Configuring SCIM Provisioning with PingFederate

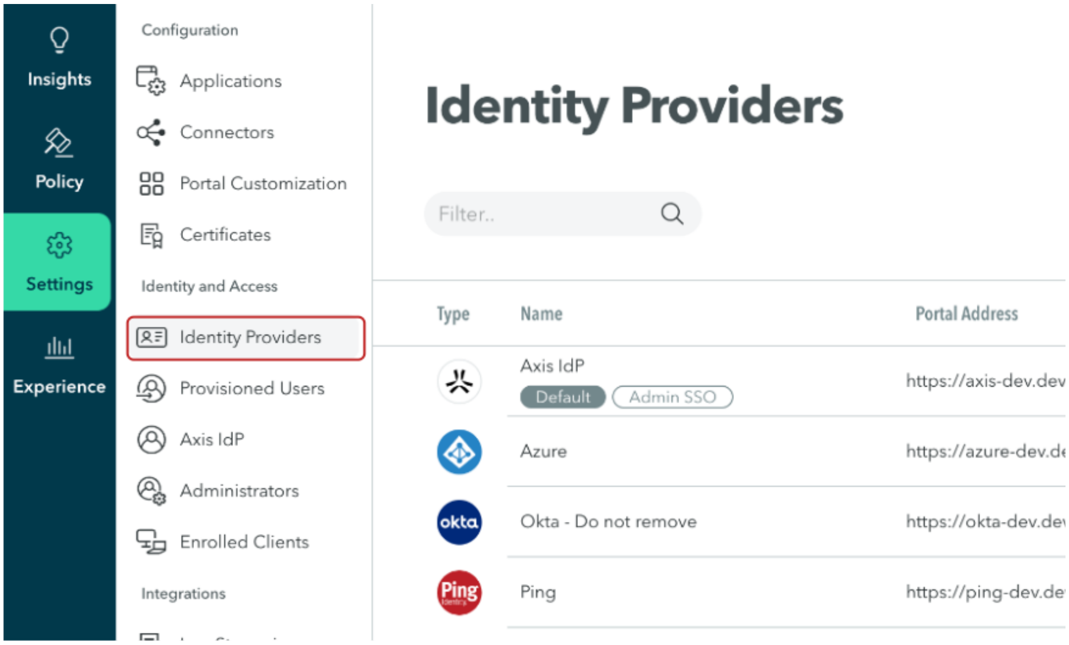
This article describes how to configure SCIM user provisioning with PingFederate as the identity provider. This will allow Axis to continuously synchronize user identity and group information from a user datastore configured in PingFederate.

Prerequisites

- PingFederate version 9.0 and later.
- The PingFederate server must have:
    - A configured user datastore where user details and attributes are stored
    - SCIM Provisioner integration files deployed
    - Provisioning and single sign-on enabled on the user datastore

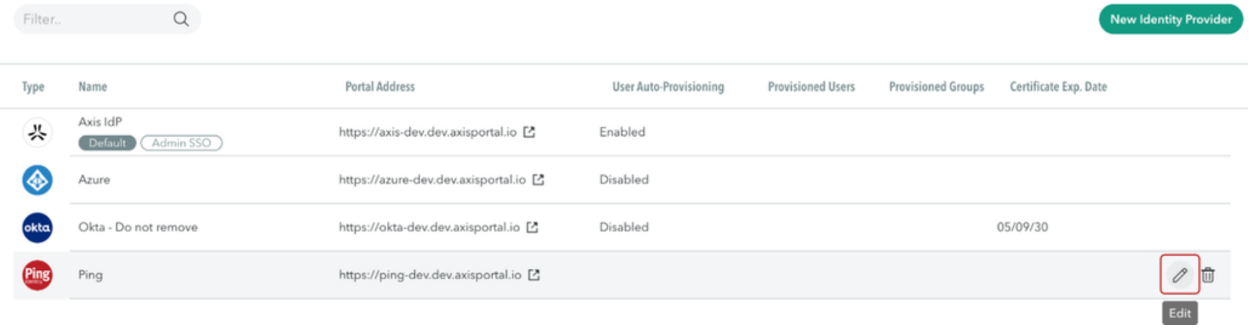
1. Enabling User Auto Provisioning with PingFederate in the Axis Management Console

1. In the **Management Console**, go to **Settings**-> **Identity Providers**.



Type	Name	Portal Address
	Axis IdP Default Admin SSO	https://axis-dev.dev
	Azure	https://azure-dev.de
okta	Okta - Do not remove	https://okta-dev.de
Ping	Ping	https://ping-dev.de

2. Hover over the **PingFederate Identity Provider** and select edit.

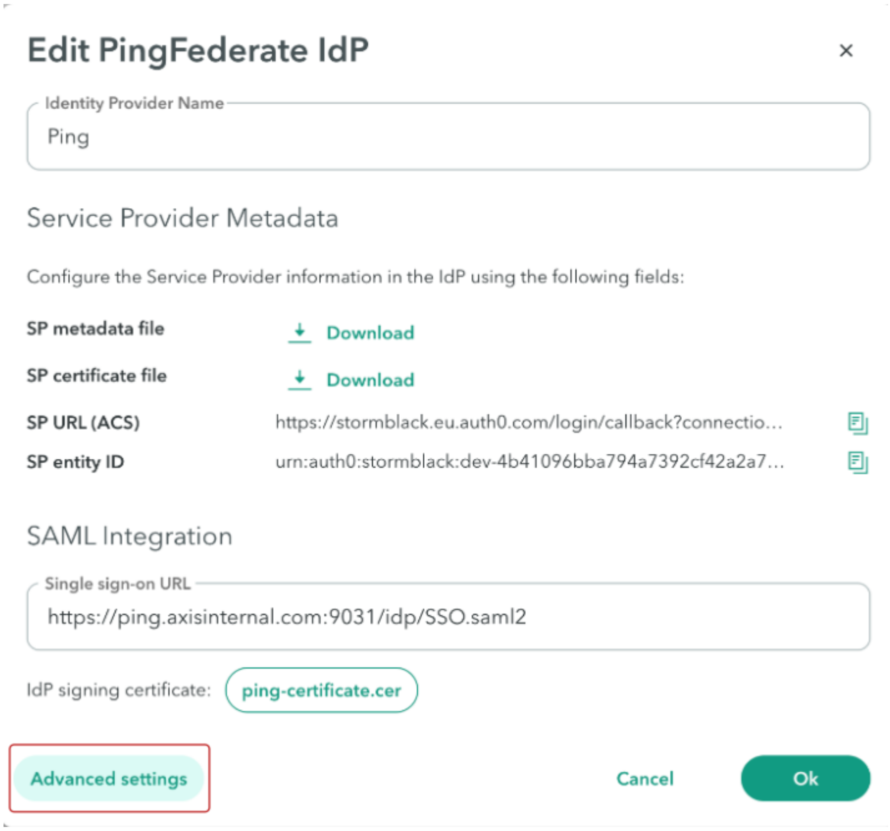


Filter..

