Technology Partner Program

Integration Guide

Orchid Security and Idira

Privileged Account Discovery and Reporting

Author: Orchid Security

Revision History	
June 2026	Initial release. Documents the Orchid to Idira privileged account discovery and reporting integration.

Table 1: Partner information	
Date	June 2026
Partner Name	Orchid Security
Website	https://www.orchid.security
Product Name	Orchid Identity Security Platform
Partner Contact	Jay Kline - jay.k@orchid.security
Support Contact	support@orchid.security
Product Description	Orchid delivers an identity-first security orchestration platform. It enables organizations to continuously discover both self-hosted and SaaS applications, assess their native identity controls (and gaps), and remediate compliance and cyber exposure from a single point of control - without extensive effort or application re-coding.

Use Cases for Integration with Palo Alto Networks

Privileged Account Discovery and Reporting to Idira

This guide describes the integration between Orchid Security and Palo Alto Networks Idira®. The integration lets Orchid report discovered privileged accounts to the Idira Discovered Accounts queue so administrators can review them and decide whether to onboard and manage them in Idira.

Orchid discovers accounts across applications and identifies accounts with privileged access. Idira manages privileged accounts that it already knows about. The integration helps close the gap by letting Orchid report privileged accounts that are not yet managed in Idira.

Table 2: Palo Alto Networks Products for Integration			
Palo Alto Networks Product	**Integration Status**	**Palo Alto Networks Versions Tested**	**Orchid Security Versions Tested**

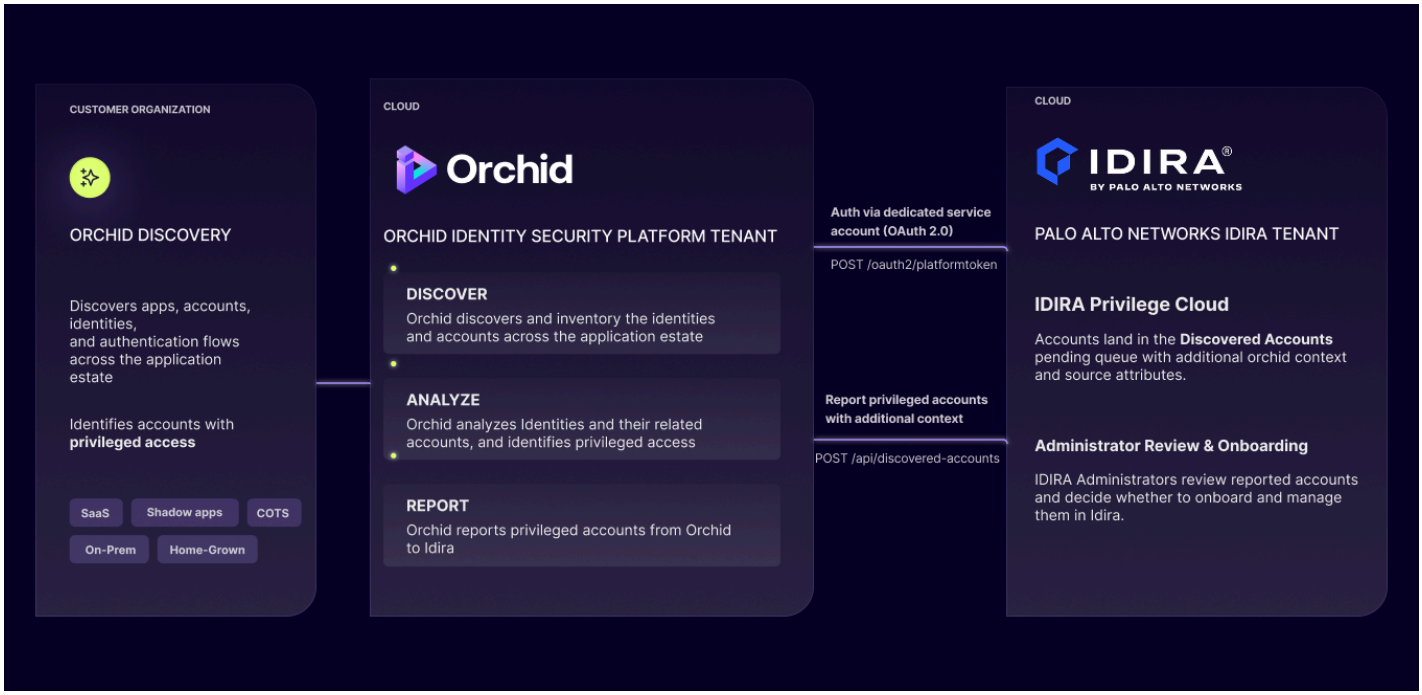
Idira Privilege Cloud	Validated	Idira Privilege Cloud Discovered Accounts service	Orchid Platform 2026.Q2

