Using LDAP with Sentry Firmware and Sentry Power Manager (SPM)

Table of Contents

Purpose

This technical note provides instructions for configuring the Lightweight Directory Access Protocol (LDAP) when using Sentry firmware with either the Web Interface (GUI) or the Command Line Interface (CLI), or when configuring LDAP using Sentry Power Manager (SPM), version 5.4 or later.

Note: This technical note applies to Server Technology Cabinet Distribution Units (CDUs) only.

Several LDAP-compliant directory types support the LDAP application protocol, however, the scope of this technical note covers LDAP configuration instructions, screen samples, and the required field settings when using the following two primary LDAP directories:

- Active Directory (AD)
- OpenLDAP

LDAP Requirements

To correctly set up LDAP support with Sentry firmware or SPM, a few configuration requirements must be met:

Requirements for LDAP Directory Services:

- Define at least one LDAP group.
- Assign users to that LDAP group.

General LDAP Requirements:

- Set LDAP support to Enabled.
- Define the IP address and domain component of at least one LDAP Directory Services server.
- Select the LDAP bind request method (Simple, TLS/SSL, MD5) used by the Directory Services server.
- Define the IP address of at least one DNS server.
- Test the DNS server configuration using the CDU Ping command.
- For the LDAP groups defined – at least one LDAP group must be defined – assign user access rights to the LDAP groups.

Note: The LDAP group names on the Directory Services server and the CDU must match.

Using LDAP with Sentry Firmware (GUI)

The LDAP authentication process begins with initiating a Sentry firmware session. Configuration of LDAP settings can then be done using the Web interface (GUI) as follows in this section.

Initiate a Sentry Session

Logging in through the Web requires directing the Web client to the configured IP address of the unit.

To Login by Web Interface:

In the Sentry firmware login window, provide your valid username/password.

The default administrative-level user login (admn/admn) was used for this example.

Click **OK**. You are now logged into Sentry firmware's Web interface.

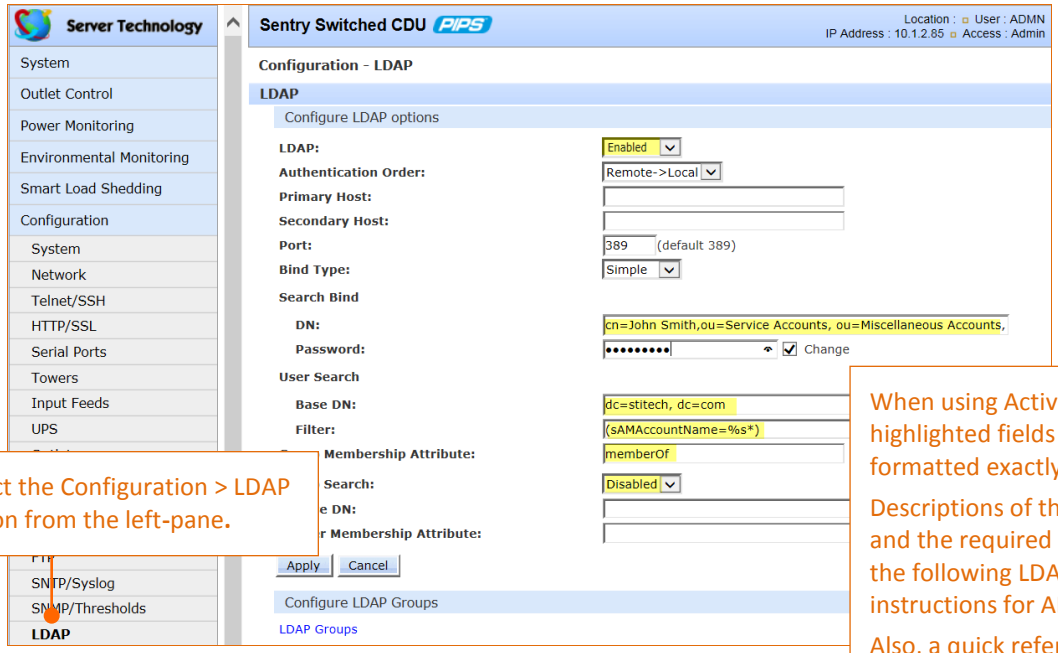
LDAP Configuration

Once you have installed and configured the LDAP Directory Services server, the next step is to configure LDAP using the firmware.

Access the LDAP Configuration Page:

From the left-pane of the interface, go to **Configuration > LDAP**. The following configuration page displays to allow setup and maintenance for all settings that enable LDAP support.

Configuring LDAP with Active Directory (AD):



Select the Configuration > LDAP option from the left-pane.

When using Active Directory (AD), the highlighted fields in this example must be formatted exactly as shown.

Descriptions of these fields, their values, and the required format are provided in the following LDAP configuration instructions for AD.

Also, a quick reference table of field values is displayed after the instructions.

Step-by-step Configuration Instructions:

For the LDAP Options section:

1. From the LDAP drop-down menu, select Enabled.
2. From the Authentication Order drop-down menu, select Remote > Local or Remote > Only.

   Notes:

   - Server Technology recommends not setting the authentication order to Remote Only until LDAP has been configured and tested.
   - With Remote Only, if authentication fails (a communication failure) with the Active Directory server, automatic authentication fallback occurs to authenticate the local user database on the CDU.

3. Provide the Primary/Secondary Host names (IPv4 or IPv6 format). The host names define the network address for the primary/secondary LDAP Directory Services server.
4. The port number receives LDAP requests for the primary/secondary servers you just defined in the previous field. Type the new LDAP server port number, or accept the default port number 389.

For the Bind Type section:

The CDU supports the following three standard LDAP bind types:

- **Simple:** Uses unencrypted delivery of username-password over the network to the LDAP server for authentication, showing user credentials in plain text.
- **TLS/SSL:** (LDAP over TLS/SSL). Uses a trusted authority certificate to provide encryption of LDAP authentication. If this option is selected, MDF binding will be disabled.
- **MD5:** Provides strong protection using 1-way hash encoding that does not transmit the username-password over the network.

