Privilege Management for Unix & Linux SailPoint IdentityIQ Integration

2

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	
Account Schema	23
Group Schema	24
Provisioning Policy	25
Accounts Created and Active	29
Requestable BIUL Roles	29

3

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.

	oplications - Intelligence -	Data Governance + Setup +	\$- 0 A
it Application BevondTrust U	Jnix & Linux		
etails Configuration Correlation Acc	counts Risk Activity Data	Sources Rules Password Policy	
Indicates a required field.			
'Name 🕑		Revoker 💽	
BeyondTrust Unix & Linux			
'Owner 1		Proxy Application	
admin .	~	•	
Application Type //		Profile Class	
Description			
	English (United States)	- Scope ?	
		· ·	
		Authoritative Application 👔	
		Case Insensitive	
		Native Change Detection 🕐	
		Maintenance Enabled	
7 of 1024 characters (including markup)			
Save Cancel Reconfigure			
Seve Cancel Reconfigure			
Save Cancel Reconfigure	oplications + Intelligence +	Data Governance + Setup +	¢-0 A
Save Cancel Reconfigure Homa My Work - Identifies - Application Idit Application BeyondTrust Details Comfiguration Correlation Application	opleations - Intelligence - Unix & Linux ccounts Risk Activity Dr	Data Covernance • Betcp • ta Sources Rules Password Policy	¢- 0 A
Same Cancel Reconfigure Home My Work = Edentifies = Application didt Application BeyondTrust Details Configuration Correlation A Settings Schema Provisioning Polici Correlation A	opleations - Intelligence - Unix & Linux .ccounts Risk Activity Dr les	Data Covernance - Betcp - ta Sources Rules Password Policy	¢- 0 A
Save Cancel Recordgare More My Work - Identifyers - A (recordgare) Citit Application Beyond Trust Details Configuration Correlation A Settings Settings Schema Provisioning Policit Aid Object Type Aid Object Type	opteasons - Enterligence - Unix & Linux eccounts Risk Activity Da ies	Oida Governance × Setup × Ata Sources Rules Password Policy	¢- 0 A
Base Cancel Reconfigures Horne My Work × Genetities × Application Edit Application Beyond Trust Details Correlation A Edit Application Schema Provisioning Policit Ad Object Type Genetities × Applications	yokastora - Intelligence - Unix & Linux cocounts Risk Activity Dr iees	Data Covernance • Setup • nta Sources Rules Password Policy	¢- 0 ≰
Bane Cancel Reconfigury Homo My Work Kertitives Application Edit Application Beyond Trust Details Correlation A Settings Schema Provisioning Policitization Correlation A Act Object Type General Settings Settings Settings Settings	colosions Medigence - Unix & Linux accounts Risk Activity Dr Jees	Data Governance • Betty • ta Sources Rules Password Policy	0+ 0 ▲
Energy Cancel Reconfigure More My Work - Kentities - Application Edit Application BeyondTrust Details Configuration Correlation Application Details Configuration Correlation Application Correlation Application General Settings General Settings Base URL * () Base URL * () Base URL * ()	opfestion • Intelligence • Unite & Linux accounts Risk Activity Do ies	Data Covernance • Setup • ta Sources Rules Password Policy	0 ∙ 0 ▲
Enne Cancel Reconfigure More My Work - Kderkthes - Application Bottalls Configuration Correlation A Sectings Bottalls Configuration Correlation A Sectings General Sectings Schema Provisioning Policition Add Deject Type	pyloations • Intelligence • Unit: & Linux accounts: Risk: Activity De ies https://mystu.coudis5000/ 	Data Convenance - Satup - Ita Sources Rules Password Policy	0 + 0 ▲
Base Cancel Reconfigures Item My Work Gardtille + A Edit Application BeyondTrust Details Correlation A Settings Schema Provisioning Policit General Settings General Settings Base UTL * / Base UTL * / A	colosion · Intelligence · Unix & Linux accounts Risk Activity Da ies	Data Governance • Setup • ta Sources Rules Password Policy	0 0 ▲
Base Cancel Reconfigury More My Work Kertitikes Application Edit Application BeyondTrust Details Configuration Correlation A Settings Schema Provisioning Pedici A General Settings Base URL * · · · Authentication Memod* · ; Authentication Memod* · ; Authentication Memod* · ; Authentication Memod* · ;	cplosions • Intelligence • Unix & Linux accounts Risk Activity Dr ies https://myotu.coud.55082/ Okuma Okuma Okuma Mittokan	Data Governance • Betty • ta Sources Rules Password Policy	0 + 0 ▲
Energy Cancel Reconfigure More My Work - Kentities - Application Edit Application BeyondTrust Details Configuration Correlation Application Details Configuration Correlation Application Correlation Application General Settings Base URL * 1/2 Base URL * 1/2 Authentication Method * 1/2	opfestion V Intelligence - Unitx & Linux counts Risk Activity De fes https://mystu.cloud.t5082// Outure O	Data Covernance • Batop • ta Sources Rules Password Policy	0 ∙ 0 ▲
See: Cascel Reconfigure Nom My Work * Genetities * Application Edit Application BeyondTrust Details Configuration Correlation A Settings Schema Provisioning Policit Add Opter Type Base URL * // General Settings Base URL * // Add Opter Type Base URL * // Schema Attribute for Account Truste account Schema Attribute for Account Truste account	pploations • Intelligence • Unix & Linux accounts Risk Activity Dr less https://mydtu.cloud.ts8088// OAunt2 OAunt2 OAunt2 OAunt2 Mit Authentication Biola Authentication Biola Authentication Extre	Data Covernance • Setup • Ita Sources Rules Password Policy	¢• 0 ▲
Base Cancel Reconfigures Ikon My Work Karelska v. A Edit Application BeyondTrust Details Correlation A Edit Application BeyondTrust Details Correlation A Add Departs Provisioning Policit A Details Correlation Add Departs Base URL * / / Authentication Method * / Details Schema Attribute for Account Enable Schema Attribute for Account Enable Details Schema Attribute for Account Enable Details	Distrigence - Unix & Linux accounts Risk Activity Dr ies Therefore Ordune	Data Covernance • Betty • tta Sources Rules Password Policy up1	0 • 0 ▲
Energy Cancel Recentiguey More My Work Keetslike or Application Edit Application BeyondTrust Correlation A Edit Application RespondTrust Correlation A Mattings Schema Provisioning Polici Autorecation Memod* Authentication Memod* Schema Attribute for Account Trustes Schema Attribute for Account Trustes Behama Attribute for Account Trustes Schema Attribute for Account Trustes Schema Attribute for Account Trustes	colosion Netificance - Unix & Linux accounts Risk Activity Dr ies https://myttu.cloud.58082/ Owner Art Totan @ Net Custom Authentication # Net Custom Authentication active	Data Governance • Betsp • ta Sources Rules Password Policy api	0 ← 0 ▲
See Casci Reconfigury Norm Ny Work Statement Variant Statement Configuration Configuration	opfications > Intelligence - Unit: & Linux accounts Risk Activity Do less >https://mythu.cloud.58082/0 Owner Owner Owner Martinaan Basic Automitication active	Data Convenance • Setup • tta Sources Rules Password Policy	¢• 0 ▲

