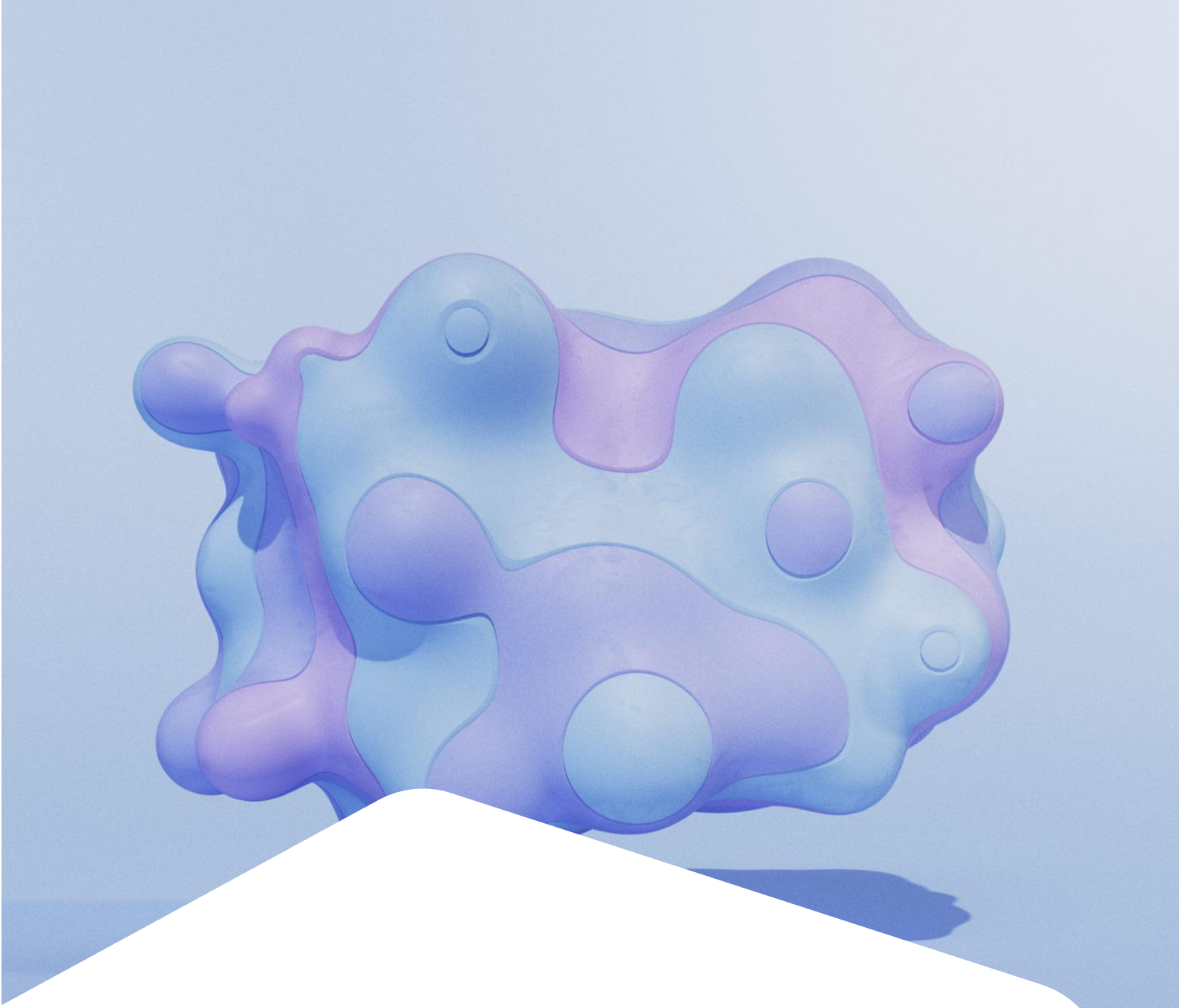

EQS

DATASYNC FAQ

Understand how DataSync works with your migration

This FAQ is designed to help you understand how DataSync works during your migration. It covers supported methods, connectors, scheduling, and key system behaviors to ensure a smooth data transfer process.

