



# BeyondTrust

## **Privilege Management for Unix & Linux SailPoint IdentityNow Integration**

## Table of Contents

---

<b>IdentityNow Connector for PMUL (BIUL)</b> .....	<b>3</b>
Prerequisites .....	3
Introduction .....	3
<b>Configuration</b> .....	<b>4</b>
Create Web Services or Connector .....	4
Base Configuration .....	5
Connection Settings .....	5
HTTP Operations .....	6
Test the Connection .....	29
Add a Correlation Rule .....	29
Create Account and Provisioning Policy .....	29
Aggregate Accounts and Entitlements .....	31
Access Profiles .....	32

# IdentityNow Connector for PMUL (BIUL)

This guide covers the steps to configure the IdentityNow Connector for PMUL (BIUL).

## Prerequisites

- IdentityNow instance
- Privilege Management for Unix and Linux (PMUL)
- BeyondInsight for Unix & Linux (BIUL) 23.1

## Use Cases

- Joiner, Mover, and Leaver (JML)
- Access Request
- Access Governance

## Introduction

BeyondInsight for Unix & Linux (BIUL) is a web-based tool that you use to:

- Manage software for AD Bridge and Privilege Management for Unix and Linux.
- Remotely assess the suitability of a remote host's state by running a profile. After a profile is complete, installs, uninstalls, domain joins, and other actions can be performed on remote hosts.
- Manage Privilege Management for Unix and Linux licenses on policy servers.
- Manage Privilege Management for Unix and Linux script, File Integrity Monitoring (FIM), and role-based policies.
- Manage Sudo host groups and FIM policy host assignment.
- View, replay, and audit Privilege Management for Unix and Linux logs.

Organizations using SailPoint IdentityNow can leverage this configuration guide to configure a Source or Connector to BeyondInsight for Unix & Linux, using the Web Services generic Source template. Supported use cases include:

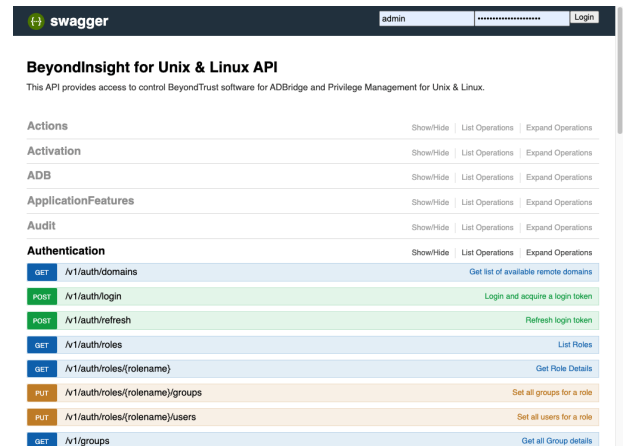
- [Account Aggregation or Discovery](#)
- [Role Aggregation](#)
- [Create Account](#)
- [Enable Account](#)
- [Disable Account](#)
- [Update Password](#)
- [Unlock Account](#)
- [Delete Account](#)
- [Add Role to User](#)
- [Remove Role from User](#)

You can use the Source for Provisioning, Access Request, Access Certification, Reporting, etc.

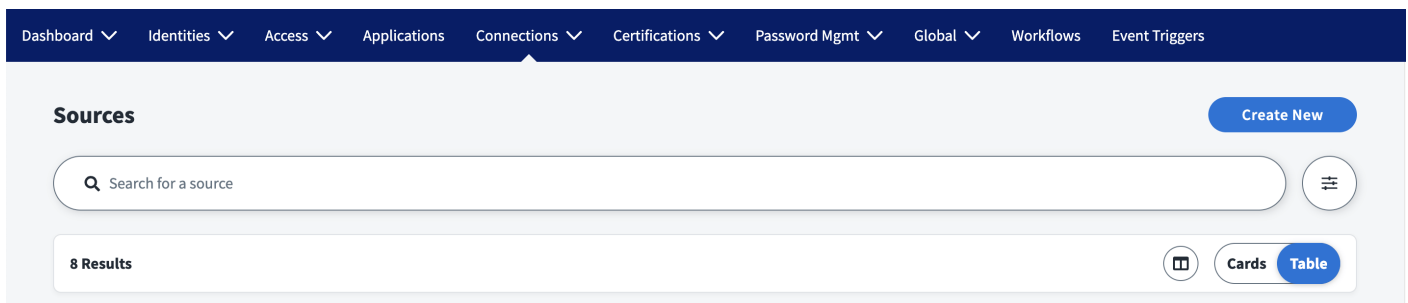
## Configuration



**Note:** A preconfigured Swagger UI /**swagger** is available as part of BeyondInsight for Unix & Linux BIUL, which can be used to test API access.

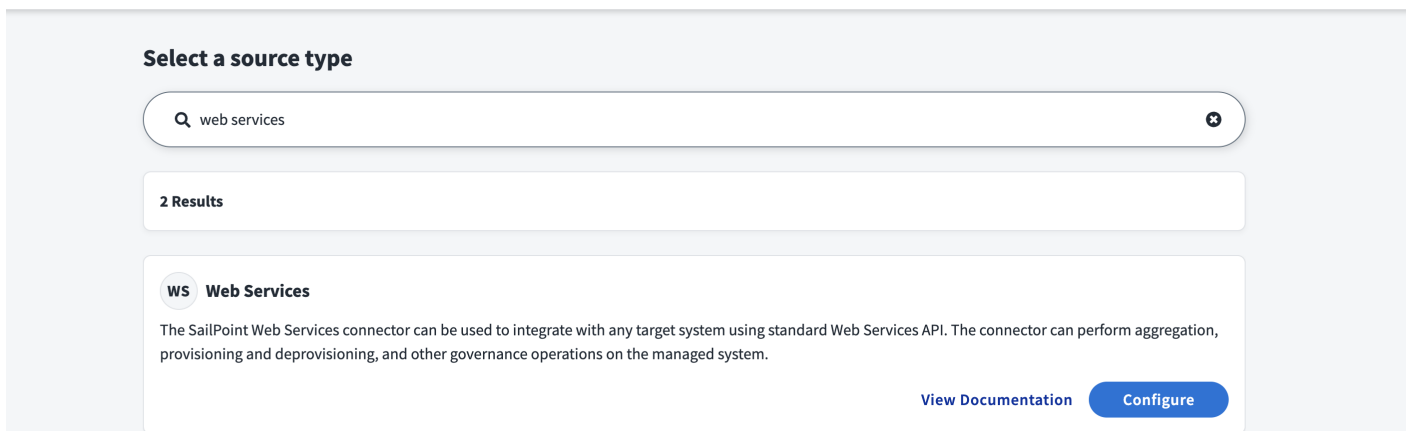


To start the configuration process, in IdentityNow, connect as **admin**, navigate to **Connections > Sources**, and then click **Create New**.



## Create Web Services or Connector

### Create Source: Select Source Type



For source type, select **Web Services**, and then click **Configure**.

## Base Configuration

On the left side menu, select **Base Configuration**.

### BeyondInsight Unix and Linux: Web Services

Direct Connection

**Base Configuration**  
Connection Settings  
HTTP Operations  
Additional Settings  
Review and Test

#### Base Configuration

The Web Services source is a type of 'Direct Connection' source used to communicate between a source server and SailPoint. To configure a Direct Connection source, provide or select values for all required fields, including a source owner and virtual appliance cluster.

The source owner is responsible for administering, operating, and managing the source system. The virtual appliance (VA) is a Linux-based virtual machine that is deployed and configured to connect to sources and apps using APIs, connectors / integrations provided by SailPoint.

(Optional) Select a governance group to specify the Source Sub-Admin users who can manage this source.

[Learn more about governance groups](#)

**Source Name \***

BU

**Source Description \***

**Source Owner \***

**Virtual Appliance Cluster \***


**Governance Group for Source Management**

Complete the **Source Name**, **Description**, **Source Owner**, and **Virtual Appliance Cluster** fields, and then click **Save**.

## Connection Settings

For the connection settings, you must provide the BIUL API URL, as well as username and password for a BIUL service account with two roles: *accountadmin* and *apiuser*.

Collect the information (see right) from the **BIUL > Console Access > Edit User Roles** page.

BeyondInsight  


Unix & Linux  
Settings > Console Access > Edit User Roles

**USER: SVC\_IDN**

IdentityNow, Service Account (svc\_idn@)

User has 2 roles

Active

User Details  
Details  
Roles  
Authentication

**User Roles**

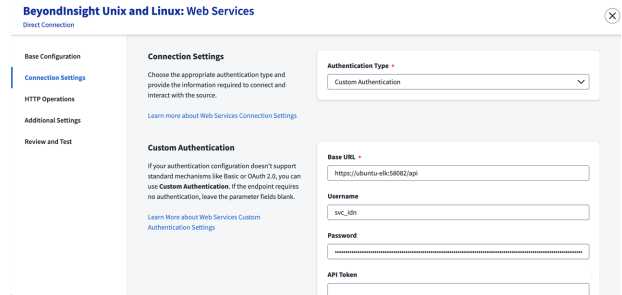
Roles configured here will be in addition to any roles that this user may inherit through membership in groups.

Note that the **System Administrator** role allows for all actions within **BeyondInsight for Unix & Linux** regardless of what other roles are enabled for the user.

- ☒ **apiuser**
- ☒ **auditor**
- ☒ **Account Administrator**
- ☐ **Policy Administrator**
- ☐ **Software Administrator**

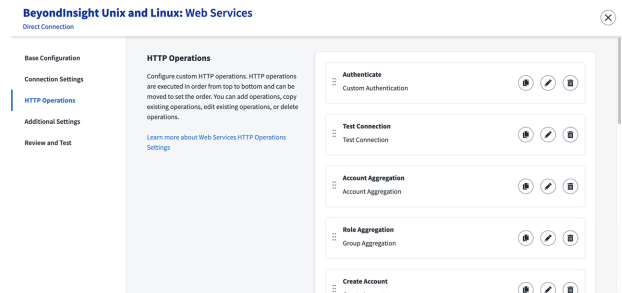
To set the connection settings:

1. On the left side menu, select **Connection Settings**.
2. Ensure that **Custom Authentication** type is selected, and then complete the **Base URL**, **Username**, and **Password** fields.
3. Click **Save**.



