



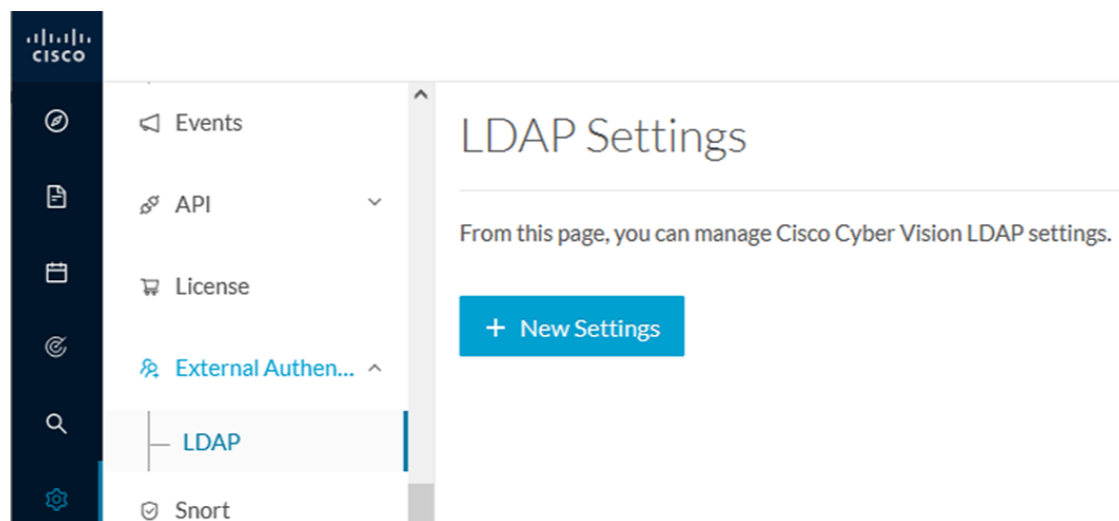
External Authentication

- [LDAP, on page 1](#)

LDAP

Cisco Cyber Vision can delegate user authentication to external services using LDAP (Lightweight Directory Access Protocol), and in particular to Microsoft Active Directory services.

You can enable LDAP authentication in the LDAP Settings administration page.



Configuring LDAP:

LDAP integration can be done through normal connection or securely by using certificates depending on the installation compatibility.

Mapping Cisco Cyber Vision roles with Microsoft Active Directory groups:

User groups available in the external directory can be mapped to Cisco Cyber Vision Product, Operator and Auditor user roles or custom roles. Refer to [Role Management](#) to create custom roles.

Because the Admin user role is exclusively reserved for Cisco Cyber Vision internal usage, it cannot be mapped to any external users and thus is not proposed in LDAP settings.

Testing LDAP connection:

After setting up LDAP, the connection between the Cisco Cyber Vision Center and the external directory is to be tested. On the LDAP test connection window, you will use a user login and a password set in the external directory. The Center will attempt to authenticate on the directory server with these credentials. In return, you will get either a successful authentication, or a failed one with an error message.

Login in Cisco Cyber Vision:

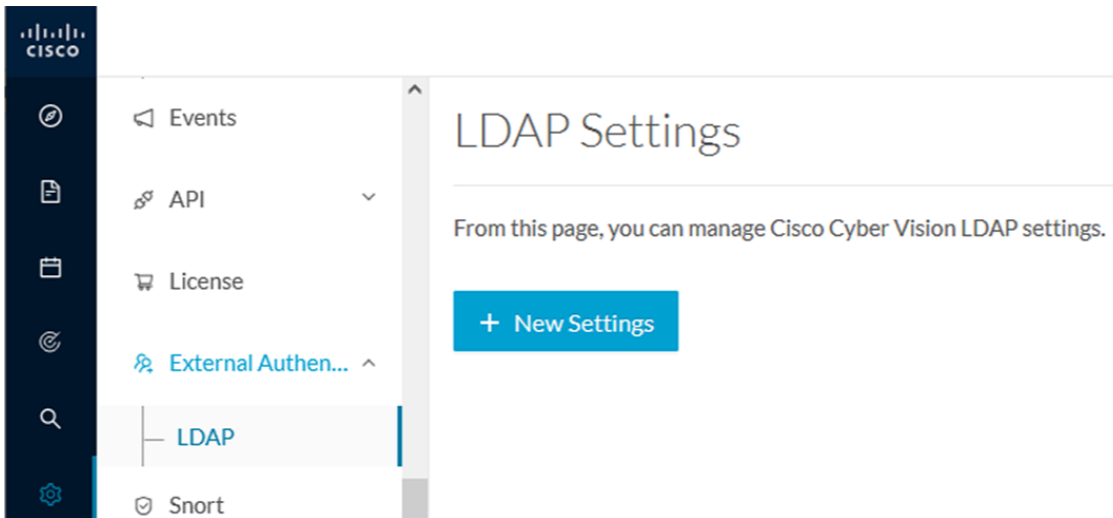
When logging into Cisco Cyber Vision, the login format used will determine the base (i.e. internal or external) to be queried:

- If you use an email, the Cisco Cyber Vision database is queried.
- If you use the Active Directory format <domain_name>\<user_name> (e.g. cisco\john_doe), then the external directory is used to authenticate users.

Configure LDAP

This section explains how to configure LDAP in Cisco Cyber Vision using a normal connection or a secure connection.

Step 1 In Cisco Cyber Vision, navigate to Admin > External Authentication > LDAP.



Step 2 Click New Settings.

The New LDAP Settings window pops up.

