



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

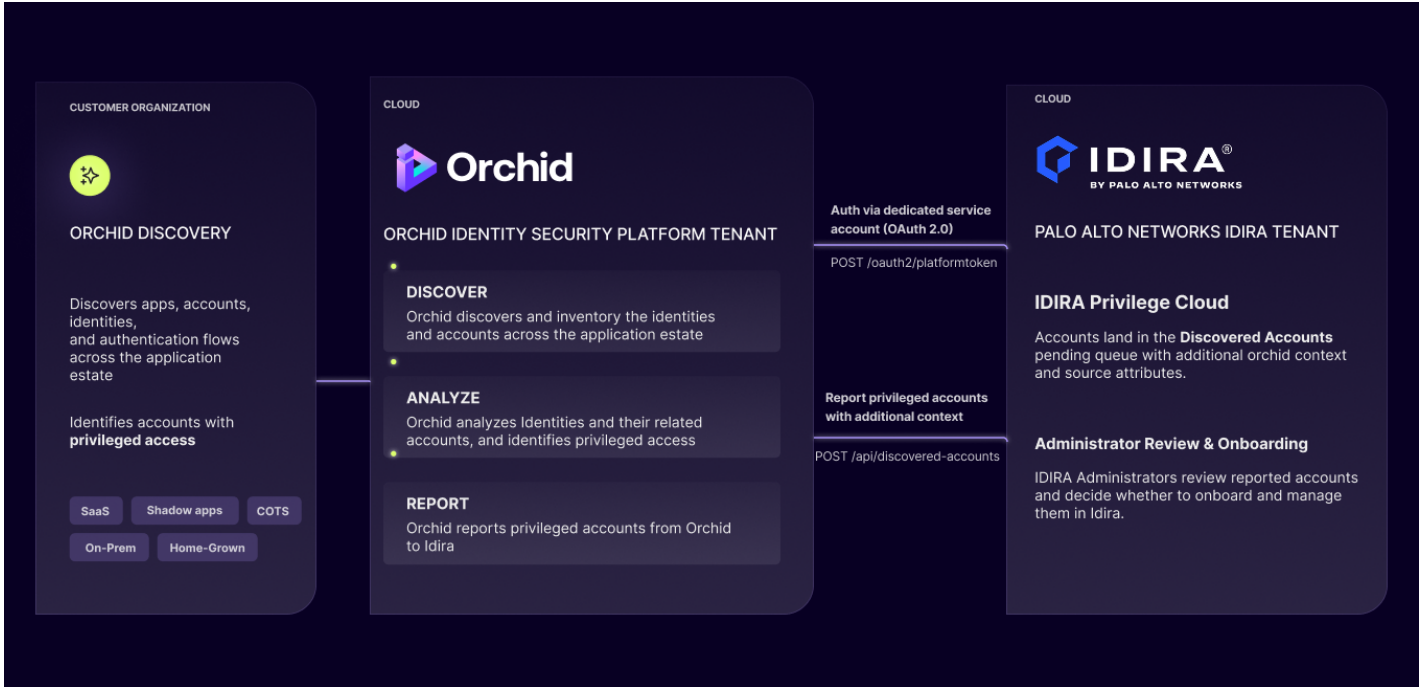
Idira Privilege Cloud	Validated	Idira Privilege Cloud Discovered Accounts service	Orchid Platform 2026.Q2
-----------------------	-----------	---	-------------------------

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

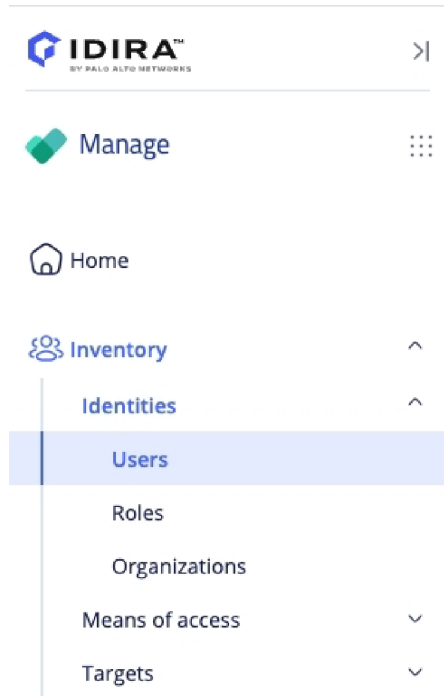
Palo Alto Networks Configuration

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.

