

CyberArk Integration

CROSS IDENTITY

Publication Date: 11/11/2024

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

Contents

1. CyberArk Integration Overview	3
2. CyberArk Integration Benefits	3
3. CyberArk Integration Architecture	3
4. CyberArk Integration Use Cases	3
5. Prerequisites	4
6. CyberArk Integration Configuration	4
7. Steps to perform the Reconciliation.....	6
8. Access Request Module.....	8
9. Access Review Module	11
11. Reports Module	12
12. Conclusion.....	13



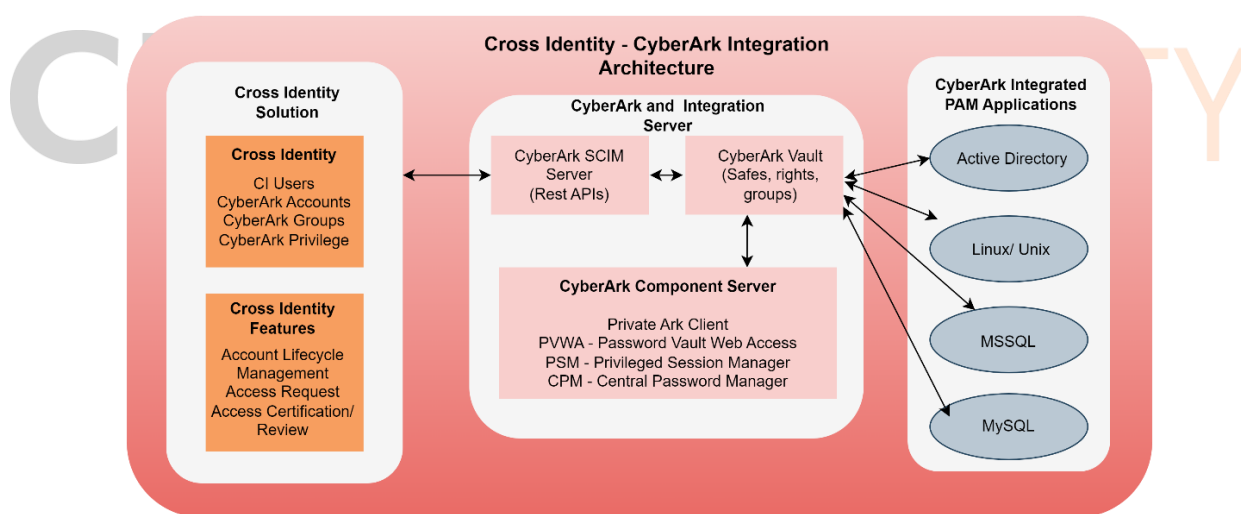
1. CyberArk Integration Overview

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 the centralized management for all Identities, CyberArk accounts and groups to ensure it aligns with organizations regulatory compliance.

2. CyberArk Integration Benefits

- Complete visibility of all privileged and non-privileged accesses with a centralized view.
- Streamline Privileged access provisioning based on user's role or based on Access Request with multi- level Approval.
- Reviewers can review for all privileged user's access and verify certified users have the right access to the right safes to access target application.
- Helps to close security gaps, reduce risk, and eliminate redundant processes related to managing privileged access.
- Automatically enforce user access policies and identify violations on Privilege Access.

3. CyberArk Integration Architecture



4. CyberArk Integration Use Cases

- CyberArk Account can be created from Cross Identity via Access Request or Role based provisioning.
- Assign additional Groups to CyberArk Account via Access Request and multi-level Approval.
- Collect all Accounts from CyberArk via Cross Identity reconciliation.
- Collect all Privileged Groups and CyberArk Account to Group mapping from CyberArk via Cross Identity reconciliation.
- Cross Identity Access Review for all privileged User's access in CyberArk.
- Suspend or Remove CyberArk Account\Accesses via Access Review.

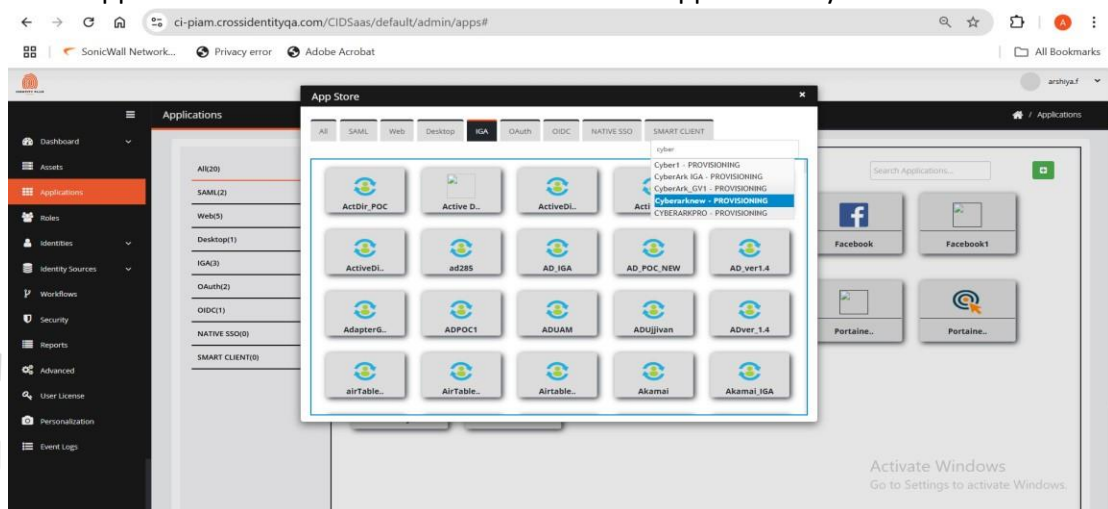
- Automatically delete or disable CyberArk account immediately after user termination.
- Generate Compliance reports for users and their access in CyberArk.