5. From the Bind Type drop-down menu, select Simple, TLS/SSL, or MD5.

For the Search Bind section:

By default, Active Directory requires that you specify a bind username and password. The **Distinguished Name (DN)** is the directory path that binds and searches the LDAP directory. Access to the LDAP Active Directory (AD) requires the DN to be in the following comma-separated format:

cn=John Smith, ou=Service Accounts, ou=Miscellaneous Accounts, dc=stitech, dc=com

where…

cn is the common name; the name of the person.
ou is the organizational unit for various accounts, such as service and miscellaneous, organized into units.
dc is the domain component, or individual domain names for the company.

6. Type the DN in the exact format as specified above.

7. Provide the password to use with the DN.

For the User Search section:

The user search base is the level in the Active Directory hierarchy, specified by the User Search Base Distinguished Name (DN), where LDAP begins searching for users, including all sub-trees.

8. For the Base DN, specify the DN (maximum length is 100 characters) in the same format as the domain component (dc) that was provided in the Search bind DN, for example: dc=stitech, dc-com

9. For the Filter, type the filter in the required format. The filter specifies which objects in the hierarchy of the LDAP Active Directory are examined and returned on query. The Active Directory requires the filter to be formatted in parenthesis, maximum string length is 100 characters, and must be in the following format:

(sAMAccountName=%s*)

For the Group Membership section:

10. The Group Membership Attribute finds members of the group(s) that are returned from the specified search. Maximum string length is 30 characters. Type the attribute exactly as required for Active Directory in this format: memberOf

For the Group Search section:

11. From the drop-down menu, select Disabled.

Note: For LDAP configuration using Active Directory (AD), the group search must be Disabled, and the Base DN and User Membership Attribute fields must be blank.

12. After providing the required LDAP settings as described for AD, click **Apply**.

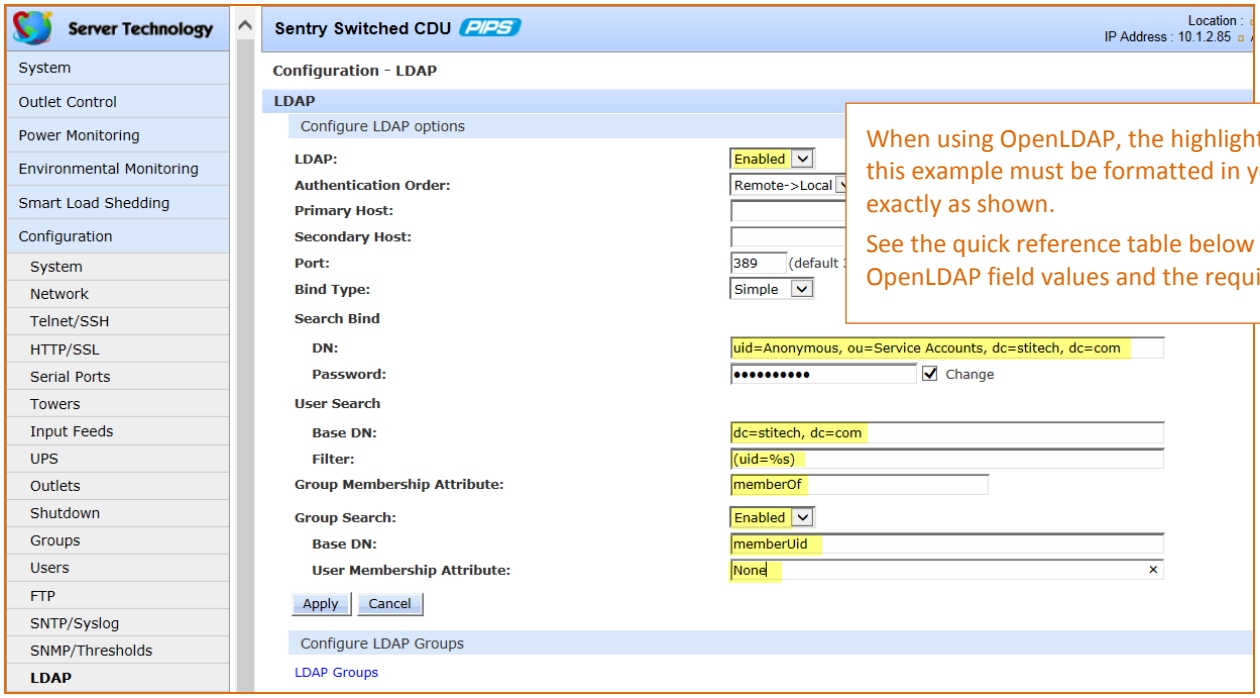
Quick Reference: Firmware Settings for Active Directory (AD)

The LDAP configuration fields in this table are the same fields that were highlighted in the screen example above. For Active Directory, the values must be formatted exactly as follows:

Field	Value Required for Active Directory
LDAP	Enabled
Search Bind DN	cn=John Smith, ou=Service Accounts, ou=Miscellaneous Accounts, dc=stitech, dc=com
User Search Base DN	dc=stitech, dc-com
User Search Base Filter	(sAMAccountName=%s*)
Group Membership Attribute	memberOf
Group Search	Disabled
Group Search Base DN	Must be blank
User Membership Attribute	Must be blank

Firmware Settings for OpenLDAP

If you are using OpenLDAP, you can follow the step-by-step instructions above for configuring LDAP with Active Directory (AD), but note the several highlighted fields below that must be formatted differently for OpenLDAP.