New Identity Provider

Type	Name	Portal Address	User Auto-Provisioning	Provisioned Users	Provisioned Groups	Certificate Exp. Date
	Axis IdP Default Admin SSO	https://axis-dev.dev.axisportal.io	Enabled			
	Azure	https://azure-dev.dev.axisportal.io	Disabled			
okta	Okta - Do not remove	https://okta-dev.dev.axisportal.io	Disabled			05/09/30
Ping	Ping	https://ping-dev.dev.axisportal.io				

3. Navigate to **Advanced Settings**.



Edit PingFederate IdP

Identity Provider Name: Ping

Service Provider Metadata

Configure the Service Provider information in the IdP using the following fields:

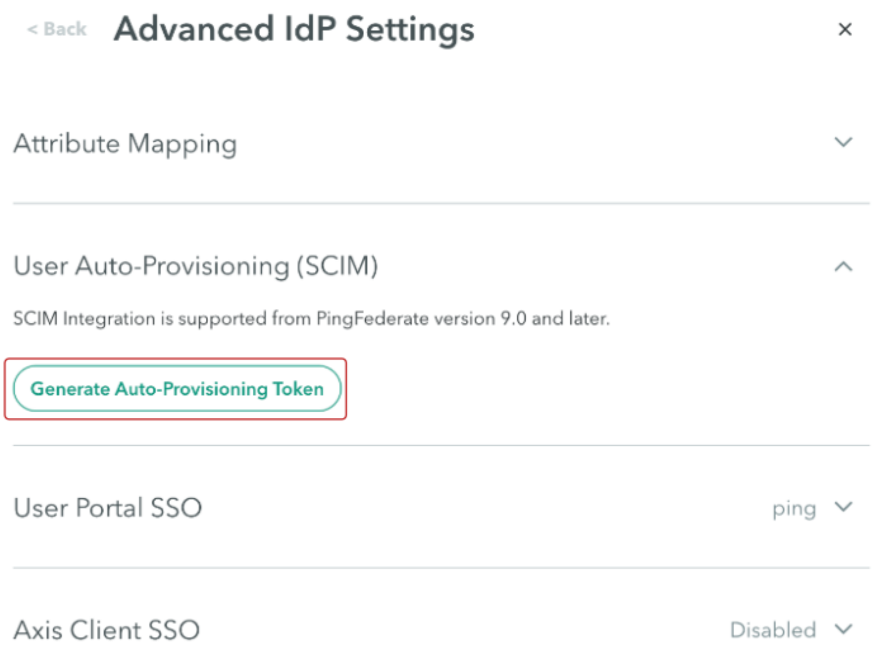
SP metadata file	Download
SP certificate file	Download
SP URL (ACS)	https://stormblack.eu.auth0.com/login/callback?connectio...
SP entity ID	urn:auth0:stormblack:dev-4b41096bba794a7392cf42a2a7...

SAML Integration

Single sign-on URL: https://ping.axisinternal.com:9031/idp/SSO.saml2

IdP signing certificate: ping-certificate.cer

4. Go to **User Auto-Provisioning (SCIM)**.
5. Click **Generate new token**.



Advanced IdP Settings

Attribute Mapping

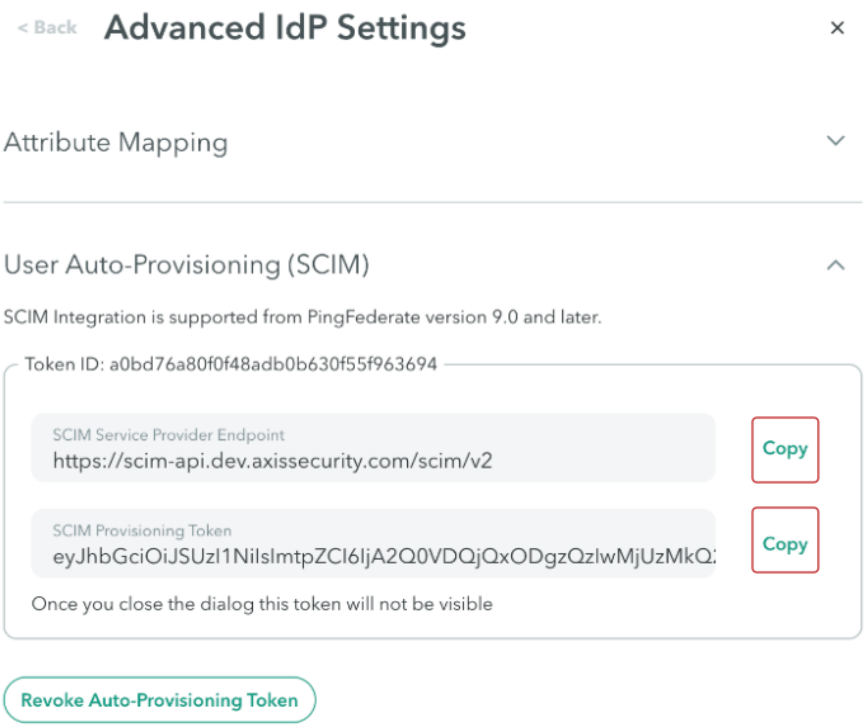
User Auto-Provisioning (SCIM)

SCIM Integration is supported from PingFederate version 9.0 and later.

User Portal SSO: ping

Axis Client SSO: Disabled

6. Copy the **SCIM Service Provider Endpoint** and **SCIM Provisioning Token** and paste them into a text editor. You will need these details for **Step 2: Creating a PingFederate SCIM Connector**.



Advanced IdP Settings

Attribute Mapping

User Auto-Provisioning (SCIM)

SCIM Integration is supported from PingFederate version 9.0 and later.