5. Prerequisites

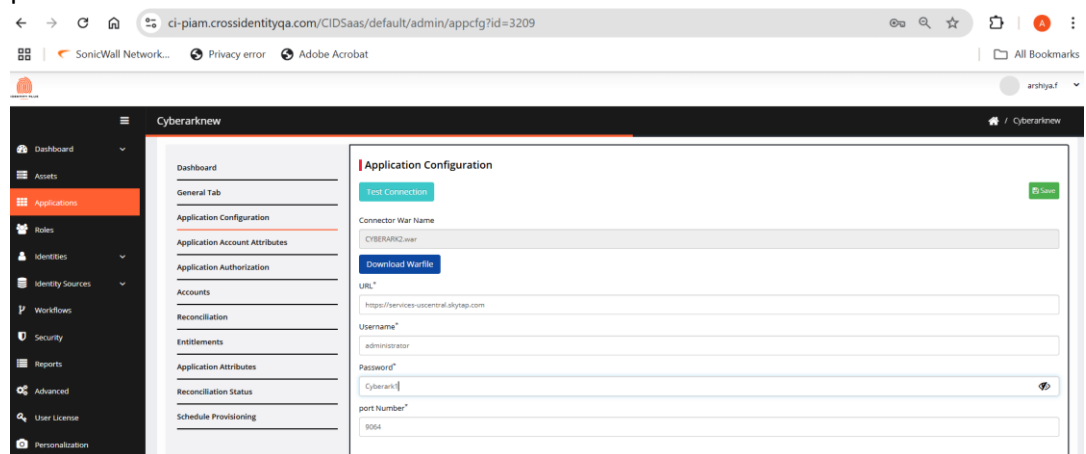
1. Configure CID communication agent.
2. Deploy CyberArk connector on the agent server.
3. Deploy the personal information certificate from CyberArk on agent server.

6. CyberArk Integration Configuration

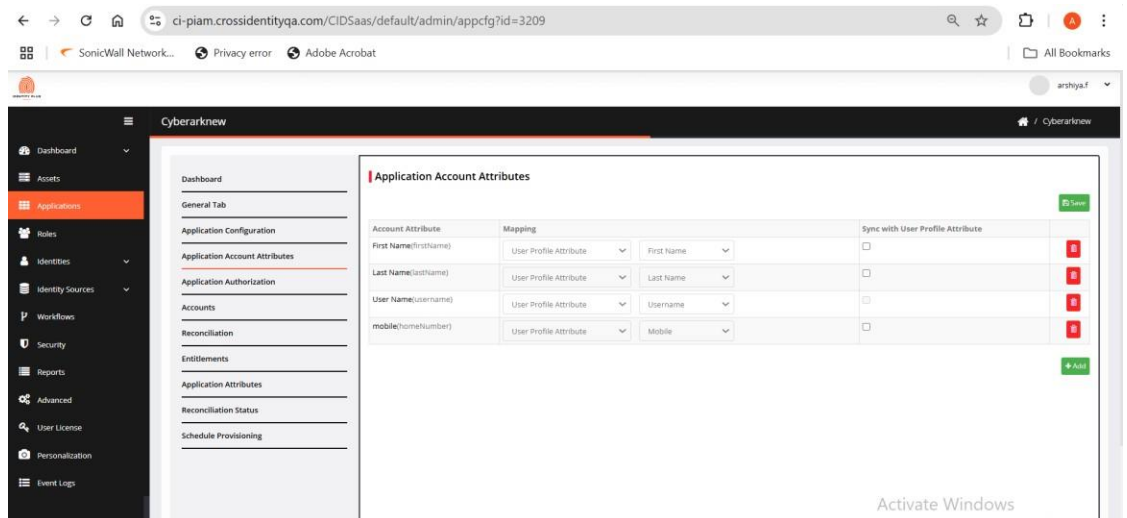
1. Login to CI as admin.
2. Go to Applications tab from the menu. Onboard IGA application CyberArk.



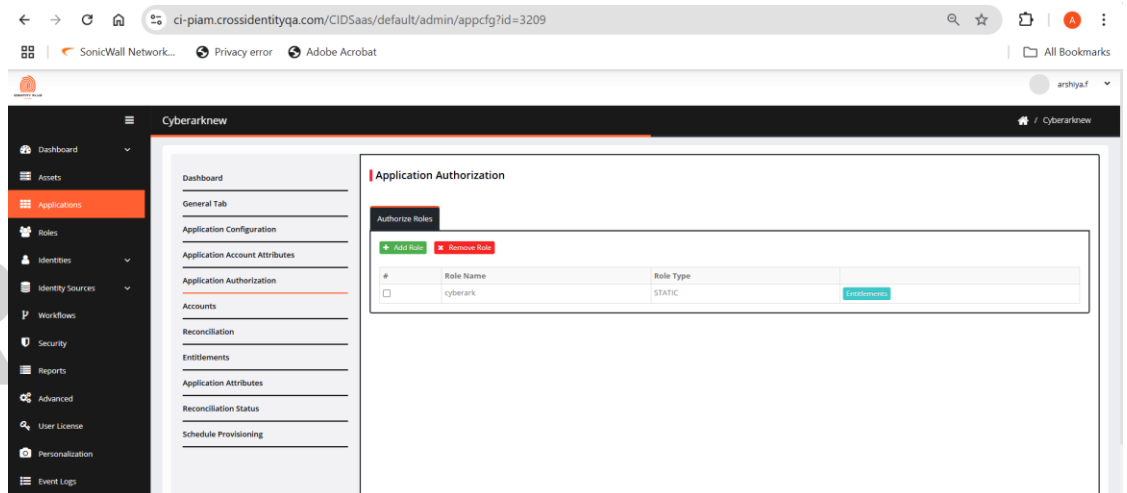
3. Configure CyberArk application as below:
 - a. **Application configuration:** Update CyberArk URL, admin username, password, port.



