

Step 3 - Security Administration

Contents

1	Introduction	1
2	User Management	2
2.1	Logging in to Sonatype CLM	3
2.2	Changing the Admin Password	3
2.3	Creating a User	4
2.4	Editing and Deleting User Information	5
3	LDAP Integration	7
3.1	Configuring the LDAP Server Connection	8
3.2	LDAP Configuration Parameters	9
3.3	Mapping LDAP Users to Sonatype CLM	11
3.4	LDAP User Parameters	12

3.5	Mapping LDAP Groups to Sonatype CLM	13
3.6	LDAP Group Parameters	15
3.6.1	Static Groups	15
3.6.2	Dynamic Groups	16
3.7	Verifying LDAP Configuration	16
3.7.1	Test Connection	17
3.7.2	Check User and Group Mapping	17
3.7.3	Check Login	18
4	Role and Permission Management	19
4.1	Organization, Applications, and Inheritance	19
4.2	Roles and Permissions	21
4.3	Assigning Users to Standard Roles	23
4.4	Assigning Users to Global Roles	25
5	Summary	27

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	Testing LDAP Server	17
3.5	Checking User Mapping	17
3.6	Checking User Login	18
4.1	Inheritance and User Roles Overview	20
4.2	Example of Roles	22

4.3	Assigning Users to Standard Roles	24
4.4	Assigning Users to Global Roles	26

[Return to the Nine Steps Main Page](#)

Chapter 1

Introduction

With the download and installation of Sonatype CLM out of the way, you've now completed two of the biggest steps. Next up Step 3, Security Administration.

By default, and don't worry this is covered in greater detail within this guide, there is an admin account (login: admin, password: admin123). This account is considered a Super User inside of Sonatype CLM. That is, you have access to perform any function. As you will see in the guide, we recommend changing the password for this account as a first point of action.

If your just looking to get Sonatype CLM up and running as quickly as possible, you can stop there. That account will allow you to move towards completion of the Nine Steps for Open Source Governance. However, if you want to go ahead and approach a more robust setup of users and roles, this guide will also walk you through the entire suite of security administration features provided by Sonatype CLM.

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
 - 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

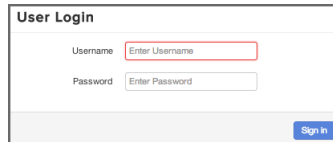
A screenshot of the 'User Login' form. It has a title 'User Login' at the top left. Below it, there are two input fields: 'Username' with a placeholder 'Enter Username' and 'Password' with a placeholder 'Enter Password'. A blue 'Sign In' button is located at the bottom right of the form.

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 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 2.4 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.

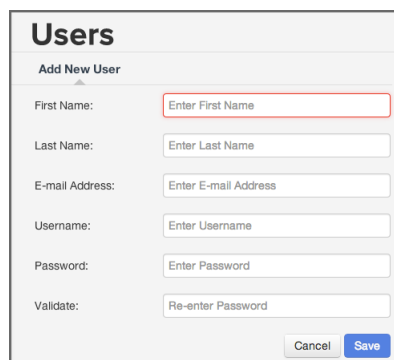
Note

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.

2.3 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.
-



The screenshot shows a web interface titled "Users" with a sub-header "Add New User". Below this, there are six input fields arranged vertically, each with a label on the left and a text box on the right. The labels are "First Name:", "Last Name:", "E-mail Address:", "Username:", "Password:", and "Validate:". The text boxes contain placeholder text: "Enter First Name", "Enter Last Name", "Enter E-mail Address", "Enter Username", "Enter Password", and "Re-enter Password". At the bottom right of the form, there are two buttons: "Cancel" and "Save".

Figure 2.2: Create User

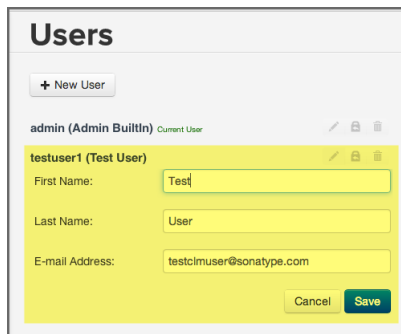
2.4 Editing and Deleting User Information

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 screenshot displays a web interface titled "Users". At the top left, there is a "+ New User" button. Below this, the current user is identified as "admin (Admin BuiltIn) Current User". The main section shows a user entry for "testuser1 (Test User)". This entry is highlighted with a yellow background and includes edit, delete, and add icons. The form for editing this user contains three fields: "First Name" with the value "Test", "Last Name" with the value "User", and "E-mail Address" with the value "testclmuser@sonatype.com". At the bottom right of the form are "Cancel" and "Save" buttons.

