



Search for articles...

All Collections > Onboarding and Configuration Guides > Onboarding Guide - CyberArk

Onboarding Guide - CyberArk



Written by Reco Product Management

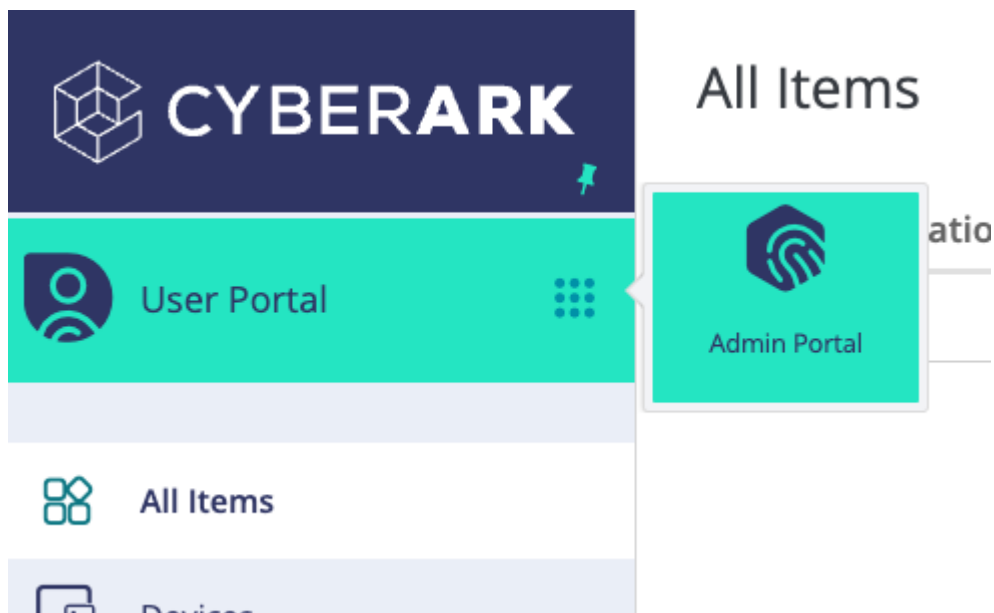
Updated in the last 15 minutes

Prerequisites for Integration

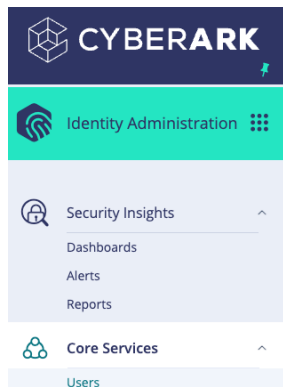
- **CyberArk Admin Role:** Required to access and manage CyberArk settings.
- **Reco Admin Role:** Necessary for setting up and managing the integration within Reco.

Configure CyberArk Identity

1. Login into your CyberArk Identity User Portal using an admin account.
2. Enter the Admin Portal



3. In the sidebar, under "Core Services" -> "Users", click on "Add User"



Users

Search All Invited Users

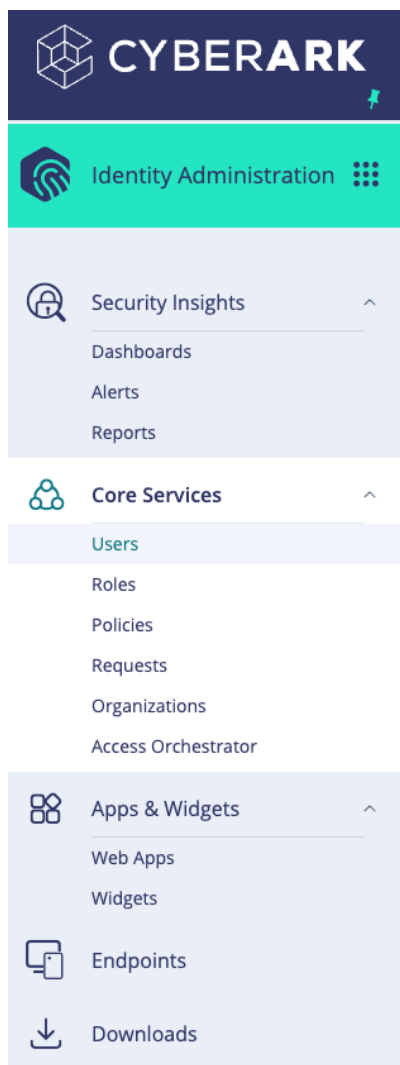
Add User

Login Name ↑	Display name	Email	Source	Organization	Status	Last Invite	Last Login
☐ someone@re...	someone	someone@re...	CyberArk Clo...		Invited	06/02/2024 1...	

4. Before filling in the user details, check the "Is OAuth confidential client" checkbox. The following checkboxes should be automatically changed:

- Send email invite for user portal setup
- Is service user
- Password never expires

5. Fill in the username and password and take note of those credentials. It is recommended to name it "Reco App":



[← 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 * ⓘ

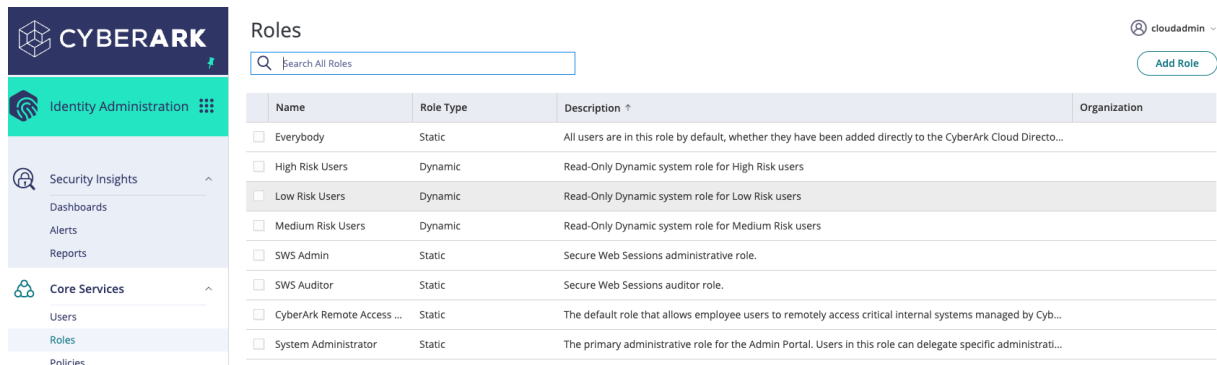
Confirm Password *

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

6. Click on "Create User".

7. In the sidebar, under "Core Services" -> "Roles", click on "Add Role"



CYBERARK

Identity Administration

Security Insights

Core Services

Roles

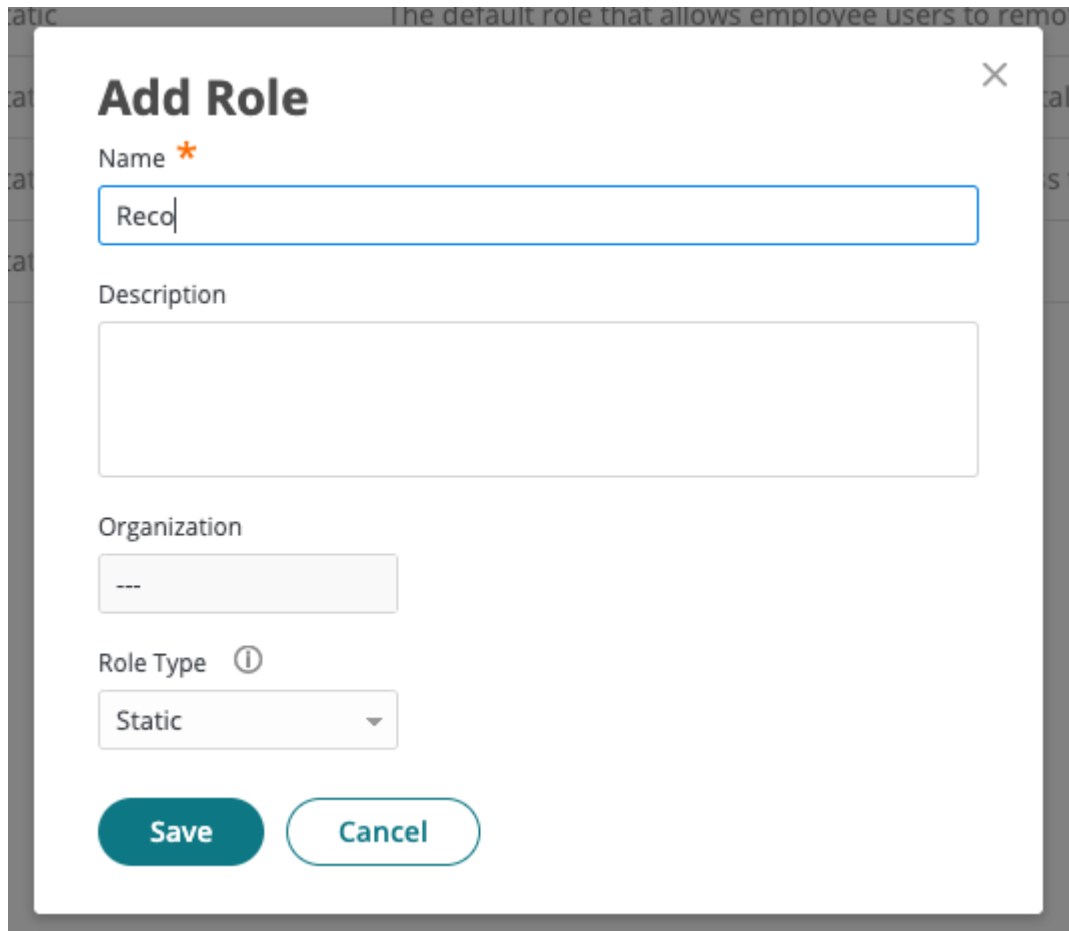
Roles

Search All Roles

Add Role

Name	Role Type	Description	Organization
☐ Everybody	Static	All users are in this role by default, whether they have been added directly to the CyberArk Cloud Directo...	
☐ High Risk Users	Dynamic	Read-Only Dynamic system role for High Risk users	
☒ Low Risk Users	Dynamic	Read-Only Dynamic system role for Low Risk users	
☐ Medium Risk Users	Dynamic	Read-Only Dynamic system role for Medium Risk users	
☐ SWS Admin	Static	Secure Web Sessions administrative role.	
☐ SWS Auditor	Static	Secure Web Sessions auditor role.	
☐ CyberArk Remote Access ...	Static	The default role that allows employee users to remotely access critical internal systems managed by Cyb...	
☐ System Administrator	Static	The primary administrative role for the Admin Portal. Users in this role can delegate specific administrati...	

8. Name the role "Reco". You can also add a meaningful description if you like. Leave all other fields with their default value



Add Role

Name *

Reco

Description

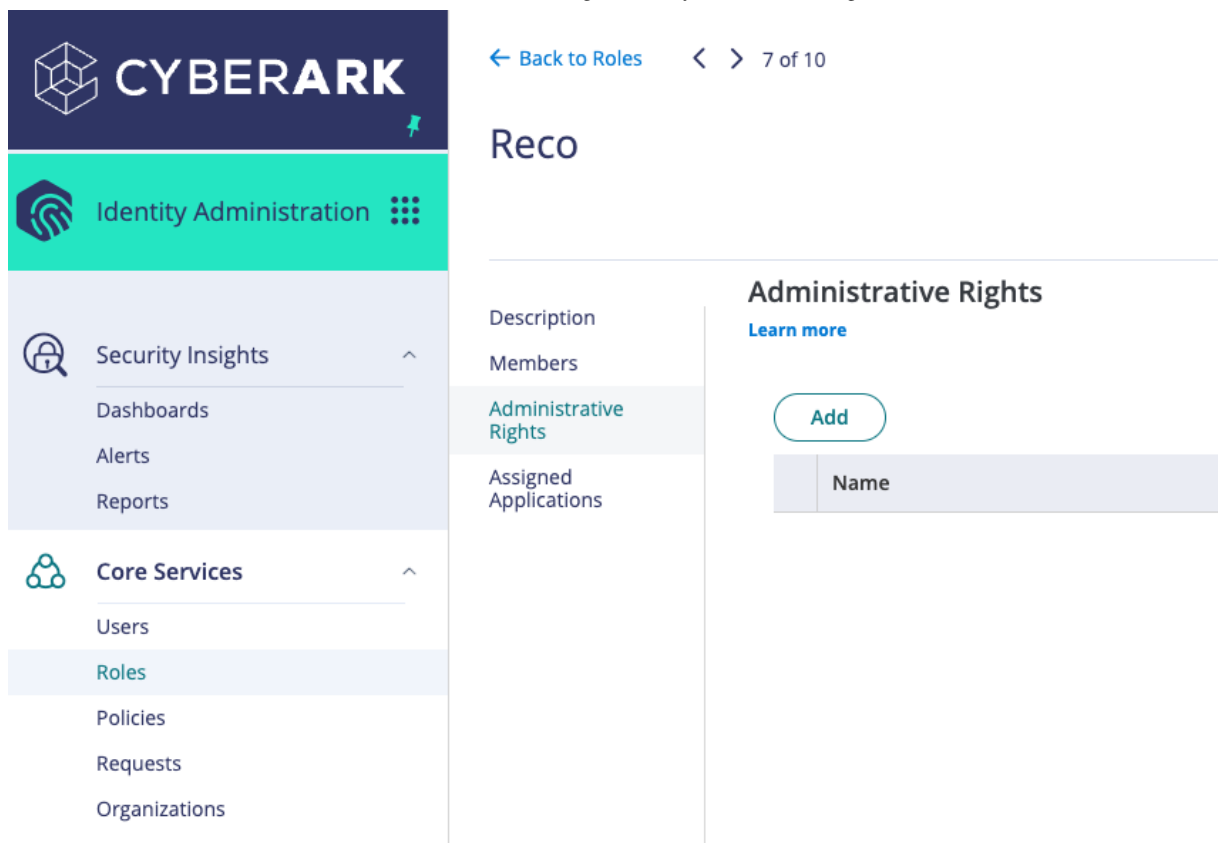
Organization

Role Type ⓘ

Static

Save Cancel

9. Click on "Administrative Rights" and then on "Add"



CYBERARK

Identity Administration

Security Insights

Dashboards

Alerts

Reports

Core Services

Users

Roles

Policies

Requests

Organizations

Back to Roles

7 of 10

Reco

Description

Members

Administrative Rights

[Learn more](#)

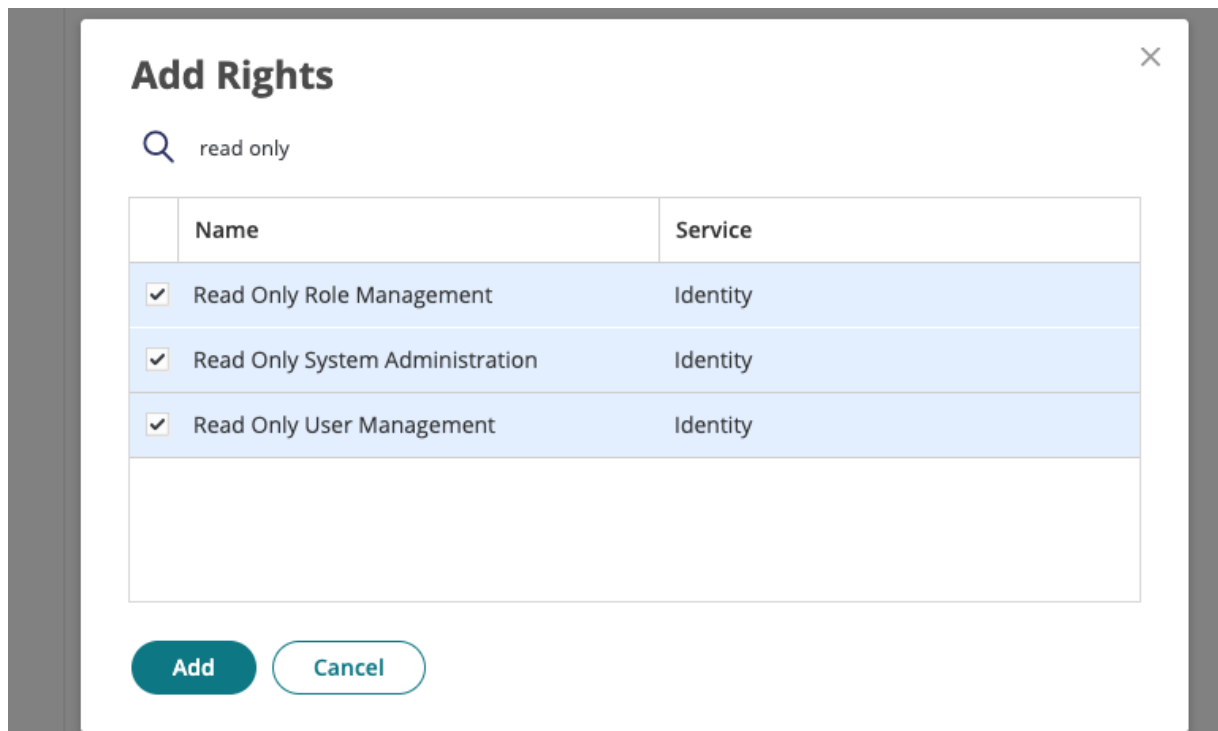
Add

Name

10. In the pop-up dialog search and enable all the following rights:

- "Read Only Role Management"
- "Read Only System Administration"
- "Read Only User Management"

11. Click on "Add"



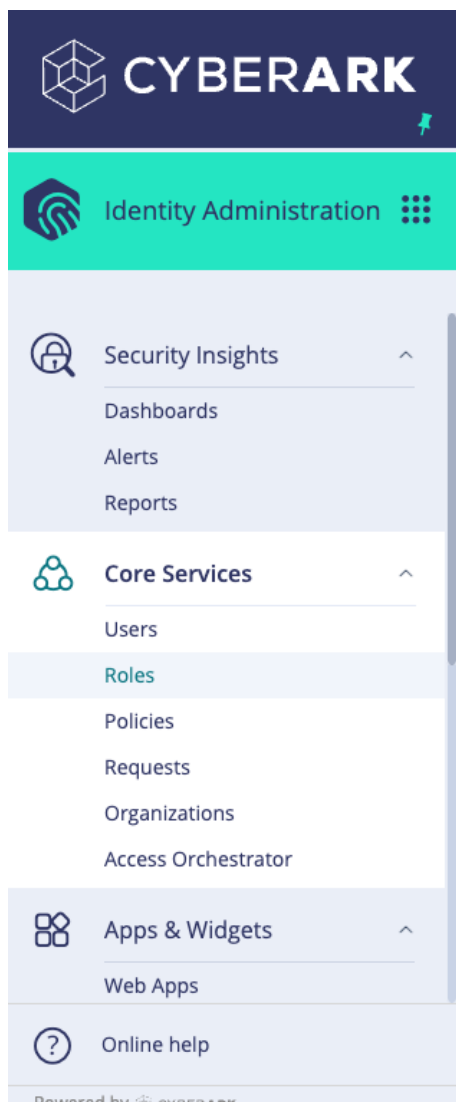
Add Rights

read only

Name	Service
☒ Read Only Role Management	Identity
☒ Read Only System Administration	Identity
☒ Read Only User Management	Identity

Add Cancel

12. At the bottom of the page, click on "Save"

[Back to Roles](#)

< > 7 of 10

Reco

Description

Members

Administrative Rights

Assigned Applications

Administrative Rights

[Learn more](#)

Add

Name

☐ Read Only Role Management☐ Read Only System Administration☐ Read Only User Management

Save

Cancel

Integrating with Reco

In the CyberArk integration, pop-up screen in Reco fill in the username and password of the service user you have created above. After that, fill in your CyberArk domain (including "https://")

Connect New CyberArk Integration

[Documentation](#)

Tenant

Choose tenant

Status

DISABLED

Connection Details

[Upload JSON File](#)

OR

Username *

Password *

Domain *

Test

Connect

Click on "Test" to verify your credentials. If everything goes well, you can click on "Connect".

Did this answer your question?



Reco

in