LDAP and Microsoft Active Directory for Chariot UI/REST Users

Chariot UI - Auth Sources

The Chariot supports two types of external Auth Sources to use when authenticating and authorizing access to Chariot via the Chariot UI.

- Microsoft Active Directory
- LDAP

These Realms use simple bind authentication to connect to the external directory to search for users and groups.

> This feature is available in Chariot v2.4.2 and newer

Microsoft Active Directory Auth Source

The Microsoft AD Source will use simple bind authentication to authenticate a user and perform searches to determine which groups the user is a member of and how they map to Chariot Roles. There are two ways in which the Auth Source can be configure to determine the name to use in the bind request.

- Bind with Login/Username
- Bind with DN

Bind with Login/Username

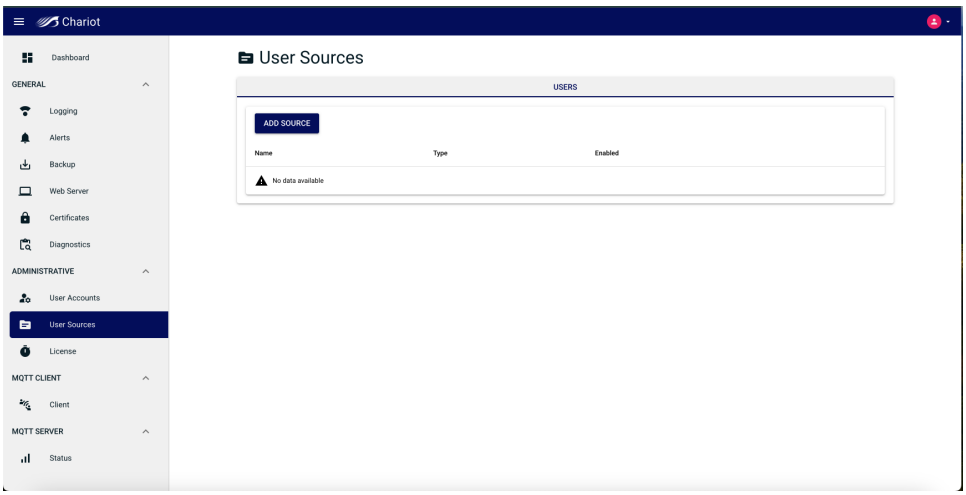
This method uses the login/username with an appended suffix and/or prefix. This is the default method and requires the administrator to configure a *Domain* that will be appended to the end of the username before the bind request. The prefix and/or suffix can also be manually configured if the *Auto Suffix* feature is disabled.

- **Example**: If Chariot is configured with the *Domain:* "example.com" and *Auto Suffix:* enabled, a login username of jdoe would use jdoe@example.com as the name for the bind request

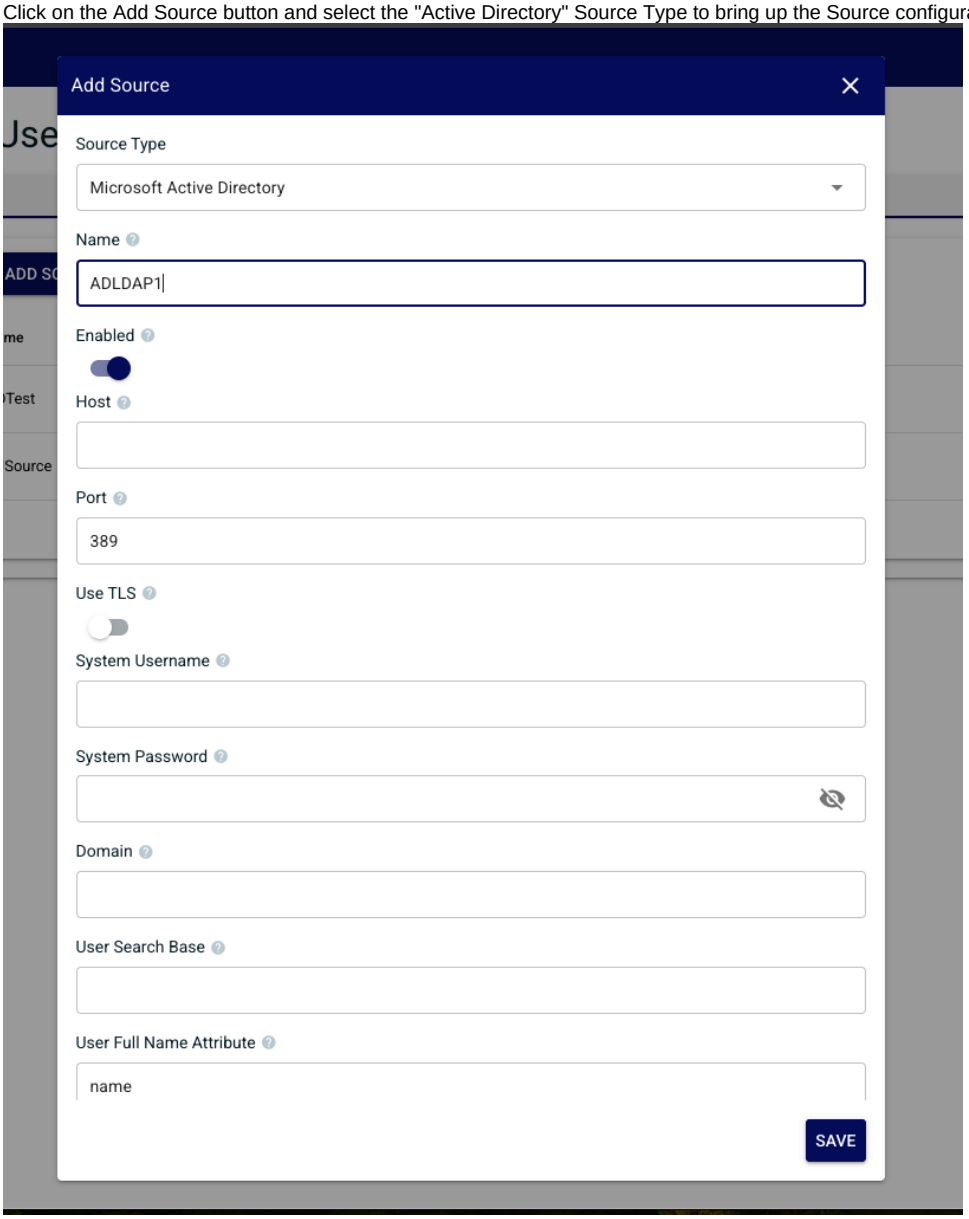
To add a Microsoft Active Directory source, complete the following steps:

1. Navigate to the following page:

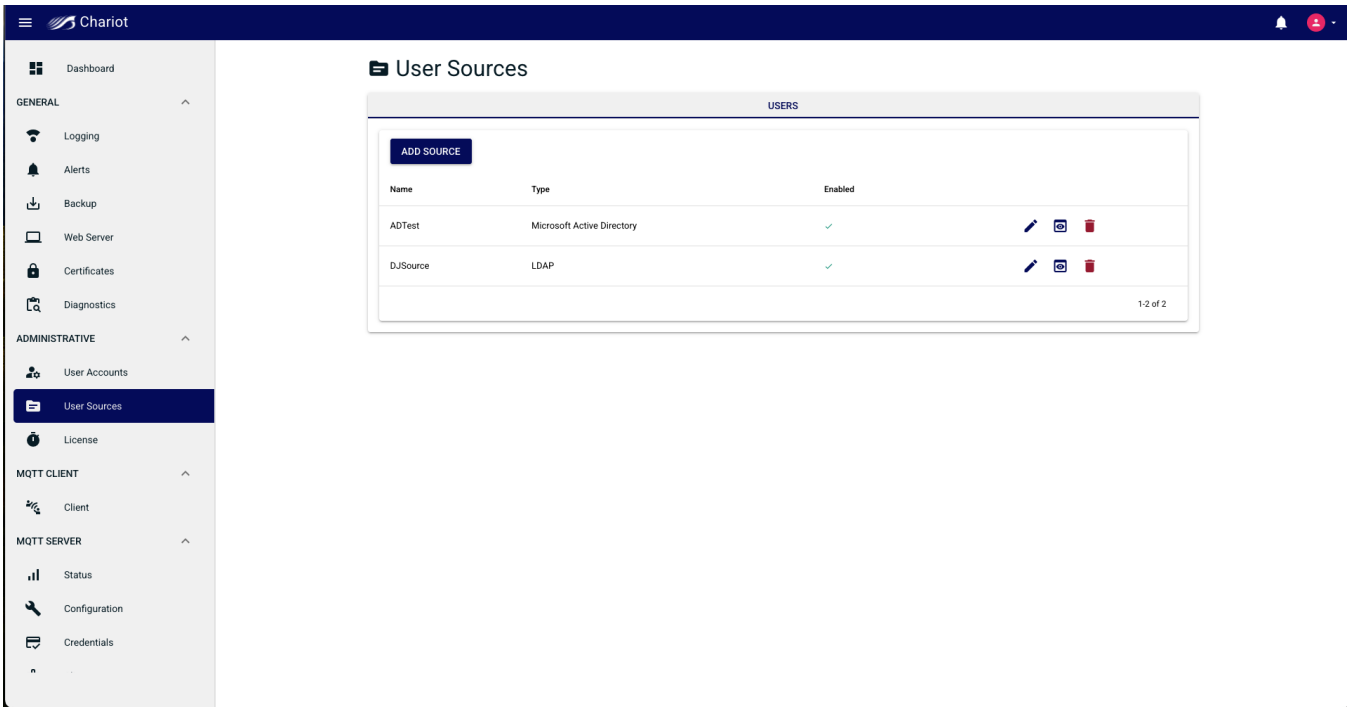
   Main Menu Administrative User Sources



2. Click on the Add Source button and select the "Active Directory" Source Type to bring up the Source configuration form.



3. Enter the Active Directory configuration (see the table below for information on the configuration fields) and click the Add button in the bottom right of the form when finished entering the configuration.



