



TRACELOCK BY ODINGARD

TraceLock Enterprise Deployment and Operations Guide

Onboarding, identity, connectors, continuous monitoring and auditor
verification for regulated enterprises

VERSION 1.0



© 2026 Odingard. All rights reserved.

TraceLock Enterprise Deployment and Operations Guide

Document title	TraceLock Enterprise Deployment and Operations Guide
Version	Version 1.0
Owner	Odingard — Architecture: James
Classification	Customer
Product	TraceLock

This document describes TraceLock, a hosted software-as-a-service platform operated by Odingard. TraceLock is not installed into customer cloud projects or on-premises environments; customer systems are connected as read-only scan targets.

The information in this document is provided for the operation and evaluation of TraceLock. Service commitments for a specific subscription are governed by the applicable order form or private offer.

Product support: support@odingard.com

Security and vulnerability reports: security@odingard.com

TraceLock and Odingard are trademarks of Odingard. All other trademarks are the property of their respective owners.

Contents

Platform overview	1
What TraceLock does for you	1
What TraceLock does not do	1
Concepts	2
How TraceLock is delivered	2
Plans and feature availability	3
Where to go next	3
Prerequisites and network requirements	5
Access you need	5
Credentials by provider	5
Network requirements	6
Recommended sequence	6
Identity, single sign-on and provisioning	8
Before you begin	8
Configure SAML single sign-on	8
Map SAML attributes and roles	10
Understand SAML validation and provisioning	11
Rotate SAML certificates	11
Configure SCIM 2.0 provisioning	12
Supported SCIM resources and operations	13
Attribute and lifecycle behavior	14
SCIM error codes	14
Troubleshoot identity failures	14
Supported and not supported	15
Using the TraceLock workspace	17
What TraceLock does	17
Core concepts	17

Get started	18
Review Dashboard	19
Operate Control Center	20
Manage Policies	20
Assign Training	21
Review Estate Map	21
Prepare Audits	21
Record Penetration Tests	22
Review Evidence	22
Review Vendors	23
Manage Risks	23
Review User Access	24
Manage People	24
Inspect Webhook Log	24
Review AI Governance	25
Complete AI Questionnaire	25
Maintain AI Inventory	26
Publish Trust Center material	26
Understand frameworks	27
Remediate failed controls	27
Troubleshoot common problems	28
Connector configuration reference	30
Connector lifecycle	30
AWS	30
Google Cloud	32
GitHub	32
Cloudflare	33
Fordefi	34
Turnkey	34
Access inventory	35

Universal webhook evidence	35
Log feed	35
Privacy Wall and evidence behavior	36
Verify the Privacy Wall	38
What the Privacy Wall does	38
Procedure: inspect a stored evidence record	38
Procedure: recompute a digest independently	39
Procedure: confirm rejection behaviour	39
What leaves TraceLock	40
Answers for your security questionnaire	40
Continuous monitoring and framework mapping	41
Read control state	41
Check freshness, not just status	41
Review framework coverage	42
Assign owners	42
Record an exception	43
AI governance obligations	43
Evidence lifecycle	43
Remediation, alerting and ticketing	45
Notification triggers	45
Configure destinations	45
Configure ticketing	46
Remediate a failing control	46
Findings that will not clear	47
Track remediation progress	47
Auditor Room and evidence verification	49
How auditor access works	49
Procedure: provision auditor access	49
Procedure: revoke auditor access	50
What the auditor sees	50

Procedure: export an audit package	50
Procedure: verify evidence independently	51
Preparing for a SOC 2 Type II or ISO 27001 engagement	51
Workspace administration	54
Organization setup	54
Roles and permissions	55
Invite and deprovision users	56
Configure MFA enforcement	57
Plans and entitlements	57
Manage connectors and credentials	58
Configure a custom domain	59
Lifecycle states	60
Review privileged audit history	60
Export and delete data	60
Platform administration	61
Hosting, security and tenant isolation	63
Architecture and hosting	63
Component tenancy	63
Tenancy and isolation	64
Data classification and storage	65
Encryption and key management	65
Secret handling	66
Customer-environment access	66
Privacy Wall and data minimization	66
Logging, monitoring, and retention	67
Availability, backup, and recovery	67
Vulnerability management and dependency scanning	67
Subprocessors and external services	68
Responsible disclosure	68
Compliance posture	68

Support and service levels	70
Contact TraceLock Support	70
Escalate a request	70
Severity and initial response	70
In scope and out of scope	71
Maintenance and releases	71
Security incidents	71
Report a vulnerability	72
Troubleshooting, FAQ and API reference	74
Troubleshooting	74
Frequently asked questions	75
API reference	76
Support	78
Glossary	79
Product terms	79
Identity and administration terms	80
AI governance terms	81
Connector terms	82

Platform overview

TraceLock is a hosted compliance monitoring and evidence platform. You connect the systems you already run, TraceLock evaluates them continuously against a single control library, and the resulting evidence is presented against every framework you report on.

What TraceLock does for you

Monitors controls continuously. Read-only connectors evaluate your cloud accounts, source control, edge and custody providers on a schedule. Control state reflects your environment as it is now, not as it was when someone last collected screenshots.

Reports one control set against nine frameworks. Each control maps to the equivalent requirement in SOC 2, ISO/IEC 27001, NIST CSF 2.0, NIST AI RMF, ISO/IEC 42001, the EU AI Act, the HIPAA Security Rule, SEC rules, and CIS Controls v8. You evaluate once and report many times.

Protects your data at ingestion. The Privacy Wall admits only an allowlisted set of posture attributes. Provider payloads, object contents, log bodies, and personal data are dropped before anything is stored.

Produces evidence that withstands challenge. Every evidence record carries a SHA-256 digest over its canonical metadata, an observation timestamp, and a retention clock. Your auditor can recompute the digest independently.

Gives auditors their own door. The Auditor Room grants time-bound, read-only access scoped to your organization, without a licensed seat and without adding the auditor to your identity provider.

What TraceLock does not do

Read this list before you plan your deployment; it removes most of the questions your security reviewer will raise.

- Nothing is installed in your cloud projects or on your premises. Your systems are connected as read-only scan targets over provider APIs.
- TraceLock does not change your environment. Connector credentials are read-only, and remediation is delivered as guidance and tickets that your team applies.
- TraceLock does not ingest your business data, customer records, log contents, or object contents.
- TraceLock does not replace your identity provider, your risk acceptance decisions, or your compliance judgment.
- Framework mappings are provided for your compliance reviewer to confirm. They are not legal advice.

Concepts

Concept	What it means
Organization	Your workspace, and the boundary around your users, connectors, controls, findings, and evidence
Control	A requirement with a code, owner, status, framework references, and verification timestamp
Finding	The result of evaluating a control, including its status and severity
Evidence record	A stored, hashed posture record with an observation timestamp and retention clock
Exception	A time-bounded, documented acceptance of a specific finding
Connector	A read-only integration with one of your providers
Privacy Wall	The ingestion boundary that filters, canonicalizes, hashes, and region-checks evidence metadata
Estate Map	Control coverage across all framework perspectives
Auditor Room	The read-only surface you provision for an external auditor

How TraceLock is delivered

TraceLock runs as a multi-tenant service in Odingard's Google Cloud environment: application tier, managed PostgreSQL, scheduler, and secret storage, all operated by Odingard. Your data is separated logically by organization, encrypted in transit with TLS 1.2 or later and at rest by the managed platform. Your connector credentials are stored under envelope encryption with key material held in a managed secret store, and are never returned by any API.

Objective	Target
Availability	99.9% monthly
Scan cadence	Connectors scheduled every 5 minutes
Notification dispatch	Queued deliveries drained every 5 minutes
Evidence retention	Seven years from observation by default
Evidence ingestion	Under 500 ms at P99 per artifact

Plans and feature availability

Feature availability is set by your plan tier and is independent of your role in the workspace. Enterprise features include SAML single sign-on, SCIM provisioning, third-party risk management, AI governance surfaces, expanded connector counts, and Auditor Room provisioning. Your administrator can confirm current entitlements in workspace settings.

Where to go next

1. Confirm the prerequisites for your environment.
2. Configure identity: single sign-on, provisioning, roles, and MFA.
3. Connect your providers and validate each connector.
4. Verify the Privacy Wall on your own evidence.
5. Assign control owners and set up remediation routing.
6. Provision an Auditor Room when your audit begins.

Prerequisites and network requirements

Complete these prerequisites before you configure connectors. Each item is something only your organization can provide.

Access you need

Requirement	Why it is needed
A TraceLock workspace with an administrator account	To configure identity, connectors, and routing
Permission to create read-only roles in each cloud account you connect	Connectors authenticate as roles you create and control
Permission to install an application in your source-control organization	Repository and branch-protection posture is read through it
Administrative access to your identity provider	To configure SAML and provisioning
Mailboxes for your control owners	Notifications and evidence-expiry alerts are addressed to owners

Credentials by provider

Create the credential in your own environment, then register it in TraceLock. Grant read-only scope only; TraceLock never requires write permission and will not use it if granted.

Provider	Credential to prepare	Scope
Amazon Web Services	An IAM role TraceLock can assume, with an external ID	Read-only posture visibility (security, IAM, logging, storage configuration)
Google Cloud	A service account with viewer-level project access	Read-only project and security posture
GitHub	An installed GitHub App with a webhook secret	Read-only organization, repository and protection settings
Cloudflare	An API token restricted to read scopes	Read-only zone and security configuration
Custody providers	A read-only API credential	Read-only policy and approval configuration
Log and webhook feeds	A signing secret you generate	Verifying event authenticity

Rotate these credentials on your normal schedule. Re-registering a rotated credential in TraceLock takes effect on the next scheduled scan.

Network requirements

TraceLock is a hosted service and initiates all connections outbound to your providers' public API endpoints. There is nothing to install and no inbound connection into your network.

Your users need outbound HTTPS access to:

- `https://tracelock.odingard.com` — the application
- Your identity provider's sign-in endpoints, if you use single sign-on

You need to permit, if you filter egress from your own automation:

- `https://tracelock.odingard.com/api/webhooks/*` — if you send webhook evidence to TraceLock
- `https://tracelock.odingard.com/api/mcp` — if you submit AI agent governance events

All traffic uses TLS 1.2 or later. Certificate pinning is not required and not recommended, because managed certificates rotate.

Note TraceLock does not require you to open inbound firewall rules, establish VPN or VPC peering, or expose a management interface. If a security review asks how TraceLock reaches your environment, the answer is: outbound API calls from Odingard's environment using read-only credentials that you issue and can revoke at any time.

Recommended sequence

1. Create the read-only credentials for each provider you intend to connect.
2. Confirm your plan entitlements cover the connectors and features you need.
3. Configure identity: single sign-on, provisioning, roles, and MFA enforcement.
4. Register and validate one connector before registering the rest.
5. Assign control owners so findings have a route to an accountable person.
6. Configure notification and ticketing destinations.
7. Review your first full scan cycle, then provision an Auditor Room when the audit begins.

Identity, single sign-on and provisioning

Before you begin

- Use an Enterprise plan. TraceLock gates SAML and SCIM configuration on the `sso.enabled` entitlement.
- Have an IdP administrator account for the organization.
- Have the IdP SSO URL and one or more PEM-formatted signing certificates.
- Know the email domains that the organization claims.
- For SCIM, plan a named bearer token and an IdP provisioning application.
- Keep certificates and bearer tokens out of tickets, chat, and source control.

Configure SAML single sign-on

TraceLock-side values

TraceLock displays the following values in **Settings** when an SSO connection exists. Replace `<organization-id>` with the organization identifier displayed by your deployment.

