LDAP, Users, Roles, & API Token

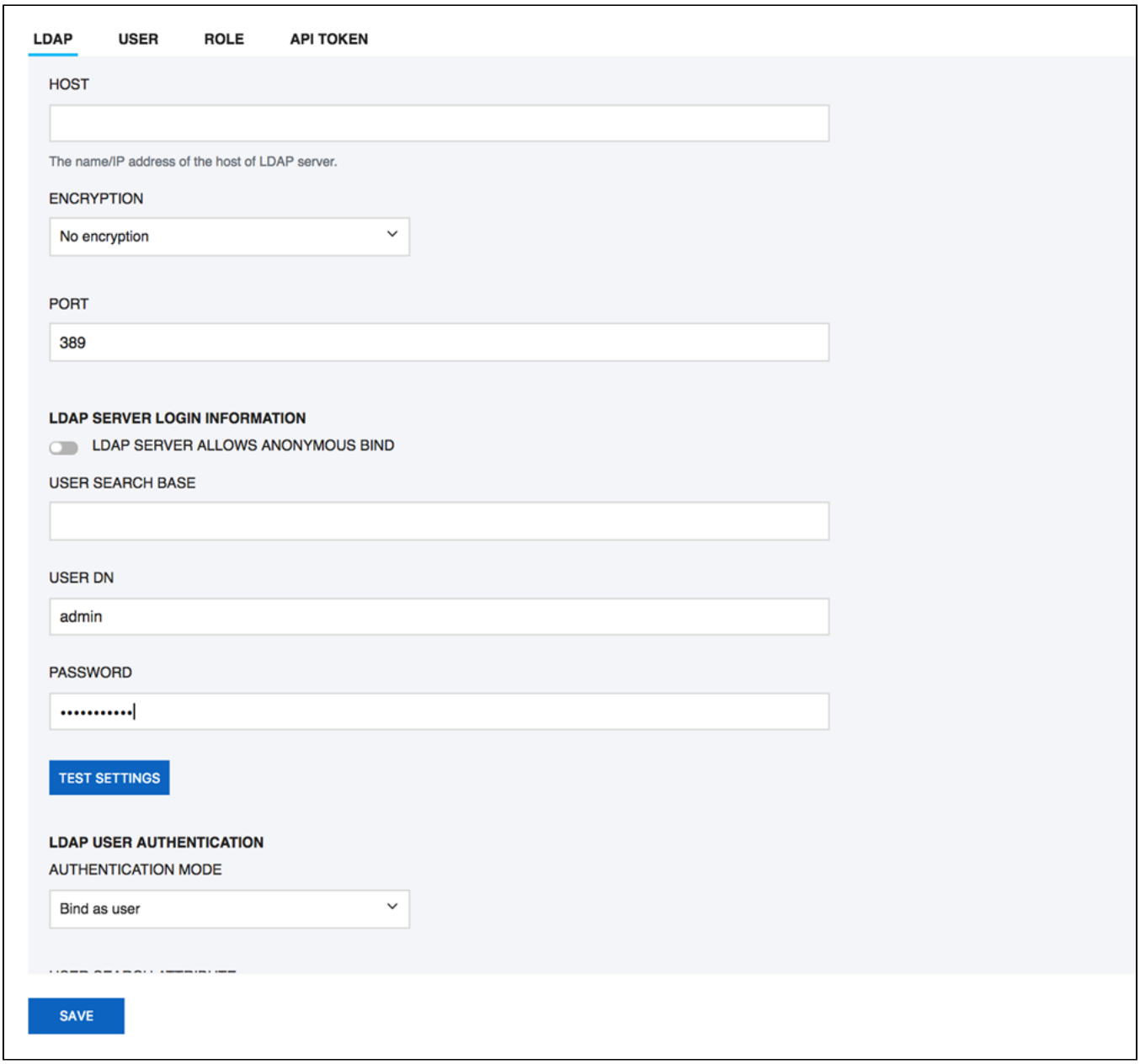
This page allows user to add LDAP authentication, create users, create different roles, and also to generate a new API token.

