases before you configure this property. See the “[Databases](#)” section on page 4-5 for information on configuring a database.

How to Get There

- Go to **Properties > Application > Node**. Select a node, then click the Edit Properties button.

Figure 4-17 shows the Node Capabilities Property page.

Figure 4-17 Node Capabilities Property

Data to Enter

The Node Capabilities property page includes the entries described in [Table 4-13](#).

Table 4-13 Node Capabilities Property Entries

Entry	Description
Name	Name of your choosing for this property.
Message Delivery Semantics Persistence	Choose off to disable Message Delivery Semantics Persistence. Choose database to enable
WCCP Service Group	Enter the WCCP service group for the virtual cluster configured for multiblade ordered message delivery.
Wait Timeout	Specified in milliseconds.
Message Store Database	Click the Edit List button to choose an available Database. See the “ Databases ” section on page 4-5 to configure a database.
Multi-Blade Database	Click the Edit List button to choose an available Database

Transformation

This property configures AON to perform XSL transformation (XSLT). The Transformation property determines the document style sheet, target content type, and transformation package. This property can be configured globally or for individual nodes.

How to Get There

- Go to **Properties > Application > Node**. Select a node, then click the Edit Properties button.

Figure 4-18 shows the Transformation Property page.

Figure 4-18 Transformation Property

The screenshot shows the 'Transformation: Add New Property Set' form. The left sidebar has a tree view with 'Node' selected under 'Application'. The main area contains the following fields:

- * Name:
- Name of XSLT Stylesheet:
- Target Content Type:
- Transformation Factory:
- Name of Package:

Buttons for 'Submit' and 'Cancel' are located at the bottom right of the form.

Data to Enter

The Transformation page includes the entries described in Table 4-14.

Table 4-14 Transformation Property Entries

Entry	Description
Name	Name of the Transformation property.
Name of XSLT Stylesheet	Specifies the name of the transform file to use. The file must be present in the Transform Bundle specified by the parameters below.
Target Content Type	This is used to set the content type of the target content when the input content is stream content and its type is not known.
Transformation Factory	Choose an XSLT transformer to be used.
Name of Bundle	Specifies the name of the transform package.

Configuring JMS Properties

Use JMS properties to configure the way AON nodes handle JMS messages. You must configure JMS properties in the following order:

1. [JMS Destination Property, page 4-23](#)
2. [JMS Source Property, page 4-24](#)
3. [JMS Reply To, page 4-25](#)
4. [JMS Connections Property, page 4-26](#)
5. [JMS Naming Property, page 4-27](#)

JMS Destination Property

The JMS Destination Property enables you to specify a new destination for JMS messages.

How to Get There

- Go to **Properties > JMS > Node**. Select a node, then click the **Edit Properties** button.

[Figure 4-19](#) shows the JMS Destination Property page.

Figure 4-19 JMS Destination Property

The screenshot shows a web-based configuration interface. At the top, there are tabs for 'Network', 'Properties', 'Deploy', 'Monitor', 'Keystores', and 'Admin'. Below these is a breadcrumb trail: 'Properties > JMS > Node > Edit Properties > Edit'. On the left, a vertical menu lists various configuration categories: 'Adapter', 'Application', 'Authentication & Authorization', 'JMS', 'Monitoring', 'AON Security', 'Node Management Security', and 'Service Profiles'. The 'JMS' category is expanded to show 'Node'. The main area is titled 'Destinations: Edit Property Set'. It features a text input field for '* Name: JMSDestination1'. Below this are four fields: 'Destination Name' (text input), 'Delivery Mode' (dropdown menu with 'PERSISTENT' selected), 'Time To Live' (text input), and 'Priority' (text input). At the bottom right, there are 'Submit' and 'Cancel' buttons.

Data to Enter

The JMS Destination Configuration page includes the entries described in [Table 4-15](#).

Table 4-15 JMS Destination Configuration Entries

Entry	Description
Name	Name of your choosing for this configuration.
Destination name	Name of the destination JMS broker.
Delivery Mode	Choose PERSISTENT or NON_PERSISTENT as appropriate.
Time To Live	Use the value specified by the JMS broker. This entry is required.
Priority	Use the value specified by the JMS broker. This entry is required.

JMS Source Property

The JMS Source Property Page enables you to specify a new source for JMS messages. It requires you to specify a JMS Destination, which you should have configured in the previous section.

How to Get There

- Go to **Properties > JMS > Node**. Select a node, then click the Edit Properties button.

Figure 4-20 shows the JMS Source Property page.

Figure 4-20 JMS Source Property

The screenshot displays the 'Sources: Edit Property Set' configuration page. The left sidebar shows a tree view with 'Node' selected under the 'JMS' category. The main content area includes the following fields and controls:

- Name:** JMSSource1
- Source Name:** [Text input field]
- Batch Size:** [Text input field]
- Ordering:** Required (dropdown menu)
- Message Selector:** [Text input field]
- Reliable Delivery:** Required (dropdown menu)
- Delivery Failure Policy:** Rollback & stop this source (dropdown menu)
- Destination:** JMSDestination1
- Buttons:** Edit List, Submit, Cancel

Data to Enter

The JMS Source Configuration page includes the entries described in Table 4-16.

Table 4-16 JMS Source Configuration Entries

Entry	Description
Name	Name of your choosing for this configuration.
Source Name	Name of the source sending JMS messages.
Batch Size	Default is zero.
Ordering	Choose Required if ordered message delivery is required.
Message Selector	Enter a header entry or property reference that is to be used to identify messages of interest.
Reliable Delivery	Specify if reliable delivery is required.
Delivery Failure Property	Select the appropriate action to take if messages fail to be delivered.
Destination	Click the Edit List button to choose an available JMS Destination property.

JMS Reply To

The JMS ReplyTo property enables you to specify a new reply queue to be used by JMS clients.

How to Get There

- Go to **Properties > JMS > Node**. Select a node, then click the Edit Properties button.

Figure 4-21 shows the JMS Reply To Property page.

Figure 4-21 JMS Reply To Property

Data to Enter

The JMS Reply To Property page includes the entries described in Table 4-17.

Table 4-17 JMS Reply To Property Entries

Entry	Description
Name	Name of your choosing for this property.
ReplyTo Name	Name of the ReplyTo.
Definition Type	Choose Template or Static.
Reliable Delivery	Specify if reliable delivery is required.
Ordering	Choose Required if ordered message delivery is required.
Batch Size	Size of batch count.
Number of Queues	Enter number of queues.

JMS Connections Property

How to Get There

- Go to **Properties > JMS > Node**. Select a node, then click the Edit Properties button.

Figure 4-21 shows the JMS Connection Property page.

Figure 4-22 JMS Connection Property

The screenshot displays the 'Connections: Edit Property Set' page. On the left is a navigation tree with 'Node' selected under the 'JMS' category. The main area contains the following fields and controls:

- Name:** * Name: JMSConnections1
- Source Name:** [Text input field]
- Type:** Topic (dropdown menu)
- User:** [Text input field]
- Password:** [Text input field]
- Vendor Name:** MQ (dropdown menu)
- Dead Letter Destination:** [Text input field]
- Transaction Queue:** [Text input field]
- Reply To List:** JMSReplyTo1 (with an 'Edit List' button)
- Destination List:** JMSDestination1 (with an 'Edit List' button)
- Source List:** JMSSource1 (with an 'Edit List' button)
- Destination Batch Size:** [Text input field]
- Destination Batch Interval:** [Text input field]
- Buttons:** Submit and Cancel

Data to Enter

The JMS Connection Property page includes the entries described in Table 4-18.