Token ID: a0bd76a80f0f48adb0b630f55f963694

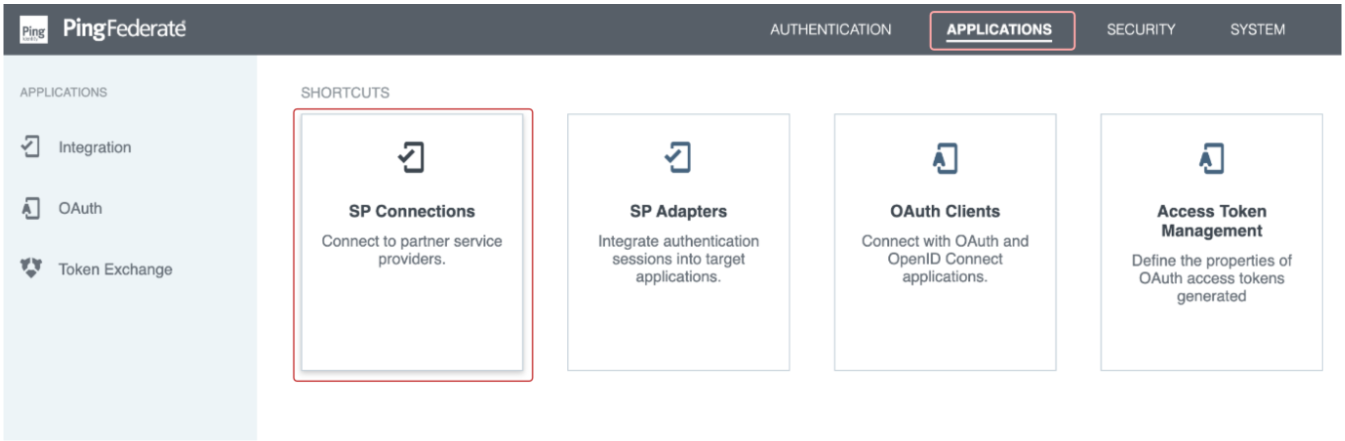
SCIM Service Provider Endpoint: https://scim-api.dev.axissecurity.com/scim/v2

SCIM Provisioning Token: eyJhbGciOiJSUzI1NiIsImtpZCI6IjA2Q0VDQjQxODgzQzIwMjUzMkQ

Once you close the dialog this token will not be visible

2 Creating a PingFederate SCIM Connector

1. Log in as an administrator to your PingFederate instance. Select **Applications**-> **SP Connections**.



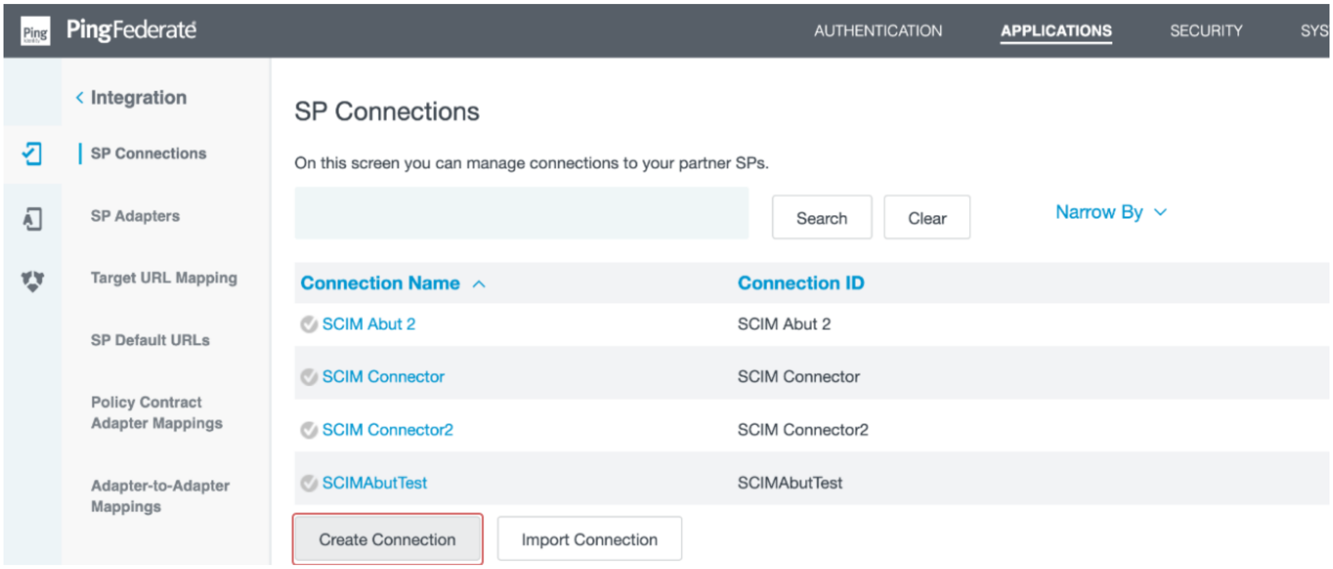
SP Connections
Connect to partner service providers.

SP Adapters
Integrate authentication sessions into target applications.

OAuth Clients
Connect with OAuth and OpenID Connect applications.

Access Token Management
Define the properties of OAuth access tokens generated

2. Select **Create Connection**.



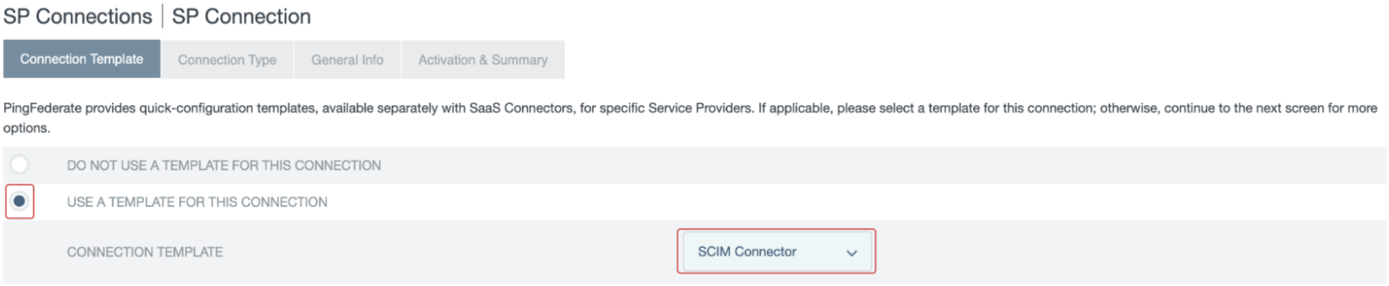
SP Connections

On this screen you can manage connections to your partner SPs.

Connection Name	Connection ID
SCIM Abut 2	SCIM Abut 2
SCIM Connector	SCIM Connector
SCIM Connector2	SCIM Connector2
SCIMAbutTest	SCIMAbutTest

3. On the **Connection Template** step, select **Use a Template for this Connection**. From the dropdown list, select **SCIM Connector** and click **Next**.

   Note: If you do not see the **SCIM Connector** option, please refer to the prerequisite section.



SP Connections | SP Connection

PingFederate provides quick-configuration templates, available separately with SaaS Connectors, for specific Service Providers. If applicable, please select a template for this connection; otherwise, continue to the next screen for more options.

