



BeyondTrust

Privilege Management for Unix & Linux SailPoint IdentityIQ Integration

Table of Contents

| | |
|---|----------|
| SailPoint IdentityIQ Connector for PMUL (BIUL) | 3 |
| Overview | 3 |
| Create and Configure Web Services Application | 4 |
| Add and Configure Operations | 5 |
| Connector Operations | 9 |
| Account Schema | 23 |
| Group Schema | 24 |
| Provisioning Policy | 25 |
| Accounts Created and Active | 29 |
| Requestable BIUL Roles | 29 |

SailPoint IdentityIQ Connector for PMUL (BIUL)

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

Overview

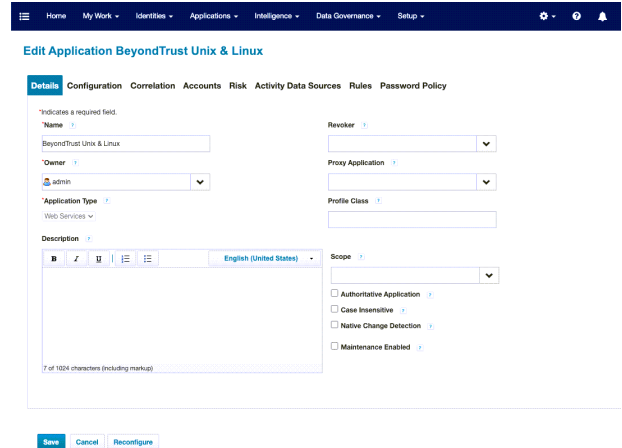
BeyondInsight for Unix & Linux (BIUL) must be configured with Privilege Management for Unix and Linux (PMUL). This integration allows SailPoint IdentityIQ (IdentityIQ) to provision access for BIUL users and add/remove roles.

Account Creation is triggered by Add Entitlement for a User without a BIUL account.

Create and Configure Web Services Application

To create a new web services application:

1. As an Administrator, log in to IdentityIQ and navigate to **Applications**.
2. Click **Add New Application**.
3. Under **Details**:
 - a. For **Name**, enter BeyondTrust Unix & Linux.
 - b. For **Owner**, select Admin (or another user).
 - c. For **Application Type**, select **Web Services**.
4. Click **Save**.



Edit Application BeyondTrust Unix & Linux

Details Configuration Correlation Accounts Risk Activity Data Sources Rules Password Policy

*Indicates a required field.

Name BeyondTrust Unix & Linux

Owner admin

Application Type Web Services

Description

Revoke

Proxy Application

Profile Class

Scope

☐ Authoritative Application

☐ Case Insensitive

☐ Native Change Detection

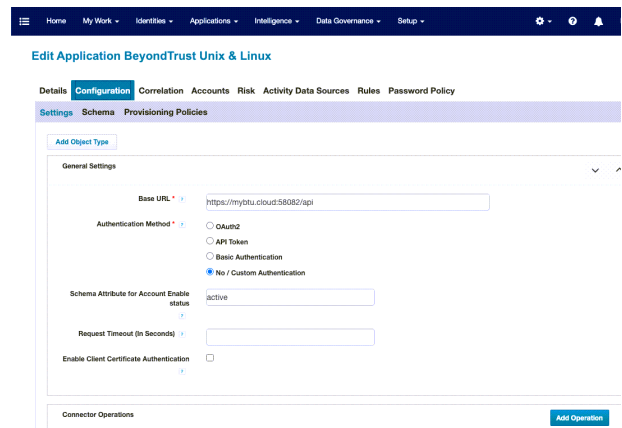
☐ Maintenance Enabled

7 of 1024 characters (including markup)

Save **Cancel** **Reconfigure**

Under **Configuration**:

1. Select **Settings**, and then provide a **Base URL**.
2. For **Authentication Method**, select **No / Custom Authentication**.
3. Set the **Schema Attribute for Account Enable status** to *active*.
4. At the bottom of the screen, click **Save**.



Edit Application BeyondTrust Unix & Linux

Details **Configuration** Correlation Accounts Risk Activity Data Sources Rules Password Policy

Settings **Schema** Provisioning Policies

Add Object Type

General Settings

Base URL https://mybtu.cloud:58082/api

Authentication Method

☐ OAuth2

☐ API Token

☐ Basic Authentication

☒ No / Custom Authentication

Schema Attribute for Account Enable status active

Request Timeout (in Seconds)

Enable Client Certificate Authentication

Connector Operations **Add Operation**

Next, you must add and configure operations.

Add and Configure Operations

First, you must add and configure Authentication and Test Connection operations. You must also successfully test the connection before moving on to the creation of other operations.

Authentication

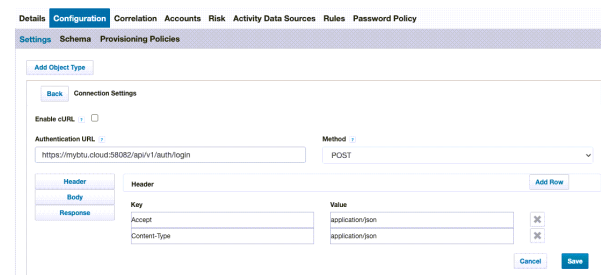
To create an Authentication operation:

1. Click the **Add Operation** button, and for the **Operation** type, select **Custom Authentication**.
2. Enter a **Name** for this operation.
3. At the right of the Custom Authentication operation row, in the **Actions** column, click the **Edit** button (pencil).
4. Under **Connection Settings**, configure the **Authentication URL** to match your instance of BIUL, and set the **Method** to **POST**.

Header

1. Select **Header**.
2. At the far right, click **Add Row**, for each entry you need to add.
3. Configure **Keys** for **Accept** and **Content-Type**, and set the value to *application/json* for both.

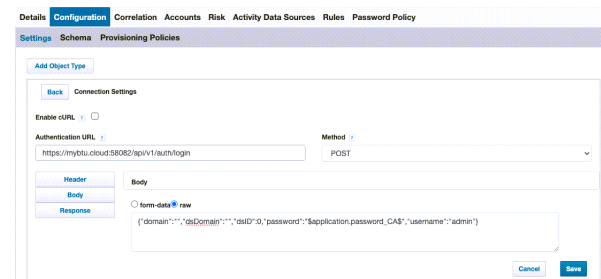
Edit Application BeyondTrust Unix & Linux



Body

1. Select **Body**.
2. Ensure the **Raw** option is selected.
3. Configure **Body** with *username* and use *\$application.password_CA\$* for the password value, as written below.

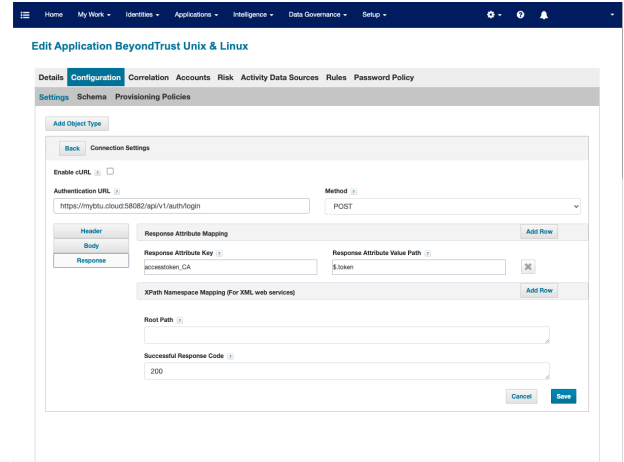
Edit Application BeyondTrust Unix & Linux



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

Response

1. Select **Response**. You must capture and save the access token.
2. For the **Response Attribute Mapping**:
 - a. Set the **Response Attribute Key** to `accesstoken_CA`.
 - b. Set the **Response Attribute Value Path** to `$.token`.
3. Under **XPath Namespace Mapping**, set the **Successful Response Code** to `200`.
4. Click **Save**.



Use /debug for Encrypted Keys and Password

We use an *encrypted* attribute to store the password.



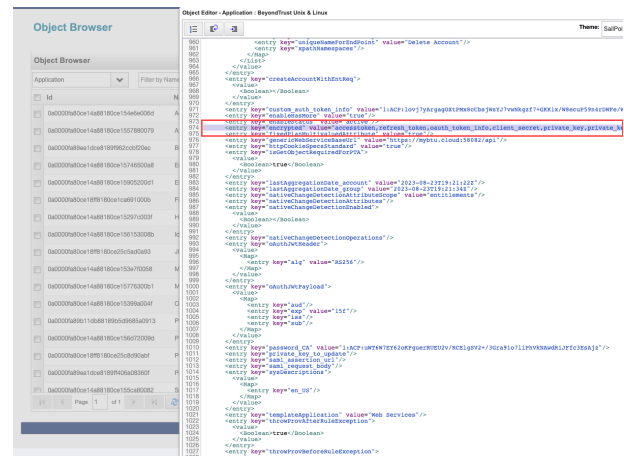
For more information, see https://documentation.sailpoint.com/connectors/identityiq/webservices/help/integrating_webservices/iiq_config_for_no_custom_authentication.html.

Access the **/debug** interface, and find your Application source.



Tip: Access the **/debug** interface by modifying the URL in the browser manually. For example, if the Url is `https://myServerName:8443/identityiq/home`, replace `/identityiq/home` by `/debug`.

