



Data management

The **Data Management** interface allows you to do the following: manage data stored on Cisco Cyber Vision by [Clear data](#) to optimize the Center performances, [Expiration settings](#), and [Ingestion configuration](#). To access Data Management, click **Admin > Data Management**.

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 [Clear data](#) 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 4.0.0 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.

- [Clear data, on page 1](#)
- [Expiration settings, on page 4](#)
- [Ingestion configuration, on page 5](#)

Clear data

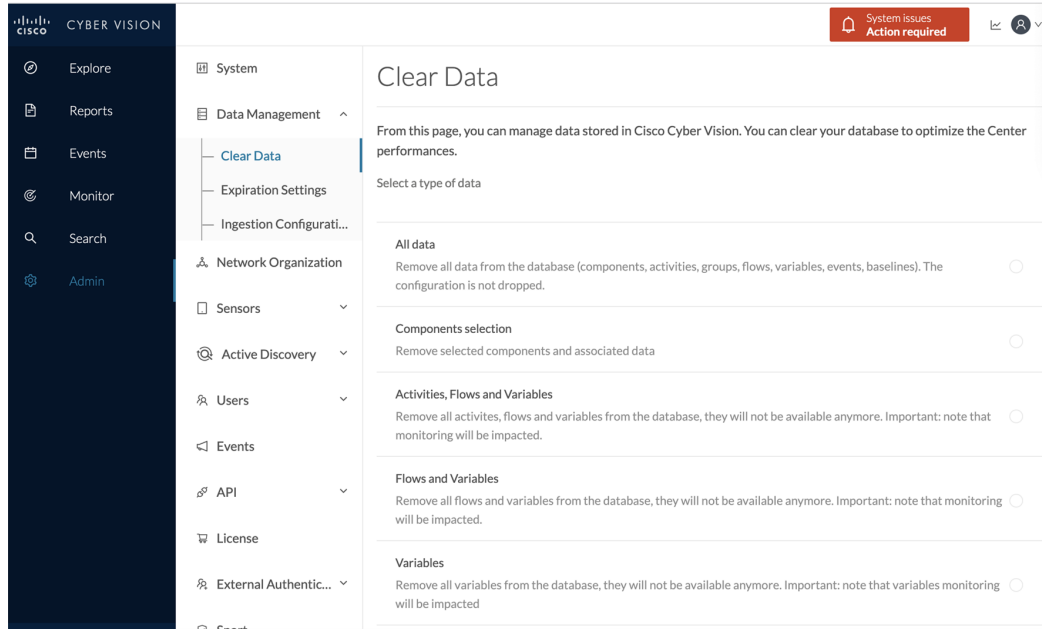
Clear data stored on Cisco Cyber Vision to optimize the Center's performances. Clear data partially or totally, as follows:

- All data
- Components selection and associated data (refer to [Purge components, on page 2](#))
- Activities, Flows and Variables

- Flows and Variables
- Variables

To clear data, click **Admin > Data Management > Clear Data**.

Clear data **very carefully**. Clearing any data can impact monitoring of the network. Please read the implications about all data clearance below.