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

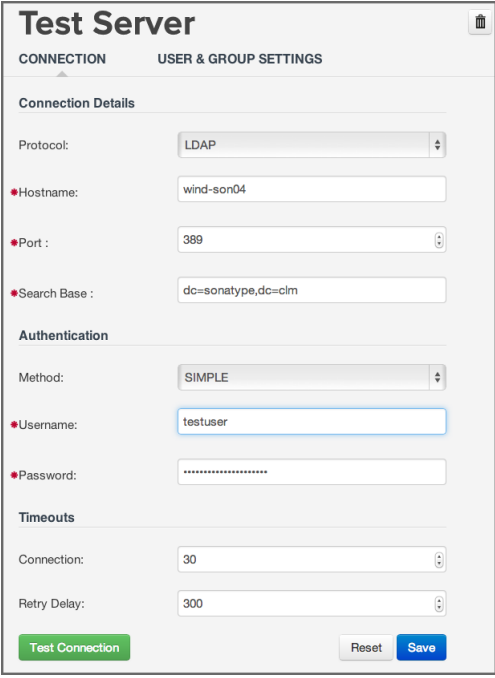
The information provide will not allow you to access an LDAP server, and is provided just for demonstration purposes. In addition, this is only a representation of a simple connection. For an explanation of all available parameters, please see the next section.

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 'Test Server' configuration window, which is divided into two tabs: 'CONNECTION' and 'USER & GROUP SETTINGS'. The 'CONNECTION' tab is currently selected. Under the 'Connection Details' section, the following fields are visible: 'Protocol' is set to 'LDAP'; 'Hostname' is 'wind-son04'; 'Port' is '389'; and 'Search Base' is 'dc=sonatype,dc=clm'. The 'Authentication' section shows 'Method' set to 'SIMPLE', 'Username' as 'testuser', and 'Password' masked with dots. The 'Timeouts' section has 'Connection' set to '30' and 'Retry Delay' set to '300'. At the bottom, there are three buttons: 'Test Connection' (green), 'Reset' (grey), and 'Save' (blue).

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
User ID 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 'Test Server' configuration interface, specifically the 'USER & GROUP SETTINGS' tab. The 'User Element Mapping' section contains the following fields: 'Base DN' (cn=users), 'User Subtree' (empty), 'Object Class' (user), 'User Filter' (empty), 'Username Attribute' (sAMAccountName), 'Real Name Attribute' (cn), and 'E-mail Attribute' (mail). There is an unchecked checkbox for 'Use Password Attribute'. The 'Group Element Mapping' section has a 'Group Type' dropdown set to 'NONE'. At the bottom, there are buttons for 'Check User Mapping', 'Check Login', 'Reset', and 'Save'.

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 User ID 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.

User ID Attribute (*required*)

This is the attribute of the Object class which supplies the User ID.

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 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. While this may not be an issue for a small number of users, for larger ones, it may be a concern and may 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	

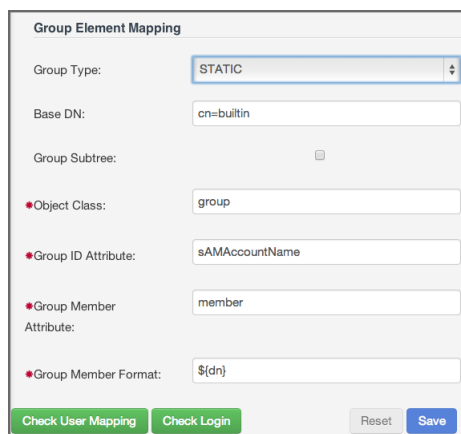
Once you have gathered this information, access the Sonatype CLM Server LDAP Configuration:

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: 'Group Type' is a dropdown menu set to 'STATIC'; 'Base DN' is a text field with 'cn=builtin'; 'Group Subtree' has an unchecked checkbox; 'Object Class' is a text field with 'group'; 'Group ID Attribute' is a text field with 'sAMAccountName'; 'Group Member Attribute' is a text field with 'member'; and 'Group Member Format' is a text field with '\$(dn)'. At the bottom, there are four buttons: 'Check User Mapping' (green), 'Check Login' (green), 'Reset' (grey), and 'Save' (blue).

