IBM Aspera Faspex Server Considerations for GDPR Readiness

For PID(s): 5725-S60

Notice:

This document is intended to help you in your preparations for GDPR readiness. It provides information about features of IBM Aspera Faspex Server that you can configure, and aspects of the product's use, that you should consider to help your organization with GDPR readiness. This information is not an exhaustive list, due to the many ways that clients can choose and configure features, and the large variety of ways that the product can be used in itself and with third-party applications and systems.

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations.

The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting, or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

Table of Contents

GDPR

General Data Protection Regulation (GDPR) has been adopted by the European Union ("EU") and applies from May 25, 2018.

Why is GDPR important?

GDPR establishes a stronger data protection regulatory framework for processing of personal data of individuals. GDPR brings:

- New and enhanced rights for individuals
- Widened definition of personal data
- New obligations for processors
- Potential for significant financial penalties for non-compliance
- Compulsory data breach notification

Read more about GDPR

- (EU GDPR Information Portal)[https://www.eugdpr.org/]
- (ibm.com/GDPR website)[http://ibm.com/GDPR]

Product Configuration - considerations for GDPR Readiness

References:

1. *IBM Aspera Faspex Admin Guide*
2. *Aspera Ecosystem Security Best Practice* (found in Appendix of Admin Guide)

How to configure our offering such that it could be used in a GDPR environment?

1. Follow the instructions in the *Aspera Faspex Admin Guide* to install the application.
2. In the *Aspera Security Best Practices Guide* located in the Appendix of the *IBM Aspera Faspex Admin Guide*, follow the instructions in the topics below:
   – Securing the Aspera Application
   – Faspex
   – Securing Content in your Workflow
3. In the *Aspera Faspex Admin Guide*, follow the instructions in Securing Faspex section.

Data Life Cycle

What is the end-to-end process through which personal data go through when using our offering?

Data Types:

- Account Data
  – Username
  – Password

    - First Name
    - Email
    - Roles & Privileges
    - Custom User Fields (see *Configuring Custom User Fields*)
- IP Address
- Server Configuration
- Logs
- User Content (Unknown / Unclassified)
    - Transferred Files/Packages
    - Uploaded Files/Packages
    - Downloaded Files/Packages
    - Package Metadata

Account Data

- When admin creates a local user account, account data is saved in the database, until an admin removes the user.
- When admin imports a directory service user, Faspex creates a new account for the user account data. Account data saved in the database, until an admin removes the Faspex user.
- When admin imports a SAML user, Faspex creates a new account for the user and saves the usernames and email addresses in the database. Passwords are not saved by Faspex. Account data remains until an admin removes the new Faspex account.
- When users log in through SAML, Faspex creates a new account for the user and saves the usernames and email addresses in the database. Passwords are not saved by Faspex. Account data remains until an admin removes the new Faspex account.
- When an admin creates a workgroup and adds a user account to the workgroup, Faspex saves that authorization until an admin removes the user form the workgroup or removes the user account.
- When an admin creates a dropbox and adds a user account to the workgroup, Faspex saves that authorization until an admin removes the user form the workgroup or removes the user account.
- When an admin elevates a user to the manager role, Faspex saves that authorization until an admin demotes the user or removes the user account.
- When an admin makes a user admin of a workgroup, Faspex saves that authorization until an admin demotes the user or removes the user account.
- When an admin creates a global distributed list, Faspex saves the email addresses until the list is deleted.
- When a user creates a distributed list, Faspex saves the email addresses until the list is deleted.
- When a user registers for an account, Faspex saves that information to the database, until ab admin rejects the request, or, if approved, an admin removes the user.
- When a user modifies his or her user account settings, Faspex updates that information in the database.

- When a user sends content to an email address, Faspex saves that email address in the user's contact list.

IP Address

- IP addresses are saved to logs whenever a user logs in. The information persists until the customer admin removes the logs.

Server Configuration Data

- When an admin adds a transfer node to Faspex, Faspex stores the node information in the database, until an admin removes the node.
- When an admin adds a file storage location from a source node to Faspex, Faspex stores the information and permissions in the database, until an admin removes the file storage or the node.
- When an admin changes system configuration settings, Faspex stores the settings in the database.

Logs

- Faspex logs all activities. The logs persist until deleted according to the customer admin's retention policies.
- When Faspex initiates a transfer, Faspex collects metadata on the transfer. This data is stored on the database until an admin deletes the entry or completely removes the package (not archived).

User Content

- When a user uploads content to a file storage, the content is stored in the file storage source node, until a user removes the content through the Faspex UI, or the customer admin directly removes the content from the directory.
- When a user uploads content to a file storage through a public link, the content is stored in the file storage source node, until a user removes the content through the Faspex UI, or the customer admin directly removes the content from the directory.
- When an end user downloads content from Faspex, the content is stored on the end user's workstation. At that point, it is up to the end user to handle the content.
- When a user sends a package, Faspex collects custom metadata (as defined by the customer admin) from the New Package form.

Data Collection

Data Collected by this product

- Account Data
    - Username
    - Password
    - First Name
    - Email
    - Roles & Privileges

    - Custom User Fields
- IP Address
- Server Configuration
- Logs
- User Content (Unknown / Unclassified)
    - Transferred Files/Packages
    - Uploaded Files/Packages
    - Downloaded Files/Packages
    - Package Metadata

Data Storage

Options to control/configure the storage of personal data

Storage in Account Data / IP Addresses / Server Configuration

- Faspex stores account data on the Faspex MySQL database. Only user passwords are encrypted on the database. Faspex relies on the customer admin to control and protect the MySQL database.
- Faspex stores IP addresses in the logs. Faspex relies on the customer admin to control and protect the logs.
- Faspex stores server configuration data on the Faspex MySQL database. Faspex relies on the customer admin to control and protect the MySQL database.

