Sonatype CLM Server - Security Administration

Contents

List of Figures

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
- 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

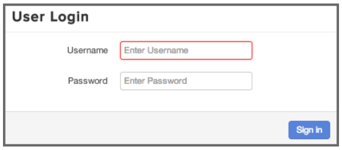


Figure 2.1: Login

Once you log in 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.

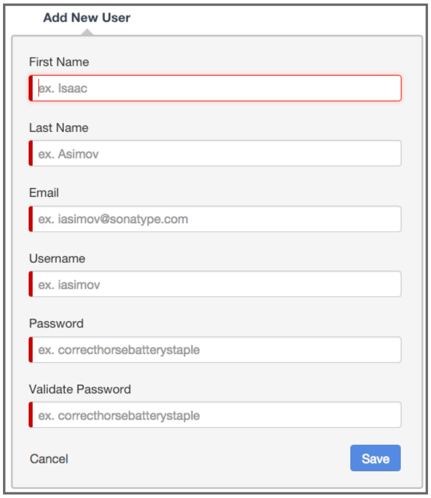


Figure 2.2: Create User

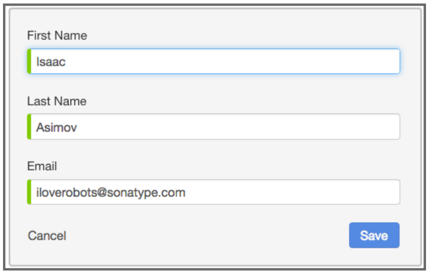
2.4 Editing and Deleting User Information

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.



First Name: Isaac

Last Name: Asimov

Email: iloverobots@sonatype.com

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

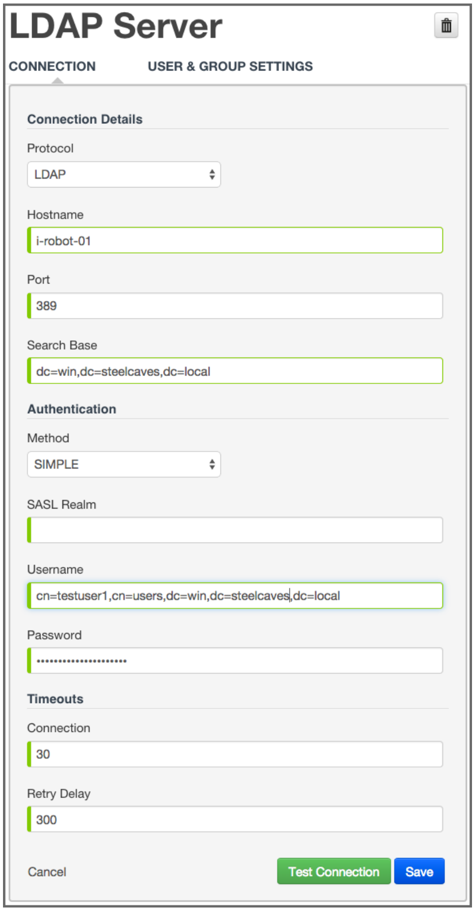
Note
The information provide will not allow you to access an LDAP server, and is provided just for demonstration purposes. In addition, this is only a representation of a simple connection. For an explanation of all available parameters, please see the next section.

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:



LDAP Server

CONNECTION USER & GROUP SETTINGS

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.

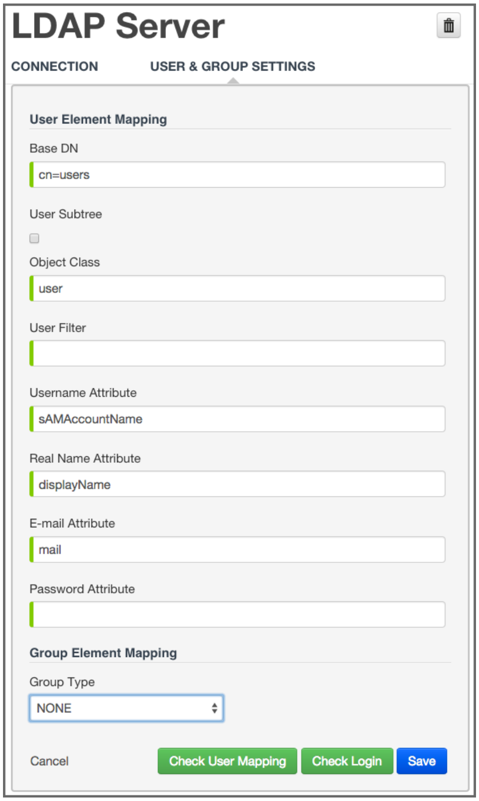
4. Click on the Second Tab, just below the Server Name, *User and Group Settings*.

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:



LDAP Server

User Element Mapping

Base DN: cn=users

User Subtree: □

Object Class: user

User Filter:

Username Attribute: sAMAccountName

Real Name Attribute: displayName

E-mail Attribute: mail

Password Attribute:

Group Element Mapping

Group Type: NONE

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.

