Configuring Trusted Points

This section includes the following topics:

Trusted Points

When setting up LDAP over Secure Sockets Layer (SSL) protocol for VNMC user authentication, you need to create a trusted point for each LDAP server. The certificate in the trusted point can be any one of the following:

- The certificate of the certificate authority (CA) that issued the LDAP server certificate.
- If the CAs are organized in a hierarchy, the certificate of any of the CAs in the hierarchy.
- The certificate of the LDAP server.

Configuring Trusted Points

Creating a Trusted Point

Procedure

Step 1 Choose **Administration > Access Control > Trusted Point**.

Step 2 Click **Create Trusted Point**.

Step 3 In the Create Trusted Point dialog box, complete the following fields, then click **OK**.

Field	Description
Name	Trusted point name.

Field	Description
Certificate Chain	Certificate information for this trusted point.

Editing a Trusted Point

Procedure

Step 1 Choose **Administration > Access Control > Trusted Point**.

Step 2 In the content pane, choose the required trusted point, then click **Edit**.

Step 3 In the Edit dialog box, modify the certificate chain as appropriate, then click **OK**.
The Name and Fingerprint fields cannot be modified.

Deleting a Trusted Point

Procedure

Step 1 Choose **Administration > Access Control > Trusted Point**.

Step 2 In the content pane, select the trusted point you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.