NEW LDAP SETTINGS

Settings Role Mapping

LDAP over TLS/SSL Use self signed certificate

* Primary Server Address * Primary Server Port

Secondary Server Address Secondary Server Port

* Base DN ⓘ

* Server Response Time ⓘ

OK Cancel

What to do next

Configure LDAP using a [LDAP normal connection](#) or a [LDAP secure connection](#).

LDAP normal connection

After clicking the New Settings button, the following New LDAP Settings window pops up.

Before you begin

Step 1 Fill in the LDAP settings.

NEW LDAP SETTINGS X

Settings

Role Mapping

LDAP over TLS/SSL Use self signed certificate

* Primary Server Address * Primary Server Port

`dc01.2019lab.local`

`389`

Secondary Server Address Secondary Server Port

`dc01.2019lab.local`

`389`

* Base DN ⓘ

`DC=2019lab,DC=local`

* Server Response Time ⓘ

`10`

OK

Cancel

Step 2 Click the Role Mapping tab.

Step 3 Fill in the following fields:

a) Map one or more Cisco Cyber Vision default roles with an Active Directory group.

Note At least one default role must be mapped.

Note Because the Admin user role is exclusively reserved for Cisco Cyber Vision internal usage, it cannot be mapped to any external users and thus is not proposed in LDAP settings.

b) Map Cisco Cyber Vision custom roles with Active Directory groups.

You must type the exact group names as configured into the remote directory so they can be retrieved and mapped to user roles.

NEW LDAP SETTINGS X

Settings ⓘ Role Mapping

Default roles ⓘ

Product	▼	Domain Users
Operator	▼	
Auditor	▼	

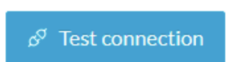
Custom roles ⓘ +

TestAD2019	▼	TestAD2019	⊗
------------	---	------------	----------------

OK Cancel

Step 4 Click OK.

Step 5 Click the Test connection button.



The Test Connection window pops up.

Step 6 Enter a user credentials to test the connection between Cisco Cyber Vision and Active Directory.

Note The Username format is domain\user.

A message Successful LDPA bind should appear.

Step 7 Click OK.

Step 8 Test the connection by logging out of Cisco Cyber Vision and logging in with the mapped user credentials.

Menus are displayed according to the rights granted to the user.

What to do next

LDAP secure connection

After clicking the New Settings button, the following New LDAP Settings window pops up.

Before you begin

Step 1 Fill in the following fields:

NEW LDAP SETTINGS X

Settings

Role Mapping

LDAP over TLS/SSL Use self signed certificate

*** Primary Server Address** *** Primary Server Port**

dc01.2019lab.local

636

Secondary Server Address Secondary Server Port

dc02.2019lab.local

636

*** Base DN** ⓘ

DC=2019lab,DC=local

*** Server Response Time** ⓘ

10

*** CA Trust Chain**

↑

Choose a file or drag and drop to upload

Accepted files: .pem

OK

Cancel

- a) Tick LDAP over TLS/SLL.
- b) Fill in the LDAP settings.
- c) Upload a .pem root certificate or a chain certificate, or tick Use a self-signed certificate.

If you upload a certificate, a message indicating that the certificate has been uploaded successfully appears.

A screenshot of a success message dialog box. The dialog box has a white background and a thin border. At the top left, there is a green checkmark icon. To its right, the text reads "2019lab-DC02-CA-1.pem certificate uploaded successfully." Below this text, there is a blue link "NEW LDAP SETTINGS" and a close button "X" in the top right corner.

The certificate appears at the bottom of the New LDAP Settings window.

External Authentication

7

NEW LDAP SETTINGS X

Settings
Role Mapping

LDAP over TLS/SSL

Use self signed certificate

* Primary Server Address

* Primary Server Port

Secondary Server Address

Secondary Server Port

* Base DN ?

* Server Response Time ?

* CA Trust Chain

Choose a file or drag and drop to upload

Accepted files: .pem

📎 2019lab-DC02-CA-1.pem

OK
Cancel

Step 2 Click OK.

Step 3 Click the Role Mapping tab.

Step 4 Fill in the following fields:

- a) Map one or more Cisco Cyber Vision default roles with an Active Directory group.

Note At least one default role must be mapped.

Note Because the Admin user role is exclusively reserved for Cisco Cyber Vision internal usage, it cannot be mapped to any external users and thus is not proposed in LDAP settings.

- b) Map Cisco Cyber Vision custom roles with Active Directory groups.

You must type the exact group names as configured into the remote directory so they can be retrieved and mapped to user roles.

NEW LDAP SETTINGS X

Settings ! Role Mapping

Default roles ⓘ

Product ▾	Domain Users
Operator ▾	
Auditor ▾	

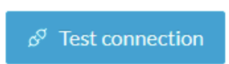
Custom roles ⓘ +

TestAD2019 ▾	TestAD2019	✖
--------------	------------	------------------------------------

OK Cancel

Step 5 Click OK.

Step 6 Click the Test connection button.



The Test Connection window pops up.

TEST CONNECTION X

* Username
2019lab\user2019

* Password
.....

Successful LDAP bind

OK Cancel

Step 7 Enter a user credentials to test the connection between Cisco Cyber Vision and Active Directory.

Note The Username format is <domain_name>\<user_name> (e.g. cisco\john_doe).

A message Successful LDPA bind should appear.

Step 8 Click OK.

Step 9 Test the connection by logging out of Cisco Cyber Vision and logging in with the mapped user credentials.

Menus are displayed according to the rights granted to the user.

90 days remaining Evaluation Mode

Signed in as 2019lab\user2019

My Settings

Logout

System

From this page, you can update the Knowledge DB.

Changing these parameters can impact your Cisco Cyber Vision setup. We recommend editing these parameters with care.

Center shutdown/reboot

Shutdown Reboot