Configure LDAP authentication on the NetScaler appliance for management purposes

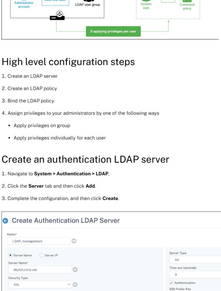
October 13, 2023 · Contributed by:

You can configure user logon to the NetScaler appliance using the active directory credentials (user name and password) for management purposes (superuser, read-only, network privileges and all others).

Prerequisites

- Windows Active Directory domain controller servers
- A dedicated domain group for NetScaler administrators
- NetScaler Gateway 10.1 and later versions

The following figures illustrate the LDAP authentication on the NetScaler appliance.

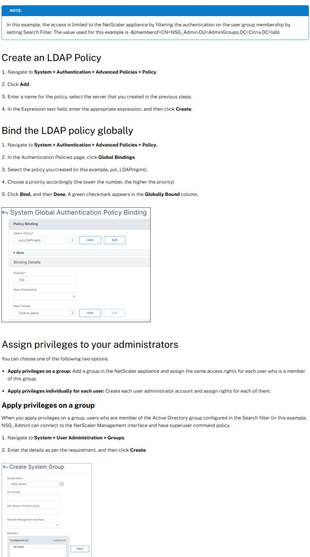


High level configuration steps

1. Create an LDAP server
2. Create an LDAP policy
3. Bind the LDAP policy
4. Assign privileges to your administrators by one of the following ways
   - Apply privileges on group
   - Apply privileges individually for each user

Create an authentication LDAP server

1. Navigate to **System > Authentication > LDAP**.
2. Click the **Server** tab and then click **Add**.
3. Complete the configuration, and then click **Create**.



NOTE:

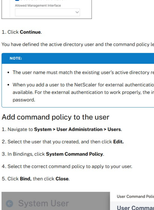
In this example, the access is limited to the NetScaler appliance by filtering the authentication on the user group membership by setting Search Filter. The value used for this example is -&memberof=CN=NSG_Admin,OU=Admin Groups,DC=Citrix,DC=lab)

Create an LDAP Policy

1. Navigate to **System > Authentication > Advanced Policies > Policy**.
2. Click **Add**.
3. Enter a name for the policy, select the server that you created in the previous steps.
4. In the Expression text field, enter the appropriate expression, and then click **Create**.

Bind the LDAP policy globally

1. Navigate to **System > Authentication > Advanced Policies > Policy**.
2. In the Authentication Policies page, click **Global Bindings**.
3. Select the policy you created (in this example, pol_LDAPmgmt).
4. Choose a priority accordingly (the lower the number, the higher the priority)
5. Click **Bind,** and then **Done**. A green checkmark appears in the **Globally Bound** column.



Assign privileges to your administrators

You can choose one of the following two options.

- **Apply privileges on a group**: Add a group in the NetScaler appliance and assign the same access rights for each user who is a member of this group.
- **Apply privileges individually for each user**: Create each user administrator account and assign rights for each of them.

Apply privileges on a group

When you apply privileges on a group, users who are member of the Active Directory group configured in the Search filter (in this example, NSG_Admin) can connect to the NetScaler Management interface and have superuser command policy.

1. Navigate to **System > User Administration > Groups**.
2. Enter the details as per the requirement, and then click **Create**.

You have defined the active directory group that the users belong to and also the command policy level that must be associated to the account when logging in. You can add new administrator users to the LDAP group you configured on the search filter.

NOTE:

The group name must match the active directory record.

Apply privileges individually for each user

In this scenario, users who are member of your Active Directory group configured in the search filter (in this example, NSG_Admin) can connect to the NetScaler management interface but do not have any privileges until you create the specific user on the NetScaler appliance and bind the command policy to it.

1. Navigate to **System > User Administration > Users**.
2. Click **Add**.
3. Enter the details as per the requirement.

   Note: Make sure to select **Enable External Authentication**.

1. Click **Continue**.

You have defined the active directory user and the command policy level that must be associated to the account when logging in.

NOTE:

- The user name must match the existing user's active directory record.
- When you add a user to the NetScaler for external authentication, you must provide a password, if the external authentication is not available. For the external authentication to work properly, the internal password must not be the same as the user account LDAP password.

Add command policy to the user

1. Navigate to **System > User Administration > Users**.
2. Select the user that you created, and then click **Edit.**
3. In Bindings, click **System Command Policy**.
4. Select the correct command policy to apply to your user.
5. Click **Bind,** then click **Close**.

To add more administrators;

- Add the administrator users to the LDAP group you configured on the search filter.
- Create the system user in NetScaler and assign the correct command policy.

To configure LDAP authentication on the NetScaler appliance for management purposes by using the CLI

Use the following commands as a reference to configure log on for a group with superuser privileges on the NetScaler appliance CLI.

1. Create an LDAP server

```
add authentication ldapAction LDAP_mgmt -serverIP myAD.citrix.lab -serverPort 636 -ldapBase "DC=citrix,DC=lab"
```

2. Create and LDAP policy

```
add authentication ldapPolicy pol_LDAPmgmt ns_true LDAP_mgmt
```

3. Binding the LDAP policy

```
bind system global pol_LDAPmgmt -priority 110
```

4. Assign privileges to your administrators
   - To apply privileges on the group

```
add system group NSG_Admin
bind system group NSG_Admin -policyName superuser 100
```

   - To apply privileges individually for each user

```
add system user adminx
bind system user adminx superuser 100
```