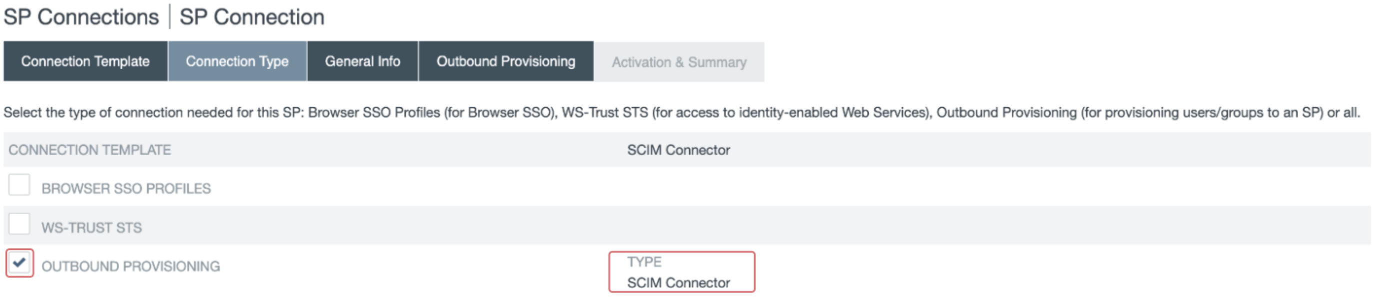
○ DO NOT USE A TEMPLATE FOR THIS CONNECTION

● USE A TEMPLATE FOR THIS CONNECTION

CONNECTION TEMPLATE: SCIM Connector

4. On the **Connection Type** step, ensure that:
   - **Outbound Provisioning** is selected.
   - The **Type** is set to **SCIM Connector**

   Click **Next**.



SP Connections | SP Connection

Select the type of connection needed for this SP: Browser SSO Profiles (for Browser SSO), WS-Trust STS (for access to identity-enabled Web Services), Outbound Provisioning (for provisioning users/groups to an SP) or all.

CONNECTION TEMPLATE: SCIM Connector

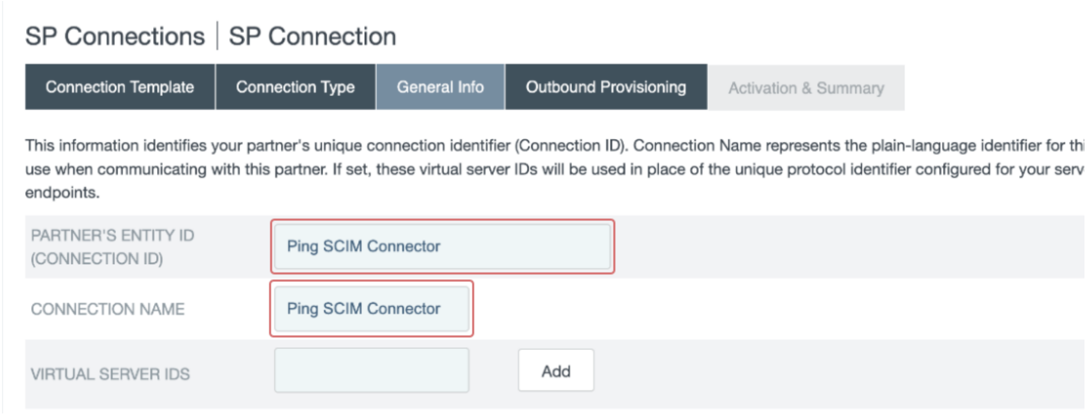
□ BROWSER SSO PROFILES

□ WS-TRUST STS

☑ OUTBOUND PROVISIONING — TYPE: SCIM Connector

5. On the **General Info** step, provide a descriptive name for the following:
   - Partner's Entity ID
   - Connection Name

   Click **Next**.



SP Connections | SP Connection

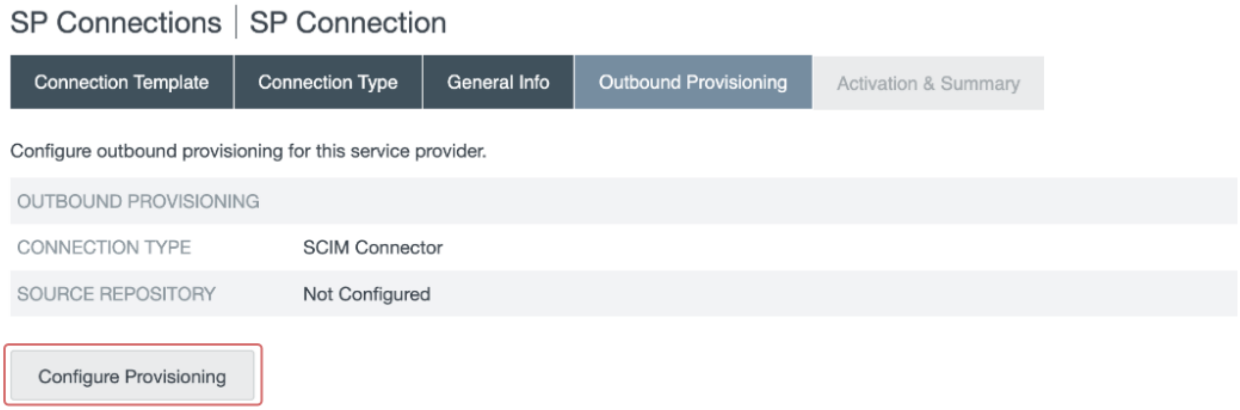
This information identifies your partner's unique connection identifier (Connection ID). Connection Name represents the plain-language identifier for thi use when communicating with this partner. If set, these virtual server IDs will be used in place of the unique protocol identifier configured for your serv endpoints.

