CyberArk CCP Reference Guide

Privitar Data Privacy Platform, version 4.5.0

Publication date September 6, 2023

Privitar Data Privacy Platform, version 4.5.0

The information in this documentation is subject to change without notice. If you find any problems in this documentation, report them to us at infa_documentation@informatica.com.

Informatica products are warranted according to the terms and conditions of the agreements under which they are provided. INFORMATICA PROVIDES THE INFORMATION IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

Table of Contents

1. Introduction

The Privitar Data Privacy Platform is a data privacy solution that enables organizations to use sensitive datasets more safely.

Note

For ease of reference, the Privitar Data Privacy Platform is referred to as the **Privacy Platform**, (or just **the platform**) in the rest of this manual.

CyberArk provides a key management system (KMS) and an access policy control software solution.

Note

For ease of reference, CyberArk's Application Access Manager (AAM) Central Credential Providers is referred to as **CyberArk CCP**, (or just **CyberArk**) in the rest of this manual.

Publisher uses the Hadoop KMS (Key Management Service) to access encryption keys used by:

The key benefits of the platform are:

- Centralized management of data privacy policies
- Comprehensive set of Privacy Enhancing Techniques (PETs).

The key benefits of integrating the platform with CyberArk CCP are:

- Another method for users to manage the credentials used by the platform.

1.1. Compatibility

Privitar v4.0.1 provides support for CyberArk CCP. It is certified, fully integrated, and tested with CyberArk CCP v9.7+.

2. Architecture

The Privacy Platform consists of two main application components:

- Policy Manager
- Event Broker

Both of these components have been integrated with CyberArk CCP.

Note

The Event Broker is an optional application component that can be installed on the platform. For the purposes of this document, it is assumed that the Event Broker **has** been installed.

2.1. Integration process

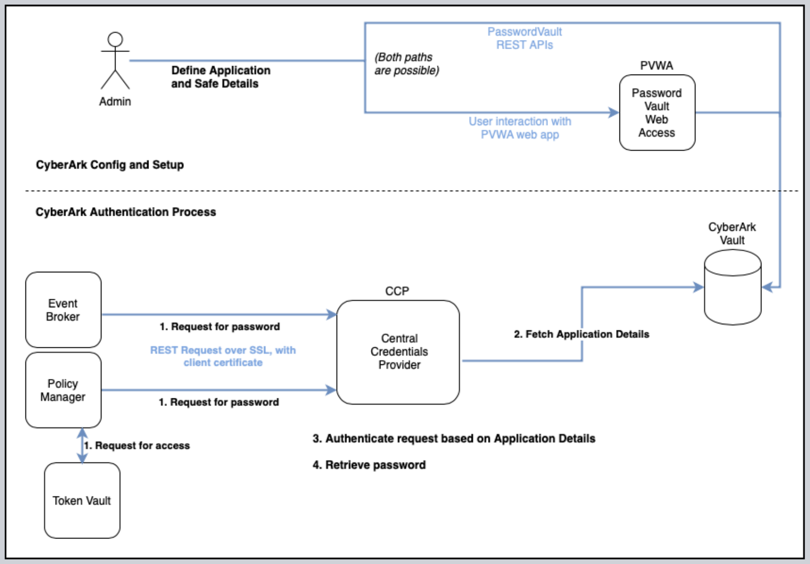
The **Policy Manager** is responsible for managing privacy policies. It runs Jobs that de-identify an input dataset according to a pre-defined privacy policy.

The **Event Broker** is an analytics and diagnostics tool for the platform.

In a typical installation, there will be two integration endpoints:

- One endpoint for the Policy Manager to retrieve credentials from CyberArk CCP.
- One endpoint for the Event Broker to retrieve credentials from the CyberArk CCP.

The following diagram shows how these application components interface to CyberArk CCP and how other CyberArk components are used during configuration and setup of an application, and for authentication purposes:


Admin
Define Application and Safe Details
(Both paths are possible)
PasswordVault REST APIs
PVWA
Password Vault Web Access
User interaction with PVWA web app
CyberArk Config and Setup
CyberArk Authentication Process
CyberArk Vault
Event Broker
1. Request for password
REST Request over SSL, with client certificate
CCP
Central Credentials Provider
2. Fetch Application Details
Policy Manager
1. Request for password
1. Request for access
Token Vault
3. Authenticate request based on Application Details
4. Retrieve password

For CyberArk configuration and setup, each application needs to be defined and application-specific details added to one or more Safes in the CyberArk Vault. This configuration and setup can be done via the CyberArk Password Vault REST API or via the Password Vault Web Access (PVWA) interface.

The CyberArk authentication process is handled by the CyberArk CCP. An application makes requests to CCP for passwords or other credentials. CCP will authenticate the request based on the details that have been defined for the application (during the configuration and setup of the application). If the details are correct, CyberArk fetches the credentials from the CyberArk Vault and returns them to the requesting application.

2.2. Credential Retrieval

There are four flows in which credential retrieval may occur on the platform:

- On start up of Policy Manager, to fetch any credentials that it requires.
- On start up of the Event Broker, to fetch any credentials that it requires.
- When a Policy Manager user enters a new CyberArk CCP query for their team-specific Job processing credentials. Credential retrieval is performed to validate the query. This could include a request to access a JDBC Token Vault.
- When Policy Manager handles a request to retrieve a Job definition to apply a privacy policy. (Typical usage is below 100 requests per hour.)

2.3. Requirements

The Integration requirements are:

- The instance on which Policy Manager is deployed requires connectivity to a CyberArk CCP that has access to credentials specified in the Policy Manager configuration and Token Vault credentials for each Team defined in the platform.
- The instance on which the Event Broker is deployed requires connectivity to a CyberArk CCP that has access to the credentials specified in the Event Broker configuration.

> **Note**
>
> This assumes you are using the Event Broker on your platform and that you want to store credentials for the Event Broker in CyberArk.

3. Installing CyberArk

For more information about how to install CyberArk CCP, refer to the CyberArk Provider Implementation Guide.

4. CyberArk Integration Overview

This section presents an overview of the steps to follow to integrate the platform with CyberArk CCP. For each step described, a link is provided to the appropriate section in the document that describes the procedure to follow to complete that step.

The table below describes the integration process in terms of the areas of the platform that need to be integrated with CyberArk. Effectively, showing the mapping that needs to be made between the objects in the platform with the corresponding objects used in CyberArk.

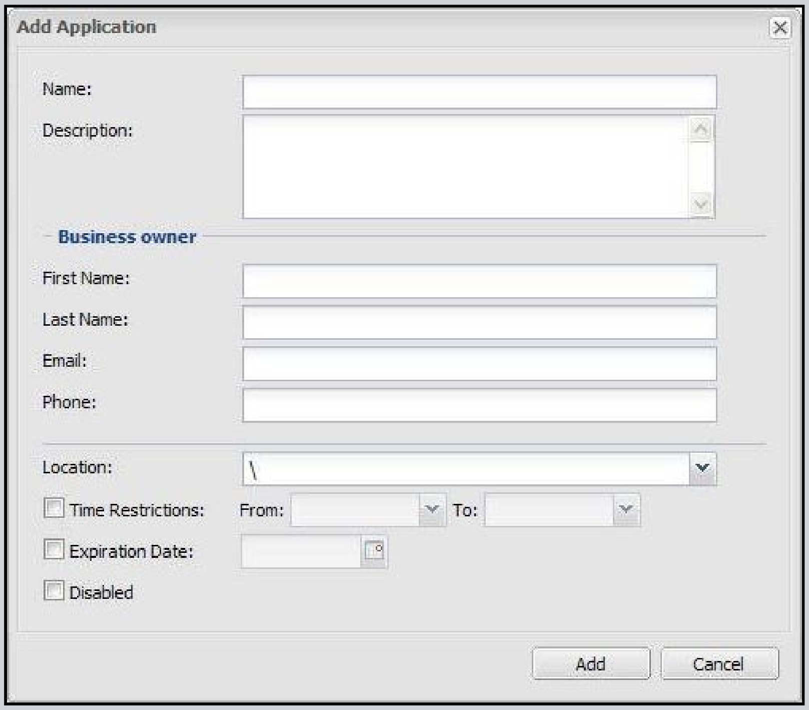
Step	Privitar object	CyberArk object	Description
1	Policy Manager	Application	Create an application in CyberArk for Policy Manager. (This is performed using PVWA.) See, Defining Policy Manager in the Vault.
	Event Broker	Application	Create an application in CyberArk for the Event Broker. (This is performed using PVWA.) See, Defining the Event Broker in the Vault.
	Teams	Application	Create an application in CyberArk for each Team in the platform that accesses a JDBC Token Vault. (This is performed using PVWA.) See, Defining Policy Manager Teams in the Vault
2		Safe	Create a Safe in the Vault for Policy Manager, the Event Broker and a Safe for each Policy Manager Team that uses a JDBC Token Vault. (A different Safe is needed for each Team.). See, Creating Safes in CyberArk.
3		Safe Member	Add the Policy Manager application as a Safe member of the Policy Manager Safe. Add the Event Broker application as a Safe member of the Event Broker Safe. Add each Policy Manager Team application as a Safe member of the Policy Manager Team Safe that uses a JDBC Token Vault. (The application needs to be added to each Safe that has been created.) See, Provisioning Accounts in CyberArk Safes.
4	ConfigDB password	Account	Create an account for the ConfigDB password in the Policy Manager Safe. See, Adding Accounts to CyberArk Safes

Step	Privitar object	CyberArk object	Description
	Token Vault password	Account	Create an account for the Token Vault password in each Safe that has been created for each Policy Manager Team. See, Adding Accounts to CyberArk Safes.