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.

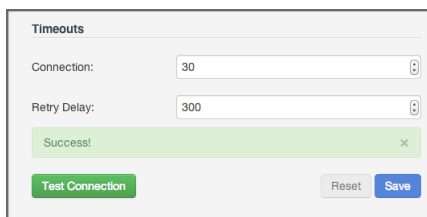
Dynamic groups are configured via the Member of Attribute parameter. Sonatype CLM will inspect this attribute of the user entry to get a list of groups that the user is a member of. In this configuration, a user entry would have an attribute such as *memberOf* which would contain the name of a group.

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.

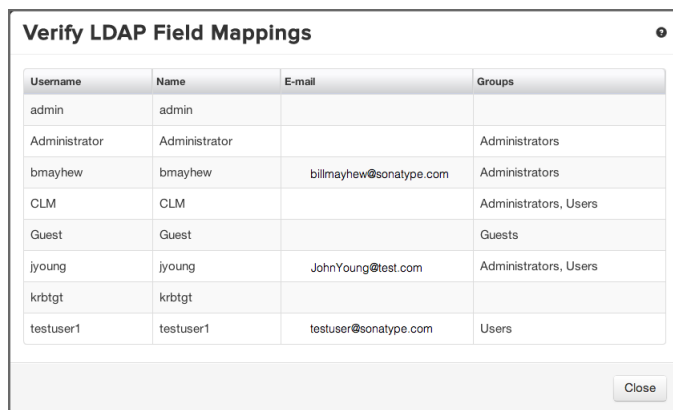


The screenshot shows a 'Timeouts' configuration window. It has two input fields: 'Connection' with the value '30' and 'Retry Delay' with the value '300'. Below these fields is a green bar with the text 'Success!' and a close icon. At the bottom, there are three buttons: 'Test Connection' (green), 'Reset' (gray), and 'Save' (blue).

Figure 3.4: Testing LDAP Server

3.7.2 Check User and Group Mapping

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



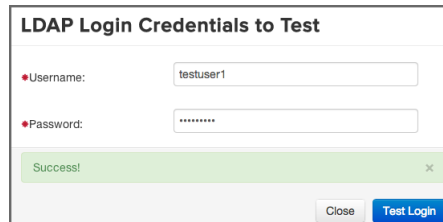
The screenshot shows a 'Verify LDAP Field Mappings' window. It contains a table with four columns: Username, Name, E-mail, and Groups. The table lists several users and their corresponding LDAP fields. A 'Close' button is located at the bottom right of the window.

Username	Name	E-mail	Groups
admin	admin		
Administrator	Administrator		Administrators
bmayhew	bmayhew	billmayhew@sonatype.com	Administrators
CLM	CLM		Administrators, Users
Guest	Guest		Guests
jyoung	jyoung	JohnYoung@test.com	Administrators, Users
krbtgt	krbtgt		
testuser1	testuser1	testuser@sonatype.com	Users

Figure 3.5: 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 image shows a dialog box titled "LDAP Login Credentials to Test". It contains two input fields: "Username:" with the value "testuser1" and "Password:" with masked characters "*****". Below the password field is a green success message "Success!" with a close icon. At the bottom right are "Close" and "Test Login" buttons.

LDAP Login Credentials to Test	
•Username:	testuser1
•Password:	*****
Success! ✕	
Close Test Login	

Figure 3.6: Checking User Login

Chapter 4

Role and Permission Management

Sonatype CLM not only limits access by login, but it also distinguishes the level of access, what a user can or can't do, using an intuitive system of roles. Each role has a specific set of permissions. Users are then assigned to these roles, granting users the ability to perform various functions or limiting access to points of data within Sonatype CLM.

Needless to say, the roles and permissions management system inside of Sonatype CLM is powerful. Unfortunately, powerful can sometimes translate to overwhelming. To help ease you into managing Sonatype CLM permissions, this section of the Security Administration Guide will walk you through everything you need to know. This includes:

- Organizations and Applications
- Roles and Permissions
- Assigning Users to Roles

4.1 Organization, Applications, and Inheritance

Whether or not you will ever interact with elements of Sonatype CLM outside of Security Administration, you will still need to understand the impact Organizations and Applications have on how roles are managed. Mainly granting at the application level is exclusive to that application, while granting at the

organization level allows access to view and make changes across any assigned applications as well as the organization itself. This is due to a concept called inheritance, and it can be used to vastly reduce the need to add every user to each application.