Integration Benefits

- Discover privileged accounts beyond Idira's native scanning reach across the full application estate, including applications that manage identities in local stores.
- Close the privileged access management coverage gap by feeding Orchid-discovered privileged accounts directly into the Idira Discovered Accounts queue.
- Accelerate onboarding with context-rich, source-tagged accounts that arrive ready for the administrator's standard review workflow.
- Support audit and operational review with a continuously updated picture of privileged accounts Orchid discovers and their management status in Idira.
- Stay in control. Orchid does not write to the vault or alter credentials. Every onboarding and management decision remains with the Idira administrator.

Integration Diagram

- The diagram below outlines the topology of the integration. Orchid discovers and analyzes accounts across the application estate, identifies privileged accounts, and reports them to the Idira Discovered Accounts queue. Idira administrators then review the reported accounts and decide whether to onboard and manage them in Idira.



Orchid Security use the following data:

Data Shared Between the Products

For each privileged account Orchid reports, Orchid sends the context it discovered, including:

- Account identifiers, such as username and address, used to identify the account in Idira.
- Source application context.
- A privileged indicator showing why the account is considered privileged.
- Source attribution, such as Source: Orchid.
- The reported_by_orchid tag, so administrators can filter and identify accounts reported by Orchid.

Orchid does not transmit credential values, secrets, or session data. Orchid sends only account metadata required for discovery review and onboarding.

How the data is shared

Orchid authenticates to the customer Idira tenant using the dedicated service account credentials configured in Orchid. When a user reports an account from Orchid, Orchid sends the account and discovery context to the Idira Discovered Accounts queue.

What action is taken as a result

Reported accounts land in the Idira Discovered Accounts queue. The Idira administrator reviews each account and continues with the standard account onboarding workflow in Idira.

- Provide information on:
  - What data is shared between our products
  - How the data is shared
  - What action is taken as a result of this sharing

Before You Begin

Make sure you have:

- An active Orchid tenant with applications discovered and analyzed
- A Palo Alto Networks Idira tenant with Idira Privilege Cloud available
- Administrator access to the Idira Identity Administration portal
- Permission to create users and assign roles in Idira Identity
- Permission to configure integrations in Orchid
- Access to the Orchid App Inventory page
- At least one application with discovered accounts in Orchid
- Access to the Idira Discovered Accounts queue

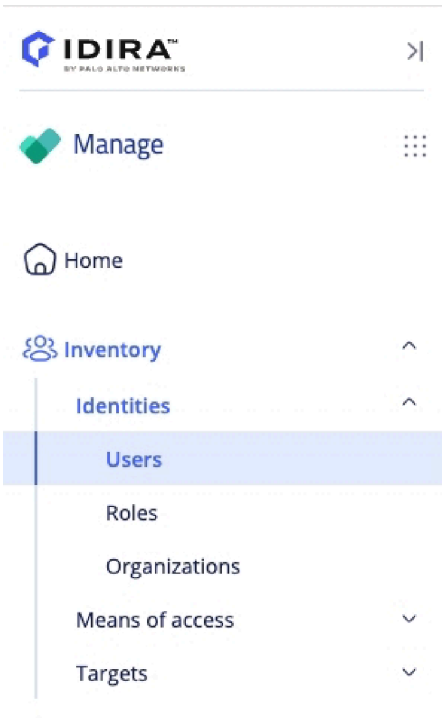
Palo Alto Networks Configuration

Configure Idira

Create a dedicated service account in Idira

Create a dedicated service account that Orchid can use to authenticate to Idira.

1. Log in to Idira.
2. Go to **Manage** > **Users**.



3. Click **Add User**.
4. In **Login Name**, enter a login name for the Orchid service account. You will use this value as the Client ID in Orchid.
5. In **Password**, enter a secure password. You will use this value as the Client Secret in Orchid.
6. Select **Is OAuth confidential client**.
7. Select **Is Service User**.
8. Select **Password never expires**.
9. Verify that the user is active and not locked out.
10. Click **Create User**.

