Permissions

Page Contents

Overview

From version 3.0, JFrog Mission Control offers a granular permissions model that provides the administrator control over how users and groups access the different resources in Mission Control. Mission Control does not have local users and groups but assigns permissions to users and groups located on an Artifactory service configured as an Authentication Provider.

> **Authentication Provider is Mandatory**
>
> It is mandatory to configure an Artifactory service as an Authentication Provider in the Mission Control onboarding wizard. The Authentication Provider manages the users, groups, and permissions using LDAP authentication tokens. When a user logs into Mission Control, he will be authenticated through the LDAP server configured in the corresponding Artifactory instance. If authentication succeeds, the Authentication Provider will assign the Mission Control permissions to the user.
>
> If the Artifactory service running as the Authentication Provider is inaccessible, you will have no access to the LDAP users and only the default Mission Control Admin user is available to manage Mission Control.

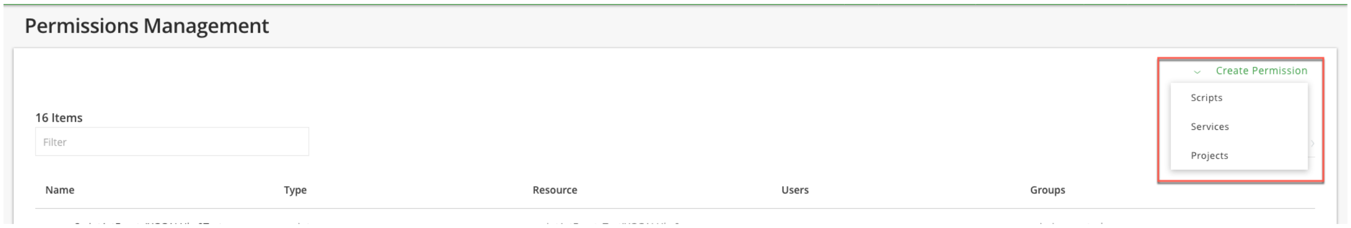
Permissions

> Only an Admin or a user belonging to the Admin permission can create permissions.

Resources

A resource is an entity that can be managed or viewed by users based on the permissions assigned by the Mission Control admin. Mission Control supports these types of resources:

- Services
- Scripts
- Projects



Users and Groups

User and groups are located and stored in the Artifactory service Authentication Provider. The Mission Control admin creates and grants permissions in Mission Control which are then saved together with the username in the Authentication Provider. If a user accesses Mission Control but has not been assigned any permissions by the Mission Control admin, he receives an error.