Quick Reference: Firmware Settings for OpenLDAP

The LDAP configuration fields in this table are the same fields highlighted in the screen example above. For OpenLDAP, the values must be formatted exactly as follows:

Field	Value Required for OpenLDAP
LDAP	Enabled
Search Bind DN	uid=Anonymous, ou=Service Accounts, dc=stitech, dc=com
User Search Base DN	dc=stitech, dc=com
User Search Base Filter	(uid=%s)
Group Search	Enabled
Group Search Base DN	memberUid
User Membership Attribute	None

Managing LDAP Groups

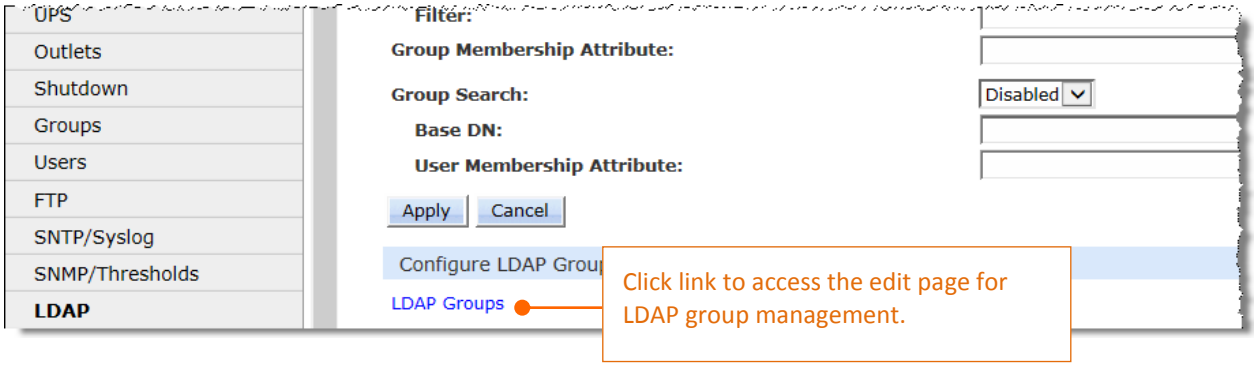
The firmware allows creation of LDAP groups, the addition of individual users to a group, and the assigning of user rights to LDAP groups for accessing CDU resources, such as outlet control.

Requirements for LDAP Groups:

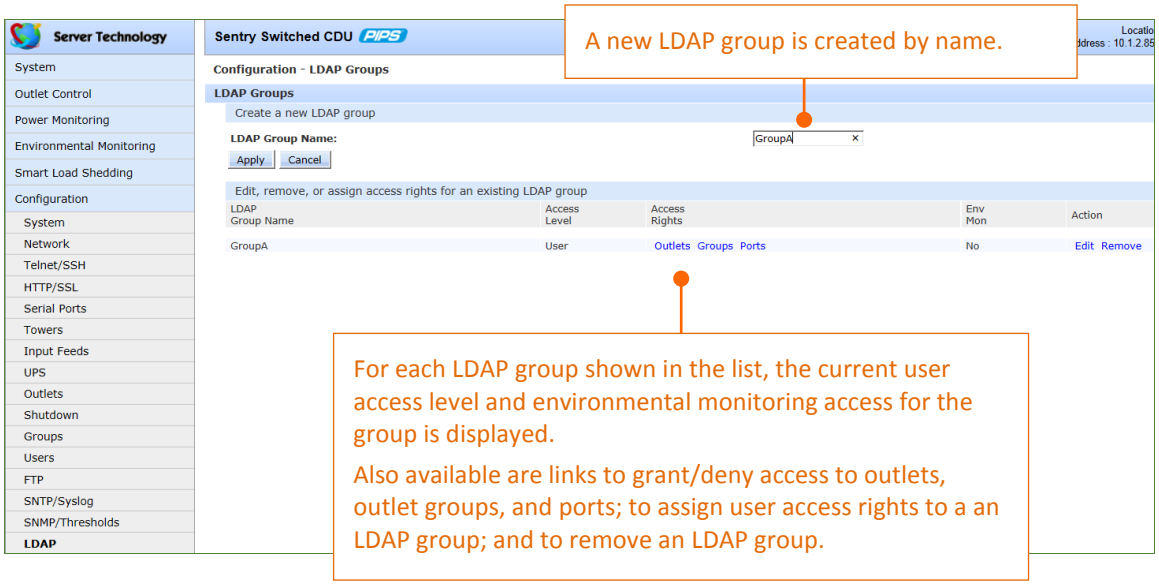
- At least one LDAP group must be defined.
- Users must be assigned to the defined LDAP group(s).
- User access rights must be granted to the LDAP group(s).
- LDAP group names on the Directory Services server and the CDU must match.

Access the LDAP Groups Page:

At the bottom of the LDAP Configuration page, click the LDAP Groups link.



The LDAP Groups page displays:



Step-by-Step LDAP Group Configuration Instructions:

Create a new LDAP group...

Type a descriptive name in the LDAP Group Name field, up to 24 alphanumeric characters, no spaces.

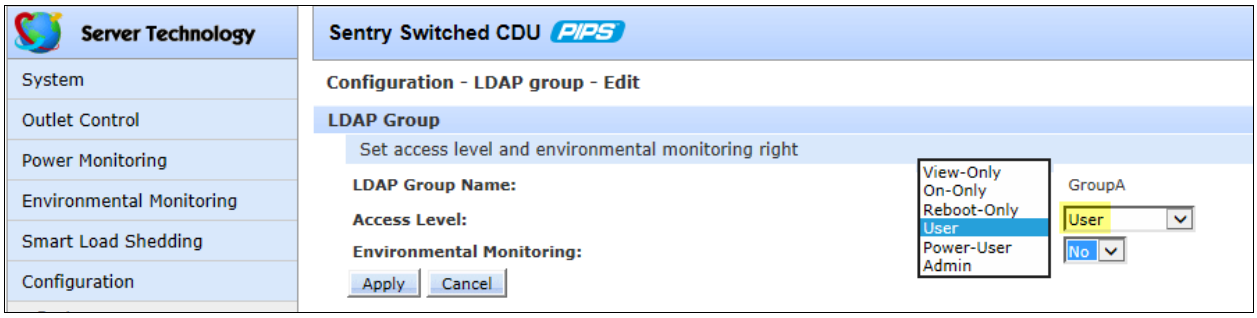
Click **Apply**. The new name displays in the list.