Grant the required Idira roles

Grant the service account permissions to read and onboard discovered accounts in Idira.

1. Idira, go to **Manage** > **Roles**.

2. Add the Orchid service account to both required roles:
   - Privilege Cloud Administrators Basic, or a custom role with equivalent Privilege Cloud administrator permissions.
   - Privilege Cloud Discovery Source.
3. Click **Save**.

Find your tenant ID and subdomain

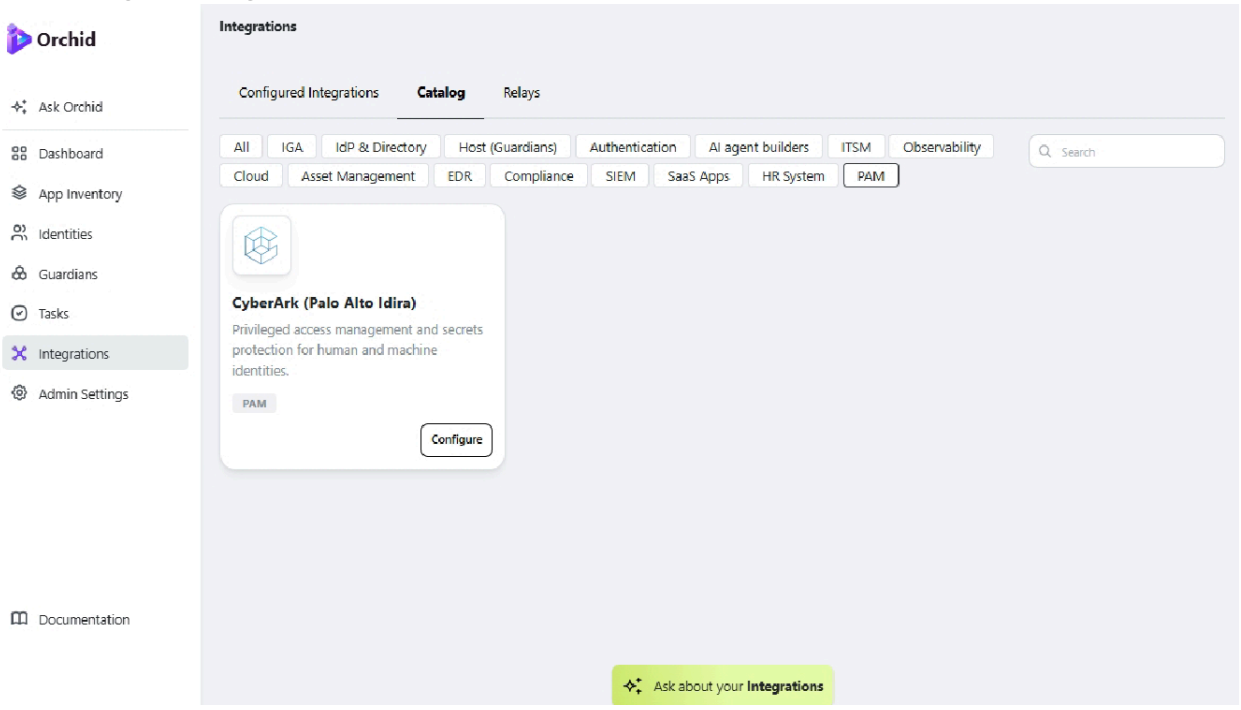
You need the Idira Identity tenant ID and the Idira Privilege Cloud subdomain to configure the integration in Orchid.

Value	Where to find it	Example
Tenant ID	In the Idira Identity Administration portal URL: https://<tenant_id>.id.cyberark.cloud	abc1234
Subdomain	In the Idira Privilege Cloud URL: https://<subdomain>.privilegecloud.cyberark.cloud	mycompany

Enter each value as a plain label. Do not include https://, dots, or a trailing slash.