Value	Format
SP entity ID	<code>https://tracelock.odingard.com/api/auth/saml/<organization-id>/metadata</code>
ACS URL	<code>https://tracelock.odingard.com/api/auth/saml/<organization-id>/acs</code>
Metadata URL	<code>https://tracelock.odingard.com/api/auth/saml/<organization-id>/metadata</code>

The entity ID and metadata URL are the same URL in the current implementation. The SAML client uses the metadata URL as its issuer and audience.

Configure the connection

Prerequisites

- The Enterprise entitlement is enabled.
- You can change workspace settings.
- Your IdP SSO URL and PEM signing certificate are available.

Steps

1. Sign in to TraceLock.
2. Select **Settings**.
3. Open the **Enterprise SAML SSO and SCIM** section.
4. Enter the IdP entity ID in **IdP entity ID**.
5. Enter the IdP SSO URL in the SSO URL field.
6. Add the PEM signing certificate to the signing-certificate configuration.
7. Add each claimed email domain.
8. Select **Save SSO settings** when that control is available in your deployment.
9. Enable the connection only after a test login succeeds.

Result: TraceLock stores an organization-scoped SAML connection with its entity ID, SSO URL, certificates, default role, attribute mapping, domains, group mappings, enabled state, and enforcement state.

The settings UI exposes those connection fields. If a displayed control uses a label different from the labels above, use the label shown in that deployment rather than inventing a replacement.

Configure the IdP

Okta

Prerequisites

- An Okta administrator account.
- The TraceLock SP entity ID and ACS URL.
- The TraceLock signing certificate value.

Steps

1. Create a SAML 2.0 application in Okta.
2. Set the Single sign-on URL to the TraceLock ACS URL.
3. Set the Audience URI to the TraceLock SP entity ID.
4. Select the signing certificate that corresponds to the certificate configured in TraceLock.
5. Assign test users and groups.
6. Map the email claim to the user's email.
7. Map a groups claim when you use TraceLock group-role mappings.
8. Test with an account in a claimed domain.
9. Enable domain enforcement only after the test succeeds.

Result: A test assignment can start the TraceLock SAML login and return to the organization's ACS URL with a signed response.

Microsoft Entra ID

Prerequisites

- A Microsoft Entra administrator account.
- The TraceLock SP entity ID and ACS URL.
- Access to the Base64 SAML signing certificate.

Steps

1. Create an Enterprise application in Microsoft Entra ID.
2. Select SAML as the single sign-on method.
3. Set Reply URL (ACS) to the TraceLock ACS URL.
4. Set Identifier (entity ID) to the TraceLock SP entity ID.
5. Set the Login URL as directed by the TraceLock configuration.
6. Download the SAML signing certificate in Base64 format.
7. Convert the certificate to the PEM value required by the TraceLock connection.
8. Assign test users and groups.
9. Add claims for email, display name, and groups when those attributes are used.
10. Validate a test assignment before enforcing claimed domains.

Result: The assigned test account can complete the SAML flow and TraceLock can validate the response against the organization connection.

Google Workspace

TraceLock's product documentation identifies Google Workspace as a supported enterprise identity provider. Use the standard SAML values above when configuring Google Workspace SAML.

Map SAML attributes and roles

IdP value	TraceLock use	Format
Email claim	Login identity and user email	Email address
Display name claim	Just-in-time user's name when supplied	String
Groups claim	Optional role mapping	Group names
Default role	Role for a new user without a matching group mapping	ADMIN , CLIENT_OWNER , CLIENT_USER , or AUDITOR

When a group mapping matches, TraceLock assigns the mapped role. Existing local credentials and roles remain unchanged unless a group mapping explicitly matches.

Understand SAML validation and provisioning

TraceLock validates a signed response and assertion. The SAML client requires signed assertions and signed authentication responses, checks the configured IdP issuer, uses the configured audience and ACS URL, accepts five seconds of clock skew, and validates an in-response-to value when present. Authn request identifiers are stored for five minutes and marked used after a successful claim.

On a successful SAML login:

- TraceLock resolves the organization from the SAML connection and claimed domain.
- A new local user can be created with the configured default role.
- A matching group mapping can assign another role.
- A deactivated user cannot claim the login token.
- SAML users use IdP MFA and are not enrolled in local time-based one-time password (TOTP) MFA.

When **Enforce claimed domains** is enabled, password login is refused for ordinary users in those domains. `ADMIN` and `CLIENT_OWNER` retain password login as break-glass operators.

The Enterprise entitlement gates SAML and SCIM configuration and token minting. The SAML login and SCIM request handlers authenticate existing connections and tokens without rechecking the configuration entitlement on each request. An existing SSO connection and an in-flight SCIM synchronization therefore continue until the connection is disabled or the token is revoked; an entitlement lapse does not itself revoke either credential.

Rotate SAML certificates

Prerequisites

- The new IdP certificate is available in PEM format.
- The old certificate remains active at the IdP during the overlap.
- You can edit the SSO connection.

Steps

1. Add the new PEM certificate alongside the old certificate in TraceLock.
2. Test a SAML login while both certificates are configured.
3. Change the IdP signing certificate to the new certificate.
4. Test another SAML login.

5. Remove the old certificate from TraceLock after the overlap.

Result: Responses signed by the configured certificate set continue to validate during the rotation. Unsigned responses and unknown certificates are rejected.

Caution: Removing the old certificate before the IdP change has propagated can interrupt SSO for the organization.

Configure SCIM 2.0 provisioning

TraceLock values

Value	Format
SCIM base URL	<code>https://tracelock.odingard.com/api/scim/v2</code>
Authentication	<code>Authorization: Bearer <token></code>
User resource	<code>/Users</code>

Prerequisites

- The Enterprise entitlement is enabled.
- You can change workspace settings.
- You have an IdP provisioning administrator account.

Steps

1. Select **Settings**.
2. Open the **Enterprise SAML SSO and SCIM** section.
3. Enter a name in **Token name**.
4. Select **Mint token**.
5. Copy the displayed token into the IdP provisioning application.
6. Configure the IdP base URL as the SCIM base URL.
7. Run the IdP connection test.
8. Confirm that the provisioned user appears in TraceLock.

Result: TraceLock authenticates SCIM requests with the named bearer token. The token value is shown once; TraceLock stores a digest for later authentication.

Rotate a SCIM token

1. Mint a replacement token with a new name.
2. Update the IdP provisioning application.
3. Confirm a provisioning request succeeds.
4. Select **Revoke** for the old token.

Result: The old token is rejected immediately after revocation.

Caution: Revoking the only token before the replacement works stops SCIM provisioning for the organization.

Supported SCIM resources and operations

Resource or operation	Support	Format or behavior
GET /ServiceProviderConfig	Supported	Patch and filter are reported as supported; bulk, sort, change password, and ETag are reported as unsupported.
GET /ResourceTypes	Supported	Returns the User resource type.
GET /Schemas	Supported	Returns the core User schema.
GET /Groups	Supported	Returns an empty list; group write provisioning is not implemented.
GET /Users	Supported	Pagination and the exact <code>userName eq "email"</code> filter are supported.
POST /Users	Supported	Creates a user and membership using the SSO default role.
GET /Users/<id>	Supported	Returns a tenant-scoped user resource.
PUT /Users/<id>	Supported	Replaces supported profile values and active state.
PATCH /Users/<id>	Supported	Supports <code>add</code> and <code>replace</code> for <code>active</code> , <code>displayName</code> , <code>userName</code> , and <code>externalId</code> .
DELETE /Users/<id>	Supported	Soft-deactivates the user.

Ask your Odingard account team for the current SCIM-specific rate limit.

Attribute and lifecycle behavior

SCIM attribute	TraceLock field	Format
<code>userName</code>	User email	Email address
<code>displayName</code>	User name	String
<code>active</code>	<code>deactivatedAt</code> and organization membership	Boolean
<code>externalId</code>	<code>scimExternalId</code>	String or null

Provisioning creates a local user with `authProvider` set to `SCIM`, creates an organization membership, and audits `SCIM_USER_CREATED`. Profile updates audit `SCIM_USER_UPDATED`. Deactivation sets `deactivatedAt`, removes the organization membership, invalidates the tenant scope immediately, and preserves the user and audit evidence. Reactivation clears `deactivatedAt` and restores membership using the user's role.

SCIM error codes

HTTP status	scimType or condition	Meaning
400	<code>invalidValue</code>	Required data is missing, a value is invalid, or a PATCH operation is unsupported.
400	<code>invalidFilter</code>	The filter is not the supported exact <code>userName</code> equality form.
401	<code>invalidValue</code>	The bearer token is missing, invalid, or revoked.
404	Not supplied	The user or resource does not exist in the token's organization.
409	<code>uniqueness</code>	The email already exists.

Troubleshoot identity failures

Symptom	Likely cause	Action
Signature mismatch	The IdP certificate is not the configured PEM value, or the response is unsigned.	Confirm the certificate and rotate with an overlap.
Request rejected after a delay	The five-second accepted clock skew was exceeded.	Synchronize the IdP clock and retry.

Symptom	Likely cause	Action
Login does not match an organization	The email domain is not claimed or the SAML connection is not enabled.	Confirm the domain, connection state, and discovery result.
Password login is refused	Domain enforcement is enabled for the user's domain.	Use SAML or sign in with an <code>ADMIN</code> or <code>CLIENT_OWNER</code> break-glass account.
User is not provisioned	The SCIM token is invalid or the request is outside the supported resource shape.	Mint a replacement token and inspect the SCIM error response.
Deactivated user still has access	A stale session or a different organization membership is being used.	Revoke the IdP assignment and start a new TraceLock session; verify the target organization.

Supported and not supported

Supported	Not supported
SAML SSO for Okta, Microsoft Entra ID, and Google Workspace	Unsigned SAML assertions or responses
Signed assertions and responses with certificate rotation	Group write provisioning through SCIM
SAML group-to-role mapping	SCIM bulk operations
Just-in-time local user creation	SCIM change-password operations
SCIM user create, update, patch, deprovision, and reactivation	SCIM sort, ETag, and resource-type writes
Tenant-scoped user access	The SCIM-specific rate limit for your subscription

Using the TraceLock workspace

What TraceLock does

TraceLock connects an organization's compliance requirements to controls, tests, evidence metadata, findings, framework crosswalks, people, vendors, risks, training, AI governance, and trust surfaces. Connectors inspect configured customer-owned systems and persist tenant-scoped control outcomes. The product does not replace the customer's policy decisions, risk acceptance, identity provider, or cloud provider.

Core concepts

Concept	Meaning
Control	A compliance requirement with a code, title, category, framework references, status, and verification information.
Control test	A check that evaluates a control and can produce a finding and evidence.
Evidence record	A persisted, tenant-scoped record containing evidence type, description, source, hash, metadata, and retention information.
Framework crosswalk	A mapping from a control to a framework reference.
Finding	A connector result with a status such as passed, failed, not applicable, indeterminate, warning, or not assessed.
Exception	A time-bounded request against a control that records reason, expiry, and approval state.
Estate Map	A view of control coverage across the framework perspectives exposed by TraceLock.
Connector	A provider-specific integration that runs posture or evidence checks.
Tenant or organization	The boundary around one customer's users, controls, integrations, findings, and evidence.
Verification Room	A read-only auditor surface for reviewing controls, evidence metadata, hashes, and audit history.

Concept	Meaning
Privacy Wall	The evidence metadata protection boundary that filters, canonicalizes, hashes, and region-checks evidence metadata.

