Entra SCIM

What is SCIM (System Cross-domain Identity Management)

SCIM is a protocol that standardizes how identity information is exchanged between one entity to another. It's an open standard and is widely used to simplify the process of granting people or groups access to cloud-based applications.

The key to understanding the purpose of SCIM is in its name:

- **System**—SCIM creates a common format for how identity data is exchanged.
- **Cross-domain**—SCIM securely communicates identity data across platforms.
- **Identity Management**—SCIM automates the flow of information between an identity provider or identity and access management (IAM) system and cloud-based applications.

In an enterprise work scenario, using SCIM reduces the effort it takes to create, modify, and synchronize employee accounts and govern the resources employees have access to. It has the added benefit of reducing IT friction for employees because it works in tandem with other technologies that simplify how users sign in to apps.

Understanding SCIM provisioning

SCIM was created to make it easier for IT admins to provision users—that is, to create, maintain, and update people's accounts and give them permission to access all of the cloud-based applications they need to do their job.

Without SCIM, provisioning can be a lengthy and tedious manual process. The identifying information apps require to determine whether a person has permission to access them is fairly standard, such as employee names, emails, job titles, and departments. However, the formats apps use to represent each element of that information, and how the apps perform simple actions, can often be just a little bit different.

Having to manually add users to each app in a slightly different way every time might not be too problematic for businesses with just a few employees and cloud-based apps or services. But for organizations with a large number of employees and hundreds of cloud applications, manual provisioning can be costly, frustrating, and counterproductive.

SCIM solves this problem by providing a standard for seamlessly and securely exchanging information between identity providers and cloud apps. That standardization makes automating the provisioning process feasible and safe.

Some efficiencies that SCIM enables are:

- Automatic provisioning of new accounts—new employees are efficiently given access to the right systems when they join your team or organization.
- Automatic deprovisioning—when people leave the organization, there’s a centralized way to deactivate their account and app privileges.
- Synchronizing data between systems—when changes are made to accounts, it’s automatically updated everywhere.
- Group provisioning—whole groups of employees can be given access to the apps that they need.
- Governing access—SCIM makes it easier to monitor and audit privileges.

How SCIM works

In addition to providing a predefined schema for common identity attributes like group name, username, first name, last name, and email, SCIM provides a standardized definition of client and service provider roles. A client is usually an identity provider or IAM system, such as Microsoft Entra ID (formerly known as Microsoft Azure AD). A service provider is typically a software-as-a-service app. The client manages core identity information that apps need to grant or refuse access.

SCIM uses JavaScript Open Notation (JSON), an open-standard file and data exchange format, to support seamless interoperability across domains. It also uses a representational state transfer (REST) API to perform the actions needed to manage identity lifecycles. The database operation acronym CRUD describes the basic REST actions SCIM provisioning uses:

- Create—add new users in applications.
- Read—retrieve or search for information from existing identities and groups.
- Update—synchronize updated identity information between the client and apps.
- Delete—deprovision identities.

Application developers can use SCIM provisioning standards to ensure their apps integrate seamlessly with enterprise systems. It avoids the problem of having slightly different APIs to perform the same basic actions. Developers that create apps conforming to the SCIM standard can instantly take advantage of pre-existing clients, tools, and code.

Jellyfish and Entra SCIM

Jellyfish integrates with Microsoft Entra SCIM. It allows Entra to automatically provision accounts. Once the account is provisioned, users will be able to log in to jellyfish using their Entra credentials.

Microsoft Entra uses the System for Cross-domain Identity Management (SCIM) protocol to manage identities across different applications. Once configured to trust Jellyfish, Entra will begin pushing user identity information to jellyfish. When a user provisioned through Entra attempts to authenticate, they will be redirected Microsoft Entra to complete authentication.

For more information on Entra user provisioning, please see:
https://learn.microsoft.com/en-us/entra/identity/app-provisioning/user-provisioning

For more information on provisioning for Jellyfish, please visit:

https://learn.microsoft.com/en-us/entra/identity/saas-apps/jellyfish-provisioning-tutorial

What Are the Benefits?

Using Entra account provisioning removes the need to manually create and manage users in Jellyfish. When disabling a user, such as a former employee, operators will need not remember to delete their Jellyfish account.

Users will benefit as they do not need to maintain separate accounts in Jellyfish and Entra.

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated ICT company, specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.