Ping (SSO and User Provisioning)

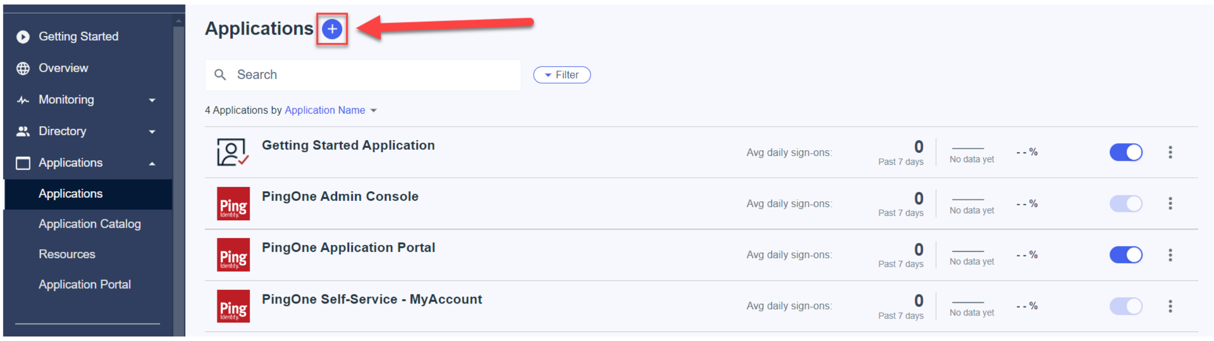
11/15/2024 12:31 pm MST

Single Sign On (SSO) is available for DocBoss. If enabled, users with the company domain will be redirected to their identity provider to sign in to access DocBoss. The instructions below outline how to set up SSO and SCIM with DocBoss when using **Ping** as the identity provider.

SSO:

1. Open Manage Environment -> Application page

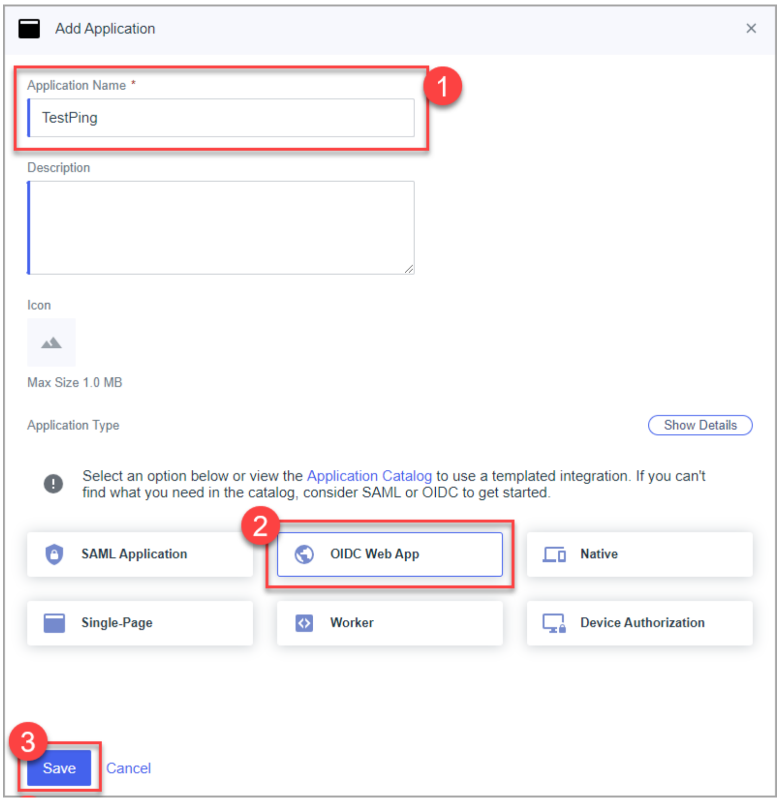
2. Click to add a new application on the "+" icon near the page title.



4 Applications by Application Name

Application					
Getting Started Application	Avg daily sign-ons:	0 Past 7 days	No data yet	- - %	●
PingOne Admin Console	Avg daily sign-ons:	0 Past 7 days	No data yet	- - %	○
PingOne Application Portal	Avg daily sign-ons:	0 Past 7 days	No data yet	- - %	●
PingOne Self-Service - MyAccount	Avg daily sign-ons:	0 Past 7 days	No data yet	- - %	○

3. Set the name for the application and choose "OIDC Web App" type. Click to save.



Add Application

Application Name * TestPing

Description

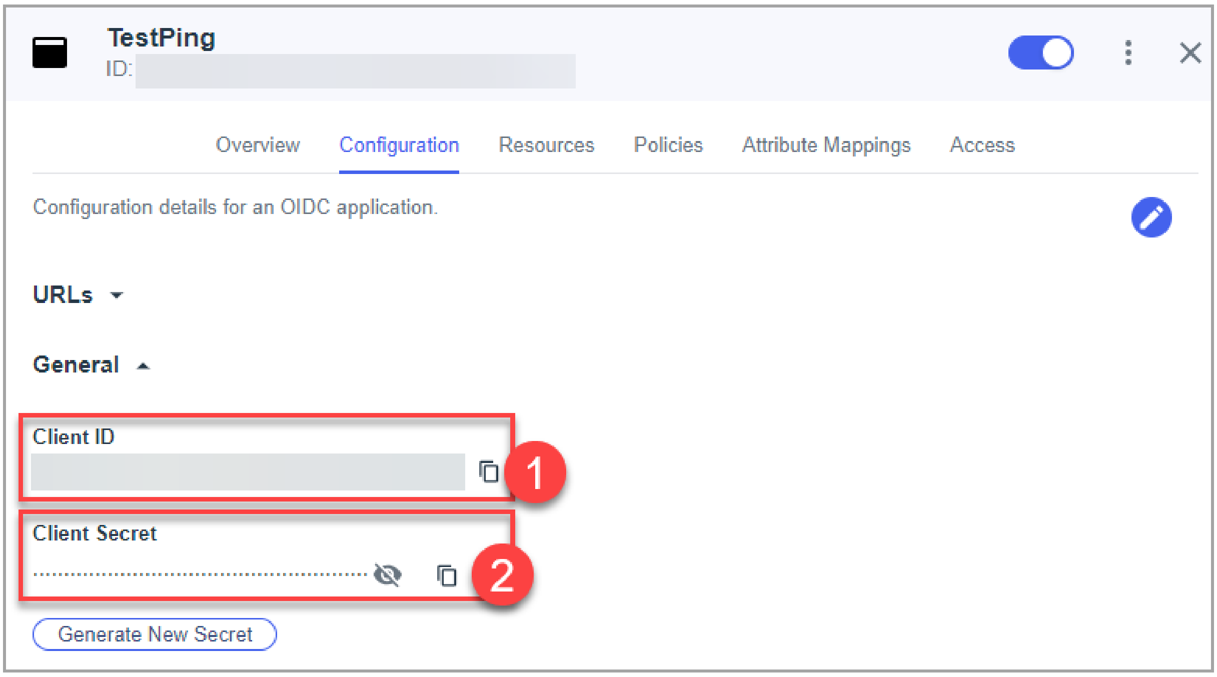
Icon

Max Size 1.0 MB

Application Type

Select an option below or view the Application Catalog to use a templated integration. If you can't find what you need in the catalog, consider SAML or OIDC to get started.