LDAP Settings

When logging into SQL DM for MySQL from the browser interface you may use authentication provided by LDAP server (including the Microsoft/Windows LDAP 'dialect' known as 'Active Directory'). In this case users need not to know SQL DM for MySQL authentication details directly, but only how to authenticate to the LDAP server. To use LDAP authentication for SQL DM for MySQL, specify settings as below:

1. Click **Settings**
2. Select **LDAP, Users, Roles & API Token,** the LDAP setting page opens, displaying the following options:

    - **Host:** Enter the hostname, IP address or URI (Uniform resource identifier) of your LDAP directory server.
    - **Encryption:** Select the type of encryption required for communication with the LDAP directory server. Supported encryption methods are None, StartTLS, and SSL(ldaps).
    - **CA CERTIFICATE:** If your encryption mode is StartTLS and SSL(Ldaps), then paste the content of your digital certificate issued by CA.
    - **Port:** Type in the port your LDAP directory server uses.
    - **LDAP server allows anonymous binds:** Select this option if your LDAP directory server allows anonymous binds to the server.
    - **User DN:** Enter the distinguished name of the entry to bind to the LDAP directory server.
    - **Password:** Enter the password of the User DN specified for binding the user to LDAP directory server.
    - **Test Settings:** Click **Test Settings** to use the mentioned **User DN**, **Password**, and binds with the LDAP directory server.
    - **Authentication mode:** Select the type of authentication mode to use for authenticating the user with the LDAP directory server. **Bind as User** binds user to LDAP directory with the password provided at login in SQL DM for MySQL interface. Authentication via Comparison is done by comparing the user credentials provided at login with the LDAP directory.
    - **User search base:** Type in the User search base filter for the object class you want to filter your users for authentication.
    - **User search attribute:** Enter the attribute name that contains the user name.
    - **Search entire subtree**: This option controls the search for objects specified in user search base. Selecting this option searchs the entire subtree of **User search base**.

