Chapter

15

15 LDAP Support for SpectrumSCM™

15.1 Introduction: Over the past few years, the Lightweight Directory Access Protocol (LDAP) has gained wide acceptance as the directory access method for the Internet and organizational intranets. A directory is a specialized database that is used for storing information regarding various users, applications or resources on a network. A company-wide implementation of an LDAP directory service provides a one-stop solution for any application, running on any platform, that needs access to company specific information like employee details, customer information, licenses, security keys etc. Of late, LDAP is gaining popularity as a centralized authentication system for users on a network. Storing user names and passwords in an LDAP directory as opposed to a local application-specific database not only provides for enhanced security but also provides users with the convenience of using a single username and password for accessing company-wide resources and applications. Of course, the security benefit realized by using a centralized LDAP authentication scheme depends on how secure the centralized database is.

An LDAP directory service is based on the client server architecture in which an LDAP client sends requests to an LDAP server that processes the request and returns the appropriate response. The server hosts the LDAP information database that is used for storing and retrieving information. The directory service is generic in nature and can be used for storing and retrieving any kind of information. The basic unit of information in a LDAP directory is an "entry". Each entry may represent an organization, user, resource or any object of interest. Entries are composed of attributes which contain information about the object. Every attribute has a name and one or more values. Entries are organized in a hierarchical, tree like structure. Each entry is uniquely identified by a "Distinguished Name" (DN). The DN acts as a primary key for the entry and is derived from the DN of its ancestor in the tree. The DN of the highest node in the tree is called the Root DN.

An LDAP server may implement its own schema or a standard schema as defined in RFC 2252. Mainstream implementations of LDAP include Netscape Directory Server, Sun One Directory, Microsoft's Active Directory and Novell's Directory Service and Open LDAP. Though LDAP defines operations for updating the stored information, it is optimized for read operations. The most common LDAP operations can be classified into two categories:

Query - This includes operations for searching a particular entry in the directory or for bulk retrieval of a set of entries that satisfy a search criterion.

Authentication - This includes operations to establish and end a session between an LDAP client and server, and access control. LDAP provides different levels of security ranging from unauthenticated anonymous access, simple authentication to secure authentication using SASL/SSL.

15.2 LDAP Support for SpectrumSCM: SpectrumSCM (version 1.3.7 and above) is LDAP enabled and is fully compliant with LDAP v3. LDAP support for SpectrumSCM includes the following features:

LDAP Authentication: This allows users of SpectrumSCM to authenticate against a centralized LDAP database as opposed to the SpectrumSCM database. LDAP authentication provides enhanced security for user credentials (passwords) by storing them in a secure centralized database instead of a local application specific database. Thus the confidence level for user password becomes a function of how secure the LDAP database is. This is particularly useful for organizations whose security policies prohibit them from storing user credentials in application-specific databases. LDAP authentication also provides users with the added convenience of using a single user name and password for all LDAP enabled applications.

LDAP Import: This feature allows an administrator to import details regarding a particular user from the LDAP database. Users in SpectrumSCM are defined by the following attributes: user-id, name, phone, email, location. The LDAP import facility allows an administrator to import these details from an LDAP database while adding/modifying users.

LDAP Search: This feature allows a user (with the required privileges) to search the LDAP database for users satisfying a particular search criteria. Users can be searched based on their name, phone number, email address or location. The search result can be used for bulk addition of users into the SpectrumSCM database. The import and search features are useful in organizations that store user-specific details on a company-wide HR database or on a publicly available LDAP server.

Security: LDAP support for SpectrumSCM defines different levels of security ranging from anonymous binding, simple password protected binding to strong SSL based mechanisms. SSL support for LDAP provides confidentiality protection for authentication through the use of certificates and integrity protection by encrypting the data transmitted over the wire. SSL support for LDAP uses SSL v3.0 or TLS v1.0. The LDAP server should support the above mentioned mechanisms before they can be used with SpectrumSCM.

15.3 Using LDAP Support for SpectrumSCM: Configuring SpectrumSCM for LDAP support is quick and easy. The *scm.properties* file includes a few parameters that need to be configured before the LDAP related features for SpectrumSCM can be used. The parameters are as follows:

LDAP.useAuth - This parameter specifies whether LDAP authentication for SpectrumSCM should be enabled.

Keywords:	YES, NO
Default:	NO

LDAP.useImport - This parameter specifies whether the LDAP import and search features should be enabled.

Keywords:	YES, NO
Default:	NO

LDAP.useSSL - This parameter specifies whether SpectrumSCM should use SSL protection for communicating with the LDAP server.