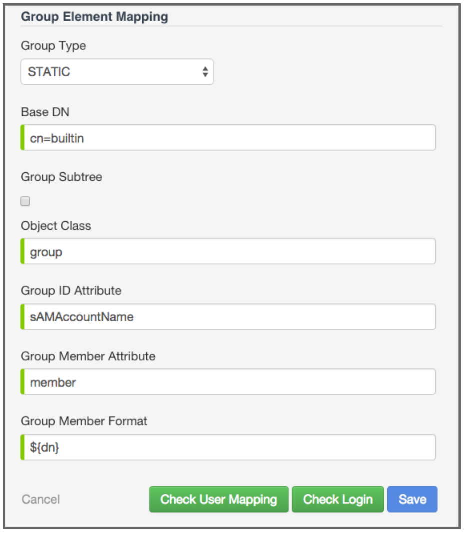
Group Type	Static
Base DN	ou=groups
Object Class	group
Group ID Attribute	sAMAccountName
Group Member Attribute	member
Group Member Format	

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:



Group Element Mapping

Group Type: STATIC

Base DN: cn=builtin

Group Subtree: □

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.

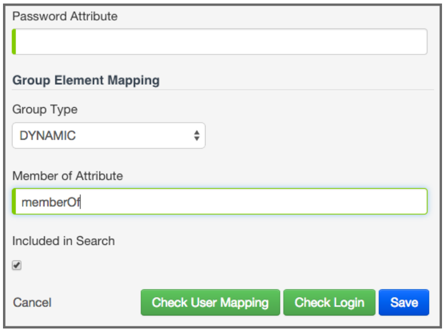
Group Member Attribute (*required*)
This field specifies the attribute of the Object class that defines a member of a group.

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.



Password Attribute

Group Element Mapping

Group Type

DYNAMIC

Member of Attribute

memberOf

Included in Search

☑

Figure 3.4: Dynamic Group Options

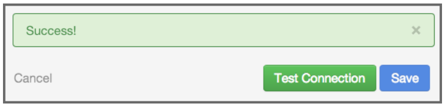
Tip
Depending on the size of your enterprise, LDAP search could be slow. If you find this is the case, uncheck the option to "Include in Search". This will change how users and groups our mapped, but should improve performance. This will disable searching for group, while searching for users will remain 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.

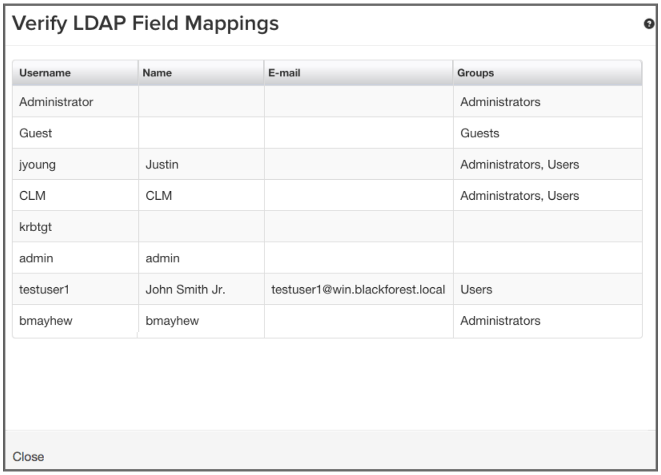


Success!

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.



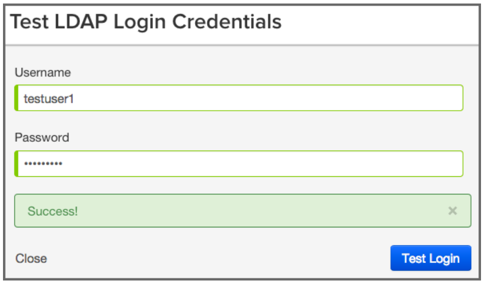
Verify LDAP Field Mappings

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

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.



Test LDAP Login Credentials

Username: testuser1

Password: •••••••••

Success!

Figure 3.7: 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 Defining Organizations, 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.

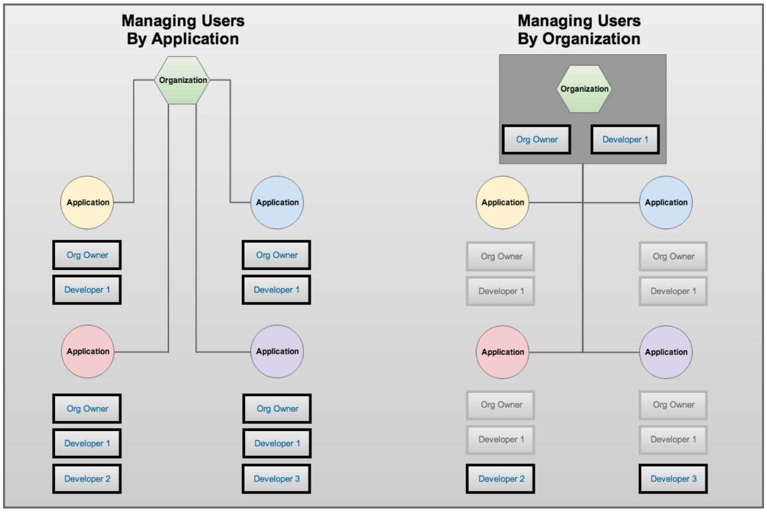


Figure 4.1: Inheritance and User Roles Overview

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 Understanding 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.