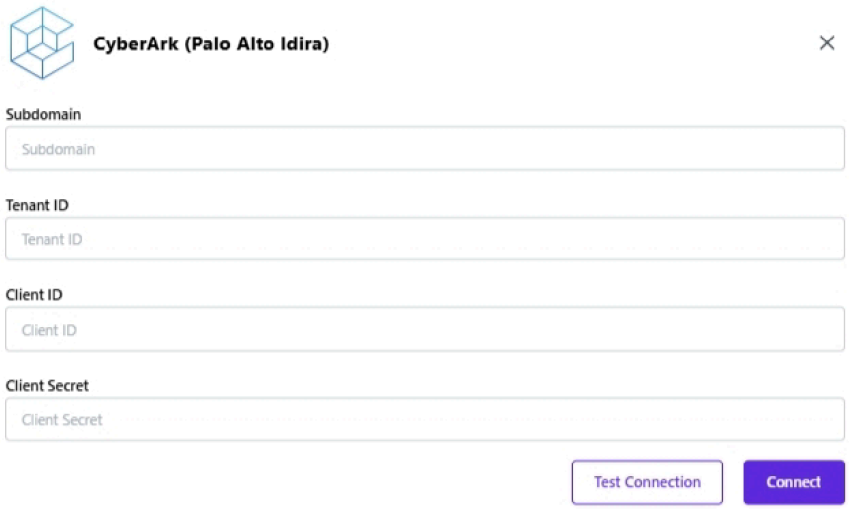
Configure the integration in Orchid

1. In Orchid, go to **Integrations**.



2. Open the **Catalog** tab.

3. Filter by **PAM**, or find the **Idira** integration in the catalog.
4. On the **Idira integration** card, click **Configure**. The **Connection** screen opens.



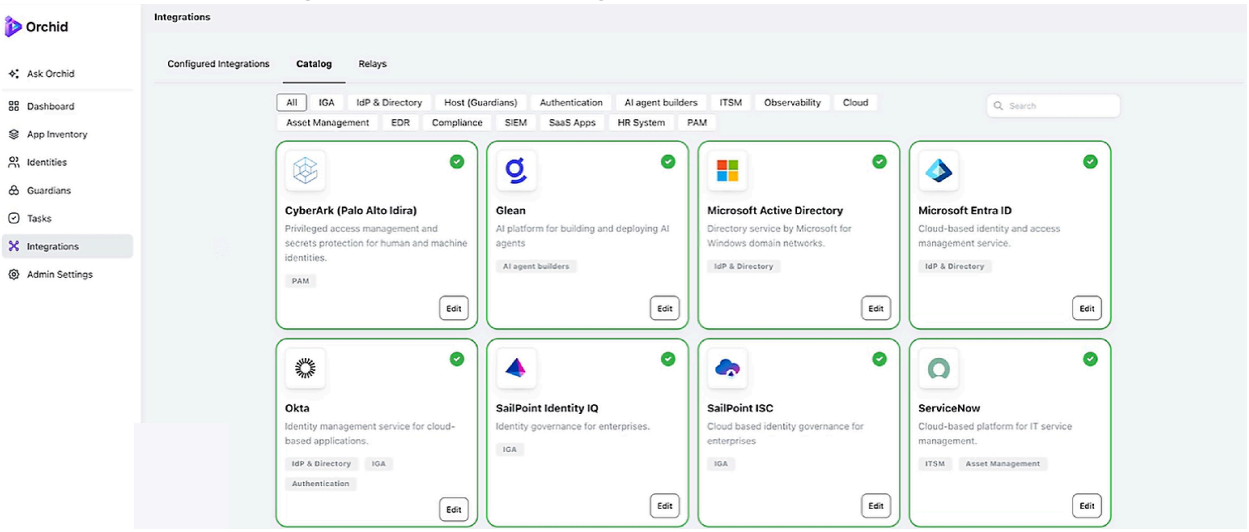
5. Enter the Idira connection details.
6. Click Test Connection.
7. After the connection test succeeds, click **Connect**.

Field	Value
Client ID	The login name of the Idira service account.
Client Secret	The password of the Idira service account.
Tenant ID	The Idira Identity tenant ID.
Subdomain	The Idira Privilege Cloud subdomain.

