Get Started with Cisco Cyber Vision

Certificate Fingerprint

Use the certificate fingerprint to register a **Global Center** with its synchronized centers and vice versa. To access the **Center Fingerprint**, choose **Admin** > **System** from the main menu. Click the copy icon to copy the **Fingerprint** and enroll your center with a global center.

For more information, refer the Centers Installation Guides.

Data Management

The **Data Management** interface allows you to do the following: manage data stored on Cisco Cyber Vision by Data clearance operations to optimize the Center performances, setting data expiration time, and customize traffic ingestion. To access Data Management, choose **Admin** > **Data Management** from the main menu.

The Cisco Cyber Vision update procedure will not purge data automatically. The Center's 3.2.x database will be migrated to the new 4.0.0 schema. All components, activities, flows, events, etc. will be migrated. Since the migration process can take hours (from 1 to 24 hours), you can perform a data purge in release 3.2.x to shorten the migration process. Launch the purge either from the Data clearance operations page or from the Command Line Interface (CLI), using the following command. Also, different options are offered.

```
sbs-db --help
```

Once migrated, the database content is managed with version 4.4.1 new data retention policies. Expiration settings apply. By default, the system will purge the following:

- Events after 6 months
- Flows after 6 months
- Variables after 2 years

Important You have 3 days once the migration from 3.2.x to 4.0.0 is done to set expiration settings as needed, before the default settings are applied by the system.

Data clearance operations

A data clearance is a maintenance operation that:

- removes stored information from Cisco Cyber Vision,
- can be performed either partially or completely, and
- affects data such as components, activities, flows, and variables.

Additional reference information

You can clear data in several ways:

- All data
- Components selection
- Activities, Flows, and Variables
- Flows and Variables
- Variables

Clearing data can impact network monitoring. Clear all data only as a last resort, for example, in cases of database overload. This action removes all network data (components, flows, events, baselines) from Cisco Cyber Vision, leaving the GUI empty. Your configurations, including capture modes, event severity, and syslog, remain intact.

Purge components from the database

Remove unnecessary or obsolete components and devices to maintain optimal database performance and prevent data ingestion issues.

The system limits the number of components (network interfaces, PCs, SCADA stations, broadcast or multicast addresses, and so on) in the database for protection.

- If the count exceeds 120,000, a pop-up and red banner alert you to purge.
- When the number of components reaches 150,000, data ingestion stops. The system deletes new sensor data without processing or storing it. A pop-up and red banner alert you to purge.

You provide selection criteria to purge components and devices. The system finds and deletes matching items. Then, the system requests synchronization with the global center.

Before you begin

Ensure you have Admin access to perform this action.

Procedure

Step 1 Open the main menu, choose **Admin** > **Data Management** > **Clear Data**.

Step 2 Select **Components selection**.

Step 3 Choose the **Component Type**: IT, OT, or both.

Step 4 Enter the required criteria:

- **IP Subnet** (optional)
- **VLAN** ID (optional; only one ID can be specified at a time)
- **Inactivity since** (optional)
- **Creation Start Time** (optional), and
- **Creation End Time** (optional).

Step 5 Click **Clear data** and confirm when prompted.

The system purges the specified components and related devices. The updated device count appears under **Explore** > **All Data**.

Note When you purge components by VLAN, IP, or date, the system triggers an event. If a Global Center (GC) is enrolled with the Local Center (LC), it also purges the components in the GC after synchronization.

What to do next

Review the device list to ensure the correct components were removed.

Expiration Settings

To configure the **Expiration Settings**, choose **Admin** > **Data Management** > **Expiration Settings** from the main menu.

On this page, you can manage the duration for which data and reports remain available. Select expiration times for reports and their versions. Use the drop-down menu to choose expiration periods of 3 months, 6 months, 1 year, 2 years, or 3 years. You can also set the maximum number of report versions from 1 to 100.

Note Selecting a high value may rapidly fill up storage and adversely affect system performance. The recommended value is 10 versions.