4. Copy Client ID, Client Secret on the Configuration tab, general block. Make note of these to send to DocBoss Support.



TestPing

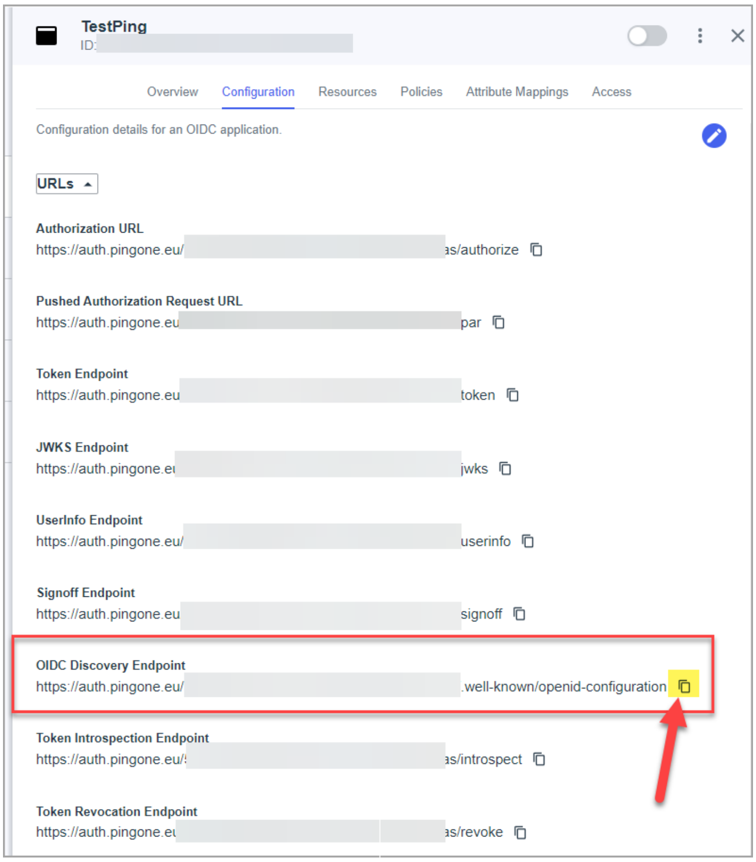
ID: [redacted]

Configuration details for an OIDC application.

Client ID [redacted]

Client Secret ···

5. Copy OIDC Discovery Endpoint on the Configuration tab, URLs block. Make note of this to send to DocBoss Support.



TestPing

ID: [redacted]

Configuration details for an OIDC application.

Authorization URL
https://auth.pingone.eu/[redacted]as/authorize

Pushed Authorization Request URL
https://auth.pingone.eu[redacted]par

Token Endpoint
https://auth.pingone.eu[redacted]token

JWKS Endpoint
https://auth.pingone.e[redacted]jwks

UserInfo Endpoint
https://auth.pingone.eu/[redacted]userinfo

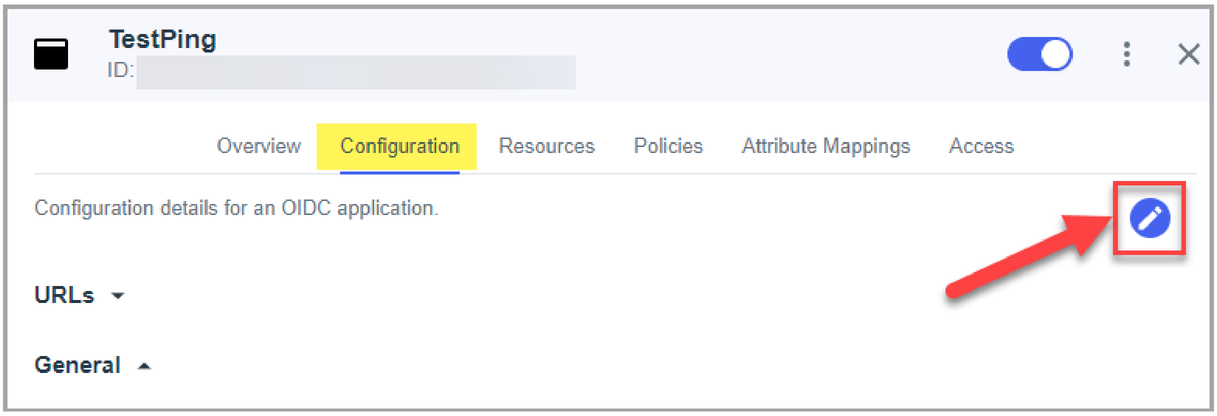
Signoff Endpoint
https://auth.pingone.eu[redacted]signoff

OIDC Discovery Endpoint
https://auth.pingone.eu/[redacted].well-known/openid-configuration

Token Introspection Endpoint
https://auth.pingone.eu/[redacted]as/introspect

Token Revocation Endpoint
https://auth.pingone.e[redacted]as/revoke

6. Click to edit Configuration settings (edit icon on the top of the configuration tab).

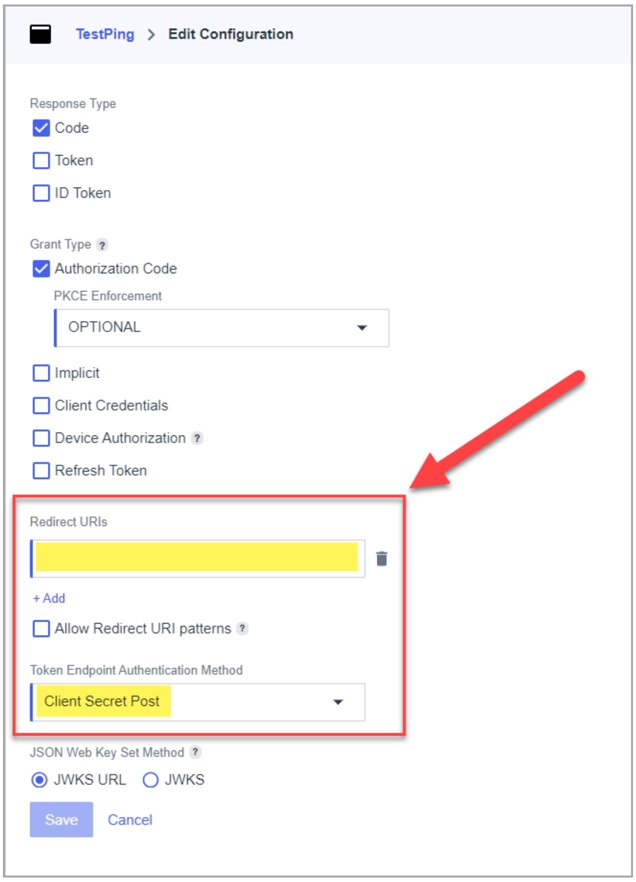


TestPing

ID: [redacted]

Configuration details for an OIDC application.

7. Set Redirect URIs [we give value to the instance] and set Token Auth Method = "Client Secret Post".



Response Type

☑ Code

□ Token

□ ID Token

Grant Type ?

☑ Authorization Code

PKCE Enforcement: OPTIONAL

□ Implicit

□ Client Credentials

□ Device Authorization ?

□ Refresh Token

Redirect URIs

□ Allow Redirect URI patterns ?

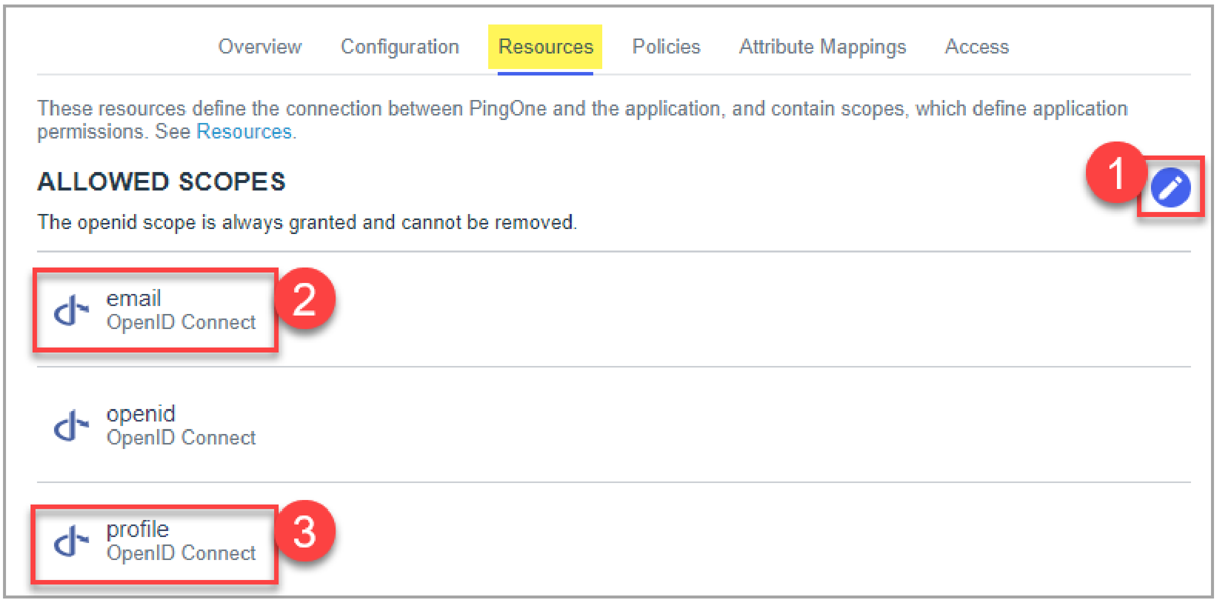
Token Endpoint Authentication Method: Client Secret Post

JSON Web Key Set Method ?

