



CyberArk Integration with Grip Security

Overview

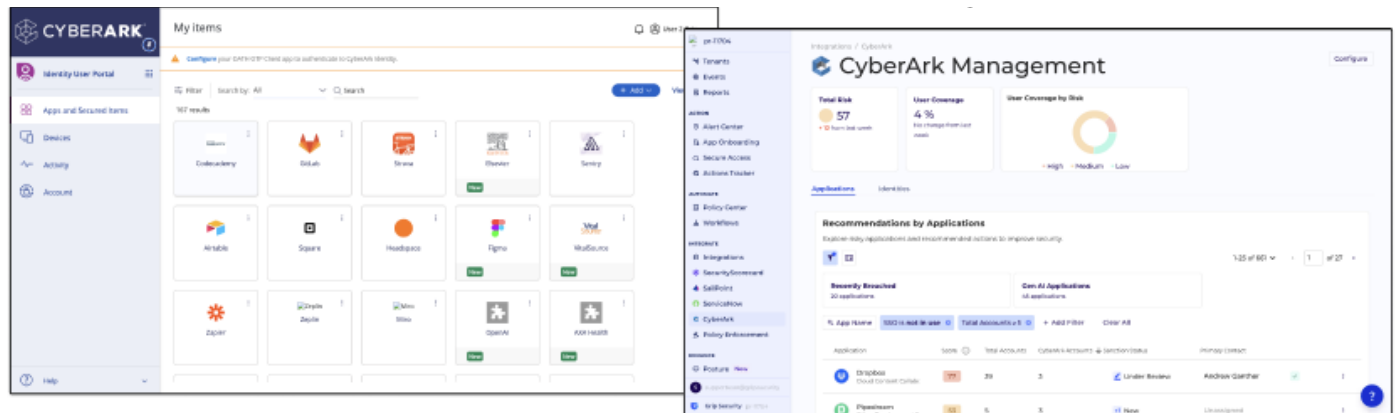
This integration links CyberArk's Workforce Password Manager with Grip to centralize the discovery and management of unmanaged SaaS applications.

Apps identified by Grip as unmanaged and shared can be onboarded into WPM, where their credentials are stored securely and can be rotated.

By integrating discovery, provisioning, and rotation into a single system, organizations obtain comprehensive visibility and governance over all shared application credentials.

This unified approach eliminates shadow-IT risks and simplifies ongoing credential management at scale.

Grip detects shared SaaS accounts as they appear and lets you push them to WPM with one click.





CyberArk Setup

The setup involves creating CyberArk service identities with the needed permissions, connecting those accounts to Grip via API credentials, configuring attribute mappings, and automated sync.

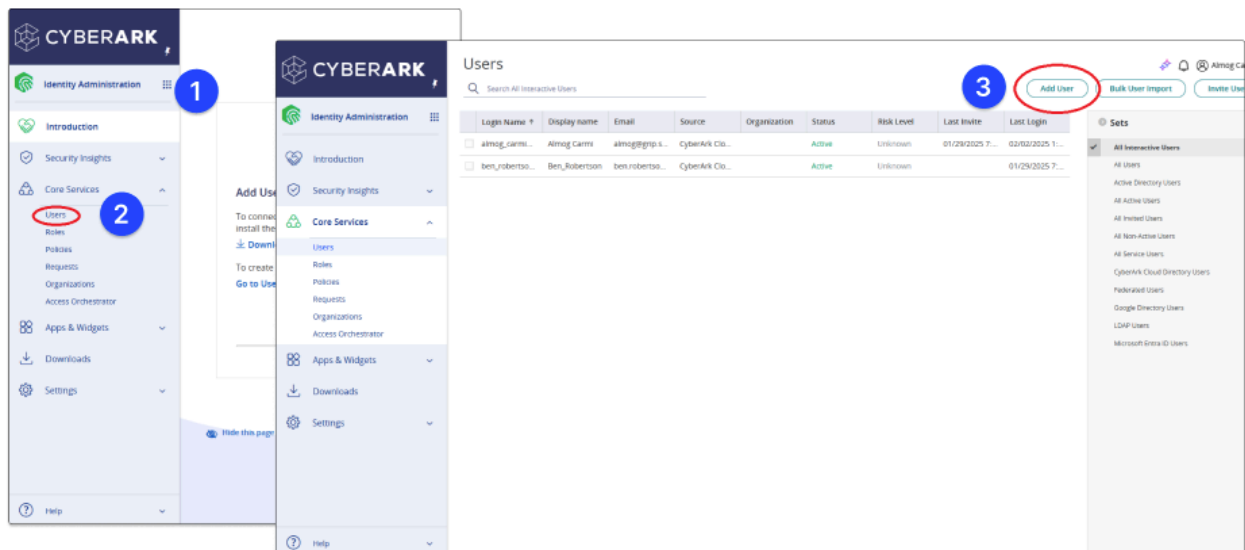
The CyberArk Integration requires a service account for authentication to various services.