Get started

Sign in

Prerequisites

- You have a TraceLock account or a valid organization invitation.
- Your account is active.

Steps

1. Go to <https://tracelock.odingard.com>, or the custom domain configured for your organization.
2. Enter your email address and password, or select the configured SAML sign-in path when your claimed domain uses SSO.
3. Complete your identity provider MFA challenge when using SAML.
4. Complete local MFA enrollment when prompted for a local account.

Result: TraceLock establishes a tenant-scoped session and displays the workspace available to your role.

Enroll local MFA

Prerequisites

- You are using local authentication.
- An authenticator application is available.

Steps

1. TraceLock redirects you to `/mfa/enroll` when MFA is enforced.
2. Scan the QR code with the authenticator application.
3. If scanning is unavailable, enter the displayed base32 secret manually.
4. Enter the current authenticator code.
5. Select **Confirm MFA**.
6. During re-enrollment, enter **Current MFA code (only for re-enrollment)**.

Result: TraceLock stores the local TOTP enrollment and uses it for subsequent local sign-ins. The QR code is generated in the browser from the enrollment URI; TraceLock does not send it to a QR service.

Tour the navigation

TraceLock groups workspace pages as follows:

Group	Pages
Compliance	Dashboard, Control Center, Policies, Training, Estate Map, Audits, Penetration Tests, Evidence
Risk	Vendors, Risks, User Access, People
Signals	Webhook Log, AI Governance, AI Questionnaire, AI Inventory
Trust	Trust Center
Workspace	Integration, Team, Billing, Settings, Log out
Platform	Administration , staff-only

Prerequisites

- You have signed in.

Steps

1. Select a page from the relevant group.
2. Review the page summary before editing a record.
3. Use the page's filters, detail views, or export controls.
4. Return to **Dashboard** to review the overall workspace state.

Result: Each page preserves the organization boundary and shows only the data available to your role and plan.

Review Dashboard

Purpose: Start with the workspace's compliance summary and current posture.

Prerequisites: You have access to the organization.

Steps

1. Select **Dashboard**.
2. Review the readiness summary and control status.

3. Follow a failing or incomplete control to its detail view.
4. Review the latest execution and evidence metadata.

Relevant fields: readiness status, control status, finding status, framework coverage, and latest verification information.

Resulting evidence: The dashboard reads tenant-scoped control and execution data; a connector execution produces an execution log and can refresh a control's verification timestamp.

Operate Control Center

Purpose: Review control health, posture categories, and controls that require attention.

Prerequisites: You have access to the organization; `controls:manage` is required for control-management actions.

Steps

1. Select **Control Center**.
2. Filter the control list by status or category.
3. Open a control with a failed, warning, indeterminate, or not-assessed result.
4. Review its guidance, execution history, and evidence metadata.
5. If authorized, run the available control action or record remediation.

Relevant fields: control code, title, category, status, check identifier, severity, message, configuration drift, evidence hash, and verification time.

Resulting evidence: A completed check writes a control execution log and, when evidence is present, a Privacy Wall-protected evidence record.

Manage Policies

Purpose: Maintain organization policy records and their review state.

Prerequisites: You have `policies:write` for changes.

Steps

1. Select **Policies**.
2. Review policy title, owner, status, review date, and linked controls.
3. Create or edit the policy record when authorized.
4. Save the policy and review its linked controls.

Relevant fields: title, description, owner, status, review date, version, and control links.

Resulting evidence: TraceLock stores the policy record and its audit metadata. Manage policy records in **Policies**; attach policy documents as evidence records.

Assign Training

Purpose: Track training requirements, assignments, completion, and expiry.

Prerequisites: You have `training:write` for assignments or updates.

Steps

1. Select **Training**.
2. Review the training catalog and assignment status.
3. Create or update an assignment with its person, due date, and completion state.
4. Export the assignment record as CSV when you need an offline review.

Relevant fields: training title, assignee, due date, completion date, status, and expiry.

Resulting evidence: TraceLock records assignment and completion history and can export the training data as CSV.

Review Estate Map

Purpose: Inspect framework coverage and control status across the mapped estate.

Prerequisites: You have organization access.

Steps

1. Select **Estate Map**.
2. Choose a framework perspective.
3. Filter by control status or category.
4. Open a mapped control to review its execution and evidence.

Relevant fields: framework, control code, mapped reference, category, status, verification date, and evidence state.

Resulting evidence: The Estate Map reads existing controls and crosswalks; it does not create a second evidence store.

Prepare Audits

Purpose: Track audit engagements and readiness context.

Prerequisites: You have `audits:write` for changes.

Steps

1. Select **Audits**.
2. Review the audit framework, progress, dates, and status.
3. Create or update the audit record when authorized.
4. Open linked controls and evidence for audit preparation.

Relevant fields: audit name, framework, status, progress, start date, end date, scope, and linked controls.

Resulting evidence: TraceLock records audit configuration and the linked control and evidence references.

Record Penetration Tests

Purpose: Track penetration-test records and findings.

Prerequisites: You have `pentests:write` for changes.

Steps

1. Select **Penetration Tests**.
2. Review test provider, scope, dates, status, and findings.
3. Add or update the penetration-test record.
4. Link remediation information when a finding requires action.

Relevant fields: provider, scope, performed date, report date, status, severity, finding, and remediation.

Resulting evidence: TraceLock stores the test record and associated remediation information.

Review Evidence

Purpose: Search the tenant's evidence metadata and inspect provenance, retention, and integrity information.

Prerequisites: You have organization access; `evidence:write` is required to add or edit evidence.

Steps

1. Select **Evidence**.
2. Filter by provider, control code, status, or observation date.
3. Open an evidence record.
4. Review its source, content hash, sanitized metadata, region, and retention end.

5. Use the Trust Center or Verification Room when an external reviewer needs a read-only evidence package.

Relevant fields: provider, control code, evidence type, description, observation time, content hash, metadata, region, and retention end.

Resulting evidence: Accepted metadata is canonicalized and SHA-256 hashed. Sensitive patterns are rejected or redacted by the Privacy Wall. Evidence retention defaults to seven years.

Review Vendors

Purpose: Maintain vendor inventory, risk context, and vendor evidence.

Prerequisites: You have organization access; vendor changes require the permission exposed by the tenant scope.

Steps

1. Select **Vendors**.
2. Review each vendor's status, owner, risk, and assessment state.
3. Open a vendor to inspect linked findings and evidence.
4. Update the vendor record when authorized.

Relevant fields: vendor name, owner, category, status, risk rating, review date, and evidence links.

Resulting evidence: TraceLock stores vendor and risk records in the tenant organization.

Manage Risks

Purpose: Record risks, treatments, owners, and exceptions.

Prerequisites: You have `risks:write` for risk changes and `risk-exceptions:approve` for exception approval.

Steps

1. Select **Risks**.
2. Review risk title, likelihood, impact, score, owner, and treatment.
3. Add or update a risk when authorized.
4. Open a linked control failure and follow its remediation guidance.
5. Request or approve a time-bounded exception when the risk owner documents why the control cannot be met.

Relevant fields: title, description, likelihood, impact, score, owner, treatment, status, control link, exception reason, and expiry.

Resulting evidence: TraceLock stores the risk record, exception state, actor, reason, approval, and expiry.

Review User Access

Purpose: Review access records synchronized from supported providers and identify excessive, inactive, or MFA-missing access.

Prerequisites: You have organization access; `user-access:manage` is required for review actions.

Steps

1. Select **User Access**.
2. Filter by provider, inactive state, MFA state, or excessive access.
3. Open a record to review email, provider, role, last login, and status.
4. Export the review data as CSV when required by the review process.
5. Revoke or correct access in the source provider, then run the relevant sync.

Relevant fields: provider, user email, role, MFA active, inactive, excessive, last login, and synchronization status.

Resulting evidence: TraceLock persists a tenant-scoped access record and its review state; it does not grant provider access from this page.

Manage People

Purpose: Review organization people records and training or access context.

Prerequisites: You have organization access.

Steps

1. Select **People**.
2. Search or filter the people list.
3. Open a person to review profile, access, training, and owner information.
4. Use **Team** for membership and invitation administration.

Relevant fields: email, name, role, status, training state, and access state.

Resulting evidence: The page reads tenant-scoped people and related records. Membership changes and role changes are recorded in access history.

Inspect Webhook Log

Purpose: Review signed webhook events and evidence ingestion.

Prerequisites: You have organization access and a configured webhook sender.

Steps

1. Select **Webhook Log**.
2. Review event type, provider, received time, payload length, hash, and retention.
3. Match the hash to the sender's event record.
4. Investigate rejected events using the HTTP status and Privacy Wall result.

Relevant fields: event type, control code, received time, payload length, SHA-256 data hash, provider, and WORM retention clock.

Resulting evidence: A valid tenant-derived HMAC request creates a universal-webhook evidence-backed finding. Sensitive content does not bypass the Privacy Wall.

Review AI Governance

Purpose: Review AI governance posture, role assessments, training, and role shift signals.

Prerequisites: You have organization access; `ai-governance:write` is required for governance changes.

Steps

1. Select **AI Governance**.
2. Review posture by AI system, operator role, risk category, and training state.
3. Open a role-shift event when the accepted role differs from the proposed role.
4. Record the rationale, reviewer, and required follow-up.

Relevant fields: system, operator role, accepted role, risk category, Annex III area, training status, human oversight, action logging, and role-shift state.

Resulting evidence: TraceLock stores the governance record and role-shift history used by the AI governance controls.

Complete AI Questionnaire

Purpose: Capture the organization's answers used for AI governance assessment.

Prerequisites: You have `ai-governance:write` for updates.

Steps

1. Select **AI Questionnaire**.
2. Answer each required governance question.

3. Review the resulting risk and operator-role assessment.
4. Save the questionnaire and follow any reassessment guidance.

Relevant fields: governance answer, AI use case, risk classification, oversight, training, logging, and control evidence.

Resulting evidence: TraceLock stores questionnaire answers and can update the AI posture used by the evaluator.

Maintain AI Inventory

Purpose: Register AI systems and maintain their governance facts.

Prerequisites: You have `ai-inventory:write`.

Steps

1. Select **AI Inventory**.
2. Add or open an AI system.
3. Record provider, purpose, risk, approval, operator role, and governance posture.
4. Record tool scope, human oversight, action logging, and shutdown procedure for an agentic system.
5. Save the record and review any resulting role-shift assessment.

Relevant fields: name, provider, purpose, risk category, approval state, operator role, autonomy level, agentic posture, tools, oversight, logs, and shutdown procedure.

Resulting evidence: The inventory record supplies facts to AI governance controls and role assessment.

Publish Trust Center material

Purpose: Present a read-only public security posture and issue metadata-only evidence downloads when the organization enables the Trust Center.

Prerequisites: You have organization access; `settings:manage` is required to enable the organization Trust Center.

Steps

1. Select **Settings**.
2. Enable the organization Trust Center option.
3. Select **Trust Center**.
4. Review the public posture, control status, exclusions, and evidence metadata.

5. Use a signed download link only when the requester's disclosure terms are accepted.

Relevant fields: public posture, control status, exclusion, evidence hash, retention, organization domain, and signed-link expiry.

Resulting evidence: Trust Center downloads contain metadata only. Evidence download links expire 15 minutes after they are generated.

Understand frameworks

TraceLock's seeded and control-supported framework perspectives include:

Framework	Product use
SOC 2	Crosswalk and control-readiness perspective.
ISO 27001	Crosswalk and control-readiness perspective.
ISO 42001	AI-management-system perspective.
NIST CSF 2.0	Cybersecurity framework perspective.
EU AI Act	AI governance, Annex III, and role-assessment perspective.

