Data management

From the system administration page, you can manage data stored on Cisco Cyber Vision by Clear data to optimize the Center performances, Expiration settings, and Ingestion configuration.

Cisco Cyber Vision update procedure will not purge any 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), it is possible to proceed to a data purge in release 3.2.x to shorten the migration process. This purge can be launched either from the Clear data page in the Graphic User Interface (GUI), or from the Command Line Interface (CLI), using the following command where different options will be offered:

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

Once migrated, the database content will be managed with version 4.0.0 new data retention policies. Expiration settings will be applied, and the system will purge by default:

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

The user will have 3 days once the migration from 3.2.x to 4.0.0 is done to set Expiration settings as needed before default settings are applied by the system.

Clear data

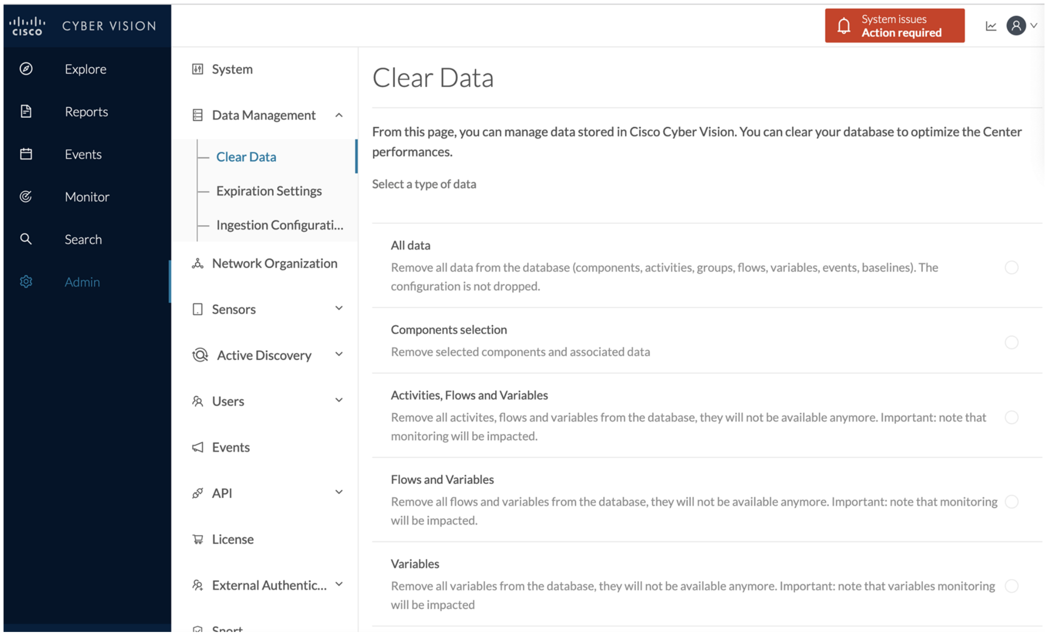
From this page, you can clear data stored on Cisco Cyber Vision to optimize the Center's performances.

You can clear data partially or totally, like below:

- all data
- components and associated data (refer to Purge components, on page 2)
- activities, flows and variables
- flows and variables

- variables

Clearing data should be performed carefully. Clearing any data can impact monitoring of the network. Please read below all implications about all data clearance.



Clear Data

From this page, you can manage data stored in Cisco Cyber Vision. You can clear your database to optimize the Center performances.

Select a type of data

All data
Remove all data from the database (components, activities, groups, flows, variables, events, baselines). The configuration is not dropped. ○

Components selection
Remove selected components and associated data ○

Activities, Flows and Variables
Remove all activites, flows and variables from the database, they will not be available anymore. Important: note that monitoring will be impacted. ○

Flows and Variables
Remove all flows and variables from the database, they will not be available anymore. Important: note that monitoring will be impacted. ○

Variables
Remove all variables from the database, they will not be available anymore. Important: note that variables monitoring will be impacted ○

About all data clearance:

Clearing all data is to be used as a last resort in case of database overload issues.

