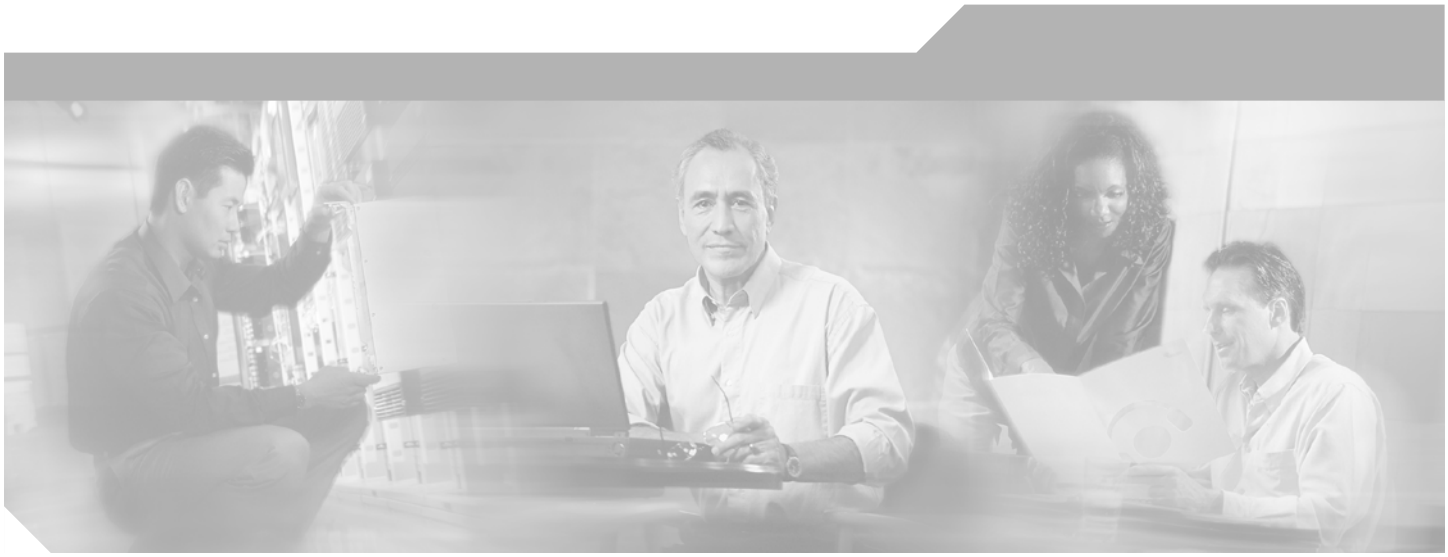


AON Installation and Administration Guide

AON release 2.1
March 2006

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.

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, 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, 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, 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. (0601R)

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

AON Installation and Administration Guide
© 2006 Cisco Systems, Inc. All rights reserved.

CONTENTS

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

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

Working with Nodes 3-1

Managing Nodes 3-1

Creating Nodes 3-2

Configuring WCCP for Traffic Redirection 3-5

Editing Nodes 3-6

Deleting Nodes 3-7

Replacing Nodes 3-8

Exporting Nodes 3-9
Importing Nodes 3-10
Managing WCCP Servers 3-11
Creating WCCP Servers 3-11
Managing Virtual Clusters 3-12
Creating a Virtual Cluster 3-12
Changing Nodes Within a Virtual Cluster 3-14
Configuring WCCP for Cluster Management 3-14
Configuring WCCP for Traffic Redirection 3-17
Configuring ACL/Classifiers 3-19
Configuring Recovery 3-21
Deploying to Nodes 3-22
Viewing Logs 3-24
Viewing Events 3-24

Managing AON Properties 4-1
Monitoring Activity 4-2
Bladelet Monitoring Property 4-2
Message Log Domain 4-2
Create a Message Log Database 4-3
Configure Message Log Domain Property 4-4
Adaptive Load Balancer 4-5
Adjusting Quality and Performance 4-7
Caching 4-7
Reliable Messaging 4-8
Application QOS 4-9
Working with Message Content 4-11
Content Parser 4-11
Content Validation 4-11
Working with XSL Transformation 4-12
Controlling Message Delivery 4-14
Configuring Delivery Connection 4-14
Configuring Delivery Notification 4-15
Configuring Delivery Semantics 4-16
Binding Message Delivery Properties to a Message Type 4-17
Next Hop Domain 4-18
Node Capabilities 4-19
Working with Adapters 4-21
Adapter Registry 4-21

Adapter Listener Domain 4-22
Service Profiles for Adapters 4-22
Working with Message Transport 4-24
Encoding 4-24
Configuring JMS Properties 4-25
JMS Destination Property 4-25
JMS Source Property 4-26
JMS Reply To 4-27
JMS Connections Property 4-28
JMS Naming Property 4-29
Configuring Cisco AON Promiscuous Mode 4-31
Prerequisites for Promiscuous Mode 4-31
Information About Promiscuous Mode 4-31
How to Configure Promiscuous Mode 4-32
Connecting to Databases 4-49

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

SSL Binding Property 5-23
Configuring Authentication and Authorization Properties 5-24
Configuring LDAP 5-24
Configuring Kerberos 5-26

AMC Administration 6-1
AMC Diagnostics 6-1
AON Licensing 6-2
Managing AON Users 6-2
Managing Local Users 6-2
Creating New Users 6-4
Displaying Information on Users 6-5
Editing Users 6-6
Assigning Roles to Users 6-6
Managing External Users 6-7
Creating an LDAP Profile 6-7
Assigning Roles to External Users 6-9
Creating an Authentication Realm 6-10
Managing AMC Certificates 6-11
Managing Extensions 6-11

Message Log Schemas A-1
Oracle A-1
Sybase A-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 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 the this chapter the first time you implement application-oriented networking.

- Chapter 3, "Managing Nodes"

  This chapter describes basics about managing nodes from AMC. You need to set up and configure nodes during your initial AON deployment. 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.

CHAPTER 2

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 he 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.

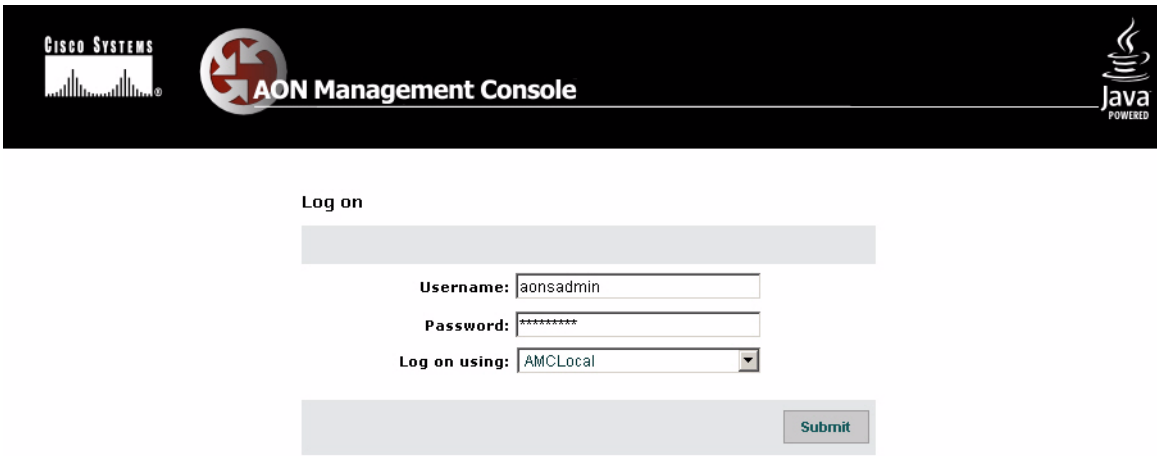
```
Would you like to run the AMC now? [y|n]:y
Starting AMC Database...Done.
Starting AMC...Done.
Installation successful.
To uninstall, run '/opt/amc/bin/amcSetup uninstall'.
```

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-doc/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 **aonsadmin**.

```
                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:

Note During start up, the AON-SM retrieves the system time from the switch. Ensure that NTP is configured on the switch before you configure the AON-SM.

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:

Note During start up, the AON-NM retrieves the system time from the router. Ensure that NTP is configured on the router before you configure the AON-NM.

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

Upgrade instructions are now located in the following stand-alone document:

- Upgrading to Cisco Applicaiton-Oriented Networking Version 2.1

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 3-5
- 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.

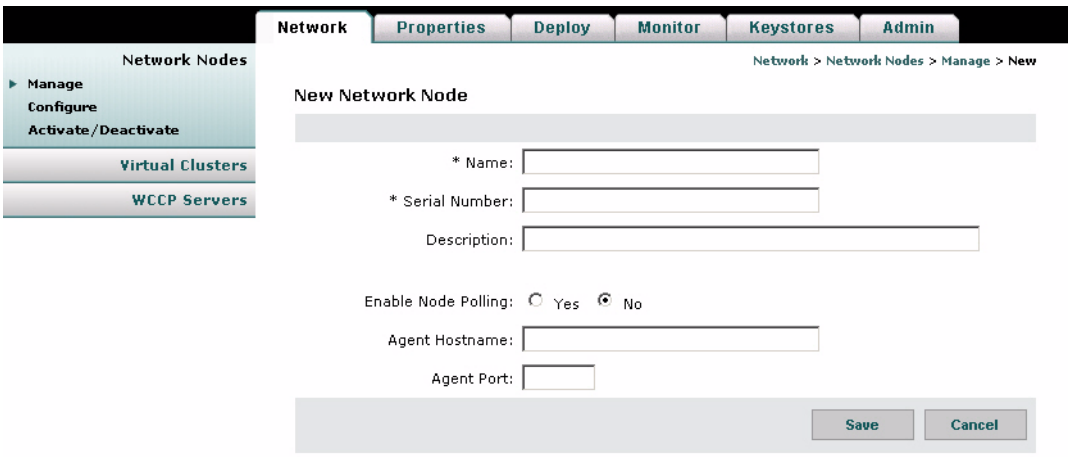
Step 1 Connect to the command-line interface of the AON node. Use the **show version** command to obtain the module serial number (highlighted below).

```
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:                Cisco 2600/3700/ISR AON Module (NM-AON-K9)
Module Serial:              FOC082313YY
AON:                        2.1.0.135
AMA:                        2.1.0.135
```

Note the module serial number in bold text 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



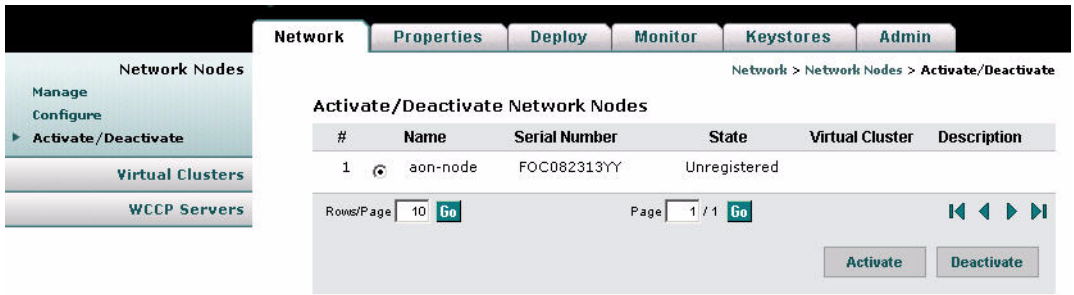
Step 3 Complete the entries on this page as described in Table 3-1.

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.
Enable Node Polling	Enable polling when AMC a firewall is between AMC and the node. Rather than waiting for the node to contact AMC, AMC will initiate contact with the node.
Agent Hostname	Name or IP address of the node.
Agent Port	Port used by node for management traffic.

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.

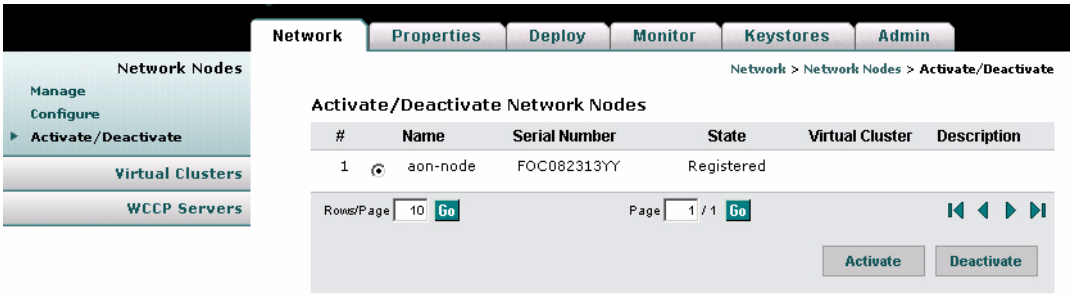
```
aon-node> configure terminal
Enter configuration commands, one per line.  End with exit.
aon-node(config)> aon config configuration_id create
aon-node(config)> aon config configuration_id ama host module_IP_address
aon-node(config)> aon config configuration_id amc host AMC_IP_address
aon-node(config)> 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

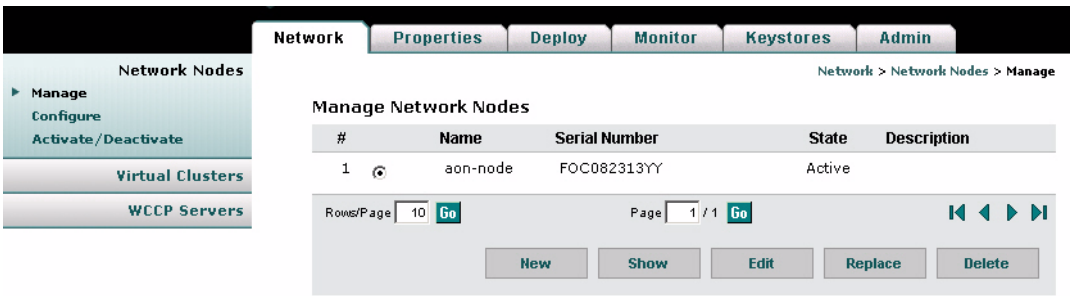


Tip If your network node remains unregistered, verify that the serial number is entered exactly as described in Step 3. The AMC will not establish trust with a node if this information is incorrect.

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



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

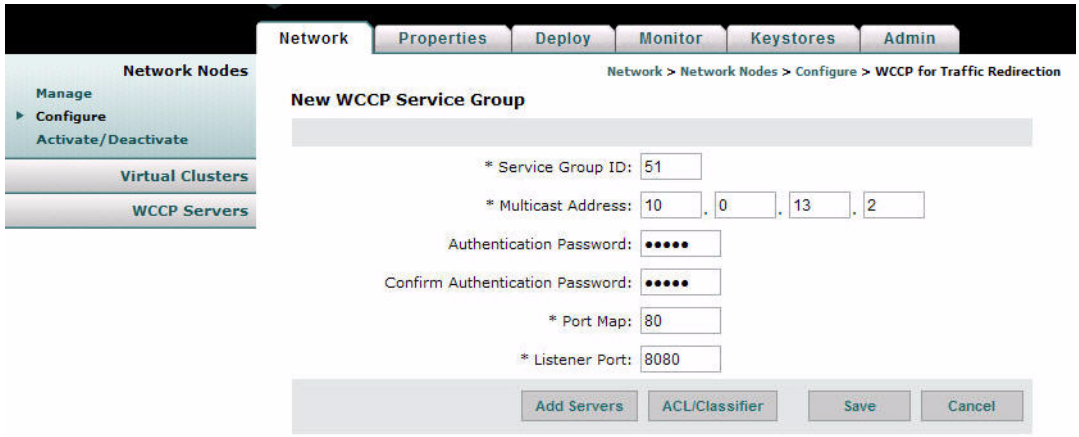


Table 3-6 shows the entries available on the New WCCP Service Group page.

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.

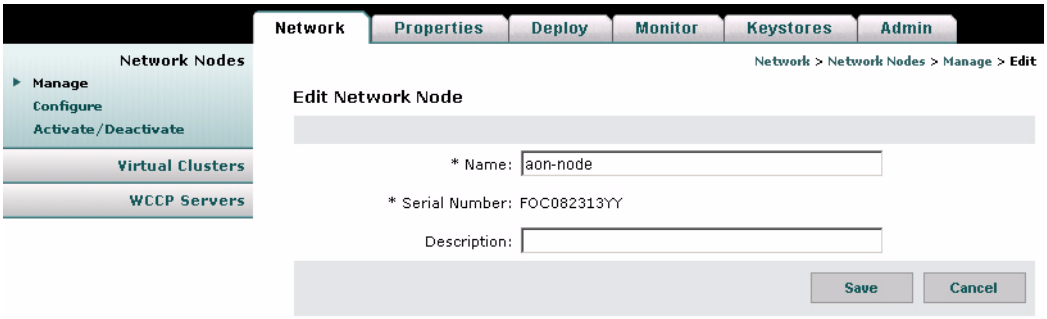
Editing Nodes

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



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.

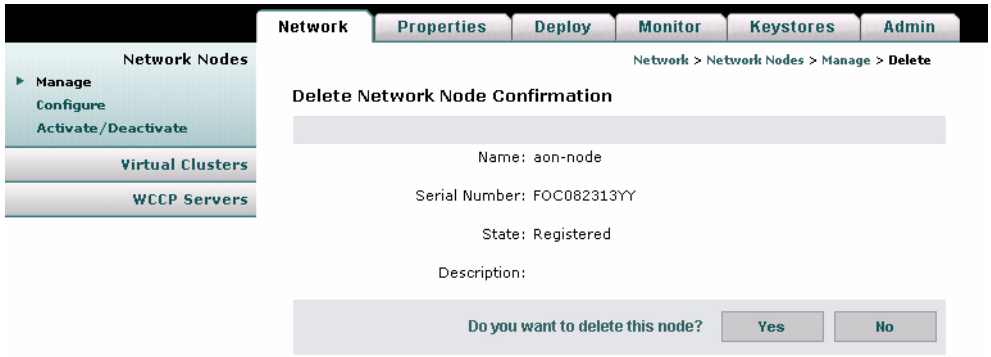
Deleting Nodes

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.

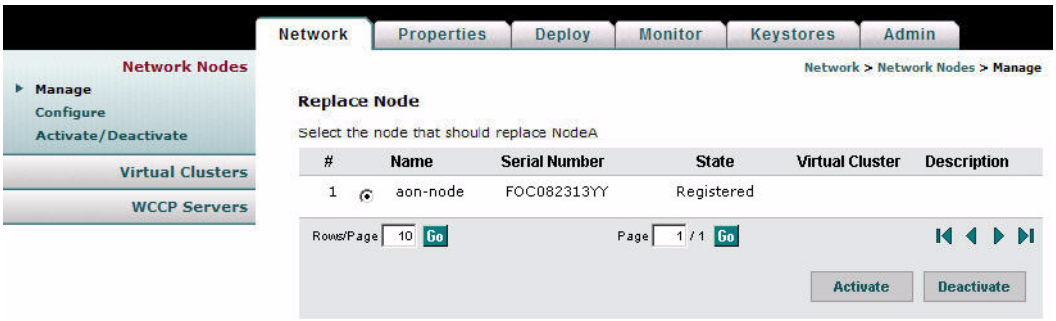
Replacing Nodes

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



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

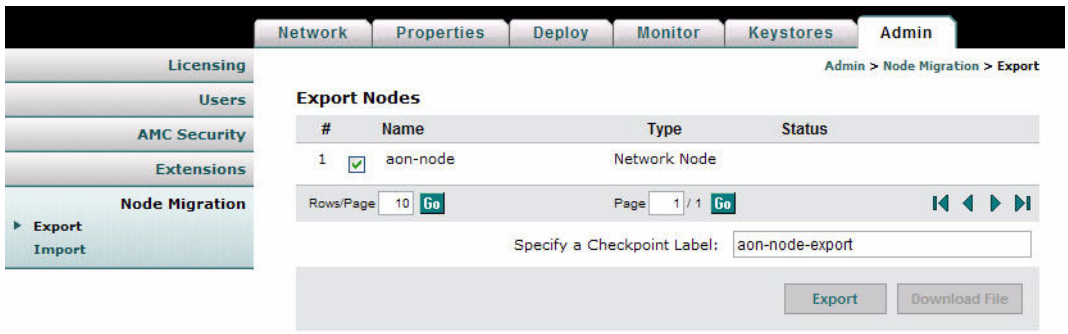
AMC provides the ability to export the configuration data from a node so that it can be imported by another AMC. Enter a unique name for the checkpoint label.

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



Actions to Take

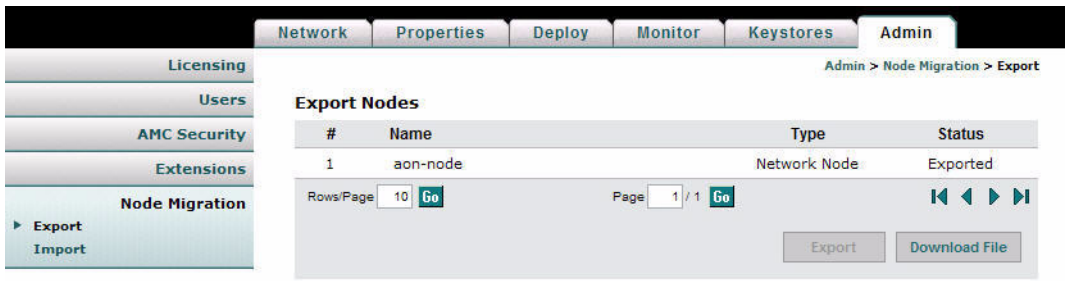
You can take the following action:

- 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



Actions to Take

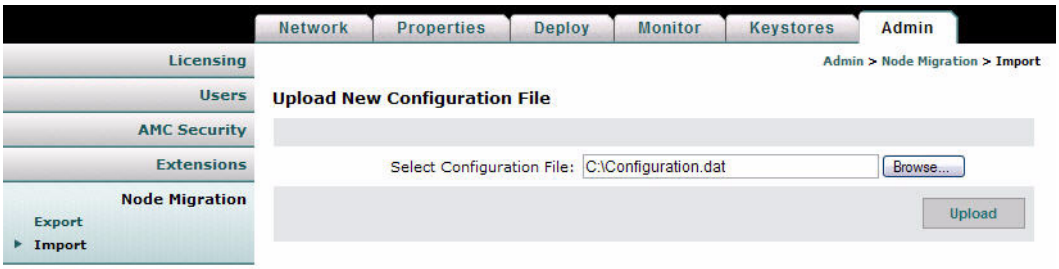
You can take the following action:

- 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



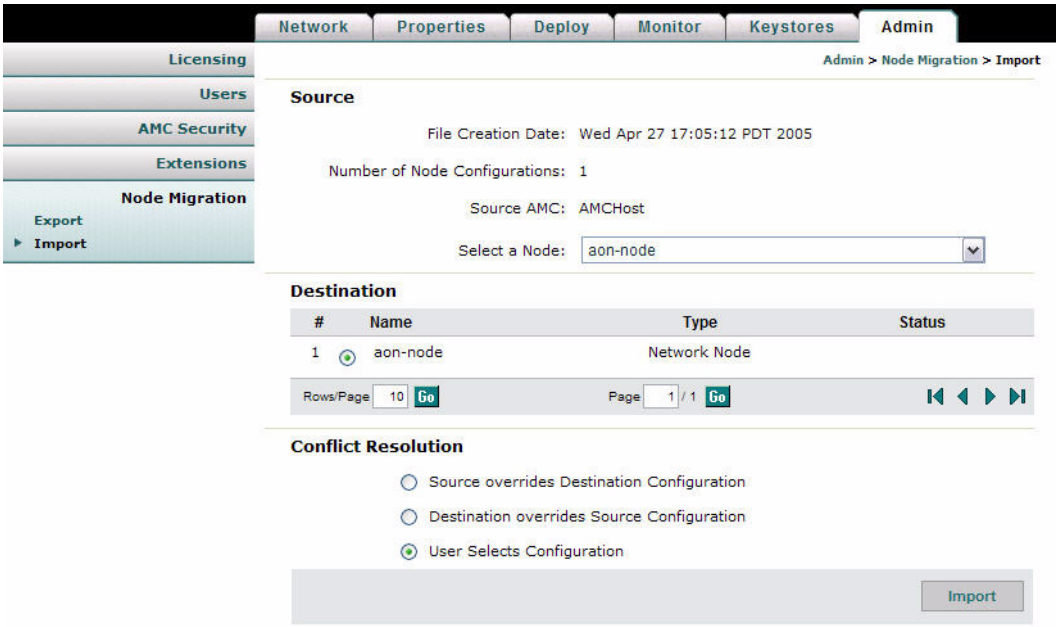
Actions to Take

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



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

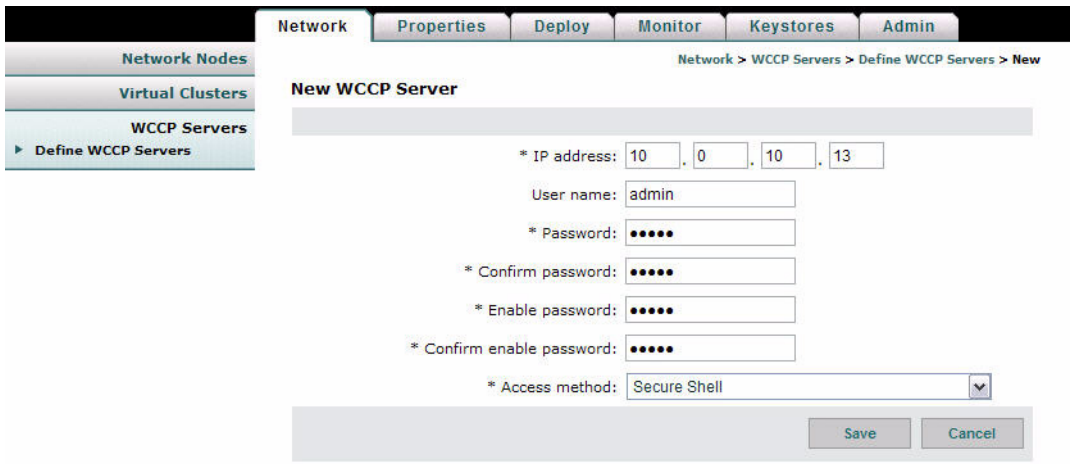


Table 3-3. shows the entries available on the New WCCP Server page.

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

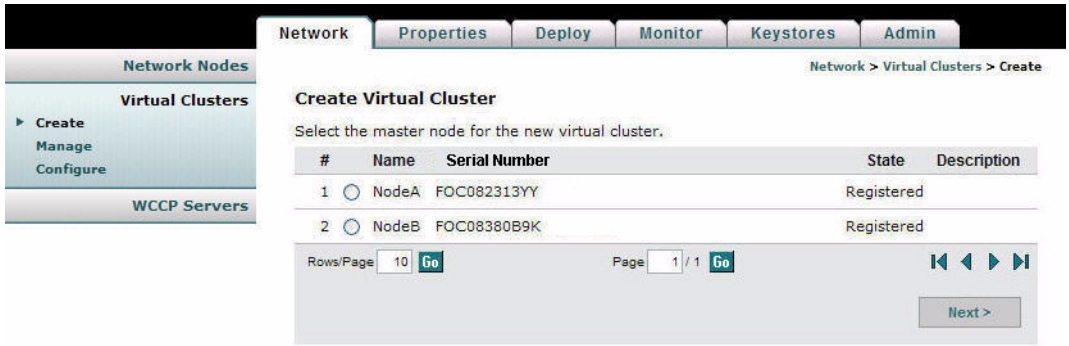
A virtual cluster consists of two or more AON nodes that are configured to share workload and ensure redundancy. The first node you choose for a cluster is called the master node. Other nodes that you add to the cluster will receive duplicate configurations to that of the master node. After the virtual 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.

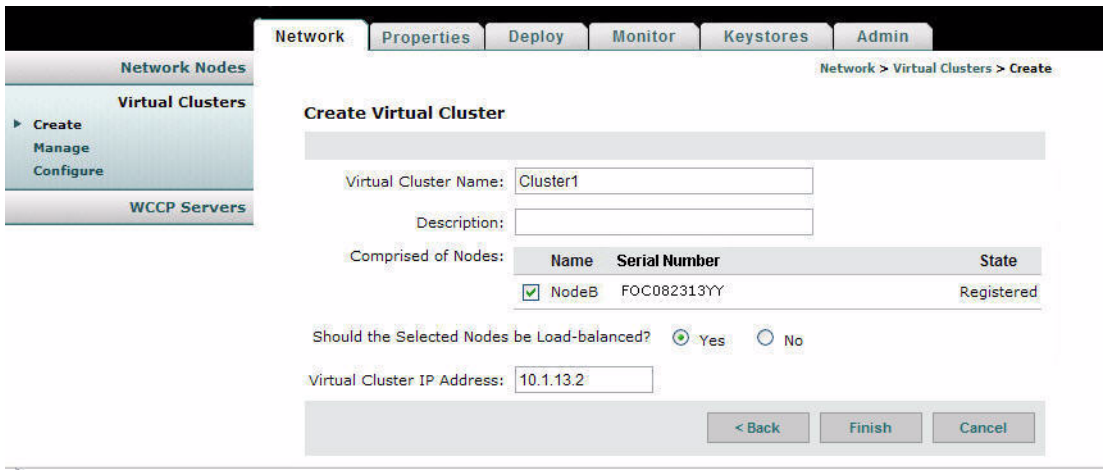
Step 1 Go to **Network > Virtual Clusters > Create**. This loads the Create Virtual Cluster page, as shown in Figure 3-14.

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.

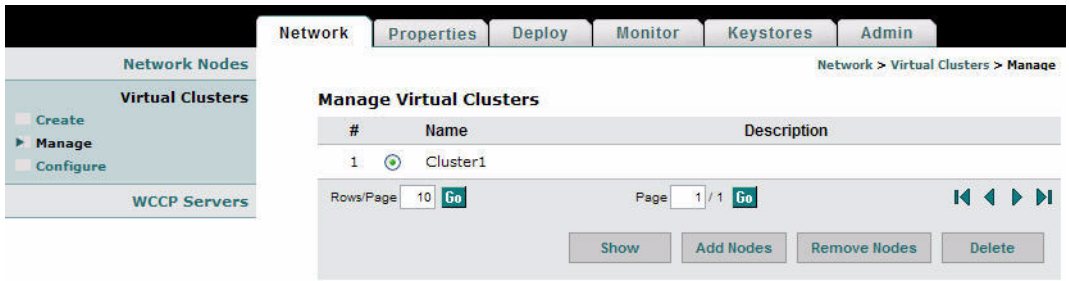
Figure 3-15 Create a Virtual Cluster



Step 3 Complete the entries as appropriate for your network and select the other nodes to be added to the cluster.

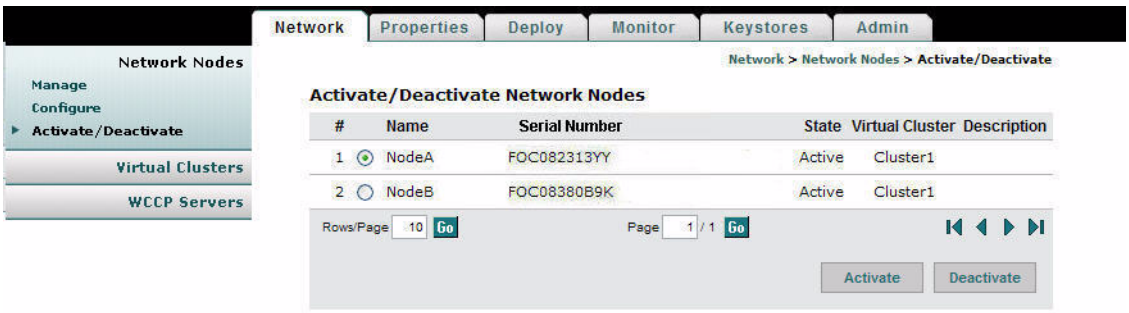
Step 4 Click the **Finish** button to save your changes, then go to **Network > Virtual Clusters > Manage** to verify that the cluster was configured. Figure 3-16 shows the Manage Virtual Clusters page.

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



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

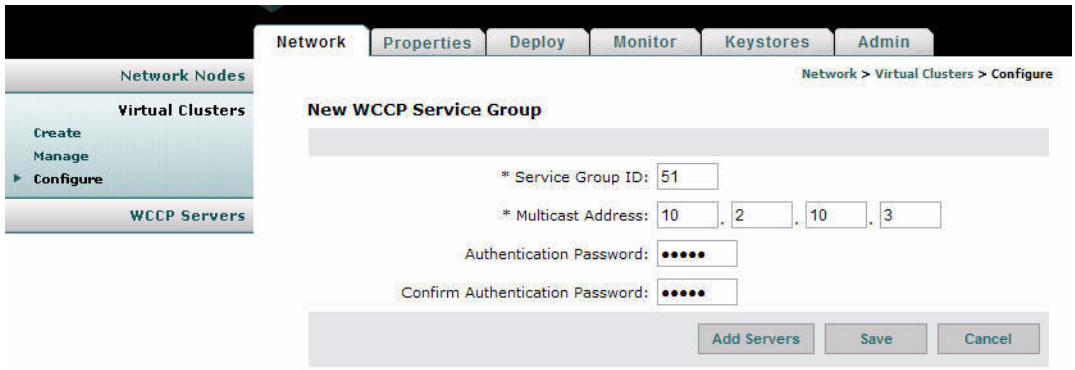


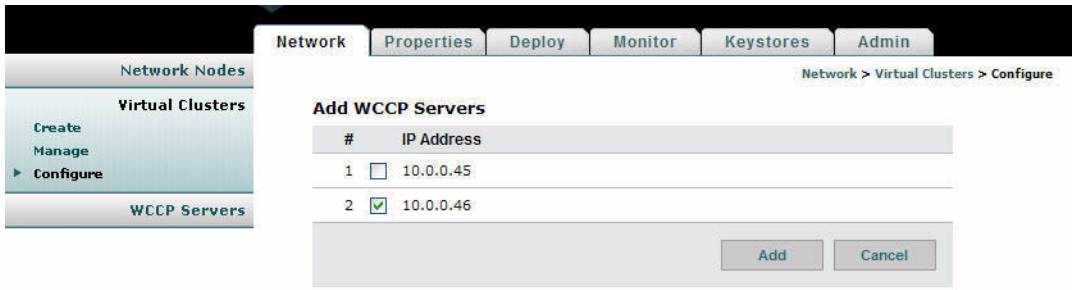
Table 3-6 shows the entries available on the New WCCP Service Group page.

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.