Bind with DN

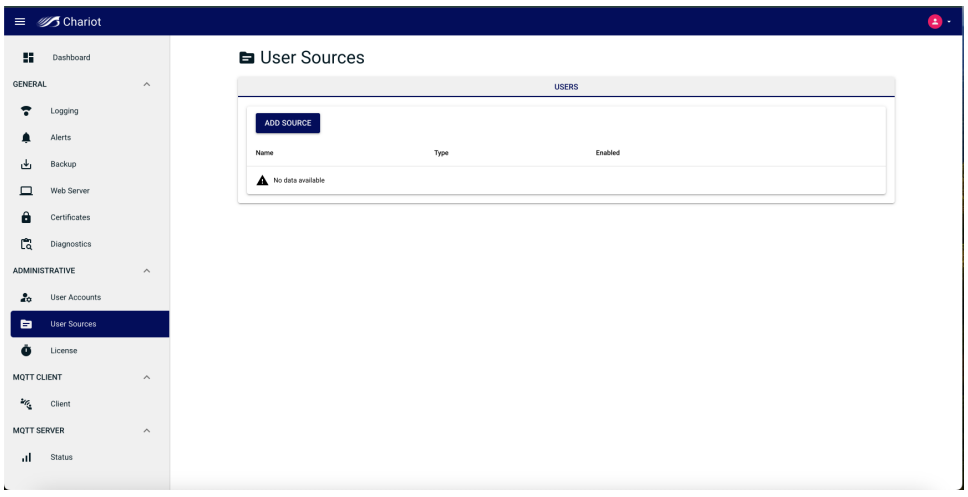
This method uses the login/username to search the AD server by matching it to the value of a specific attribute of the User entry. If a match is found, the DN of the entry is used as the name in the bind request. This method requires that the *Domain* is left empty, the *Auto Suffix* disabled, and the *Username Prefix and Suffix* fields are also empty. Chariot will use the *User Search Base* and *User Search Filter* to search for user that matches the login/username to the value of the *User Name Attribute* on an entry.

- **Example**: If Chariot is configured with the *User Search Base:* "CN=Users,DC=example,DC=com", *User Search Filter:* "(&(objectClass=user)(sAMAccountName={0}))", and *User Name Attribute: "*sAMAccountName" a user entry might be found and use CN=John Doe,CN=Users, DC=example,DC=com for the simple bind authentication

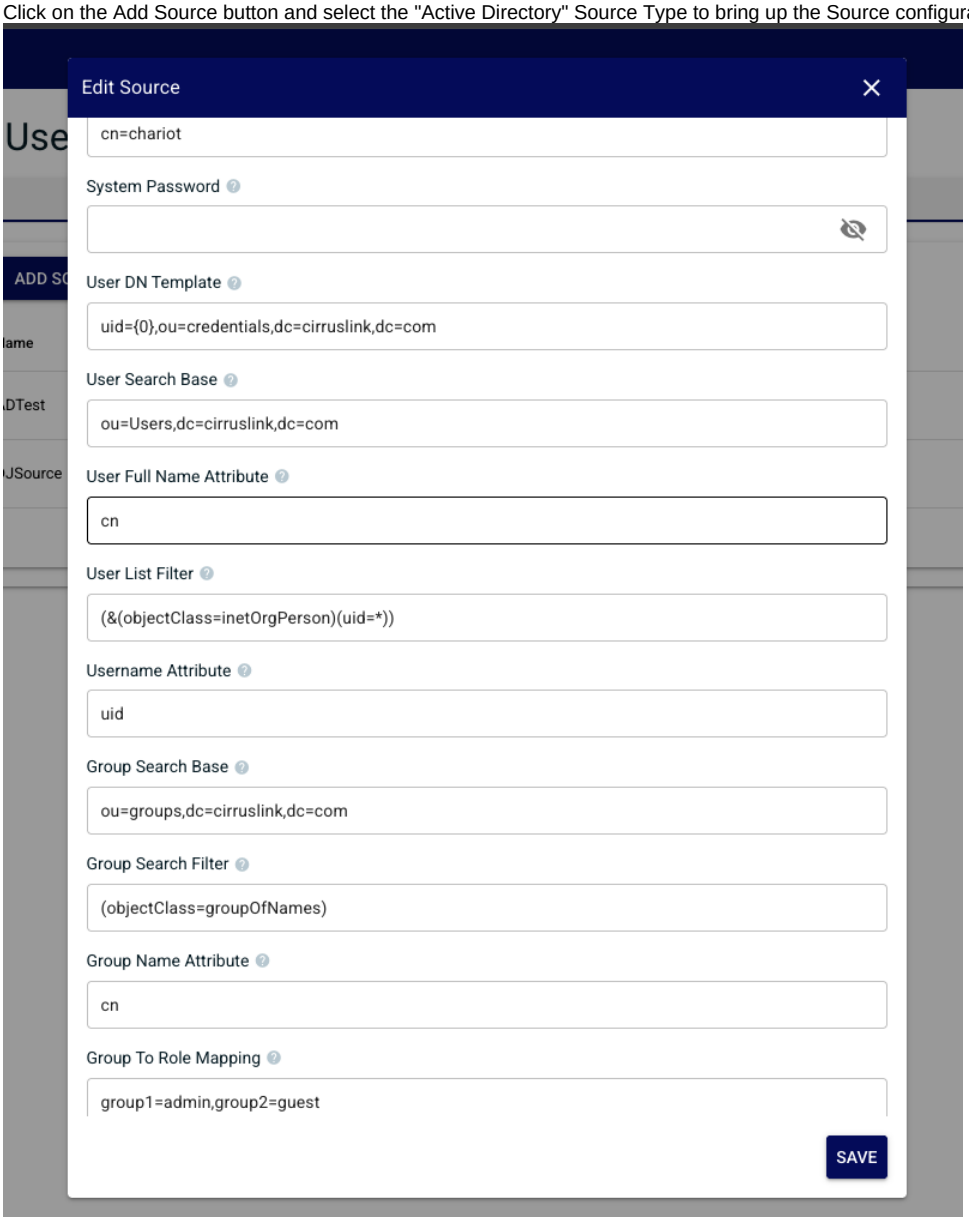
To add a Microsoft Active Directory source using this method, complete the following steps:

1. Navigate to the following page:

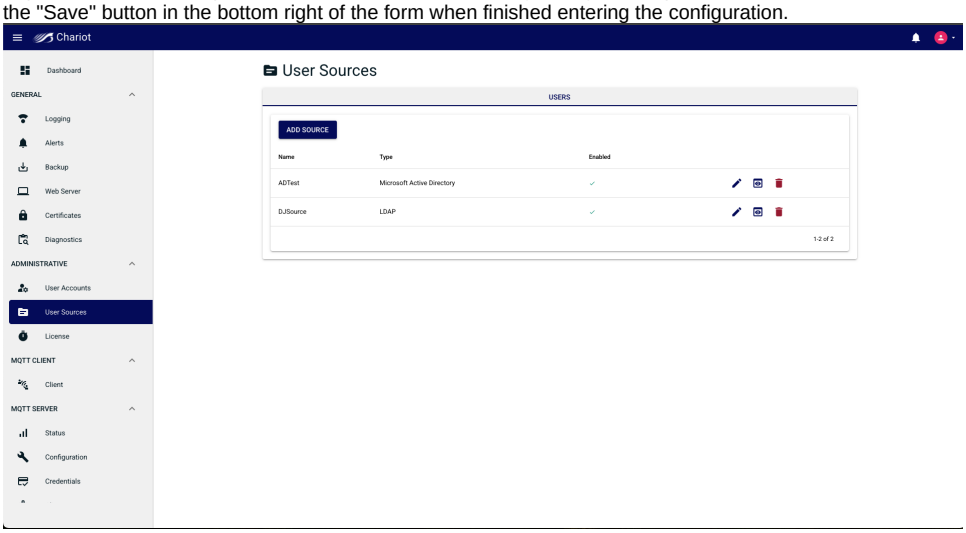
   Main Menu Administrative User Sources



2. Click on the Add Source button and select the "Active Directory" Source Type to bring up the Source configuration form.

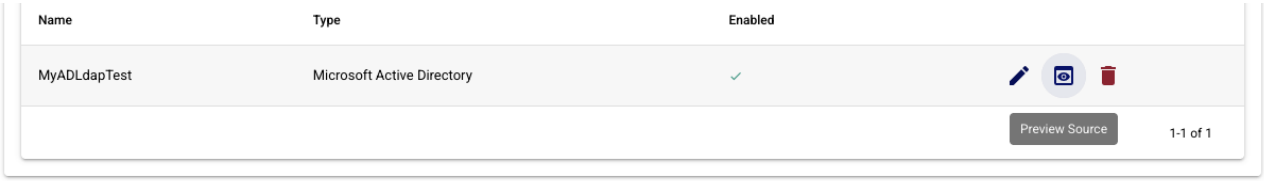


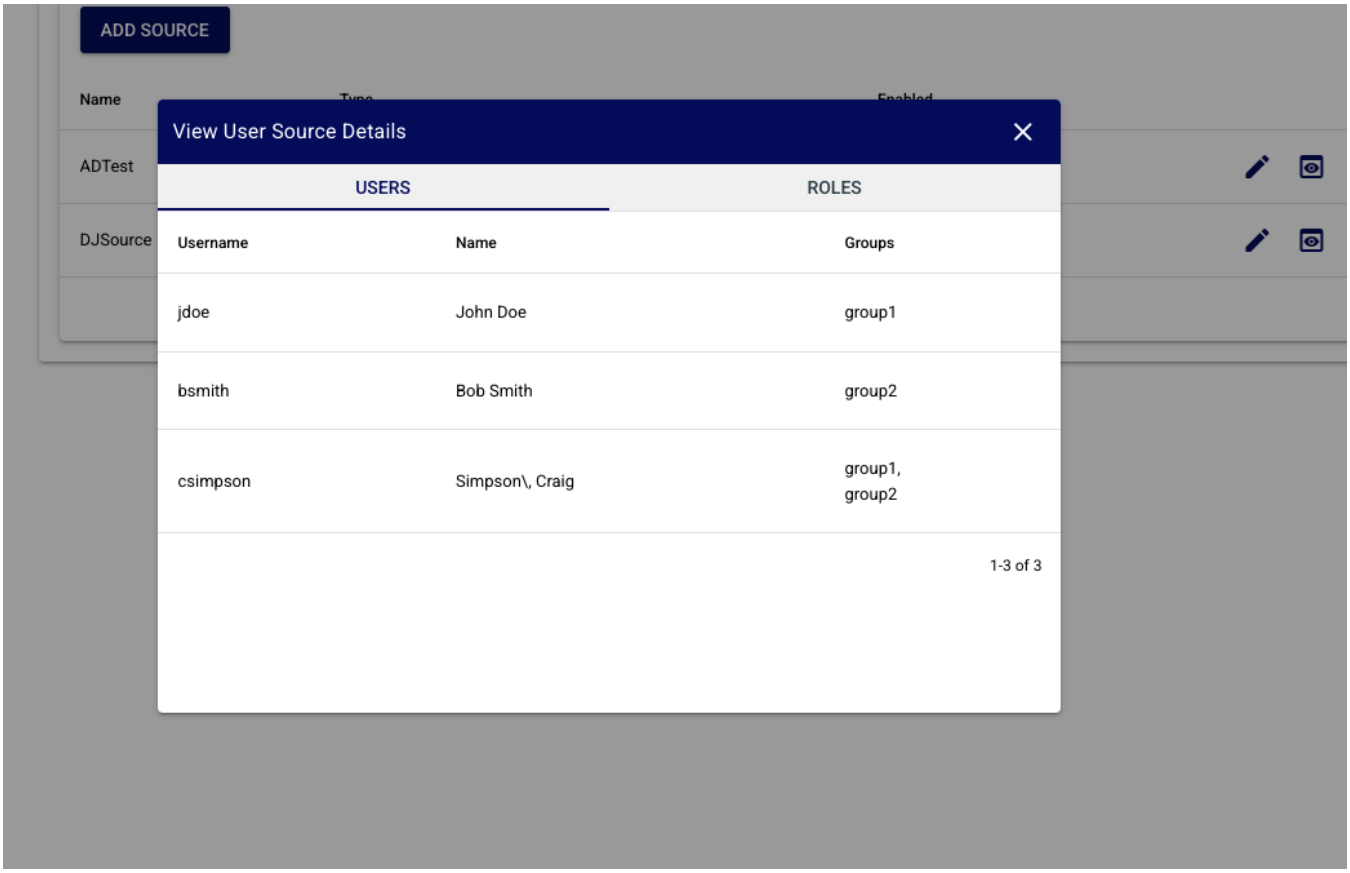
3. Expand the advanced options and enter the Active Directory configuration (see the table below for information on the configuration fields) and click the "Save" button in the bottom right of the form when finished entering the configuration.