4

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.

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

Edit Application BeyondTrust Unix & Linux

tings Schema Pro	visioning Policies		
Add Object Type			
Back Connection	Settings		
Enable cURL 🔻 🗌			
Authentication URL		Method 💽	
Authentication URL : https://mybtu.cloud:	58082/api/v1/auth/login	Method 1 POST	
Authentication URL 2 https://mybtu.cloud: Header	58082/api/v1/auth/login Header	Method T POST	Add Row
Authentication URL 2 https://mybtu.cloud: Header Body	58082/api/v1/auth/login Hesder Key	Method y POST	Add Row
Authentication URL : https://mybtu.cloud: Header Body Response	8082/api/V1/auth/login Header Key Accept	Method II POST Value icorcation/pon	Add Row

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.

Add Object Tons			
Back Connection Se	ettings		
Enable cURL 💿 🗌			
Authentication URL		Method 2	
https://mybtu.cloud:58	3082/api/v1/auth/login	POST	
Header	Body		
Body			
Response	⊖ form-data® raw		
	("domain":"","dsDomain":"","dsID":0,	password1:"\$application.password_CA\$*,"username1:"admin"}	

5

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

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

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.

≔	Home	My Work 👻	Identities +	Applications +	Intelligence +	Data Govern	nance +	Setup +	۰.	04	1	÷
E	dit Ap	plication B	eyondTru	st Unix & L	inux							
	Details	Schema P	Correlation	Accounts Ri	sk Activity Da	ata Sources	Rules P	Password Policy				
	outings	ounonia 1.	i i i i i i i i i i i i i i i i i i i									1.
	Add O	Object Type										
	Ba	ack Connectio	n Settings									
	Enable	le cURL 💿 🗌										
	Authe	intication URL 💽					Method 💌					
	http	ps://mybtu.cloud	1:58082/api/v1/a	iuth/login			POST				~	
		Header	Response	e Attribute Mappin						Add R	low	
		Body	Response	Attribute Key 💿			Response	e Attribute Value Path				
		Hesponse	accession	ien_GA			\$.token			ж		
			XPath Na	mespace Mapping	(For XML web ser	vices)				Add R	low	
			Root Pati									
			Successi	ul Response Code	T							
			200									
										Cancel	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.



6

<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"/>

^{©2003-2023} BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 11/17/2023 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

- 5. You also must add the value for key(password), as written below.
- 6. Click Save.
- 7. Close the /debug interface.



<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.

