CHAPTER 4

# Managing AON Security

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



**Note** You must have System Administrator or Security Administrator privileges to perform most of the tasks described in this chapter. Application Administrator and Application Developer have limited abilities on the Keystore Tab. See the "Assigning Roles to Users" section on page 5-3 for further details.

# 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

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.

### How to Get There

Go to **Keystores > Configuration**. Enter your old and new passwords, then click the **Submit** button.

# 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.

### Actions to Take

You can perform any of the following actions:

- Upload a PCKS#12 file. See the "Upload PKCS#12" section on page 4-2.
- Generate and register a MPKI Keypair. See the "Generate and Register a New Key" section on page 4-3.
- Generate a self-signed keypair. See the "Generate a Self-Signed Keypair and Certificate" section on page 4-3.
- Add an SSL Certificate. See the "Generate an SSL Certificate" section on page 4-4.
- Import a keystore from another source. See the "Import a Keypair or Keystore" section on page 4-4.

## 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**.

### Data to Enter

The Upload PKCS#12 File page includes the entries described in Table 4-1.

*Table 4-1 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**.

### What to Enter

The Generate and Register Key page includes the entries described in Table 4-2.

*Table 4-2 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:<br>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. |

### 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 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**.

### 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**.

### 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.

### 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.

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.

Complete the enrollment process to register the certificate generated by AMC.

After completing the process at Verisign, return to the Active Repository in AMC and click the Pending link for your new certificate.

On the screen that loads, click the **Next** button to display the Install SSL Digital Certificate page.

### 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**

### Data to Enter

The Import Keystore page includes the entries described in Table 4-3.

*Table 4-3 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. |

*Table 4-3 Import Keystore Entries (continued)*

| Entry | Description |
|---|---|
| Is Keystore Password Different from Key Alias Password | Click **Yes** or **No** |

### 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 4-5
- Import a Keystore, page 4-6

# 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**.

### Data to Enter

The Add Certificate page includes the entries described in Table 4-4.

*Table 4-4 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 4-4 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

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**.

#### 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.

## SSL Configuration Property

SSL Configuration Property specifies SSL-related parameters to be used by a node.

#### 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 4-6 for details.

#### Data to Enter

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

*Table 4-5 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 of the following properties:<br>• **TLS_v1**—Transport Layer Security version 1 (also known as SSL version 3.1)<br>• **SSL_v23**.— Secure Sockets Layer version 2 or version 3. |
| 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.

### 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 4-6 and the "SSL Configuration Property" section on page 4-6 for details.

### Data to Enter

The SSL Binding property page includes the entries described in Table 4-6.

*Table 4-6 SSL Binding Property Entries*

| Entry | Description |
|---|---|
| Source IP Address | IP address of source. |
| Source Netmask | Netmask of source in dot-decimal notation. |
| Destination IP Address | IP address of destination. |
| Destination Netmask | Netmask of destination in dot-decimal notation. |
| 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. |

*Table 4-6 SSL Binding Property Entries (continued)*

| Entry | Description |
|---|---|
| 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. |
| 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 4-8
- Configuring Kerberos, page 4-9


## 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**

#### 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**.

**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.**

**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**.

**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.

**Step 6** Click the **Submit** button to save your changes.

---