



SECRETS MANAGER AGENTLESS CENTRAL CREDENTIAL PROVIDER (CCP_ INTEGRATION)

Name of Company: Claroty
Website: Claroty.com
Name of Product: xDome Secure Access
Version: 5.2.1
Date: March, 2026

Table of Contents

1	<i>Partner solution overview.....</i>	3
2	<i>Key benefits.....</i>	3
3	<i>Product diagram & Description of Product Integration.....</i>	4
3.1	Secrets Manager Integration.....	4
3.2	Credential Retrieval.....	4
4	<i>Requirements.....</i>	4
5	<i>Secrets manager installation.....</i>	4
6	<i>Secrets manager configuration.....</i>	5
6.1	Defining The Application ID (APPID) and Authentication Details.....	5
6.2	Provisioning Accounts and Setting Permissions for Application Access.....	7
7	<i>Partner Product installation & integration configuration.....</i>	10
8	<i>Partner contact info.....</i>	11

1 PARTNER SOLUTION OVERVIEW

xDome Secure Access provides both employees and third-party contractors with secure remote access to Industrial Control Systems for monitoring, maintenance, and upgrading. It offers secure access to target devices, and monitors and records the activities of users accessing them to comply with regulatory requirements.

The xDome Secure Access solution provides granular control over the users who may access the system, the specific parts of the system to which they have access, and the precise duration for which they are permitted access.

This integration allows xDome Secure Access customers to store their device credentials within CyberArk CCP. At the start of each session, xDome Secure Access automatically retrieves these device credentials on demand directly from the vault.

Version: 5.2.1

Platform components:

- **Access Manager:** The Access Manager is an entity that allows users to see an aggregate picture of all Access Points, manage and control all Access Points, and create remote sessions. However, the Access Manager cannot initiate remote sessions without an Access Point. Remote sessions are initiated from the Access Manager to the Access Point, and actions performed on the Access Point's target Devices are handled from the Access Point. The actions on the Access Point's target Devices and the connections from the Access Manager to the Access Point are created transparently.
- An **Access Point** is an entity that allows users to create local sessions to Access Point target Devices and to manage remote access at the Access Point level without initiating a session from the Access Manager or having connectivity to the Access Manager. If the Access Manager is down, the Access Point can operate independently and allow users to directly access the Access Point for connecting to target Devices, viewing session recordings, and uploading/downloading files.

2 KEY BENEFITS

Benefits of xDome Secure Access:

- **Enhancing Operational Productivity:** Claroty's xDome Secure Access is designed for the OT domain, enabling seamless connectivity for both first- and third-party users. It effectively reduces Mean Time to Repair (MTTR) by facilitating quick issue resolution, even in low bandwidth conditions, ensuring high system availability and resilience in critical sites.
- **Strengthens Security Controls with Zero Trust :** xDome Secure Access incorporates a Zero Trust framework, enhanced by Privileged Access Management (PAM) and Identity Governance and Administration (IGA) functionalities, to safeguard your organization's OT systems. This comprehensive approach manages the entire identity lifecycle with utmost precision, significantly reducing the risk landscape and strengthening network defenses against both internal and external threats.

