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.

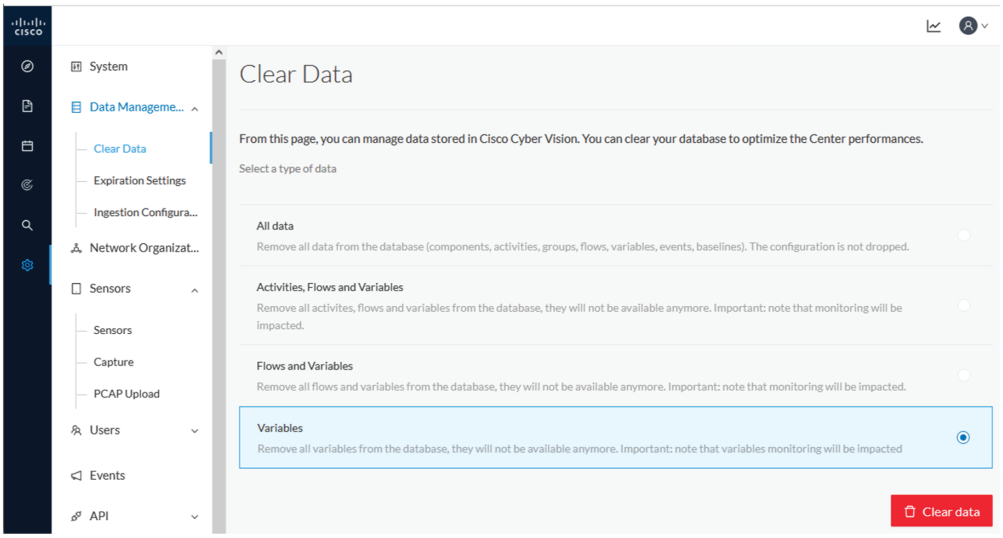
Clear data

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
- activities, flows and variables
- flows and variables
- variables

Clearing data should be performed carefully with the help of Cisco Cyber Vision product support and be used only as a last resort when all other troubleshooting attempts have failed. Clearing any data can impact monitoring of the network. Please read below all implications about all data clearance.



About all data clearance:

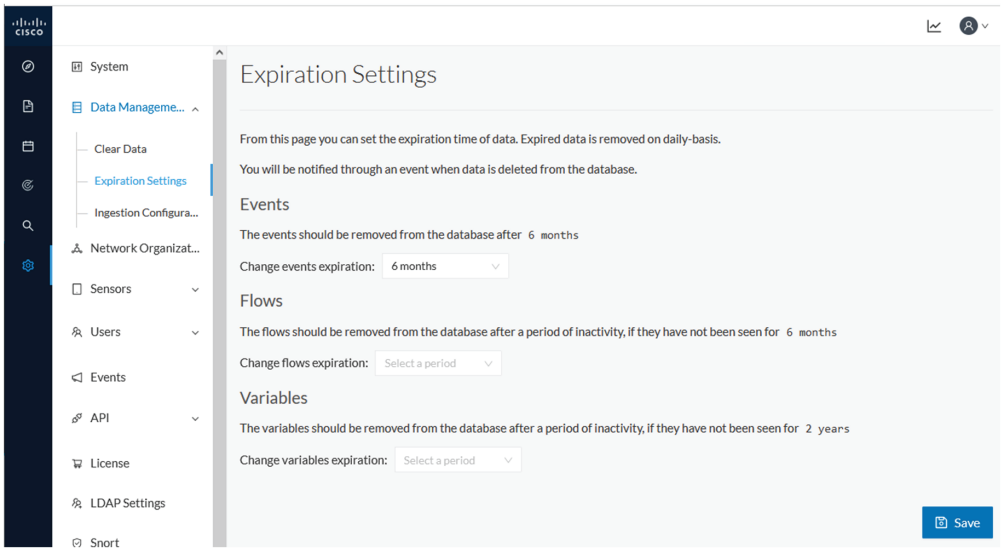
Clearing all data is to be used as a last resort in case of database overload issues.

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.

Expiration settings

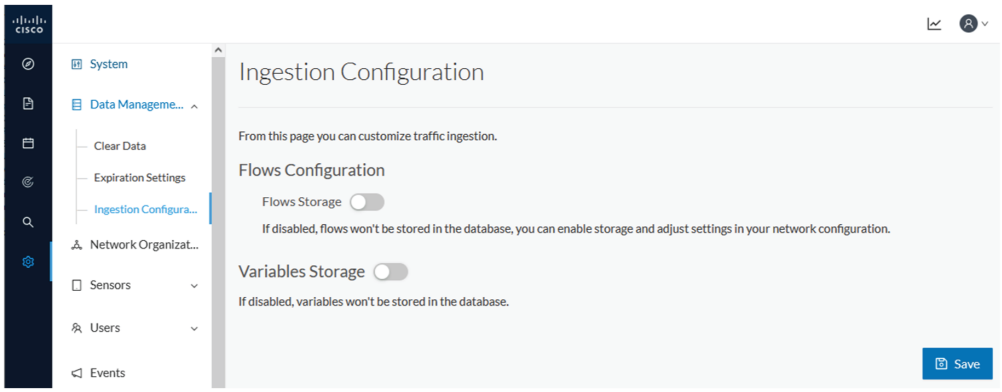
From this page, you can set data expiration time. Data is removed on a daily-basis once they expire. You can set an expiration time to events, flows and variables independently, and for a period of 7 days, 1 month, 3 months, 6 months or 1 year.



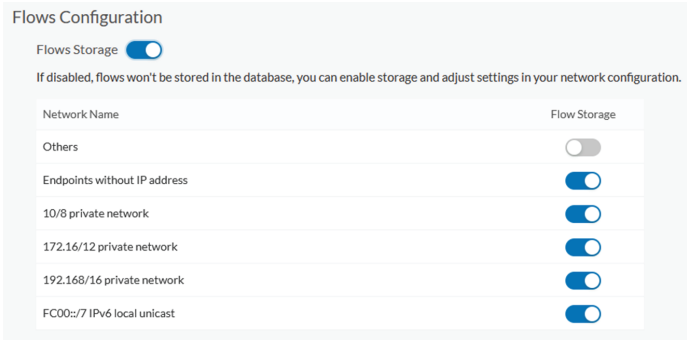
Ingestion configuration

The ingestion configuration page allows you to configure flow and variable traffic storage.

You can choose whether to store flows and variables.



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", that is, flows that are not part of the industrial private network, is disabled by default.



It is also possible to choose if enabling flows aggregation and port scan detection.