Storage in User Content (Unknown/Unclassified)

- Faspex stores user content on configured Aspera nodes. Faspex relies on customer admins of those nodes for encryption and local file permissions. Customer admins can take additional measures to control and protect their nodes by referring to the guidance provided by the *Aspera Ecosystem Security Best Practices* document as well as the GDPR guidelines for *IBM Aspera Enterprise Server*.
- Admins can manage content storage location through Faspex. Admins can restrict users from accessing external file storage; these users can only upload and download from the configured default file storage (default inbox). Faspex relies on the customer admin to manage permissions in Faspex.
- Faspex relies on the end user to control and protect user content downloaded from Faspex.

Storage in Databases

- The MySQL database can be on the same server as the application or on a separate database. Faspex relies on the customer admin to control and protect the database and its host server.

Storage in Backups

- Admins can backup the MySQL database and configuration files with a backup script in an unencrypted backup directory. Faspex relies on the customer admin for encryption, storage location, and retention policy.

Storage in Logs

- Faspex saves user activities in unencrypted logs. User activities include: user login, change of management, and access to client data. By default, the logs will be overwritten in a rotated manner. Faspex relies on the customer admin to encrypt, save, or archive logs and set retention policies.

Storage in Backups

- Customer admin has full control of the backup files.

Storage in Archives

- Customer admin can manage archival of packages in the Faspex UI. Archives stay on the transfer node, so Faspex relies on the customer admin to protect the node.

Data Access

Controlling access to personal data

Roles and Access Rights

Customer admin can create user accounts with the following roles:

- Admin: Admins can create and configure all system, user, workgroup, and dropbox settings and permissions. They can also elevate users to managers or admins.
- Manager: Managers can can create and manage regular users and workgroup users. They cannot create new managers or admin accounts, or promote user accounts to manager or amdin roles.
- Workgroup Admins: Workgroup admins can configure workgroup-specific settings.
- Dropbox admins can configure dropbox-specific settings and archive and delete packages in the dropbox.
- User: Users can only access data they are given permission to access.

See *User Roles*.

Separation of Duties

Faspex managers can create and manage regular users and workgroup users. Otherwise, customer admin has full control.

Authentication

Faspex supports two methods of authentication: username / password and SAML.

Authenticating with Username / Password

- The username and password is provided by the user during initial registration or configured by an admin. Faspex saves both into the database, but encrypts only the password.
- Admins can configure Faspex to import Directory Service users and groups. Those usernames and passwords are handled as above.

Authenticating with SAML

- Faspex saves usernames but does not save passwords. The SAML IdP is responsible for security of user passwords.

Data Processing

Protecting personal data

Data protection in Motion

- Admins can configure Faspex to initiate transfers using AES-128 encryption mode. See *Configuring Security Settings*.

Data protection at Rest

- Admins can configure encryption-at-rest (EAR) on Aspera Nodes to store content uploaded to the server in an encrypted state. When downloaded from the server, server-side EAR first decrypts the files and then transfers the files to the client's disk in an unencrypted state. For more information, See the *Aspera Enterprise Server Admin Guide: Server-Side Encryption at Rest (EAR)*.
- The encryption key for EAR is saved in the aspera.conf configuration file as cleartext. The customer admin needs to take proper protection to avoid unauthorized access.
- Faspex relies on the customer admin to handle account data, content storage, and access to databases and files on the server.

Data Deletion

Deleting User Content

- Customer admin can archive and delete packages.
- Dropbox admins can archive and delete packages in the dropbox.
- Regular users cannot archive or delete packages.

Deleting Account Data

- Only admin accounts can remove user accounts.

Data Monitoring

Monitor and logging

- Admins can see an activity log for the entire application.
- Diagnostics data is saved in logs. Admins can change the logging level to gather more data (though at the cost of performance).

Log Files

Faspex logs can be found in the following locations in the Aspera and Common Files folders in the Program Files directory:

- Aspera\Faspex\log\
- Common Files\Aspera\Common\asctl\
- Common Files\Aspera\Common\mysql\data\mysqld.log
- Common Files\Aspera\Common\apache\logs\Log

Customer admin has full file access control to the logs.

Responding to Data Subject Rights

Right to Access

- End users can access their account data.
- Customer admins can grant or revoke a user's permission to access certain customer data.
- Customer admins can give external users permission to upload content to a public link.
- Customer admins can give external users permission to upload content to a dropbox.
- Customer admins can give Faspex users permission to send content to external users.
- Customer admins can access all personal data except for passwords.
- Faspex does not have the off-the-shelf functionality to single out a specific user's data from logs or database backup.

Right to Modify

- End users can modify their own account data.
- Customer admins can modify any user's management data.
- Customer admins can grant or revoke a user's permission to modify certain customer data.
- The activity log data cannot be modified by Faspex.

Right to Restrict Processing

- Faspex requires all data to provide adequate service. Customer admin is in control of restricting data usage for other purposes.

Right to Object

- Customer admin is in control.

Right to Be Forgotten

- Customer admin can remove any end user from the active system.
- Faspex managers can remove any regular or workgroup user from the active system.
- Faspex does not provide off-the-shelf functionality to remove data from logs or database backups. It is up to the customer admin to design a way to remove data from logs and database backups.

Right to Data Portability

- Faspex does not provide off-the-shelf functionality to port data from logs or database backups. It is up to the customer admin to design a way to port user data.

Appendix

1. *IBM Aspera Faspex Admin Guide*
2. *Aspera Ecosystem Security Best Practice* (found in Appendix of Admin Guide)