Delete an LDAP group…

For an LDAP Group in the list, click the Remove link. You will be asked to confirm the deletion.

Change user access rights for an LDAP group…

For an LDAP Group in the list, click the Edit link. The LDAP Group Edit page displays:

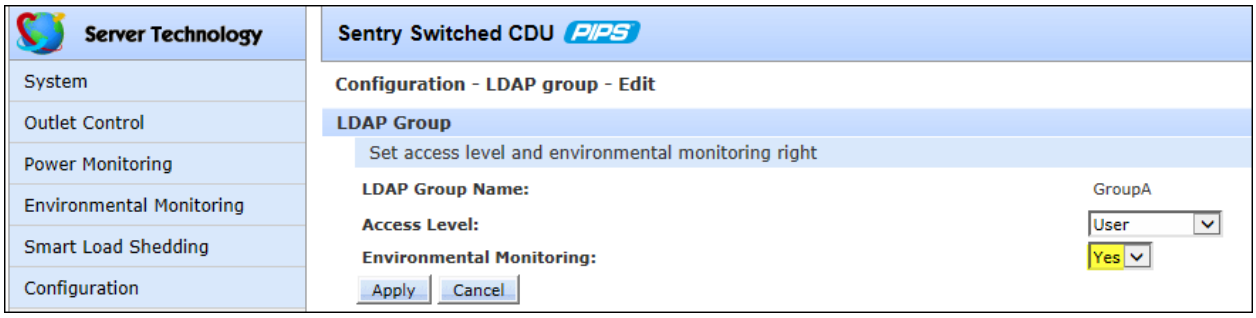


From the Access Level drop-down menu, select the desired user access level as the above screen sample shows (View-Only, On-Only, Reboot-Only, User, Power User, or Admin) to assign to the LDAP group.

For a description of these levels, see user access rights.

Grant or deny environmental viewing rights…

For an LDAP Group in the list, click the Edit link. The LDAP Group Edit page displays:

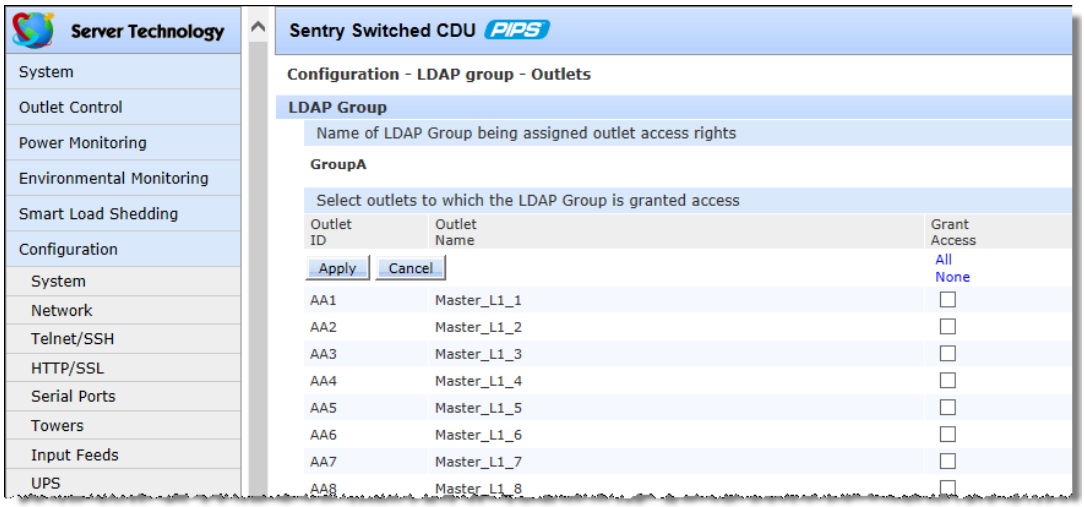


From the Environmental Monitoring drop-down menu, select Yes or No.

Note: Granting access to environmental monitoring (temperature/humidity/sensors) to a non-admin user also grants that non-admin user access to power monitoring, such as outlets, infeeds, towers – all the environmental data of the CDU.

Grant or deny individual outlet access to an LDAP group…

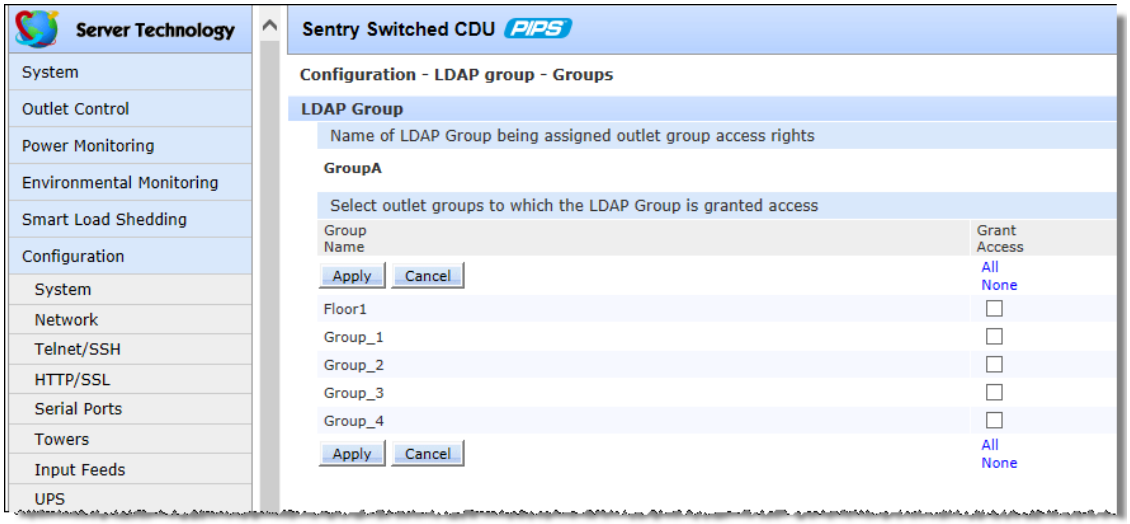
For an LDAP group in the list, click the Outlets link. The LDAP Group Outlets page shows a list of available outlets, displayed by absolute and descriptive names:



For the LDAP group shown, grant outlet access by selecting checkboxes for individual outlets, or clear checked boxes to deny access.