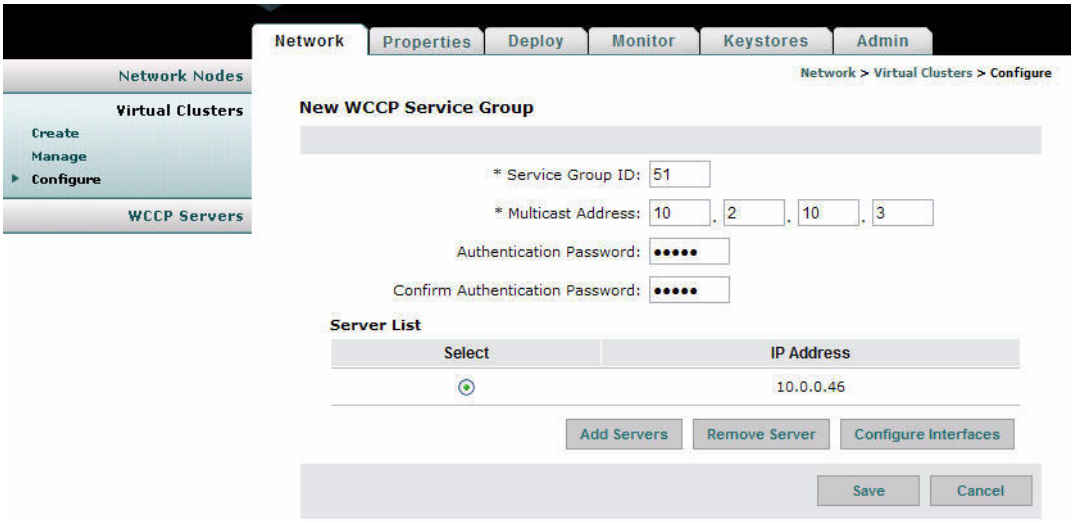
Step 2 After completing the entries, click the **Add Servers** button. This loads the a page that lists available WCCP servers, as shown in Figure 3-19.

Figure 3-19 Add WCCP Servers



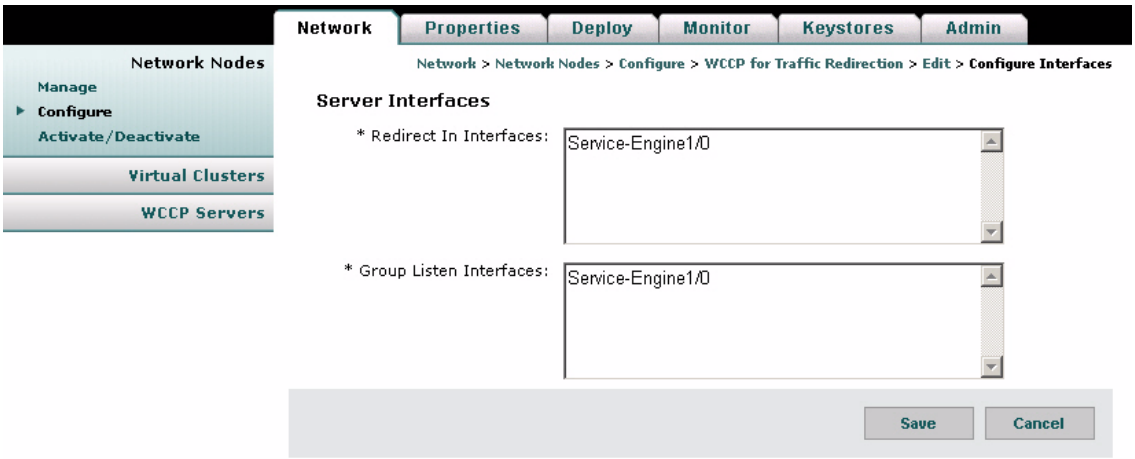
Step 3 Choose one or more servers, then click the **Add** button. The servers are added to the WCCP service group, as shown in Figure 3-20.

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

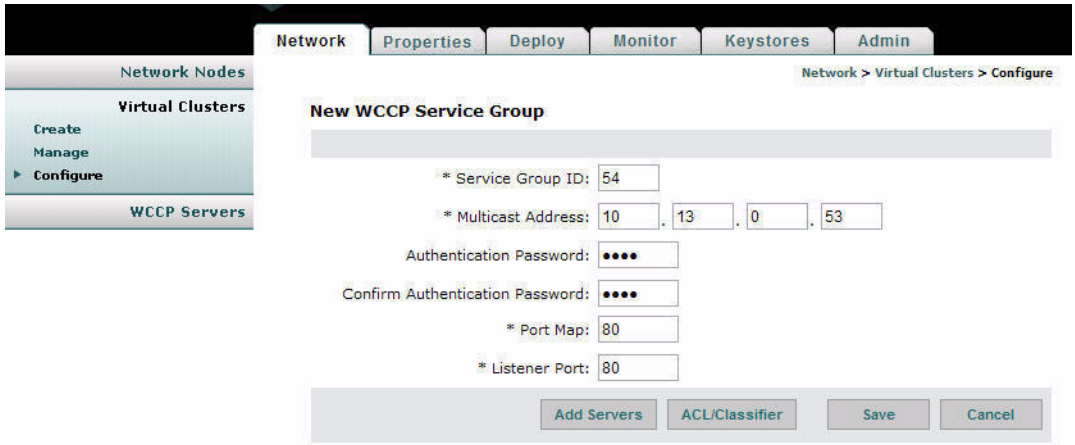


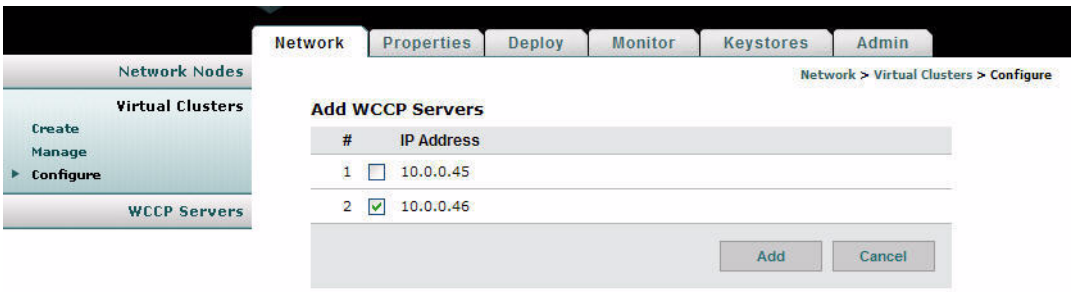
Table 3-5. shows the entries available on the New WCCP Service Group page.

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.

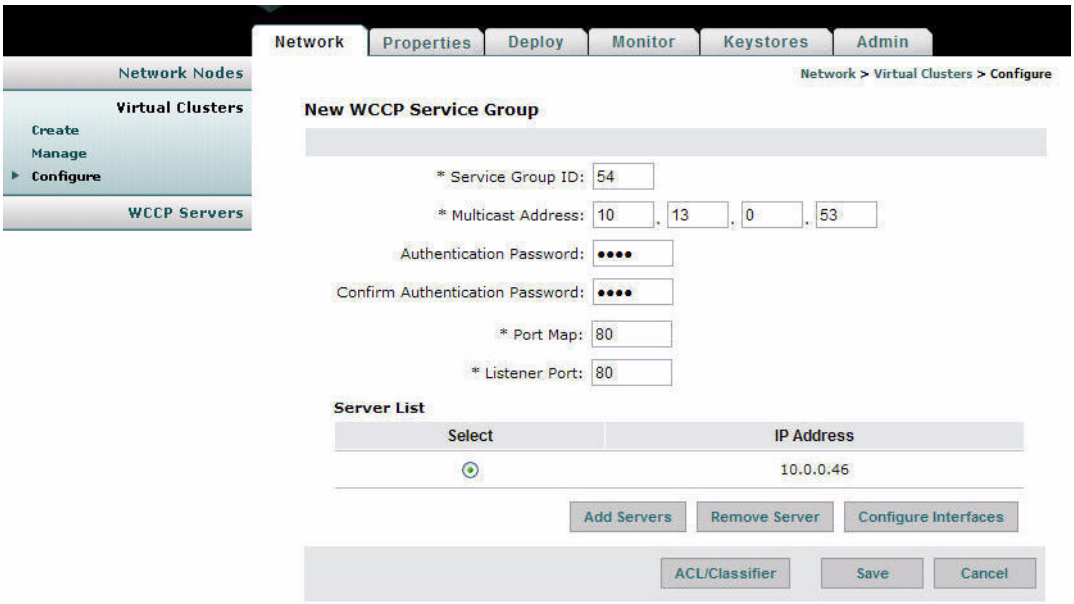
Step 2 Complete the entries as appropriate for your network, then click the **Add Servers** button. This loads a page that lists available WCCP servers, as shown in Figure 3-23.

Figure 3-23 Add WCCP Servers



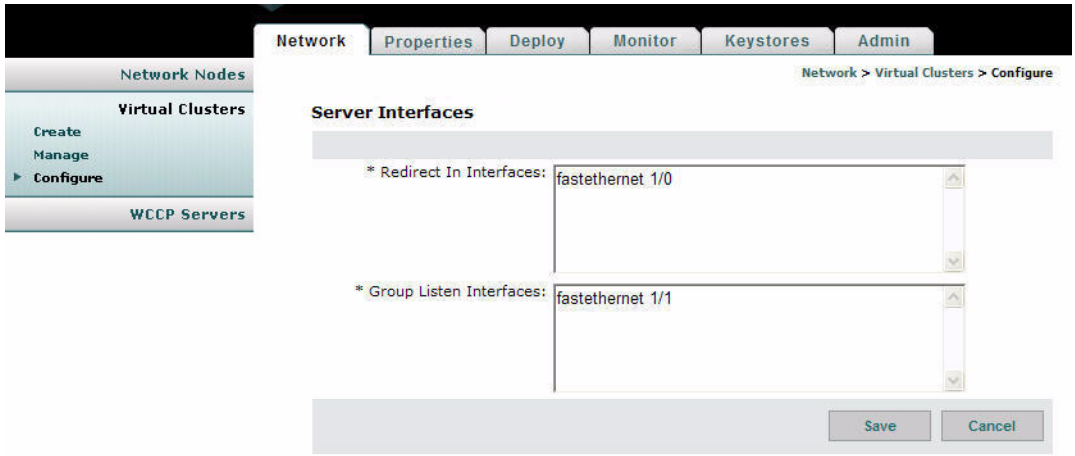
Step 3 Choose one or more servers, then click the **Add** button. The servers are added to the WCCP service group, as shown in Figure 3-24.

Figure 3-24 New WCCP Service Group



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.

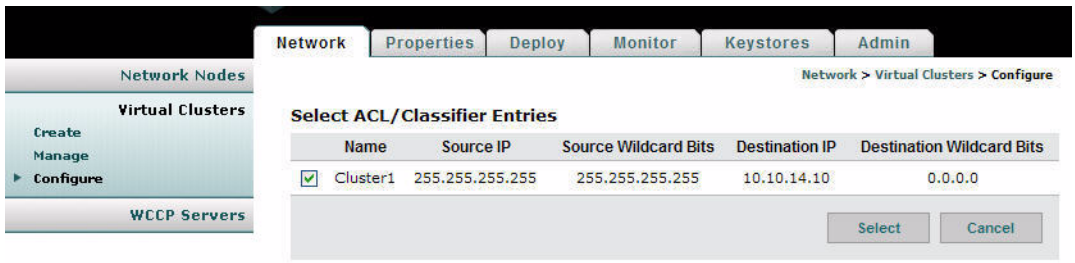
Figure 3-25 Server Interfaces



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

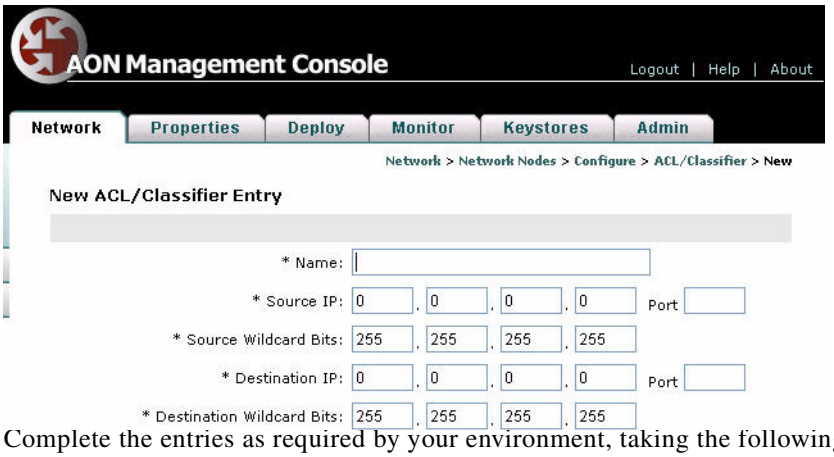
An ACL/Classifier contains an ordered list of access control entries. Each entry contains a source and destination IP address that are matched against the contents of a packet to determine if messages are to be redirected by WCCP. ACL/Classifiers are also used for message classification.

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



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

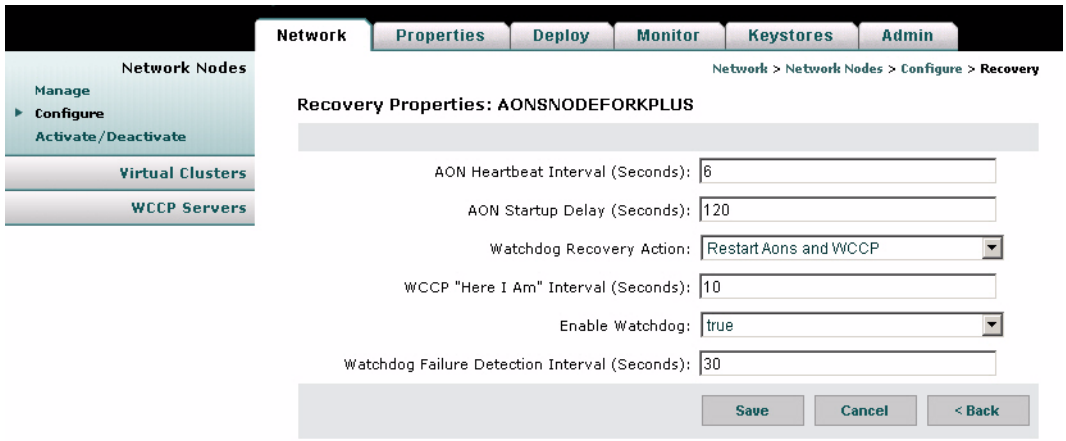


Table 3-6. shows the entries available on the Recovery page.

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 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 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

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

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

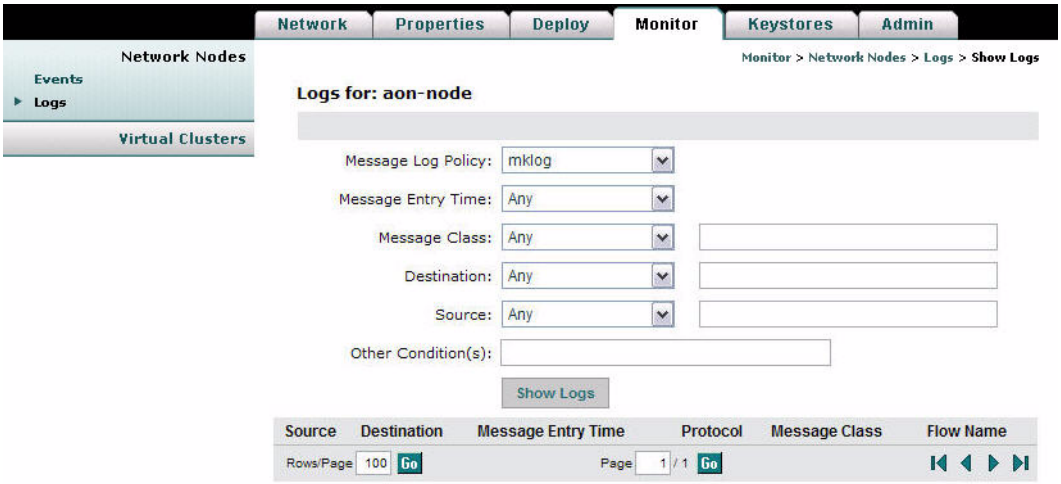
Viewing Logs

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



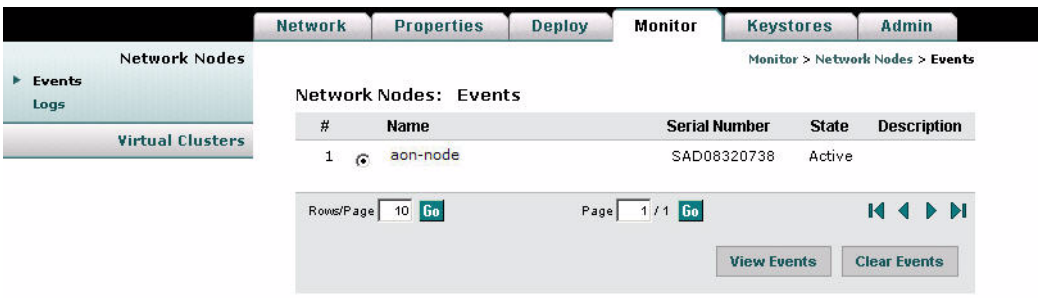
Viewing Events

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



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. Additional AMC properties related to security, authentication, and authorization are in Chapter 5, "Managing AON Security."

This chapter includes the following sections:

- Monitoring Activity, page 4-2
- Adjusting Quality and Performance, page 4-7
- Working with Message Content, page 4-11
- Controlling Message Delivery, page 4-14
- Working with Adapters, page 4-21
- Working with Message Transport, page 4-24
- Connecting to Databases, page 4-49

Monitoring Activity

Bladelet Monitoring Property

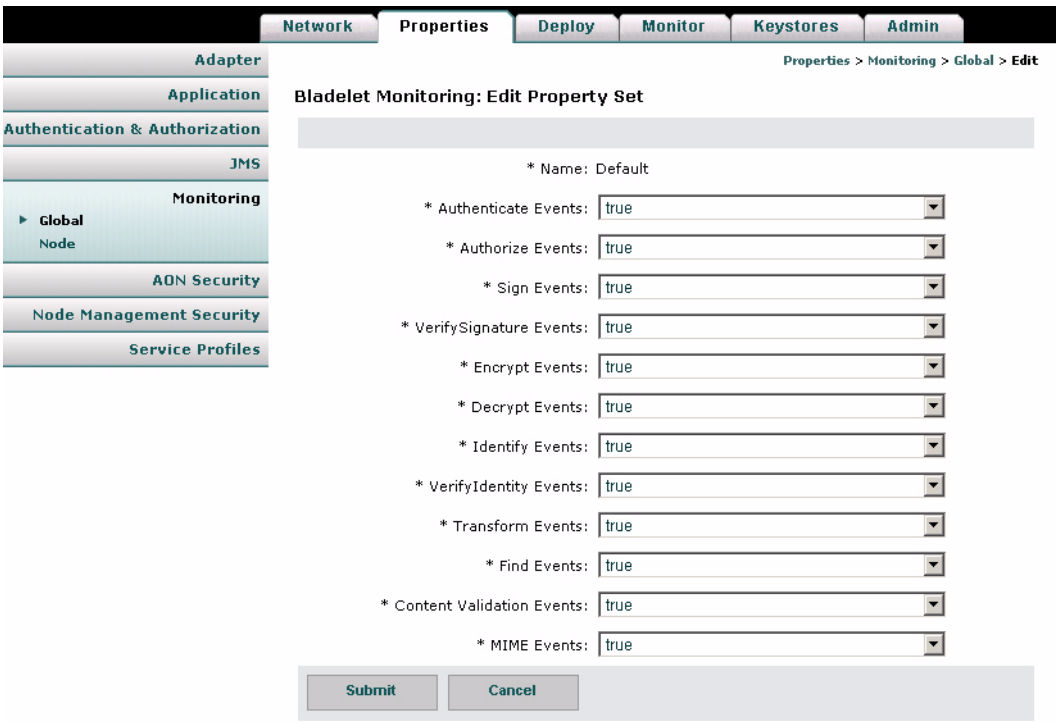
The Bladelet Monitoring Property configures which events are stored for retrieval using the screen at **Monitor > View Events**. You can configure this property globally, or you can apply it to individual nodes.

How to Get There

Go to **Properties > Monitoring.**

Figure 4-1 shows the Monitoring Property page.

Figure 4-1 Bladelet Monitoring Property



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

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 Sever (database) for AON message logging, The requirements for this external database are summarized below.

  - Page size >= 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

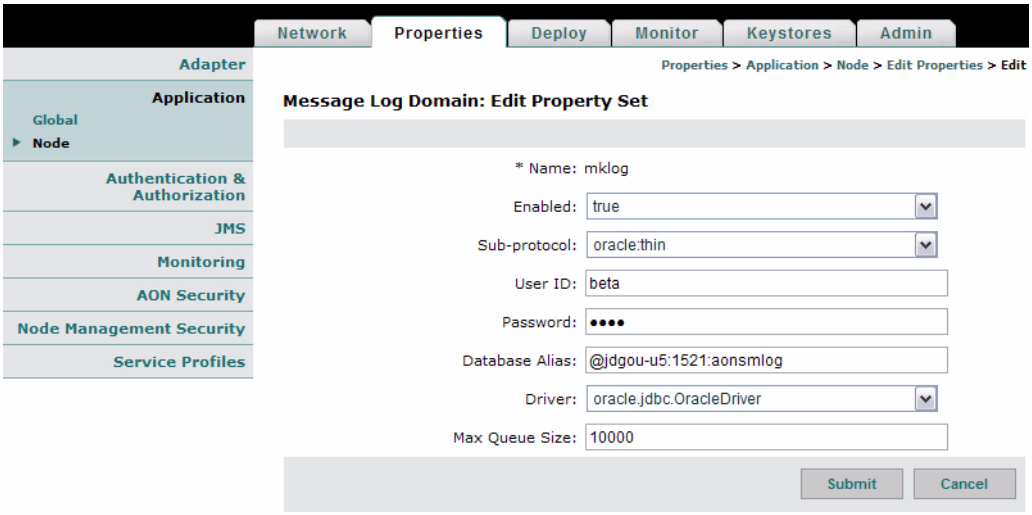
After a database as been configured, you can configure Message Log Domain Property. This is a device level property.

How to Get There

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

Figure 4-2 shows the Message Log Domain Property page.

Figure 4-2 Message Log Domain Property



Data to Enter

The Message Log Domain Property page includes the entries described in Table 4-1.

Table 4-1 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.

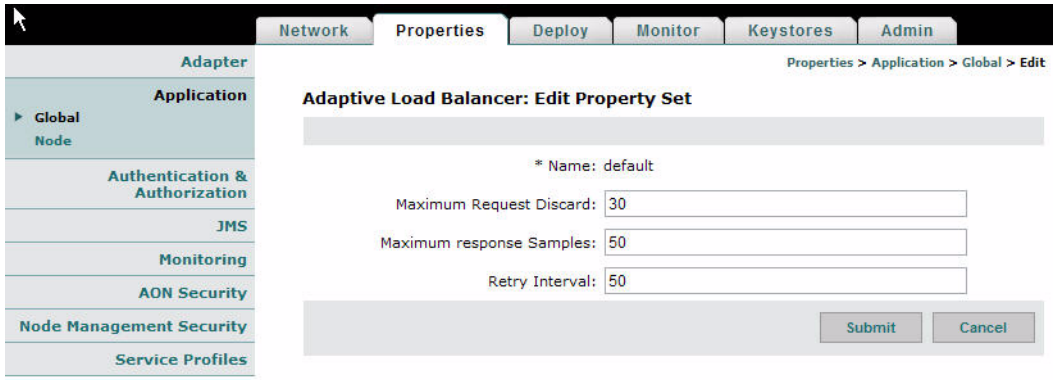
Table 4-1 Message Log Domain Property Entries (continued)

Entry	Description
Database alias	Alias pointing to the database. This value depends on the configuration of the database. The format for this entry is <*IP address*> **:** <*port*> **:** <*name of database*> The following are examples: • Oracle**—@10.1.1.1:1521:aonmlog** • Sybase**—10.1.1.2:5000/aonmlog** The last part in the alias is the name of the database instance. The message log schema should be provided by your database administrator.
Driver	The JDBC driver name. AON supports the following two drivers: • Oracle**—oracle.jdbc.OracleDriver** • Sybase**—com.sybase.jdbc2.jdbc.SybDriver**
Max Queue Size	Maximum size of the Message Log queue.

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 4-2.

Table 4-2 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.

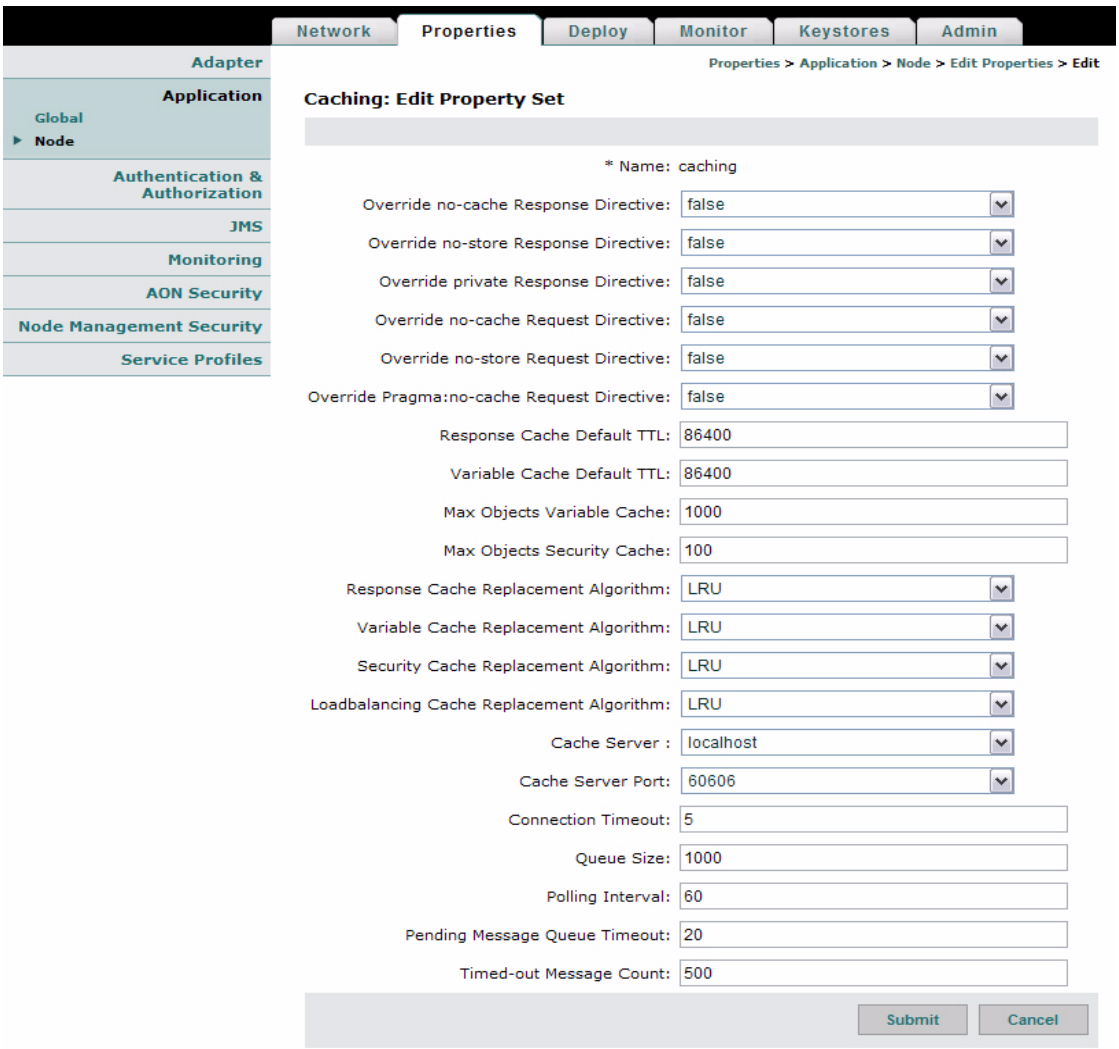
Adjusting Quality and Performance

AON allows you to measure and control runtime control quality and performance for message types that you specify.

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 4-4 shows the Caching Property page.

Figure 4-4 Caching Property



Data to Enter

The Caching Property page includes the entries described in Table 4-20.

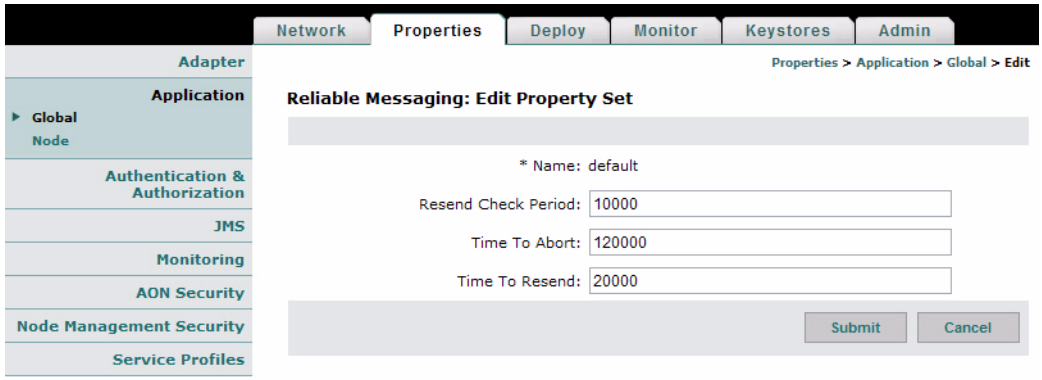
Table 4-3 Entries on Caching Property

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.

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



Data to Enter

The Reliable Messaging Property page includes the entries described in Table 4-4.

Table 4-4 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.

Application QOS

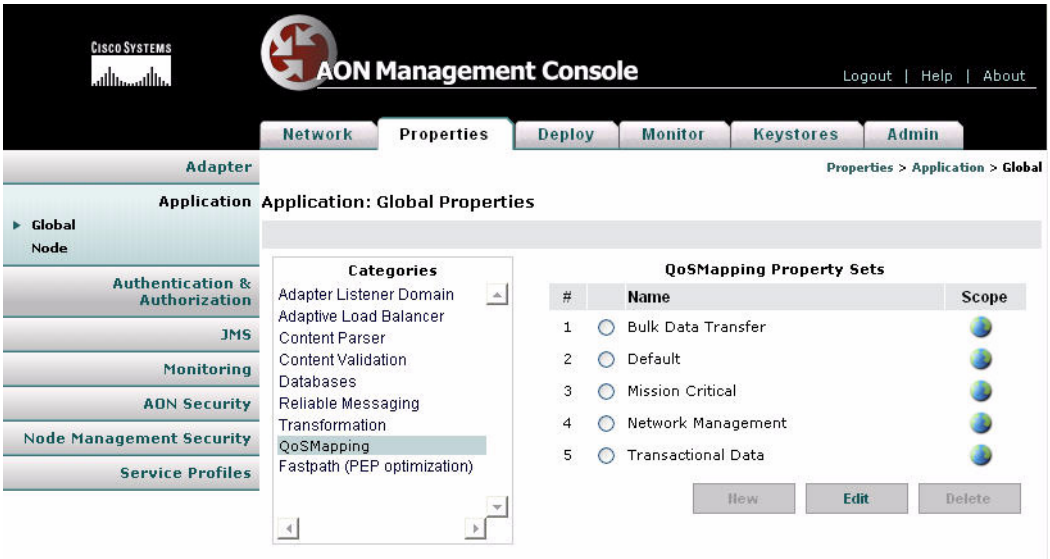
The Application QOS feature enables AON to prioritize message processing based on the Differentiated Services Code Point (DSCP) contained in the IP header. Use the QoSMapping page in AMC to define appropriate DSCP values for the following categories (listed in priority order):

- Bulk data transfer
- Default
- Mission critical
- Network management
- Transactional data

These categories are available to PEP developers who use the Application QOS bladelet.

How to Get There

Go to **Properties > Application > Global**, then select QoSMapping.



Actions to Take

Click the radio button for the property set you want to change, then click the **Edit** button. On the screen that follows, enter the new DSCP value and click the **Submit** button.

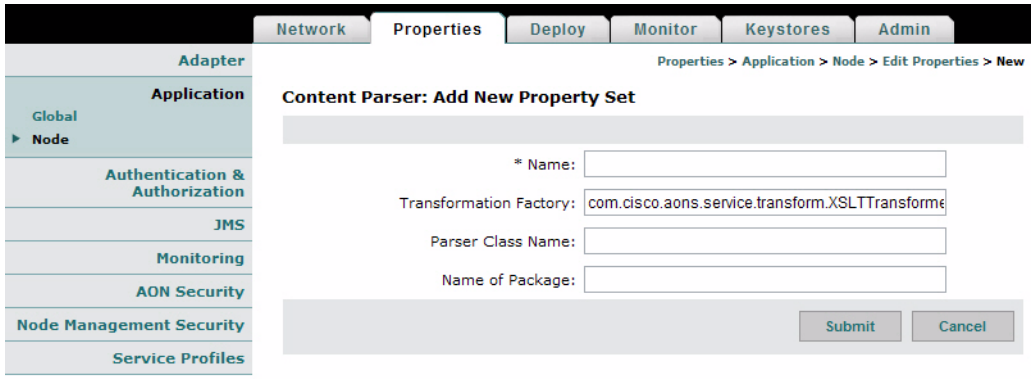
Working with Message Content

AON allows you to work with the content of your messages based on properties that you set.

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 4-6 shows the Content Parser Property page.

Figure 4-6 Content Parser Property



Data to Enter

The Content Parser Property page includes the entries described in Table 4-5.

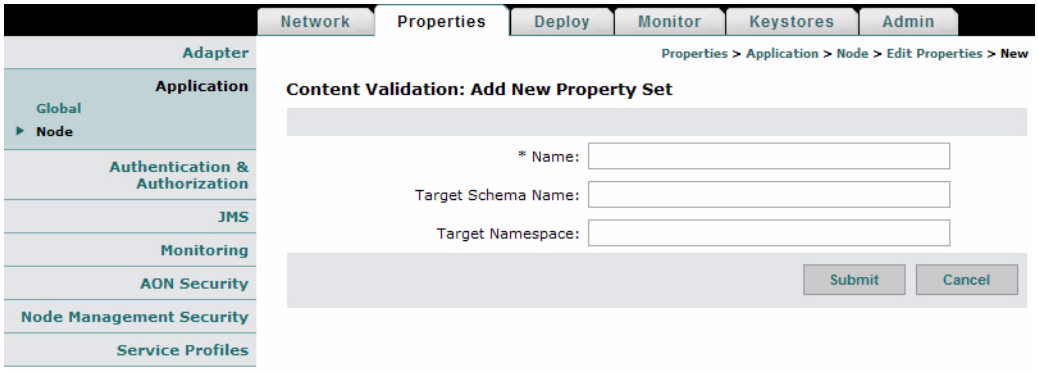
Table 4-5 Entries on Content Parser Property

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 4-6 shows the Content Validation Property page.

Figure 4-7 Content Validation Property



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.

