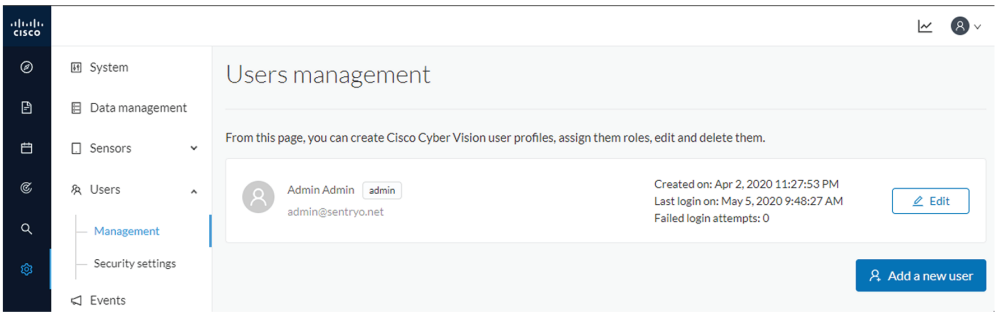
Users

Management

You can create, edit and delete users through the users administration page.



During their creation each user must be assigned with one of the following user roles (from full rights to read-only) or with a custom role (refer to Role Management).

- **Admin**

  The Admin user has full rights on the Cisco Cyber Vision platform. Users who have this role assigned oversee all sensitive actions like user rights management, system updates, syslog configuration, reset and capture modes configuration on sensors.

- **Product**

  The product user has access to several features of the system administration page (i.e. the system, sensors and events administration pages). This access level is for users who manage sensors from a remote location. In addition, they can manage the severity of events and, if enabled by the Admin user, can manage their export to syslog.

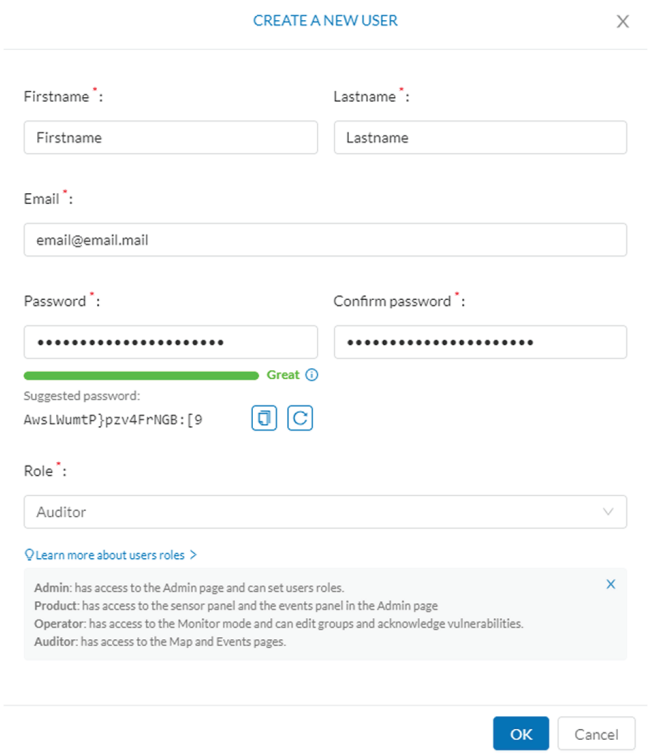
- **Operator**

This access level is for users who use the Monitor mode and manage groups but do not have to work with the platform administration. Thus, the Operator user has access to all pages, except the system administration page.

- **Auditor**

  This access level provides read-only access to the Explore, Reports, Events and Search pages. Auditors can use sorting features (such as search bars and filters) that do not require persistent changes to the Cisco Cyber Vision data (unlike Autolayout), and generate reports.

You can create as many users as needed with any user rights. Thus, several administrators can use and administrate the whole platform.



However, each user must have their own account. That is:

- Accounts must be nominative.
- One email address for several accounts is not allowed (note that email will be requested for login access).

  Passwords must contain at least 6 characters and comply with the rules below. Passwords:

  - Must contain a lower case character: a-z.
  - Must contain an upper case character: A-Z.
  - Must contain a numeric character: 0-9.
  - Cannot contain the user id.
  - Must contain a special character: ~!"#$%&’()*+,-./:;<=>?@[]^_{|}.

