

Sonatype CLM Server - Security Administration

Contents

1	Introduction	1
2	User Management	2
2.1	Logging in to Sonatype CLM	3
2.2	Viewing Notifications	3
2.3	Changing the Admin Password	4
2.4	Creating a User	4
2.5	Editing and Deleting User Information	5
3	LDAP Integration	7
3.1	Configuring the LDAP Server Connection	8
3.2	LDAP Configuration Parameters	10
3.3	Mapping LDAP Users to Sonatype CLM	11

3.4	LDAP User Parameters	13
3.5	Mapping LDAP Groups to Sonatype CLM	14
3.6	LDAP Group Parameters	15
3.6.1	Static Groups	16
3.6.2	Dynamic Groups	16
3.7	Verifying LDAP Configuration	17
3.7.1	Test Connection	17
3.7.2	Check User and Group Mapping	18
3.7.3	Check Login	18
4	Role Management (Permissions) Overview	19
4.1	Role Definitions	19
4.2	Mapping Roles	20
4.3	Excluding Groups from Search Results	21

List of Figures

2.1	Login	3
2.2	Create User	5
2.3	Edit User	6
3.1	Sample LDAP Server Configuration	9
3.2	User Mapping	12
3.3	Group Mapping	15
3.4	Dynamic Group Options	17
3.5	Testing LDAP Server	17
3.6	Checking User Mapping	18
3.7	Checking User Login	18
4.1	Mapping Users to roles	21

4.2 Mapping Groups When Not Included With Search	22
--	----

Chapter 1

Introduction

Sonatype CLM uses the term *Security* to broadly refer to user accounts, passwords, and associated permissions. Regardless of the name, it shares a similarity to most systems in that open access isn't something that is permitted. This means, that unless you have a Sonatype CLM user account, you won't be able to view and make edits to policies, policy elements, and/or reports. Of course there are a variety of ways this can be accomplished, including simply using the default admin account that ships with the system.

In this guide we'll walk you through logging into the server and creating additional users. We will also cover common user management protocols like Light Weight Directory Protocol (LDAP). Ultimately what we provide here is a set of best practices aimed at walking you through both an initial setup of Sonatype CLM security, as well as assist those that may just be looking to make modifications to one that already exists.

**Important**

It is important to note, that this guide is aimed at administrators, and isn't a guide for other users of Sonatype CLM. Most areas discussed here will require a user account with administrative rights.

Chapter 2

User Management

The Sonatype CLM Server requires a username and password before any policies or policy elements can be created, viewed, and edited. When a user is created specific to Sonatype CLM, we consider this user to be part of the *Sonatype Realm*. This is also considered independent of other connected realms such as [LDAP](#).

While Sonatype does suggest using a security protocol such as LDAP for managing users and permissions, the *Sonatype Realm* is still available for those who would like a lighter setup, where all users, groups and rights are stored directly in the Sonatype CLM server.. The function of user management in the Sonatype Realm focuses on managing all the elements of a user account. In this section we will cover:

- Logging In and Logging Out
 - Managing the Admin Password / Account
 - Viewing Notifications
 - Creating, Editing and Deleting Users
 - First and Last Names
 - E-mail Addresses
 - Changing Passwords
-

2.1 Logging in to Sonatype CLM

Any user that wants to access Sonatype CLM will need a username and a password. To perform the functions described throughout this section, you will need to use a user account with administrative rights. By default the Sonatype CLM server has a preconfigured account

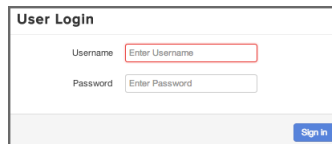
A screenshot of the 'User Login' form. It has a title 'User Login' at the top left. Below it, there are two input fields: 'Username' with a placeholder 'Enter Username' and 'Password' with a placeholder 'Enter Password'. A blue 'Sign In' button is located at the bottom right of the form.

Figure 2.1: Login

Once you log in for the first time, be sure to [change the admin password](#).


To logout, click on the *Log Out* link located in the upper right corner.

Note

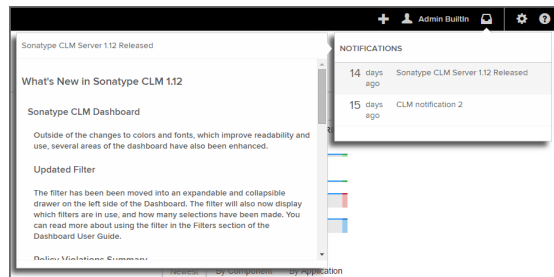
The server will timeout after 30 minutes of inactivity.