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.

tinge Cohoma De	ovisioning Polision	Activity Data Oblices	Tures	T assessed T only		
ungs ocherna Pro	ovisioning Policies					
Add Object Type						
the order the						
Back Connection	Settings					
Enable cURL 💽 🗌						
Context URL 💽			Method	1		
Arthreere/memorie us	0.040		OFT			
TTTT addet ar get terro_at	9019		GET			
Header	Mandar		GET		Add F	Row
Header	Header		GET		Add F	Row
Header Body Besparse	Header		Value		Add F	Row
Header Body Response	Header Key Authorization		Value Bearer	Sapplication.accesstoken_CA\$	Add F	Row
Header Body Response Before Rule	Header Key Authorization Accept		Value Bearer applice	\$application.accesstoken_CA\$ ation/son	Add F	Row
Header Body Response Before Rule After Rule	Hesder Key Authorization Accept		Value Bearer applica	\$application.accesstoken_CA\$	Add F	Row

7

Edit Application BeyondTrust Unix & Linux

Response

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

Edit Application BeyondTrust Unix & Linux

Details Configuration C	orrelation Accounts Ris	k Activity Data Sources	Rules Password Policy	
Settings Schema Prov	sioning Policies			
Add Object Type				
Back Connection Se	ttings			
Enable cURL 👔 🗌				
Context URL 💽			Method 👔	
/v1/users/generic_user	8		GET	~
Header	Response Attribute Mapping			Add Row
Body				
Response	XPath Namesnace Manning I	For XMI web services)		Add Row
Before Rule				
After Bule	Root Path 👔			
	Successful Response Code	2		
	200			
				Cancel Save

Edit Application BeyondTrust Unix & Linux

General Settin	ings							~ ^
	Base URL * 💽	https://	/mybtu.cloud:58082/api					
Au	thentication Method * 🕐	O OAu	th2					
			Token					
		O Basi	ic Authentication					
		🖲 No /	Custom Authentication					
Schema At	ttribute for Account Enable status	active						
	1							
Description								
Fnable Client	t Timeout (in Seconds)							
Enable Client	t Timeout (In Seconds) 💿							
Enable Client	t Timeout (in Seconds) ()						Add O	peration
Enable Client Connector Op Order	Timeout (in Seconds)) Certificate Authentication) perations Operation		Name	Status	Before Rule	After Rule	Add O Actions	peration
Connector Op Order	Trimeout (in Seconds) Certificate Authentication peretitions Operation Custom Authenticati	ion v	Name Authentication	Status Configured	Before Rule	After Rule	Add O Actions	peration
Connector Op Order	Creation Coperation Custom Authentication Custom Authentication	ion v	Name Authentication	Status Configured	Before Rule	After Rule	Add O	peration
Connector Op Order	Trmeout (in Seconds) () Certificate Authentication () Certificate Second (i) () Certains Custom Authenticati Custom Authenticati Test Connection	ion v	Name Authentication Test Connection	Status Configured Configured	Before Rule	After Rule	Add O	peration 30
Connector Op Order	Treneout (in Seconda) Certificate Authentication 2 2 peration Custom Authenticat Custom Authenticat Test Connection		Name Authentication	Status Configured	Before Rule	After Rule	Add O	peratiken

8

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.

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs



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.
- 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.

itext URL 👔		Method 2	
v1/users/generic_u	sers	GET	
Header	Header		Add Row
Body	Mari	Maker	
Response	Authorization	Reser Semilation second ken CAS	
Before Rule	A		~
After Rule	Accela	appicatoryson	~
Paging			
Darrent Endopiet			

9

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.

ntext URL 📷		Method 💌	
/v1/users/generic_us	ers	GET	
Header	Besponse Attribute Manning		Add Row
Body			
Response	Schema Attribute	Attribute Path >	
Before Rule	Instrame	nistriame	
After Rule	created	created	×
Paging	roles	roles["].rolename	×
Parent Endpoint	active	active	×
	admin	admin	x
	an	cn	×
	requiresGroup	requiresGroup	×
	lastname	lastname	×
	peth	path	×
	externalApiID	externalApiID	×
	name	name	×
	guid	guid	×
	remoteUserID	remoteUserID	×
	userType	userType	×
	localLiserID	locali keciD	×
	undefield	undated	
	amai	amil	
	eritali	ema	
	usemame	username	~
	XPath Namespace Mapping (For XML web	services)	Add Row
	Boot Path		
	\$ Data		
	w. Data		h
	Successful Response Code 👔		

depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

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.
- 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.

ings Schema Pro	visioning Policies		
Add Object Type			
Back Connection	Settings		
Enable cURL 💿 🗌			
Context URL 💿		Method :	
/v1/auth/roles		GET	
Header	Mandan		Add Bow
Body	Heaver		
Response	Key	Value	
Before Rule	Authorization	Bearer \$application.accesstoken_CA\$	×
After Rule	Accept	application/json	×
Paging			
Parent Endpoint			

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.

