RFC

RFC: Automated User Lifecycle Management via SCIM 2.0

Status: Draft / Request for Comment

Target Audience: IT Managers, Azure AD/Entra ID Administrators, and Security Officers

Date: March 2026

1. Executive Summary

ActivityInfo currently supports Single Sign-On (SSO) for authentication. However, the **deprovisioning** of users remains a manual process. When an employee leaves an organization, their access to the identity provider (e.g., Entra ID) is revoked, but they remain listed as "Active" within ActivityInfo databases and consume a license until manually removed by a Database Administrator.

We propose implementing **SCIM 2.0 (System for Cross-domain Identity Management)** to automate the user lifecycle, specifically targeting the secure and immediate removal of departed staff.

2. The Proposed Solution

ActivityInfo will provide a dedicated SCIM 2.0 endpoint for each customer tenant. This will allow your identity provider (IdP) to "push" user status changes to ActivityInfo in near real-time.

- **Endpoint:** https://activityinfo.org/resources/billingAccounts/{billingAccountId}/scim/v2
- **Authentication:** Secret Bearer Token (Long-lived).
- **Primary Action:** Synchronize the active status of users.

3. Scope of Implementation (Phase 1)

To ensure a focused and reliable rollout, we are defining clear boundaries between *Provisioning* and *Authorization*:

A. Provisioning

When a user is added to the ActivityInfo enterprise app in your AD, a record is created in ActivityInfo.

- **Note:** Provisioning a user does **not** consume a license and does **not** grant access to any data.
- **Benefit:** This ensures the user’s identity is pre-verified and ready for database-level invitation.

- Future options: add additional metadata to user profile based on directory attributes, such as “department” or “duty station”.

B. Non goal: role assignment

At this time we do not anticipate assigning roles automatically based on AD group membership

- **The Rationale:** AD groups (e.g., "Staff - Tunisia") are often too broad for the granular permissions required in the field (e.g., "Caseworkers supervised by M. Aziz").
- **The Workflow:** Database Administrators will continue to invite users and assign fine-grained roles within the ActivityInfo interface. This avoids making HQ IT a bottleneck for daily field operations.

C. Primary goal: Deprovisioning

When a user is disabled or deleted in your Entra ID directory:

- ActivityInfo will automatically **revoke the user’s access from all databases** to which they were granted access.
- The database owner will be notified by email that the user has been automatically removed.
- Visually indicate the user’s account as “inactive” in the audit log
- The user’s seat is immediately vacated, **freeing up the license** for another staff member.
- Security is tightened by ensuring "orphan" accounts do not persist in the system.
- The user account would NOT be deleted, and their name and email address would still be visible in the audit log for records they have added or updated.

4. Security

Managing this integration will require time from your IT team. We would like to find the right balance of security and IT staff time requirements. We propose:

- **Bearer Token Authentication:** Customers will generate a Secret Token within their ActivityInfo Account Settings. It is not clear whether Client ID/Secret OAuth flow effectively reduces risk as the Client Secret is also a long-lived credential that will need to be shared with potentially multiple IT staff members.
- **Token Rotation:** Tokens will have a maximum lifetime of **6 months**. ActivityInfo will send automated email reminders to IT admins 30 days before expiration.
- **IP Whitelisting:** For defense in depth, ActivityInfo will restrict traffic to this endpoint to **Microsoft Entra ID’s published IP ranges**.

5. Feedback requested

We value your input on this roadmap. Specifically:

1. Is a 6-month token rotation policy feasible for your IT team?
2. Are there specific user attributes (beyond Name and Email) that you require to be synced

via SCIM?

