File Analysis Suite

Software Version 3.7.0

Frequently Asked Questions

MICRO FOCUS

Document Release Date: May 2022
Software Release Date: May 2022

Legal notices

Contents

Get started

This document addresses frequently asked questions about File Analysis Suite.

About File Analysis Suite

Micro Focus File Analysis Suite lets you find, protect, and secure sensitive and high-value data within on-premises and cloud unstructured data repositories across your enterprise. Identify, collect, and organize content to ensure discovery of sensitive data. Configure how sources and repositories are processed and categorized with Connect. Analyze your data under management with Analyze. Organize, review, and take action with Manage.

3.7.0.20220601

Security

The following FAQs address security questions.

How is the File Analysis Suite environment secured in AWS (Amazon Web Services)?

Back office implementations follow industry standard security practices. including but not limited to:

- **All** incoming communication (from web users, on-premises agents, FTP clients, and so on) is transmitted exclusively via TLS 1.2+ using only high strength cipher suites (Encryption in Transit).
- Object and volume storage containing non-ephemeral data is encrypted using the industry standard AES-256 algorithm (Encryption at Rest).
- Industry standard Principle of least privilege (PoLP) is consistently applied. This is applied within the application, as well as within the back office (governing access to infrastructure resources, limiting intra-back office communications, and so on).

Consult the available Service Description documentation for more information.

File Analysis Suite is multi tenanted. What protects my data from being seen by others?

Individual tenant data is stored in separate indexes and object storage locations.

Does File Analysis Suite backup the indexes, and if so for how long are the indexes kept?

Yes, the indexes are backed up. Consult the available Service Description documentation for more information.

What metadata is copied to the cloud ?

When objects are captured by the File Analysis Suite processing agent, the extracted content and relevant metadata is transmitted to the back office for further enrichment. The end results are then held in index storage within the back office.

Optionally, you may elect to also collect data (either by choice or to enforce a hold). In this case, a copy of the original data object is then also transmitted to the back office, which will be held in object storage within the back office.

What security is in place for transferring data from cloud repositories? From agent repositories?

File Analysis Suite processing agents performing data capture and collection follow the same security procedures, regardless of the repository type.

1. During configuration, the tenant provides information about the repository type, path to the repository, and access credentials. This information makes up a repository's definition, which is used to reach the repository. Repository definitions are encrypted and held securely within the back office.

2. An agent system connects to the back office and retrieves any pending tasks that have been delegated to it.
3. The repository definition is provided to the authorized agent for use only when performing the specific task.
4. Data captured/collected is then transferred by the agent to the back office.

This applies to both individual private tenant on-premises agents and repositories assigned to be managed by cloud to cloud (C2C) agents operated from within the back office.

On-premises agents can operate on repositories that may only be available to the particular private customer system (such as, file system, private Exchange) or public locations (such as, SharePoint Online, Office 365) if the customer permits access to those.

C2C agents are restricted to exclusively operate on those repository types that can be reached through public locations (such as, SharePoint Online, Office 365).

File access

The following FAQs address questions about accessing files under management.

What are the file path restrictions for File System sources and repositories?

Files whose full accessed share path exceeds 255 characters will not be accessible.

For File System **sources**, the following limitations exist.

- The source path cannot be more than a single directory beyond the host. For example, `\\server01.domain.com\folderA`. Further path refinement is defined by repositories.
- The hostname portion of the source path can contain only the following characters.
  - upper and lowercase alpha-numeric characters
  - `.` (period)
  - `-` (dash)
  - `_` (underscore)
- The source path cannot contain any of the following special characters.
  - `<` (less than)
  - `>` (greater than)
  - `:` (colon)
  - `"` (double quote)
  - `|` (vertical bar or pipe)
  - `?` (question mark)
  - `*` (asterisk)
  - `/` (forward slash)
- Files whose full accessed share path exceeds 255 characters will not be accessible.
- The path cannot contain `.` or `..` before, after, or in between slashes (`\`) with no other characters.
  - Not valid:

    `\\company.domain.com\..` `\\company.domain.com\.`

  - Valid:

    `\\company.domain.com\abc..` `\\company.domain.com\.abc`

For file system **repositories**, the following limitations exist.

- The sub-directory path cannot contain any of the following special characters.
  - < (less than)
  - > (greater than)
  - : (colon)
  - " (double quote)
  - | (vertical bar or pipe)
  - ? (question mark)
  - * (asterisk) / (slash)
- Files whose full accessed share path exceeds 255 characters will not be accessible.
- The path cannot contain `.` or `..` before, after, or in between slashes (\) with no other characters.
  - Not valid:

    ```
    \..\        \.\abc        \abc\..        \abc\.\def
    ```

  - Valid:

    ```
    \abc..        \.abc        \abc\def.        \abc\.def\gh
    ```

What are the file path restrictions for File System targets and destinations?