4.1. Defining Policy Manager in the Vault

To authenticate applications and check their access control authorizations in CyberArk CCP the applications must be defined in the CyberArk Password Vault. This section describes how to define Policy Manager as an application in the Password Vault using the CyberArk Password Vault Web Access (PVWA) interface:

1. Log in to the CyberArk Vault as a user with access rights to to manage applications. (The user must have **Manage Users** authorization.)
2. Click **Add Application**, in the **Applications** tab. The **Add Application** window is displayed:



Enter the following information:

- In the **Name** field, specify the unique name (ID) for the Policy Manager application. This name must match the name that is defined in the Policy Manager application property:

  `agrotera.cyberark.application_id`

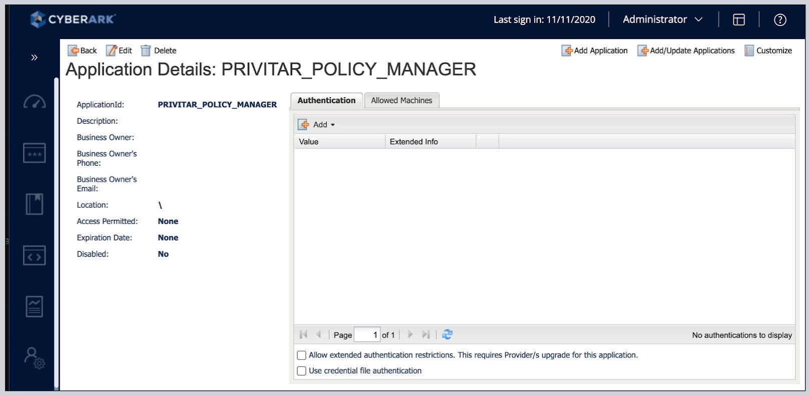
  For more information, see CyberArk Application Properties.
- In the **Description** field, add a short description of the application.
- In the **Business owner** section, specify the contact information for the application's business owner.

- In the **Location** field, specify the location of the application in the Vault hierarchy. (If a location is not specified, the application will be added in the same location as the user who is creating the application.)

The remaining options do not need to be completed. For reference, they are described in the following table:

Option	Description
Time Restrictions	Time restrictions for secret retrieval.
Expiration Date	An expiration date for the application.
Disabled	If selected, the application is disabled.

3. Click **Add**. Policy Manager is added an an application to the Vault and displayed in the **Application Details** page:



Application Details: PRIVITAR_POLICY_MANAGER

ApplicationId: PRIVITAR_POLICY_MANAGER
Description:
Business Owner:
Business Owner's Phone:
Business Owner's Email:
Location: \
Access Permitted: None
Expiration Date: None
Disabled: No

No authentications to display

□ Allow extended authentication restrictions. This requires Provider/s upgrade for this application.
□ Use credential file authentication

4. Select the **Authentication** tab from the **Application Details** page.
5. Check the **Allowing extended authentication restrictions** box.

   This setting enables an unlimited number of machines and Windows domain OS users to be specified for a single application.

6. In the **Authentication** tab, click **Add**. A list box is displayed containing a list of authentication characteristics that can be added for an application.

   These characteristics can be used by the CyberArk CCP to check the application before retrieving the application password.

7. Select **Certificate Serial Number** from the list box. The **Add Certificate Serial Number Authentication** dialog box is displayed.
8. Enter the Certificate Serial Number in the **SN** field.

   The serial number that is entered must match the client certificate serial number that is defined in the application property:

   ```
   agrotera.cyberark.certificate.path
   ```

   For more information, see CyberArk Application Properties.

9. Click **Add** to save the details.

4.2. Defining the Event Broker in the Vault

If the Event Broker is running on your platform and you want to use CyberArk CCP to store the credentials for this application, then you need to add the Event Broker as an application to the CyberArk Password Vault.

The procedure to follow is exactly the same procedure as outlined for adding Policy Manager to the CyberArk Password Vault. (See, Defining Policy Manager in the Vault.)

The only differences are that you would add the following application property definitions that have been configured in the Event Broker `application.properties` file:

- `agrotera.cyberark.application_id`
- `agrotera.cyberark.certificate.path`

For more information about the application properties, see CyberArk Application Properties.

4.3. Defining Policy Manager Teams in the Vault

This section describes how to define Policy Manager Teams in the CyberArk Password Vault and add authentication details for the Teams, using the CyberArk Password Vault Web Access (PVWA) interface.

Requests that are made to CyberArk are made using the **application id** that is specified by the following property in the platform `application.properties` file. (This file is used to configure many areas of Policy Manager):

```
agrotera.cyberark.application_id
```

For more information, see CyberArk Application Properties.

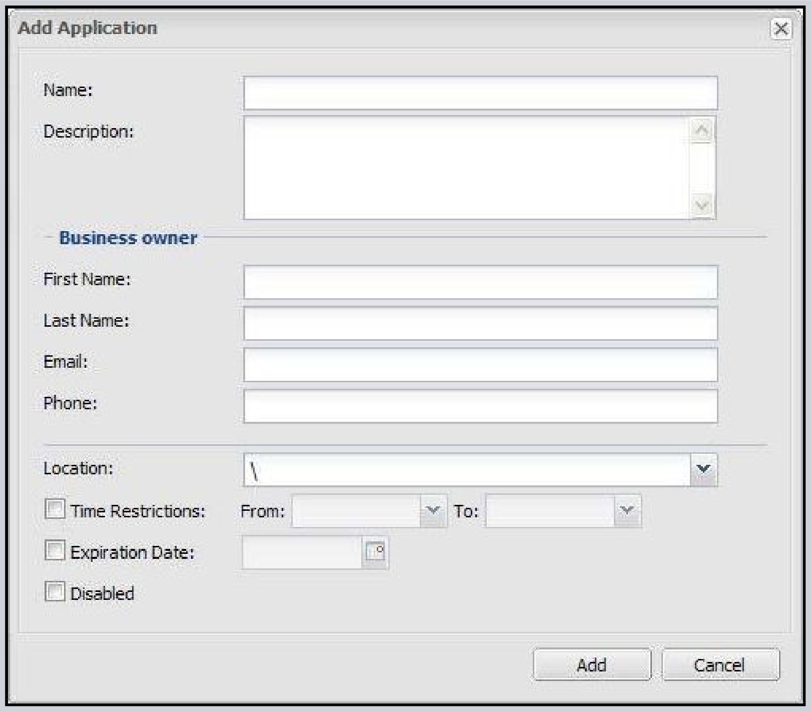
However, the platform mandates that when using a JDBC Token Vault with CyberArk, all JDBC credentials must be stored, managed and retrieved from CyberArk. This means that when making requests to CyberArk to retrieve JDBC Token Vault credentials, a team-specific application id (**Team ID**) is required. Any Teams in the platform that need to retrieve these credentials will need to be defined in the Password Vault. This enables access to secrets to be restricted between different Teams.

For more information about Teams and how to obtain the **Team ID** for a Team, see the *Privitar User Guide*.

For more information about configuring the platform to store JDBC credentials in CyberArk, see Configuring JDBC Token Vault credentials.

To add a Privitar Team to the Password Vault:

1. Log in to the CyberArk Vault as a user with access rights to to manage applications. (The user must have **Manage Users** authorization.)
2. Click **Add Application**, in the **Applications** tab. The **Add Application** window is displayed:



Enter the following information:

- In the **Name** field, specify the Team id defined in the application. This name must be defined using the format that is defined in the platform application property:

  ```
  agrotera.cyberark.application_id.team_format
  ```

  By default, the format is specified as:

  ```
  {globalAppId}_Team_{teamId}
  ```

  For example, if the `globalAppId` for the platform application is `POLICY_MANAGER` and the `teamID` for the Team is `12345`, then the definition to add to the Password Vault would be:

  ```
  POLICY_MANAGER_Team_12345
  ```

  For more information, see CyberArk Application Properties.
- In the **Description** field, specify a short description of the platform application that will help you identify it.
- In the **Business owner** section, specify the contact information for the platform application's business owner.
- In the **Location** field, specify the location of the platform application in the Vault hierarchy. (If a location is not specified, the application will be added in the same location as the user who is creating this application.)

3. Click **Add**. The Team details are added to the Vault and displayed in the **Application Details** page.
4. Select the **Authentication** tab from the **Application Details** page.
5. Check the **Allowing extended authentication restrictions** box.

   This setting enables an unlimited number of machines and Windows domain OS users to be specified for a single application.
6. In the **Authentication** tab, click **Add**. A list box is displayed containing a list of authentication characteristics that can be added for an application.

These characteristics can be used by the CyberArk CCP to check the application before retrieving the application password.

7. Select **Certificate Serial Number** from the list box. The **Add Certificate Serial Number Authentication** dialog box is displayed.
8. Enter the Certificate Serial Number in the **SN** field.

   The serial number that is entered must match the client certificate serial number that is defined in the application property:

   ```
   agrotera.cyberark.certificate.path
   ```

   For more information, see CyberArk Application Properties.
9. Click **Add** to save the details.

4.4. Creating Safes in CyberArk

This section describes the Safes that need to be created in CyberArk for use with the platform.

CyberArk grants permissions to applications (such as Policy Manager, Event Broker, Teams in Policy Manager) to access Accounts that are stored in Safes by making the application a **Safe Member** of that Safe.

Typically, you might configure the following Safes in the CyberArk Password Vault as follows:

- A Safe containing accounts used by Policy Manager.
- A Safe containing accounts used by the Event Broker (if installed).
- A Safe for each Policy Manager Team that uses a JDBC Token Vault.

> **Note**
>
> It might be that you are using a completely different Vault setup in CyberArk CCP to manage users and applications, but the overall process to follow will be the same

For more information about creating and managing Safes in CyberArk, see Adding Safes in the CyberArk Password Vault.

4.5. Provisioning Accounts in CyberArk Safes

This section describes how to add applications and provider users as Safe Members of a Safe.

CyberArk grants permissions to applications (such as Policy Manager, Event Broker, Teams in Policy Manager) to access Accounts that are stored in Safes by making the application a **Safe Member** of that Safe.

For each Safe you have created, you need to provision the privileged accounts that will be required to access that Safe. You can do this in either 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 require the **Add accounts** authorization in the Password Safe.)