## HTTP Operations

Once you have created the Web Services Source or Connector, you must create each individual HTTP Operation.



On the left side menu, select **HTTP Operations**.

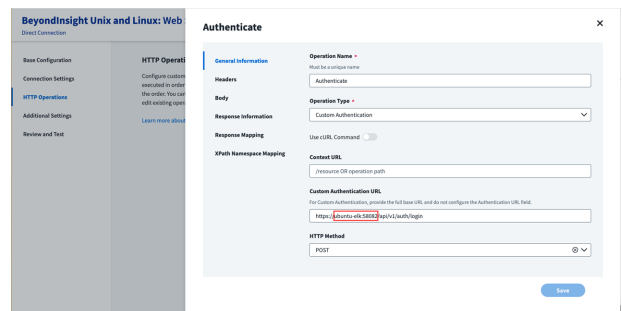
## Authenticate (Custom Authentication)

On the **HTTP Operations** panel, click **Add Operation** and set the **Operation Type** to **Custom Authentication**.

## General Information

To set the **Authenticate** information:

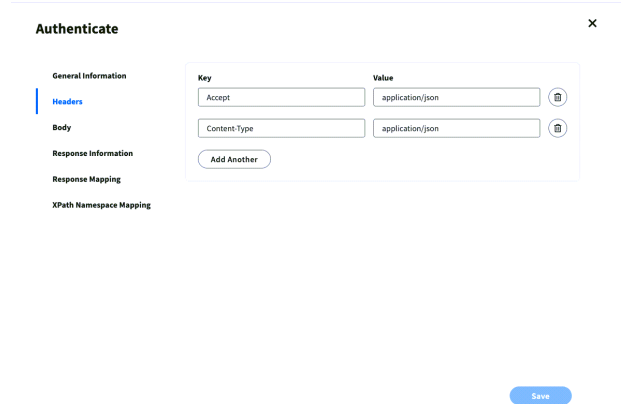
1. On the **Authenticate** panel, ensure that **General Information** is selected.
2. Enter a unique **Operation Name**.
3. Ensure the **Operation Type** is set to **Custom Authentication**.
4. Enter the **Context URL**.
5. Replace the BIUL instance **https://ubuntu-elk:58082** with the actual BIUL server URL you want to configure the connector for.
6. Ensure the **HTTP Method** is set to **POST**.
7. Click **Save**.



## Headers

To set the **Headers** information:

1. On the **Authenticate** panel, select **Headers**.
2. Complete the **Key** and **Value** fields.
3. To add additional key and value information, click **Add Another**.
4. When done, click **Save**.

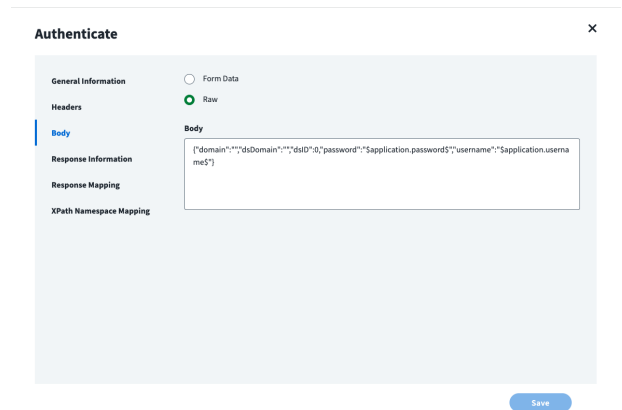


The screenshot shows the 'Authenticate' panel with the 'Headers' tab selected. On the left, a sidebar lists 'General Information', 'Headers', 'Body', 'Response Information', 'Response Mapping', and 'XPath Namespace Mapping'. The 'Headers' section contains a table with two columns: 'Key' and 'Value'. The first row has 'Accept' in the Key field and 'application/json' in the Value field. The second row has 'Content-Type' in the Key field and 'application/json' in the Value field. Below the table is an 'Add Another' button. At the bottom right of the panel is a 'Save' button.

## Body

To set the **Body** information:

1. On the **Authenticate** panel, select **Body**.
2. Select **Raw**.
3. Complete the **Body** information by entering the text as written below.



The screenshot shows the 'Authenticate' panel with the 'Body' tab selected. On the left, the same sidebar as in the Headers section is visible. The 'Body' section has two radio buttons: 'Form Data' (unselected) and 'Raw' (selected). Below the radio buttons is a text area containing the JSON string: `{"domain":"","dsDomain":"","dsID":0,"password":"$application.password$","username":"$application.username$"}` . At the bottom right of the panel is a 'Save' button.

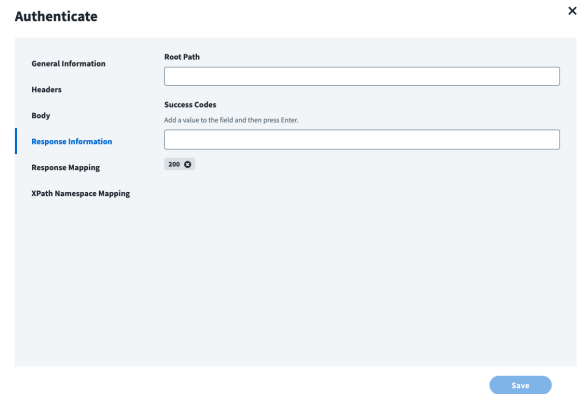
```
{"domain":"","dsDomain":"","dsID":0,"password":"$application.password$","username":"$application.username$"} 
```

4. Click **Save**.

## Response Information

To set the **Response Information**:

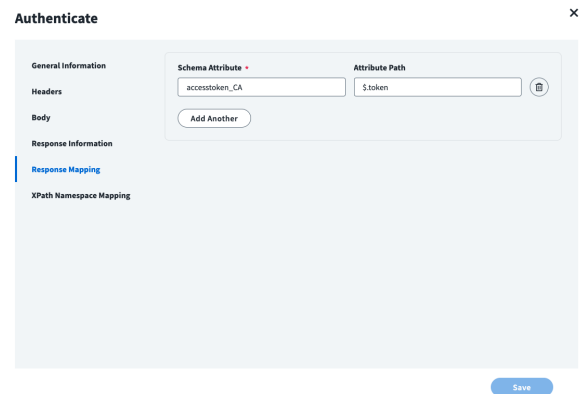
1. On the **Authenticate** panel, select **Response Information**.
2. Set the **Root Path** and **Success Codes**.
3. Click **Save**.



## Response Mapping

To set the **Response Mapping** information:

1. On the **Authenticate** panel, select **Response Mapping**.
2. Save the token included in the response into a **\_CA** variable for encrypted values.
3. Click **Save**.



## Test Connection

Here we arbitrarily decided to use Account Aggregation within the Test Connection.

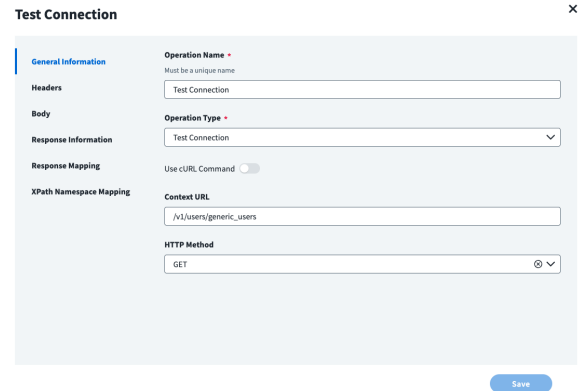
On the **HTTP Operations** panel, click **Add Operation** and set the **Operation Type** to **Test Connection**.



## General information

To set the **Test Connection** information:

1. On the **Test Connection** panel, ensure that **General Information** is selected.
2. Enter a unique **Operation Name**.
3. Ensure the **Operation Type** is set to **Test Connection**.
4. Enter the **Context URL**.
5. Ensure the **HTTP Method** is set to **GET**.
6. Click **Save**.



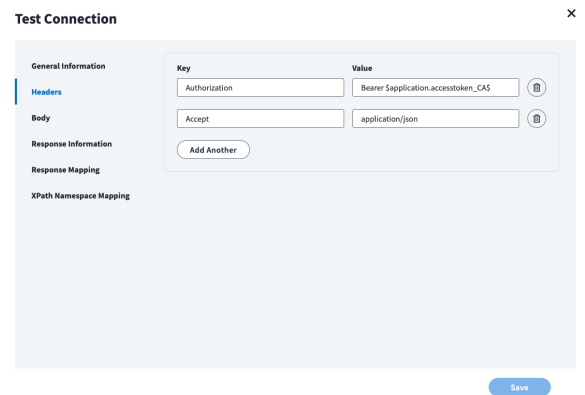
The screenshot shows the 'Test Connection' panel with the 'General Information' tab selected. The 'Operation Name' field contains 'Test Connection'. The 'Operation Type' dropdown is set to 'Test Connection'. The 'Context URL' field contains '/v1/users/generic\_users'. The 'HTTP Method' dropdown is set to 'GET'. A 'Save' button is at the bottom right.

## Headers

**Headers** must include the Access Token generated by Custom Authentication. All HTTP Operations will need the Authorization Header with the token value.

To set the **Headers** information:

1. On the **Test Connection** panel, select **Headers**.
2. Complete the **Key** and **Value** fields.
3. To add additional key and value information, click **Add Another**.
4. When done, click **Save**.

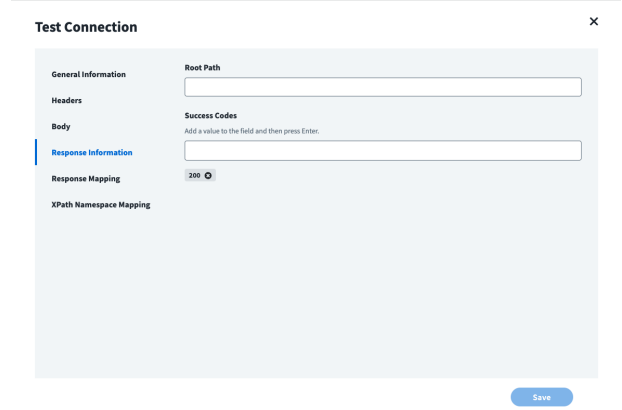


The screenshot shows the 'Test Connection' panel with the 'Headers' tab selected. There are two header entries: 'Authorization' with value 'Bearer Application.accesstoken\_CAS' and 'Accept' with value 'application/json'. An 'Add Another' button is below the entries. A 'Save' button is at the bottom right.