The Estate Map also includes mappings for HIPAA, SEC rule, CIS Controls v8, and NIST AI RMF. A mapped control is not evidence of certification or regulatory compliance by itself. TraceLock does not claim that it holds SOC 2 or ISO certification.

Remediate failed controls

Prerequisites: You have access to the failed control; `evidence:write`, `risks:write`, or the applicable management permission is required for changes.

Steps

1. Open the failed control from **Control Center** or **Evidence**.
2. Read the connector message, severity, configuration-drift state, and remediation guidance.
3. Correct the source configuration in the connected provider.
4. Run the connector smoke test or wait for the next scheduled scan.
5. Review the new execution and evidence result.
6. If the requirement cannot be met temporarily, request an exception with a reason and expiry.
7. Have an authorized reviewer approve or reject the exception.
8. Complete the remediation before the exception expires.

Result: A later passing execution updates control verification and produces fresh evidence. An approved exception remains time-bounded; an expired exception requires a new decision.

Troubleshoot common problems

Symptom	Likely cause	Action
Page shows no records	The session is scoped to another organization, or the role lacks the required permission.	Confirm the organization and role in Team and sign in again.
Connector shows not assessed	Credential, target, entitlement, or scheduled credential path is missing.	Review Integration , plan entitlements, and the connector reference.
Evidence is rejected	The Privacy Wall found sensitive text, invalid metadata, or a disallowed region.	Remove sensitive content, submit declared metadata, and use an allowed region.
SAML login fails	Certificate, issuer, audience, clock, or claimed domain does not match.	Use the identity integration troubleshooting table.
SCIM request returns an error	Token is invalid/revoked or the resource operation is unsupported.	Rotate the token and use the supported SCIM operation table.
Trust Center download is unavailable	Trust Center is disabled, the link expired, or disclosure terms were not accepted.	Ask an authorized administrator to enable the Trust Center and request a new link.
A role change is refused	The actor lacks the required permission or the organization is read-only.	Review the permission matrix and lifecycle state with an administrator.
A control remains stale	The scan has not run, or a connector execution is pending or failed.	Review the latest execution log and schedule status on Integration .

Connector configuration reference

Connector lifecycle

Prerequisites

- You have `integrations:manage`.
- Your organization has connector capacity.
- The provider credential is available.

Steps

1. Select **Integration**.
2. Configure the provider-specific credential or role.
3. Connect the provider.
4. Run its smoke test.
5. Review the connection and schedule status.
6. Review resulting controls and evidence in **Control Center**, **Estate Map**, and **Evidence**.
7. Disconnect the provider when access is no longer required.

Result: A connected provider can be resolved by the tenant-scoped connector runner. A missing connection, unavailable credential, failed entitlement, or unsupported schedule records a not-assessed execution rather than inventing a passing result.

Scheduled connector scans are drained every five minutes by `/api/cron/scans`.

AWS

AWS scope and controls

The AWS connector reads:

Read action	Check	Control
<code>iam:GetAccountSummary</code>	Root account MFA	CC6.1
<code>iam:GetAccountPasswordPolicy</code>	IAM password policy	CC6.6
<code>ec2:DescribeRegions</code>	Regional checks	Connector regional posture
<code>s3:ListAllMyBuckets</code>	S3 public access	CC6.6

Read action	Check	Control
s3:GetBucketPublicAccessBlock	S3 public access	CC6.6
s3:GetBucketPolicyStatus	S3 public access	CC6.6
cloudtrail:DescribeTrails	CloudTrail multi-region logging	CC7.1
cloudtrail:GetTrailStatus	CloudTrail multi-region logging	CC7.1
rds:DescribeDBInstances	RDS storage encryption	CC6.1

The customer role name must start with `TraceLockAudit` ; the generated template uses `TraceLockAuditReadOnly` . The role policy grants only the actions in the table, on `Resource: "*"` .

Configure AWS cross-account access

Prerequisites

- An AWS role in the customer account.
- The TraceLock AWS account identifier and the generated external ID.
- Permission to create the read-only role and trust policy.

Steps

1. Download or generate the customer role template from the AWS setup material.
2. Supply the TraceLock AWS account identifier.
3. Supply the external ID displayed for the organization.
4. Deploy the `TraceLockAuditReadOnly` role.
5. Paste the resulting role ARN into **IAM role ARN** on **Integration**.
6. Confirm the customer role trust policy permits `sts:AssumeRole` with the exact external ID.
7. Run the AWS smoke test.

Result: TraceLock obtains short-lived credentials by first assuming its own AWS role with Google web identity, then assuming the customer role with the tenant external ID. A successful check reports that the customer role was assumed and read-only checks completed.

The complete generated policy and activation sequence are in the AWS cross-account setup and AWS integration activation procedures.

AWS evidence and revocation

Evidence metadata includes the source, check identifier, resource type and counts, configuration drift, region, and observation time. Raw long-lived AWS customer credentials are not stored. Revoke by disconnecting AWS in TraceLock and removing or changing the customer role trust policy and external ID.

Google Cloud

Google Cloud scope and controls

The GCP connector uses a service-account bearer credential and reads:

Read	Check	Control
Cloud Storage bucket IAM	Public bucket access	CC6.6
Workforce identity pools	Workforce MFA	CC6.1
Cloud Logging sinks	Audit logging sink	CC7.1
Compute Engine instances	Public IP exposure	CC6.8

Google Cloud configure and revoke

Steps

1. Provide the GCP service-account JSON and project identifier through the configured integration path.
2. Connect the GCP target.
3. Run the scan.
4. Review the four control outcomes.
5. Revoke the service-account credential or remove its project access.

Result: The connector records passed, failed, not-applicable, or indeterminate findings with resource counts and configuration-drift metadata.

GitHub

GitHub scope and controls

The GitHub connector accepts a personal access token and an `owner/repo` target. It reads project metadata, the default branch, and branch protection. It feeds:

Check	Control
Production branch protection	CC8.1

The access-inventory sync also reads organization members, members with two-factor authentication disabled, and membership roles to populate User Access records.

GitHub configure and revoke

Steps

1. Select **Integration**.
2. Enter a GitHub personal access token.
3. Enter a code target in `owner/repo` format.
4. Connect GitHub.
5. Run the smoke test.
6. Review branch-protection evidence and User Access data.
7. Revoke the token in GitHub and select **Disconnect** in TraceLock.

Result: A protected default branch produces a passed `CC8.1` finding; an unprotected branch produces a failed finding. A missing token or invalid target is recorded as not assessed.

Cloudflare

Cloudflare scope and controls

The Cloudflare connector uses `CLOUDFLARE_API_TOKEN` and `CLOUDFLARE_ACCOUNT_ID` when configured. It resolves an account and zone and reads:

Read	Check	Control
<code>always_use_https</code> zone setting	HTTPS edge setting	CC7.1
<code>security_level</code> zone setting	Edge security posture	CC7.1

Cloudflare configure and revoke

Steps

1. Provide the Cloudflare API token and account identifier through the configured integration path.
2. Connect the Cloudflare target.
3. Run the scan.

4. Review the edge-protection finding.
5. Revoke the API token in Cloudflare and disconnect the integration.

Result: TraceLock records whether the zone settings are aligned or require review, together with the zone, account, and configuration-drift metadata.

Fordefi

Fordefi scope and controls

The Fordefi connector uses `FORDEFI_API_KEY` and `FORDEFI_ORGANIZATION_ID`. It reads vaults and transactions and feeds:

Check	Control
Custody and transaction audit	<code>RULE-204-2</code>

The connector records wallet count, transaction count, a wallet address for its ledger representation, custody provider, and posture status. It requires the `custody.enabled` entitlement.

Fordefi configure and revoke

Steps

1. Confirm the organization plan enables custody.
2. Provide the Fordefi API key and organization identifier.
3. Connect and scan the provider.
4. Review the custody posture and ledger metadata.
5. Revoke the API key in Fordefi and disconnect the integration.

Result: The posture is monitored when the connector sees the expected account data and no listed error transaction states.

Turnkey

Turnkey scope and controls

The Turnkey connector uses `TURNKEY_API_KEY` and `TURNKEY_ORGANIZATION_ID`. It reads wallet accounts and policies and feeds:

Check	Control
Custody posture	<code>RULE-204-2</code>

The connector records wallet count, policy count, a wallet address, custody provider, and posture status. It requires the `custody.enabled` entitlement.

Turnkey configure and revoke

Steps

1. Confirm the organization plan enables custody.
2. Provide the Turnkey API key and organization identifier.
3. Connect and scan the provider.
4. Review wallet and policy posture.
5. Revoke the API key in Turnkey and disconnect the integration.

Result: The posture is monitored when wallet accounts and policies are present.

Access inventory

Access inventory is implemented for GitHub and GCP. GitHub records organization members, roles, MFA state, and administrator-level excessive-access flags. GCP records user IAM members, their roles, and excessive-access flags; GCP records are treated as MFA-active by the sync implementation.

The User Access Review page can show over-privileged, MFA-missing, and inactive records. A missing credential or target causes the sync to be skipped with a reason.

Universal webhook evidence

The universal webhook is an evidence ingestion path rather than a provider credential connector. It requires a tenant-derived HMAC signature, an organization identifier, an event identifier, a message, metadata, a control code, and a region. It hashes the raw payload, applies the Privacy Wall, and writes an evidence-backed finding. The **Webhook Log** page displays the event type, hash, received time, payload length, and seven-year SEC 204-2 WORM retention clock.

Revoke or rotate the configured custom webhook secret and update the sender. Do not send credentials or sensitive payload content in the webhook.

Log feed

Log feed scope and controls

The `LOG_FEED` evidence connector uses `LOG_FEED_URL` and `LOG_FEED_TOKEN`. It fetches the configured log feed with a bearer token and feeds:

Check	Control
Append-only diagnostic evidence feed	CC7 . 2
Evidence archive posture	RULE - 204 - 2

Log feed configure and revoke

Prerequisites

- You have `integrations:manage`.
- An append-only diagnostic feed URL and bearer token are available.

Steps

1. Provide the log-feed URL and token through the configured integration path.
2. Connect the log feed.
3. Run the smoke test.
4. Review the append-only diagnostic evidence result.
5. Revoke the bearer token at the feed and disconnect the integration.

Result: TraceLock records the provider mode and an evidence-backed `CC7 . 2` finding. A live mode fetch confirms that the configured feed can be reached.

Privacy Wall and evidence behavior

All connector evidence passes through the Privacy Wall. It retains declared metadata keys, rejects sensitive text patterns, canonicalizes accepted metadata, computes a SHA-256 hash, and enforces the allowed region. The evidence writer persists a metadata record and refreshes the control verification time by default.

If a connector is disconnected, cannot decrypt its credential, is not entitled, or returns an unsupported execution, TraceLock records a not-assessed attempt and does not turn the missing observation into a pass.

Verify the Privacy Wall

Your security reviewer should not have to take the Privacy Wall on trust. This chapter shows you how to confirm, using your own tenant, what TraceLock stores and what it discards.

What the Privacy Wall does

Every evidence write passes through four stages before anything is persisted:

1. **Inspection** — the metadata is walked recursively and tested for email addresses, national identifiers, payment card numbers, and telephone numbers. A match on a field that is not a declared owner or learner address rejects the write.
2. **Allowlist reduction** — only declared posture keys survive: provider, control code, status, severity, freshness, region, resource type and count, configuration drift, timestamps, framework references, and similar attributes. Everything else is dropped rather than stored.
3. **Canonicalization** — remaining keys are sorted deterministically so that the same posture always produces the same stored form.
4. **Digest and residency** — a SHA-256 digest is computed over the canonical form, and the declared region is checked against the residency allowlist.