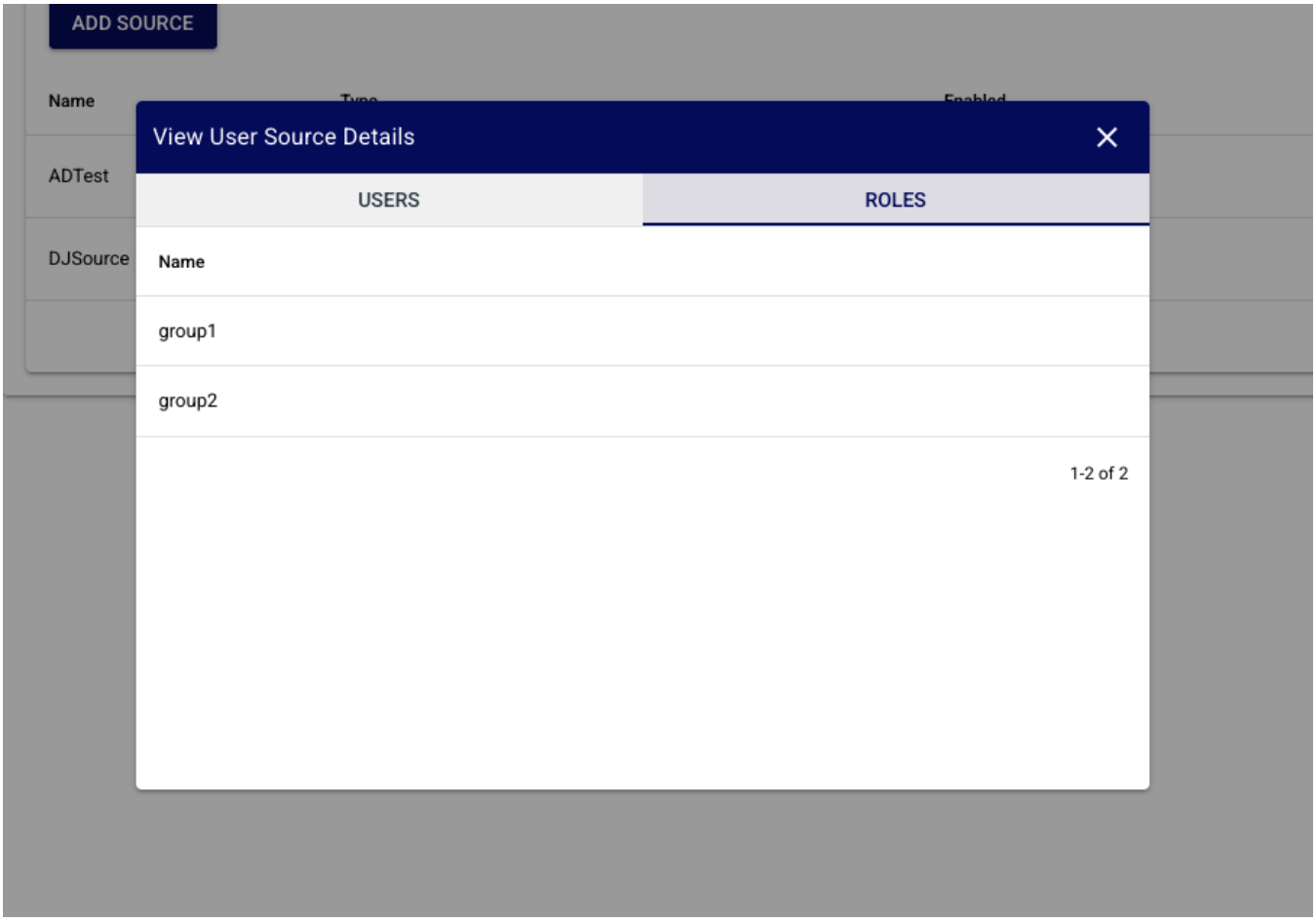


Viewing the Users and Roles

1. On the newly created Source entry click the preview button to open a modal showing the sources Users, and Roles







Configuration Fields:

As of release v2.5.0 Chariot will use the supplied login username as the name for the simple bind request with the Microsoft AD server. Additionally the **Domain, Auto Suffix, and/or Username Suffix & Prefix** properties can be configured to support bind requests with a user principal name (UPN) of another form.

