Get Started with Cisco Cyber Vision

Data management operations

Data management operations are Cyber Vision Center features that

- manage and optimize data stored on Cyber Vision Center,
- support tasks such as data clearance, setting data expiration, and customizing data ingestion, and
- improve system performance by enabling effective storage and retention policies.

Table 1: Feature History Table

Feature	Release Information	Feature Description
Clear multiple components using a VLAN ID	Release 5.3.x	When you clear data, you can enter a VLAN ID to purge all the components associated with it. You can clear data for one VLAN ID at a time.

Caution: Understand the impact before clearing all data

Clear all data only when absolutely necessary, such as when the database becomes overloaded.

Be aware of these consequences:

- The system deletes all network data, including components, flows, events, and baselines, from Cyber Vision Center.
- The GUI becomes empty.
- The system preserves only configuration settings, such as capture modes, event severity, and syslog settings.
- Clearing all data disrupts network monitoring.

Data storage and expiration settings

This table explains storage limits, expiration policies, and purge methods for each data type. You can use this information to manage system resources effectively.

Table 2: Settings

Data type	Storage	Expiration
Components or Devices	Storage is internal only. You receive a warning when you reach 120,000 components. Data ingestion stops at 150,000 components.	No expiration. Manual purge is needed.
Activities	Activities are stored internally and do not have a high storage limit.	The data does not expire. You must purge it manually.
Flows	You can enable or disable storage configuration; there is no upper storage limit. You can then define networks.	The system automatically deletes data after seven days of inactivity.
Events	You can configure the storage for each category, with a high limit of 10,000 per event category.	No expiration. The oldest event is purged when the 10,000 limit is reached.
External communications	Communications are stored externally only. You can save up to one million communications.	The system deletes data automatically after 30 days.
Variables	You can enable or disable the storage configuration, with no high storage limit.	The system deletes data automatically after seven days of inactivity.
Reports	You can set the storage period from three months to three years. The default is six months. The storage duration also depends on the maximum number of versions you set.	The system automatically deletes data when the creation date is older than the defined period or when the number of versions exceeds the limit.

Purge components from the database

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

To protect the database, the system limits the number of components such as network interfaces, PCs, SCADA stations, broadcast or multicast addresses, and similar items.

- 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 data without processing or storing it. A pop-up and red banner alert you to purge.

Before you begin

- Ensure you have Admin access.

Procedure

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

Step 2 Select **Components selection**.

Step 3 Choose the **Component Type**:

- **IT**: This selects components in the IP range with the **IT Internal** network type.
- **OT**: This selects components in the IP range with the **OT Internal** network type.
- Both: This selects components in the IP range with both network types.

Step 4 Specify any criteria for purging (all fields optional):

- IP Subnet
- VLAN ID (one at a time)
- Inactivity since
- Creation Start Time
- Creation End Time

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

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

Note Purging components by VLAN, IP, or date triggers an event. If a Global Center is enrolled, those components are also purged in the Global Center after synchronization.

What to do next

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

Expiration settings

Expiration settings help you manage system storage and performance.

Key aspects of expiration settings:

- Expiration settings control the retention period and number of versions for reports only. Other data types (such as Components, Devices, Activities, Flows, Events, External communications, and Variables) have fixed retention periods.
- Expiration settings manage storage consumption by automatically purging reports older than the configured retention period.
- Increasing the retention period increases storage usage and may negatively impact system performance.
- Access expiration settings at **Admin** > **Data Management** > **Expiration Settings** in the Cyber Vision Center interface.

Ingestion configurations

An ingestion configuration is a data management feature that determines whether flow and variable traffic data are stored and processed by Cyber Vision Center.

You can enable or disable storage of flows and variables. By default, both options are disabled. To limit data storage, you can specify which flows from subnetworks are stored. These subnetworks are defined within Network Organization settings.

If flows and variables are disabled, data will not be stored in the database.

Flows Aggregation

- Cyber Vision records each flow that it detects, and includes details such as client and server ports for your reference.
- For protocols such as DNS, HTTP, or SSH, client ports can vary, so you may see many similar entries in your data.
- If you enable **Flow Aggregation**, Cyber Vision does not consider the client port for those specific protocols. This combines similar flows and limits the number of records in the database.

Port scan detection

Port scan detection helps you identify and respond to suspicious network probing, which may indicate cyberattack attempts.

Users

A user is an account holder in Cyber Vision Center that

- accesses and interacts with the Cyber Vision Center platform,
- is assigned one or more roles that define permissions and access privileges, and
- is managed using user management features, such as roles and security settings.