The following guide will take you step by step through the integration process.

1- Create Service Account

This step will create a new entity in your IdP that serves solely as the means of authentication for Grip to integrate with the CyberArk API.

- Go to the Identity Administration console (1)
- Under Core Services → Users (2)
- Choose Add User (3)



- Enter the values for the Grip service account. (4)
Note that it is recommended to use the generated password (5)
- Service accounts are a type of user that cannot be accessed through interactive interfaces and function like regular users, but their primary purpose is to serve as a means of authentication for API calls.
- To ensure the new user is a **service account**, select the following checkboxes: (6)
 - Password never expires.
 - Is service user.
 - Is OAuth confidential client.

← Back to Users

Create CyberArk Cloud Directory User

Add users to your organization with CyberArk Cloud Directory

Account
[Learn more](#)

Login name * Suffix

Email address

Display name *

Password Type
☐ Manual ☒ Generated

Password [Copy](#)

Status

☐ Locked
☒ Password never expires
☐ Require password change at next login (recommended)
☒ Is service user
☒ Is OAuth confidential client
☐ Send email invite for user portal setup
☐ Send SMS invite for device enrollment

[Create User](#) [Cancel](#)

2- Granting Permissions

Configure which CyberArk services this user has access to.

- Under **"Core Services" → "Roles"**
- Click on **"Add Role"** and name it: **"grip-service"**
- Click **"Save"**

Welcome to CyberArk Identity Administration
Get up and running in three steps.

Add Role

Name *

Description

Organization

Role Type ⓘ

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

3

Customize the platform access policies and authentication requirements (optional)

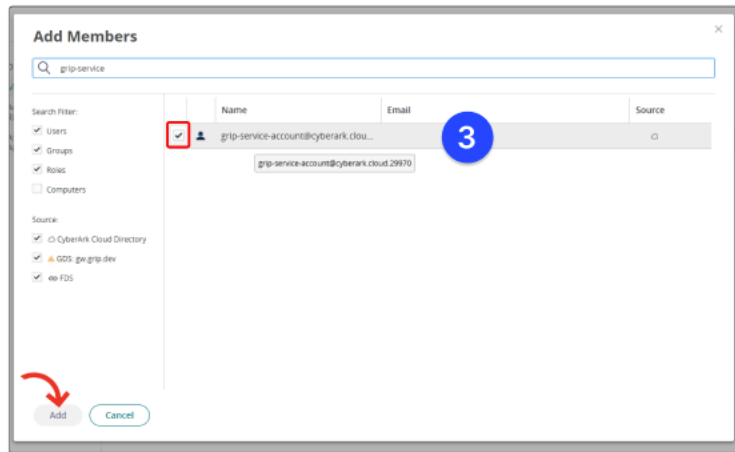
You can create conditional access policies with custom MFA profiles to enhance security and user convenience

To review or update the platform access policies
[Go to Policies >](#)

To set custom MFA challenges for those policies
[Go to Authentication >](#)



- In the **Role** page, go to **"Add Members"** and add the Grip member to the role **(3)**.
- Click on **"Add."**

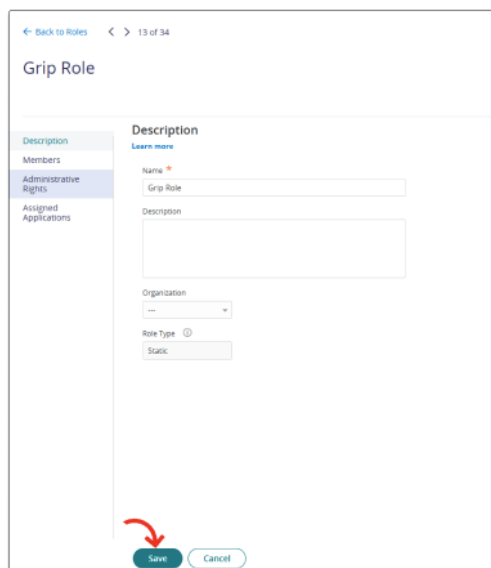


Under **"Administrative Rights"**, search and add the following (for more details - see permissions section):