Important Passwords should be changed regularly to ensure the platform and the industrial network security.

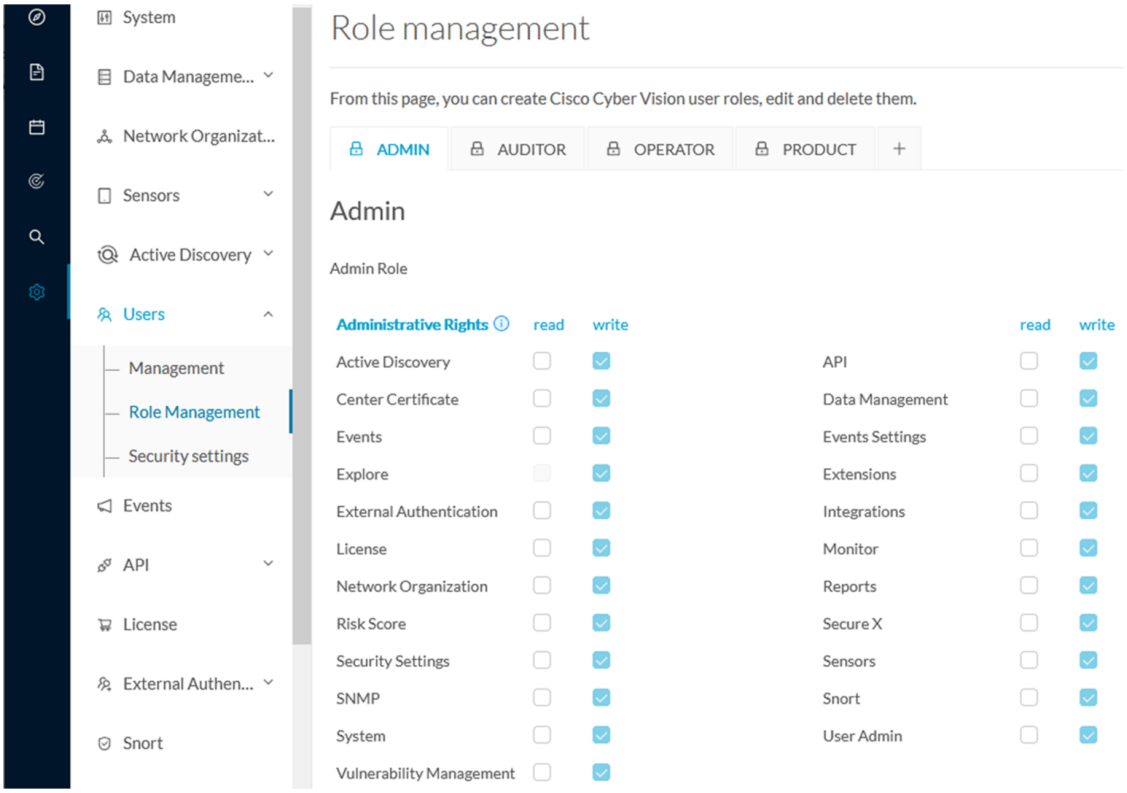
Passwords' lifetime is defined in the Security settings.

You can create custom user roles in the Role Management.

You can map Cisco Cyber Vision user roles with an external directory's user groups in the LDAP settings page.

Role Management

In addition to the four Cisco Cyber Vision default roles (i.e. Admin, Auditor, Operator and Product), customized roles can be created and modified from the Role management page.



These roles will help you defining specific privileges and accesses for each group of users.

Default roles cannot be edited or deleted.

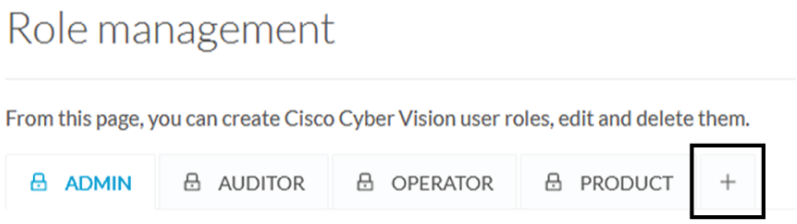
You can map Cisco Cyber Vision custom roles with an external directory's user groups in the LDAP settings page.