Working with XSL Transformation

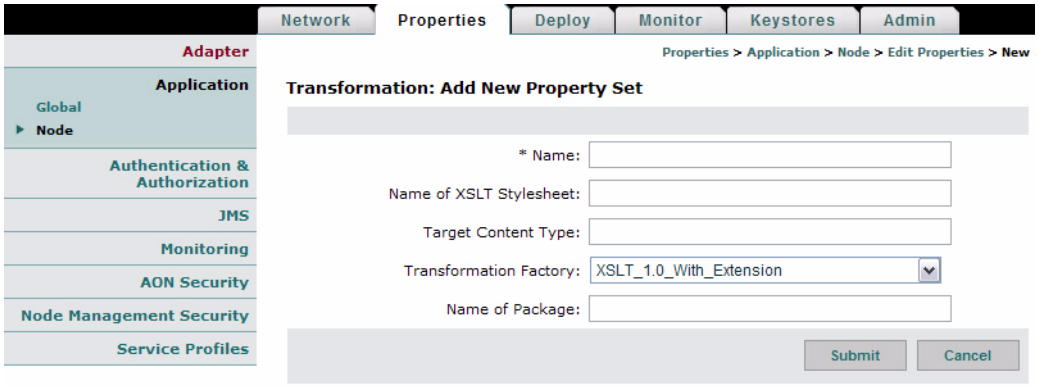
This property configures AON to perform XSL transformation (XSLT). The Transformation property determines the document style sheet, target content type, and transformation package. This property can be configured globally or for individual nodes.

How to Get There

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

Figure 4-8 shows the Transformation Property page.

Figure 4-8 Transformation Property



Data to Enter

The Transformation page includes the entries described in Table 4-7.

Table 4-7 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.

Controlling Message Delivery

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

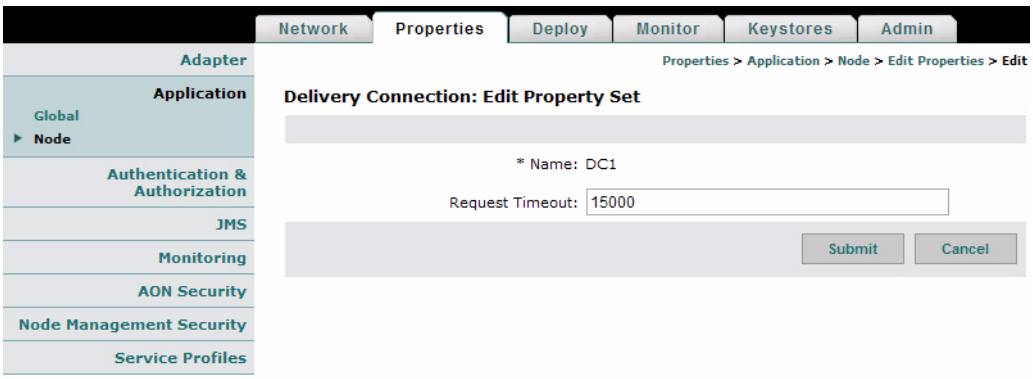
The Delivery Connection property specifies how long a message type should wait for a timeout.

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 4-8.

Table 4-8 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.

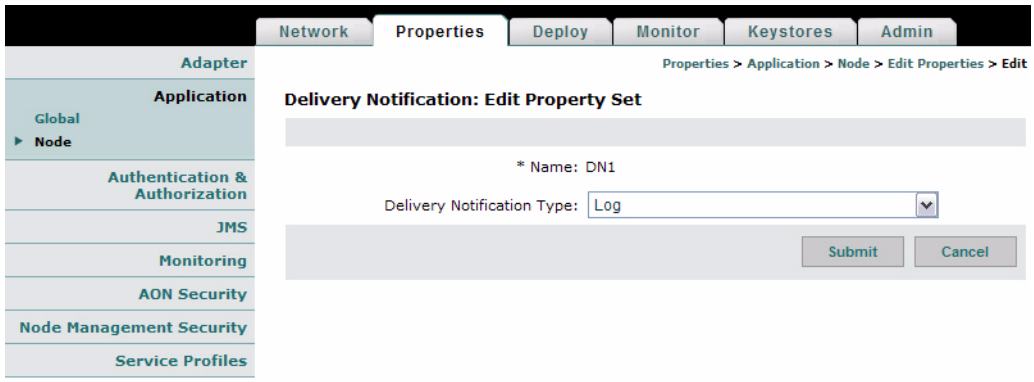
Note You must configure Configuring Delivery Connection before configuring this property.

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 4-9.

Table 4-9 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.

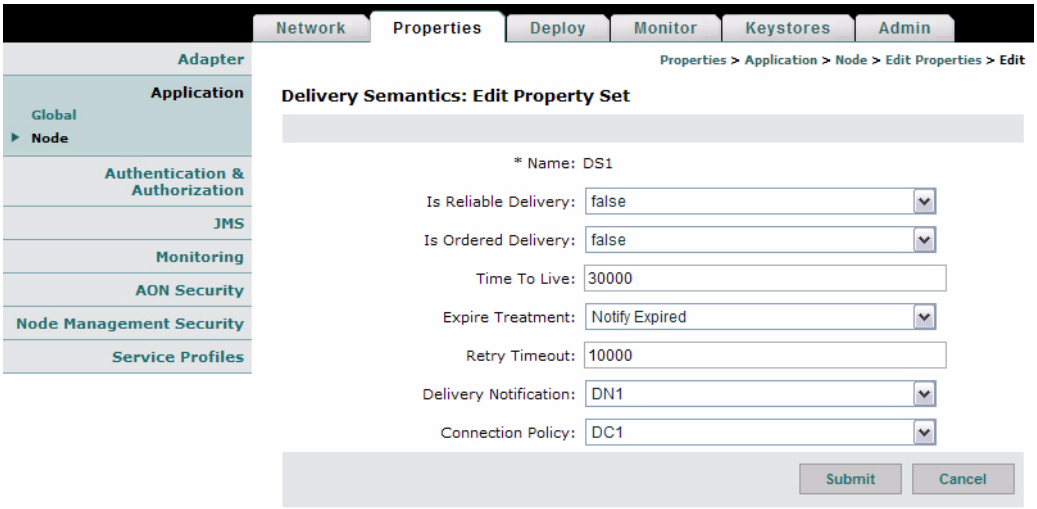
Note You must configure Configuring Delivery Connection and Configuring Delivery Notification before configuring this property.

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 4-10.

Table 4-10 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

Table 4-10 Delivery Semantics Property Entries (continued)

Entry	Description
Delivery Notification	Select an available Delivery Notification Property.
Connection Property	Select an available Delivery Connection Property.

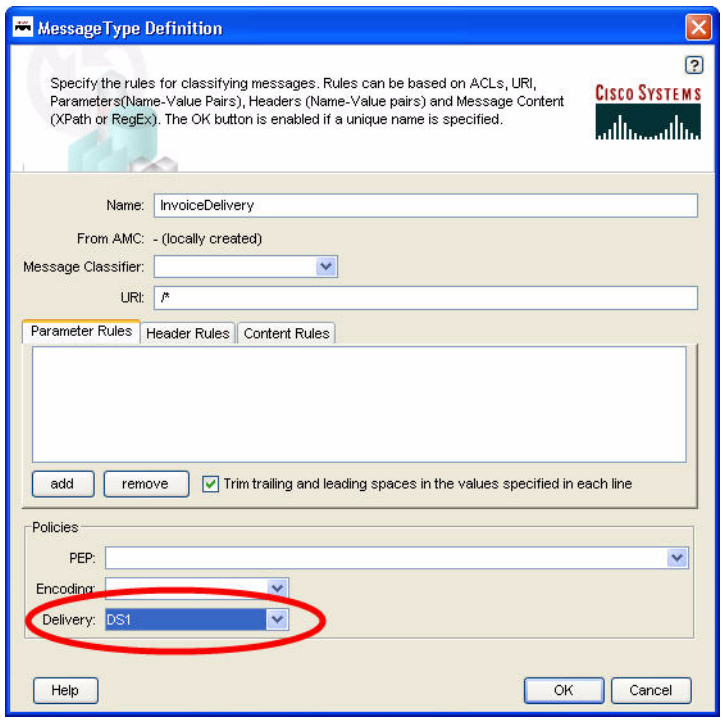
Actions to Take

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

Binding Message Delivery Properties to a Message Type

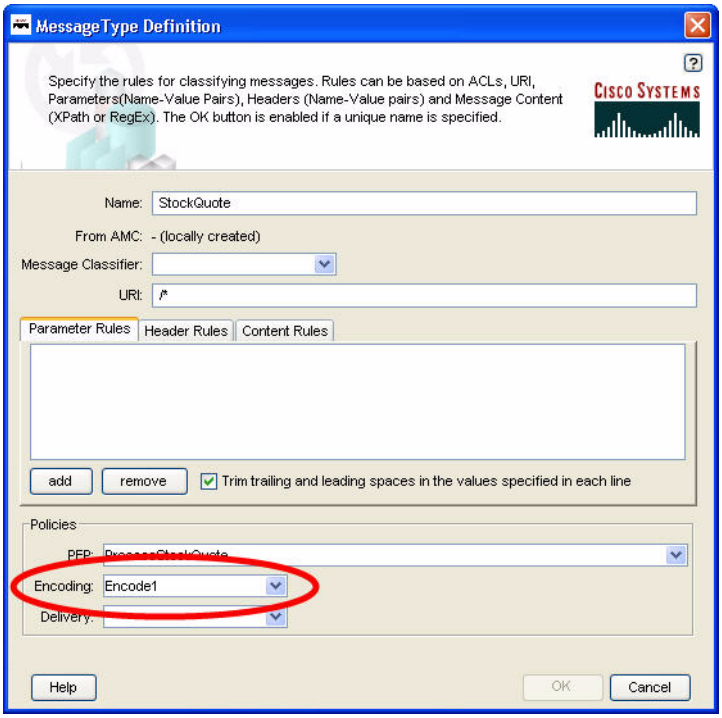
After you configure message delivery properties in the AMC, the property is available to ADS users when they configure message types. Figure 4-12 shows the ADS Message Type Properties window with the Delivery Properties drop-down list highlighted.

Figure 4-12 MDS Drop-Down List



After you configure an Encoding profile, it is available to ADS users when they configure a message type. See Figure 4-13.

Figure 4-13 Binding an Encoding Property to a Message Type



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.

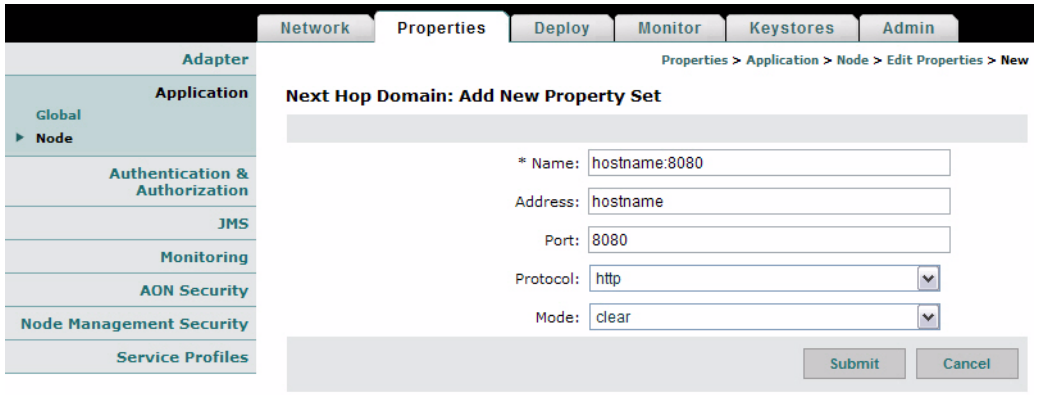
Note In a two-node scenario, configure this property on the client proxy with the configuration details necessary to route messages to the server proxy.

How to Get There

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

Figure 4-14 shows the Next Hop Domain Property page.

Figure 4-14 Next Hop Domain Property Entries



Data to Enter

The Next Hop Domain Property page includes the entries described in Table 4-11.

Table 4-11 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. *ip_address*:*port* or *hostname*:*port*
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: • **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.

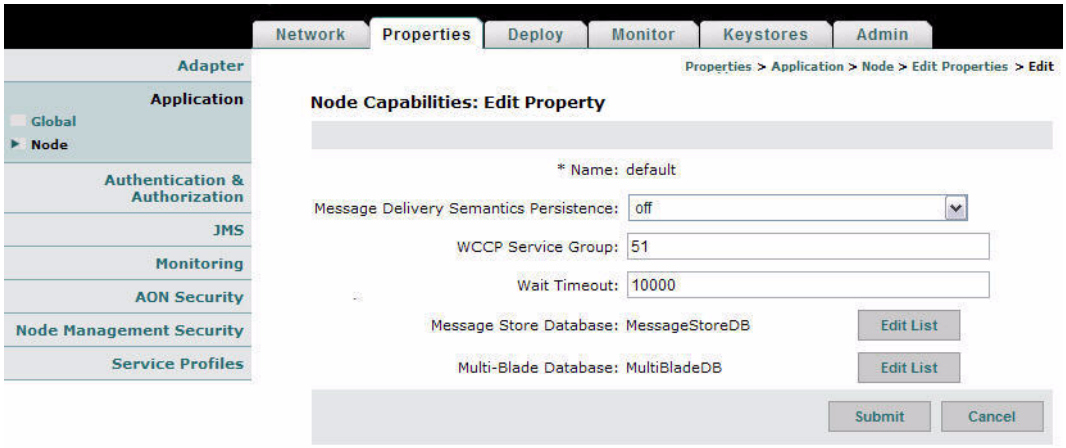
Note If message delivery persistence is to be stored in a database, you must configure two databases before you configure this property. See the "" section on page 4-6 for information on configuring a database.

How to Get There

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

Figure 4-15 shows the Node Capabilities Property page.

Figure 4-15 Node Capabilities Property



Data to Enter

The Node Capabilities property page includes the entries described in Table 4-12.

Table 4-12 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 "" section on page 4-6 to configure a database.
Multi-Blade Database	Click the Edit List button to choose an available Database

Working with Adapters

You can use AMC to control how adapters function within your AON implemetation. You can also configure additional properties and extensions for each adapter. For more details about adapters, properties, and extensions, see the *AON Programming Guide.*

Adapter Registry

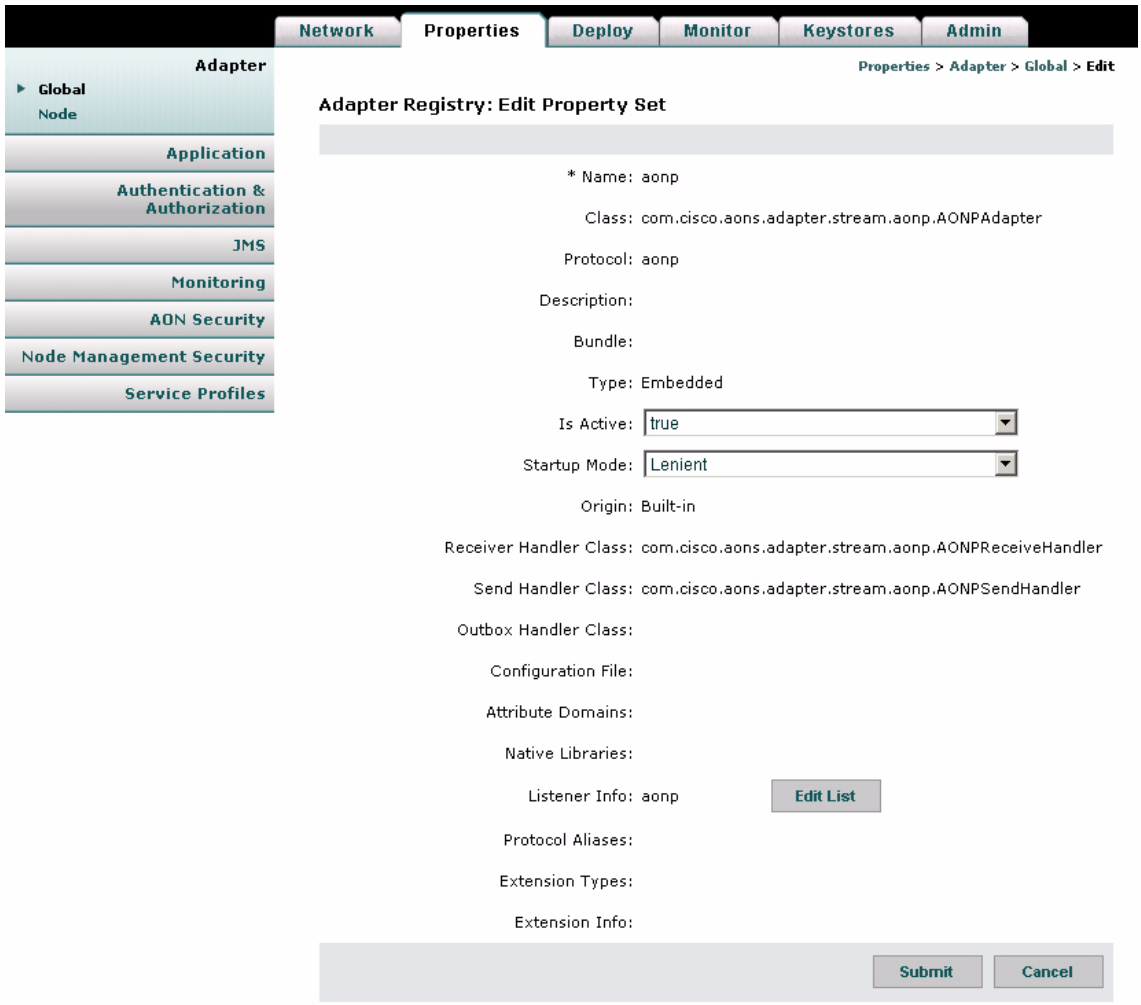
The Adapter Registry page enables you to manage the properties of both built-in and custom adapters. You can activate or deactivate an adapter, change the start-up mode, and change the protocol to be used by the adapter.

How to Get There

Go to **Properties > Adapter.**

Figure 4-16 shows the Adapter Registry page.

Figure 4-16 Adapter Registry



Adapter Listener Domain

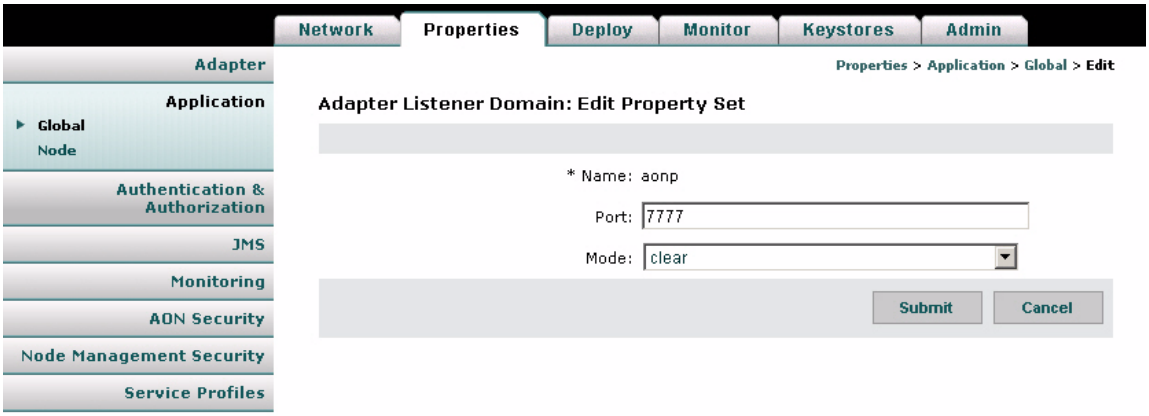
Adapter Listener Domain enables you to configure the listening parameters of an adapter. You can specify the port on which the adapter listens, and you can choose either clear or secure communication.

How to Get There

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

Figure 4-17 shows the Adapter Listener Domain page. For more information about adapters, see the *AON Programming Guide*.

Figure 4-17 Adapter Listener Domain



Service Profiles for Adapters

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.

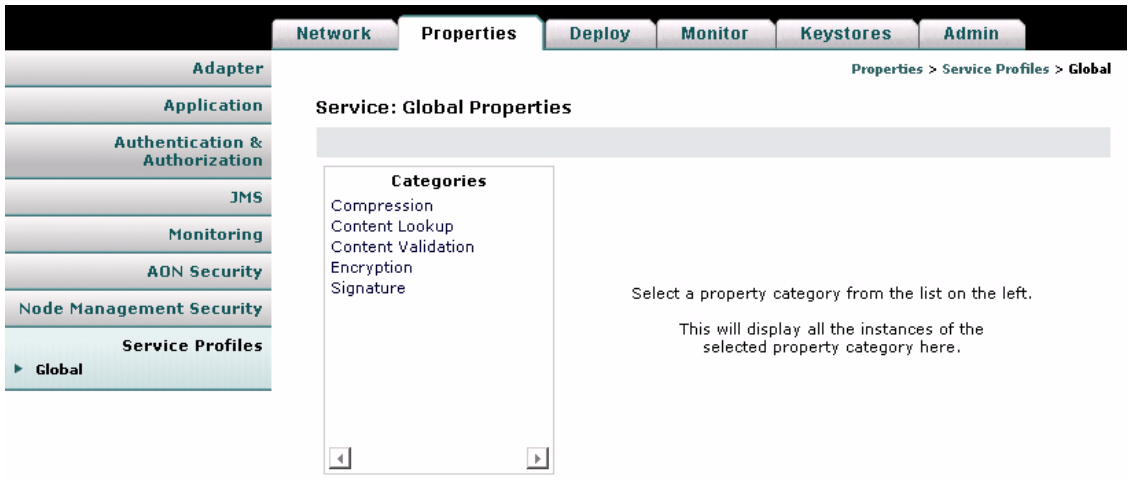
For more details about custom bladelets, custom adapters, and external services, see the *AON Programming Guide.*

How to Get There

Go to **Properties > Service Profiles.**

Figure 4-18 shows the Service Profile page.

Figure 4-18 Service Profiles

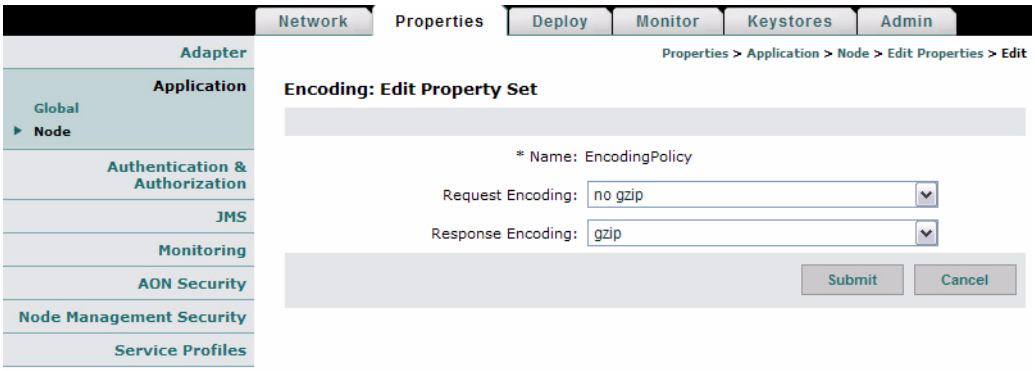


Working with Message Transport

Encoding

The Encoding property enables you to configure AON nodes to compress outgoing traffic. Figure 4-19 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 4-19 Encoding Property



Data to Enter

The Encoding property page includes the entries described in Table 4-13.

Table 4-13 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.

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 4-25
2. JMS Source Property, page 4-26
3. JMS Reply To, page 4-27
4. JMS Connections Property, page 4-28
5. JMS Naming Property, page 4-29

JMS Destination Property

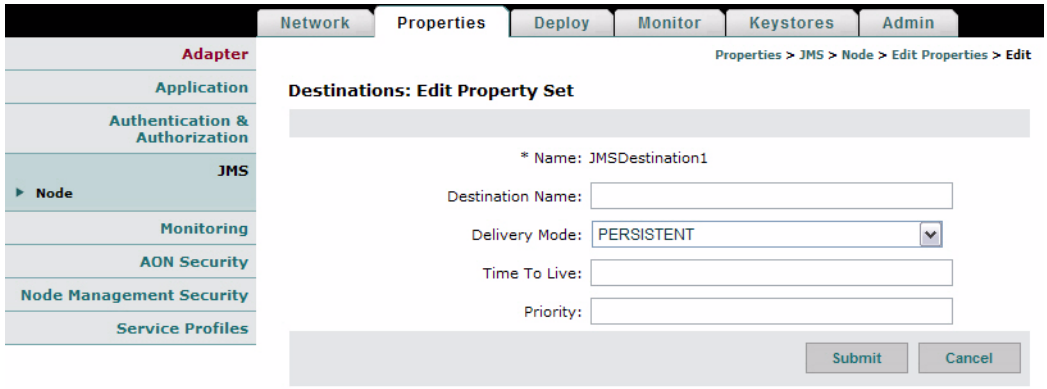
The JMS Destination Property enables you to specify a new destination for JMS messages.

How to Get There

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

Figure 4-20 shows the JMS Destination Property page.

Figure 4-20 JMS Destination Property



Data to Enter

The JMS Destination Configuration page includes the entries described in Table 4-14.

Table 4-14 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

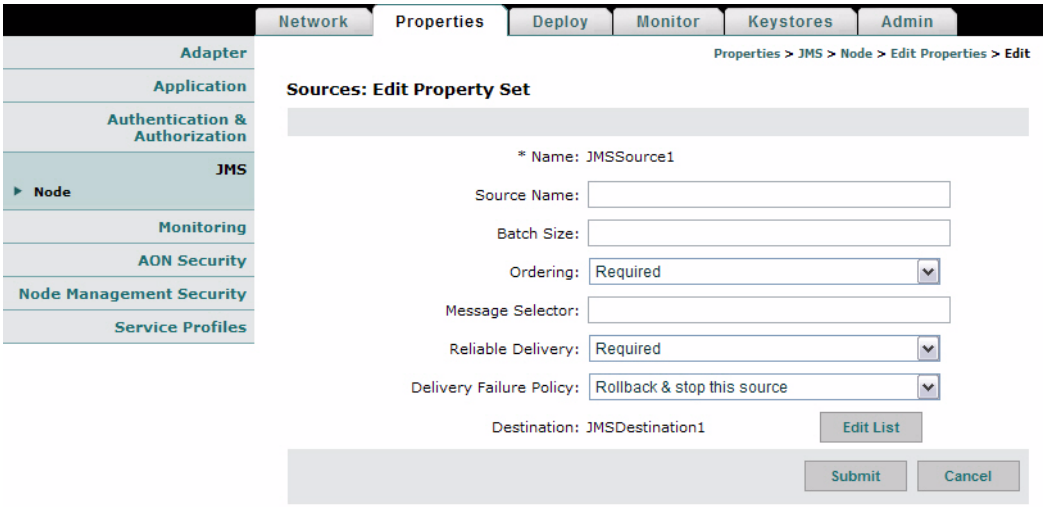
The JMS Source Property Page enables you to specify a new source for JMS messages. It requires you to specify a JMS Destination, which you should have configured in the previous section.

How to Get There

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

Figure 4-21 shows the JMS Source Property page.

Figure 4-21 JMS Source Property



Data to Enter

The JMS Source Configuration page includes the entries described in Table 4-15.

Table 4-15 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

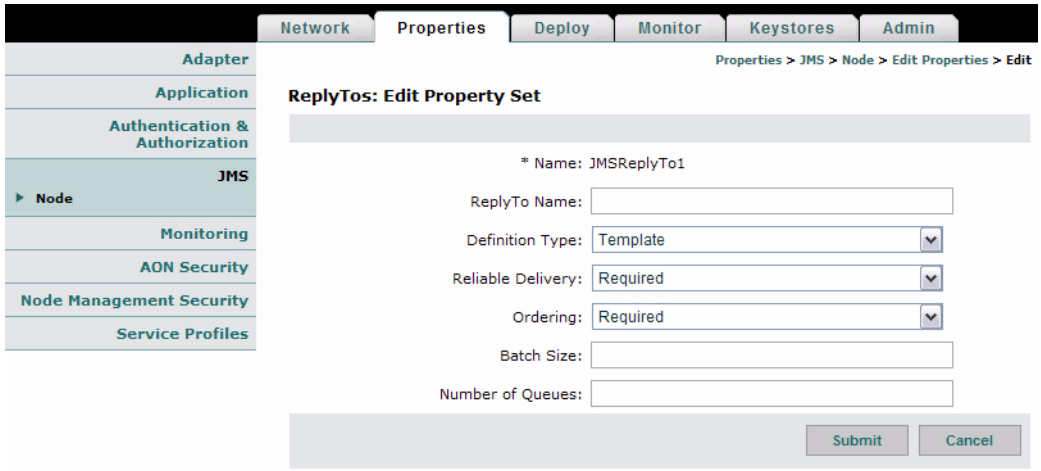
The JMS ReplyTo property enables you to specify a new reply queue to be used by JMS clients.

How to Get There

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

Figure 4-22 shows the JMS Reply To Property page.

Figure 4-22 JMS Reply To Property



Data to Enter

The JMS Reply To Property page includes the entries described in Table 4-16.

Table 4-16 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.

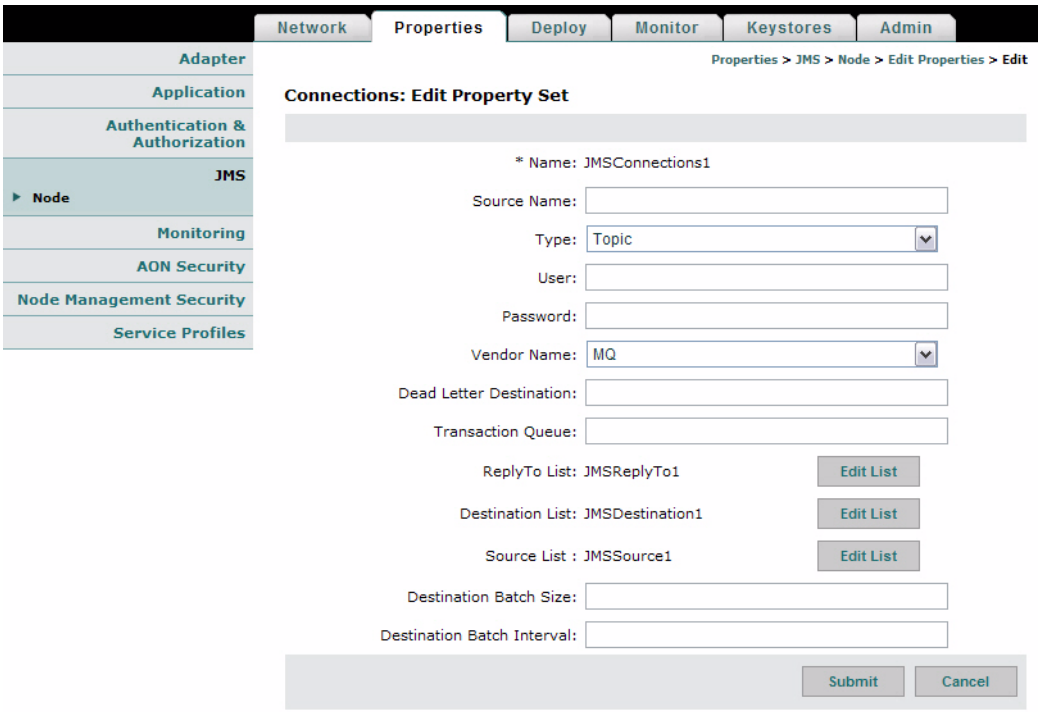
JMS Connections Property

How to Get There

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

Figure 4-22 shows the JMS Connection Property page.

Figure 4-23 JMS Connection Property



Data to Enter

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

Table 4-17 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 4-17 JMS Connection Configuration Entries (continued)

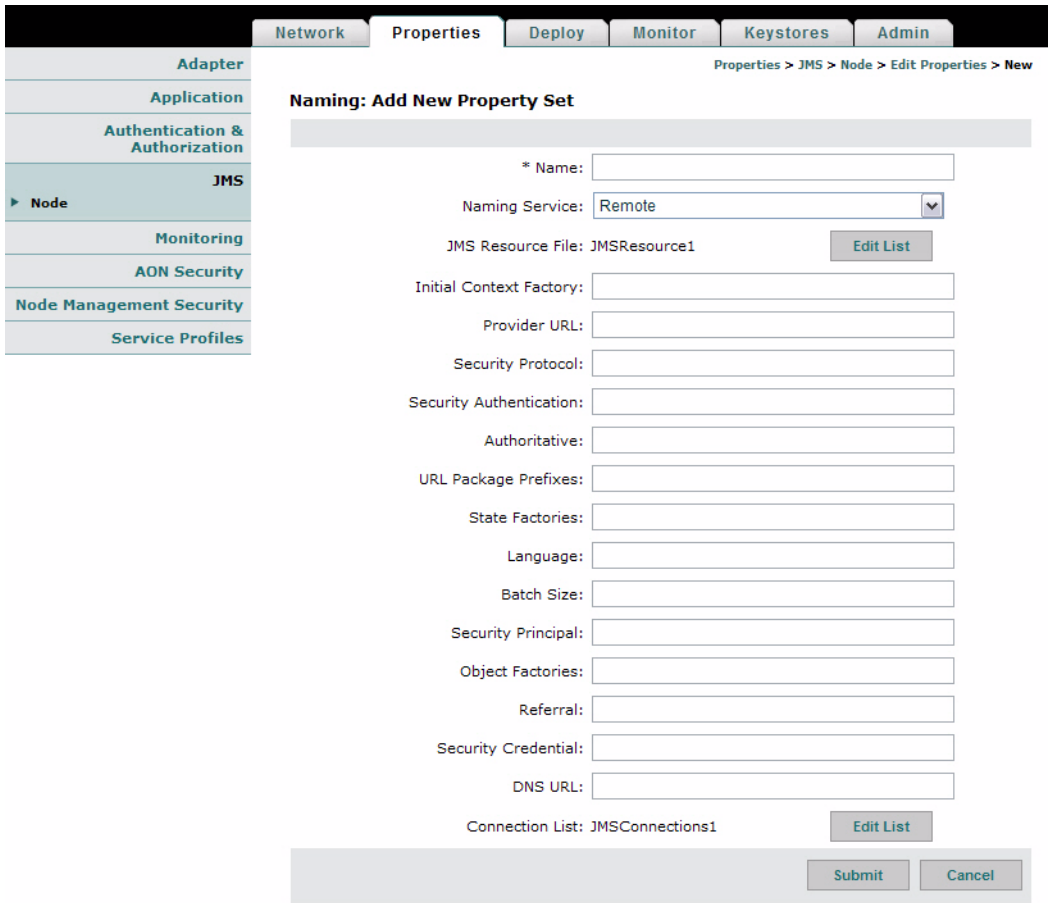
Entry	Description
Source List	Click the Edit List button to make a selection.
Destination Batch Size	Size of the batch at the destination broker.
Destination Batch Interval	Specified in milliseconds.