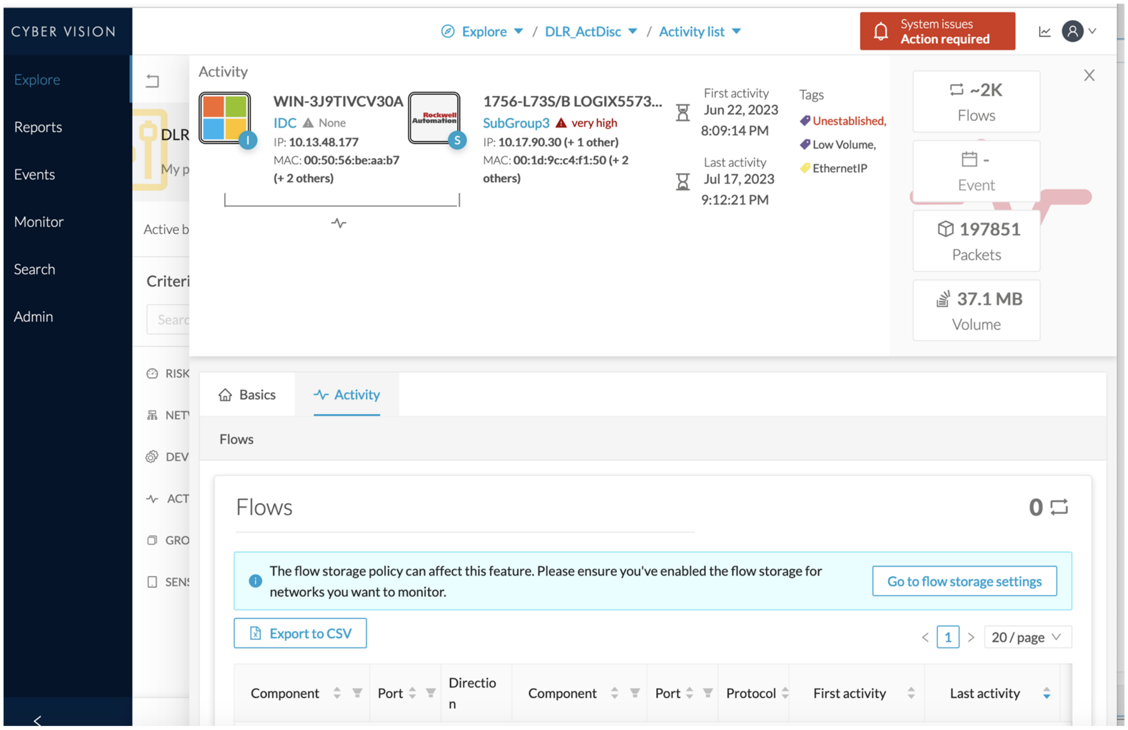
Ingestion configuration

The **Ingestion Configuration** page allows you to configure flow and variable traffic storage. You can choose whether to store flows and variables. Flows and variables storage is disabled by default.

See Enable variable processing in a sensor template to enable **Variable Storage**.

To access the **Ingestion Configuration**, choose **Admin** > **Data Management** > **Ingestion Configuration**from the main menu.

Messages can appear in Cisco Cyber Vision's user interface to indicate to the user that features may be limited due to absence of flows in the database. For example, in the activity technical sheet, at the top of the flows table:



The flow storage policy can affect this feature. Please ensure you've enabled the flow storage for networks you want to monitor.

In this case, you can click **Go to flow storage settings** and enable **Flow Storage**.

If **Flow Storage** is enabled, it is possible to choose from which subnetworks flows should be stored. These subnetworks can be set on the Network organization page. The option "others" includes flows that are not part of the industrial private network.

An automatic purge will occur on selected flows when a period of inactivity exceeds 7 days.

You can click the **Flows Aggregation** and **port scan detection** toggle buttons to enable them.

Users

Management

You can create, edit and delete users through the **Users management** page. To access the **Users management** page, choose **Admin** > **Users** > **Management** from the main menu.

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 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 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. To access the **CREATE A NEW USER** window, choose **Admin** > **Users** > **Management** from the main menu. Click **Add a new user**, and the window appears.

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 page.

You can create custom user roles in the Role Management page.

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. To access the **Role management** page, choose **Admin** > **Users** > **Role Management** from the main menu.

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 a user role

Define a customized user role to assign specific permissions in Cisco Cyber Vision.

Custom roles allow administrators to tailor access control. You can later map them to Active Directory groups for role-based user management.

Before you begin

Ensure the **Cyber Vision New UI** is enabled for your center.

Procedure

Step 1 From the main menu, choose **Admin** > **Users** > **Role Management**.

Step 2 Click **+** to add a new role.

Step 3 Enter the **Role Name** and **Role Description**.

Step 4 Select existing permissions by selecting a role from **Search/Add existing permission**, or click **Add New Permissions** to define new permissions.

Step 5 Under **Classic UI Permissions**, select required permissions (**Read** or **Read + Write**).

Note
By default, the **Explore** section has read permission in Classic UI.

Step 6 Under **New UI Permissions**, select required permissions (**Read** or **Read + Write**).

Note

By default, **Assets and Vulnerabilities** and **Vulnerability Acknowledgement** have read permission, and **Dashboard** has both read and write permissions in the New UI.

Step 7 Click **Save**.

The new user role appears in the **Role Management** list.

What to do next

You can modify or delete the role in **Role Management**, or map custom roles to external directory groups in LDAP settings.

Security Settings

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

To access **Users security settings**, from the main menu, choose **Admin** > **Users** > **Security settings**.

Center Web Server Certificate

The **Center web server certificate** page is to configure Cisco Cyber Vision user interface security with an enterprise certificate. You will have the option to upload a .p12 or to generate a CSR.

To access **Center web server certificate** page, from the main menu, choose **Admin** > **Web Server Certificate**.

For more information, see to the corresponding Center Installation Guide.