- **Application Management**
- **User Management**



Once completed, click **"Save."**





Application Management Permissions

- The Grip integration involves retrieving data from CyberArk WPM to provide an accurate snapshot of the organization's status. This process includes fetching the applications listed in WPM, which requires read permissions for those applications.
- The Grip integration provisions applications to specific accounts. To achieve this, applications must be maintained by the Grip service account (created or modified), which requires write permissions for applications.

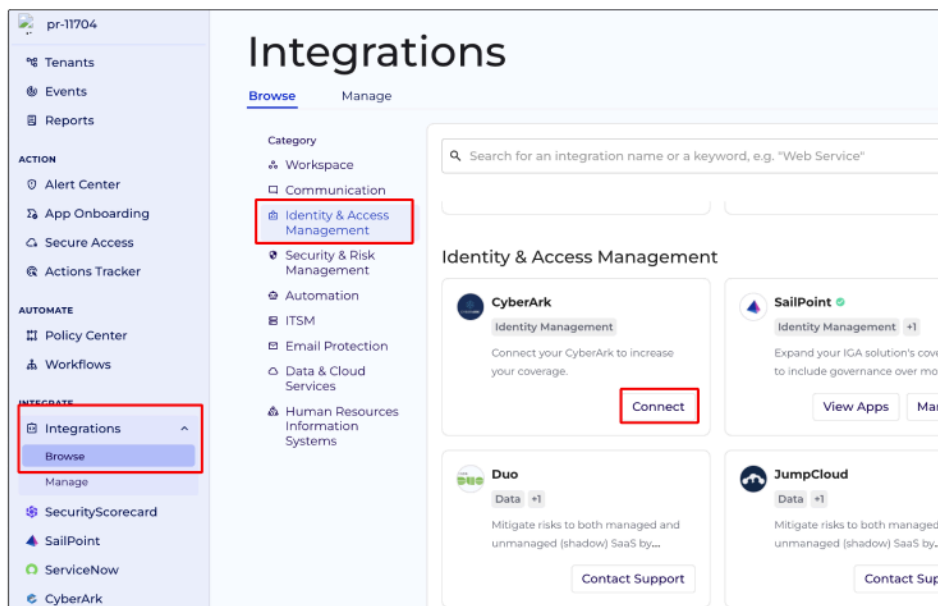
Reference

[API token authentication for CyberArk Identity Security Platform Shared Services | Before you begin](#)

3- Integration with Grip Security

Add the created Grip service account to Grip Security.

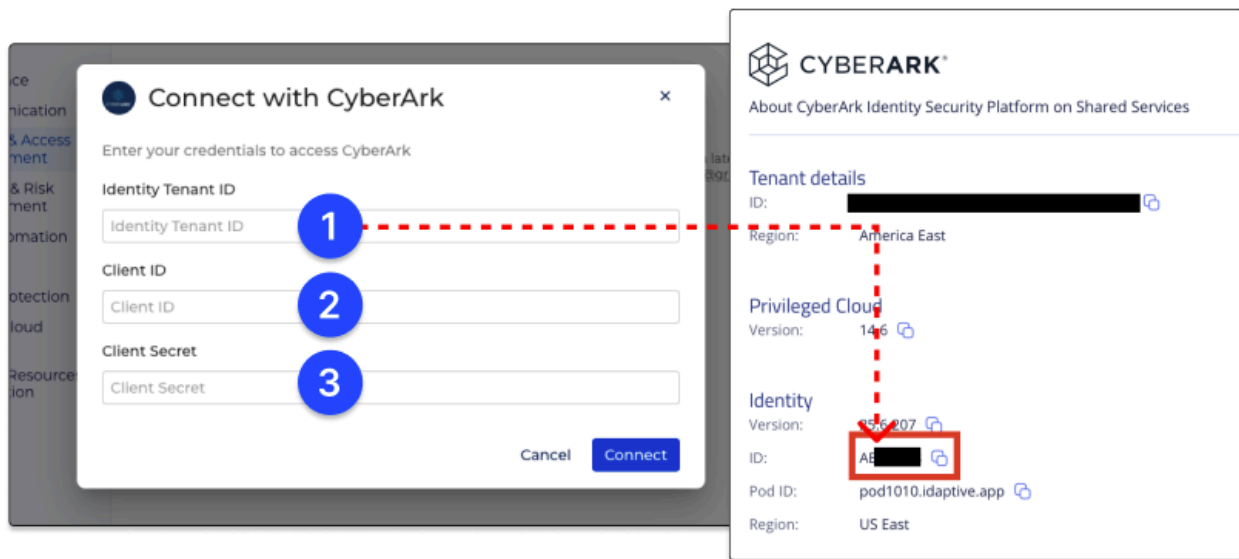
- In Grip platform, go to **"Integrations"** → **Identity & Access Management** > **CyberArk."**
- Click on **"Connect."**



- **Identity Tenant ID (1)-** CyberArk **tenant ID**.
Your **<identity-tenant-id>** can be retrieved by clicking on the User avatar and navigating to the **About** section.
The ID is located under the **Identity** section.
- **Client ID (2)** - The username of the created service account.

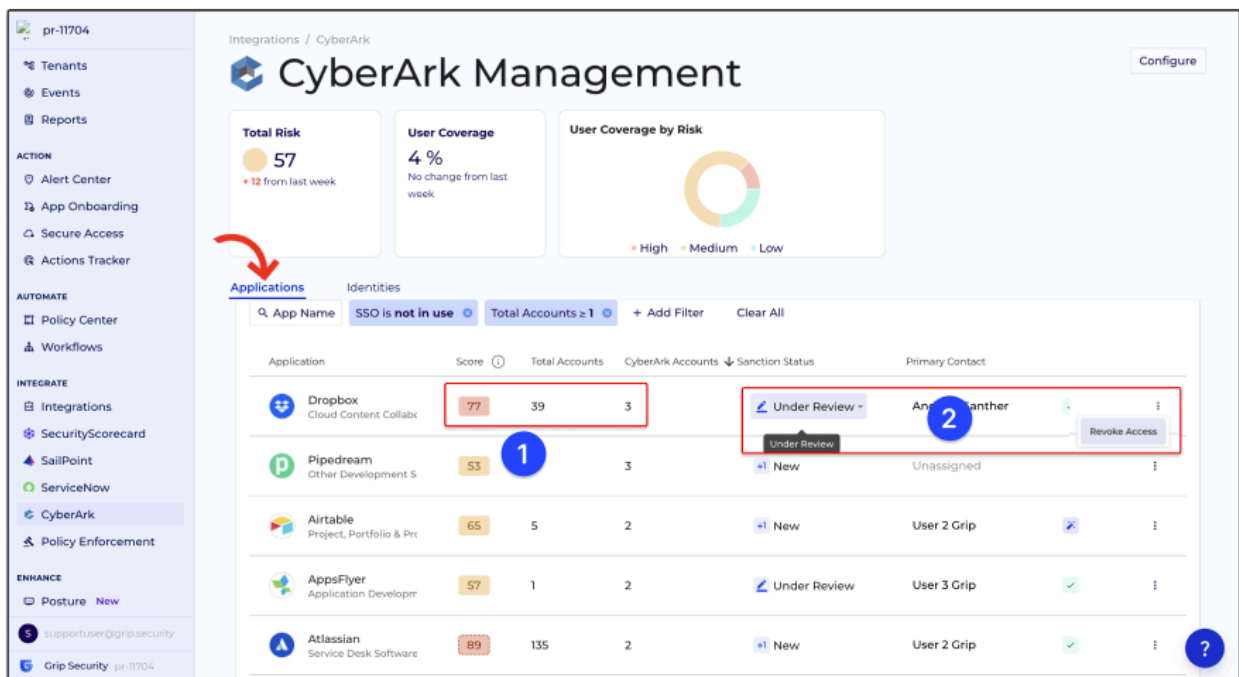


- **Client Secret (3)** - The password of the created service account.



View Applications

- A table links each Grip application to its corresponding CyberArk application, displaying key details from both platforms, including application risk level, total service accounts, password rotation status, last synchronization time, and more **(1)**.
- In addition, there is a list of actionable operations available for each application entry **(2)**.



View Entities



- A table listing each Grip user along with their corresponding CyberArk user, including key attributes from both systems, Grip identity risk score, number of Grip accounts, number of CyberArk accounts, last login timestamp, and more.

CyberArk Management

Total Risk
57
+12 from last week

User Coverage
6
+5 from last week

User Coverage by Risk
High Medium Low

Recommendations by Identities
Explore risky identities and recommended actions to improve security.

Custom View 1-25 of 76 1 of 4

Identity SSO is between 0% - 98% + Add Filter Clear All Save View

Employee	Identity Risk	CyberArk User	CyberArk Accounts	Accounts	Last Login
PR password reset password.reset.1@gw.grip.dev	100	Inactive user	3	500	N/A
PR password-reset-2 reset password.reset.2@gw.grip.dev	100	Inactive user	3	899	N/A
TA Tester Grip Access accessor@gw.grip.dev	100	No user	0	509	N/A
AA Admin Admin admin@o365.grip.dev	91	No user	0	79	N/A

CyberArk User View

CYBERARK

Identity User Portal

My items

167 results

Codecademy GitLab Airtable Square Zapier Zapier

Application Settings

GitLab
GitLab's DevOps platform is a single application for unparalleled collaboration, visibility, and development velocity. Learn more here!

URL

Match detection

Add Tags

Add to folder

Notes

Auto-login at site ☐

User Identity

Username

Password

Save Cancel Delete this app?

CyberArk Admin View



The screenshot shows the CyberArk Identity Administration interface. On the left, the 'Apps & Widgets' menu is highlighted with a red box. The main content area is divided into two sections: 'Web Apps' and 'Users'.

Web Apps Section:

Name	Type	Descri...	Provisio...	App Gat...	Organiz...	Status
Carva	Web - User Pass...	Ama...				Deployed
CareerBuilder	Web - User Pass...	Care...				Deployed
CareerBuilder	Web - User Pass...	Care...				Ready to De...
CircleCI	Web					
Citrix	Web					
Classdojo	Web					
Classdojo	Web					
ClickUp	Web					
Clockify	Web					
CloudApp	Web					
CloudApp	Web					
Cloudera	Web					
Cloudera	Web					
Cloudflare	Web					
Cloudtalk	Web					
Cloze	Web					

Users Section:

Login Na...	Display ...	Email	Source	Organiz...	Status	Risk Level	Last Invite	Last Login
accesso...	Tester ...	ben.ro...	CyberA...		Active	Medium	03/24/...	04/09/...
actiona...	Action ...	actiona...	CyberA...		Invited	Unkno...	03/30/...	
adam.h...	Adam ...	adam.h...	CyberA...		Invited	Unkno...	02/11/...	
adam.h...	Adam ...	adam.h...	CyberA...		Invited	Unkno...	02/11/...	
admin...	Idan Fast	zohar.f...	CyberA...		Invited	Unkno...	03/23/...	
admin...	Idan Fast	admin...	Google ...		Not Inv...	Unkno...		
almog...	Almog ...	almog...	CyberA...		Invited	Unkno...	03/30/...	
alon@...	Alon Sh...	alon@g...	CyberA...		Invited	Unkno...	02/11/...	
amit.gr...	Amit Gr...	amit.gr...	CyberA...		Invited	Unkno...	02/11/...	
ariel.tz...	Ariel Tz...	ariel.tz...	CyberA...		Invited	Unkno...	02/12/...	

Actions explanation

Grip operates a browser automation that accesses the SaaS portal to change passwords and manage mailboxes for reset links, OTPs, and additional tasks flows.

Once the new password is generated and changed, it is automatically updated in the WPM account. For more details, please contact the Grip team.

The screenshot shows the 'Account Mapping' configuration page. The left sidebar contains a list of settings: Application Settings, Description, Permissions, Policy, Account Mapping (selected), Advanced, App Gateway, Workflow, Changelog, and Additional Attributes.

Account Mapping

[Learn more](#)

☐ Directory Service Field

☒ All users share one name

☐ Prompt for user name

☐ Account Mapping Script

All users share one name

All users share the following user name

☐ Get password from Safe ⓘ

User Name *

Password *

☐ Allow users to view credentials

Authentication key