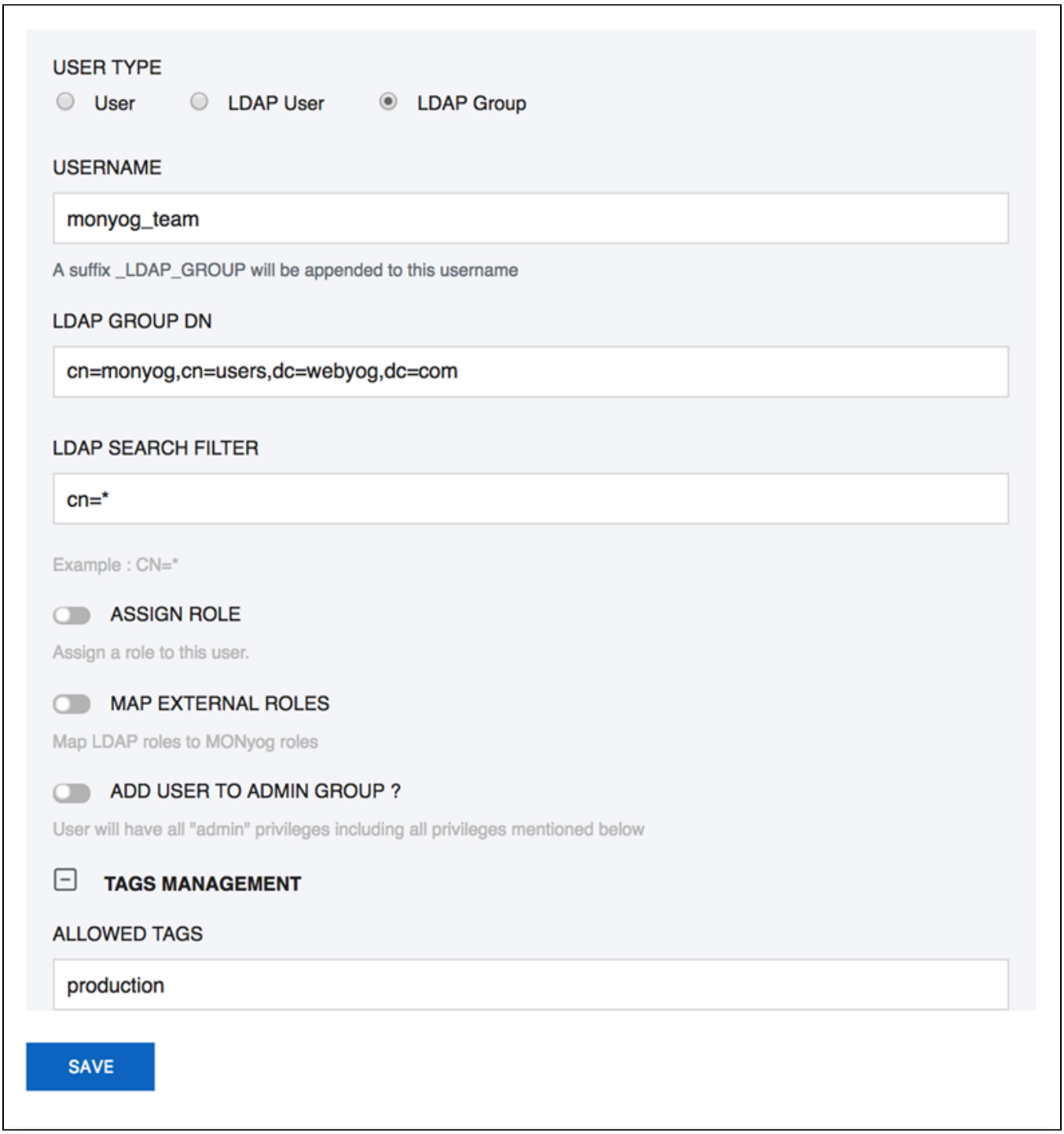


User Management

Using this option User Management, allows you to create, edit, and delete users.

How To Create User?

1. Click **Settings,** and select **LDAP, Users, Roles & API Token**. The window opens where you can create and delete users.
2. To create a new user under the USER tab, click **Add user**, add username, and password in the appropriate fields.
3. To add LDAP group, select **LDAP Group** from the options and specify Username, LDAP group DN, and LDAP search filter.
4. **Assign Role:** Select this option to assign SQL DM for MySQL role.
5. **External Roles:** Use this option to Map LDAP roles to SQL DM for MySQL roles.
6. **Add user to Admin group:** You can refer Managing multiple users for further more information.
7. **Action management:** Use this option to give different privileges like server edit, kill query, etc.
8. **T ags management:** You can give the list of allowed/disallowed tags to the user.
9. **Tab management**: An Admin user can create other users with restrictions to individual Custom Dashboards and permissions to create New Dashboards.



Managing multiple users

You can manage access to your servers and settings based on your needs using User Management. This feature is useful in creating users who will have limited access to the particular servers - which helps in preventing accidentally killing queries, executing FLUSH STATUS on your MySQL servers, or changing your server settings without your knowledge.

Admin

The SQL DM for MySQL admin user can now create other users having access to a subset of available servers only. Also, the Admin is the only allowed to create, delete server, and user registrations.

The Admin can create users with restrictions to individual Custom Dashboards and permissions to create New Dashboards.

Non-Admin

Following restrictions applies to non-admin users:

- Cannot register a new server.
- Cannot delete a registered server.
- Cannot change tags of a server.
- Can edit a server only if "Server Edit" permission is granted.
- Can kill a query from the 'Processlist' page only if 'Kill Query' permission is granted.
- Can execute 'FLUSH STATUS' from the Monitors page only if 'FLUSH STATUS' permission is granted.
- If no 'Allowed tags' are specified, normal users will have access to servers with no tags only.
- If the same tag is specified in 'Allowed tags' as well as 'Disallowed tags', then the user will not have access to servers with that tag.
- Cannot change user settings (except own password).
- Cannot change Preferences.

