Configure Additional Storage

This section explains the following topic:

Configure Additional External Storage

Crosswork Service Health provides internal storage of monitored data up to a maximum limit of 50 GB. This data is stored on your system. If you exceed the limit of the internal storage, historical data will be deleted.

If you anticipate monitoring health of many services, Cisco recommends configuring external storage after you install Crosswork Service Health and before you begin monitoring the services. When the storage reaches 70% capacity, Crosswork Network Controller generates an alarm prompting you to configure external storage in order to save older Service Health monitoring data. If you do not configure external storage, the oldest files are deleted when 80% of 50 GB storage capacity is reached.

By leveraging external storage, all existing internal storage data will be automatically moved to the external cloud storage and your internal storage will act locally as cache storage. Configuring external storage for Crosswork Service Health ensures that you do not lose historical data for services that continue to monitor a service's health. Also, it ensures the service health data is retained for any service you choose to stop monitoring when you select the option to retain historical monitoring service for the data. For more information on how to retain the historical monitoring service data when stopped, see Stop Service Health Monitoring.

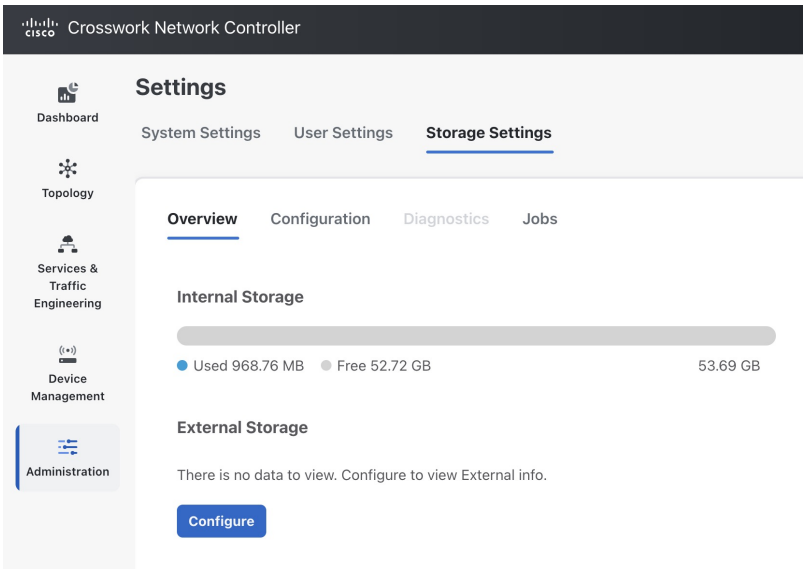
You can use an Amazon Web Services (AWS) cloud account to configure external storage in the cloud. Only AWS S3, which is object storage, is supported. The data is stored by Service Health in the tar.gz archive file format. This data includes the VPN service status at the time of storage and historical data about the service. Each tar.gz file represents an EoS (Event of Significance). Service Health uses this data to display it visually in the Crosswork Network Controller UI when you click on an EoS.

After you configure AWS storage, only 80% of the 50 GB space or 100,000 files are stored locally in Crosswork Network Controller. The oldest files are automatically moved to AWS.

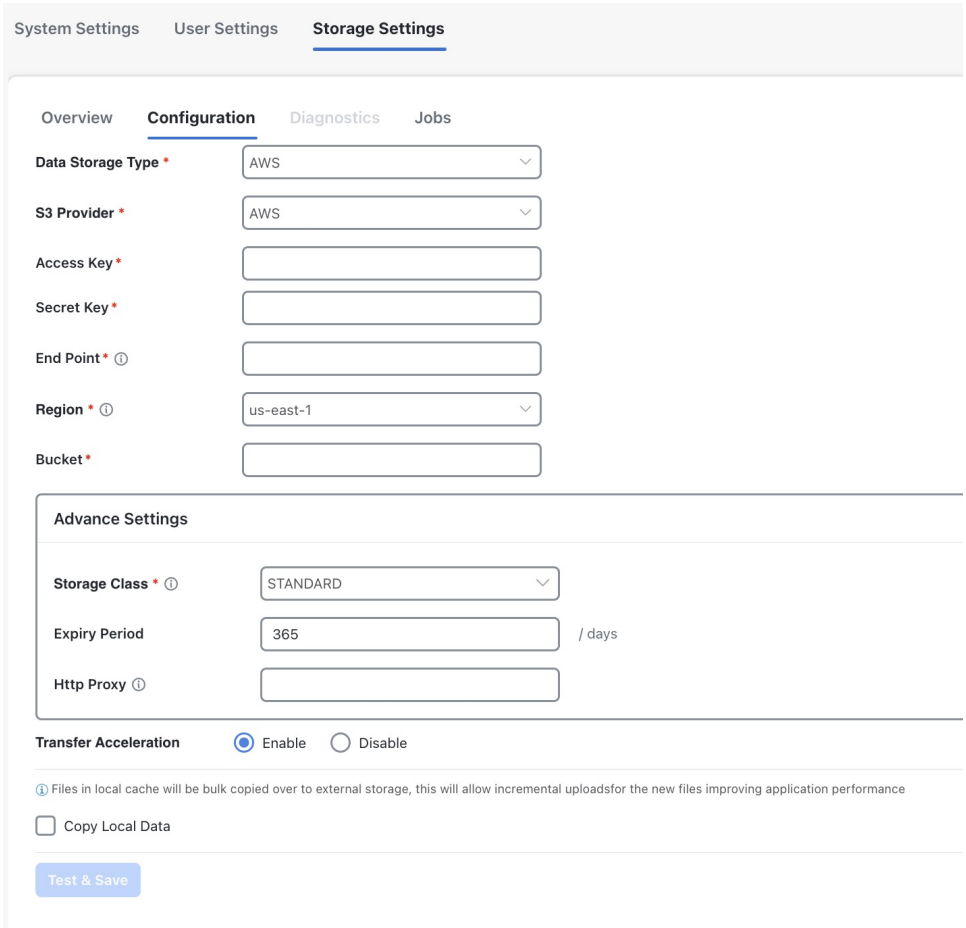
Before you begin

You must have an AWS cloud account set up so to configure the external storage.

Step 1 From the main menu, choose **Administration** > **Settings** and click the **Storage Settings** tab.



Step 2 With the Overview tab selected, click **Configure** under the **External Storage** section. The Configuration page appears with the Data Storage Type and S3 Provider fields pre-populated with AWS.



Step 3 Provide your AWS authentication information for all of the required fields (such as Access Key, Secret Key, End Point, and so on).

Step 4 Check the **Copy Local Data** check box if you want all files, previously stored in the local cache, to be bulk copied to the external storage. This action will allow for incremental upload of the new files.

Note This option is a one-time action when moving from only maintaining local storage and moving to external storage. This action also helps to improve the application performance.

Note The Expiry Period refers to the number of days that historical data files will be stored before being deleted. For example, if the Expiry Period is set to 1, the files will be deleted two days later, at midnight of the operational time zone of the second day.

Step 5 Click **Test & Save**.

Step 6 To check the health of your storage setup, click the **Diagnostics** tab and click **Run Test**.

By running a test, you can review the external storage diagnostics such as bandwidth, latency, and multiple access test details to help identify the possible storage performance issues.