2.2 Viewing Notifications

Notifications provide a way for Sonatype to distribute important information about Sonatype CLM.

Unread notifications are indicated by a count, in blue, displayed over the notification icon . This icon is located in the Sonatype CLM header, next to the display of the logged-in user.

To view notifications, click on the notifications icon. This will open the Notification Panel, allowing you to click on any available notifications.



2.3 Changing the Admin Password

Sonatype CLM ships with a default admin account with a username `admin` and a password `admin123`. If you do nothing else related to security in Sonatype CLM, be sure to change this password. We'll cover this in Section 2.5 section below in more details, while we detail the process to change this default password now.


1. Log into the Sonatype CLM Server using a user with administrative permissions.
2. In the top right-click on the button with your username to the left of the *System Preferences* gear-shaped, icon. For the default administrator the user name will show `Admin Builtin`.
3. A list of options will be displayed, click *Change Password*.
4. Enter the current password (`admin123` for the default admin user), the new password, and then confirm the new password.
5. Click the *Change* button to save the new password.

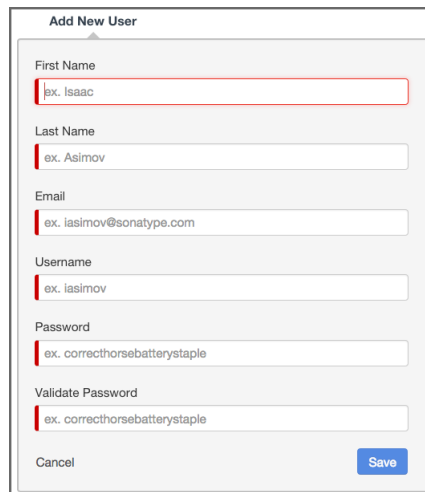
Note

Any user, including an admin, can change their password following the instructions above. However, only an admin can reset a user's password (discussed later in this Guide) without knowledge of the current password.

2.4 Creating a User

To create a new user in the Sonatype realm, follow the instructions below.

1. Log into the Sonatype CLM Server using a user with administrative permissions.
2. Click the *System Preferences* icon  located in the top right of the header.
3. Choose *Users* from the drop down menu. The **Users** administration area will now be displayed.
4. Click the *New User* button located at the top of the list of users.
5. The **Add New User** form will now be displayed. Enter the following information:
 - a. First Name
 - b. Last Name
 - c. E-mail Address
 - d. Username
 - e. Password
 - f. Password Validation
6. Click the *Save* button, to save the new user.



Add New User

First Name
ex. Isaac

Last Name
ex. Asimov

Email
ex. iasimov@sonatype.com

Username
ex. iasimov

Password
ex. correcthorsebatterystaple


Validate Password
ex. correcthorsebatterystaple

Cancel Save

Figure 2.2: Create User

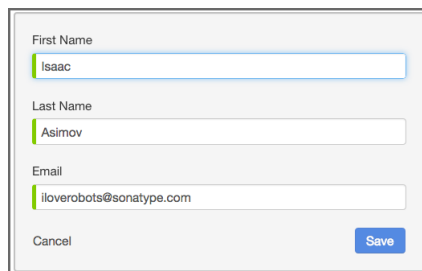
2.5 Editing and Deleting User Information

Editing user information is only available to an admin. The information that can be edited includes the first name, last name, email address, and password. To edit an existing user, follow these steps:

1. Log into the Sonatype CLM Server using a user with administrative permissions.
2. Click the *System Preferences* icon  located in the top right of the CLM header.
3. Choose *Users* from the drop down menu. The **Users** administration area will now be displayed.
4. At least one user - the initial `admin` account - will be displayed. If you hover your pointer over the user record you will notice that there are three icons on the right.
 - a. The icon shaped like a pencil will allow you to edit user information (i.e. first name, last name, and e-mail address).
 - b. The icon shaped like a bag with an arrow back is for resetting a user's password. If you use this option a random, secure password will be generated and displayed in a dialog. Click the icon to the right of the field to copy it to clipboard.
 - c. The icon shaped like a trashcan will allow you to delete the user after you confirm the deletion in a dialog.
5. Make any desired changes, and unless you chose to delete the record, click the *Save* button.