JMS Naming Property

Figure 4-22 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 4-24 JMS Naming Property



Data to Enter

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

Table 4-18 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.

Configuring Cisco AON Promiscuous Mode

Promiscuous mode (PMode) enables out-of-band message processing using a Cisco AON node. It provides the capability to receive and process messages without introducing latency in the flow of inline network traffic, supporting out-of-band monitoring and analysis.

Prerequisites for Promiscuous Mode

- Ensure that AMC and all AON nodes are correctly configured and running.
- Ensure that any nodes to be used in this procedure are active on AMC.
- Ensure that you have available a valid framing extension. HTTP framing extensions, in addition to FIX extensions, are available for download with other AON software.
- Ensure that the switch or router that hosts any node using PMode meets the requirements in Table 19.

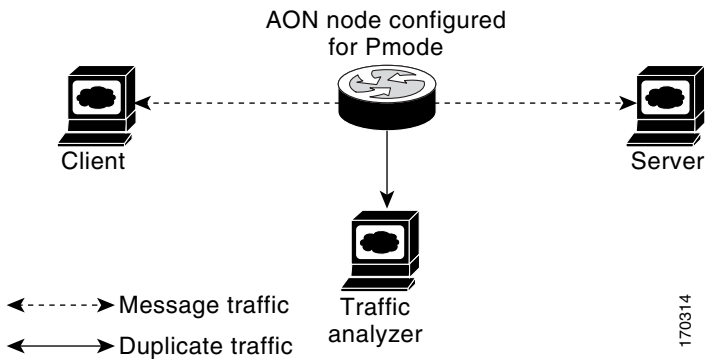
Table 19 PMode Operating System Requirements

Platform	Required Operating System
AON-SM with Supervisor Engine 2	Catalyst OS Release 8.5(3) recommended **Note** Minimum requirement is Catalyst OS Release 8.4(2a).
AON-SM with Supervisor Engine 720	PMode not supported
AON-NM	Cisco IOS Release 12.3(14)T1

Information About Promiscuous Mode

Promiscuous mode enables an AON node to monitor traffic between a client and server without affecting traffic flow. Messages are not terminated by the AON node. Instead, packets are duplicated and forwarded, in the form of framed application messages, to a third-party application. Once forwarded, they can be analyzed or other processed. Figure 25 shows a sample runtime topology where an AON node is using PMode to forward traffic to a traffic analyzer.

Figure 25 Promiscuous Mode Sample Topology



The sample topology shown in Figure 25 requires the following runtime components:

- **Client**—sends traffic to the server. The client is configured with a default gateway IP address that is assigned to an interface on the router hosting the AON node.
- **Server**—receives traffic from the client through the AON node. The server is configured with the default gateway IP address of the router interface into which it connects.
- **AON node**—the router or switch, configured with IP addresses and port numbers for the traffic to be captured. The node makes copies of this traffic and passes it to AON. AON in turn processes these messages, packages them into AON monitoring messages (AMM), and sends them to the analyzer. Depending on the node's location in the network, the AON node requires a specific IP and VLAN configuration to perform this function.
- **Traffic analyzer**—receives duplicate traffic from the AON node. The analyzer is a third-party or customer-provided component. It is not part of the AON product.

Pmode Deployment Options

You can run promiscuous mode both on AON-NM and on AON-SM.

When you use AMC to deploy PMode on an AON-NM, PMode is enabled, by default, on the external interface—with the option of changing to an internal monitoring interface. You can choose to use either of the interfaces, or set up a deployment that uses both interfaces simultaneously. For information on changing to an internal monitoring interface, see the section Enabling the Internal Interface on an AON-NM, page 4-33.

When you use AMC to deploy PMode on an AON-SM, PMode is enabled on Gigabit Ethernet 3, a deployment for which you must configure either SPAN or VACL for forwarding the traffic.

The following options available to copy the traffic to AON:

- Configure RITE (Router IP Traffic Export) at the router.

  AON can reside in the same router you configured for RITE, or it can reside in a separate router. If AON resides in a separate router from the RITE-configured router, AON should be deployed within the same VLAN as the RITE-configured router.
- Use SPAN or VACL in a switch to capture and direct traffic to AON.

To configure RITE, see the following:

- http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a0080455b94.html

To configure either SPAN or VACL see the following:

- SPAN—http://www.cisco.com/warp/public/473/41.html
- VACL—http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/vacl.htm

Note Use either SPAN or VACL, but not both.

For information on SPAN and on VACL configurations, see the following documents:

- SPAN—http://www.cisco.com/warp/public/473/41.html
- VACL—http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/vacl.htm

How to Configure Promiscuous Mode

PMode configuration involves the following:

- Enabling the Internal Interface on an AON-NM, page 4-33 (optional)
- Configuring PMode Adapter on AMC, page 4-33 (required)

Enabling the Internal Interface on an AON-NM

This optional procedure is required only if you are enabling PMode on the internal interface of an AON-NM. To configure this, complete the following steps.

Step 1 Establish a session to the AON-NM and enter configuration terminal mode.

```
aon-nm> configuration terminal
Enter configuration commands, one per line. End with exit.
```

Step 2 Use the **aon monitoring interface** command to enable the internal interface.

```
aon-nm(config)>aon monitoring interface internal
```

Step 3 Exit configuration terminal mode.

```
aon-nm(config)>exit
```

Configuring PMode Adapter on AMC

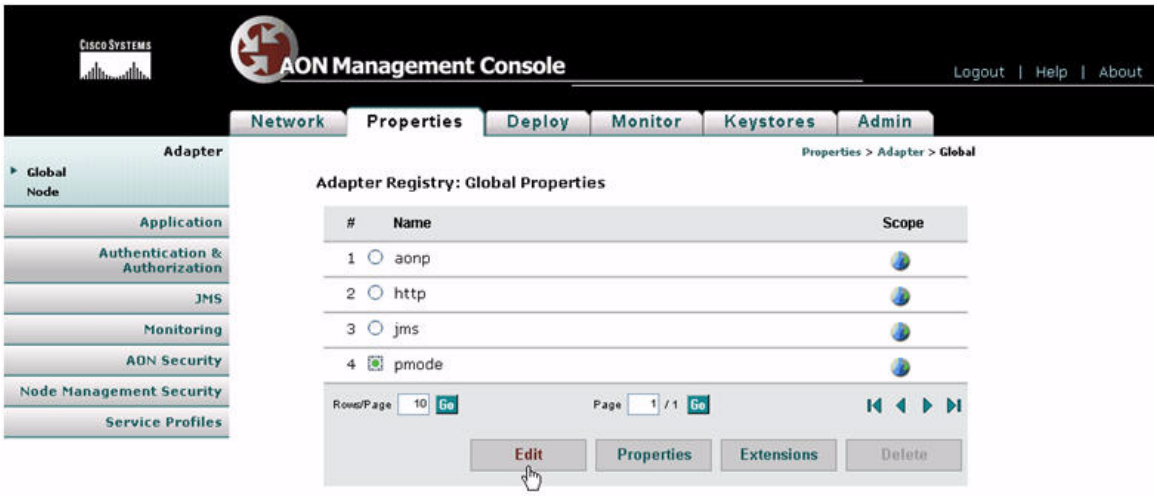
Activate the Cisco AON PMode adapter by performing the following steps.

Step 1 Click the **Properties** tab in the top menu of AMC.

Step 2 Click **Global** in the **Adapter** menu on the left side of the window. The global properties of each registered adapter are displayed as shown in Figure 26.

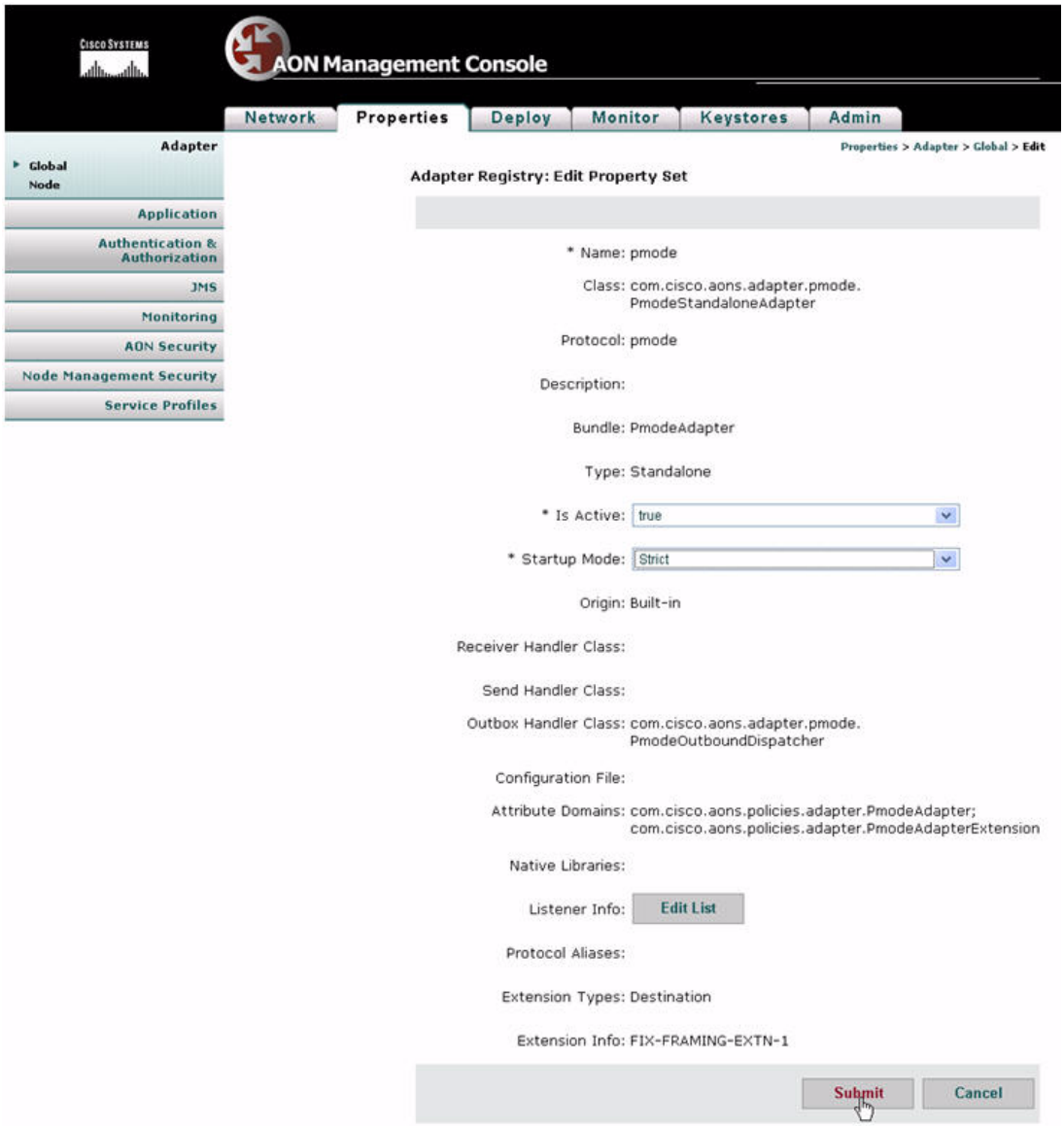
Step 3 Make sure **PMode** adapter is checked. On the bottom part of the window, click **Edit** to display the **Edit Property Set** window.

Figure 26 Enabling the PMode Adapter: Properties



Step 4 In the **Is Active** field, choose **true** as shown in Figure 27.

Figure 27 Enabling the PMode Adapter: Edit Property Set



Step 5 Click **Submit**.

Configuring the PMode Adapter

To configure the PMode adapter and deploy the changes to the node, perform the following steps:

Step 1 Click on the **Properties** Tab in the top menu of AMC.

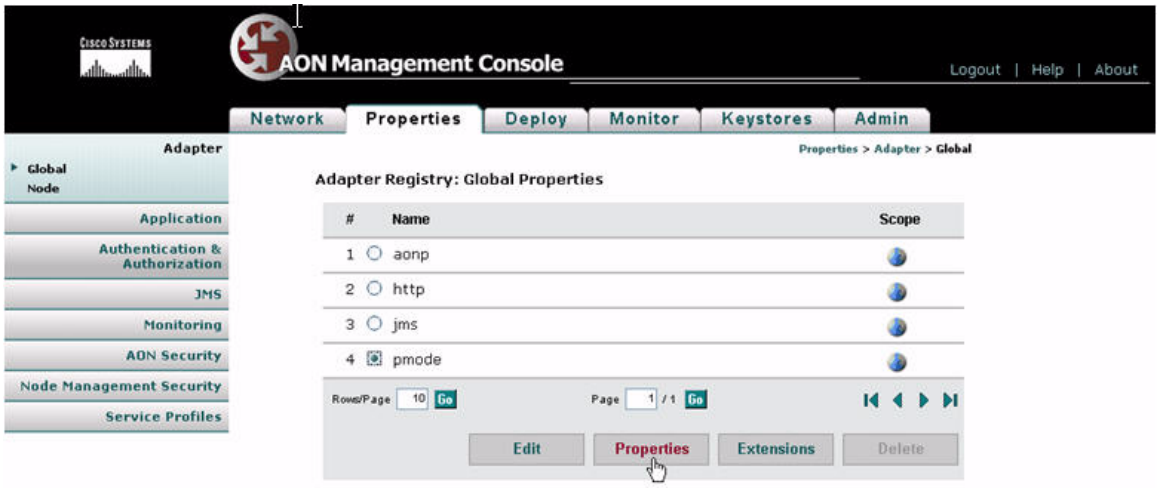
Step 2 Select the **Adapter** menu in the left pane.

Step 3 Select the sub-menu **Global** under **Adapter**.

Step 4 Select **PMode**.

Step 5 Click the **Properties** button, as shown in Figure 28.

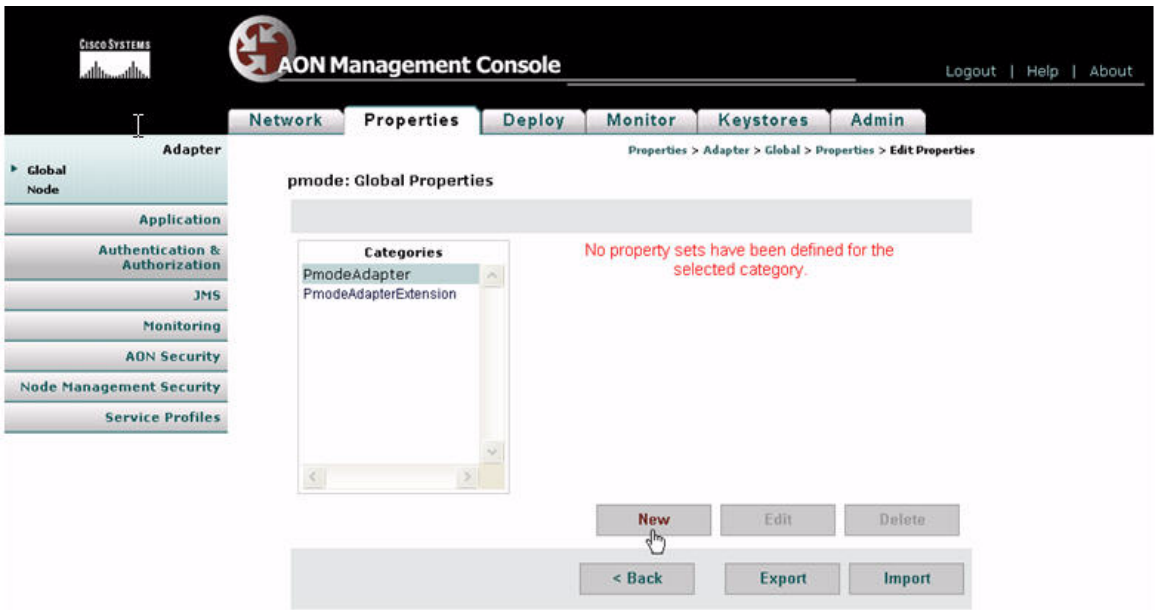
Figure 28 Configuring the PMode Adapter: Global Properties



Step 6 Select **PmodeAdapter** under **Categories**.

Step 7 Click on **New**, as shown in Figure 29.

Figure 29 Configuring the PMode Adapter: Creating New Property Set



Step 8 Enter the name as **default**.

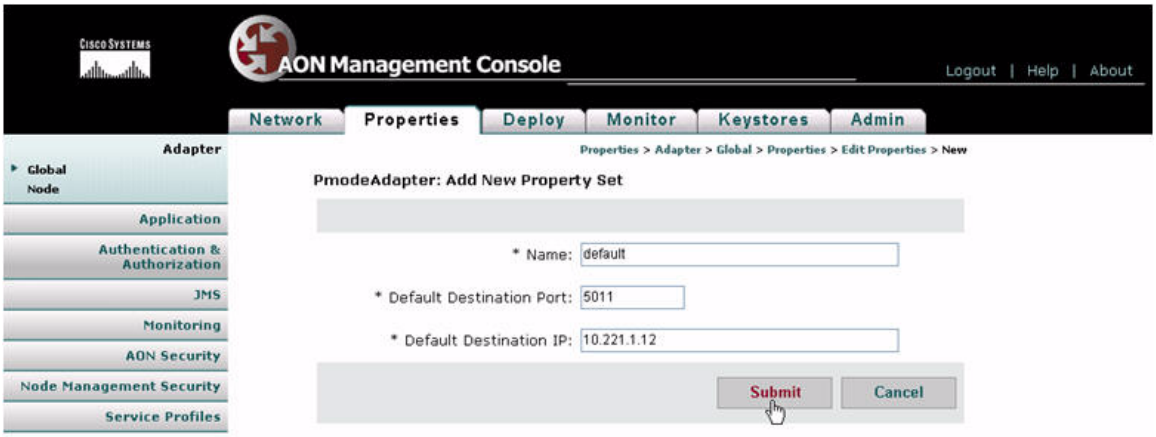
Warning **If you enter a name other than "default," the configuration will fail.**

Step 9 Enter the **Default Destination port** as 5011 for our example.

Step 10 Enter the **Default Destination IP** as the IP address of the analyzer.

Step 11 Click **Submit**.

Figure 30 Configuring the PMode Adapter: Configuring New Property Set

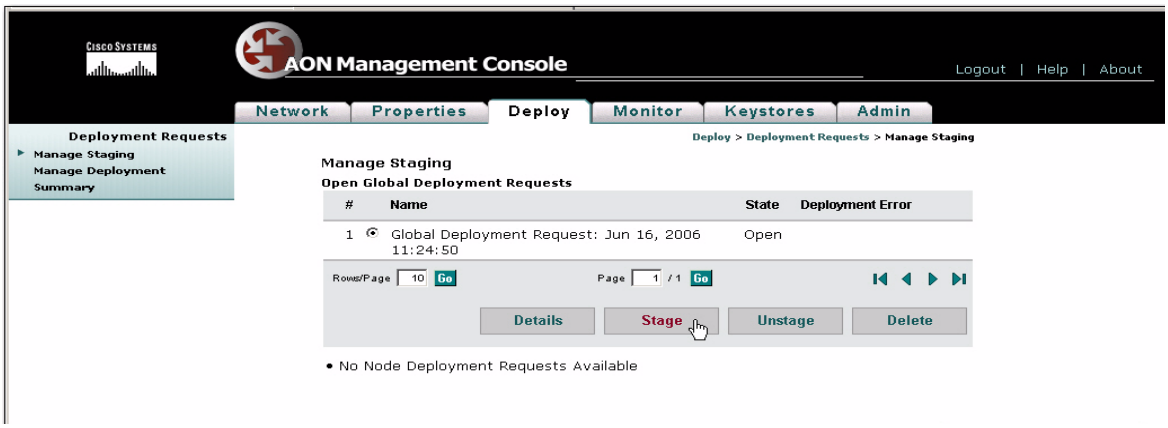


Step 12 Click the **Deploy** Tab in the top menu of AMC.

Step 13 Click **Manage Staging** on the menu in the left window.

Step 14 Notice a **Global Deployment Request**. Select the Global deployment request and click **Stage** as shown below.

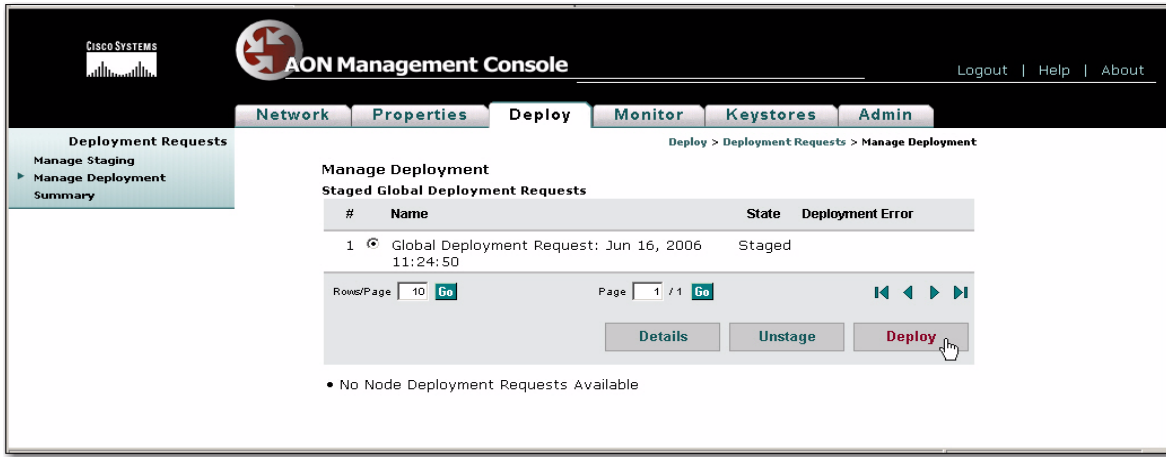
Figure 31 Configuring the PMode Adapter: Staging New Property Set



Step 15 Click on **Manage Deployment** in the menu in the left window.

Step 16 Select the Global deployment Request and click **Deploy**.

Figure 32 Configuring the PMode Adapter: Deploying New Property Set



Once deployed, a message ‘Successfully deployed all configurations to the node’ displays.

Loading the HTTP Extension

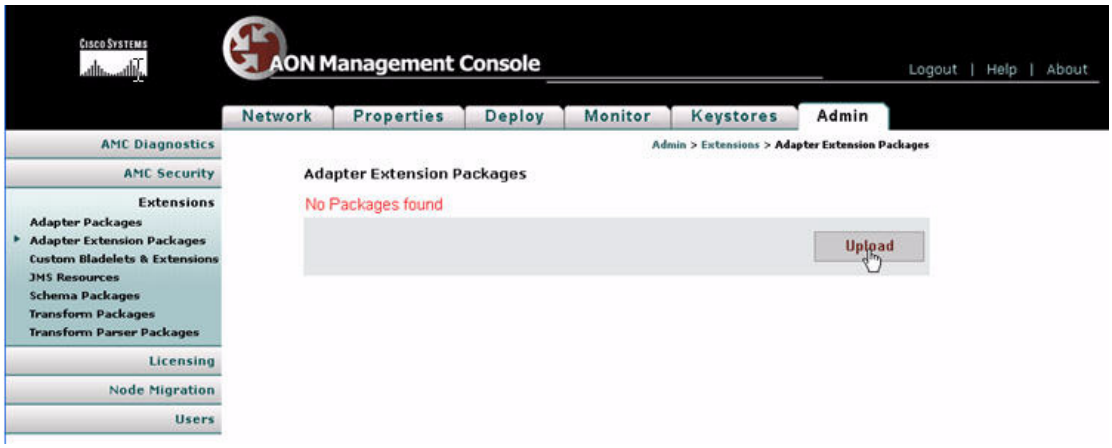
To load the HTTP extension, perform the following steps:

Step 1 Click **Admin** tab on the top right of the window of AMC.

Step 2 On the left side window, click Adapter Extension Packages in the Extensions menu.

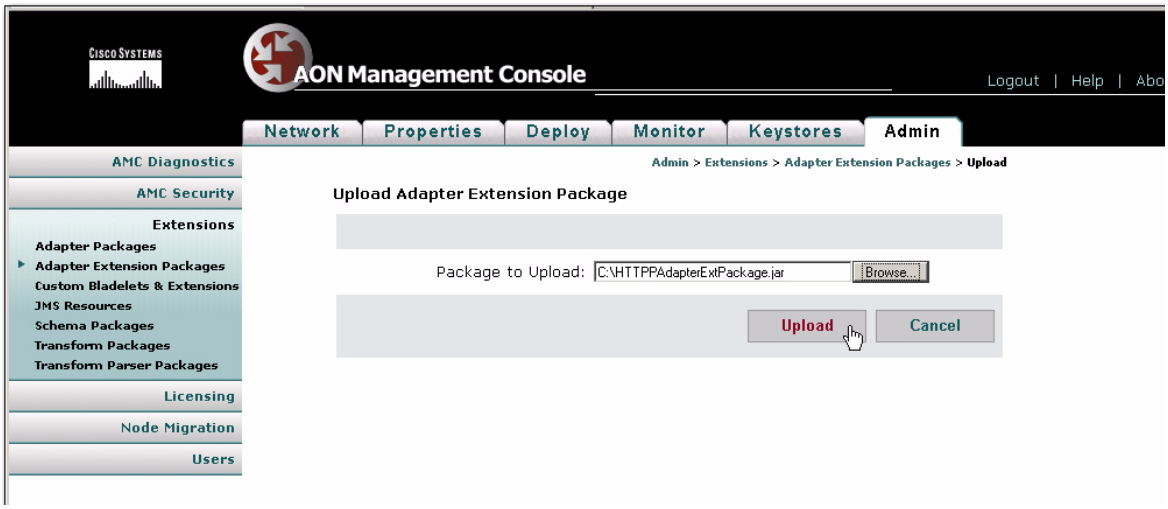
Step 3 Click **Upload** as shown below.

Figure 33 Loading HTTP Extension: Uploading Package



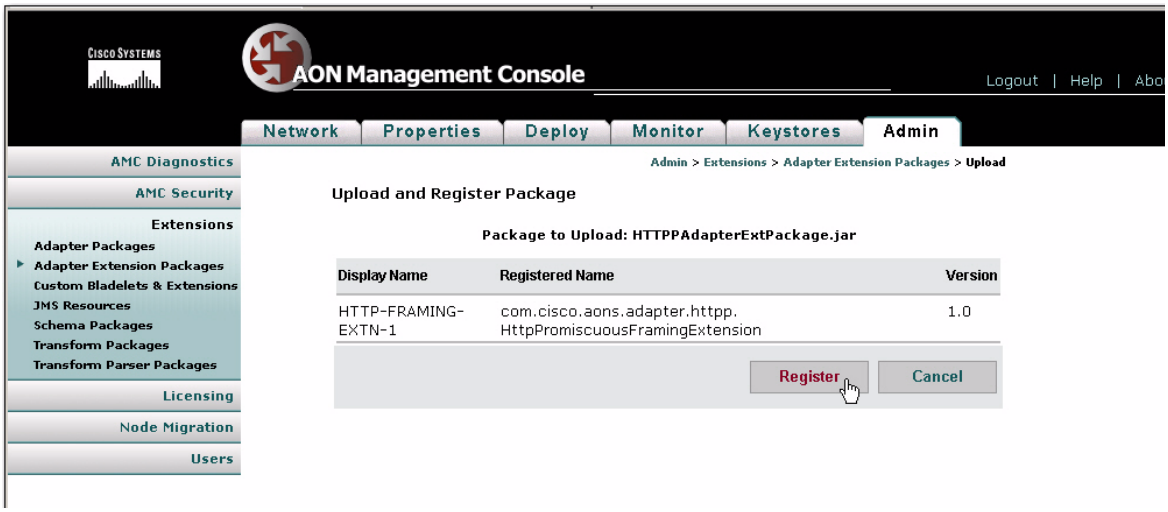
Step 4 In the **Package to Upload** field, browse to the location of the **HTTPAdapterExtPackage.jar** file, then click the Upload button.

Figure 34 Loading HTTP Extension: Uploading Extension



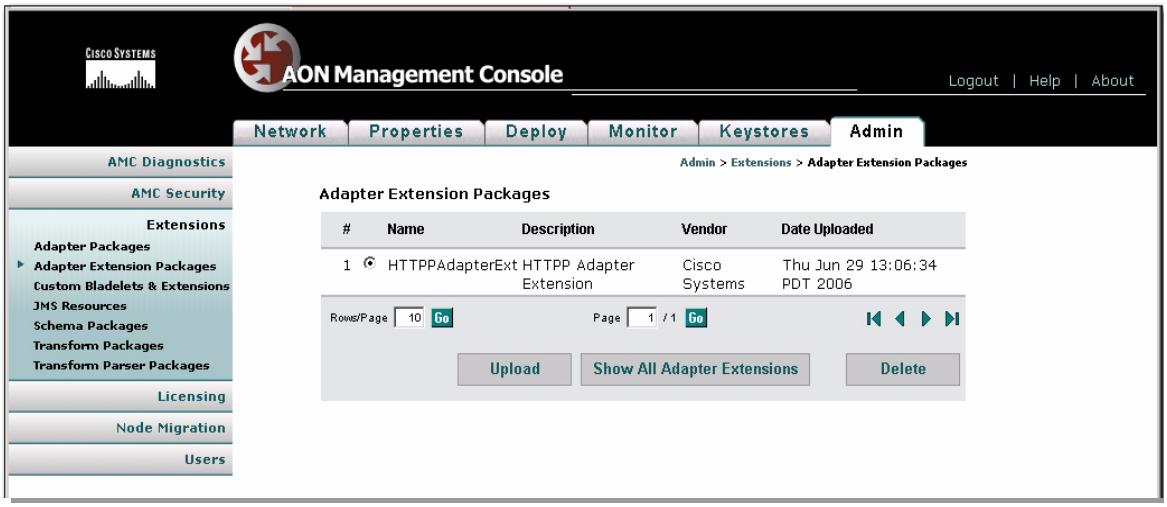
Step 5 Click **Register** on the **Upload and Register Package** window.

Figure 35 Loading HTTP Extension: Registering Extension



The AON HTTP Extension is registered, as shown in Figure 36.

Figure 36 Loading HTTP Extension: Registering Package



Enabling the HTTP Extension

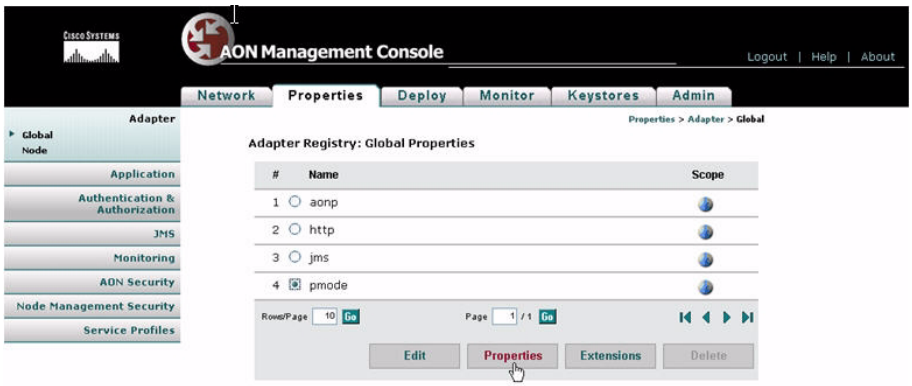
To enable the HTTP Extension, perform the following steps:

Step 1 Click the **Properties** tab on the top of the window.

Step 2 On the left hand side of the window, click **Global** in the **Adapter** menu.

Step 3 Select the **PMode** radio button, then click the Extensions button, as shown in Figure 37.

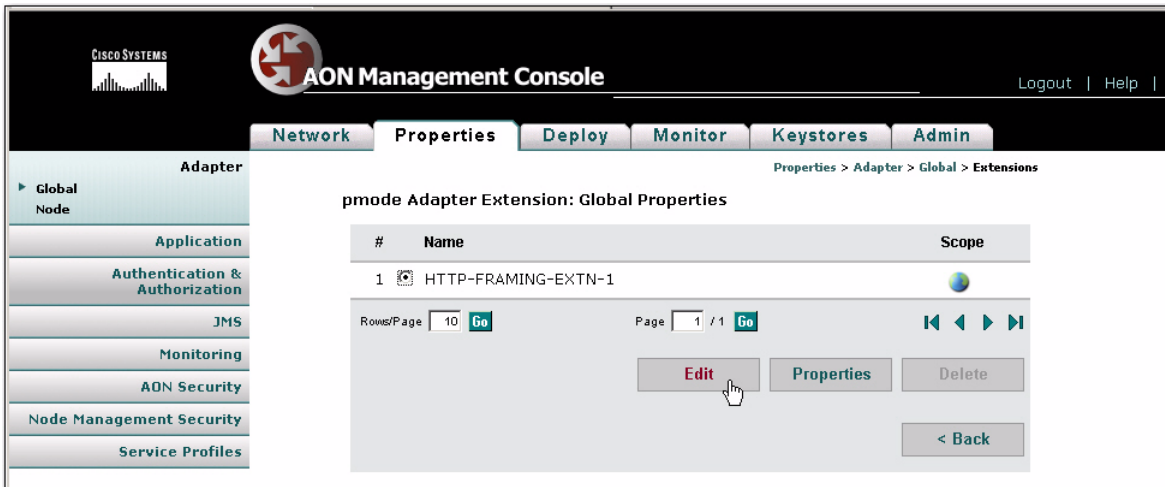
Figure 37 Enabling HTTP Extension



The **PMode Adapter Extensions: Global Properties** window displays.

Step 4 Select the **HTTP-FRAMING-EXTN-1** radio button, then click the **Edit** button as shown in Figure 38.