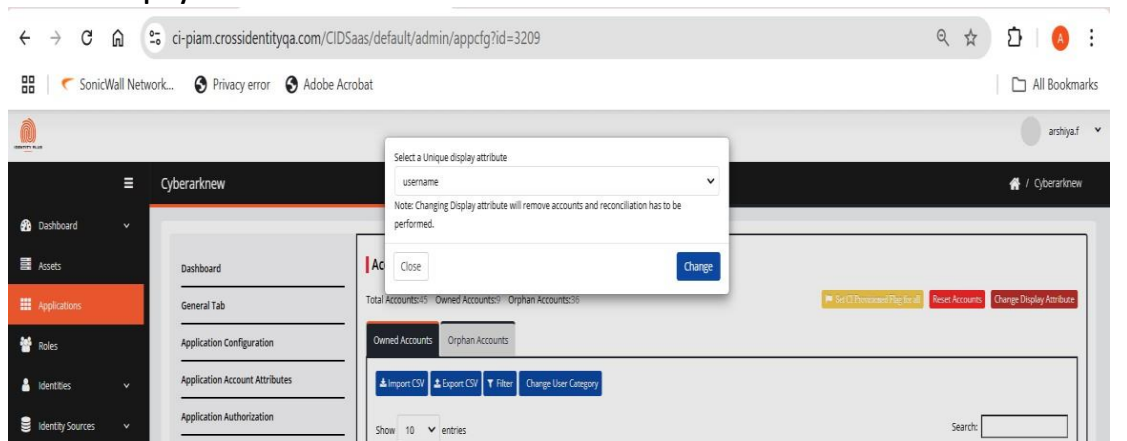
- b. **Application Account Attributes:** Map application attributes to cross identity attributes.