Once the accounts are managed by CyberArk, you need to set up access to the accounts for:

- Each of the **Privitar Applications**.
- CyberArk Application Password **Provider users** serving the platform applications.

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

If the Safe is configured for object level access, make sure that both the provider user and the application have access to the password(s) to retrieve.

4.5.1. Adding the application

Each platform application needs to be added as a member to the Safe it uses, with the following authorization:

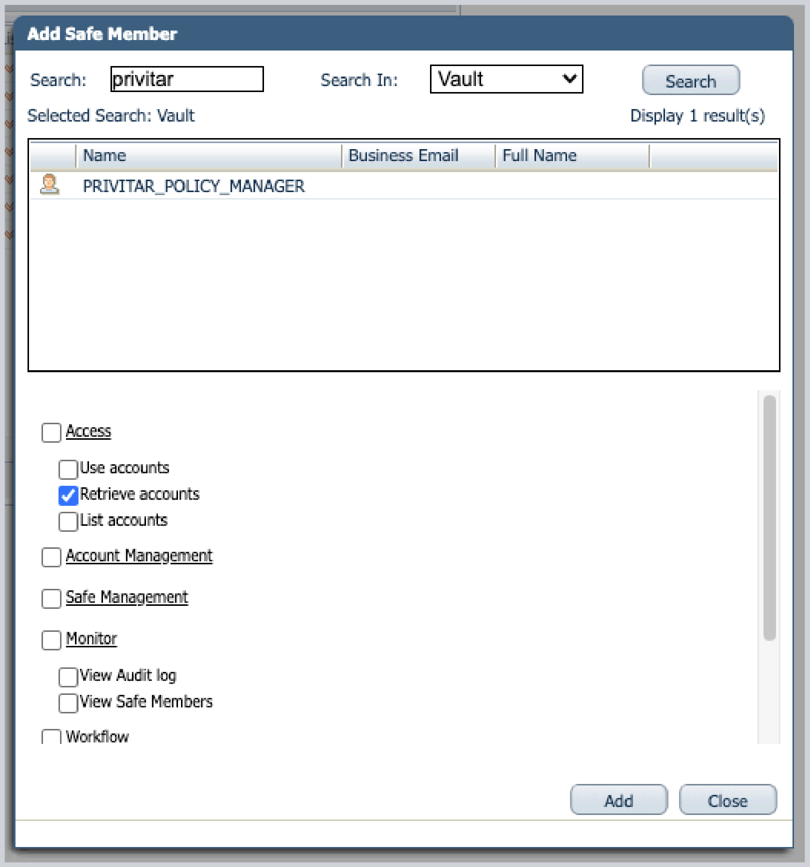
- **Retrieve accounts**

The name to be added for the application is shown in the following table:

Safe	Name
Policy Manager	The Application ID that is defined in the application properties file for Policy Manager: `agrotera.cyberark.application_id` For example, `POLICY_MANAGER`
Event Broker	The Application ID that is defined in the application properties file for the Event Broker: `agrotera.cyberark.application_id` For example, `EVENT_BROKER`
JDBC Token Vault	The descriptor that is defined in the the application properties file for each Team in Policy Manager that uses a JDBC Token Vault: `agrotera.cyberark.application_id.team_format` For example, `POLICY_MANAGER_Team_12345` For more information, see Defining Policy Manager Teams in the Vault.

For more information, refer to CyberArk Application Properties.

For example, the following **Add Safe Member** dialog box shows the authorization settings that need to be applied for a Policy Manager with the Application ID set to **PRIVITAR_POLICY_MANAGER**:



Add Safe Member

Search: privitar Search In: Vault

Selected Search: Vault Display 1 result(s)

Name	Business Email	Full Name
PRIVITAR_POLICY_MANAGER		

□ Access

□ Use accounts

☑ Retrieve accounts

□ List accounts

□ Account Management

□ Safe Management

□ Monitor

□ View Audit log

□ View Safe Members

□ Workflow

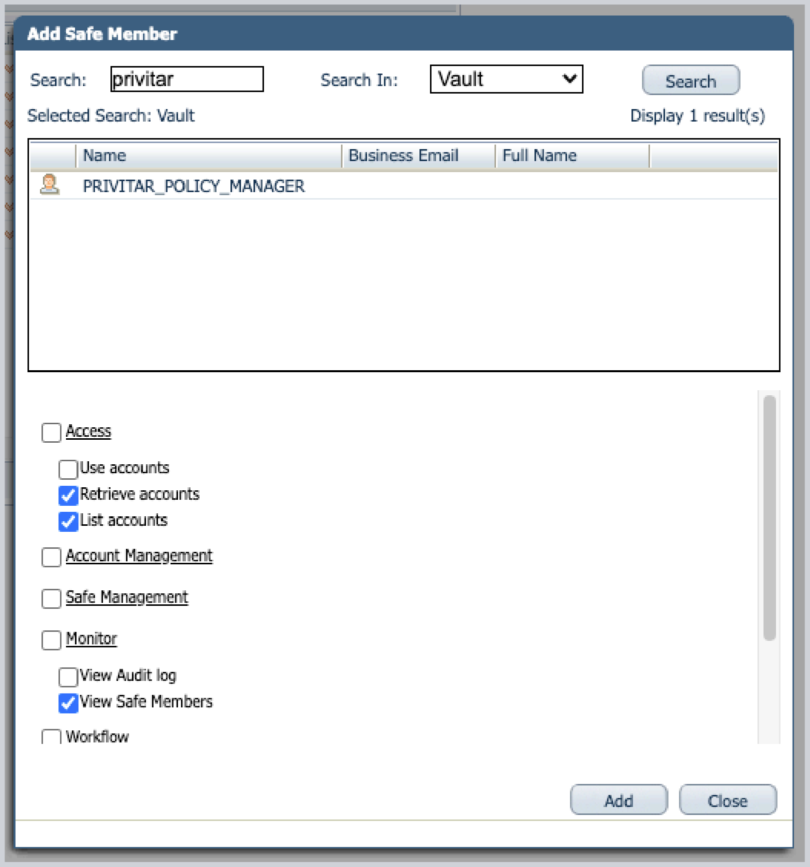
4.5.2. Adding Provider users

Provider users need to be added as Safe Members with the following authorizations:

- **List accounts**
- **Retrieve accounts**
- **View Safe Members**

If you are installing multiple providers, it is recommended that the users are created as a group. The users can then be added to the Safe as a single group, rather than creating separate entries for each user.

The following **Add Safe Member** dialog box shows the authorization settings that need to be applied for Provider users:



Add Safe Member

Search: privitar Search In: Vault Search

Selected Search: Vault Display 1 result(s)

Name	Business Email	Full Name
PRIVITAR_POLICY_MANAGER		

- □ Access
  - □ Use accounts
  - ☑ Retrieve accounts
  - ☑ List accounts
- □ Account Management
- □ Safe Management
- □ Monitor
  - □ View Audit log
  - ☑ View Safe Members
- □ Workflow

For more information about adding and managing privileged accounts, refer to the CyberArk Privileged Access Security Implementation Guide.

4.6. Adding Accounts to CyberArk Safes

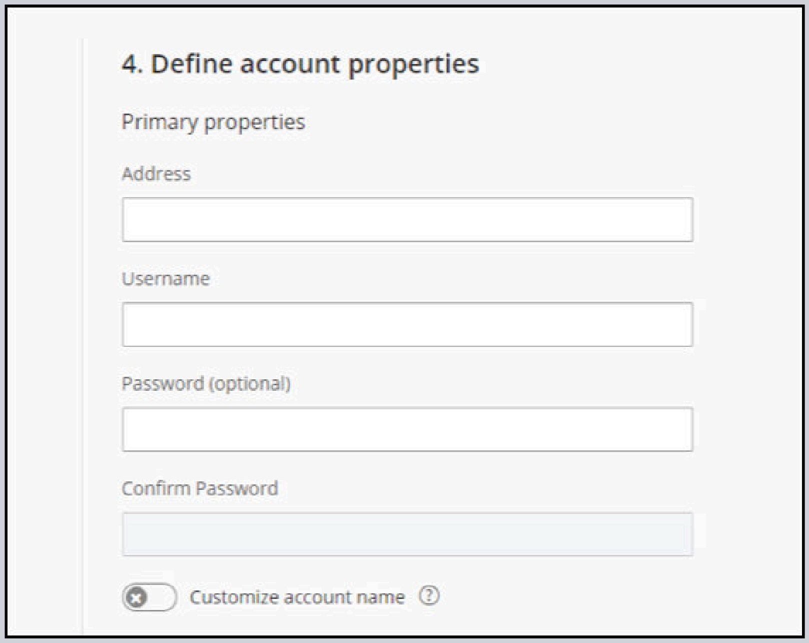
This section describes how to add accounts to the CyberArk Safes that have been created for use by platform applications.

The two accounts that would typically be added to a CyberArk Safe would be:

- An account to store ConfigDB credentials. This would be added to the Policy Manager Safe.
- An account to store Token Vault credentials. This would be added to each Safe that has been created for Policy Manager Teams to access a JDBC Token Vault.

For general information about how to add accounts in CyberArk, see CyberArk Account Management Guide.