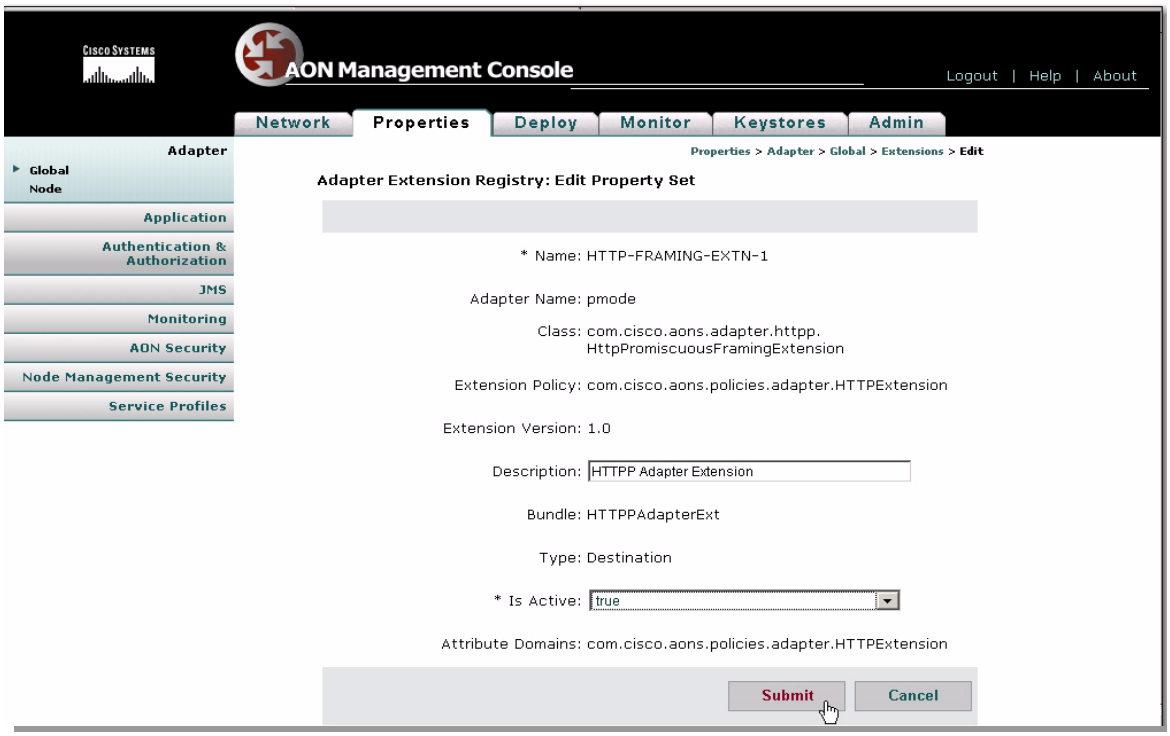
Figure 38 Enabling HTTP Extension: Editing Extension



Step 5 The **Adapter Extension Registry: Edit Property Set** window displays. In the **Is Active** field choose **True**, then click the **Submit** button, as shown in Figure 39.

The adapter extension is now activated.

Figure 39 Enabling HTTP Extension: Editing Extension



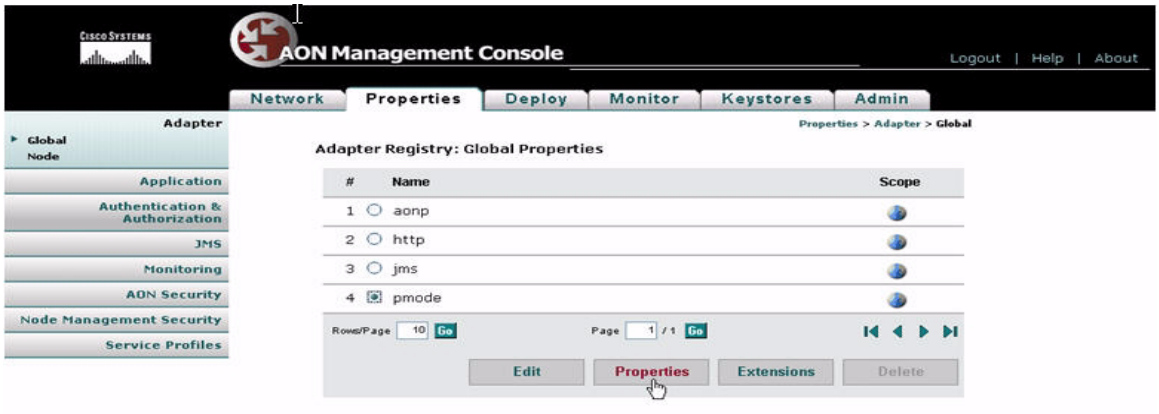
Configuring HTTP Extension

To configure the HTTP Extension, perform the following steps:

Step 1 Click on the **Properties** Tab.

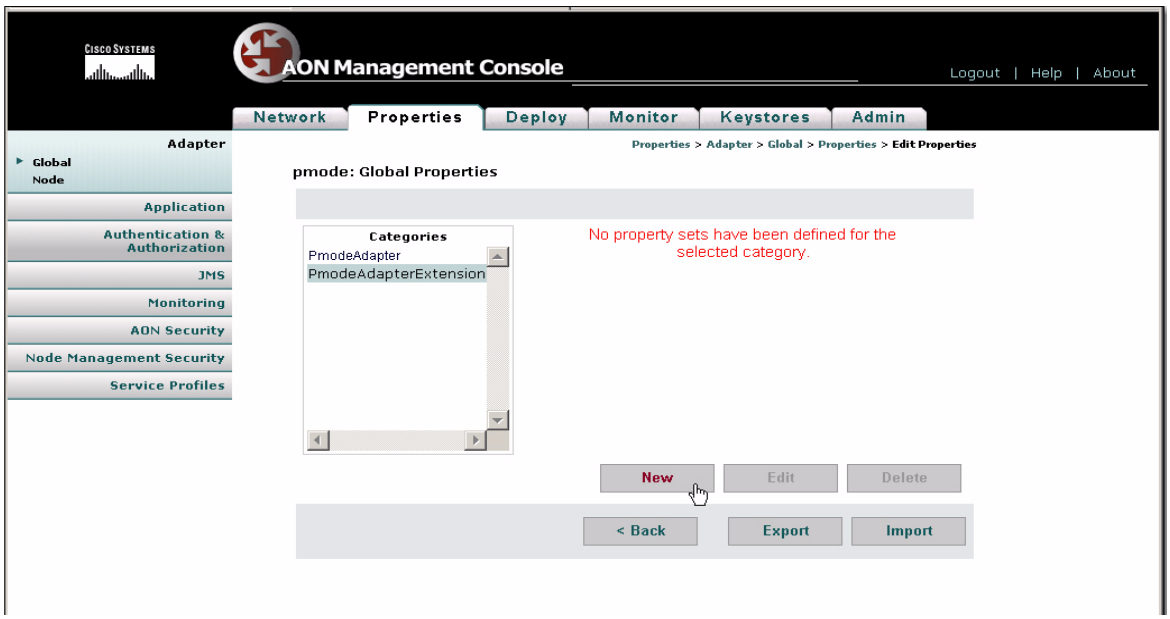
Step 2 Make sure that **Global** is selected under **Adapter** menu in the left hand pane. Select the **PMode** radio button, then click the **Properties** button, as shown in Figure 40.

Figure 40 Configuring HTTP Extension: Selecting PMode Adapter



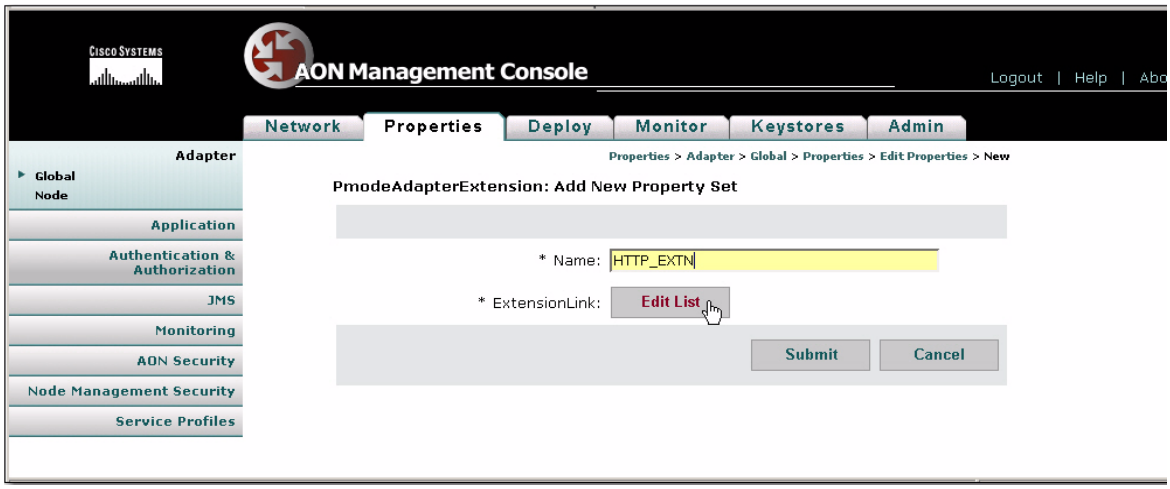
Step 3 Select **PmodeAdapterExtension** and click the **New** button.

Figure 41 Configuring HTTP Framing Extension: Creating New Property Set



Step 4 Enter a name for this extension, then click the **Edit List** button.

Figure 42 Configuring HTTP Framing Extension: Creating New Extension



Step 5 Select **HTTP-FRAMING-EXTN-1**, click the **Save** button then click the **Submit** button.

Figure 43 Configuring HTTP Framing Extension: Creating New Extension

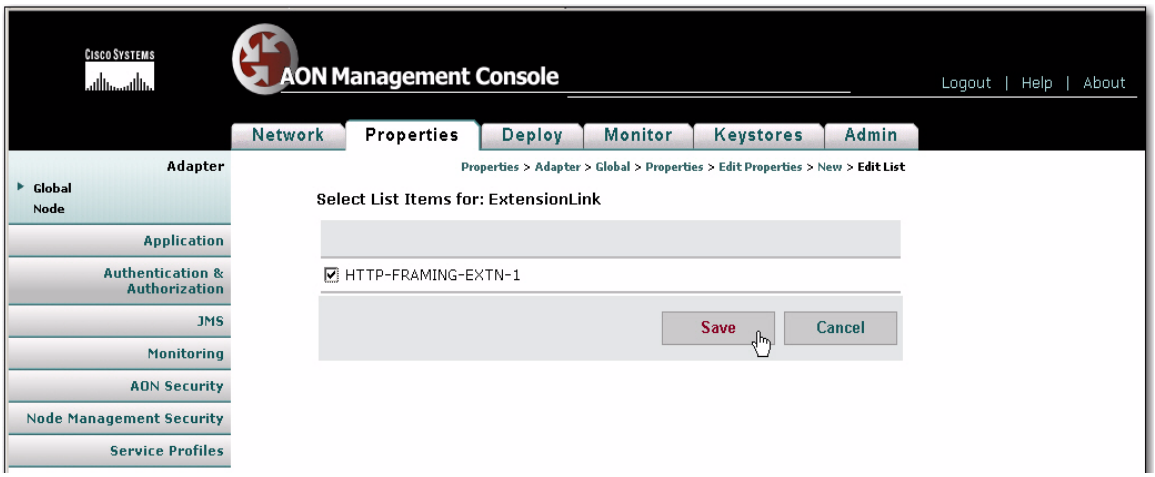
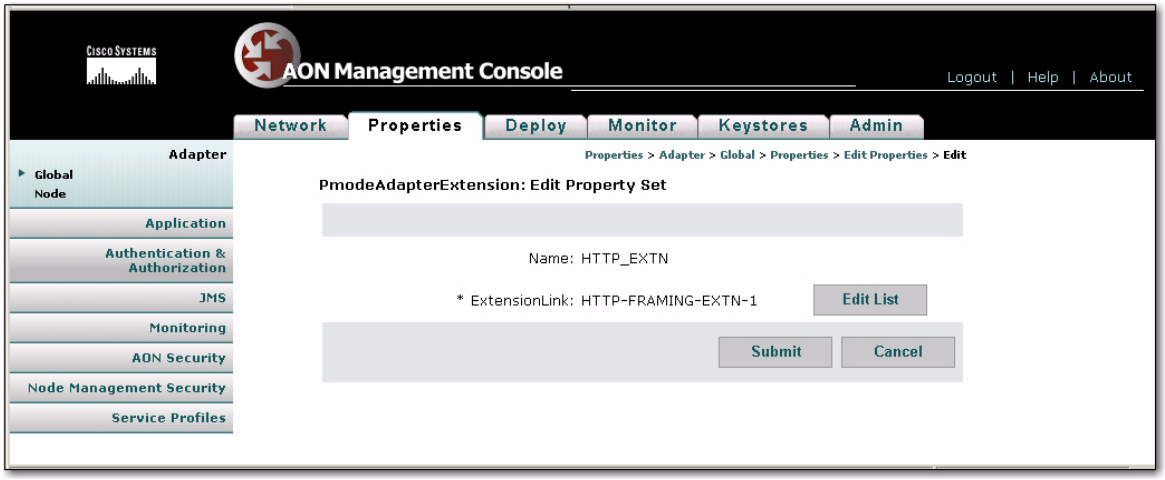


Figure 44 Configuring HTTP Framing Extension: Creating New Extension

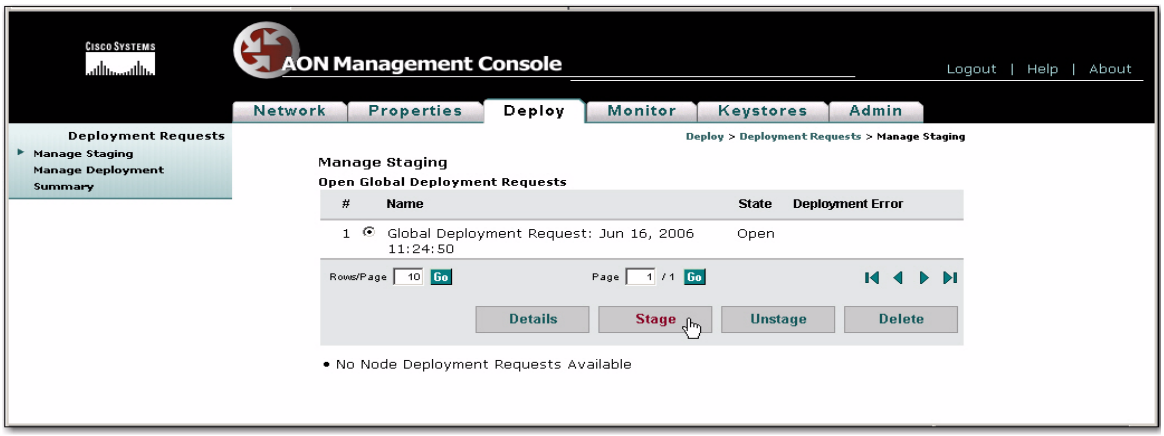


Step 6 Click the **Deploy** Tab in the top menu of AMC.

Step 7 Click **Manage Staging** on the menu in the left window.

Step 8 Notice a new **Global Deployment Request**. Select the Global deployment request and click **Stage** as shown below.

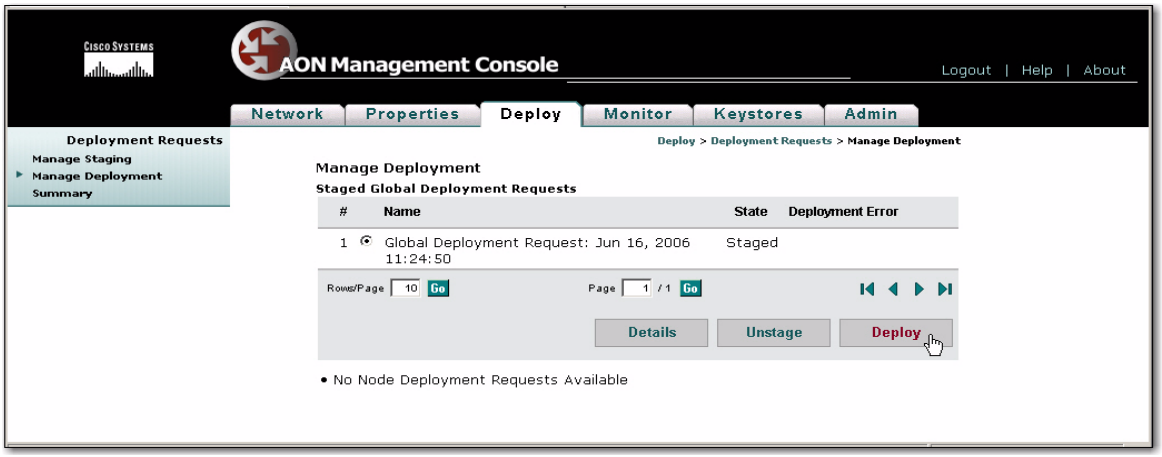
Figure 45 Configuring the PMode Adapter: Staging New Property Set



Step 9 Click on **Manage Deployment** in the menu in the left window.

Step 10 Select the Global deployment Request and click **Deploy**.

Figure 46 Configuring the PMode Adapter: Deploying New Property Set



Once deployed a message 'Successfully deployed all configurations to the node' is displayed.

Step 11 Click the **Properties** tab on the top right window of AMC.

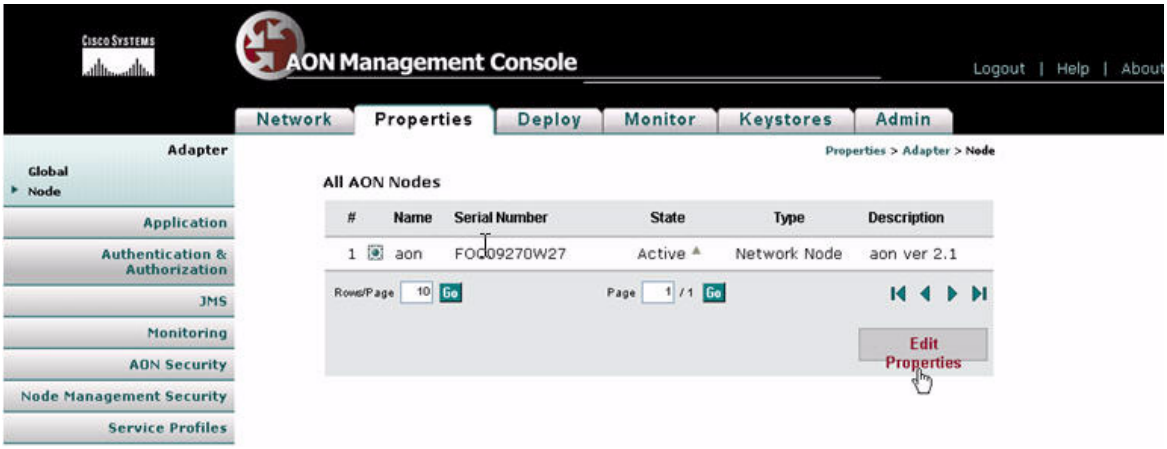
Step 12 Ensure that the **Adapter** menu is selected on the left pane.

Step 13 Click on the **Node** sub-menu under **Adapter**.

Step 14 Select the AON node for which to configure the connection.

Step 15 Click on **Edit Properties** button.

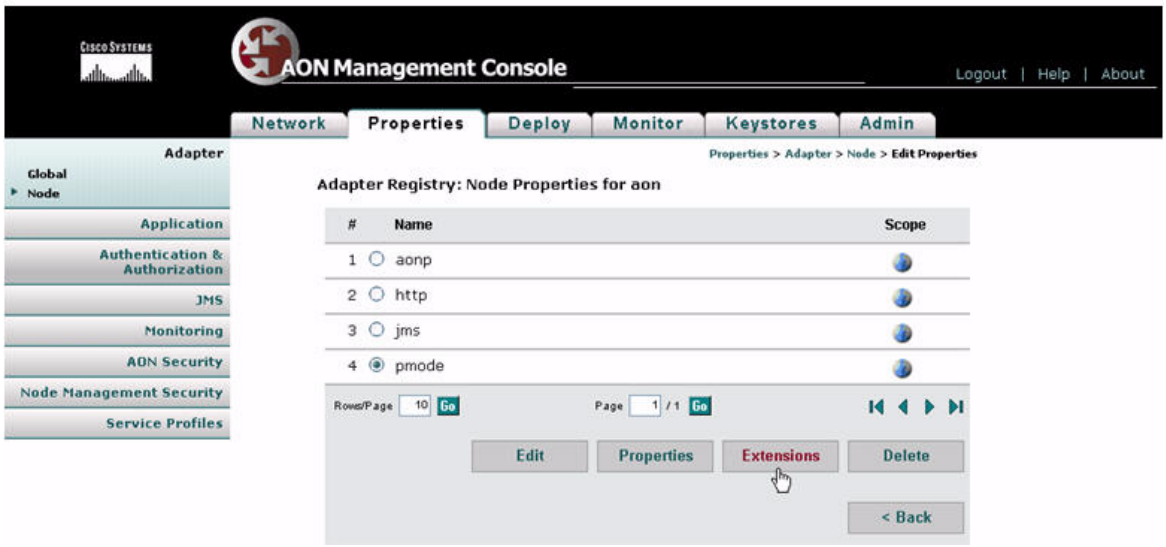
Figure 47 Configuring HTTP Framing Extension: Edit Node Adapter Properties



Step 16 Select the **PMode** property from the list of Node Properties for the AON node.

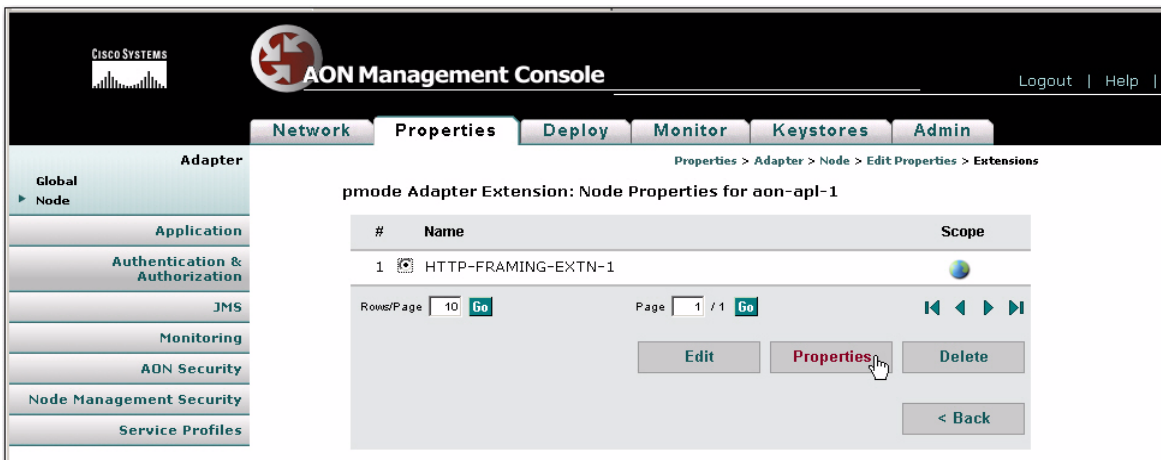
Step 17 Click on the **Extensions** button.

Figure 48 Configuring HTTP Framing Extension: Edit Node Adapter Properties



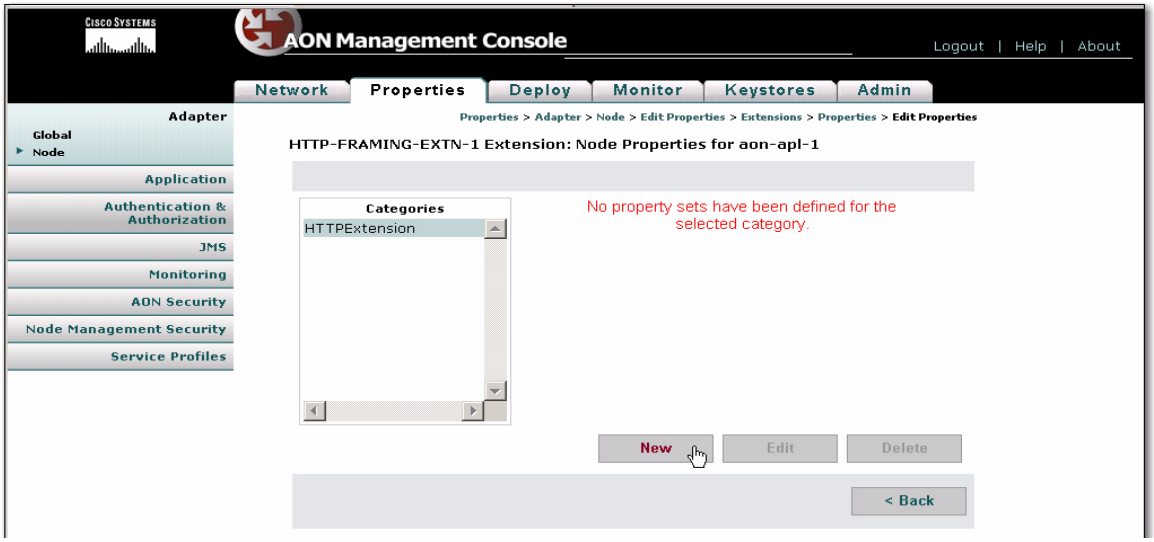
Step 18 Select **HTTP-FRAMING-EXTN-1** and then click the **Properties** button.

Figure 49 Configuring HTTP Framing Extension: Edit Node Adapter Properties



Step 19 Under **Categories** select **HTTPExtension** and click **New**.

Figure 50 Configuring HTTP Framing Extension: Edit Node Adapter Properties



Step 20 For **Name**, enter a name for the connection—**Connection1** in the example

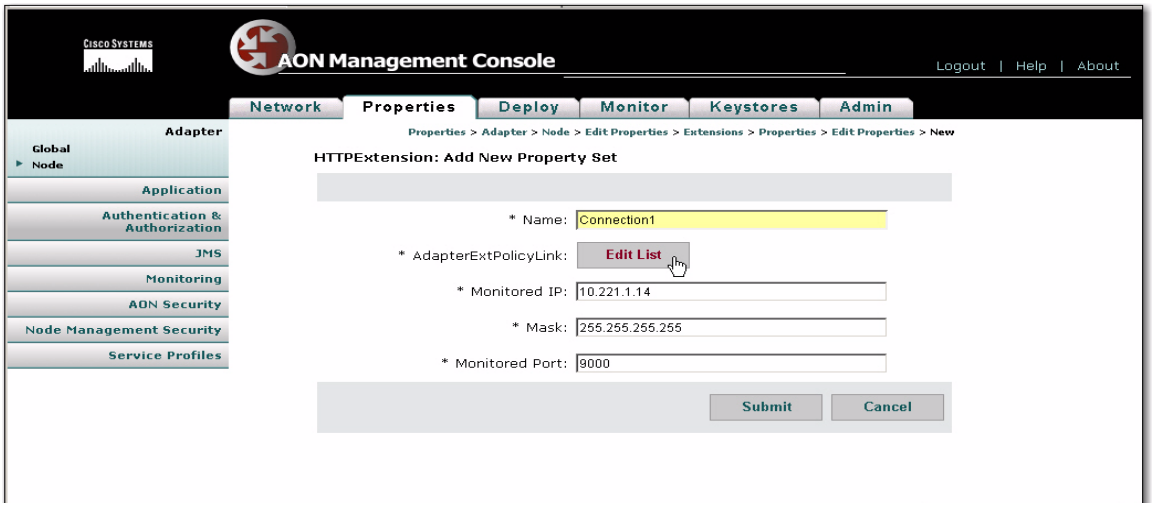
Step 21 For **Monitored IP**, enter the IP address of the Server machine—10.221.1.14 in the example.

Step 22 For **Mask**, enter 255.255.255.255

Step 23 For **Monitored Port**, enter the value of the port to monitor—while 9000 is used in the example below, the default value is 80.

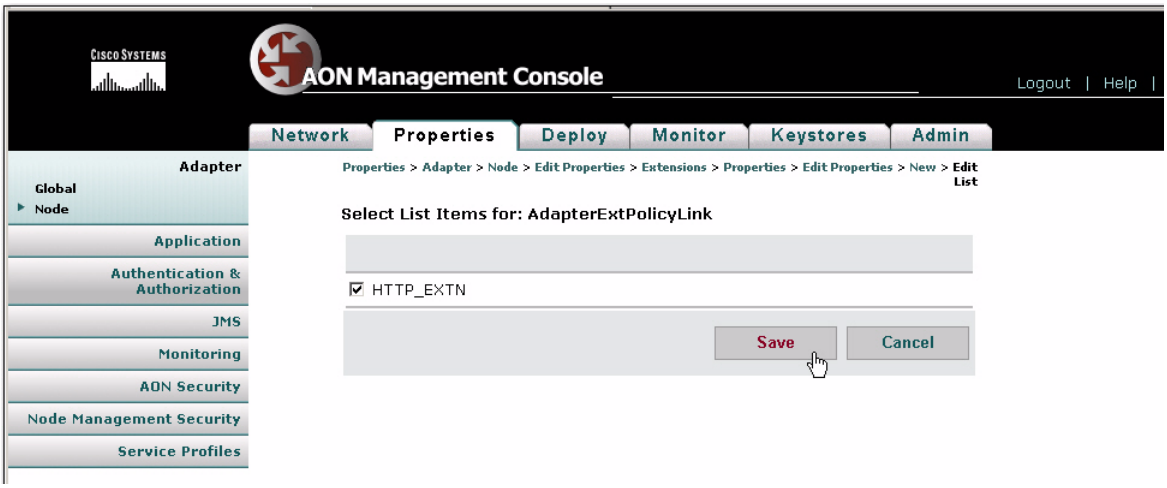
Step 24 Click the **Edit List** button next to **AdapterExtPolicyLink**.

Figure 51 Configuring HTTP Framing Extension: Edit Node Adapter Properties



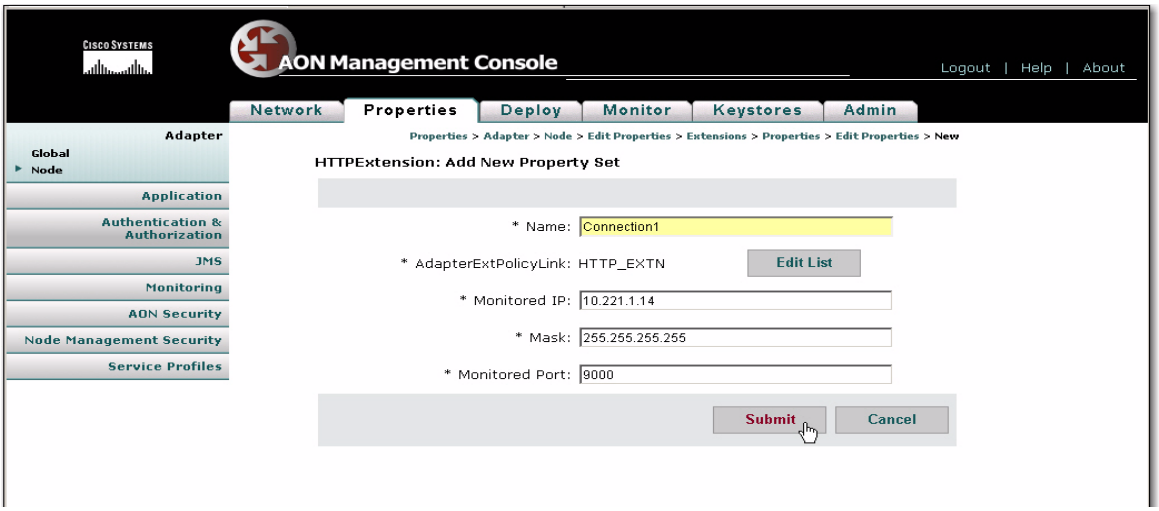
Step 25 Select the **HTTP_EXTN** and click **Save**.

Figure 52 Configuring HTTP Framing Extension: Edit Node Adapter Properties



Step 26 Review your entries and click the **Submit** button.

Figure 53 Configuring HTTP Framing Extension: Edit Node Adapter Properties



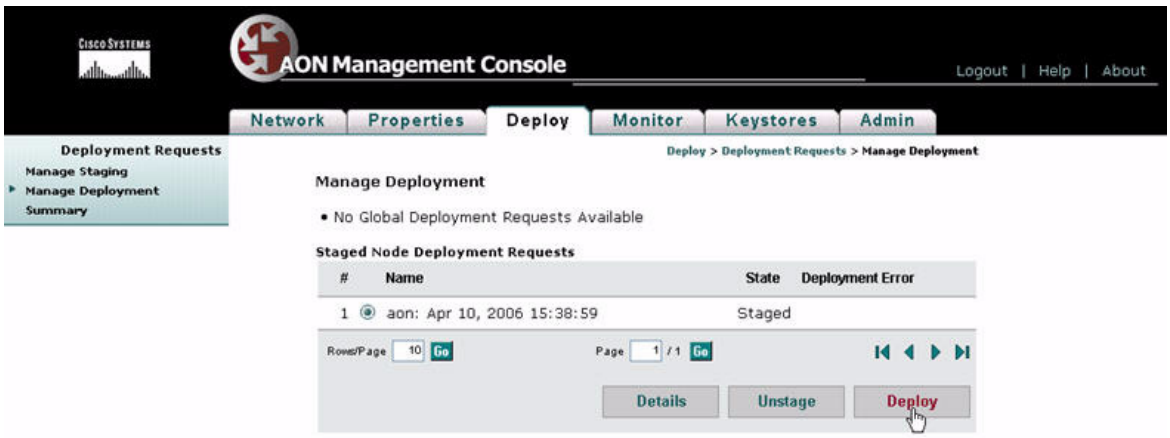
Step 27 Select the **Deploy** Tab.

Step 28 Notice a listing under **Open Node Deployment Requests**. Stage the request by clicking **Stage**.

Figure 54 Configuring HTTP Framing Extension: Staging Deployment Request

Step 29 Select **Manage Deployment** in the left hand window and select the deployment request, then deploy it by clicking **Deploy**.

Figure 55 Configuring HTTP Framing Extension: Deploying the Request



Once the request is successfully deployed, a message 'Successfully deployed configuration to node' displays.

Step 30 Establish a session to the AON node and restart it as follows:

```
aon-node> enable
aon-node# aon restart force
CAUTION! Stopping all AON processes!
Are you sure[n]? y
```

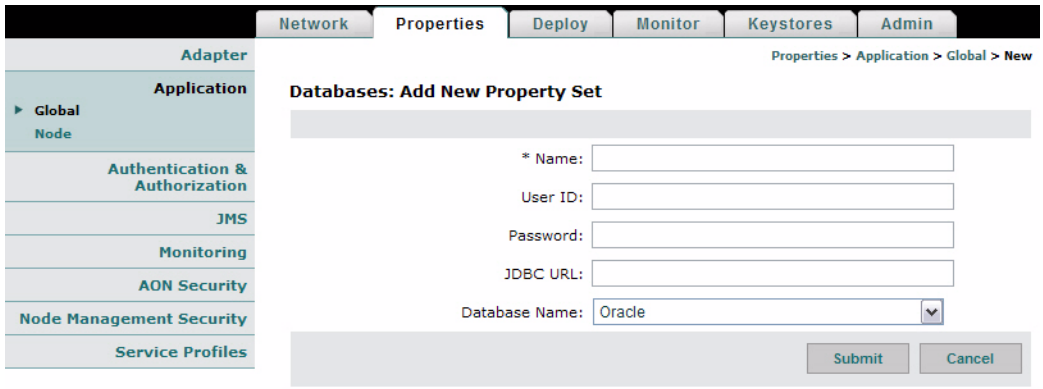
Note The PMode configuration will take affect once the node is restarted.

To validate that the extension is successfully deployed, check the AON log files. For instructions on viewing logs, see Chapter 3, "Viewing Logs".

Connecting to 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 4-56 shows the Database Property page.

Figure 4-56 Database Property



Data to Enter

The Database Property page includes the entries described in Table 4-20.

Table 4-20 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:\ Oracle: **jdbc:oracle:thin:@***ip_address*:*port*:*database_name* Sybase: **jdbc:sybase:Tds:** *ip_address*:*port*/*database_name*
Database name	One of the following: • 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.