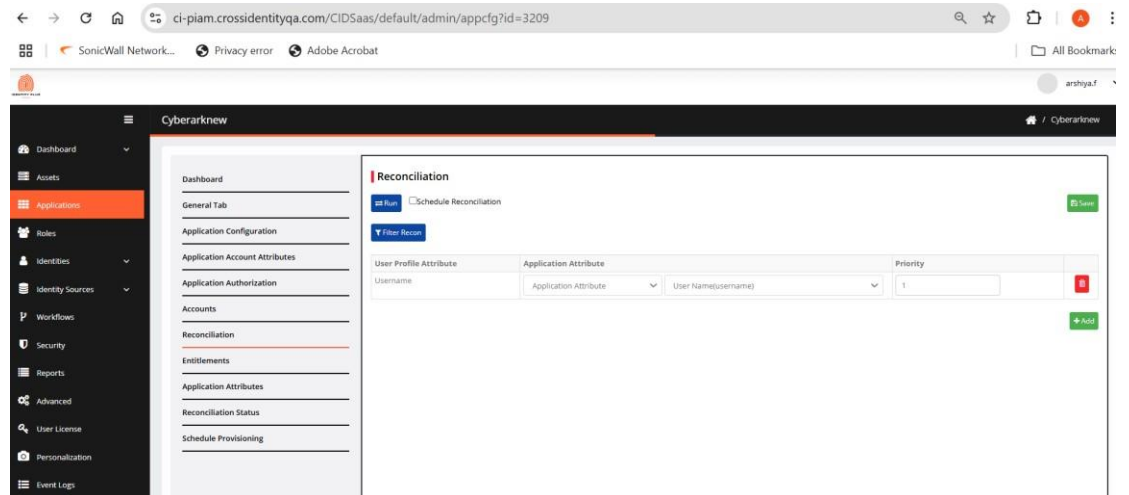
c. Application Authorization



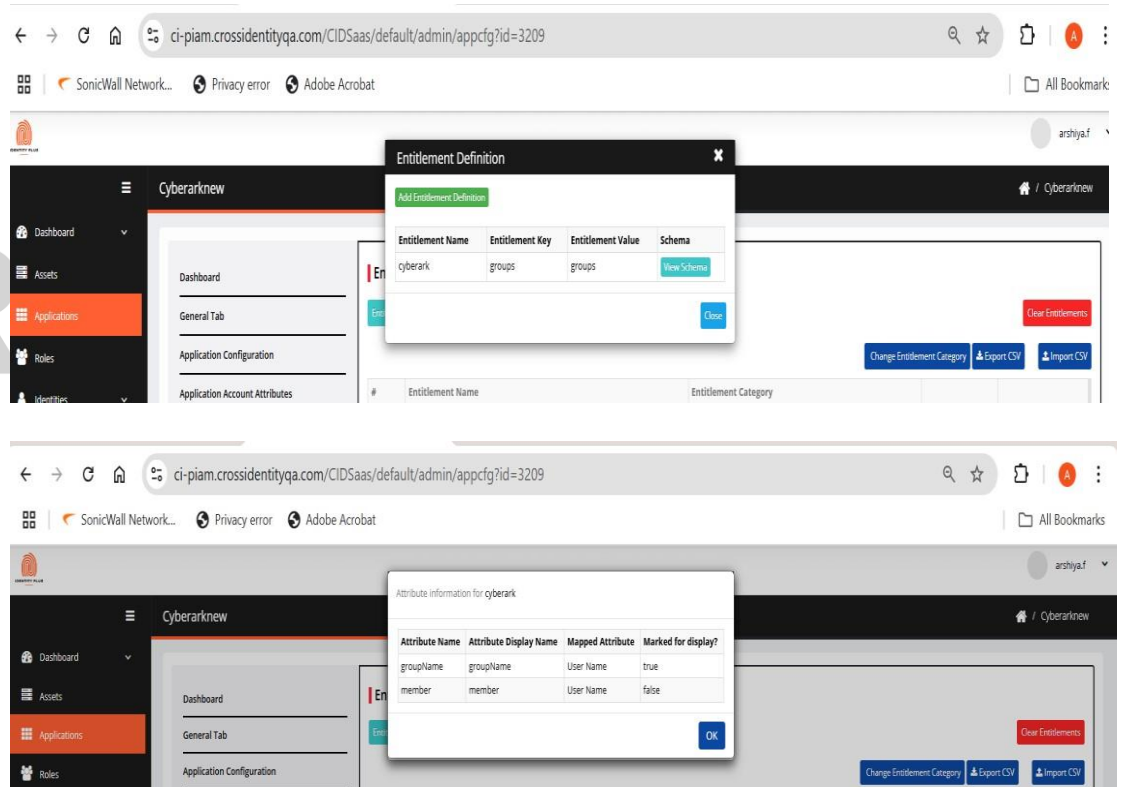
d. Accounts Display attributes



e. Reconciliation

