Data Storage

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 Host 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, as well as User Indications of Compromise flags.

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
Events	Information about syslog and other resources in Event Analysis Using External Tools Remote Data Storage in the Stealthwatch Cloud, on page 4 Remote Data Storage on a Secure Network Analytics Appliance, on page 4 If you store connection events remotely, consider disabling storage of connection events on your FMC. For information, see Database Event Limits and subtopics.

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.

Comparison of Cisco Security Analytics and Logging Remote Event Storage Options

Similar but different options for storing event data externally to your FMC:

On Premises	SaaS
You purchase, obtain the license for, and set up the storage system behind your firewall.	You purchase licenses and a data storage plan and send your data to the Cisco Security Cloud.
Supported event types: • Connection • Security-related connection • Intrusion • File and Malware	Supported event types: • Connection • Security-related connection • Intrusion • File and Malware
Send events to storage via syslog.	Send events to storage via syslog.

On Premises	SaaS
View events using your Secure Network Analytics Manager appliance. Cross-launch from FMC event viewer.	View events in CDO or Secure Network Analytics, depending on your license. Cross-launch from FMC event viewer.
For more information, see the links in Remote Data Storage on a Secure Network Analytics Appliance, on page 4.	For more information, see the links in Remote Data Storage in the Stealthwatch Cloud, on page 4.

Remote Data Storage in the Stealthwatch Cloud

Send select Firepower event data via syslog to the Secure Network Analytics Cloud using Cisco Security Analytics and Logging (SaaS). Supported events: Connection, Security Intelligence, intrusion, file, and malware.

For details, see the *Firepower Management Center and Cisco Security Analytics and Logging (SaaS) Integration Guide* at https://cisco.com/go/firepower-sal-saas-integration-docs.

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.

Remote Data Storage on a Secure Network Analytics Appliance

If you require more data storage than your Firepower appliance can provide, you can use Cisco Security Analytics and Logging (On Premises) to store Firepower data on a Secure Network Analytics appliance. For complete information, see the documentation available from https://cisco.com/go/sal-on-prem-docs.

Optionally, to pivot quickly from events in FMC to related events in Secure Network Analytics, see Configure Cross-Launch Links for Secure Network Analytics and Investigate Events Using Contextual Cross-Launch.

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.

History for Data Storage

Feature	Version	Details
Remote data storage on a Secure Network Analytics appliance	6.7	You can now store large volumes of Firepower event data remotely, using Cisco Security Analytics and Logging (On Premises). When viewing events in FMC, you can quickly cross-launch to view events in your remote data storage location. Supported events: Connection, Security Intelligence, intrusion, file, and malware. Events are sent usin syslog. This solution depends on availability of Stealthwatch Management Console (SMC) Virtual Edition running Stealthwatch Enterprise (SWE) version 7.3. See Remote Data Storage on a Secure Network Analytics Appliance, on page 4.
Remote data storage in the Secure Network Analytics Cloud	6.4	Use syslog to send select Firepower data using Cisco Security Analytics and Logging (SaaS). Supporte events: Connection, Security Intelligence, intrusion, file, and malware. For details, see the *Firepower Management Center and Cisco Security Analytics and Logging (SaaS Integration Guide* at https://cisco.com/go/firepower-sal-saas-integration-docs.