
Cross Identity nimbleNOVA – CyberArk

INTEGRATION

OCTOBER 22, 2025

Cross Identity nimbleNOVA

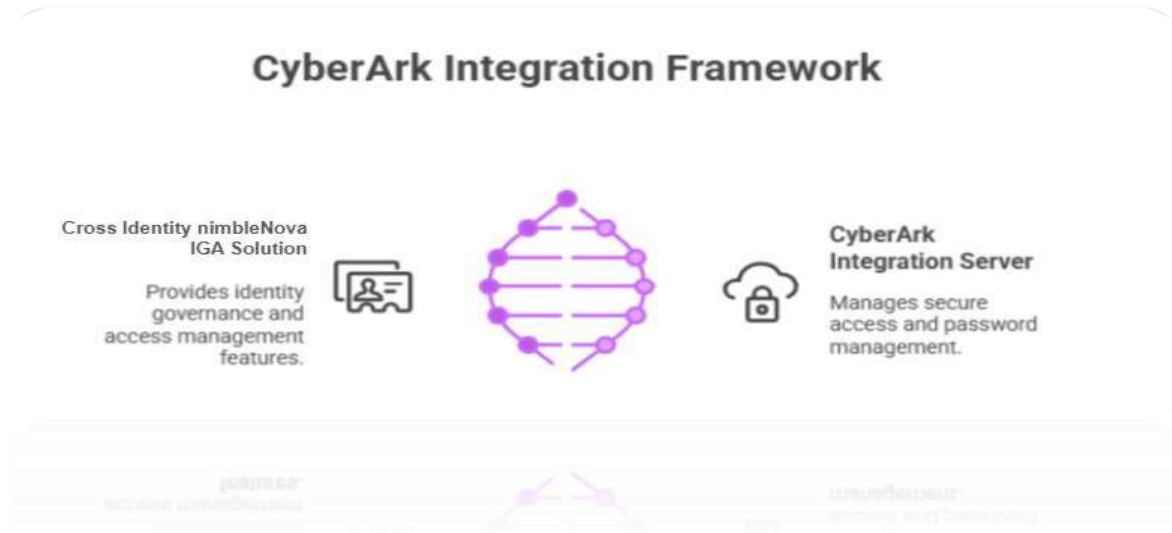
CROSS IDENTITY | INFANTRY TECHNO PARK, AL-RAZACK GROUP, 104, INFANTRY RD,
TASKER TOWN, SHIVAJI NAGAR, BENGALURU, KARNATAKA 560001

Contents

- 1. CI nN – CyberArk Integration Overview 2
- 2. CI nN – CyberArk Integration Benefits 2
- 3. CI nN – CyberArk Integration Architecture 3
- 4. CI nN – CyberArk Integration Use Cases 4
- 5. Steps to Deploy Connector 5
- 6. Connector Configuration Guide 5
 - 6.1 Initial Configuration – CyberArk Connector UI 5
 - Configuration Parameters 6
 - 6.2 Configuring Provisioning Authorization 7
 - 6.3 CyberArk Connector Configuration – Application Setup 10
 - 6.4 CyberArk Configuration – Connectivity 11
 - 6.5 CyberArk Configuration – Schema 11
 - 6.6 CyberArk Configuration – Attributes 12
 - 6.7 CyberArk Configuration – Mapping 12
 - 6.8 CyberArk Configuration – Discovery 13
- 7. Access Request Module 16
 - Steps to Request Access 16
- 8. Access Review Module 20
 - Steps to View Campaign Details as a Campaign Owner 20
- 9. Reports Module 23

1. CI nN – CyberArk Integration Overview

The CyberArk Privileged Access Solution integrated with Cross Identity nimbleNova to provide a centralized view of both regular user access and privileged user access. This integration enables access requests for privileged access, multi-level approval workflows, access reviews for privileged access, and compliance reports. It also provides centralized management for all identities, CyberArk accounts, and groups to ensure alignment with organizational regulatory compliance.



Cross Identity nimbleNova integrates with CyberArk using a connector (CyberArk version 14) and is working as expected. The following use cases have been successfully tested:

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

2. CI nN – CyberArk Integration Benefits

Cross Identity nimbleNOVA's integration with CyberArk provides organizations with a unified framework to manage both privileged and non-privileged accounts securely. 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.

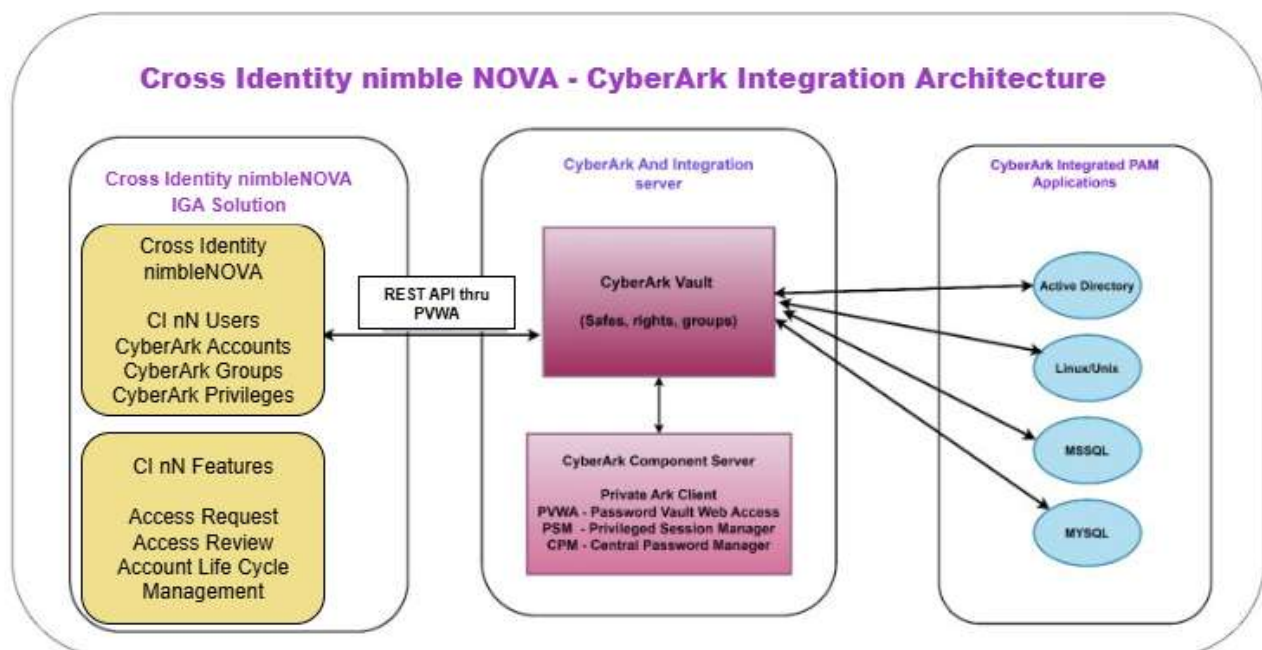
4. Risk Reduction and Compliance Alignment