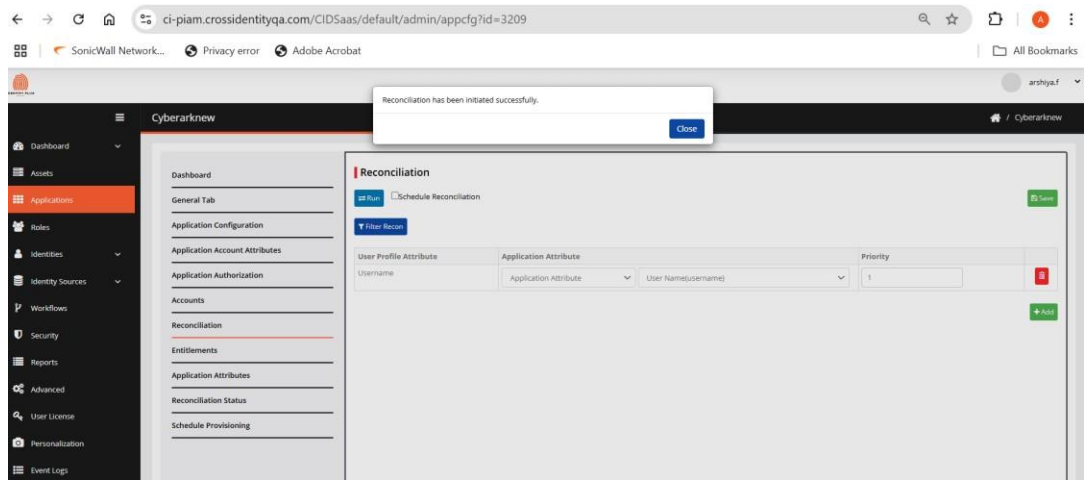


f. Entitlement Definition

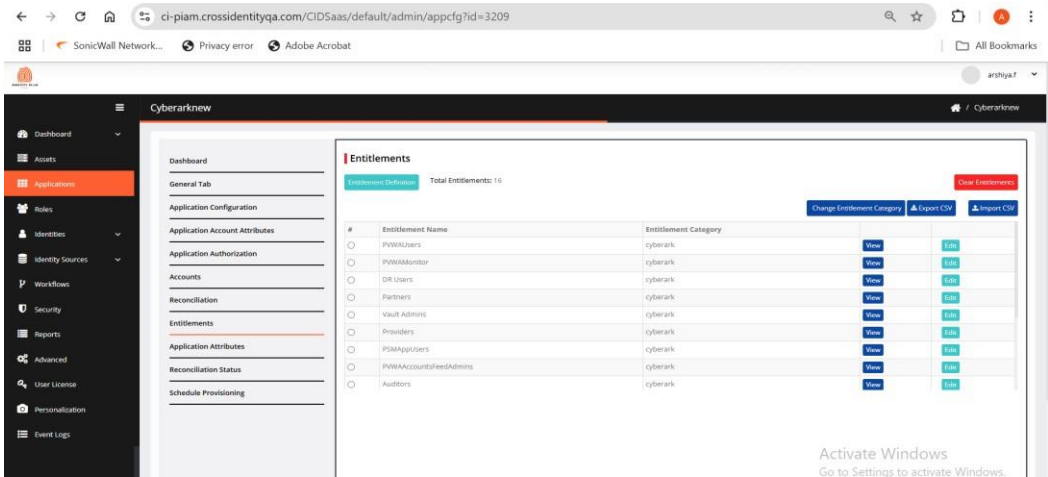
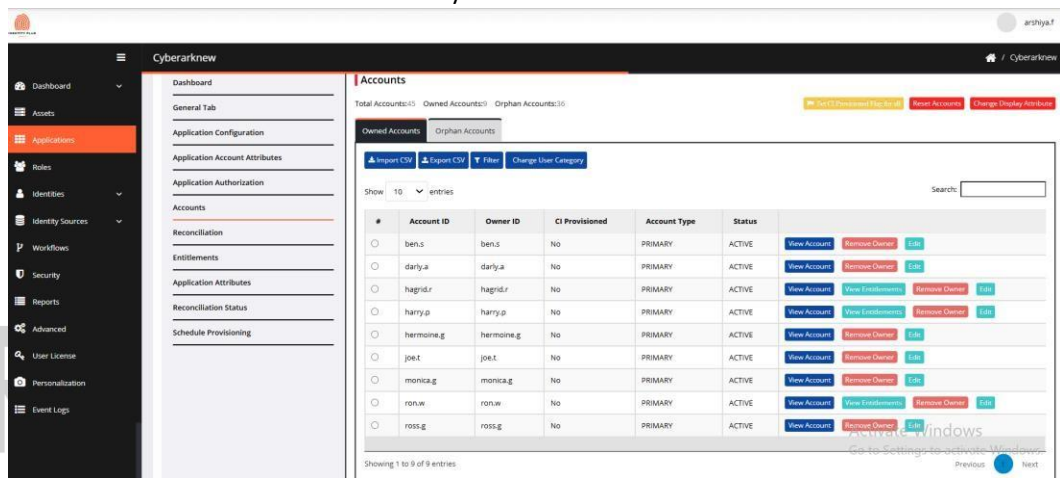