Modify the list of **encrypted keys**, as written below.



```
<entry key="encrypted" value="accesstoken,refresh_token,oauth_token_info,client_secret,private_key,private_key_password,clientCertificate,clientKeySpec,resourceOwnerPassword,custom_auth_token_info,password_CA"/>
```

-
- The screenshot shows the IntelliJ IDEA IDE with the 'Object Browser' on the left and the 'Object Editor' on the right. The 'Object Editor' displays the XML configuration for the 'SpringBootUser' bean. The 'SpringBootUser' bean is highlighted in red in the original image. The XML configuration includes properties for 'username', 'password', 'email', 'phone', 'sex', 'age', 'status', 'role', and 'permissions'.
- ```

560 <entry key="username@roleId" value="delete Account"/>
561 </entry>
562 </map>
563 </field>
564 </bean>
565 <!-->
566 <!-->
567 <!-->
568 <!-->
569 <!-->
570 <!-->
571 <!-->
572 <!-->
573 <!-->
574 <!-->
575 <!-->
576 <!-->
577 <!-->
578 <!-->
579 <!-->
580 <!-->
581 <!-->
582 <!-->
583 <!-->
584 <!-->
585 <!-->
586 <!-->
587 <!-->
588 <!-->
589 <!-->
590 <!-->
591 <!-->
592 <!-->
593 <!-->
594 <!-->
595 <!-->
596 <!-->
597 <!-->
598 <!-->
599 <!-->
600 <!-->
601 <!-->
602 <!-->
603 <!-->
604 <!-->
605 <!-->
606 <!-->
607 <!-->
608 <!-->
609 <!-->
610 <!-->
611 <!-->
612 <!-->
613 <!-->
614 <!-->
615 <!-->
616 <!-->
617 <!-->
618 <!-->
619 <!-->
620 <!-->
621 <!-->
622 <!-->
623 <!-->
624 <!-->
625 <!-->
626 <!-->
627 <!-->
628 <!-->
629 <!-->
630 <!-->
631 <!-->
632 <!-->
633 <!-->
634 <!-->
635 <!-->
636 <!-->
637 <!-->
638 <!-->
639 <!-->
640 <!-->
641 <!-->
642 <!-->
643 <!-->
644 <!-->
645 <!-->
646 <!-->
647 <!-->
648 <!-->
649 <!-->
650 <!-->
651 <!-->
652 <!-->
653 <!-->
654 <!-->
655 <!-->
656 <!-->
657 <!-->
658 <!-->
659 <!-->
660 <!-->
661 <!-->
662 <!-->
663 <!-->
664 <!-->
665 <!-->
666 <!-->
667 <!-->
668 <!-->
669 <!-->
670 <!-->
671 <!-->
672 <!-->
673 <!-->
674 <!-->
675 <!-->
676 <!-->
677 <!-->
678 <!-->
679 <!-->
680 <!-->
681 <!-->
682 <!-->
683 <!-->
684 <!-->
685 <!-->
686 <!-->
687 <!-->
688 <!-->
689 <!-->
690 <!-->
691 <!-->
692 <!-->
693 <!-->
694 <!-->
695 <!-->
696 <!-->
697 <!-->
698 <!-->
699 <!-->
700 <!-->
701 <!-->
702 <!-->
703 <!-->
704 <!-->
705 <!-->
706 <!-->
707 <!-->
708 <!-->
709 <!-->
710 <!-->
711 <!-->
712 <!-->
713 <!-->
714 <!-->
715 <!-->
716 <!-->
717 <!-->
718 <!-->
719 <!-->
720 <!-->
721 <!-->
722 <!-->
723 <!-->
724 <!-->
725 <!-->
726 <!-->
727 <!-->
728 <!-->
729 <!-->
730 <!-->
731 <!-->
732 <!-->
733 <!-->
734 <!-->
735 <!-->
736 <!-->
737 <!-->
738 <!-->
739 <!-->
740 <!-->
741 <!-->
742 <!-->
743 <!-->
744 <!-->
745 <!-->
746 <!-->
747 <!-->
748 <!-->
749 <!-->
750 <!-->
751 <!-->
752 <!-->
753 <!-->
754 <!-->
755 <!-->
756 <!-->
757 <!-->
758 <!-->
759 <!-->
760 <!-->
761 <!-->
762 <!-->
763 <!-->
764 <!-->
765 <!-->
766 <!-->
767 <!-->
768 <!-->
769 <!-->
770 <!-->
771 <!-->
772 <!-->
773 <!-->
774 <!-->
775 <!-->
776 <!-->
777 <!-->
778 <!-->
779 <!-->
780 <!-->
781 <!-->
782 <!-->
783 <!-->
784 <!-->
785 <!-->
786 <!-->
787 <!-->
788 <!-->
789 <!-->
790 <!-->
791 <!-->
792 <!-->
793 <!-->
794 <!-->
795 <!-->
796 <!-->
797 <!-->
798 <!-->
799 <!-->
800 <!-->
801 <!-->
802 <!-->
803 <!-->
804 <!-->
805 <!-->
806 <!-->
807 <!-->
808 <!-->
809 <!-->
810 <!-->
811 <!-->
812 <!-->
813 <!-->
814 <!-->
815 <!-->
816 <!-->
817 <!-->
818 <!-->
819 <!-->
820 <!-->
821 <!-->
822 <!-->
823 <!-->
824 <!-->
825 <!-->
826 <!-->
827 <!-->
828 <!-->
829 <!-->
830 <!-->
831 <!-->
832 <!-->
833 <!-->
834 <!-->
835 <!-->
836 <!-->
837 <!-->
838 <!-->
839 <!-->
840 <!-->
841 <!-->
842 <!-->
843 <!-->
844 <!-->
845 <!-->
846 <!-->
847 <!-->
848 <!-->
849 <!-->
850 <!-->
851 <!-->
852 <!-->
853 <!-->
854 <!-->
855 <!-->
856 <!-->
857 <!-->
858 <!-->
859 <!-->
860 <!-->
861 <!-->
862 <!-->
863 <!-->
864 <!-->
865 <!-->
866 <!-->
867 <!-->
868 <!-->
869 <!-->
870 <!-->
871 <!-->
872 <!-->
873 <!-->
874 <!-->
875 <!-->
876 <!-->
877 <!-->
878 <!-->
879 <!-->
880 <!-->
881 <!-->
882 <!-->
883 <!-->

```

```
<entry key="password_CA" value="Clear_Text_Value"/>
```

Back in the SailPoint IdentityIQ interface, click **Save**.

After you save the application, the *clear text value* for password is replaced with *encrypted* value.

After you save the application, the *clear text value* for password is replaced with *encrypted value*.

## Test Connection

To create a Test Connection operation:

1. Click **Add Operation**, and for the **Operation** type, select **Test Connection**.
2. Enter a **Name** for this operation.
3. At the right of the Test Connection operation row, in the **Actions** column, click the **Edit** button (pencil).
4. Under **Connection Settings**, set the **Context URL** to *generic\_users* endpoint, and set the **Method** to **GET**.

## Header

1. Select **Header**.
2. Set the following **Keys** and **Values**:
  - a. An **Authorization** key, with a value of *Bearer \$application.accesstoken\_CA\$*.
  - b. An **Accept** key, with a value of *application/json*.

## Edit Application BeyondTrust Unix & Linux

[Details](#)[Configuration](#)[Correlation](#)[Accounts](#)[Risk](#)[Activity Data Sources](#)[Rules](#)[Password Policy](#)

[Settings](#)[Schema](#)[Provisioning Policies](#)

[Add Object Type](#)

[Back](#) [Connection Settings](#)

Enable cURL ☐

Context URL  Method

[Header](#)[Body](#)[Response](#)[Before Rule](#)[After Rule](#)

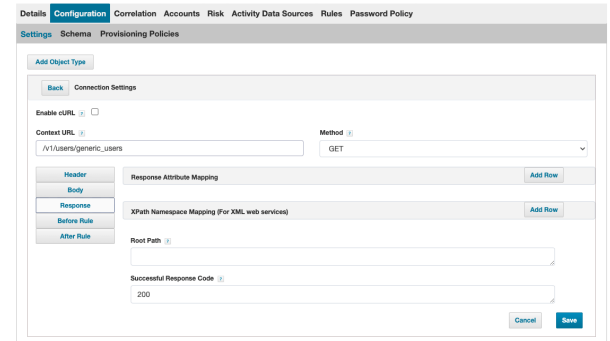
| Header        |                                                                          | <a href="#">Add Row</a> |
|---------------|--------------------------------------------------------------------------|-------------------------|
| Key           | Value                                                                    |                         |
| Authorization | <input type="text" value="Bearer &lt;Application.access_token_CAS&gt;"/> | <a href="#">✕</a>       |
| Accept        | <input type="text" value="application/json"/>                            | <a href="#">✕</a>       |

[Cancel](#) [Save](#)

## Response

1. Select **Response**.
2. Under **XPath Namespace Mapping**, set the **Successful Response Code** to **200**.
3. Click **Save**.

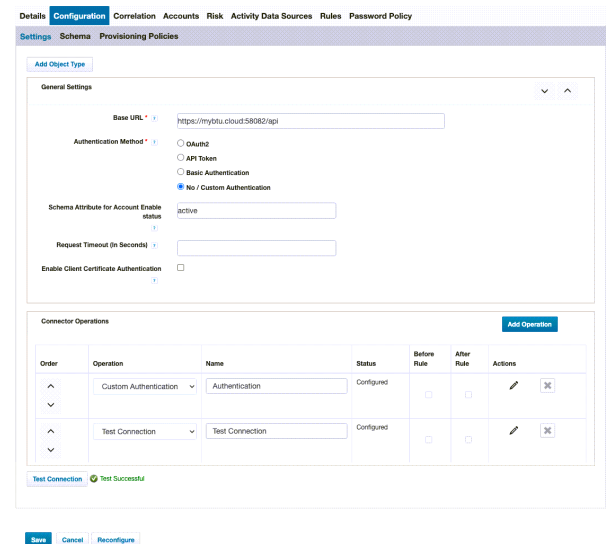
### Edit Application BeyondTrust Unix & Linux



So far, your application should look like this.