Permissions

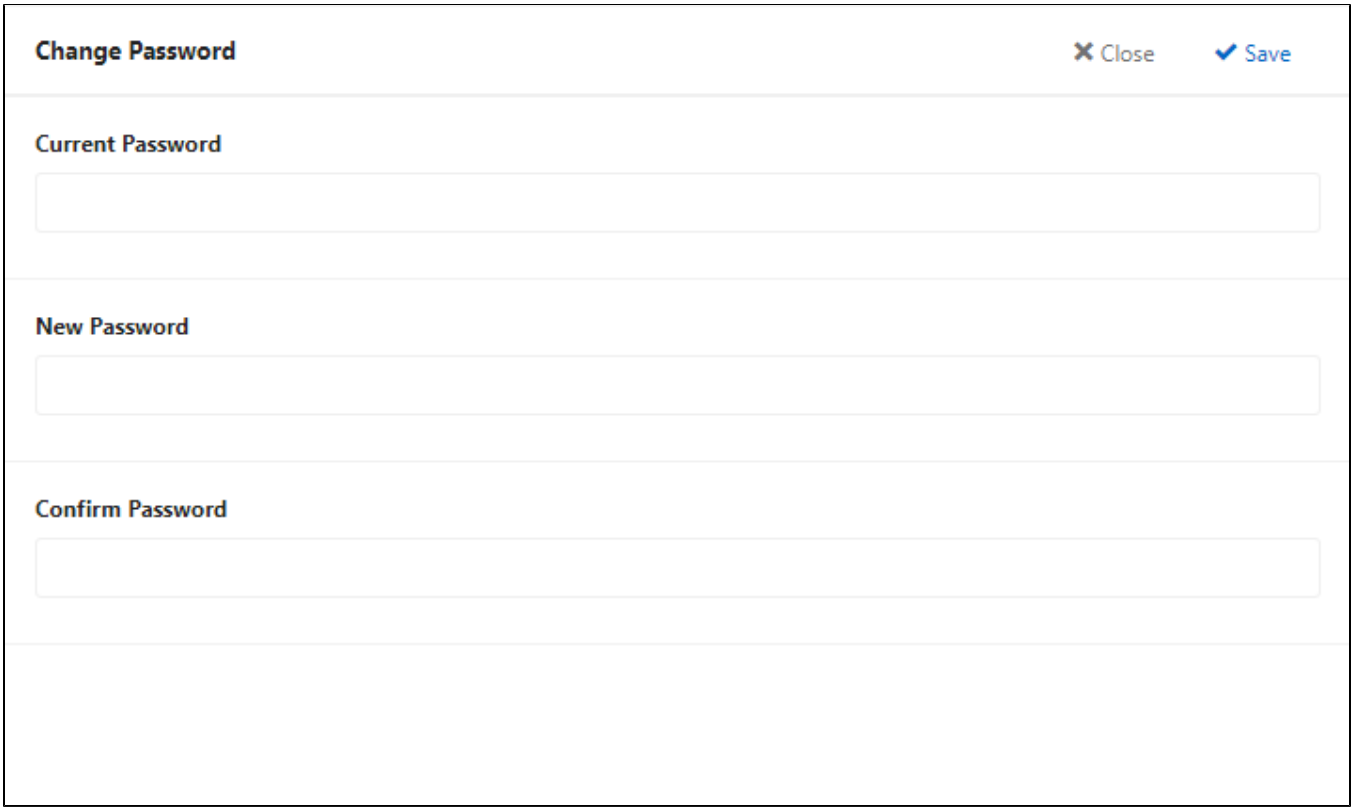
A user can be granted a combination of the following permissions:

- **Server Edit:** Allows the user to edit the settings of servers accessible to him/her.
- **Kill Query:** Allows the user to kill queries through the 'Processlist' page on servers.
- **FLUSH STATUS:** Allows the user to execute the FLUSH STATUS command on servers.
- **View Literals in Queries:** Allows the users to view literals in the Query Analyzer page.
- **Open/Close alert:** Allows the users to open/close alerts through the "Monitors" and "Events" pages.

Change Password

Users can change their password by using the Change Password option under the User Profile on the SQL DM for MySQL interface. Click the **User Profile -> Change password**.

Enter your old password in the first field. Enter your new password in the second field, and confirm the new password exactly the same way in the third field and save it.