7. Steps to perform the Reconciliation

1. From the Reconciliation tab click on Run to reconcile the Account and Entitlements from CyberArk. We also have the option to schedule reconciliation.



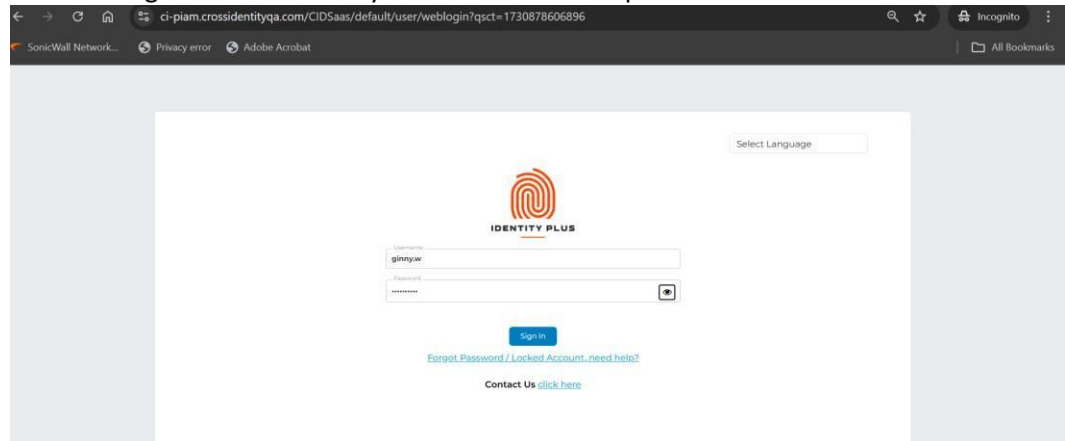
2. All the accounts and entitlements from CyberArk are fetched into CI.



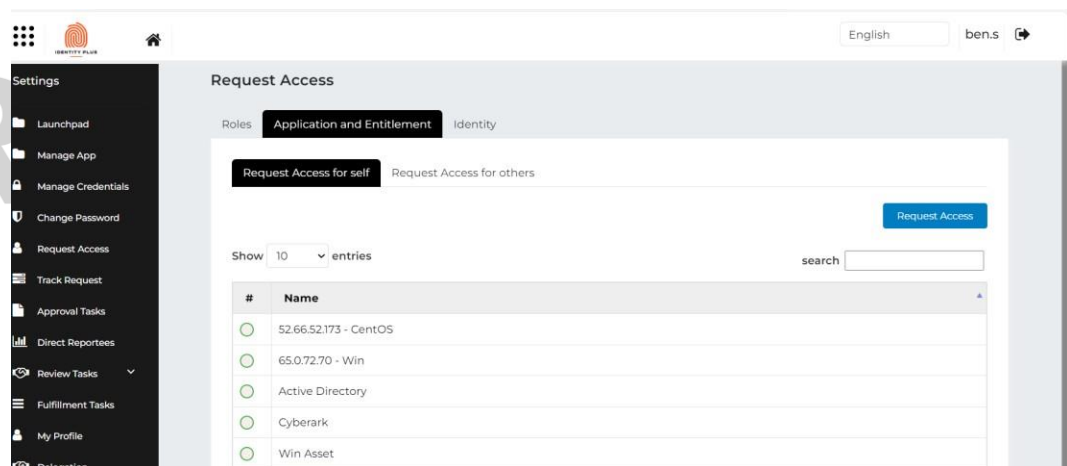
8. Access Request Module

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.

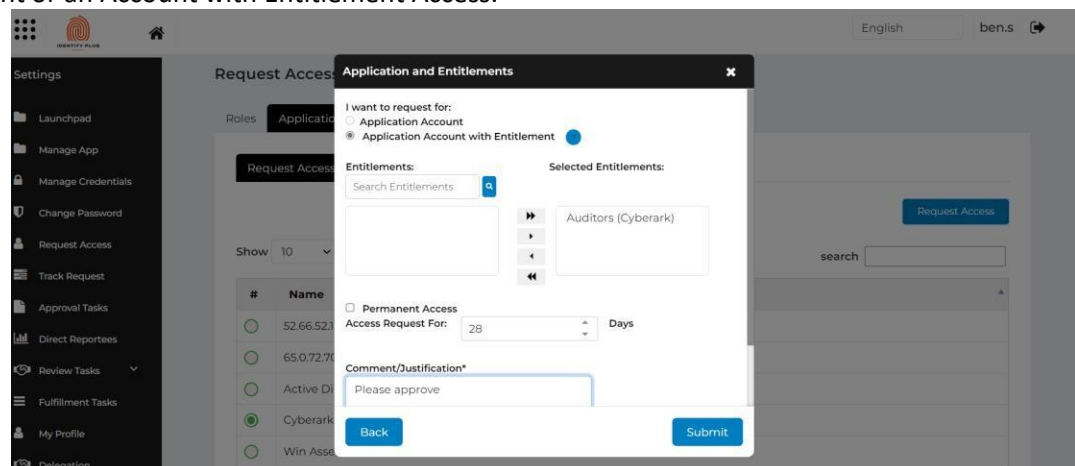
1. End-User should log into Cross Identity with username and password.