PARTNER'S ENTITY ID (CONNECTION ID): Ping SCIM Connector

CONNECTION NAME: Ping SCIM Connector

VIRTUAL SERVER IDS:

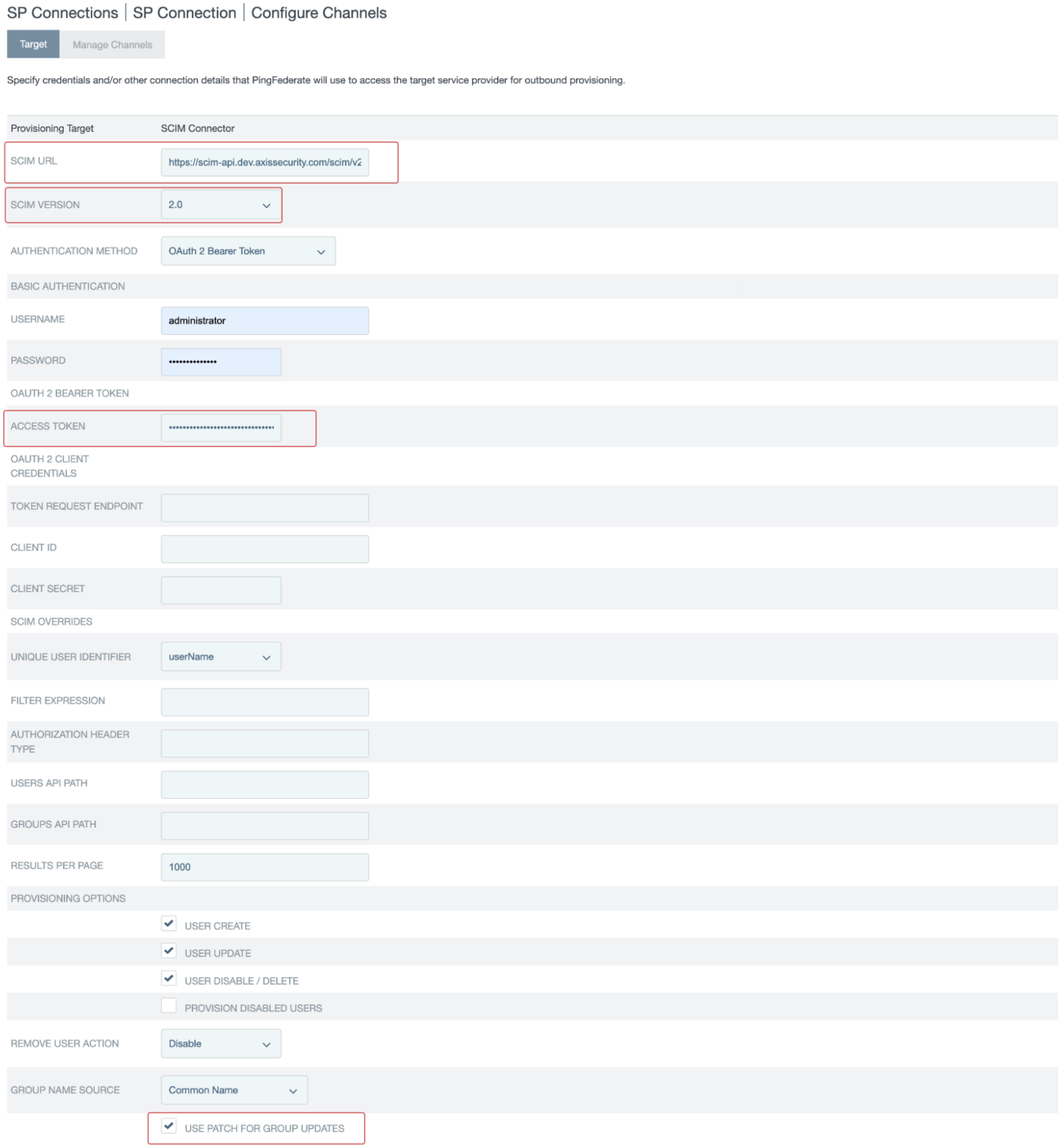
6. On the **Outbound Provisioning** step, select the **Configure Provisioning** button.



Configure outbound provisioning for this service provider.

OUTBOUND PROVISIONING	
CONNECTION TYPE	SCIM Connector
SOURCE REPOSITORY	Not Configured

7. Under the **Target** tab, we will leverage the User Auto-Provisioning (SCIM) values obtained in Step 1:
    - Paste the **SCIM Service Provider Endpoint** in the **SCIM URL** field.
    - Paste the **SCIM Provisioning Token** in the **Access Token** field.
    - Ensure the **SCIM Version** is set as **2.0** and the **Authentication Method** is set as **OAuth 2 Bearer Token**.
    - Check **USE PATCH FOR GROUP UPDATES**.
    - Click **Next**

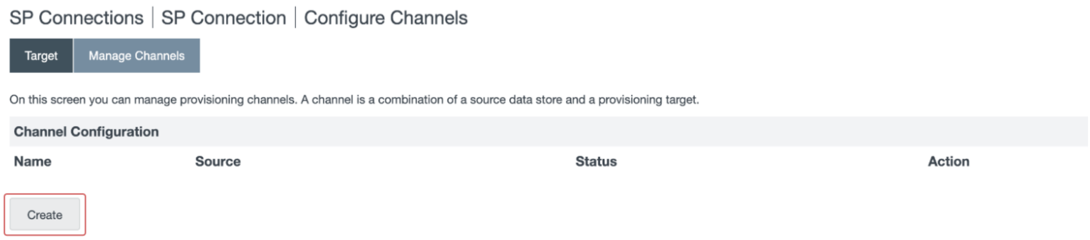


SP Connections | SP Connection | Configure Channels

Specify credentials and/or other connection details that PingFederate will use to access the target service provider for outbound provisioning.

Provisioning Target	SCIM Connector
SCIM URL	https://scim-api.dev.axissecurity.com/scim/v2
SCIM VERSION	2.0
AUTHENTICATION METHOD	OAuth 2 Bearer Token
BASIC AUTHENTICATION	
USERNAME	administrator
PASSWORD	••••••••••••••
OAUTH 2 BEARER TOKEN	
ACCESS TOKEN	••••••••••••••••••••••••••••••••
OAUTH 2 CLIENT CREDENTIALS	
TOKEN REQUEST ENDPOINT	
CLIENT ID	
CLIENT SECRET	
SCIM OVERRIDES	
UNIQUE USER IDENTIFIER	userName
FILTER EXPRESSION	
AUTHORIZATION HEADER TYPE	
USERS API PATH	
GROUPS API PATH	
RESULTS PER PAGE	1000
PROVISIONING OPTIONS	
	☑ USER CREATE
	☑ USER UPDATE
	☑ USER DISABLE / DELETE
	☐ PROVISION DISABLED USERS
REMOVE USER ACTION	Disable
GROUP NAME SOURCE	Common Name
	☑ USE PATCH FOR GROUP UPDATES

