OPTIONAL WORKSPACE ACCESS

Atomation Okta SSO and SCIM Setup Guide (Optional)

Optional: let your team sign in to Atomation through Okta with SAML 2.0 SSO and provision or deprovision users automatically with SCIM 2.0. Assessments do not require it - workspace sign-in works with email + MFA out of the box.

Field	Value
Owner	Customer IAM admin
Audience	IAM, security, app owners
Use case	Optional workspace access rollout
Source page	/docs/okta-sso-scim/
PDF filename	atomation-okta-sso-scim-setup-guide.pdf
Status	Optional - SAML 2.0 SSO + SCIM 2.0

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

Contents

Is This Required?

No. You do not need SSO or SCIM to run assessments. Workspace sign-in works with email + MFA out of the box, and the assessment uses a separate read-only API Service App - that connection is the only required one (see /docs/okta-api-access/). Set up SSO and SCIM only if you want your team to sign in to Atomation through Okta with automatic user provisioning.

> One org per workspace - the first org is your primary org. SSO and SCIM apply to exactly one Okta org per workspace. The first org you configure becomes the workspace's primary (identity) org - the org your team signs in from and where user lifecycle events originate. Every other connected org stays assessment-only. Multi-org SSO is a planned enhancement - contact support@atomation.io if you need it.

Before You Start

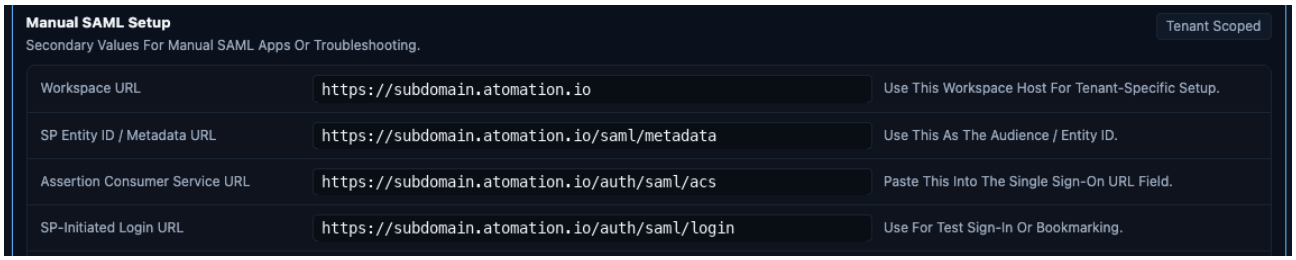
Atomation creates the workspace and first administrator during onboarding. The customer's IAM team completes the SAML setup below, then continues to SCIM if automatic user lifecycle or role group synchronization is needed.

This is separate from the read-only Okta API Service apps used for assessment data - every connected org keeps its own read-only connection, covered in the Okta API access guide.