Verify the integration

1. In Orchid, go to **Integrations**.

2. Verify that the Idira integration appears with a green check mark status indicator.

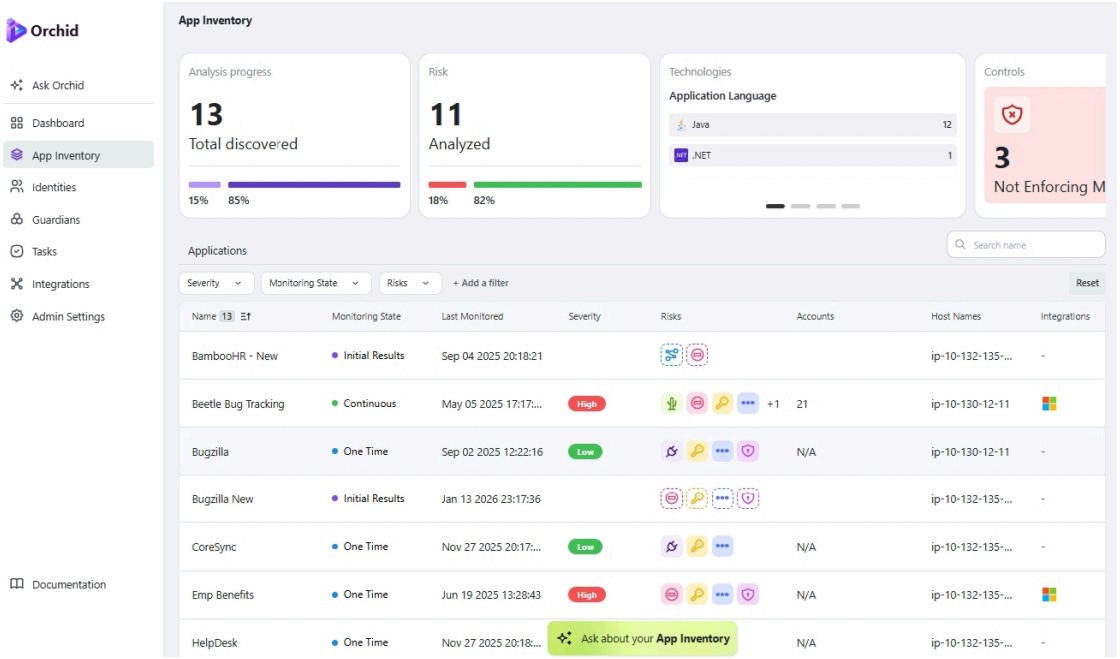


Report a privileged account to Idira

Report a privileged account from Orchid to Idira so the account can be reviewed in the Idira Discovered Accounts queue.

