Archiving incident forensics

Topic 80000/ Updated: 26-Aug-2014

Applies To:	Websense Data Security v7.6.x, v7.7.x, and v7.8.x

What is an archive?

On occasion, you may want to place forensics records in an archive to free storage space for new records. In the Data Security manager, you can manually request that records be archived, or you can set a threshold (maximum repository size) that, when surpassed, automatically triggers the archiving process.

Select **Settings > Archive** to archive, restore, or delete a partition.

Select **Settings > System** > **Archive Storage** to configure the threshold.

Related topics:

- *Automatic archiving*
- *Manual archiving*

Partition limits

Incidents are archived in partitions. Each partition contains records for a 91-day interval. Up to 25 accessible partitions (6 years and 1 months) are supported, stored in the following groups:

- Active
- Online
- Restored
- Archived

If you are using Microsoft SQL Server Standard or Enterprise for your TRITON database, you can have a maximum of 8 online partitions (approximately 2 years).

If you are using SQL Server Express, you can have 1 active partition for the current quarter. In addition, you can have up to 4 online partitions (approximately 1 year), 4 restored partitions (1 year), and 12 archived partitions representing 3 years of records.

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 available managed partitions	**25**	**21**

Automatic archiving

There are two scenarios in which incidents are automatically archived:

1. When there are too many partitions

As specified in the Partition limits section, depending on the server type, the forensics repository stores up to 8 partitions online, and 1 active partition. When a new active partition is created after the 91-day period, the old active partition is designated **online**. If the maximum designated **online** partition has been reached when the new active partition is created, then the oldest partition is archived. There archived records can be viewed and restored by the user.

2. When there is not enough disc space

The size of the forensics repository is capped by a maximum value. When the repository consumes 100 percent of that allowed space, a system logging notification is issued, and archiving is automatically initiated. Automatic archiving starts with the oldest records, and continues archiving until at least 15 percent of the allowed disk space is free. This action is triggered every time the repository reaches 100 percent of its allowed space. This is not visible to the user. All records archived in this manner retain **online** status and are still accessible to the user.

When an automatic archiving operation is initiated, the system verifies that the newly archived records will not cause the archive folder to exceed its designated maximum size. If so, the oldest automatically archived records will be deleted to free 10 percent of the archive folder's maximum size. If 10 percent cannot be made available, by deleting automatically archived records, a system log message (With a severity of **warning**) is issued.

These archived records are considered private, in that the user cannot see them, and cannot restore them. Unlike user-initiated archiving, these archives cannot be restored by the user, but are stored in the same place. These records must be stored in a format that can be restored by a Sales Engineer. A Sales Engineer must also be able to identify the creation dates of archived records. They are only available for restoration by the user if they were merged into a public archive by a user-triggered archiving operation.

Select **Settings > System** > **Archive Storage** to configure the maximum repository size.

Manual archiving

You can initiate an archiving operation on a partition. This archives all incident data records from that 91-day period. This archiving method is called public, because you can view and restore these records once they are archived. If you choose to archive a partition— some or all of which have already been automatically archived—the previously archived records are merged into the manual archive. These records are now also available to you for viewing and restoring. The original copies of all merged records are then deleted to conserve disk space.

When you trigger an archiving operation, an archiving record ID number is issued which you can use to restore this record.

To initiate archiving manually, select **Settings > Archive** in the Data Security manager, and select the **Archive** button.

See Data Security Manager Help for more information.

Threshold alerts

The default repository size is 50 GB, though this is configurable.

By default, the maximum archive size is 40 GB. This is also configurable. (Select **Settings > System** > **Archive Storage**.)

The Incident Repository issues the following alerts when these thresholds are surpassed. Each alert is issued once each time the threshold is surpassed.

- "Disk space usage crossed X% of allowed space": Two alerts of this type are issued. One for crossing each designated disk space threshold (first is 80 and second is 90, by default). At crossing the first threshold the severity of the alert is **information**. At the second threshold the severity is **warning**.
- "Disk space usage crossed 100% of allowed space, some records were automatically archived, a user": The severity of this alert is **warning**.

You can configure alerts to be sent when the archive disk space approaches its limit as well. To do so, navigate to **Settings > System > Alerts** in the Data Security manager.

Archive format

When incident records are archived, they are stored in the same disk layout as they are in the repository 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 - The date of the oldest record in the archive (i.e, 20000910)
- yyyymmdd - The date of the newest record in the archive
- xxx - The size, in bytes, that the archive occupies in the repository
- id - An optional, archive record id for the user-triggered archives (see below)

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

Archive restoration

If necessary, you can restore manual archives using the archiving record ID number.

To do so, select **Settings > Archive** in the Data Security manager.

Before restoring an archive, the system checks the total disk space that would be consumed, were the archive restored. If that exceeds 95 percent of the maximum allowed space, the action is canceled. Once the restore operation is successfully completed, the archived 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 Data Security Manager Help for more information.