The following dialog box shows the details that need to be added for an account that is added to a CyberArk Safe:



4. Define account properties

Primary properties

Address

Username

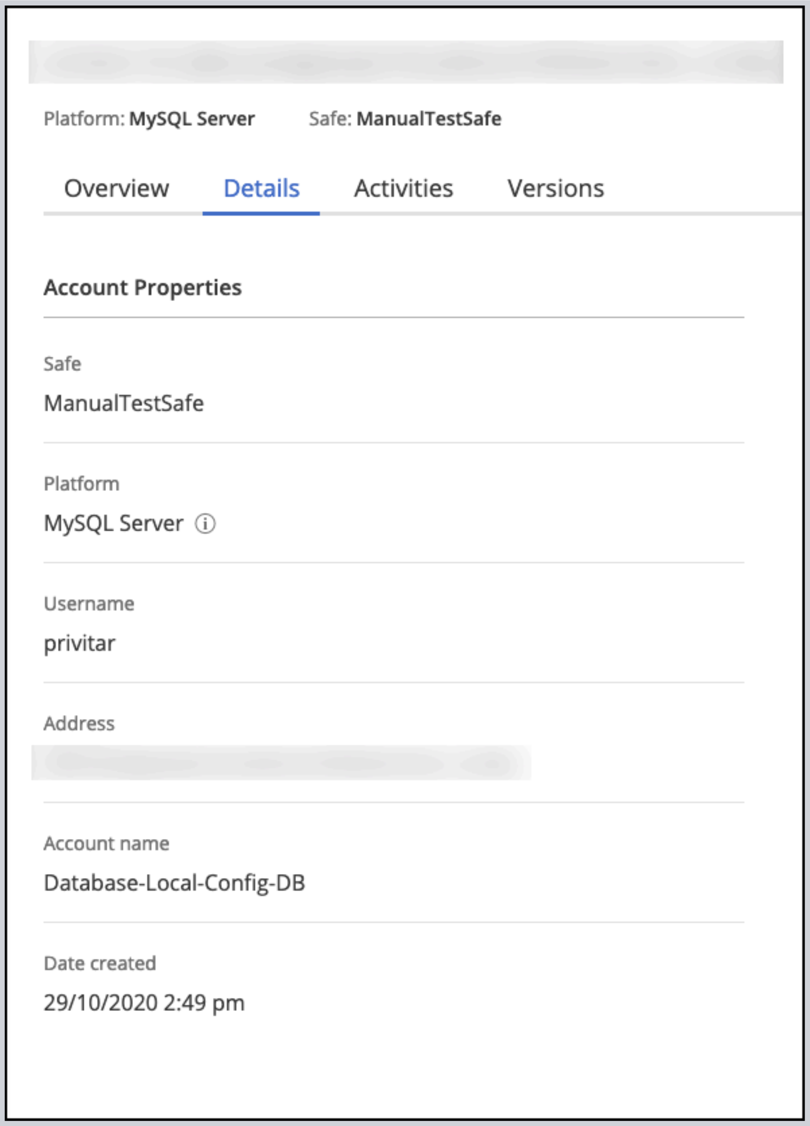
Password (optional)

Confirm Password

Note

When adding the account, select the **Customize account name** button so that you can specify the name of the account that is created in CyberArk.

The following dialog box shows the details of an account that has been added to CyberArk:



[redacted]

Platform: **MySQL Server** Safe: **ManualTestSafe**

Account Properties

Safe
ManualTestSafe

Platform
MySQL Server ⓘ

Username
privitar

Address
[redacted]

Account name
Database-Local-Config-DB

Date created
29/10/2020 2:49 pm

The **Account name** is used when defining the account in the `application.properties` file to retrieve the credentials from CyberArk.

For example, the following entry would be used to define the above account in the platform:

```
agrotera.database_password.secret_descriptor=Safe=ManualTestSafe;Object=Datab
ase-Local-Config-DB
```

For more information, see CyberArk Descriptor Format.

5. Configuring Privacy Platform to use CyberArk

There are three areas of the platform that need to be configured when CyberArk CCP is used as the external secrets provider for the platform:

- Settings for CyberArk in the `application.properties` configuration file for Policy Manager and the Event Broker (if installed). See, Configuring application properties for CyberArk.
- JDBC Token Vault credentials (URL, username and password). (This is only required if you are using a JDBC Token Vault.) See, Configuring JDBC Token Vault credentials.
- Additional settings in the `application.properties` file that you want to be manged by CyberArk CCP. For example, the ConfigDB password. See, CyberArk Descriptor Format.

5.1. Configuring application properties for CyberArk

To configure CyberArk Central Credential Provider (CCP) as the external secrets provider for the platform, use the following application properties.

To enable CyberArk :

- `agrotera.secret_provider` must be set to `CYBERARK_CCP`

The following properties **must** also be specified:

- `agrotera.cyberark.provider_url`
- `agrotera.cyberark.application_id`

The following properties are **optional**:

- `agrotera.cyberark.application_id.team_format`
- `agrotera.cyberark.certificate.authority`
- `agrotera.cyberark.certificate.path`
- `agrotera.cyberark.certificate.secret`

  This property must be specified if the `agrotera.cyberark.certificate.path` property is specified.

5.1.1. CyberArk Application Properties

This section lists the application properties in Privitar that are used to configure the CyberArk Central Credential Provider (CCP).

Name	Description
agrotera.secret_provider	The name of a credentials provider that manages usernames and passwords. This can be set to `INTERNAL` or `CYBERARK_CCP`. (This is set to `INTERNAL` if not specified.)

Name	Description
agrotera.cyberark.provider_url	The base URL of the CyberArk Central Credential Provider. For example: `https://<host name>:<port>/AIMWebService` (This name is only required if `agrotera.secret_provider` is set to `CYBERARK_CCP`.)
agrotera.cyberark.application_id	The global application id that identifies the Privitar component created in CyberArk. This id is used when making requests to CyberArk CCP. Note that application IDs containing + or & are *not* supported. (This name is only required if `agrotera.secret_provider` is set to `CYBERARK_CCP`.)
agrotera.cyberark.certificate.path	The absolute path to the client certificate for communication with CyberArk CCP. The certificate file must be a PKCS #12 file. The filename extension for PKCS #12 files is `.p12` or `.pfx`. (This name is only required if `agrotera.secret_provider` is set to `CYBERARK_CCP`.)
agrotera.cyberark.certificate.secret	The password (secret) for the client certificate to be authenticated against. This must be specified if the `agrotera.cyberark.certificate.path` property is specified. (This name is only required if `agrotera.secret_provider` is set to `CYBERARK_CCP`.)
agrotera.cyberark.certificate.authority	The absolute path to the trusted certificate used to establish a secure connection to CyberArk CCP. (This name is only required if `agrotera.secret_provider` is set to `CYBERARK_CCP`.)

Name	Description
agrotera.cyberark.application_id.team_format	The format to be used when defining a specific Team in Privitar to make requests to CyberArk CCP. The default setting is: `{globalAppId}_Team_{teamId}` where: • `{globalAppId}` corresponds to the setting defined in:`agrotera.cyberark.application_id` • `{teamId}` is the Team Id for a Team in Privitar. A Team in Privitar that requires access to a JDBC Token Vault would need to be defined in the CyberArk Password Vault using this format. For more information, see Defining Policy Manager Teams in the Vault. (This name is only required if `agrotera.secret_provider` is set to CYBERARK_CCP.)

5.2. Configuring JDBC Token Vault credentials

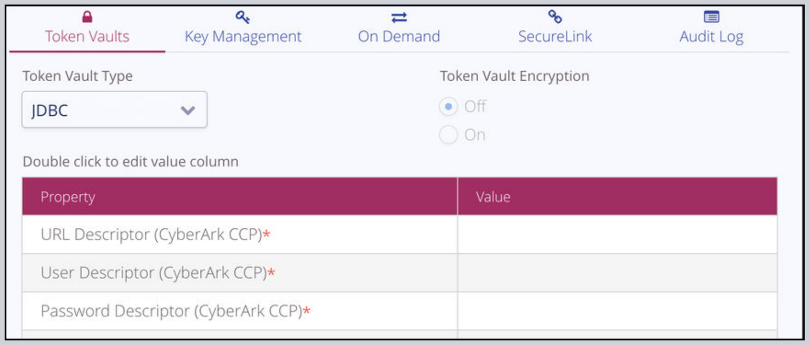
If you are using a JDBC Token Vault with CyberArk, the platform mandates that all JDBC credentials are stored, managed and retrieved from CyberArk.

This means that instead of providing the URL, user and password as part of the token vault configuration during the setup of a platform Environment, you need to provide the relevant descriptor queries that can be used to retrieve the values from CyberArk CCP.

The Descriptor values required are:

- **URL Descriptor (CyberArk CCP)**
- **User Descriptor (CyberArk CCP)**
- **Password Descriptor (CyberArk CCP)**

In the platform (using CyberArk CCP), these values are defined in the **Token Vaults** tab, when the **Token Vault Type** list box is set to **JDBC**:



Token Vault Type

JDBC

Token Vault Encryption

● Off
○ On

Double click to edit value column

Property	Value
URL Descriptor (CyberArk CCP)*	
User Descriptor (CyberArk CCP)*	
Password Descriptor (CyberArk CCP)*	

For more information about the descriptor format that can be used to define these values, see CyberArk Descriptor Format.

5.3. CyberArk Descriptor Format

In order to use CyberArk to manage settings for other application properties, you can add a suffix to the given property and put the CyberArk CCP query as its value.

The suffix to use is:

```
.secret_descriptor
```

The format to use for the descriptor is:

```
Safe=<safe name>;Folder=<folder name>;Object=<object name>##<attribute>
```

The following table defines each part of the format:

Item	Description
`safe name`	The name of the safe that stores the credentials. (This item is optional, but recommended for increased lookup performance.)
`folder name`	The folder containing the credentials. (This item is optional. The default is *Root* (/).)
`object name`	The name of the secret (password) object to retrieve. (This is the **Account name** entry for the account that has been setup in CyberArk.)
`attribute`	The name of the value to be retrieved, or placeholder for multiple values with the use of double brackets `{{name of value}}` to surround the name of each value. (This item is optional. The default is `Content`, which will return the password. `UserName` would return the user name credentials.)