Table 4-18 JMS Connection Configuration Entries

Entry	Description
NAME	Name of your choosing for this connection configuration.
Source Name	Name of the JMS broker.
Type	Choose Topic or queue.
User	Enter the user name if one is required by the JMS broker.
Password	Enter the password if one is required by the JMS broker.
Vendor Name	Choose MQ or Tibco from the drop-down list.
Dead Letter Destination	Specify the queue where AON can store undeliverable messages.
Transaction queue	Specify the transaction queue.
Reply To List	Click the Edit List button to make a selection.
Destination List	Click the Edit List button to make a selection.

Table 4-18 JMS Connection Configuration Entries (continued)

Entry	Description
Source List	Click the Edit List button to make a selection.
Destination Batch Size	Size of the batch at the destination broker.
Destination Batch Interval	Specified in milliseconds.

JMS Naming Property

Figure 4-21 shows the JMS Naming Property Page.



Note

Before configuring this property, go to **Admin > Extensions > JMS Resources** to upload a JMS resource file. See the *AON Programming Guide* for information on creating a JMS resource file.

Figure 4-23 JMS Naming Property

Data to Enter

The JMS Naming Property page includes the entries described in [Table 4-19](#).

Table 4-19 Entries on JMS Naming Property

Entry	Description
Name	Name of your choosing for this property.
Naming Service	Choose remote or local.
JMS Resource File	Click the Edit List button so select the file you have uploaded to AMC.
Initial Context Factory	Constant that holds the name of the environment property for specifying the initial context factory to use.
Provider URL	Constant that holds the name of the environment property for specifying configuration information for the service provider to use.
Security Protocol	Constant that holds the name of the environment property for specifying the security protocol to use.
Security Authentication	Constant that holds the name of the environment property for specifying the security level to use
Authoritative	Constant that holds the name of the environment property for specifying the authoritativeness of the service requested.
URL Package Prefixes	Constant that holds the name of the environment property for specifying the list of package prefixes to use when loading in URL context factories.
State Factories	Constant that holds the name of the environment property for specifying the list of state factories to use.
Language	Constant that holds the name of the environment property for specifying the preferred language to use with the service.
Batch Size	Constant that holds the name of the environment property for specifying the batch size to use when returning data via the service's protocol.
Security Principal	Constant that holds the name of the environment property for specifying the identity of the principal for authenticating the caller to the service.
Object Factories	Constant that holds the name of the environment property for specifying the list of object factories to use.
Referral	Constant that holds the name of the environment property for specifying how referrals encountered by the service provider are to be processed.
Security Credentials	Constant that holds the name of the environment property for specifying the credentials of the principal for authenticating the caller to the service.
DNS URL	Constant that holds the name of the environment property for specifying the DNS host and domain names to use for the JNDI URL context.
Connection List	Click the Edit List button to choose a JMS Connections property.

Bladelet Monitoring Property

The Bladelet Monitoring Property configures which events are stored for retrieval using the screen at **Monitor > View Events**. You can configure this property globally, or you can apply it to individual nodes.

How to Get There

Go to **Properties > Monitoring**.

Figure 4-24 shows the Monitoring Property page.

Figure 4-24 Bladelet Monitoring Property

The screenshot displays the 'Bladelet Monitoring: Edit Property Set' configuration page. The left-hand navigation pane includes sections for Adapter, Application, Authentication & Authorization, JMS, Monitoring (selected), AON Security, Node Management Security, and Service Profiles. The 'Monitoring' section is further divided into 'Global' and 'Node'. The main configuration area shows the following settings:

- * Name: Default
- * Authenticate Events: true
- * Authorize Events: true
- * Sign Events: true
- * VerifySignature Events: true
- * Encrypt Events: true
- * Decrypt Events: true
- * Identify Events: true
- * VerifyIdentity Events: true
- * Transform Events: true
- * Find Events: true
- * Content Validation Events: true
- * MIME Events: true

At the bottom of the form are two buttons: 'Submit' and 'Cancel'.

To configure the Monitoring Property, change events that you want monitored to True, then click the **Submit** button.

Service Profiles

Service Profiles are used in conjunction with the development of custom bladelets and custom adapters. Available services include the following:

- Compression
- Content Lookup
- Content Validation
- Encryption
- Signature

Developers can create profiles, which are sets of attributes that describe how the services listed above are implemented in custom bladelets or adapters. Profiles contain multiple named contexts for a service, and these profiles must be created in AMC in order for developers to access these contexts by name.

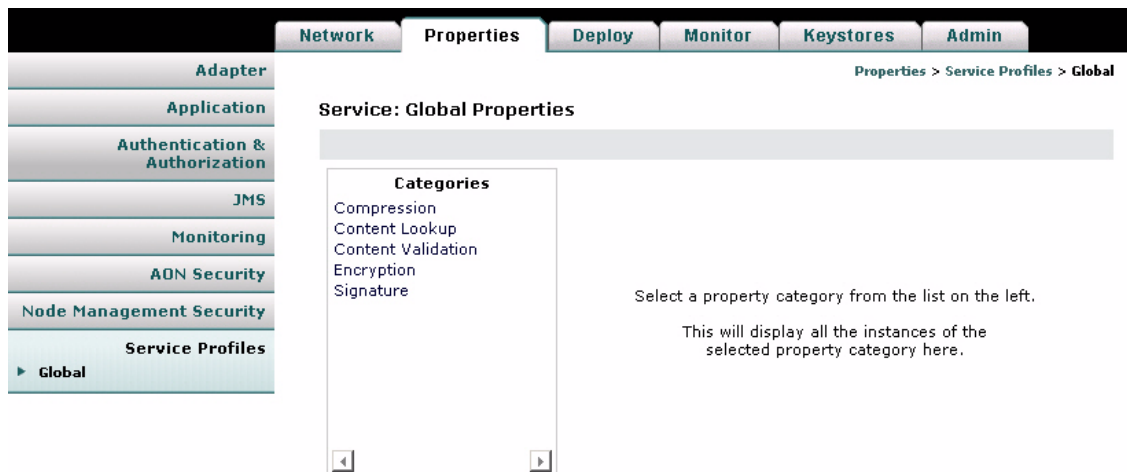
For more details about custom bladelets, custom adapters, and external services, see the *AON Programming Guide*.

How to Get There

Go to **Properties > Service Profiles**.

Figure 4-25 shows the Service Profile page.

Figure 4-25 Service Profiles





Managing AON Security

This chapter describes AON functions relating to security, authentication, and authorization. It includes the following topics.

- [Managing AON Users, page 5-1](#)
- [Managing Keystores, page 5-10](#)
- [Configuring Security Properties, page 5-20](#)
- [Configuring Authentication and Authorization Properties, page 5-24](#)

Managing AON Users

AMC users fall into one of the following categories:

- Local users—these users are created and managed within AMC.
- External users—these users are created on and managed by an external LDAP server.



Note

A new installation of AMC includes five local users with **aonsadmin** as their default password. To ensure that only authorized personnel have access to the AMC, change the default passwords or delete unneeded users.