Keywords:	YES, NO
Default:	NO

LDAP.server - This parameter specifies the LDAP server's address

Examples:	ldap.xyz.com, directory.verisign.com, 192.168.100.7

LDAP.port - This parameter specifies the port number for the LDAP server

Default:	389 for LDAP, 636 for LDAP with SSL

LDAP.dn - This parameter specifies the distinguished name (DN) used for LDAP authentication and binding. UU in the DN string acts as a placeholder for the login string entered by the user when he/she attempts to login to SpectrumSCM The place holder is replaced with the login string entered by the user when he/she attempts to login to SCM. If the 'useNameAsUU' option is set, then the users name as recorded in the SpectrumSCM database is used as UU instead of the user id.

Also note: multiple DNs can be specified, LDAP.dn would be the primary, LDAP.dn2 the secondary, LDAP.dn3 the tertiary, etc

LDAP.useNameAsUU	true
LDAP.dn	uid=UU,dc=SpectrumSoftware,dc=net
LDAP.dn2	uid=UU,ou=Development,dc=SpectrumSoftware,dc=net

LDAP.useNameAsUU – As above. If false, the user-id is used to replace the UU tag. If true, the user name as specified in the SpectrumSCM database relative to the supplied user-id, is used.

Keywords:	TRUE, FALSE
Default:	FALSE

LDAP.searchbase - This parameter specifies the search base for the LDAP server i.e. the starting point for all searches. In most cases, it is the DN of the top-most entry in the hierarchy defined by the LDAP database

Default:	NULL

The following parameters are used to map between the attributes defined in the LDAP server's schema and the information required by SpectrumSCM. *Ldap.uid.mapping* is a required parameter while other parameters are optional. The *LDAP.uid.mapping* attribute maps the LDAP login name to the SpectrumSCM user ID. The value of this attribute in the LDAP directory MUST match the user ID used in SpectrumSCM.

Parameter	**Example**
LDAP.uid.mapping	uid

LDAP.name.mapping	cn
LDAP.phone.mapping	telephonenumber
LDAP.mail.mapping	mail
LDAP.location.mapping	loc

The example attributes are based on the standard LDAP schema defined by RFC 2252. Once the above parameters are correctly specified, SpectrumSCM should be able to communicate with the specified LDAP server. The authentication and import/search features can be used separately or in tandem. In either case, the integrity of the information transmitted between the SpectrumSCM server and the LDAP server can be protected by enabling SSL.

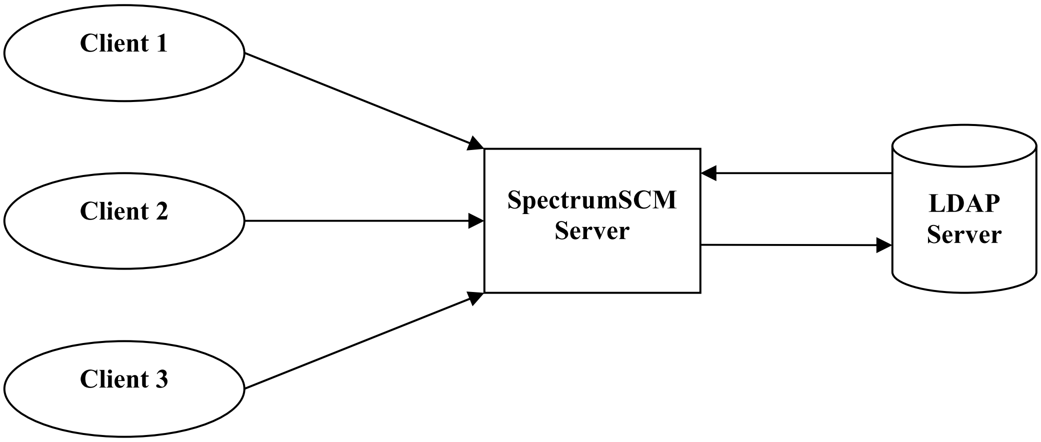
In general it is usually better to ensure that all the parameters are correct and functioning through the use of the import/search features BEFORE turning on the useAuth. If useAuth is turned on but the LDAP parameters are not correct, the login authentication will fail and you won't be able to log in to SpectrumSCM.

Additional note
The location attribute is by default a general information text field. If, however your organization has many disparate organizational units within the LDAP database this can be in-efficient to search. Instead, SpectrumSCM can use the location attribute/field to cache the users specific distinguished name (DN).