4. At the bottom left, click **Test Connection**, and look for a **Test Successful** response.
5. Click **Save**.

### Edit Application BeyondTrust Unix & Linux





## Connector Operations

Next, configure the following **Connector Operations**.

- ["Account Aggregation" on page 9](#)
- [Group Aggregation](#)
- [Create Account](#)
- [Add Entitlement](#)
- [Remove Entitlement](#)
- [Disable Account-1](#)
- [Disable Account-2](#)
- [Enable Account-1](#)
- [Enable Account-2](#)
- [Change Password](#)
- [Unlock Account](#)
- [Delete Account](#)

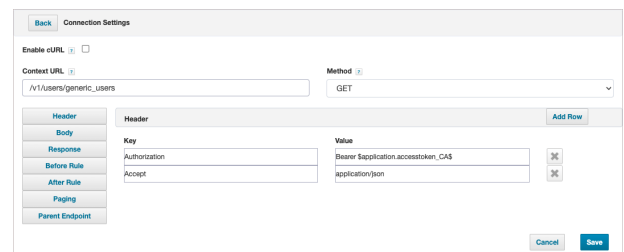
## Account Aggregation

To create an Account Aggregation operation:

1. Click **Add Operation**, and for the **Operation** type, select **Account Aggregation**.
2. Enter a **Name** for this operation.
3. At the right of the Account Aggregation operation row, in the **Actions** column, click the **Edit** button (pencil).
4. Under **Connection Settings**, set the **Context URL** to *generic\_users* endpoint, and set the **Method** to *GET*.

### Header

1. Select **Header**.
2. At the right of the Header section, click **Add Row**, and set the following **Keys** and **Values**:
  - a. An **Authorization** key, with a value of *Bearer \$application.accesstoken\_CA\$*.
  - b. An **Accept** key, with a value of *application/json*.



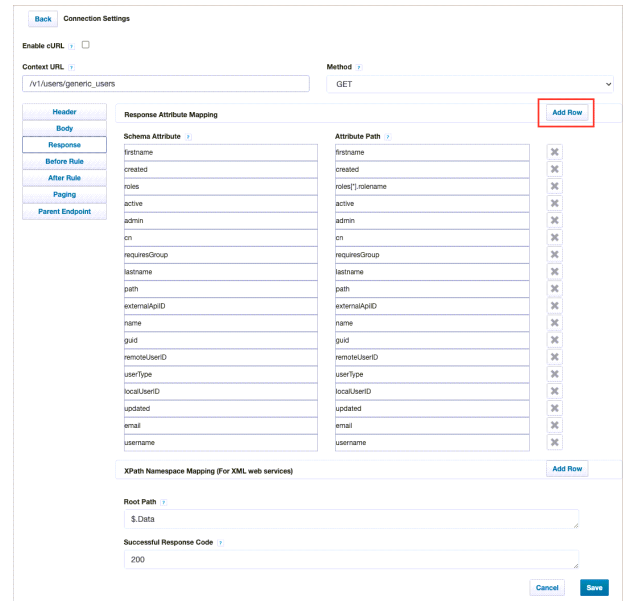
The screenshot shows the 'Connection Settings' dialog box. The 'Context URL' is set to '/v1/users/generic\_users' and the 'Method' is 'GET'. The 'Header' section is expanded, showing a table with two rows:

| Key           | Value                                 |
|---------------|---------------------------------------|
| Authorization | Bearer \$application.accesstoken_CA\$ |
| Accept        | application/json                      |

Buttons for 'Add Row', 'Cancel', and 'Save' are visible.

## Response

1. Select **Response**.
2. Configure the **Response Attribute Mappings** by clicking the Response Attribute Mapping **Add Row** button, and setting the following **Schema Attributes** and **Attribute Paths**.
  - 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
3. Click **Save**.



Connection Settings

Enable cURL ☐

Context URL: /v1/users/generic\_users Method: GET

**Response Attribute Mapping** Add Row

| 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          |

XPath Namespace Mapping (For XML web services) Add Row

Root Path: \$.Data

Successful Response Code: 200

Cancel Save

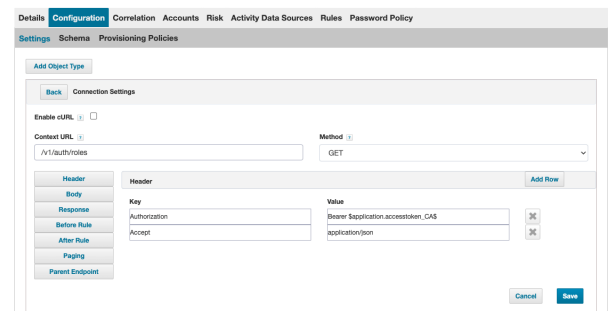
## Group Aggregation

To create a Group Aggregation operation:

1. Click **Add Operation**, and for the **Operation** type, select **Group Aggregation**.
2. Enter a **Name** for this operation.
3. At the right of the Group Aggregation operation row, in the **Actions** column, click the **Edit** button (pencil).
4. Under **Connection Settings**, set the **Context URL** to `/v1/auth/roles` endpoint, and set the **Method** to **GET**.

## Header

1. Select **Header**.
2. At the right of the Header section, click **Add Row**, and set the following **Keys** and **Values**:
  - a. An **Authorization** key, with a value of `Bearer $application.accesstoken_CA$`.
  - b. An **Accept** key, with a value of `application/json`.

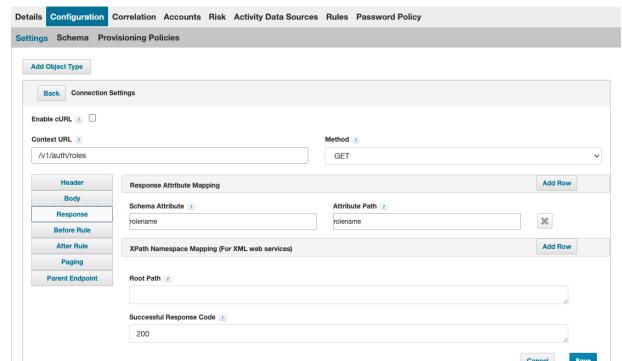


The screenshot shows the 'Configuration' tab with the 'Header' section selected. The 'Context URL' is set to `/v1/auth/roles` and the 'Method' is set to 'GET'. Under the 'Header' section, two rows are added:

| Key           | Value                                 |
|---------------|---------------------------------------|
| Authorization | Bearer \$application.accesstoken_CA\$ |
| Accept        | application/json                      |

## Response

1. Select **Response**.
2. At the right of **Response Attribute Mapping**, click **Add Row**.
  - a. Set the **Schema Attribute** to `rolename`.
  - b. Set the **Attribute Path** to `rolename`.
3. Under **XPath Namespace Mapping**, set the **Successful Response Code** to `200`.
4. Click **Save**.



The screenshot shows the 'Configuration' tab with the 'Response' section selected. The 'Context URL' is set to `/v1/auth/roles` and the 'Method' is set to 'GET'. Under the 'Response' section, the 'Response Attribute Mapping' table is configured as follows:

| Schema Attribute | Attribute Path |
|------------------|----------------|
| rolename         | rolename       |

Below this, the 'XPath Namespace Mapping (For XML web services)' section is also visible, with the 'Successful Response Code' set to `200`.

## Create Account

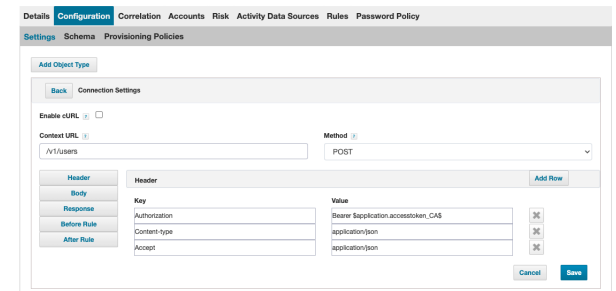
To create a Create Account operation:

1. Click **Add Operation**, and for the **Operation** type, select **Create Account**.
2. Enter a **Name** for this operation.
3. At the right of the Create Account operation row, in the **Actions** column, click the **Edit** button (pencil).
4. Under **Connection Settings**, set the **Context URL** to `/v1/users` endpoint, and set the **Method** to **POST**.

## Header

1. Select **Header**.
2. At the right of Header, click **Add Row** to add each of the following **Keys and Values**:
  - a. For **Authorization**, set the value as `Bearer $application.accesstoken_CA$`.
  - b. For **Content-type**, set the value as `application/json`.
  - c. For **Accept**, set the value as `application/json`.

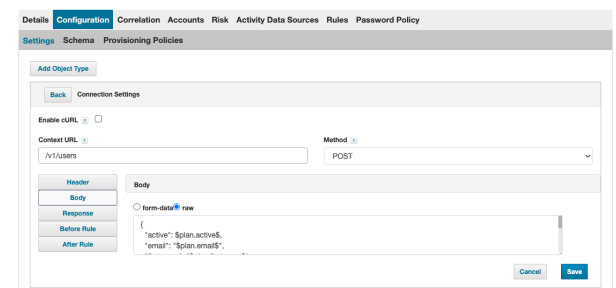
Edit Application BeyondTrust Unix & Linux



## Body

1. Select **Body**.
2. Ensure the **Raw** option is selected.
3. Configure **Body** using the text as written below.

Edit Application BeyondTrust Unix & Linux

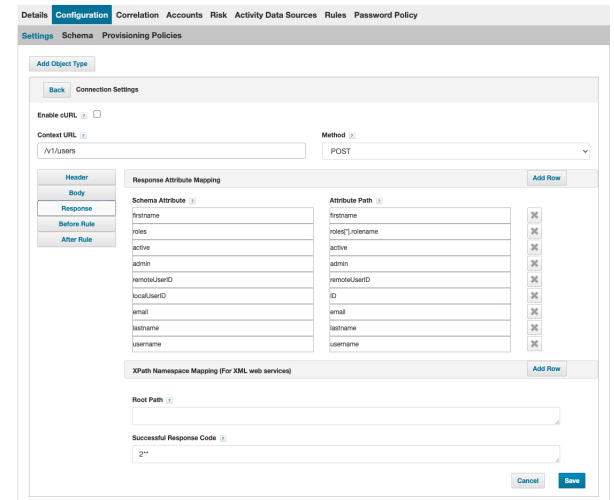


```
{
 "active": $plan.active$,
 "email": "$plan.email$",
 "firstname": "$plan.firstname$",
 "lastname": "$plan.lastname$",
 "password": "$plan.password$",
 "passwordConfirm": "$plan.password$",
 "username": "$plan.username$"
}
```

## Response

1. Select **Response**.
2. Configure the **Response Attribute Mappings** by clicking the Response Attribute Mapping **Add Row** button, and setting the following **Schema Attributes** and **Attribute Paths**.
  - firstname - firstname
  - roles - roles[\*].rolename
  - active - active
  - admin - admin
  - remoteUserID - remoteUserID
  - localUserID - localUserID
  - email - email
  - lastname - lastname
  - username - username
3. Under **XPath Namespace Mapping**, set the **Successful Response Code** to 2\*\*.
4. Click **Save**.