● JWKS URL ○ JWKS

8. Choose "Resources" tab and click to edit allowed scopes.

9. Select "email" and "profile" scopes and save.



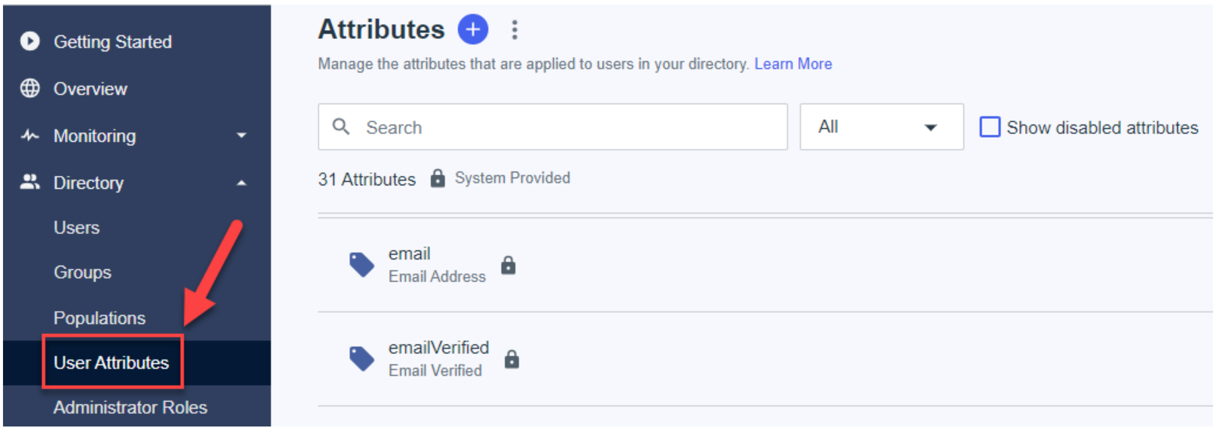
These resources define the connection between PingOne and the application, and contain scopes, which define application permissions. See Resources.

ALLOWED SCOPES

The openid scope is always granted and cannot be removed.

SCIM:

1. Open Manage Environment -> Directory -> User Attributes page.



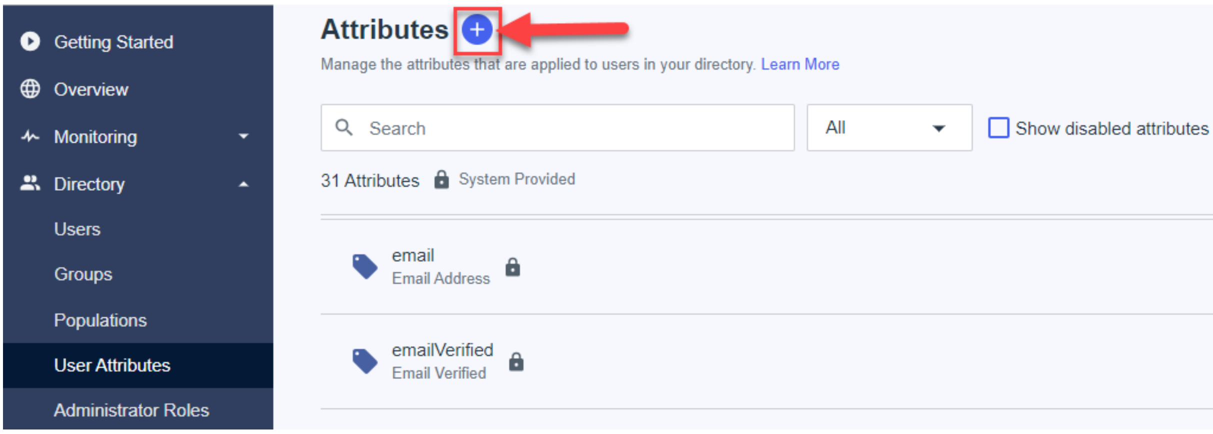
Manage the attributes that are applied to users in your directory. Learn More

31 Attributes 🔒 System Provided

email
Email Address 🔒

emailVerified
Email Verified 🔒

2. Click to add a new attributes on the "+" icon near the page title.



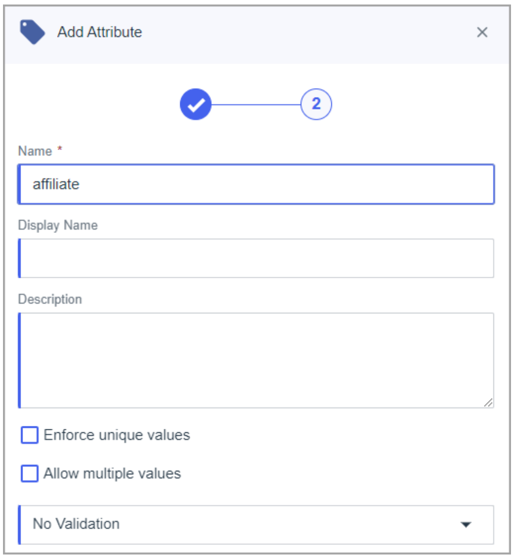
Manage the attributes that are applied to users in your directory. Learn More

