

SCIM User Scenarios

Background & Context

The Simple Cloud Identity Management (SCIM) specification is designed to make managing user identity in cloud based applications and services easier. The specification suite seeks to build upon experience with existing schemas and deployments, placing specific emphasis on simplicity of development and integration, while applying existing authentication, authorization, and privacy models. It's intent is to reduce the cost and complexity of user management operations by providing a common user schema and extension model, as well as binding documents to provide patterns for exchanging this schema using standard protocols. In essence, make it fast, cheap, and easy to move users in to, out of, and around the cloud.

The SCIM scenarios are overview user stories designed to help clarify the intended scope of the SCIM effort. They are part use case, part user story and part overall positioning document.

To aid reading, understanding and commenting on the SCIM scenarios, this document makes consistent use of the three key model concepts called *Triggers*, *Actors* and *Modes*. Each of these concepts is discussed in more detail in the Model Concepts section below. In summary, *Triggers* are things that start SCIM flows, *Actors* are the operating parties participating in the flow, and *Modes* represent the overall intent of the action (push or pull).

There's nothing normative or overly definitive about these model terms. They are only relevant to SCIM to the extent in which they help frame the discussion and create a common language for the ongoing discussion.

Model Concepts

Triggers

Quite simply, triggers are actions or activities that start SCIM flows. Triggers may not be relevant at the protocol or schema level, they really serve to help identify the type or activity that resulted in a SCIM protocol exchange.

The terms Joiner/Mover & Leaver are frequently used Human Resource Management terms that refer to the life cycle of an employee or contractor. We have chosen these terms in preference to the traditional C.R.U.D (Create Read Update & Delete) terms used in existing provisioning standards. So far, we have identified the following five SCIM Triggers:

- Joiner Trigger - Service On-boarding

A joiner trigger is a service on-boarding activity in which a business action such as a new hire or new service subscription is initiated by one of the SCIM Actors.

- **Mover Trigger - Service Change**
A mover trigger is a service change activity as a result of an identity moving or changing its service level. A mover trigger might be the result of a change in a service subscription level or a change to key identity data used to denote a service subscription level.
- **Leaver Trigger - Service Termination/Suspension**
A leaver trigger is simply an action or activity to suspend or terminate a service subscription. At this stage it's unclear if SCIM needs to identify separate protocol exchanges or identify a difference between a termination/deletion and a suspension. This may be relevant as target services may well differentiate between the two.
- **Sync Trigger – Bulk Synchronization**
- **Single-Sign On (SSO) Trigger – Real-time Service Access Request**
A SSO trigger is a special class of activity or action in which a Joiner or Mover action is initiated during an SSO interaction, which has resulted from a real-time service access request by the user.

Actors

Actors are the operating parties that take part in both sides of a SCIM protocol exchange, and help identify the source of a given Trigger. So far, we have identified the following SCIM Actors:

- Cloud Service Provider (CSP)
- Enterprise Cloud Subscriber (ECS)
- Cloud Service User (CSU)

Modes & Flows

Modes identify the functional intent of a data-flow initiated in a SCIM scenario. The modes identified so far are '*push*' and '*pull*' referring to the fact of pushing data to, or pulling data from an authoritative identity data store.

In the SCIM scenarios, *Modes* are often used in the context of a *flow* between two *Actors*. For example, one might refer to a Cloud-to-Cloud Pull mode. Here one Cloud Service Provider (CSP) is pulling identity information from another CSP. Commonly referenced flows are:

- Cloud Service Provider to Cloud Service Provider (CSP->CSP)
- Enterprise Cloud Subscriber to Cloud Service Provider (ECS-CSP)

Modes & flows simply help us understand what is taking place; they are likely to be technically meaningless at the protocol level, but again they help the reader follow the SCIM scenario's and apply them to real work use cases.

Bulk & Batch Operational Semantics

It is assumed that each of the triggers action outlined in this document may be part of the larger bulk or batch operation. Individual SCIM actions should be able to be collected together to create single protocol exchanges.

This draft of the SCIM scenarios document however, does not specifically address the complexity and behavioral semantics of bulk and batch (things such as rollback, one-fail-stop etc.). Our initial focus is on identifying base flows and single operations. The specific complexity of full bulk and batch operations is left to a later version of the scenarios or to the main specification.

Cloud Service Provider to Cloud Service Provider Flows

These scenarios represent flows between two Cloud Service Providers (CSP's). It is assumed that each CSP maintains an Identity Data Store for its Cloud Service Users (CSU's). These scenarios address various joiner, mover, leaver and JIT triggers, resulting in push and pull data exchanges between the CSP's.

CSP->CSP - Joiner Push

In this scenario two CSP's (CSP-1 & CSP-2) have a shared service agreement in place that requires the exchange of Cloud Service User (CSU) accounts. CSP-1 receives a Joiner trigger action from its Enterprise Cloud Subscriber (ECS). CSP-1 creates a local user account for the new CSU. CSP-1 then pushes the new CSU joiner push request down-stream to CSP-2 and gets confirmation that the account was successfully created. After receiving the confirmation from CSP-2, CSP-1 sends an acknowledgement to the requesting ECS.