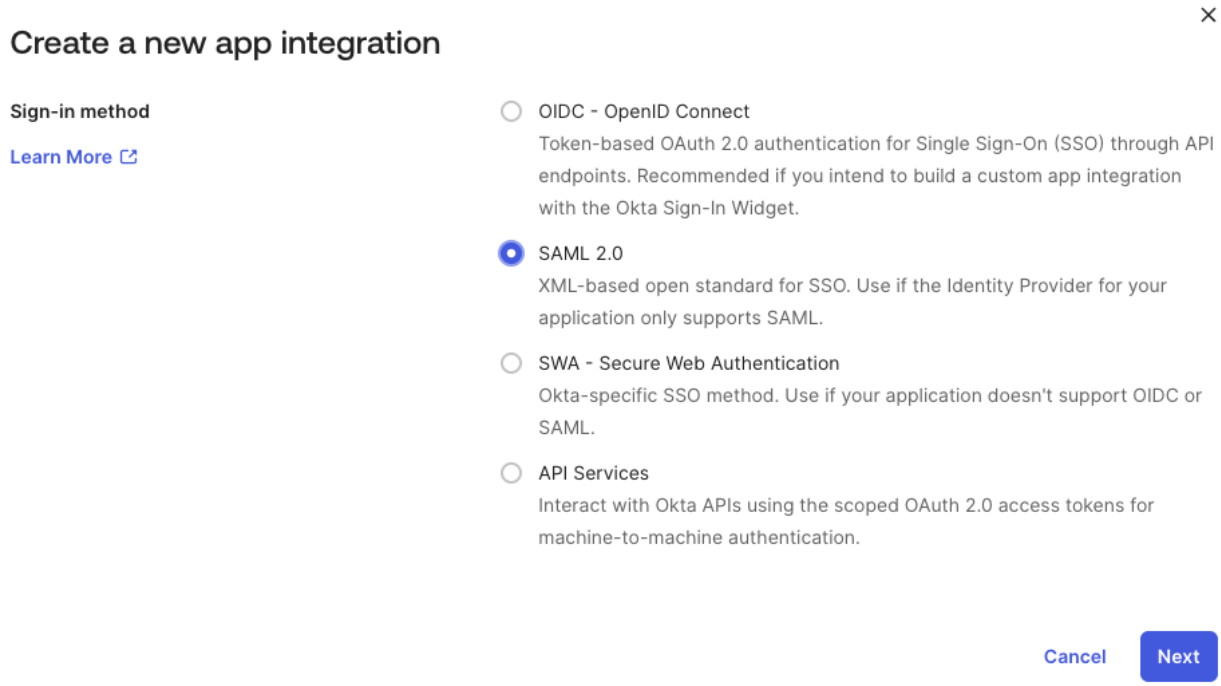
SAML SSO Setup

Create a SAML 2.0 app integration in Okta and enter the Atomation service provider values from Administration -> SSO / SAML in your workspace.

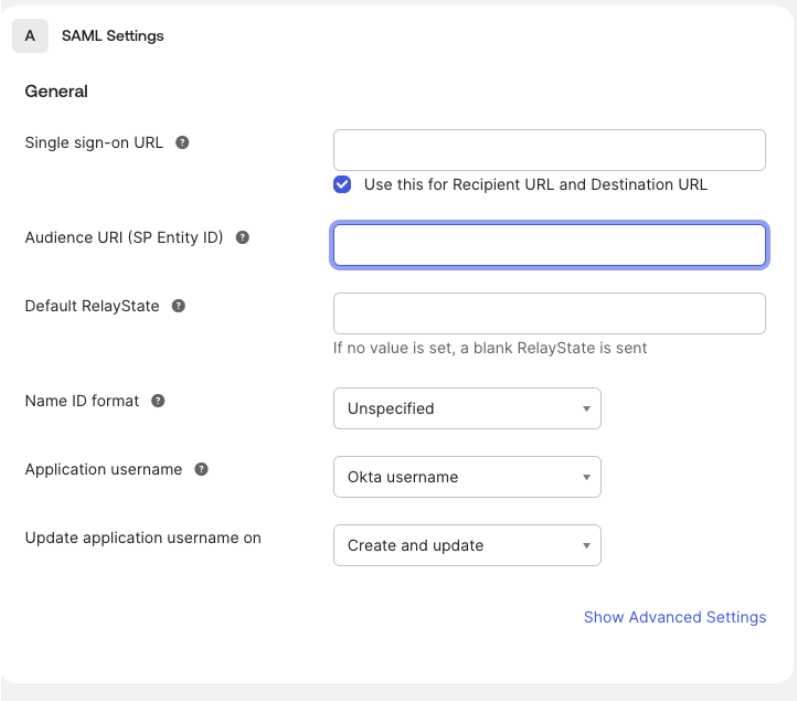
Okta Field	Atomation Value
Single Sign-On URL	https://subdomain.atomation.io/auth/saml/acs
Use this for Recipient URL and Destination URL	Checked
Recipient URL	https://subdomain.atomation.io/auth/saml/acs
Destination URL	https://subdomain.atomation.io/auth/saml/acs
Audience URI / SP Entity ID	https://subdomain.atomation.io/saml/metadata
SP-Initiated Login URL	https://subdomain.atomation.io/auth/saml/login
Default RelayState	Leave blank
Name ID format	Unspecified
Application username	Okta username
Update application username on	Create and update



Atomation Manual SAML Setup: copy the workspace-specific SAML values for the customer subdomain.