## Response Information

To set the **Response Information**:

1. On the **Test Connection** panel, select **Response Information**.
2. Set the **Root Path** and **Success Codes**.
3. Click **Save**.



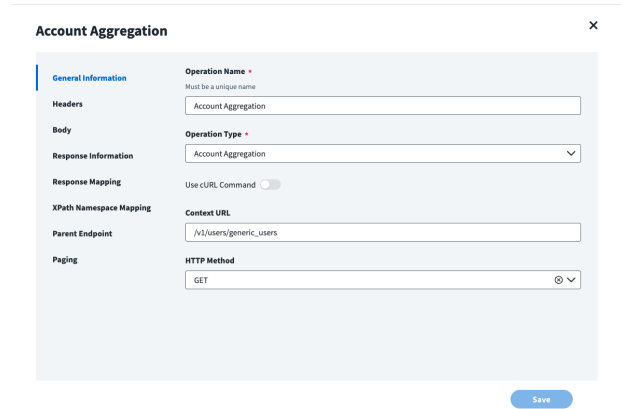
The screenshot shows the 'Test Connection' window with the 'Response Information' tab selected. The 'Root Path' field is empty. The 'Success Codes' section has a text input field with the placeholder 'Add a value to the field and then press Enter'. The 'Response Mapping' section shows a status of '200' with a circular icon. The 'XPath Namespace Mapping' section is empty. A 'Save' button is at the bottom right.

## Account Aggregation

### General information

To set the **Account Aggregation** information:

1. On the **Account Aggregation** panel, ensure that **General Information** is selected.
2. Enter a unique **Operation Name**.
3. Ensure the **Operation Type** is set to **Account Aggregation**.
4. Enter the **Context URL**.
5. Ensure the **HTTP Method** is set to **GET**.
6. Click **Save**.

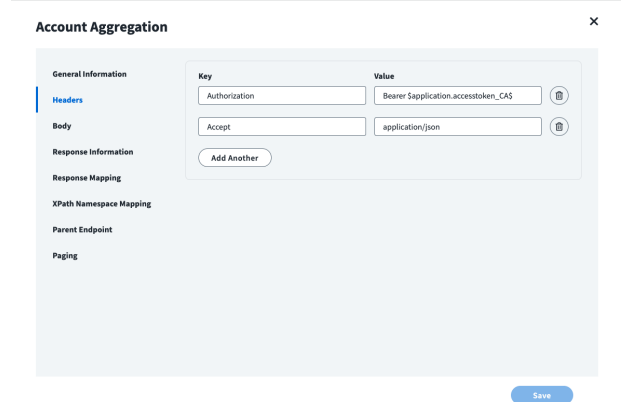


The screenshot shows the 'Account Aggregation' window with the 'General Information' tab selected. The 'Operation Name' field contains 'Account Aggregation' with a note 'Must be a unique name'. The 'Operation Type' dropdown is set to 'Account Aggregation'. The 'Context URL' field contains '/v1/users/generic\_users'. The 'HTTP Method' dropdown is set to 'GET'. A 'Save' button is at the bottom right.

## Headers

To set the **Headers** information:

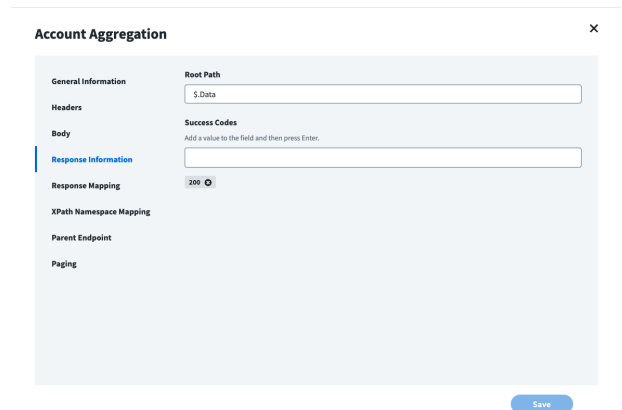
1. On the **Account Aggregation** panel, select **Headers**.
2. Complete the **Key** and **Value** fields.
3. To add additional key and value information, click **Add Another**.
4. When done, click **Save**.



## Response Information

To set the **Response Information**:

1. On the **Account Aggregation** panel, select **Response Information**.
2. Set the **Root Path** and **Success Codes**.
3. Click **Save**.



## Response Mapping

To set the **Response Mapping** information:

1. On the **Account Aggregation** panel, select **Response Mapping**.
2. Set a **Schema Attribute** and the **Attribute Path**.
3. To add additional values, click **Add Another**.
4. When done, click **Save**.

Account Aggregation ×

General Information  
Headers  
Body  
Response Information  
**Response Mapping**  
XPath Namespace Mapping  
Parent Endpoint  
Paging

Schema Attribute	Attribute Path
firstname	firstname
created	created
roles	roles[*].rolename
active	active
admin	admin
cn	cn
requiresGroup	requiresGroup
lastname	lastname
path	path
externalApiID	externalApiID
name	name
guid	guid
remoteUserID	remoteUserID
userType	userType
localUserID	localUserID
updated	updated
email	email
username	username

Add Another

## Role Aggregation

### General information

To set the **Role Aggregation** information:

1. On the **Role Aggregation** panel, ensure that **General Information** is selected.
2. Enter a unique **Operation Name**.
3. Ensure the **Operation Type** is set to **Group Aggregation**.
4. Enter the **Context URL**.
5. Ensure the **HTTP Method** is set to **GET**.
6. Click **Save**.

Role Aggregation ×

General Information  
Headers  
Body  
Response Information  
Response Mapping  
XPath Namespace Mapping  
Parent Endpoint  
Paging

Operation Name

Must be a unique name

Role Aggregation

Operation Type

Group Aggregation

Use cURL Command

Context URL

/v1/auth/roles

HTTP Method

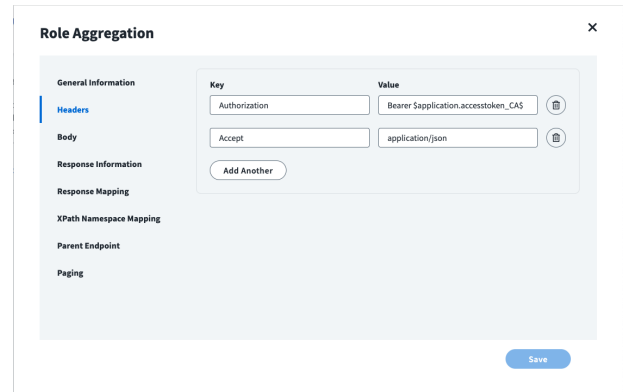
GET

Save

## Headers

To set the **Headers** information:

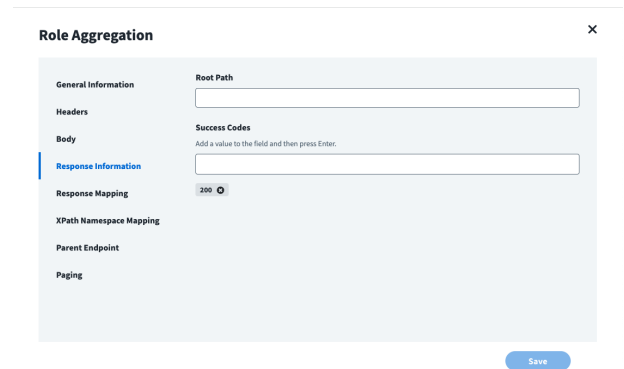
1. On the **Role Aggregation** panel, select **Headers**.
2. Complete the **Key** and **Value** fields.
3. To add additional key and value information, click **Add Another**.
4. When done, click **Save**.



## Response Information

To set the **Response Information**:

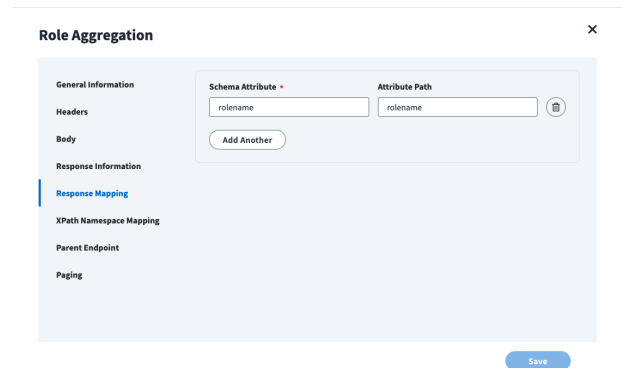
1. On the **Role Aggregation** panel, select **Response Information**.
2. Set the **Root Path** and **Success Codes**.
3. Click **Save**.



## Response Mapping

To set the **Response Mapping** information:

1. On the **Role Aggregation** panel, select **Response Mapping**.
2. Set a **Schema Attribute** and the **Attribute Path**.
3. To add additional values, click **Add Another**.
4. When done, click **Save**.

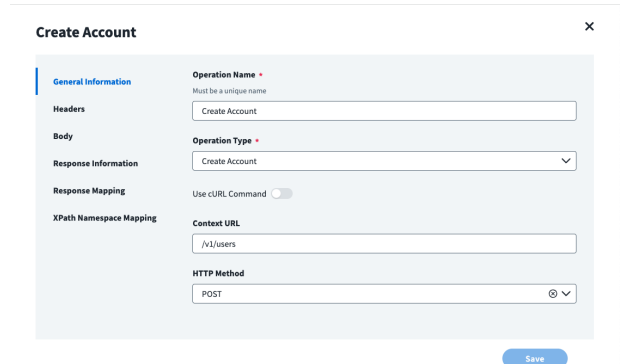


## Create Account

### General information

To set the **Create Account** information:

1. On the **Create Account** panel, ensure that **General Information** is selected.
2. Enter a unique **Operation Name**.
3. Ensure the **Operation Type** is set to **Create Account**.
4. Enter the **Context URL**.
5. Ensure the **HTTP Method** is set to **POST**.
6. Click **Save**.