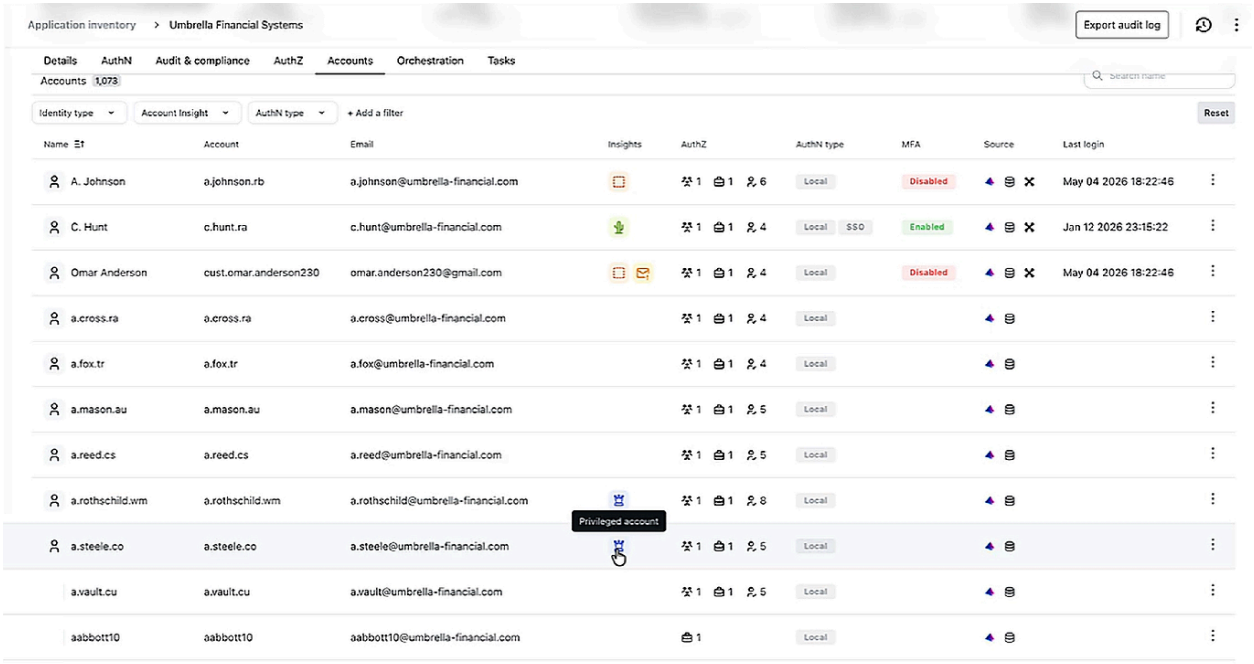
Find a privileged account in Orchid

1. In Orchid, go to App Inventory.



2. Open an application.

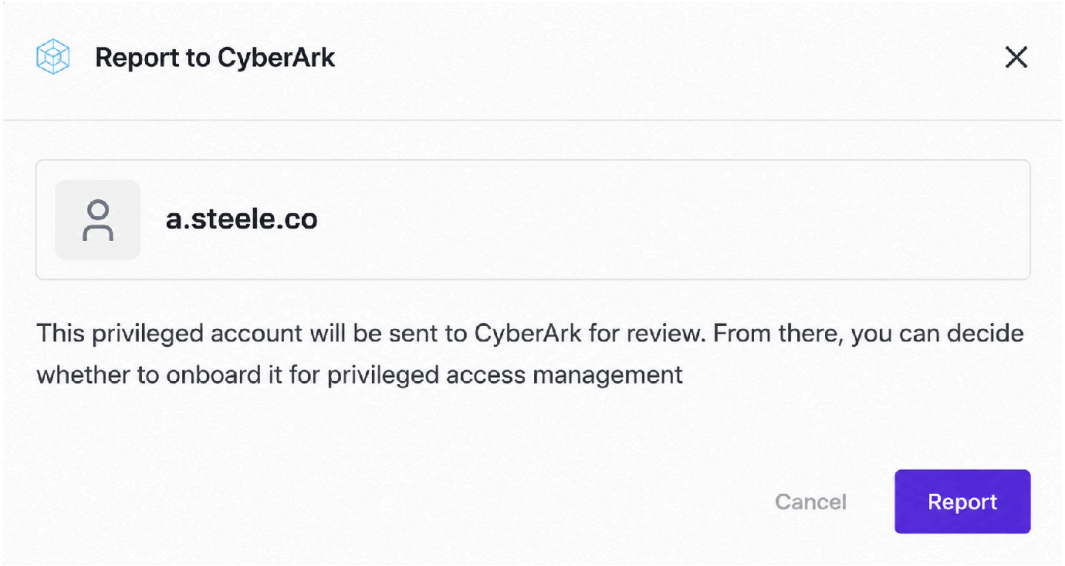
3. Open the **Accounts** tab.



4. Find an account with the **Privileged account** insight.

Report the account to Idira

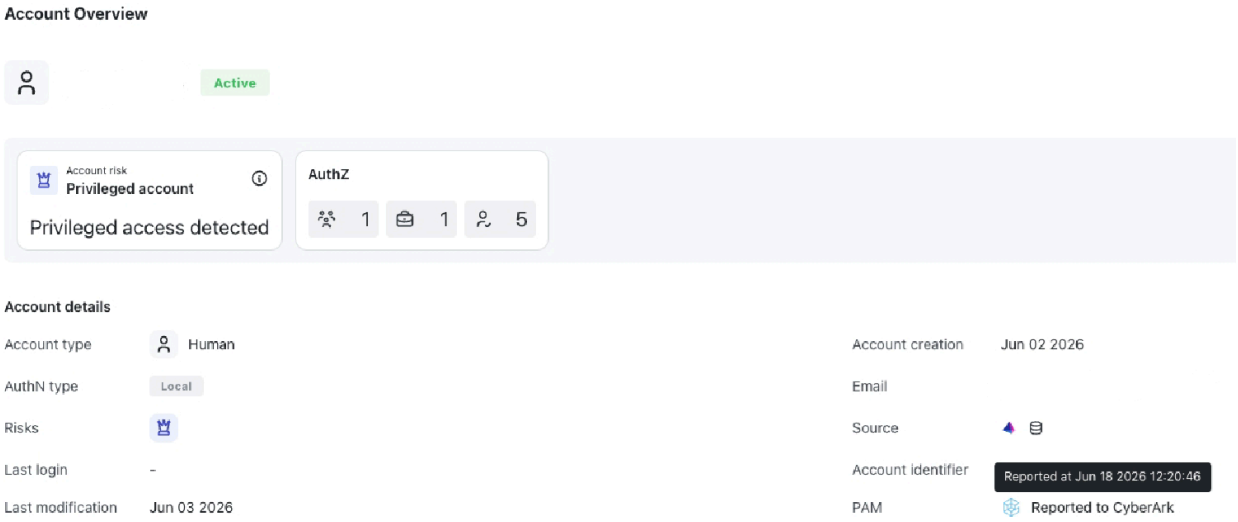
1. In the account row, click **More options** and select the Report to CyberArk.