Managing Local Users

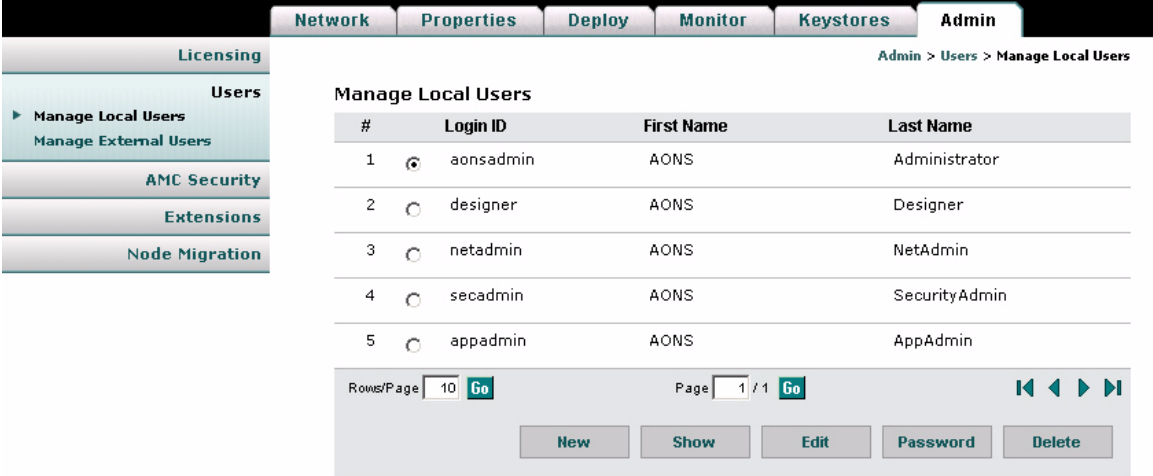
Local users are created and managed by the AMC. You can use the Manage Local Users page to perform the following tasks:

- Add and delete users
- Display information about users
- Edit a user's information, including privileges.
- Change a user's password

How to Get There

Go to Admin > Users > Manage Local Users. [Figure 5-1](#) shows this page

Figure 5-1 Manage AMC Local Users



Actions to Take

Click one of the following buttons:

- **New**—creates a new users. See [Creating New Users, page 5-3](#)
- **Show**—displays information on the selected user. See [Displaying Information on Users, page 5-4](#)
- **Edit**—changes information about the selected user. See [Editing Users, page 5-5](#)
- **Password**—changes the password of the selected user.
- **Delete**—removes the selected user from the system.

Creating New Users

AMC enables you to create new local users.

How to Get There

Go to **Admin > Users > Manage Local Users**, then click the New button. [Figure 5-2](#) shows the New User page.

Figure 5-2 New User

The screenshot shows the 'New User' form in the AMC interface. The form is titled 'New User' and is located under the 'Admin > Users > Manage Local Users > New' path. The form contains several input fields: 'Login ID' (User1), 'First Name' (User), 'Last Name' (User), 'Email Address' (user@company.com), 'Password' (masked with dots), and 'Confirm Password' (masked with dots). A 'Roles' dropdown menu is open, showing four options: 'ApplicationAdministrator', 'ApplicationDesigner', 'NetworkAdministrator' (highlighted), and 'SecurityAdministrator'. At the bottom right, there are 'Submit' and 'Cancel' buttons.

Actions to Take

Enter the appropriate information for the user and select a role. Use Control+click to select multiple roles. For description of available roles, see [Assigning Roles to Users, page 5-5](#).

After completing the entries, click the **Submit** button to save your changes.

Displaying Information on Users

You can use AMC to display information on a selected user, including name, email address, and roles assigned.

How to Get There

Go to **Admin > Users > Manage Local Users**, then select a user. Click the Show button to display the information. [Figure 5-3](#) shows the Show User Details page.

Figure 5-3 Show User Details

The screenshot shows the AMC web interface. At the top, there is a navigation bar with tabs for Network, Properties, Deploy, Monitor, Keystores, and Admin. The Admin tab is selected. On the left, a sidebar menu shows the following options: Licensing, Users (with sub-items Manage Local Users and Manage External Users), AMC Security, Extensions, and Node Migration. The main content area is titled "Show User Details" and contains the following information:

- Login ID: aonsadmin
- First Name: AONS
- Last Name: Administrator
- Email Address:
- Roles: ApplicationAdministrator, ApplicationDesigner, NetworkAdministrator, SecurityAdministrator
- Created: Wed Feb 16 15:49:20 PST 2005
- Last Modified: Wed Feb 16 15:49:20 PST 2005

At the bottom right of the main content area, there is a button labeled "< Back".

Editing Users

AMC provides the ability to edit the properties of local users.

How to Get There

Go to Admin > Users > Manage Local Users, then select a user. Click the Edit button. [Figure 5-4](#) shows the Edit Local User page.

Figure 5-4 Edit Local User

The screenshot shows the 'Edit User' page in the AMC interface. The navigation menu on the left includes 'Licensing', 'Users', 'AMC Security', 'Extensions', and 'Node Migration'. The 'Users' section is expanded, showing 'Manage Local Users' and 'Manage External Users'. The main form area is titled 'Edit User' and contains the following fields:

- Login ID: aonsadmin
- First Name: AONS
- Last Name: Administrator
- Email Address: (empty)
- Roles: ApplicationAdministrator, ApplicationDesigner, NetworkAdministrator, SecurityAdministrator

At the bottom right of the form, there are 'Submit' and 'Cancel' buttons.

Actions to Take

Make changes as necessary, then click the **Submit** button to save your changes.

Assigning Roles to Users

AMC users can be given roles based on their need to perform certain actions on AMC. Each role grants specific privileges within AMC. For example, the Application Designer role can only upload extensions to the AMC, however, a Network Administrator can access functions related to managing and monitoring nodes. To give a user full access to AMC, assign all four roles to that user. [Table 5-1](#) shows the roles available in AMC, and the sections on each tab these roles can access.

Table 5-1 AMC User Roles

Role	Network Tab	Properties Tab	Deploy Tab	Monitor Tab	Keystores Tab	Admin Tab
Application Administrator	—	<ul style="list-style-type: none"> • Adapter • Application • JMS • Monitoring • Service Profiles 	<ul style="list-style-type: none"> • All 	<ul style="list-style-type: none"> • All 	—	<ul style="list-style-type: none"> • All
Application Designer	—	—	—	—	—	<ul style="list-style-type: none"> • Extensions

Table 5-1 AMC User Roles (continued)

Role	Network Tab	Properties Tab	Deploy Tab	Monitor Tab	Keystores Tab	Admin Tab
Network Administrator	<ul style="list-style-type: none"> All 	<ul style="list-style-type: none"> Monitoring 	—	<ul style="list-style-type: none"> All 	—	—
Security Administrator	—	<ul style="list-style-type: none"> Authentication and Authorization Security 	—	<ul style="list-style-type: none"> All 	<ul style="list-style-type: none"> All 	<ul style="list-style-type: none"> Users AMC Security

To assign roles to a user, see one of the following sections:

- [Creating New Users, page 5-3](#)
- [Editing Users, page 5-5](#)
- [Assigning Roles to External Users, page 5-8](#)

Managing External Users

AMC provides the ability to use an existing LDAP server for user management. To do this, complete the following tasks in the order specified:

1. [Creating an LDAP Profile, page 5-6](#)
2. [Assigning Roles to External Users, page 5-8](#)
3. [Creating an Authentication Realm, page 5-9](#)

Creating an LDAP Profile

An LDAP profile provides the information needed by AMC to retrieve user data from an existing LDAP server.

How to Get There

Go to **Admin > Users > Manage Local Users > LDAP**, then click the **New** button. [Figure 5-5](#) shows the LDAP page.