Create roles

This section explains how to create customized user roles on Cisco Cyber Vision. These can be later mapped to groups in Active Directory.

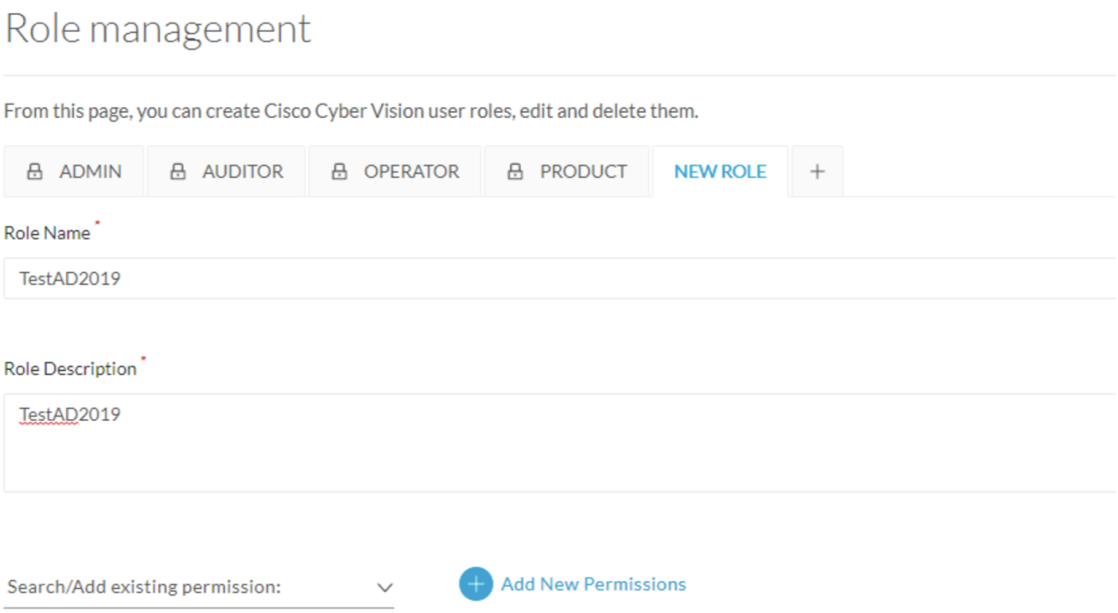
Step 1 In Cisco Cyber Vision, navigate to Admin > Users > Role Management.

Step 2 Click the + button next to default user roles.

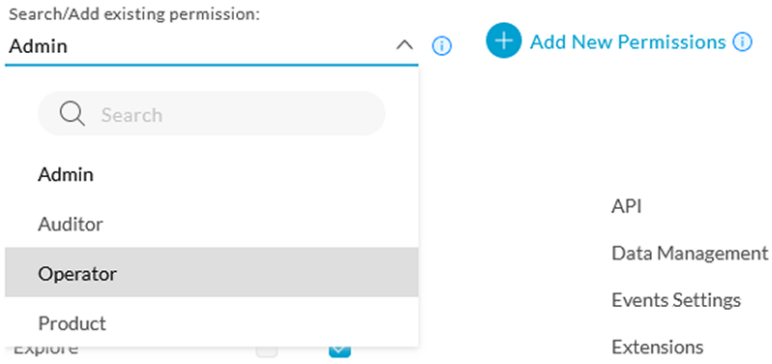


A new role tab appears.