To grant or deny outlet group access to an LDAP group…

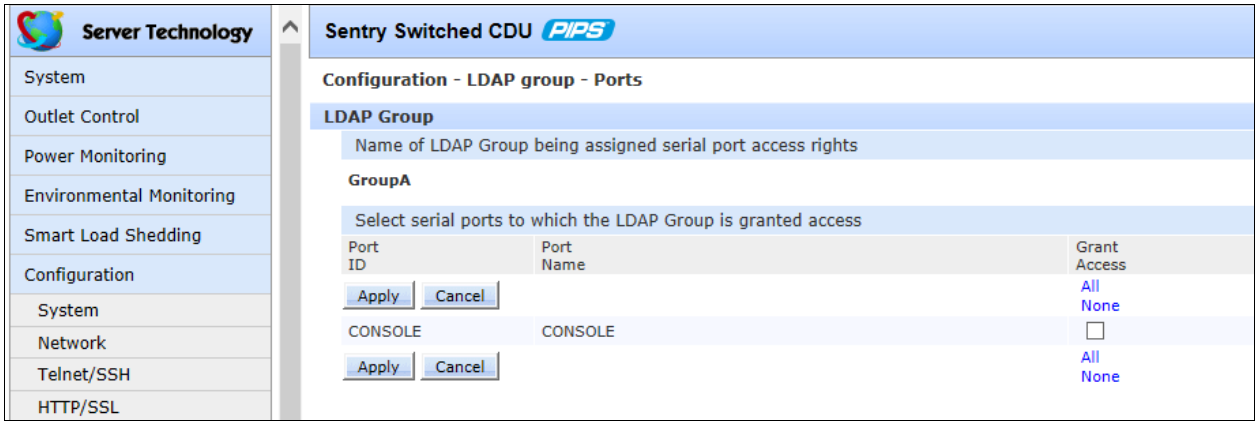
For an LDAP Group in the list, click the Groups link. The LDAP Group Outlets page shows a list of available outlet groups, displayed by name:



For the LDAP group shown, grant outlet group access by selecting checkboxes for individual outlet groups, or clear checked boxes to deny access.

To add or delete serial port access…

For an LDAP Group in the list, click the Ports link. The LDAP Group Ports page shows a list of available ports, displayed by name:



For the LDAP group shown, grant port access by selecting the checkboxes for individual ports, or clear checked boxes to deny access.

Using LDAP with Sentry Firmware (CLI)

The LDAP authentication process begins with initiating a Sentry firmware session. Configuration of LDAP settings can then be done using the Command Line Interface (CLI) as follows in this section.

Initiate a Sentry CLI Session

Logging in through Telnet requires directing the Telnet client to the configured IP address of the unit.

A login through the console (RS232) port requires the use of a terminal or terminal emulation software configured to support ANSI or VT100, and a supported data rate of 300, 1200, 2400, 4800, 9699, 19200, 38400, 57600, or 115200 bps (default rate is 9600); 8 data bits-no parity, 1 stop bit, and device ready output signal (DTR or DSR).

To login by Telnet or RS232 (CLI):

At the command prompt, initiate a Telnet session (telnet [Sentry IP address]). The Telnet session automatically opens the Sentry login prompt, showing the current CDU product and firmware version.

```
Sentry Switched CDU Version 7.0m

Username: admn
Password:

Location:

Switched CDU:
```

The default administrative-level user login (admn/admn) was used for this example.

Press **Enter**.

The command line prompt, such as “Switched CDU:” in this example, displays for the CDU product, and you are now logged into the Sentry firmware Command Line Interface (CLI).

If a location identifier was user-defined, that location will also be displayed, as shown in the example.

Commands for LDAP Configuration

This section provides command reference tables for general LDAP configuration and LDAP group configuration.

LDAP Configuration:

Once you have installed and configured the LDAP Directory Services server, the following CLI commands can be used for LDAP configuration:

CLI Command Name	Description	Command Syntax
Set LDAP	Enables or disables LDAP. **Note:** Value must be "Enabled" when using AD or OpenLDAP.	set ldap [enabled or disabled]<Enter>
Set LDAP Host	Sets the IP address of the Directory Services server.	set ldap [host 1 or host2)<Enter>
Set LDAP Port	Sets the port number where the CDU sends LDAP requests for the defined LDAP server. Default I 389.	set ldap port [port number] <Enter>
Set Authentication Order	Sets the authentication order for remote authentication sessions.	set order [remotelocal or remoteonly] <Enter>
Set LDAP Bind Type	Specifies the LDAP bind request to authenticate a client with the LDAP server (Simple, TLS/SSL, or MD5).	set ldap bind [simple, TLS, md5] <Enter>
Set LDAP Search Bind DN	Sets distinguished name (DN) to bind user accounts. Used only with Simple binds. Maximum length is 124 characters. If left blank, an anonymous bind will be attempted. **Note 1:** For AD, format must be: cn=John Smith, ou=Service Accounts, ou=Miscellaneous Accounts, dc=stitech, dc=com **Note 2:** For OpenLDAP, format must be: uid=Anonymous, ou=Service Accounts, dc=stitech, dc=com	set ldap binddn [DN] <Enter>
Set LDAP Bind Password	Sets the password for the user account specified in the Bind DN.	set ldap bindpw; at prompt type the bind password <Enter>
Set User Search Base DN	Specifies where LDAP begins searching for users in the directory, including all sub-trees. Maximum length is 100 characters; must be in the same format as the domain component (dc=) specified in the search bind DN. **Note:** For both AD and OpenLDAP, format must be: dc=stitech, dc-com	set ldap userbasedn<Enter>; at prompt, type the search base DN <Enter>
Set User Search Base Filter	Sets the search filter for the user name provided in the User Search Base DN. The filter must be formatted in parenthesis, maximum string length is 100 characters. **Note 1:** For AD, format must be: (sAMAccountName=%s*) **Note 2:** For OpenLDAP, format must be: (uid=%s)	set ldap userfilter<Enter>; at prompt, type the user search filter<Enter>.
Set Group Membership Attribute	Locates members of the group(s) that are returned from the specified search. Maximum length is 30 characters.	set ldap groupattr [attribute string] <Enter>

