# LDAP for Chariot UI/REST Users

## Chariot UI - LDAP Users and Groups/Roles

The Chariot Security Service can be configured to add an LDAP Realm to use when authenticating and authorizing access via the Chariot UI. Each LDAP Realm uses a simple bind authentication to connect to the LDAP server to search for users and groups. 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.

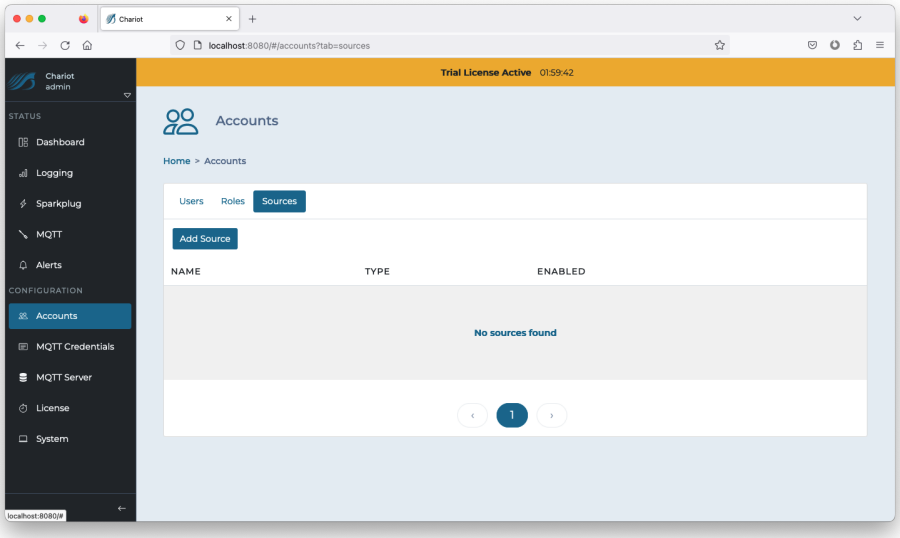
> This feature is available in Chariot v2.4.2 and newer

## Adding a Microsoft Active Directory source

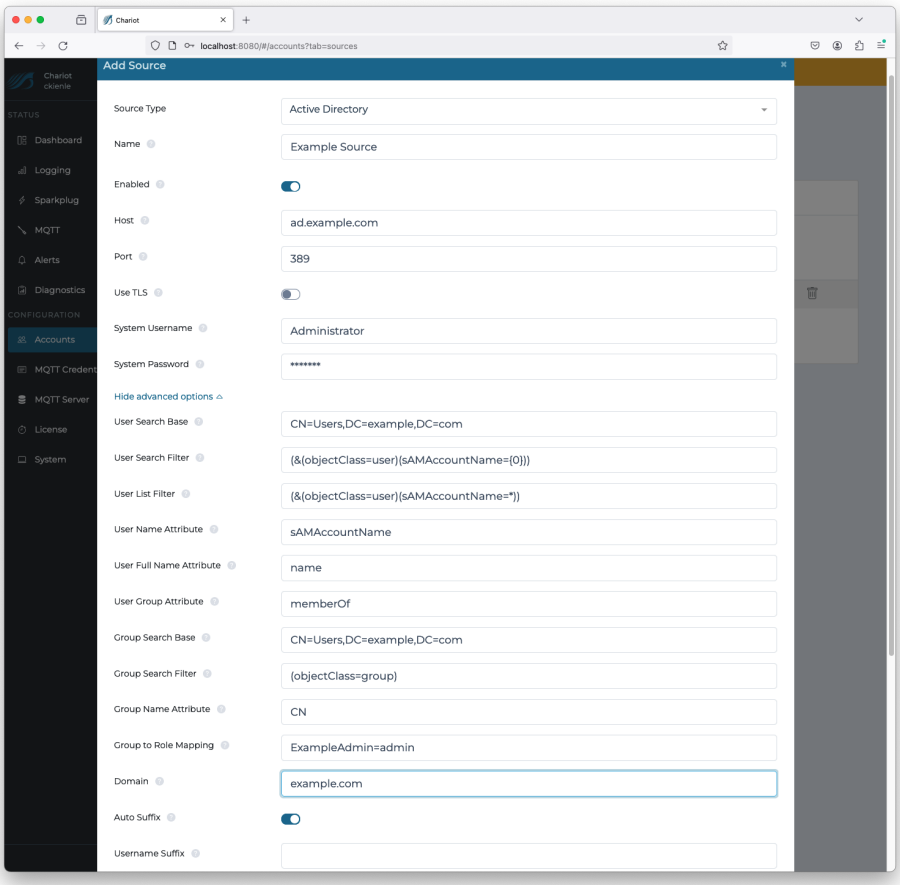
To add a Microsoft Active Directory source, complete the following steps:

1. Navigate to the following page:

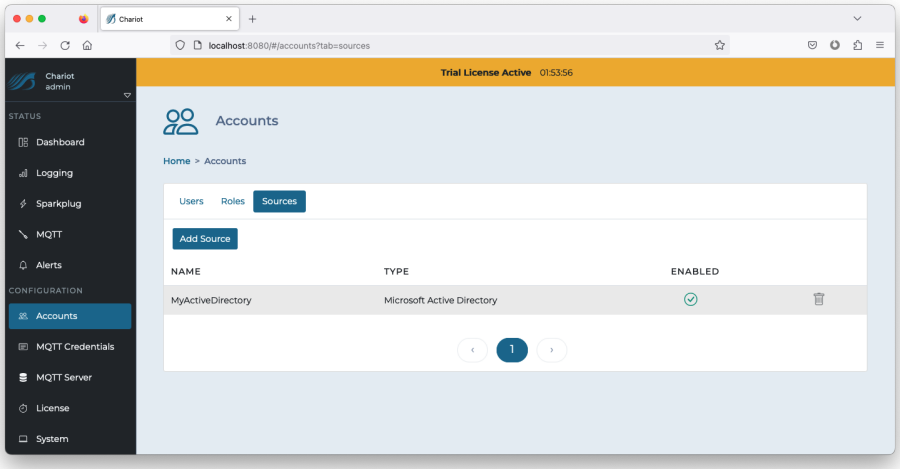
   **CONFIGURATION Accounts Sources**



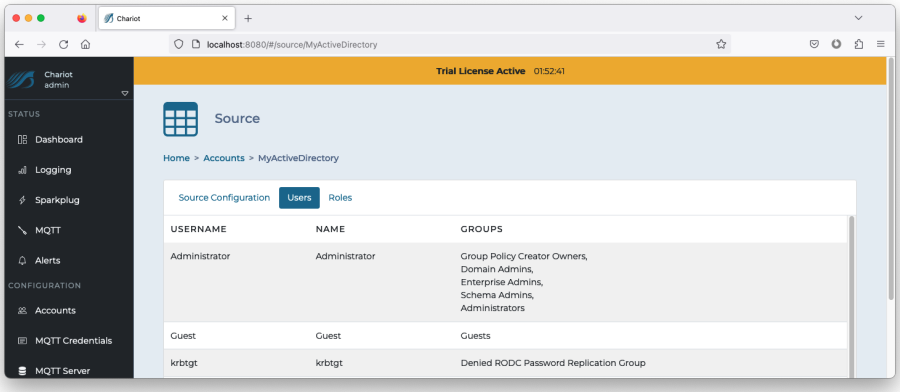
2. Click on the Add Source button and select the "Active Directory" Source Type to bring up the Source configuration form.