Figure 5-5 LDAP Property Set

The screenshot shows the 'LDAP: Add New Property Set' configuration page. The left sidebar contains navigation options: Licensing, Users (with sub-options 'Manage Local Users' and 'Manage External Users'), AMC Security, Extensions, and Node Migration. The top navigation bar includes Network, Properties, Deploy, Monitor, Keystores, and Admin. The breadcrumb trail is 'Admin > Users > Manage External Users > New'. The main form contains the following fields:

- * Name:
- Primary LDAP Server:
- Backup LDAP Server:
- Connection Maximum Retry:
- Connection Timeout (in seconds):
- Server Port:
- Authentication Type:
- Connect DN:
- Connect Password:
- UID Attribute:
- Base DN:
- User Object Class:

At the bottom right, there are 'Submit' and 'Cancel' buttons.

Actions to Take

Complete the entries as appropriate for the LDAP server being used. Contact your LDAP administrator for details.

Assigning Roles to External Users

How to Get There

Go to **Admin > Users > Manage Local Users > Role Mapping**, then click the **New** button. [Figure 5-6](#) shows the Role Mapping page.

Figure 5-6 Role Mapping

Data to Enter

[Table 5-2](#) shows the entries of the Role Mapping page.

Table 5-2 Role Mapping Entries

Entry	Description
Name	Name of your choosing for this property set.
LDAP Attribute Name	The LDAP attribute that is to be used to specify the AMC role.
Condition Operator	Choose one of the following from the drop-down list: <ul style="list-style-type: none"> • equals—information retrieved from LDAP server must match exactly with LDAP attribute value specified below. • contains—information retrieved from LDAP server must contain LDAP attribute value specified below. • defineRoles—information retrieved from LDAP will define the role of the user.
LDAP Attribute Value	The value for the attribute specified above.
Assign Roles	Click the Edit List button to choose roles that are to be assigned to users who match the LDAP attribute. See “AMC User Roles”

Actions to Take

After completing the entries, click the **Submit** button to save your changes.

Creating an Authentication Realm

The LDAP Authentication Realm binds the LDAP information specified in the “[Creating an LDAP Profile](#)” section on page 5-6 with the role mapping information specified in “[Assigning Roles to External Users](#)” section on page 5-8.

How to Get There

Admin > Users > Manage Local Users > Authentication Realm, then click the **New** button. [Figure 5-7](#) shows the Authentication Realm page.

Figure 5-7 Authentication Realm

Data to Enter

[Table 5-3](#) shows the Authentication Realm page.

Table 5-3 Authentication Realm

Entry	Description
Name	Name of your choosing for this property set.
Realm Name	Name of your choosing for the realm.
LDAP Connection Profile	Choose an available LDAP profile from the drop-down list. See the “ Creating an LDAP Profile ” section on page 5-6 to create a new profile.
Role Mapping Policies	Click the Edit List button to select from the available Role Mapping property sets. See the “ Assigning Roles to External Users ” section on page 5-8 to create a new property set.

Actions to Take

After completing the entries, click the Submit button to save your changes. Once you completed this task, the LDAP configuration appears in the drop-down list on the AMC log-in page.

Managing Keystores

The Keystore tab is used for managing the keypairs, trustpoints, and root certificates used in the AON network. See the following sections:

- [Configuring a Keystore Passphrase, page 5-10](#)
- [Managing Keypairs, page 5-10](#)
- [Manage Public Certificates or Root Certificates, page 5-18](#)

Configuring a Keystore Passphrase

When AMC is started for the first time, the global keystores used by AMC are automatically created with the passphrase **aonsadmin**. To ensure the security of the keystores, it is recommended that you immediately change this password.

Managing Keypairs

Keypairs are the public and private keys used by devices in the AON network to encrypt messages. Most keypair management tasks are performed in the Active Repository. AMC also includes a keypair archive, for expired or revoked keypairs.

How to Get There

Go to **Keystores > Keypairs > Active Repository**. This opens the Keypair Active Repository (see [Figure 5-8](#)).

Figure 5-8 Keypair Active Repository

Alias	Type	Not Valid Before	Not Valid After	Actions
amc-test		Apr 1, 2005	Apr 1, 2015	Show Archive

Rows/Page: 10 Go Page: 1 / 1 Go

Key, Certificate

Upload PKCS#12 MPKI Keypair Self-Signed Keypair SSL Certificate Import Keystore

Actions to Take

You can perform any of the following actions:

- Upload a PKCS#12 file. See the [“Upload PKCS#12” section on page 5-11](#).
- Generate and register a MPKI Keypair. See the [“Generate and Register a New Key” section on page 5-12](#).
- Generate a self-signed keypair. See the [“Generate a Self-Signed Keypair and Certificate” section on page 5-13](#).

- Add an SSL Certificate. See the “Generate an SSL Certificate” section on page 5-14.
- Import a keystore from another source. See the “Import a Keypair or Keystore” section on page 5-17.

Upload PKCS#12

PKCS#12 is a standard for securely storing private keys and certificates. You can upload a PKCS#12 file (with a .pfx file extension) containing this information.

How to Get There

Go to **Keystores > Keypairs > Active Repository > Upload PKCS#12**. See [Figure 5-9](#).

Figure 5-9 Upload a PKCS#12 File

Data to Enter

The Upload PKCS#12 File page includes the entries described in [Table 5-4](#).

Table 5-4 Upload PKCS#12 File Entries

Entry	Description
Alias	Name of your choosing for this key.
PKCS#12 file	Full path and file name. Click the Browse button to locate the file to be imported. The file must have a .pfx extension.
Password	Password used to secure the key.

Actions to Take

After completing the entries, you can take one of the following actions:

- Click **Submit** to save your changes and upload the file.
- Click **Cancel** to discard your changes and return to the previous screen.

Generate and Register a New Key

If you have a managed public key infrastructure (PKI) account with Verisign, you can use AMC to generate and register a new key.

How to Get There

Go to **Keystores > Keypairs > Active Repository > MPKI Keypair**. See [Figure 5-10](#).

Figure 5-10 Generate and Register a New Key

The screenshot shows the 'Generate and Register Key' page in the Verisign management console. The breadcrumb trail is 'Keystores > Keypairs > Active Repository > MPKI Keypair'. The page title is 'Generate and Register Key'. Below the title, there is a brief instruction: 'Register a generated key in your Managed PKI account. Any registered keys can be validated by your business partners.' The form is divided into sections: 'Managed PKI Information' with a 'Key Name' field and a 'Passcode' field; 'Description' with 'Key Alias', 'Revocation Password', and 'Confirm Revocation Password' fields; and 'XKMS Service' with radio buttons for 'Production' (selected) and 'Pilot'. 'Submit' and 'Cancel' buttons are at the bottom right.

What to Enter

The Generate and Register Key page includes the entries described in [Table 5-5](#).

Table 5-5 Generate and Register Key Entries

Entry	Description
Key name	The key name is provided by your managed PKI administrator. It looks similar to the following: <code>http://xkms.verisign.com/keyname?jurisdiction=d7ea68c518b2602ca4bbc....</code>
Passcode	The passcode is provided by your managed PKI administrator.
Key alias	Name of your choosing for this key. Lower case characters only.
Revocation password	Enter a password to be used should this key need to be revoked.
XKMS service	Click Pilot for pre-production environments. Click Production for production environments.

Generate a Self-Signed Keypair and Certificate

If you do not need a key validated by third parties or business partners, AMC can generate a key without a managed PKI account.

How to Get There

Go to **Keystores > Keypairs > Active Repository > Self-Signed Keypair**. See [Figure 5-11](#).