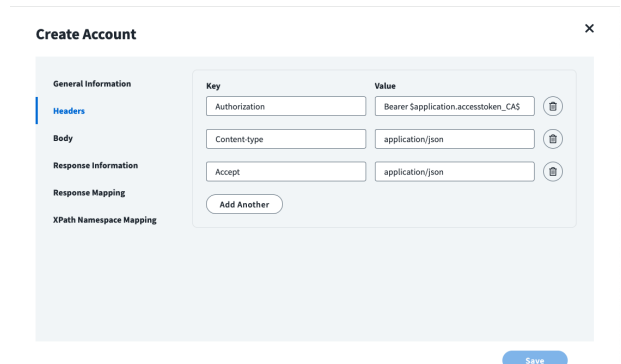


The screenshot shows the 'Create Account' panel with the 'General Information' tab selected. The 'Operation Name' field contains 'Create Account'. The 'Operation Type' dropdown is set to 'Create Account'. The 'Context URL' field contains '/v1/users'. The 'HTTP Method' dropdown is set to 'POST'. A 'Save' button is at the bottom right.

### Headers

To set the **Headers** information:

1. On the **Create Account** panel, select **Headers**.
2. Complete the **Key** and **Value** fields.
3. To add additional key and value information, click **Add Another**.
4. When done, click **Save**.

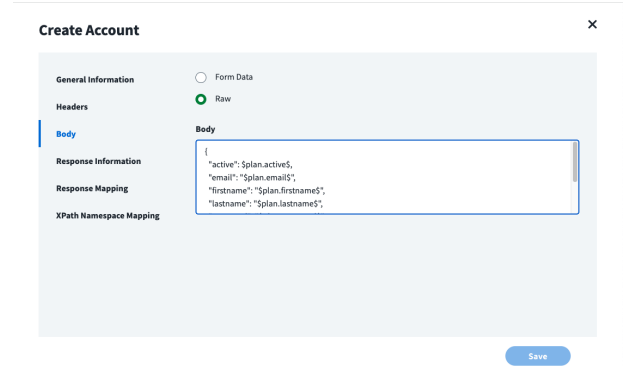


The screenshot shows the 'Create Account' panel with the 'Headers' tab selected. It displays a table with two columns: 'Key' and 'Value'. The first row has 'Authorization' as the key and 'Bearer Sapplication.accesstoken\_CAS' as the value. The second row has 'Content-type' as the key and 'application/json' as the value. The third row has 'Accept' as the key and 'application/json' as the value. There is an 'Add Another' button below the table. A 'Save' button is at the bottom right.

## Body

To set the **Body** information:

1. On the **Create Account** panel, select **Body**.
2. Select **Raw**.
3. Complete the **Body** information by entering the text as written below.



**Create Account** [X]

General Information ☐ Form Data ☒ Raw

Headers

**Body**

Response Information

Response Mapping

XPath Namespace Mapping

Body Content:

```
{
  "active": "$plan.active$",
  "email": "$plan.email$",
  "firstname": "$plan.firstname$",
  "lastname": "$plan.lastname$",
  "password": "$plan.password$",
  "passwordConfirm": "$plan.password$",
  "username": "$plan.username$"
}
```

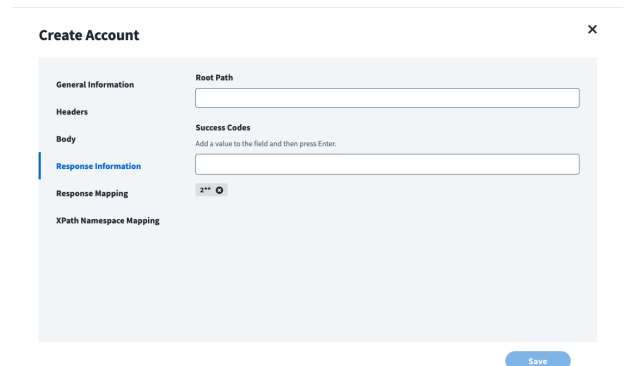
Save

```
{
  "active": "$plan.active$",
  "email": "$plan.email$",
  "firstname": "$plan.firstname$",
  "lastname": "$plan.lastname$",
  "password": "$plan.password$",
  "passwordConfirm": "$plan.password$",
  "username": "$plan.username$"
}
```

## Response Information

To set the **Response Information**:

1. On the **Create Account** panel, select **Response Information**.
2. Set the **Root Path** and **Success Codes**.
3. Click **Save**.



**Create Account** [X]

General Information

Headers

Body

**Response Information**

Response Mapping

XPath Namespace Mapping

Root Path

Success Codes

Add a value to the field and then press Enter.

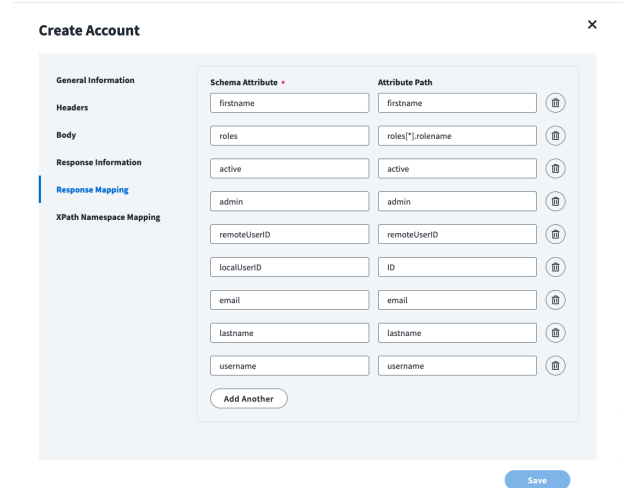
2\*\*

Save

## Response Mapping

To set the **Response Mapping** information:

1. On the **Create Account** panel, select **Response Mapping**.
2. Set a **Schema Attribute** and the **Attribute Path**.
3. To add additional values, click **Add Another**.
4. When done, click **Save**.

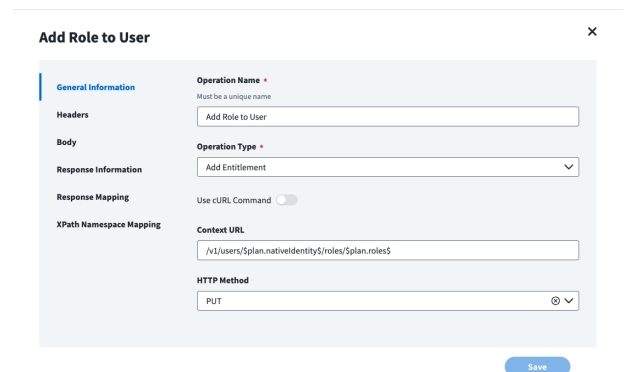


## Add Role to User and Remove Role from User

### General Information

To set the **Add Role to User** information:

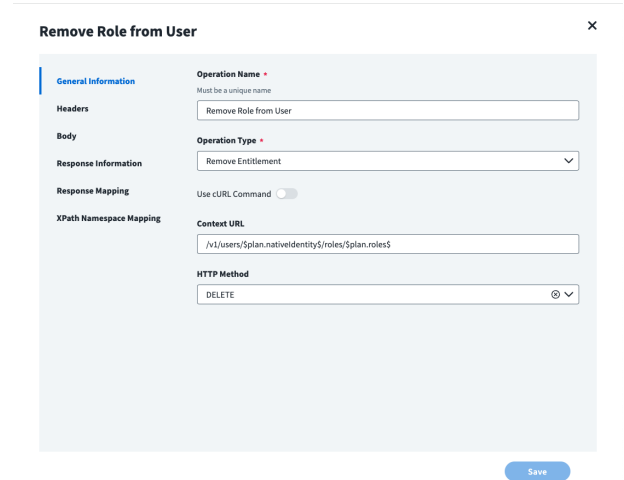
1. On the **Add Role to User** panel, ensure that **General Information** is selected.
2. Enter a unique **Operation Name**, such as **Add Role to User**.
3. Ensure the **Operation Type** is set to **Add Entitlement**.
4. Enter the **Context URL**.
5. Ensure the **HTTP Method** is set to **PUT**.
6. Click **Save**.





To set the **Remove Role from User** information:

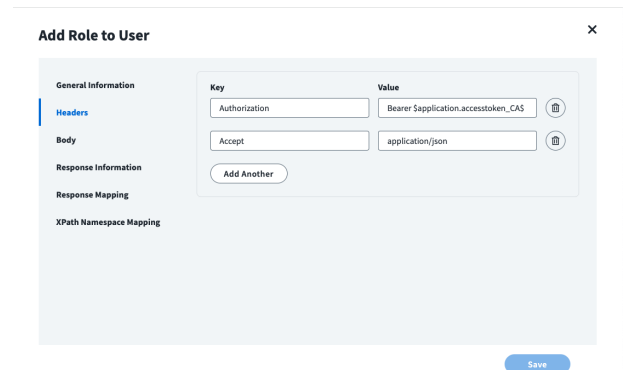
1. On the **Remove Role from User** panel, ensure that **General Information** is selected.
2. Enter a unique **Operation Name**, such as **Remove Role from User**.
3. Ensure the **Operation Type** is set to **Remove Entitlement**.
4. Enter the **Context URL**.
5. Ensure the **HTTP Method** is set to **DELETE**.
6. Click **Save**.



## Headers

To set the **Headers** information:

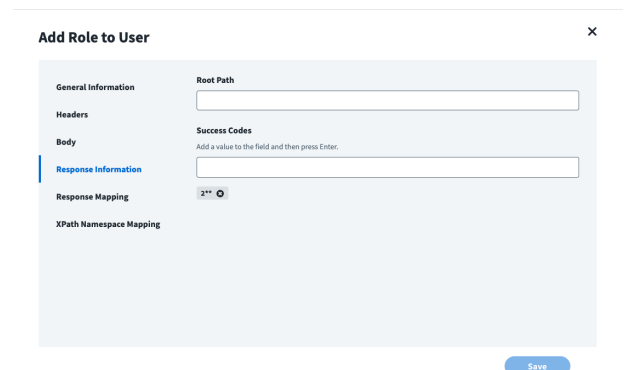
1. On the **Add Role to User** (or **Remove Role from User**) panel, select **Headers**.
2. Complete the **Key** and **Value** fields.
3. To add additional key and value information, click **Add Another**.
4. When done, click **Save**.