For example, to specify an object without specifying a `folder name`, use:

```
Safe=Privitar;Object=PM-config-db##UserName
```

In the following example, the `attribute` is not specified. This means that the default `Content` will be retrieved:

```
Safe=Privitar;Folder=Test-Env;Object=PM-config-db
```

For example, if you want to configure the platform to retrieve the configuration database (`ConfigDB`) password from CyberArk CCP instead of storing the password in plain text in the application properties file, you can specify:

```
agrotera.database_password.secret_descriptor=Safe=Privitar;Object=PM-config-
db
```

This entry specifies that the password will be retrieved from the `PM-config-db account` in the `Privitar` safe in the CyberArk CCP.

You can also specify the other attributes for the same account. For example, the username (`UserName`) and URL (`Address`) of the user can be specified as:

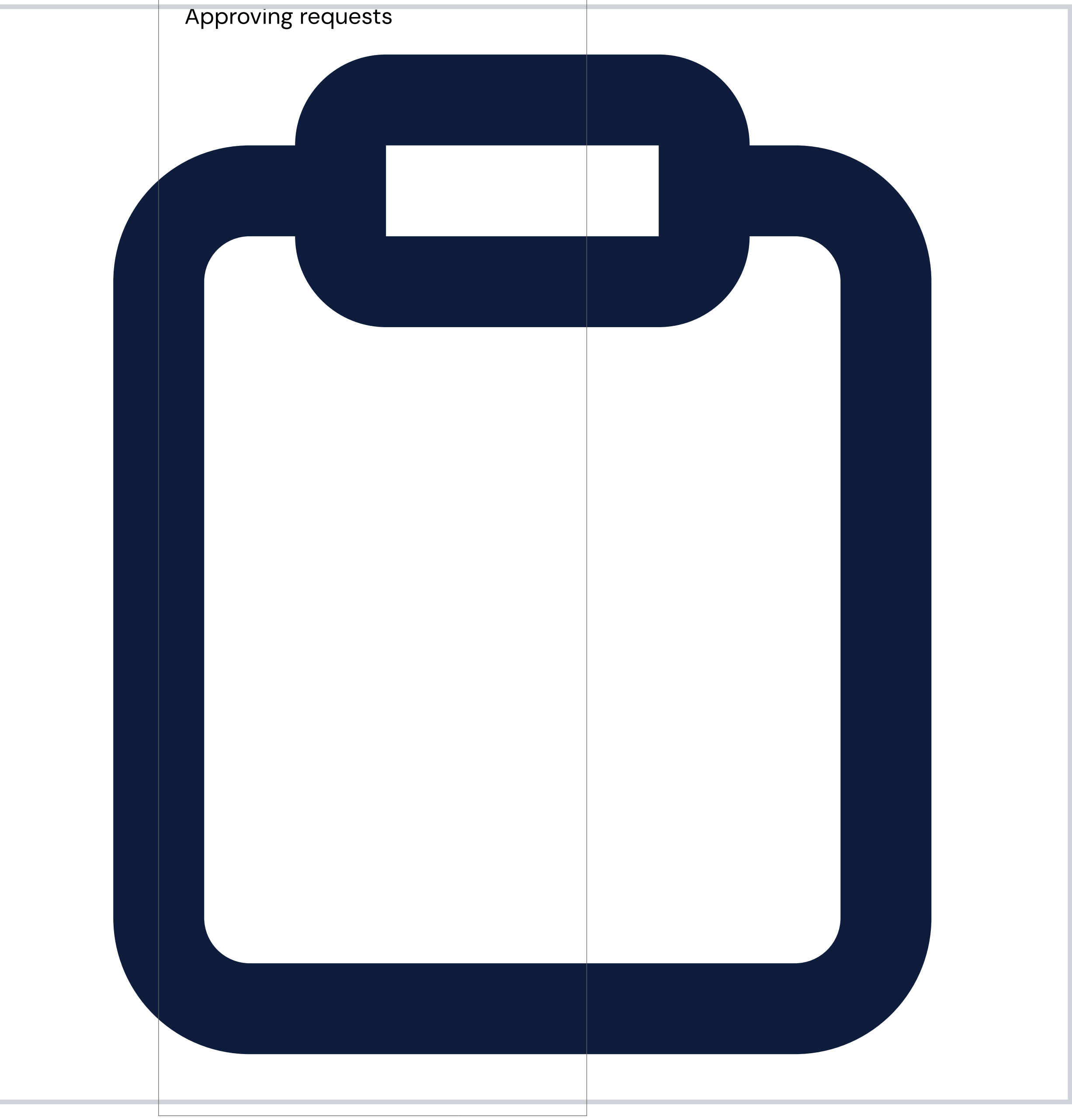
```
agrotera.database_user.secret_descriptor=Safe=Privitar;Object=PM-config-
db##UserName
agrotera.database_url.secret_descriptor=Safe=Privitar;Object=PM-config-
db##Address
```

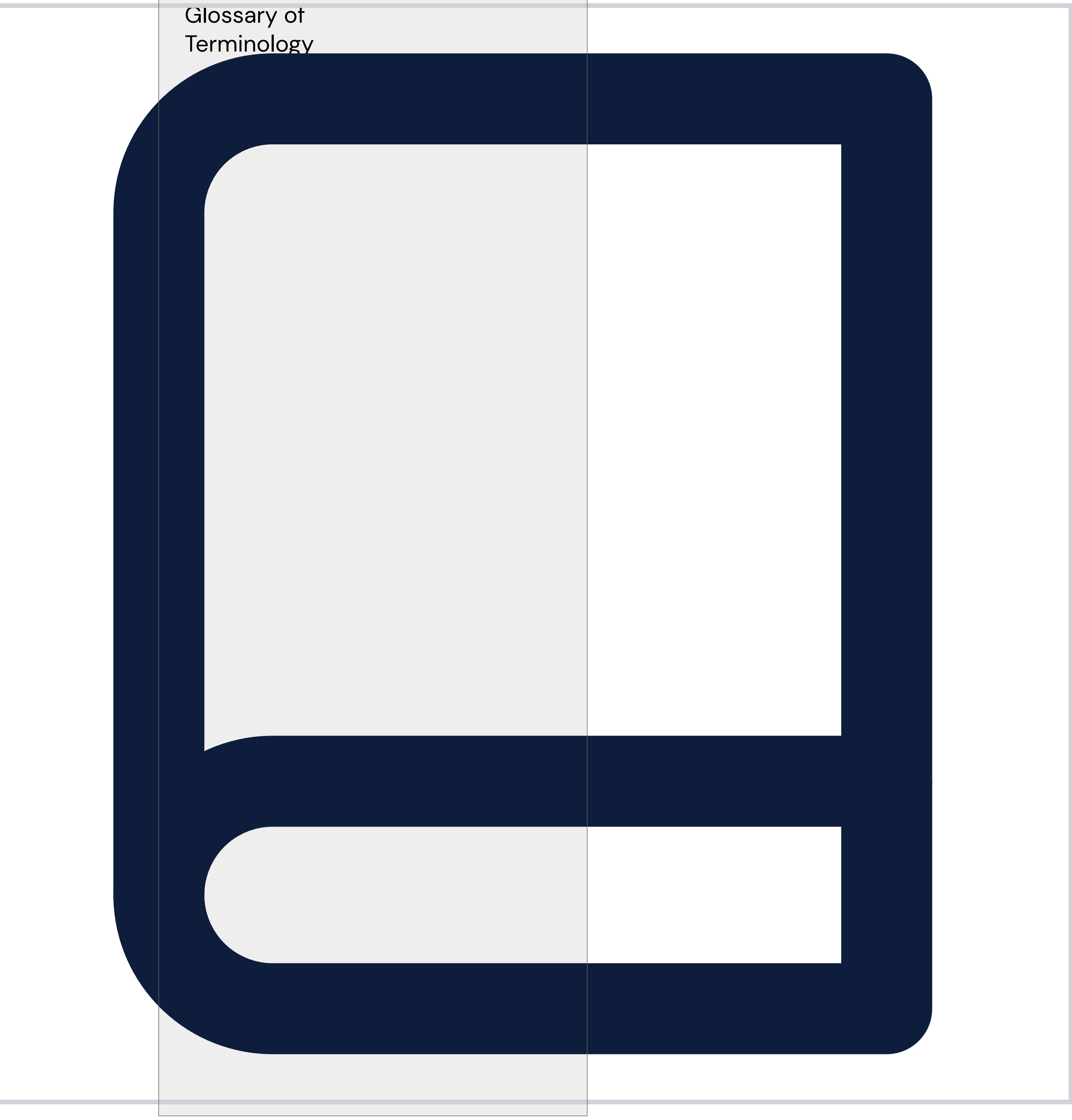
To construct a connection string for the application property `agrotera.database_url`, multiple values (`Address` , `Port` and `Database`) from the `PM-config-db` account can be incorporated using `{{}}` as given in the example below:

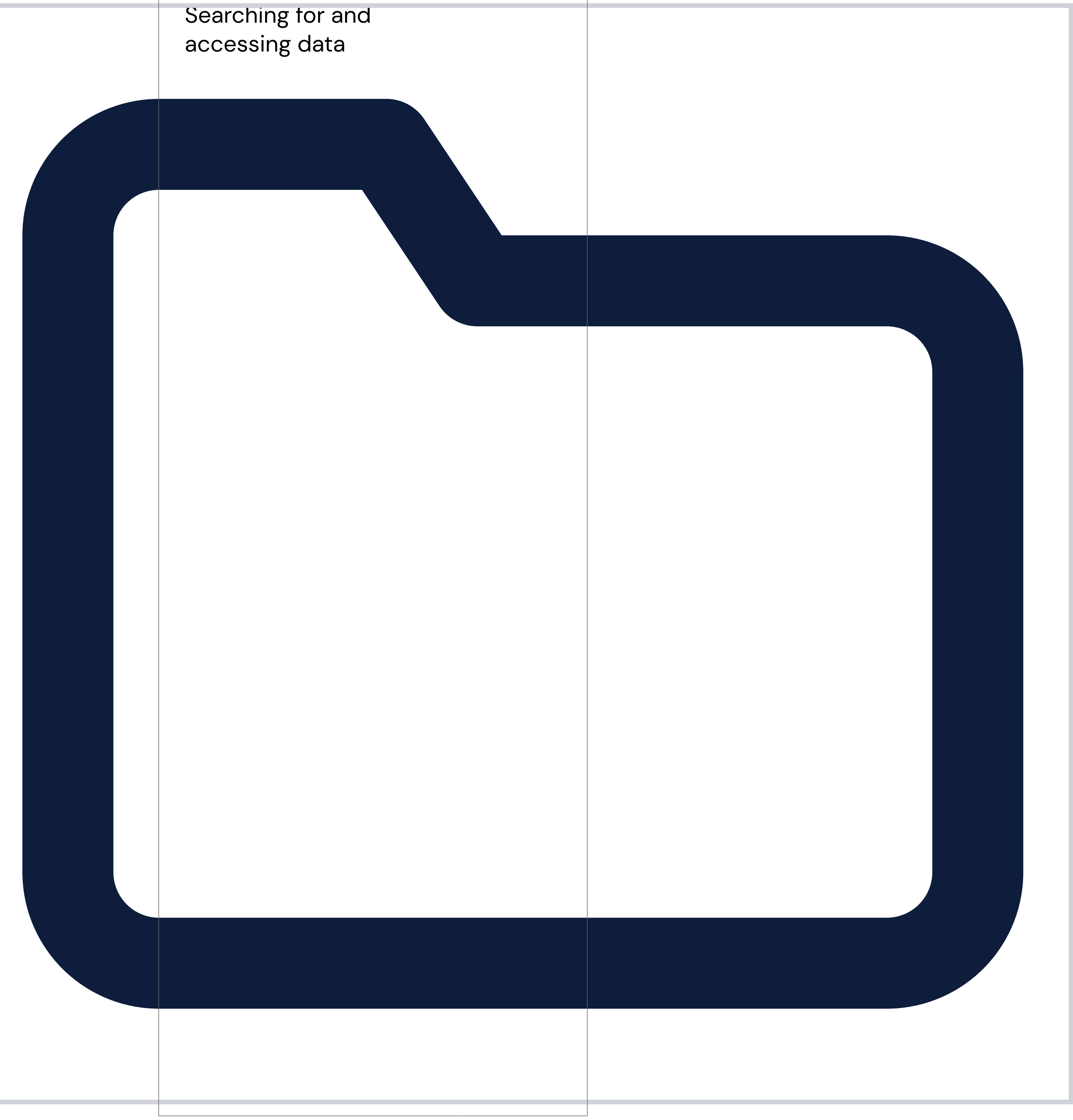
```
agrotera.database_url.secret_descriptor=Safe=Privitar;Object=PM-config-
db##jdbc:postgresql://{{Address}}:{{Port}}/{{Database}}
```

For more information about how credentials can be retrieved using the CyberArk CCP API, see the CyberArk Web Service REST API.

Icons for Portal Landing Page (not included in TOC)

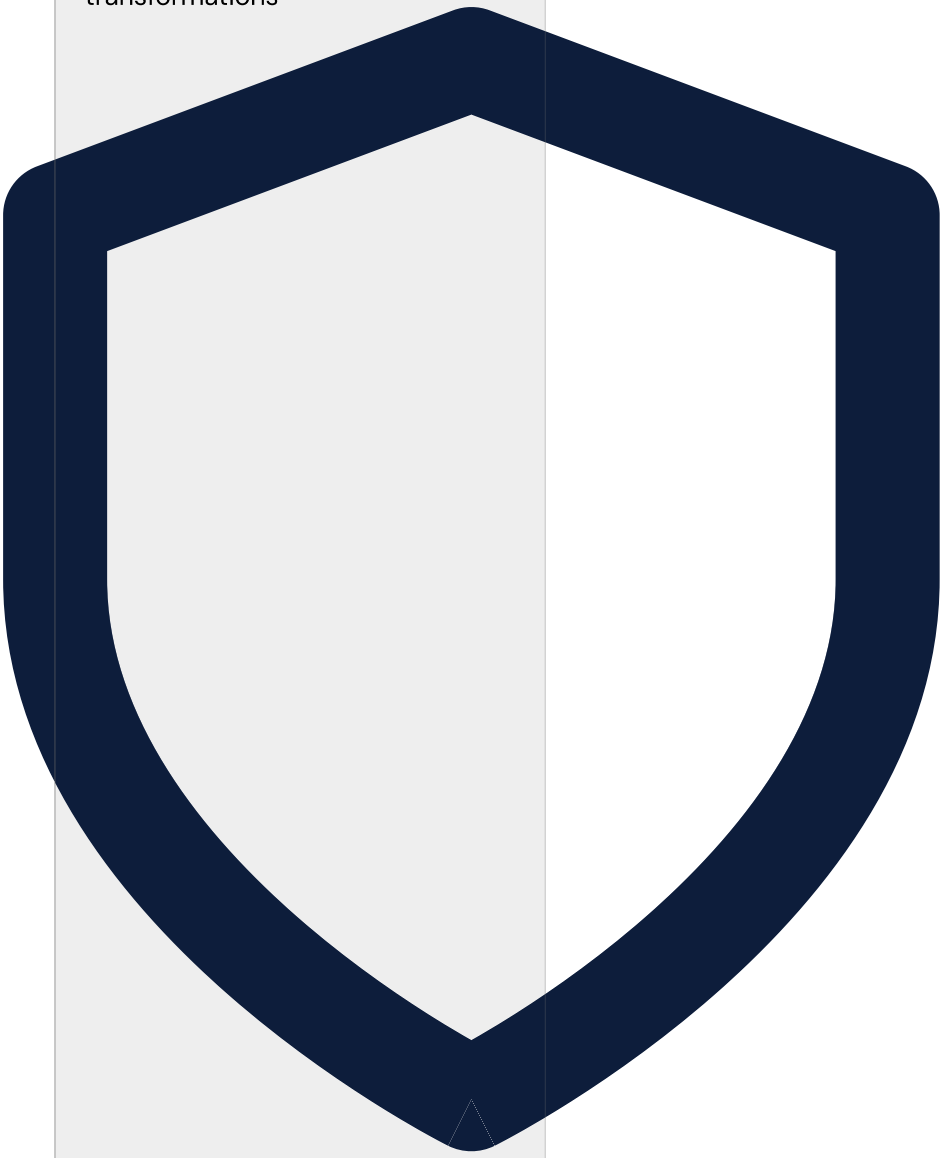
Description	Icon (76px)
Approving requests	

Description	Icon (76px)
Glossary of Terminology	

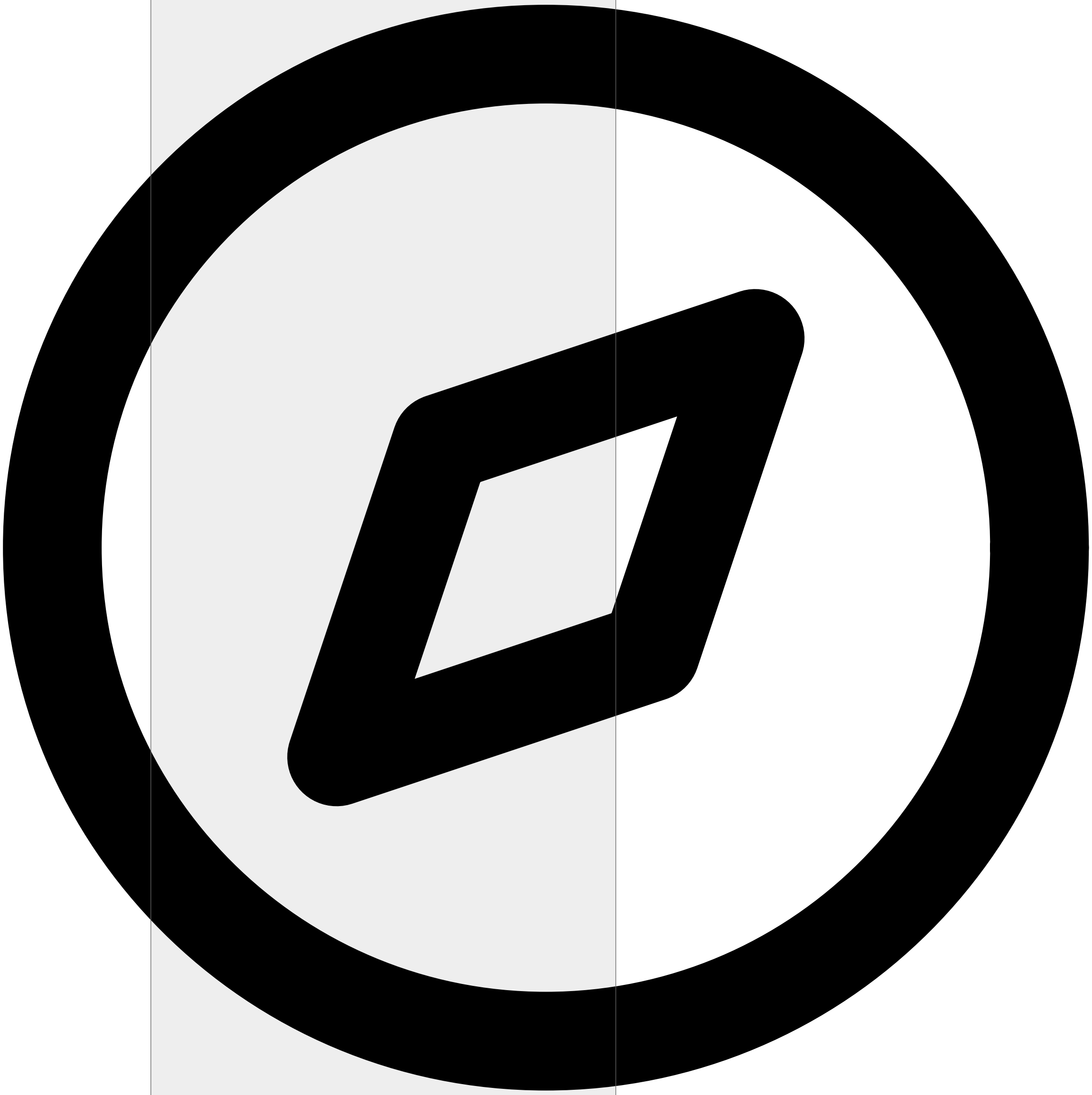
Description	Icon (76px)
Searching for and accessing data	

