# Implementing Delegated User Administration in Verify SaaS

## Background

The purpose of this solution is to provide a limited scope delegation model in Verify SaaS such that a delegated admin can only manage the users within their organization.

Currently Verify SaaS supports the ability to scope management of users to a specific group(s), such that an organization delegated admin can only view, modify, change password and delete the user’s contained in their group. The issue is that the user must first be created and assigned to the delegated group before the admin can manage the user, and the delegated admin can’t be granted the ability to create or manage users outside of their group.

To overcome this issue, a custom orchestration flow was created that could be run by the delegated admin to create a user and assign to their group. After that, standard out-of-the-box user administration is available for the delegated admin, restricted only to users in their group.

The flow is available in the “always on demo” Verify SaaS tenant: <https://demos.verify.ibm.com> as “Delegated Admin Use Case” flow. This document goes through what was configured to enable this capability.

At time of writing, Verify SaaS has a more comprehensive Delegated Administration capability in its roadmap which will provide a more comprehensive approach. The intent of this customization is to provide a tactical approach until such a time that a more strategic capability is available.

## Pre-Req

You must have a Verify SaaS tenant. The tenant needs to be enabled with the feature flag that enables “Scope” on the Administrator Role.

## Setup

The solution entails the following:

* A custom Administrator Role that restricts the Verify SaaS functions to user management and scoped to a designated group of users
* A custom workflow that is run by the delegated admin to create users. The users are automatically assigned to the group specified in the admin’s user profile. The workflow uses a custom theme and form.

### Obtain a Privileged client\_id/client\_secret:

* If you don’t already have a privileged API client\_id/client\_secret, you’ll need to create one in your tenant. Under Security..API access then “Add API Client”.
* Initially, just select All Permissions and take note of the generated client\_id/client\_secret.

### Create Users/Groups/Administration Role:

1. Under “Directory..Attributes”:
   1. Create a “Custom Attribute”:
      1. Name: delegatedAdminGroup
      2. Description: “groupid of where delegated users are created. Used in the Delegated Admin User Create flow”
      3. Availability: SSO
      4. Defaults for everything else
2. Under “Directory..Users & Groups”:
   1. Create a delegated administrator: e.g. [delegated.admin001@yopmail.com](mailto:delegated.admin001@yopmail.com) and login and change the password.
   2. Create a delegation group: e.g. DelegatedAdminUseCase
   3. Retrieve the groupid:

# obtain an privileged access token

curl -X POST https://demos.verify.ibm.com/v1.0/endpoint/default/token -d "client\_id=<your\_client\_id>&client\_secret=<your\_client\_secret>&grant\_type=client\_credentials"

# save the access token

export AT=<returned access\_token>

# resolve the id of the “DelegatedAdminUseCase” group

curl --request GET \

--url 'https://demos.verify.ibm.com/v2.0/Groups?filter=displayName%20eq%20%22DelegatedAdminUseCase%22' \

--header 'accept: application/scim+json' \

--header "Authorization: Bearer $AT"

Output:

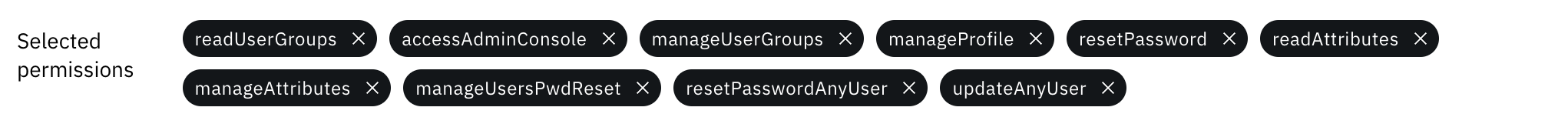
{"totalResults":1,"schemas":["urn:ietf:params:scim:api:messages:2.0:ListResponse"],"Resources":[{"displayName":"DelegatedAdminUseCase","meta":{"created":"2023-12-15T14:20:35Z","lastModified":"2024-04-15T18:16:28Z"},"id":"6450005UOL","urn:ietf:params:scim:schemas:extension:ibm:2.0:Group":{"totalMembers":3,"groupType":"standard","description":"Use case to showcase delegated administration"}}]}

* 1. Add the groupid to the delegated.admin001 user as the “delegatedAdminGroup” attribute (this is used in the workflow later so it must be populated with the corrected).
  2. The following is the result of the delegated.admin001 profile:

A close-up of a number

Description automatically generated

1. Under “Global Configuration..Administrator roles”, create a new role.
2. The following are the attributes:
   1. Role Name: DelegatedAdminUseCaseRole
   2. Description: Used to scope user administration to a specific group
   3. Permissions:



* 1. Scope: Limit group-related permissions to specific groups: <checked>
  2. Groups: DelegatedAdminUseCase

1. Under the “DelegatedAdminUseCaseRole”..manage membership:
   1. Add your delegated admin: e.g. [delegated.admin001@yopmail.com](mailto:delegated.admin001@yopmail.com)

## Create the Theme:

1. In Branding..Theme..Create a Theme
2. Name: DelegatedAdmin
3. Upload: DelegatedAdmin.zip

## Create the Orchestration Flow:

1. Import the flow: delegated\_admin\_create\_user.bpmn
2. Modify the following in the “Init Vars” function:

* <your\_client\_id>
* <your\_client\_secret>

1. In the Page: “Get User Info”
   * Ensure that Theme is: Delegated Admin
   * Ensure that Template name is: custom\_page1
2. If you need to debug the flow, uncomment out the references to “webhookUrl”. This is initialized in the “Init Vars” function and then used throughout in an hc.Post call (commented out).

## Test

1. Trigger the workflow: https://<your\_tenant\_id>/flows/?reference=delegated\_admin\_create\_user
2. Login as your delegated admin: e.g. delegated.admin001@yopmail.com
3. Provide the form details to create a new user. For example:
   * email: jeff.smith002@yopmail.com
   * First Name: Jeff
   * Last Name: Smith002
4. Once completed you will land on the launchpad. Select “Switch to Admin”
5. Select Directory..Users and Groups and manage the user just created

END OF DOCUMENT