## Response Information

To set the **Response Information**:

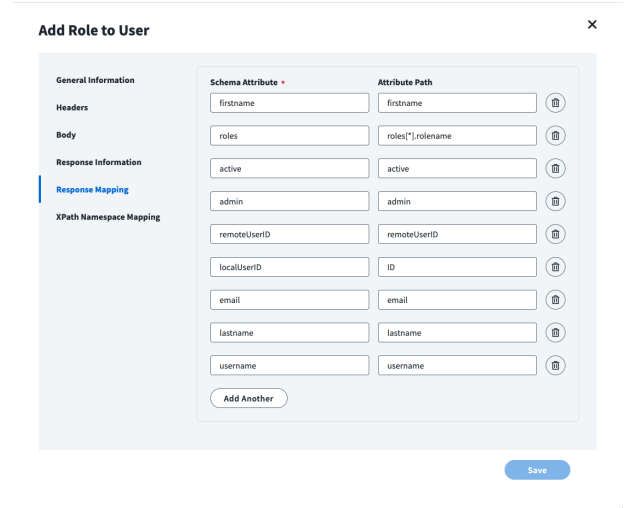
1. On the **Add Role to User** (or **Remove Role from User**) panel, select **Response Information**.
2. Set the **Root Path** and **Success Codes**.
3. Click **Save**.



## Response Mapping

To set the **Response Mapping** information:

1. On the **Add Role to User** (or **Remove Role from User**) panel, select **Response Mapping**.
2. Set a **Schema Attribute** and the **Attribute Path**.
3. To add additional values, click **Add Another**.
4. When done, click **Save**.



## Disable Account and Enable Account

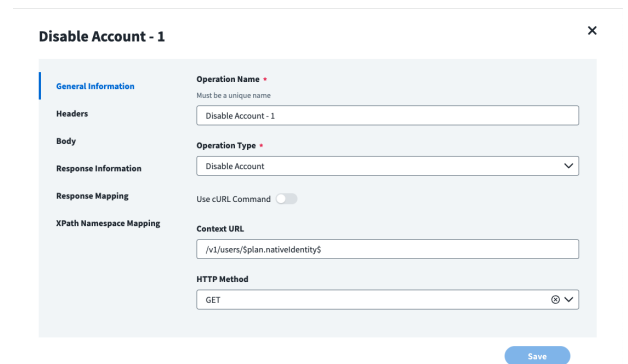
Both HTTP Operations are accomplished in two steps, and only differ in the **General Information** and **Body** page for step 2 (Disable Account – 2 and Enable Account – 2).

## Disable Account -1 and Enable Account -1

### General Information

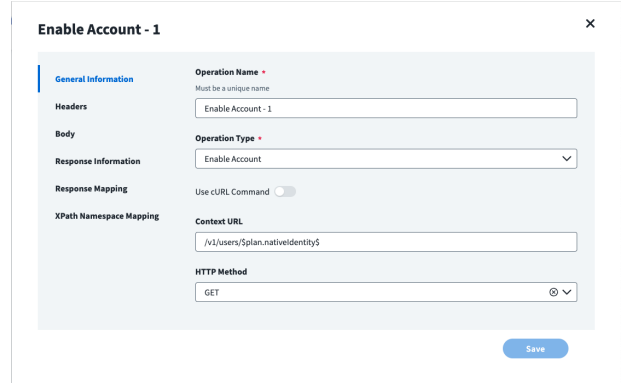
To set the **Disable Account-1** information:

1. On the **Disable Account -1** panel, ensure that **General Information** is selected.
2. Enter a unique **Operation Name**, such as **Disable Account-1**.
3. Ensure the **Operation Type** is set to **Disable Account**.
4. Enter the **Context URL**.
5. Ensure the **HTTP Method** is set to **GET**.
6. Click **Save**.



To set the **Enable Account-1** information:

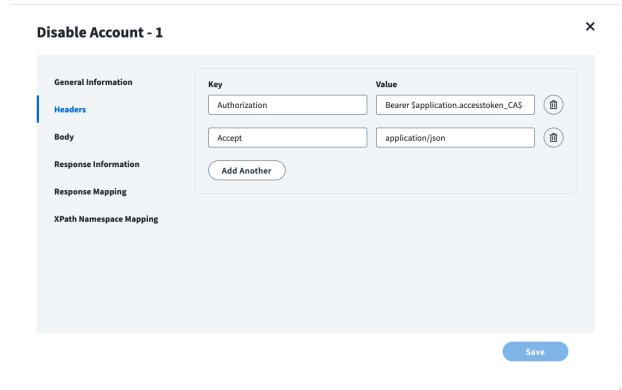
1. On the **Enable Account -1** panel, ensure that **General Information** is selected.
2. Enter a unique **Operation Name**, such as **Enable Account-1**.
3. Ensure the **Operation Type** is set to **Enable Account**.
4. Enter the **Context URL**.
5. Ensure the **HTTP Method** is set to **GET**.
6. Click **Save**.



## Headers

To set the **Headers** information:

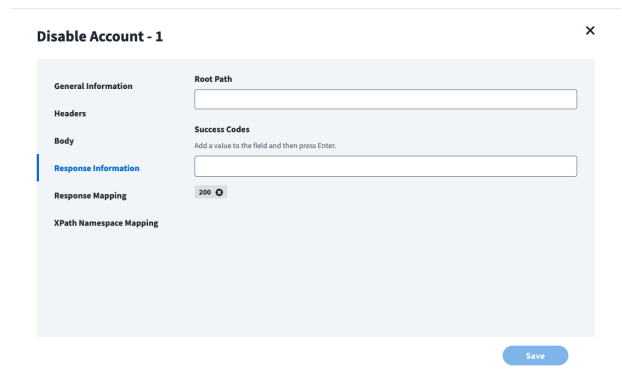
1. On the **Disable Account-1** (or **Enable Account-1**) panel, select **Headers**.
2. Complete the **Key** and **Value** fields.
3. To add additional key and value information, click **Add Another**.
4. When done, click **Save**.



## Response Information

To set the **Response Information**:

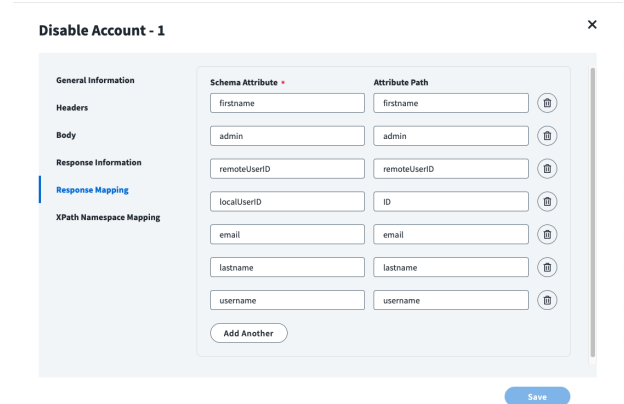
1. On the **Disable Account-1** (or **Enable Account-1**) panel, select **Response Information**.
2. Set the **Root Path** and **Success Codes**.
3. Click **Save**.



## Response Mapping

To set the **Response Mapping** information:

1. On the **Disable Account-1** (or **Enable Account-1**) panel, select **Response Mapping**.
2. Set a **Schema Attribute** and the **Attribute Path**.
3. To add additional values, click **Add Another**.
4. When done, click **Save**.



**Disable Account - 1**

Schema Attribute	Attribute Path	
firstname	firstname	🗑️
admin	admin	🗑️
remoteUserID	remoteUserID	🗑️
localUserID	ID	🗑️
email	email	🗑️
lastname	lastname	🗑️
username	username	🗑️
Add Another		

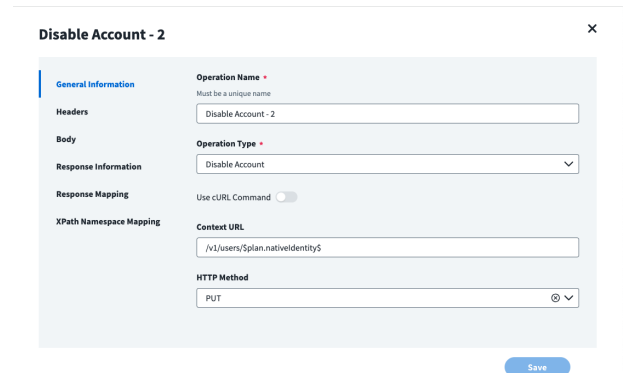
Save

## Disable Account-2 and Enable Account-2

### General Information

To set the **Disable Account-2** information:

1. On the **Disable Account -2** panel, ensure that **General Information** is selected.
2. Enter a unique **Operation Name**, such as **Disable Account-2**.
3. Ensure the **Operation Type** is set to **Disable Account**.
4. Enter the **Context URL**.
5. Ensure the **HTTP Method** is set to **PUT**.
6. Click **Save**.



**Disable Account - 2**

**General Information**

**Operation Name** Must be a unique name  
Disable Account - 2

**Operation Type**  
Disable Account

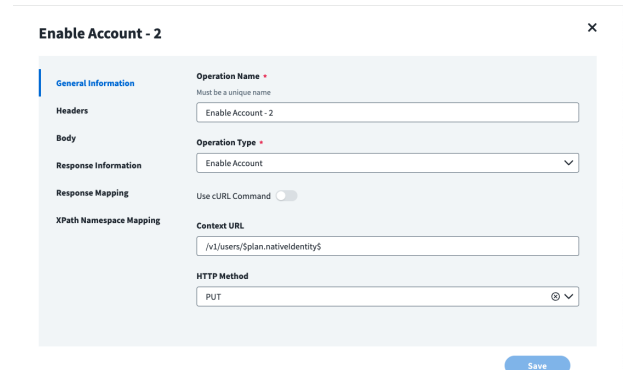
**Context URL**  
/v1/users/\$plan.nativeidentity\$

**HTTP Method**  
PUT

Save

To set the **Enable Account-2** information:

1. On the **Enable Account -2** panel, ensure that **General Information** is selected.
2. Enter a unique **Operation Name**, such as **Enable Account-2**.
3. Ensure the **Operation Type** is set to **Enable Account**.
4. Enter the **Context URL**.
5. Ensure the **HTTP Method** is set to **PUT**.
6. Click **Save**.