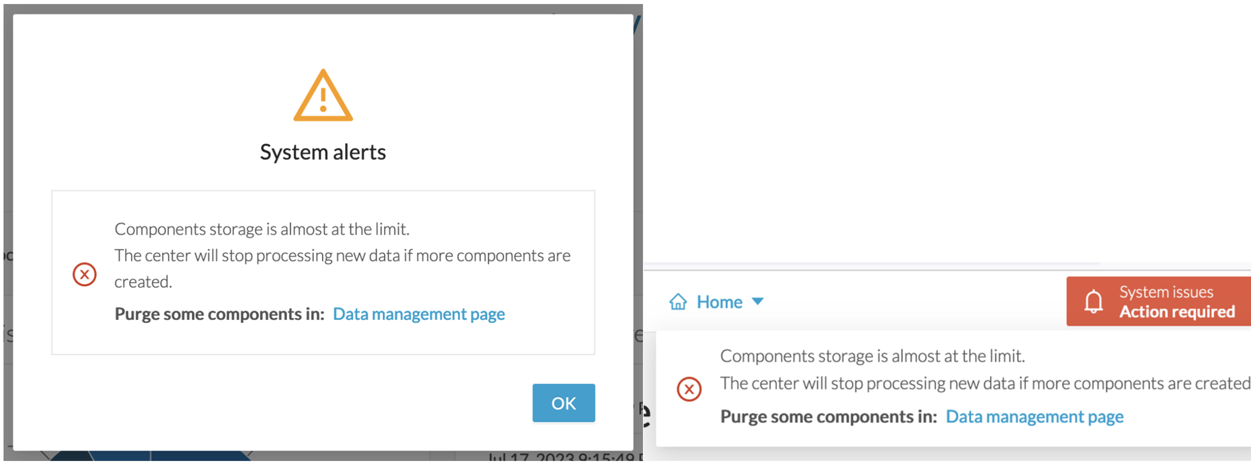
This will result in the entire database content deletion. Network data such as components, flows, events and baselines will be deleted from Cisco Cyber Vision and the GUI will be emptied.

All configurations will be saved. Existing users and user data configuration (such as capture modes, events severity set up, syslog configuration) will remain unchanged.

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. To protect the system the number of components stored in the database is limited.

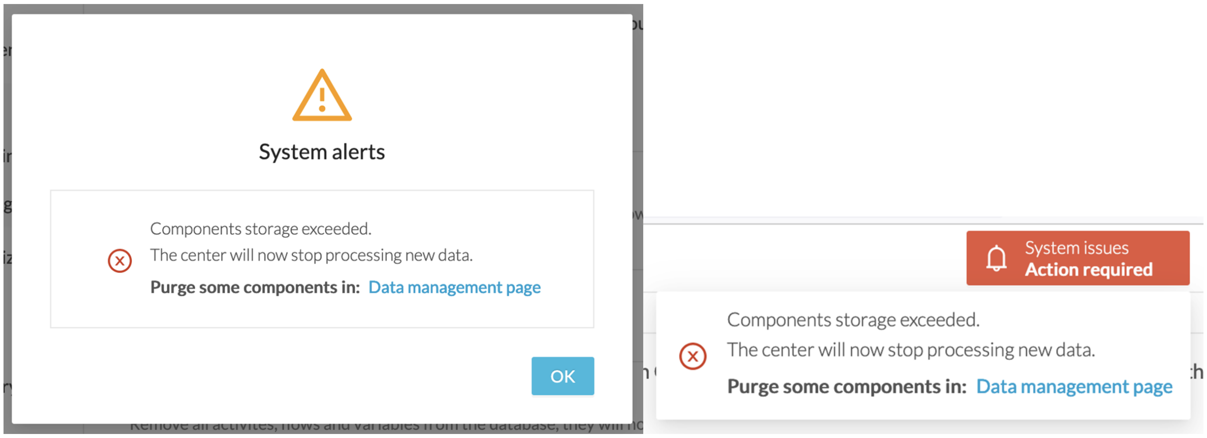
As the system reaches more than 120,000 components a popup and red banner alert appears on the user interface to inform the user that a purge must be performed. Components purge can be based on several criteria.