Microsoft Entra

Set up / Testing guide

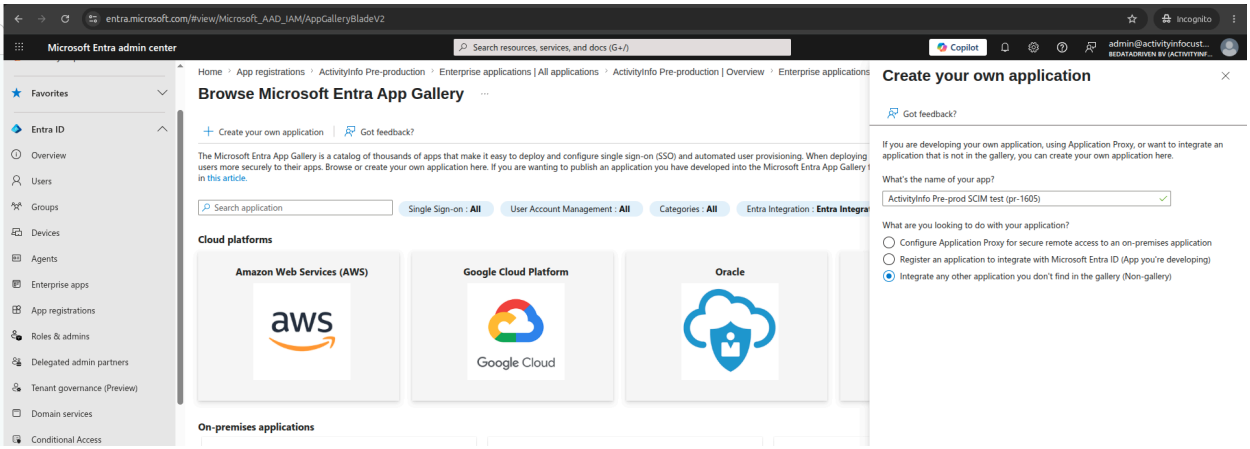
Step 1: Create the application

Navigate to https://entra.microsoft.com/ and log in with admin user

Select “Enterprise Apps” from the “Entra ID” section on the left hand side.

Click “+ Create your own application”

Choose “Integrate any other application you don't find in the gallery (Non-gallery)



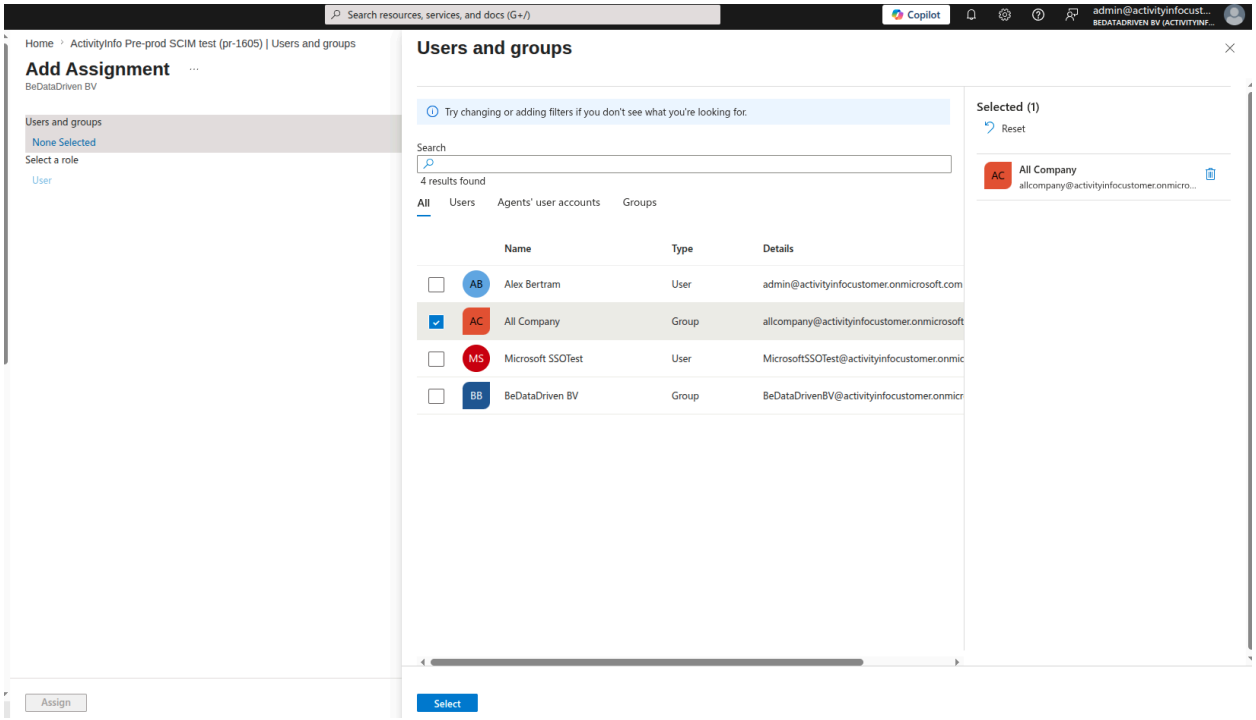
Click “Create”

