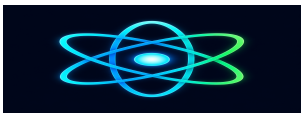

GETTING STARTED GUIDE

# Getting Started with Atomation Okta Assessment

A practical first-setup guide for sign-in, per-Okta-org settings, framework selection, Okta API access, optional SSO and SCIM, manual evidence, and potential-risk review.

| Field | Value |
| --- | --- |
| Owner | Atomation Support |
| Audience | COO, CISO, IAM owner |
| Use case | New customer handoff |
| Source page | /docs/client-onboarding/ |
| PDF filename | atomation-client-onboarding-guide.pdf |
| Status | Ready for customer tailoring |
| Screenshot policy | Insert approved Okta Admin Console or Atomation workspace captures before final distribution. |

This document is an original Atomation guide. Vendor documentation is used as reference material only.

# Contents

# Overview

Use this guide after the Atomation welcome email arrives. It shows what the customer does in Atomation, what the Okta administrator does in the Okta Admin Console, and where manual evidence or accepted business decisions are recorded.

| Area | Customer action | Why it matters |
| --- | --- | --- |
| Atomation workspace | First login, MFA, org contacts, framework selection, manual checklist, uploads. | Keeps customer-owned scope and evidence attached to the right Okta org. |
| Okta Admin Console | API Services app, SAML app, SCIM provisioning, group linking, app assignments. | These settings are controlled by the customer's Okta administrator. |
| Findings review | Review potential risks, add notes, accept business decisions, or track remediation. | Creates report context behind each recommendation. |

# Executive Packet

This section is the short version for the sponsor, COO, CISO, or security leader reviewing readiness. It separates customer-owned decisions from Atomation validation so the handoff is clear and defensible.

| Decision area | Customer owner | Atomation output |
| --- | --- | --- |
| Okta org scope | Confirm which production or preview orgs are included. | Per-org settings, evidence, and findings stay separated. |
| Framework selection | Select HIPAA, SOX ITGC, SOC 2, GLBA/FFIEC, or ISO 27001 per org. | Findings and reports map to the selected framework context. |
| Assessment access | Create the Okta API Services app and approve the read-only access model. | Connection verification, snapshots, potential risks, and evidence trail. |
| Business decisions | Accept, remediate, or track recommendations where the choice is risk-based. | Report notes explain accepted decisions without hiding potential risks. |

Executive summary: the customer controls scope, access approval, framework selection, and accepted business decisions. Atomation validates setup, records evidence, identifies potential risks, and packages the report for review.

# Getting Started Steps

Step 1

## Open the welcome email

Open the Atomation welcome email from support@atomation.io, click the workspace button, and create your account. The button points to the customer's tenant slug.

Step 2

## Sign in and complete MFA

Complete first login and MFA before setup work begins. This confirms that the primary customer contact can reach the tenant workspace.

**SCREENSHOT PLACEHOLDER**

**Welcome page and MFA prompt**

Atomation first-login screen and MFA setup state.

Step 3

## Update each Okta org profile

Open Settings -> Organizations. For each connected Okta org, confirm the org name, support contact name, support email, and support phone. Each Okta org has its own editable card.

**SCREENSHOT PLACEHOLDER**

**Per-Okta-org profile card**

Settings - Organizations card showing org name and support contact fields.

Step 4

## Select frameworks for the org

In the same org card, check the frameworks that apply to that Okta org: HIPAA, SOX ITGC, SOC 2, GLBA/FFIEC, and ISO 27001. Use customer or auditor controls for scopes not listed in Atomation.

**SCREENSHOT PLACEHOLDER**

**Framework checkboxes**

HIPAA, SOX ITGC, SOC 2, GLBA/FFIEC, and ISO 27001 selected where applicable.

Step 5

## Connect read-only Okta API access

Create the Okta API Services app by following /docs/okta-api-access/. This Admin Console step is used for snapshot collection, evidence, potential risks, and reports.

SCREENSHOT PLACEHOLDER

**API connection verified**

Atomation verification screen after Client ID, scopes, JWKS, and role checks pass.

Step 6

## Set up SSO and SCIM when needed

If the customer wants Atomation sign-in and provisioning through Okta, follow /docs/okta-integration/. This is separate from the read-only assessment service app.

SCREENSHOT PLACEHOLDER

**SSO and SCIM verified**

Atomation SSO and provisioning settings after Okta verification is complete.

Step 7

## Add manual evidence and answers

Use the Security Checklist for manual org-level questions. Use monitoring or compliance upload areas for SIEM exports, policies, control evidence, or notes requested by Atomation.

SCREENSHOT PLACEHOLDER

**Manual control questions**

Security Checklist questions that the Okta API cannot derive.

SCREENSHOT PLACEHOLDER

**Evidence upload**

Monitoring or compliance upload area for customer-owned evidence.

Step 8

### Review potential risks and decisions

Atomation shows potential risks and recommendations after the first scan. Some are direct gaps. Others are business decisions that the customer may remediate, accept, or track with notes.

**SCREENSHOT PLACEHOLDER**

**Dashboard potential risks**

Customer dashboard boxes showing potential risks by severity and area.

**SCREENSHOT PLACEHOLDER**

**Accepted decision note**

Findings review showing an accepted business decision with supporting note.

## Ready for First Scan Criteria

| Criterion | Ready when |
|---|---|
| Workspace access | Primary customer admin has signed in and completed MFA. |
| Org profile | Every in-scope Okta org has support contact name, email, phone, and org type. |
| Frameworks | Customer-selected frameworks are checked for each in-scope Okta org. |
| Okta API access | API Services app Client ID is saved and Atomation verification succeeds. |
| Manual evidence | Known manual checklist answers and requested uploads are complete or explicitly deferred. |
| Business decisions | Accepted decisions have owner notes so the final report explains the risk choice. |

# Resources

- Getting started guide: /docs/client-onboarding/
- Okta API access guide: /docs/okta-api-access/
- Okta SSO and SCIM guide: /docs/okta-integration/
- Roles and permissions: /docs/okta-integration/roles-permissions/
- Reports and evidence: /okta/docs/reports/
- Evidence and findings: /okta/docs/evidence-findings/