8. Go to the **Manage Channels** table and select **Create**.



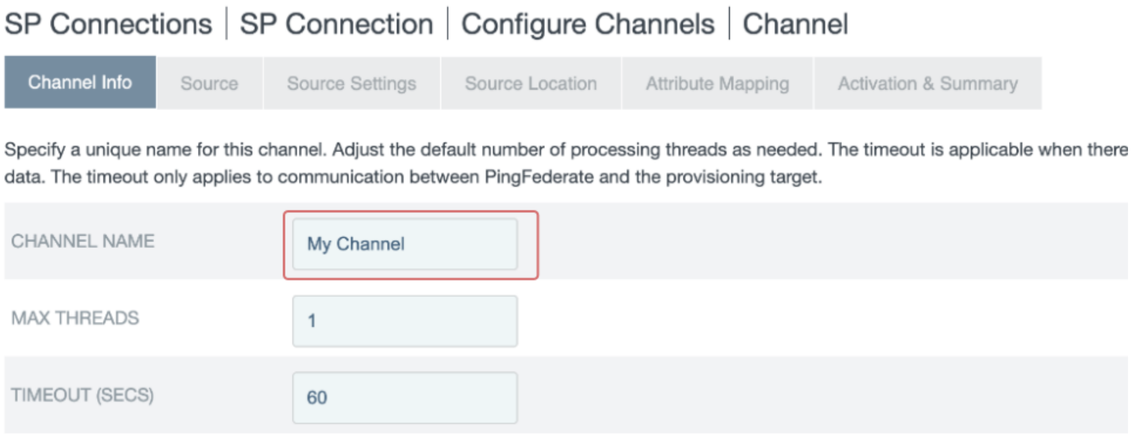
SP Connections | SP Connection | Configure Channels

On this screen you can manage provisioning channels. A channel is a combination of a source data store and a provisioning target.

Channel Configuration

Name	Source	Status	Action

9. In the **Channel Info** step, add a descriptive name and click **Next**.



SP Connections | SP Connection | Configure Channels | Channel

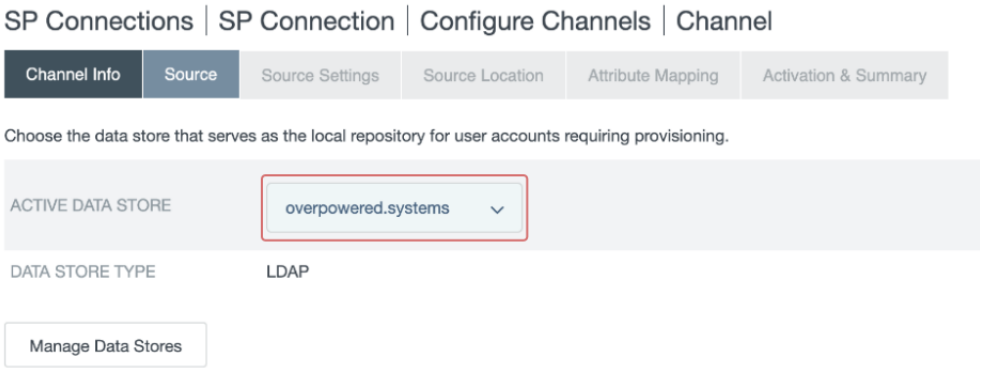
Specify a unique name for this channel. Adjust the default number of processing threads as needed. The timeout is applicable when there data. The timeout only applies to communication between PingFederate and the provisioning target.

CHANNEL NAME	My Channel
MAX THREADS	1
TIMEOUT (SECS)	60

10. Select an **Active Data Store** from the dropdown menu. The selected datastore is where the identity and group information will be synced from.

    Note: The data store must be enabled for provisioning and single sign-on, as described in the **Prerequisites**.

    Click **Next**.



SP Connections | SP Connection | Configure Channels | Channel

Choose the data store that serves as the local repository for user accounts requiring provisioning.

ACTIVE DATA STORE	overpowered.systems
DATA STORE TYPE	LDAP

11. In the **Source Settings** step, keep the default values. Click **Next**.
12. In the **Source Location** step, select the location of the users/groups you want to sync from your active data store.

    Note that the setup may vary depending on the datastore type. The example below is based on an LDAP datastore. For further information, refer to the [PingFederate documentation](#).

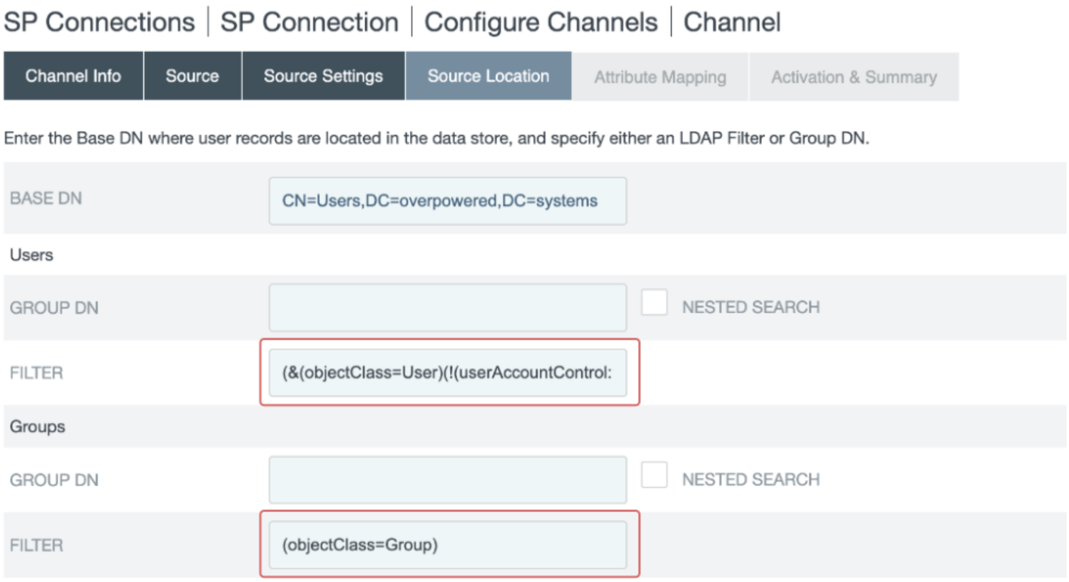
    - Set a **Base DN**
    - Set either a **Group DN** or **Filter** for the **Users** and for the **Groups**. The following values are recommended:

Users	
GROUP DN	(empty)
FILTER	(&(objectClass=User)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))

Note: The following expression **MUST** be included in the **Users FILTER**: !(userAccountControl:1.2.840.113556.1.4.803:=2)

Groups	
GROUP DN	(empty)
FILTER	(objectClass=Group)

- Click **Next**.



Enter the Base DN where user records are located in the data store, and specify either an LDAP Filter or Group DN.