The consequence for you: TraceLock cannot disclose provider payloads, log contents, object contents, or customer records, because it never stores them.

Procedure: inspect a stored evidence record

Prerequisites

- You are signed in with a role that can view evidence.
- At least one connector has completed a scan.

Steps

1. Open **Evidence**.
2. Select a record produced by a connector — its type is `AUTOMATED`.
3. Review the stored metadata.
4. Note the recorded digest, the source provider, the observation timestamp, and the retention clock end.

Result: the record contains posture attributes and provenance only. There is no provider response body, no resource content, and no end-user identity.

Procedure: recompute a digest independently

Prerequisites

- You have exported or copied the canonical metadata of an evidence record.
- You have a local environment with Python 3 or Node.js.

Steps

1. Save the metadata object to a file, for example `metadata.json`.
2. Recompute the digest over the canonical form:

```
python3 - <<'PY'
import hashlib, json
with open("metadata.json") as handle:
    metadata = json.load(handle)
canonical = json.dumps(metadata, sort_keys=True, separators=(",", ":"))
print(hashlib.sha256(canonical.encode()).hexdigest())
PY
```

3. Compare the output with the digest recorded on the evidence record.

Result: the digests match, which confirms that the record you are reading is the record that was collected and hashed.

Important Compute the digest over the canonical form — keys sorted, no insertion whitespace. A digest computed over reordered or pretty-printed JSON will not match, and the mismatch is a formatting artifact rather than an integrity failure.

Procedure: confirm rejection behaviour

Prerequisites

- You can send a webhook event to your workspace, or you have a connector under your control.

Steps

1. Send a test event containing a value that looks like personal data — for example an email address — in a field that is not a declared owner field.
2. Open **Webhook Log**.
3. Review the outcome recorded for the event.

Result: the submission is rejected at the Privacy Wall rather than being stored with the value redacted. Rejection, not silent sanitization, is the designed behaviour: it surfaces an over-collecting integration instead of hiding it.

What leaves TraceLock

Text sent to destinations you configure — Slack, email, webhooks, Jira, ServiceNow — passes through an outbound redaction pass and a length bound. Notifications therefore carry the control code, status, severity, and remediation reference, not environment detail. If your policy prohibits any compliance signal in chat, route notifications to email or webhook only.

Answers for your security questionnaire

Question	Answer
Is software installed in our environment?	No. Connections are outbound API calls from Odingard's environment.
What data is stored?	Allowlisted posture attributes, provenance, digests, and the owner addresses you supply.
Is customer or personal data stored?	No, other than the owner and learner addresses required for ownership and assignment.
Can TraceLock change our environment?	No. Credentials are read-only and there is no write path to your providers.
How is data protected in transit and at rest?	TLS 1.2 or later in transit; managed encryption at rest; connector credentials under envelope encryption with key material in a managed secret store.
Can we revoke access unilaterally?	Yes. Revoke the credential at your provider; affected controls then report as indeterminate.
How do we verify evidence independently?	Recompute SHA-256 over the canonical metadata and compare with the recorded digest.

Continuous monitoring and framework mapping

Once your connectors are running, TraceLock evaluates your control library on a schedule and projects every result onto the frameworks you report on. This chapter covers how to read that output and how to make it yours.

Read control state

Open **Control Center** to see the full control library with code, title, owner, status, and last verification time.

Status	What it means	What you do
Passed	Evaluated and satisfied	Nothing; confirm the verification time is current
Failed	Evaluated and not satisfied	Remediate, or record an exception with a rationale and expiry
Indeterminate	Evaluation could not conclude, usually lost connector permission	Restore the connector's read access
Not applicable	The control does not apply to your environment	Confirm the determination is still correct
Exempt	An approved exception is suppressing the finding	Track the expiry date
Not started	No evaluation recorded yet	Connect the provider the control depends on

Important Indeterminate is not a pass and not a failure. It means TraceLock lost the visibility required to judge the control. Treat it with the same urgency as a failure, because an audit will.

Check freshness, not just status

Each control records when it was last verified. A control that passed six weeks ago and has not been verified since is not evidence of a working control; it is evidence of a stalled connector. Sort **Control Center** by last verification and investigate anything outside its expected cadence.

Review framework coverage

Open **Estate Map** to see coverage across every framework perspective. Because all frameworks are projections of the same evaluations, a single failing control appears consistently everywhere it is mapped — a control cannot be green in your SOC 2 view and red in your ISO view.

Framework	Reference granularity you will see
SOC 2	Trust services criteria
ISO/IEC 27001	Annex A controls
NIST CSF 2.0	Function and category outcomes
HIPAA Security Rule	Safeguard citations
SEC	Rule references
CIS Controls v8	Control and safeguard families
NIST AI RMF	Function-level references
ISO/IEC 42001	Clause references
EU AI Act	Article references

Controls with no mapping for a framework are shown as unmapped rather than assumed satisfied. An unmapped control is a deliberate statement that no defensible mapping exists.

Note Have your compliance reviewer confirm the mappings that matter to your audit before you submit them as a deliverable. The references are curated to be checkable for exactly this purpose.

Assign owners

Prerequisites

- You have a role that can manage controls.

Steps

1. Open **Control Center** and select a control.
2. In the control detail view, set the owner.
3. Repeat for every control your organization relies on.

Result: findings, evidence expiry, and remediation notifications for that control are addressed to an accountable person rather than to a shared inbox.

Record an exception

Use an exception when you accept a gap deliberately and for a bounded period.

Steps

1. Open the control and select the finding you intend to accept.
2. Create an exception with a rationale, an owner, and an expiry date.
3. Submit it for approval according to your internal process.

Result: the control reports as exempt, the underlying evaluation continues, and the original state returns automatically at expiry. Exceptions are recorded in audit history and are shown to auditors with their rationale and expiry — they suppress noise, not accountability.

AI governance obligations

If your organization builds, buys, or operates AI systems, the AI surfaces carry the determinations that a control status alone cannot express.

1. Open **AI Governance** for your current obligations and status.
2. Complete the **AI Questionnaire** to record your role — provider or deployer — for each system.
3. Maintain the **AI Inventory** with each system's autonomy level, operator role, EU AI Act risk category, and Annex III high-risk area where applicable.
4. Review role-shift alerts. A change in how you use a system can move you from deployer to provider obligations, which materially expands what the EU AI Act requires of you.

Result: AI systems are evaluated against ISO/IEC 42001 clauses, NIST AI RMF functions, and EU AI Act articles alongside your security controls, using the same evidence and the same crosswalk.

Evidence lifecycle

Evidence is written automatically on every evaluation, deduplicated by digest so unchanged posture does not inflate your evidence set, and retained for seven years from observation by default. Approaching expiry raises a notification to the control owner so that a control does not silently lose its substantiation. Upload manual evidence — penetration test reports, signed policies, vendor attestations — from **Evidence**, where it is stored with a digest and retention clock alongside connector output.

Remediation, alerting and ticketing

A finding is only useful if it reaches the person who can fix it. This chapter covers how TraceLock routes findings and how to close them.

Notification triggers

TraceLock raises four notification triggers.

Trigger	Raised when
Control failed	A control evaluation returns a failing result
Evidence expired	An evidence record approaches or passes its retention clock end
Training overdue	An assigned training item passes its due date
AI role shift	A change moves your organization between deployer and provider obligations

Queued deliveries are drained every five minutes, and each delivery attempt is recorded so a missed alert is diagnosable.

Configure destinations

Prerequisites

- You have a role that can manage workspace settings.
- For Slack, you have an incoming webhook URL. For a custom endpoint, you have an HTTPS URL that can accept a signed POST.

Steps

1. Open **Settings** → **Notifications**.
2. Add a destination and select its channel: Slack, email, or webhook.
3. Select the triggers the destination should receive.
4. Send a test delivery.
5. Confirm receipt at the destination, then save.

Result: matching events are delivered to the destination. Message content is passed through outbound redaction and a length bound, so it carries control codes, statuses, severities, and remediation references rather than environment detail.

Configure ticketing

Connect Jira or ServiceNow so that a failing control opens a work item in the system your engineers already use.

Prerequisites

- The base URL of your instance.
- A service account with permission to create issues in the target project.
- An API token for that account.
- For Jira, the project key. For ServiceNow, the destination table or team identifier.

Steps

1. Open **Settings** → **Integrations** → **Ticketing**.
2. Select your provider and enter the base URL, project or team identifier, and account email.
3. Enter the API token. It is stored encrypted and is never displayed again.
4. Run the connection test.
5. Save the configuration.

Result: failing controls create an issue containing the control code, the finding summary, the remediation guidance, and a link back to the control in TraceLock. The token is held under envelope encryption and is not returned by any API.

Caution Use a dedicated service account rather than a personal account. When a personal account is disabled during offboarding, ticket creation stops silently and findings stop reaching your engineers.

Remediate a failing control

Steps

1. Open **Control Center** and select the failing control.
2. Read the finding: what was observed, on which provider, and when.
3. Follow the remediation guidance in the control detail view.
4. Apply the change in your own environment.
5. Wait for the next scheduled scan, or trigger a scan from the connector, and confirm the control returns to passed.

Result: the control passes, a new evidence record with a new digest is written, and the prior record remains in place as the history of the earlier state.

Note Do not close a finding by editing evidence or by deleting the control. Both leave a gap that an auditor will find. If you accept the gap deliberately, record an exception with a rationale and expiry — that is a defensible position; a missing record is not.

Findings that will not clear

Symptom	Likely cause	Action
Control stays failed after you fixed the environment	The next scan has not run yet	Wait for the cadence or trigger a scan
Control turns indeterminate after your fix	The change narrowed the connector's read permission	Restore the read scope, then rescan
Control passes but evidence is stale	The connector is authenticating but not returning the resource	Run the connector smoke test and check the provider's scope
Notifications stopped	The destination revoked the webhook or the ticket account was disabled	Re-test the destination in settings

Track remediation progress

The dashboard reports failing controls by severity and framework impact, so you can prioritise the failures that block the audit you are actually preparing for. Owner assignment makes each item attributable, and the audit history records who changed a control's state, who approved an exception, and when — which is the record your auditor will ask for when they ask how the finding was resolved.

Auditor Room and evidence verification

The Auditor Room is how you give an external auditor or examiner read access to your controls and evidence without giving them a seat in your workspace, adding them to your identity provider, or exporting a spreadsheet that immediately goes stale.

How auditor access works

Access is granted as a signed, time-bound capability rather than as an account.

Property	Value
Scope	Read-only, bound to your organization
Lifetime	15 minutes from issue
Method restriction	Read requests only; no write path exists
Surfaces	Controls, evidence, evaluation history, comments, export
Excluded	Administration, billing, identity configuration, connector credentials
Credential	A dedicated auditor session, separate from your users' sessions

The organization identifier is inside the signed payload, so the link cannot be altered to reach another tenant, and it cannot be escalated by an existing browser session.

Procedure: provision auditor access

Prerequisites

- Your plan includes Auditor Room provisioning.
- You have a role that can manage the workspace.
- You have the auditor's email address.

Steps

1. Open the Auditor Room provisioning surface in workspace settings.
2. Enter the auditor's email address.
3. Issue the access link.
4. Send the link to the auditor through your normal secure channel.

Result: the auditor opens a read-only view of your organization. The link expires 15 minutes after issue.

