

SecZetta-CyberArk Remote Access Integration Overview

The SecZetta and CyberArk Remote Access integration enables collaboration between the SecZetta platform and CyberArk Remote Access. This integration allows for coordination of non-employee (third-party vendor) lifecycle activities in SecZetta and invitations or access within Remote Access.

Contents

Overview	1
Key Capabilities.....	1
Key Benefits	1
Supported Use Cases.....	2
Specifications	2
Use Cases	3
UC01: Invite New Vendor User into CyberArk Remote Access	3
UC02: Terminate Non-Employee and Delete Remote Access Account	4
Additional Considerations and Future Use Cases.....	5
References.....	5
Appendix: Sample Workflows and API Configuration.....	6
Example Workflow: Onboard Non-Employee.....	6
Rest API Workflow Step: Send Invite to User.....	7
Example Workflow: Terminate Non-Employee.....	9
Rest API Workflow Step: Look up user by phone	10
Rest API Workflow Step: Delete Remote Access Vendor Account	11

Overview

Key Capabilities

- Non-employee onboarding within SecZetta triggers vendor user invitations in CyberArk Remote Access
- Non-employee termination within SecZetta drives user account deletion in CyberArk Remote Access

Key Benefits

- Lifecycle of non-employees in SecZetta is supported by unique, collaborative workflows for each population which results in trusted, authoritative user data, relationships and status
- Policy checks, risk scoring, and approval processes within SecZetta enable informed, risk-based decision-making for the management of third party vendor access within CyberArk Remote Access

- Updates and status changes in SecZetta result in immediate updates to CyberArk Remote Access, enabling quick access via CyberArk Remote Access for newly onboarded vendor users as well as immediate removal of access when a vendor user is terminated within SecZetta

Supported Use Cases

UC01	Invite New Non-Employee into CyberArk Remote Access
UC02	Terminate Non-Employee and Delete Remote Access Account

Specifications

Version: 1.0

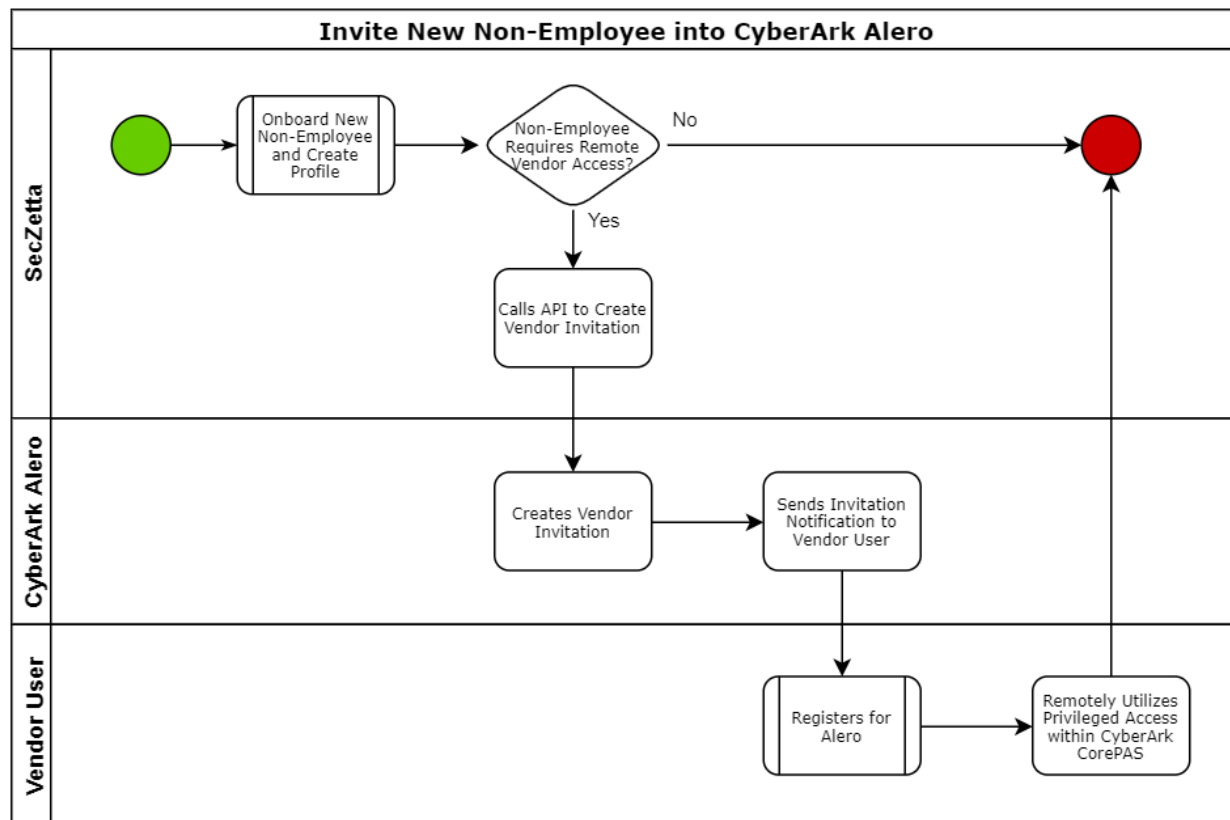
Release Date: January 2021

Developed by: SecZetta, Inc.

Supported by: SecZetta, Inc.

Use Cases

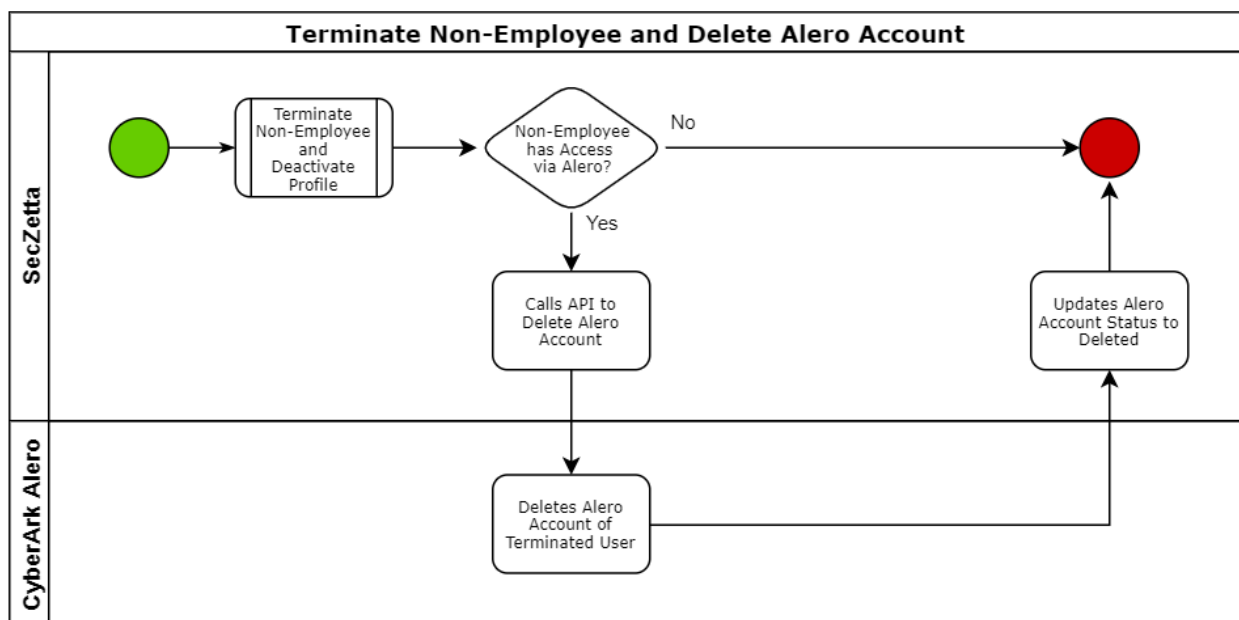
UC01: Invite New Vendor User into CyberArk Remote Access



UC01: Invite New Non-Employee into CyberArk Remote Access	
Summary:	New Non-Employee onboarded in SecZetta requires and qualifies for remote vendor access via CyberArk Remote Access. Upon completion of onboarding in SecZetta, CyberArk Remote Access vendor invitation is triggered and non-employee registers for Remote Access to utilize vendor access policies available in CyberArk CorePAS.
Actors:	SecZetta User, CyberArk Remote Access, Vendor User
Preconditions:	Profile is created in SecZetta via onboarding or other workflow.
Post conditions:	Vendor invitation exists in Remote Access and, once accepted, account in Remote Access is created.
Assumptions:	✓ API authentication is established and successful between SecZetta and SailPoint ✓ Vendor access policies and details are properly configured in CyberArk for vendor organizations ✓ CyberArk CorePAS is configured to allow access to vendors via Remote Access.
Trigger:	New non-employee profile is created in SecZetta
Use Case	

1	BEGIN: SecZetta completes workflow to onboard new non-employee and create SecZetta profile.
2	If non-employee requires remote access via Remote Access, go to step 3. If not, got to step 8.
3	SecZetta calls Remote Access API endpoint to create and send vendor invitation.
4	CyberArk Remote Access creates vendor invitation.
5	CyberArk Remote Access sends invitation notification to vendor user.
6	Vendor user registers for CyberArk Remote Access.
7	Vendor user remotely utilizes privileged access within CyberArk CorePAS.
8	END

UC02: Terminate Non-Employee and Delete Remote Access Account



UC02: Terminate Non-Employee and Delete Remote Access Account	
Summary:	Existing Non-Employee with vendor user Remote Access account is terminated in SecZetta, and this termination results in deletion of Remote Access account for the Non-Employee. Non-Employee no longer has access to CyberArk CorePAS via Remote Access.
Actors:	Non-Employee, SecZetta, CyberArk
Preconditions:	Non-Employee has Remote Access vendor user account mapped to SecZetta profile.
Post conditions:	Remote Access account owned by terminated Non-Employee is deleted and Non-Employee no longer has access via Remote Access.
Assumptions:	✓ API authentication is established and successful between SecZetta and SailPoint
Trigger:	Non-Employee profile is terminated/deactivated within SecZetta.
Use Case	
1	BEGIN: SecZetta completes workflow that deactivates non-employee profile

2	If non-employee Remote Access invitation status is complete and account UID exists, go to step 3. If not, go to step 6.
3	SecZetta calls Remote Access API to delete vendor user account.
4	Remote Access deletes vendor user account linked to non-employee.
5	SecZetta updates Remote Access account status on profile to deleted.
6	END

Additional Considerations and Future Use Cases

- CyberArk Remote Access triggers collaborative workflows in SecZetta to vet or revalidate non-employee relationships and status to ensure appropriateness of access achieved through Remote Access.

References

- SecZetta API Documentation: <https://seczetta.nonemployee.com/api/v1/index.html>
- CyberArk Remote Access API Documentation: <https://api.RemoteAccess.io/swagger-ui.html#/>
- CyberArk Remote Access Service Account Documentation: <https://docs.cyberark.com/Product-Doc/OnlineHelp/RemoteAccess/Latest/en/Content/WebServices/ServiceAccounts.htm>

Appendix: Sample Workflows and API Configuration

Example Workflow: Onboard Non-Employee

 **Onboard Non-employee**

+ action

+ condition

disable workflow

save

×

ACTIONS

INFO

ROUTING

PERMISSIONS

 **1 Request Form**
Provides the requester a page with forms.

 **2 Create**
Creates a profile with all attributes collected during the workflow.

 **3 Remote Access Required.**

 **3.1 Request Form**
Enter Mobile Phone Number

 **3.2 Create**
Creates a profile with all attributes collected during the workflow.

 **3.3 REST API**
Alero API - Send Invite to user

Rest API Workflow Step: Send Invite to User

Endpoint:

<https://api.RemoteAccess.io/v1-edge/invitations/vendor-invitations>

BASIC SETTINGS

Description

Alero API - Send Invite to user

AUTHENTICATION

Auth type

OAuth2 w/private key jwt

Access token url

<https://auth.alero.io/auth/realms/serviceacc>

Private key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAoFhgpb7uPqLfvPt
eI7CM/rI5MMCPKMI0TEeYhano7m6ch
SI2
E+Ru1aXREz14gMJrqPs+7sxZcsoLQP
```

Encryption type

RS256

Claim set configuration

Iss

11eaab2250acefe0b97f95ccc5c5e407.11eb;

Sub

11eaab2250acefe0b97f95ccc5c5e407.11eb;

Aud

<https://auth.alero.io/auth/realms/serviceacc>

REQUEST

Http verb

POST

Endpoint

<https://api.alero.io/v1-edge/invitations/vendor-invitations>

Headers

Header	Value
Content-Type	application/json

Header	Value
accept	*/*

+ Add header

Json body

```
1 {
2   "accessEndDate": 0,
3   "accessStartDate": 0,
4   "applications": [
5     {
6       "applicationId": "11eab4cd6bf27b0f9327cf43487da52e",
7       "siteId": "11eaab2463a4d3399816d3b7450c5b10"
8     }
9   ],
10  "comments": "ex.comments",
11  "companyName": "SecZetta",
12  "emailAddress": "{{attribute.personal_email}}",
13  "firstName": "{{attribute.first_name_ne_attribute}}",
14  "initialStatus": "Activated",
15  "invitedVendorsInitialStatus": "Activated",
16  "lastName": "{{attribute.last_name_ne_attribute}}",
17  "maxNumOfInvitedVendors": 0,
18  "phoneAndEmailAuth": true,
19  "phoneNumber": "+1{{attribute.mobile_phone_number_ne_attribute}}",
20  "provisioningGroups": [
21  ]
22 }
```

RESPONSE

The status code and data from the response can be mapped to attributes to update or create values.

Status Code Mapping

alero_invitation_id

Data Mapping(s)

Path	Attribute
Key label	alero_invitation_id (alero_invitation_id)

🔍 attribute label, uid

Sample REST API JSON Body:

```
{
  "accessEndDate": 0,
  "accessStartDate": 0,
  "applications": [
    {
      "applicationId": "11eab4cd6bf27b0f9327cf43487da52e",
      "siteId": "11eaab2463a4d3399816d3b7450c5b10"
    }
  ],
  "comments": "ex.comments",
  "companyName": "SecZetta",
  "emailAddress": "{{attribute.personal_email}}",
  "firstName": "{{attribute.first_name_ne_attribute}}",
  "initialStatus": "Activated",
  "invitedVendorsInitialStatus": "Activated",
  "lastName": "{{attribute.last_name_ne_attribute}}",
  "maxNumOfInvitedVendors": 0,
  "phoneAndEmailAuth": true,
  "phoneNumber": "+1{{attribute.mobile_phone_number_ne_attribute}}",
  "provisioningGroups": [
    "11eacd00e5d4e488baa5514eb0311de7"
  ],
  "provisioningType": "ProvisionedByRemote Access",
  "provisioningUsername":
    "{{attribute.first_name_ne_attribute}}.{{attribute.last_name_ne_attribute}}",
  "role": "Vendor"
}
```

Example Workflow: Terminate Non-Employee

 **Terminate**

+ action

+ condition

disable workflow

save

X

ACTIONS

INFO

ROUTING

PERMISSIONS



1

Request Form

Termination Confirm





2

Update

Updates a profile with all attributes collected during the workflow.





3

Termination Confirmed



3.1

REST API

Look up user by phone





3.2

Status Change

Changes the status of a non-employee.





3.3

Update

Updates a profile with all attributes collected during the workflow.





4

Request Form

Show Attributes





5

Termination Confirmed and User has Account



5.1

REST API

Delete Alero Vendor Account



Rest API Workflow Step: Look up user by phone

Endpoint:

[https://api.RemoteAccess.io/v1-](https://api.RemoteAccess.io/v1-edge/vendors/phone/+1{{attribute.mobile_phone_number_ne_attribute}})

[edge/vendors/phone/+1{{attribute.mobile_phone_number_ne_attribute}}](https://api.RemoteAccess.io/v1-edge/vendors/phone/+1{{attribute.mobile_phone_number_ne_attribute}})

BASIC SETTINGS

Description

Look up user by phone

AUTHENTICATION

Auth type

OAuth2 w/private key jwt

Access token url

<https://auth.alero.io/auth/realms/serviceacc>

Private key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAoFhgpb7uPqLfVpT
el7CM/r15MMCPKMI0EeYhano7m6ch
St2
E+Ru1aXREz14gMJrqPs+7sxZcsoLQP
```

Encryption type

RS256

Claim set configuration

Iss

11eaab2250acefe0b97f95ccc5c5e407.11eb;

Sub

11eaab2250acefe0b97f95ccc5c5e407.11eb;

Aud

<https://auth.alero.io/auth/realms/serviceacc>

REQUEST

Http verb

GET

Endpoint

<https://api.alero.io/v1-edge/vendors/phone/->

Headers

Header	Value
Content-Type	application/json

Header	Value
accept	*/*

+ Add header

Json body

1

RESPONSE

The status code and data from the response can be mapped to attributes to update or create values.

Status Code Mapping

alero_http_status_code

Data Mapping(s)

Path	Attribute
id	alero_user_id (alero_user_id)

Rest API Workflow Step: Delete Remote Access Vendor Account

Endpoint:

`https://api.Remote Access.io/v1-edge/vendors/{{attribute.Remote Access_user_id}}`

BASIC SETTINGS

Description

Delete Alero Vendor Account

AUTHENTICATION

Auth type

OAuth2 w/private key jwt

Access token url

`https://auth.alero.io/auth/realms/serviceacc`

Private key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEoFhgb7uPqLfvPt
el7CM/rI5MMCPKMIOTeEYhano7m6ch
St2
E+Ru1aXREz14gMJrqPs+7sxZcsoLQP
-----
```

Encryption type

RS256

Claim set configuration

Iss

`11eaab2250acefe0b97f95ccc5c5e407.11eb;`

Sub

`11eaab2250acefe0b97f95ccc5c5e407.11eb;`

Aud

`https://auth.alero.io/auth/realms/serviceacc`

REQUEST

Http verb

DELETE

Endpoint

`https://api.alero.io/v1-edge/vendors/{{attribu`

Headers

Header	Value	
Content-Type	application/json	✖
accept	*/*	✖

+ Add header

Json body

1

RESPONSE

The status code and data from the response can be mapped to attributes to update or create values.

Status Code Mapping

alero_http_status_code

Data Mapping(s)

attribute label, uid