Components storage is almost at the limit.
The center will stop processing new data if more components are created.
Purge some components in: Data management page

Components storage is almost at the limit.
The center will stop processing new data if more components are created
Purge some components in: Data management page

If the system reaches 150,000 components the ingestion stops. Incoming sensor data are not treated nor stored and are directly deleted. A popup and a red banner alert appears on the user interface to inform the user that a purge must be performed.



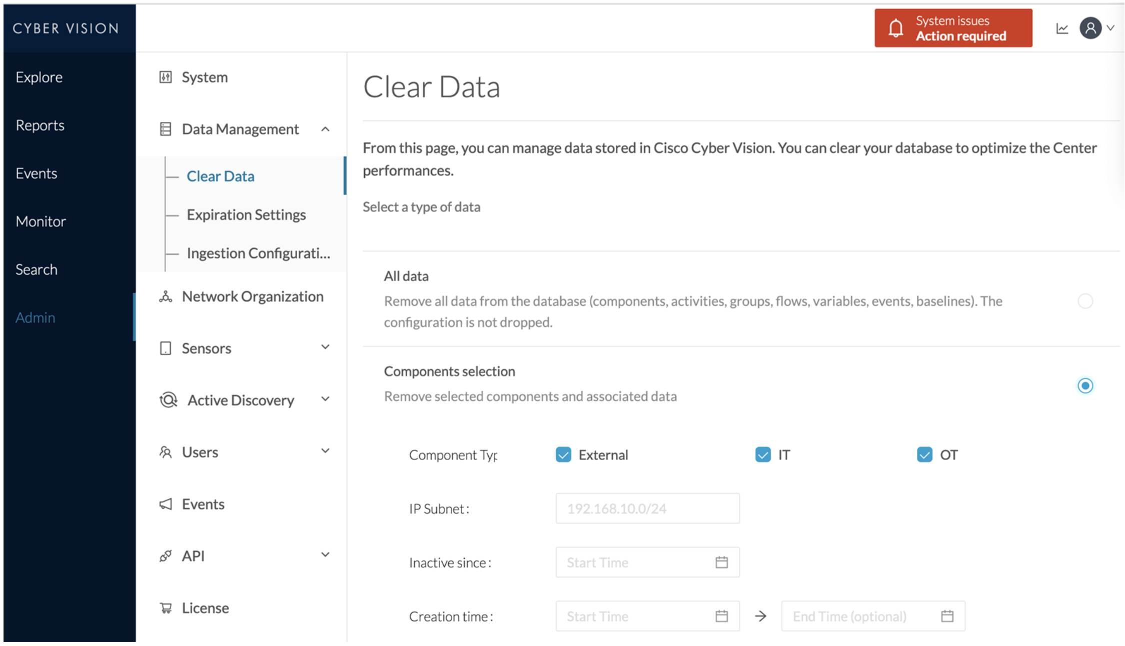
Components storage exceeded.
The center will now stop processing new data.
Purge some components in: Data management page

Components storage exceeded.
The center will now stop processing new data.
Purge some components in: Data management page

To do so:

Step 1 Navigate to Admin > Data management > Clear Data.

Step 2 Deploy the **Components selection** menu.



Clear Data

From this page, you can manage data stored in Cisco Cyber Vision. You can clear your database to optimize the Center performances.

Select a type of data

○ All data
Remove all data from the database (components, activities, groups, flows, variables, events, baselines). The configuration is not dropped.