CLI Command Name	Description	Command Syntax
Display LDAP Configuration Information	Shows LDAP configuration values. **Note:** For AD only, format must be: memberOf	show ldap<Enter>
Set Group Search	Enables or disables the LDAP group search. **Note 1:** For AD, must be Disabled. **Note 2:** For OpenLDAP,must be Enabled.	set ldap groupsearch [enabled or disabled] <Enter>
Set Group Search Base DN	Group Search Base Distinguished Name (DN). Indicates where the LDAP group search starts. **Note 1:** For AD, must be blank. **Note 2:** For OpenLDAP, must be "memberOf".	set ldap groupsearch basedn [base distinguished name] <Enter>
Set User Membership Attribute	Allows the searching of group directory names by a user membership attribute to find the groups for which the user is a member. This option allows searching of directory entry groups for a user membership attribute to find the groups for which the user is a member. Maximum length is 61 characters. **Note 1:** For AD, must be blank. **Note 2:** For OpenLDAP, must be "None".	set ldap groupsearch userattr [attribute string] <Enter>

LDAP Group Configuration:

Once you have installed and configured the LDAP Directory Services server, the following CLI commands can be used for LDAP group configuration:

CLI Command Name	Description	Command Syntax
Create LDAP Group	Creates a new LDAP group by name.	create ldapgroup [1-16 character group name, no spaces] <Enter>
Delete LDAP Group	Deletes an LDAP group by name.	remove ldapgroup [LDAP groupname] <Enter>
Set LDAP Group Access Level	Sets the user access level for an LDAP group.	set ldapgroup access [admin, poweruser, user, rebootonly, ononly, viewonly] <Enter>
Grant or Remove Access to Environmental Monitoring	Grants or denies input status viewing rights to/from an LDAP group. Note: Granting access to environmental monitoring (temperature/humidity/sensors) to a non-admin user also grants that user acces to power monitoring (outlets, infeeds, towers – all the environmental data of the CDU).	set ldapgroup envmon [on, off] [groupname] <Enter>
List LDAP Groups	Displays all defined LDAP groups and their user access level.	list ldapgroups <Enter>
Add Outlets to LDAP Group	Grants or denies access to one or all outlets for an LDAP group. **Note:** This command grants access to one outlet at a time. To grant access to more than one outlet, you must issue the command multiple times.	add outlettoldap [outlet name] [LDAP group name] <Enter>
Delete Individual Outlets from an LDAP Group	Deletes individual outlets by name from the LDAP group, one outlet at a time.	delete outletfromldap [outlet name] [LDAP group name] <Enter>

CLI Command Name	Description	Command Syntax
Delete All Outlets from an LDAP Group	Deletes all outlets from the LDAP group in one command.	delete outletfromldap [all]] <Enter>
Add Outlet Group Access for LDAP Group	Grants an LDAP group access to an outlet group. This command grants access to one outlet group at a time. To grant access to more than one outlet group, you must issue the command multiple times.	add grouptoldap [outlet group name] [LDAP group] <Enter>
Delete Outlet Group Access for an LDAP Group	Deletes an LDAP group access to an outlet group. Note that you cannot remove access to any group for an administrative level group.	deletegroupfromldap [outlet group name] [LDAP group name] <Enter>
Add Serial Port Access to an LDAP Group	Grants an LDAP group access to the serial port.	add porttoldap console [LDAP group name] <Enter>
Delete Serial Port Acces to an LDAP Group	Deletes an LDAP group access to the serial port. Note that you cannot remove access to the serial port for an administrative level group.	delete portfromldap console [LDAP group name] <Enter>
Display LDAP Group Access Rights	Shows LDAP group access rights.	list ldapgroup [LDAP group name] <Enter>

Using LDAP with Sentry Power Manager (SPM)

The LDAP authentication process begins with initiating an SPM session. Configuration of LDAP settings can then be done using the SPM's LDAP configuration window.

Logging into SPM

An SPM session begins with the SPM login window. Provide your value username/password.

The default administrative-level user login (admn/admn) was used for this example.

Click **Login**. You are now logged into SPM's GUI.