- 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 nN – CyberArk Integration Architecture



Cross Identity nimbleNova IGA Solution

Components Managed:

- CI Users
- CyberArk Accounts
- CyberArk Groups
- CyberArk Privileges

Core Features:

- Access Request
- Access Review
- Account Lifecycle Management

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

4. CI nN – CyberArk Integration Use Cases

The Cross Identity nimbleNova 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 nimbleNova 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 nimbleNova can automatically collect and synchronize all CyberArk accounts into its identity repository.
- This ensures that the CI nN 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 nimbleNova.
- Provides administrators with clear visibility into 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 nimbleNova, the associated CyberArk account is immediately disabled or deleted.
- Eliminates orphaned privileged accounts, reducing insider threat risks.

8. Compliance Reporting

- Cross Identity nimbleNova generates detailed compliance and audit reports showing users, their CyberArk accounts, and entitlements.
- Each campaign's history maintains detailed records of actions taken against each user.

5. Steps to Deploy Connector

1. Ensure Apache Tomcat is installed and running
2. Copy the connector .war file into the Tomcat webapps directory
3. Tomcat will automatically extract and deploy the connector
4. Verify deployment by accessing the connector endpoint in a browser:
`http://<server>:8080/<connector-name>/`

6. Connector Configuration Guide

6.1 Initial Configuration – CyberArk Connector UI

The first step in setting up the CyberArk Connector involves configuring the connector using its web-based interface.

Navigate to the CyberArk Connector UI (usually hosted locally or at your deployment URL). You will be required to fill in the following essential configuration parameters:

Configuration Parameters

1. Tenant Identifier

Description: Unique identifier for your organization's tenant

How to retrieve:

1. Log in to the Cross Identity Admin Console
2. From the left sidebar, expand the Applications menu
3. Select Manage Applications
4. Click the Configured CyberArk Application
5. Copy the Tenant Identifier value displayed

2. Sub-Tenant Identifier

Description: Identifier for the specific subtenant under your main tenant

How to retrieve:

Located in the same Configured CyberArk Application section as the Tenant Identifier above

3. Application UUID

Description: Unique identifier for the identity source application

How to retrieve:

1. In the Configured CyberArk Application (see Tenant Identifier steps above)
2. Locate the Identity Source Identifier field

3. Copy this value as your Application UUID

4. API URL

Description: The endpoint URL through which the connector communicates with CI nN.

Value: Varies by tenant (provided by your administrator)

Example : `https://<tenant-domain>/Zscaler/idx2api/`

5. Polling Interval (seconds)

Recommended Value: 5 seconds

Description: Sets how frequently the connector checks CI nN for pending activities

Saving Your Configuration

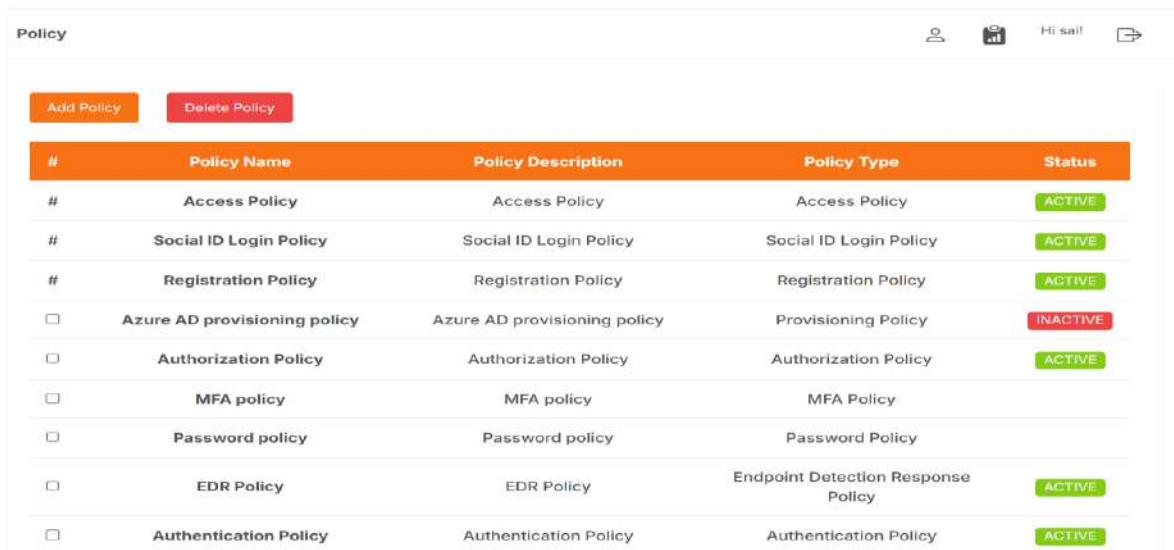
Once you've entered all required details:

1. Click Save to store the connector configuration
2. Click Start to begin the connector polling process.
3. (Optional) Click Persist Config to ensure the configuration persists across system reboots or service restarts.