Figure 5-11 Generate a Self-signed Keypair and Certificate

The screenshot shows a web interface for generating a self-signed keypair and certificate. The breadcrumb trail is: Keystores > Keypairs > Active Repository > MPKI Keypair > Self-Signed Keypair. The form title is 'Generate Self-signed Keypair and Certificate'. The form fields are as follows:

Field	Value	Example
Alias	<input type="text"/>	
Modulus Length	1024	
Algorithm	MD5withRSA	
Validity	365 (days)	
Common Name (CN)	<input type="text"/>	(e.g. my.host.name)
Organizational Unit (OU)	<input type="text"/>	(e.g. Human Resources)
Organization (O)	<input type="text"/>	(e.g. Cisco Systems)
Location (L)	<input type="text"/>	(e.g. San Jose)
State (ST)	<input type="text"/>	(e.g. California)
Country (C)	<input type="text"/>	(e.g. US)
Email	<input type="text"/>	

Buttons: Submit, Cancel

Data to Enter

Complete the entries as required for your organization and click the **Submit** button.

Generate an SSL Certificate

AMC includes the ability to submit a Certificate Signing Request (CSR) to Verisign. This request can be for a free trial certificate valid for 14 days, or if you are a MPKI SSL customer, it can be for a permanent certificate.

How to Get There

Go to **Keystores > Keypairs > Active Repository > SSL Certificate**. This page is shown in [Figure 5-12](#).

Figure 5-12 Generate a Key for an SSL Server ID

Data to Enter

Complete the entries as required for you organization and click the **Submit** button. AMC generates the server certificate and displays it on the Add SSL Server ID page.

Figure 5-13 shows the Add SSL Server ID Page.

Actions to Take

Use the mouse to select and copy the entire Certificate Signing Request. You will paste this certificate into the appropriate form at the Verisign.

Figure 5-13 Add SSL Server ID

Network Properties Deploy Monitor Keystores Admin

Keystores > Keypairs > Active Repository > SSL Certificate

Keypairs

- Active Repository
- Archive
- Public Certificates
- Root Certificates
- Configuration

VeriSign

Add SSL Server ID

Enroll for a VeriSign Server ID for SSL. The Server ID you obtain from VeriSign can be used for securely accessing this console and for enabling transport security (SSL/TLS).

1. Generate an SSL key for SSL Server ID

Enter information about your machine and the entity to whom the certificate will be issued. An SSL key with a temporary issuer will be generated.

Next >
2. Submit Certificate Signing Request (CSR) to VeriSign

A CSR for the server key you created in step (1) will be displayed below. Copy this CSR. By selecting **Next**, you will be directed to VeriSign's Server ID enrollment pages, where you will submit this CSR by pasting it into the appropriate form. 14-day trial Server ID's arrive immediately. Production certificates arrive after you have been properly authenticated by VeriSign.