Step 2: Assign users

Choose “Users and groups” from the left-hand side

Click “+ Add user/group”

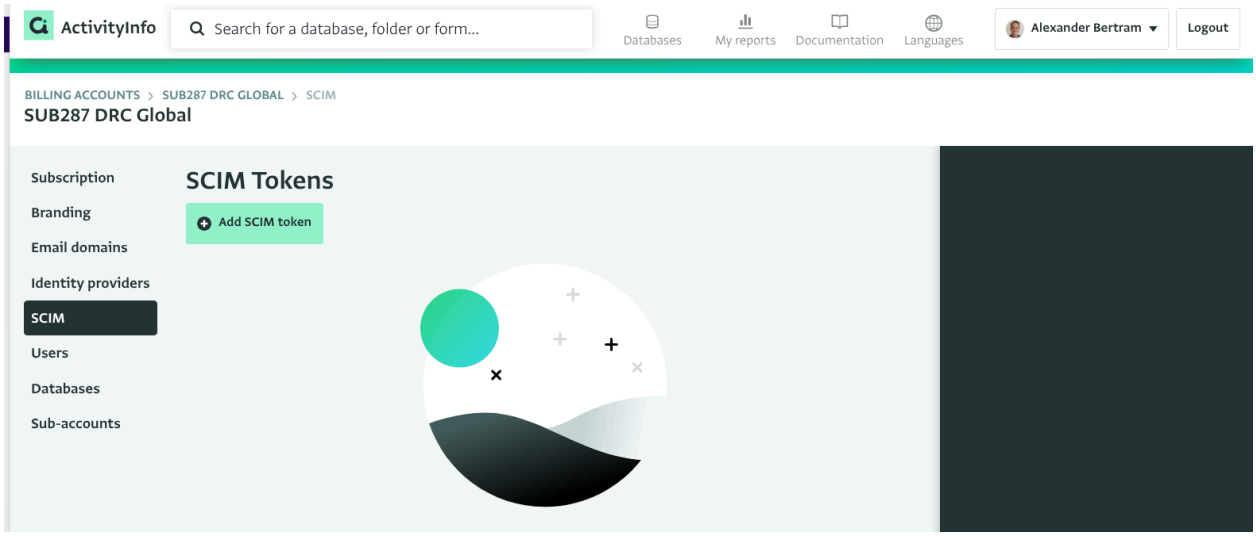
Click “None selected” under “Users and Groups”. Then check “All Company” and then click the “Select” button.