**Enable Account - 2**

**General Information**

**Operation Name** Must be a unique name  
Enable Account - 2

**Operation Type**  
Enable Account

**Context URL**  
/v1/users/\$plan.nativeidentity\$

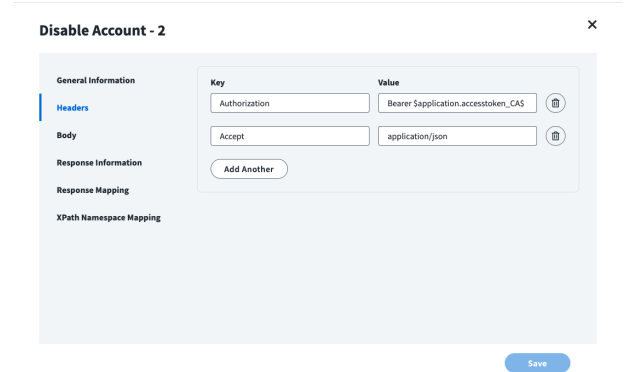
**HTTP Method**  
PUT

Save

## Headers (Disable Account-2 only)

To set the **Headers** information:

1. On the **Disable Account-2** panel, select **Headers**.
2. Complete the **Key** and **Value** fields.
3. To add additional key and value information, click **Add Another**.
4. When done, click **Save**.

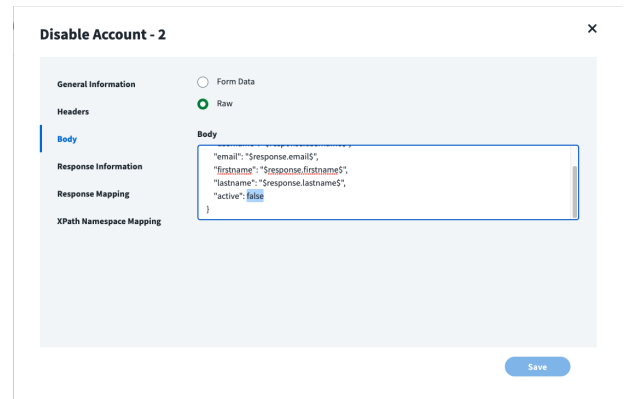


The screenshot shows the 'Disable Account - 2' configuration window with the 'Headers' tab selected. The 'Key' field contains 'Authorization' and the 'Value' field contains 'Bearer \$application.accesstoken\_CAS'. There is an 'Add Another' button below the fields. The 'Body' tab is also visible, showing 'Accept' as the key and 'application/json' as the value.

## Body (Disable Account-2 and Enable Account-2)

To set the **Body** information for **Disable Account-2**:

1. On the **Disable Account-2** panel, select **Body**.
2. Select **Raw**.
3. Complete the **Body** information by entering the text as written below.



The screenshot shows the 'Disable Account - 2' configuration window with the 'Body' tab selected. The 'Form Data' radio button is unselected, and the 'Raw' radio button is selected. The 'Body' text area contains the following JSON:

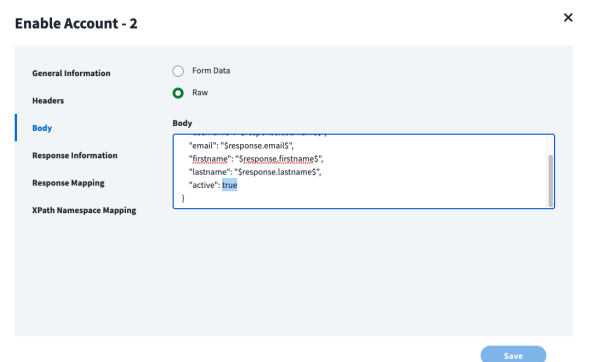
```
{
  "email": "$response.email$",
  "firstname": "$response.firstname$",
  "lastname": "$response.lastname$",
  "active": false
}
```

```
{
  "username": "$response.username$",
  "email": "$response.email$",
  "firstname": "$response.firstname$",
  "lastname": "$response.lastname$",
  "active": false
}
```

4. When done, click **Save**.

To set the **Body** information for **Enable Account-2**:

1. On the **Enable Account-2** panel, select **Body**.
2. Select **Raw**.
3. Complete the **Body** information by entering the text as written below.



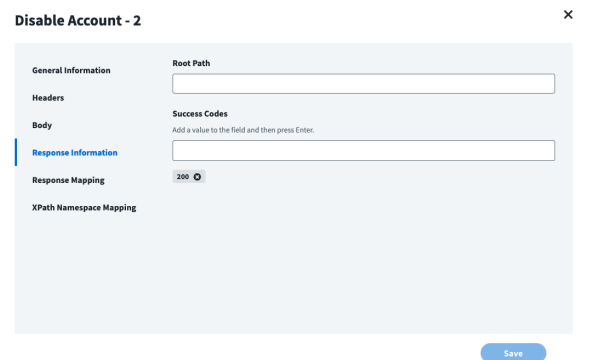
```
{
  "username": "$response.username$",
  "email": "$response.email$",
  "firstname": "$response.firstname$",
  "lastname": "$response.lastname$",
  "active": true
}
```

4. When done, click **Save**.

## Response Information (Disable Account-2 only)

To set the **Response Information**:

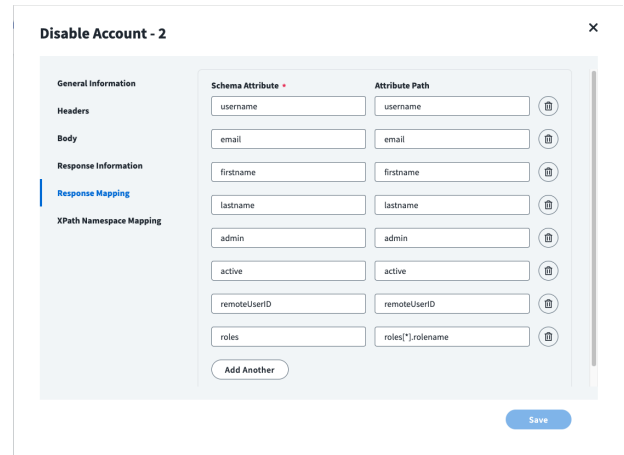
1. On the **Disable Account-2** panel, select **Response Information**.
2. Set the **Root Path** and **Success Codes**.
3. Click **Save**.



## Response Mapping (Disable Account-2 only)

To set the **Response Mapping** information:

1. On the **Disable Account-2** panel, select **Response Mapping**.
2. Set a **Schema Attribute** and the **Attribute Path**.
3. To add additional values, click **Add Another**.
4. When done, click **Save**.

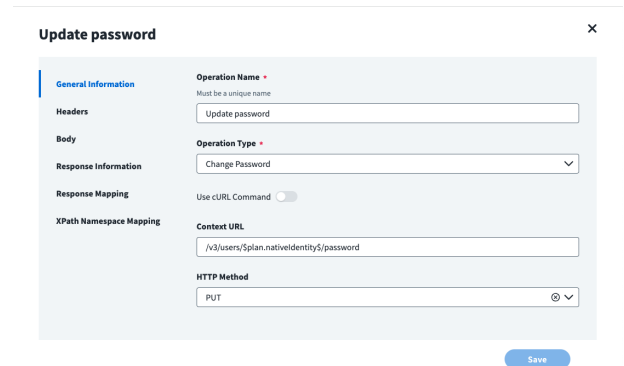


## Update Password

### General Information

To set the **Update Password** information:

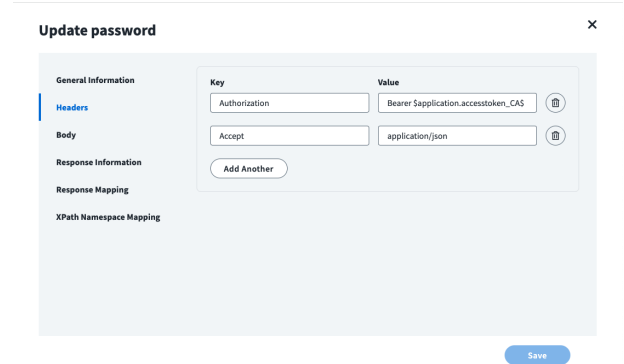
1. On the **Update Password** panel, ensure that **General Information** is selected.
2. Enter a unique **Operation Name**.
3. Ensure the **Operation Type** is set to **Change Password**.
4. Enter the **Context URL**.
5. Ensure the **HTTP Method** is set to **PUT**.
6. Click **Save**.



## Headers

To set the **Headers** information:

1. On the **Update Password** panel, select **Headers**.
2. Complete the **Key** and **Value** fields.
3. To add additional key and value information, click **Add Another**.
4. When done, click **Save**.



**Update password** [X]

General Information

**Headers**

Key	Value
Authorization	Bearer \$application.accesstoken_CAS
Accept	application/json

Add Another

Body

Response Information

Response Mapping

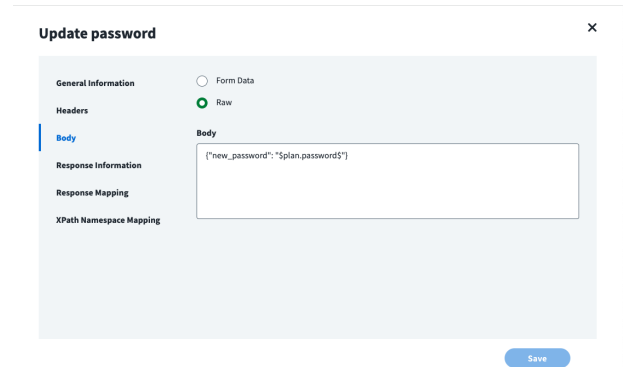
XPath Namespace Mapping

Save

## Body

To set the **Body** information:

1. On the **Update Password** panel, select **Body**.
2. Select **Raw**.
3. Complete the **Body** information by entering the text as written below.



