Data Purge and 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
Backups	Manage Backups and Remote Storage and subtopics
Reports	Configure Local Storage
Events	Connection Logging Database and subtopics
Network discovery data	*Network Discovery Data Storage Settings* and subsequent topics in the Firepower Management Center Device Configuration Guide
Files	Information about storing files in the *Network Malware Protection and File Policies* chapter of the Firepower Management Center Device Configuration Guide, including best practices. *Tuning File and Malware Inspection Performance and Storage* Firepower Management Center Device Configuration Guide
Packet data	*Edit General Settings* in the Firepower Management Center Device Configuration Guide

For	See
Users and user activity	*The Users Database* in the Firepower Management Center Device Configuration Guide *The User Activity Database* in the Firepower Management Center Device Configuration Guide

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 FMC. After the data is deleted, it *cannot* be recovered.

Before you begin

You must have Admin or Security Analyst privileges to purge data. To perform this action, you must be in the global domain.

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 > **Security Intelligence Events** 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 Device and subtopics
Reports	Remote Storage Device and subtopics Moving Reports to Remote Storage
Events	Information about syslog and other resources in Event Analysis Using External Tools Remote Data Storage in Cisco Secure Cloud Analytics, 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 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 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, license, and set up the storage system behind your firewall.	You purchase licenses and a data storage plan and send your data to the Cisco cloud.

On Premises	SaaS
Supported event types: • Connection • Security Intelligence • Intrusion • File and Malware • LINA	Supported event types: • Connection • Security Intelligence • Intrusion • File and Malware
Supports both syslog and direct integration.	Supports both syslog and direct integration.
• View all events on the Secure Network Analytics Manager. • Cross-launch from FMC event viewer to view events on the Secure Network Analytics Manager. • View remotely stored connection and Security Intelligence events in FMC	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 Cisco Secure Cloud Analytics, on page 4.

Remote Data Storage in Cisco Secure Cloud Analytics

Send select Firepower event data to Secure Cloud Analytics using 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*.

You can send events either directly or via syslog.

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 Security Analytics and Logging (On Premises) to store Firepower data on a Secure Network Analytics appliance. For complete information, see the documentation available from Cisco Security Analytics and Logging.

You can view connection events in FMC even if they are stored on a Secure Network Analytics appliance. See Work in Firepower Management Center with Connection Events Stored on a Secure Network Analytics Appliance.

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	Minimum FMC	Minimum FTD	Details
Exempt low priority connection events from event rate limits	7.0	Any	If you choose not to store connection events on the FMC because you are storing them on a remote volume, those events do not count towards the flow rate limits for your FMC hardware device. If you send events to Security Analytics and Logging (On Premises) using the new 7.0 configurations, you configure this setting as part of that integration. Otherwise, see information about the Connection Database in Database Event Limits. New/Modified pages: None. Behavior change only.
Improved process for sending events to a Secure Network Analytics appliance	7.0	Any	A new wizard streamlines sending events directly to a Secure Network Analytics appliance using Security Analytics and Logging (On Premises). The wizard also allows you to see remotely stored connection events while viewing event pages on your FMC, and to cross-launch from FMC to view events on your Secure Network Analytics appliance. If you have already configured your system to send events using syslog, events will continue to be sent using syslog unless you disable those configurations. For details, see the documentation referenced in Remote Data Storage on a Secure Network Analytics Appliance, on page 4. New/Modified pages: The **System** > **Logging** > **Security Analytics & Logging** page now displays the wizard instead of the configuration for creating cross-launch options.

Feature	Minimum FMC	Minimum FTD	Details
Remote data storage on a Secure Network Analytics appliance	6.7	Any	You can now store large volumes of Firepower event data remotely, using 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 using 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 Cisco Secure Cloud Analytics	6.4	Any	Use syslog to send select Firepower data using 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.