

Configuring an Infranet Controller LDAP Server Instance (NSM Procedure)

The Infranet Controller supports two LDAP-specific authentication options:

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

To define 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 Infranet Controller for which you want to configure an LDAP server instance.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Auth Servers**.
4. Add or modify an LDAP server instance as specified in Table 1.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 1: LDAP Server Instance Configuration Details

Option	Function	Your Action
Auth Server Name	Specifies a name for the auth server.	Enter a name for the auth server.
Auth Server Type	Specifies the auth server type.	Select LDAP server .
LDAP Settings > Basic Settings tab		
LDAP Server	Specifies the name or IP address of the LDAP server that the Infranet Controller 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: LDAP Server Instance Configuration Details (continued)

Option	Function	Your Action
Backup LDAP Server1	Specifies the parameters for backup LDAP server1 (optional). NOTE: The Infranet Controller uses this type of server for failover processing. Also, backup LDAP servers 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 Infranet Controller and the LDAP Directory Service should be unencrypted, use SSL (LDAPs), or use TLS.	Select the type of connection from the drop-down list.
Connection Timeout (seconds)	Specifies how long you want the Infranet Controller 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 Infranet Controller to wait for search results from a connected LDAP server.	Set the time required for the search to time out.
LDAP Settings > Authentication tab		

Table 1: LDAP Server Instance Configuration Details (continued)

Option	Function	Your Action
Authentication required to search LDAP	Specifies if the Infranet Controller needs to authenticate against the LDAP directory 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	Specifies the administrator DN.	Enter the admin DN name.
Password	Specifies the password for the admin DN name.	Enter the password.
Strip domain from Windows user names	Removes the domain from a domain\username pair. This feature allows the Infranet Controller to pass the username without the domain to the LDAP server.	Select the check box.
Enable Challenge-Response open protocols	Specifies challenge-response protocol for authentication, if you are configuring this LDAP server instance for noninteractive endpoints.	Select the check box. NOTE: If the LDAP server is configured to limit the rate of password-guessing attacks, and you select the Enable Challenge-Response open protocols check box, the LDAP server's rate-limiting feature is bypassed.
LDAP Settings > Finding User Entries tab		
Base DN	Searches for user entries.	Enter a base DN name. For example, enter DC = eng, DC = Juniper, DC = com .
Filter	Fine tunes the search.	Enter a filter value. For example, enter samAccountname = <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 Infranet Controller uses the first DN returned if more than one DN is returned.
LDAP Settings > Determining Group Membership tab		

Table 1: LDAP Server Instance Configuration Details (continued)

Option	Function	Your Action
Base DN	Searches for user groups.	Enter a base DN name.
Filter	Fine tunes the search for a user group.	Enter a filter value.
Member Attribute	Specifies members of a static group.	Enter a name if you want to identify all the members of a static group. For example, enter memberuniquemember (iPlanet-specific) .
Reverse group search	Specifies that the search starts from the member instead of the group.	Select LDAP Settings > Determining Group Membership > Reverse group search .
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: Because the higher the number, the longer the query time, we recommend that you specify to perform the search no more than two levels deep.	Set the number for the search query time.
Nested Group Search	Specifies the types of nested group search available. They are: <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 Infranet Controller searches the Server Catalog first. If the Infranet Controller finds no match in the catalog, then it queries LDAP to determine if a group member is a subgroup. 	Select one type of nested group search from the drop-down list.
LDAP Settings > Meetings tab		

Table 1: LDAP Server Instance Configuration Details (continued)

Option	Function	Your Action
User Name	Specifies the username attribute for the LDAP server.	Enter the username for the server. For example, enter 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.</p> <p>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, enter 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		
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.	<p>Enter a base DN name.</p> <p>NOTE: If you do not know the exact container of your groups, you can specify the domain root as the BaseDN, such as dc = juniper, dc = com. The search page returns a list of groups from your server, from which you can choose groups to enter into the Groups list</p>

Table 1: LDAP Server Instance Configuration Details (continued)

Option	Function	Your Action
Group Type	Specifies the group type.	Select any one group type from the drop-down list.

- Related Topics**
- Configuring an Infranet Controller RADIUS Server Instance (NSM Procedure)
 - Configuring an Infranet Controller Anonymous Server Instance (NSM Procedure)
 - Configuring an Infranet Controller Local Authentication Server Instance (NSM Procedure)

Published: 2009-08-20