Edit Application BeyondTrust Unix &amp; Linux



## Add Entitlement

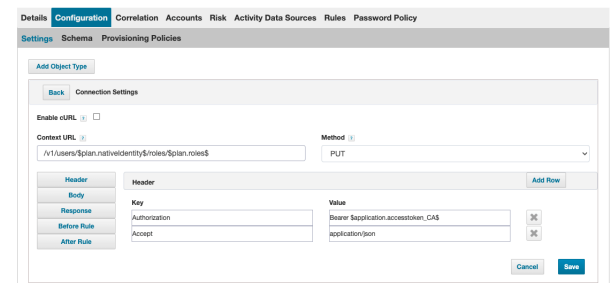
To create an Add Entitlement operation:

1. Click **Add Operation**, and for the **Operation** type, select **Add Entitlement**.
2. Enter a **Name** for this operation.
3. At the right of the Add Entitlement operation row, in the **Actions** column, click the **Edit** button (pencil).
4. Under **Connection Settings**, set the **Context URL** to `/v1/users/$plan.nativeIdentity$/roles/$plan.roles$` endpoint, and set the **Method** to **PUT**.

## Header

1. Select **Header**.
2. At the right of Header, click **Add Row** to add each of the following **Keys** and **Values**:
  - a. For **Authorization**, set the value as `Bearer $application.accesstoken_CA$`.
  - b. For **Accept**, set the value as `application/json`.

Edit Application BeyondTrust Unix &amp; Linux



## Response

1. Select **Response**.
2. Configure the **Response Attribute Mappings** by clicking the Response Attribute Mapping **Add Row** button, and setting the following **Schema Attributes** and **Attribute Paths**.
  - firstname - firstname
  - roles - roles[\*].rolename
  - active - active
  - admin - admin
  - remoteUserID - remoteUserID
  - localUserID - localUserID
  - email - email
  - lastname - lastname
  - username - username
3. Under **XPath Namespace Mapping**, set the **Successful Response Code** to 2\*\*.
4. Click **Save**.

Edit Application BeyondTrust Unix & Linux

Details Configuration Correlation Accounts Risk Activity Data Sources Rules Password Policy

Settings Schema Provisioning Policies

Add Object Type

Back Connection Settings

Enable cURL ☐

Context URL  Method

| Header                     | Body              | Response | Before Rule | After Rule |
|----------------------------|-------------------|----------|-------------|------------|
| Response Attribute Mapping |                   |          |             |            |
| Schema Attribute           | Attribute Path    |          |             |            |
| firstname                  | firstname         |          |             |            |
| roles                      | roles[*].rolename |          |             |            |
| active                     | active            |          |             |            |
| admin                      | admin             |          |             |            |
| remoteUserID               | remoteUserID      |          |             |            |
| localUserID                | localUserID       |          |             |            |
| email                      | email             |          |             |            |
| lastname                   | lastname          |          |             |            |
| username                   | username          |          |             |            |

XPath Namespace Mapping (For XML web services)

Root Path

Successful Response Code

Cancel Save

## Remove Entitlement

To create a Remove Entitlement operation:

1. Click **Add Operation**, and for the **Operation** type, select **Remove Entitlement**.
2. Enter a **Name** for this operation.
3. At the right of the Remove Entitlement operation row, in the **Actions** column, click the **Edit** button (pencil).
4. Under **Connection Settings**, set the **Context URL** to `/v1/users/$plan.nativeIdentity$/roles/$plan.roles$` endpoint, and set the **Method** to **DELETE**.

## Header

1. Select **Header**.
2. At the right of Header, click **Add Row** to add each of the following **Keys** and **Values**:
  - a. For **Authorization**, set the value as `Bearer $application.accesstoken_CA$`.
  - b. For **Accept**, set the value as `application/json`.

Edit Application BeyondTrust Unix & Linux

Details Configuration Correlation Accounts Risk Activity Data Sources Rules Password Policy

Settings Schema Provisioning Policies

Add Object Type

Back Connection Settings

Enable cURL ☐

Context URL  Method

| Header        | Body                                  | Response | Before Rule | After Rule |
|---------------|---------------------------------------|----------|-------------|------------|
| Header        |                                       |          |             |            |
| Key           | Value                                 |          |             |            |
| Authorization | Bearer \$application.accesstoken_CA\$ |          |             |            |
| Accept        | application/json                      |          |             |            |

Cancel Save

## Response

1. Select **Response**.
2. Configure the **Response Attribute Mappings** by clicking the Response Attribute Mapping **Add Row** button, and setting the following **Schema Attributes** and **Attribute Paths**.
  - firstname - firstname
  - roles - roles[\*].rolename
  - active - active
  - admin - admin
  - remoteUserID - remoteUserID
  - localUserID - localUserID
  - email - email
  - lastname - lastname
  - username - username
3. Under **XPath Namespace Mapping**, set the **Successful Response Code** to 2\*\*.
4. Click **Save**.

Edit Application BeyondTrust Unix & Linux

Details **Configuration** Correlation Accounts Risk Activity Data Sources Rules Password Policy

Settings Schema Provisioning Policies

Add Object Type

Back Connection Settings

Enable cURL ☐

Context URL  Method

Header Body Response Before Rule After Rule

Response Attribute Mapping

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

XPath Namespace Mapping (For XML web services)

Root Path

Successful Response Code

Cancel Save

## Disable Account-1

To create a Disable Account-1 operation:

1. Click **Add Operation**, and for the **Operation** type, select **Disable Account-1**.
2. Enter a **Name** for this operation.
3. At the right of the Disable Account-1 operation row, in the **Actions** column, click the **Edit** button (pencil).
4. Under **Connection Settings**, set the **Context URL** to `/v1/users/$plan.nativeidentity$` endpoint, and set the **Method** to **GET**.

## Header

1. Select **Header**.
2. At the right of Header, click **Add Row** to add each of the following **Keys** and **Values**:
  - a. For **Authorization**, set the value as `Bearer $application.accesstoken_CA$`.
  - b. For **Accept**, set the value as `application/json`.

Edit Application BeyondTrust Unix & Linux

Details **Configuration** Correlation Accounts Risk Activity Data Sources Rules Password Policy

Settings Schema Provisioning Policies

Add Object Type

Back Connection Settings

Enable cURL ☐

Context URL  Method

Header Body Response Before Rule After Rule

Header

| Key           | Value                                 |
|---------------|---------------------------------------|
| Authorization | Bearer \$application.accesstoken_CA\$ |
| Accept        | application/json                      |

Cancel Save

## Response

1. Select **Response**.
2. Configure the **Response Attribute Mappings** by clicking the Response Attribute Mapping **Add Row** button, and setting the following **Schema Attributes** and **Attribute Paths**.
  - firstname - firstname
  - roles - roles[\*].rolename
  - active - active
  - admin - admin
  - remoteUserID - remoteUserID
  - localUserID - localUserID
  - email - email
  - lastname - lastname
  - username - username
3. Under **XPath Namespace Mapping**, set the **Successful Response Code** to **200**.
4. Click **Save**.

Edit Application BeyondTrust Unix & Linux

Details Configuration Correlation Accounts Risk Activity Data Sources Rules Password Policy

Settings Schema Provisioning Policies

Add Object Type

Back Connection Settings

Enable cURL ☐

Context URL  Method

Header Body Response Before Rule After Rule

Response Attribute Mapping

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

XPath Namespace Mapping (For XML web services)

Root Path

Successful Response Code

Cancel Save

## Disable Account-2

To create a Disable Account-2 operation:

1. Click **Add Operation**, and for the **Operation** type, select **Disable Account-2**.
2. Enter a **Name** for this operation.
3. At the right of the Disable Account-2 operation row, in the **Actions** column, click the **Edit** button (pencil).
4. Under **Connection Settings**, set the **Context URL** to **/v1/users/\$plan.nativeidentity\$** endpoint, and set the **Method** to **PUT**.

## Header

1. Select **Header**.
2. At the right of Header, click **Add Row** to add each of the following **Keys** and **Values**:
  - a. For **Authorization**, set the value as *Bearer \$application.accesstoken\_CA\$*.
  - b. For **Accept**, set the value as *application/json*.

