SCIM

Overview

JFrog Subscription Levels

CLOUD (SaaS)	SELF-HOSTED
ENTERPRISE with SECURITY PACK ENTERPRISE+	ENTERPRISE X ENTERPRISE+

Page Contents

JFrog provides Enterprise and Enterprise+ customers with the ability to manage user access to the Platform through the System for Cross-domain Identity Management (SCIM 2.0) protocol, which is designed to make managing user identities easier.

The SCIM protocol complements SSO (such as SAML or OAuth), which allows to receive updates regarding users and groups. To this end, the JFrog Platform implements the parts of SCIM 2.0 required for managing users and groups, and the association between them. We have used Okta and Azure Active Directory (AD) to verify this capability.

Requirements

To implement the JFrog SCIM protocol, you will need the following:

- JFrog Platform 7.17.0 (and above)
- An identity service (e.g., Okta, Azure AD) with provisioning mode enabled

User Names

User names are the unique identifiers for users in Access. User names are case insensitive.

Associating API Keys

If you want to associate API Keys with users added through SCIM, in the SAML SSO configuration in Access, verify that the option "Allow Created Users Access To Profile Page" is selected (for more information, see SAML SSO Configuration).

Implemented Endpoints

The JFrog Platform implements the subset of SCIM 2.0 endpoints that are required to support the scenarios for managing users and groups, and the association between them:

- Get user
- Find user
- Create user
- Update user
- Disable user
- Delete user
- Get group by filter
- Get group by name
- Create group
- Update group
- Patch group
- Delete group

For more information, see Artifactory REST APIs.

WebUI Changes implemented in Artifactory 7.38.x and above

Security is now called Authentication Providers. All the relevant text and images on this page have been updated to reflect this change.

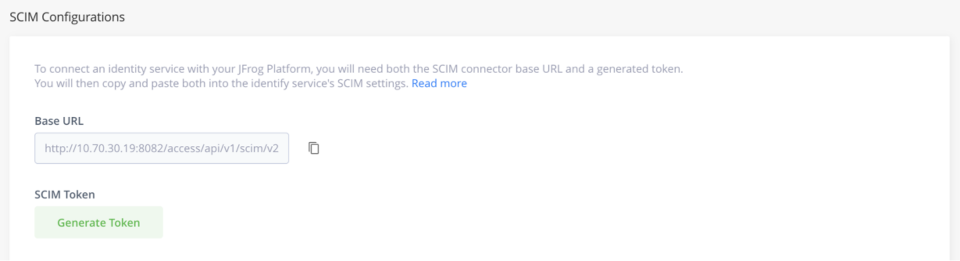
Generating an Admin Access Token

WebUI Changes implemented in Artifactory 7.38.x and above

Security is now called Authentication Providers. All the relevant text and images on this page have been updated to reflect this change.

To implement SCIM with any identity service, you will need to generate an admin access token in the JFrog Platform, and then use that token in the identity service setup.

1. In the JFrog Platform, navigate to **Administration | Authentication Providers | SCIM**.
   This displays the SCIM Configurations window.



SCIM Configurations

To connect an identity service with your JFrog Platform, you will need both the SCIM connector base URL and a generated token. You will then copy and paste both into the identify service's SCIM settings. Read more

Base URL

http://10.70.30.19:8082/access/api/v1/scim/v2

SCIM Token

To connect an identity service with your JFrog Platform, you will need both the SCIM connector base URL and a generated token.

2. Click the copy button next to the URL and paste it into the identify service's SCIM settings.
3. Click the **Generate Token** button, and then click the **Copy Token** button, and paste the token into the identify service's SCIM settings.

> **Security Note**
>
> The token can be revoked at any time via the same page. As with any other security token, it is recommended to revoke the token and recreate it occasionally for security reasons. The identity service configuration should be adjusted accordingly.

4. Go to the identity service you will be using with SCIM and follow the steps for that tool. We have used Okta and Azure Active Directory (AD) to verify this capability:
5. Go to the identity service (for example, Okta, Azure AD, etc.), and select the relevant provisioning.
6. In the Provisioning section, set the following details according to the tool. The steps below are examples of the tools you can use.

Okta

1. Go to the **Provisioning** tab.
2. Set the options **Create Users, Update User Attributes**, and **Deactivate Users** to the **To App** settings.
3. Go to the **Integration** page.
4. Set the **SCIM connector base URL** to: `https://<Artifactory_URL>/access/api/v1/scim/v2`
5. In the Unique identifier field for users, enter the **userName**.
6. In the **Supported provisioning actions** field, select all of the following options:
   - Import New Users and Profile Updates
   - Push New Users
   - Push Profile Updates
   - Push Group.
7. From the **Authentication Mode** dropdown, select **HTTP Header** and then paste the admin token you created in the JFrog Platform (see Generate an Admin Access Token).

For more information, refer to the Okta tutorial how to configure the SCIM application.

Azure AD

Follow these guidelines by specifying :

- Tenant URL: `https://<Artifactory_URL>/access/api/v1/scim/v2`
- Secret: Enter the admin access token from your JFrog Platform

> The current JFrog Artifactory template app should not be used with Azure AD.

More on Managing Users and Groups with SCIM

Click here to learn more about managing managing users and groups with SCIM in the JFrog Platform.