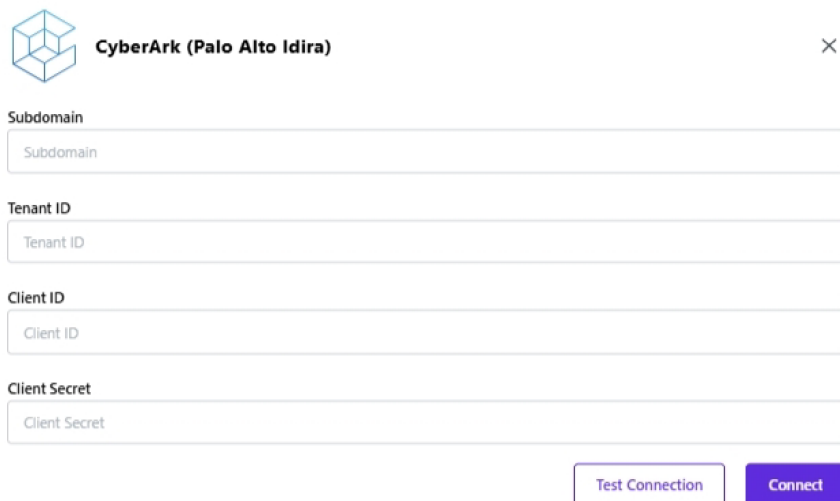
Configure the integration in Orchid

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

The screenshot displays the Orchid Security interface. On the left is a sidebar with navigation options: Ask Orchid, Dashboard, App Inventory, Identities, Guardians, Tasks, Integrations (selected), Admin Settings, and Documentation. The main area is titled 'Integrations' and has three tabs: 'Configured Integrations', 'Catalog' (active), and 'Relays'. Under the 'Catalog' tab, there are filter buttons for various categories: All, IGA, IdP & Directory, Host (Guardians), Authentication, AI agent builders, ITSM, Observability, Cloud, Asset Management, EDR, Compliance, SIEM, SaaS Apps, HR System, and PAM. A search bar is located on the right. The 'CyberArk (Palo Alto Idira)' integration is featured in a card, showing a cube icon, the name 'CyberArk (Palo Alto Idira)', a description 'Privileged access management and secrets protection for human and machine identities.', a 'PAM' tag, and a 'Configure' button. At the bottom right, there is a green button that says 'Ask about your 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.



CyberArk (Palo Alto Idira) ×

Subdomain
Subdomain

Tenant ID
Tenant ID

Client ID
Client ID

Client Secret
Client Secret

Test Connection Connect

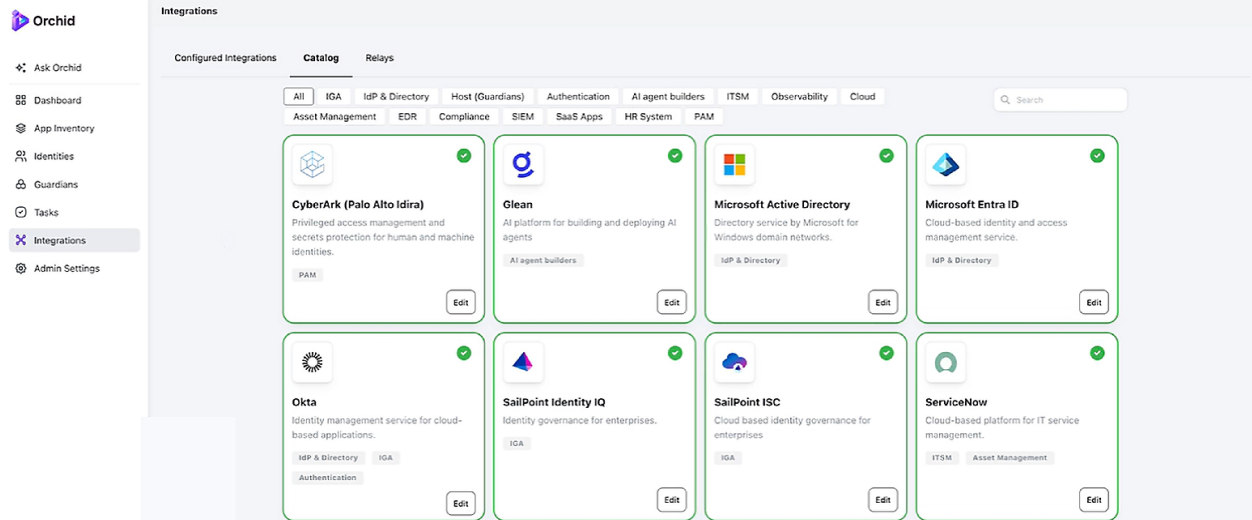
5. Enter the Idira connection details.
6. Click **Test Connection**.
7. After the connection test succeeds, click **Connect**.

