Privilege Management for Unix & Linux SailPoint IdentityNow Integration

2

Table of Contents

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

3

IdentityNow Connector for PMUL (BIUL)

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

Prerequisites

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

Use Cases

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

Introduction

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

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

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

- Account Aggregation or Discovery
- Role Aggregation
- Create Account
- Enable Account
- Disable Account
- Update Password
- Unlock Account
- Delete Account
- Add Role to User
- Remove Role from User

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



Configuration

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

\varTheta sv	vagger	admin			Log
Bevo	ndInsight for Unix & Linux API				
This API p	provides access to control BeyondTrust software for ADBridge and Privile	ege Management for Unix 8	k Linux.		
Action	S	Show/Hide	List Operations	Expand Oper	ratio
Activat	tion	Show/Hide	List Operations	Expand Oper	ratio
ADB		Show/Hide	List Operations	Expand Oper	ratio
Applica	ationFeatures	Show/Hide	List Operations	Expand Oper	ratio
Audit		Show/Hide	List Operations	Expand Oper	ratio
Authen	ntication	Show/Hide	List Operations	Expand Oper	ratic
GET	/v1/auth/domains		Get list of avai	lable remote do	oma
POST	/v1/auth/login		Login and	acquire a login	n to l
POST	/v1/auth/refresh			Refresh login	n to l
GET	/v1/auth/roles			List	Ro
GET	/v1/auth/roles/{rolename}			Get Role	Deta
PUT	/v1/auth/roles/(rolename)/groups		S	et all groups for	ran
PUT	/v1/auth/roles/{rolename}/users			Set all users for	rano
_					

4

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

Dashboard 🗸	Identities \checkmark	Access 🗸	Applications	Connections 🗸	Certifications 🗸	Password Mgmt 🗸	Global 🗸	Workflows	Event Triggers	
Sources	i									Create New
Q Sea	rch for a source									
8 Results										Cards Table

Create Web Services or Connector

Create Source: Select Source Type Select a source type Q we services Results Image: Comparison of the Services connector can be used to integrate with any target system using standard Web Services API. The connector can perform aggregation, rovisioning and deprovisioning, and other governance operations on the managed system. We Decumentation Configure

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

 \mathbf{X}

5

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

Base Configuration

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

BeyondInsight Unix and Linux: Web Services

Direct Connection

Base Configuration	Base Configuration	Source Name *
Connection Settings	The Web Services source is a type of 'Direct Connection' source used to communicate between a	Bu Bu
HTTP Operations	source server and SailPoint. To configure a Direct Connection source, provide or select values for all	Source Description *
Additional Settings	required fields, including a source owner and virtual appliance cluster.	PMUL(BIUL) source via REST API
Review and Test	The source owner is responsible for administering, operating, and managing the source system. The virtual appliance (VA) is a Linux-based virtual machine that is deployed and configured to connect to sources and apps using APIs, connectors / integrations provided by SailPoint.	Source Owner *
	(Optional) Select a governance group to specify the Source Sub-Admin users who can manage this source. Learn more about governance groups	Virtual Appliance Cluster *
		Governance Group for Source Management
		None

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

Connection Settings

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

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

BeyondInsight Un	hix & Linux og: - <u>Constitutions</u> - Entitient River
USER: SVC_IDN IdentityNow, Service User has 2 roles @ Active	Account (wc.jdn@))
User Details	User Roles
Details	Roles configured here will be in addition to any roles that this user may inherit through membership in groups.
Roles	System Administrator
Authentication	Note that the System Administrator role allows for all actions within Beyondinsight for Unix & Linux regardless of what other roles are enabled for the user.
	C API User
	C Auditor
	Account Administrator
	Delicy Administrator
	Software Administrator

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

To set the connection settings:

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

BeyondInsight Unix	and Linux: Web Services		×
Base Configuration Connection Settings HTTP Operations Additional Settings	Connection Settings Chove the appropriate authentication type and provide the information required to connect and interact with the source. Learn more about Web Services Connection Settings	Authentication Type • Cantom Autometication V	
Novem and Jett	Custom Authentication Hyper antimetication origination density hospital strategies enclosations lite lites or OWID 2.3, you can use Castler Authentications. If the register in their Salau. Laws Here and work for Antimetications Authentications Settings	Base UBL - Totage/Johanneth/Sold/apil Userama Soc.56 Passeod API Takan	