Important Access links are short-lived by design. For a multi-day engagement, expect to issue a link at the start of each working session rather than issuing one long-lived credential. This is what keeps an old link from being a standing door into your evidence.

Procedure: revoke auditor access

Steps

1. Stop issuing new links to the auditor.
2. Confirm the engagement is closed in your own records.
3. If you need immediate invalidation of every outstanding link, contact Odingard support to request rotation of the auditor signing key.

Result: outstanding links expire within their 15-minute window; key rotation invalidates all of them at once.

What the auditor sees

- The control library with codes, titles, owners, statuses, and last verification times.
- Framework mappings at criterion, clause, and article level for all nine frameworks.
- Evaluation history per control.
- Evidence records with type, source provider, description, digest, observation timestamp, and retention clock.
- Exceptions with rationale, owner, and expiry.
- Audit history for privileged and control-affecting actions.

The auditor cannot change a status, resolve a finding, upload evidence, approve an exception, view connector credentials, or see any other organization's data.

Procedure: export an audit package

Steps

1. In the Auditor Room, open the export surface.
2. Select the scope of the package: the framework, the control set, or the evidence period.
3. Generate and download the export.

Result: a package containing the control set with framework mappings, evaluation history, evidence records with digests and timestamps, and exceptions with their rationale. The package is verifiable offline, so the auditor's conclusions do not depend on further access to TraceLock.

Procedure: verify evidence independently

Give this procedure to your auditor. It requires nothing from Odingard.

Steps

1. Take an evidence record from the export.
2. Serialize its metadata in canonical form — object keys sorted, no added whitespace.
3. Compute SHA-256 over that serialization:

```
python3 - <<'PY'
import hashlib, json
with open("artefact.json") as handle:
    artefact = json.load(handle)
canonical = json.dumps(artefact["recorded_custody_metadata"], sort_keys=True, separators=(",", ":")
digest = hashlib.sha256(canonical.encode()).hexdigest()
print("recomputed:", digest)
print("recorded:  ", artefact["sha256_digest"])
print("match:     ", digest == artefact["sha256_digest"])
PY
```

4. Compare the recomputed digest with the recorded digest.
5. Confirm the observation timestamp precedes the recording timestamp, and that both precede the retention clock end.
6. Confirm the observation timestamp is consistent with the control's evaluation history.

Result: a record whose digest recomputes and whose timestamps agree with the control history is a record that has not been altered since collection.

Preparing for a SOC 2 Type II or ISO 27001 engagement

1. Resolve every indeterminate control, so the auditor sees judgements rather than gaps in visibility.
2. Confirm control owners are current, including for controls whose owner has left the organization.
3. Review evidence freshness across the audit period and re-run connectors that have gone stale.
4. Review open exceptions and either close them or confirm the rationale and expiry are accurate.
5. Upload manual evidence — penetration tests, signed policies, vendor attestations — so the package is complete.

6. Have your compliance reviewer confirm the framework mappings you intend to submit.
7. Provision auditor access at the start of the engagement and reissue per session.

Workspace administration

Organization setup

Create an organization

Prerequisites

- You have a work email address.
- You can choose an organization name.

Steps

1. Open the TraceLock sign-up page.
2. Enter **Your name**.
3. Enter **Organization**.
4. Enter **Work email**.
5. Select **Create workspace**.
6. Follow the secure link sent to your email address.
7. Set a password when TraceLock prompts you.

Result: TraceLock creates a local account and organization projection and lets you sign in to the workspace.

Update the organization profile

Prerequisites

- You have `settings:manage`.

Steps

1. Select **Settings**.
2. Update **Organization name**.
3. Select or clear the public Trust Center option.
4. Select **Save profile**.

Result: TraceLock saves the organization profile. The settings page displays custom-domain and verification state when configured.

Roles and permissions

TraceLock defines four permission roles. `ADMIN` has all 18 permissions. `CLIENT_OWNER` has every permission except `platform:admin`. `CLIENT_USER` and `AUDITOR` have no permissions in the role fallback matrix. The application uses the effective permissions carried by the tenant scope when a membership is resolved.

Permission	ADMIN	CLIENT_OWNER	CLIENT_USER	AUDITOR
<code>evidence:write</code>	Yes	Yes	No	No
<code>policies:write</code>	Yes	Yes	No	No
<code>audits:write</code>	Yes	Yes	No	No
<code>training:write</code>	Yes	Yes	No	No
<code>risks:write</code>	Yes	Yes	No	No
<code>risk-exceptions:approve</code>	Yes	Yes	No	No
<code>findings:exclude</code>	Yes	Yes	No	No
<code>ai-inventory:write</code>	Yes	Yes	No	No
<code>ai-governance:write</code>	Yes	Yes	No	No
<code>controls:manage</code>	Yes	Yes	No	No
<code>user-access:manage</code>	Yes	Yes	No	No
<code>pentests:write</code>	Yes	Yes	No	No
<code>domains:manage</code>	Yes	Yes	No	No
<code>integrations:manage</code>	Yes	Yes	No	No
<code>settings:manage</code>	Yes	Yes	No	No
<code>billing:manage</code>	Yes	Yes	No	No
<code>org:manage</code>	Yes	Yes	No	No

Permission	ADMIN	CLIENT_OWNER	CLIENT_USER	AUDITOR
platform:admin	Yes	No	No	No

Change a member role

Prerequisites

- You can manage the organization membership.
- The target member is active.

Steps

1. Select **Team**.
2. Find the member in **Organization members**.
3. Select the new role.
4. Enter a reason when TraceLock asks for **Reason for this role change**.
5. Confirm the change.

Result: TraceLock updates the membership and records an access-history event with the subject, actor, role change, actor kind, and reason.

Invite and deprovision users

Invite a teammate

Prerequisites

- You have the permission required to manage team membership.
- You know the teammate's email address and intended role.

Steps

1. Select **Team**.
2. In **Invite a teammate**, enter **Email address**.
3. Select **Role**.
4. Select **Send invite**.
5. Copy the resulting **Invitation link** if you need to deliver it through an approved channel.

Result: The invitation appears in **Pending invitations** until it is accepted, revoked, or expires. The available invitation roles are Owner, Member, and Auditor.

Revoke an invitation

1. Select **Team**.
2. Find the invitation in **Pending invitations**.
3. Select **Revoke**.

Result: The pending invitation can no longer be used.

Deprovision a user

Use SCIM deprovisioning for an identity-provider-managed user. A SCIM deactivation sets `deactivatedAt`, removes the organization membership, invalidates tenant scope immediately, and preserves the user and audit evidence. A SCIM reactivation clears `deactivatedAt` and restores membership with the user's role.

For a local membership change, use the team role controls and the approved organization access process.

Configure MFA enforcement

Prerequisites

- You can manage organization settings.
- Members can access an authenticator application.

Steps

1. Sign in with your TraceLock account.
2. Open the MFA enrollment page.
3. For first enrollment, select **Generate enrollment secret**.
4. Scan the displayed QR code with an authenticator application.
5. If scanning is unavailable, enter the displayed secret manually.
6. Enter the current value in **Authenticator code**.
7. Select **Confirm MFA**.
8. If re-enrolling, enter **Current MFA code (only for re-enrollment)** first.

Result: The account has a local TOTP enrollment. SAML users use IdP MFA and are not enrolled in local TOTP. Local accounts enroll from the MFA page.

Plans and entitlements

The local billing entitlement matrix defines these plans:

Plan	Connector limit	Monitored-user limit	Custody	MCP	User access review	Custom domain	TPRM	AI Act	SSO and SCIM	Auditor room
Starter	3	20	No	No	No	No	No	No	No	No
Growth	10	100	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Enterprise	100	500	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Enterprise auditor-room capacity is unlimited in the base entitlement matrix. Subscription add-ons can add three connectors per extra connector pack, add monitored-user overage units, add one auditor room for non-Enterprise plans, and enable premium support when the subscription carries that setting. The catalog also defines white-glove onboarding, premium support, monitored-user overage, extra connector packs, and extra auditor rooms as add-ons.

When no active or trialing local subscription is present, TraceLock returns Starter feature flags with connector and monitored-user limits set to zero. An entitlement decision can also come from the configured Studio billing path when both Studio authentication and Studio billing are enabled.

Change a plan

Prerequisites

- You have `billing:manage`.
- You have an approved billing method or marketplace procurement path.

Steps

1. Select **Billing**.
2. Review the current plan, billing status, interval, add-on quantities, and current entitlements.
3. Choose the plan or add-on action presented by the billing page.
4. Complete the provider checkout or procurement flow.
5. Return to **Billing** and confirm the active subscription and entitlements.

Result: The active subscription and add-on quantities resolve to the plan limits and feature flags shown in the workspace. A workspace without an active subscription remains fail-closed for paid features.

Manage connectors and credentials

Prerequisites

- You have `integrations:manage`.
- The organization plan includes the connector or you have available connector capacity.
- You have the provider credential or role configuration.

Steps

1. Select **Integration**.
2. Review the current connection status and scan status.
3. Enter the provider-specific fields.
4. Select the provider connection control.
5. Run the provider smoke test.
6. Review the checks and the queued baseline scan.
7. Select **Disconnect** when the credential must be removed.

Result: The connection status, last scan, schedule status, and latest error appear in the integration view. Disconnecting deletes the stored credential.

Rotate a provider credential at the provider first, connect with the replacement, run a smoke test, and then revoke the old provider credential. For SAML certificates and SCIM tokens, use the overlap procedures in the the identity integration chapter. For AWS, use the external-ID procedure in the connector configuration reference.

Configure a custom domain

Prerequisites

- The plan includes `customDomain.enabled`.
- You have `domains:manage`.
- You control the domain's DNS.

Steps

1. Select **Settings**.
2. Review **Custom domain** and its verification state.
3. Add the CNAME and ownership TXT records shown by the Trust Center configuration.
4. Select **Refresh status**.
5. Confirm the state changes to **Verified**.

Result: TraceLock stores the custom domain and displays its verification state. The Trust Center page states that Cloudflare for SaaS provides the CNAME and ownership TXT record.

Lifecycle states

State	Meaning	Tenant effect
ACTIVE	Normal organization operation.	Tenant reads and writes are allowed when the caller has the permission.
SUSPENDED	Organization is suspended.	Writable tenant operations return a read-only response; reads may continue.
OFFBOARDING	Organization is being offboarded.	Writable tenant operations return a read-only response while offboarding continues.
OFFBOARDED	Organization is offboarded.	Tenant scope returns no access.

The platform lifecycle console is not available to customers. Organization administrators should use the documented support or procurement process for organization-level lifecycle changes.

Caution: Offboarding and deletion can remove access or data for the entire organization. Verify the target organization, retention requirements, and approvals before taking action.

Review privileged audit history

The Team page displays access-history events for membership role changes. Identity provisioning writes SAML and SCIM access-audit events. The platform administration console records cross-tenant lifecycle and deletion actions in `PlatformActionLog`.

Review the hosting, security and tenant isolation chapter for logging, evidence retention, and recovery boundaries.

Export and delete data

TraceLock provides these export surfaces:

- Training assignments can be exported as CSV.
- User access review details can be exported as CSV.
- Auditor sessions can export an evidence package.
- Public Trust Center visitors can request a metadata-only evidence package after accepting the click-through non-disclosure terms; the signed link expires after 15 minutes.

The platform organization console supports permanent deletion only for approved platform staff. It requires the exact organization name and records refusal rules such as protected baseline, active subscription, and self-organization checks. Use the supported export surfaces before contacting TraceLock Support about organization-wide deletion.