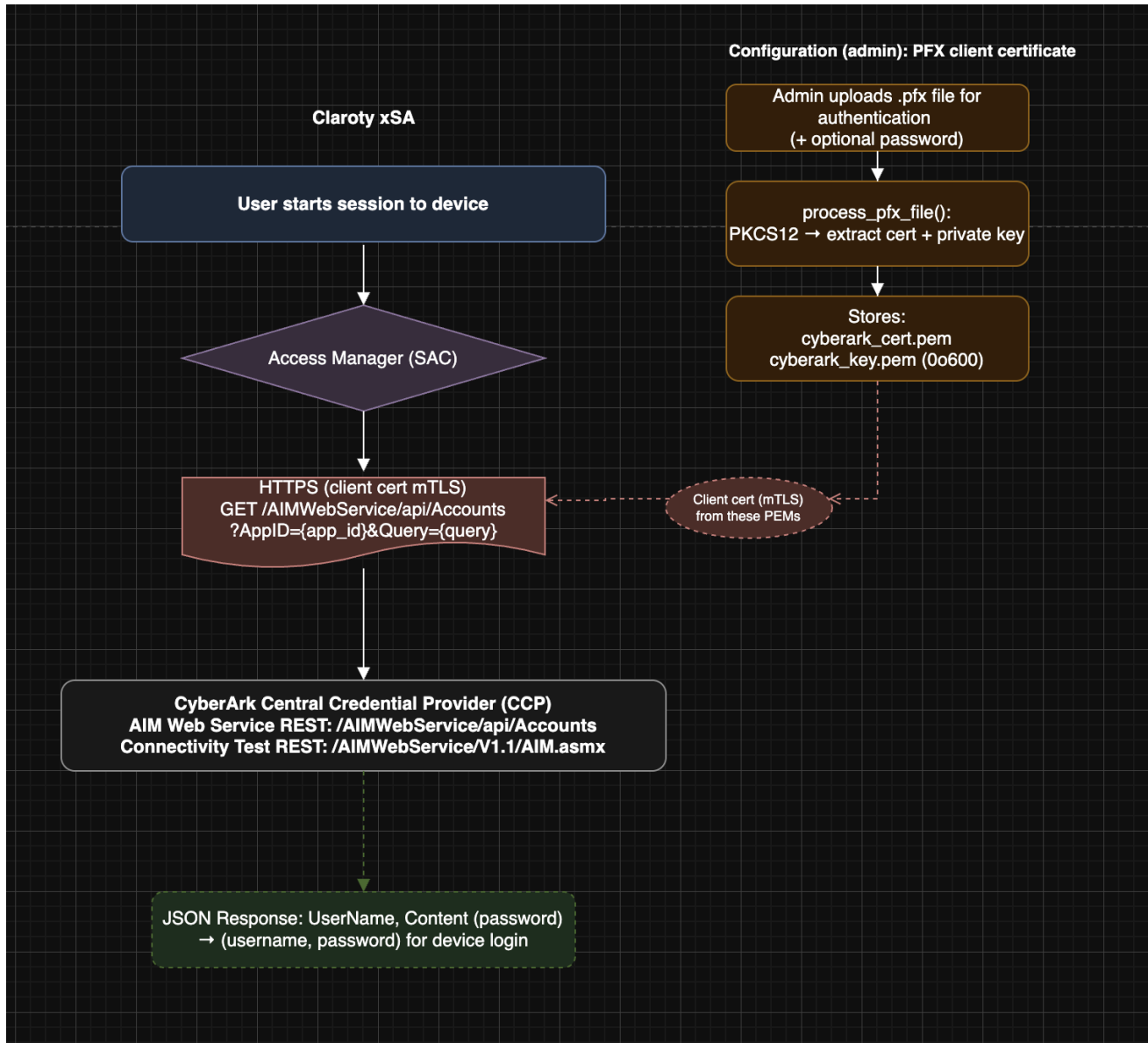
- **Streamlining Administrative Processes:** With its scalable architecture, xDome Secure Access simplifies administrative tasks, operating seamlessly across both on-premises and cloud environments. It leverages the advanced asset inventory capabilities of the broader Claroty xDome Platform to enhance system onboarding, swiftly importing assets for a faster and more comprehensive setup. Integration with leading IAM tools further improves user identity management and centralizes control over policy creation and site management, minimizing downtime and boosting production resilience.
- **Ensuring Compliance and Auditing Integrity:** xDome Secure Access offers necessary controls for real-time logging and auditing, essential for upholding comprehensive audit trails and adhering to stringent regulatory standards. This ensures your operations comply with the latest mandates, protecting your organization from potential legal and financial consequences.

Benefits of integrating xDome Secure Access with CyberArk Central Credential Provider:

1. **Provide a Credential Vault External to xDome Secure Access** – Enable retrieving credentials directly from CyberArk.
2. **Retrieve passwords dynamically** – Fetch passwords in real-time when a session with a device starts.
3. **Support CyberArk's password rotation** – Our system should always pull the latest password from CyberArk.
4. **Implement logging and auditing** – Maintain a record of password retrievals for security and compliance.

3 **PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION**

The following image describes the system architecture, including the CyberArk component.



Credential Retrieval

This is the high-level sequence of events for integrating CyberArk with xDome Secure Access.

1. Establish Integration in xDome Secure Access

An administrator configures the integration by providing CyberArk Vault connection details (address, certificate, timeout, and AppID) in xDome Secure Access's settings. Integration can be enabled, disabled, and connectivity tested from the UI at any time.

2. Device Credential Association

Devices in xDome Secure Access can be linked to the CyberArk Vault by specifying lookup parameters (such as Safe, Folder, Object, etc.), ensuring each device's credentials are retrieved from CyberArk when needed.

3. Session Initiation

When a remote access session is initiated to a device, xDome Secure Access authenticates to CyberArk using a certificate, queries the vault for the device's current credentials using the pre-configured parameters, and uses those credentials only in memory for the duration of the session.