Details Configuration	Correlation Accounts Risl	Activity Data Sources	Rules Password Policy	
Settings Schema Prov	visioning Policies			
Add Object Type				
Back Connection S	ettings			
Enable cURL 💌 🗌				
Context URL 💽			Method 2	
/v1/auth/roles			GET	~
Header	Response Attribute Mapping			Add Row
Body	Rohama Attribute		Attribute Bath	
Response	rojename		miename	×
Before Rule				
After Rule	XPath Namespace Mapping (F	or XML web services)		Add Row
Paging				
Parent Endpoint	Root Path 💽			
	Successful Response Code			
	200			
				Cancel Save

11

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

tails Configuration	Correlation Accounts R	isk Activity Data Sources	Rules Password Policy	
ttings Schema Pr	visioning Policies			
Add Object Type				
Back Connection	Settings			
Enable cURL 💌 🗌				
Context URL 💽			Method 🕑	
/v1/users			POST	~
Header	Header			Add Row
Body	Key		Value	
Response	Authorization		Bearer Sapplication.accesstoken_CAS	×
Before Rule	Content-type		application/json	×
After Rule	Accept		application/son	×
				Cancel
				Carrol Carro

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

tails Configuration	Correlation Accounts	Risk Activit	y Data Sources	Rules	Password Policy	
ttings Schema Pro	visioning Policies					
Add Object Type						
Back Connection S	iettings					
Enable cURL 💿 🗌						
Context URL 💿				Method	7	
/v1/users				POST		
Header	Body					
Body	form data any					
Response	C form-Galas Taw					
Before Rule	f factive": Solan act	ivo\$				
After Rule	"email": "\$plan.em	all\$",				

12

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

^{©2003-2023} BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 11/17/2023 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

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.

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 & Linux

Edit Application BeyondTrust Unix & Linux

etails Configuration	Correlation	Accounts	Risk	Activity Data Sources	Rules	Password Policy			
ttings Schema Pro	visioning Po	licies							
Add Object Type									
Back Connection	Settings								
Enable cURL 💽 🗌									
Context URL 👔					Method	F			
/v1/users/\$plan.nath	veldentity\$/role	s/\$plan.roles	\$		PUT				
Header	Header							Add Row	
Body					Malua				
Response	Ney				Value	familiarity annuality CAR		**	
Before Bule	Autorizat	ion			Dearer	sapprozoon.zoonszown_oxs		~	
After Rule	Accept				appeca	lborvjson		*	
							Can	cet	Silve

13

©2003-2023 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or	TC: 11/17/2023
depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.	

etails Configuration ettings Schema Pro	Correlation Accounts Risk Activity Data Source ovisioning Policies	es Rules Password Policy	
Add Object Type Back Connection	Settings		
Enable cURL 💿 🗌		Method 🦻	
/v1/users		POST	~
Header	Bessense Attribute Manalan		Add Bow
Body	Schema Attribute (2)	Attribute Path	
Response	firstname	firstname	×
Before Rule	roles	rolesi"].rolename	×
After Rule	active	active	26
	admin	admin	×
	remoteUserID	remoteUserID	×
	localUserID	D	×
	email	email	×
	lastname	lastname	×
	username	username	×
	XPath Namespace Mapping (For XML web services)		Add Row
	Root Path 👔		
	Successful Response Code 💿		
	2**		
			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.

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

Edit Application BeyondTrust Unix & Linux

etails Configuration	Correlation	Accounts	Risk	Activity Data Sources	Rules	Password Policy			
ettings Schema Pro	visioning Poli	cles							
Add Object Type									
Back Connection	Settings								
Enable cURL 2					Method				
/v1/users/\$plan.nativ	eldentity\$/roles	/\$plan.roles/	5		DELE	TE			
Header	Header						~	id Row	
Body	Key				Value				
Response	Authorizatio	m			Bearer	\$application.accesstoken_CA\$	х		
Before Rule	Accept				applica	don/json	×		
After Rule									
							0		-

14

SALES: www.beyondtrust.com/contac	SUPPORT: www.beyondtrust.com/support	DOCUMENTATION: www.beyondtrust.com/docs
-----------------------------------	--------------------------------------	---

and Object Taxe	summing, and a		
and Object Type			
Back Connection	Settings		
nable cUBL 📧 🗌			
Content 1971		Method (9)	
Ad Assem/Rolan path	aldeatit & wales & ales wales	Method 2	
/vi/usela/apidit.ttauv	render nit yan oriesraphian noriesa	Pol	
Header	Response Attribute Mapping		Add Row
Body	Schema Attribute	Attribute Path	
Response	firstname	firstname	36
Before Rule	roles	roles("].rolename	×
After Rule	active	active	×
	admin	admin	×
	remoteUserID	remoteUserID	×
	localUserID	localUserID	×
	email	email	×
	lastname	lastname	×
	username	username	36
	XPath Namespace Mapping (For XML web services	0	Add Row
	Boot Path		
	Successful Response Code 3		6
	014		

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.