2. Go to Request Access tab. There is CyberArk application for which the workflow is configured.



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



4. The End-User should provide the information in the comment/Justification field to justify the request, After Completing the information, Click Submit.
5. 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.

Track Request

Search Access Name

Show 10 entries

Access Name	Requested By	Requested For	Type	Status	
Auditors	ben.s	ben.s	ENTITLEMENT	REVOKED	Details
Auditors	ben.s	ben.s	ENTITLEMENT	PENDING	Details

Showing 1 to 2 of 2 entries

Previous **1** Next

6. Once the request is submitted. The request goes to the manager or Approver for approval as per the Cross Identity workflow configuration.
7. When the manager or Approver logs in, he will be able to see access request that is pending for his approval.

Approval Tasks

Pending Approvals Past Approvals

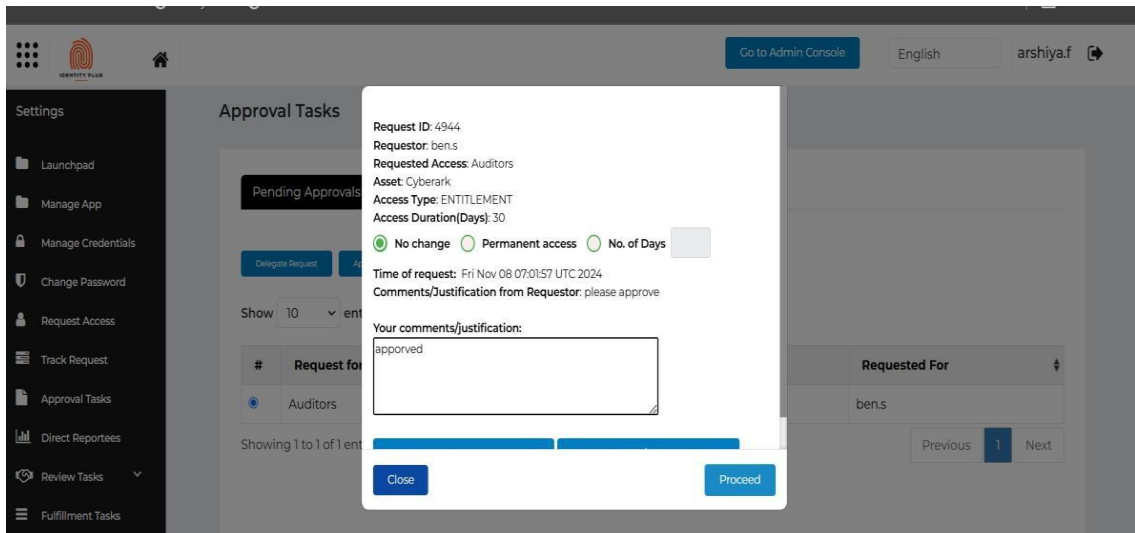
Show 10 entries

#	Request for	Access Type	Requested By	Requested For
0	Auditors	ENTITLEMENT	ben.s	ben.s

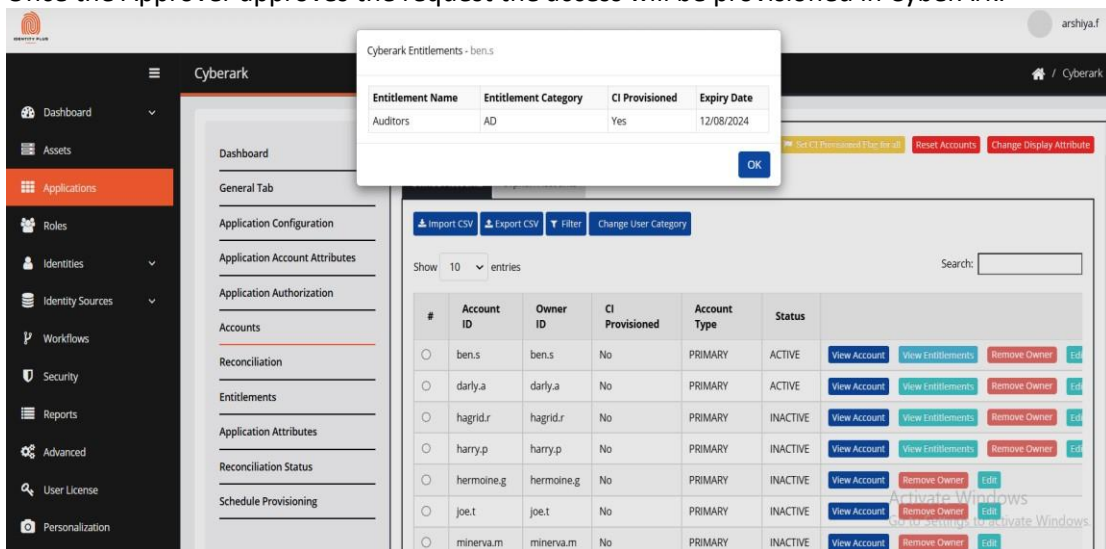
Showing 1 to 1 of 1 entries

Previous **1** Next

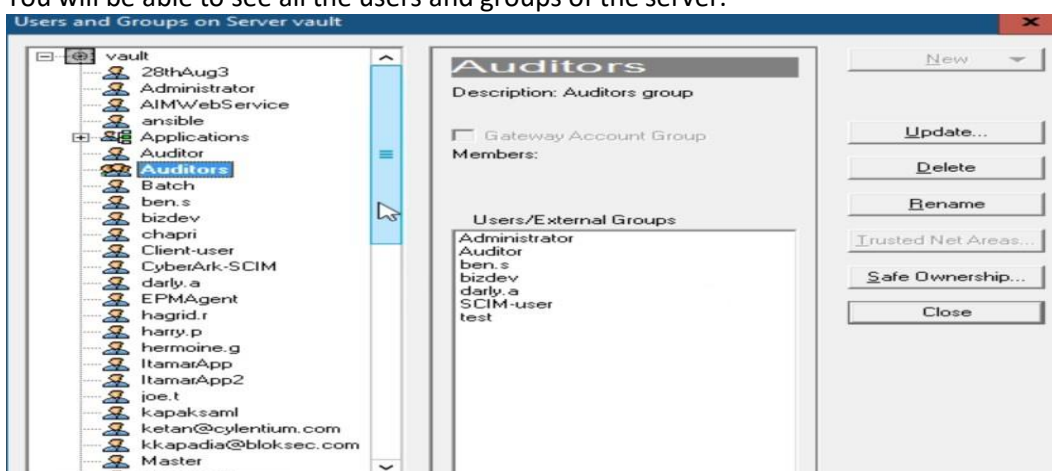
8. The Approver can either approve or deny the request or can delegate the requests, as shown above for Access Request Approval.



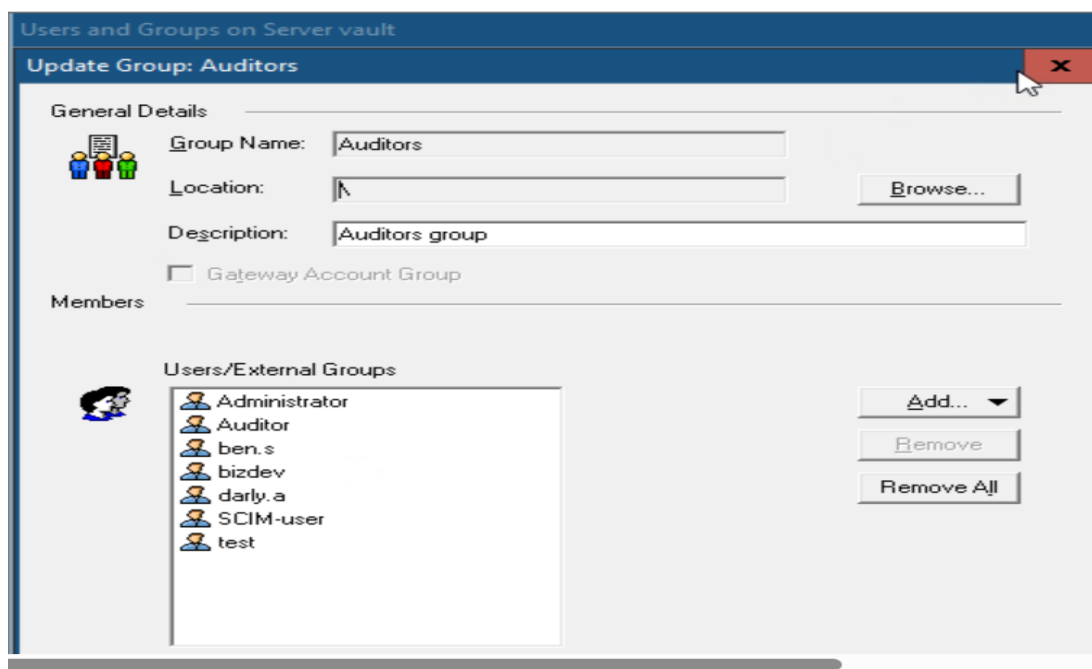
9. Once the Approver approves the request the access will be provisioned in CyberArk.



10. You can go to CyberArk server vault > go to tools > administrative tools > users and groups.
 11. You will be able to see all the users and groups of the server.