HTTP Operations

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

BeyondInsight Un Direct Connection	nix and Linux: Web Services		
Base Configuration	HTTP Operations		
Connection Settings	Configure custom HTTP operations. HTTP operations	Authenticate	
ATTP Operations	moved to set the order. You can add operations, copy existing operations, edit existing operations, or delete	Custom Authentication	
Additional Settings	operations.	Test Connection	
Review and Test	Learn more about Web Services HTTP Operations Settings	Test Connection	
		Account Aggregation	
		Role Aggregation	
		Group Aggregation	
		Create Account	
		Create Account	• • • •

On the left side menu, select HTTP Operations.

Authenticate (Custom Authentication)

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

General Information

To set the Authenticate information:

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



6

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

Headers

To set the **Headers** information:

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

A	uthenticate			×
	General Information	Key	Value	
L	Headers	Accept	application/json	
Ì	Body	Content-Type	application/json	
	Response Information	Add Another		
	Response Mapping			
	XPath Namespace Mapping			

Body

To set the **Body** information:

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

Authenticate		×
General Information	Form Data	
Headers Body	Body	
Response Information	("domain":"","dsDomain":"","dsID":0,"password":"Sapplication.passwordS","username":"Sapplication.userna me\$"}	
Response Mapping		
	Save	

7

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

4. Click Save.

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

Response Information

To set the Response Information:

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



Response Mapping

To set the **Response Mapping** information:

- 1. On the Authenticate panel, select Response Mapping.
- Save the token included in the response into a <u>CA</u> variable for encrypted values.
- 3. Click Save.

eneral Information	Schema Attribute +	Attribute Path	
eaders	accesstoken_CA	\$.token	
ody	Add Another		
esponse Information			
esponse mapping			
ath Namespace Mapping			
Path Namespace Mapping			
Path Namespace Mapping			
aponse mapping Path Namespace Mapping			
eponse mapping Path Namespace Mapping			
aponas mapping			

8

Test Connection

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

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

General information

To set the **Test Connection** information:

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

est Connection			×
General Information	Operation Name + Must be a unique name		
Body	Prest Connection Operation Type +		
Response Information	Test Connection	~	
Response Mapping	Use cURL Command		
XPath Namespace Mapping	Context URL		
	/v1/users/generic_users		
	HTTP Method		
	GET	⊗ ∨	

Headers

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

To set the Headers information:

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

	Key	Value	
iders	Authorization	Bearer \$application.accesstoken_CA\$	
ly	Accept	application/json	
ponse Information	Add Another		
ponse Mapping			
th Namespace Mapping			

9

Response Information

To set the Response Information:

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

est Connection		
General Information	Root Path	
Headers Body	Success Codes Add a value to the field and then press Enter.	
Response Information		
XPath Namespace Mapping		
		Save

Account Aggregation

General information

To set the Account Aggregation information:

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

General Information	Operation Name •	
Headers	Must be a unique name Account Aggregation	
Body	Operation Type *	
Response Information	Account Aggregation	~
Response Mapping	Use cURL Command	
XPath Namespace Mapping	Context URL	
Parent Endpoint	/v1/users/generic_users	
Paging	HTTP Method	
	GET	⊗ ∨

10

Headers

To set the **Headers** information:

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

Accoun	t Aggregation			×
General Headen Body Respon Respon XPath N Parent I Paging	Information se Information se Mapping annespace Mapping Endpoint	Key Authorization Accept Add Another	Velue Bener Stapplication accessitoken_CAS (application/json) (
			_	

Response Information

To set the Response Information:

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

A	ccount Aggregation		×
	General Information	Root Path	
	Headers	5.03ta	
	Body	Success Codes Add a value to the field and then press Enter.	
T	Response Information		
ľ	Response Mapping	200 🖸	
	XPath Namespace Mapping		
	Parent Endpoint		
	Paging		
		Save)

11

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

Response Mapping

To set the **Response Mapping** information:

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

neral Information	Schema Attribute *	Attribute Path	
iders	firstname	firstname	
ly	created	created	
ponse Information	roles	roles[*].rolename	
ponse Mapping	active	active	
th Namespace Mapping			
ent Endpoint	admin	admin	
ing	cn	cn	
	requiresGroup	requiresGroup	
	lastname	lastname	
	path	path	
	externalApilD	externalApiID	
	name	name	
	guid	guid	
	remoteUserID	remoteUserID	
	userType	userType	
	localUserID	localUseriD	
	updated	updated	
	email	email	
	uramama	uromama.	

Account Aggregation

Rol

Role Aggregation

General information

To set the Role Aggregation information:

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

e Aggregation		×
ieneral Information leaders	Operation Name * Mott be a unique name Role Aggregation	
ody	Operation Type •	
esponse Information	Group Aggregation	
esponse Mapping	Use cURL Command	
Path Namespace Mapping	Context URL	
arent Endpoint	/v1/auth/roles	
aging	HTTP Method	
	GET OV	
	Save	

12

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

Headers

To set the **Headers** information:

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

R	ole Aggregation			×
I	General Information Headers Body Response Information Response Mapping XPath Namespace Mapping Parent Endpoint Paging	Key Authorization Accept Add Another	Value Besrer Sapplication accesstoken_CAS B pplication/json B	
			Save	

Response Information

To set the Response Information:

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

ble Aggregation		×
General Information	Root Path	
Headers		
Body	Success Codes Add a value to the field and then press Enter.	
Response Information		
Response Mapping	200 0	
XPath Namespace Mapping		
Parent Endpoint		
Paging		
	Save	

Re

Response Mapping

To set the Response Mapping information:

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

General Information Headers Gody Add Another Response Mapping XPath Namespace Mapping Parent Endpoint Paging	Role Aggregation			×
Response Mapping XPath Namespace Mapping Parent Endpoint Paging	General Information Headers Body Response Information	Schema Attribute • rolename Add Another	Attribute Path	
Paging	Response Mapping XPath Namespace Mapping Parent Endpoint			
	Paging			

13

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



Create Account

General information

To set the Create Account information:

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

Cı	eate Account		×
I	General Information Headers	Operation Name + Most be a unique name Create Account)
	Body	Operation Type •	
	Response Information	Create Account V	J
	Response Mapping	Use cURL Command	
	XPath Namespace Mapping	Context URL	
		/v1/users	
		HTTP Method	
		POST ® V	
		Save	

Headers

To set the **Headers** information:

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

General Informat	on Key	Value
Headers	Authorization	Bearer \$application.accesstoken_CA\$
Body	Content-type	application/json
Response Inform	Accept	application/json
Response Mappir	a Add Annahar	
XPath Namespac	Mapping	

14

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

Body

To set the **Body** information:

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

Create Account	,
General Information	O Form Data
Headers	O Raw
Body	Body
Response Information	{ "active": \$plan.active\$,
Response Mapping	"email": "\$plan.email\$", "firstname": "\$plan.firstname\$",
XPath Namespace Mapping	"lastname": "\$plan.lastname\$",
	Saue

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

Response Information

To set the Response Information:

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

Create Acc	ount		×
General Inform	nation Root F	Path	
Headers			
Body	Succes Add a v	ss Codes value to the field and then press Enter.	
Response Info	rmation		
Response Map	ping 2** (0	
XPath Namesp	ace Mapping		
		Save	

Response Mapping

To set the **Response Mapping** information:

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

eneral Information	Schema Attribute •	Attribute Path	
eaders	firstname	firstname	
ody	roles	roles[*].rolename	
esponse Information	active	active	
esponse Mapping	admin	admin	
Path Namespace Mapping	metalizatb	remotel (cert)	
	remoteoseno	Temoteoseno	
	localUserID	ID	
	email	email	
	lastname	lastname	
	username	username	
	Add Another		

Add Role to User and Remove Role from User

General Information

To set the Add Role to User information:

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

dd Role to User		×
General Information	Operation Name *	
Headers	Must be a unique name Add Role to User	
Body	Operation Type •	
Response Information	Add Entitlement	~
Response Mapping	Use cURL Command	
XPath Namespace Mapping	Context URL	
	/v1/users/\$plan.nativeldentity\$/roles/\$plan.roles\$	
	HTTP Method	
	PUT	⊗ ∽
		Save

16

To set the Remove Role from User information:

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

Arri Information Operation Name • Mattebe surrigen name Arris Remove Role from User V Operation Type • Remove Entitlement > In Namespace Mapping Use cURL Command • In Namespace Mapping Cantest URL V/LAUSers/Splan.nolveddentityS/roles/Splan.nolvesS XIT Method ELETE ©	move Role from U	ser	
der Remove Rolle from User // Operation Type * remove Rolle from User // Remove Rolle from User // Remove Rolle from User // Remove Rolle from User // Remove Rolle from User // Remove Rolle from User // Remove Rolle from User // V// // Context URL /// //// // Remove Rolle from User // Context URL /// //// // Remove Rolle from User	General Information	Operation Name *	
V Operation Type • Dense Information Remove Entitlement. Dense Mapping Use cURL Command Context URL Information Context URL Information Manaspace Mapping BELETE ©	Headers	Remove Role from User	
Internation Remove Entitlement Internation Entitlement Internation Internation	Body	Operation Type *	
Inserseption Use cURL Command In Namespace Mapping Context URL ////www.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.space.spac	Response Information	Remove Entitlement	~
h Namespace Mapping Context URL //d/wem/Splan.nativeidentity5/roles/Splan.nolesS MTTP Method DELETE © V	Response Mapping	Use cURL Command	
/vl/user/Splan.noles\$ HTTP Method DELETE ⊗ ♥	XPath Namespace Mapping	Context URL	
NTTP Method DELETE		/v1/users/\$plan.nativeldentity\$/roles/\$plan.roles\$	
delete Ov		HTTP Method	
		DELETE	⊗ ∨
		/vl/useru/Splan.nativeldentitys/roles/Splan.rolesS HTTP Method DELETE	© ~
_			Save

Headers

To set the **Headers** information:

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



Response Information

To set the Response Information:

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

A	dd Role to User		×
	General Information	Root Path	
	Headers		
	Body	Success Codes Add a value to the field and then press Enter.	
	Response Information		
ľ	Response Mapping	2** 0	
	XPath Namespace Mapping		

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

Response Mapping

To set the **Response Mapping** information:

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

neral Information	Schema Attribute •	Attribute Path	
eaders	firstname	firstname	
lody	roles	roles[*].rolename	
Response Information	active	active	
Response Mapping	admin	admin	(1)
XPath Namespace Mapping	remoteUserID	remoteUserID	
	localUserID	ID	
	email	email	
	lastname	lastname	
	username	username	
	Add Another		

Disable Account and Enable Account

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

Disable Account -1 and Enable Account -1

General Information

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

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

Di	sable Account - 1		×
	General Information	Operation Name • Must be a unique name Disable Account - 1	
	Body	Operation Type •	
	Response Information	Disable Account V	
	Response Mapping	Use cURL Command	
	XPath Namespace Mapping	Context URL	
		/v1/users/\$plan.nativeldentity\$	
		HTTP Method	
		GET 🛞 🗸	
		Save	

18

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

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

hable Account - 1		
General Information	Operation Name *	
Headers	Enable Account - 1	
Body	Operation Type *	
Response Information	Enable Account	~
Response Mapping	Use cURL Command	
XPath Namespace Mapping	Context URL	
	/v1/users/\$plan.nativeldentity\$	
	HTTP Method	
	GET	⊗∨

Headers

To set the Headers information:

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

General Information	Key	Value	
Headers	Authorization	Bearer \$application.accesstoken_CA\$	
Body	Accept	application/json	
Response Information	Add Another		
Response Mapping			
XPath Namespace Mapping			

Response Information

To set the Response Information:

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

Disable Account - 1		×
General Information	Root Path	
Headers		
Body	Success Codes Add a value to the field and then press Enter.	
Response Information		
Response Mapping	200 0	
XPath Namespace Mapping		
	Save	

19

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

Response Mapping

To set the **Response Mapping** information:

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

eneral Information	Schema Attribute •	Attribute Path	
eaders	firstname	firstname	
Body	admin	admin	
Response Information	remoteUserID	remoteUserID	
Response Mapping	localUserID	ID	
XPath Namespace Mapping	email	email	
	lastname	lastname	
	username	username	
	Add Another		

Disable Account-2 and Enable Account-2

General Information

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

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

To set the Enable Account-2 information:

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

L	General Information	Must be a unique name	
	Headers	Disable Account - 2]
	Body	Operation Type +	
	Response Information	Disable Account V]
	Response Mapping	Use cURL Command	
	XPath Namespace Mapping	Context URL	
		/v1/users/\$plan.nativeIdentity\$]
		HTTP Method	
		PUT & V]
		Save	
E	nable Account - 2		×
I	General Information	Operation Name + Must be a unique name	
	Headers	Enable Account - 2]

 \sim

× ×

20

Disable Account - 2

Ope

Operation Type

Enable Account

HTTP Method

Use cURL Command

/v1/users/\$plan.nativeIdentity\$

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

Headers (Disable Account-2 only)

To set the **Headers** information:

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

D	isable Account - 2			×
1	Ceneral Information Headers Body Response Information Response Mapping XPath Namespace Mapping	Key Authorization Accept Add Another	Value Bearer Sapplication.accesstoken_CAS	
			Save	

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

To set the Body information for Disable Account-2:

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

D	isable Account - 2		×
I	General Information Headers Body Response Information Response Mapping XPath Namespace Mapping	<pre>form Data Raw Eccy *email*: Sresponse emails*: *finstrame**Sresponse lastrames*: *factive*: face }</pre>	
			Save

21

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

4. When done, click Save.

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

To set the Body information for Enable Account-2:

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

Enable Acco	unt - 2	×
General Informa Headers Body Response Inform Response Inform XPath Namespa	tion Form Data Form Data Raw Body sation rfmstmme: "Sresponse.amails": rfmstmme: "Sresponse.atmails": response.lastnames": ractive: tope cative: tope }	
	Save	

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

4. When done, click Save.

Response Information (Disable Account-2 only)

To set the Response Information:

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

Disable Account - 2		×
General Information	Root Path	
Headers		
Body	Success Codes Add a value to the field and then press Enter.	
Response Information		
Response Mapping	200 0	
XPath Namespace Mapping		
	Save	

22

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

Response Mapping (Disable Account-2 only)

To set the Response Mapping information:

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

ieneral Information	Schema Attribute •	Attribute Path	
leaders	username	username	
lody	email	email	
esponse Information	firstname	firstname	
tesponse Mapping	lastname	lastname	
Path Namespace Mapping	admin	admin	
	active	active	
	remoteUserID	remoteUserID	
	roles	roles[*].rolename	
	Add Another	, (

Update Password

General Information

To set the Update Password information:

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

pdate password		2
General Information	Operation Name •	
Headers	Must be a unique name Update password	
Body	Operation Type *	
Response Information	Change Password V	J
Response Mapping	Use cURL Command	
XPath Namespace Mapping	Context URL	
	/v3/users/\$plan.nativeldentity\$/password	
	HTTP Method	
	PUT ® V	

Headers

To set the **Headers** information:

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

Update password			×
General Information Headers Body Response Information Response Mapping	Key Authorization Accept Add Another	Value Beaver Sapplication.accesstoken_CAS (B) application/json (B)	
XPath Namespace Mapping			
		Save	

Body

To set the **Body** information:

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

U	pdate password		×
	General Information Headers	 Form Data Raw 	
I	Body Response Information Response Manning	Body ("new_password": "Splan.password5")	
	XPath Namespace Mapping		
		Save	
	Body Response Information Response Mapping XPath Namespace Mapping	Bdy ["new_password": "\$plan.password\$"] 	

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

Response Information

To set the Response Information:

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



Response Mapping

To set the Response Mapping information:

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

eral Information	Schema Attribute •	Attribute Path	
ders	firstname	firstname	
/	roles	roles[*].rolename	
onse Information	active	active	
onse Mapping	admin	admin	
h Namespace Mapping	remoteUserID	remoteUserID	
	localUserID	D	
	email	email	•
	lastname	lastname	
	username	username	(1)

25

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



Unlock Account

General Information

To set the Unlock Account information:

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

U	nlock Account		×
I	General Information Headers	Operation Name + Must be a unique name Uniock Account	
	Body	Operation Type •	
	Response Information	Unlock Account	
	Response Mapping	Use cURL Command	
	XPath Namespace Mapping	Context URL	
		/v3/users/\$plan.nativeldentity\$/lock	
		HTTP Method	
		DELETE 🛛 🛇 🗸	
		Save	

Headers

To set the **Headers** information:

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

neral Information	Kev	Value	
aders	Authorization	Bearer \$application.accesstoken_CA\$	D
dy	Accept	application/json	D)
sponse Information	Add Another		
sponse Mapping			
ath Namespace Mapping			
ath Namespace Mapping			
ath Namespace Mapping			

Response Information

To set the Response Information:

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



Response Mapping

To set the Response Mapping information:

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

neral Information	Schema Attribute •	Attribute Path	
iders	firstname	firstname	
dy	roles	roles[*].rolename	
esponse Information	active	active	
esponse Mapping	admin	admin	
Path Namespace Mapping			
	remoteUserID	remoteUserID	
	localUserID	D	
	email	email	
	lastname	lastname	
	username	username	
	Add Another		

27

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



Delete Account

General Information

To set the **Delete Account** information:

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

D	elete Account		×
	General Information Headers	Operation Name + Matt be aurique name Delete Account	
	Body	Operation Type *	I.
	Response Information	Delete Account V	
	Response Mapping	Use cURL Command	I.
	XPath Namespace Mapping	Context URL	I.
		/v1/users/\$plan.nativeIdentity\$	
		HTTP Method	
		DELETE	
		Save	

Headers

To set the **Headers** information:

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



Response Information

To set the Response Information:

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

This completes the list of HTTP Operations.

D	elete Account		×
	General Information Headers Body Response Information	Root Path	
	Response Mapping XPath Namespace Mapping	200 0	

28

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

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

Test the Connection

To test the connection:

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



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

Add a Correlation Rule

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

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



Create Account and Provisioning Policy

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



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

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

Provisioning Policies:



29

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

30

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

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

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

Aggregate Accounts and Entitlements

You can now aggregate accounts and set entitlements.

Aggregate Accounts

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

Dashboard 🗸 Identities 🗸	Access - Applications Connect	ions 🗸 Certifications 🗸	Password Mgmt V Global V	Workflows Event Tr	iggers	
< Source Name: Beyond	Insight Unix and Linux Source Typ	e: Web Services Connecti	on Type: Direct Connection			Healthy for 25 hours
Import Data Connections	Accounts 9 Entitlements 6	Access Profiles		Delete Source	Edit Configuration	Test Connection
User Accounts	Accounts 9				▲ CSV Search Acc	ounts Q
	User Name	Accour	rt Name	Account ID		
Create Account	Alvin Abril	> Alvin.At	nii - bilab.blu.cloud	6		
Attribute Sync	Alvin Smith	> Avin.Sr	nith - btieb.btu.cloud	5		
	Amanda Julio	> Amanda	s.Julio	16		
	Chris Abril	> Chris.A	bril - bliab.blu.cloud	2		
	Devon Julio	> Devon.	lutio	17		
	Oliver Smith	> Oliver.S	mith	18		
	Ubald Junio	> Ubaid.J	unio - btlab.btu.cloud	4		
	Uncorrelated Account	Alan.Ma	ryo - briab.btu.cloud	3		

31

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

Entitlements

Under Connections, select the Entitlements tab.

Dashboard ~ Identities ~ Access ~ App	lications Connections V Certifica	rtions 🗸 Password Mgmt 🗸	Global V Workflows Event To	riggers
< Source Name: BeyondInsight Unix and	Linux Source Type: Web Services	Connection Type: Direct Conne	ction	Healthy for 25 hours
Import Data Connections Accounts 9	Entitlements 6 Access Profiles		Delete Source	Edit Configuration Test Connection
Source Entitlements 6				Add
Actions V			∆ cev	± CBV Search Entitlements Q
Name ^	Description	Type Own	er Permissions	Requestable Status
accountadmin	·	group	No	No
apluser	>	Buorb	No	No
auditor	>	group	No	No
policyadmin	•	group	No	No
softwareadmin	>	group	No	No
sysadmin	>	group	No	No
II < Page 1 of 1 > > ₽				1-090

Access Profiles

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

mport Data Connections	Accounts 9 Entitlements 6 Access Profil	H 3	Delete Source Edit C	onliguration Test Connection
Access Profiles 3				+ New
				Search Access Profiles 🛛 🔍
Name 🔿	Description			Entitlements
BIUL - Linux SysAdmin	 BIUL - Linux SysAdmin 			1
BIUL - Policy Admin	BIUL - Policy Admin			1
BIUL - Software Admin	> BIUL - Software Admin			1

32

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