31 Attributes 🔒 System Provided

email
Email Address 🔒

emailVerified
Email Verified 🔒

3. Add two attributes: userType and affiliate, type = declared.



Add Attribute

Name *

affiliate

Display Name

Description

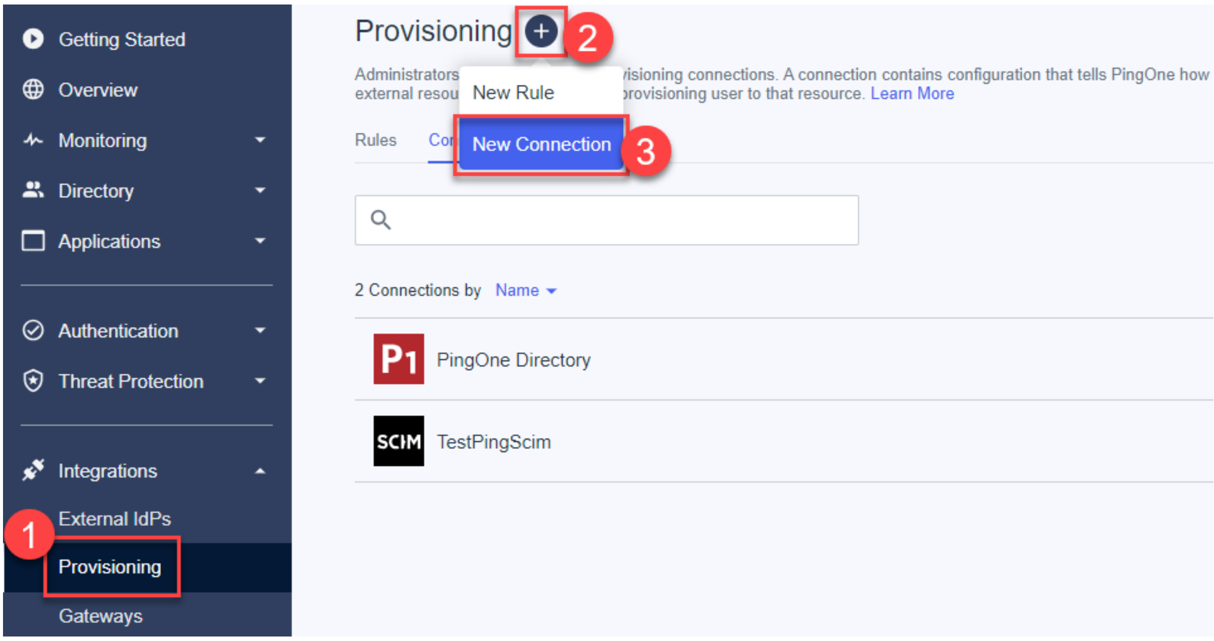
□ Enforce unique values

□ Allow multiple values

No Validation

4. Open Manage Environment ->Integrations -> Provisioning page (see below)

5. Click to add a new connection on the "+" icon near the page title.



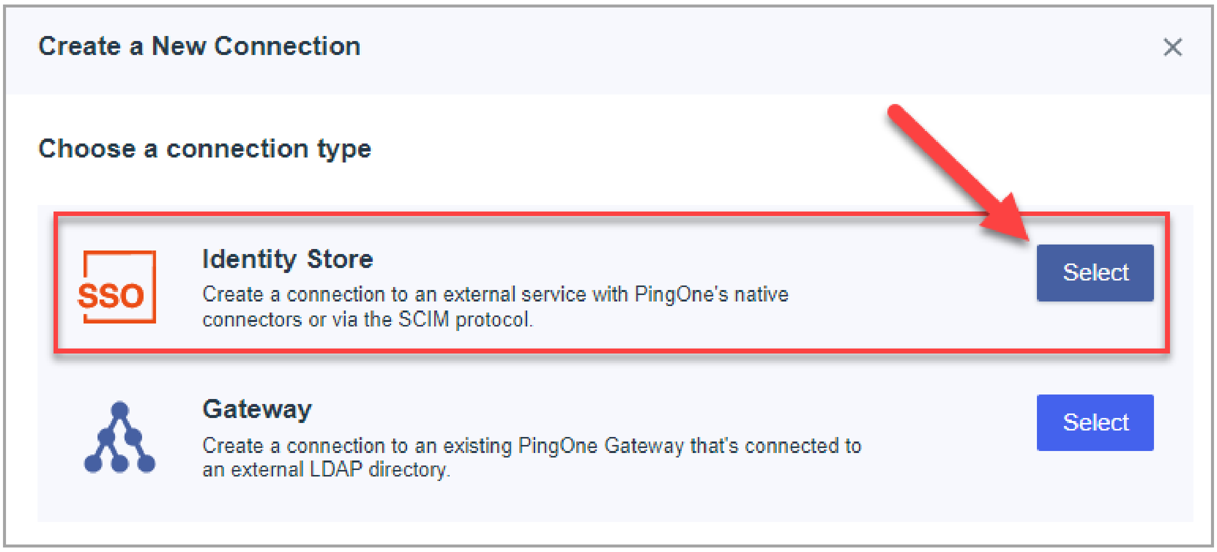
Provisioning

Administrators … isioning connections. A connection contains configuration that tells PingOne how external resou … provisioning user to that resource. Learn More

2 Connections by Name

P1	PingOne Directory
SCIM	TestPingScim

6. Choose a connection type "Identity Store".



Create a New Connection

Choose a connection type

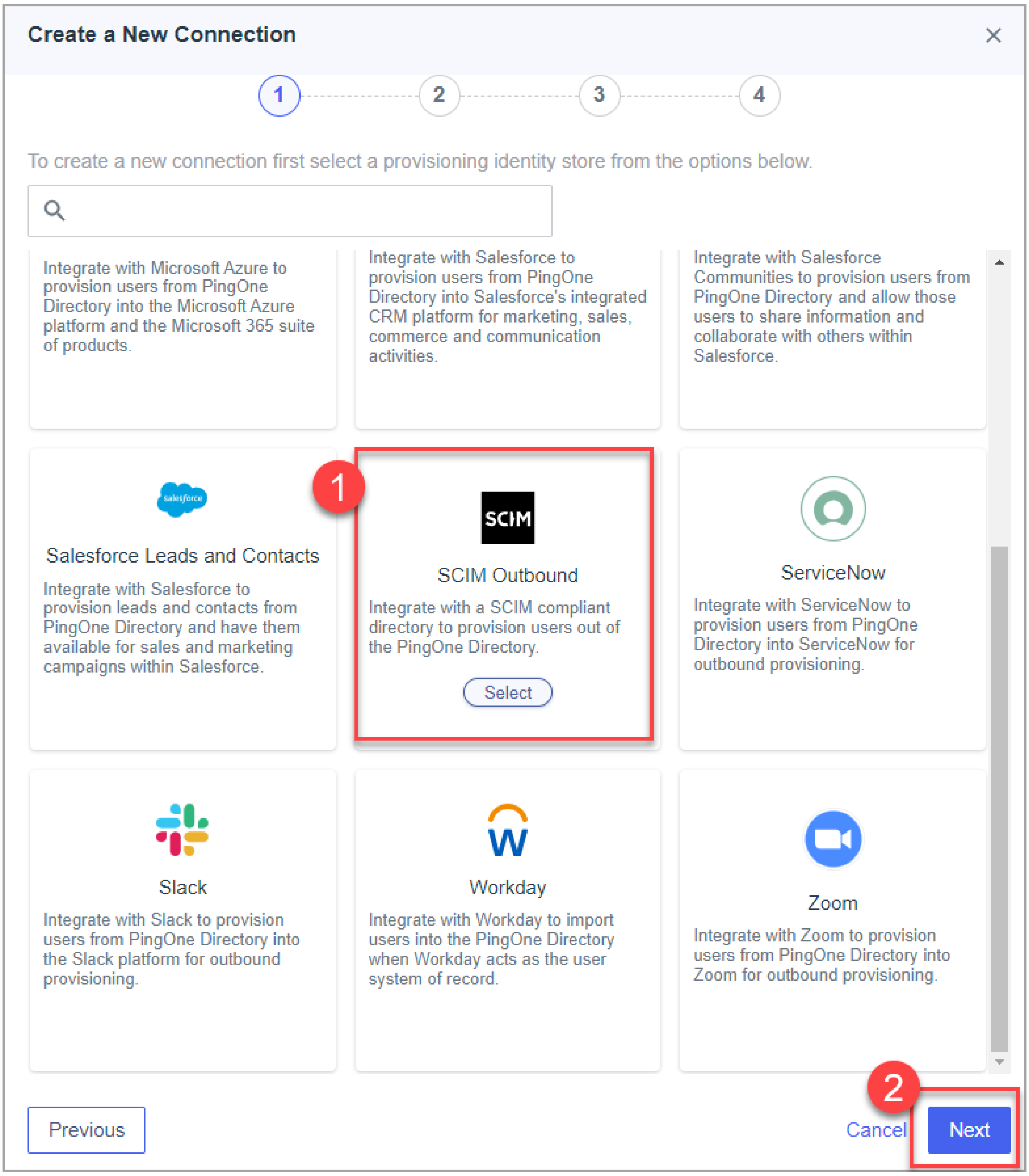
Identity Store

Create a connection to an external service with PingOne's native connectors or via the SCIM protocol.

Gateway

Create a connection to an existing PingOne Gateway that's connected to an external LDAP directory.

7. Choose "SCIM Outbound" and click next.



Create a New Connection

To create a new connection first select a provisioning identity store from the options below.

Integrate with Microsoft Azure to provision users from PingOne Directory into the Microsoft Azure platform and the Microsoft 365 suite of products.

Integrate with Salesforce to provision users from PingOne Directory into Salesforce's integrated CRM platform for marketing, sales, commerce and communication activities.

Integrate with Salesforce Communities to provision users from PingOne Directory and allow those users to share information and collaborate with others within Salesforce.

Salesforce Leads and Contacts

Integrate with Salesforce to provision leads and contacts from PingOne Directory and have them available for sales and marketing campaigns within Salesforce.