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 Ap	plication B	eyondTru	st Unix &	Lin	шх		
Details	Configuration	Correlation	Accounts	Bisk	Activity Data Sources	Bules	Password Policy

dd Object Type			
Back Connection	Settings		
inable cURL 💿 🗌			
Context URL 💿		Method 💿	
/v1/users/\$plan.nat/	veldentity\$/roles/\$plan.roles\$	DELETE	
Header	Response Attribute Mapping		Add Row
Body	Reference Attribute	Andreas Park an	
Response	Schema Attribute :	Attribute Path >	
Before Rule	- Inschame	manane minetti minome	~
After Rule	roles	roesi proetane	~
	active	active	
	admin	aomin	
	remoteusenD	remoteusenu	
	iocal UseriD	locausenu	
	emai	emai	
	lastname	lastname	×
	usemame	username	×
	XPath Namespace Mapping (For XML w	ab services)	Add Row
	Root Path 🦻		
	Successful Response Code 🗵		
	2**		

Edit Application BeyondTrust Unix & Linux

tails Configuration	Correlation Accounts	Risk Activity Data S	ources Rules Password Policy	
tings Schema Pr	ovisioning Policies			
Add Object Type				
Back Connection	Settings			
Enable cURL 💽 🗌			Method 1	
/v1/users/\$plan.nati	/eldentity\$		GET	
Header	Header			Add Row
Body	Key		Value	
Response	Authorization		Bearer \$application.accesstoken_CA\$	34
Balana Dola	Accept		application/json	×
before hale				
After Rule				

15

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

Response

- 1. Select Response.
- 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.

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.

Id Object Type	Sattians		
Back Commeteou	Gettinga		
able cURL 👔 🗆			
ontext URL 💽	un la la cantila di	Method 2	
/vi/users/spian.nau	verdemitys	GET	
Header	Response Attribute Mapping		Add Row
Body	Schema Attribute	Attribute Path	
Response	firstname	firstname	×
Before Rule	roles	roles["].rolename	×
After Rule	active	active	×
	admin	admin	×
	remoteUserID	remoteUserID	×
	localUserID	localUserID	×
	email	email	×
	lastname	lastname	ж
	username	username	ж
	XPath Namespace Mapping (For XML w	ab services)	Add Row
	Root Path 2		
	Successful Response Code 👔		

Edit Application BevondTrust Unix & Linux

Edit Application BeyondTrust Unix & Linux

tings Schema Pr	ovisioning Pol	licies					
Add Object Turne							
And colect type							
Back Connection	Settings						
Easthin still -							
Enable cURL 💌 🗌							
Enable cURL 💌 🗌				Method			
Enable cURL Context URL Av1/users/\$plan.nati	veldentity\$			Method PUT	5		
Enable cURL () Context URL () /v1/users/\$plan.nati Header	veldentity\$ Header			Method PUT	8	Add Row	
Enable cURL 2 Context URL 2 Art/users/\$plan.nati Header Body	Header			PUT	0	Add Row	
Enable cURL 🔋 🗌 Context URL 🔋 Art/users/\$plan.nati Header Body Response	Header Key			Method PUT Value	8	Add Row	
Enable cURL	Header Key Authorizati	on		Method PUT Value Bearer	Sepplication accessiblen_CA\$	Add Row	
Enable cURL 2 Context URL 2 Context URL 3 V1/users/\$plan.nati V1/users/\$plan.nati Header Body Response Before Rule	Header Key Authorizati Accept	on		Value Bearer applice	sapptcation.accesstoken_CA\$	Add Row	

16

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

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

Details Configuration	Correlation Accounts Risk Activity Data	Sources Rules Password Policy	
Settings Schema Pro	visioning Policies		
Add Object Type			
Back Connection 5	iettings		
Enable cURL 🝸 🗌			
Context URL		Method 💌	
/v1/users/\$plan.nativ	eldentity\$	PUT	~
Header	Body		
Body	o form-data® raw		
Response			
Before Rule	"username": "\$response.username\$".		
After Rule	"email": "\$response.email\$",		
			Gancel Save

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

Response

- 1. Select Response.
- 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

dd Object Type			
Back Connection	Settings		
nable cliBL .			
Context LIDI		Method a	
/v1/users/Splan path	alcientitu\$	PLIT	
Header	Response Attribute Mapping		Add Row
Body	Schema Attribute	Attribute Path 3	
Response	firstname	firstname	×
Before Rule	roles	roles(").rolename	×
After Rule	active	active	×
	admin	admin	×
	remoteUserID	remoteUserID	×
	localUserID	localUserID	×
	email	email	×
	lastname	lastname	x
	username	username	ж
	XPath Namespace Mapping (For XML web services)		Add Row
	Root Path 2		
	Successful Response Code 👔		

17

^{©2003-2023} BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 11/17/2023 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