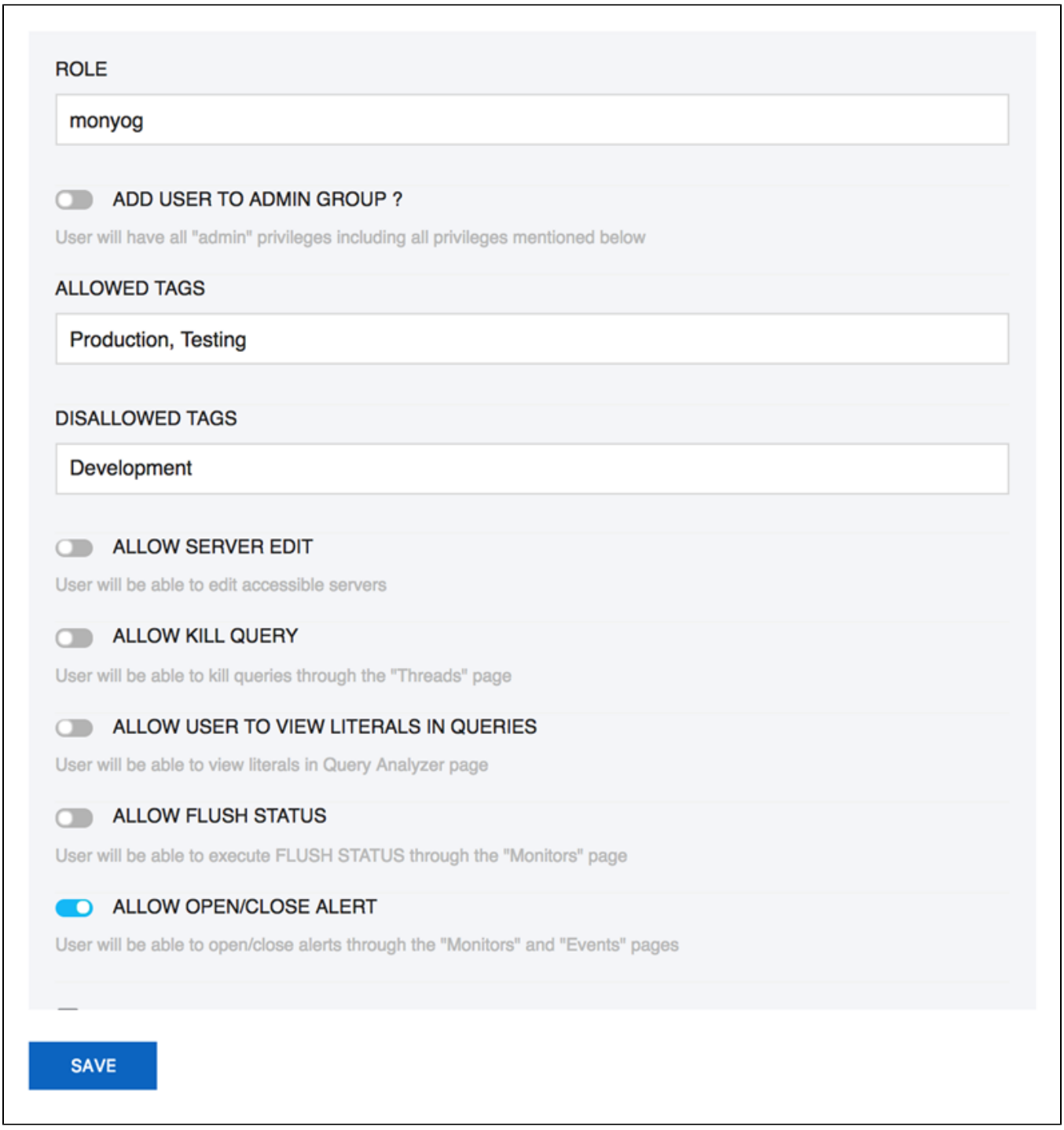


Role Manager

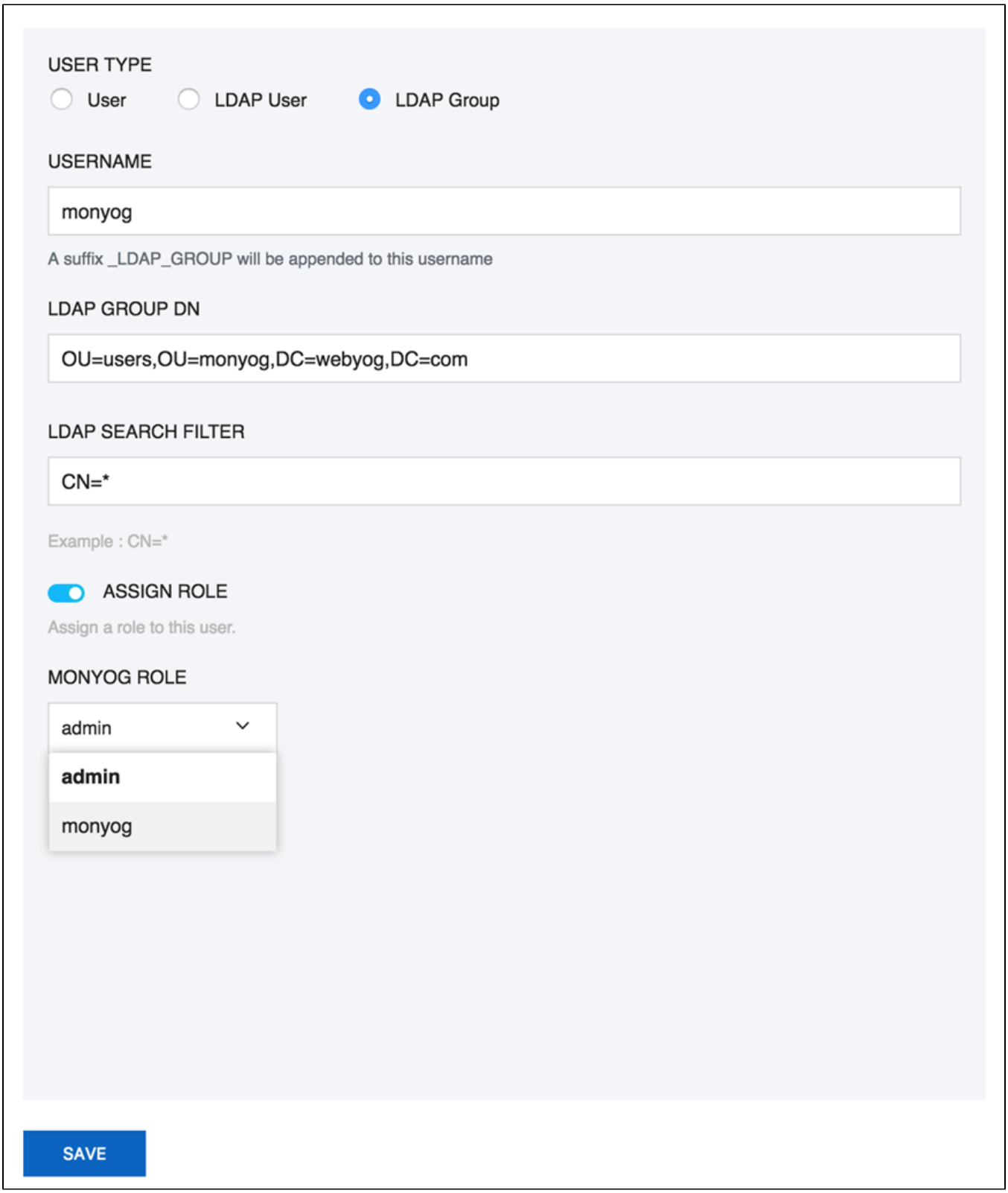
The Role Manager feature allows to create roles in SQL DM for MySQL, which can be then mapped to any users like external LDAP/AD users or the local users created in SQL DM for MySQL. The roles created can then be given different privileges like Allow server edit, Allow kill query, etc. along with the option to restrict access to selected tabs in SQL DM for MySQL.