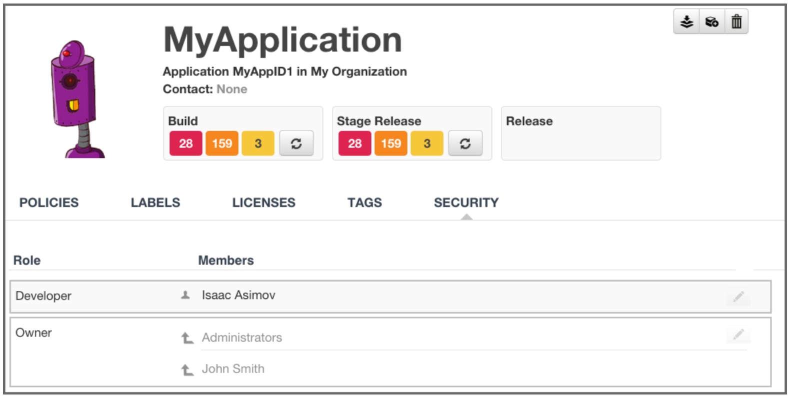
If you are still dissuaded, here is the abbreviated version:

- Mapping a user to a role for an application grants access to only that application.
- Mapping 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 mapping 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.



MyApplication

Application MyAppID1 in My Organization
Contact: None

Role	Members
Developer	Isaac Asimov
Owner	Administrators John Smith

Figure 4.2: Example of Roles

Note

In the image above, inherited users (or groups) are indicated by the arrow pointing up, located to the left of the corresponding name.

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 lets 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 application. 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 Mapping Users to Roles

Mapping a user (or group if you have configured LDAP) to a role simply means finding a user, and assigning them to the desired role. Doing so grants the user the level of permissions for the role. These permissions were described above, with possible scenarios for using each one. Below, we've described the typical process for mapping a user to a role.

1. From the security tab of an application or organization, click the *Edit* icon (it resembles a pencil).

Tip
Remember mapping a user to a role at the organization level will grant that user the same role and permissions to any associated applications.

2. A search widget will be displayed. In the search field, enter the user’s name exactly as it is entered in your LDAP server. For example if you are looking for Isaac Asimov, you would enter that complete name. In cases where you don’t know a user’s complete name, leading or trailing wildcards (*) can be added. Using the example above, if I only knew the first name of the user, I could simply enter *Isaac A**.

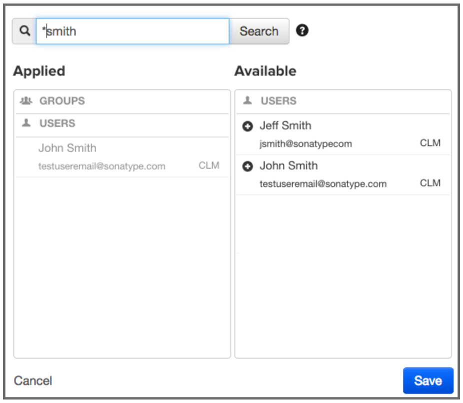
Warning
Use of leading wildcards can greatly impact user search times.

Note
Wildcards are only applicable for users of Sonatype CLM including, and beyond, version Sonatype CLM 1.11.1. All prior versions of Sonatype CLM do not support wildcard usage when mapping users to roles, as this is automatically appended/prepended to the search text (i.e. searching for *smith* is equivalent to **smith** in 1.11.1 and later).

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).

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

Tip
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.



*smith

John Smith testuseremail@sonatype.com CLM

Jeff Smith jsmith@sonatypecom CLM

John Smith testuseremail@sonatype.com CLM

Figure 4.3: Mapping Users to Roles

Note

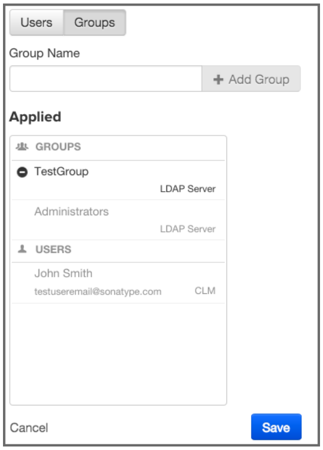
Global roles are managed via system preferences ⚙. They are also unique in that they only have one role type, Administrator. Because of this, it can't be stressed enough, that caution should be used when mapping users to this role.

Special Instructions When Groups Are Excluded 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.



Applied

GROUPS

TestGroup
LDAP Server

Administrators
LDAP Server

USERS

John Smith
testuseremail@sonatype.com CLM

Figure 4.4: Mapping Groups When Not Included With Search