SCIM: The future of universities' integration with Cloud Service Providers - The Webex case study

Fotis Memis, GUnet
Paulo Correia, Cisco

Contents

- Introduction
- Current Status of CSP's integrations
- Introducing SCIM
- SCIM Identities' representation
- The SCIM API
- Benefits for Universities
- Integrating SCIM in GUnet's IDM flows
- The CSP's point of view: Webex and SCIM

Introduction

- Cloud Service Providers in the Academic Landscape

- Requirement for Identity Provisioning/Deprovisioning

Current status of CSP's integrations

Custom solutions per Cloud Service Provider

- ▶ Dedicated APIs
- ▶ User upload via Excel files
- ▶ LDAP/AD syncing services
- ▶ VM appliances
- ▶ Authentication protocol based Just-In-Time(JIT) provisioning

Need for a standardized uniformed Identity Lifecycle Management Solution

Introducing SCIM

- SCIM: System for Cross-domain Identity Management
- Envisioned by Cloud Service providers to handle Identity Management at scale in the cloud.
- SCIM 1.0 released in 2011
- SCIM 2.0 released in 2015

Introducing SCIM

- A standard defined in RFCs 7642, 7643, 7644

- Platform-neutral schema and extension model ⟶ RFC 7643

- Service protocol ⟶ RFC 7644

SCIM Identities' representation

RFC 7643

▶ Two core schemas:

User, Group

▶ Secondary Schemas:

EnterpriseUser, ServiceProviderConfig, ResourceType

▶ Well-defined extension model to facilitate specific needs

The SCIM API

RFC 7644

Identity Provisioning/Deprovisioning via a standardized RESTful API:

- User creations occur with a POST
- User updates occur with a PUT/PATCH
- User deletes occur with a DELETE
- User lookups occur with a GET

/Users

- Same RESTful behavior with /Groups

Standardization leads to Globalization

- ❑ Identity exchange between organizations in a standardized/easy/scalable way

- ❑ No need for custom APIs, middleware services, excel file exchanges, etc

Benefits for Universities

▶ Less development effort

▶ Knowledge acquired in one integration applies to every CSP

▶ Fewer bureacratic interactions

▶ Fewer errors due to less complexity

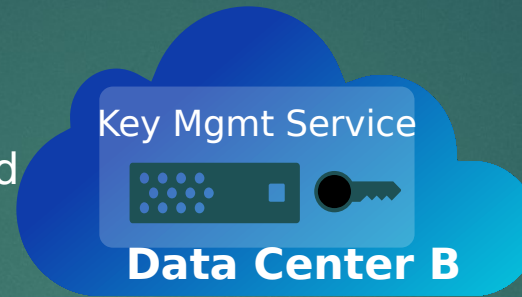# Integrating SCIM in GUnet's IDM flows

Main integration points:

- ▶ User-initiated provisioning: The SSO (Single-Sign-On) user login acts as a JIT (Just-in-Time) trigger.

- ▶ Admin-initiated provisioning/deprovisioning: Our new Identity Actions Service offers an API for mass operations against all connected Services. Updating/Deprovisioning require a single API call.

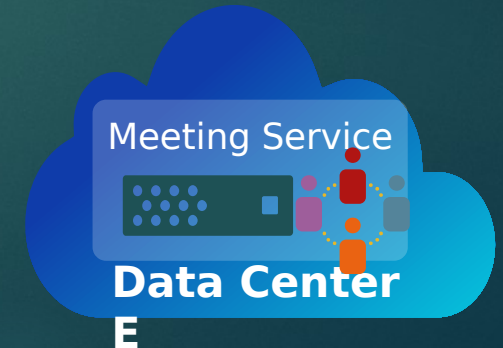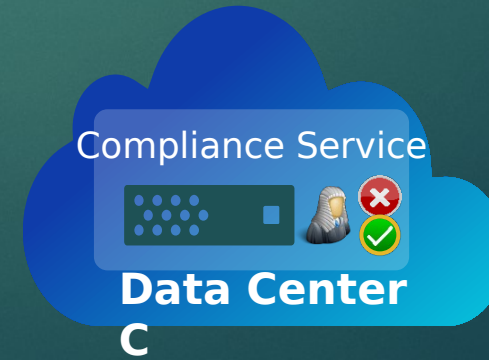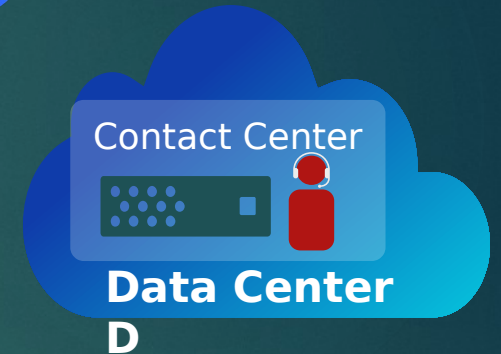# The CSP's point of view: Webex and SCIM

▶ By Paulo Correia, Principal Sales Architect at Cisco Systems

SCIM interservice protocol for Webex

- We started in 2012 implementing SCIM 1.0 to use the protocol to allow the different services to provision objects and its attributes
- Where Webex Identity Services was the IdM that would sync all attributes of the objects

Key Mgmt Service
Data Center B

webex

Contact Center
Data Center D

Identity Service
Data Center A

SCIM

Calling Service
Data Center E

Compliance Service
Data Center C

Meeting Service
Data Center E

SCIM 1.1 external interface

- We started in 2017 We introduce an external SCIM 1.1 interface to allow external IdM to provision users in Webex

- Webex was the Server in the SCIM protocol, providing the /user endpoint

- Limit set of attributes were allowed to be passed to Webex Identity Service backend.
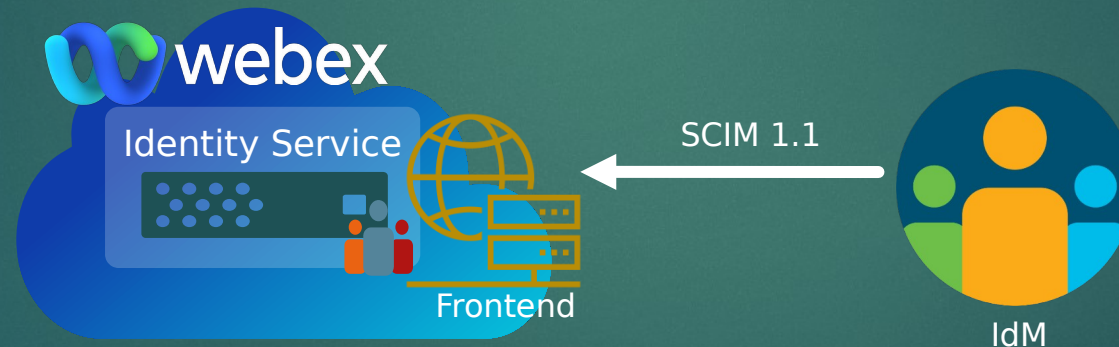
SCIM 2.0 external interface

- SCIM 2.0 APIs provide **additional methods** that are not available with SCIM 1.1 (e.g., additional search filters for filtering users).

- The SCIM 2.0 **schema supports more fine-grained requirements**.

- There is more **focus on feature development** for SCIM 2.0 APIs.

- SCIM 2.0 implementation is more **standardize** across different vendors

- Allow us to really open to any vendor that can provide an SCIM client

Thank you!
Any question ?