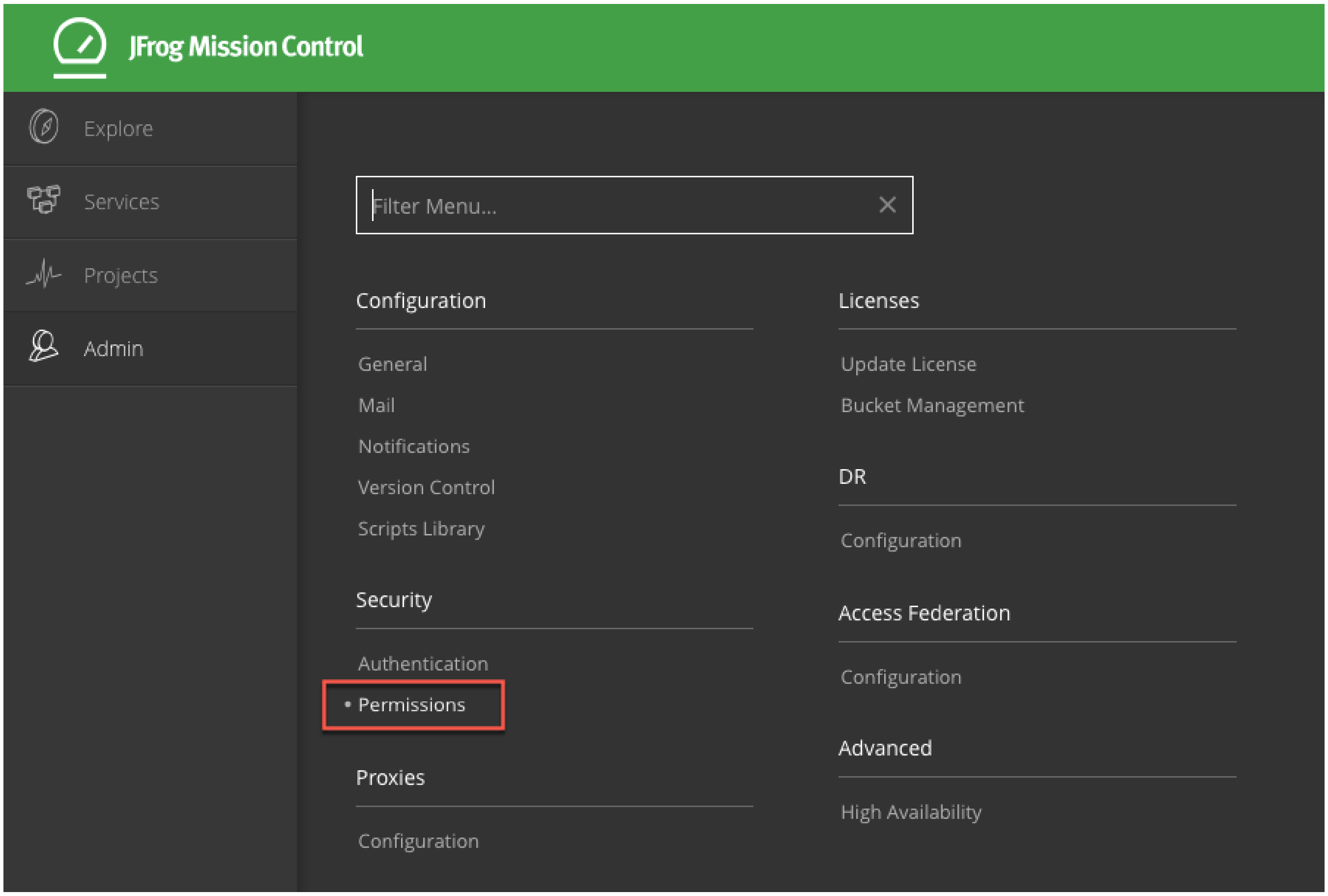
Permissions

Permissions are the actions that users can run on selected resources and vary depending on the selected resource type.

Resource Type	Permissions
Services	Configure Service, View Service
Scripts	Execute Script
Projects	Configure Project, View Project

Creating Permissions

You configure permissions in the **Admin** Module under **Security | Permissions**.



Creating a permission is a three-step process in which you select the resources, include users and groups to receive this permission and select the permission types.

After completing these steps, make sure to click **Save & Finish** to save your changes.

Services