LDAP.useLocationForDN	true
LDAP.location.mapping	distinguishedName

With this setting, an import operation will import the users distinguishedName attribute from the LDAP database and place it in the location field in the SpectrumSCM database. If this user then attempts to perform LDAP operations such as authentication (login with useAuth on), the DN from the location field will be used ahead of the LDAP.dn parameters.

15.4 Architectural Diagram:



15.5 Frequently Asked Questions:

How do I use LDAP authentication ?

Configure the LDAP parameters in the scm.properties file. Make sure that the user IDs can be mapped to entries on the LDAP server. Turn LDAP authentication ON (with or without SSL). Restart the SpectrumSCM server. Use your LDAP user name and password to login

How do I use LDAP authentication with SSL ?

Make sure that the JRE on the client machine will accept certificates signed by the Certificate Authority used by the LDAP server's certificate. Turn on SSL support by specifying YES for the LDAP.useSSL parameter. CA certificates can be installed using the 'keytool' program provided by JAVA as follows:

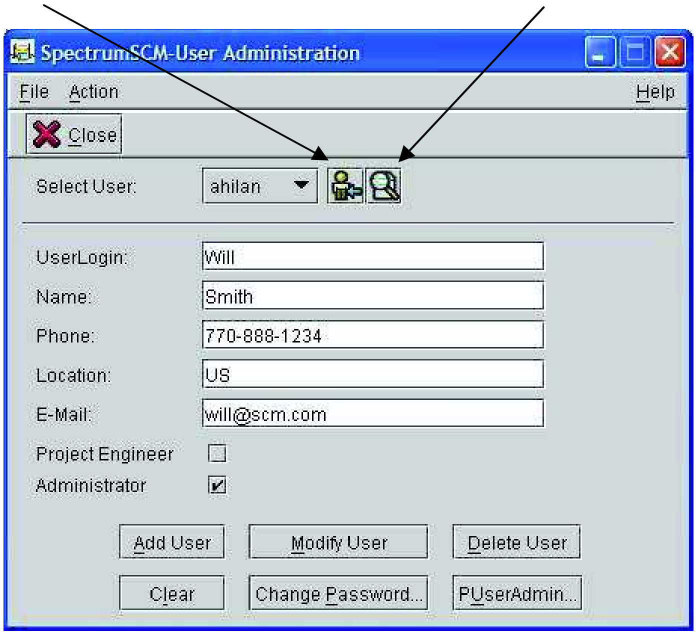
```
# cd JAVA_HOME/lib/security ...
# keytool -import -file ca.cert -keystore cacerts
```

JAVA_HOME is the JRE install directory**.** *ca.cert* is the CA certificate file. The *cacerts* (or similar) keystore can be found in the /lib/security directory under JAVA_HOME

How do I use LDAP import ?

The name field acts as the main input box for the import feature. Use the LDAP import icon to import user details from the LDAP server. Details are imported based on the mappings specified in the *scm.properties* file

LDAP Import Button **LDAP Browse Button**



Select User: ahilan

UserLogin: Will

Name: Smith

Phone: 770-888-1234

Location: US

E-Mail: will@scm.com

Project Engineer □

Administrator ☑

Screen Shot: SpectrumSCM User Admin with LDAP Support

What part does the mapping play ?

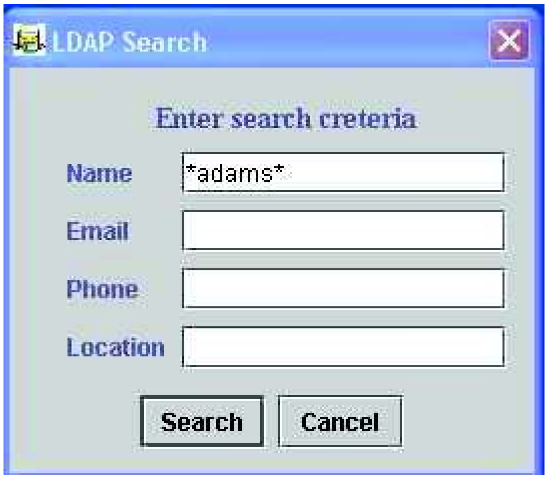
The mapping parameters are used to map between the attributes defined in the LDAP server's schema and the user details in the SpectrumSCM database. SpectrumSCM users are defined by five attributes (uid, name, mail, phone, location). The uid mapping is important for LDAP authentication. Each user on the LDAP server must have a unique ID which can be identified by some attribute name say 'user_id'. This attribute must map to the uid attribute used to identify a user in SpectrumSCM. Thus the mapping will be configured as:

LDAP.uid.mapping   user_id

Other attributes are mapped in a similar manner. However these are attributes are optional.