**Update password** [X]

General Information

Form Data ☐ Raw ☒

**Body**

{"new\_password": "\$plan.password\$"}

Response Information

Response Mapping

XPath Namespace Mapping

Save

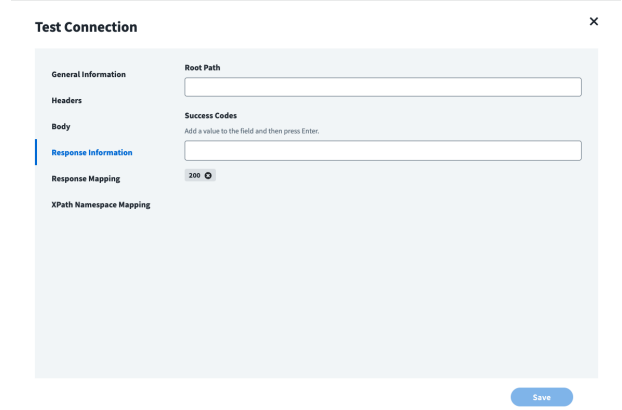
```
{"new_password": "$plan.password$"} 
```



## Response Information

To set the **Response Information**:

1. On the **Update Password** panel, select **Response Information**.
2. Set the **Root Path** and **Success Codes**.
3. Click **Save**.

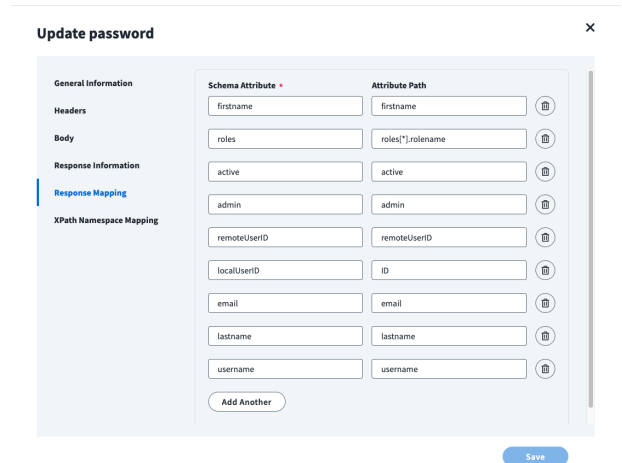


The 'Test Connection' dialog box has a sidebar with tabs: General Information, Headers, Body, Response Information (selected), Response Mapping, and XPath Namespace Mapping. The main area shows fields for 'Root Path' and 'Success Codes' (with a placeholder text 'Add a value to the field and then press Enter'). A '200' status code is displayed with a dropdown arrow. A 'Save' button is at the bottom right.

## Response Mapping

To set the **Response Mapping** information:

1. On the **Update Password** panel, select **Response Mapping**.
2. Set a **Schema Attribute** and the **Attribute Path**.
3. To add additional values, click **Add Another**.
4. When done, click **Save**.



The 'Update password' dialog box has a sidebar with tabs: General Information, Headers, Body, Response Information, Response Mapping (selected), and XPath Namespace Mapping. The main area shows a table with two columns: 'Schema Attribute' and 'Attribute Path'. The table contains several rows of mappings, each with a delete icon. An 'Add Another' button is at the bottom. A 'Save' button is at the bottom right.

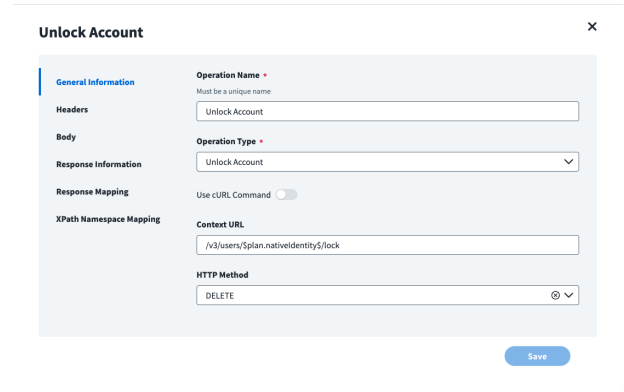
Schema Attribute	Attribute Path
firstname	firstname
roles	roles[*].rolename
active	active
admin	admin
remoteUserID	remoteUserID
localUserID	ID
email	email
lastname	lastname
username	username

## Unlock Account

### General Information

To set the **Unlock Account** information:

1. On the **Unlock Account** panel, ensure that **General Information** is selected.
2. Enter a unique **Operation Name**.
3. Ensure the **Operation Type** is set to **Unlock Account**.
4. Enter the **Context URL**.
5. Ensure the **HTTP Method** is set to **DELETE**.
6. Click **Save**.



**Unlock Account** [X]

**General Information**

**Operation Name** Must be a unique name

**Headers**

**Body**

**Operation Type** ▼  
 Unlock Account

**Response Information**

**Response Mapping** Use cURL Command ☐

**XPath Namespace Mapping**

**Context URL**

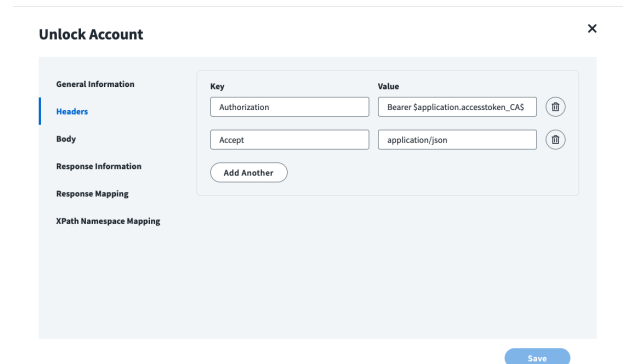
**HTTP Method** ⊙ ▼  
 DELETE

**Save**

### Headers

To set the **Headers** information:

1. On the **Unlock Account** panel, select **Headers**.
2. Complete the **Key** and **Value** fields.
3. To add additional key and value information, click **Add Another**.
4. When done, click **Save**.



**Unlock Account** [X]

**General Information**

**Headers**

Key	Value	
Authorization	Bearer \$application.accesstoken_CAS	⊗
Accept	application/json	⊗

**Body**

**Response Information**

**Response Mapping**

**XPath Namespace Mapping**

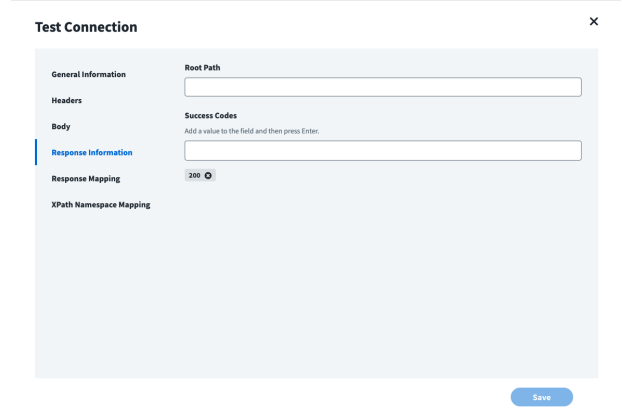
**Add Another**

**Save**

## Response Information

To set the **Response Information**:

1. On the **Unlock Account** panel, select **Response Information**.
2. Set the **Root Path** and **Success Codes**.
3. Click **Save**.



**Test Connection** [X]

General Information

Root Path

Headers

Body

**Response Information**

Success Codes

Add a value to the field and then press Enter.

Response Mapping

XPath Namespace Mapping

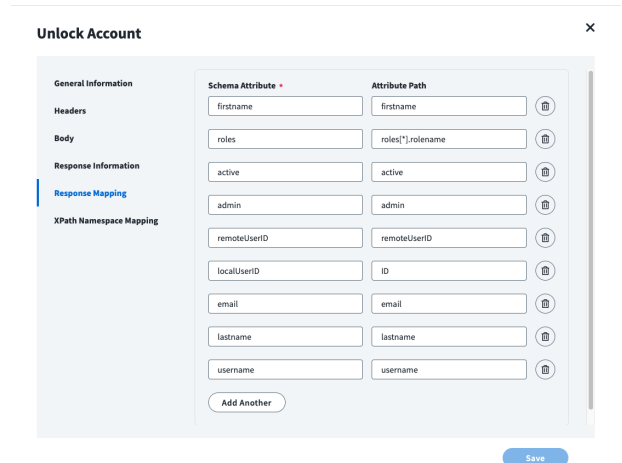
200 [X]

Save

## Response Mapping

To set the **Response Mapping** information:

1. On the **Unlock Account** panel, select **Response Mapping**.
2. Set a **Schema Attribute** and the **Attribute Path**.
3. To add additional values, click **Add Another**.
4. When done, click **Save**.



**Unlock Account** [X]

General Information

Headers

Body

**Response Mapping**

XPath Namespace Mapping

Schema Attribute	Attribute Path	
firstname	firstname	[X]
roles	roles[*].rolename	[X]
active	active	[X]
admin	admin	[X]
remoteUserID	remoteUserID	[X]
localUserID	ID	[X]
email	email	[X]
lastname	lastname	[X]
username	username	[X]

Add Another

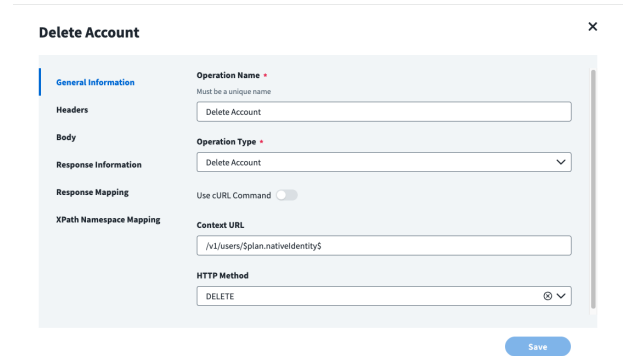
Save

## Delete Account

### General Information

To set the **Delete Account** information:

1. On the **Delete Account** panel, ensure that **General Information** is selected.
2. Enter a unique **Operation Name**.
3. Ensure the **Operation Type** is set to **Delete Account**.
4. Enter the **Context URL**.
5. Ensure the **HTTP Method** is set to **DELETE**.
6. Click **Save**.

