

Data Storage

- Data Stored on the FMC, on page 1
- External Data Storage, on page 3

Data Stored on the FMC

For	See
General information about data storage on the FMC	The Disk Usage Widget
Purging old data	Purging Data from the FMC Database, on page 2
Allowing external access to the data on the FMC (this is an advanced feature)	External Database Access Settings
Backups	Manage Backups and Remote Storage and subtopics
Reports	Configuring Local Storage
Events	Connection Logging Database Event Limits and subtopics
Network discovery data	Network Discovery Data Storage Settings and subsequent topics
Files	Information about storing files in File Policies and Malware Protection, including best practices. File and Malware Inspection Performance and Storage Tuning
Packet data	Edit General Settings
Users and user activity	The Users Database The User Activity Database

Purging Data from the FMC Database

You can use the database purge page to purge discovery, identity, connection, and Security Intelligence data files from the FMC databases. Note that when you purge a database, the appropriate process is restarted.

Caution Purging a database removes the data you specify from the Firepower Management Center. After the data is deleted, it *cannot* be recovered.

Before you begin

You must have Admin or Security Analyst privileges to purge data. You can be in the global domain only.

Procedure

Step 1 Choose **System** > **Tools** > **Data Purge**.

Step 2 Under **Discovery and Identity**, perform any or all of the following:

- Check the **Network Discovery Events** check box to remove all network discovery events from the database.
- Check the **Hosts** check box to remove all hosts and Indications of Compromise flags from the database.
- Check the **User Activity** check box to remove all user activity events from the database.
- Check the **User Identities** check box to remove all user login and user history data from the database.

Step 3 Under **Connections**, perform any or all of the following:

- Check the **Connection Events** check box to remove all connection data from the database.
- Check the **Connection Summary Events** check box to remove all connection summary data from the database.
- Check the **Security Intelligence Events** check box to remove all Security Intelligence data from the database.

Note Checking the **Connection Events** check box does not remove Security Intelligence events. Connections with Security Intelligence data will still appear in the Security Intelligence event page (available under the Analysis > Connections menu). Correspondingly, checking the **Security Intelligence Events** check box does not remove connection events with associated Security Intelligence data.

Step 4 Click **Purge Selected Events**.
The items are purged and the appropriate processes are restarted.

External Data Storage

You can optionally use remote data storage for store certain types of data.

For	See
Backups	Manage Backups and Remote Storage and subtopics Remote Storage Management and subtopics
Reports	Remote Storage Management and subtopics Moving Reports to Remote Storage

Important If you will use syslog or store events externally, avoid special characters in object names such as policy and rule names. Object names should not contain special characters, such as commas, that the receiving application may use as separators.