Edit Application BeyondTrust Unix & Linux

Details Configuration Correlation Accounts Risk Activity Data Sources Rules Password Policy

Settings Schema Provisioning Policies

Add Object Type

Back Connection Settings

Enable cURL ☐

Context URL  Method

Header Body Response Before Rule After Rule

Header

| Key           | Value                                 |
|---------------|---------------------------------------|
| Authorization | Bearer \$application.accesstoken_CA\$ |
| Accept        | application/json                      |

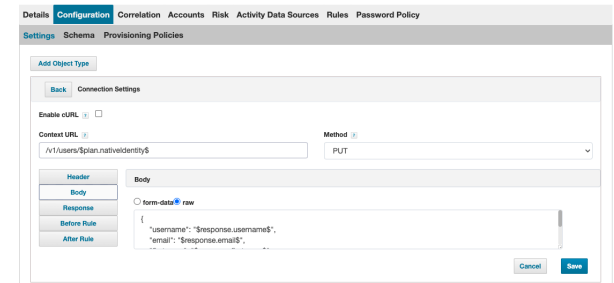
Cancel Save



## Body

1. Select **Body**.
2. Ensure the **Raw** option is selected.
3. Configure **Body** using the text as written below.

Edit Application BeyondTrust Unix &amp; Linux

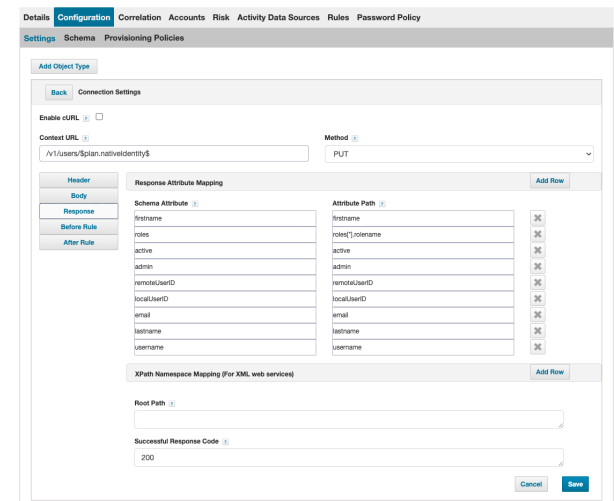


```
{
 "username": "$response.username$",
 "email": "$response.email$",
 "firstname": "$response.firstname$",
 "lastname": "$response.lastname$",
 "active": false
}
```

## Response

1. Select **Response**.
2. Configure the **Response Attribute Mappings** by clicking the Response Attribute Mapping **Add Row** button, and setting the following **Schema Attributes** and **Attribute Paths**.
  - firstname - firstname
  - roles - roles[\*].rolename
  - active - active
  - admin - admin
  - remoteUserID - remoteUserID
  - localUserID - localUserID
  - email - email
  - lastname - lastname
  - username - username
3. Under **XPath Namespace Mapping**, set the **Successful Response Code** to **200**.
4. Click **Save**.

Edit Application BeyondTrust Unix &amp; Linux



## Enable Account-1

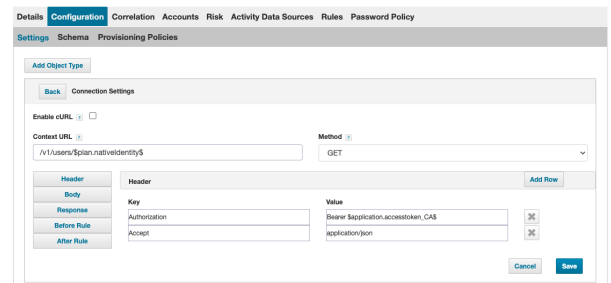
To create an Enable Account-1 operation:

1. Click **Add Operation**, and for the **Operation** type, select **Enable Account-1**.
2. Enter a **Name** for this operation.
3. At the right of the Enable Account-1 operation row, in the **Actions** column, click the **Edit** button (pencil).
4. Under **Connection Settings**, set the **Context URL** to `/v1/users/$plan.nativeIdentity$` endpoint, and set the **Method** to **GET**.

## Header

1. Select **Header**.
2. At the right of Header, click **Add Row** to add each of the following **Keys** and **Values**:
  - a. For **Authorization**, set the value as `Bearer $application.accesstoken_CA$`.
  - b. For **Accept**, set the value as `application/json`.

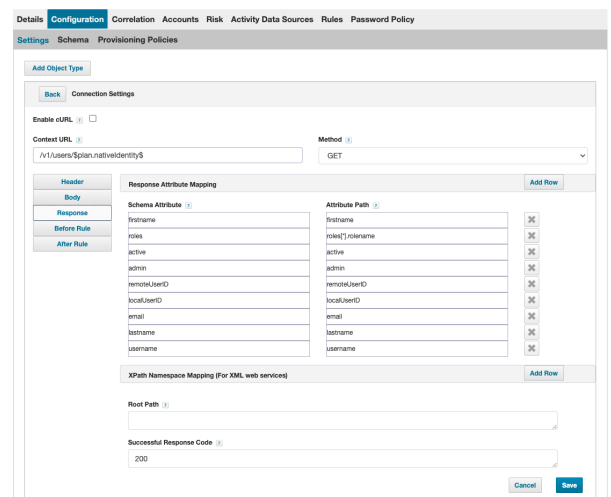
Edit Application BeyondTrust Unix & Linux



## Response

1. Select **Response**.
2. Configure the **Response Attribute Mappings** by clicking the Response Attribute Mapping **Add Row** button, and setting the following **Schema Attributes** and **Attribute Paths**.
  - firstname - firstname
  - roles - roles[\*].rolename
  - active - active
  - admin - admin
  - remoteUserID - remoteUserID
  - localUserID - localUserID
  - email - email
  - lastname - lastname
  - username - username
3. Under **XPath Namespace Mapping**, set the **Successful Response Code** to **200**.
4. Click **Save**.

Edit Application BeyondTrust Unix & Linux



## Enable Account-2

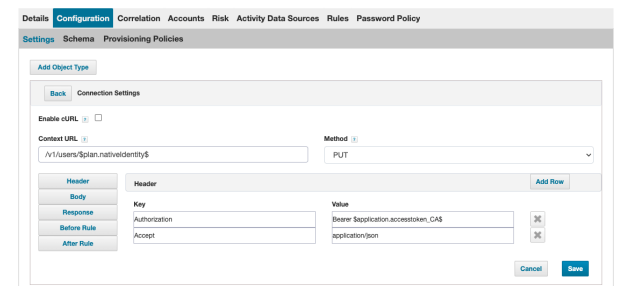
To create an Enable Account-2 operation:

1. Click **Add Operation**, and for the **Operation** type, select **Enable Account-2**.
2. Enter a **Name** for this operation.
3. At the right of the Enable Account-2 operation row, in the **Actions** column, click the **Edit** button (pencil).
4. Under **Connection Settings**, set the **Context URL** to `/v1/users/$plan.nativeIdentity$` endpoint, and set the **Method** to **PUT**.

## Header

1. Select **Header**.
2. At the right of Header, click **Add Row** to add each of the following **Keys** and **Values**:
  - a. For **Authorization**, set the value as `Bearer $application.accesstoken_CA$`.
  - b. For **Accept**, set the value as `application/json`.

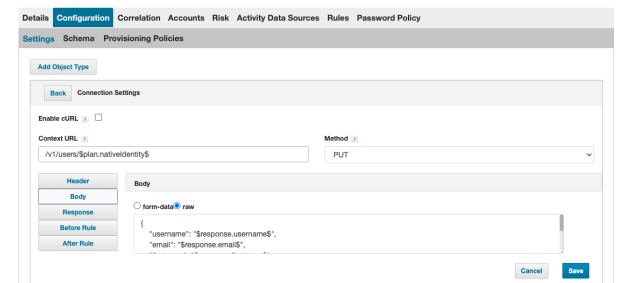
Edit Application BeyondTrust Unix & Linux



## Body

1. Select **Body**.
2. Ensure the **Raw** option is selected.
3. Configure **Body** using the text as written below.

Edit Application BeyondTrust Unix & Linux



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

## Response

1. Select **Response**.
2. Configure the **Response Attribute Mappings** by clicking the Response Attribute Mapping **Add Row** button, and setting the following **Schema Attributes** and **Attribute Paths**.
  - firstname - firstname
  - roles - roles[\*].rolename
  - active - active
  - admin - admin
  - remoteUserID - remoteUserID
  - localUserID - localUserID
  - email - email
  - lastname - lastname
  - username - username
3. Under **XPath Namespace Mapping**, set the **Successful Response Code** to **200**.
4. Click **Save**.

Edit Application BeyondTrust Unix & Linux

Details Configuration Correlation Accounts Risk Activity Data Sources Rules Password Policy

Settings Schema Provisioning Policies

Add Object Type

Back Connection Settings

Enable cURL ☐

Context URL  Method

| Header                     | Body              | Response | Before Rule | After Rule |
|----------------------------|-------------------|----------|-------------|------------|
| Response Attribute Mapping |                   |          |             |            |
| Schema Attribute           | Attribute Path    |          |             |            |
| firstname                  | firstname         |          |             |            |
| roles                      | roles[*].rolename |          |             |            |
| active                     | active            |          |             |            |
| admin                      | admin             |          |             |            |
| remoteUserID               | remoteUserID      |          |             |            |
| localUserID                | localUserID       |          |             |            |
| email                      | email             |          |             |            |
| lastname                   | lastname          |          |             |            |
| username                   | username          |          |             |            |

XPath Namespace Mapping (for XML web services)

Root Path

Successful Response Code

Cancel Save

## Change Password

To create a Change Password operation:

1. Click **Add Operation**, and for the **Operation** type, select **Change Password**.
2. Enter a **Name** for this operation.
3. At the right of the Change Password operation row, in the **Actions** column, click the **Edit** button (pencil).
4. Under **Connection Settings**, set the **Context URL** to **/v1/users/\$plan.nativeidentity\$/password** endpoint, and set the **Method** to **PUT**.