Avoid hidden or system level CIFS share (such as, `\\server01\c$\folderA`).

Files whose full accessed share target and destination path exceeds 255 characters will not be accessible on the destination.

Processing and processing agent

The following FAQs address questions about file processing and the processing agent.

The task status on the Agent Activity page in Connect is listed as "waiting". What does this mean?

Some tasks require multiple processes, or steps, to complete and the task requested is in between steps and waiting to be picked up for the next step. For example, you want to send the items in a workbook to a target. For the items in this workbook, only the metadata was indexed and the source repository and destination are managed by different agent clusters. In this scenario, the items must be collected before they can be sent to the defined target. This task may show a "waiting" task status after the items are collected as the task waits to be picked up to send the items to the target.

The assigned agent may not be reachable. If the task status remains "waiting", ensure that the agents in the agent cluster assigned to the task are running and accessible. Specifically, verify that the agentAPI service is running on the agent host assigned to perform the task.

The Custom installation for the processing agent fails during the database installation and then rolls back. Why is this happening?

If you are located in a region that typically uses a character set other than Latin, your SQL Server installation most likely defaults to a collation other than what is supported by the processing agent.

When installing SQL Server, you must set the server collation to **SQL_Latin1_General_CP1_CI_AS**.

Re-install SQL Server with the supported collation defined. Proper collation must be set during installation because it cannot be changed after SQL Server is installed.

How are deleted items tracked in File Analysis Suite?

File Analysis Suite tracks file deletions when a processing job runs against a File Analysis Suite repository. A job run occurs when a repository is updated, either run on a schedule or manually updated from the Manage Repositories page in Connect (click the inline update icon for the repository or the Update button in the repository detail panel).

File systems

File Analysis Suite tracks file deletions by directly comparing with the original file system location identified by the repository path. Items are removed from the File Analysis Suite index seven days after the deletion is detected. If an item within a container file (such as ZIP) is deleted in the original file system location, the item is removed from the index as part of updating the container file when the File Analysis Suite job run occurs. In this case, the item may be removed from File Analysis Suite sooner than seven days after deletion is detected.

Exchange

No deletion detection from Exchange. File Analysis Suite retains items it has already processed until a delete action is initiated from File Analysis Suite.

SharePoint

File Analysis Suite tracks the deletion of managed SharePoint items using the SharePoint change logs. Each time processing is run on a repository—on a schedule, or on demand—File Analysis Suite checks the SharePoint logs for deleted items. For each managed item that is deleted in SharePoint, File Analysis Suite deletes that item from the File Analysis Suite index. If an item within a container file (such as ZIP) is deleted in SharePoint, the item is removed from the index as part of updating the container file when the File Analysis Suite job run occurs.

To ensure accurate tracking of items deleted from SharePoint, ensure that the SharePoint repositories in File Analysis Suite are updated more often than the maximum number of days SharePoint logs are kept. For example, if your SharePoint logs are configured to be stored for 60 days, verify that your SharePoint repositories are updated at least every 59 days.

Content Manager

File Analysis Suite tracks the deletion of managed Content Manager items using the Content Manager delete events. Each time processing is run on a repository—on a schedule, or on demand—File Analysis Suite checks the delete events. For each managed item that is deleted in Content Manager, File Analysis Suite deletes that item from the File Analysis Suite index. If an item within a container file (such as ZIP) is deleted from Content Manager, the item is removed from the index as part of updating the container file when the File Analysis Suite job run occurs.

To ensure accurate tracking of items deleted from Content Manager, ensure that the Content manager repositories in File Analysis Suite are updated more often than Content Manager administrator purges delete events. For example, if your Content Manager administrator purges delete events every 60 days, verify that your Content Manager repositories are updated at least every 59 days.

Google Drive

File Analysis Suite tracks the deletion of managed Google Drive items using the change log for the Google drive defined by the File Analysis Suite repository. Each time processing is run on a repository—on a schedule, or on demand—File Analysis Suite checks the change logs for deleted items. For each managed item that is deleted in Google Drive, File Analysis Suite deletes that item from the File Analysis Suite index. If an item within a container file (such as ZIP) is deleted in Google Drive, the item is removed from the index as part of updating the container file when the File Analysis Suite job run occurs.

To ensure accurate tracking of items deleted from Google Drive, ensure that the Google Drive repositories in File Analysis Suite are updated more often than the maximum number of days Google Drive change logs are kept. For example, the default retention for change logs is 30 days. Verify that your Google Drive repositories are updated at least every 29 days.

Send documentation feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Micro Focus File Analysis Suite 3.7.0 Frequently Asked Questions

Add your feedback to the email and click **Send**.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to FAS.docFeedback@microfocus.com.

We appreciate your feedback!