4. Password Retrieval and Rotation

CyberArk supplies the latest credentials for the device. Credentials are fetched for each new session, allowing for seamless password rotation as managed within CyberArk.

5. Auditing and Logging

Every credential retrieval is logged for compliance/audit purposes, enabling organizations to monitor all access to privileged credentials.

4 REQUIREMENTS

Before you begin:

1. CyberArk Vault Readiness

- CyberArk Central Credential Provider (CCP) must be deployed and accessible from the network where xDome Secure Access operates. This typically means the CyberArk Vault is running in the customer's data center, storing credentials for OT assets that xDome Secure Access will manage.
- CyberArk must be configured to manage the credentials (passwords) for target devices that will be accessed via xDome Secure Access. This includes password rotation policies, safe and folder structure, and objects for each account.

2. Authentication and Certificate Configuration

- **API Certificates:**
 - xDome Secure Access requires a valid client certificate (in Base64 format) for authentication with the CyberArk API endpoint, which must be provisioned in CyberArk.
- **AppID**
 - The CyberArk *AppID* is required for authorized application credential retrieval. This should be set up in CyberArk to allow access to xDome Secure Access according to organizational policy.

3. Administrator Permissions

- **CyberArk:** The administrator performing the integration must have CyberArk rights to create AppIDs, manage safes/folders/objects, and grant xDome Secure Access access to required passwords.
- **xDome Secure Access:** The user must have Claroty xDome Secure Access admin privileges to configure integrations (Settings > Supported Integrations) and device-level credential retrieval policies.

4. Network Connectivity

- **Reachability:** Direct and secure network connectivity must exist between xDome Secure Access (both Access Manager and, if required, Access Point) and the CyberArk server's API endpoint (often AIMWebService). Any required firewall rules must be opened between the xDome Secure Access components and CyberArk, in accordance with organizational security policy.

- **Timeouts:** Properly configured connection timeouts are necessary to avoid integration failures caused by slow network links.
5. **Device Query Parameters**
- For each device to be managed by xDome Secure Access via CyberArk, one or more of the following query parameters must be defined. These are used by xDome Secure Access to fetch the correct credentials from CyberArk:
 - Safe (logical password container)
 - Folder (organizes objects inside the Safe)
 - Object (unique credential identifier)
 - Username (if applicable)
 - Address/Host/IP
 - Policy ID (optional, for advanced controls)
 - These parameters should be mapped and stored in xDome Secure Access to avoid ambiguity. Ensure the query is unique, so that only one password is retrieved per session request.
6. **Test Connectivity**
- Use xDome Secure Access's *Connectivity Test* feature to validate live CyberArk API access before enabling integration for production workflows. Successful connectivity should be logged, and failures must be analyzed and resolved before formal enablement.

5 CENTRAL CREDENTIAL PROVIDER INSTALLATION

To install Central Credential Provider (CCP), see the [Central Credential Provider installation documentation](#).

6 CENTRAL CREDENTIAL PROVIDER CONFIGURATION

The following sections provide details on Central Credential Provider (CCP) configuration with your CyberArk PAM solution (PAM Self-hosted / Privilege Cloud).

Define the application ID (app ID) and authentication details

To define the application, define it manually through the CyberArk Password Vault Web Access (PVWA) / Privilege Cloud interface:

1. Log in with a user who has permissions to manage applications (it requires **Manage Users** authorization).
2. In the Applications tab, click **Add Application**. The Add Application page appears.

Add Application

Name:

Description:

Business owner

First Name:

Last Name:

Email:

Phone:

Location:

☐ Time Restrictions: From: To:

☐ Expiration Date:

☐ Disabled

3. Specify the following information:
 - In the Name box, provide the unique name (ID) of the application. The recommended application ID for this integration is: APP ID = CCP_Claroty_AppID
 - In the **Description** box, provide a short description of the application that will help you identify it.
 - In the **Business owner** section, provide contact information about the application's business owner.
 - In the **Location** box, specify the location of the application within the Vault/Privilege Cloud hierarchy. If a location is not selected, the application will be added to the same location as the user creating it.
4. Click **Add**. The application has been added and is displayed on the Application Details page.

Application Details: PartnerName-ApplicationName

ApplicationId: PartnerName-ApplicationName

Description:

Business Owner:

Business Owner's Phone:

Business Owner's Email:

Location: \

Access Permitted: None

Expiration Date: None

Disabled: No

Authentication

Allowed Machines

Add

OS user

Path

Hash

Certificate Serial Number

Info

Value

Page 1 of 1

No authentications to display

Allow extended authentication restrictions. This requires Provider/s upgrade for this application.

