Quickstart Setup Guide

Prendio SCIM User Provisioning

For customer administrators | Typical setup time: 30–60 minutes

Before You Begin

Confirm the following before starting setup:

Requirement	Details
Identity Provider	Okta (additional IdP support – contact your Account Manager for current availability. Soon to support Microsoft Entra ID (Azure AD), or OneLogin)
IdP Admin Access	You need admin privileges in your IdP to configure SCIM provisioning
Prendio Admin Access	Administrator or Company Admin role in Prendio
SCIM Enabled	Contact your Account Manager to enable SCIM for your Prendio account
SSO Configured	Prendio SSO must be configured prior to SCIM setup. Prendio does not manage password – authentication remains within your IdP
Departments Configured	Department names in your IdP must exactly match department names in Prendio

Why SSO first? Prendio does not synchronize passwords. SSO ensures your users can authenticate through your identity provider from day one. Skipping this step means provisioned users will have no login path until SSO is in place — a common source of support escalations that delays time-to-value.

Step 1: Generate Your SCIM Credentials

1. Log in to Prendio as a **Administrator** or **Company Admin**.
2. Navigate to **Admin Dashboard > General > User Provisioning**.
3. Copy the **SCIM Base URL** using the Copy URL button.
4. Click **Generate Token** to create your API bearer token.
5. **Copy the token immediately and store it securely.** The token is shown only once. If lost, you can regenerate it, but the previous token will be invalidated.

Why does token security matter? This bearer token grants write access to your user base in Prendio, including approval limits and spend controls. A compromised token creates direct procurement compliance risk — unauthorized changes to approval routing could allow purchases to bypass financial controls entirely.

Step 2: Configure Your Identity Provider

In your identity provider, create a new SCIM provisioning connection using the credentials from Step 1:

Setting	Value
SCIM Base URL	https://api.prendio.com/scim/v2/
Authentication	OAuth 2.0 Bearer Token
API Token	The bearer token generated in Step 1
Provisioning Direction	IdP to Prendio (one-way only)

Why one-way only? Prendio treats your IdP as the system of record for identity. Allowing edits to flow back from Prendio would create conflicting sources of truth, making it impossible to enforce consistent approval structures across your organization — a key concern for Finance and compliance teams.

Step 3: Map User Attributes

Configure the following attribute mappings in your IdP. Required fields must be mapped for provisioning to work. Optional fields enable richer purchasing controls.

SCIM Attribute	Prendio Field	Required	Notes
user.userName	Email	**Yes**	Primary identifier
user.name.givenName	First Name	**Yes**	
user.name.familyName	Last Name	**Yes**	
user.phoneNumbers[primary=true]	Direct Phone	**Yes**	
user.manager.value	Next Approver	No	Sets manager as approver, proxy delegate, and delegate
user.prendio.prendioApprovalLimit	Approval Limit	No	Requires custom schema extension (see below)
user.prendio.prendioSpendLimit	Spend Limit	No	Requires custom schema extension (see below)
user.department	Department	No	Must exactly match department name in Prendio

Custom Prendio Attributes (Optional)

Prendio supports custom approval-related attributes via a SCIM schema extension. To use these, create a custom schema extension in your IdP using the namespace:

urn:ietf:params:scim:schemas:extension:prendio:2.0:User

This extension supports attributes such as approval limits and spend limits, mapped to the corresponding Prendio purchasing controls. The exact attribute names will vary based on your organization's configuration — work with your Prendio Account Manager to identify the correct mappings for your setup.

Your IdP documentation will have instructions for adding custom SCIM attributes using a custom schema namespace.

Why the full URN namespace? Using the complete IETF-standard namespace (urn:ietf:params:scim:schemas:extension:prendio:2.0:User) ensures that custom attributes are correctly scoped and won't conflict with other extensions in your IdP. Shorthand namespaces can cause silent attribute-mapping failures that are difficult to diagnose post-rollout.

Why are custom attributes important for leadership? Approval limits and spend limits are the core financial controls that give Prendio its compliance value. When these attributes flow automatically from your IdP — reflecting promotions, role changes, or org restructures — Finance gains confidence that purchasing authority is always current. Stale limits are one of the leading causes of audit findings and maverick spend.

Default behavior: All users provisioned via SCIM are automatically assigned the **Requester** role in Prendio. Role upgrades (e.g., to Approver or Administrator) are managed inside Prendio after provisioning.

Step 4: Run a Pilot (Recommended)

We strongly recommend piloting with a small group before full rollout. This validates that attribute mapping is correct and that purchasing controls are working as expected.

Recommended Pilot Approach

1. **Select 3–5 test users** in your IdP. Choose users across different departments if possible.
2. **Assign them to the Prendio SCIM application** in your IdP and trigger a sync.
3. **Verify in Prendio** that each user was created with the correct name, email, department, approval limit, and spend limit.
4. **Test an attribute change** (e.g., update a department or approval limit in the IdP) and confirm it flows through to Prendio.
5. **Test a deactivation** by removing a test user from the Prendio application in your IdP. Confirm the user is deactivated in Prendio and that approval paths auto-adjust.

Why pilot first? SCIM will overwrite existing Prendio user data upon first provisioning. Running a controlled pilot limits the blast radius of any misconfigured attribute mappings — particularly approval levels — before they affect live purchasing workflows across your organization.

Step 5: Full Rollout

Once the pilot is validated, expand provisioning to your full user population:

1. Assign all target users to the Prendio SCIM application in your IdP.

2. Trigger a full sync from your IdP.
3. Spot-check a sample of provisioned users in Prendio to verify attribute accuracy.
4. Communicate to your team that user management is now automated. Manual user creation in Prendio should be discontinued for SCIM-managed users.

How to Revert

If you need to disconnect SCIM provisioning:

1. **Remove user assignments** from the Prendio SCIM application in your IdP (this stops future syncs).
2. **Delete the API token** in Prendio under Admin > User Provisioning (this invalidates the connection).
3. **Existing users are not affected.** Disconnecting SCIM does not delete or deactivate any users already provisioned. You can resume manual user management.

Important Notes

- **One-way sync only:** Changes flow from your IdP to Prendio. Edits made directly in Prendio are not synced back to the IdP.
- **Single-company only:** Each SCIM integration maps to one Prendio company. Multi-company users are not supported via SCIM at this time.
- **Department names must match exactly:** The department value sent from your IdP must be identical to the department name configured in Prendio (case-sensitive).
- **Token security:** Your bearer token is shown only once at generation. Store it in a secure location. If compromised, regenerate immediately in Prendio.
- **SSO is required:** Prendio does not manage or synchronize passwords. SSO must be configured before or alongside SCIM provisioning to ensure users can log in.

Need Help?

If you encounter issues during setup or have questions about attribute mapping, contact your Prendio Account Manager or submit a support ticket through the standard Prendio support process.