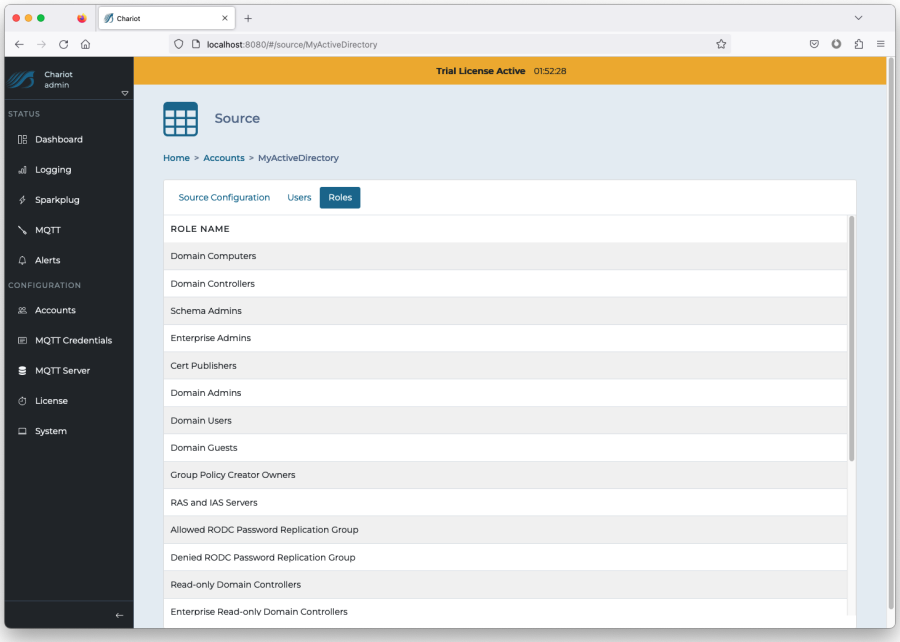



3. Enter the Active Directory configuration (see the table below for information on the configuration fields and click the Add button in the bottom right of the form when finished entering the configuration.



4. Click on the newly created Source entry to inspect the Configuration, 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 | |
| User Search Base | X | The base Distinguished Name (DN) for searching for users in the directory server | |
| 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=*)) |

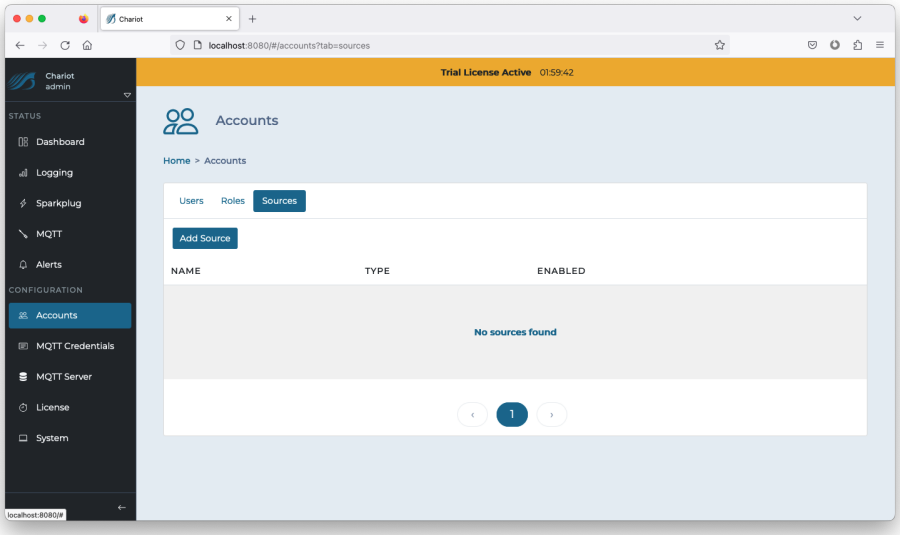
| | | | |
|---|---|---|---|
| User Name Attribute | | The directory server attribute that represents the short name of the user | sAMAccountName |
| User Full Name Attributes | | The directory server attribute that represents the full name of the user | name |
| User Group Attribute | | The directory 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 | |
| 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 | |
| Domain | | The Windows Active Directory domain name. Example: "MyDomain.com". | |
| Auto Suffix | | If Chariot should automatically append "@<domain>" to the username when authenticating | 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 | |
| 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 |