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.

The screenshot displays the Orchid App Inventory dashboard. On the left is a sidebar with navigation links: Ask Orchid, Dashboard, App Inventory (selected), Identities, Guardians, Tasks, Integrations, and Admin Settings. Below the sidebar is a 'Documentation' link. The main content area is titled 'App Inventory' and includes several summary cards: 'Analysis progress' showing 13 total discovered accounts with a 15% to 85% progress bar; 'Risk' showing 11 analyzed accounts with an 18% to 82% risk bar; 'Technologies' showing application languages like Java (12) and .NET (1); and 'Controls' showing 3 not enforcing measures. Below these cards is a table of applications with columns for Name, Monitoring State, Last Monitored, Severity, Risks, Accounts, Host Names, and Integrations. The table lists applications such as BambooHR, Beetle Bug Tracking, Bugzilla, Bugzilla New, CoreSync, Emp Benefits, and HelpDesk. A 'Reset' button is located at the top right of the table. A green callout box at the bottom of the table says 'Ask about your App Inventory'.

Name	Monitoring State	Last Monitored	Severity	Risks	Accounts	Host Names	Integrations
BambooHR - New	Initial Results	Sep 04 2025 20:18:21				ip-10-132-135-...	-
Beetle Bug Tracking	Continuous	May 05 2025 17:17:...	High		+1 21	ip-10-130-12-11	
Bugzilla	One Time	Sep 02 2025 12:22:16	Low		N/A	ip-10-130-12-11	-
Bugzilla New	Initial Results	Jan 13 2026 23:17:36				ip-10-132-135-...	-
CoreSync	One Time	Nov 27 2025 20:17:...	Low		N/A	ip-10-132-135-...	-
Emp Benefits	One Time	Jun 19 2025 13:28:43	High		N/A	ip-10-132-135-...	
HelpDesk	One Time	Nov 27 2025 20:18:...			N/A	ip-10-132-135-...	-