6.2 Configuring Provisioning Authorization

Step 1: Navigate to Policy

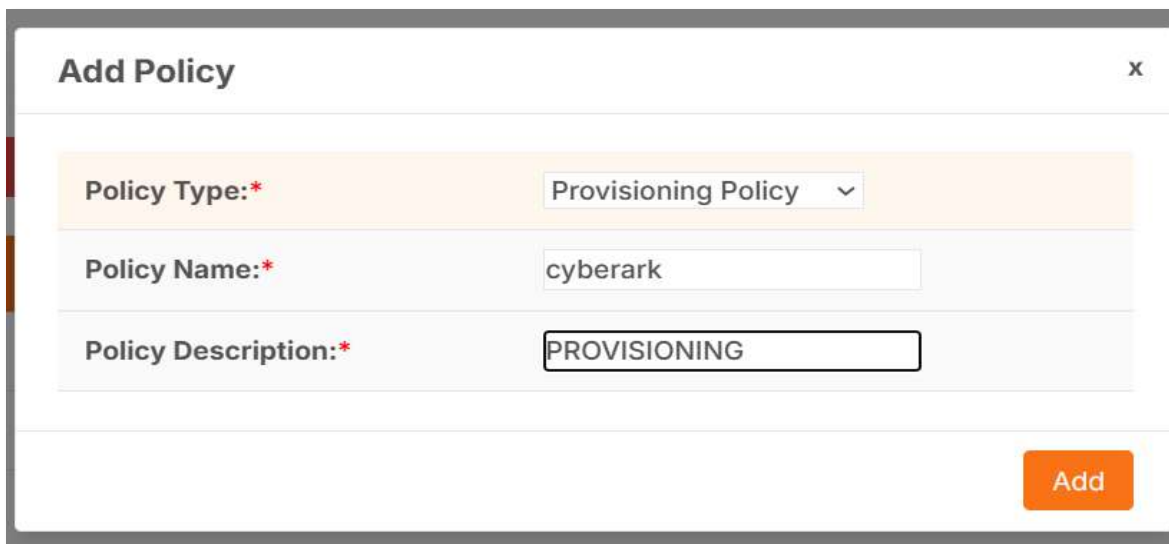
Navigate to the **Security** tab and click on **Policy**.



#	Policy Name	Policy Description	Policy Type	Status
#	Access Policy	Access Policy	Access Policy	ACTIVE
#	Social ID Login Policy	Social ID Login Policy	Social ID Login Policy	ACTIVE
#	Registration Policy	Registration Policy	Registration Policy	ACTIVE
☐	Azure AD provisioning policy	Azure AD provisioning policy	Provisioning Policy	INACTIVE
☐	Authorization Policy	Authorization Policy	Authorization Policy	ACTIVE
☐	MFA policy	MFA policy	MFA Policy	
☐	Password policy	Password policy	Password Policy	
☐	EDR Policy	EDR Policy	Endpoint Detection Response Policy	ACTIVE
☐	Authentication Policy	Authentication Policy	Authentication Policy	ACTIVE

Step 2: Add Policy

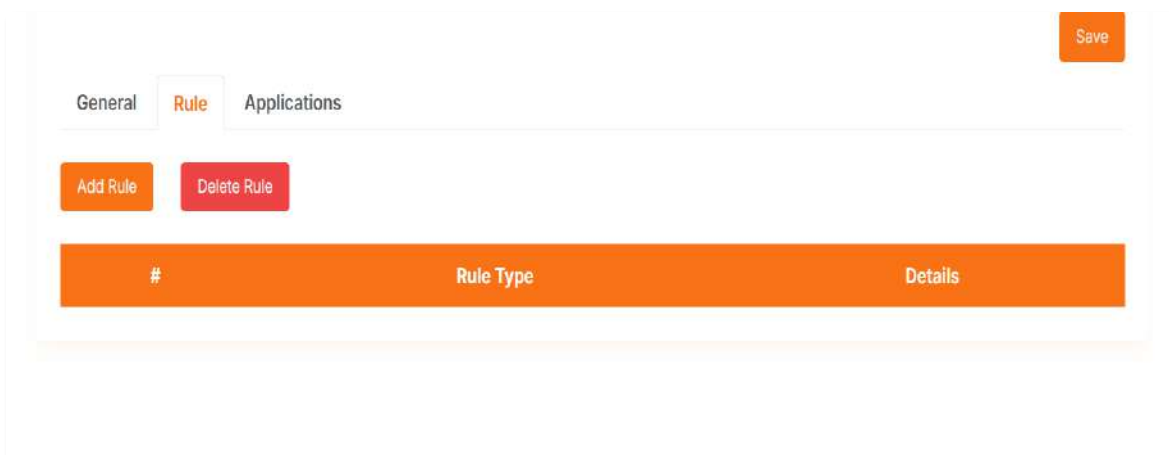
Click **Add Policy**, then provide a user-friendly name and description for the policy, and click **Add**



The 'Add Policy' form is a modal window with a title bar containing 'Add Policy' and a close button 'x'. It contains three input fields: 'Policy Type:*' with a dropdown menu showing 'Provisioning Policy', 'Policy Name:*' with the text 'cyberark', and 'Policy Description:*' with the text 'PROVISIONING'. An orange 'Add' button is located at the bottom right of the form.

Step 3: Add Rule

After adding the policy, navigate to **Rule** and click **Add Rule**.



The 'Rule' management interface shows three tabs: 'General', 'Rule' (selected), and 'Applications'. In the 'Rule' tab, there are two buttons: 'Add Rule' (orange) and 'Delete Rule' (red). Below these buttons is a table with three columns: '#', 'Rule Type', and 'Details'. The table is currently empty.

Select the role, identity profile, and identity attribute, then choose the corresponding target based on your selection.

Add Rule

Choose type:*

Please choose a target type ▾

Please choose a target type

Role

Identity Profile

Identity Attribute

Add

Step 4: Add Application

Click on **Application** and select **Add Application**. The rule will now be applied to all members.

Add Application

cyberark

#	Application
✓	CYBERARK

Add

Step 5: Enable Policy

Enable the policy in the General tab.

Policy

General

Rule

Applications

Policy Name:*

cyberark

Policy Description:*

PROVISIONING

Policy Type:

Provisioning Policy

Status:

☐

6.3 CyberArk Connector Configuration – Application Setup

Navigate to **Applications** select **Manage Applications** from the left-hand menu.

Add the application by specifying:

- **Application Name** (e.g., CYBERARK)
- **Description** (e.g., IGA)
- **Application Type** (e.g., Regular)

This initializes the connector setup in the CI nN platform.

CROSS IDENTITY - MS

Dashboard

Applications

Identity

Roles

Workflows

Reports

Security

Settings

Support

Manage Applications

Add Application

Application Name:*

CYBERARK

Application Description:*

IGA

Application Type:

Regular

Add

Oauth

Oauth

OAuthDevicegrant

OAuthDevicegrant

6.4 CyberArk Configuration – Connectivity

Once the connector is initialized, configure the connection parameters. This section allows the connector to communicate with CyberArk using the appropriate authentication details.

Important: Deploy the CyberArk Personal Information Exchange (.p12 / .pfx) certificate on the same server where the CI nN connector is installed.