Platform administration

Platform administration is an Odingard-staff-only surface. It requires both the `platform:admin` permission and membership in the `TRACELOCK_BILLING_RECONCILIATION_ALLOWLIST` staff allowlist. It provides cross-tenant organization counts, plan and lifecycle breakdowns, recent `PlatformActionLog` activity, lifecycle controls, deletion controls, and a raw diagnostics JSON link. It is not available to customers.

Hosting, security and tenant isolation

Architecture and hosting

TraceLock is a vendor-hosted software-as-a-service application delivered from Google App Engine Standard. The documented runtime is Node.js 22 on F2 instances, with automatic scaling configured from zero to four instances. The application and connector orchestration run in a dedicated Odingard-owned Google Cloud project in `us-west1`. Cloud SQL for PostgreSQL 16 is the data plane and the only system of record for tenants, controls, findings, evidence, audit history, and entitlements.

The production hostname is `https://tracelock.odingard.com`. Google Frontend terminates TLS for the custom hostname. Cloudflare is authoritative DNS for the parent domain; the documented hostname is an unproxied CNAME, so Cloudflare does not provide an application proxy or web application firewall in this path.

TraceLock is not installed into a buyer's Google Cloud project, another cloud provider, or an on-premises environment. There is no customer-side agent, virtual machine image, Kubernetes chart, or customer deployment in the documented model.

Component tenancy

Component	Boundary	Function
App Engine Standard	Odingard Google Cloud tenant, <code>us-west1</code>	TraceLock UI, APIs, connector orchestration, cron, MCP, auditor room, and application services.
Cloud SQL for PostgreSQL 16	Odingard Google Cloud tenant, <code>us-west1</code>	Tenants, controls, findings, evidence, audit history, and entitlements.
Secret Manager	Google-managed, project-scoped	Runtime credentials and connector configuration.
Cloud KMS	Google-managed, project-scoped	Key custody for tenant-safe derived identifiers.
IAM	Google-managed, project-scoped	Least-privilege service identities.
Cloud Logging, Monitoring, and Trace	Google-managed, project-scoped	Application and audit logs, health and latency signals, and request tracing.

Component	Boundary	Function
Cloud Build	Google-managed, project-scoped	Source-to-deploy build for App Engine.
App Engine cron	Odingard Google Cloud tenant, us-west1	Scheduled scans, training, evidence expiry, and notification delivery.
Google Cloud Marketplace	Google-operated commerce surface	Buyer purchase and plan lifecycle.
Stripe	Stripe-hosted SaaS	Direct card billing and billing webhooks.
Resend	Resend-hosted SaaS	Transactional email delivery.
GitHub Actions	GitHub-hosted SaaS	Continuous integration and App Engine deployment.
Cloudflare	Cloudflare-hosted SaaS	Authoritative DNS only for the documented TraceLock hostname.
Customer cloud, code, and custody systems	Customer-owned environment	Read targets for configured scans; no TraceLock component is deployed there.

The component tenancy model is documented in the component tenancy reference.

Tenancy and isolation

TraceLock stores each organization's local projection and scopes application queries with the organization identifier. The server-side tenant scope carries the authenticated user, organization, role, lifecycle state, and permissions. Connector execution resolves a connection using both its identifier and organization identifier. Evidence, findings, control execution logs, user access records, and integration state are persisted with the organization boundary.

SAML connections, SCIM tokens, users, memberships, integrations, controls, evidence, and action history are organization-scoped. SCIM requests authenticate to a token whose organization is used for every user query. Auditor links and Trust Center downloads also resolve the requested organization before returning data.

Data classification and storage

Data class	TraceLock storage or handling
Account and organization data	Local user, membership, organization, role, lifecycle, and entitlement records in Cloud SQL.
Compliance configuration	Controls, framework references, policies, audits, risks, training, and questionnaire assessments in Cloud SQL.
Connector metadata	Provider, control code, status, resource counts, regions, timestamps, and configuration-drift metadata.
Evidence metadata	Content hash, type, description, source provider, file reference when present, sanitized metadata, and retention clock.
Credential material	Connector tokens are encrypted before persistence; SCIM tokens and SAML login tokens are stored as digests or hashes.
AI governance records	AI system inventory, role assessment, governance fields, role-shift events, and hashes of local agent activity.
Raw provider payloads	Only fields accepted by the Privacy Wall are retained in evidence metadata; rejected sensitive text is not persisted as accepted evidence.

Ask your Odingard account team for the current data-retention schedule, encryption configuration detail, provider revocation SLA, and subprocessor list as part of the assurance package.

Encryption and key management

The connector token envelope uses versioned AES-GCM encryption. Version 2 generates a random 32-byte data key, encrypts that key with a master key, uses independent initialization vectors, and stores the envelope version, wrapped key, IVs, and ciphertext. The implementation derives the master-key bytes from `TRACELOCK_KMS_MASTER_KEY`; deployment maps that secret from Secret Manager.

SAML login tokens and SCIM bearer tokens are not stored in plaintext: the code stores SHA-256 digests and compares candidate digests using a timing-safe comparison. AWS external IDs are derived with an HMAC-based organization-bound value when a connection does not already have one.

The hostname is served through Google Frontend with TLS termination. Cloud SQL, Secret Manager, and Cloud KMS are Google-managed services in the documented architecture.

Secret handling

The deployment script maps database URLs, authentication secrets, connector credentials, billing secrets, the master key, and the platform-staff allowlist to Secret Manager values. Secret values are not included in TraceLock's evidence inventory. Connector tokens are decrypted only when the connector runner needs to execute a scan. Disconnecting an integration deletes its stored credential through the integration route.

Do not place credentials in a ticket, webhook payload, source file, or support request. Do not copy a SCIM token, SAML certificate, or AWS external ID into a public location.

Customer-environment access

TraceLock reads customer systems outbound from the Google Cloud partner tenant. TraceLock supports these customer targets:

Target	Access model	Scope
Customer AWS account	<code>AssumeRoleWithWebIdentity</code> , then <code>AssumeRole</code> with a tenant external ID	Temporary credentials and the exact read-only actions in the AWS template.
Customer Google Cloud project	Service-account bearer credential	Storage IAM, workforce MFA, logging sinks, and Compute public-IP posture reads.
Customer GitHub project or organization	GitHub token	Branch-protection and access inventory reads.
Customer Cloudflare zone	Cloudflare API token and account or zone lookup	HTTPS and security-level posture reads.
Customer Fordefi account	Fordefi API key and organization identifier	Vault and transaction posture reads.
Customer Turnkey account	Turnkey API key and organization identifier	Wallet-account and policy posture reads.

The customer can revoke access by removing the IAM role trust relationship, revoking the provider token or API key, disconnecting the integration in TraceLock, or removing the customer-side service-account permission.

Least-privilege setup details are in the connector configuration reference.

Privacy Wall and data minimization

The Privacy Wall:

1. accepts a declared set of metadata keys;
2. rejects sensitive text patterns unless the field is an explicitly declared email field;
3. canonicalizes and sorts accepted metadata;
4. computes a SHA-256 data hash; and
5. enforces the configured allowed region.

The evidence writer persists sanitized metadata, the hash, observation time, source provider, control code, and a seven-year retention clock by default. A universal webhook uses tenant-derived HMAC authentication and validates payload shape before it creates evidence.

Logging, monitoring, and retention

TraceLock uses Cloud Logging, Monitoring, and Trace in the documented Google Cloud architecture. Application routes expose health and readiness surfaces. Privileged lifecycle and deletion actions are written to `PlatformActionLog`. Identity provisioning writes access-audit events. Control execution logs preserve connector status, reason data, and evidence hashes.

Evidence metadata created by the evidence writer defaults to a retention end seven years after observation. The universal webhook view describes this as a seven-year SEC 204-2 WORM retention clock. This describes the implemented evidence metadata behavior; it is not a statement that TraceLock is a registered broker-dealer or that every stored record has the same retention.

Availability, backup, and recovery

The documented Cloud SQL instance is zonal, with no standby or automatic failover. Regional high availability is planned remediation rather than a current property. Automated backups run at 00:00 UTC with seven retained backups, and point-in-time recovery retains seven days of transaction logs. The practical recovery point is on the order of seconds while the required transaction logs remain available.

Recovery creates and validates a replacement Cloud SQL instance, updates the App Engine attachment and database URL secrets, deploys a candidate, health-gates it, and promotes traffic. Read the Disaster Recovery Runbook before a recovery exercise.

Vulnerability management and dependency scanning

TraceLock's CI security pipeline includes:

- Gitleaks for secret scanning;
- Semgrep for static analysis; and
- `npm audit --audit-level=high` for dependency auditing.

The deployment workflow applies guarded additive Prisma schema changes before deploying a candidate. Destructive schema changes fail closed in the documented deployment path.

Subprocessors and external services

TraceLock uses the following vendor-hosted services outside the Google Cloud application and data plane:

Service	Function	Request-path role
Cloudflare	Authoritative DNS	DNS only for <code>tracelock.odingard.com</code> ; no proxy or WAF in the documented path.
Stripe	Direct billing	Billing requests and webhooks only.
Resend	Transactional email	Outbound email only.
GitHub Actions	CI and deployment	Build and deployment only, not runtime.
Sentry	Optional error reporting	Active only when <code>SENTRY_DSN</code> is configured; it is not configured in production.

Responsible disclosure

Report suspected vulnerabilities using the process in the support and service levels chapter.

Compliance posture

TraceLock includes controls and framework mappings for compliance work, including SOC 2, ISO 27001, ISO 42001, NIST perspectives, and the EU AI Act. The Estate Map also exposes NIST CSF 2.0, HIPAA, SEC rule, and CIS Controls v8 perspectives where the control crosswalk contains a mapping.

These mappings and product controls do not establish that TraceLock holds a SOC 2 or ISO certification. TraceLock's own SOC 2 program is in progress. Ask your Odingard account team for the current assurance package.

Support and service levels

Note: These service levels describe TraceLock's standard support program. Service levels for a specific subscription are governed by the applicable order form or private offer.

Contact TraceLock Support

Email TraceLock Support at support@odingard.com. Include your organization name, the affected page or integration, the time of the event, and the observed behavior.

Support hours are 09:00–18:00 Pacific Time, Monday to Friday, excluding United States public holidays. Severity 1 requests from Enterprise subscriptions are handled 24×7.

Escalate a request

Reply to the existing support thread with **Escalate** in the subject line. Escalation is owned by the TraceLock service owner.

Severity and initial response

Severity	Definition	Target initial response
Severity 1	TraceLock is unavailable, or control monitoring and evidence collection have stopped for an entire organization, or a confirmed security incident affects customer data.	1 hour, 24×7 (Enterprise); next business hour (Starter and Growth).
Severity 2	A major function is degraded with no workaround: a connector repeatedly fails to collect, single sign-on or SCIM provisioning is broken, or evidence cannot be exported.	4 business hours.
Severity 3	A function is impaired and a workaround exists, or a single control or record behaves incorrectly.	1 business day.
Severity 4	A question, documentation request, or feature request.	2 business days.

Response targets measure TraceLock's initial substantive response, not resolution.

In scope and out of scope

In scope

TraceLock support covers product behavior questions and operational investigation for:

- tenant-scoped controls, evidence, findings, and execution history;
- local authentication, SAML SSO, SCIM provisioning, and MFA;
- configured cloud, code, custody, and webhook integrations;
- connector collection failures and Privacy Wall rejection;
- workspace lifecycle, access, and entitlement behavior;
- Trust Center and Verification Room behavior.