CSR:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBrDCCARUCAQAwbDELMAkGA1UEBhMCVVMxMzAxBG9NVBAgTAKNBMRewDwYDVQQQ
HEwhTYW4gSm9z
ZTEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczENMAAsGA1UECXMEdGVzdDEWMBQGA1UE
AxMNyW9uLmNp
c2NvLmNvbTcBnzANBjkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAmmCB7JJaSJ+y6FR5P1fMq
JA7n/KW
vyRDj2kIQ3VjyE4QShL5FrSYGvb00Jq7GCDdl+kfuLetUkVEMVTEJwescoHmLSYWq3iGCSex
mkQV
niiS3x+0hKgOTyMqN1oG8GuTpydN9d5fQ4eSLtIZG0L/Pfo1KbUcjTik8F2GiUmdECAwEAAaA
A
MA0GCSqGSIb3DQEBAUAA4GBAF0ZR2xZHO4j+DgiPI0KxtBRHeioe2SsoKUy6dJ3dR7Xkt
peqnt
DkUZmxpk1e3nibZphyYlyS45sblwFAET8QWth8ezVGZhp1NRV64abKIKww8Kuvr3q531tpAd
```

Finish Next >
3. Install the certificate you receive from VeriSign

After you receive your SSL Server certificate in an email from VeriSign, you replace the temporary certificate created in step 1, above.

Next >

After copying the CSR and clicking Next, a new browser window opens and loads the Verisign where you complete the process for registering your SSL server ID.

Figure 5-14 Shows the Verisign enroll for an SSL certificate. Complete the enrollment process to register the certificate generated by AMC.

Figure 5-14 Verisign SSL Certificate Enrollment

VeriSign ENROLL FOR A TRIAL SSL CERTIFICATE

WELCOME TECHNICAL ENTER CSR VERIFY CSR ORDER SUMMARY FINISH

Welcome [HELP ?](#)

Product: TRIAL SSL CERTIFICATE

Includes: Free SSL Trial SSL Certificate, 14 days validity period.

Enrolling for a certificate includes the following steps:

- Step 1.** Enter your Technical Contact information.
- Step 2.** Identify your server platform and enter your Certificate Signing Request (CSR).
- Step 3.** Verify your CSR and enter a challenge phrase for this certificate.
- Step 4.** Confirm and submit your order.
- Step 5.** Install the Test CA Root.
- Step 6.** Receive (via e-mail) and install your Trial SSL certificate.

[Continue](#)

After completing the process at Verisign, return to the Active Repository in AMC and click the Pending link for your new certificate, as shown in Figure 5-15.

Figure 5-15 Active Repository with Pending Entries

Network Properties Deploy Monitor Keystores Admin

Keypairs Active Repository Archive Public Certificates Root Certificates Configuration

Keypair Active Repository

Alias	Type	Not Valid Before	Not Valid After	Actions
aon.pending-trial-ssl	Key	Apr 28, 2005	Jul 27, 2005	Show Pending Archive
testing.pending-trial-ssl	Key	Apr 28, 2005	Jul 27, 2005	Show Pending Archive

Rows/Page: 10 Go Page: 1 / 1 Go

Key, Certificate

Upload PKCS#12 MPKI Keypair Self-Signed Keypair SSL Certificate Import Keystore

On the screen that loads, click the **Next** button to display the Install SSL Digital Certificate page, as shown in Figure 5-16.

Figure 5-16 Install SSL Digital Certificate

Keystores > Keypairs > Active Repository > Pending > Next

VeriSign

Install SSL Digital Certificate

Copy the SSL Server ID you received from VeriSign into the text box below and click **Submit**.

Base64 Certificate: `/mesFnjGbeW6ZjAfBgNVHSMEGDAWgBQQF69jUeCKAv+izdCsPfqhFrCbSDBGBgNVHR8EPzA9MDUgOaA3hjVodHRwOi8vd3d3LmNpY2NvLmNvbS9zZWZWN1cmI0eS9wa2kvY3UsL0NBUC1SVFAiMDAzLmNybDBTBggrBgEFBQcBAQRHMEUwQWYlKwYBBQUHMAKGN2h0dHA6Ly93d3cuY2lzY28uY29tL3NIY3VyaXR5L3BraS9jZXJ0cy9DQVAtUURQLTAwMy5jZlhwPwYJKwYBBAGCNxQCBDleMABJAFAAUwBFAEMASQBuAHQAZQByAG0AZQBkAGkAYQB0AGUATwBmAGYAbABpAG4AZTANBgkqhkiG9w0BAQUFAAOCAQEAc7fF+duklmS02+N4NTdcy/nPxBMhjbSshvHzqt+QyPhkXypZgAhtxU1afQvWwBT3zUig5FdpEvl0A5o pGZDJ7PD4LEy3HZ2hmk5p7PNEjW9LvZLxJpi7F/siorUtedx8iwlarYDMN+yK2cOl6TmRh64WLENVnQ2eYYbs11JTW5g65gfQk+uXTs1pxeuMCrVoB9MESF MfuKma9uoAXu1J1qjrxZe95/6hLng2yeV9L7rQBC4dsOyFPNRc/7VDqfEPasSakQuhOHVEdRF Y3C0lanhLRDYHU8WqGIY+Mi2N+arBnCaHvKrG80exYWAlIXyndZKSryGCXgWhYRFu3JZw==`

< Back Submit

Actions to Take

Paste the certificate you received from Verisign and click the **Submit** button.

Import a Keypair or Keystore

You can import an existing keystore that contains your public and private certificates.

How to Get There

- Keystores > Keypairs > Active Repository > Import Keystore.
- Keystores > Public Certificates > Active Repository > Import Keystore
- Keystores > Root Certificates > Active Repository > Import Keystore

See [Figure 5-17](#).

Figure 5-17 Import Keystore

Keystores > Keypairs > Active Repository > Import Keystore

Import Keystore

File: Browse...

Keystore Password:

Keystore password different from key alias passwords? Yes No

Submit Cancel

Data to Enter

The Import Keystore page includes the entries described in [Table 5-6](#).

Table 5-6 *Import Keystore Entries*

Entry	Description
File	Full path and filename. Click the Browse button to locate the file to be imported. The file must be a Java 1.4 JKS format keystore file
Keystore password	Password used to secure this keystore.

Actions to Take

After completing the entries, you can take one of the following actions:

- Click **Submit** to save your changes.
- Click **Cancel** to discard your changes and return to the previous screen.

Manage Public Certificates or Root Certificates

The procedure for managing public certificates and root certificates are identical. This section covers the following functions:

- [Add a Certificate, page 5-18](#)
- [Import a Keystore, page 5-20](#)

Add a Certificate

The Add Certificate page enables you to retrieve, upload, or paste a digital certificate.

How to Get There

Navigate one of the following paths:

- **Keystores > Public Certificates > Active Repository > Add Certificate**
- **Keystores > Root Certificates > Active Repository > Add Certificate.**

See [Figure 5-18](#).

Figure 5-18 Add Certificate

Keypairs
Public Certificates
Root Certificates
Active Repository
Archive
Configuration

Keystores > Root Certificates > Active Repository > Add Certificate

Add Certificate

Upload a file, retrieve certificates from via an SSL connection, or paste a digital certificate.

Alias:

Choose a name (lower case characters only) that will identify this certificate.

Get from SSL Connection

URL: Must start with https://

The root certificate presented by the server will be added.

Upload

File:

Cut and Paste Digital Certificate

Base64 Certificate:

Digital certificate example:
 -----BEGIN CERTIFICATE-----
 MIIBfjCCASgCEQCghAI3rOTGBwbocA1QrkngMA0GCSqGSIb3DQEBAUME1xCzAJ
 ...
 CGpZ+RY0GJ8zJNgg05NDm6AIiMHmU/8WtlXmgPA7ocQw68V3QzL6KRYZVmG83uw0
 ULc=
 -----END CERTIFICATE-----

Data to Enter

The Add Certificate page includes the entries described in [Table 5-7](#).

Table 5-7 Add Certificate Entries

Entry	Description
Alias	Name of your choosing for this certificate.
URL	URL from which AMC can retrieve the certificate. Click the Get from SSL connection radio button to use this entry.
File	Full path and file name. Click the Browse button to locate the file to be imported. Click the Upload radio button to use this entry.
Base64 certificate	Paste the certificate in this entry. Click the Cut and paste digital certificate radio button to use this entry.

Actions to Take

After completing the entries, you can take one of the following actions:

- Click **Submit** to save your changes.
- Click **Cancel** to discard your changes and return to the previous screen.

Import a Keystore

You can retrieve a certificate by importing an existing keystore. See the [“Import a Keypair or Keystore” section on page 5-17](#) for detailed instructions.

Configuring Security Properties

These properties enable you to configure the security settings of individual nodes. This section covers the following sections:

- [Endpoint SSLID Property, page 5-21](#)
- [SSL Configuration Property, page 5-22](#)
- [SSL Binding Property, page 5-23](#)

Endpoint SSLID Property

The Endpoint SSLID property is used to specify the keypair alias to be used by a node for SSL.

How to Get There

Go to **Properties > AON Security > Node > Endpoint SSLID > New**. [Figure 5-19](#) shows the SSLID property page.

Figure 5-19 Endpoint SSSLID Property

Endpoint SSLID: Add New Property Set

* Name:

Data to Enter

Enter a name for the Endpoint SSLID property, then click the **Next** button. This loads a page on which you can choose a keypair to associate with this property. [Figure 5-20](#) shows this page.

Figure 5-20 Key Alias

Key Alias

#	Alias	Type	Not Valid Before	Not Valid After
1	amc-test	Key	Apr 1, 2005	Apr 1, 2015

Rows/Page: Page: /

SSL Configuration Property

SSL Configuration Property specifies SSL-related parameters to be used by a node. [Figure 5-21](#) shows the SSLID Property page.

How to Get There

Go to **Properties > AON Security > Node > SSL Configuration**



Note

Before configuring the SSL Configuration Property, you must configure SSLID. See the “[Endpoint SSLID Property](#)” section on page 5-21 for details.

Figure 5-21 SSL Configuration Property

The screenshot shows the management console interface. On the left is a navigation tree with categories: Adapter, Application, Authentication & Authorization, JMS, Monitoring, AON Security (expanded to show Node, Node Management Security, and Service Profiles), and Service Profiles. The main area has tabs for Network, Properties, Deploy, Monitor, Keystores, and Admin. The breadcrumb trail is Properties > AON Security > Node > Edit Properties > Edit. The title is 'SSL Configuration: Edit Property Set'. Below the title is a text input field for the name, currently set to 'Default SSL Policy'. There are three dropdown menus: 'Endpoint Identity' with 'SSSLID1' selected, 'SSL Protocol Version' with 'SSL_v23' selected, and 'Extract Peer Certificate' with 'no' selected. At the bottom right are 'Submit' and 'Cancel' buttons.

Data to Enter

The Security Property page includes the entries described in [Table 5-8](#).

Table 5-8 Security Property Entries

Entry	Description
Name	Name of your choosing for this property.
Endpoint Identity	Choose an available SecurityID from the drop-down list.
SSL Protocol Version	Drop-down list of available versions of SSL. Choose either TLS_v1 or SSL_v23 .
Extract Peer Certificate	Specifies whether peer certificate extraction is to be used. If PEPs are to use the extracted certificate, this option must be set to yes .

Actions to Take

After completing the entries, you can take one of the following actions:

- Click **Submit** to save your changes.
- Click **Cancel** to discard your changes and return to the previous screen.

SSL Binding Property

The SSL Binding property enables you to bind a message's source IP, destination IP, and destination port to an SSL property. [Figure 5-22](#) shows the SSL Binding Property page.

How to Get There

Go to **Properties > AON Security > Node > SSL Binding**



Note

Before configuring SSL Binding, you must configure SecurityID and Security Property. See the “Endpoint SSLID Property” section on page 5-21 and the “SSL Configuration Property” section on page 5-22 for details.

Figure 5-22 SSL Binding Property

Data to Enter

The SSL Binding property page includes the entries described in [Table 5-9](#).

Table 5-9 SSL Binding Property Entries

Entry	Description
Source IP Address	IP address of source.
Destination IP Address	IP address of destination.
Destination Port	Port on which outbound peer is listening for SSL traffic.
Inbound SSL Property	Select an available SSL property from the drop-down list.
Outbound SSL Property	Select an available SSL property from the drop-down list.
Inbound Peer Verification	Select yes or no to specify whether inbound peer verification is to be used.

Table 5-9 *SSL Binding Property Entries (continued)*

Entry	Description
Outbound Peer Verification	Select yes or no to specify whether outbound peer verification is to be used.

Actions to Take

After completing the entries, you can take one of the following actions:

- Click **Submit** to save your changes.
- Click **Cancel** to discard your changes and return to the previous screen.

Configuring Authentication and Authorization Properties

This section covers the following properties:

- [Configuring LDAP, page 5-24](#)
- [Configuring Kerberos, page 5-26](#)

Configuring LDAP

Lightweight Directory Access Protocol (LDAP) is a protocol for accessing online directory services. This property can be configured at the node or global levels. After configuring this property, nodes in your AON network are able to access an LDAP directory for authentication and authorization.

How to Get There

- **Properties > Authentication & Authorization > Global > LDAP**
- **Properties > Authentication & Authorization > Node > Edit Properties**

Figure 5-23 shows the LDAP Property page.

Figure 5-23 LDAP Property

The screenshot displays the 'LDAP: Add New Property Set' configuration page. The left sidebar contains a navigation menu with the following items: Adapter, Application, Authentication & Authorization (selected), Global Node, JMS, Monitoring, AON Security, Node Management Security, and Service Profiles. The main content area has tabs for Network, Properties (selected), Deploy, Monitor, Keystores, and Admin. The breadcrumb trail is 'Properties > Authentication & Authorization > Global > New'. The configuration form includes the following fields:

- * Name: LDAP1
- Primary LDAP Server: 10.10.10.10
- Backup LDAP Server: 10.10.10.11
- Connection Maximum Retry: 2
- Connection Timeout (in seconds): 3
- Server Port: 389
- Authentication Type: simple
- Connect DN: cn=Administrator, cn=users, dc=security, dc=aon
- Connect Password: masked with dots
- UID Attribute: AccountName
- Base DN: cc=security, dc=aon
- User Object Class: user
- User Membership Attribute Name: memberOf

At the bottom right of the form are 'Submit' and 'Cancel' buttons.

Data to Enter

This information varies from site to site. Contact your LDAP administrator for proper configuration data.

Actions to Take

After completing the entries, you can take one of the following actions:

- Click **Submit** to save your changes.
- Click **Cancel** to discard your changes and return to the previous screen.

Configuring Kerberos

Kerberos is an authentication protocol that enables entities communicating over an insecure network to prove their identities to each other. In so doing, Kerberos provides detection of modification and the prevention of eavesdropping.

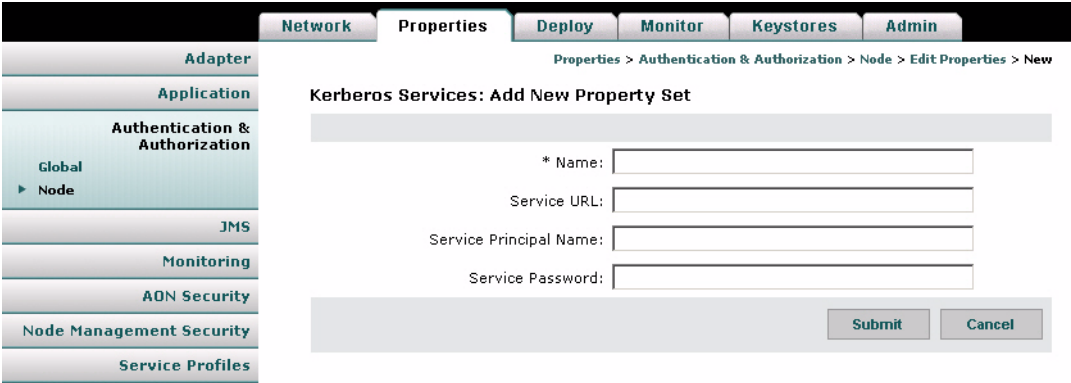
Kerberos configuration is controlled by three properties, which must be configured in the following order:

1. Kerberos Services.
2. Kerberos Realms.
3. Kerberos Info.

In order to complete this configuration, you need specific data from the Kerberos service running on your network.

Step 1 Go to **Properties > Authentication & Authorization > Node > Kerberos Services**. This page is shown in [Figure 5-24](#).

Figure 5-24 Kerberos Services Property



Data to Enter

This information varies from site to site. Contact your Kerberos administrator for appropriate values.

Step 2 Go to **Properties > Authentication & Authorization > Node > Kerberos Realms**. [Figure 5-26](#) shows the Kerberos Realms property page.

Figure 5-25 Kerberos Realms Property

The screenshot shows the 'Kerberos Realms: Add New Property Set' form. The left sidebar contains a navigation tree with 'Authentication & Authorization' expanded to 'Node'. The main content area has the following fields:

- * Name:
- Realm Name:
- Primary KDC Server:
- Secondary KDC Server:
- Kerberos Services:

At the bottom right, there are 'Submit' and 'Cancel' buttons. The breadcrumb trail at the top reads: Properties > Authentication & Authorization > Node > Edit Properties > New.

Data to Enter

This information varies from site to site. Contact your Kerberos administrator for appropriate values.

- Step 3** Click the **Edit List** button and select the Kerberos Services property you created.
- Step 4** Go to **Properties > Authentication & Authorization > Node > Kerberos Info**. Figure 5-26 shows the Kerberos Info property page.

Figure 5-26 Kerberos Info Property

The screenshot shows the 'Kerberos Info: Add New Property Set' form. The left sidebar is the same as in Figure 5-25. The main content area has the following fields:

- * Name:
- KDC Server Connection Timeout:
- Kerberos Realms:

At the bottom right, there are 'Submit' and 'Cancel' buttons. The breadcrumb trail at the top reads: Properties > Authentication & Authorization > Node > Edit Properties > New.

Data to Enter

This information varies from site to site. Contact your Kerberos administrator for appropriate values.

- Step 5** Click the **Edit List** button and select the Kerberos Realms property you created.



Message Log Schemas

This appendix contains scripts that configure an Oracle or Sybase database for message log. For message log configuration instructions, see the [“Message Log Domain” section on page 4-17](#).



Note

Before running either of these scripts, be sure to remove any earlier versions of the Message Log schema.

This information spans multiple pages, making it difficult to select and copy when this guide is viewed in Adobe Acrobat. For best results, go to Cisco.com to view this information on a single page:

Oracle

Log in to SQLPlus as the user created for Message Log, then run this script to configure an Oracle database.