How many provisioning methods will be supported?

Only one method of data transfer can be used per migration. If multiple methods are required, expect additional implementation time and potential fees.

What data connectors are supported for migration?

SFTP, SCIM, and manual bulk import.

Does the system perform full delete and insert or delta transformations for import?

Delta transformations.

1. SFTP

Does EQS host their own SFTP server?

No. Clients are responsible for hosting and configuring their own SFTP server.

What functions as the primary key for employee records?

Employee ID is the primary key for updating user accounts.

Are custom user attributes supported?

Yes. Custom User Attributes (CUAs) are currently supported by SFTP and manual bulk import.

What fields are required for HR Data?

The following fields are required: Employee ID, Email Address, First Name, Last Name, and Status.

Does EQS support SSH authentication for SFTP servers?

Yes.

When can files be scheduled for import?

Imports can be scheduled daily, weekly, or monthly at a designated start time (UTC).

- **Weekly:** synchronization occurs on the first day of the week.
- **Monthly:** synchronization occurs on the first day of the month.

Does EQS support PGP decryption?

Yes, the key pair is unique for every SFTP connector. The public key can be downloaded from Compliance Cockpit.

What file types are supported for flat file integrations?

XLSX & JSON.

Does leaving users off of a file deactivate their account?

No. User accounts must be explicitly marked for deactivation.

Is role synchronization required?

No. If roles are not specified, the system automatically assigns the "employee" role if either policy or approvals modules are licensed. For clients that only have integrity line, new users will be created without a role if not specified .

Does the SFTP file template need to include all fields?

No. The file template can exclude fields that are not being utilized other than the required fields

Can file names be dynamic?

No. Files names must be fixed and hard coded into the connector.

Where can I review the error log?

Select the time stamp in the provisioning log and then download excel file

Locations, Department, or Business Unit are not populating on user record

If there are existing Locations present in Data Center, that value is displayed here. You cannot add a new Location. You can only add an existing Location name to the user. If you want to add a new value, then that should be done via the Attributes tab on Data Center or bulk upload via the Organization Attribute excel.

2. SCIM

Are custom user attributes supported?

No, custom user attributes for SCIM are scheduled to release Spring 2026.

What fields are required for provisioning?

ID, userName, familyName, givenName

Does EQS support roles via group membership?

No

Does EQS support DELETE transactions?

No, users can only be deleted in Compliance Cockpit by an administrator.

Does EQS support Entitlements?

No EQS does not have the SCIM 2.0 Roles & Entitlements extension. Role provisioning is supported as part of the core schema but not Roles as an extension resource.

3. SSO

Does EQS support Just-In-Time Provisioning?

No, JIT provisioning is not supported.

Does EQS support multiple SSO configurations?

Yes. Multiple SSO configurations can be enabled.

What attribute claims are required for SSO?

You can use either Employee ID or Email Address as the attribute identifier.
If your migration includes Integrity Line, you must also add a Cryptokey attribute from EQS Compliance Cockpit SSO Configuration into your enterprise application.

Does EQS support MFA?

Yes. If MFA is enabled for a system with hybrid login, users who log in to Compliance Cockpit and Integrity Hub using email and password will be prompted to enter an MFA token. Users who log in via SSO will not be required to complete the MFA flow.

Why can't I access Integrity Line when I SSO authenticate into EQS?

The account does have permissions for IL, or the crypto key is not being passed correctly by the identity provider.

How do you troubleshoot SSO?

Install a SAML tracer to your web browser and review the log. In the attribute statement, validate that the assertion for Email or Employee ID matches the user record in EQS. Validating the Entity ID and ACS Location are properly configured in both EQS and the Identity Provider.