2. Open an application.

3. Open the **Accounts** tab.

Application inventory > Umbrella Financial Systems Export audit log 🔔 ⋮

Details AuthN Audit & compliance AuthZ **Accounts** Orchestration Tasks

Accounts 1,078 🔍 Search name

Identity type Account Insight AuthN type + Add a filter Reset

Name	Account	Email	Insights	AuthZ	AuthN type	MFA	Source	Last login	
A. Johnson	a.johnson.rb	a.johnson@umbrella-financial.com		🔒 1 🗄️ 1 📄 6	Local	Disabled	🔗 📄 ✕	May 04 2026 18:22:46	⋮
C. Hunt	c.hunt.ra	c.hunt@umbrella-financial.com		🔒 1 🗄️ 1 📄 4	Local SSO	Enabled	🔗 📄 ✕	Jan 12 2026 23:15:22	⋮
Omar Anderson	cust.omar.anderson230	omar.anderson230@gmail.com		🔒 1 🗄️ 1 📄 4	Local	Disabled	🔗 📄 ✕	May 04 2026 18:22:46	⋮
a.cross.ra	a.cross.ra	a.cross@umbrella-financial.com		🔒 1 🗄️ 1 📄 4	Local		🔗 📄		⋮
a.fox.tr	a.fox.tr	a.fox@umbrella-financial.com		🔒 1 🗄️ 1 📄 4	Local		🔗 📄		⋮
a.mason.au	a.mason.au	a.mason@umbrella-financial.com		🔒 1 🗄️ 1 📄 5	Local		🔗 📄		⋮
a.reed.cs	a.reed.cs	a.reed@umbrella-financial.com		🔒 1 🗄️ 1 📄 5	Local		🔗 📄		⋮
a.rothschild.wm	a.rothschild.wm	a.rothschild@umbrella-financial.com		🔒 1 🗄️ 1 📄 8	Local		🔗 📄		⋮
a.steele.co	a.steele.co	a.steele@umbrella-financial.com		🔒 1 🗄️ 1 📄 5	Local		🔗 📄		⋮
a.vault.cu	a.vault.cu	a.vault@umbrella-financial.com		🔒 1 🗄️ 1 📄 5	Local		🔗 📄		⋮
aabbott10	aabbott10	aabbott10@umbrella-financial.com		🗄️ 1	Local		🔗 📄		⋮

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.

Report to CyberArk
✕

a.steele.co

This privileged account will be sent to CyberArk for review. From there, you can decide whether to onboard it for privileged access management

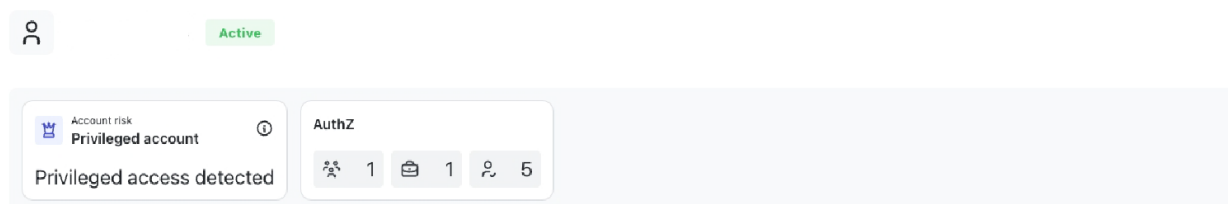
Cancel
Report

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.

Account Overview



The screenshot shows the 'Account Overview' page. At the top left is a user icon and a green 'Active' status tag. Below this, there are two main sections: 'Account risk' and 'AuthZ'. The 'Account risk' section shows 'Privileged account' and 'Privileged access detected'. The 'AuthZ' section shows three icons with counts: a key icon with '1', a briefcase icon with '1', and a person icon with '5'.