How do I use the search feature ?

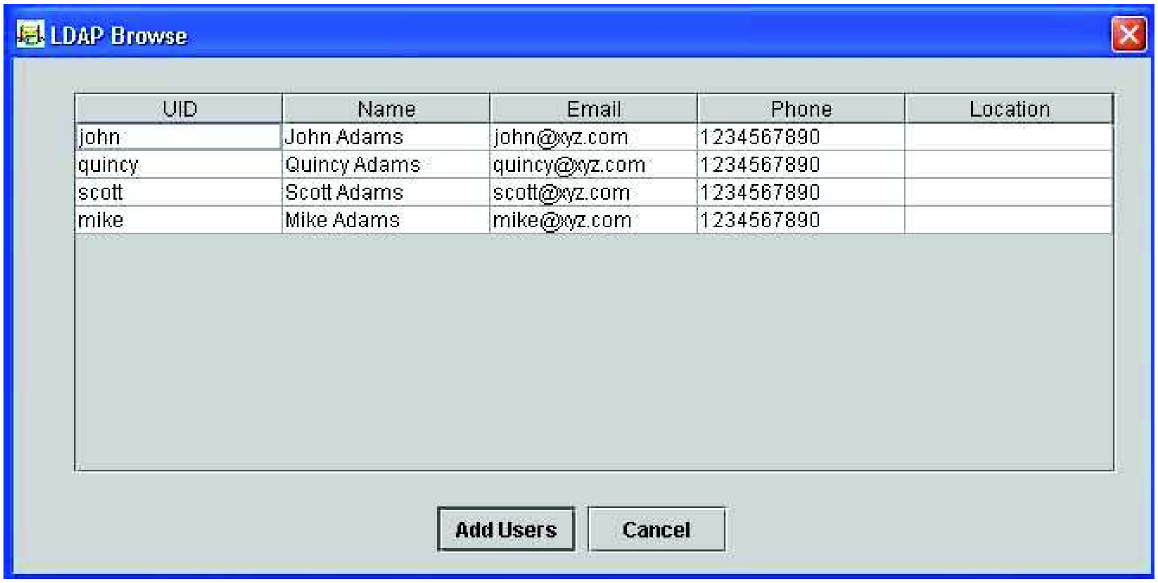
Click the LDAP search icon. If you are not yet authenticated, you will be prompted for authentication. Enter the search criteria. The results table will allow you to add users in bulk. If you are using a public server with thousands of entries, there is a possibility of exceeding the server limit if your search criterion is not refined.



LDAP Search

Enter search creteria

Name *adams*



UID	Name	Email	Phone	Location
john	John Adams	john@xyz.com	1234567890	
quincy	Quincy Adams	quincy@xyz.com	1234567890	
scott	Scott Adams	scott@xyz.com	1234567890	
mike	Mike Adams	mike@xyz.com	1234567890	

Screen Shot: LDAP Search Panel and Results Table

Can I use a public server ?

Of course, you just need the proper configuration parameters. However, in most cases you cannot use a publicly available server for authentication unless you happen to have an account with the server. You can definitely use the server to import information. As an example, here are the settings for the Verisign Server

LDAP.useAuth	NO
LDAP.useImport	YES
LDAP.useSSL	NO
LDAP.server	directory.verisign.com
LDAP.port	DEFAULT
LDAP.uid.mapping	mail
LDAP.name.mapping	cn
LDAP.phone.mapping	telephonenumber
LDAP.mail.mapping	mail
LDAP.location.mapping	loc

Comment out the LDAP.dn and LDAP.searchbase parameters

Where can I find out more about what went wrong ?

If the client side dialogs do not provide a clue as to what went wrong, check the server log file.

Why does SSL authentication seem a bit slow ?

SSL authentication employs an encryption, decryption, message code checking and other mechanisms. The speed depends upon the key length used. The longer the key, the higher is the level of security and the slower is the processing speed.

How do I use the UU keyword in scm.properties ?

The UU is a placeholder for the login that you enter. If your LDAP.dn parameter has been set to uid=UU,dc=SpectrumSoftware,dc=net and you enter 'john', the fully resolved distinguished name (DN) that is passed to the LDAP server is uid=john,dc=SpectrumSoftware,dc=net. As another example, if you typically enter the full DN set the LDAP.dn parameter to UU

Can I use wildcards in my searches ?

Yes, you can use LDAP compliant wildcards. The most common is *.

What if multiple entries match the input value while importing an LDAP user ?

The tool will always accept the first value in the set if multiple entries are found.