The screenshot shows the NIMBLENOVA Manage Applications interface. The left sidebar contains a navigation menu with items like Dashboard, Applications, Identity, Roles, Workflows, Reports, Security, Settings, Support, and License. The main content area is titled 'Manage Applications' and has several tabs: General, SSO, Authorization, Connectivity (selected), Schema, Attributes, Mapping, Discovery, Accounts, and Entitlements. Below the tabs are three buttons: 'Add Parameter', 'Delete Parameter', and 'Test Connection'. A table with three columns (ID, Name, Value) lists the following parameters:

ID	Name	Value
☐	baseUrl	***** View
☐	adminUser	***** View
☐	adminPassword	***** View
☐	certFilePath	***** View
☐	certPassword	***** View

Required Parameters:

- **baseUrl** – The base URL of the CyberArk instance along with the port number (e.g., <https://service-usa.sky.com:8080>) used to initiate API calls.
- **adminUser** – The administrator username used to authenticate and perform operations on the CyberArk vault.
- **adminPassword** – The password for the admin user, required for secure login to the CyberArk instance.
- **certFilePath** – The local path to the CyberArk client certificate (.cer or .p12) used for certificate-based authentication.
- **certPassword** – The password to unlock the certificate file and enable secure HTTPS communication.

Note: Parameter names are **case sensitive**. Please enter them exactly as shown above.

6.5 CyberArk Configuration – Schema

Under **Schema**, you can fetch all available attributes from CyberArk to get a complete view of the attributes present. Click **Discover Schema** to fetch them.

General	SSO	Authorization	Connectivity	Schema	Attributes	Mapping	Discovery	Accounts	Entitlements
Add Schema Attributes	Delete Schema Attribute	Discover Schema	Display Attribute						
#	Attribute Name	Attribute Display Name	Script Enabled?	Script					
☐	id	id	NO						
☐	username	username	NO						
☐	source	source	NO						
☐	userType	userType	NO						
☐	componentUser	componentUser	NO						
☐	vaultAuthorization	vaultAuthorization	NO						
☐	location	location	NO						
☐	personalDetails	personalDetails	NO						
☐	enableUser	enableUser	NO						
☐	suspended	suspended	NO						
☐	firstName	personalDetails.firstName	NO						
☐	middleName	personalDetails.middleName	NO						
☐	lastName	personalDetails.lastName	NO						

If you need to add attributes that are not available in CyberArk, you can manually create them by clicking on **Add Schema Attributes**. These attributes can then be used for further mapping.

6.6 CyberArk Configuration – Attributes

You can select the available attributes fetched from CyberArk. Click on *Add Attributes* to include the attributes you want to assign when users are provisioned.

General

SSO

Authorization

Connectivity

Schema

Attributes

Mapping

Discovery

Accounts

Entitlements

Add Attribute

Delete Attribute

#	Attribute
☐	Id
☐	username
☐	firstName
☐	lastName

6.7 CyberArk Configuration – Mapping

Under **Mapping**, click **Add Profile**. Here, you can add the profiles whose attributes will be used for mapping and provisioning.

Add Mapping - Administrator
x

Schema Attribute	Identity Profile Attribute
id	id
username	username
firstName	firstName
lastName	lastname

Save

6.8 CyberArk Configuration – Discovery

i) Add Discovery Rule

Under **Discovery**, click **Add Discovery Rule** and select what you want to fetch:

- Accounts
- Entitlements
- Both
- Apply a Filter (see the next section for details on adding filters)

General
SSO
Authorization
Connectivity
Schema
Attributes
Mapping
Discovery
Accounts
Entitlements

Discovery Rule:

Add Discovery Rule
Delete Discovery Rule

#	Rule	Filter	
☐	All entitlements	NA	Run
☐	All accounts	NA	Run

ii) Filter

To fetch users based on specific values such as username or email:

- First, select the attribute under **Filter**

2. Go back to **Discovery**
3. Click **Filter** and choose the filter you just created

This will allow you to fetch users along with their associated accounts and entitlements.

Add Filter

x

Schema Attribute	Value
id ▼	1
username ▼	testUser

Then click **Add**.

iii) Assignment

Click **Add Assignment Rule** and define the criteria based on which the accounts should be fetched.

Assignment Rule:

Add Assignment Rule
Delete Assignment Rule

#	Identity Profile	Identity Profile Attribute	Application Schema Attribute
☐	Administrator	username	name

Select the Identity Profile, choose the Identity Attribute, and then select the corresponding Schema Attribute (the Identity Attribute will be mapped to the Schema Attribute).

Add Assignment Rule

x

Identity Profile:

Administrator

Identity Profile Attribute:

username

Schema Attribute:

name

Add

When you run a discovery for accounts, entitlements, or both:

- Discovered accounts will appear under the **Accounts** section.
- Entitlements will be listed under the **Entitlements** section.

Dashboard	General	SSO	Authorization	Connectivity	Schema	Attributes	Mapping	Discovery	Accounts	Entitlements
Applications										
Identity										
Roles										
Workflows										
Reports										
Security										
Settings										
Support										

Search accounts...

#	Account ID	Owner	Status	Entitlements	Permissions
☐	Master	Master	ACTIVE	View Entitlements	View Permissions
☐	Backup	Backup	ACTIVE	View Entitlements	View Permissions
☐	Administrator	Administrator	ACTIVE	View Entitlements	View Permissions
☐	Auditor	Auditor	ACTIVE	View Entitlements	View Permissions
☐	Operator	Operator	ACTIVE	View Entitlements	View Permissions
☐	Batch	Batch	ACTIVE	View Entitlements	View Permissions
☐	DR	DR	ACTIVE	View Entitlements	View Permissions
☐	NotificationEngine	NotificationEngine	ACTIVE	View Entitlements	View Permissions
☐	PVWAGWUser	PVWAGWUser	ACTIVE	View Entitlements	View Permissions
☐	DUWAAppUser	DUWAAppUser	ACTIVE	View Entitlements	View Permissions

General

SSO

Authorization

Connectivity

Schema

Attributes

Mapping

Discovery

Accounts

Entitlements

Entitlements

Permission Tree

#	Entitlement Name	Accounts	Permissions
☐	Backup Users	View Accounts	View Permissions
☐	Auditors	View Accounts	View Permissions
☐	Operators	View Accounts	View Permissions
☐	DR Users	View Accounts	View Permissions
☐	Vault Admins	View Accounts	View Permissions
☐	Notification Engines	View Accounts	View Permissions
☐	PVWAMonitor	View Accounts	View Permissions
☐	PVWAUsers	View Accounts	View Permissions

7. Access Request Module

In Cross Identity nimbleNova, end users and approvers interact through two key sections of the End User Console:

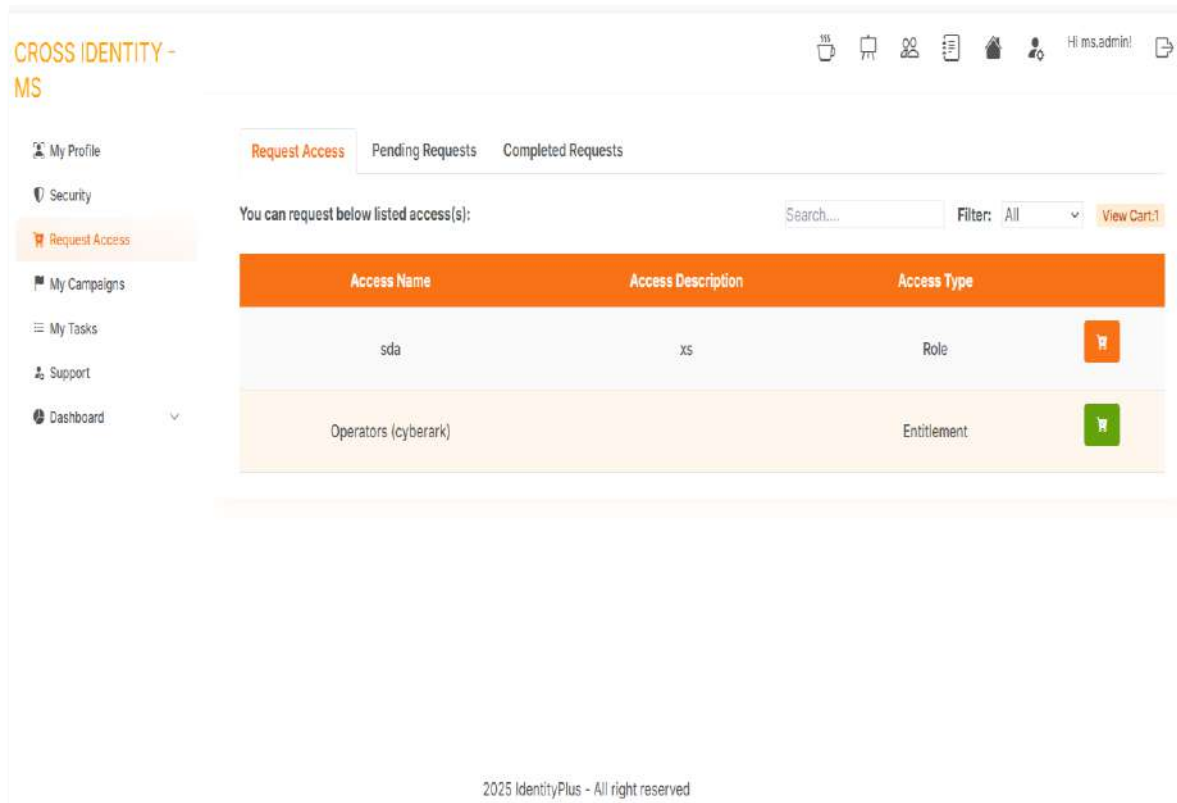
- **Request Access** – Lets users search, view, and request roles, accounts, or entitlements based on configured workflows and their eligibility.
- **My Tasks** – Gives approvers a consolidated view of pending requests for timely review and action.

This structure streamlines access governance while enhancing compliance and minimizing risk.

Steps to Request Access

Step 1: Navigate to Request Access

Navigate to the **Request Access** menu option in the End User console.



Step 2: View Available Assets

Suppose users fall within the eligible requester category as set by the admin in the workflow (based on identity profile, role, or attributes). In that case, they will see the list of available assets such as roles, applications, or entitlements.

Step 3: Add Items to Cart

To request the desired asset, click on the cart icon associated with the entity. You can add more than one entity to the cart.

Step 4: Review Cart

Click **View Cart** to review and proceed with raising the request for the desired entities.

CROSS IDENTITY - MS

My Profile
Security
Request Access
My Campaigns
My Tasks
Support
Dashboard

Your cart:

Access Name	Access Description	Access Type	Permanent Access	I need access for (Days)	Priority	Comments
Operators (CYBERARK)		Entitlement	☐		Low	

Items in the cart are for: ☒ Myself ☐ My reportee(s)

Process

Step 5: Configure Access Duration

Choose whether the access should be permanent or temporary. For temporary access, specify the number of days required.

CROSS IDENTITY - MS

My Profile
Security
Request Access
My Campaigns
My Tasks
Support
Dashboard

Your cart:

Access Name	Access Description	Access Type	Permanent Access	I need access for (Days)	Priority	Comments
Operators (CYBERARK)		Entitlement	☐	10	Low	kindly approve

Items in the cart are for: ☒ Myself ☐ My reportee(s)

Process

Step 6: Set Priority

Set the priority level of the request depending on the urgency.

Step 7: Provide Justification

Provide justification comments explaining why access is needed to help approvers make informed decisions.

Step 8: Select Requestor

Users can either request for themselves or for their reports by selecting the respective radio button.

Step 9: Remove Unwanted Requests

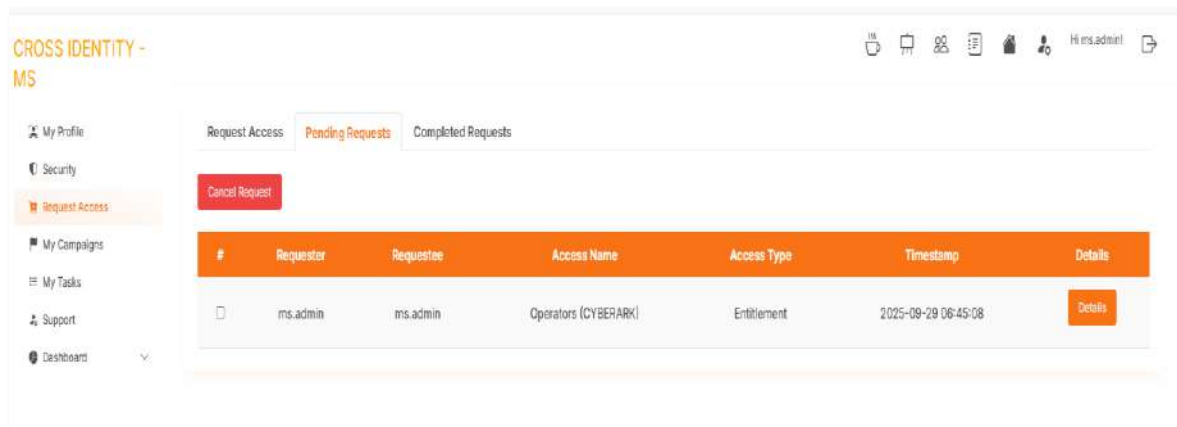
Users can delete unwanted requests from being raised by clicking on the associated **X** mark.