Use credential file authentication

5. Select the **Allowing extended authentication restrictions** option. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.
6. Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password.

Clarity recommends using a certificate encrypted with a passkey, as well as using the TLS protocol for enhanced security.

In the Authentication tab, click **Add**. A drop-down list of authentication characteristics is displayed.

- a. Select the authentication characteristic to specify.
- b. Select **OS user**. The Add Operating System User Authentication window appears.

Add Operating System User Authentication

OS User:

Add

Cancel

- c. Specify the name of the OS user who will run the application, then click **Add**. The OS user is listed in the Authentication tab.

7. Specify the Certificate Serial Number:

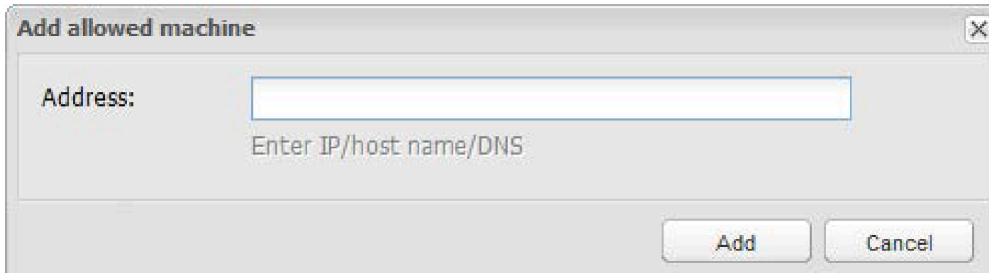
Add Certificate Serial Number Authentication

SN:

Add

Cancel

8. Specify the application's Allowed Machines. This information enables the Credential Provider to ensure that only applications running from specified machines can access their passwords.
 - a. In the Allowed Machines tab, click **Add**. The Add allowed machine window is displayed.



- b. In the **Address** box, specify the IP address / host name/ DNS of the machine where the application will run and request passwords, then click **Add**. The IP address is listed in the Allowed Machines tab.

Provision accounts and set permissions for application access

For the application to perform its functionality or tasks, the application must have access to particular accounts that already exist, or to new accounts to be provisioned in CyberArk Vault / Privilege Cloud.

In the **Clarity Safe**, provision privileged accounts that will be required by the application. You can do this in one of the following ways:

- **Manually** – Add accounts manually one at a time, and specify all the account details
- **Automatically** – Add multiple accounts automatically using the Password Upload feature

For this step, you need **Add accounts** permissions in the **Clarity Safe**.

For more information about adding and managing privileged accounts, see the documentation for your [PAM solution](#).

Once the accounts are managed by CyberArk, make sure to set up access to both the application and CyberArk Application Credential Providers serving the Application.

Add the CCP user (where the Central Credential Provider is installed) and application users as members of the **Clarity Safe** where the application passwords are stored. This can be done manually in the **Safes** tab, or by specifying the Safe names in the CSV file for adding multiple applications.

1. Add the CCP user as a Safe member with the following access:
 - o **List accounts**
 - o **Retrieve accounts**
 - o **View Safe Members**

Note: When installing multiple Providers for this integration, it is recommended to create a group for them, and add the group to the Safe once with the above authorization.

Add Safe Member

Search: Search In: **Vault**

Selected Search: Vault

Name	Business Email	Full Name
------	----------------	-----------

☐ Access

- ☐ Use accounts
- ☒ Retrieve accounts
- ☒ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

- ☐ View Audit log
- ☒ View Safe Members

- b. Add the application (the app ID) as a Safe member with the following access:
- o **Retrieve accounts**

Add Safe Member

Search: Search In: **Vault**

Selected Search: Vault

Name	Business Email	Full Name

☐ Access
☐ Use accounts
☒ Retrieve accounts
☐ List accounts
☐ Account Management
☐ Safe Management
☐ Monitor
☐ View Audit log
☐ View Safe Members

- c. If the Safe is configured for object level access, make sure that both the CP user and the application have access to the passwords to retrieve.
- d. For more information about configuring Safe members, see the documentation for your [PAM solution](#).

7 xDOME SECURE ACCESS INTEGRATION CONFIGURATION

This section describes how to configure the integration between xDome Secure Access and Credential Providers.