● Components selection
Remove selected components and associated data

Component Typ ☑ External ☑ IT ☑ OT

IP Subnet : 192.168.10.0/24

Inactive since : Start Time

Creation time : Start Time → End Time (optional)

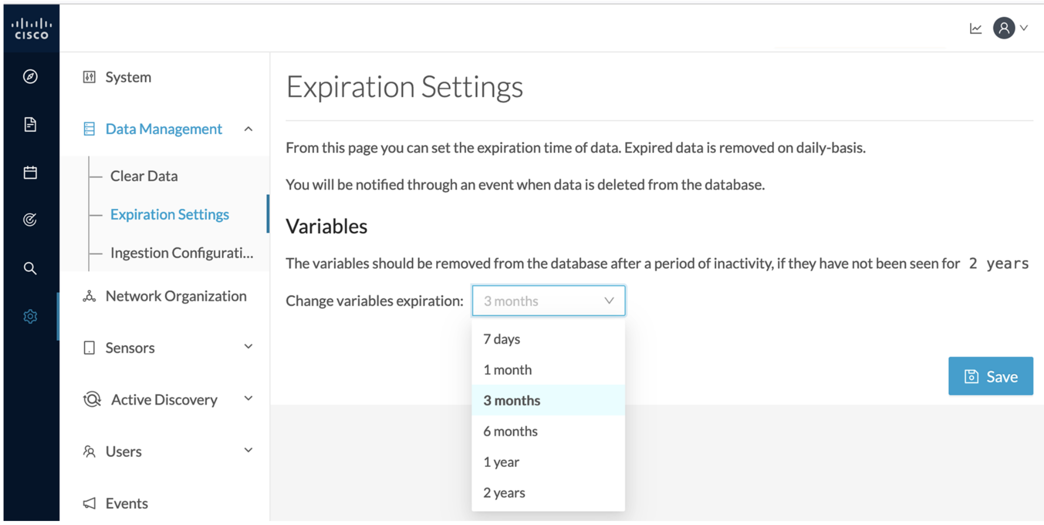
Step 3 Select which components to delete based on:

- the component type (External, IT or OT),
- their IP subnet,
- their inactivity,
- their creation time.

Step 4 Click **Clear data**.

Expiration settings

From this page, you can set data expiration time. Data is removed on a daily-basis once they expire. You can set an expiration time to variables for a period of 7 days, 1 month, 3 months, 6 months, 1 year or 2 years.



Expiration Settings

From this page you can set the expiration time of data. Expired data is removed on daily-basis.

You will be notified through an event when data is deleted from the database.

Variables

The variables should be removed from the database after a period of inactivity, if they have not been seen for `2 years`

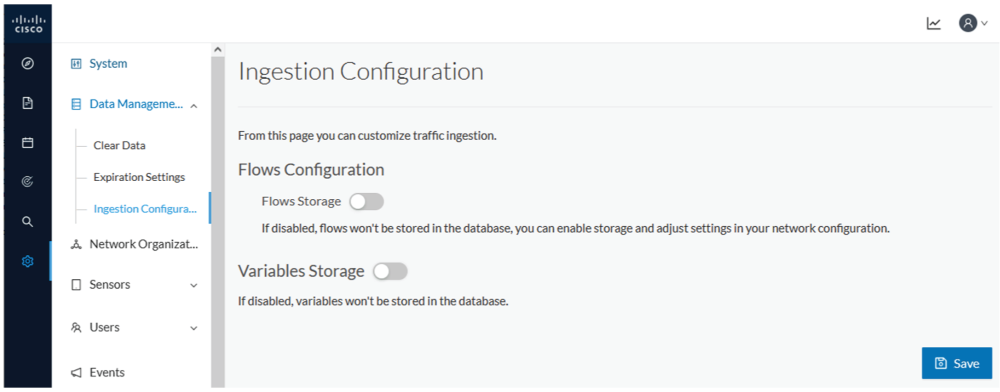
Change variables expiration: 3 months

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.



Ingestion Configuration

From this page you can customize traffic ingestion.