Step 10: Submit Request

Click **Proceed** to raise the requests.

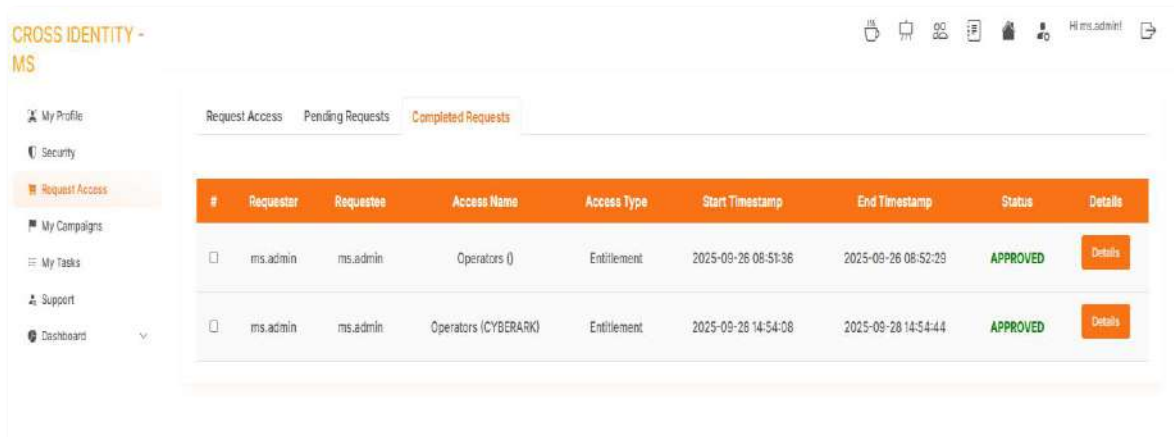
Step 11: Track Pending Requests

Requests can be tracked under the **Pending Requests** section for those still awaiting action.



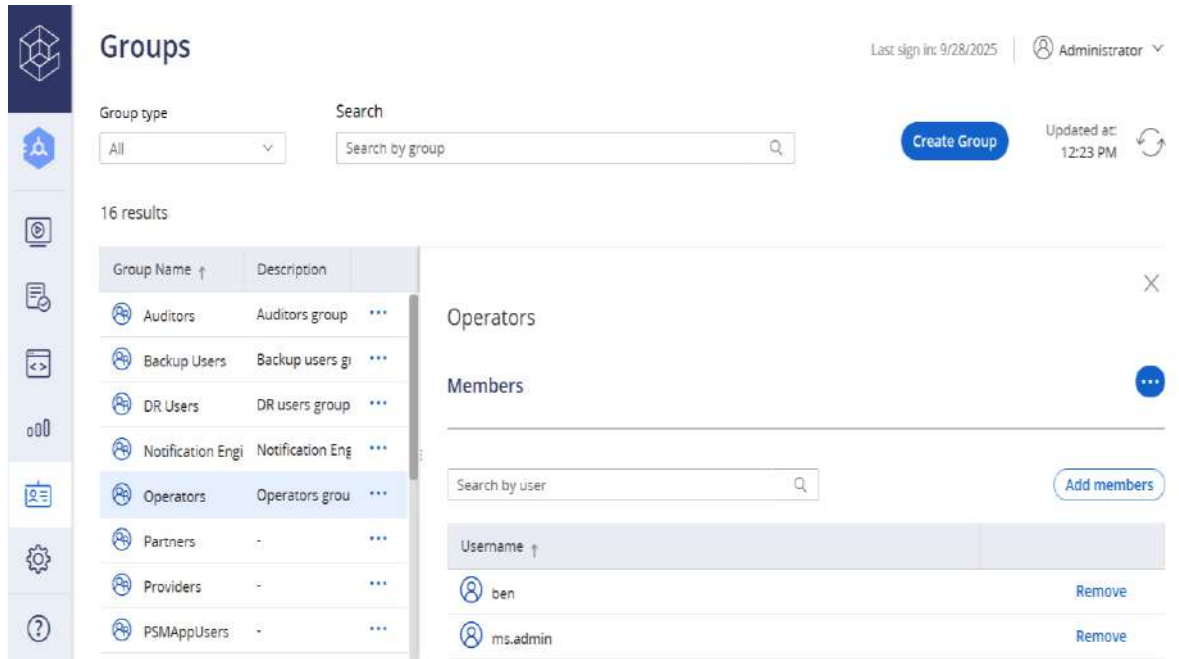
Step 12: View Completed Requests

Under **Completed Requests**, view requests that have been addressed (approved/rejected).



Step 13: Access Provisioning

Once the approver approves the request, the access will be provisioned in CyberArk.



8. Access Review Module

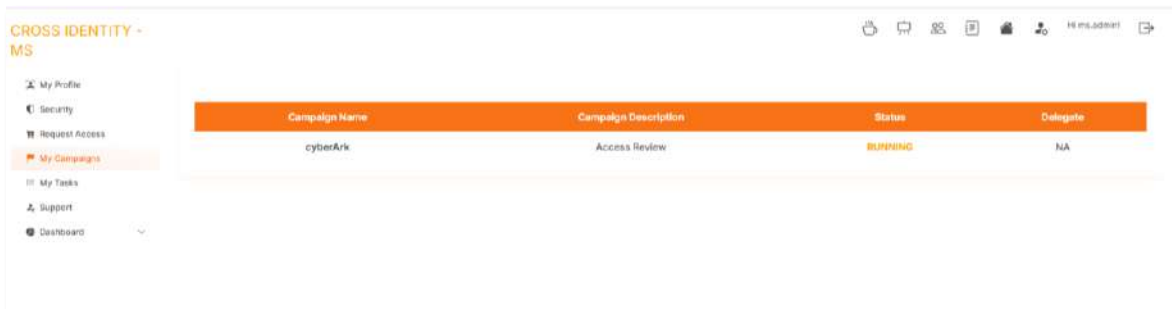
Access Review Campaigns in Cross Identity allow organizations to systematically validate and certify user access. Campaign Owners manage the complete lifecycle—starting and closing campaigns, assigning reviewers, and monitoring progress to ensure timely completion. They also ensure the accuracy of review outcomes, resolve issues during the process, and maintain accountability throughout.

This structured approach supports compliance requirements, strengthens security, and provides clear visibility into access governance activities.