Tip

With regard to changing a user's password, a user can always change their own password. However, this requires knowledge of the existing password. If you encounter a user that has forgotten their password, you can reset it for them.



The image shows a dialog box for editing a user. It has three text input fields: 'First Name' with the value 'Isaac', 'Last Name' with the value 'Asimov', and 'Email' with the value 'iloverobots@sonatype.com'. Each field has a small green icon to its left. At the bottom left is a 'Cancel' button, and at the bottom right is a blue 'Save' button.

Figure 2.3: Edit User

Chapter 3

LDAP Integration

Light Weight Directory Protocol, also known more commonly as LDAP, provides both a protocol and a directory for storing user information. In some ways LDAP has become a ubiquitous part of most organizations' efforts to create a single sign on environment, as well as streamline user management for various applications. While we will cover some LDAP basics, the information provided here is limited and should not be considered a full reference.

Sonatype CLM supports a single LDAP realm, which simply means we support connection to a single LDAP server. This connection is configured via the Sonatype CLM Server. There are essentially two parts to integrating Sonatype CLM with LDAP:

- Configure the LDAP Server Connection
- Map LDAP User and Group Elements to Sonatype CLM

Our setup instructions provide an example using the Active directory format, and represent only the most basic approach. What we provide in this guide assumes a simple authentication method for LDAP. However, on a standard installation of Sonatype CLM, you would likely not want to use Simple Authentication as it sends the password in clear text over the network. Additionally, we have indicated a search base which corresponds to our organization's top-level domain components "dc=sonatype,dc=com". The structure can vary greatly based on your own LDAP server configuration.

Note

Once the LDAP server is configured and user attributes have been mapped, both LDAP users and users created in the Sonatype CLM Realm will be able to login into Sonatype CLM.

3.1 Configuring the LDAP Server Connection


The first step to establish the LDAP connection is to configure Sonatype CLM to point to your LDAP server. Those instructions are pretty straightforward as long as you have the necessary information. For this example, let's assume we have been provided the following information:

Server Name	Test LDAP Server
Protocol	LDAP
Hostname	wind-son04
Port	389
Search Base	dc=sonatype,dc=com
Authentication Type	Simple
Username	testuser
Password	tester

Note

The information provide will not allow you to access an LDAP server, and is provided just for demonstration purposes. In addition, this is only a representation of a simple connection. For an explanation of all available parameters, please see the next section.

Now, access the Sonatype CLM Server:

1. Log into the Sonatype CLM Server (*by default this is available at <http://localhost:8070>*) using a user account with Admin-level permissions (a member of the Admin Group).
 2. Click the system preferences icon  located in the top right of the CLM Header/Screen (resembles a cog/gear).
 3. Choose LDAP from the available option. The *LDAP Administration* area will be displayed.
 4. Enter the various parameters, and then use the **Test Connection** button to ensure a connection can be made to the configured LDAP Server.
-

5. Click the **Save** button when finished.

Using the information from the table above, our configuration should look something like this:

The screenshot displays the 'LDAP Server' configuration window. It has two tabs: 'CONNECTION' (selected) and 'USER & GROUP SETTINGS'. The 'CONNECTION' tab contains three sections: 'Connection Details', 'Authentication', and 'Timeouts'. In the 'Connection Details' section, 'Protocol' is set to 'LDAP', 'Hostname' is 'i-robot-01', 'Port' is '389', and 'Search Base' is 'dc=win,dc=steelcaves,dc=local'. The 'Authentication' section shows 'Method' as 'SIMPLE', 'SASL Realm' is empty, 'Username' is 'cn=testuser1,cn=users,dc=win,dc=steelcaves,dc=local', and 'Password' is masked with dots. The 'Timeouts' section has 'Connection' set to '30' and 'Retry Delay' set to '300'. At the bottom, there are 'Cancel', 'Test Connection', and 'Save' buttons.

Section	Field	Value
Connection Details	Protocol	LDAP
	Hostname	i-robot-01
	Port	389
	Search Base	dc=win,dc=steelcaves,dc=local
Authentication	Method	SIMPLE
	SASL Realm	
	Username	cn=testuser1,cn=users,dc=win,dc=steelcaves,dc=local
	Password	*****
Timeouts	Connection	30
	Retry Delay	300

Figure 3.1: Sample LDAP Server Configuration

Note

If at any point you wish to reset the form, click the reset button and any value that have been entered will be removed.