Okta manual setup starts by creating a new SAML 2.0 app integration.



Okta SAML Settings: paste the ACS URL into Single Sign-On URL and SP Entity ID / Metadata URL into Audience URI.

1

Create a SAML 2.0 app integration

In the Okta Admin Console, go to Applications -> Applications, click Create App Integration, choose SAML 2.0, then click Next.

2

Name the app

Use a clear name such as Atomation - subdomain or Atomation - Production, upload the Atomation logo if desired, then continue to SAML settings.

3

Paste the manual SAML values

In Atomation, open Administration -> SSO / SAML and use the Manual SAML Setup card. In Okta, paste the Assertion Consumer Service URL into Single Sign-On URL. Leave Use this for Recipient URL and Destination URL checked. Paste the SP Entity ID / Metadata URL into Audience URI (SP Entity ID). Copy the Login URL if Okta shows the SP-Initiated Login URL field.

4

Set Name ID and basic attributes

Set Name ID format to Unspecified and application username to Okta username. If the customer uses JIT provisioning, include basic user attributes such as first name, last name, and email. Role membership should still be handled through SCIM Group Push or Group Linking, not a SAML group attribute.

5

Finish the Okta app

On Okta's final feedback screen, select This is an internal app that we have created, then click Finish.

6

Copy metadata back into Atomation

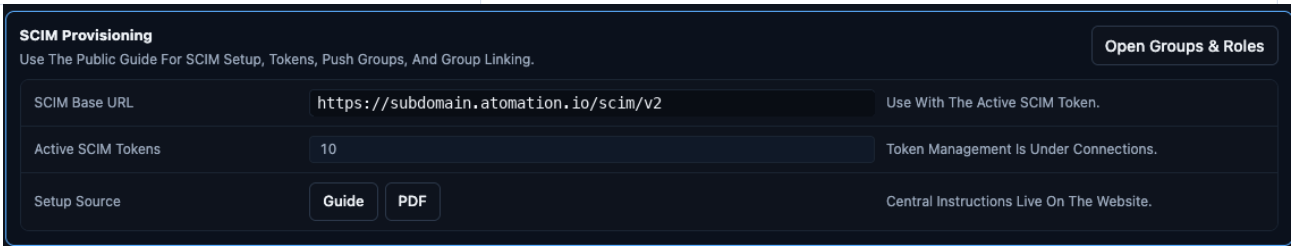
Open the app's Sign On tab and copy the Okta Metadata URL. Paste that URL back into Atomation under Administration -> SSO / SAML for the matching connected org, then save and verify.

SCIM Provisioning Setup

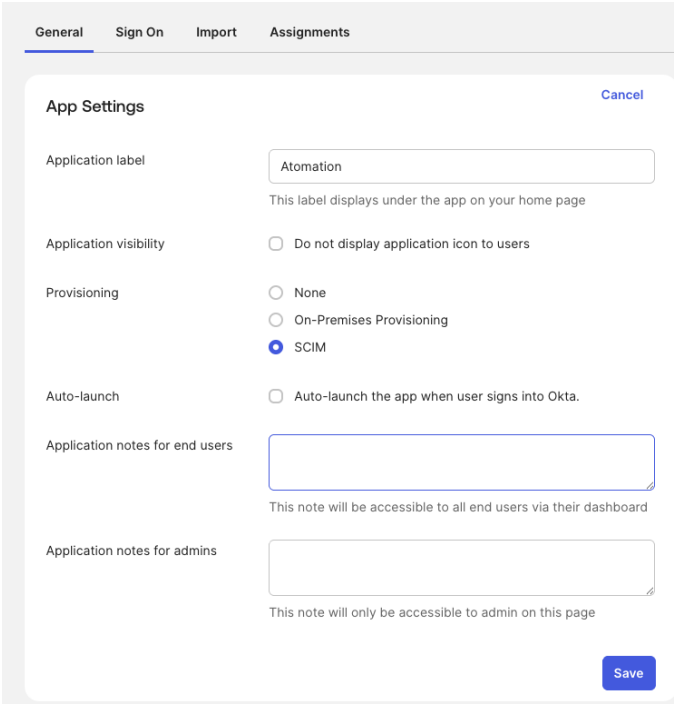
After SAML metadata is saved and verified, configure SCIM if the customer wants Okta to create, update, deactivate, and group-link Atomation users.