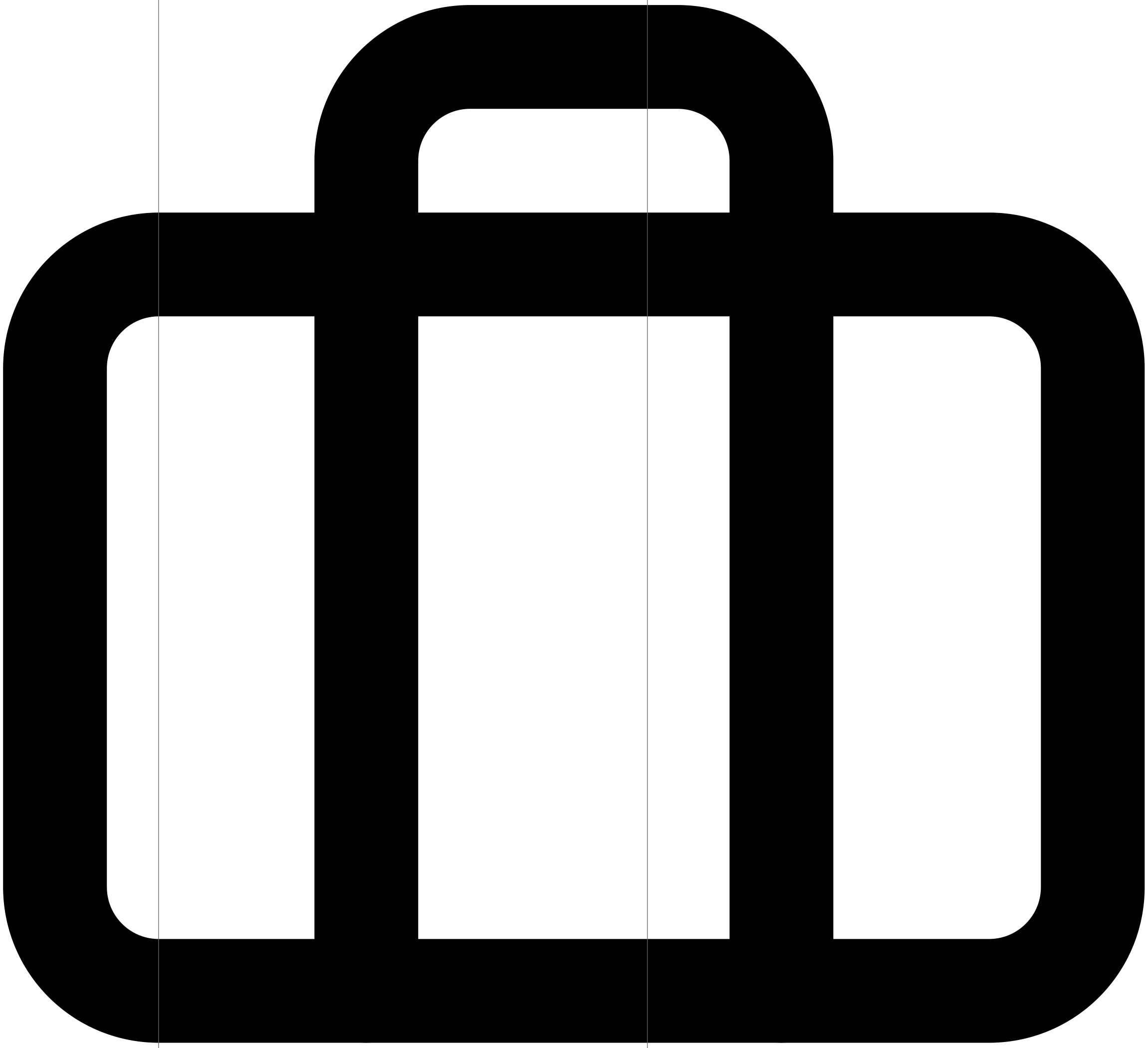
Description	Icon (76px)
Adding data	

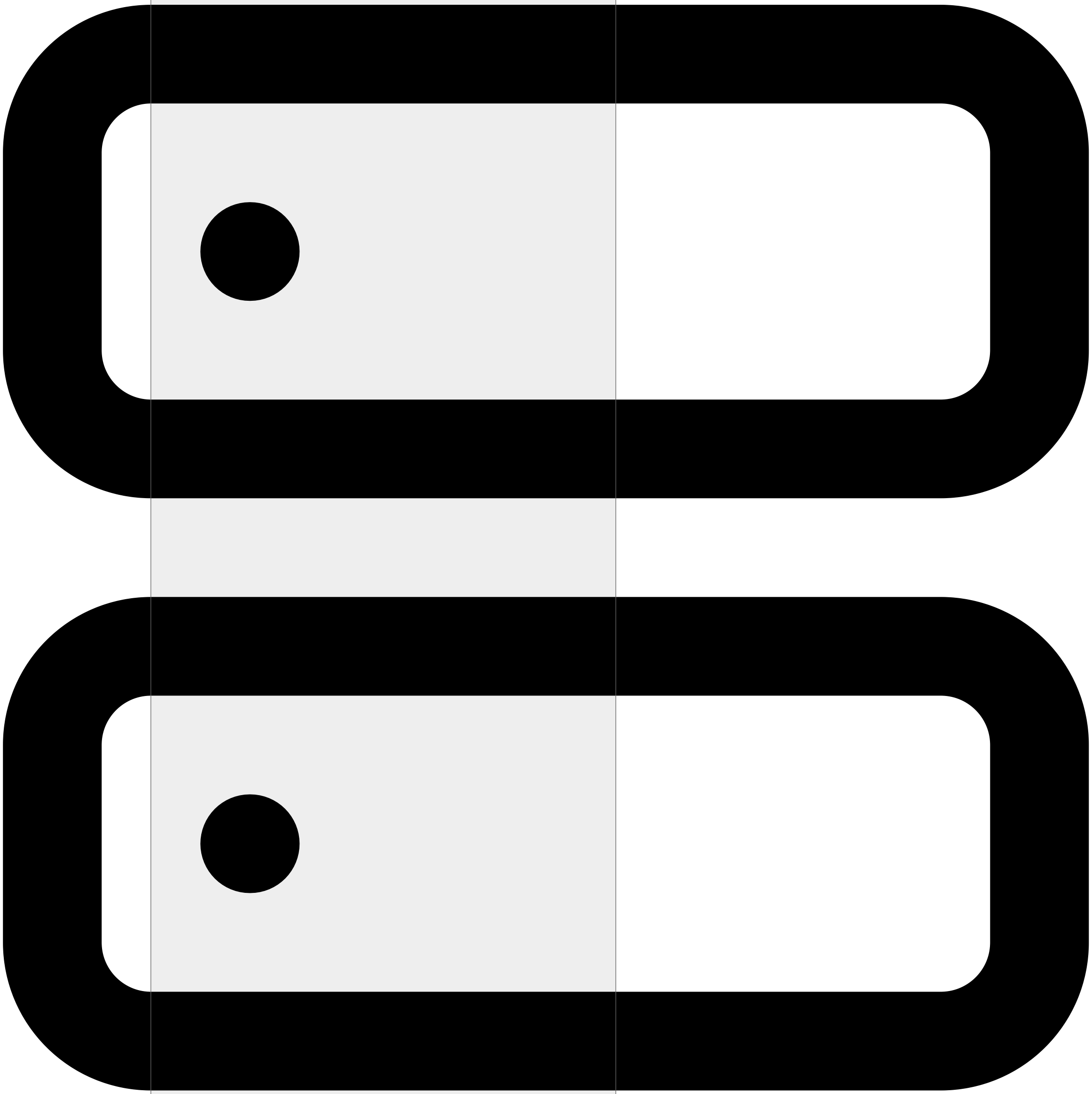
Description	Icon (76px)
Welcome	🏠

Description	Icon (76px)
Policies, rules & transformations	

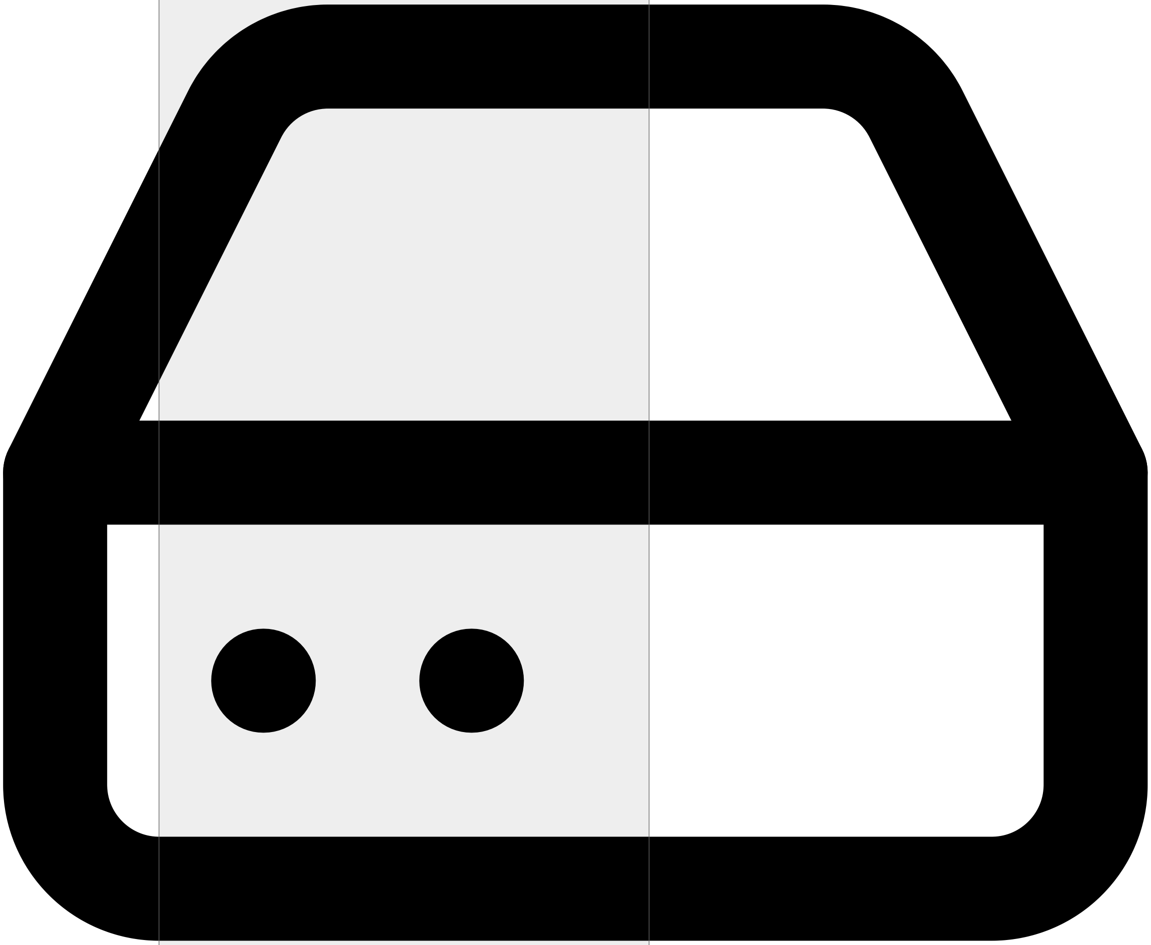
Description	Icon (76px)