## Header

1. Select **Header**.
2. At the right of Header, click **Add Row** to add each of the following **Keys** and **Values**:
  - a. For **Authorization**, set the value as *Bearer \$application.accesstoken\_CA\$*.
  - b. For **Accept**, set the value as *application/json*.

Edit Application BeyondTrust Unix & Linux

Details Configuration Correlation Accounts Risk Activity Data Sources Rules Password Policy

Settings Schema Provisioning Policies

Add Object Type

Back Connection Settings

Enable cURL ☐

Context URL  Method

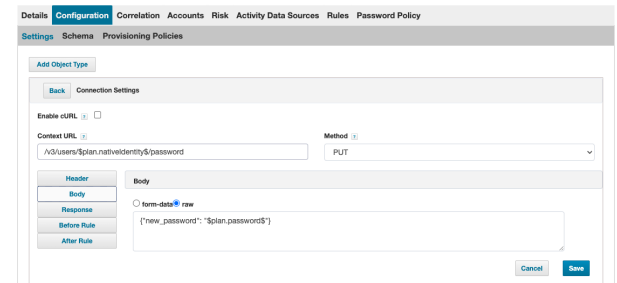
| Header        | Body                                  | Response | Before Rule | After Rule |
|---------------|---------------------------------------|----------|-------------|------------|
| Header        |                                       |          |             |            |
| Key           | Value                                 |          |             |            |
| Authorization | Bearer \$application.accesstoken_CA\$ |          |             |            |
| Accept        | application/json                      |          |             |            |

Cancel Save

## Body

1. Select **Body**.
2. Ensure the **Raw** option is selected.
3. Configure **Body** using the text as written below.

Edit Application BeyondTrust Unix &amp; Linux



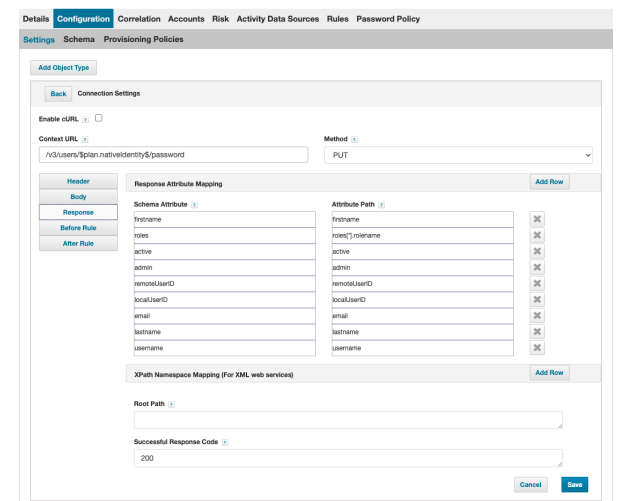
```
{"new_password": "$plan.password$"}

```

## Response

1. Select **Response**.
2. Configure the **Response Attribute Mappings** by clicking the Response Attribute Mapping **Add Row** button, and setting the following **Schema Attributes** and **Attribute Paths**.
  - firstname - firstname
  - roles - roles[\*].rolename
  - active - active
  - admin - admin
  - remoteUserID - remoteUserID
  - localUserID - localUserID
  - email - email
  - lastname - lastname
  - username - username
3. Under **XPath Namespace Mapping**, set the **Successful Response Code** to **200**.
4. Click **Save**.

Edit Application BeyondTrust Unix &amp; Linux



## Unlock Account

To create an Unlock Account operation:

1. Click **Add Operation**, and for the **Operation** type, select **Unlock Account**.
2. Enter a **Name** for this operation.
3. At the right of the Unlock Account operation row, in the **Actions** column, click the **Edit** button (pencil).
4. Under **Connection Settings**, set the **Context URL** to `/v3/users/$plan.nativeIdentity$/lock` endpoint, and set the **Method** to **DELETE**.

## Header

1. Select **Header**.
2. At the right of Header, click **Add Row** to add each of the following **Keys** and **Values**:
  - a. For **Authorization**, set the value as *Bearer \$application.accesstoken\_CA\$*.
  - b. For **Accept**, set the value as *application/json*.

Edit Application BeyondTrust Unix & Linux

Details Configuration Correlation Accounts Risk Activity Data Sources Rules Password Policy

Settings Schema Provisioning Policies

Add Object Type

Back Connection Settings

Enable cURL ☐

Context URL  Method

| Header | Key           | Value                                 |
|--------|---------------|---------------------------------------|
|        | Authorization | Bearer \$application.accesstoken_CA\$ |
|        | Accept        | application/json                      |

Cancel Save

## Response

1. Select **Response**.
2. Configure the **Response Attribute Mappings** by clicking the Response Attribute Mapping **Add Row** button, and setting the following **Schema Attributes** and **Attribute Paths**.
  - firstname - firstname
  - roles - roles[\*].rolename
  - active - active
  - admin - admin
  - remoteUserID - remoteUserID
  - localUserID - localUserID
  - email - email
  - lastname - lastname
  - username - username
3. Under **XPath Namespace Mapping**, set the **Successful Response Code** to **200**.
4. Click **Save**.

Edit Application BeyondTrust Unix & Linux

Details Configuration Correlation Accounts Risk Activity Data Sources Rules Password Policy

Settings Schema Provisioning Policies

Add Object Type

Back Connection Settings

Enable cURL ☐

Context URL  Method

| Header | Response Attribute Mapping | Attribute Path    |
|--------|----------------------------|-------------------|
| Body   | Schema Attribute           | firstname         |
|        | roles                      | roles[*].rolename |
|        | active                     | active            |
|        | admin                      | admin             |
|        | remoteUserID               | remoteUserID      |
|        | localUserID                | localUserID       |
|        | email                      | email             |
|        | lastname                   | lastname          |
|        | username                   | username          |

XPath Namespace Mapping (For XML web services)

Root Path

Successful Response Code

Cancel Save

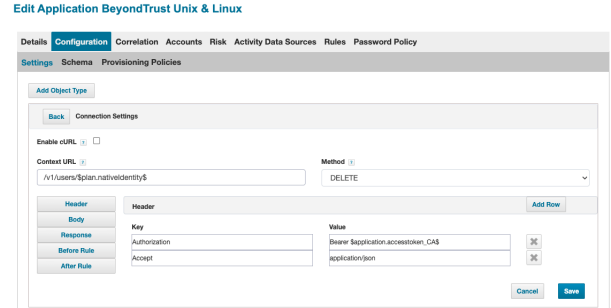
## Delete Account

To create a Delete Account operation:

1. Click **Add Operation**, and for the **Operation** type, select **Delete Account**.
2. Enter a **Name** for this operation.
3. At the right of the Delete Account operation row, in the **Actions** column, click the **Edit** button (pencil).
4. Under **Connection Settings**, set the **Context URL** to */v1/users/\$plan.nativeidentity\$/lock* endpoint, and set the **Method** to **DELETE**.

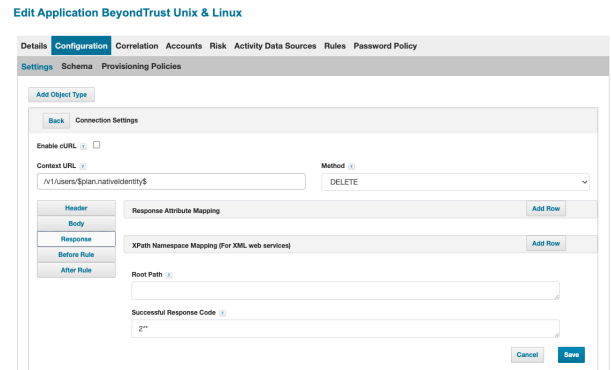
## Header

1. Select **Header**.
2. At the right of Header, click **Add Row** to add each of the following **Keys** and **Values**:
  - a. For **Authorization**, set the value as *Bearer \$application.access\_token\_CA\$*.
  - b. For **Accept**, set the value as *application/json*.



## Response

1. Select **Response**.
2. Under **XPath Namespace Mapping**, set the **Successful Response Code** to *2\*\**.
3. Click **Save**.



Now that we have all Connector Operations configured, let's configure the Schema.

## Account Schema

To configure the Account Schema:

1. Under **Configuration**, select **Schema**, and then click **Add Object Type**.
2. For the object type, select **Account**.

## Details

Complete the **Details** section as follows:

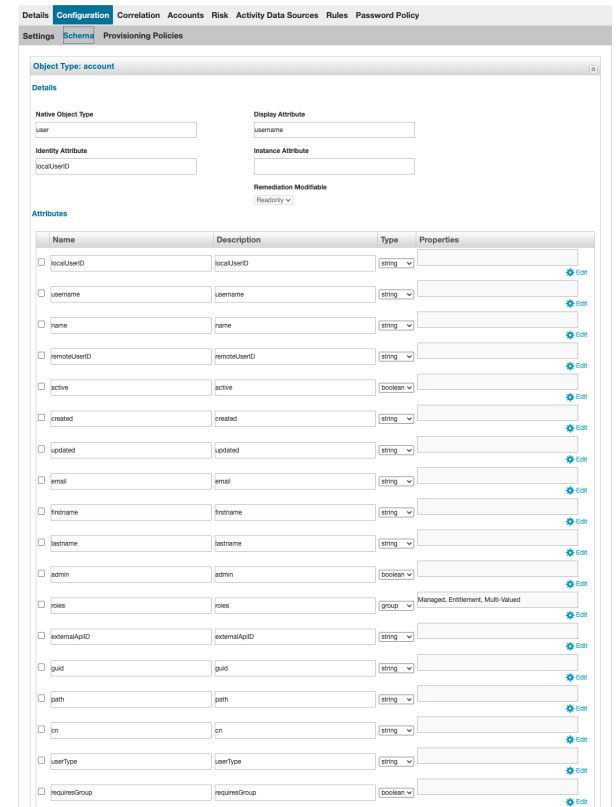
1. For **Native Object Type**, enter *user*.
2. For **Display Attribute**, enter *username*.
3. For **Identity Attribute**, enter *localUserID*.