While, we do cover this in our other guides, we should start by taking a basic look at these two areas. The image below gives an example of how we can reduce repetition of users by choosing to manage by organization.

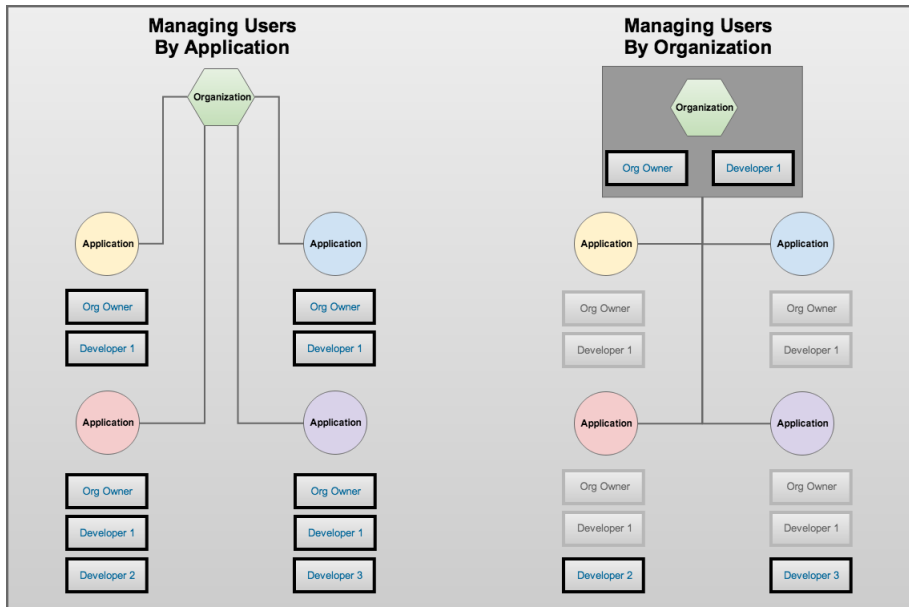


Figure 4.1: Inheritance and User Roles Overview

Applications

Applications are created in Sonatype CLM. They allow users to identify a specific project, and then track the health of components in that project. Each application must have a specific name, a unique identifier (Application ID), and an organization. Each application may also have policies (rules) and other associated policy elements (e.g. license threat groups and labels). Finally, an application will inherit policies and policy elements from its selected organization.

The important piece to see here is that applications are very singular. Changes made here will have an impact, but will be isolated to the particular application. This is very different compared to organizations.

Organizations

Similar to applications, an organization will have a specific name, but it does not need a specified

identifier. Organizations may also have policies (rules) and a number of associated policy elements (e.g. license threat groups and labels). However, unlike applications, organizations aren't tied to a specific project / application. Instead, they function more like a container to hold multiple applications. Given this, in cases where an organization has policies or policy elements, any application that has selected this organization, will inherit all those policies and policy elements.

Again, the important piece to pay attention to here is that users assigned to an organization have the potential to view and/or interact with not just the organization, but also any application attached to that organization.

4.2 Roles and Permissions

If you skipped to here, we understand, you are in a hurry to get Sonatype CLM working in your business. However, in bypassing our basic organization and application overview, we will assume you are familiar with those concepts. If you haven't, go take a look again. Even if you don't plan on using CLM beyond a role of installation, deployment, and/or security administration, the previous section can help prevent unwanted access and reduce unnecessary repetition.

If you are still dissuaded, here is the abbreviated version:

- Adding a user to a role for an application grants access to only that application.
- Adding a user to a role for an organization grants access to the organization **AND** all attached applications due to a principle called inheritance.

OK, so we know to be careful when adding a user to a role for an organization or application, but what is a role exactly?