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

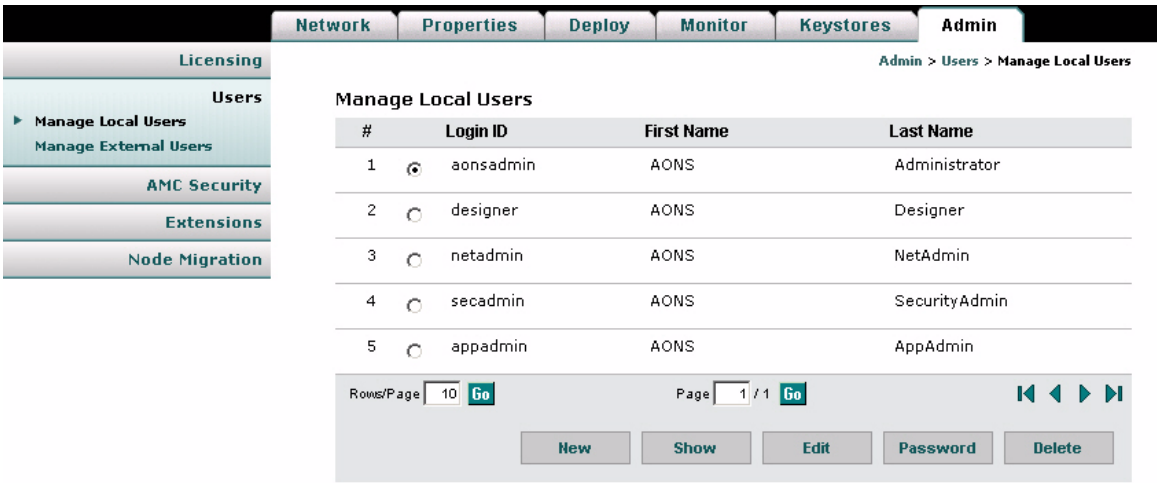
Local users are created and managed by the AMC. You can use the Manage Local Users page to perform the following tasks:

- 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.

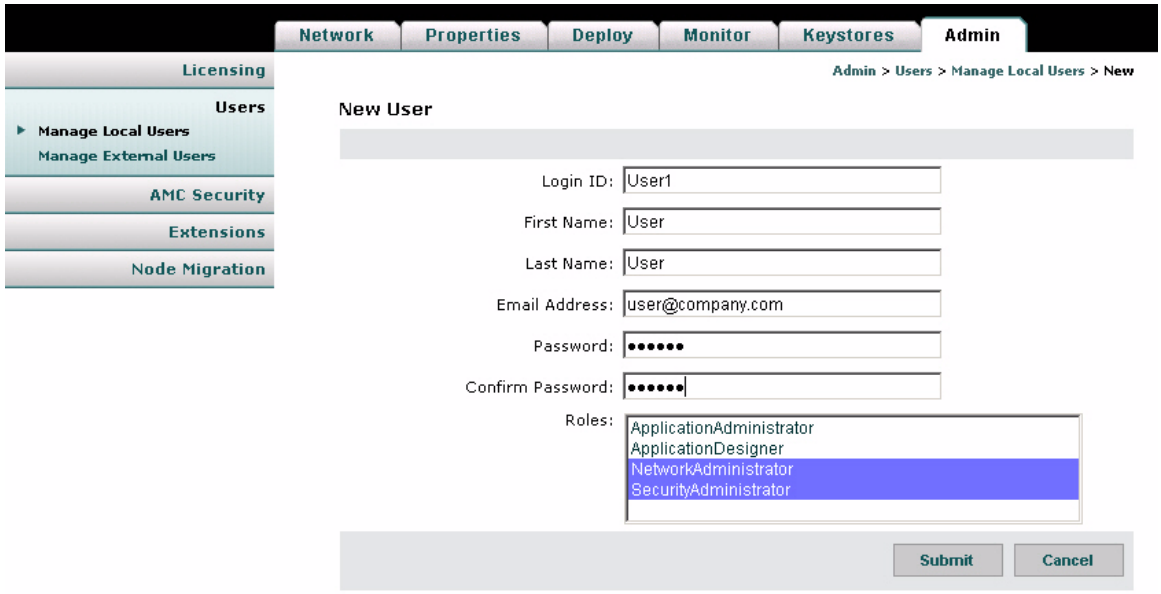
Creating New Users

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



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.

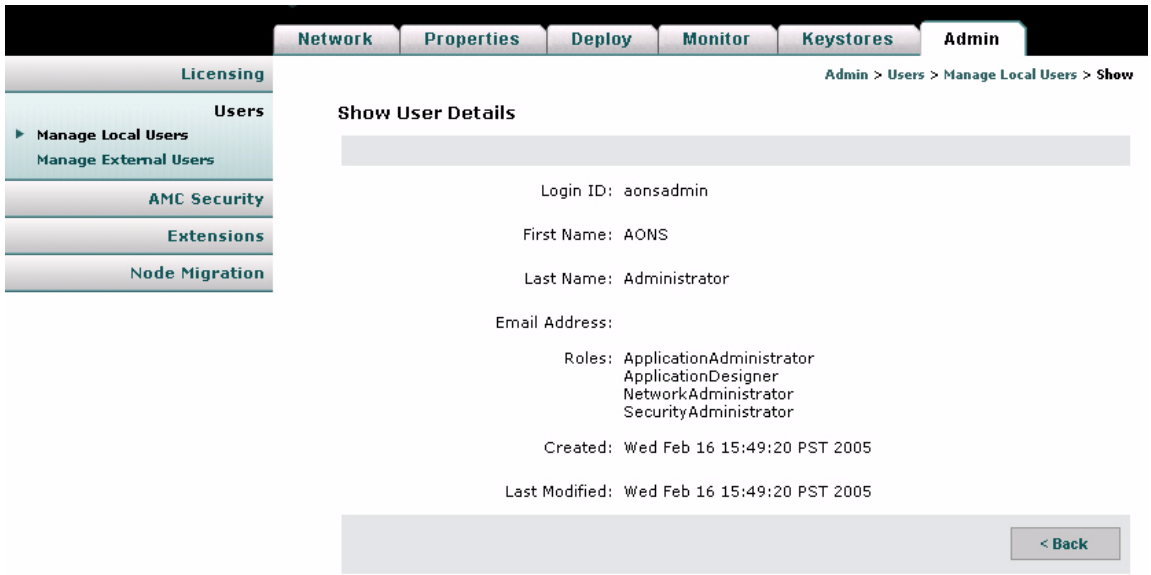
Displaying Information on Users

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



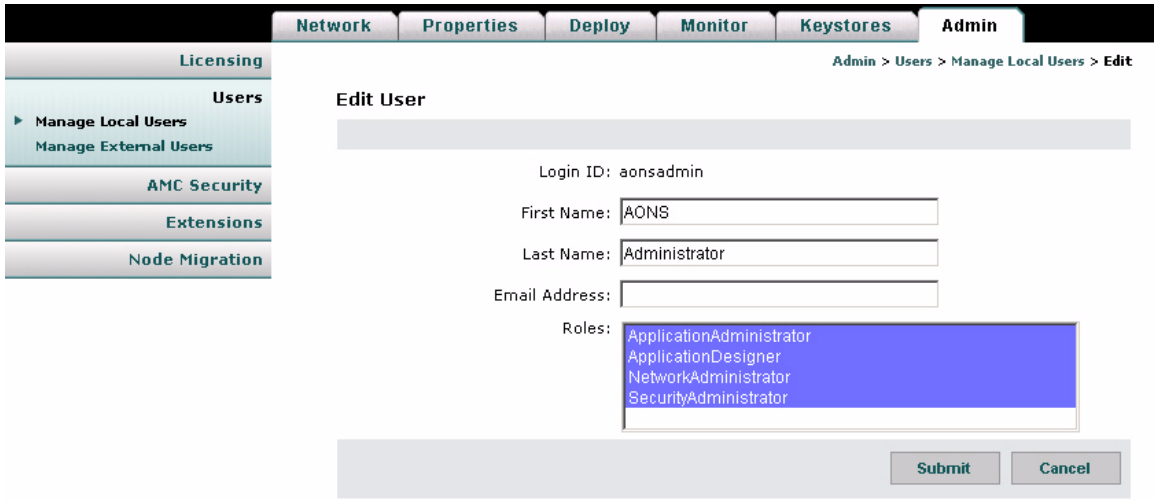
Editing Users

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



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	—	• Adapter • Application • JMS • Monitoring • Service Profiles	• All	• All	—	• All
Application Designer	—	—	—	—	—	• Extensions

Table 5-1 AMC User Roles (continued)

Role	Network Tab	Properties Tab	Deploy Tab	Monitor Tab	Keystores Tab	Admin Tab
Network Administrator	• All	• Monitoring	—	• All	—	—
Security Administrator	—	• Authentication and Authorization • Security	—	• All	• All	• 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

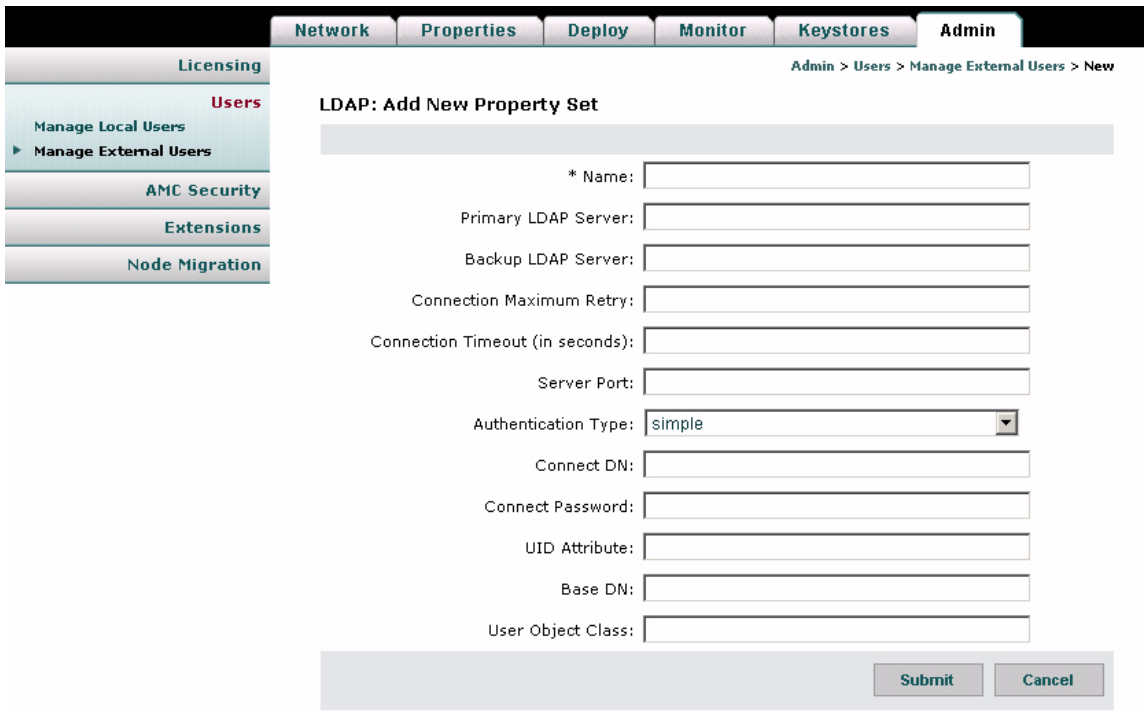
Creating an LDAP Profile

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



Actions to Take

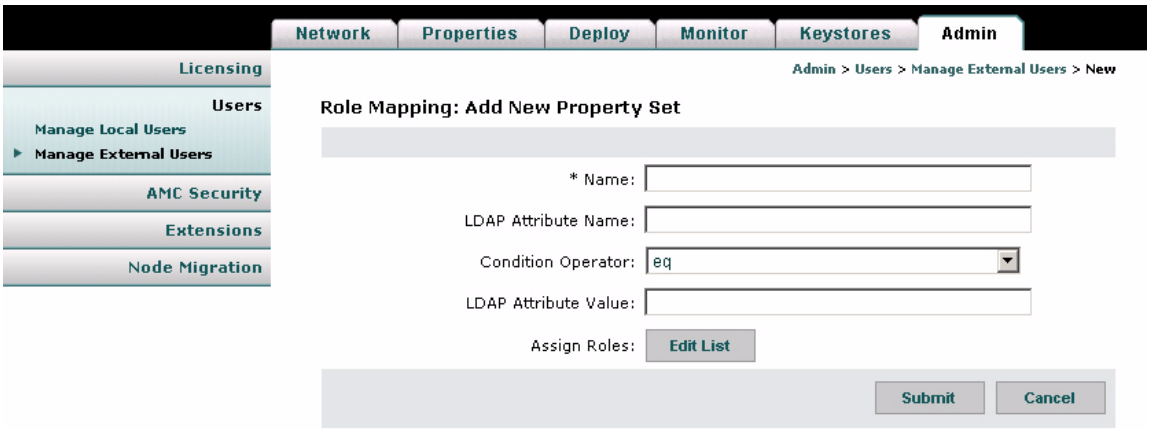
Complete the entries as appropriate for the LDAP server being used. Contact your LDAP administrator for details.

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: • 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.

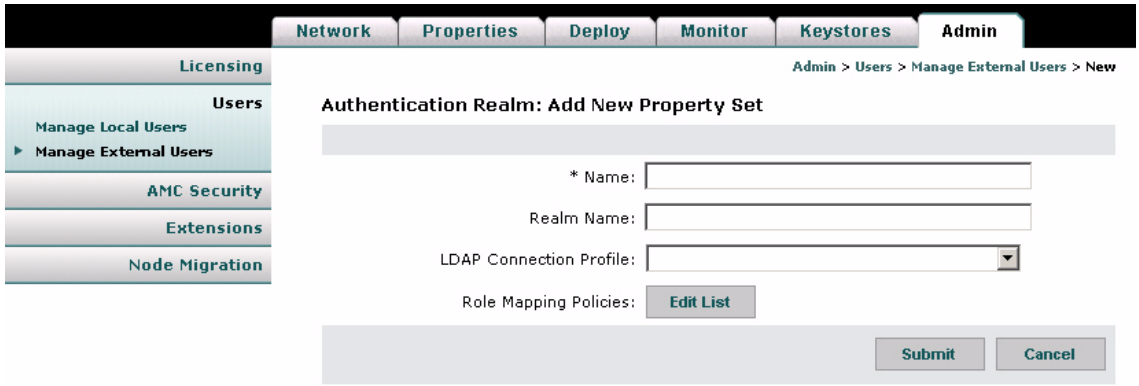
Creating an Authentication Realm

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.

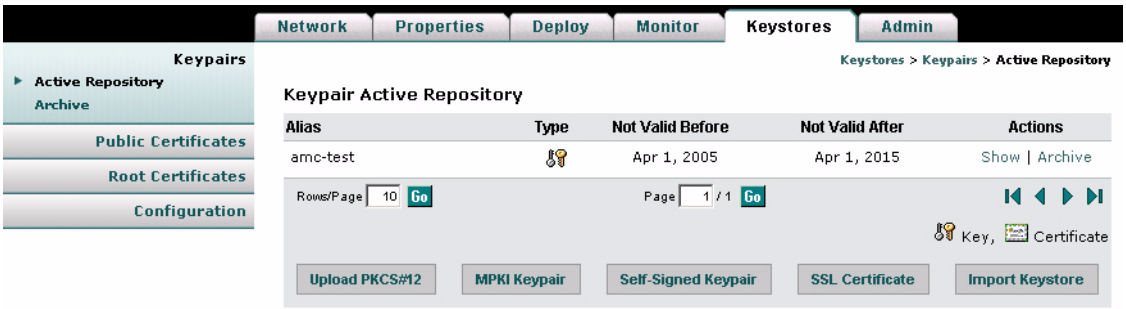
Managing Keypairs

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



Actions to Take

You can perform any of the following actions:

- Upload a PCKS#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.

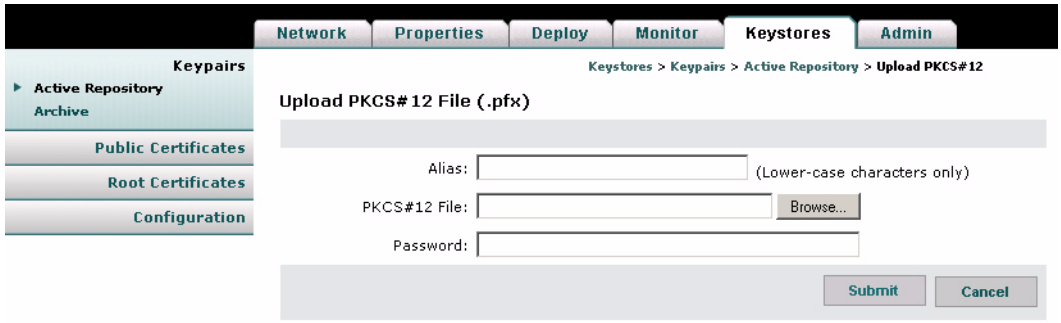
Upload PKCS#12

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.

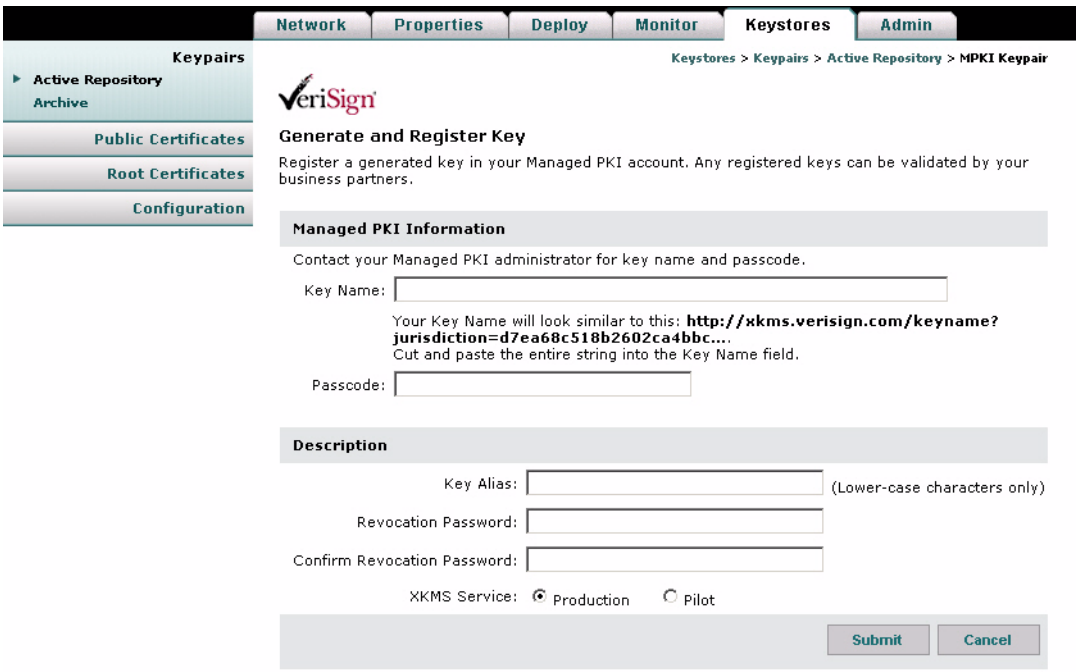
Generate and Register a New Key

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



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: http://xkms.verisign.com/keyname?jurisdiction=d7ea68c518b2602ca4bbc....
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.

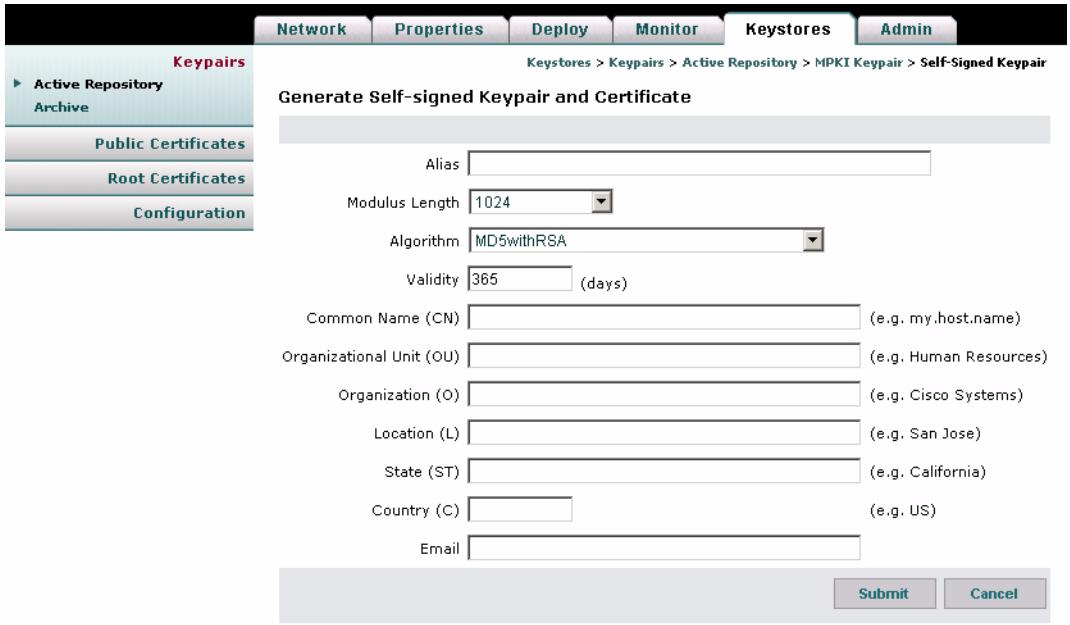
Generate a Self-Signed Keypair and Certificate

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



Data to Enter

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

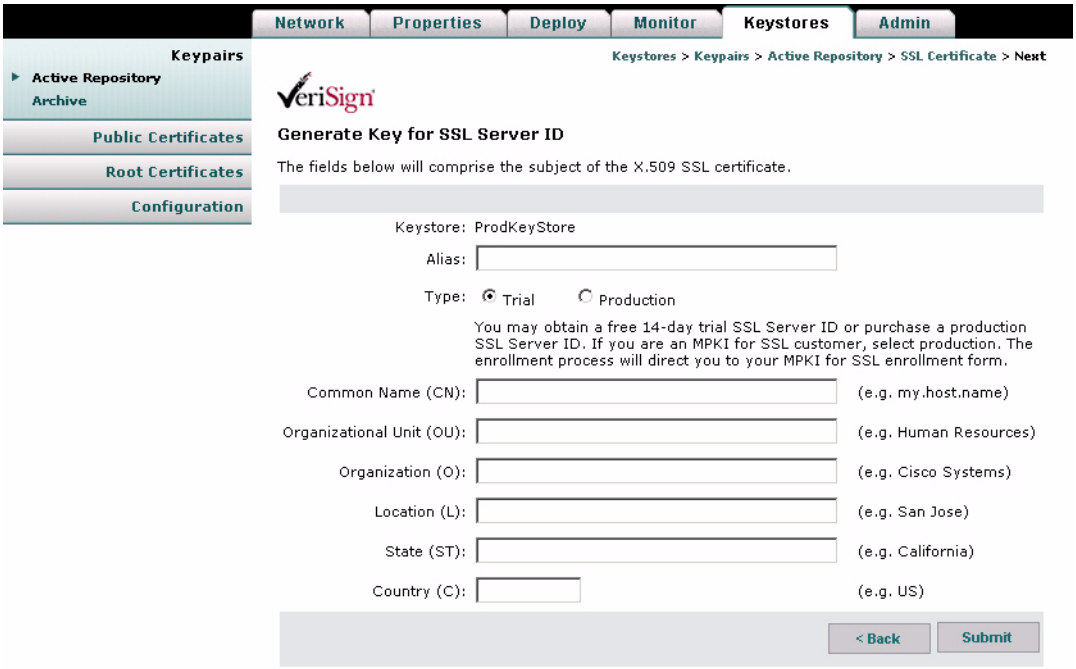
Generate an SSL Certificate

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

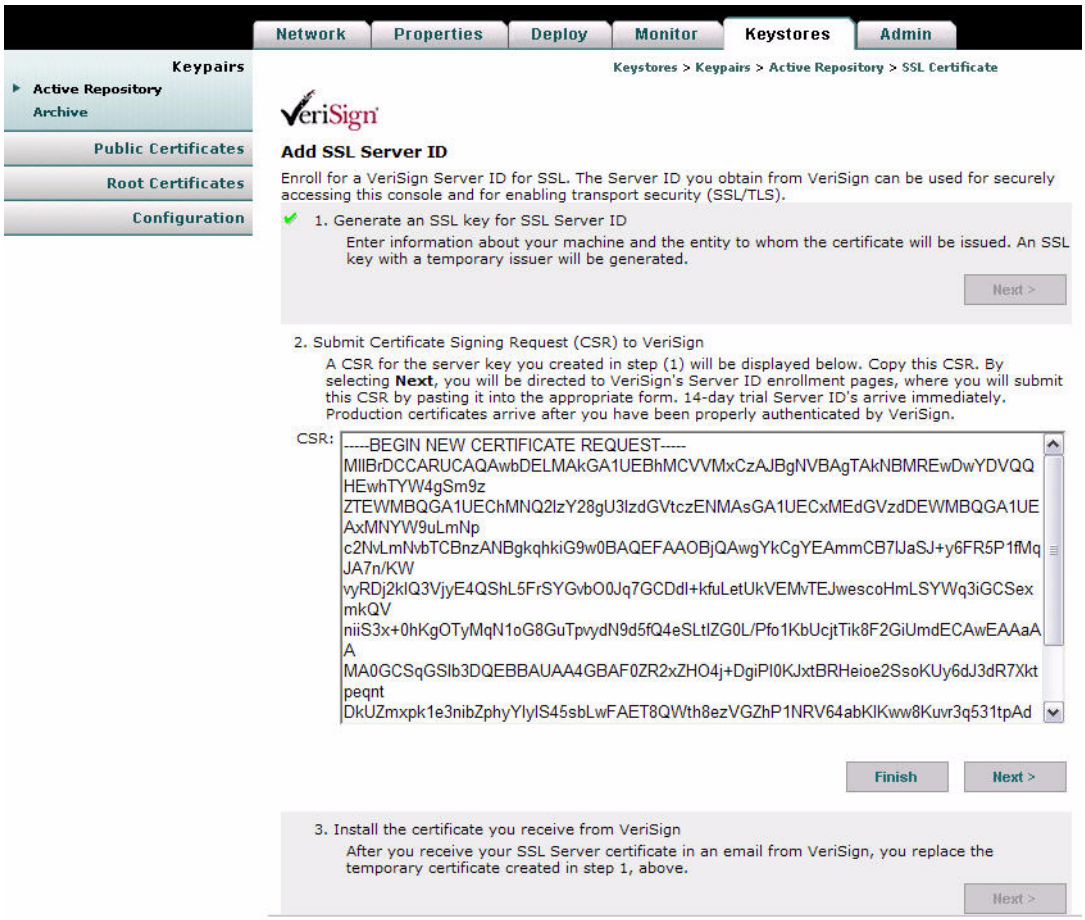
Complete the entries as required for you organization and click the **Submit** button. AMC generates the server certificate and displays it on the Add SSL Server ID page.

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.

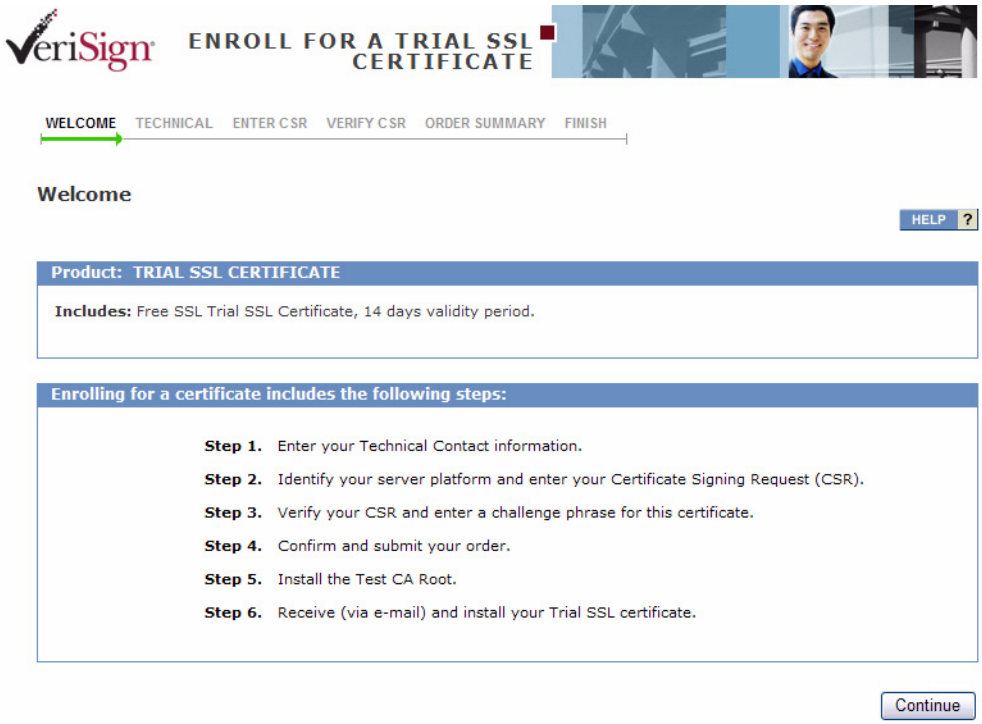
Figure 5-13 Add SSL Server ID



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.

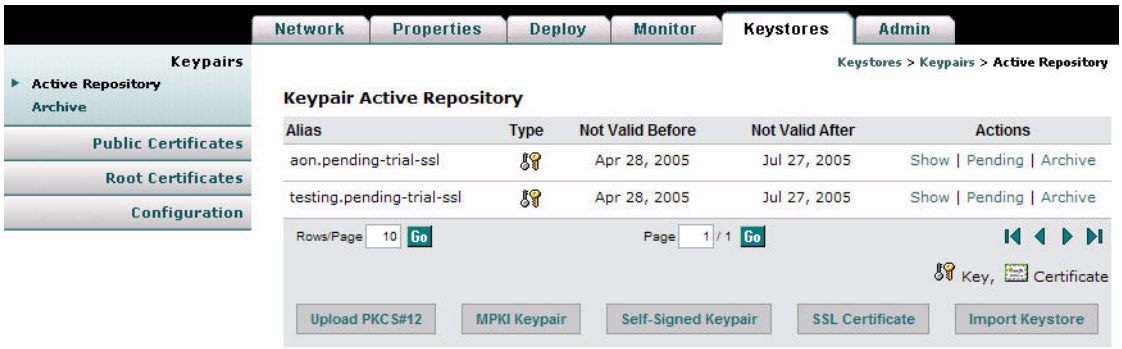
Figure 5-14 Shows the Verisign enroll for an SSL certificate. Complete the enrollment process to register the certificate generated by AMC.

Figure 5-14 Verisign SSL Certificate Enrollment



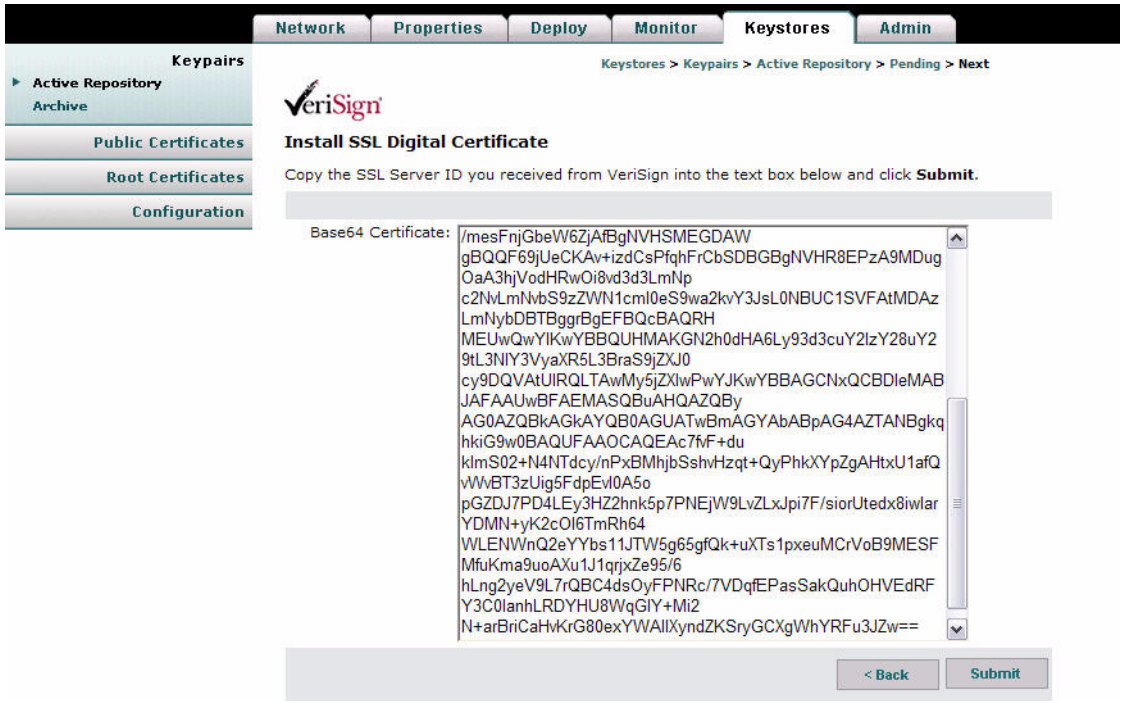
After completing the process at Verisign, return to the Active Repository in AMC and click the Pending link for your new certificate, as shown in Figure 5-15.

Figure 5-15 Active Repository with Pending Entries



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



Actions to Take

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

Import a Keypair or Keystore

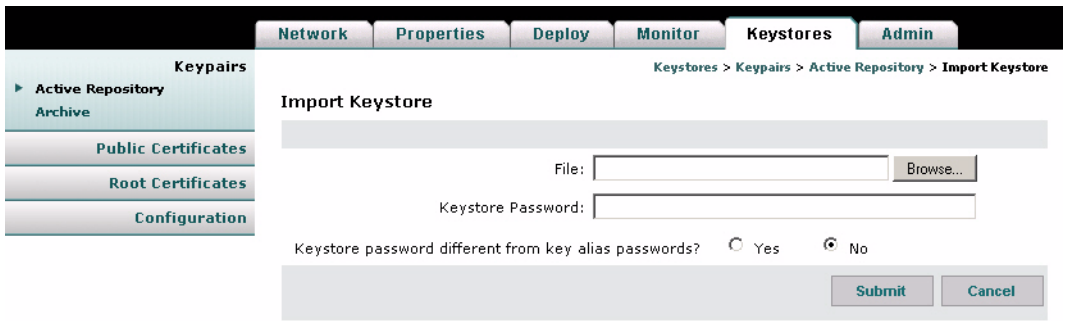
You can import an existing keystore that contains your public and private certificates.