```
CREATE TABLE MESSAGE_LOG_INSTANCE
(  "USE_COUNT"    number(18,0),
   "ID"           varchar2(100),
   "DESCRIPTION"  varchar2(256),
   "VERSION"      varchar2(100)
);

INSERT INTO MESSAGE_LOG_INSTANCE (ID,USE_COUNT,VERSION,DESCRIPTION) VALUES
('AONS-MLOG-001', 0, '1.0', 'Database for storing AONS message logs');

CREATE TABLE MESSAGE_LOG
(
   "LOGID"          number(28,0) not null primary key,
   "HOSTNAME"       varchar2(64),
   "SOURCE_NODE_ID" number(10,0),
   "ENTRY_TIME"     timestamp,
   "CREATION_TIME"  timestamp not null,
   "MESSAGE_ID"     varchar2(100) not null,
   "SESSION_ID"     varchar2(100),
   "DESTINATION"    varchar2(256),
   "NEXT_HOP"       varchar2(256),
   "SOURCE"         varchar2(256),
   "SENDING_NODE"   varchar2(256),
   "FLOW_ID"        varchar2(100),
   "BLADELET_ID"    varchar2(32),
   "FLOW_NAME"      varchar2(100),
   "BLADELET_NAME"  varchar2(100),
   "CONTENT_TYPE"   varchar2(64),
   "PAYLOAD_TYPE"   varchar2(32),
```