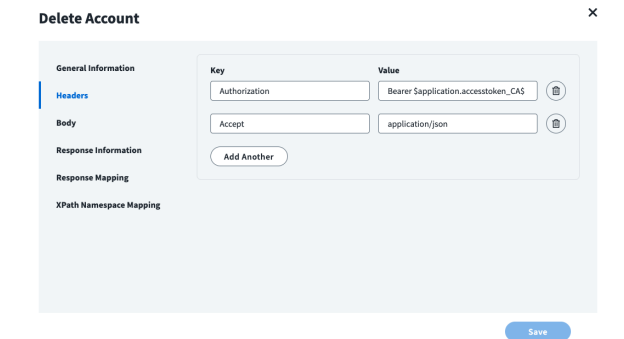


The screenshot shows the 'Delete Account' panel with the 'General Information' tab selected. The 'Operation Name' field contains 'Delete Account'. The 'Operation Type' dropdown is set to 'Delete Account'. The 'Context URL' field contains '/v1/users/\$plan.nativeidentity\$'. The 'HTTP Method' dropdown is set to 'DELETE'. A 'Save' button is at the bottom right.

### Headers

To set the **Headers** information:

1. On the **Delete Account** panel, select **Headers**.
2. Complete the **Key** and **Value** fields.
3. To add additional key and value information, click **Add Another**.
4. When done, click **Save**.



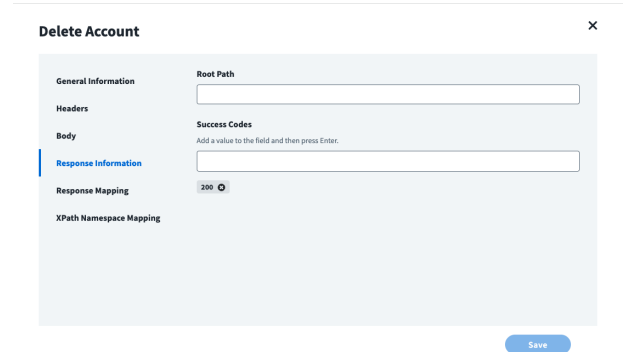
The screenshot shows the 'Delete Account' panel with the 'Headers' tab selected. There are two header entries: 'Authorization' with value 'Bearer \$application.access\_token\_CAS' and 'Accept' with value 'application/json'. An 'Add Another' button is below the entries. A 'Save' button is at the bottom right.

### Response Information

To set the **Response Information**:

1. On the **Delete Account** panel, select **Response Information**.
2. Set the **Root Path** and **Success Codes**.
3. Click **Save**.

This completes the list of **HTTP Operations**.



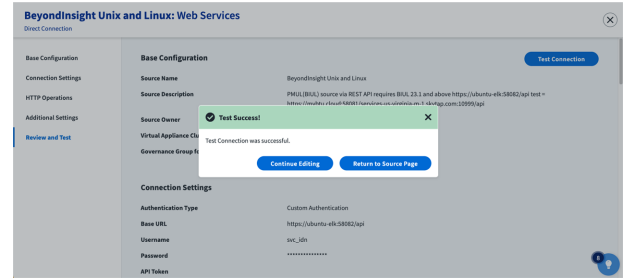
The screenshot shows the 'Delete Account' panel with the 'Response Information' tab selected. The 'Root Path' field is empty. The 'Success Codes' field contains '200'. A 'Save' button is at the bottom right.

Now that we have HTTP Operations defined, we can test the connection.

## Test the Connection

To test the connection:

1. On the left side menu, select **Review and Test**.
2. On the **Base Configuration** panel, click **Test Connection**. Upon a successful connection, a **Test Success!** message appears.
3. Click **Return to Source Page**.

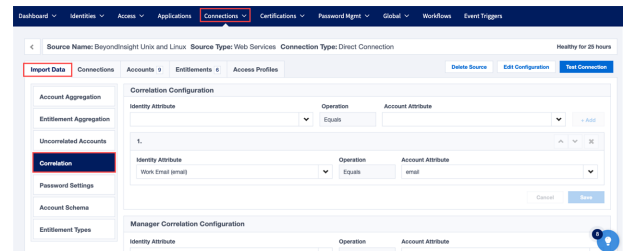


**Note:** If BIUL is using a self-signed certificate, or a certificate from a Certification Authority that is not trusted already by IdentityNow, the BIUL root certificate (base64 encoded) needs to be put on each Virtual Appliance, in the `~/sailpoint/certificates` directory. Refer to the SailPoint documentation for the detailed steps.

## Add a Correlation Rule

You need to add a correlation rule so BIUL Accounts are mapped to Identities.

1. Under **Connections**, select the **Import Data** tab.
2. Select **Correlation**.
3. Complete the **Correlation Configuration** fields.



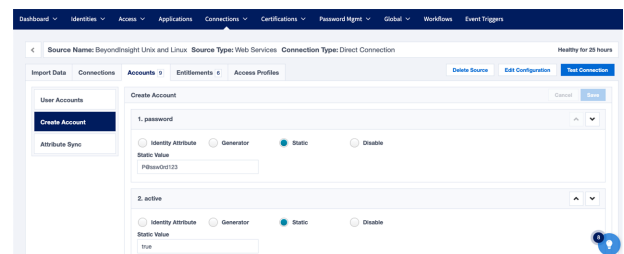
## Create Account and Provisioning Policy

For **Create Account**, you need a provisioning policy. The provisioning policy must be uploaded into the Connector using the IdentityNow REST API.



### IMPORTANT!

This step requires a SailPoint REST API call by someone who is a developer (typically). For more information, see [SailPoint APIs](https://developer.sailpoint.com/idn/api/v3/), at <https://developer.sailpoint.com/idn/api/v3/>.



1. Under **Connections**, select the **Accounts** tab.
2. Select **Create Account**.

Provisioning Policies:

```
{
  "name": "Account",
  "description": null,
  "usageType": "CREATE",
  "fields": [
    {
      "name": "password",
      "transform": {
        "type": "static",
        "attributes": {
          "value": "P@ssw0rd123"
        }
      },
      "attributes": {},
      "isRequired": false,
      "type": "string",
      "isMultiValued": false
    },
    {
      "name": "active",
      "transform": {
        "type": "static",
        "attributes": {
          "value": true
        }
      },
      "attributes": {},
      "isRequired": false,
      "type": "boolean",
      "isMultiValued": false
    },
    {
      "name": "username",
      "transform": {
        "type": "identityAttribute",
        "attributes": {
          "name": "uid"
        }
      },
      "attributes": {},
      "isRequired": false,
      "type": "string",
      "isMultiValued": false
    },
    {
      "name": "email",
      "transform": {
        "type": "identityAttribute",
        "attributes": {
          "name": "email"
        }
      },
      "attributes": {},
      "isRequired": false,
      "type": "string",
    }
  ]
}
```

```

        "isMultiValued": false
    },
    {
        "name": "firstname",
        "transform": {
            "type": "identityAttribute",
            "attributes": {
                "name": "firstname"
            }
        },
        "attributes": {},
        "isRequired": false,
        "type": "string",
        "isMultiValued": false
    },
    {
        "name": "lastname",
        "transform": {
            "type": "identityAttribute",
            "attributes": {
                "name": "lastname"
            }
        },
        "attributes": {},
        "isRequired": false,
        "type": "string",
        "isMultiValued": false
    }
]
}

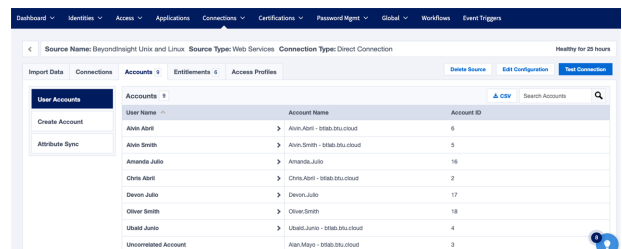
```

## Aggregate Accounts and Entitlements

You can now aggregate accounts and set entitlements.

### Aggregate Accounts

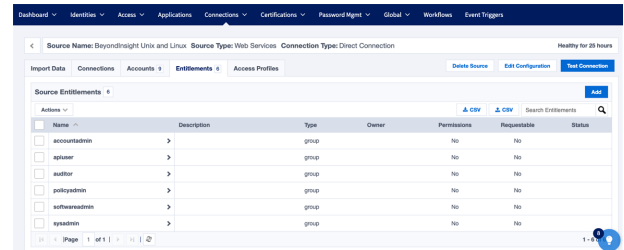
1. Under **Connections**, select the **Accounts** tab.
2. Select **User Accounts**.



User Name	Account Name	Account ID
Alvin Abert	Alvin.Abert@stbldtstcloud	6
Alvin Smith	Alvin.Smith@stbldtstcloud	5
Amanda Julio	Amanda.Julio	16
Chris Abert	Chris.Abert@stbldtstcloud	2
Devon Julio	Devon.Julio	17
Oliver Smith	Oliver.Smith	18
Uthaid Julio	Uthaid.Julio@stbldtstcloud	4
Unconnected Account	Alan.Mayo@stbldtstcloud	3

## Entitlements

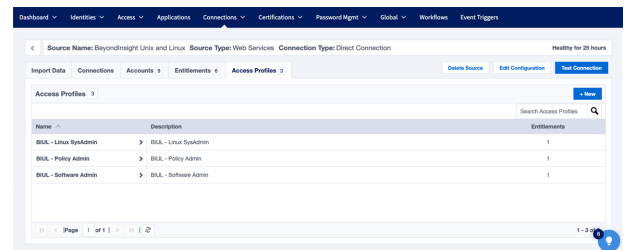
Under **Connections**, select the **Entitlements** tab.



Name	Description	Type	Owner	Permissions	Requestable	Status
accountadmin		group		No	No	
apuser		group		No	No	
auditor		group		No	No	
policyadmin		group		No	No	
softwareadmin		group		No	No	
sysadmin		group		No	No	

## Access Profiles

Access Profiles with associated Roles and Applications allows support for various Use Cases including Joiner, Mover, Leaver (JML), and Access Request.



Name	Description	Entitlements
BIA - Linux SysAdmin	BIA - Linux SysAdmin	1
BIA - Policy Admin	BIA - Policy Admin	1
BIA - Software Admin	BIA - Software Admin	1