3.2 LDAP Configuration Parameters

As mentioned, the example above is a basic setup. Given this, there are a number of parameters not utilized. This section provides descriptions for all available parameters that can be configured in the Connection section of the LDAP Configuration area on the Sonatype CLM Server. When applicable, required fields have been noted.

General

Protocol

Valid values in this drop-down are LDAP and LDAPS, which correspond to the Lightweight Directory Access Protocol and the Lightweight Directory Access Protocol over SSL.

Hostname

The hostname or IP address of the LDAP.

Port

The port on which the LDAP server is listening. Port 389 is the default port for the LDAP protocol and port 636 is the default port for the LDAPS.

Search Base

The search base is the Distinguished Name (DN) to be appended to the LDAP query. The search base usually corresponds to the domain name of an organization. For example, the search base on the Sonatype LDAP server could be "dc=sonatype,dc=com".

Authentication

Method

Sonatype CLM provides four distinct authentication methods to be used when connecting to the LDAP Server:

- Simple Authentication - Simple authentication is not recommended for production deployments not using the secure LDAPS protocol as it sends a clear-text password over the network.
- Anonymous Authentication - Used when Sonatype CLM only needs read-only access to non-protected entries and attributes when binding to the LDAP.
- Digest-MD5 - This is an improvement on the CRAM-MD5 authentication method. For more information, see <http://www.ietf.org/rfc/rfc2831.txt>.
- CRAM-MD5 - The Challenge-Response Authentication Method (CRAM) based on the HMAC-MD5 MAC algorithm. In this authentication method, the server sends a challenge string to the client, the client responds with a username followed by a Hex digest which the server compares to an expected value. For more information, see RFC 2195. For a full discussion of LDAP authentication approaches, see <http://www.ietf.org/rfc/rfc2829.txt> and <http://www.ietf.org/rfc/rfc2251.txt>.

SASL Realm

The Simple Authentication and Security Layer (SASL) Realm to connect with. The SASL Realm is only available if the authentication method is Digest-MD5.

Username

Username of an LDAP User to connect (or bind) with. This is a Distinguished Name of a user who has read access to all users and groups.

Password

Password for an Administrative LDAP User.

Timeouts**Connection**

The number of seconds Sonatype CLM should try and connect to the configured server before returning an error.

Retry Delay


The number of seconds Sonatype CLM should wait before attempting to connect to the configured server again (after an error).

3.3 Mapping LDAP Users to Sonatype CLM

Once the LDAP Server has been configured, you can map information attributes of an LDAP user to match those of Sonatype CLM. Similar to configuring the LDAP Server, this will require that you have information related to the location of various user attributes. Here is a sample set of data, that you would likely see:

Base DN	cn=users
Object Class	user
Username Attribute	sAMAccountName
Real Name Attribute	cn
Email Attribute	mail

Once you have gathered this information, access the Sonatype CLM Server LDAP Configuration:

1. Log into the Sonatype CLM Server (*by default this is available at <http://localhost:8070>*) using a user account with Admin-level permissions (a member of the Admin Group).
2. Click the system preferences icon  located in the top right of the CLM Header/Screen (resembles a cog/gear).

3. Choose LDAP from the available option. The *LDAP Administration* area will be displayed.
4. Click on the Second Tab, just below the Server Name, *User and Group Settings*.
5. Enter the various settings, using the Test Mapping button to ensure the correct information has been mapped.
6. Click the **Save** button when finished.

Note

If at any point you wish to reset the form, click the reset button; Any values that have been entered will be removed.

Using the information from the table above, our configuration would look like this:

The screenshot shows the 'LDAP Server' configuration window with the 'USER & GROUP SETTINGS' tab selected. The 'User Element Mapping' section includes the following fields:

- Base DN:
- User Subtree: ☐
- Object Class:
- User Filter:
- Username Attribute:
- Real Name Attribute:
- E-mail Attribute:
- Password Attribute:

The 'Group Element Mapping' section includes:

- Group Type:

At the bottom, there are three buttons: 'Cancel', 'Check User Mapping', and 'Check Login'. A 'Save' button is also present at the bottom right.