Property	Required	Description	Default
Name	X	A unique name for this source configuration	
Enabled		A boolean indicating if the LDAP Realm should be enabled	true
Host	X	The IP address or hostname of the directory server	
Port	X	The port number of the directory server	389
Use TLS		Whether to use a TLS encrypted connection	false
System Username	X	The Distinguished Name (DN) used to authenticate with the directory server	
System Password	X	The password used to authenticate with the directory server	
Domain		The Windows Active Directory domain name. Example: "MyDomain.com".	
Auto Suffix		If Chariot should automatically append "@<domain>" to the username when authenticating	true
System Suffix/Prefix		If the Auto Suffix and/or Username Suffix/Prefix setting should also be applied to the System Username	true
Username Suffix		A manually specified suffix to append to the username when authenticating	
Username Prefix		A manually specified prefix to prepend to the username when authenticating	
User Search Base	X	The base Distinguished Name (DN) for searching for users in the directory server Multiple DNs can be listed by surrounding each one with parenthesis	
User Search Filter		The search filter for querying a user	(&(objectClass=user)(sAMAccountName={0}))

User List Filter		The search filter for listing users	(&(objectClass=user)(sAMAccountName=*))
User Name Attribute		The directory server attribute that represents the login username of the user	sAMAccountName
User Full Name Attributes		The directory server attribute that represents the full name of the user	name
User Group Attribute		The directory server attribute that represents the groups of a user	memberOf
Group Search Base	X	The base Distinguished Name (DN) for searching for groups in the directory server Multiple DNs can be listed by surrounding each one with parenthesis	
Group Search Filter		The search filter for querying groups in the directory server	(objectClass=group)
Group Name Attribute		The directory server attribute that represents the group name	cn
Group To Role Mapping	X	A comma separated mapping of directory server group names to Chariot role names	
Referral		How Chariot should handle referrals returned by the directory server ('ignore' or 'follow')	ignore
Connect Timeout		The maximum time in milliseconds that Chariot will attempt a connection to the directory server	10000
Read Timeout		The maximum time in milliseconds that Chariot will attempt a read with the directory server	5000
Enable Cache		Whether results from the directory serve should be cached locally	true
Cache Timeout		The period of time cached results will be held before needing to be updated	10000

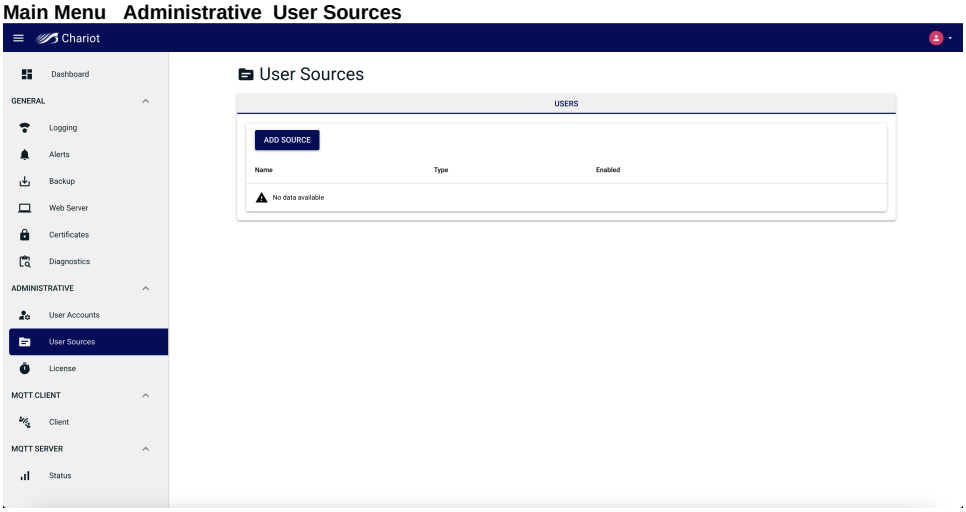
LDAP Auth Source

A user that is logging in to the Chariot UI will have their username mapped to the distinguished name (DN) of an LDAP entry using a configure template (see below). Chariot will use simple bind authentication to authenticate the user and will search for group membership to determine the corresponding Chariot Role membership using the configured mapping.

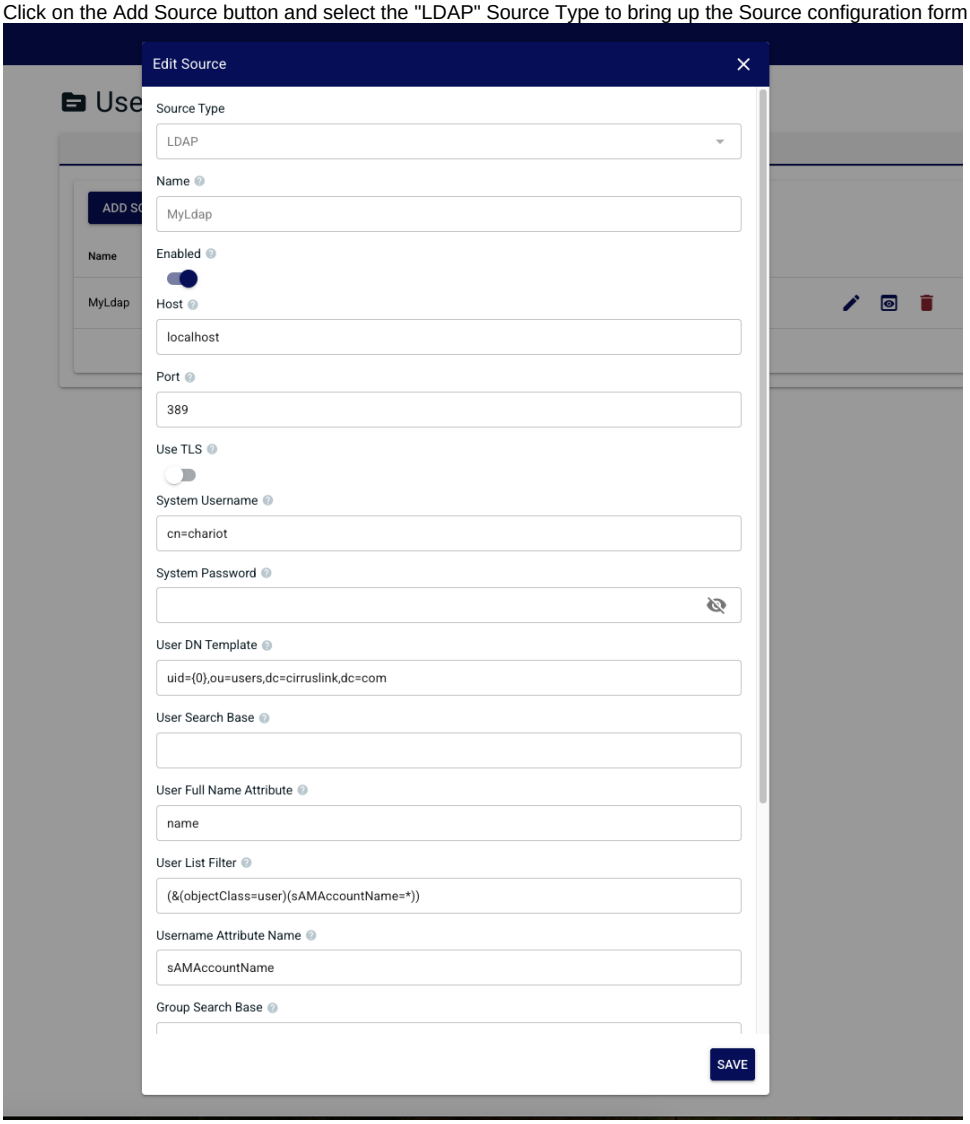
To add a generic LDAP directory server source, complete the following steps:

1. Navigate to the following page:

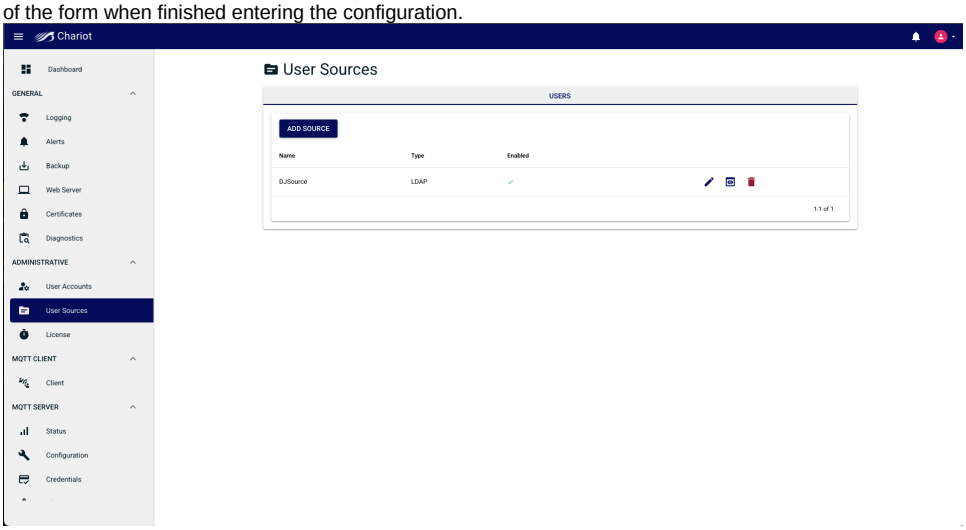
Main Menu Administrative User Sources



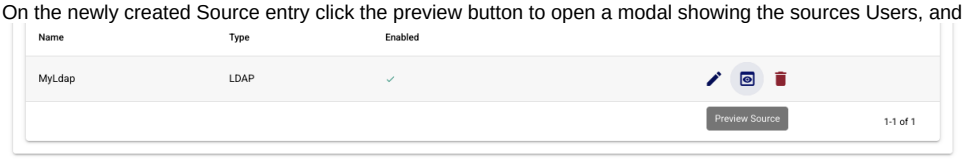
2. Click on the Add Source button and select the "LDAP" Source Type to bring up the Source configuration form

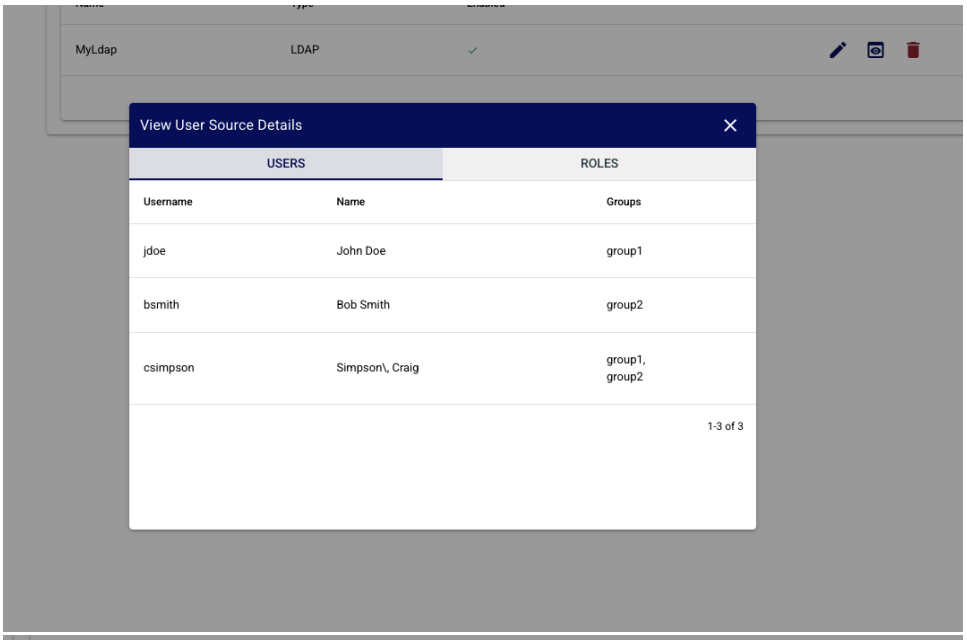


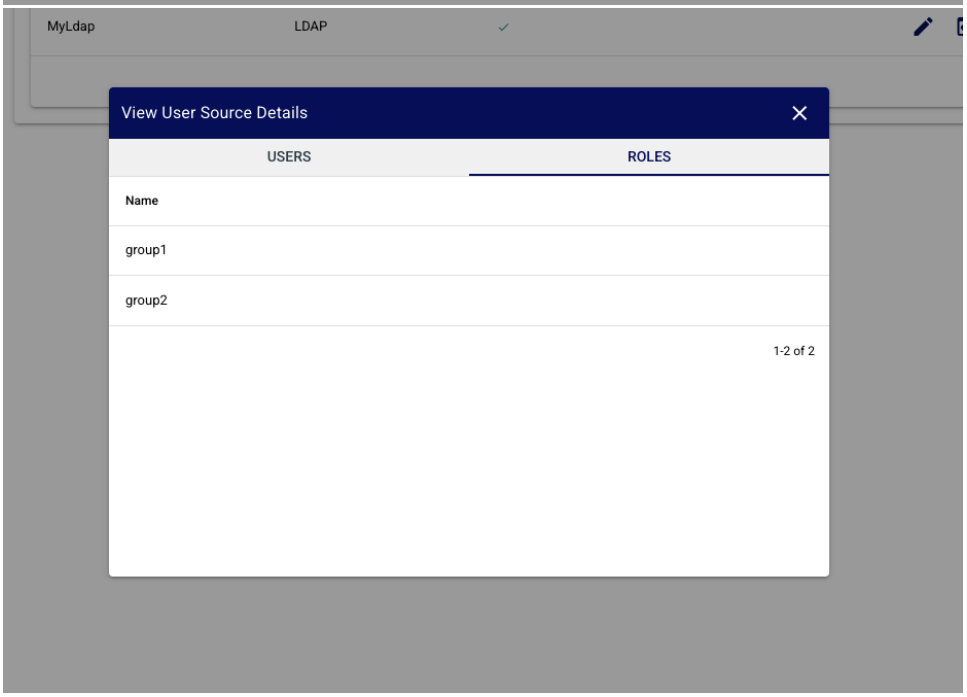
3. Enter the LDAP directory configuration (see the table below for information on the configuration fields and click the Add button in the bottom right of the form when finished entering the configuration.



4. On the newly created Source entry click the preview button to open a modal showing the sources Users, and Roles







Configuration Fields:

Property	Required	Description	Default
Name	X	A unique name for this source configuration	
Enabled		A boolean indicating if the LDAP Realm should be enabled	true
Host	X	The IP address or hostname of the directory server	
Port	X	The port number of the directory server	389
Use TLS		Whether to use a TLS encrypted connection	false
System Username	X	The Distinguished Name (DN) used to authenticate with the directory server	
System Password	X	The password used to authenticate with the directory server	
User Search Base	X	The base Distinguished Name (DN) for searching for users in the directory server Multiple DNs can be listed by surrounding each one with parenthesis.	ou=users,dc=example,dc=com
User DN Template	X	The template for building the user's Distinguished Name (DN)	uid={0},ou=users,dc=example,dc=com

User List Filter		The search filter for listing users	(&(objectClass=inetOrgPerson)(uid=*))
User Name Attribute		The directory server attribute that represents the short name of the user	uid
User Full Name Attributes		The directory server attribute that represents the full name of the user	cn
Group Search Base	X	The base Distinguished Name (DN) for searching for groups in the directory server Multiple DNs can be listed by surrounding each one with parenthesis.	ou=groups,dc=example,dc=com
Group Search Filter		The search filter for querying groups in the directory server	(objectClass=groupOfNames)
Group Name Attribute		The directory server attribute that represents the group name	cn
Group To Role Mapping	X	A comma separated mapping of directory server group names to Chariot role names	
Referral		How Chariot should handle referrals returned by the directory server ('ignore' or 'follow')	ignore
Connect Timeout		The maximum time in milliseconds that Chariot will attempt a connection to the directory server	10000
Read Timeout		The maximum time in milliseconds that Chariot will attempt a read with the directory server	5000
Enable Cache		Whether results from the directory serve should be cached locally	true
Cache Timeout		The period of time cached results will be held before needing to be updated	10000