Out of scope unless separately agreed

- changes to a customer's identity provider, cloud account, code host, or custody provider;
- customer-side policy decisions, risk acceptance, or legal determinations;
- recovery of customer credentials that were not provided to TraceLock;
- unsupported integrations or provider APIs not supported by TraceLock;
- a certification or compliance attestation on behalf of the customer.

Do not include passwords, connector tokens, SAML certificates, SCIM bearer tokens, or unredacted sensitive payloads in a support request.

Maintenance and releases

TraceLock deploys continuously. Releases do not require a scheduled maintenance window or customer downtime. TraceLock notifies subscription administrators at least 5 business days before any change that requires customer action, such as an identity or connector configuration change.

Security incidents

TraceLock notifies affected subscription administrators within 72 hours of confirming an incident that affects their organization's data. The notification provides the scope, the affected data classes, the containment actions taken, and the remediation plan.

Report a vulnerability

Report suspected vulnerabilities to security@odingard.com. TraceLock acknowledges a report within 3 business days and provides a triage outcome within 10 business days. Do not include customer data, credentials, or exploit output against another organization's tenant in a report.

Troubleshooting, FAQ and API reference

Troubleshooting

A connector stopped returning results

Symptom. Controls that depend on one provider turn indeterminate, and the integration shows an error state.

1. Open **Settings** → **Integrations** and read the recorded error for the connector.
2. Run the connector smoke test to confirm whether the credential still authenticates.
3. If authentication fails, confirm the credential still exists at your provider and has not expired or been rotated.
4. If authentication succeeds but the scope is insufficient, restore the read permissions the connector requires.
5. Re-register the credential if it was rotated, then trigger a scan.

Result: the connector returns to connected and the dependent controls are re-evaluated on the next cycle.

Controls are stale but the connector is healthy

Check whether your organization is in a suspended lifecycle state — a suspended workspace is read-only and is not scanned. If the workspace is active and the connector authenticates, run the smoke test: a credential that authenticates but no longer sees the resource produces exactly this pattern.

A control is indeterminate rather than failed

The evaluation could not conclude. Almost always this is lost read permission at the provider rather than a control problem. Restore the scope and rescan; the control will then report a real pass or fail.

Evidence is expiring

Evidence carries a retention clock and raises a notification as it approaches expiry. For connector evidence, confirm the connector is still scanning — fresh scans produce fresh evidence automatically. For manual evidence such as a penetration test report, upload the current document.

A user cannot sign in

Case	Action
Local account, forgotten password	Use the password reset link on the sign-in page
Local account, MFA device lost	An administrator resets MFA for the member, who then re-enrols
SSO user, assertion rejected	Confirm the identity provider certificate in TraceLock matches the current signing certificate
SSO user, not a member	Confirm provisioning is enabled or that just-in-time provisioning is permitted for your organization
Deactivated account	Reactivate the member, or confirm the deactivation was intentional

Notifications or tickets stopped arriving

Open **Settings** → **Notifications** and re-test the destination. For ticketing, confirm the service account is still enabled and its token has not been rotated at your provider. Delivery attempts are recorded, so a destination that is rejecting deliveries is visible rather than silent.

Frequently asked questions

Is anything installed in our environment? No. TraceLock is a hosted service that calls your providers' APIs outbound using credentials you issue.

Can TraceLock change our environment? No. Connector credentials are read-only and there is no write path to your providers.

What happens if we revoke a credential? The next scan fails to authenticate, the integration is marked in error, and dependent controls turn indeterminate. Nothing is deleted.

Do you store our logs or customer data? No. The Privacy Wall admits allowlisted posture attributes only.

How long is evidence retained? Seven years from observation by default, tracked per record.

Can we use our own identity provider? Yes. SAML 2.0 with SCIM 2.0 provisioning is available on Enterprise plans.

Can our auditor be given access without a licence? Yes. Auditor Room access is a signed, time-bound, read-only capability rather than a seat.

Is TraceLock itself certified? Odingard operates TraceLock against the same control set the product monitors. Ask your Odingard contact for the current status of TraceLock's own attestations rather than inferring them from this document.

API reference

All requests are HTTPS against `https://tracelock.odingard.com`. User-facing endpoints authenticate with your session; the machine endpoint authenticates with an organization key.

Service health

```
curl -s https://tracelock.odingard.com/api/health
# {"status":"ok","service":"tracelock"}
```

Control state

```
curl -s https://tracelock.odingard.com/api/controls \
-H "Cookie: <your authenticated session cookie>"
```

Returns the tenant-scoped control library with codes, titles, statuses, owners, framework mappings, and verification timestamps.

```
curl -s https://tracelock.odingard.com/api/controls/CC6.1 \
-H "Cookie: <your authenticated session cookie>"
```

Returns a single control with its evaluation history and linked evidence.

Evidence digests

```
curl -s https://tracelock.odingard.com/api/evidence \
-H "Cookie: <your authenticated session cookie>"
```

Returns evidence records with type, source provider, description, digest, and retention clock end.

Trigger a connector run

```
curl -s -X POST https://tracelock.odingard.com/api/integrations/smoke-test \
-H "Content-Type: application/json" \
-H "Cookie: <your authenticated session cookie>" \
-d '{"provider":"AWS"}'
```

Validates the stored credential and its read scope without waiting for the scheduled cycle.

Submit an AI agent governance event

Machine submissions authenticate with your organization key, presented in the `x-tracelock-mcp-key` header. The key is stored as a hash and is rate limited per key.

```
curl -s -X POST https://tracelock.odingard.com/api/mcp \
  -H "Content-Type: application/json" \
  -H "x-tracelock-mcp-key: $TRACELOCK_MCP_KEY" \
  -d '{
    "method": "tools/write_compliance_event",
    "params": {
      "agentId": "release-assistant",
      "actionType": "deployment_approval",
      "promptRaw": "<prompt text>",
      "responseRaw": "<response text>",
      "hitlApproved": true
    }
  }'
```

Prompt and response text are hashed on receipt; the raw text is not stored.

Read your failing controls the same way:

```
curl -s -X POST https://tracelock.odingard.com/api/mcp \
  -H "Content-Type: application/json" \
  -H "x-tracelock-mcp-key: $TRACELOCK_MCP_KEY" \
  -d '{"method":"tools/read_compliance_state","params":{}}'
```

Verify a digest in Python

```
import hashlib, json, urllib.request

def canonical_digest(metadata: dict) -> str:
    canonical = json.dumps(metadata, sort_keys=True, separators=(",", ":"))
    return hashlib.sha256(canonical.encode()).hexdigest()

with open("evidence-export.json") as handle:
    records = json.load(handle)
```

```

for record in records:
    recomputed = canonical_digest(record["recorded_custody_metadata"])
    status = "OK" if recomputed == record["sha256_digest"] else "MISMATCH"
    print(f'{record["control_id"]:<12} {status}')

```

Response codes

Code	Meaning
200	Success
400	Malformed request body
401	Missing or invalid session
403	Authenticated but not permitted, or entitlement required
404	Resource not found, or method not supported on the machine endpoint
429	Rate limit exceeded; retry after the indicated interval

Support

Need	Contact
Product support	support@odingard.com
Security and vulnerability reports	security@odingard.com

Glossary

Product terms

Term	Definition
Audit	A workspace record for an audit engagement. The application displays framework, progress, dates, and readiness context.
Control	A tenant-scoped compliance requirement represented by a code, title, description, category, framework references, status, and verification information.
Control Center	The compliance overview for readiness, control health, failing controls, and posture by category.
Control execution log	A record of a connector check attempt, including its connector type, status, raw mode/reason data, and evidence hash.
Control test	A connector or other verification operation that evaluates a control and can produce a finding and evidence.
Crosswalk	The mapping between a control and one or more framework references. TraceLock uses the mapping to calculate framework coverage and display mapped controls.
Evidence record	A persisted record associated with a control. It includes a type, description, file reference when present, content hash, retention end, metadata, and source provider.
Estate Map	The live view of control coverage across the framework perspectives exposed by the application, with status filtering and framework drill-down.
Exception	A time-bounded request against a specific control. A request includes a reason and expiry and can be approved, rejected, or marked expired by an authorized reviewer.
Finding	A connector result describing a passed, failed, not-applicable, indeterminate, warning, or not-assessed outcome for a control check.

Term	Definition
Framework	A compliance or regulatory perspective used by controls and crosswalks, such as SOC 2, ISO 27001, NIST CSF 2.0, or EU AI Act.
Integration	A configured external provider connection used by a workspace for posture or evidence collection.
Privacy Wall	The metadata protection boundary that permits declared metadata fields, rejects sensitive text patterns, canonicalizes accepted metadata, hashes it, and enforces allowed regions.
Remediation	Guidance associated with a failed check. TraceLock can also dispatch a configured remediation ticket for a failure.
Tenant	A TraceLock organization boundary. Tenant-scoped queries include the organization identifier and do not use another organization's records.
Verification Room	The read-only auditor surface for reviewing mapped controls, evidence metadata, content hashes, and audit timeline information.
WORM	Write once, read many. TraceLock's universal webhook evidence view describes a seven-year SEC 204-2 WORM retention clock for signed events.

Identity and administration terms

Term	Definition
ACS URL	The SAML assertion consumer service URL that receives an identity provider response. TraceLock derives it from the public origin and organization identifier.
Claimed domain	An email domain associated with an enabled SAML connection. When enforcement is enabled, ordinary users in claimed domains must use SAML.
JIT provisioning	Just-in-time user creation during a successful SAML flow. TraceLock creates a local user when the SAML login does not find one.

Term	Definition
Lifecycle state	An organization's operational state. The implementation recognizes <code>ACTIVE</code> , <code>SUSPENDED</code> , <code>OFFBOARDING</code> , and <code>OFFBOARDED</code> .
Platform administration	The cross-tenant organization and action surface reserved for approved Odingard staff. It requires the platform permission and the staff allowlist.
SCIM	System for Cross-domain Identity Management 2.0, used here for bearer-token-based user provisioning and deprovisioning.
SSO	Single sign-on. In TraceLock's identity configuration, SAML SSO uses an enterprise identity provider.
Tenant scope	The server-side object containing the authenticated user, organization, role, lifecycle state, and permissions used for authorization and tenant scoping.

AI governance terms

Term	Definition
Accepted role	The recorded organization role for an AI system after reviewing the proposed operator role. A written justification is required when it differs from the proposal.
Agentic system	An AI inventory record with an agentic posture and autonomy level. TraceLock records tool scope, human oversight, action logging, and shutdown procedure fields.
Article 25 role shift	A TraceLock AI-governance review event produced when recorded facts can change the proposed operator role under the EU AI Act logic implemented by the application.
AI inventory	The registry of AI systems, their purpose, provider, risk, approval, operator role, and governance posture.
AI role assessment	The saved determination input and result used to record an AI system's operator role, risk category, Annex III fit, and related rationale.

Term	Definition
Governance ledger	The AI Governance view of locally hashed agent activity. Prompt and response hashes are displayed instead of prompt or response content.

Connector terms

Term	Definition
Connector	A provider-specific implementation that declares a category, control codes, credential environment variables, and a check operation.
Connector mode	The execution mode returned by a connector: <code>live</code> , <code>demo</code> , or <code>not_executed</code> .
External ID	The tenant-specific AWS value used in the customer role trust policy to reduce confused-deputy risk.
Least privilege	Granting only the provider actions required by the connector checks. The AWS template lists the exact read actions used by the AWS connector.
Smoke test	An explicit connection test from the Integrations page that exercises the provider configuration and reports checks.