Figure 3.2: User Mapping

3.4 LDAP User Parameters

As mentioned, the example above is a basic setup. Specifically, we do not turn on the User Subtree option or utilize the User Filter. Descriptions for those fields, as well as all available parameters for mapping LDAP User Attributes to Sonatype CLM have been provided below. When applicable, required fields have been noted.

Base DN (*required*)

Corresponds to the Base DN (Distinguished Name) containing user entries. This DN is going to be relative to the Search Base. For example, if your users are all contained in "cn=users,dc=sonatype,dc=com" and you specified a Search Base of "dc=sonatype,dc=com" you would use a value of "cn=users"

User Subtree

Enable this parameter if there is a tree below the Base DN which can contain user entries. For example, if all users are in "cn=users" this field should not be toggled. However, if users can appear in organizational units below "cn=users", such as "ou=development,cn=users,dc=sonatype,dc=com" this field should be toggled

Object Class (*required*)

The object class defines what attributes are expected for a given object. What is entered here must be the object class for the Username Attribute, Real Name Attribute, Email Attribute, and the Password Attribute.

User Filter

The user filter allows you to isolate a specific set of users under the Base DN.

Username Attribute (*required*)

This is the attribute of the Object class which supplies the username.

Real Name Attribute (*required*)

This is the attribute of the Object class which supplies the real name of the user.

E-Mail Attribute (*required*)

This is the attribute of the Object class which supplies the email address of the user.

Password Attribute

This is the attribute of the Object class which supplies the User Password. By default it is not toggled, which means authentication will occur as a bind to the LDAP server. Otherwise this is the attribute of the Object class which supplies the password of the user.


3.5 Mapping LDAP Groups to Sonatype CLM

In most LDAP implementations users are collected into various groups. This allows for better organization of a larger numbers of users, as well as provides a mechanism to isolate particular groups for specific permissions and integration into other systems such as Sonatype CLM. If LDAP groups are not mapped, Sonatype CLM will pull in all users from the Base DN. This isn't so much an an issue for a small number of users. However, for larger ones it may be a concern and might grant unintended access.

As we've done with the other configuration areas, let's look at a sample set of data. In example below we'll be configuring a static LDAP group.

Group Type	Static
Base DN	ou=groups
Object Class	group
Group ID Attribute	sAMAccountName
Group Member Attribute	member
Group Member Format	

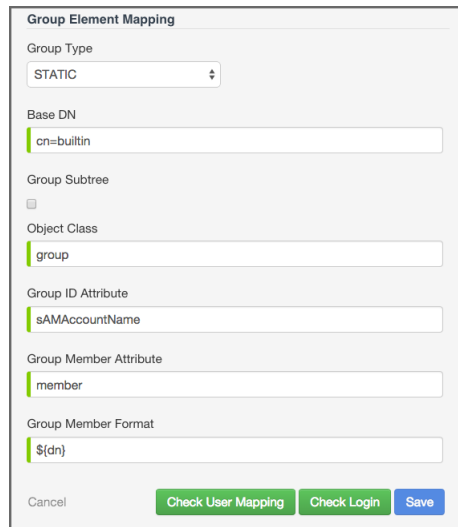
Once you have gathered this information, access the Sonatype CLM Server LDAP Configuration:

1. Log into the Sonatype CLM Server (*by default this is available at <http://localhost:8070>*) using a user account with Admin-level permissions (a member of the Admin Group).
2. Click the system preferences icon  located in the top right of the CLM Header/Screen (resembles a cog/gear).
3. Choose LDAP from the available option. The *LDAP Administration* area will be displayed.
4. Click on the Second Tab, just below the Server Name, *User and Group Settings*.
5. Just below the User Element mapping, you will see Group Element Mapping. The Group Type field will be set to *none*. Change this to *static* or *dynamic* based on the parameter descriptions below.
6. Enter the various settings.
7. Click the **Save** button when finished.

Note

If at any point you wish to reset the form, click the reset button; Any values that have been entered will be removed.

Using the information from the table above our configuration would look like this:



The image shows a 'Group Element Mapping' configuration window. It contains several fields for setting up a group. The 'Group Type' is set to 'STATIC'. The 'Base DN' is 'cn=builtin'. The 'Group Subtree' checkbox is unchecked. The 'Object Class' is 'group'. The 'Group ID Attribute' is 'sAMAccountName'. The 'Group Member Attribute' is 'member'. The 'Group Member Format' is '\$(dn)'. At the bottom, there are three buttons: 'Cancel', 'Check User Mapping', and 'Check Login', followed by a 'Save' button.