BASE DN: CN=Users,DC=overpowered,DC=systems

Users

GROUP DN: □ NESTED SEARCH

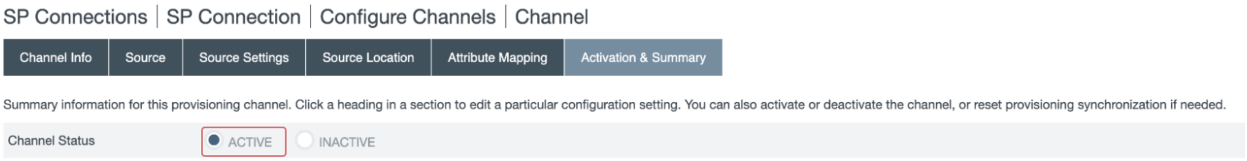
FILTER: (&(objectClass=User)(!(userAccountControl:

Groups

GROUP DN: □ NESTED SEARCH

FILTER: (objectClass=Group)

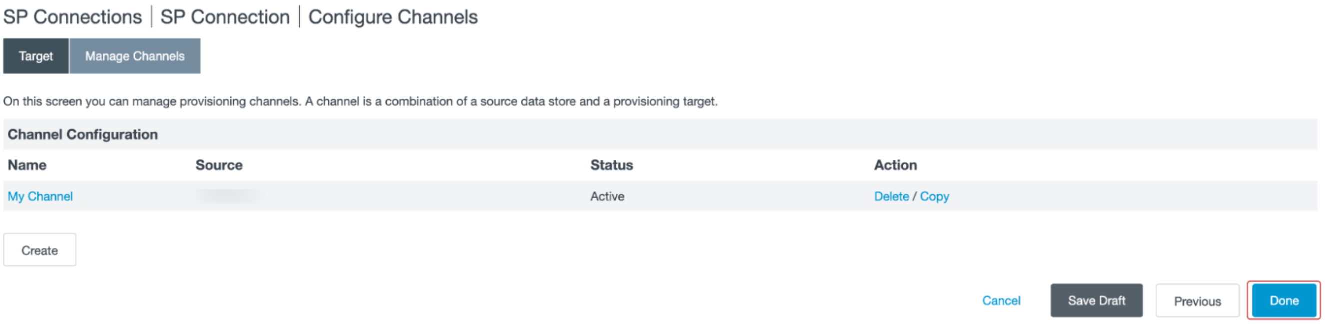
13. In the **Attribute Mapping** step, keep the default settings, and click **Next**.
14. In the **Activation & Summary** step, review the configured settings. Set the **Channel Status** as **Active,** and click **Done**.



Summary information for this provisioning channel. Click a heading in a section to edit a particular configuration setting. You can also activate or deactivate the channel, or reset provisioning synchronization if needed.

Channel Status ● ACTIVE ○ INACTIVE

15. You will be redirected to the **Manage Channels** page. Click **Done**.

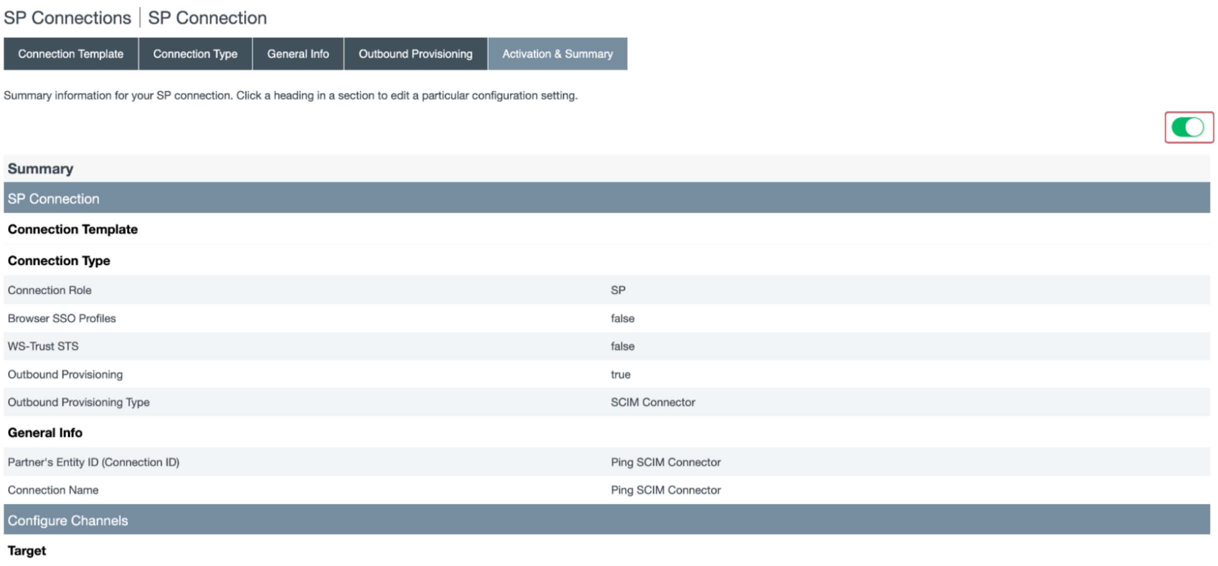


On this screen you can manage provisioning channels. A channel is a combination of a source data store and a provisioning target.

Channel Configuration

Name	Source	Status	Action
My Channel	[redacted]	Active	Delete / Copy

16. You will be redirected to the **Outbound Provisioning** step. Click **Next**.
17. On the **Activation & Summary** step, activate the SP Connection in PingFederate by toggling the connection status. Click **Save**.



Summary information for your SP connection. Click a heading in a section to edit a particular configuration setting.

Summary	
SP Connection	
Connection Template	
Connection Type	
Connection Role	SP
Browser SSO Profiles	false
WS-Trust STS	false
Outbound Provisioning	true
Outbound Provisioning Type	SCIM Connector
General Info	
Partner's Entity ID (Connection ID)	Ping SCIM Connector
Connection Name	Ping SCIM Connector
Configure Channels	
Target	

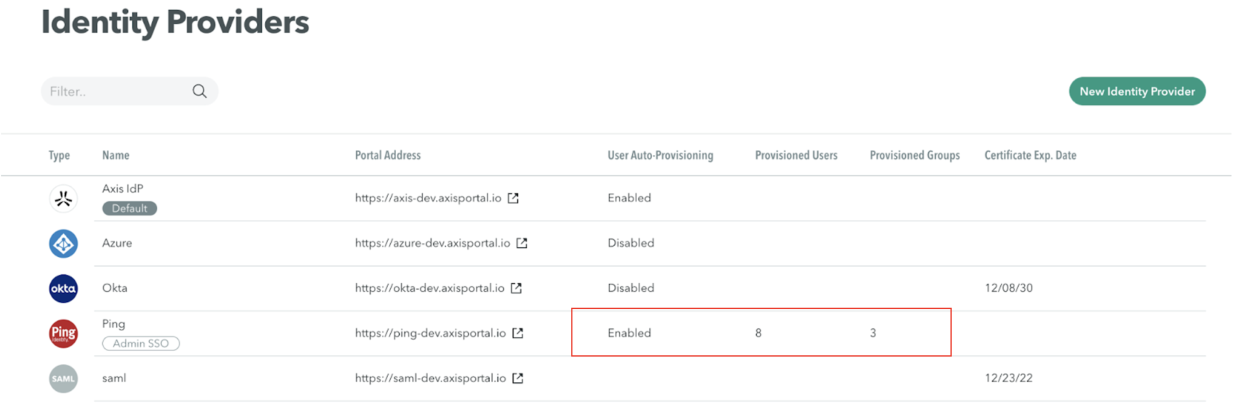
18. Upon successful completion, the SCIM connector will be listed in the SP Connections page

3 Verifying the SCIM Provisioning Integration

Provisioning will begin shortly after the SP connection has been activated. Note that the provisioning process can take several minutes to complete.