## Attributes

Complete the **Attributes** section as follows:

1. Click **Add New Schema Attribute** and enter **Name**, **Description**, **Type**, and **Properties** (if any) for each:
  - a. LocalUserID, LocalUserID, string
  - b. username, username, string
  - c. name, name, string
  - d. remoteUserID, remoteUserID, string
  - e. active, active, boolean
  - f. created, created, string
  - g. updated, updated, string
  - h. email, email, string
  - i. firstname, firstname, string
  - j. lastname, lastname, string
  - k. admin, admin, boolean
  - l. roles, roles, group, Managed, Entitlement, Multi-Valued
  - m. externalApiID, externalApiID, string
  - n. guid, guid, string
  - o. path, path, string
  - p. cn, cn, string
  - q. userType, userType, string
  - r. requiresGroup, requiresGroup, boolean

Edit Application BeyondTrust Unix & Linux



| Name          | Description   | Type    | Properties                         |
|---------------|---------------|---------|------------------------------------|
| localUserID   | localUserID   | string  |                                    |
| username      | username      | string  |                                    |
| name          | name          | string  |                                    |
| remoteUserID  | remoteUserID  | string  |                                    |
| active        | active        | boolean |                                    |
| created       | created       | string  |                                    |
| updated       | updated       | string  |                                    |
| email         | email         | string  |                                    |
| firstname     | firstname     | string  |                                    |
| lastname      | lastname      | string  |                                    |
| admin         | admin         | boolean |                                    |
| roles         | roles         | group   | Managed, Entitlement, Multi-Valued |
| externalApiID | externalApiID | string  |                                    |
| guid          | guid          | string  |                                    |
| path          | path          | string  |                                    |
| cn            | cn            | string  |                                    |
| userType      | userType      | string  |                                    |
| requiresGroup | requiresGroup | boolean |                                    |

## Group Schema

To configure the Group Schema:

1. Under **Configuration**, select **Schema**, and then click **Add Object Type**.
2. For the object type, select **Group**.



## Details

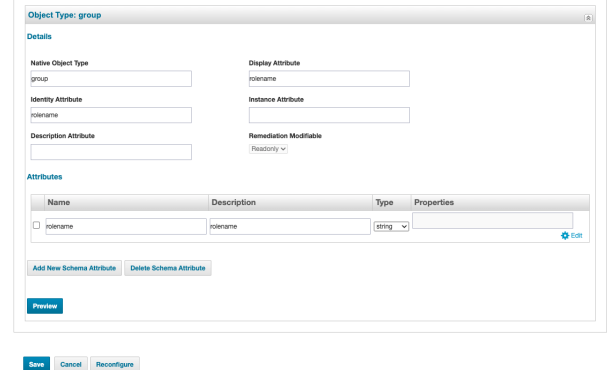
Complete the **Details** section as follows:

1. For **Native Object Type**, enter *group*.
2. For **Display Attribute**, enter *rolename*.
3. For **Identity Attribute**, enter *rolename*.

## Attributes

Complete the **Attributes** section as follows:

1. Click **Add New Schema Attribute** and enter **Name**, **Description**, **Type**, and **Properties** (if any) for each:
  - a. rolename, rolename, string
2. Click **Save**.



## Provisioning Policy

You also need a Provisioning Policy for account creation.

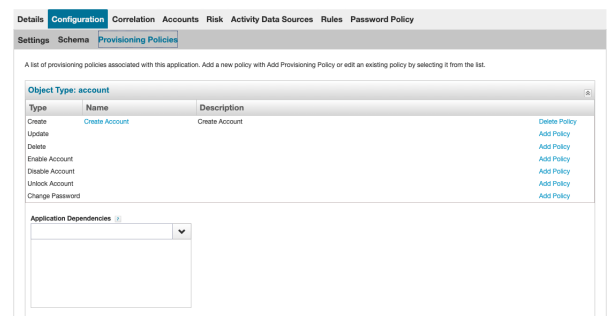
To configure the Provisioning Policy:

1. Under **Configuration**, select **Provisioning Policies**, and then click **Add Object Type**.
2. For the object type, select **Account**.

## Account

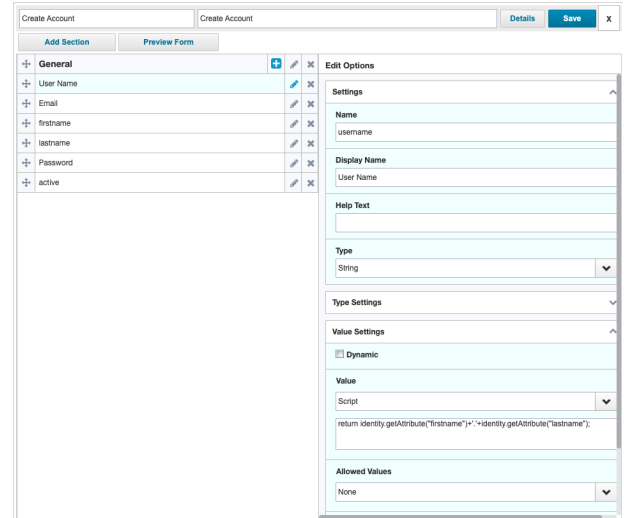
1. To add a new policy, click **Add Provisioning Policy**.
2. For **Name**, enter **Create Account**.
3. For **Description**, enter **Create Account**.

Edit Application BeyondTrust Unix & Linux



## User Name

1. Click **Add Section**, and enter **User Name**.
2. Under the **Edit Options > Settings**, enter the following:
  - a. **Name:** username
  - b. **Display Name:** User Name
  - c. **Type:** String
3. Under **Edit Options > Value Settings**, enter the following:
4. **Value:** Script
5. Type in the **script text** as follows:



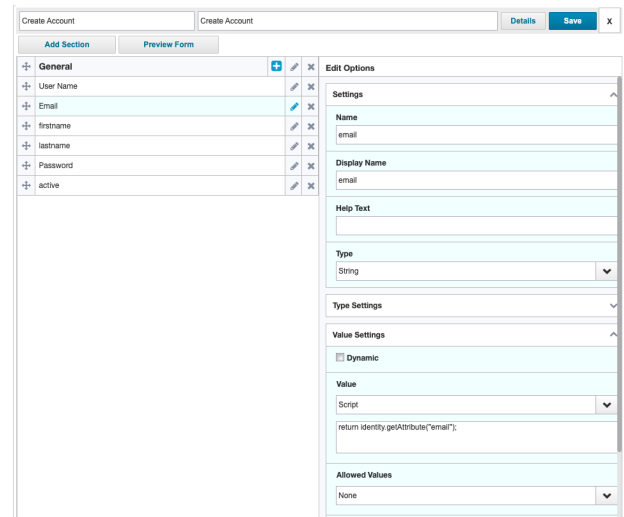
The screenshot shows the 'Create Account' configuration window. On the left, a list of sections includes 'General', 'User Name', 'Email', 'firstname', 'lastname', 'Password', and 'active'. The 'User Name' section is selected. On the right, the 'Edit Options' panel is open, showing the 'Settings' tab. The 'Name' field is set to 'username', the 'Display Name' is 'User Name', and the 'Type' is 'String'. The 'Value Settings' tab is also visible, showing the 'Value' set to 'Script' with a corresponding script text area.

```
return identity.getAttribute("firstname")+ '.' +identity.getAttribute("lastname");
```

6. **Allowed Values:** None

## Email

1. Click **Add Section**, and enter **Email**.
2. Under the **Edit Options > Settings**, enter the following:
  - a. **Name:** email
  - b. **Display Name:** email
  - c. **Type:** String
3. Under **Edit Options > Value Settings**, enter the following:
4. **Value:** Script
5. Type in the **script text** as follows:



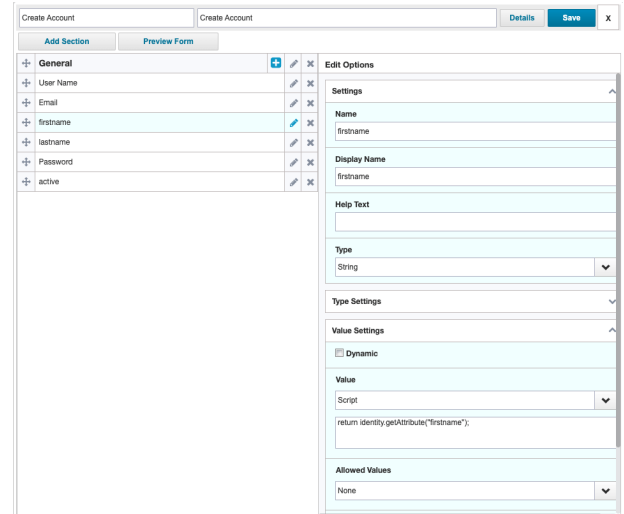
The screenshot shows the 'Create Account' configuration window. On the left, the 'Email' section is selected. On the right, the 'Edit Options' panel is open, showing the 'Settings' tab. The 'Name' field is set to 'email', the 'Display Name' is 'email', and the 'Type' is 'String'. The 'Value Settings' tab is also visible, showing the 'Value' set to 'Script' with a corresponding script text area.

```
return identity.getAttribute("email");
```

6. **Allowed Values:** None

## Firstname

1. Click **Add Section**, and enter **firstname**.
2. Under the **Edit Options > Settings**, enter the following:
  - a. **Name:** firstname
  - b. **Display Name:** firstname
  - c. **Type:** String
3. Under **Edit Options > Value Settings**, enter the following:
4. **Value:** Script
5. Type in the **script text** as follows:

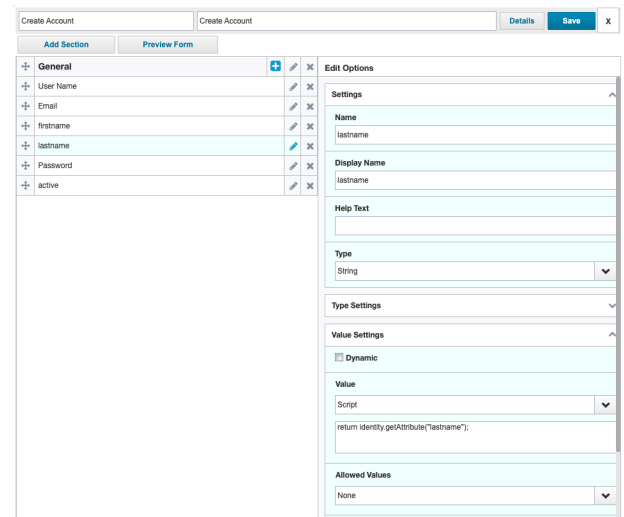


```
return identity.getAttribute("firstname");
```

6. **Allowed Values:** None

## Lastname

1. Click **Add Section**, and enter **lastname**.
2. Under the **Edit Options > Settings**, enter the following:
  - a. **Name:** lastname
  - b. **Display Name:** lastname
  - c. **Type:** String
3. Under **Edit Options > Value Settings**, enter the following:
4. **Value:** Script
5. Type in the **script text** as follows:



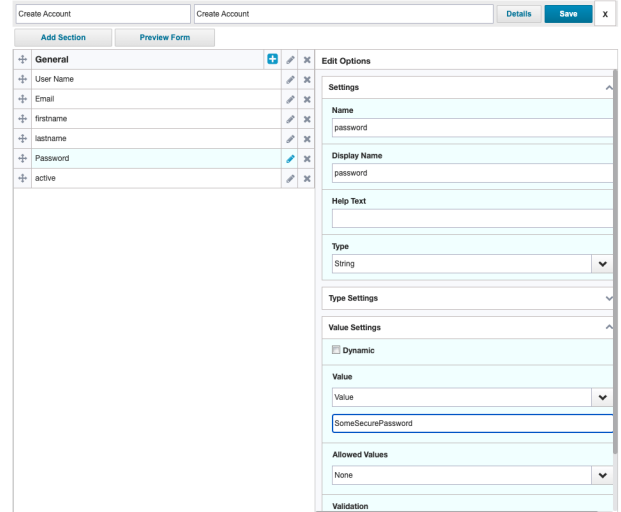
```
return identity.getAttribute("lastname");
```

6. **Allowed Values:** None

## Password

For **Password**, you can start with a *static* value, then later configure a *generated* value.

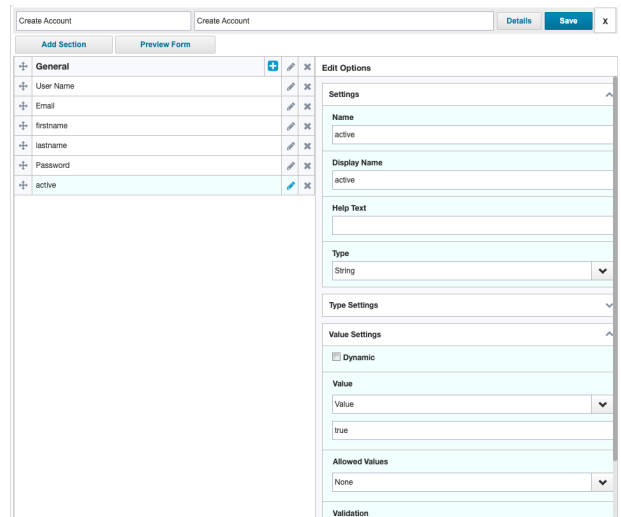
1. Click **Add Section**, and enter **Password**.
2. Under the **Edit Options > Settings**, enter the following:
  - a. **Name:** password
  - b. **Display Name:** password
  - c. **Type:** String
3. Under **Edit Options > Value Settings**, enter the following:
4. **Value:** Value
5. Type in a static value such as [SomeSecurePassword] (example only).
6. **Allowed Values:** None



The screenshot shows the 'Create Account' configuration window. The 'General' tab is active, and the 'Add Section' button has been used to add a new section named 'Password'. The 'Edit Options' panel on the right shows the 'Settings' section expanded. The 'Name' field is set to 'password', the 'Display Name' is 'password', and the 'Type' is 'String'. The 'Value Settings' section shows 'Value' set to 'Value' and 'Allowed Values' set to 'None'.

## Active

1. Click **Add Section**, and enter **active**.
2. Under the **Edit Options > Settings**, enter the following:
  - a. **Name:** active
  - b. **Display Name:** active
  - c. **Type:** String
3. Under **Edit Options > Value Settings**, enter the following:
4. **Value:** Value, and enter **true** as value.
5. **Allowed Values:** None
6. At the top right, click **Save**.



The screenshot shows the 'Create Account' configuration window. The 'General' tab is active, and the 'Add Section' button has been used to add a new section named 'active'. The 'Edit Options' panel on the right shows the 'Settings' section expanded. The 'Name' field is set to 'active', the 'Display Name' is 'active', and the 'Type' is 'String'. The 'Value Settings' section shows 'Value' set to 'Value' and 'Allowed Values' set to 'None'.

Now you should have a fully configured application. You must create Setup tasks for **Aggregating Accounts** and **Aggregating Groups** and execute those tasks.

## Accounts Created and Active

After Aggregation, under the **Application**, you can now see the **Accounts**.

| Details Configuration Correlation <b>Accounts</b> Risk Activity Data Sources Rules Password Policy                                                                                                                                                                                                                                                                                                                                                                                        |                |        |              |                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|--------|--------------|----------------|
| Filter by Name <input type="text"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                |        |              |                |
| Account ID                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Account Name   | Status | Last Refresh | Identity Name  |
| 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | admin          | Active | 8/15/23      | admin          |
| 10                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | bella.simpson  | Active | 8/15/23      | bella.simpson  |
| 11                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Carl.Marco     | Active | 8/15/23      | Carl.Marco     |
| 12                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | David.Abril    | Active | 8/15/23      | David.Abril    |
| 13                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Eric.Abril     | Active | 8/15/23      | Eric.Abril     |
| 19                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Ben.Julio      | Active | 8/15/23      | Ben.Julio      |
| 2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | jerith         | Active | 8/15/23      | jerith         |
| 20                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Aaron.Nichols  | Active | 8/15/23      | Aaron.Nichols  |
| 21                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Amanda.Pose    | Active | 8/23/23      | Amanda.Pose    |
| 22                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Alice.Ford     | Active | 8/23/23      | Alice.Ford     |
| <div> <div>active</div> <div>trun</div> <div>admin</div> <div>created 2023-08-23T19:20:03.154872487Z</div> <div>email Alice.Ford@beyondtrust.com</div> <div>externalid 0</div> <div>first_name Alice</div> <div>last_name Ford</div> <div>localisedid 22</div> <div>name Alice.Ford</div> <div>remoteid 0</div> <div>requiredGroup false</div> <div>roles policyadmin</div> <div>updated 2023-08-23T19:20:03.154872487Z</div> <div>userType 0</div> <div>username Alice.Ford</div> </div> |                |        |              |                |
| 6                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Amanda.Aspen   | Active | 8/15/23      | Amanda.Aspen   |
| 7                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Martin.Hilbert | Active | 8/15/23      | Martin.Hilbert |
| 8                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Alan.Hansen    | Active | 8/15/23      | Alan.Hansen    |

## Requestable BIUL Roles

Under **Applications > Entitlement Catalog**, you can see the **Requestable BIUL Roles**.

| Entitlement Catalog                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |           |               |       |             |               |                                     |                 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|---------------|-------|-------------|---------------|-------------------------------------|-----------------|
| Filter Entitlements <input type="text"/> Advanced Search <input type="button" value="Import"/> <input type="button" value="Export"/> <input type="button" value="Add New Entitlement"/>                                                                                                                                                                                                                                                                                                                                                                                                                                            |           |               |       |             |               |                                     |                 |
| <div> <div> <div>Application</div> <div>BeyondTrust Unix &amp; Linux</div> </div> <div> <div>Type</div> <div></div> </div> <div> <div>Attribute</div> <div></div> </div> <div> <div>Value</div> <div></div> </div> <div> <div>Owner</div> <div></div> </div> <div> <div>Effective Access</div> <div></div> </div> <div> <div>Classification</div> <div></div> </div> <div> <div>Elevated Access</div> <div></div> </div> <div> <div>Account Group Permissions</div> <div></div> </div> <div> <div>Target</div> <div></div> </div> <div> <div>Rights</div> <div></div> </div> <div> <div>Annotation</div> <div></div> </div> </div> |           |               |       |             |               |                                     |                 |
| Application                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Attribute | Display Name  | Type  | Description | Owner         | Requestable                         | Classifications |
| BeyondTrust Unix & Linux                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | roles     | accountadmin  | Group |             | Michel Buteau | <input checked="" type="checkbox"/> |                 |
| BeyondTrust Unix & Linux                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | roles     | apluser       | Group |             |               | <input checked="" type="checkbox"/> |                 |
| BeyondTrust Unix & Linux                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | roles     | auditor       | Group |             |               | <input checked="" type="checkbox"/> |                 |
| BeyondTrust Unix & Linux                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | roles     | policyadmin   | Group |             |               | <input checked="" type="checkbox"/> |                 |
| BeyondTrust Unix & Linux                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | roles     | softwareadmin | Group |             |               | <input checked="" type="checkbox"/> |                 |
| BeyondTrust Unix & Linux                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | roles     | sysadmin      | Group |             |               | <input checked="" type="checkbox"/> |                 |