Great question, a role is a set of permissions that have been predefined by Sonatype. These permissions are based on the concept of being able to either view data or manipulate. And by manipulate, we mean the ability to create, edit or delete. In Sonatype CLM, two standard roles are included:

- Owner - allows a user to view, create, edit and delete.
 - Developer - allows only the ability to view.
-

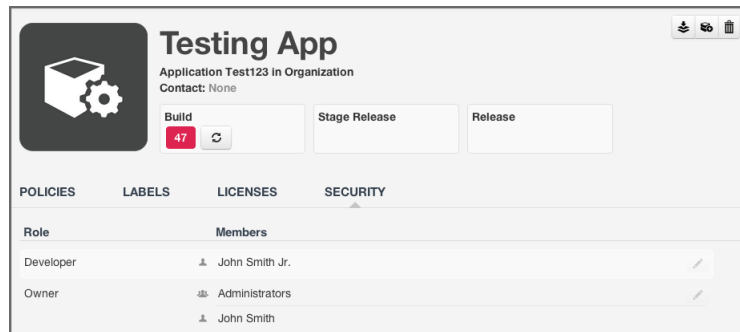


Figure 4.2: Example of Roles

In both cases, the second most important aspect of roles is where the role is assigned, either at the organization, or the application. To understand this a little better, let's look at a few examples.

Using the Developer Role

First, I have a member of the development team for my application, Awesome App. I only want this team member to be able to view aspects of Awesome App, such as the report displaying policy violations, or see the policy itself. This team member shouldn't be able to edit, and again I only want them to see information for Awesome App. In this example, I would assign my user to the developer role for Awesome App.

Using the Owner Role

Alright, now let's look at a slightly different example. A member of your security team, responsible for ensuring components in applications meet your business's specific standards, needs access to review policy and violation results for all applications. He/She is also responsible for managing policies, meaning he/she will need to make changes. However, they are only responsible for Awesome App, so the access this individual needs is Owner access, and like before, this would be at the application level. Specifically, I would make them an owner for Awesome App.

Inheriting a Role

Well, it seems easy enough to assign a role to an individual, but what happens if you need to add someone to all the applications under an organization, say like the Director of Development? OK, one more example then.

The Director of Development, who is also responsible for managing policies and setting up new applications, needs access to Sonatype CLM. The director will need to have full access to create, view, edit and delete multiple applications. Now, we could go in and make the Director an owner of each application. However, just like policies and policy elements (what we discussed previously), applications also inherit role members based on their organization. So, all we need to do for our direction, is assign them as an owner for a specific organization, or perhaps even multiple organizations, if you have set CLM up that way.

Tip

You can use inheritance when assigning developers as well. Just like the example above, if you want a user to be in the Developer Role for all applications in an organization, simply add the individual to the Developer Role at the organization level.

Obviously, there are lots of examples we could run through. However, just remember that the level of the Role you are assigning a user to is as important as the role itself. Now that you know, let's go assign some users to roles.

Note

We specifically left out one role, Administrator, which is identical to the default admin account that ships with Sonatype CLM. It is considered a Global Role, and if you are looking to grant a user access to full rights in Sonatype CLM, this is the role you would use. It is important to note, that limited use of this role is suggested, and modification must be made by an existing member of the Administrator role.

4.3 Assigning Users to Standard Roles

The process for assigning a user to a standard role is identical whether you are doing it at the organization or application level. While there are differences applied to the scope of access the role will have, these have been outlined in the sections above, and won't be discussed here. It's also important to point out that if you have configured [LDAP Users](#) or [LDAP Groups](#), those will be returned when searching for users. With all of that out of the way, let's assign a user to a role.

1. First, 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. Next, make sure you are in the **Organizational Design** area. If not, click the *Organizational Design* icon .
 3. Once in the **Organizational Design** area, click on a specific organization or application, and then click the *Security* tab.
 4. A list of roles will be displayed, as well as the members of that role.
 5. To edit this list, hover over the role you wish to add a user to, and then click the *Edit* icon.
 6. To find a user, begin typing the user's name in the *search* field. No matter what you type, Sonatype CLM will find the best match, bolding the matched text in both the applied and available columns.
-

7. Once you see the user you wish to add in the Available column, click the *Plus* icon to move them to the Applied column.
8. Click the *Save* button to save your changes.