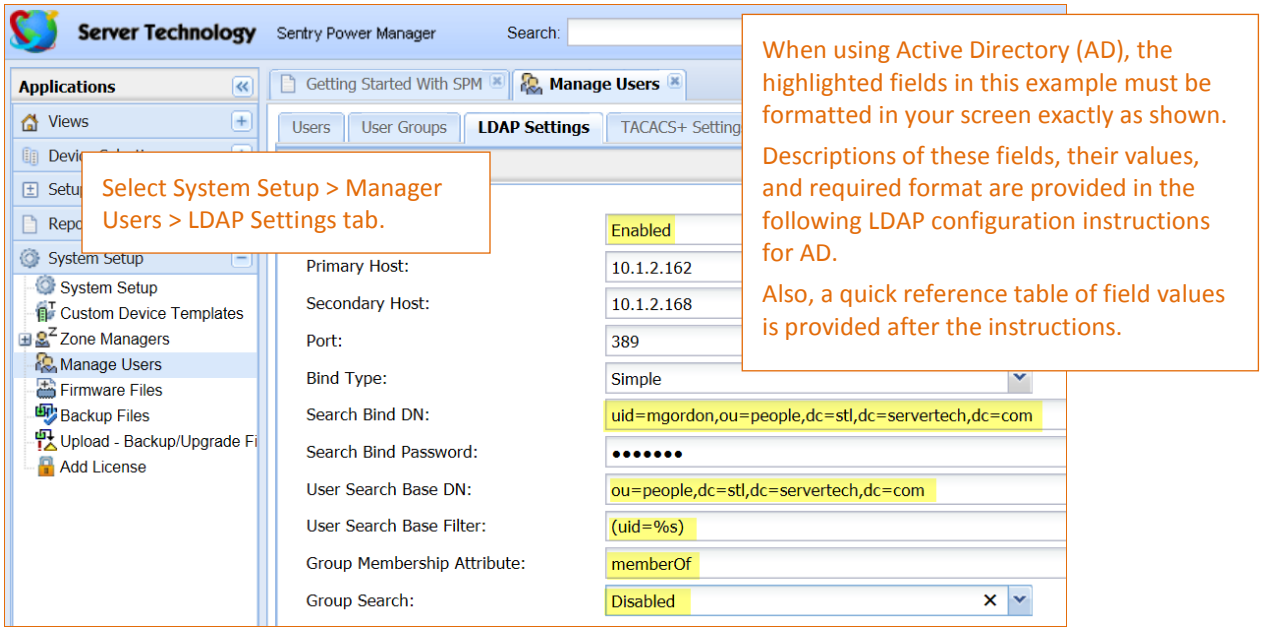
LDAP Configuration with SPM

Once you have installed and configured the LDAP Directory Services server, the next step is to configure LDAP using SPM.

Access the LDAP Configuration Page:

From the SPM interface, go to **System Setup > Manage Users > LDAP Settings**. The LDAP Settings window displays to allow server authentication and configuration for LDAP support with SPM.

Configuring LDAP Active Directory (AD):



Step-by-step configuration instructions:

1. From the LDAP Server drop-down menu, select Enabled.
2. Provide the Primary/Secondary Host names (IPv4 or IPv6 format). The host names define the network address for the primary/secondary LDAP Directory Services server.
3. The port number receives LDAP requests for the primary/secondary servers you just defined in the previous field. Type the new LDAP server port number, or accept the default port number 389.

The CDU supports the following three standard LDAP bind types:

- **Simple:** Uses unencrypted delivery of username-password over the network to the LDAP server for authentication, showing user credentials in plain text.
- **TLS/SSL:** (LDAP over TLS/SSL) Uses a trusted authority certificate to provide encryption of LDAP authentication. If this option is selected, MDF binding will be disabled.
- **MD5:** Provides strong protection using 1-way hash encoding that does not transmit the username-password over the network.

4. From the Bind Type drop-down menu, select Simple, TLS/SSL, or MD5.
5. By default, Active Directory requires that you specify a bind username and password. The Search Bind Distinguished Name (DN) is the DN directory path that binds and searches the LDAP directory. Access to the LDAP Active Directory (AD) requires the DN to be in the following comma-separated format, maximum length is 124 characters:

   uid=jsmith,ou=people,dc=sti,dc=servertech,dc=com

   where…
   uid is the user ID or common name of the person.
   ou is the organizational unit or various accounts, such as service and miscellaneous, organized into units.
   dc is the domain component or individual domain name for the company.
6. Provide the password to use with the DN. Maximum password length is 20 characters.
7. The User Search Base DN is the level in the Active Directory (AD) hierarchy, specified by the User Search Base Distinguished Name (DN), where LDAP begins searching for users, including all sub-trees. Specify the DN in the same format as the domain component (dc) that was provided in the Search Bind DN: ou=people,dc=sti,dc=servertech,dc=com
8. For the username entered at the SPM login, the User Search Base Filter specifies which objects in the hierarchy of the Active Directory are examined and returned on query. The LDAP Active Directory (AD) requires the filter to be formatted in parenthesis, maximum string length is 100 characters, and must be in this format: (uid=%s)

   where "uid" is the name of the attribute in the user class which has a value that represents the user's login name. In this string, the "%s" will be replaced by the entered username.
9. The Group Membership Attribute finds members of the group(s) that are returned from the specified search. Maximum string length is 30 characters. Type the attribute exactly as required for Active Directory in this format: memberOf
10. From the Group Search drop-down menu, select Disabled.

    Note: For LDAP configuration using Active Directory, the group search must be Disabled.