Flows Configuration

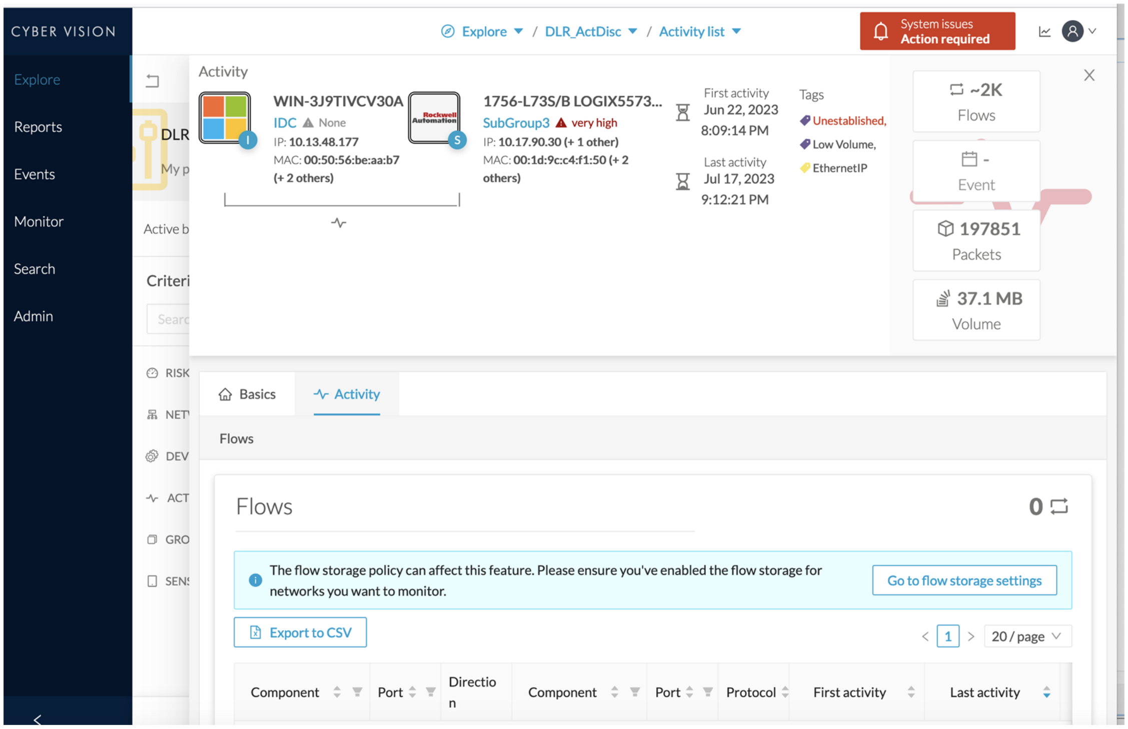
Flows Storage

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

Variables Storage

If disabled, variables won't be stored in the database.

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:

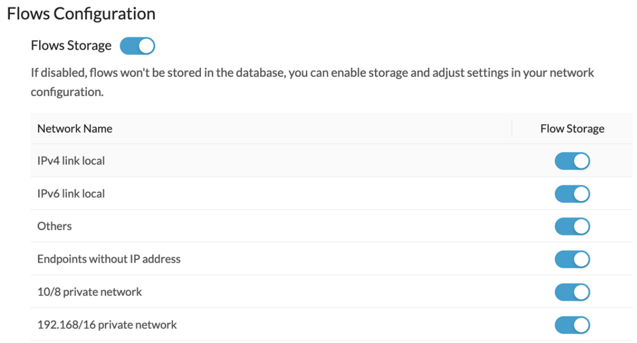


The flow storage policy can affect this feature. Please ensure you've enabled the flow storage for networks you want to monitor.

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

If 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.



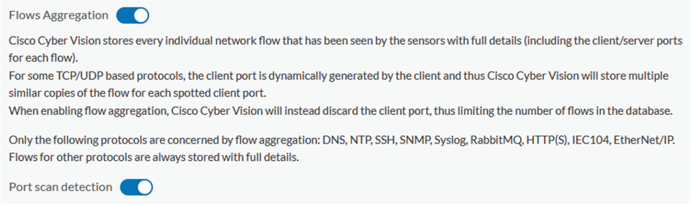
Flows Configuration

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	☑
IPv6 link local	☑
Others	☑
Endpoints without IP address	☑
10/8 private network	☑
192.168/16 private network	☑

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 ☑