

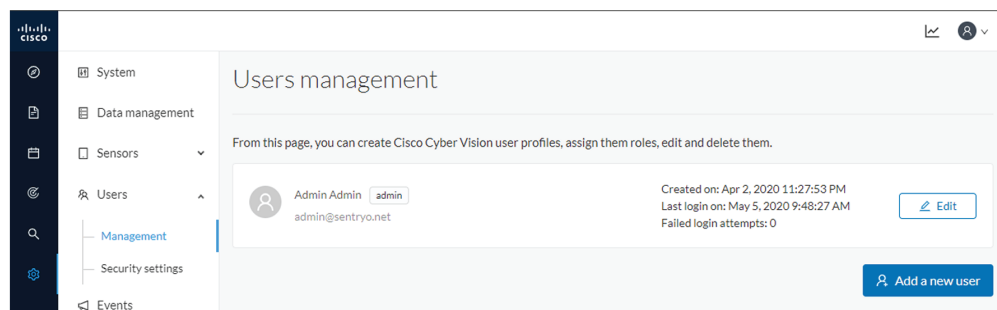


Users

- [Management, on page 1](#)
- [Role Management, on page 3](#)
- [Security settings, on page 6](#)

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.

CREATE A NEW USER X

Firstname * :

Lastname * :

Email * :

Password * :

Confirm password * :

Great ⓘ

Suggested password:
 AwsLWumtP}pzv4FrNGB: [9] i c

Role * :

Auditor
▼

[Learn more about users roles >](#)

Admin: has access to the Admin page and can set users roles. X

Product: has access to the sensor panel and the events panel in the Admin page.

Operator: has access to the Monitor mode and can edit groups and acknowledge vulnerabilities.

Auditor: has access to the Map and Events pages.

OK

Cancel

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.

Role management

From this page, you can create Cisco Cyber Vision user roles, edit and delete them.

ADMIN AUDITOR OPERATOR PRODUCT +

Admin

Admin Role

Administrative Rights ⓘ	read		write	
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Active Discovery	<input type="checkbox"/>	<input checked="" type="checkbox"/>	API	<input type="checkbox"/>
Center Certificate	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Data Management	<input type="checkbox"/>
Events	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Events Settings	<input type="checkbox"/>
Explore	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Extensions	<input type="checkbox"/>
External Authentication	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Integrations	<input type="checkbox"/>
License	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Monitor	<input type="checkbox"/>
Network Organization	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Reports	<input type="checkbox"/>
Risk Score	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Secure X	<input type="checkbox"/>
Security Settings	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Sensors	<input type="checkbox"/>
SNMP	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Snort	<input type="checkbox"/>
System	<input type="checkbox"/>	<input checked="" type="checkbox"/>	User Admin	<input type="checkbox"/>
Vulnerability Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>		

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

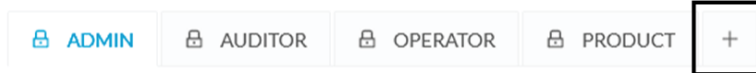
This section explains how to create customized user roles on Cisco Cyber Vision. These can be later mapped to groups in Active Directory.

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

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

Role management

From this page, you can create Cisco Cyber Vision user roles, edit and delete them.

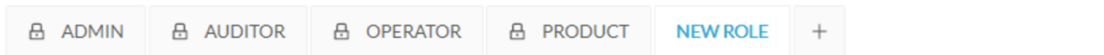


A new role tab appears.

Step 3 Type a role name and a description.

Role management

From this page, you can create Cisco Cyber Vision user roles, edit and delete them.



Role Name *

TestAD2019

Role Description *

TestAD2019

Search/Add existing permission:

[+ Add New Permissions](#)

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.