Field	Value
Group Type	STATIC
Base DN	cn=builtin
Group Subtree	<input type="checkbox"/>
Object Class	group
Group ID Attribute	sAMAccountName
Group Member Attribute	member
Group Member Format	\$(dn)

Figure 3.3: Group Mapping

3.6 LDAP Group Parameters

Groups are generally one of two types in LDAP systems - static or dynamic. A static group contains a list of users. A dynamic group is where the user contains a list of groups the user belongs to. In LDAP a static group would be captured in an entry with an Object class `groupOfUniqueNames` which contains one or more `uniqueMember` attributes. In a dynamic group configuration, each user entry in LDAP contains an attribute which lists group membership. This means the available parameters will be different based on whether you've chosen static or dynamic.

Tip

Static groups are preferred over dynamic ones, and will generally perform better if you have a large number of LDAP users.

3.6.1 Static Groups

Static groups are configured with the following parameters:

Base DN (*required*)

This field is similar to the Base DN field described for User Element Mapping. If your groups were defined under "ou=groups,dc=sonatype,dc=com", this field would have a value of "ou=groups"

Group Subtree

This field is similar to the User Subtree field described for User Element Mapping. If all groups are defined under the entry defined in Base DN, this field should not be selected. If a group can be defined in a tree of organizational units under the Base DN, this field should be selected.

Object Class (*required*)

This is a standard object class defined as a collection of references to unique entries in an LDAP directory, and can be used to associate user entries with a group.

Group ID Attribute (*required*)

This field specifies the attribute of the Object class that defines the Group ID.

Group Member Attribute (*required*)

This field specifies the attribute of the Object class that defines a member of a group.

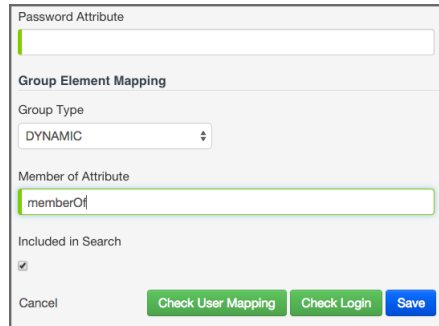
Group Member Format (*required*)

This field captures the format of the Group Member Attribute, and it is used by Sonatype CLM to extract a username from this attribute. For example, if the Group Member Attribute has the format `uid=brian,ou=users,dc=sonatype,dc=com`, then the Group Member Format would be `uid=${username},ou=users,dc=sonatype,dc=com`. If the Group Member Attribute had the format "brian", then the Group Member Format would be `${username}`.

3.6.2 Dynamic Groups

If your installation does not use Static Groups, you can configure Sonatype CLM LDAP integration to refer to an attribute on the User entry to derive group membership. To do this, select Dynamic Groups in the Group Type field in Group Element Mapping.

Dynamic groups are configured via the Member of Attribute parameter. Sonatype CLM will inspect this attribute of the user entry to get a list of groups that the user is a member of. In this configuration, a user entry would have an attribute such as *memberOf* which would contain the name of a group.



The dialog box titled "Dynamic Group Options" contains the following fields and controls:

- Password Attribute:** A text input field.
- Group Element Mapping:**
 - Group Type:** A dropdown menu currently showing "DYNAMIC".
 - Member of Attribute:** A text input field containing "memberOf".
- Included in Search:** A checkbox that is currently checked.
- Buttons:** "Cancel", "Check User Mapping", "Check Login", and "Save".

Figure 3.4: Dynamic Group Options

Tip

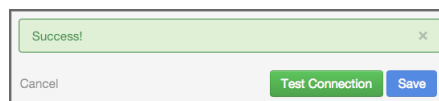
Depending on the size of your enterprise, LDAP search could be slow. If you find this is the case, uncheck the option to "Include in Search". This will [exclude groups from search results](#) when mapping users to roles. Searching for users will remain unaffected.

3.7 Verifying LDAP Configuration

It's easy to make a typo, or even have entered the wrong information when mapping LDAP users or groups. There are a number of tools provided within the LDAP configuration area to assist in making sure everything has been mapped correctly. Each of these is discussed below.

3.7.1 Test Connection

Testing the LDAP connection is the first step. If you can't connect to your LDAP server, user and group mapping will fail as well.