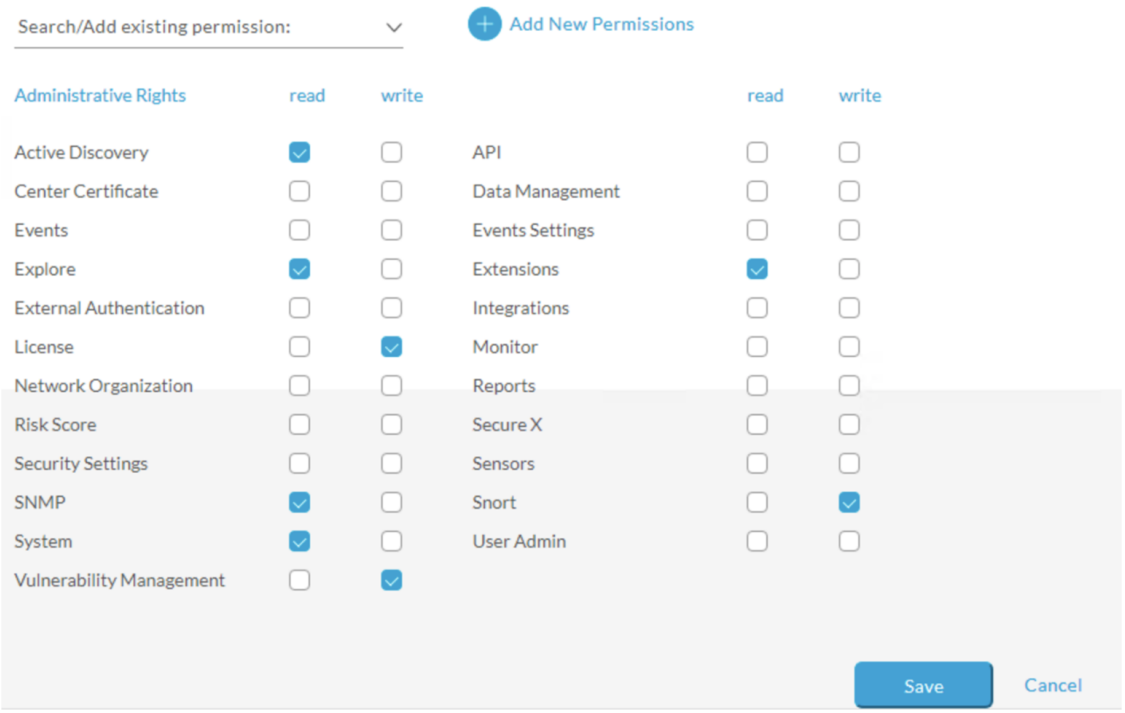
Step 3 Type a role name and a description.



Step 4 Select an existing role from the Search/Add existing permissions drop down menu, or click the Add New Permissions button to build the new user role from scratch.



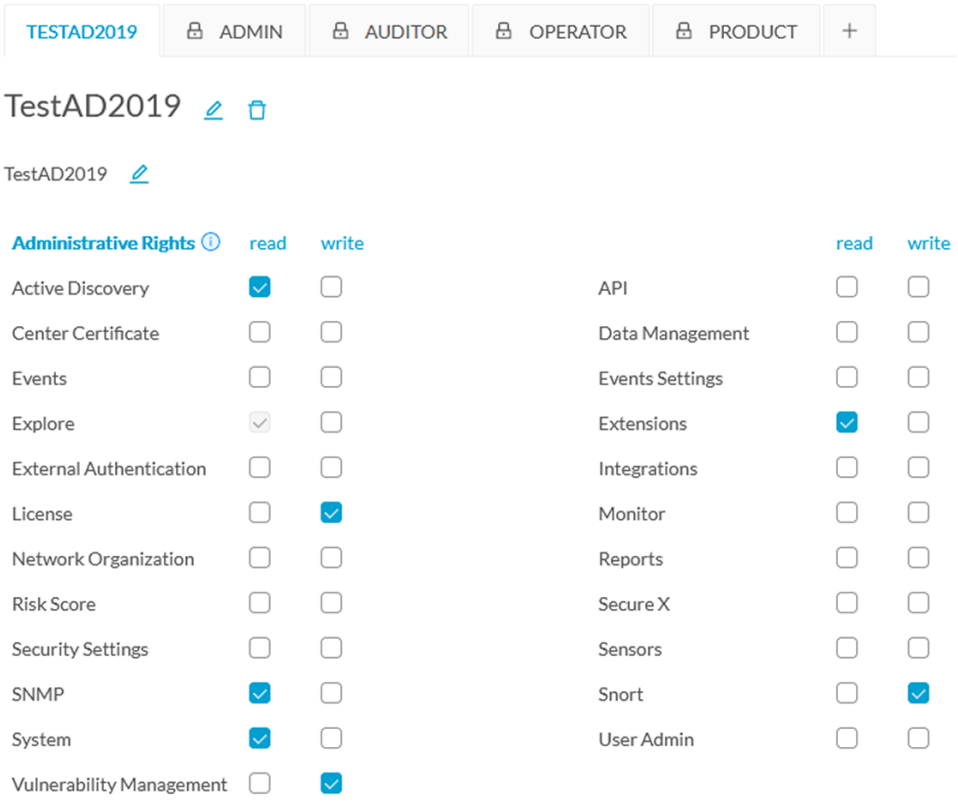
Step 5 Select/unselect permissions from the list as read or write