Service is a managed entity in Mission Control. All services have to be added and managed by Mission Control to be part of the permissions object. You can assign permissions to the following services:

- Artifactory/ Artifactory Edge
- Jenkins
- Xray
- Distribution

Service Filters

Mission Control supports a set of filters that provide additional granuality for managing your services.

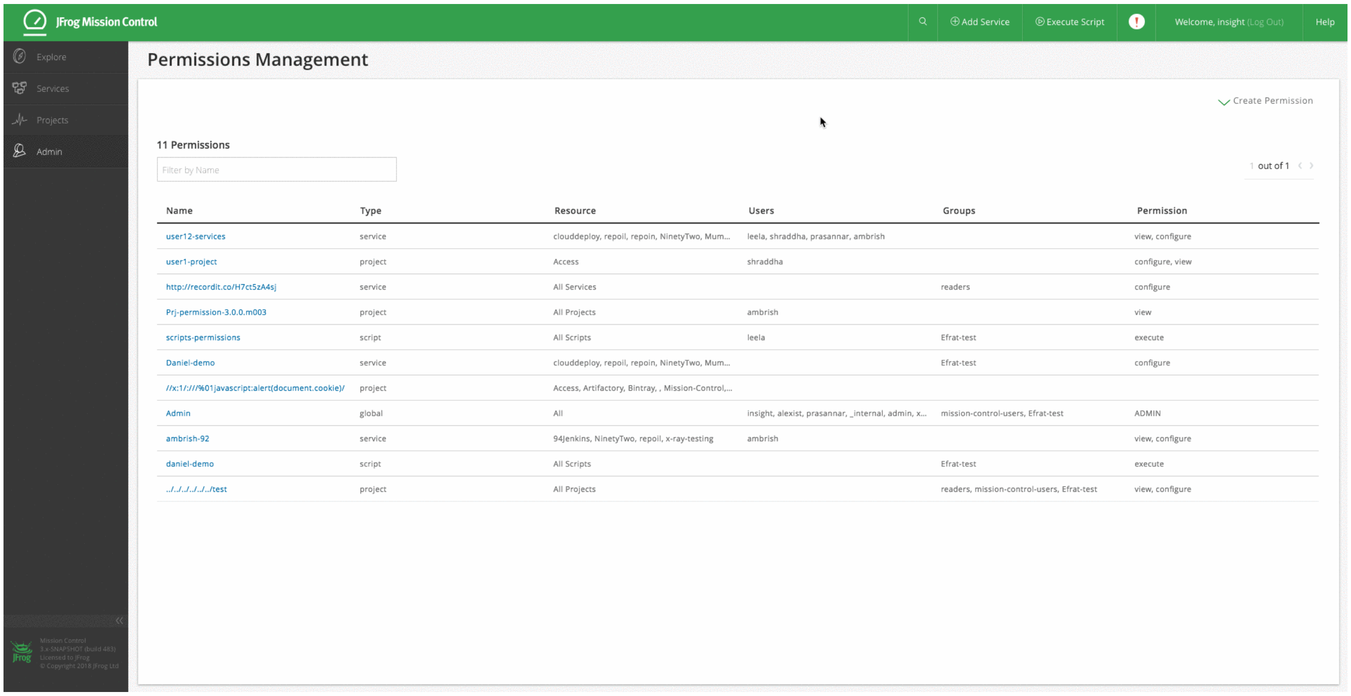
Service type	Description
Service by Type	Permissions can be assigned on a selected service type: Artifactory, Xray or Jenkins.
Service by Site	Permissions can be assigned on the selected site. All services on the selected site will be included.
Service by Name	Permissions can be assigned on a specific service.