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



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.

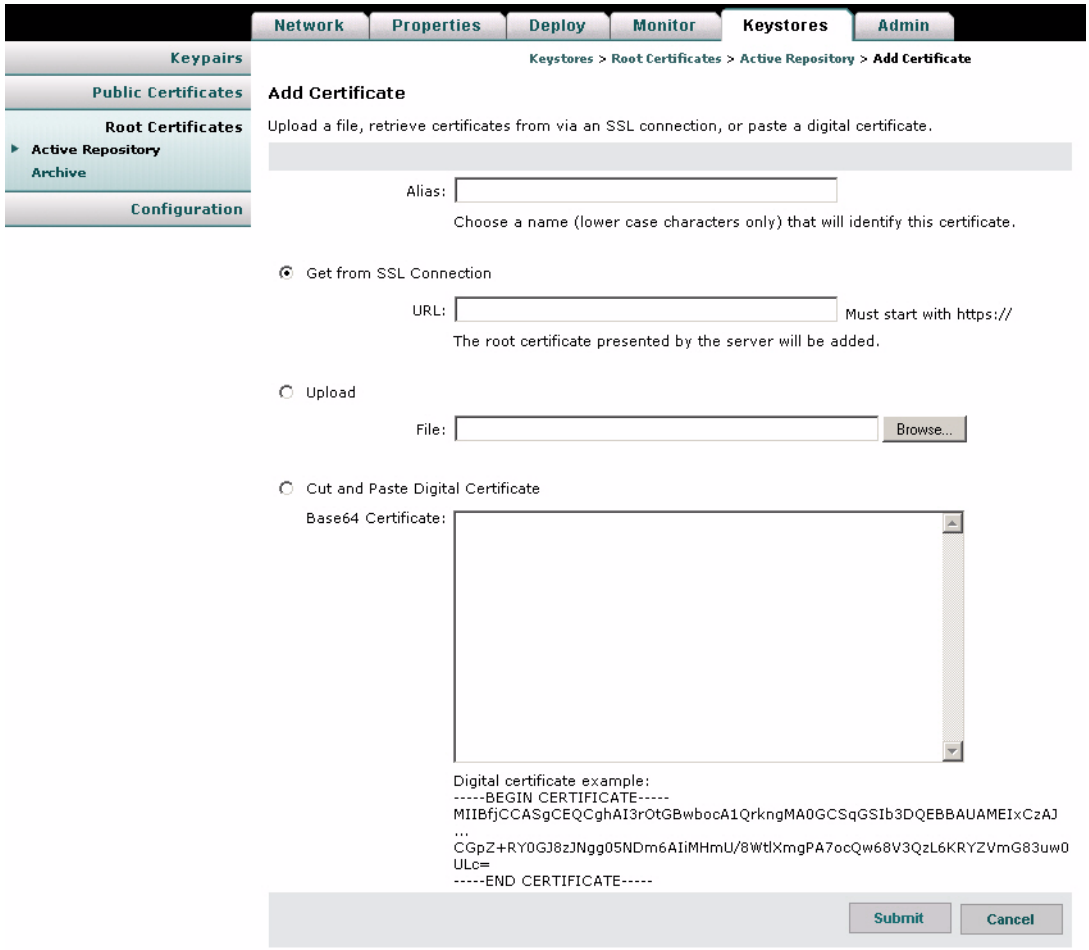
How to Get There

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



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

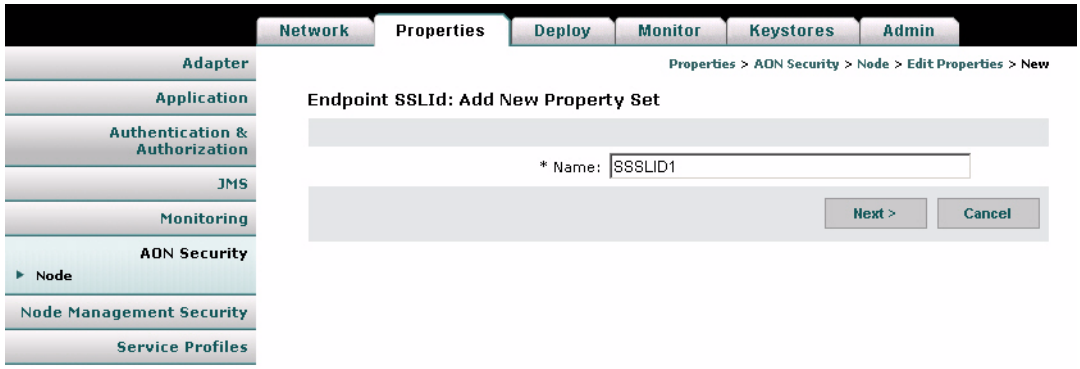
Endpoint SSLID Property

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.

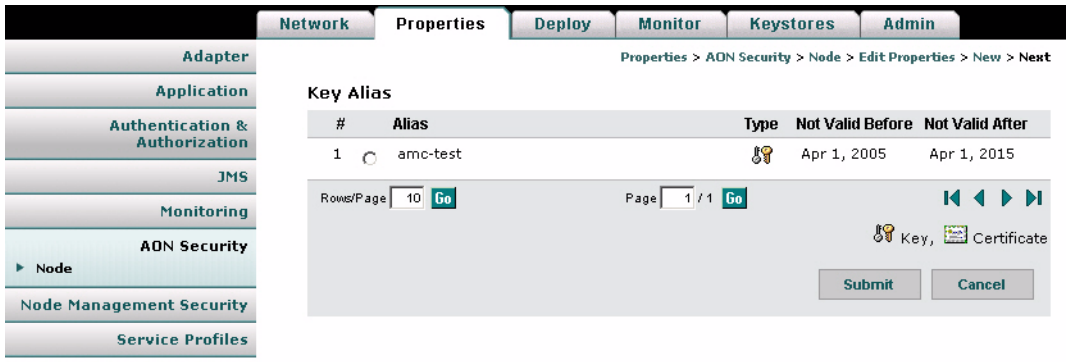
Figure 5-19 Endpoint SSSLID Property



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



SSL Configuration Property

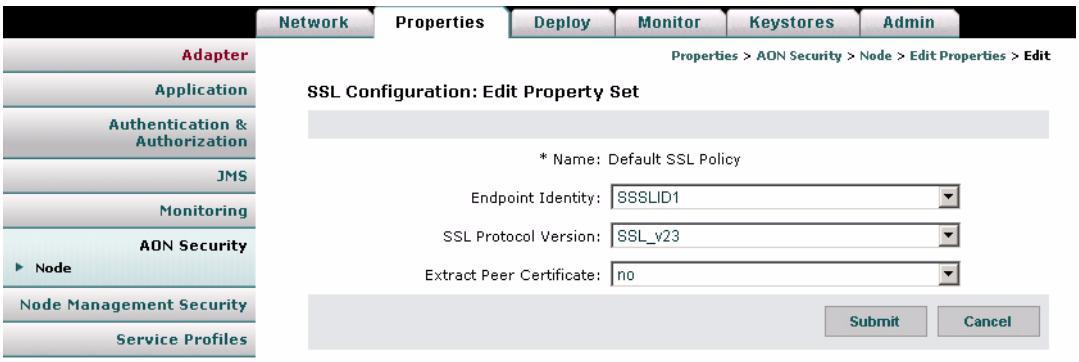
SSL Configuration Property specifies SSL-related parameters to be used by a node. Figure 5-21 shows the SSLID Property page.

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



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

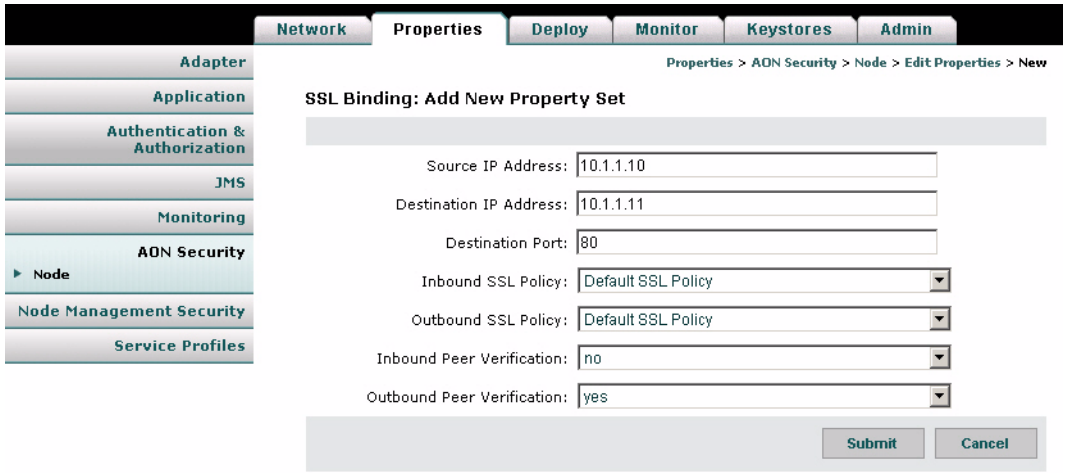
The SSL Binding property enables you to bind a message's source IP, destination IP, and destination port to an SSL property. Figure 5-22 shows the SSL Binding Property page.

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

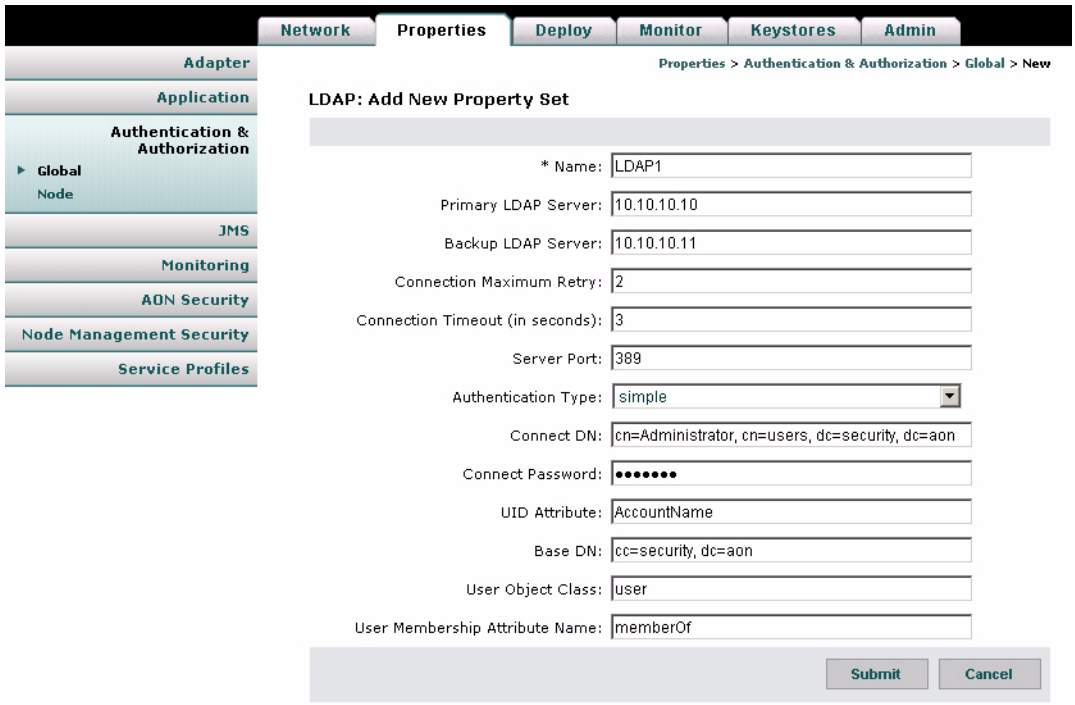
Lightweight Directory Access Protocol (LDAP) is a protocol for accessing online directory services. This property can be configured at the node or global levels. After configuring this property, nodes in your AON network are able to access an LDAP directory for authentication and authorization.

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



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.

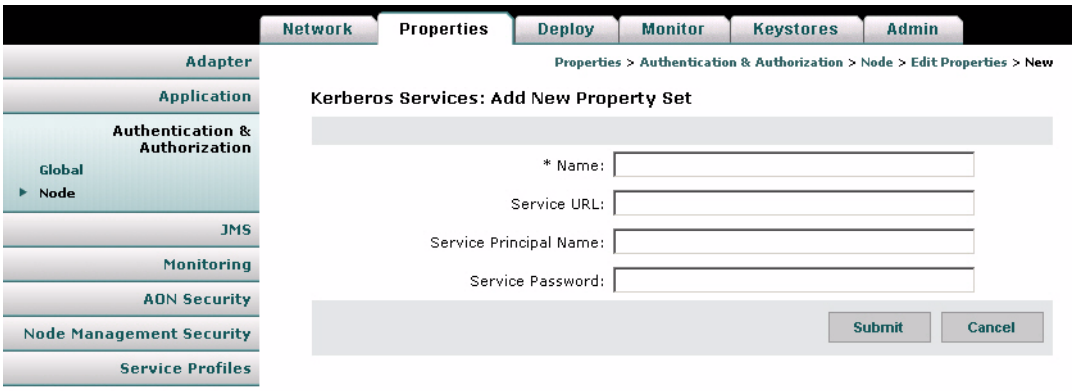
Kerberos configuration is controlled by three properties, which must be configured in the following order:

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

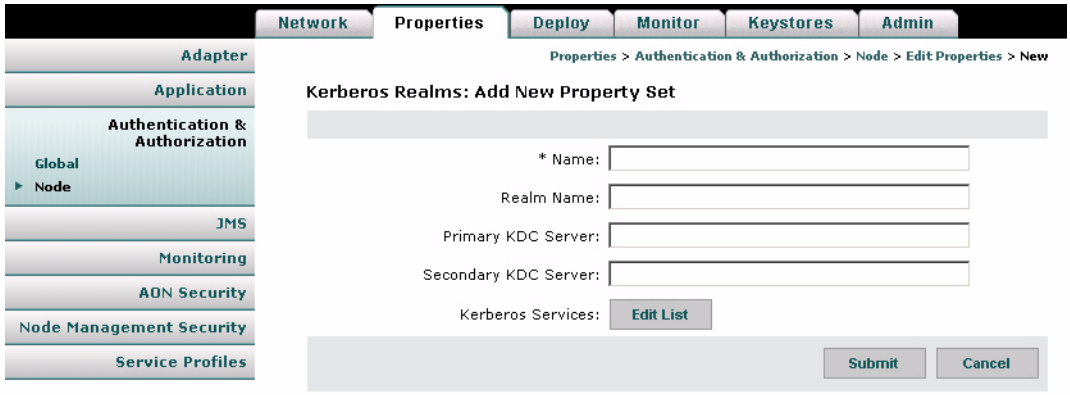


Data to Enter

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



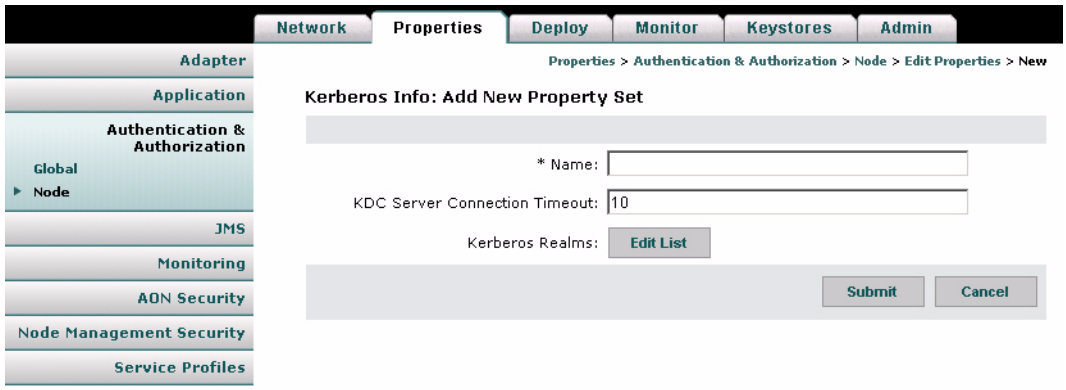
Data to Enter

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



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.

CHAPTER 6

AMC Administration

This chapter covers the Admin portion of AMC. It includes the following sections:

- AMC Diagnostics, page 6-1
- AON Licensing, page 6-2
- Managing AON Users, page 6-2
- Managing AMC Certificates, page 6-11
- Managing Extensions, page 6-11

AMC Diagnostics

AMC Diagnostics enable you to set the log reporting level of various AON functions. For each of the given functions, you can set one of the following log levels:

- TRACE
- DEBUG
- INFO
- WARN
- ERROR
- FATAL

AMC displays the current logging level for each category. New logging level take effect as soon as you click the Save button. There is no need to restart the system, and the logging levels survive subsequent restarts of AMC.

Only administrators have the ability to change log levels.

AON Licensing

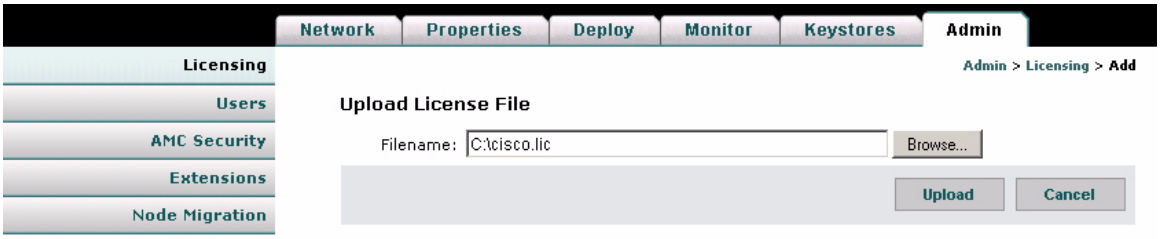
AMC provides the ability to upload licenses that enable additional features and functionality. Contact your Cisco representative to obtain more information about licensing.

How to Get There

Go to **Admin > Licensing**, then click the Add button.

Figure 6-1 shows the licensing page.

Figure 6-1 AMC Licensing



Actions to Take

Click the Browse button to navigate to the location on your PC where the license file is stored, then click the Upload button to send the file to the AMC.

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

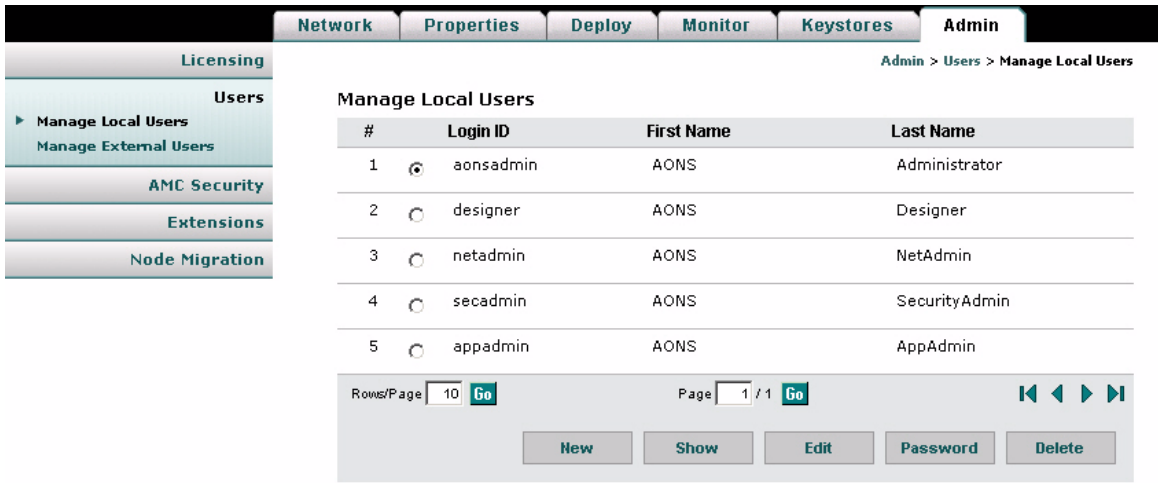
Local users are created and managed by the AMC. You can use this page add to perform the following tasks:

- 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 6-2 shows this page

Figure 6-2 Manage AMC Local Users



Actions to Take

Click one of the following buttons:

- **New**—creates a new users. See Creating New Users, page 6-4
- **Show**—displays information on the selected user. See Displaying Information on Users, page 6-5
- **Edit**—changes information about the selected user. See Editing Users, page 6-6
- **Password**—changes the password of the selected user.
- **Delete**—removes the selected user from the system.

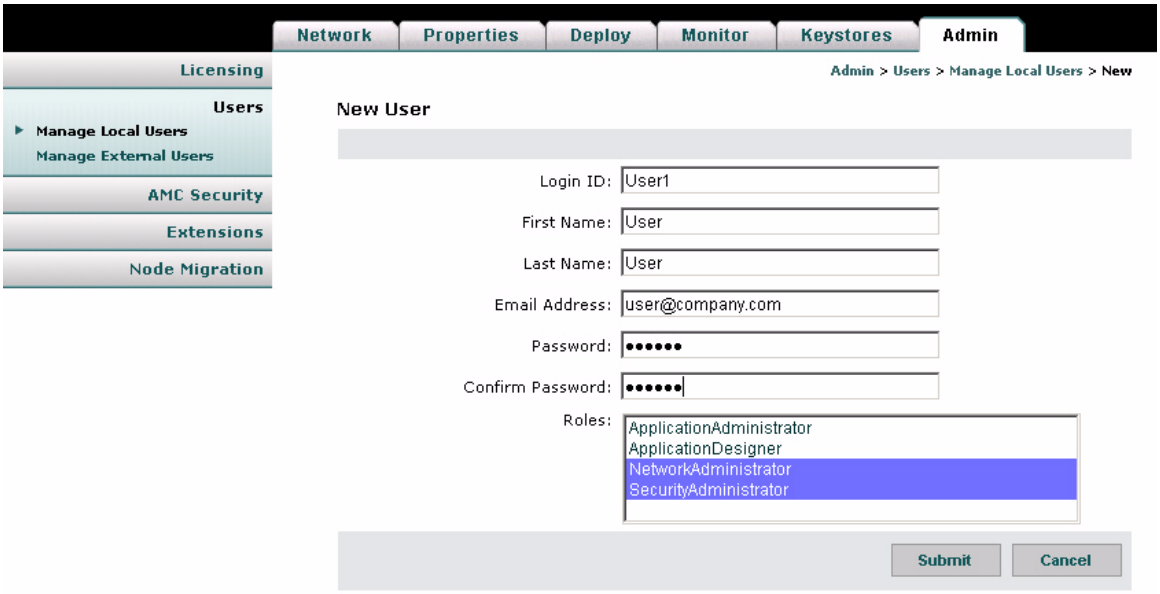
Creating New Users

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 6-3 shows the New User page.

Figure 6-3 New User



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 6-6.

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

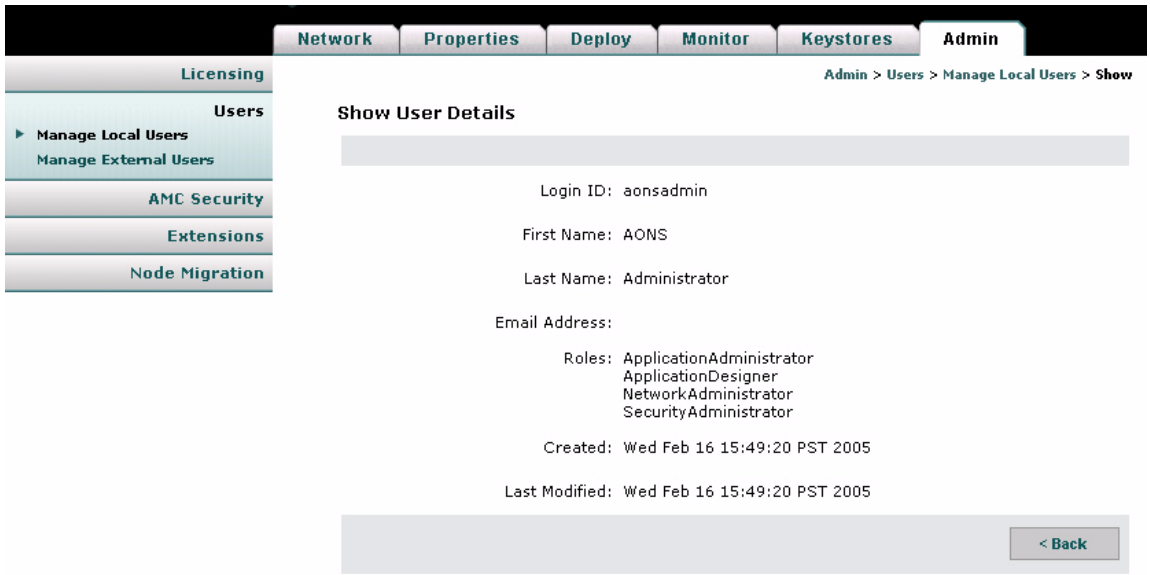
Displaying Information on Users

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 6-4 shows the Show User Details page.

Figure 6-4 Show User Details



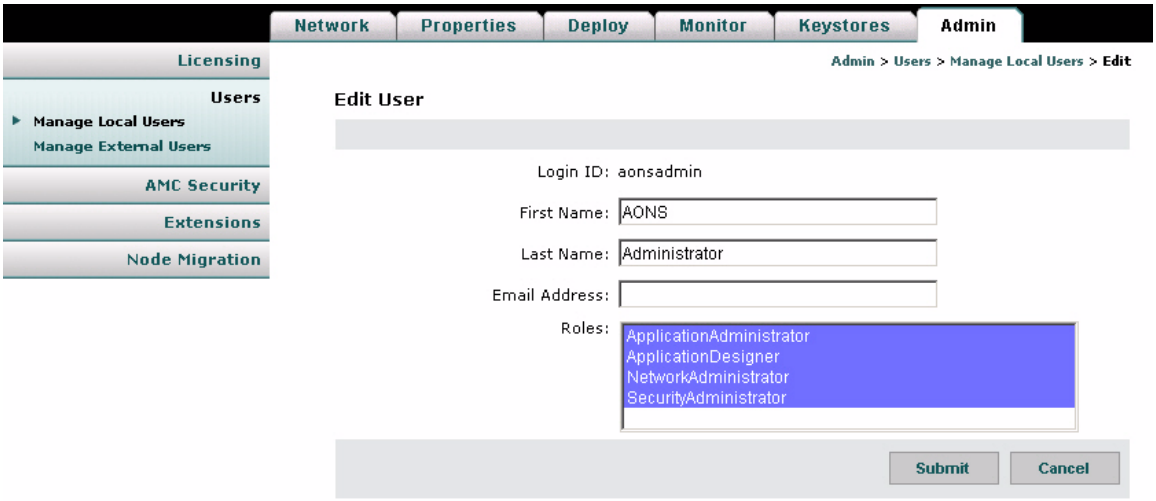
Editing Users

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 6-5 shows the Edit Local User page.

Figure 6-5 Edit Local User



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 6-1 shows the roles available in AMC, and the sections on each tab these roles can access.

Table 6-1 AMC User Roles

Role	Network Tab	Properties Tab	Deploy Tab	Monitor Tab	Keystores Tab	Admin Tab
Application Administrator	—	• Adapter • Application • JMS • Monitoring • Service Profiles	• All	• All	—	• All
Application Designer	—	—	—	—	—	• Extensions

Table 6-1 AMC User Roles (continued)

Role	Network Tab	Properties Tab	Deploy Tab	Monitor Tab	Keystores Tab	Admin Tab
Network Administrator	• All	• Monitoring	—	• All	—	—
Security Administrator	—	• Authentication and Authorization • Security	—	• All	• All	• Users • AMC Security

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

- Creating New Users, page 6-4
- Editing Users, page 6-6
- Assigning Roles to External Users, page 6-9

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 6-7
2. Assigning Roles to External Users, page 6-9
3. Creating an Authentication Realm, page 6-10

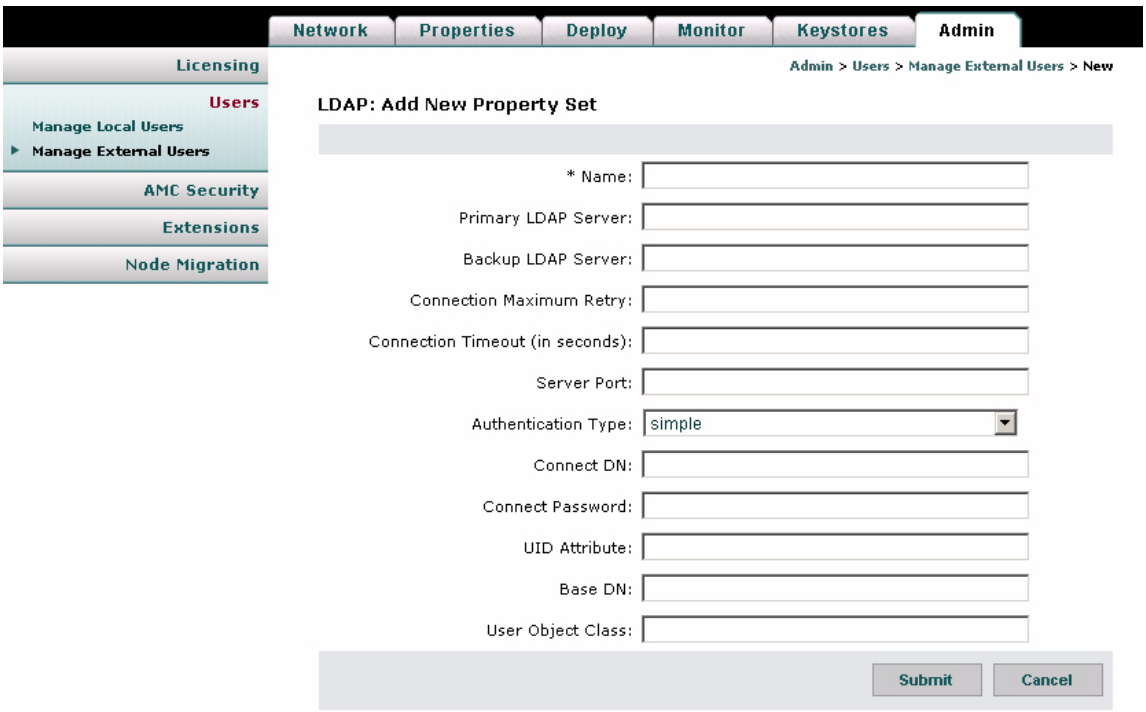
Creating an LDAP Profile

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 6-6 shows the LDAP page.

Figure 6-6 LDAP Property Set



Actions to Take

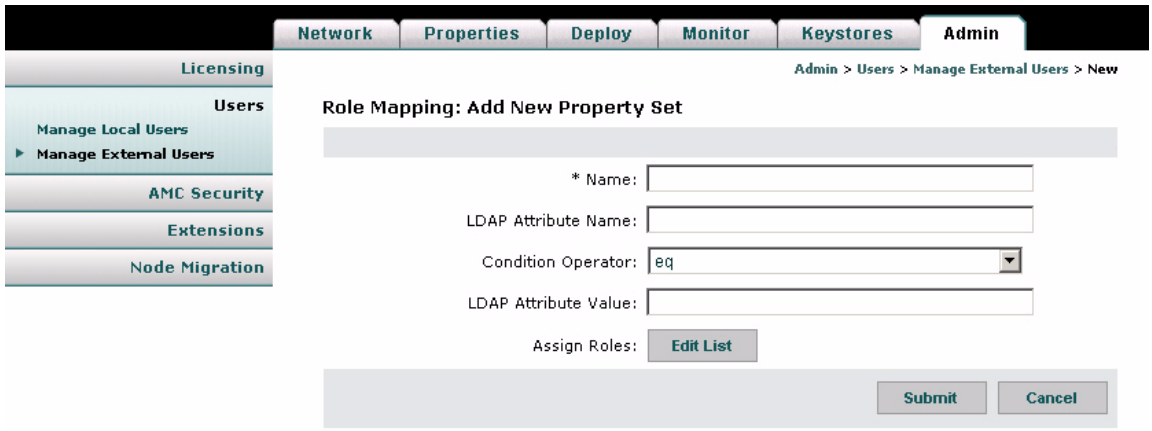
Complete the fields as appropriate for the LDAP server being used. Contact your LDAP administrator for details.

Assigning Roles to External Users

How to Get There

Go to **Admin > Users > Manage Local Users > Role Mapping**, then click the **New** button. Figure 6-7 shows the Role Mapping page.

Figure 6-7 Role Mapping



Data to Enter

Table 6-2 shows the field of the Role Mapping page.

Table 6-2

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: • 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 fields, click the **Submit** button to save your changes.

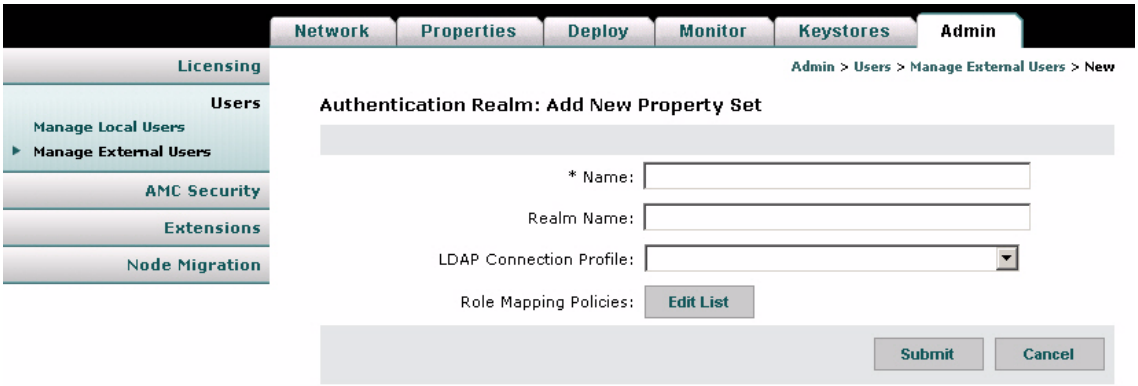
Creating an Authentication Realm

The LDAP Authentication Realm binds the LDAP information specified in the "Creating an LDAP Profile" section on page 6-7 with the role mapping information specified in "Assigning Roles to External Users" section on page 6-9.

How to Get There

Admin > Users > Manage Local Users > Authentication Realm, then click the **New** button. Figure 6-8 shows the Authentication Realm page.

Figure 6-8 Authentication Realm



Data to Enter

Table 6-3 shows the Authentication Realm page.

Table 6-3 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 6-7 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 6-9 to create a new property set.

Actions to Take

After completing the fields, 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 AMC Certificates

The AMC Security Page enables you to manage the keypairs and certificates used by AMC for secure communication.

- **Keypairs**–view, edit, or delete keypairs that have been assigned to AMC.
- **Public Certificates**–view, edit, or delete public certificates that have been assigned to AMC.
- **Root Certificates**–view, edit, or delete root certificates that have been assigned to AMC.

Note If no keypairs or certificates are present, you must use the Keystores tab to generate them.