2. Review the account details and click **Report**.

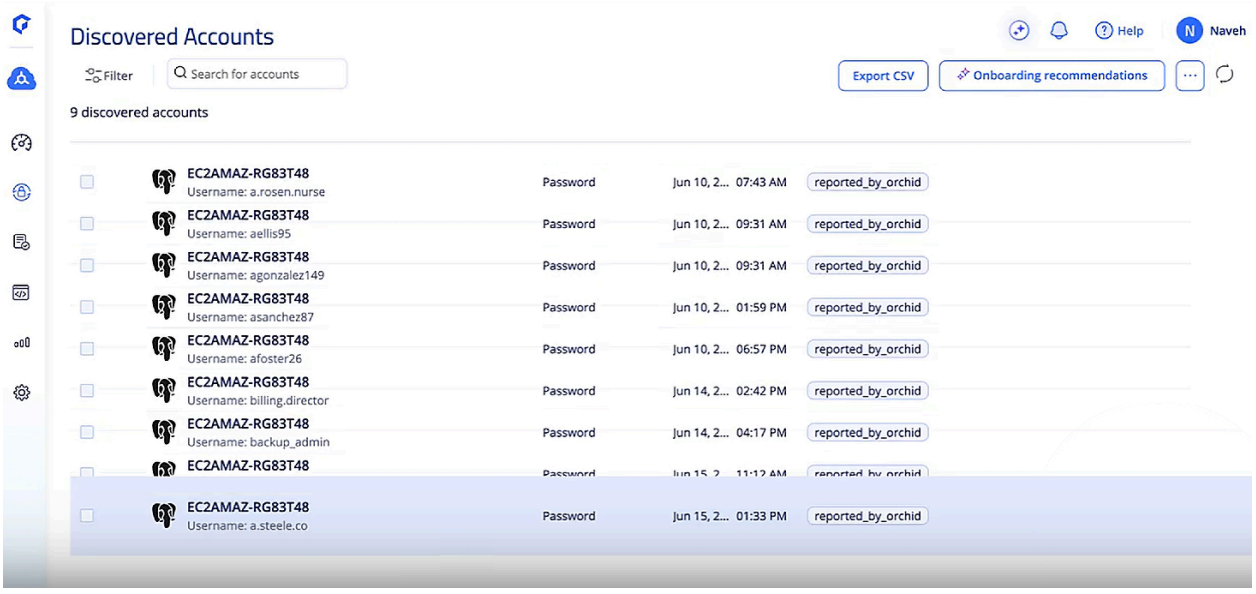
Orchid sends the account to Idira with the context Orchid discovered, including the account, the application context, and why the account is considered privileged.

Orchid adds the reported status to the account PAM field.