Step 6 Click save.

A message saying that the user role has been created successfully appears.

The new user role is displayed in the tab list.



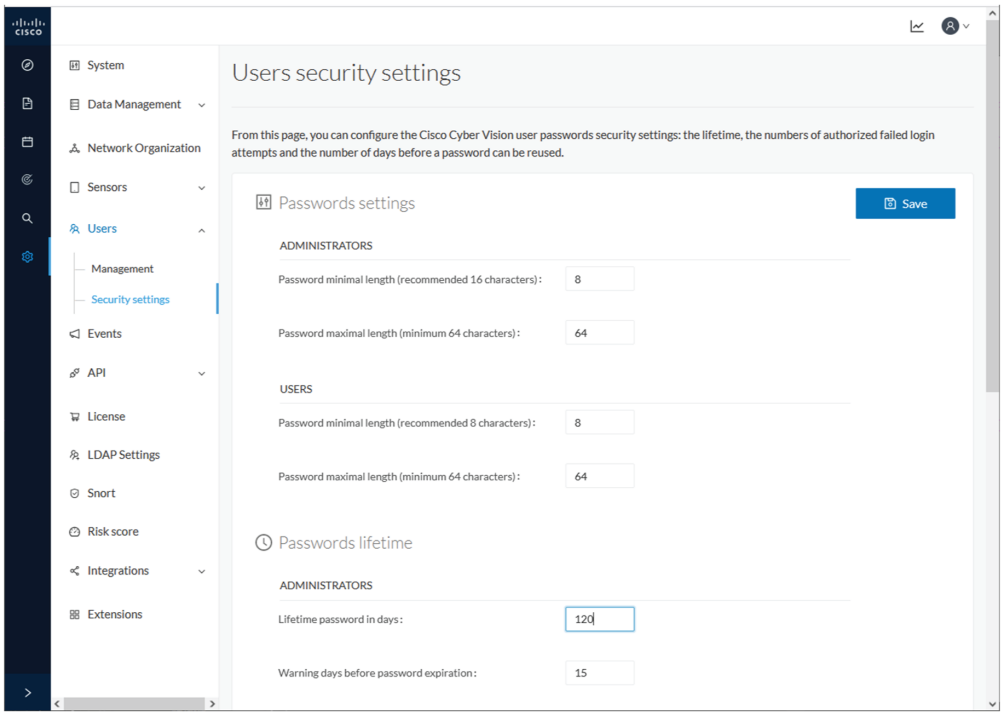
You can modify or delete directly in the tab.

What to do next

Custom roles created can be mapped with an external directory's user groups in the LDAP settings page.

Security settings

From this page you can configure the security settings of users' password such as its lifetime, the number of authorized login attempts, the number of days before a password can be reused, etc.


System
Data Management
Network Organization
Sensors
Users
Management
Security settings
Events
API
License
LDAP Settings
Snort
Risk score
Integrations
Extensions
Users security settings
From this page, you can configure the Cisco Cyber Vision user passwords security settings: the lifetime, the numbers of authorized failed login attempts and the number of days before a password can be reused.
Passwords settings
Save
ADMINISTRATORS
Password minimal length (recommended 16 characters):
8
Password maximal length (minimum 64 characters):
64
USERS
Password minimal length (recommended 8 characters):
8
Password maximal length (minimum 64 characters):
64
Passwords lifetime
ADMINISTRATORS
Lifetime password in days:
120
Warning days before password expiration:
15