Steps to View Campaign Details as a Campaign Owner

Step 1: Navigate to My Campaigns

Navigate to the **My Campaigns** menu option in the End User console.



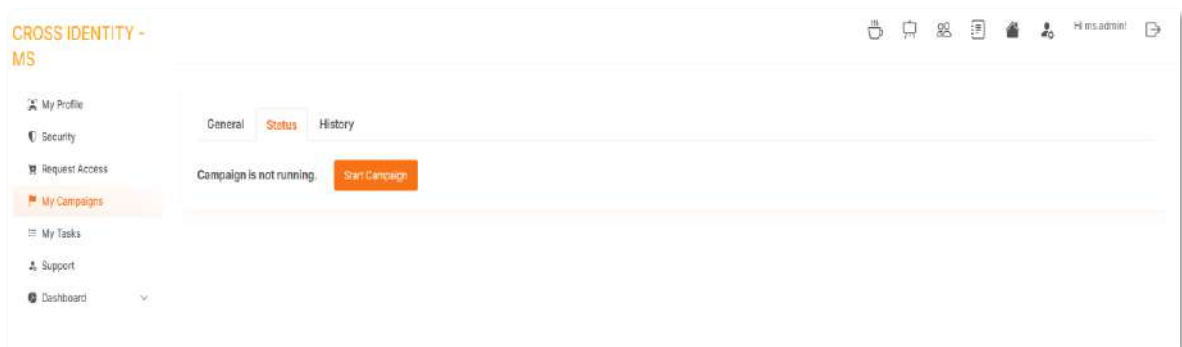
Step 2: View Active Campaigns

A list of active campaigns will be displayed. If you have the necessary permissions, you can start or stop any campaign by clicking on the link/name of the campaign.

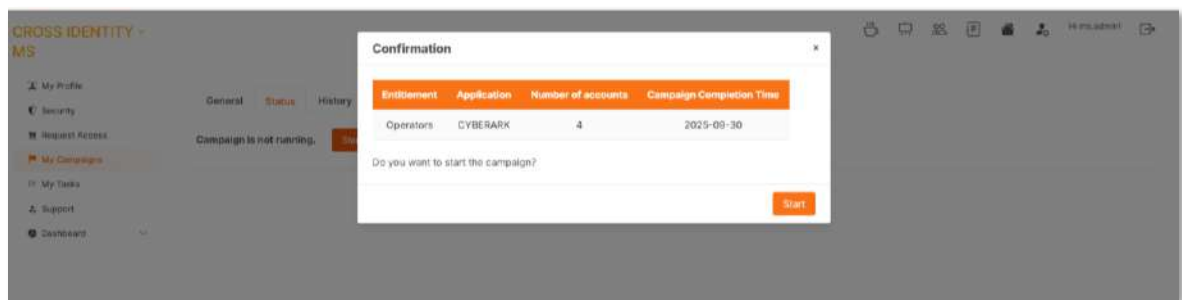


Step 3: Start Campaign

To check the status of the campaign, navigate to the **Status** tab and click **Start Campaign** to start the campaign.

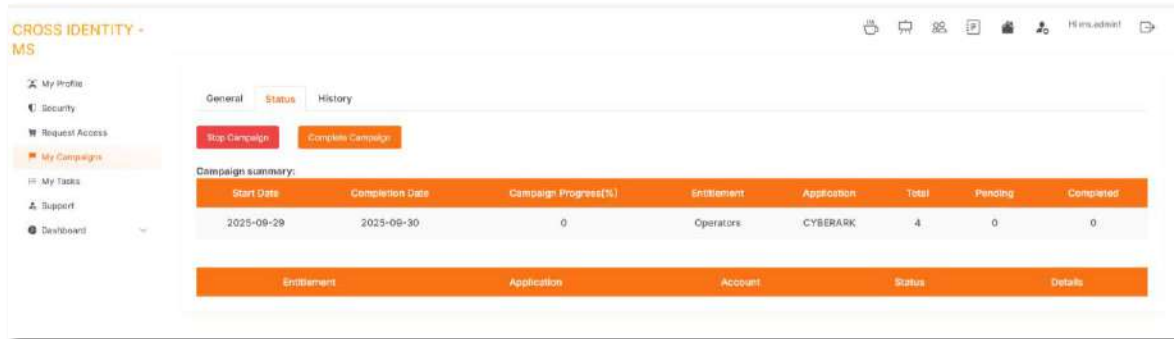


In the popup window, click **Start**.



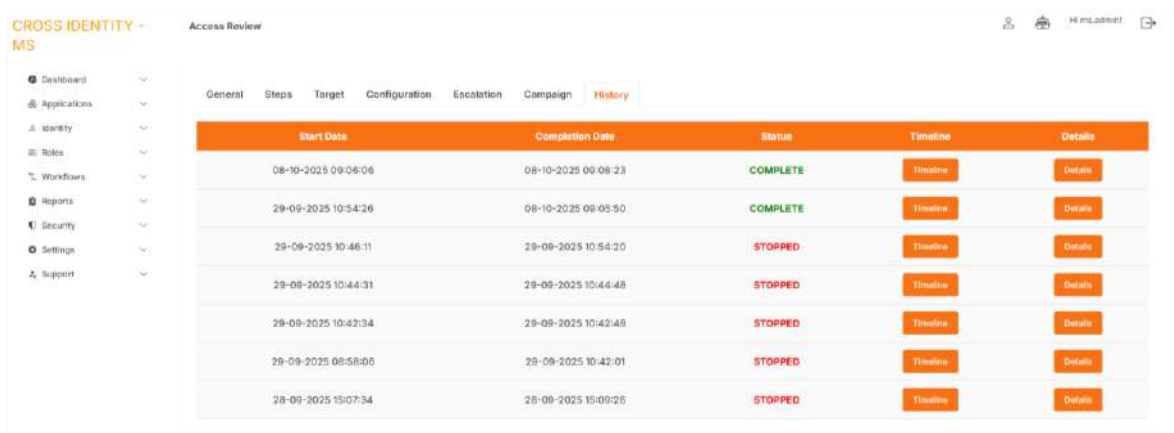
Step 4: Monitor Campaign Progress

In the same tab, the Campaign Owner can stop a started campaign and view the review status of the campaign members.