Managing Extensions

The Extensions page enables you to upload custom software to adapt your AON environment to the specific business needs of your network. This page provides the ability to upload the following:

- Adapter Packages
- Adapter Extension Packages
- JMS Resources
- Schema Packages
- Transform Packages
- Transform Parser Packages

Note Before you can upload an extension with AMC, you must use AON Development Studio to package it.

For more information about developing and packaging extensions, see the *AON Programming Guide.*

APPENDIX A

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 5-17.

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
```

A

AbstractCustomBladelet — Basic custom bladelet class. It implements the CustomBladelet interface and must be included in all new custom bladelets. See Custom Bladelet API, page -6.

ACK — Short message that acknowledges receipt of a message.

AccessDB — Security bladelet that makes JDBC callouts to external databases. This bladelet can execute basic SQL queries against Oracle/Sybase databases. It outputs the query results in case of select queries and the update count in case of insert/update/delete queries. See Bladelet, page -3.

AccessHTTP — Security bladelet that makes HTTP GET/POST callouts to HTTP servers. With a similar function, Send is the preferred bladelet for sending out HTTP requests. See Bladelet, page -3.

Adapter — Adapters process a variety of network traffic including industry standard and custom protocols. AON has a set of built-in adapters to handle these formats. In addition, you can use the Custom Adapter API to create a custom adapter.

Adapter Package — Package, included in Custom Adapter API, whose interfaces provide definitions for all constants (adapter request, response, protocol, and so on) used by the adapter, get the adapter context, define adapter types (such as embedded, standalone, and start up model), define the adapter manager, listen for events, obtain connection information (ConnectionID, Reader, SourceIP, SourcePort, Writer, and SSLCertificate), define the connection receiver, return the DeliveryContext, define the outbound delivery group, and so on. For more information, see package, page -12 and Custom Adapter API, page -5. Also, see “Custom Adapter API Specification” in Chapter 4. Custom Adapters of the *AON Programming Guide*.

Administrator — Super user of the AON Management Console.

ADS — AON Development Studio (ADS) is the graphical user interface used to create (and update) PEPs for upload to AMC. The main components of the ADS are the PEP Explorer, Navigator, PEP Developer, Problems, and the Repository.

AES128/192/256 — Advanced Encryption Standard (AES) is a encryption algorithm that secures information as it passes over a network. 128, 192, and 256 indicates the number of bits used by the key.

Algorithm — An algorithm is a set of predefined rules or processes for solving a problem or performing a specific task. For examples, see DSA, page -7, RSA, page -14, and SHA1, page -15.

Alias — Typically, an alias is a user friendly name for an item such as a program component for function. AON incorporates many aliases. For example, message protocols are sometimes identified by aliases (see “Protocol Alias” in the *AON Programming Guide*).

AMC — A Web-based application, AON Management Console (AMC) is used to manage the AON installation, upgrade, and operation.

A

ANT Ant is a scripting tool that is used to compile and run Java programs.

AON Application Oriented Network.

AONSCommon AONSCommon software is in conjunction with the Custom Bladelet API, Custom Adapter APIs, External Service API, XSLT Transformation SDK, and Schema Validation SDK. This key file includes the following packages:

Exception Package, page -7

External Services API, page -8

PEP Package, page -13

Log Package, page -10

Message Package, page -11

Net Package, page -12

Utilities Package, page -17

XPath Engine Package, page -18

For more information, see Appendix A. AONSCommon Specification in the *AON Programming Guide*.

AON-SM AON service module for Catalyst 6500 Series Switches.

AON node A switch or router running configured to perform application-oriented networking.

AON-NM AON network module for Cisco 2600, Cisco 2800, Cisco 3700, and Cisco 3800 series routers.

AONSTransformer An External Services API interface that defines a transformer object in AON to perform transformation services. The interface takes XML data as input (SAXSource or DOMSource) and puts the transformed result in the target result object. AONSTransformer is implemented in the AON transformation service that provides XSLT based transformation in AON. An AON transformer object is created by AONSTransformerFactory. See External Services API, page -8and “APIs” in Chapter 5. Transformation of the *AON Programming Guide*.

AONSTransformerFactory An External Services API class that defines a factory for an AONSTransformer object. Each type of transformation implements this interface to provide a specific transformer object factory. The Transformation bladelet is included in message PEPs to provide transformation services. See External Services API, page -8.

API Application programming interface. AON is supplied with many Java-coded APIs such as the custom bladelet and custom adapter APIs. The *AON Programming Guide* describes the APIs supplied with AON.

Asynchronous message An asynchronous message is transmitted intermittently instead of in a steady stream. For example, a one way message is usually asynchronous because it may occur unpredictably and does not require a response.

A

Authenticate

Security bladelet that authenticates various credentials from the Identity bladelet. An HTTP header or SOAP message are among the variety of sources that the Authenticate bladelet can obtain identities from. See Bladelet, page -3.

Authentication

A process that checks user credentials. Authentication is also an External Services API class that authenticates given user credentials. See External Services API, page -8.

Authorize

Security bladelet that computes authorization decisions and enforces authorization decisions on incoming message. Authorize supports three different authorization mechanisms: SAML based, LDAP group based, and rule based authorization.

B

Balance Load

Routing bladelet that uses one of four different algorithms to decide which particular end point should receive the next message. It updates the destination URI of the message based on the algorithm. The Send bladelet that follows the BalanceLoad bladelet sends the message to the chosen destination. See Bladelet, page -3.

BAR

Bladelet archive file. This file (.bar) contains metadata about a bladelet. See SCAR, page -14.

Bladelet

A bladelet is a piece of software that performs a specific message handling function. Bladelets are combined together into PEPs. The ADS is used to combine bladelets into PEPs. You can create a custom bladelet by following directions in the *AON Programming Guide*. AON is supplied with the bladelets grouped by type and listed below.

PEP Markers—Exception PEP Marker and Response Marker

External Access—AccessDB and AccessHTTP

General—Log, Cache Data, and Retrieve Cache

Logic—Find and Branch

Message Handling—Validate, Build Composite Content, Discard, Create Message, Update Message, Create Content, Extract Composite Content, and Create Response.

Routing—Distribute, Set Destination, Send and Balance Load.

Security—Authorize, Encrypt, Verify Signature, Sign, Bladelet, Identity, Authenticate, and Verify Identity.

Transformation—Transform.

For more information, see the “AON Bladelet Reference” in *AON Development Studio Guide*.

bladelet archive file

AON bladelets are defined in bladelet archive (.bar) files. This file stores meta-data about one or more bladelets. When a message PEP is constructed, the ADS uses information in the bladelet archive file to generate user interface and other code. The bar file is also used at runtime to load the bladelet name and class name.

B

bladelet parameters AON bladelet parameters are displayed in the ADS by right-clicking on a bladelet icon (displayed in the PEP developer) and selecting Bladelet Properties. The resulting window displays parameter information and enables you to change some of them.The display is partially determined by the bladelet-info.xml file. In the file, parameters are grouped hierarchically by <configuration-group>, <configuration-subgroup>, <parameter-group>, and <parameter>.

bladelet-info.xml Provided with AON, the bladelet-info.xml contains definitions of all supplied bladelets.

Branch Logic bladelet that evaluates a set of conditions and activates the bladelet's output port corresponding to the rule that evaluates to true. This should be used to implement if-then-else structure within a PEP. See Bladelet, page -3.

Build Composite Content Message Handling bladelet that creates a multipart content from the given input message and the parts that need to be added, deleted, or overwritten. See Bladelet, page -3.

C

Cache Data General purpose bladelet that sets data into the named caches configured on an AON node. The named caches are “response” and “variable”. The response cache caches server responses. The variable cache caches PEP variables. Data from the named caches can be retrieved using the RetrieveCache bladelet. In addition, data from the variable cache can be retrieved using the Caching Service API exposed to Custom Bladelets. See Bladelet, page -3.

CacheService An External Services API interface that puts the object into a cache, gets the object from the cache, and removes the object from the cache. The object cache (local to each blade) is shared across PEPs and PEP instances and uses the LRU replacement algorithm. See External Services API, page -8.

Caching The ability of an AON node to store frequently-used content locally and make it available for future requests.

Certificate The public half of an asymmetric key algorithm key pair (the “public key”), together with identity information such as a person's name, email address, title, phone number, an so forth. A certificate is digitally signed by a person or entity, binding the public key to the entity described by the attributes.

Class A class is a category of objects such as program elements. A class is not an object; instead, it is used to create (instantiate) object instances of itself. AON classes are grouped together into packages. The properties and operations of a class instance are largely determined by its methods. For more information, see the descriptions of exposed AON packages and classes in the *AON Programming Guide*.

Compression An External Services API interface that compresses and decompresses input data. See External Services API, page -8.

Content-based routing The process for determining the destination of a message based on its content.

ContentLookup An External Services API interface that evaluates regular expressions on the given content and produces a collection of objects. See External Services API, page -8.

C

Content Parser — A content parser plug-in extension that parses input data and converts it to an equivalent XML format on which AON XSLT transformation can be applied.

ContentValidation — An External Services API that validates the input document with the given XML schema or DTD (document type definition). Schema-DTD meta data is stored in the AON network node profile as domain (property) sets. AON parses XML grammar, already stored in cache. Policies are stored in attribute domain files as com.cisco.aons.policies.validation.ContentValidation. See External Services API, page -8.

Create Content — Message Handling bladelet that updates an existing AON message in the PEP. You can use this bladelet to update the destination, content or the headers of the message. Create Content can update the payload of the incoming message or modify header information as it is forwarded on to an end-point or to the client. See Bladelet, page -3.

Create Message — Message Handling bladelet that creates a new AON message in a PEP. Typically, adapters create messages at input and output points. See Bladelet, page -3.

Create Response — Message Handling bladelet that tags an existing AON message in a PEP as the response message that has to be sent back to the client. Ordinarily, response messages by a Send or Distribute bladelet in a PEP. You can also use Create Message to handcraft response messages without involving an end point. RetrieveCache can put a response message into the PEP that was previously cached by the CacheData bladelet. In PEPs that do not involve Send and Distribute, Create Response is used to mark a particular message as the response message. See Bladelet, page -3.

Credentials — Information that identifies a user, message component, or program element. For example, the AON Authentication interface verifies given user credentials.

custom adapter — AON Custom Adapter Software Development Kit (SDK).

Custom Adapter API — APIs that are used to develop embedded or standalone custom adapters. This set includes the following packages:

Adapter Package, page -1

IO Package, page -9

Message Package, page -11

Utilities Package, page -17

Exception Package, page -7

Utilities Pool Package, page -17

For more information, see “Custom Adapter API Specification” in Chapter 3. Custom Adapters of the *AON Programming Guide*.

Custom Bladelet — The AONS custom bladelet SDK is used to create new bladelets (“custom bladelets”) that may be included in PEPs. Custom bladelets are uploaded to the AMC during synchronization.

Also, part of the CustomBladelet API. This basic custom bladelet interface must be included in all new custom bladelets. It accesses PEP variables via methods that get and set context data. See Custom Bladelet API, page -6.

C

Custom Bladelet API

A package that may be used by developers to create new bladelets. The package includes the following components:

AbstractCustomBladelet, page -1

Custom Bladelet, page -5

CustomBladeletContext, page -6

PEPData, page -13

For detailed information, see “Custom Bladelet API Specification, in Chapter 2. Custom Bladelets of the *AON Programming Guide*.

CustomBladeletContext

Part of the Custom Bladelet API. This interface provides context to the custom bladelet. It passes variables, gets PEP details, sets output path and logs messages.

D

data type

Defines the type of data. A variety of data types are used in AON including AON-specific (AONSubject, Content, MessageTypeInfo, PlatformInfo, SecurityContext, and so on) and Java-standard data types (for example, boolean). The DataType.xml file defines all data types used in AON. AON-specific data type are described in Appendix B. AON Data Types in the *AON Programming Guide*.

Decrypt

Security bladelet that decrypts encrypted XML, SOAP or non-XML messages as well as attachments. See Bladelet, page -3.

Decryption

Decryption reverses Encryption action, decrypting a previously encrypted message making it human-readable. See External Services API, page -8.

DES

Data Encryption Standard. Cryptographic algorithm developed by the U.S. National Bureau of Standards.

Discard

Message Handling bladelet that informs AON when PEP processing should stop and the connection to the client be closed. This bladelet should not be used after Send or Distribute. This is useful mainly with a CreateMessage or RetrieveCache. It may also be used when the PEP has multiple Sends and based on some logic, one of the replies needs to be picked. See Bladelet, page -3.

Distribute

Routing bladelet that sends the same message over to multiple end-points. Distribute is a terminal bladelet. In a PEP, no bladelet can follow Distribute. For request-response PEPs, it gathers the responses, chooses one based on a selection criteria, and sets it as the response message. See Bladelet, page -3.

DNS

Domain Name System. This is the system used on the Internet to translate names of network nodes into addresses.

D

DSA Digital signature algorithm.

DTD Document type definition. AON can be configured to validate only those incoming XML messages that contain a DTD (.dtd file) declaration or schema reference or both. The DTD or schema meta data is stored in the AON network node profile as domain (property) sets.

E

Embedded Adapter An adapter that is tightly integrated with the AON framework and may use all AON resources. An embedded adapter opens a socket and reads a stream of data off it. See Standalone Adapter, page -16.

Encrypt Security bladelet that encrypts either parts of or the entire input message to maintain data integrity. Parts of an XML or SOAP message can be encrypted by specifying the XPath locations of the elements to be encrypted in the message. AON can encrypt XML, SOAP and non-XML messages and their attachments. See Bladelet, page -3.

Encryption Encryption obscures information, making it unreadable without special knowledge. The External Services API Encryption encrypts message input and decrypts previously encrypted documents. See External Services API, page -8.

Exception Package A Custom Adapter API interface that gets the exception type, provides exception services, provides runtime exception services, and identifies exception conditions to be caught. See Custom Adapter API, page -5.

Also, an AONSCommon Exception package that includes a class that return the exception type and the following exceptions:

AONSException—Exception returns AONSException, get arguments, get error codes, and so on.

AONSRuntimeException—Exception that handles AON runtime exceptions. AONSRuntimeException inherits methods from java.lang and has a set of constructors.

ExtServiceException—Exception that indicates conditions that service clients are expected to catch. ExtServiceException inherits methods from java.lang and has a set of constructors.

InitializationException—Exception that handles exceptions that occur during AON initialization. InitializationException inherits methods from java.lang and has a set of constructors.

NoSuchVariable—Exception that handles calls to non-existent PEP variables.

See AONSCommon, page -2 and “Exception Package” in Appendix A. AONSCommon Specification in the *AON Programming Guide*.

Exception PEP Marker PEP Marker bladelet that tracks and records exceptions in the PEP. It is a good way to create instances that can be stored as database records to audit exceptions as information is routed through the PEP. See Bladelet, page -3.

Explicit mode

A deployment in which an AON node processes messages exchanged by two entities with the knowledge of those entities. The sender and receiver of a message are configured to communicate with the AON nodes.

External Services API

Each AON service operates through a set of APIs. Customers and partners can expand existing AON service functions by creating custom bladelets that operate in a message Policy Execution Plan (PEP). The External Services APIs can be incorporated into custom bladelets and adapters to provide these extended services. The AON External Services package incorporates the following Java-coded interfaces:

AONSTransformer, page -2

AONSTransformerFactory, page -2

Authentication, page -3

CacheService, page -4

Compression, page -4

ContentLookup, page -4

ContentValidation, page -5

Encryption, page -7

ExtService, page -8

ExtServiceContent, page -9

ExtServiceProfile, page -9

MessageLog, page -10

MIME, page -12

ServiceFactory, page -15

Signature, page -15

Transform, page -16

Although the External Services API is part of the AONSCommon, it is separately discussed in the AON Programming Guide in the “External Services API Specification” in Chapter 4. External Services.

Extensibility

You can enhance AON capabilities by creating several types of extensions: custom bladelets, custom adapters, XSLT transformations, and schema validations. Extensions are packaged in ADS and uploaded to AMC for use at AON nodes. See External Services API, page -8.

Extract Composite Content

Message Handling bladelet that extracts the contents from a multipart content message. See Bladelet, page -3.

ExtService

An External Services API interface that gets the name and profile of a service. See External Services API, page -8.

ExtServiceContent An External Services API interface that gets message context name, attribute information, and set attributes. See External Services API, page -8.

ExtServiceProfile An External Services API interface that sets the context and get the profile name, service names, contexts defined in the profile, and current context. See External Services API, page -8.

F

Find Logic bladelet that queries an XML message and extracts all nodes identified by regular (for regular expressions, the message type does not need to be in XML format) and XPath expressions from the message currently being processed by the PEP. After regular and common XPath expressions are evaluated by this bladelet, they may be used by other bladelets. See Bladelet, page -3.

I

Identity AON messages can use several types of claims or proof of identity. These items are generically referred to as "subjects." This Security bladelet can extract all subjects of specified types from the message being processed by the PEP. See Bladelet, page -3.

Interface AON has user and software interfaces. The AMC and ADS are managed through GUI user interfaces. AON software interfaces (also generally referred to as APIs) are used by programs or applications to connect to other pieces of internal or external software or hardware and exchange data updates (such as synchronization), message requests and responses, notifications, pings, and so forth.

IO Input-output.

IO Package Package in the Custom Adapter API. This package has components for defining the adapter reader for reading and writing data, encapsulating the native buffers, defining the adapter buffer manager, and defining a read-only view of the IAONSBuffer. For more information, see "Custom Adapter API Specification" in Chapter 3. *AON Programming Guide*. Also, see Custom Adapter API, page -5.

J

Jar file Java archive files. You can open JAR files with a standard ZIP application (such as WinZIP).

JDBC Java Database Connectivity.

L

LDAP Light Weight Directory Access Protocol (LDAP) is used to access information directories. LDAP supports TCP/IP. The AON LDAP Group Based Policy Rules defines Authorization policies based on the subject's group membership in an LDAP directory. See Authorize, page -3.

Log General purpose bladelet that provides logging services to capture information about the message and PEP that includes properties of the message, contents of the message and PEP variables. See Bladelet, page -3.

Log Package AONSCommon package that contains a class (Log) to handle AON logging activities. See AONSCommon, page -2 and "Log Package" in Appendix A. AONSCommon Specification in the *AON Programming Guide*.

M

MDS Message Delivery Semantics. AON uses MDS to guarantee reliable and/or ordered delivery of messages based on user-defined message types.

message A document that is exchanged between applications. Within a message, the data fields are enclosed by headers that describe the field context and content. The target server interprets the received message content, extracts the relevant fields, and invokes the needed application process.

MessageLog An External Services API interface that provides database backed logging with predefined schema. In addition to attributes of the request/response message, users can select message contents by XPath. Users can also log Java objects that have appropriate String representation. In addition, message logging can be synchronous or asynchronous. Users can choose a destination from a pre-configured set of data sources configured on AMC. See External Services API, page -8.

Message Package

Package in t he Custom Adapter API. This package has components that create each type of content, decode and encode content, stream content, define a message handler, and implement objects that are attached to IMessageHandler. See Custom Adapter API, page -5.

Message is also an AONSCommon package that contains the following interfaces:

IAONSMessage—Interface serves as a canonical container for representing messages.

ICloseable—Interface that is implemented by classes whose instances are to be tracked in PEP execution and closed at the end of the PEP.

IContent—Top level interface for all content types.

IContentAttachment—Interface that releases any resources held by the attachment.

IContentVisitable—Interface that accepts a content visitor.

IContentVisitor—Interface that visits IContent subtypes.

IContentSerializable—Generic generic interface for serialization of AON message context.

IDeliveryContext—Interface that holds the contextual information of an AONS message.

IEncodingConstants—Interface that handles standard encoded constants where the content is chunked, content-encoded, transfer-encoded, or gzipped.

IMapContent—Interface that maps message content, representing data as name-value pairs.

IMessageBuilder—Interface that builds AON messages.

IMessageConstants—Interface that defines a variety of message constants remote_host, session_id, HTTP_query_string, control message, error message, and so on.

IMessageContext—Interface that maintains the contextual information of a message.

IMessageDeliveryContext—Interface that holds contextual information of an AONS message.

IMessageHeaders—Interface that is a container for message headers.

IMIMEContext—Interface that handles MIME content.

IMsgAttachment—Interface that handles message attachments.

INullContent—Interface that represents all null content.

IRNContent—Interface that gets the signature associated with an envelope and get and set the version.

ISOAPContent—Interface that represents SOAP XML content.

IStreamContent—Interface that represents stream content.

IXMLContent—Interface that creates a container representing an XML document.

See AONSCommon, page -2 and “Message Package” in Appendix A. AONSCommon Specification in the *AON Programming Guide*.

method A method is a procedure that executes when an object receives a message. Methods are associated with classes.

MIME Multipurpose Internet Mail Extensions specification. MIME prescribes formatting for non-ASCII messages (for example, graphics, audio, and video files) that enables them to be transmitted over the Internet. MIME.

MIME is also an External Services API interface that performs add, update, delete, extract operations on MIMEContent. See External Services API, page -8.

N

Navigator In the ADS, the Navigator is a map of your current policy execution plan (PEP). It illustrates the portion of the entire PEP that the PEP Developer window represents and allows you to navigate across different parts of the entire PEP quickly and easily. This is useful when you are creating PEPs that are large and complex because it indicates where you are in the PEP. See ADS, page -1.

Net Package AONSCommon package that defines the Date Format Cache, help to avoid unnecessary list creation, define a multi valued map, define a map like class of strings, provide fast string utilities, provide static utility methods for manipulating types and their string representations, assist with encoding and decoding or HTTP URIs, handles encoding and decoding of MIME “x-www-form-urlencoded” for either the query string of a URL or the content of a POST HTTP request. See AONSCommon, page -2 and “Net Package” in Appendix A. AONSCommon Specification in the *AON Programming Guide*.

Network filter Combination of source IP, source port, destination IP, destination port, and protocol. These elements are used by AON to filter messages and enforce policies.

Node A switch or router running configured to perform application-oriented networking.

Non-repudiation For digital security, non-repudiation indicates that a transferred message has been sent and received by the correct points.

P

package An AONpackage is a set of software that provides a specific type of functionality. AONS is supplied with many packages including the Log Package, Message Package, Net Package, Utilities Package, Exception Package, and others. The ADS is used to create new packages containing all files for a custom bladelet, adapter, schema validation, or transformation (content parser or transform) and upload them. ADS is also used to upload packages to AMC, making them available in AON.

packaging The ADS is used to properly aggregate (package) all the software components of a custom bladelet, adapter, transform, or schema validation so that it can be recognized by AON. The components are collected together into an archive file (for example, a .scar file for a custom bladelet) and subsequently uploaded to AON.

PEP Policy execution plan. A PEP is a sequence of bladelets that determine how a message is processed in AON. ADS is used to create and update PEPs.

P

PEPData Part of the Custom Bladelet API. This class is used to obtain meta information (name, ID, and so forth) about a PEP. See Custom Bladelet API, page -6.

PEP Developer In the ADS, the PEP Developer is used to create PEPs. Bladelets are placed onto the PEP Developer window where they can be connected to other bladelets to create the PEP. The bladelets are represented graphically to provide an easy-to-use design environment. At any given time, multiple PEPs can be displayed. Each PEP appears in the form of a tabbed view in the PEP Developer window. See Bladelet, page -3 and ADS, page -1.

PEP Explorer In the ADS, the PEP Explorer (in the lower left) displays a macro-level view of the PEPs and message types in your current ADS directory. The available PEPs in the PEP Explorer are listed so that you can easily see your current PEP type structure. See ADS, page -1.

PEP Package AONSCommon package that contains an interface (PEPData) to generates meta information about a PEP. See AONSCommon, page -2 and "PEP Package" in Appendix A. AONSCommon Specification in the *AON Programming Guide*.

PEP Variable When a new PEP is created, the PEP Properties window pops up with fields for PEP information including the PEP Variables, Msg_Type, Platform, Request_Message, and System. See PEP, page -12.

policy In AON, a policy is a user-defined or automatic rule or set of rules that narrowly limit specific operations or determine exactly how they will occur. For example, a policy could determine how an adapter connects to an external message queue.

Problems In the ADS, the Problems area is located directly under the PEP Developer window. The Problems area displays alerts that indicate what PEP components need attention. A successful PEP depends on the resolution of these tasks before the PEP can be synchronized to an AMC or saved as a template for future PEP development. See ADS, page -1.

provisioning The process of sending message PEPs and polices from AMC to an AON node.

R

RAM Random access memory.

Repository In the ADS, the Repository is section on the right from which various bladelets can be dragged and dropped onto the PEP Developer window. It display functionally similar bladelets in the same group. See Bladelet, page -3 and ADS, page -1.

Request PEP A PEP that contains bladelets for processing request messages. See PEP, page -12 and Bladelet, page -3.

Response Marker PEP Marker bladelet that marks a point (in a PEP) for responding to a particular action that a message has undergone. It is a useful way to record information based on actual actions within a PEP. See Bladelet, page -3.

Response PEP A PEP that contains bladelets for processing response messages. See PEP, page -12 and Bladelet, page -3.

R

Retrieve Cache General purpose bladelet that retrieves data from two named caches configured on an AON node. The named caches are “response” and “variable”. The response cache caches server responses. The variable cache caches PEP variables. These named caches can be populated using the Cache Data bladelet. In addition, the variable cache can be populated using the Custom Adapter API exposed to custom bladelets. SeeBladelet, page -3.

Reverse proxy caching An AON cache engine that can be used as a proxy cache or reverse proxy cache depending on the cache placement and associated administrative domain. The device-level AMC Caching Property screen (accessed at AMC > Properties > Application > Node and Global) is used to configure the cache engine. This device-level screen is used with PEPs that include the CacheData and RetrieveCache bladelets.

Round-robin A policy that determines how to distribute incoming messages. This policy (in ADS, a type of configuration group) sends messages to destinations identified on a list, one after the other. In ADS, BalanceLoad Properties screens are used to set message distribution to round robin. See Weighted round-robin.

RSA Rural service (or statistical) area.

rule A rule prescribes how an activity will occur. In AON, you can create a variety of rules. For example, when a PEP is constructed in ADS, a Validator rule (part of the bladelet archive file) validates user inputs of parameter values. The rule denies invalid inputs (generally showing an error message) and accepts valid ones. See Authorize, page -3.

S

SAML Security assertion markup language. XML standard that allows a user to log on once for affiliated but separate Web sites. See Authorize, page -3.

sandbox A sandbox is a mechanism for isolating a piece of software, an application, or an entire system from unwanted access or inputs. The AON sandbox feature enables uses to open up various permissions by default and restrict customizable permissions for custom bladelets. At the same time, it protects AON by restricting certain permissions from customization.

SCAR Custom bladelet archive file. This file (.scar) contains the metadata needed to build PEPs and execute a custom bladelet. See BAR, page -3.

schema package A schema package includes the package name, version, vendor name, description, package properties, and one or more schema files, XML schema (.xsd), or Document Type Definition (.dtd) files. The schemas-info.xml file, in the package, defines metadata for schema extensions. For detailed information, see Chapter 6. Schema Validation in the *AON Programming Guide*.

schema validation A way to validate incoming XML messages by comparing them with predefined schemas or DTDs. For detailed information, see Chapter 6. Schema Validation in the *AON Programming Guide*.Also, see ContentValidation, page -5.

SDK Software development kit. You can use these kits to create custom bladelets, adapters, external service extensions, XSLT transformations, and schema validations. See the *AON Programming Guide* for more details.

S

Send Routing bladelet that sends a message to a selected destination. This bladelet performs protocol translation if the destination URI of the message to be sent out has to go out via an adapter that is different from the one which received the message. See Bladelet, page -3.

ServiceFactory An external Services API interface that gets the current service. See External Services API, page -8.

Service-oriented Architecture A platform and language-independent framework which enables enterprise-wide application communications across systems

Service-oriented Computing Service Oriented Architecture (SOA) is an architectural approach to integration. This architecture is defined as a collection of standard software services, available to other applications across the network, and accessible using a standard interface.

service profile A set of attributes that describe a service. Each service has one profile. A profile contains multiple named contexts. AMC screens are used to create named contexts.

The Service API is used to access a context. A supplied interface is used to obtain the attributes of a given context from the profile. A profile is associated with an attribute domain; a context is associated with a property set.

Set Destination Routing bladelet that routes the given message to a destination based on rule evaluation. It updates the input message's destination to be the corresponding to the first rule that evaluates to true. See Bladelet, page -3.

SHA1 Secure hash algorithm version 1.

Sign Security bladelet that creates a digital signature on partial or entire SOAP/XML documents. This bladelet is capable of signing non-XML and multi-part messages. See Bladelet, page -3.

Signature An External Services API interface that signs the input XML document. See External Services API, page -8.

SMTP Simple mail transport protocol.

SOAP Simple Object Access Protocol (SOAP) enables an application on a computer to communicate with an application on another computer, regardless of the operating systems involved. SOAP specifies how the contents of the HTTP header and XML file used in these communications.

SQL Structured query language. This language is used to interact (request information, update d tables, and so on) with databases.

SSL Secure sockets layer. Protocol used for managing the security of a message transmission on the Internet.

S

Standalone Adapter A standalone adapter uses few or none of the resources provided by the adapter framework. When the standalone adapter has received enough information to transform the incoming message into an AON message, it dispatches the AON message. A standalone adapter is well-suited to handle integration with data sources such as databases, message-oriented middleware, and native libraries. See Embedded Adapter, page -7.

synchronization A mechanism for bringing the AMC and ADS into component agreement. Synchronization occurs automatically when you first start ADS. You can also manually select Synchronize on the ADS. The synchronization process downloads PEPs (created on other ADSs) from the AMC to the current ADS. It also uploads newly created PEPs from the current ADS to AMC, making them available for AON.

T

TCP Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack

Transform Security bladelet that transforms AON message content. It can transform an XML message content to an XML or Non-XML content using XSLT Based Transformation mechanism. Further, Non-XML message content can also be transformed to XML or Non-XML message content by providing a content parser extension. See Bladelet, page -3.

Also, an External Services API interface that defines an input source document with the given profile. The interface is implemented by the default transformer in the AON transformation service that provides XSL Transformation (XSLT) based transformation. An AONSTranformer object is created by a com.cisco.aons.service.transform.AONSTransformerFactory. The caller gets an instance of a specific transformer using the particular transformer factory object. Before this service is used, the transform policy must be setup. See External Services API, page -8.

Transparent mode A deployment in which an AON node processes messages exchanged by two entities without the knowledge of those entities. The sender and receiver of a message are configured to communicate with each other, however, the AON node is configured to intercept the message for processing.

Triple DES Triple data encryption standard. More secure version of DES. Uses three stages of encryption. Also known as 3DES.

tunnel Tunneling is the transmission of data intended for use only within a private, usually corporate network through a public network in such a way that the routing nodes in the public network are unaware that the transmission is part of a private network. Tunneling is generally done by encapsulating the private network data and protocol information within the public network transmission units so that the private network protocol information appears to the public network as data.

U

Update Message Message Handling bladelet that updates an existing AON message in the PEP. You can use the bladelet to update the destination, content or the headers of the message. Update Message can be used to update the payload of the incoming message or modify header information as it is forwarded on to an end-point or to the client. See Bladelet, page -3.

URI A URI (Uniform Resource Identifier) is the way you identify any content in the Internet space, whether it be a page of text, a video or sound clip, a still or animated image, or a program. The most common form of URI is the Web page address, which is a particular form or subset of URI called a Uniform Resource Locator (URL). A URI typically describes:

- mechanism used to access the resource
- specific computer that the resource is housed in
- specific name of the resource (a file name) on the computer.

URL URL (Uniform Resource Locator) is the unique Internet address for a file. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

Utilities Package Package in the Custom Adapter API that defines a byte buffer input stream, the byte buffer output stream, and the byte buffer array writer. See Custom Adapter API, page -5.

Also, an AONSCommon package that gets domain information and defines exceptions used by the DomainReader. See AONSCommon, page -2 and “Utilities Package” in Appendix A. AONSCommon Specification in the *AON Programming Guide*.

Utilities Pool Package Package in the Custom Adapter API that has a class to pool jobs. See Custom Adapter API, page -5.

V

Validate Message Handling bladelet that validates XML messages based on a schema (XSD) or DTD. The schema referred by the XML message should have been pre-loaded into AON in an appropriate Schema Extension package using AMC. See Bladelet, page -3.

Verify Identity Security bladelet that determines whether or not identities are trusted by the AON node. See Bladelet, page -3.

Verify Signature Security bladelet that verifies the digital signature contained in XML/SOAP/non-XML message. See Bladelet, page -3.

Virtual cluster A set of AON nodes that is temporarily grouped together. All members of the virtual cluster are treated identically in certain operations (for example, updates). You create virtual clusters in AMC.

W

WCCP Web Cache Communication Protocol. WCCP. A protocol for communication between routers and Web caches.

Weighted round-robin This policy adds weighting to specific addresses in the message distribution list. When a message is transmitted, it is sent to a weighted address instead of the next address in the list. In ADS, BalanceLoad Properties screens are used to set message distribution to weighted round robin. See Round-robin.

WSDL The Web Services Description Language (WSDL) is an XML-based language used to describe the services a business offers and to provide a way for individuals and other businesses to access those services electronically.

WSI Web services intermediary

WS Security WS-Security (Web Services Security) is a proposed IT industry standard that addresses security when data is exchanged as part of a Web service.

X

X509 v3 certificate A certificate that is compliant with the X.509 ITU-T standard for public key infrastructure.

XKMS The XML Key Management Specification (WKMS) is proposed standard from the World Wide Wed Consortium (W3C). It specifies protocols for distributing and registering public keys.

XSLT transformation XSLT Transformation (Transform and Content Parser) enables AON to transform a message or part of a message to fit the requirements at the sending end, receiving end, or both. This feature can be used to transform a XML message to HTML, non-XML to XML, and so forth.

XML XML (Extensible Markup Language) is a flexible way to create common information formats and share both the format and the data on the World Wide Web, intranets, and elsewhere. XML, a formal recommendation from the World Wide Web Consortium (W3C), is similar to the language of today's Web pages, the Hypertext Markup Language (HTML). Both XML and HTML contain markup symbols to describe the contents of a page or file. HTML, however, describes the content of a Web page (mainly text and graphic images) only in terms of how it is to be displayed and interacted with. For example, the letter “p” placed within markup tags starts a new paragraph. XML describes the content in terms of what data is being described.

XPath XML path language is a syntax for addressing portions of an XML document.

XPath Engine Package AONSCommon package for XPath engine processing. Contains interfaces that define a raw stream buffer and an XPath processor. See AONSCommon, page -2 and “XPath Package” in Appendix A. AONSCommon Specification in the *AON Programming Guide*.

XSLT XSLTransformation (XSLT) is a standard way to transform (change) the structure of an XML (Extensible Markup Language) document into an XML document with a different structure. XSLT is a recommendation of the World Wide Web Consortium (W3C).

Z

ZIP ZIP is a popular file compression algorithm that reduces it in size but the reverse of the algorithm will return it to its original form without loss of data.