12. You can see that the User is assigned to the group.



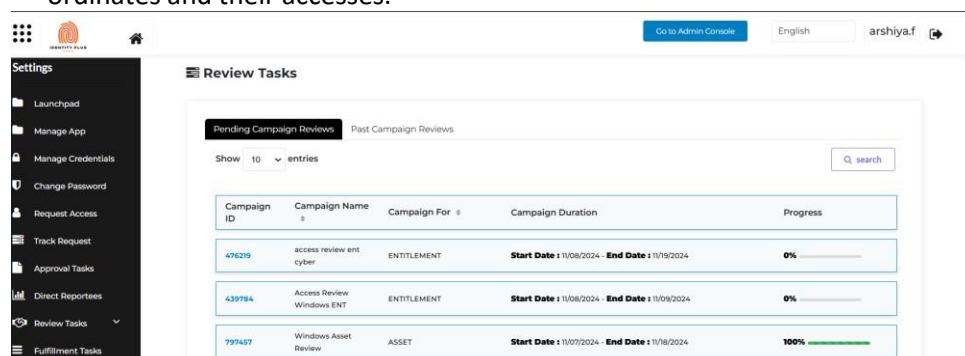
9. Access Review Module

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

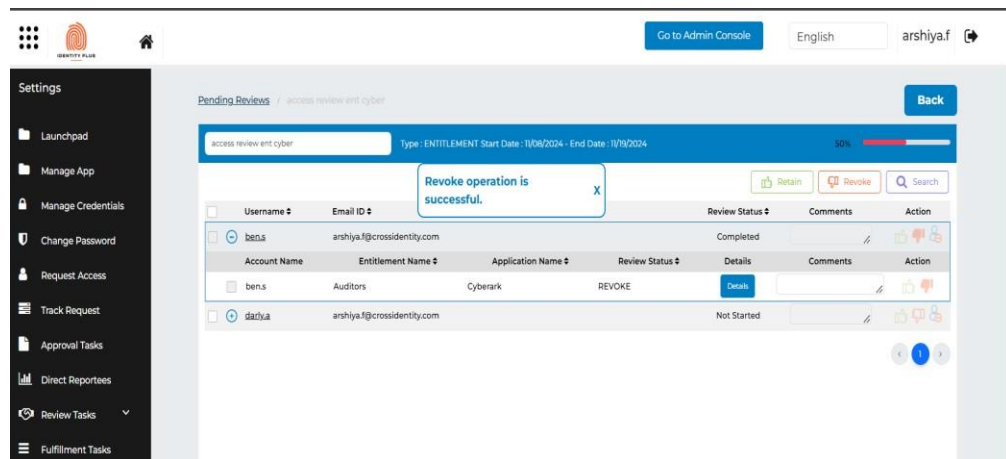
1. User Access Review – Manager as reviewer.
2. Application Owner Review – App Owner is the reviewer.
3. Entitlement Review – Manager as reviewer.
4. Role Review – Manager or Any authorized role can review.
5. The admin can configure different types of workflows for Access Review.

In this case shown below for an Entitlement Review.

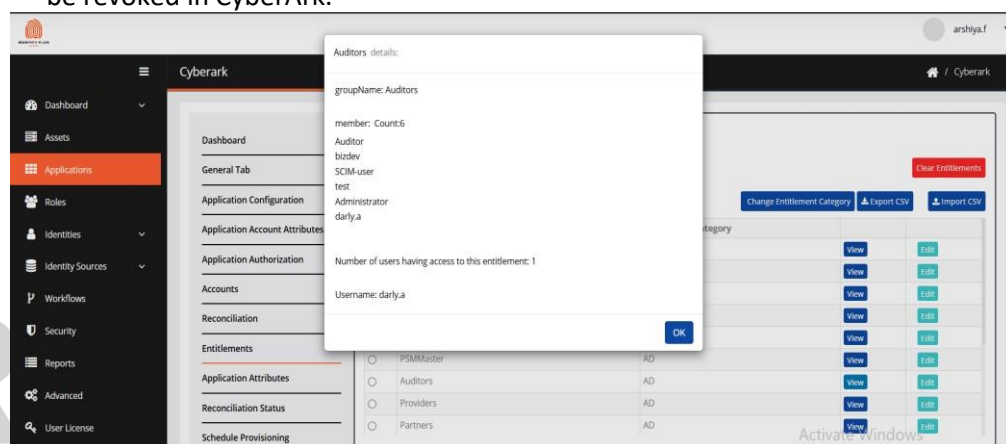
1. Once the admin starts the review, Cross Identity will send email notification to all the reviewers.
2. Once the reviewer logs in to cross identity, they will be able to see all their subordinates and their accesses.



3. The reviewer has the option to revoke or retain any of the Access. Here We are taking revoke action.



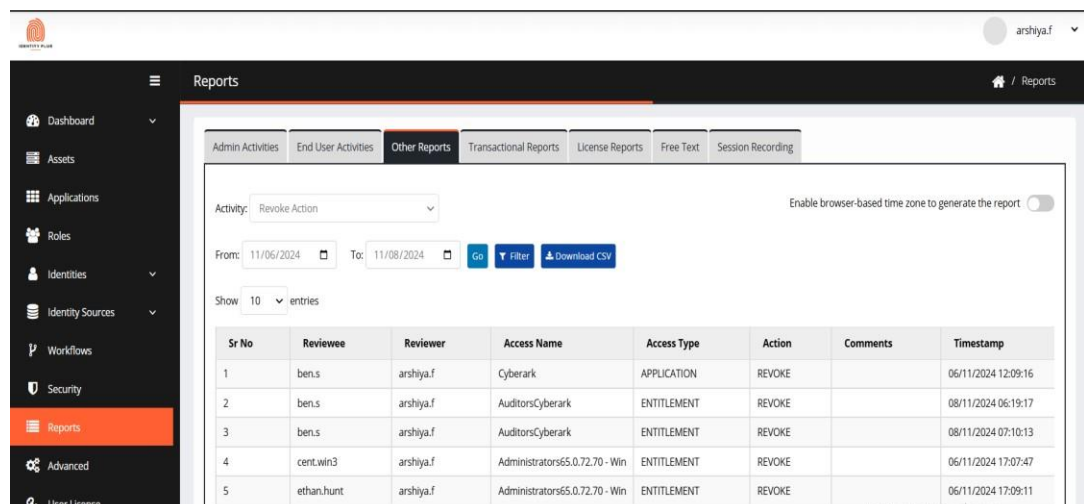
4. If he retains no action is required. If the Reviewers revokes, then the access will be revoked in CyberArk.



11. Reports Module

We can generate multiple compliance reports from Cross Identity such as reports that shows all the users who have AD accounts in the organization and the user's different access. Compliance Reports can be generated, either Excel or PDF format.

The below screenshot shows the report you can generate from Cross Identity for Revoke Action that has been taken.



12. Conclusion

Integrating CyberArk's Privileged Access Solution with Cross Identity offers a robust approach to managing both privileged and non-privileged access. This integration provides comprehensive visibility, streamlined access provisioning, and centralized management of user identities and CyberArk accounts, ensuring alignment with regulatory compliance requirements. The solution enables efficient access reviews, enhances security by enforcing access policies, and reduces risks associated with privileged access management. By automating multi-level approvals and identifying policy violations, the CyberArk and Cross Identity integration strengthens security while simplifying privileged access management across the organization.

CROSS IDENTITY