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

ings Schema Pr	ovisioning Polici	95					
Add Object Type							
Back Connection	Settings						
Enable cURL 👔 🗌							
Context URL 💽				Method	2		
Context URL 💽 /v1/users/\$plan.nati	veldentity\$			GET	2		
Context URL 💽 /v1/users/\$plan.nati Header	veldentity\$			GET	2		Add Row
Context URL () /v1/users/\$pian.nati Header Body	Header			Method GET Value	2		Add Row
Context URL () /v1/users/\$pian.nati Header Body Response	Header Key Authorization			Method GET Value Bearer	8 Sapplication.accesstoken, CAS		Add Row
Context URL Cut/users/\$plan.nati Header Body Response Before Rule	Header Key Authorization Accept			Method GET Value Bearer applic	3 Sapplication.accesstoken, CAS tition/json		Add Row K
Context URL /v1/users/\$plan.nati Header Body Response Before Rule After Rule	Header Header Key Authorization Accept			Method GET Value Bearer applic	3 Sapplication.accesstoken, CAS titorition	3	Add Row K

Response

- 1. Select Response.
- 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

gs Schema Pro	vvisioning Policies		
Back Connection	Settings		
able cURL 💽 🗌			
ntext URL 💽		Method 💌	
v1/users/\$plan.nativ	veldentity\$	GET	
Header	Deserves Michaels Manalas		Add Row
Body	Response Attribute Mapping		
Response	Schema Attribute 😨	Attribute Path 🦻	-
Before Rule	trstname	hrstname	
After Bule	roles	roles[].rolename	
	active	active	<u>x</u>
	admin	admin	×
	remoteUserID	remoteUserID	×
	localUserID	localUserID	×
	email	email	26
	lastname	lastname	×
	username	username	×
	XPath Namespace Mapping (For XML web set	rvices)	Add Row
	Root Path 👔		
	Successful Response Code 👔		6
	200		

18

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

tings Schema Pr	ovisioning Policies	HISK ACTIVITY Data Soc	roes rules rassword rolloy	
Add Object Type				
Back Connection	Settings			
Enable cURL 💿 🗌				
Context URL 💽			Method :	
/v1/users/\$plan.nati	veldentity\$		PUT	
Header	Header			Add Row
Header Body	Header		Value	Add Row
Header Body Response	Header Key Authorization		Value Bearer Sapplication.accesstoken_CAS	Add Row
Header Body Response Before Rule	Header Key Authorization Accept		Value Betrer Sapplication.socesstoken_CAS septication/pon	Add Row

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

tails Configuration	Correlation Accounts Risk Activity Dat	Sources Rules Password Policy	
ttings Schema Pr	ovisioning Policies		
Add Object Type			
Back Connection	Settings		
Enable cURL 👔 🗌			
Context URL 👔		Method 👔	
/v1/users/\$plan.nati	veldentity\$	PUT	
Header	Body		
Body			
Response	o form-data® raw		
Before Rule	<pre>{ "username": "\$response.username\$",</pre>		
After Rule	"email": "\$response.email\$",		

19

"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.

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

	Correlation Accounts hisk Activity Data Sou	ces nues rassword rolley	
attings Schema Pro	ovisioning Policies		
Add Object Type			
Back Connection	Settings		
0			
Enable CORL 🕐 🕒			
Context URL		Method 🗵	
/v1/users/splan.nativ	veidentitys	PUT	Ŷ
Header	Response Attribute Mapping		Add Row
Body	Schams Attribute (1)	Attribute Path (1)	
Response	firstraine	firstname	2
Before Rule	roles	roles!"L/olename	x
After Rule	active	active	×
	admin	admin	×
	remoteUserID	remoteUserID	×
	localUserID	localUserID	×
	email	email	×
	lastname	lastname	×
	usemame	username	×
	XPath Namespace Mapping (For XML web services)		Add Row
	Root Path 👔		
			4
	Successful Response Code 2		
	200		
			Cancel Save

Edit Application BeyondTrust Unix & Linux

Add Object Type			
Back Connection	Settings		
Enable cURL 👔 🗌			
Context URL 💽		Method 💽	
/v3/users/\$plan.nati	veldentity\$/password	PUT	
	Handar		Add Row
Header	Header		
Header Body	Key	Value	
Header Body Response	Key Authorization	Value Bearer \$application.accesstoken_CA\$	*
Header Body Response Before Rule	- Key Authorization	Value Bears Sapplication.accesstoken_CAS	X

20

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

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

Details Configuration Co	orrelation Accounts Risk	Activity Data Sources	Rules Password Policy		
Settings Schema Provis	sioning Policies				
Add Object Type					
Back Connection Set	tings				
Enable cURL 💿 🗌					
Context URL 💿			Method T		
/v3/users/\$plan.nativelo	lentity\$/password		PUT		~
Header	Body				
Body	form-data? raw				
Response	Channe and a state of				
Before Rule	{ new_password : aprant	Asseworde }			
After Rule					
				Cancel	Save

{"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.

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.