Log into the Axis Management console and follow the steps below to verify if the SCIM integration working:

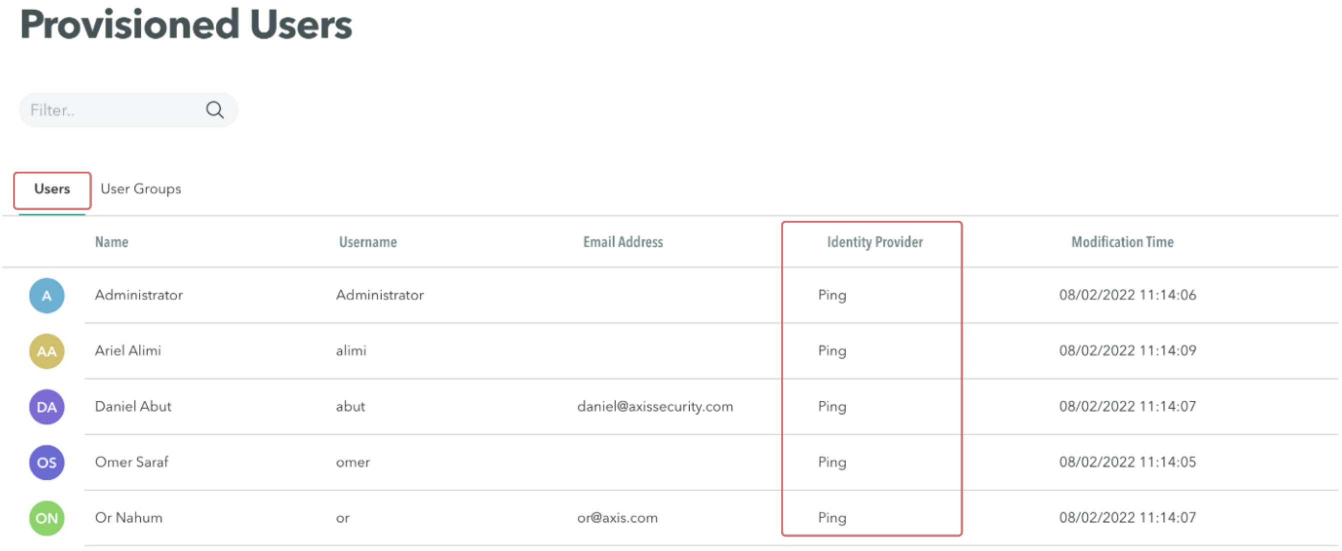
- Go to **Settings**-> **Identity Providers**. In the **Identity Providers** table, the configured PingFederate IdP will now show the number of synchronized users and groups



Identity Providers

Type	Name	Portal Address	User Auto-Provisioning	Provisioned Users	Provisioned Groups	Certificate Exp. Date
	Axis IdP Default	https://axis-dev.axisportal.io	Enabled			
	Azure	https://azure-dev.axisportal.io	Disabled			
okta	Okta	https://okta-dev.axisportal.io	Disabled			12/08/30
Ping	Ping Admin SSO	https://ping-dev.axisportal.io	Enabled	8	3	
SAML	saml	https://saml-dev.axisportal.io				12/23/22

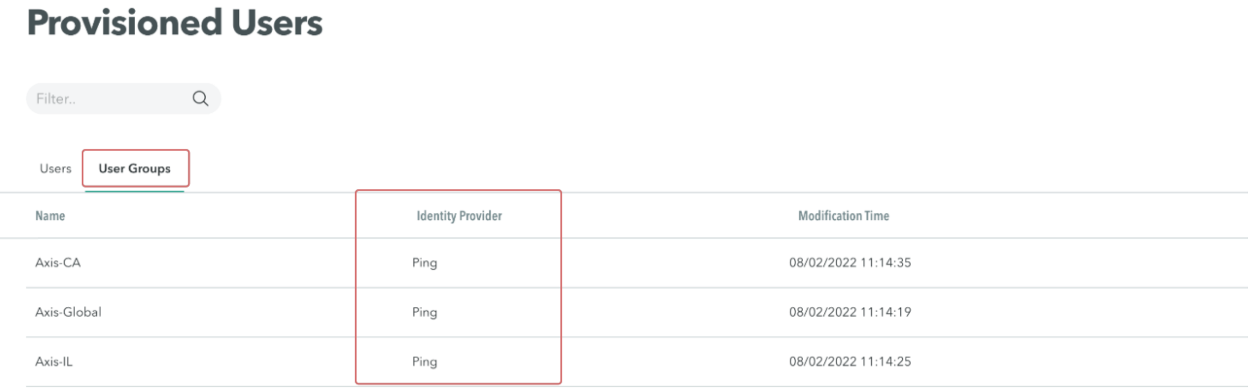
- Go to **Settings** -> **Provisioned Users**. On the **Users** tab, verify that the configured users have been synced from your PingFederate Identity Provider.



Provisioned Users

	Name	Username	Email Address	Identity Provider	Modification Time
A	Administrator	Administrator		Ping	08/02/2022 11:14:06
AA	Ariel Alimi	alimi		Ping	08/02/2022 11:14:09
DA	Daniel Abut	abut	daniel@axissecurity.com	Ping	08/02/2022 11:14:07
OS	Omer Saraf	omer		Ping	08/02/2022 11:14:05
ON	Or Nahum	or	or@axis.com	Ping	08/02/2022 11:14:07

- Select the **User Groups** tab. Verify the configured groups have been synced from your PingFederate Identity Provider.



Provisioned Users

Name	Identity Provider	Modification Time
Axis-CA	Ping	08/02/2022 11:14:35
Axis-Global	Ping	08/02/2022 11:14:19
Axis-IL	Ping	08/02/2022 11:14:25