Creating and Assigning Roles

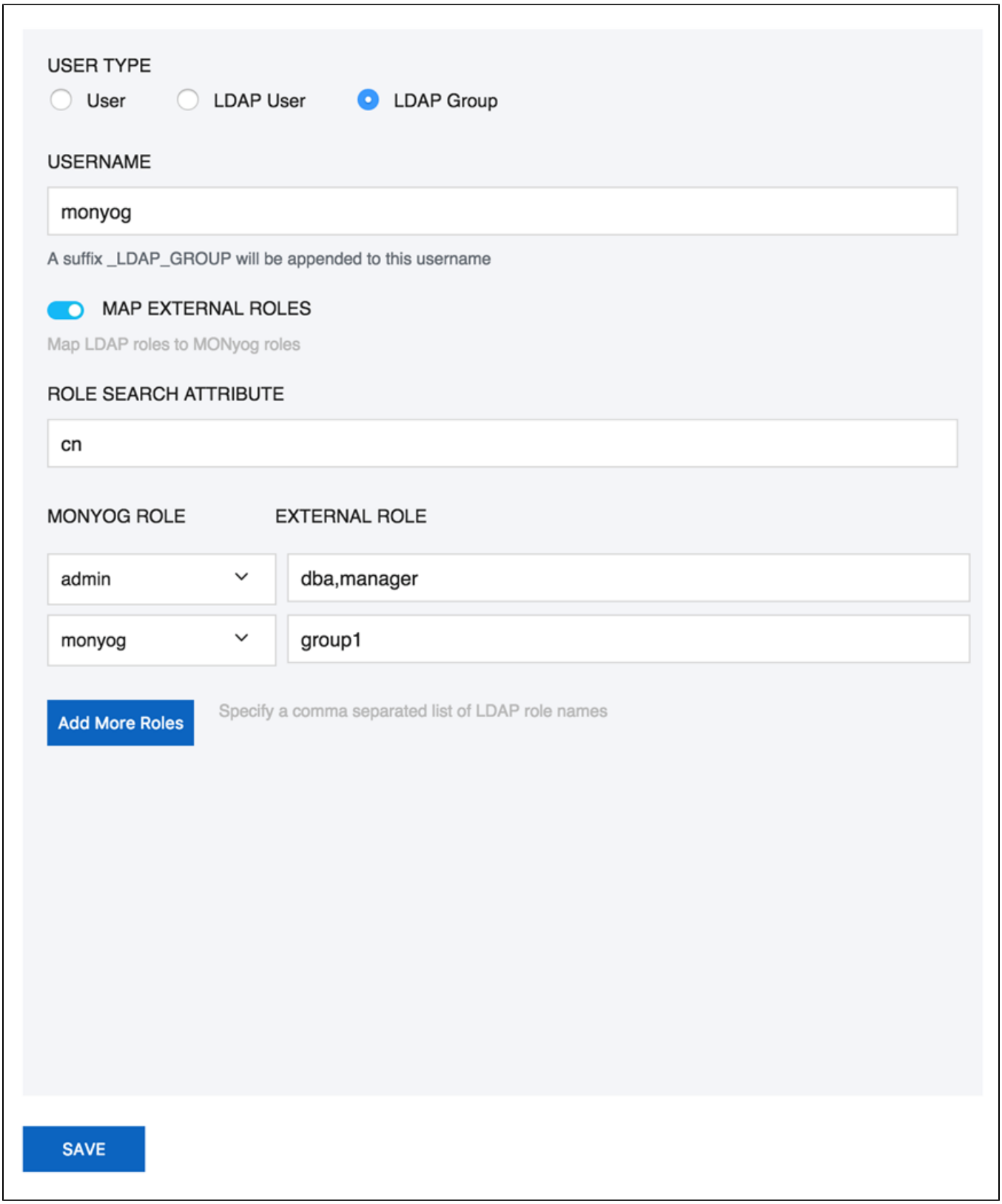
To create a Role in SQL DM for MySQL, go to **Settings**, select **LDAP, Users, Roles & API Token**, and press **Add role.**



Go to **Settings,** select **LDAP, Users, Roles & API Token** to create, edit a user, and assign the created role(s). Select the **Assign Role** option in the Create, Edit user pop up page, and select a role to assign from the drop down menu.



You can Map the LDAP group to the SQL DM for MySQL role created from the Create, Edit user pop up page, and by selecting the option **Map External Roles**. You can specify the comma separated LDAP group names and select the corresponding SQL DM for MySQL role from the drop-down menu.



API Token Manager

This gives an option to generate token in SQL DM for MySQL and use it in API as an alternative to user and password. This feature is available only for Admin users in SQL DM for MySQL. Admin can create multiple tokens for different purposes; like revoke or delete it from inside SQL DM for MySQL whenever required. This also helps to not share the password with anyone else as well as save it from getting logged in some logs. After clicking **GENERATE NEW TOKEN**, the user should give a name which is associated with the generated token. The generated token can be used in SQL DM for MySQL API in the following way:

```
curl -H "X-MONYOG-TOKEN: 1234567890abcedfghijklmnopqrstuvwxyz"
      "http://192.168.1.1:5555/?_object=MONyogAPI&_action=DataCollection
      &_value=enable&_server=Production001"
```