```

"MESSAGE_TYPE" varchar2(32),
"MESSAGE_CLASS" varchar2(64),
"PROTOCOL" varchar2(32),
"LOG_VERSION" varchar2(10),
"LOG_TYPE" varchar2(32),
"LOG_LEVEL" number(5),
"SOAP_OPERATION" varchar2(256),
"STATUS" number(10),
"REASON" varchar2(100),
"PROTOCOL_HEADER" raw(2000),
"CUSTOM_STRING1" varchar2(32),
"CUSTOM_STRING2" varchar2(64),
"CUSTOM_STRING3" varchar2(128),
"CUSTOM_STRING4" varchar2(256),
"CUSTOM_STRING5" varchar2(1024),
"CUSTOM_NUMBER1" number(5,0),
"CUSTOM_NUMBER2" number(10,0),
"CUSTOM_NUMBER3" number(18,2)
);

CREATE INDEX "MESSAGE_ID_IDX" ON "MESSAGE_LOG" ("MESSAGE_ID");
CREATE INDEX "MESSAGE_DESTINATION_IDX" ON "MESSAGE_LOG" ("DESTINATION");
CREATE INDEX "MESSAGE_SOURCE_IDX" ON "MESSAGE_LOG" ("SOURCE");

CREATE TABLE SOURCE_NODE
(
  ID NUMBER(10) NOT NULL PRIMARY KEY,
  DN VARCHAR2(256) NOT NULL,
  CREATED_TIME NUMBER(18) NOT NULL,
  NODE_ID NUMBER(10),
  AMC_IP VARCHAR2(64),
  AMC_HOST_NAME VARCHAR2(256),
  AMC_ID VARCHAR2(256),
  AMC_VERSION VARCHAR2(64),
  VIRTUAL_NODE_ID NUMBER(10),
  VIRTUAL_NODE_NAME VARCHAR2(64)
);

create table MESSAGE_CONTENTS (
  LOGID number(28,0) not null,
  CONTENT_TYPE varchar2(64),
  NAME varchar2(64),
  CONTENT long raw,
  EXPRESSION varchar2(256),
  CONTENT_LENGTH number(10,0)
);

CREATE TABLE FLOW_VARIABLES
(
  "LOGID" number(28,0) NOT NULL,
  "NAME" varchar2(100),
  "VALUE" long raw,
  "TYPE" varchar2(100)
);

CREATE SEQUENCE LOGID_SEQ
START WITH 1
INCREMENT BY 50000
NOMAXVALUE;

CREATE OR REPLACE PROCEDURE GET_LOGID_BLOCK (
  blockSize out int,
  beginValue out number
)

```

```

as
begin
  select LOGID_SEQ.nextval INTO beginValue from dual;
  select INCREMENT_BY INTO blockSize from USER_SEQUENCES;
  beginValue := beginValue - blockSize;
  return;
end;
/

select LOGID_SEQ.nextval from dual;

```

Sybase

Log in to SQLAdvantage as the user created for Message Log, then run this script to configure a Sybase database.

```

CREATE TABLE MESSAGE_LOG_INSTANCE
(
  USE_COUNT      numeric(18),
  ID             varchar(100),
  DESCRIPTION    varchar(256),
  VERSION        varchar(100)
)

go

INSERT INTO MESSAGE_LOG_INSTANCE (ID,USE_COUNT,VERSION,DESCRIPTION) VALUES
('AONS-MLOG-001', 0, '1.0', 'Database for storing AONS message logs')

go

create table MESSAGE_LOG (
  LOGID                numeric(28,0)                not null primary key
,
  HOSTNAME             varchar(64)                   null
,
  SOURCE_NODE_ID       numeric(10,0)                 null
,
  ENTRY_TIME           datetime                     null
,
  CREATION_TIME        datetime                     not null
,
  MESSAGE_ID           varchar(100)                  not null
,
  SESSION_ID           varchar(100)                  null
,
  DESTINATION           varchar(256)                  null
,
  NEXT_HOP             varchar(256)                  null
,
  SOURCE               varchar(256)                  null
,
  SENDING_NODE         varchar(256)                  null
,
  FLOW_ID              varchar(100)                  null
,
  BLADELET_ID          varchar(32)                   null
,
  FLOW_NAME            varchar(100)                  null
,
  BLADELET_NAME        varchar(100)                  null
,
  CONTENT_TYPE         varchar(64)                   null
,
  PAYLOAD_TYPE         varchar(32)                   null
,
  MESSAGE_TYPE         varchar(32)                   null
,
  MESSAGE_CLASS        varchar(64)                   null
,
  PROTOCOL             varchar(32)                   null
,
  LOG_VERSION          varchar(10)                   null
,
  LOG_TYPE             varchar(32)                   null
,
  LOG_LEVEL            numeric(5,0)                  null
,
  SOAP_OPERATION       varchar(256)                  null
,
  STATUS               int                          null
,
  REASON               varchar(100)                  null
,
  PROTOCOL_HEADER      varbinary(2000)              null
)

```

```

CUSTOM_STRING1 varchar(32) null ,
CUSTOM_STRING2 varchar(64) null ,
CUSTOM_STRING3 varchar(128) null ,
CUSTOM_STRING4 varchar(256) null ,
CUSTOM_STRING5 varchar(1024) null ,
CUSTOM_NUMBER1 numeric(5,0) null ,
CUSTOM_NUMBER2 numeric(10,0) null ,
CUSTOM_NUMBER3 numeric(18,2) null
)
go

CREATE INDEX MESSAGE_ID_IDX ON MESSAGE_LOG (MESSAGE_ID)
go

CREATE INDEX MESSAGE_DESTINATION_IDX ON MESSAGE_LOG (DESTINATION)
go

CREATE INDEX MESSAGE_SOURCE_IDX ON MESSAGE_LOG (SOURCE)
go

CREATE TABLE SOURCE_NODE
(
    ID numeric(10,0) not null primary key,
    DN varchar(256) not null,
    CREATED_TIME numeric(18,0) not null,
    NODE_ID numeric(10,0) null,
    AMC_IP varchar(64) null,
    AMC_HOST_NAME varchar(256) null,
    AMC_ID varchar(256) null,
    AMC_VERSION varchar(64) null,
    VIRTUAL_NODE_ID numeric(10,0) null,
    VIRTUAL_NODE_NAME varchar(64) null
)
go

create table MESSAGE_CONTENTS (
    LOGID numeric(28,0) not null,
    CONTENT_TYPE varchar(64) null,
    NAME varchar(64) null,
    CONTENT image null,
    EXPRESSION varchar(256) null,
    CONTENT_LENGTH int null
)
go

create table FLOW_VARIABLES (
    LOGID numeric(28,0) not null ,
    NAME varchar(100) null ,
    TYPE varchar(100) null ,
    VALUE image null
)
go

create table LOGID_KEY (

```

```
        ID      numeric(28,0) not null
    )
go

insert into LOGID_KEY values (1)

go

CREATE PROCEDURE GET_LOGID_BLOCK
@blockSize int output,
@beginValue numeric(28,0) output
AS
BEGIN
    select @beginValue=ID from LOGID_KEY
    select @blockSize = 50000
    update LOGID_KEY set ID = @beginValue + @blockSize
END

go

sp_procxmode 'GET_LOGID_BLOCK', chained
go
```

