ORYELE DOCUMENTATION

Security and Compliance

Protect your firm's data with enterprise-grade encryption, governance controls, and compliance tooling.

This guide covers data encryption at every layer, legal hold for litigation and audit preservation, audit trail exports in CSV and PDF format, and SSO and MFA configuration.

Data Encryption

Oryele uses industry-standard encryption at every layer of the platform to protect your firm's data and your clients' information.

Layer	Encryption Standard	Details
Data in Transit	TLS 1.3	All API traffic, web sessions, and integration connections
Data at Rest	AES-256	Database records, backups, and file attachments
File-Level Encryption	AES-256-GCM	Individual documents encrypted with per-file keys
Key Management	AWS KMS / Azure Key Vault	Keys rotated automatically every 90 days
Backups	AES-256	Encrypted before transfer to off-site storage

Legal Hold

Legal Hold prevents any content from being modified, deleted, or overwritten for the duration of a litigation, investigation, or audit. Content under hold is preserved exactly as it exists at the moment the hold is applied.

Applying a Legal Hold

- Go to Governance > Legal Hold and click New Hold.
- Name the hold (e.g., Matter 2024-47) and set a reason from the dropdown.
- Scope the hold by contact, engagement, date range, worker, or workflow.
- Click Confirm. All content matching the scope is immediately locked.
- The hold is logged in the audit trail with the applying user's identity and timestamp.

Managing Active Holds

- View all active holds on the Legal Hold dashboard with their scope, creator, and creation date.
- Holds do not have expiry dates by default. They must be explicitly released by an authorized user.
- Only users with the Compliance Officer or Owner role can release a legal hold.
- When a hold is released, content returns to the standard retention policy timeline immediately.

Important	Placing a legal hold does not create a separate copy of the data. It prevents the original records from being altered or removed. Always apply holds promptly when litigation is reasonably anticipated.

Exporting Audit Trails

Complete audit trails can be exported in CSV or PDF format for regulators, external auditors, or internal compliance review.

Exporting in CSV Format

- Go to Governance > Audit Logs and apply the filters defining your export scope.
- Click Export > CSV. For sets under 50,000 records, the file downloads immediately.
- Larger exports are queued and delivered to your notification email within 30 minutes.
- CSV columns include: timestamp, actor, actor type, event type, resource, resource ID, outcome, and IP address.

Exporting in PDF Format

- Select Export > PDF from the Audit Logs view.
- PDF exports include the Oryele logo, your firm name, the export scope filters, and page numbers.
- Each log entry is rendered in a structured table suitable for inclusion in formal reports.
- PDF exports are signed with a digital certificate to verify authenticity and detect tampering.

SSO and MFA Configuration

Oryele supports SAML 2.0 and OIDC for single sign-on, and requires multi-factor authentication for all privileged roles.

Configuring SSO

- Go to Settings > Security > Single Sign-On and click Configure.
- Choose SAML 2.0 or OIDC depending on your identity provider.
- Download the Oryele metadata file and upload it to your identity provider (Okta, Azure AD, Google, Ping).
- Enter the identity provider's SSO URL, entity ID, and public certificate in Oryele.
- Test the SSO flow with a non-admin test account before enabling it organization-wide.

Enforcing Multi-Factor Authentication

- Go to Settings > Security > Multi-Factor Authentication.
- Choose enforcement scope: All Users, Admins Only, or Custom Role set.
- Supported MFA methods: TOTP authenticator app, hardware security key (FIDO2), and push notification.
- Set a grace period (recommended: 7 days) during which users can enroll before being locked out.
- Users who fail MFA enrollment within the grace period are suspended automatically.

Recommendation	Enable SSO and MFA together. SSO centralizes identity management in your existing IdP, while MFA ensures that a compromised IdP credential alone is not sufficient to access the Oryele platform.