CSP->CSP - Mover Push

In this scenario two CSP's (CSP-1 & CSP-2) have a shared service agreement in place that requires the exchange of Cloud Service User (CSU) accounts. The Enterprise Cloud Subscriber (ECS-1) has already created an account with CSP-1 and supplied a critical attribute "department" that is used by CSP-1 to drive service options. CSP-1 then receives a mover trigger action from its Enterprise Cloud Subscriber (ECS). CSP-1 updates its local directory account with the new department value. CSP-1 then pushes the mover change request down-stream to CSP-2 and gets confirmation that the account was successfully updated. After receiving the confirmation from CSP-2, CSP-1 sends an acknowledgement to the requesting ECS.

CSP->CSP - Leaver Push

In this scenario two CSP's (CSP-1 & CSP-2) have a shared service agreement in place that requires the exchange of Cloud Service User (CSU) accounts. CSP-1 receives a Leaver trigger action from its Enterprise Cloud Subscriber (ECS). CSP-1 suspends the local directory account for the specified CSU account. CSP-1 then pushes a termination request for the specified CSU account down-stream to CSP-2 and gets confirmation that the account was successfully removed. After receiving the confirmation from CSP-2, CSP-1 sends an acknowledgement to the requesting ECS.

CSP->CSP - Sync

In this scenario two CSP's (CSP-1 & CSP-2) have a shared service agreement in place that requires the synchronization of Cloud Service User (CSU) accounts. On a periodic basis, CSP-1 sends a synchronization request to CSP-2 for a sub-set of its managed accounts. CSP-1 has the option to send a change-delta data set or a full data set as part of the synchronization requests. In either case, CSP-2 receives the data set and successfully carries out any required additions, updates or deletes.

CSP->CSP - JIT Push

In this scenario two CSP's (CSP-1 & CSP-2) have a shared service agreement in place that requires the exchange of Cloud Service User (CSU) accounts. However, rather than pre-provisioning accounts from CSP-1 to CSP-2, CSP-1 waits for a service access request from the Cloud Service User (CSU) before issuing account creation details to CSP-2. When the CSU completes a SSO transaction from CSP-1 to CSP-2, CSP-2 then creates an account for the CSU based on information pushed to it from CSP-1.

CSP->CSP - JIT Pull

In this scenario two CSP's (CSP-1 & CSP-2) have a shared service agreement in place that requires the exchange of Cloud Service User (CSU) accounts. However, rather than pre-provisioning accounts from CSP-1 to CSP-2, CSP-2 waits for a service access request from CSP-1's Cloud Service User (CSU). When the CSU completes a SSO transaction from CSP-1 to CSP-2, CSP-2 then pulls sufficient information from CSP-1 to create a local account for the CSU.

Enterprise Cloud Subscriber to Cloud Service Provider Flows

These scenarios represent flows between an Enterprise Cloud Subscriber (ECS) and a Cloud Service Providers (CSP). It is assumed that both the ECS and the CSP maintains an LDAP service for the relevant Cloud Service Users (CSU's). These scenarios address various joiner, mover, leaver and JIT triggers, resulting in push and pull data exchanges between the ECS and the CSP.

Many of these scenarios are very similar to those defined in the Cloud Service Provider to Cloud Service Provider section above. They are identified separately here so that we may explore any differences and might emerge.

ECS->CSP - Joiner Push

In this scenario an Enterprise Cloud Subscriber (ECS-1) maintains a service with a Cloud Service Provider (CSP-1) that requires the sharing of various Cloud Service User (CSU) accounts. A new user joins ECS-1 and so ECS-1 pushes an account creation request to CSP-1, supplying all required base SCIM schema attribute values and additional extended SCIM schema values as required.

ECS ->CSP - Mover Push

In this scenario an Enterprise Cloud Subscriber (ECS-1) maintains a service with a Cloud Service Provider (CSP-1) that drives service definition from a key account schema attribute called Department. ECS-1 wishes to move a given CSU from Department A to Department B and so it pushes an attribute update request to the CSP.

ECS ->CSP - Leaver Push

In this scenario an Enterprise Cloud Subscriber (ECS-1) maintains a service with a Cloud Service Provider (CSP-1). Upon termination of one of its employees, ECS-1 sends a suspend account request to CSP-1. One week later the ECS wished to complete the process by fully removing the Cloud Service User (CSU) account and so it sends a terminate account request to CSP-1.

ECS ->CSP - JIT Push

In this scenario an Enterprise Cloud Subscriber (ECS-1) maintains a service with a Cloud Service Provider (CSP-1). No accounts are created or exchange in advance. However, rather than pre-provisioning accounts from ECS-1 to CSP-1, ECS-1 waits for a service access request from the Cloud Service User (CSU) before issuing account creation details to CSP-1. When the CSU completes a SSO transaction from ECS-1 to CSP-2, CSP-2 then creates an account for the CSU based on information pushed to it from CSP-1.

ECS ->CSP - JIT Pull

In this scenario an Enterprise Cloud Subscriber (ECS-1) maintains a service with a Cloud Service Provider (CSP-1). No accounts are created or exchange in advance. However, rather than pre-provisioning accounts from ECS-1 to CSP-1, ECS-1 waits for a service access request from the Cloud Service User (CSU) before issuing account creation details to CSP-1. When the CSU completes a SSO transaction from ECS-1 to CSP-1, CSP-2 then creates an account for the CSU based on information pushed to it from ECS-1.