SCIM Outbound

Integrate with a SCIM compliant directory to provision users out of the PingOne Directory.

ServiceNow

Integrate with ServiceNow to provision users from PingOne Directory into ServiceNow for outbound provisioning.

Slack

Integrate with Slack to provision users from PingOne Directory into the Slack platform for outbound provisioning.

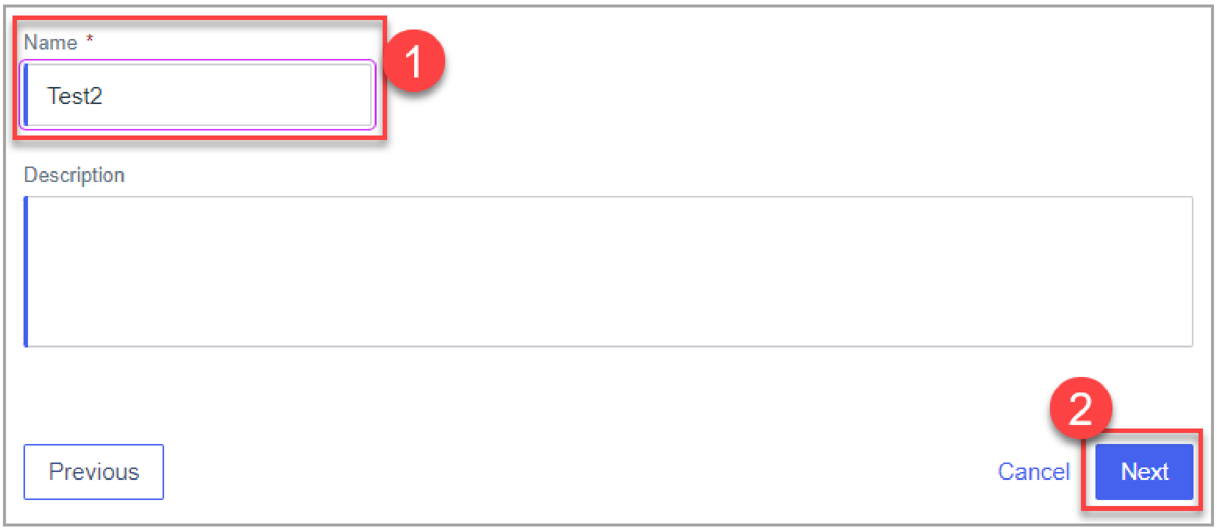
Workday

Integrate with Workday to import users into the PingOne Directory when Workday acts as the user system of record.

Zoom

Integrate with Zoom to provision users from PingOne Directory into Zoom for outbound provisioning.

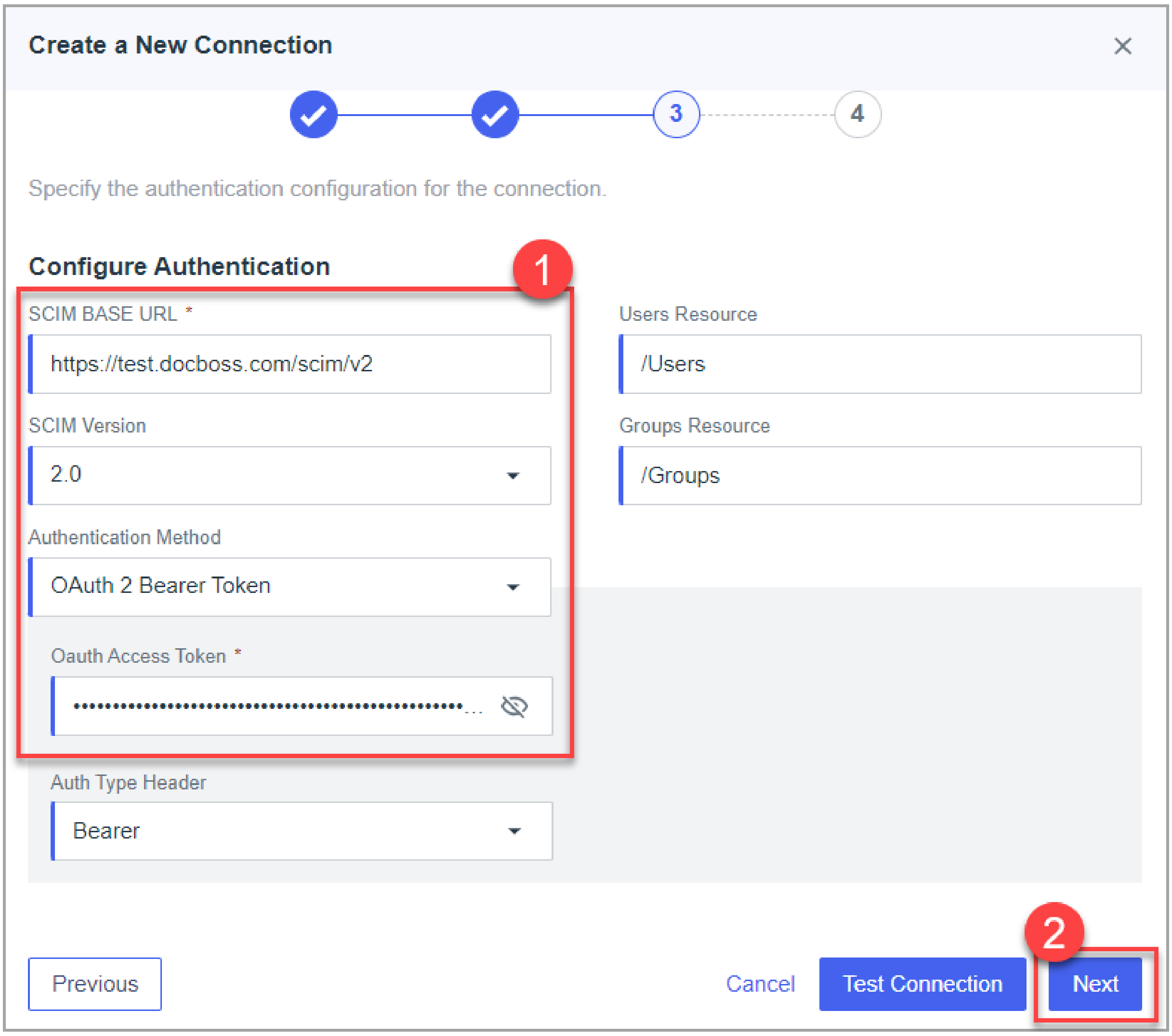
8. Set the name for the application and click next.



Name * Test2

Description

9. Set following values and click next :



Create a New Connection

Specify the authentication configuration for the connection.

Configure Authentication

SCIM BASE URL * https://test.docboss.com/scim/v2

SCIM Version 2.0

Authentication Method OAuth 2 Bearer Token

Oauth Access Token * ••…

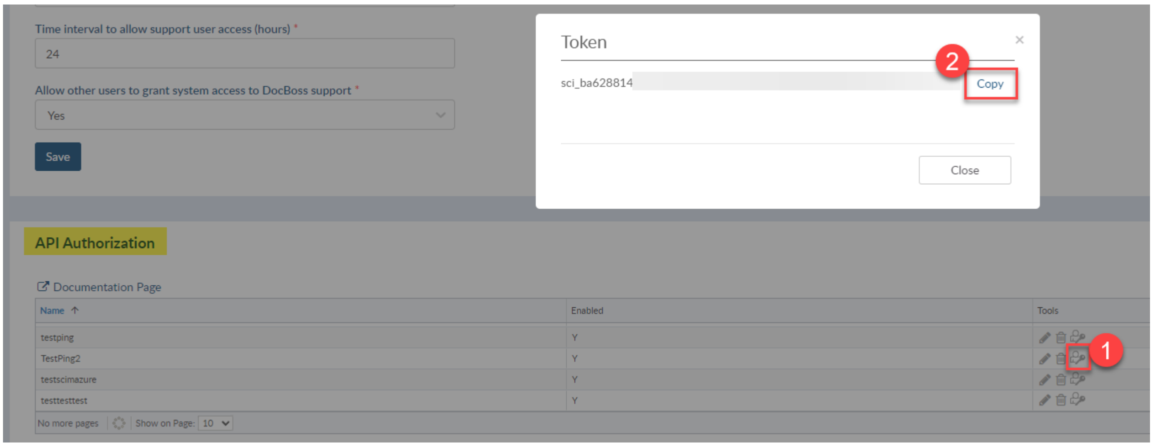
Auth Type Header Bearer

Users Resource /Users

Groups Resource /Groups

- SCIM BASE URL = [X should be replaced with system number empty or 2, 3, 4, 5, 6]
- SCIM Version = 2.0
- Authentication Method = OAuth 2 Bearer Token