Edit Application BeyondTrust Unix & Linux

Add Object Type			
Back Connection	Settings		
Enable cURL 💌 🗌			
Context URL 👔		Method 2	
/v3/users/\$plan.nativ	eldentity\$/password	PUT	
Mandar			Add Down
Body	Response Attribute Mapping		Page 100
Besponse	Schema Attribute 💽	Attribute Path 💽	
Before Bule	firstname	firstname	×
Atter Pula	roles	roles[1].rolename	20
Pilot Halo	active	active	×
	admin	admin	×
	remoteUserID	remoteUserID	26
	localUserID	localUserID	×
	email	email	×
	lastname	lastname	×
	usemame	username	×
	XPath Namespace Mapping (For XML web services)		Add Row
	Root Path 👔		
	Successful Response Code 👔		
	200		

21

Header

1. Select Header.

BeyondTrust

- 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

Settings Schema Provisio	ning Policies			
Add Object Type				
Back Connection Setting	gs			
Enable cURL 💿 🗌				
Context URL 1		Method 💿		
/v3/users/\$plan.nativelden	tity\$/lock	DELETE		~
Header	Header			Add Row
Body	Key	Value		
Response	Authorization	Bearer \$app	plication.accesstoken_CA\$	×
Before Rule	Accept	application/)	(json	×
After Rule				
				Cancel

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.

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.

Edit Application BeyondTrust Unix & Linux

dd Object Type			
Back Connection	Settings		
inable cURL 💿 🗌			
ontext URL 💽		Method 📧	
/v3/users/\$plan.nativ	reldentity\$/lock	DELETE	
Header			
Body	Response Attribute Mapping		ADD HOW
Besoonse	Schema Attribute 💽	Attribute Path 📧	
Before Rule	firstname	firshame	×
After Rule	roles	roles["].rolename	×
	active	active	×
	admin	admin	26
	remoteUserID	remoteUserID	24
	localUserID	localUserID	×
	email	email	×
	lastname	lastname	×
	usemame	username	ж
	XPath Namespace Mapping (For XML web services)		Add Row
	Read Date 19		
	NOOL PAUL I		
	Successful Response Code 👔		

22

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 C	orrelation Accounts Ris	k Activity Data Sources	Rules Password Policy	
Settings Schema Provi	sioning Policies			
Add Object Type				
Back Connection Se	ttings			
Enable cURL 👔 🗌				
Context URL			Method 1	
/v1/users/\$plan.nativel	dentity\$		DELETE	~
Header	Header			Add Row
Body	Key		Value	
Response	Authorization		Bearer \$application.accesstoken_CA\$	×
Before Rule	Accept		application/json	×
Alter Hale				
				Gancel Save

Response

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

dit Applicatio	n Beyona	Trust Unix	& Linux

ettings Schema Pr	ovisioning Policies		
Add Object Type			
Back Connection	Settings		
Enable cURL 👔 🗌			
Context URL 💽		Method 💿	
/v1/users/\$plan.nati	veldentity\$	DELETE	v
Header	Response Attribute Mapping		Add Row
Body			
Response	XPath Namespace Mapping (For XML web ser	vices)	Add Row
Before Rule			
After Rule	Root Path 👔		
	Successful Response Code 👔		
	2**		
			Control
			Gancer

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
 - I. 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

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.

ails ting	Schema Provisioning Policies	ounts Risk Activity Data Sources	Rules Password Polic	y		
Obie	ect Type: account					
	ule					
/010	ina					
Nati	ive Object Type	Display Attribute				
LISER	ſ	usemame				
Ider	ntity Attribute	Instance Attribute				
attri	butes	Remediation Modifiable Readonly ~				
	Name	Description	Туре	Properties		
0	localUserID	localUserID	string v			
					•	Ed
0	username	username	string v		~	
					-	
	name	name	string V		٠	Ed
	remoteUserID	remoteUserID	string v			
					*	Ed
	active	active	boolean v		•	Ed
п	created	created	string			
					•	Ed
0	updated	updated	string 🗸			l.
					- *	1
0	emai	email	string V		\$	Ed
0	firstname	firstname	string ~			
					*	Ed
	lastrame	lastname	string v		•	Ed
_	admin	admin	honlass of			
			Coonair •		•	Ed
	roles	roles	group 🗸	Managed, Entitlement, Multi-Valued		Į,
					•	1
Π.	externalApIID	externalApiID	string v		•	Ed
0	auid	auld	string v			
	C				•	Ed
0	path	path	string v			
						ĩ
	cn	cn	[string ∨		٠	Ed
	userType	userType	string ~			
					•	Edi

24

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

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 Provisionig 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

ype	Name			
		C	Description	
reate	Create Account	Cr	ireate Account	Delete Policy
pdate				Add Policy
elete				Add Policy
hable Account				Add Policy
sable Account				Add Policy
nlock Account				Add Policy
hange Password	d			Add Policy
Application Dep	pendencies 👔			

25

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

Native Object Type	Display Attribute			
group	rolename			
Identity Attribute	Instance Attribute			
rolename				
Description Attribute	Remediation Modifiable			
	Readonly ~			
Name	Description	Туре	Properties	
	and a manufacture of the second se	string 🗸		A.2
rolename	loenarie			
D polename	Puerta ne			
Add New Schema Attribute Delete Sch	ema Attribute			
Add New Schema Attribute Delete Sch	ema Attribute			