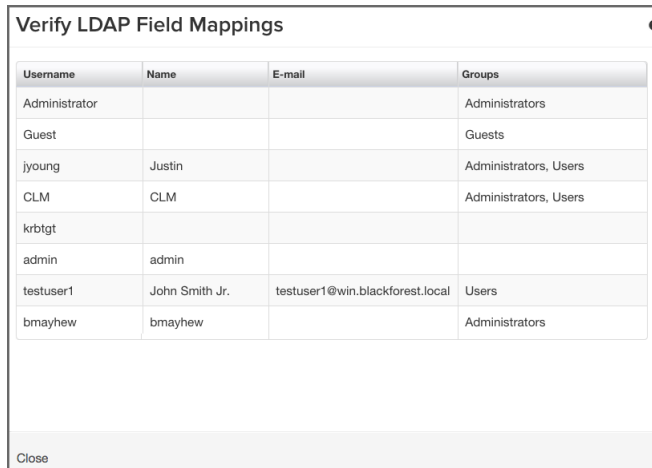
The dialog box titled "Testing LDAP Server" shows a successful outcome:

- Message:** A green box at the top contains the text "Success!".
- Buttons:** "Cancel", "Test Connection", and "Save".

Figure 3.5: Testing LDAP Server

3.7.2 Check User and Group Mapping

Making sure that usernames, real names, email addresses, and groups have been mapped correctly can be verified with the Check User Mapping.



The dialog box titled "Verify LDAP Field Mappings" contains a table with four columns: Username, Name, E-mail, and Groups. It lists several LDAP entries and their corresponding mappings.

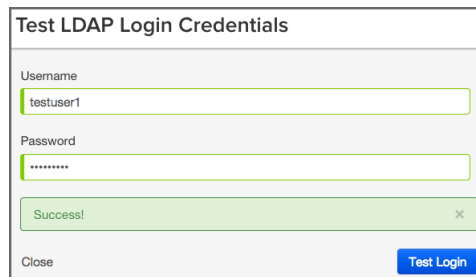
Username	Name	E-mail	Groups
Administrator			Administrators
Guest			Guests
jyoung	Justin		Administrators, Users
CLM	CLM		Administrators, Users
krbtgt			
admin	admin		
testuser1	John Smith Jr.	testuser1@win.blackforest.local	Users
bmayhew	bmayhew		Administrators

Close

Figure 3.6: Checking User Mapping

3.7.3 Check Login

As a final test to ensure users can log in, the Check Login allows you to enter a user name and password, and ensure ensure that this can be authenticated with the LDAP server.



The dialog box titled "Test LDAP Login Credentials" contains input fields for Username and Password. The Username field is filled with "testuser1" and the Password field is filled with "*****". Below the fields is a green "Success!" message with a close icon. At the bottom, there is a "Close" button and a blue "Test Login" button.

Test LDAP Login Credentials

Username
testuser1

Password

Success! ✕

Close Test Login

Figure 3.7: Checking User Login

Chapter 4

Role Management (Permissions) Overview

Roles control the permissions for use within the CLM Server as well as the connected suite of tools. When users are mapped to a role they are granted a set of permissions associated with that role. This section describes the available roles, as well as how to map users to those roles.

4.1 Role Definitions

Administrator

The Administrator role is considered a global role, and is managed via system preferences `figs/web/clm-server-system-preferences-icon.png`. It has the full permissions to view, create, and modify any element of the Sonatype CLM Server. This extends to interaction with the entire suite of Sonatype CLM tools, and includes permission to evaluate applications or components and review the results.



Warning

Due to the unrestricted access of the Administrator role, [changing the password](#) from the provided default is highly recommended.

Owner

The Owner role provides full permissions for the user mapped to the Organization or Application. This includes viewing, creating, and modifying any element within the scope of the respective

organization/application. It also includes permission to evaluate applications or components and review the results.

Developer

The Developer role provides view permissions for the user mapped to the Organization or Application. It also includes permission to evaluate components and review the results.

Application Evaluator

The Application Evaluator role provides permission to submit applications for evaluation and retrieve summary-level results for the user mapped to the Organization or Application. This role is useful for tools such as continuous integration (e.g. [CLM for Bamboo](#) or [CLM for Hudson/Jenkins](#)) and command line evaluation (e.g. [CLM for CLI](#)). This role can also be used to configure these tools and allows these tools to display a summary of the policy evaluation.