Service Permissions

Once you have defined the resources and users/groups to which a permission applies, you can specify the actions that those users/groups can perform on the specified resources. The table below describes the actions you can specify for a permission.

Action	Description

Configure	Specifies on which services users and groups can configure services. At this point, this permission is only intended for executing scripts. The Configure permission is used together with the "Execute Script" permission to grant users the option to execute scripts on services. Only Admins can modify services settings.
View	Allows the specified users/groups to view services. This applies to any activity related to services such as service search, service details, site view, map view, service lists impact of issues etc.



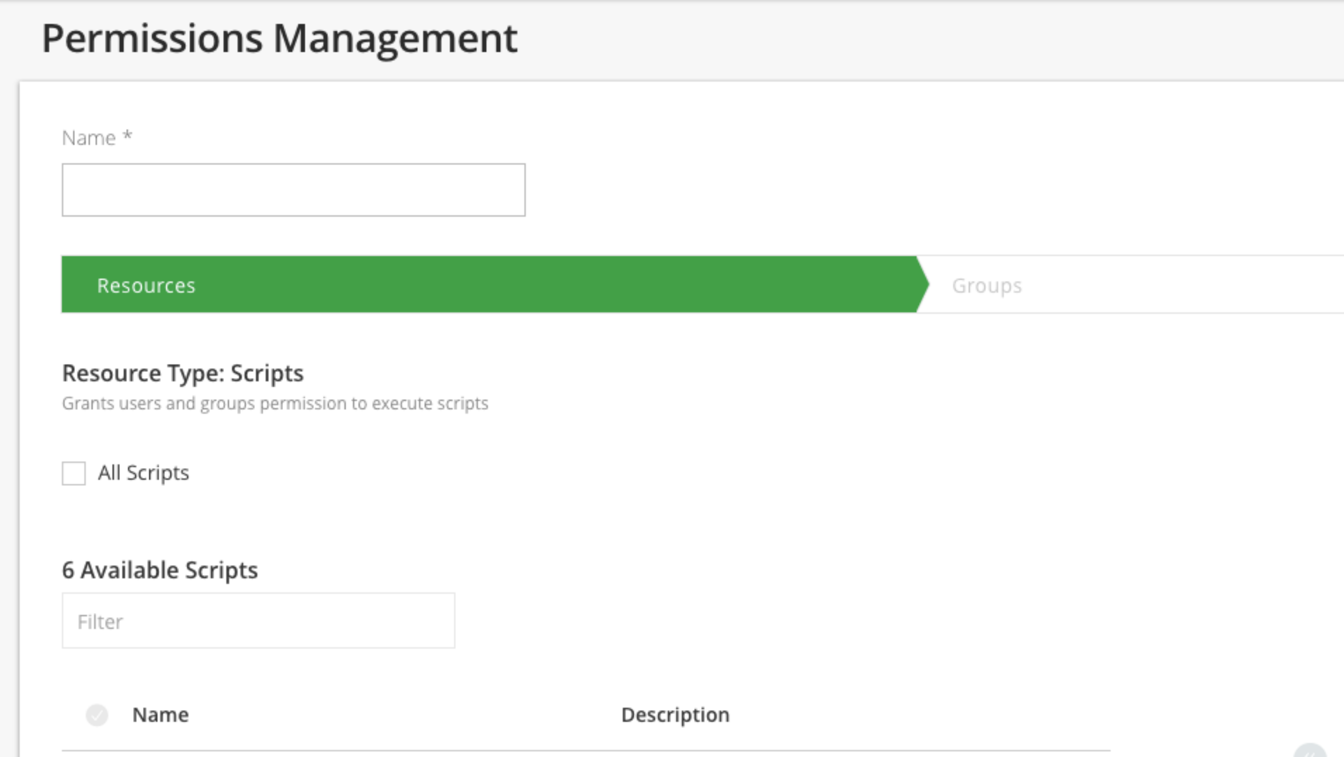
Permissions Management

11 Permissions

Name	Type	Resource	Users	Groups	Permission
user12-services	service	clouddeploy, repoil, repoin, NinetyTwo, Mum...	leela, shraddha, prasannar, ambrish		view, configure
user1-project	project	Access	shraddha		configure, view
http://recordit.co/H7ct5zA4sj	service	All Services		readers	configure
Prj-permission-3.0.0.m003	project	All Projects	ambrish		view
scripts-permissions	script	All Scripts	leela	Efrat-test	execute
Daniel-demo	service	clouddeploy, repoil, repoin, NinetyTwo, Mum...		Efrat-test	configure
//x:1/:///%01javascript:alert(document.cookie)/	project	Access, Artifactory, Bintray, , Mission-Control,...			
Admin	global	All	insight, alexist, prasannar, _internal, admin, x...	mission-control-users, Efrat-test	ADMIN
ambrish-92	service	94Jenkins, NinetyTwo, repoil, x-ray-testing	ambrish		view, configure
daniel-demo	script	All Scripts		Efrat-test	execute
../../../../../../test	project	All Projects		readers, mission-control-users, Efrat-test	view, configure

Scripts

Mission Control grants users or groups the permission to execute scripts. In the Resources tab, you select the scripts you want the users to run. The scripts displayed in the Resources tab are available on the services that you have been granted access to using the **Configure** services permission.



Permissions Management

Name *

Resource Type: Scripts

Grants users and groups permission to execute scripts

□ All Scripts

6 Available Scripts

Filter

Name	Description

Script Filters

Grants users and groups the permission to execute all scrips or only for selected scripts.

Script Permissions

Action	Description
Execute Scripts	Allows the specified users/groups to run scripts.

Admin Object Permissions

The Admin permission is automatically created when you install Mission Control with a default admin user. You can add additional users to this permission and thereby give them admin rights to manage Mission Control.

Members of the Admin permission can:

- Create sites, services and and permissions
- Gain access to the Admin Module
- Managed services

Mission Control Admin Permission

Only a Mission Control Admin can manage and create permissions. When installing Mission Control, the default Admin user is automatically created. If Mission Control is not set with an authentication provider, then effectively, there is only one user defined - the default Admin user - and this will be the only user who can access Mission Control. Once an authentication provider is set, additional users, those defined in the authentication provider, may be given access to Mission Control.

Upgrading to Mission Control Enterprise Plus removes users from previous versions

When upgrading Mission Control from version 2.x to 3.0 and above, new permission model was introduced in which there is only one locally user defined - the Admin user. All local users and groups previously defined in older (2.x) versions of Mission Control were removed. The one local Admin user can now create and manage permissions for users and groups defined in the Authentication Provider set for Mission Control.

Permission Use Cases

Script Executor Example

In this example, we will show how to provide a group called **wine-devops** with permission to execute a script called **create-my-repo** on Artifactory services RT-234 and RT-345.

This is done in two phases:

Phase 1: Grant the **wine-devops** group a **configure** permission on RT-234 and RT-345

Permission object name	Users/Groups	Actions	Resource
wine-dev-config	wine-devops	configure	Artifactory: RT-234, RT-345

Phase 2: Grant the **wine-devops** group an **execute** permission to run the **create-my-repo.groovy** script.

Permission object name	Users/Groups	Actions	Resource
wine-dev-execute	wine-devops	execute	create-my-repo. groovy

Script Writer Example

To provide any user with the permissions to write/edit a script, the user needs to be an Admin. In this example, we will provide a user called "Adam" with Admin permissions

Permission object name	Users/Groups	Actions	Resource
Admins	Adam	none	none