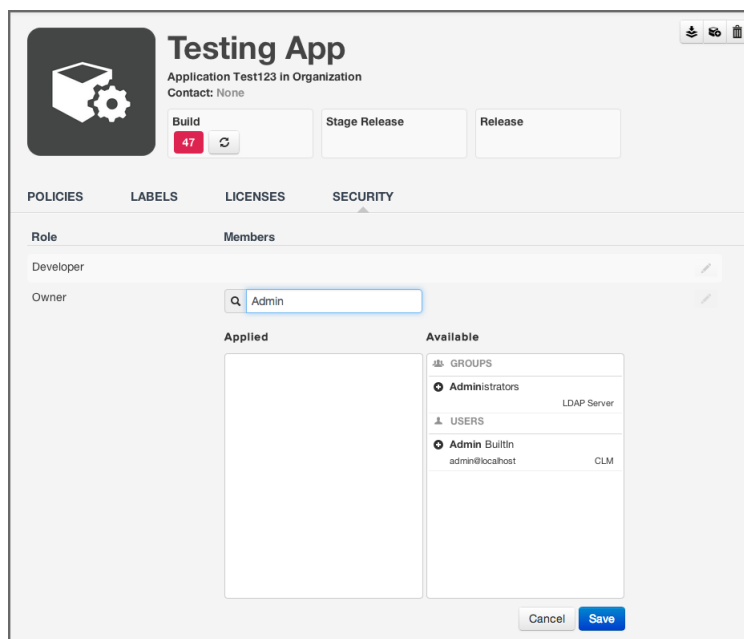


Figure 4.3: Assigning Users to Standard Roles

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. CLM). Use this to ensure you add the appropriate account (e.g. when working with CLM the local realm, and LDAP).

Note

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. However, if the user has been inherited, these must be removed at the organization level, and can be identified by no Minus icon.

4.4 Assigning Users to Global Roles

As we mentioned previously, there is another role type, the Global Role. Global roles operate independently from standard roles, and at this time only includes Administrators. Any member of the Administrator Role will have access to every aspect of Sonatype CLM, including the ability to create new organizations and delete existing ones. Additionally, this administration role has the ability to assign users to any other role on Sonatype CLM.

Adding a user to the Administrator role is similar to standard roles, however it is managed in the **Security** section of CLM System Preferences. Also, just as with Standard Roles, if you have configured [LDAP Users](#) or [LDAP Groups](#), those will be returned when searching for users. To add a user to this role:

1. First, 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 *Global Roles* from the drop down menu. The **Global Roles System Preferences** area, and a list of roles will be displayed.
4. Next to the role name a list of users that are assigned to will be displayed. To edit this list, hover over the role you wish to add a user to, and then click the *Edit* icon.
5. To find a user, begin typing the user's name in the *search* field. No matter what you type, Sonatype CLM will find the best match, bolding the matched text in both the applied and available columns. As mentioned above, if configured, LDAP Users and Groups will also be displayed here.
6. In some cases, you may be using multiple realms beyond that of Sonatype CLM, for example, LDAP for Active Directory. In these cases the Realm information will also be displayed.
7. Once you see the user you wish to add in the Available column, click the *Plus* icon to move them to the Applied column.
8. Click the *Save* button to save your changes.

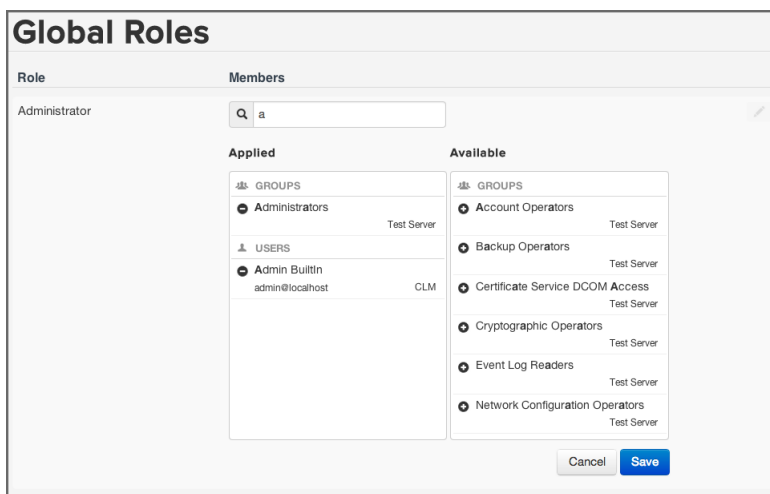


Figure 4.4: Assigning Users to Global Roles

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. CLM). Use this to ensure you add the appropriate account (e.g. when working with CLM the local realm, and LDAP).

Note

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.

Chapter 5

Summary

OK, Sonatype CLM is now installed, configured, and secured to your specifications. With those out of the way, we can start learning how Sonatype CLM enables your business to improve visibility of risky component usage. This starts with understanding two core concepts, Organizations and Applications. We'll be discussing those in [Step 4 - Policy Guide](#).