To add the CyberArk Integration to your Access Manager:

1. Go to **Settings >Supported Integrations**, locate the CyberArk card, and click **+Add**.



Enabled



CyberArk Secrets Manager CCP

Integrate with CyberArk's Central Credential Provider to retrieve device credentials upon session creation

2. Complete the following fields on the CyberArk CCP dialog:

Save CyberArk Secrets Manager CCP Integration

×

Connection Details

Address - IP/Hostname*

Enter IP Address or Hostname

Authentication Details

AppID*

Enter AppID

Client Certificate*

⬆

Drag & Drop a file or [Browse](#)

.pfx

Passkey

Enter Passkey

TLS Configurations

☐ Enable TLS Verification ⓘ

☐ Check Hostname ⓘ

Use Custom Certificate Authority ⓘ

⬆

Drag & Drop a file or Browse

.pem,.der,crt,.cer

Certificate Expiration Date

General Integration Settings

Timeout* ⓘ

30 Seconds

Connectivity Test

Save

- **Address - IP/Hostname**—Enter the IP Address of the CyberArk vault.
- **AppID**—Enter the identifier for an application authorized to retrieve credentials from the Vault.

- **Client Certificate**—Upload a CyberArk certificate.
 - **Passkey**—If the CyberArk certificate was encrypted, enter the passkey here.
 - **Enable TLS verification**—If the TLS protocol is selected, then it will also be possible to select **Check Hostname**. To verify TLS, upload a **Custom Certificate Authority**.
 - **Timeout**—Set the number of seconds after which the CyberArk connection will time out.
3. Click **Test Connectivity** to ensure that xDome Secure Access can successfully communicate with CyberArk.

To configure a device to use credentials from CyberArk:

1. Click Devices > +Add Device for a new device, or click the 3-dot menu on an existing card to Edit Device. You will see the following screen:

The screenshot shows the 'Add Device' configuration interface. At the top, there are three input fields: 'Device Name*' with the value 'CyberArk test', 'Access Point*' with a dropdown showing 'site-1', and 'Protocol*' with a dropdown showing 'SSH'. Below this is a sidebar with four options: 'Connection & Authentication' (highlighted in purple), 'Session Settings', 'User Permissions', and 'Custom Attributes'. The main content area is titled 'Connection Configuration' and contains two fields: 'Address - IP/Hostname*' with a placeholder 'Enter IP/Hostname' and 'Port*' with the value '22'. Below this is the 'Authentication Details' section. It starts with a radio button selection for 'xSA Password Vault' (which is selected). Under this, there is a 'Use stored credentials' dropdown menu set to 'Always Use'. Below that are two input fields: 'Username*' with a placeholder 'Enter Username' and 'Password' with a placeholder 'Enter Password' and a toggle icon. At the bottom of the 'Authentication Details' section, there is an unselected radio button for 'Cyberark Password Vault'. An 'Add' button is located in the bottom right corner of the form.

2. The default setting is xDome Secure Access Password Vault. This option allows you to enter your Username and Password and to decide when to use the xDome Secure Access stored credentials: Always Use, Never Use, or Optional.
3. To use the CyberArk password vault, click that option. Complete the following fields:

Add Device

Device Name*
CyberArk test

Access Point*
site-1

Protocol*
SSH

Connection & Authentication
Session Settings
User Permissions
Custom Attributes

Use stored credentials
Never Use

Username*
Enter Username
Password
Enter Password

Cyberark Password Vault

Use stored credentials
Always Use

+ Custom Parameters (0)

Select Key
Enter a query parameter

Test Password Vault

Add

- a. You can choose to use the CyberArk stored credentials:
 - i. Always, or
 - ii. Optional

Note: If you choose Optional, you can either use credentials from CyberArk or enter your credentials manually.
- b. Select a Key to unlock your credentials, and add the relevant query parameter.
 - i. Select one or more of the following preset parameters, and then add values for them:
 - Username
 - Address
 - Policy ID
 - Safe
 - Folder
 - Object
 - ii. Optionally, you can define one or more **Custom Parameters** and then add values for them.
4. To verify that your query will successfully retrieve the device's credentials, click **Test Password Vault**. The system will let you know whether the password was retrieved successfully or not.
5. When you are done defining your parameters and your test has succeeded, click **Add** for a new device or **Save** for an existing device.

8 PARTNER CONTACT INFO

Business Contact	Name	Peter Lund
------------------	------	------------

	Email	peter.l@claroty.com
	Tel	
Technical Contact	Name	Shani Bentov
	Email	shani.b@claroty.com
	Tel	
Support Contact	Name	Doron Nuni
	Email	doron.n@claroty.com
	Tel	

