

Configuring a Secure Access LDAP Server Instance (NSM Procedure)

The Secure Access device supports two LDAP-specific authentication options:

- **Unencrypted**—the device sends the username and password to the LDAP Directory Service in clear and simple text.
- **LDAPS**—the device encrypts the data in the LDAP authentication session using the Secure Socket Layer (SSL) protocol before sending it to the LDAP Directory Service.

To configure an LDAP server instance:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure an LDAP server instance.
3. Click the **Configuration** tab and select **Authentication > Auth Servers**. The corresponding workspace appears.



NOTE: If you want to update an existing server instance, click the appropriate link in the Auth Server Name box and perform the Steps 5 through 8.

4. Click the **New** button. The New dialog box appears.
5. Specify a name to identify the server instance.
6. Select **LDAP Server** from the **Auth Server Type** list.
7. Configure the server using the settings described in Table 1.
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 1: Secure Access LDAP Server Instance Configuration Details

Option	Function	Your Action
LDAP Settings > Basic Settings tab		
LDAP Server	Specifies the name or IP address of the LDAP server that the Secure Access device uses to validate your users.	Enter the name or IP address of the LDAP server.
LDAP Port	Specifies the port on which the LDAP server responds. NOTE: This port is 389 when using an unencrypted connection and 636 when using SSL.	Set the port for the LDAP server.

Table 1: Secure Access LDAP Server Instance Configuration Details (continued)

Option	Function	Your Action
Backup LDAP Server1	Specifies the parameters for backup LDAP server1 (optional). NOTE: The device uses this type of server for failover processing. Also, backup LDAP server must be the same version as the primary LDAP server.	Enter the IP address of the backup LDAP server1. NOTE: We do not recommend entering hostname as it may accelerate failover processing by eliminating the need to resolve the hostname to an IP address.
Backup LDAP Port1	Specifies the parameters for backup LDAP port1.	Enter the port number for the backup LDAP port1.
Backup LDAP Server2	Specifies the parameters for backup LDAP server2 (optional).	Enter the IP address of the backup LDAP server2.
Backup LDAP Port2	Specifies the parameters for backup LDAP port2.	Enter the port number for the backup LDAP port2.
LDAP Server Type	Specifies the type of LDAP server that you want to authenticate users against.	Select the type of LDAP server from the drop-down list.
Connection	Specifies whether or not the connection between the Secure Access device and LDAP Directory Service should be unencrypted, use SSL (LDAPs), or should use TLS.	Select the type of connection from the drop-down list.
Connection Timeout (seconds)	Specifies how long you want the Secure Access device to wait for a connection to the primary LDAP server first, and then each backup LDAP server in turn.	Set the time required for the connection to time out.
Search Timeout (seconds)	Specifies how long you want the Secure Access device to wait for search results from a connected LDAP server.	Set the time required for the search to time out.
LDAP Settings > Authentication tab		
Authentication required to search LDAP	Specifies if the device needs to authenticate against the LDAP Directory Service to perform a search or to change passwords using the password management feature.	Select LDAP Settings > Authentication > Authentication required to search LDAP to enable this option.
Admin DN	Performs an anonymous search on the LDAP server with an authentication.	Enter the admin DN name.
Password	Specifies the password for the admin DN name.	Enter the password.
LDAP Settings > Finding User Entries tab		

Table 1: Secure Access LDAP Server Instance Configuration Details (continued)

Option	Function	Your Action
Base DN	Starts searching for user entries.	Enter a base DN name. For example, DC = eng, DC = Juniper, DC = com .
Filter	Fine tunes the search.	Enter a filter value. For example, entersamAccountname = < username > or cn = < username > . NOTE: <ul style="list-style-type: none"> ■ Include < username > in the filter to use the username entered on the sign-in page for the search. ■ Specify a filter that returns 0 or 1 user DN's per user; the device uses the first DN returned if more than 1 DN is returned.
LDAP Settings > Determining Group Membership tab		
Base DN	Starts searching for user groups.	Enter a base DN name.
Filter	Fine tunes the search for a user group.	Enter a filter value.
Member Attribute	Identifies all the members of a static group.	Enter a name if you want to identify all the members of a static group. For example, enter member uniquemember (iPlanet-specific) .
Reverse group search	Starts the search from the member instead of the group.	Select LDAP Settings > Determining Group Membership > Reverse group search to enable this option.
Query Attribute	Specifies an LDAP query that returns the members of a dynamic group.	Enter a name for the query attribute. For example, enter memberURL .
Nested Group Level	Specifies how many levels within a group to search for the user. NOTE: The higher the number, the longer the query time, so we recommend that you specify to perform the search no more than two levels deep.	Set the number for the search query time.

Table 1: Secure Access LDAP Server Instance Configuration Details (continued)

Option	Function	Your Action
Nested Group Search	<p>Specifies the types of nested group searches available. They are:</p> <ul style="list-style-type: none"> ■ Nested groups in Server Catalog — This option is faster because it can search within the implicit boundaries of the nested group. ■ Search all nested groups — With this option, the device searches the Server Catalog first. If the device finds no match in the catalog, then it queries LDAP to determine if a group member is a sub-group. 	Select any one type of nested group search from the drop-down list.
LDAP Settings > Meetings tab		
User Name	Specifies the username attribute for the LDAP server.	Enter the username for the server. For example, SamAccountName for an Active Directory server or uid for an iPlanet server.
Email Address	Specifies the e-mail attribute for the LDAP server.	Enter the e-mail address for the server.
Display Name, Attributes	Specifies if there are any additional LDAP attributes whose contents you want to allow meeting creators to view (optional).	<p>Enter a name. For example, to help the meeting creator easily distinguish between multiple invitees with the same name, you may want to expose an attribute that identifies the departments of individual users.</p> <p>NOTE: Enter the additional attributes one per line using the format: DisplayName,AttributeName. You may enter up to 10 attributes.</p>
Server Catalog > Expressions tab		
Name	Specifies the name that is used to show a list of common LDAP expressions.	Enter a name. For example, cn, uid, uniquemember, and memberof .
Value	Specifies the custom value of the LDAP server.	Enter a value for the LDAP server.
Server Catalog > Attributes tab		
Name	Specifies the name that is used to show a list of common LDAP attributes.	Enter a name for the LDAP attributes.
Server Catalog > Groups tab		

Table 1: Secure Access LDAP Server Instance Configuration Details (continued)

Option	Function	Your Action
Name	Specifies the name that is used to easily retrieve group information from an LDAP server and add it to the server's device server catalog.	Enter a name.
DN	Specifies the base DN name of the group.	Enter a base DN name. NOTE: If you do not know the exact container of your groups, you can specify the domain root as the base DN, such as dc = juniper, dc = com . The search page returns a list of groups from your server that you can use to enter into the Groups list.
Group Type	Specifies the group type.	Select any one group type from the drop-down list.

- Related Topics**
- Configuring a Secure Access RADIUS Server Instance (NSM Procedure)
 - Configuring a Secure Access Anonymous Server Instance (NSM Procedure)
 - Configuring a Secure Access Local Authentication Server Instance (NSM Procedure)

Published: 2009-08-20