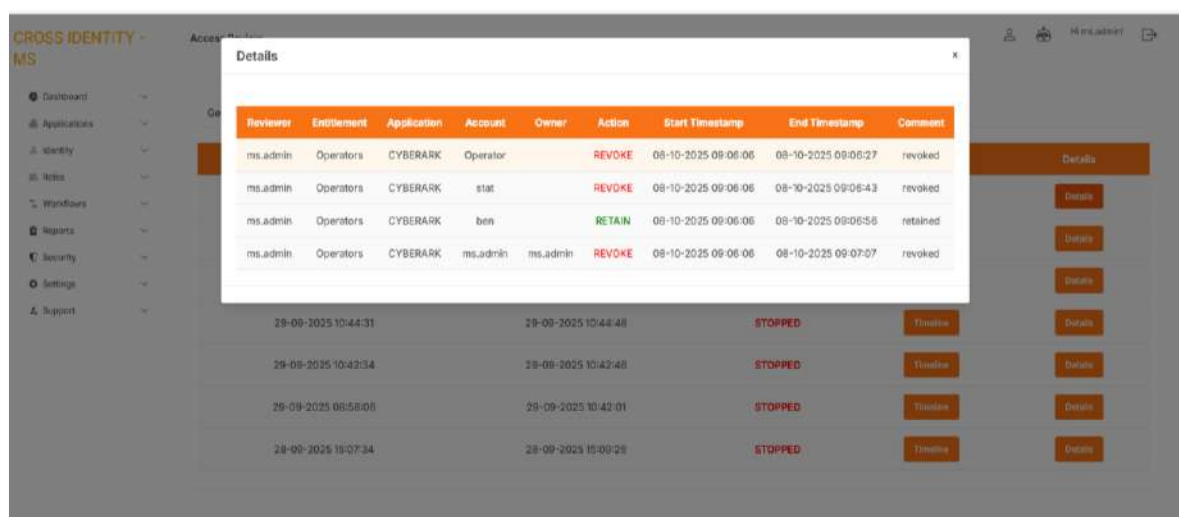
Step 5: View Campaign History

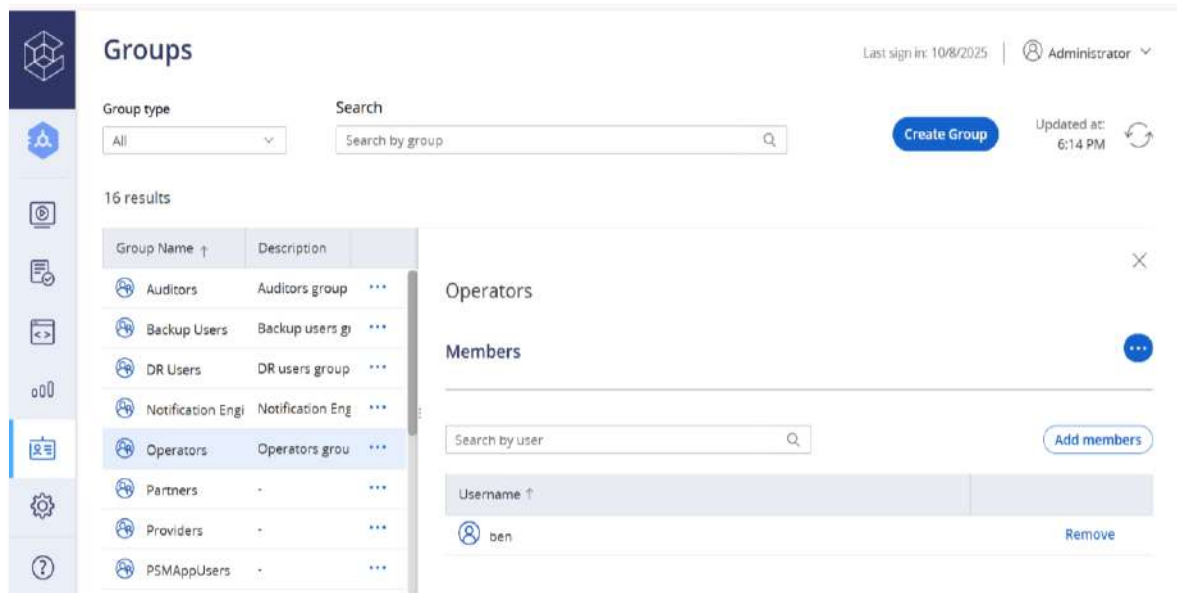
To view the history of the campaign, navigate to the **History** tab.



Step 6: View Campaign Results

Click **Details** to view the campaign results.





9. Reports Module

Cross Identity nimbleNova enables the generation of multiple compliance reports, such as reports listing all users' CyberArk accounts in the organization, along with their various access rights.

CROSS IDENTITY - MS

Access Review

General Steps Target Configuration Escalation Campaign History

Start Date	Completion Date	Status	Timeline	Details
08-10-2025 09:06:06	08-10-2025 09:08:23	COMPLETE	Timeline	Details
29-09-2025 10:54:26	08-10-2025 09:05:50	COMPLETE	Timeline	Details
29-09-2025 10:46:11	29-09-2025 10:54:20	STOPPED	Timeline	Details
29-09-2025 10:44:31	29-09-2025 10:44:48	STOPPED	Timeline	Details
29-09-2025 10:42:34	29-09-2025 10:42:48	STOPPED	Timeline	Details
29-09-2025 08:58:00	29-09-2025 10:42:01	STOPPED	Timeline	Details
28-09-2025 15:07:34	28-09-2025 15:09:26	STOPPED	Timeline	Details

CROSS IDENTITY - MS

Details

Reviewer	Entitlement	Application	Account	Owner	Action	Start Timestamp	End Timestamp	Comment
ms.admin	Operators	CYBERARK	Operator		REVOKE	08-10-2025 09:06:06	08-10-2025 09:06:27	revoked
ms.admin	Operators	CYBERARK	stat		REVOKE	08-10-2025 09:06:06	08-10-2025 09:06:43	revoked
ms.admin	Operators	CYBERARK	ben		RETAIN	08-10-2025 09:06:06	08-10-2025 09:06:56	retained
ms.admin	Operators	CYBERARK	ms.admin	ms.admin	REVOKE	08-10-2025 09:06:06	08-10-2025 09:07:07	revoked

29-09-2025 10:44:31 29-09-2025 10:44:48 STOPPED Timeline Details

29-09-2025 10:42:34 29-09-2025 10:42:48 STOPPED Timeline Details

29-09-2025 08:58:08 29-09-2025 10:42:01 STOPPED Timeline Details

28-09-2025 15:07:34 28-09-2025 15:09:29 STOPPED Timeline Details

Campaign execution details can be viewed under each campaign's **History** tab. Clicking '**Details**' reveals the operations performed for each user, which can be used for audit and compliance tracking.