

# Data Purge and Storage

Data purge and storage is a system management process that controls the retention, archiving, and removal of historical configuration data and operational logs within the management environment.

- Categorization of remote data storage options.
- Management of historical configuration updates.
- Tracking of feature deprecations and enhancements.


- Data stored on the Firewall Management Center, on page 1
- External data storage, on page 3
- History for data storage, on page 5


# Data stored on the Firewall Management Center

This reference provides information about the various types of data stored on the Firewall Management Center and directs you to relevant documentation for managing each data type.

| For | See |
|---|---|
| General information about data storage on the Firewall Management Center | Disk usage widget categories and features |
| Purging old data | Purge data from the Firewall Management Center Database , on page 2 |
| Allowing external access to the data on the Firewall Management Center (this is an advanced feature) | External database access |
| Backups | Manage backups and remote storage and subtopics |
| Reports | Configure local storage |
| Events | Connection Logging<br>Database and subtopics |

| For | See |
|---|---|
| Network discovery data | *Network Discovery Data Storage Settings* and subsequent topics in the *Cisco Secure Firewall Management Center Device Configuration Guide* |
| Files | Information about storing files in the *Network Malware Protection and File Policies* chapter of the *Cisco Secure Firewall Management Center Device Configuration Guide*, including best practices.<br>*Tuning File and Malware Inspection Performance and Storage* *Cisco Secure Firewall Management Center Device Configuration Guide* |
| Packet data | *Edit General Settings* in the *Cisco Secure Firewall Management Center Device Configuration Guide* |
| Users and user activity | *The Users Database* in the *Cisco Secure Firewall Management Center Device Configuration Guide*<br>*The User Activity Database* in the *Cisco Secure Firewall Management Center Device Configuration Guide* |

# Purge data from the Firewall Management Center Database

Use the database purge page to purge discovery, identity, connection, and security intelligence data files from the Firewall Management Center databases. Note that the respective processes restart with purging.

**Caution** Purging a database removes the data you specify from the Firewall 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. Perform this action in the global domain.

Follow these steps to purge data from the Firewall Management Center database:

**Procedure**

**Step 1** Choose **System** (⚙) > **Tools** > **Data Purge**.

**Step 2** Under **Discovery and Identity**, perform any or all of these actions:

- 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 these actions:

- 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**.
Once the items are purged, the appropriate processes restart.

The selected data types are permanently removed from the Firewall Management Center database to optimize storage and performance.

# External data storage

Remote data storage supports storing data under different categories. The classification is as follows:

| For | See |
|---|---|
| Backups | Manage backups and remote storage and subtopics<br>Remote storage devices and subtopics |
| Reports | Remote storage devices and subtopics<br>Moving reports to remote storage |
| Events | Information about syslog and other resources in Event Analysis Using External Tools<br>Remote data storage in Cisco Secure Cloud Analytics, on page 4<br>Remote data storage on a Secure Network Analytics appliance, on page 5<br>If you store connection events remotely, consider disabling storage of connection events on your Firewall Management Center. 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

Different options for storing event data externally to your Firewall Management Center:

| 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. |
| **Supported event types:**<br>• **Connection**<br>• **Security Intelligence**<br>• **Intrusion**<br>• **File and Malware**<br>• **LINA** | Supported event types:<br>• Connection<br>• Security Intelligence<br>• Intrusion<br>• File and Malware |
| **Supports both syslog and direct integration.** | Supports both syslog and direct integration. |
| • **View all events on the Secure Network Analytics Manager.**<br>• **Cross-launch from FMC event viewer to view events on the Secure Network Analytics Manager.**<br>• **View remotely stored connection and Security Intelligence events in FMC** | View events in Security Cloud Control 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 5**.** | 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

Remote data storage in Cisco Secure Cloud Analytics is a security data management capability that

- sends select Secure Firewall event data to Secure Cloud Analytics using Security Analytics and Logging (SaaS),
- supports connection, Security Intelligence, intrusion, file, and malware events, and
- allows event transmission either directly or via syslog.

### Additional information

For more information, refer to *Secure Firewall Management Center and Cisco Security Analytics and Logging (SaaS) Integration Guide*.

**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

A remote data storage on a Secure Network Analytics appliance is a storage solution that

- provides additional data storage capacity when your Secure Firewall appliance storage is insufficient
- uses Security Analytics and Logging (On Premises) to store Secure Firewall data externally, and
- allows you to view connection events in Firewall Management Center even when data is stored remotely.

### Remote data storage capabilities

You can view connection events in Firewall Management Center even if they are stored on a Secure Network Analytics appliance. See Work in Firewall Management Center with connection events stored on a Secure Network Analytics appliance.

For complete information, see the documentation available from Cisco Security Analytics and Logging.

**Note** 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

This reference details the historical updates in data storage functionalities and configurations. It provides insights into deprecated and improved features across various product versions.

| Feature | Minimum Firewall Management Center | Minimum Firewall Threat Defense | Details |
|---|---|---|---|
| Exempt low priority connection events from event rate limits | 7.0 | Any | If you choose not to store connection events on the Firewall Management Center because you are storing them on a remote volume, those events do not count towards the flow rate limits for your Firewall Management Center hardware device.<br><br>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.<br><br>Otherwise, see information about the Connection Database in Database event limits.<br><br>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).<br><br>The wizard also allows you to see remotely stored connection events while viewing event pages on your Firewall Management Center, and to cross-launch from Firewall Management Center to view events on your Secure Network Analytics appliance.<br><br>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.<br><br>For details, see the documentation referenced in Remote data storage on a Secure Network Analytics appliance, on page 5.<br><br>New/Modified pages: The **System** > **Logging** > **Security Analytics & Logging** page now displays the wizard instead of the configuration for creating cross-launch options. |
| 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 Firewall Management Center, you can quickly cross-launch to view events in your remote data storage location.<br><br>Supported events: Connection, Security Intelligence, intrusion, file, and malware. Events are sent using syslog.<br><br>This solution depends on availability of Stealthwatch Management Console (SMC) Virtual Edition running Stealthwatch Enterprise (SWE) version 7.3.<br><br>See Remote data storage on a Secure Network Analytics appliance, on page 5. |
| 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.<br><br>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. |