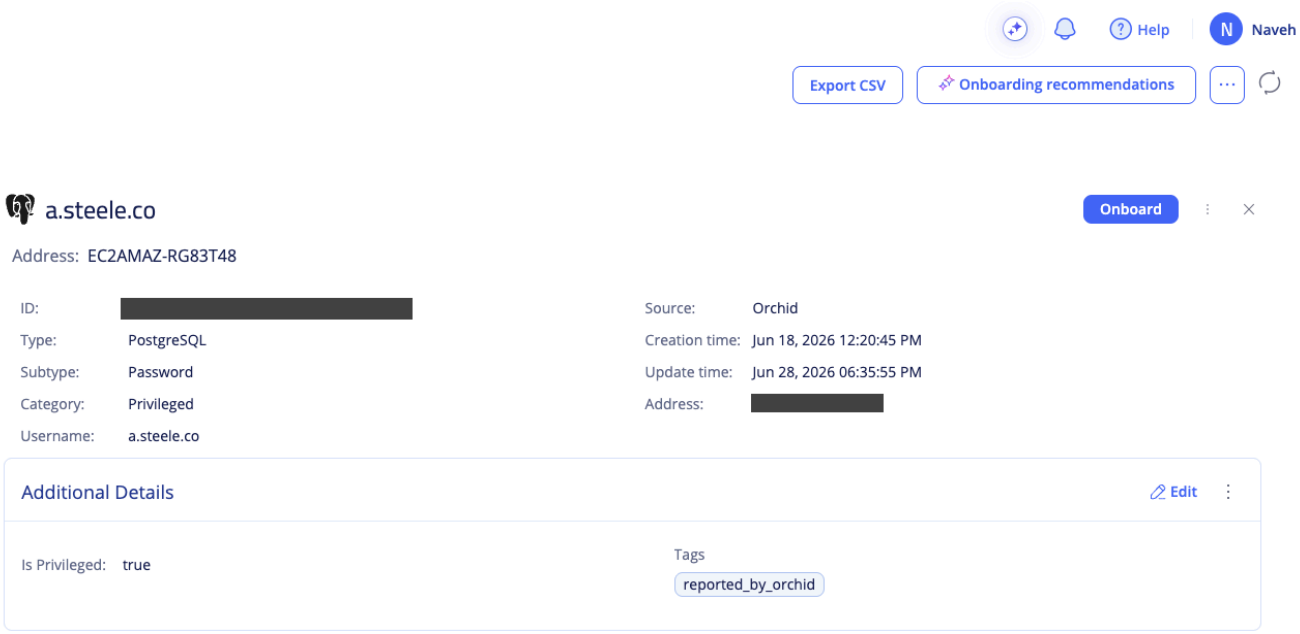
Review the reported account in Idira

1. In Idira, open **Discovered Accounts**.



2. Search for the account, or filter by the `reported_by_orchid` tag.

3. Open the discovered account.



4. Verify that the account details include:
   - **Source**: Orchid
   - **Category**: Privileged
   - **Tags**: `reported_by_orchid`
   - Account details such as username and address.
5. Review the account and continue with your standard account onboarding workflow in Idira.

Troubleshooting

Common troubleshooting steps

Error	What it means	What to check
Invalid CyberArk credentials	The Client ID or Client Secret is incorrect, or the service account is not configured as an OAuth confidential client.	Verify the service account login name and password. Verify that Is OAuth confidential client is selected.

CyberArk service account missing onboarding permissions	The service account can authenticate but does not have the required discovery permissions.	Add the service account to Privilege Cloud Discovery Source, or to an equivalent role.
CyberArk Privilege Cloud not reachable	The Privilege Cloud subdomain is incorrect or misspelled.	Verify the subdomain in https://<subdomain>.privilegecloud.cyberark.cloud.
CyberArk request timed out	Orchid could not complete the request to CyberArk.	Check connectivity to CyberArk and retry the connection test.

Helpful Resources

Orchid Security:

- Orchid Platform documentation (Documentation link in the Orchid console; Orchid Chat for how-to questions).

Palo Alto Networks:

- Idira / CyberArk Discovered Accounts documentation
  Idira product overview

Contact Information for Support

For Orchid Security specific issues:

- Orchid Platform documentation (Documentation link in the Orchid console; Orchid Chat for how-to questions).

For Palo Alto Networks specific issues:

- Palo Alto Networks Live Community
- Palo Alto Networks Customer Support

Technical Details

Idira API Endpoints used

- **Authentication**: POST https://{tenantId}.id.cyberark.cloud/oauth2/platformtoken - generates the service-user OAuth2 platform token used to authorize the Discovered Accounts calls.
- **Discovered Accounts**: POST https://{subdomain}.privilegecloud.cyberark.cloud/api/discovered-accounts - reports discovered privileged accounts into the Discovered Accounts queue, including identifiers, isPrivileged, source, tags, and account context; and reads account state back for status reflection in Orchid.