Table 3: Feature History Table

Feature	Release Information	Feature Description
Restrict users to a specific preset category	Release 5.4.x	This feature enables precise data access control by assigning preset categories to Cyber Vision user roles, limiting users to the Explore menu with read-only permissions. **Note** Once you restrict a user to a specific preset category, they will not have access to the New UI.

User roles and management

Cyber Vision Center provides default user roles such as Admin, Auditor, Operator, and Product. You can also create custom roles to tailor specific permissions and access levels for different users or groups. Roles control the actions that you can perform within the platform. You can map user roles (except Admin) to external directory groups through LDAP. To provide admin privileges through LDAP, clone the admin role and map it to the external directory group.

User security settings

The Security settings page (**Admin** > **Users** > **Security settings**) allows configuration of password policies, such as password lifetime, login attempt limits, and password reuse restrictions, to help protect user accounts.

User roles

User roles define access and administrative privileges in the platform.

Table 4: User role types and privileges

Role	Privilege
Admin	If you have the admin role, you have full rights and oversee all sensitive actions. These actions include managing user rights, updating the system, configuring syslog, and setting up sensor reset or sensor capture mode.
Product	If you have the product role, you can access system, sensor, and event administration pages and manage sensors remotely. You may manage event severity and export events to syslog if an admin allows it.
Operator	If you have the operator role, you work in monitor mode and can manage groups, but do not have administration privileges. You can access all pages except system administration.

Role	Privilege
Auditor	If you have the auditor role, you have read-only access to Explore, Reports, Events, and Search pages. You can use non-persistent sorting features and generate reports.

Password requirements

Passwords protect user accounts and systems against unauthorized access.

Passwords must meet these requirements:

- Contain at least 6 characters.
- Must include:
  - A lowercase character from a to z
  - An uppercase character from A to Z
  - A numeric character from zero to nine
  - A special character (~!"#$%&’()*+,-./:;<=>?@[]^_{|})
- Not contain your user ID.

Additional best practices:

- Change your password regularly.
- Configure password lifetime settings in **Admin** > **Users** > **Security settings**.

Add a new user

Add a new user account to Cyber Vision Center to log in and access assigned roles.

Before you begin

Ensure you have administrator privileges in Cyber Vision Center.

Procedure

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

Step 2 Click **Add a new user**.

Step 3 Enter the required user details: **Firstname**, **Lastname**, **Email**, **Password**, and **Confirm password**.

Step 4 Select the appropriate role for the user.

Step 5 Click **OK**.

You can see the new user in the **Users management** page, and the user can log in with the assigned credentials.

What to do next

To edit or delete the user later, use the **Users management** page.

Create a user role

Create a user role in Cyber Vision with specific permissions to meet your needs.

Use user roles to define precise access and manage permissions for each user in Cyber Vision.

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 the add button **(+)** to create a new role.

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

Step 4 Set permissions for the new user role using one method:

- **Restrict user access to a single preset category**:
  1. Enable **Restrict user access to a single preset category**.
  2. Select a preset category and click **Save**.

  Note
  - To delete a preset category, first unassign it from any user role.
  - If a user is restricted to a preset category, they have read-only access to the **Explore** menu only.

- **Search/Add existing permission**:
  1. Select a role from **Search/Add existing permission**.
  2. Click **Save**

- **Add New Permissions**:
  1. Click **Add New Permissions**.
  2. Select required permissions (**Read** or **Read + Write**) from **Classic UI Permissions** and **New UI Permissions**.
  3. Click **Save**.

  Note
  You receive read access to **Explore** in the Classic UI and to **Assets and Vulnerabilities** in the New UI by default.

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

What to do next

- You can edit or delete roles in **Role Management**.
- You can map custom roles to external directory groups in LDAP settings.

Center web server certificates

A center web server certificate is a digital security credential that

- enables encrypted communication between the Cyber Vision Center and web browsers,
- ensures data integrity and confidentiality during browser sessions, and
- allows client devices to verify the Center's identity before exchanging sensitive data.

Options for managing web server certificates

You can manage Center web server certificates in two ways:

- Default internal certificate:
  - The system automatically generates a default internal (self-signed) certificate. To establish secure communication when using this certificate, you need to download it from the Center and install it on your laptop or client device. Adding this certificate to your device's trusted certificate store secures your communications with the Center.
- Enterprise certificate management:
  - Alternatively, you can configure the Center to use an enterprise certificate. The Center can use an enterprise certificate by uploading a P12 file, generating a certificate signing request (CSR) for your Certificate Authority (CA), or using the ACME protocol. Once in place, browsers will automatically trust the Center web interface. For more information, see the "Configure the Center" chapter in the Center Installation Guide.