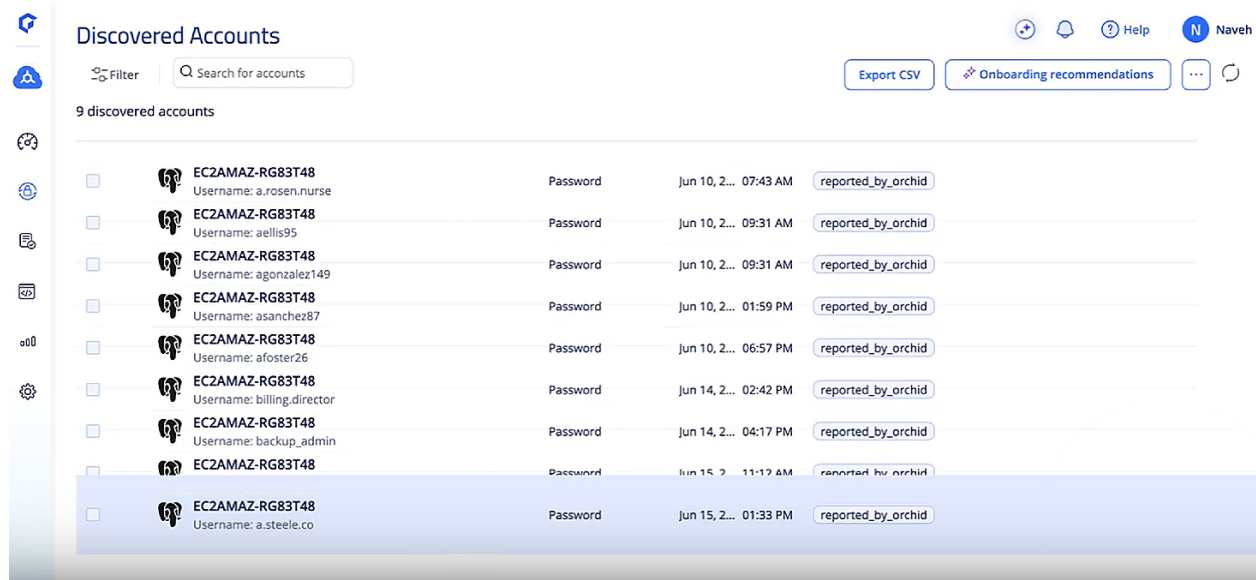
Account details

Account type: Human
AuthN type: Local
Risks: 
Last login: -
Last modification: Jun 03 2026

Account creation: Jun 02 2026
Email:
Source: 
Account identifier: Reported at Jun 18 2026 12:20:46
PAM:  Reported to CyberArk

Review the reported account in Idira

1. In Idira, open Discovered Accounts.



The screenshot shows the 'Discovered Accounts' page in Idira. The page has a sidebar with navigation icons and a main content area. The main content area has a search bar and a table of discovered accounts. The table has columns for account ID, username, password type, creation time, and a 'reported_by_orchid' tag. There are 9 accounts listed, all with the 'reported_by_orchid' tag.

Account ID	Username	Password	Creation Time	Tag
EC2AMAZ-RG83T48	Username: a.rosen.nurse	Password	Jun 10, 2... 07:43 AM	reported_by_orchid
EC2AMAZ-RG83T48	Username: aellis95	Password	Jun 10, 2... 09:31 AM	reported_by_orchid
EC2AMAZ-RG83T48	Username: agonzalez149	Password	Jun 10, 2... 09:31 AM	reported_by_orchid
EC2AMAZ-RG83T48	Username: asanchez87	Password	Jun 10, 2... 01:59 PM	reported_by_orchid
EC2AMAZ-RG83T48	Username: afoster26	Password	Jun 10, 2... 06:57 PM	reported_by_orchid
EC2AMAZ-RG83T48	Username: billing.director	Password	Jun 14, 2... 02:42 PM	reported_by_orchid
EC2AMAZ-RG83T48	Username: backup_admin	Password	Jun 14, 2... 04:17 PM	reported_by_orchid
EC2AMAZ-RG83T48	Username: a.steele.co	Password	Jun 15, 2... 11:12 AM	reported_by_orchid
EC2AMAZ-RG83T48	Username: a.steele.co	Password	Jun 15, 2... 01:33 PM	reported_by_orchid

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

3. Open the discovered account.

The screenshot shows the Idira interface with a top navigation bar containing a plus icon, a bell icon, a help icon, and a user profile icon labeled 'N Naveh'. Below the navigation bar are buttons for 'Export CSV', 'Onboarding recommendations', and a refresh icon. The main content area displays the account details for 'a.steele.co' with an 'Onboard' button and a close icon. The account address is 'EC2AMAZ-RG83T48'. The details are organized into two columns: the left column lists 'ID' (redacted), 'Type: PostgreSQL', 'Subtype: Password', 'Category: Privileged', and 'Username: a.steele.co'; the right column lists 'Source: Orchid', 'Creation time: Jun 18, 2026 12:20:45 PM', 'Update time: Jun 28, 2026 06:35:55 PM', and 'Address' (redacted). Below these details is an 'Additional Details' section with an 'Edit' link and a dropdown menu. It shows 'Is Privileged: true' and a 'Tags' section with a tag labeled 'reported_by_orchid'.

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 <code>https://<subdomain>.privilegecloud.cyberark.cloud</code> .
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.