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:

	ate Account		Create Account				Details Save	,
	Add Section	Preview Form						
÷	General			0	ø	×	Edit Options	
÷	User Name				1	×	Settings	
÷	Email				ø	×		
÷	firstname				ø	×	Name	
÷	lastname				ø	×		
÷	Password				ø	×	Display Name	
÷	active				ø	×	User Name	
							Туре	
							Type String Type Settings	•
							Type String Type Settings Value Settings	•
							Type Sting Type Settings Unkue Settings Dynamic	•
							Type Sting Type Settings Unlue Settings Dynamic Value	•
							Type Sting Type Settings Dynamic Value Sorgt	•
							Type String Type Settings Value Settings Opmamic Value Script	•
							Type Settings Type Settings Value Settings Opmmic Value Sorigt return Sentity get/Attribute("finahame")="-"identity get/Attribute["lashname"): Allowed Values	•

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:



26

return identity.getAttribute("email");

6. Allowed Values: None

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

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:

	10 A000011		Create Account			Details	Save	1
	Add Section	Preview Form						
÷	General		÷	ø	×	Edit Options		
÷	User Name			ø	×	Settions		
÷	Email			ø	×			
÷	firstname			1	×	Name		
÷	lastname			ø	×			
÷	Password			ø	×	Display Name		
ŀ	active			ø	×	firstname		
						7		
						Type String Type Settings Value Settings		
						Type Song Type Settings Value Settings Oynamic Value		
						Type String Type Settings Value Settings Opramic Value Sorgt		
						Type String Type Settings Usus Settings Opmanis Vulue Softy return dentity get/Attrbute("finitianar"):		
						Type String Type Settings Wake Settings Dynamic Vibue Sorgt: return identity get/Attribute("finitianer"); Allowed Values		

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:



27

return identity.getAttribute("lastname");

6. Allowed Values: None

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

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

Cre	aate Account		Create Account				Details	Save	
	Add Section	Preview Form							
÷	General		•	ø	×	Edit Options			
÷	User Name			ø	ж	Settings			
÷	Email			ı	×	Heres			
÷	firstname			1	х	name			
÷	lastname			ſ	х	potonia			
÷	Password			1	×	Display Name			
÷	active			ø	×	password			
						String Type Settings Value Settings Dynamic			•
						Value			
						Value			•
						SomeSecurePassword			
						Allowed Values			
						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.

Freate A	Account		Create Account					Details	Save	
A	dd Section	Preview Form	n							
Ge	eneral			•	ø	×	Edit Options			
Use	er Name				ø	×	Settings			
Ema	nail				ø	×	Nama			
ŀ first	tname				ø	×	active			
lasti	tname				ø	×				
Pas	ssword				ø	×	Display Name			
l+ acti	tive				ø	×	active			
							Type String			•
							Type String Type Settings			
							Type String Type Settings Value Settings			•
							Type String Type Settings Value Settings Dynamic			
							Type Soling Type Settings Value Settings Opmanic Value			•
							Type Soring Type Settings Value Settings Opramic Value Value			•
							Type Soring Type Settings Value Settings Utable Value Utable Tube			
							Type String Type Settings Value Settings Utable Value True Allowed Values			
							Type Soling Type Settings Usitue Settings Usitue Settings Value Value True Allowed Values			

28

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 Con	relation Accounts Risk A	Activity Data Sources Rule	Password Policy	
Filter by Name	Q			
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.Marzo 🖌	 Active 	8/15/23	Carl.Marzo
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	BenJulio
2	jamith 🗸	 Active 	8/15/23	jsmith
20	Aaron.Nichols 🗸	 Active 	8/15/23	Aaron Nichols
21	Amanda.Ross 🗸	 Active 	8/23/23	Amanda Ross
22 active that act	NosFad A	Active	823/23	Also Ford
6	Amanda.Aspen 🗸	Active	8/15/23	Amanda.Aspen
7	Martin.Hilbert 🗸	Active	8/15/23	Martin, Hilbert
8	Alain Hanson 🐱	Active	8/15/23	Alain Hanson

Requestable BIUL Roles

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

Filter Entidements		Q,	Advanced S	earch				Import Export	Add New Entitlem
Standard Attribute									
Application B		BeyondTrust Unix & Linux 🛛 🗸			Classification		~		
Туре			*			Elevated Access		*	
Attribute				*		Account Group Perm	issions		
Value				~		Target			
Owner				~		Rights			
Effective Access						Annotation			
									Search Re
Application	Attribute		Display Na	me	Туре	Description	Owner	Requestable	Classifications
BeyondTrust Unix &	roles		accountade	nin	Group		Michel Bluteau	0	
BeyondTrust Unix &	roles		apiuser		Group			0	
BeyondTrust Unix &	roles		auditor		Group			0	
	roles		policyadmir		Group			0	
BeyondTrust Unix &			softwaread	nin	Group			0	
BeyondTrust Unix & BeyondTrust Unix &	roles								
BeyondTrust Unix & BeyondTrust Unix & BeyondTrust Unix &	roles		sysadmin		Group			0	

29

Entitlement Catalog

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs