

Cross Identity - CyberArk

INTEGRATION **CROSS**IDENTITY

Publication Date: 11/09/2025

CROSS IDENTITY | INFANTRY TECHNO PARK, AL-RAZACK GROUP, 104, INFANTRY RD,
TASKER TOWN,SHIVAJI NAGAR, BENGALURU, KARNATAKA 560001

Table of Contents

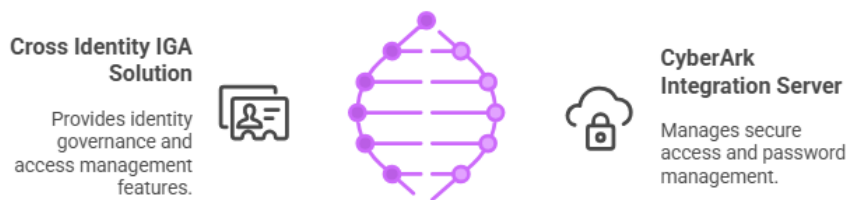
1. CI – CyberArk Integration Overview.....	3
2. CI – CyberArk Integration Benefits	3
3. CI – CyberArk Integration Architecture	4
4. CI – CyberArk Integration Use Cases	5
5. Configure CID Communication Agent.....	6
6. Install the CIDAgent	6
7. Integration Configuration	8
8. Cross Identity Access Request Module	10
9. Cross Identity - Access Review Module	13
10. Cross Identity - Reports Module.....	14

CROSS IDENTITY

1. CI – CyberArk Integration Overview

The CyberArk Privileged Access Solution is integrated with Cross Identity helps to provides a Centralized view of both regular user access and Privilege user access, access request for Privileged Access, multi-level approval, Access Review for Privileged access and Compliance reports. It also provides centralized management for all Identities, CyberArk accounts and groups to ensure it aligns with organizations regulatory compliance.

CyberArk Integration Framework



Cross identity integrated with CyberArk by using connector (CyberArk version 14), and it is working as expected. The following use cases have been successfully tested:

- Reconciliation
- Create account
- Modify account
- Suspend account
- Restore account
- Add entitlement
- Remove entitlement

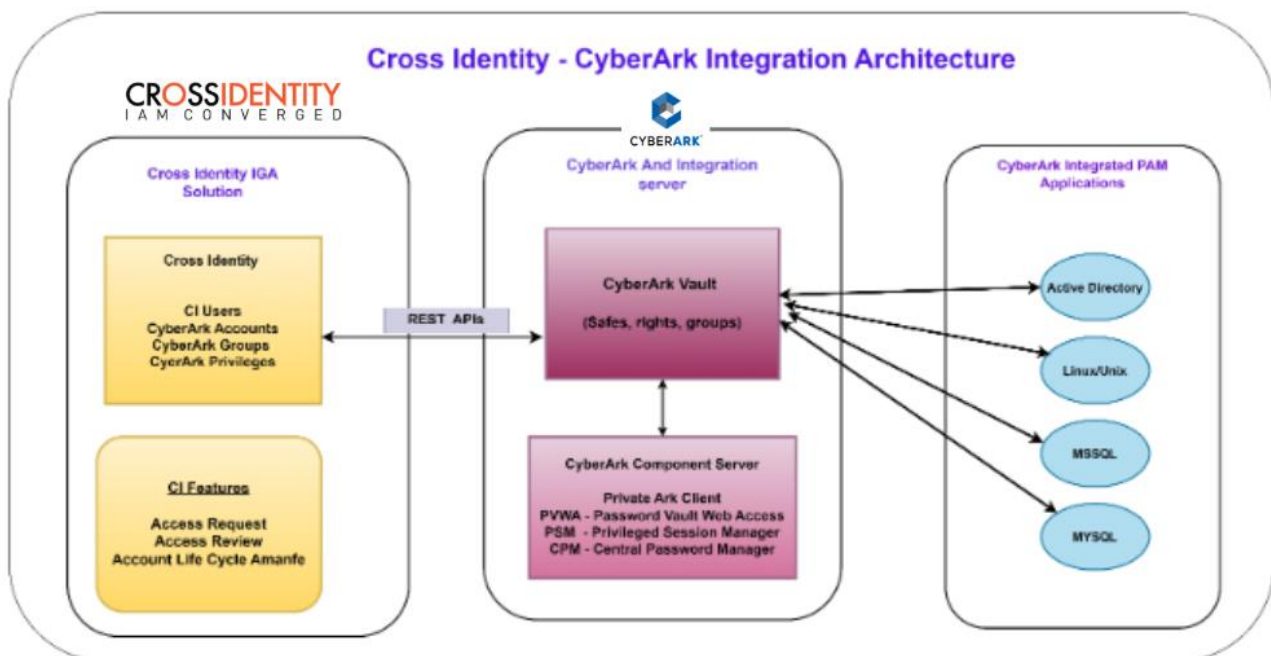
2. CI – CyberArk Integration Benefits

Cross Identity's integration with CyberArk provides organizations with a unified framework to securely manage privileged and non-privileged accounts. The key benefits include:

1. **Centralized Visibility**
 - A single dashboard to monitor and track both privileged and standard user accesses.
 - Helps administrators maintain a complete inventory of accounts and permissions.
2. **Streamlined Privileged Access Provisioning**
 - Privileged account provisioning can be automated based on user roles or triggered through access requests.
 - Multi-level approval workflows ensure that access is granted only after proper validation.
3. **Effective Access Reviews**

- Reviewers can evaluate privileged users' access rights to ensure alignment with the principle of least privilege.
 - Verification ensures that users retain access only to the safes and target applications they legitimately require.
4. **Risk Reduction and Compliance Alignment**
- Eliminates redundant processes by centralizing privileged access management.
 - Proactively identifies and closes security gaps to reduce exposure to insider threats and external attacks.
5. **Automated Policy Enforcement**
- Policies for privileged access are automatically applied, ensuring consistent security practices.
 - Violations or anomalies are detected quickly, enabling corrective actions before they escalate into risks.

3. CI – CyberArk Integration Architecture



Cross Identity IGA Solution

- **Components Managed:**
 - CI Users
 - CyberArk Accounts
 - CyberArk Groups

- CyberArk Privileges
- **Core Features:**
 - Access Request
 - Access Review
 - Account Life Cycle Management

This ensures that privileged accounts and entitlements in CyberArk can be managed just like any other identity within CI.

4. CI – CyberArk Integration Use Cases

The Cross Identity and CyberArk integration enables multiple identity lifecycle and governance use cases that strengthen security, improve compliance, and streamline operations:

1. **Account Creation & Provisioning**
 - CyberArk accounts can be provisioned directly through Cross Identity using **role-based provisioning** or **end-user access requests**.
 - Ensures that privileged accounts are created with consistent policies and approval workflows.
2. **Group Assignment with Approvals**
 - Administrators or end-users can request additional group memberships for CyberArk accounts.
 - Requests are routed through **multi-level approval workflows**, providing strong governance over privileged access.
3. **Account Reconciliation**
 - Cross Identity can automatically **collect and synchronize all CyberArk accounts** into its identity repository.
 - This ensures that the CI platform has a complete and up-to-date view of privileged accounts.
4. **Entitlement & Group Mapping Reconciliation**
 - Privileged groups and account-to-group mappings from CyberArk are reconciled into Cross Identity.
 - Provides administrators with clear visibility of entitlements and their associated users.
5. **Access Review for Privileged Accounts**
 - Managers and reviewers can conduct **periodic access reviews** of CyberArk accounts.
 - Access certifications help ensure that users have only the necessary privileges, supporting compliance audits.
6. **Access Suspension or Removal**
 - Privileged account access can be **suspended or revoked** directly through the Access Review process.
 - Prevents unauthorized continued access when roles or responsibilities change.
7. **Automatic Account De-provisioning**
 - When a user is terminated in Cross Identity, the associated CyberArk account is **immediately disabled or deleted**.
 - Eliminates orphaned privileged accounts, reducing insider threat risks.

8. Compliance Reporting

- Cross Identity generates detailed **compliance and audit reports** showing users, their CyberArk accounts, and entitlements.
- Reports can be exported in Excel or PDF formats to support regulatory audits and internal governance.

5. Configure CID Communication Agent

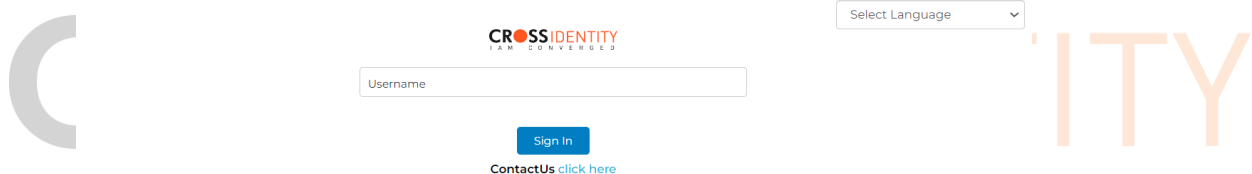
Cross Identity (CI) is a cloud hosted solution. To enable Cross Identity to communicate to on-premises applications like Active Directory (AD) as well as to other cloud applications it is essential that a data communication component ties these three together.

This is accomplished via an on-premises agent that needs to be downloaded and installed. This document describes the steps needed to achieve this.

To begin, use any internet connected system running 64-bit Windows for the installation.

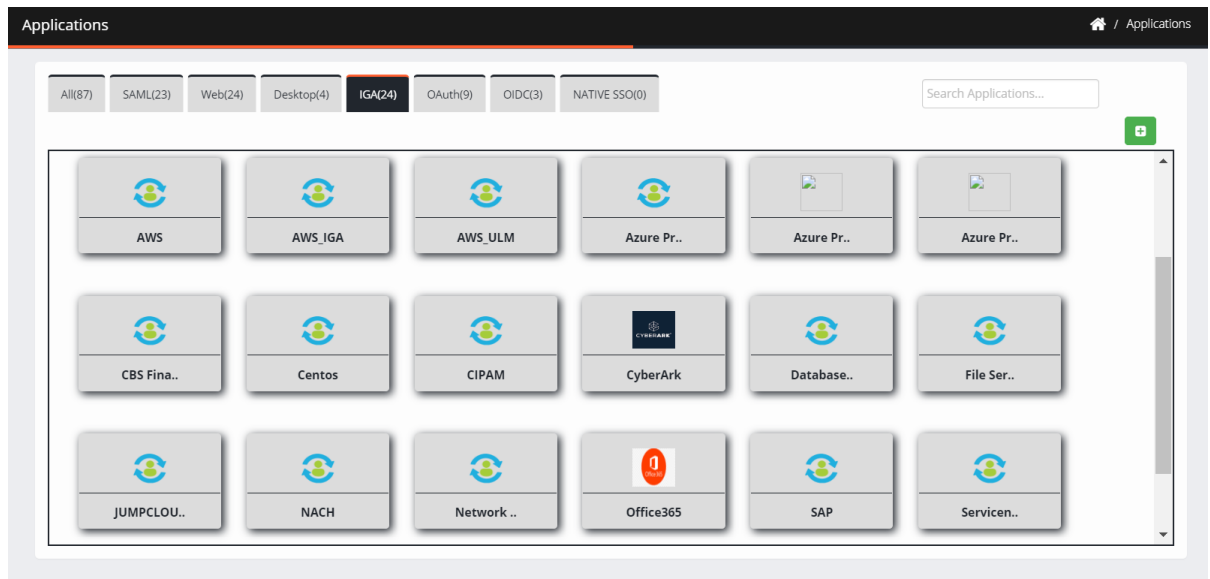
6. Install the CIDAgent

1. Login to Cross Identity from the End-user Portal using end user credentials.

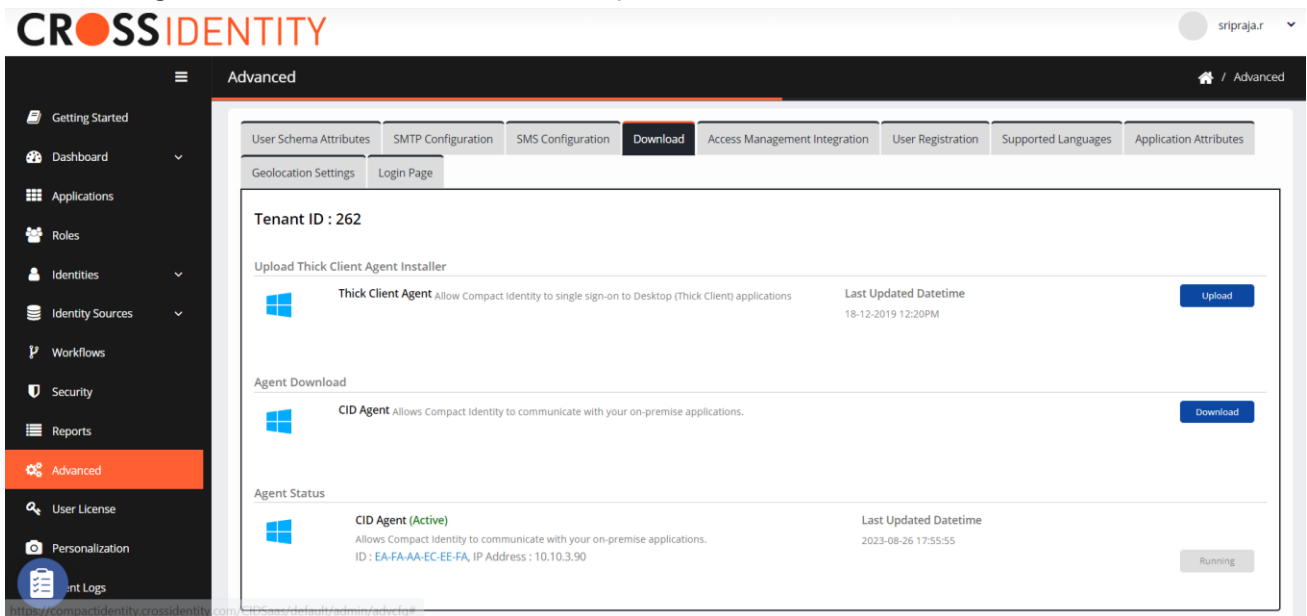


2. If the End-user has privileges to be an admin, the user will be able to see the 'Go to admin console' button on their end-user landing page.

Note: After Clicking on the 'Go to admin console' button the user will land on the Application's page.



3. Navigate to "Advanced" from the left menu pane then Click on the "Download" tab



Note: the "Tenant ID" that is displayed – "Tenant ID: 262".

4. Note the list of Agents, Download the "CID Agent" (~350MB download).
5. To Install the agent, administrator privileges on the server will be needed.
6. When prompted to enter the "Tenant ID", enter the one you noted in step 4.
7. You can change the suggested HTTP and HTTPS ports. Save and you are ready to go.
8. After Completing the above Installation process, check the status of the agent in the same Download tab. Status could be Active and Running or Inactive.

7. Integration Configuration

1. When the user logs into CID as an Admin, the admin user will land on the Application's page as seen below.
2. From the menu on the left side, select 'Applications', then select the IGA tab.
3. On the IGA tab, Select the CyberArk Application.
4. Update Applications name, Application Logo, CyberArk tenant URL, admin username, password , port number in application configuration page.

CyberArk

Application Configuration | Application Account Attributes | Application Authorization | Accounts | Reconciliation | Entitlements | License | Application Attributes | Reconciliation Status

Application Name*
CyberArk

Connector War Name
CYBERARK2.war
Download Warfile

Application Logo*
Choose File | No file chosen

URL*
https://services-uscentral.skytap.com

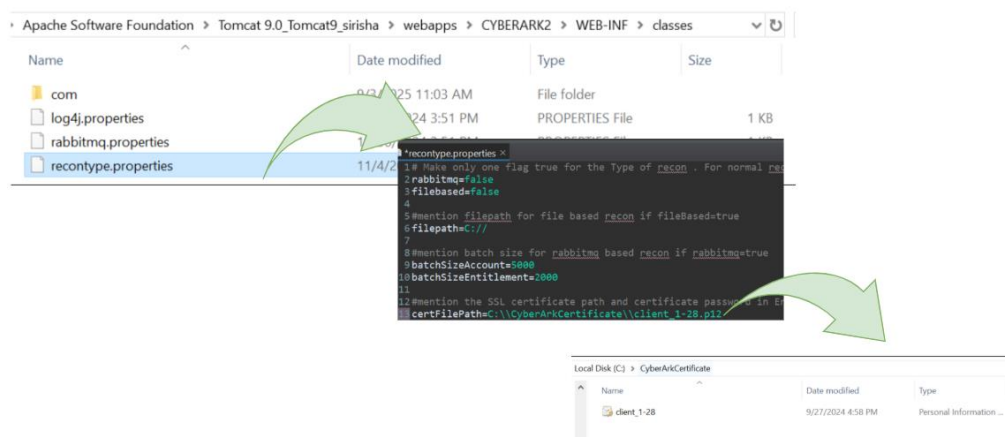
Username*
Administrator

Password*
.....

Port Number*
19189

Save

Please note: The SSL certificate should be in the cyberArk connector to enable a secure channel.



- Configure the Application Account Attributes as seen below to map application attributes to Cross Identity attributes.

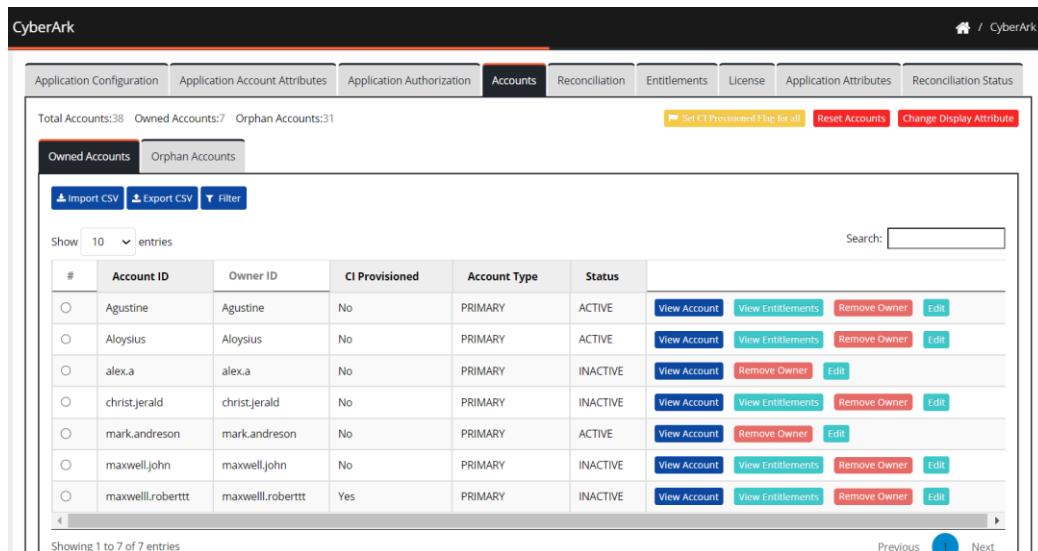
Account Attribute	Mapping	Evaluation Operation	Sync with User Profile Attribute	
User Name(username)	User Profile Attribute Username	Both	☐	
First Name(firstName)	User Profile Attribute First Name	Both	☐	
Last Name(lastName)	User Profile Attribute Last Name	Both	☐	
Middle Name(middleName)	User Profile Attribute Middle Name	Both	☐	
Email(homeEmail)	User Profile Attribute Email Address	Both	☐	
mobile(homeNumber)	User Profile Attribute Mobile	Both	☐	

- Configure the reconciliation attributes as seen below. These will be used to populate account attributes in Cross Identity and give the priority.

- The Run button on the upper left of the screen is used to manually reconcile the Account and Entitlements from CyberArk. We also have the option to schedule reconciliation.

User Profile Attribute	Application Attribute	Priority	
Username	Application Attribute User Name(username)	1	

- Once reconciled, the Cross identity admin can view the Account and Entitlements from CyberArk.



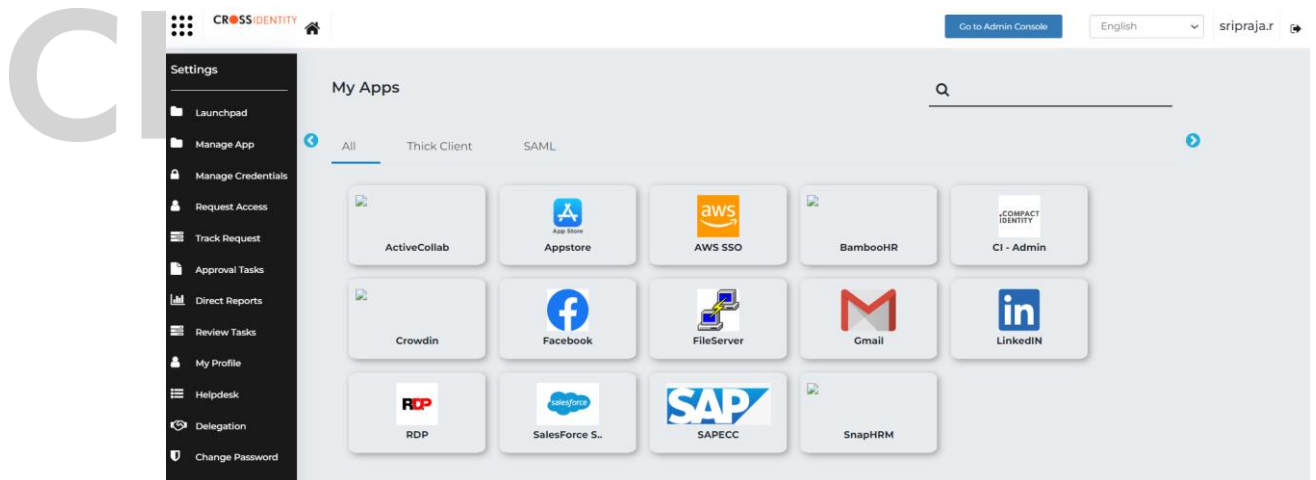
The screenshot shows the CyberArk Accounts Management interface. At the top, there are tabs for Application Configuration, Application Account Attributes, Application Authorization, **Accounts**, Reconciliation, Entitlements, License, Application Attributes, and Reconciliation Status. Below the tabs, it displays 'Total Accounts:38', 'Owned Accounts:7', and 'Orphan Accounts:31'. There are buttons for 'Set CI Provisioned Flag for all', 'Reset Accounts', and 'Change Display Attribute'. The 'Owned Accounts' tab is selected, showing a table of accounts with columns for #, Account ID, Owner ID, CI Provisioned, Account Type, and Status. Each row has action buttons: View Account, View Entitlements, Remove Owner, and Edit.

#	Account ID	Owner ID	CI Provisioned	Account Type	Status
○	Agustine	Agustine	No	PRIMARY	ACTIVE
○	Aloysius	Aloysius	No	PRIMARY	ACTIVE
○	alex.a	alex.a	No	PRIMARY	INACTIVE
○	christ.jerald	christ.jerald	No	PRIMARY	INACTIVE
○	mark.andreson	mark.andreson	No	PRIMARY	ACTIVE
○	maxwell.john	maxwell.john	No	PRIMARY	INACTIVE
○	maxwell.roberttt	maxwell.roberttt	Yes	PRIMARY	INACTIVE

8. Cross Identity Access Request Module

In Cross Identity, an end-user can request Access for any application. Based on the workflow configuration, it will go through a single level or multi-level approval process. Once approved access will be provisioned in the target application. Here is the process.

1. End-User should log into Cross Identity with username and password.
2. On the left side menu, click on Request Access.



3. Select any of the 4 entities for the access request (Note: This is Shown for CyberArk application and Entitlement).

Request Access

Roles **Application and Entitlement** Identity

Request Access for self Request Access for others

Show entries Request Access

Search:

#	Name
☐	Active Directory
☐	active_test
☐	AWS
☐	AWS_IGA
☐	AWS_ULM
☐	Azure Provisioning
☐	CBS Finacle
☐	Centos
☐	CIPAM
☐	CyberArk

Showing 1 to 10 of 15 entries Previous **1** 2 Next

- The End User can select the access that is required. He can either request an Application Account or an Account with Entitlement (Auditors) Access.

Application and Entitlements X

I want to request for:

☐ Application Account

☒ Application Account with Entitlement ?

Entitlements: Q

Notification Engines (CyberArk)

PVWAMonitor (CyberArk)

PVWAUsers (CyberArk)

PVWAGWAccounts (CyberArk)

PVWAAppUsers (CyberArk)

»

»

«

«

Auditors (CyberArk)

☐ Permanent Access

Access Request For: Days

Comment/Justification*

✍

Back Submit

- The End-User should provide the information in the comment/Justification field to justify the request, After Completing the information, Click Submit.
- The End-User can also track their requests made by selecting 'Track Request' from the left side of the menu pane. In the Track Request, the end-user can check who is the Approver and the status of the access request.
- Once the request is submitted. The request goes to the manager or Approver for approval as

per the Cross Identity workflow configuration.

Pending Approvals Past Approvals

Show 10 entries

Delegate Request Approve Request Deny Request

#	Request for	Access Type	Requested By	Requested For
☐	API based Role	ROLE	george.allan	george.allan
☐	API based Role	ROLE	Immanuel	Immanuel
☐	API based Role	ROLE	test.one	test.one
☐	API based Role	ROLE	abinaya.r	abinaya.r
☐	Auditors	ENTITLEMENT	mark.andreson	mark.andreson
☒	Auditors	ENTITLEMENT	allan.paul	allan.paul
☐	AWS_ULM	APPLICATION	akash.jain	akash.jain
☐	CT_IT Infra	ENTITLEMENT	Immanuel	Immanuel
☐	CT_IT Infra	ROLE	Immanuel	Immanuel
☐	CT_IT Infra	ENTITLEMENT	Austin	Austin

Showing 11 to 20 of 73 entries Previous 1 2 3 4 5 ... 8 Next

© Copyright 2022 Ilantus Technologies Private Limited v22.42.04 Powered By Ilantus

8. When the manager or Approver logs in, he will be able to see access request that is pending for his approval.
9. The Approver can either approve or deny the request or can delegate the requests, as shown above for Access Request Approval.
10. The Approver selects an Approve Request item, then there will be an option to update comments.

Pending Approvals Past Approvals

Show 10 entries

Approve Request Deny Request

Request ID: 1465
 Requestor: allan.paul
 Requested Access: Auditors
 Asset: CyberArk1
 Access Type: ENTITLEMENT
 Access Duration(Days): 30
 Time of request: Wed Dec 07 06:49:39 UTC 2022
 Comments/Justification from Requestor: Please Provide Access to Auditors Entitlement.

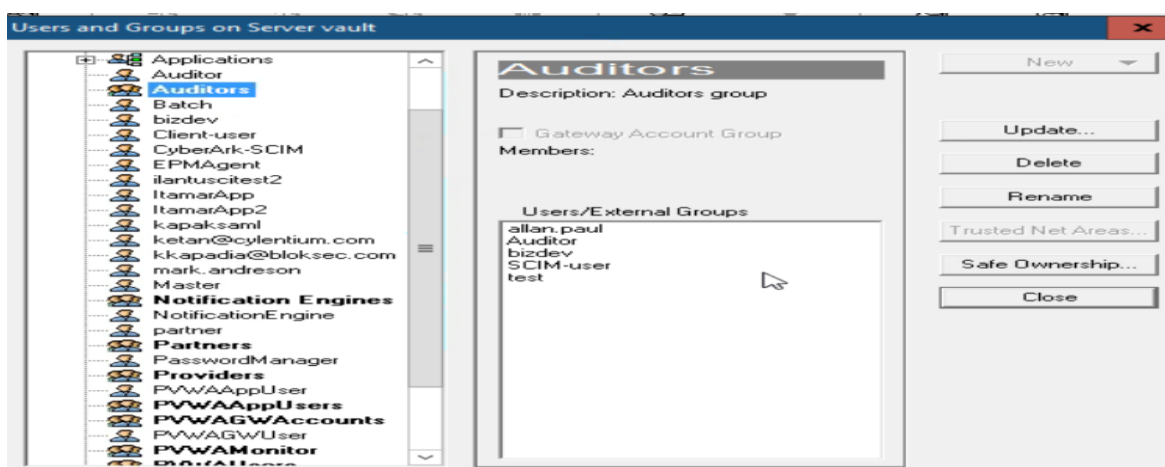
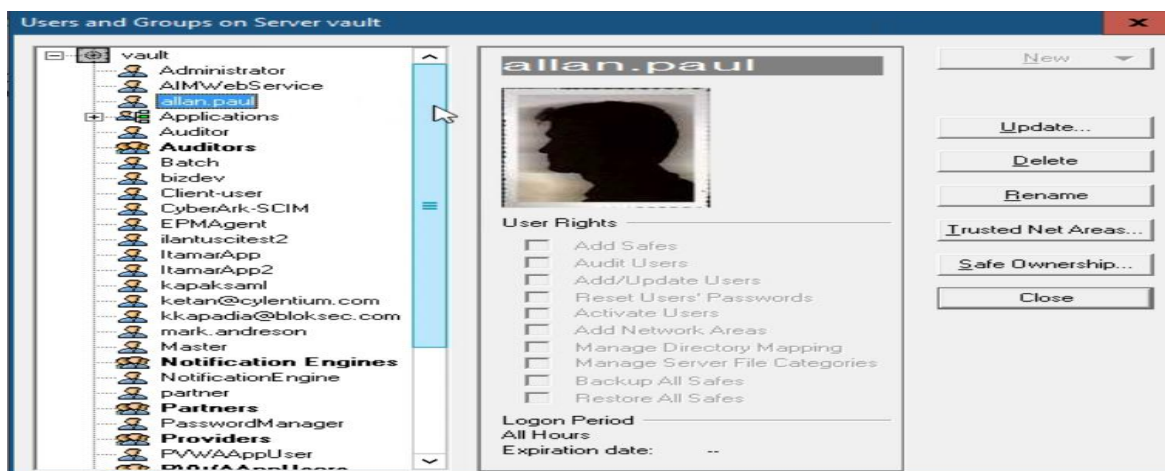
☐ No change
 ☐ Permanent access
 ☒ No. of Days 30

Your comments/justification:

Your request is approved for Auditors Entitlement

Showing 11 to 20 of 73 entries Previous 1 2 3 4 5 ... 8 Next

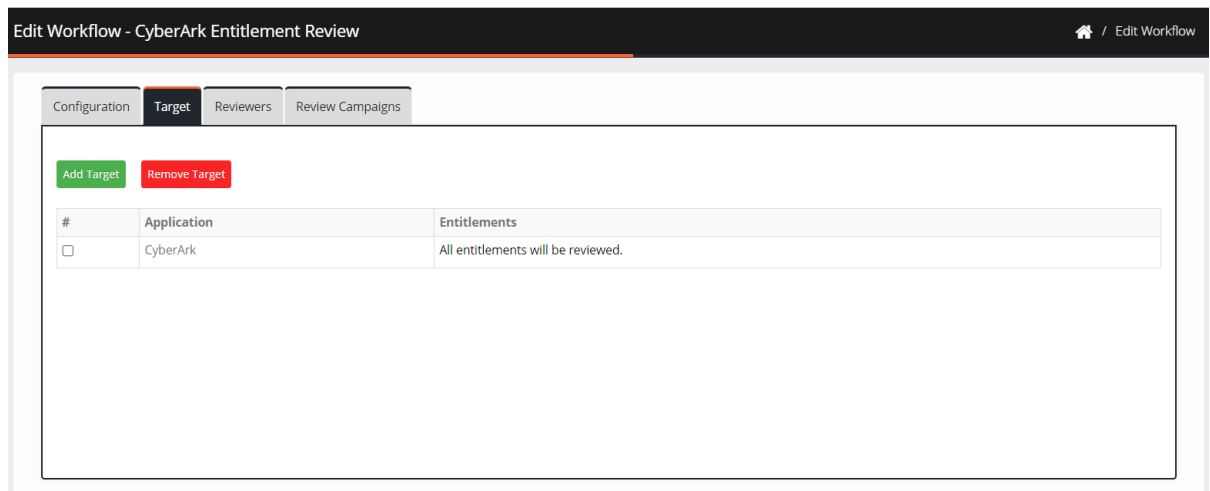
11. Once the Approver approves the request the access will be provisioned in CyberArk.



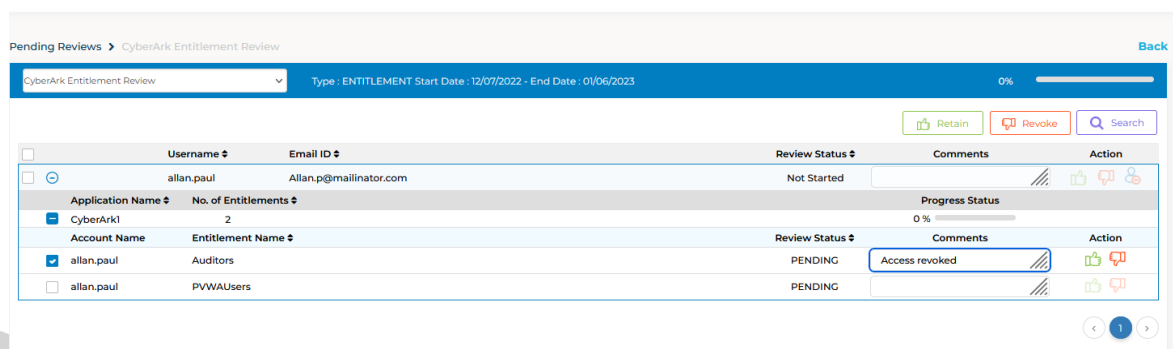
9. Cross Identity - Access Review Module

In Cross Identity, the admin can configure different types of access reviews such as –

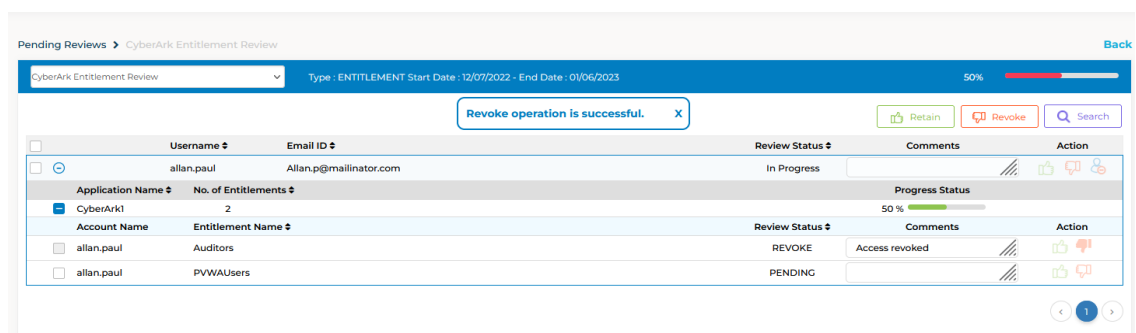
- User Access Review – Manager as reviewer.
 - Application Owner Review – App Owner is the reviewer.
 - Entitlement Review – Manager as reviewer.
 - Role Review – Manager or Any authorized role can review.
1. The admin can configure different types of workflows for Access Review. In this case shown below for an Entitlement Review.



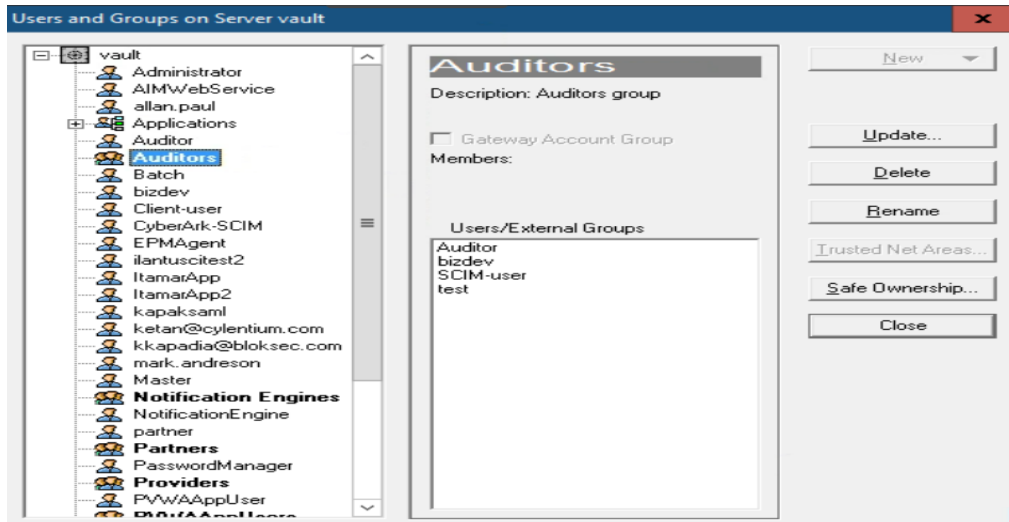
2. Once the admin starts the review, Cross Identity will send email notification to all the reviewers.



3. Once the reviewer logs in to Cross Identity, they will be able to see all their sub-ordinates and their accesses.
4. The reviewer has the option to revoke or retain any of the Accesses.

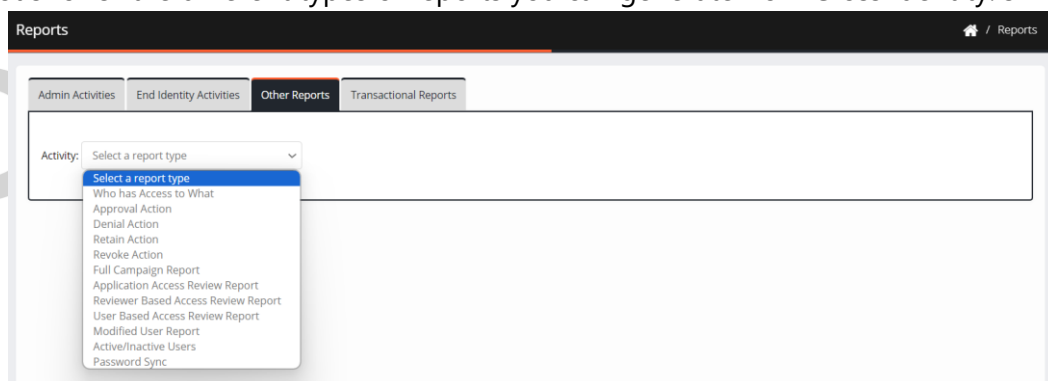


5. If he retains no action is required. If the Reviewers revokes, then the access will be revoked in CyberArk.

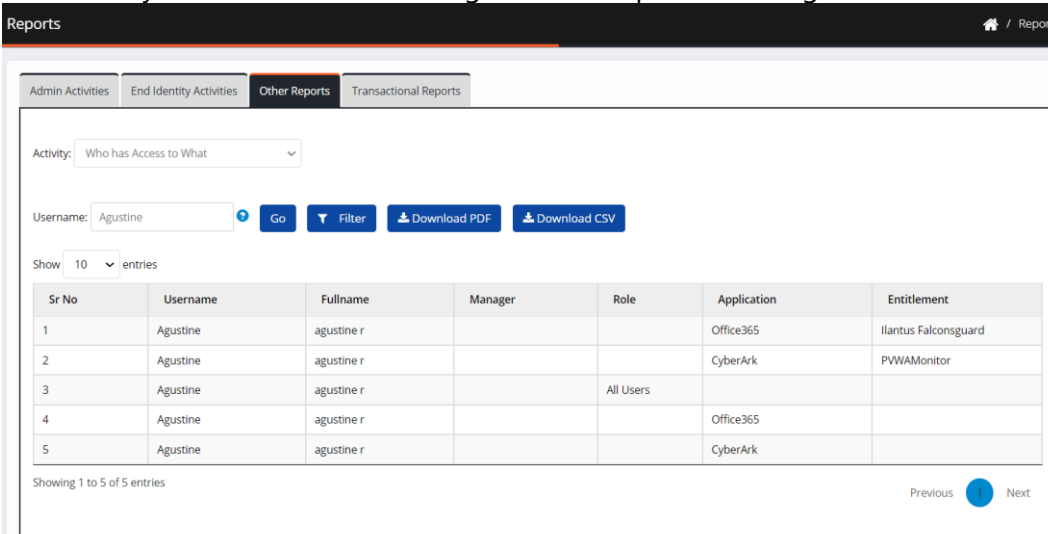


10. Cross Identity – Report Module

We can generate multiple compliance reports from Cross Identity such as reports that show all the users who have AD accounts in the organization and the user's different accesses. The below screenshot shows the different types of reports you can generate from Cross Identity.



1. Cross Identity can drill down and can generate a report for a single user as seen below.



Note the screenshot below for an Access Review status report.

Reports

Home / Reports

Admin Activities

End Identity Activities

Other Reports

Transactional Reports

Activity: Revoke Action

From: To:

Go

Filter

Download PDF

Download CSV

Show 10 entries

Sr No	Reviewee	Reviewer	Access Name	Access Type	Action	Comments	Timestamp
1	queency.r		CyberArk	APPLICATION	REVOKE		Wed Dec 28 07:46:35 UTC 2022
2	queency.r		CyberArk	APPLICATION	REVOKE		Wed Dec 28 07:50:09 UTC 2022
3	queency.r		CyberArk	APPLICATION	REVOKE		Wed Dec 28 08:06:51 UTC 2022

Showing 0 to 0 of 0 entries

PreviousNext

2. Compliance Reports can be generated in either Excel or PDF format.
3. Reports can be customized as per the organization's requirement.

CROSS IDENTITY