## Adding an LDAP directory server source

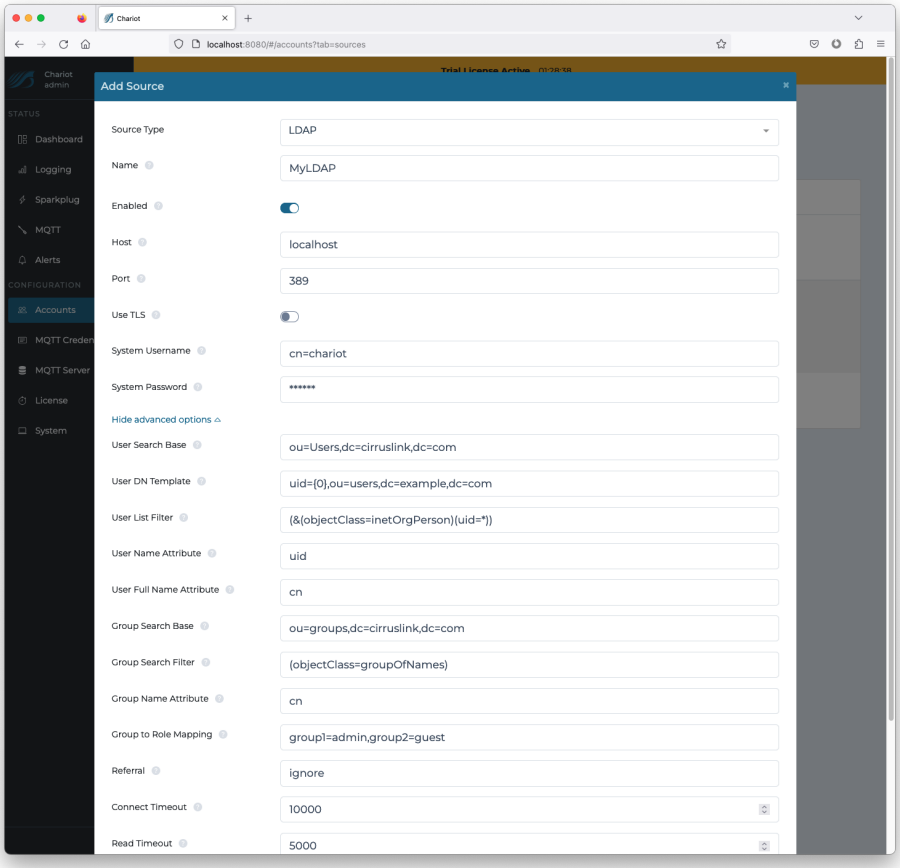
To add a generic LDAP directory server source, complete the following steps:

1. Navigate to the following page:

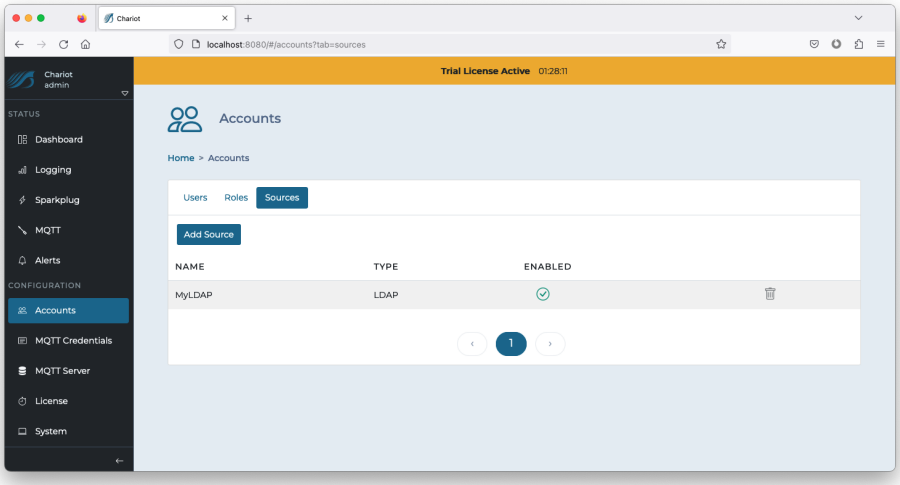
   **CONFIGURATION Accounts Sources**



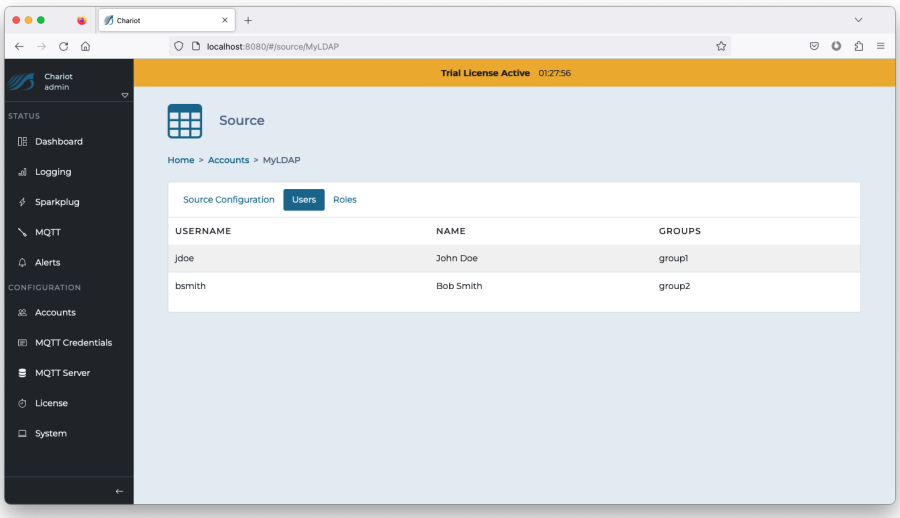
2. Click on the Add Source button and select the "LDAP" Source Type to bring up the Source configuration form

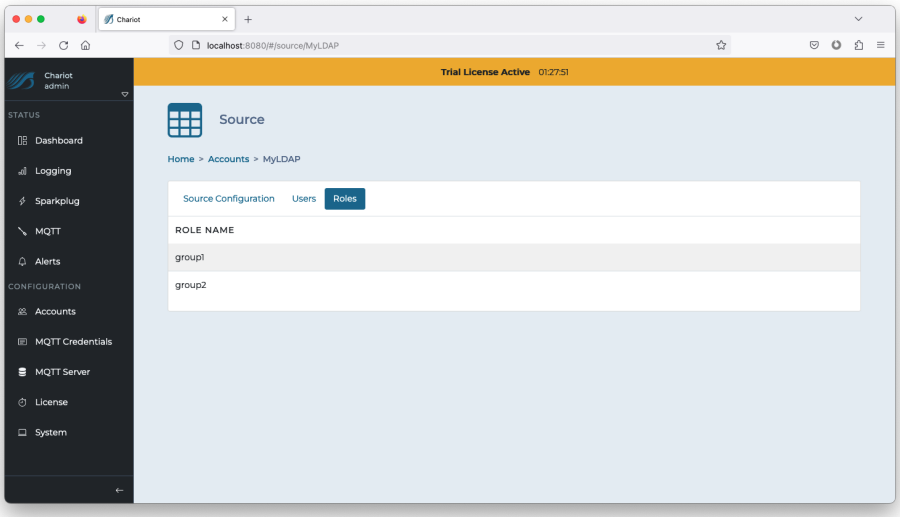



3. Enter the LDAP directory configuration (see the table below for information on the configuration fields and click the Add button in the bottom right of the form when finished entering the configuration.



4. Click on the newly created Source entry to inspect the Configuration, 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 | 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 | 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 |