- Oauth Access Token = Docboss long term token [copy from docboss]



Time interval to allow support user access (hours) *

24

Allow other users to grant system access to DocBoss support *

Yes

Save

Token

sci_ba628814[redacted]

API Authorization

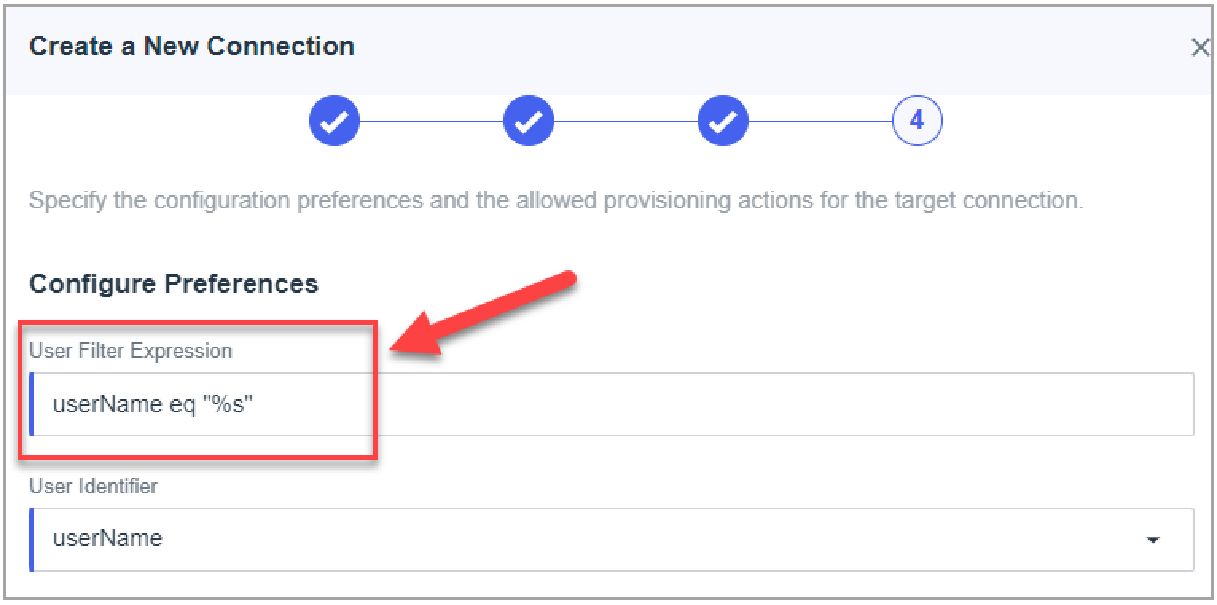
Documentation Page

Name ↑	Enabled	Tools
testping	Y	
TestPing2	Y	
testscimazure	Y	
testtesttest	Y	

No more pages

Show on Page: 10

10. Set User Filter Expression = userName eq "%s" and click to save [case sensitive]



Create a New Connection

Specify the configuration preferences and the allowed provisioning actions for the target connection.

Configure Preferences

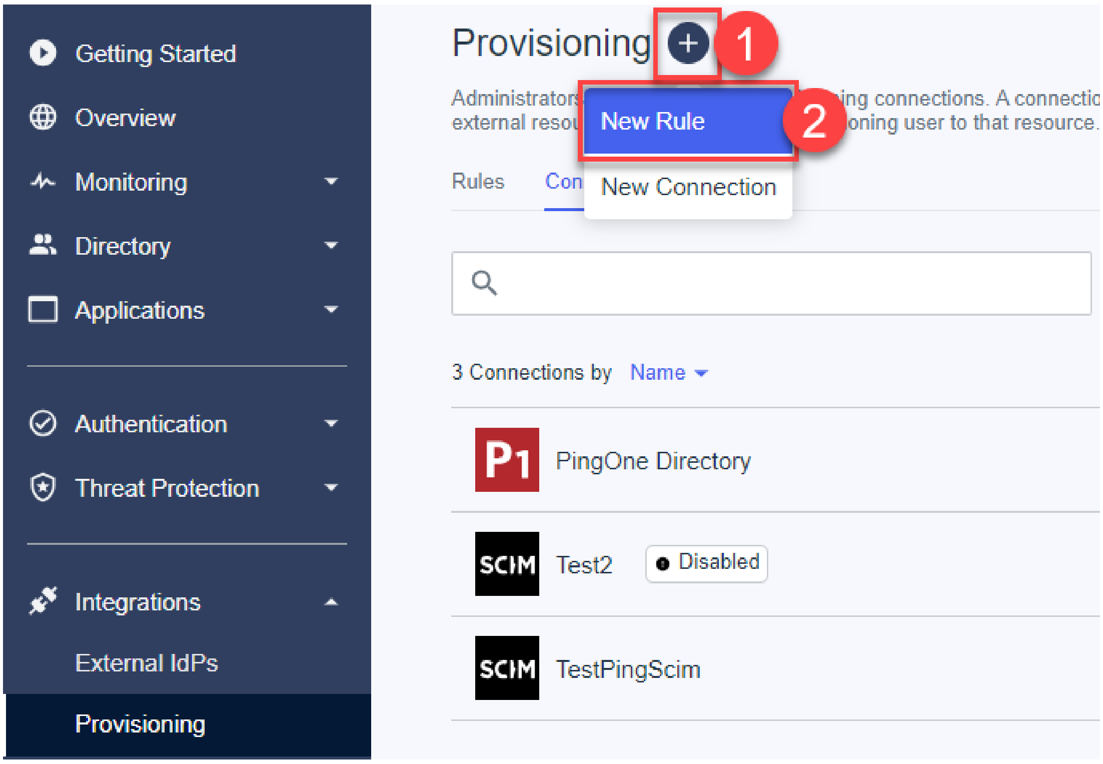
User Filter Expression

userName eq "%s"

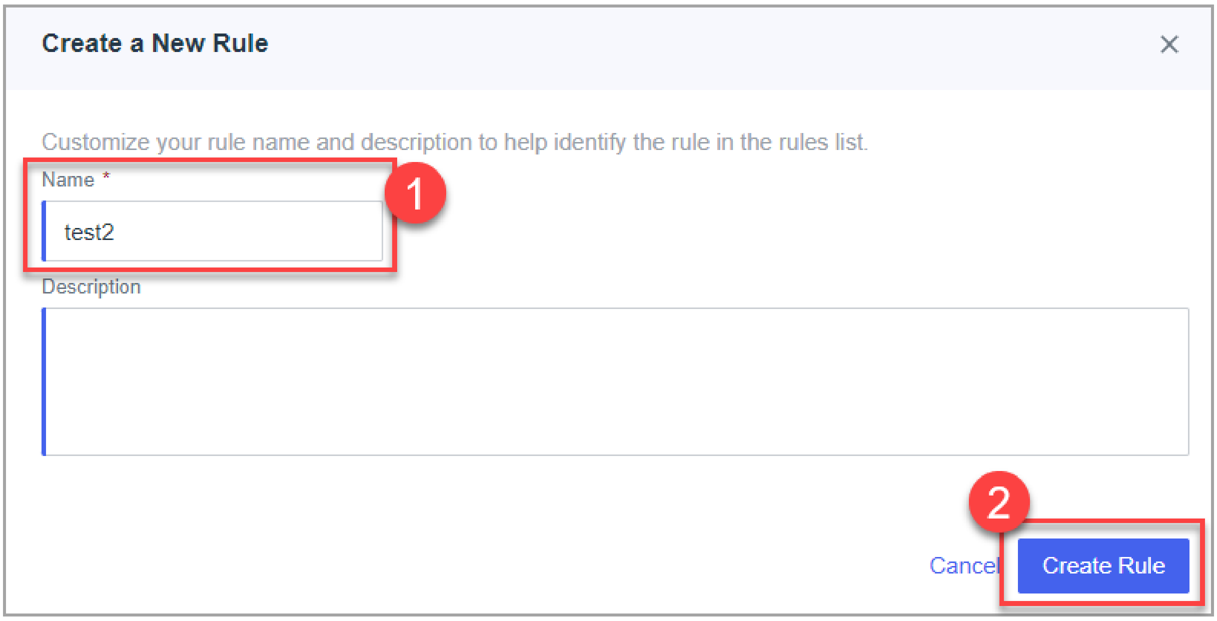
User Identifier

userName

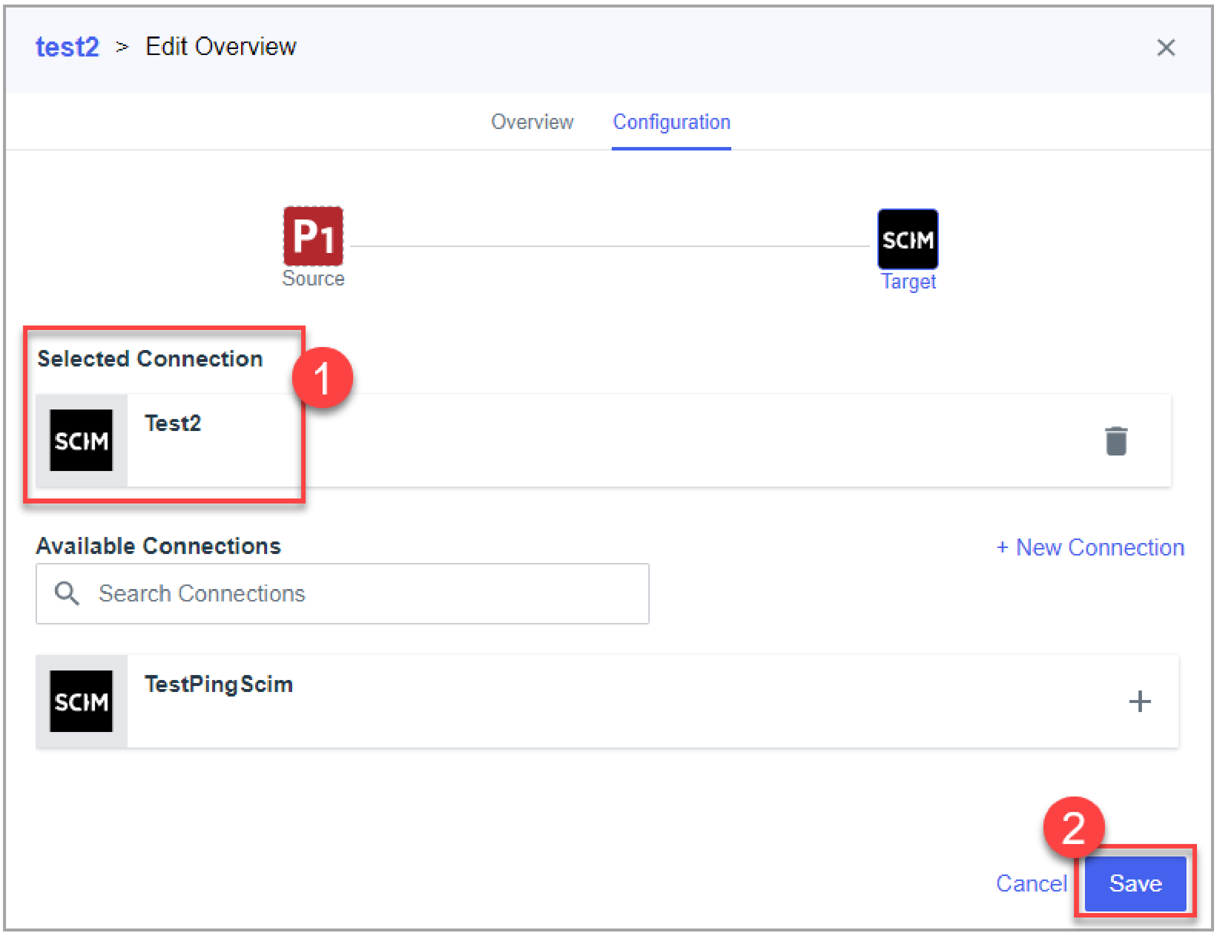
11. Click on the "+" icon near the page title to add a new rule



12. Set the name and click to create the rule.


Create a New Rule
Customize your rule name and description to help identify the rule in the rules list.
Name *
test2
1
Description
2
Cancel
Create Rule

13. Select created connection and save



test2 > Edit Overview

Selected Connection

SCIM Test2

Available Connections

+ New Connection

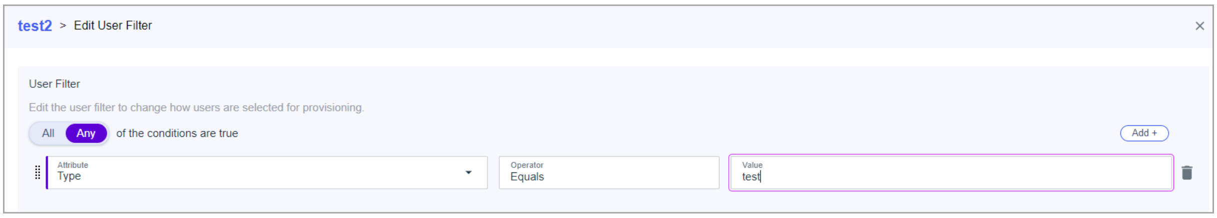
Search Connections

SCIM TestPingScim

Cancel Save

14. Click to edit filter and set how the users should be selected for provisioning and save

15.



test2 > Edit User Filter

User Filter

Edit the user filter to change how users are selected for provisioning.

All [✓ Any] of the conditions are true

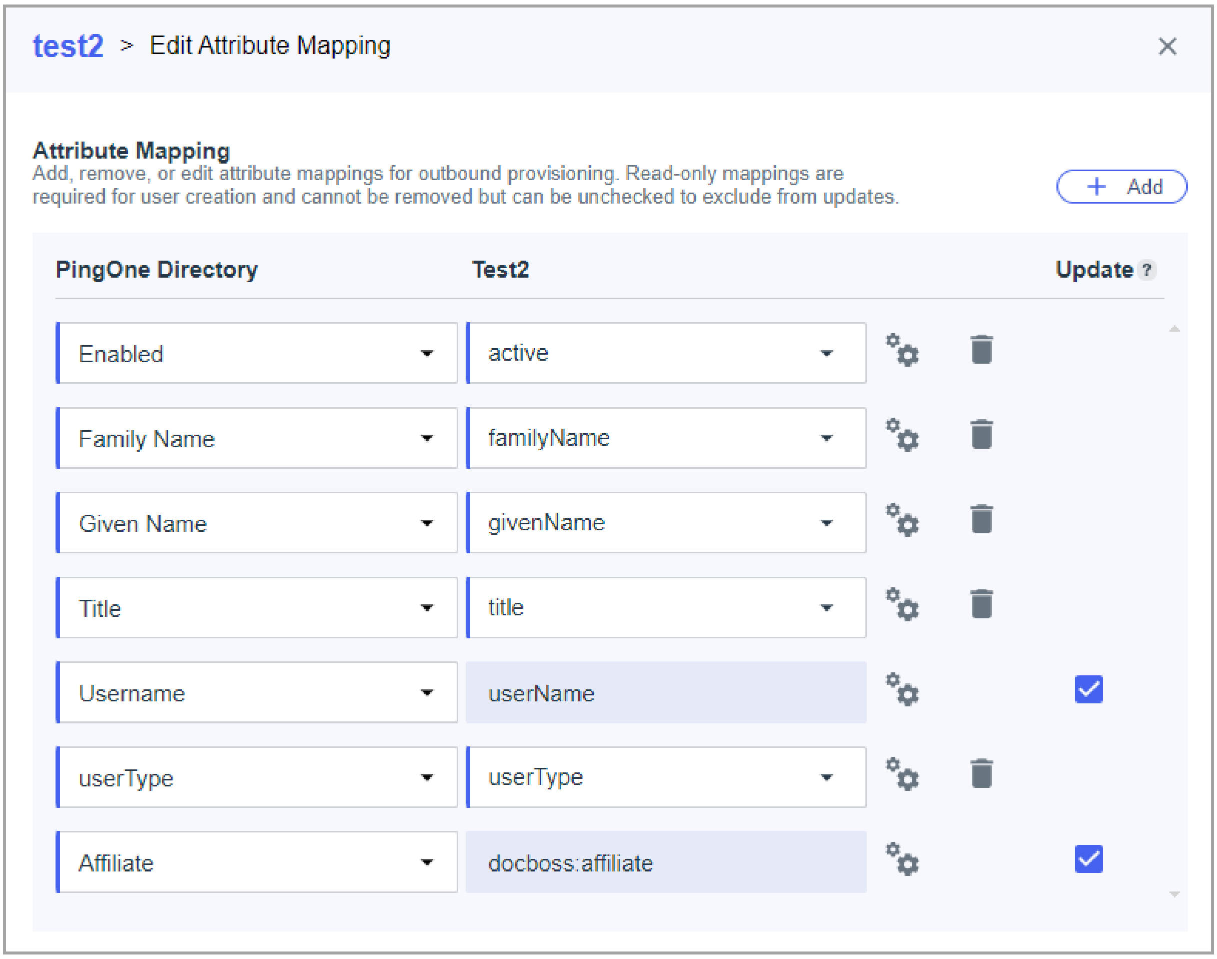
Add +

Attribute: Type

Operator: Equals

Value: test

16. Add mapping for fields. Remove excess fields added for mapping by default.



test2 > Edit Attribute Mapping

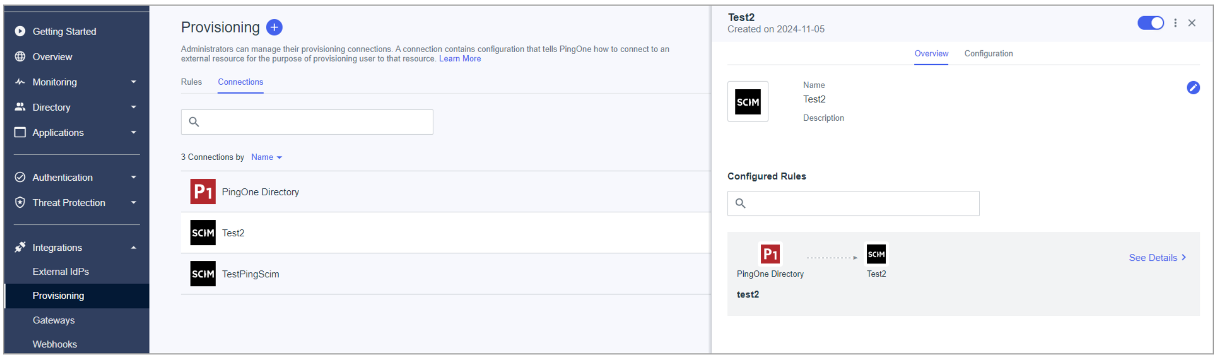
Attribute Mapping

Add, remove, or edit attribute mappings for outbound provisioning. Read-only mappings are required for user creation and cannot be removed but can be unchecked to exclude from updates.

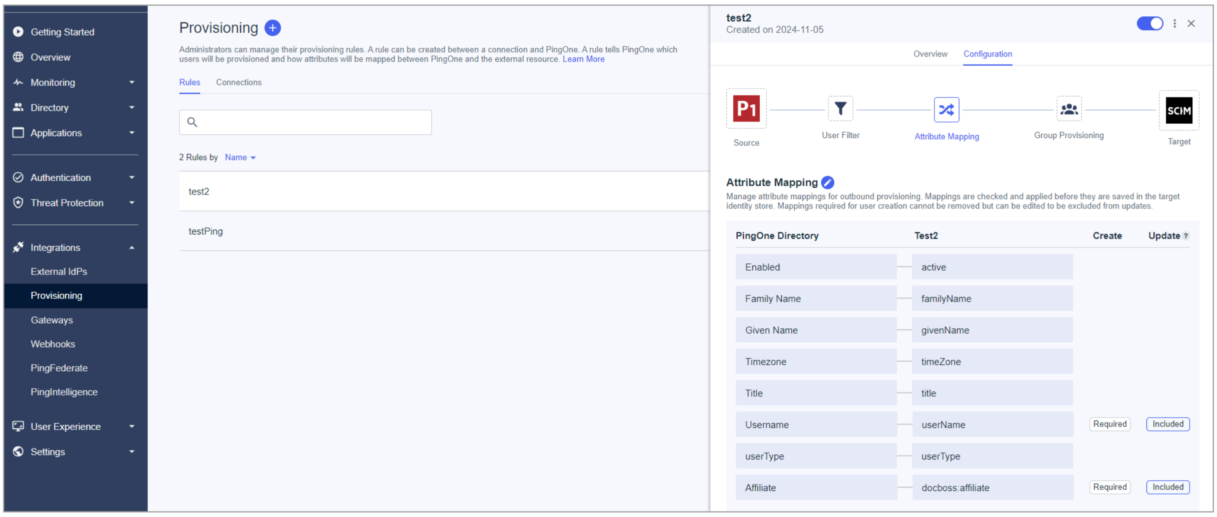
PingOne Directory	Test2	Update ?
Enabled	active	
Family Name	familyName	
Given Name	givenName	
Title	title	
Username	userName	☑
userType	userType	
Affiliate	docboss:affiliate	☑

17. List of all avaliable parameters:
    - "userName" - required, value should be unique. Value will be saved as login for user
    - "familyName" - required
    - "givenName" - required
    - "active" - required. Value is used to disable\enable user
    - "userType" - not required. If user doesn't add field to mapping OR send empty value "View" role will be saved. Allowed values are Admin, Full, Reviewer, View [case sensetive]
    - "affiliate" - not required. Created with instance affiliate will be set for user
    - "title" - not required. User can skip adding this field to mapping

18. Enable connection



19. Enable rule


Getting Started
Overview
Monitoring
Directory
Applications
Authentication
Threat Protection
Integrations
External IdPs
Provisioning
Gateways
Webhooks
PingFederate
PingIntelligence
User Experience
Settings
Provisioning
Administrators can manage their provisioning rules. A rule can be created between a connection and PingOne. A rule tells PingOne which users will be provisioned and how attributes will be mapped between PingOne and the external resource. Learn More
Rules
Connections
2 Rules by Name
test2
testPing
test2
Created on 2024-11-05
Overview
Configuration
Source
User Filter
Attribute Mapping
Group Provisioning
Target
Attribute Mapping
Manage attribute mappings for outbound provisioning. Mappings are checked and applied before they are saved in the target identity store. Mappings required for user creation cannot be removed but can be edited to be excluded from updates.

PingOne Directory	Test2	Create	Update
Enabled	active		
Family Name	familyName		
Given Name	givenName		
Timezone	timeZone		
Title	title		
Username	userName	Required	Included
userType	userType		
Affiliate	docboss:affiliate	Required	Included

Implementing

Once the steps above are complete and you have provided the information to DocBoss as noted in them, reach out to DocBoss Support and we will schedule a meeting to enable SSO (and user provisioning, if using). Our Support will also provide a redirect URI for your application. This will redirect users back to DocBoss after authentication in your identity provider. This must be added in your identity provider application for SSO to function.

If you want to try the function, then schedule a roll out for your users we can schedule the meeting to enable, test (have a user login), then disable within a few minutes. Already logged in users would not be affected. You can then communicate to your user base with a timeline for the switch. Alternatively, we can just leave it enabled after the test is successful.