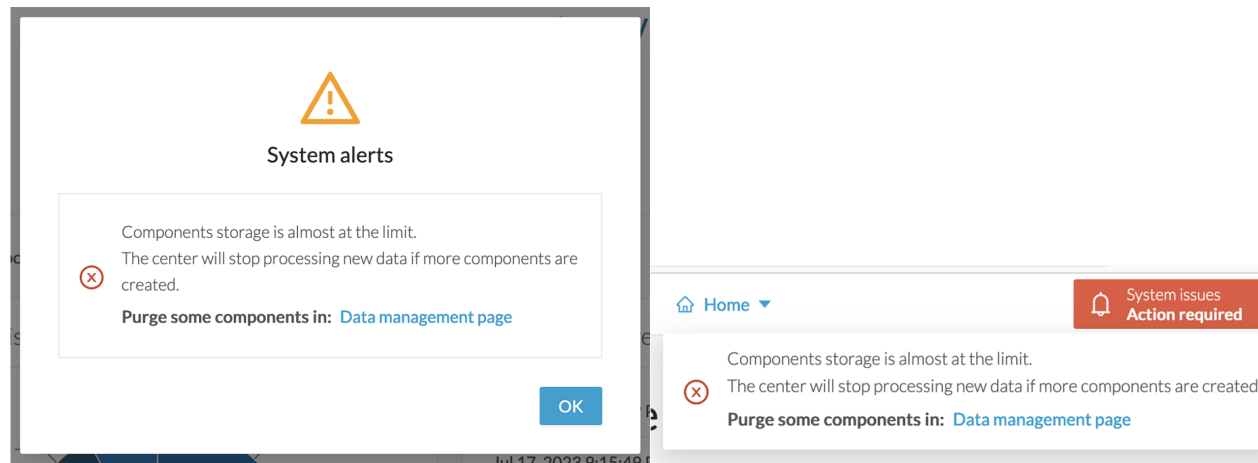
Data Clearance

Use **Clear All data** as a last resort, in case of database overload issues. This action results in the entire database content deletion. Network data such as components, flows, events and baselines are deleted from Cisco Cyber Vision and the GUI empties. All configurations are saved. Existing users and user data configuration (such as capture modes, events severity set up, syslog configuration) persist.

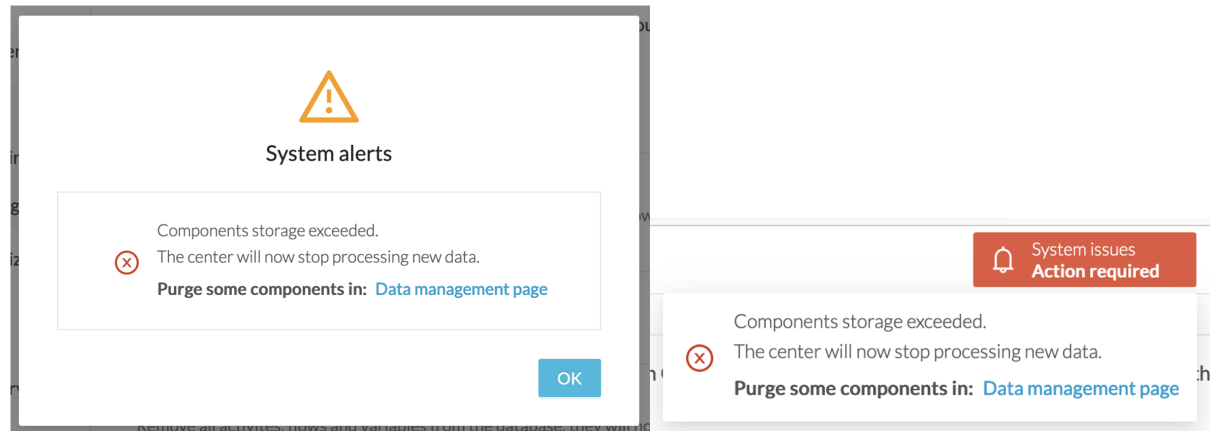
Purge components

In Cisco Cyber Vision, a component represents an object of the industrial network from a network point of view. It can be the network interface of a PLC, a PC, a SCADA station, etc., or a broadcast or multicast address. The system protects itself by limiting the number of components stored in the database.

When the system reaches more than 120,000 components, a popup and red banner alert appear to inform you that a purge is required. Components purge is based on several criteria.



If the system reaches 150,000 components, ingestion stops. Incoming sensor data are not treated or stored and are deleted. A popup and a red banner alert appear to inform you that a purge is required.



To purge components:

Step 1 Click **Admin > Data Management > Clear Data**.

Step 2 Click the **Components selection** radio button.

Step 3 Select the component type (**External, IT** or **OT**).

Step 4 Type the **IP Subnet**.

Step 5 Click the calendar icon to add an **Inactivity since** date.

Step 6 Click the calendar icon to add a **Creation time** date. Provide a **Start Time** and **End Time** (optional).

Step 7 Click **Clear data**.

Expiration settings

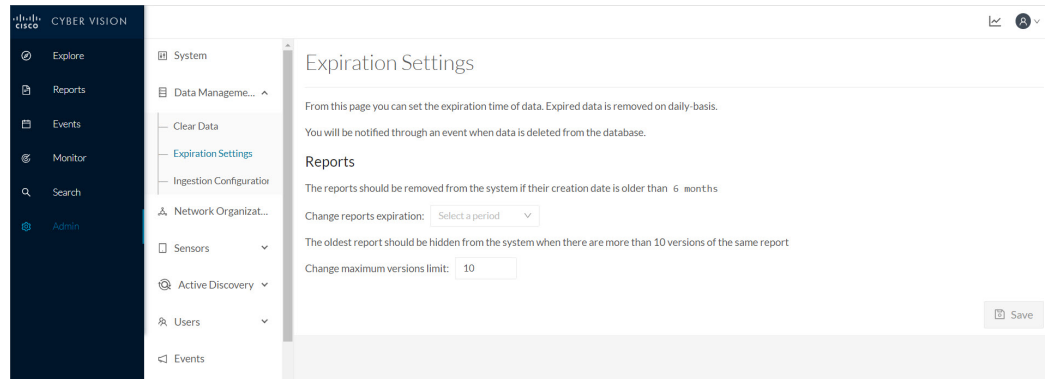
Follow these steps to configure the **Expiration Settings**:

1. From the left pane, click **Admin**.
2. Click **Data Management > Expiration Settings**

On this page, you can control how long data and reports stay available. You can choose expiration times for reports and their versions. Use the dropdown menu to select expiration periods of 3 months, 6 months, 1 year, 2 years, or 3 years. You can also limit the maximum number of report versions from 1 to 100.



Note Selecting a high value might fill up storage rapidly and affect system performance. Recommended value: 10 versions.

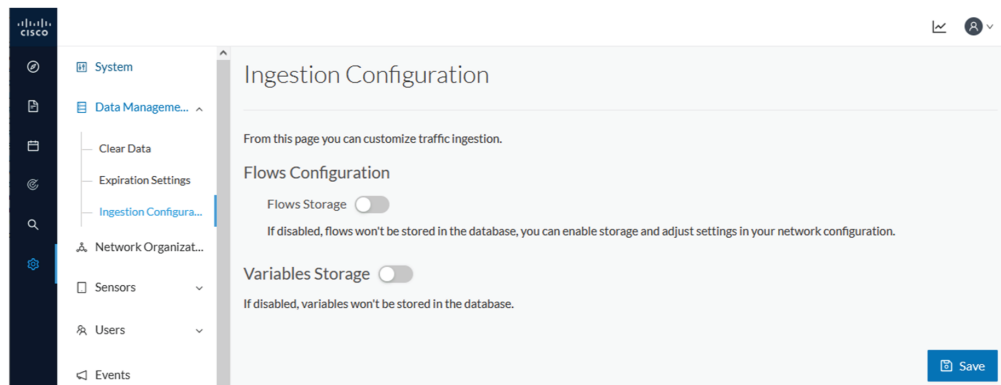


Ingestion configuration

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.



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 screenshot shows the Cisco Cyber Vision interface. On the left is a navigation menu with options: Explore, Reports, Events, Monitor, Search, and Admin. The main content area displays an activity list with details for two items:

- WIN-3J9TIVCV30A**: IDC (None), IP: 10.13.48.177, MAC: 00:50:56:be:aa:b7 (+2 others). Status: **Unestablished**.
- 1756-L73S/B LOGIX5573...**: SubGroup3 (very high), IP: 10.17.90.30 (+1 other), MAC: 00:1d:9c:c4:f1:50 (+2 others). Status: **Unestablished**.

Summary statistics on the right show: ~2K Flows, 0 Events, 197851 Packets, and 37.1 MB Volume. A red arrow points to the 'Event' button. Below the activity list, the 'Flows' section is visible, showing a message: "The flow storage policy can affect this feature. Please ensure you've enabled the flow storage for networks you want to monitor." with a "Go to flow storage settings" button. A table header for flows is partially visible with columns: Component, Port, Direction, Component, Port, Protocol, First activity, and Last activity.

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

If flows 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.

Flows Configuration

Flows Storage

If disabled, flows won't be stored in the database, you can enable storage and adjust settings in your network configuration.

Network Name	Flow Storage
IPv4 link local	<input checked="" type="checkbox"/>
IPv6 link local	<input checked="" type="checkbox"/>
Others	<input checked="" type="checkbox"/>
Endpoints without IP address	<input checked="" type="checkbox"/>
10/8 private network	<input checked="" type="checkbox"/>
192.168/16 private network	<input checked="" type="checkbox"/>

It is also possible to enable flows aggregation and port scan detection.

Flows Aggregation

Cisco Cyber Vision stores every individual network flow that has been seen by the sensors with full details (including the client/server ports for each flow).
For some TCP/UDP based protocols, the client port is dynamically generated by the client and thus Cisco Cyber Vision will store multiple similar copies of the flow for each spotted client port.
When enabling flow aggregation, Cisco Cyber Vision will instead discard the client port, thus limiting the number of flows in the database.

Only the following protocols are concerned by flow aggregation: DNS, NTP, SSH, SNMP, Syslog, RabbitMQ, HTTP(S), IEC104, EtherNet/IP. Flows for other protocols are always stored with full details.

Port scan detection