Component Evaluator

The Component Evaluator role provides permission to submit components for evaluation and retrieve summary-level results for the user mapped to the Organization or Application. This role is useful for tools such as an IDE (e.g. [CLM for IDE](#)) and Nexus (e.g. [CLM for Nexus](#)) which retrieve policy evaluation at the component level. While this role can retrieve evaluation results, it cannot override any component data nor apply component labels.

Note

For all roles except the Administrator role, when a user is mapped to a role for an Organization, the user will have the same permissions associated with that role for any attached Applications.

4.2 Mapping Roles

To map a user (or group if you have configured LDAP) to a role, follow the instructions below:

1. Log in to the Sonatype CLM Server with a user mapped to either the Administrator role, or the Owner role (for an Organization and/or Application).

Note

When mapping users with the Owner role, you will only be able to map users to the Organization and/or Application you are an owner for.

2. Navigate to an Organization or Application, click on the Security tab, and then click the *Edit* icon (it resembles a pencil).
-

3. A search widget will be displayed. In the search field, enter as much of the user's complete name as possible, followed by a trailing wildcard (e.g. Isaac A*), and then click the *Search* button.

Note

Practice caution as use of leading wildcards can greatly impact user search times.

4. Once you see the user you wish to add in the Available column, click the *Plus* icon to move them to the Applied column. To remove users from a role, follow the same process above, just click the *Minus* icon to move the user from the Applied column to the Available column. Click the *Save* button to save your changes.

Tip

You may notice that below each user, there is additional information. Most often this is the email. However, to the right of the email you will see the Realm (e.g. LDAP). Use this to ensure you add the appropriate account.

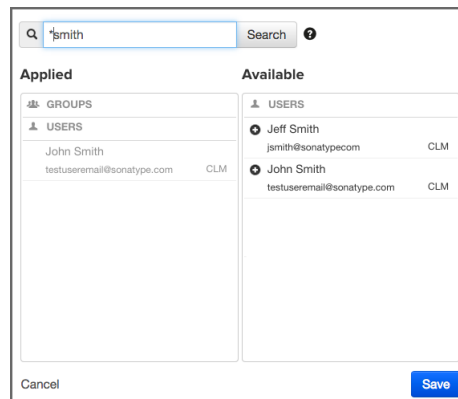


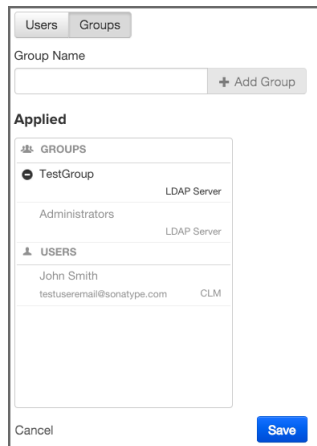
Figure 4.1: Mapping Users to roles

4.3 Excluding Groups from Search Results

Mapping a group to a role utilizes elements that are configured via the [LDAP System Preferences area](#). If you go with the default options, groups will be included with the search results. That is, when you enter something into the *Find User* field, both groups and single users will be returned.

However, because the size of LDAP implementation can vary, you may want to consider not including groups with your search results. This option can be adjusted when using [Dynamic Groups settings](#).

Making this change will then allow you to manually enter group names. However, when entering groups this way, no search or validation will be performed.



The screenshot shows the 'Groups' tab in the Sonatype CLM Server Security Administration interface. At the top, there are two tabs: 'Users' and 'Groups'. Below the tabs, there is a 'Group Name' input field and an '+ Add Group' button. The 'Applied' section is divided into two parts: 'GROUPS' and 'USERS'. The 'GROUPS' section shows a list of groups, including 'TestGroup' (selected), 'Administrators', and 'LDAP Server'. The 'USERS' section shows a list of users, including 'John Smith' (selected) and 'testuseremail@sonatype.com'. At the bottom, there are 'Cancel' and 'Save' buttons.

GROUPS	
<input checked="" type="radio"/> TestGroup	LDAP Server
<input type="radio"/> Administrators	LDAP Server

USERS	
<input checked="" type="radio"/> John Smith	CLM
<input type="radio"/> testuseremail@sonatype.com	

Figure 4.2: Mapping Groups When Not Included With Search