Use the exact tenant-specific SCIM Base URL shown under Administration -> SSO / SAML. Generate the SCIM token under Connections, copy it once, and paste it into Okta as the bearer token.

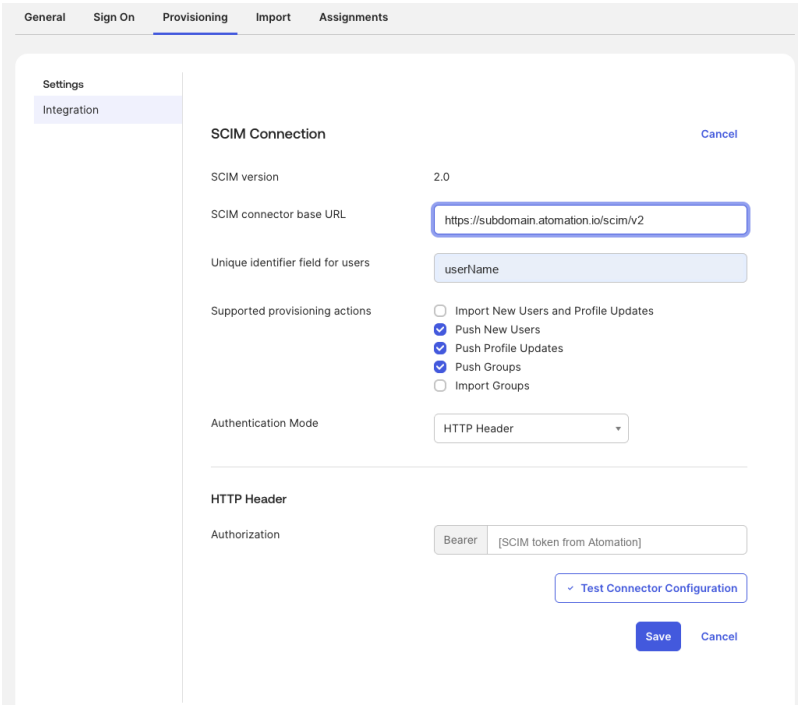
Okta Provisioning Field	Value To Use
SCIM version	2.0
SCIM connector base URL	https://subdomain.atomation.io/scim/v2
Unique identifier field for users	userName
Supported provisioning actions	Push New Users, Push Profile Updates, Push Groups
Authentication Mode	HTTP Header
Authorization	Bearer + SCIM token generated in Atomation



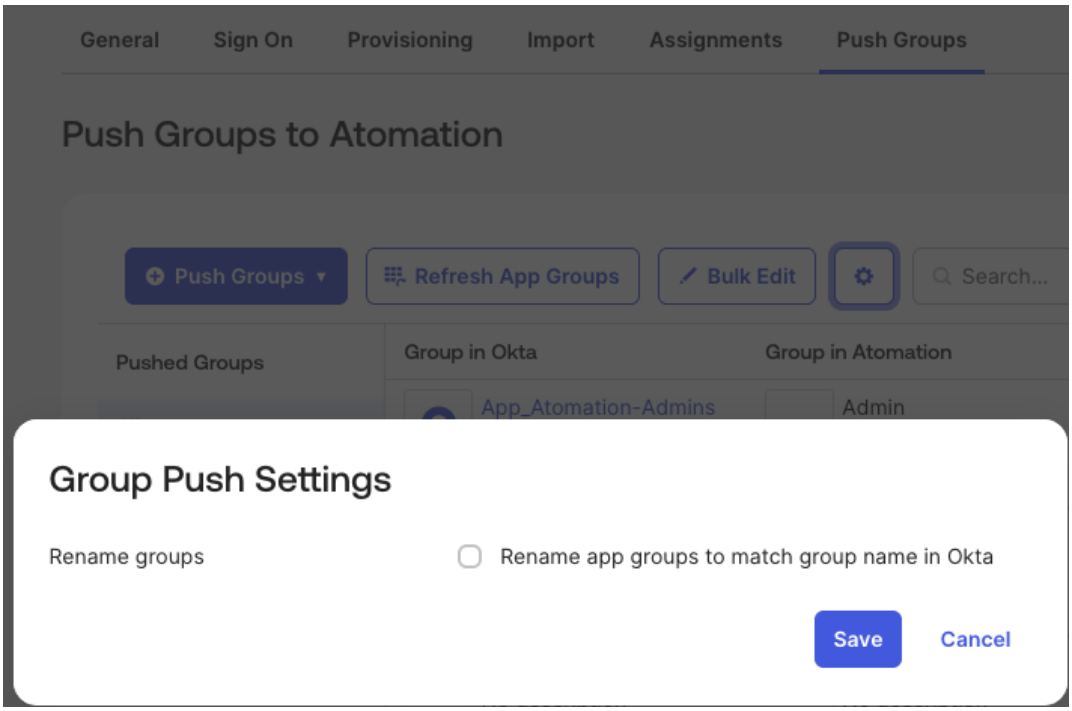
Atomation SCIM Provisioning: copy the SCIM Base URL and use an active SCIM token.



