Archiving Forcepoint DLP Incident Data

Archiving Incident Forensics | Forcepoint DLP | v8.4.x, v8.5.x, v8.6.x, v8.7.x

To free storage space for new incidents and forensics records, older records can be moved to an archive partition.

This can either be done manually (see *Manual archiving*, page 2) or via an automatic process triggered when a certain threshold is reached (see *Automatic archiving*, page 3).

Each archive partition contains records for a 91-day interval. Up to 25 accessible partitions (6 years and 1 month) are supported, stored in the following groups: Active, Online, Restored, and Archived.

Partition type	Microsoft SQL Server Standard or Enterprise	SQL Server Express
Active	1 partition (current quarter)	1 partition (current quarter)
Online	up to 8 partitions (2 years)	up to 4 partitions (1 year)
Restored	up to 4 partitions (1 year)	up to 4 partitions (1 year)
Archived	up to 12 partitions (3 years)	up to 12 partitions (3 years)
Total	**25**	**21**

- View and manage partitions on the **Settings > General > Archive Partitions** page in the Forcepoint Security Manager.
- Manage the size of the forensics repository on the **Settings > Deployment > System Modules** page. Select the repository to configure its properties, including its maximum size.
- Manage the size of the archive folder on the **Settings > General > Archive Storage** page.

Manual archiving

Administrators can manually initiate archiving for a partition. This archives all incident records and their forensics data from that 91-day period. This archiving method is called public, because Forcepoint DLP administrators can view and restore the manually archived records.

If an administrator archives a partition that has already—in whole or in part—been automatically archived, the previously archived records are merged into the manual archive (see *Automatic archiving*, page 3). These records are now also available to Forcepoint DLP administrators for viewing and restoring. The original (automatically-created) copies of all merged records are then deleted to conserve disk space.

When an administrator triggers an archiving operation, an archiving record ID number is issued. This can be used to restore the archive (see *Archive formatting and restoration*, page 5).

To initiate manual archiving:

1. Log on to the Data Security module of the Security Manager.
2. Go to the **Settings > General > Archive Partitions** page.
3. Select one or more partitions.
4. Click **Archive** in the toolbar at the top of the page.
5. Optionally add comments.
6. Click **OK**.

See the Forcepoint DLP Administrator Help for more information.

Automatic archiving

Automatic archiving occurs when there are too many incident partitions, or when there is insufficient disk space for the forensics repository.

When there are too many online partitions

The incident database has one active partition and stores up to 8 partitions online.

When a new active partition is created after the 91-day period, the old active partition changes to online status.

When the maximum number of online partitions has been reached, the oldest partition is archived.

- Both incidents and their forensics data are archived.
- Forcepoint DLP administrators can view and restore the archived partitions.

When there is not enough disk space

When the forensics repository consumes 100 percent of the allotted space (50 GB, by default), a notification is issued, and archiving occurs automatically.

- Automatic archiving starts with the oldest records and continues archiving until at least 15 percent of the allotted disk space is free.
- Archiving includes forensics data, but not incidents.

When this type of automatic archiving is initiated, the system checks to see whether the newly archived data will cause the archive folder to exceed its designated maximum size (50 GB, by default).

- If the addition of new records will make the folder too large, the oldest automatically archived records are deleted to free 10 percent of the archive folder's maximum size.
- If 10 percent of the allotted space cannot be made available by deleting automatically archived records, a system log message (with a severity of "warning") is issued.

Configure the size of the archive folder on the **Settings > General > Archive Storage** page in the Security Manager.

Automatically archived records created when there is not enough disk space are considered private. Forcepoint DLP administrators cannot see them.

These archives:

- Cannot be restored by the administrator, even though they are stored in the same place

- Are stored in a format that can be restored by Forcepoint Technical Support

  The Technical Support representative can also identify the creation dates of archived records.

Threshold alerts

An alert is sent when the forensics repository approaches or reaches the maximum alloted disk space (50 GB, by default).

Configure the maximum size of the forensics repository on the **Settings > Deployment > System Modules** page in the Security Manager.

The following alerts are issued once each time the thresholds are surpassed.

- Disk space usage crossed X% of allowed space

  Two alerts of this type are issued: one at 80% and one at 90%, by default. At crossing the first threshold, the alert severity is “information.” At the second threshold, the severity is “warning.”
- Disk space usage crossed 100% of allowed space, some records were automatically archived

  The severity of this alert is “warning.”

Administrators can also configure alerts to be sent when the archive disk space approaches its limit. This is done on the **Settings > General > Alerts** page.

Archive formatting and restoration

Archived records are stored in a subfolder of the archive folder. They can be restored using their record ID number.

Archive record format

When incident records are archived, they have the same disk layout as when in the database. The archived records are stored in a subfolder of the archive folder. The folder name is in the following format: FR-ARC-YYYYMMDD-yyyymmdd-xxx[-id]

- YYYYMMDD is the date of the oldest record in the archive (i.e., 20000910).
- yyyymmdd is the date of the newest record in the archive.
- xxx is the size, in bytes, that the archive occupies in the repository.
- id is an optional archive record ID for user-triggered archives.

Note that archives are stored at the resolution of one full day.

Restoring an archive

Manually created archives can be restored using the archiving record ID number:

1. Log on to the Data Security module of the Security Manager.
2. Go to the **Settings > General > Archive Partitions** page.
3. Select one or more archived partitions.
4. Click **Restore** in the toolbar at the top of the page.
5. Click **OK** in the confirmation dialog box.

Before restoring an archive, the system checks the total disk space needed. If the required space exceeds 95 percent of the maximum allotted space, the action is canceled.

When the restore operation is successfully completed, the records are deleted from the archive folder. A maximum of 4 restored archives can be online at the same time. Restored archives are not counted toward the maximum 8 online partitions or 12 archived partitions.

See Forcepoint DLP Administrator Help for more information.