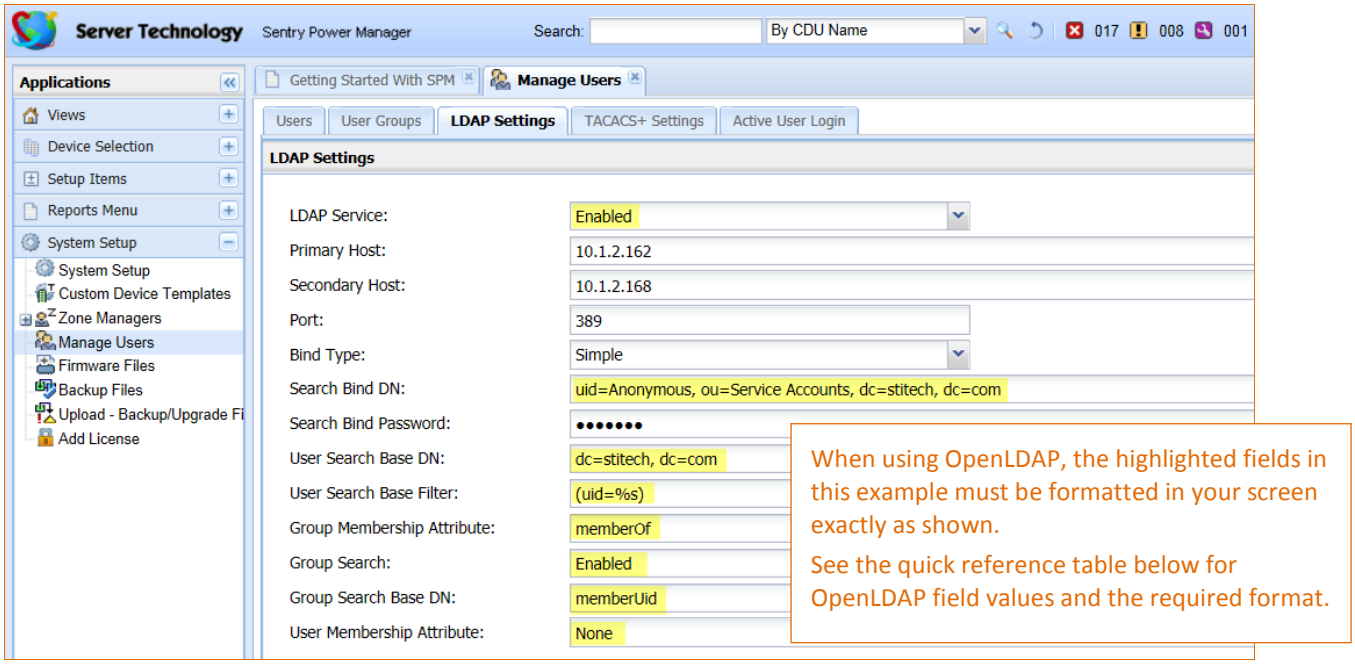
Quick Reference: SPM Settings for Active Directory (AD)

The LDAP configuration fields in this table are the same fields that were highlighted in the screen example above. For Active Directory, the values must be formatted exactly as follows:

Field	Value Required for Active Directory
LDAP	Enabled
Search Bind DN	cn=John Smith, ou=Service Accounts, ou=Miscellaneous Accounts, dc=stitech, dc=com
User Search Base DN	dc=stitech, dc-com
User Search Base Filter	(sAMAccountName=%s*)
Group Membership Attribute	memberOf
Group Search	Disabled
Group Search Base DN	Must be blank
User Membership Attribute	Must be blank

SPM Settings for OpenLDAP

If you are using OpenLDAP, you can follow the step-by-step instructions above for configuring LDAP with Active Directory (AD), but note the several highlighted fields below that must be formatted differently for OpenLDAP.



Quick Reference: SPM Settings for OpenLDAP

The LDAP configuration fields in this table are the same fields highlighted in the screen example above. For OpenLDAP, the values must be formatted exactly as follows:

Field	Value Required for OpenLDAP
LDAP	Enabled
Search Bind DN	uid=Anonymous, ou=Service Accounts, dc=stitech, dc=com
User Search Base DN	dc=stitech, dc=com
User Search Base Filter	(uid=%s)
Group Search	Enabled
Group Search Base DN	memberUid
User Membership Attribute	None

User Access Rights – Firmware

The following user access levels are defined in the Sentry firmware for the CDU and apply to the LDAP group:

Level	Description
Admin	Full access for all configuration, control (on, off, reboot), status, and serial/pass-thru ports.
Power User	Full access for all control (on, off, reboot), status, and serial/pass-thru ports.
User	Partial access for control (on, off, reboot), status, and pass-thru of assigned outlets, groups, and serial/pass-thru ports.
Reboot-Only	Partial access for control (reboot), status, and pass-thru of assigned outlets, groups, and serial/pass-thru ports.
On-Only	Partial access for control (on), status, and pass-thru of assigned outlets, groups, and serial/pass-thru ports.
View-Only	Partial access for status and pass-thru of assigned outlets, groups, and serial/pass-thru ports.

Notes:

- The administrator can also grant administrative rights to other user accounts, allowing the CDU to have more than one administrative user account.
- You cannot remove administrative privileges from the default admin user account unless you have already granted administrative access to another user account.

User Group Capabilities – SPM

Capabilities are the predefined levels of user group access to SPM system objects as granted by the SPM Administrator or Power User. An SPM user group can have the same permissions an LDAP group uses:

Level	Description
Administrator	Full access for all configuration, control (on, off, reboot), status, and serial/pass-thru ports.
Power	Same capabilities as the Administrator
Regular	Partial access for outlet control action (on, off, reboot), outlet status, and pass-thru of assigned outlets, outlet groups, outlet clusters, and serial/pass-thru ports. The Administrator can grant the following options to the Regular user group: • No Access: User has no access to any of the SPM system objects. • Off: User has partial access for control (off), status, and pass-thru of assigned outlets, groups, and serial/pass-thru ports. Off is available only to SPM system objects that contain outlets. • On: User has partial access for control (on) status, and pass-thru of assigned outlets, groups, and serial/pass-thru ports. On is available only to SPM system objects that contain outlets. • Outlet Control: User has full outlet control access. Outlet Control is available only to SPM system objects that contain outlets. • Reboot: User has partial access for control (reboot) status, and pass-thru of assigned outlets, groups, and serial/pass-thru ports. Reboot is available only to SPM system objects that contain outlets. • Setup: User has full Administrator access to the CDU. • View Only: User has data view access only. User cannot save changes and user cannot perform actions on SPM system objects.

Contact Technical Support

Experience Server Technology's FREE Technical Support

Server Technology understands that there are often questions when installing and/or using a new product. Free Technical Support is provided from 8 a.m. to 5 p.m. PST, Monday through Friday. After-hours service is provided to ensure your requests are handled quickly no matter what time zone or country you are located in.

Server Technology, Inc.

1040 Sandhill Drive Tel: 775.284.2000 Web: www.servertech.com

Reno, Nevada 89521 USA Fax: 775.284.2065 Email: support@servertech.com

end