Okta General tab: edit App Settings, select SCIM under Provisioning, and save.



Okta Provisioning -> Integration: enter the SCIM Base URL, userName, HTTP Header authentication, and bearer token.



Push Groups settings: leave Rename app groups to match group name in Okta unchecked.

1

Copy the SCIM Base URL and token from Atomation

In Atomation, go to Administration -> SSO / SAML and copy the SCIM Base URL. Then open Connections, generate a SCIM token for the active org, and copy it immediately. Okta will use this token for ongoing provisioning requests until the token is revoked.

2

Enable SCIM on the Okta app

In Okta, open the Atomation app. On the General tab, click Edit, select SCIM under Provisioning, then click Save.

3

Enter the SCIM integration settings

Go to Provisioning -> Integration. Set SCIM version to 2.0, paste the Atomation SCIM connector base URL, set Unique identifier field for users to userName, select Push New Users, Push Profile Updates, and Push Groups, then set Authentication Mode to HTTP Header. In Authorization, keep Bearer selected and paste the SCIM token generated in Atomation. Click Test Connector Configuration, confirm the test passes, then click Save.

4

Enable To App lifecycle actions

Under Provisioning -> To App, enable Create Users, Update User Attributes, and Deactivate Users. Confirm mappings for userName, name.givenName, name.familyName, email, and emailType.

5

Link groups to Atomation roles

On the Push Groups tab, click Refresh App Groups so Okta can import Atomation role-groups such as Admin, Security Admin, Org Admin, Developer, Viewer, and User. Open Group Push Settings, leave Rename app groups to match group name in Okta unchecked, then use + Push Groups -> Find groups by name. Choose Link Group, not Create Group, and select the matching Atomation role-group.

6

Assign users after SCIM is ready

Assign users only after SCIM is enabled, the connector test passes, lifecycle actions are enabled, and role groups are linked. If a user is assigned before provisioning completes, remove the assignment, wait, and add it again. Recommended approach: create one Okta app-access group and use Okta Group Rules to add users based on the source or role groups you use for SCIM Group Push.

Keep app assignment groups and pushed role groups separate when the customer's Okta model supports it. This avoids confusing app access with role membership.

Data Access Separate From SSO and SCIM

Atomation's posture assessment reads Okta configuration through a separate, read-only API Services app that the customer creates during onboarding. It is not part of this SSO/SCIM integration and grants no write access to the customer's Okta org.

The API Services connection flow should stay focused on assessment access. It does not require the Okta SAML Metadata URL.

Support and References

- Support: support@atomation.io
- Roles and permissions: /docs/okta-integration/roles-permissions/
- Okta SAML app integration reference: https://help.okta.com/oie/en-us/content/topics/apps/apps_app_integration_wizard_saml.htm

- Okta SCIM provisioning reference: https://help.okta.com/oie/en-us/content/topics/apps/apps_app_integration_wizard_scim.htm

See It First

Walk a real finding queue, evidence drawers, and reports in the read-only Atomation demo - no Okta tenant required, no signup.

> Explore the live demo at demo.atomation.io