Then click “Assign”

Step 3: Generate token in ActivityInfo

Navigate to the SCIM section in the Billing admin page:



Click “Add SCIM Token”

Step 4: Configure provisioning

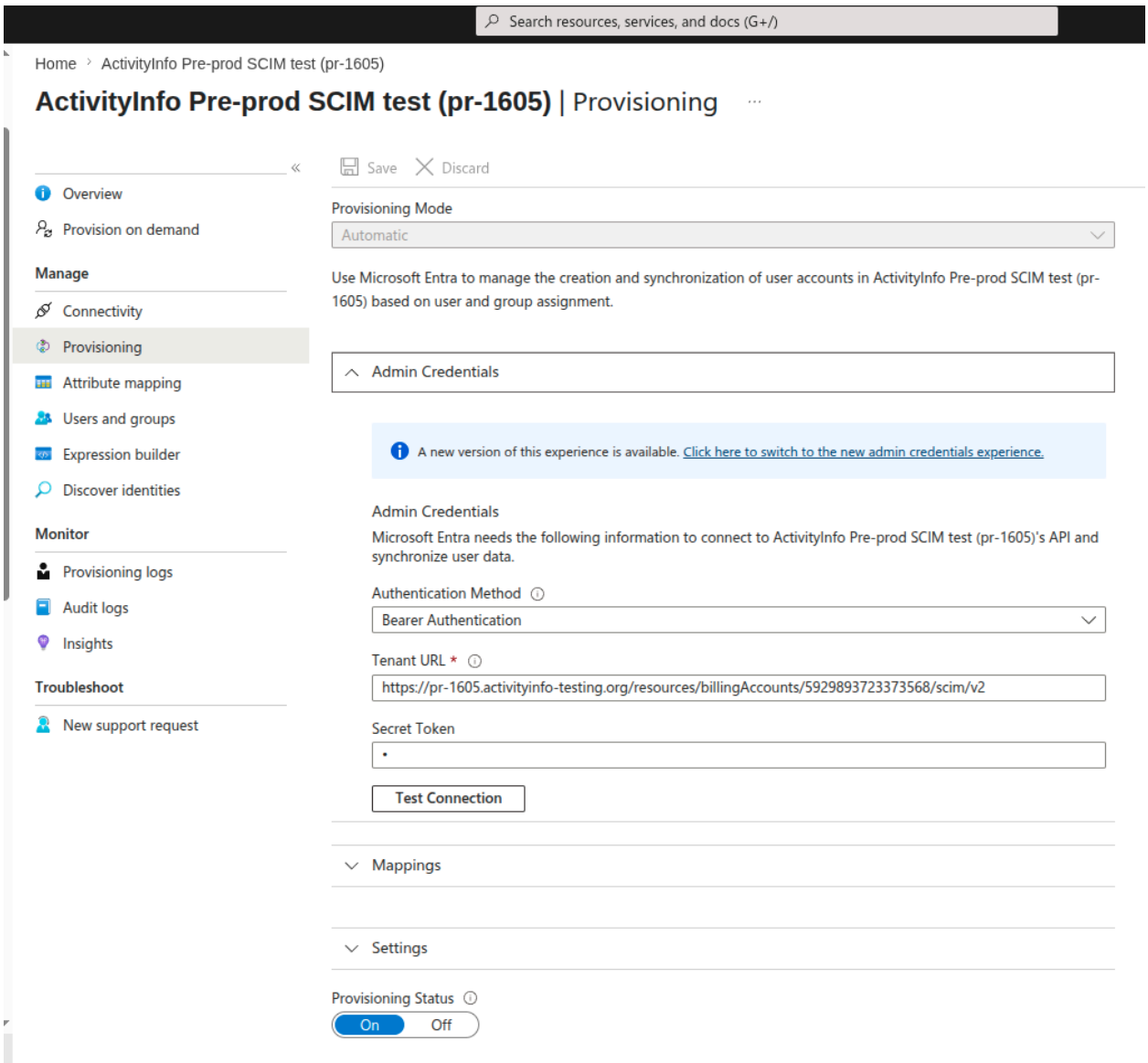
Choose “Provisioning” from the left-hand side

Click “+ New configuration”

In Admin Credentials, copy the details from ActivityInfo, including the Tenant URL and the Secret Token.

Click “Test Connection”

Set “Provisioning Status” to “On”



Step 5: Configure provisioning