Search/Add existing permission:

Admin ^ ⓘ + Add New Permissions ⓘ

Search

Admin

Auditor

Operator

Product

Explore

API

Data Management

Events Settings

Extensions

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

Search/Add existing permission: ∨ + Add New Permissions ⓘ

Administrative Rights	read	write		read	write
Active Discovery	<input checked="" type="checkbox"/>	<input type="checkbox"/>	API	<input type="checkbox"/>	<input type="checkbox"/>
Center Certificate	<input type="checkbox"/>	<input type="checkbox"/>	Data Management	<input type="checkbox"/>	<input type="checkbox"/>
Events	<input type="checkbox"/>	<input type="checkbox"/>	Events Settings	<input type="checkbox"/>	<input type="checkbox"/>
Explore	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Extensions	<input checked="" type="checkbox"/>	<input type="checkbox"/>
External Authentication	<input type="checkbox"/>	<input type="checkbox"/>	Integrations	<input type="checkbox"/>	<input type="checkbox"/>
License	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Monitor	<input type="checkbox"/>	<input type="checkbox"/>
Network Organization	<input type="checkbox"/>	<input type="checkbox"/>	Reports	<input type="checkbox"/>	<input type="checkbox"/>
Risk Score	<input type="checkbox"/>	<input type="checkbox"/>	Secure X	<input type="checkbox"/>	<input type="checkbox"/>
Security Settings	<input type="checkbox"/>	<input type="checkbox"/>	Sensors	<input type="checkbox"/>	<input type="checkbox"/>
SNMP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Snort	<input type="checkbox"/>	<input checked="" type="checkbox"/>
System	<input checked="" type="checkbox"/>	<input type="checkbox"/>	User Admin	<input type="checkbox"/>	<input type="checkbox"/>
Vulnerability Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>			

Save Cancel

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.

TESTAD2019 ADMIN AUDITOR OPERATOR PRODUCT +

TestAD2019 [✎](#) [🗑](#)

TestAD2019 [✎](#)

Administrative Rights ⓘ	read	write		read	write
Active Discovery	<input checked="" type="checkbox"/>	<input type="checkbox"/>	API	<input type="checkbox"/>	<input type="checkbox"/>
Center Certificate	<input type="checkbox"/>	<input type="checkbox"/>	Data Management	<input type="checkbox"/>	<input type="checkbox"/>
Events	<input type="checkbox"/>	<input type="checkbox"/>	Events Settings	<input type="checkbox"/>	<input type="checkbox"/>
Explore	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Extensions	<input checked="" type="checkbox"/>	<input type="checkbox"/>
External Authentication	<input type="checkbox"/>	<input type="checkbox"/>	Integrations	<input type="checkbox"/>	<input type="checkbox"/>
License	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Monitor	<input type="checkbox"/>	<input type="checkbox"/>
Network Organization	<input type="checkbox"/>	<input type="checkbox"/>	Reports	<input type="checkbox"/>	<input type="checkbox"/>
Risk Score	<input type="checkbox"/>	<input type="checkbox"/>	Secure X	<input type="checkbox"/>	<input type="checkbox"/>
Security Settings	<input type="checkbox"/>	<input type="checkbox"/>	Sensors	<input type="checkbox"/>	<input type="checkbox"/>
SNMP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Snort	<input type="checkbox"/>	<input checked="" type="checkbox"/>
System	<input checked="" type="checkbox"/>	<input type="checkbox"/>	User Admin	<input type="checkbox"/>	<input type="checkbox"/>
Vulnerability Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>			

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.

The screenshot displays the Cisco Cyber Vision interface for configuring user security settings. On the left is a navigation sidebar with categories like System, Data Management, Network Organization, Sensors, Users, Events, API, License, LDAP Settings, Snort, Risk score, Integrations, and Extensions. The 'Users' section is expanded to show 'Security settings'. The main content area is titled 'Users security settings' and includes a brief instruction: '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.' Below this, there are two main sections: 'Passwords settings' and 'Passwords lifetime'. The 'Passwords settings' section has a 'Save' button and is divided into 'ADMINISTRATORS' and 'USERS'. For Administrators, the 'Password minimal length (recommended 16 characters)' is set to 8 and the 'Password maximal length (minimum 64 characters)' is set to 64. For Users, the 'Password minimal length (recommended 8 characters)' is set to 8 and the 'Password maximal length (minimum 64 characters)' is set to 64. The 'Passwords lifetime' section is also divided into 'ADMINISTRATORS' and 'USERS'. For Administrators, the 'Lifetime password in days' is set to 120 and the 'Warning days before password expiration' is set to 15.

Category	Setting	Value
Passwords settings	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