Business Information	🏷

Description	Icon (76px)
Architecture	

Description	Icon (76px)
Enterprise	

Description	Icon (76px)
Exchange	

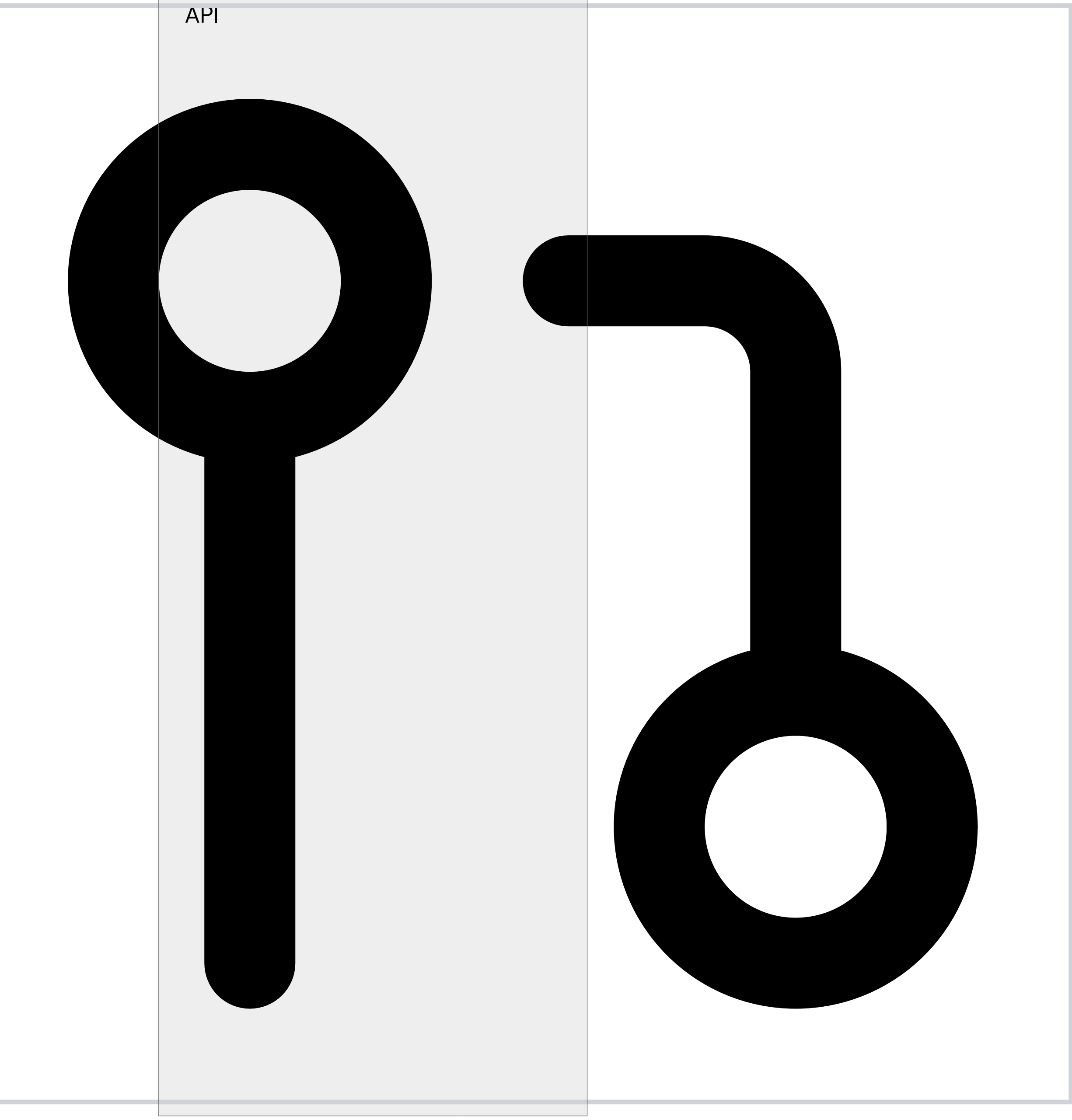
Description	Icon (76px)
Third-Party Licensing	💳

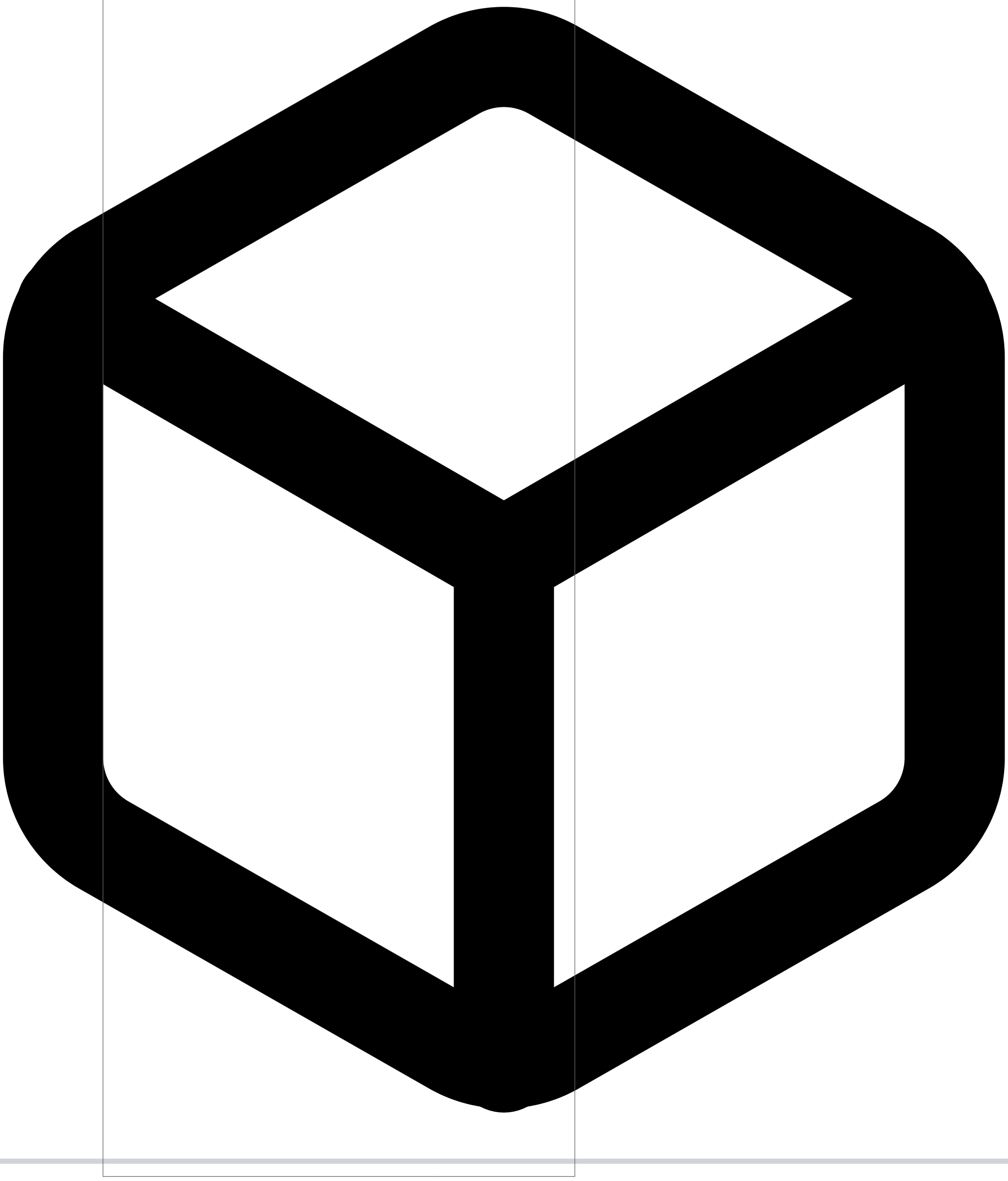
Description	Icon (76px)
Backup	

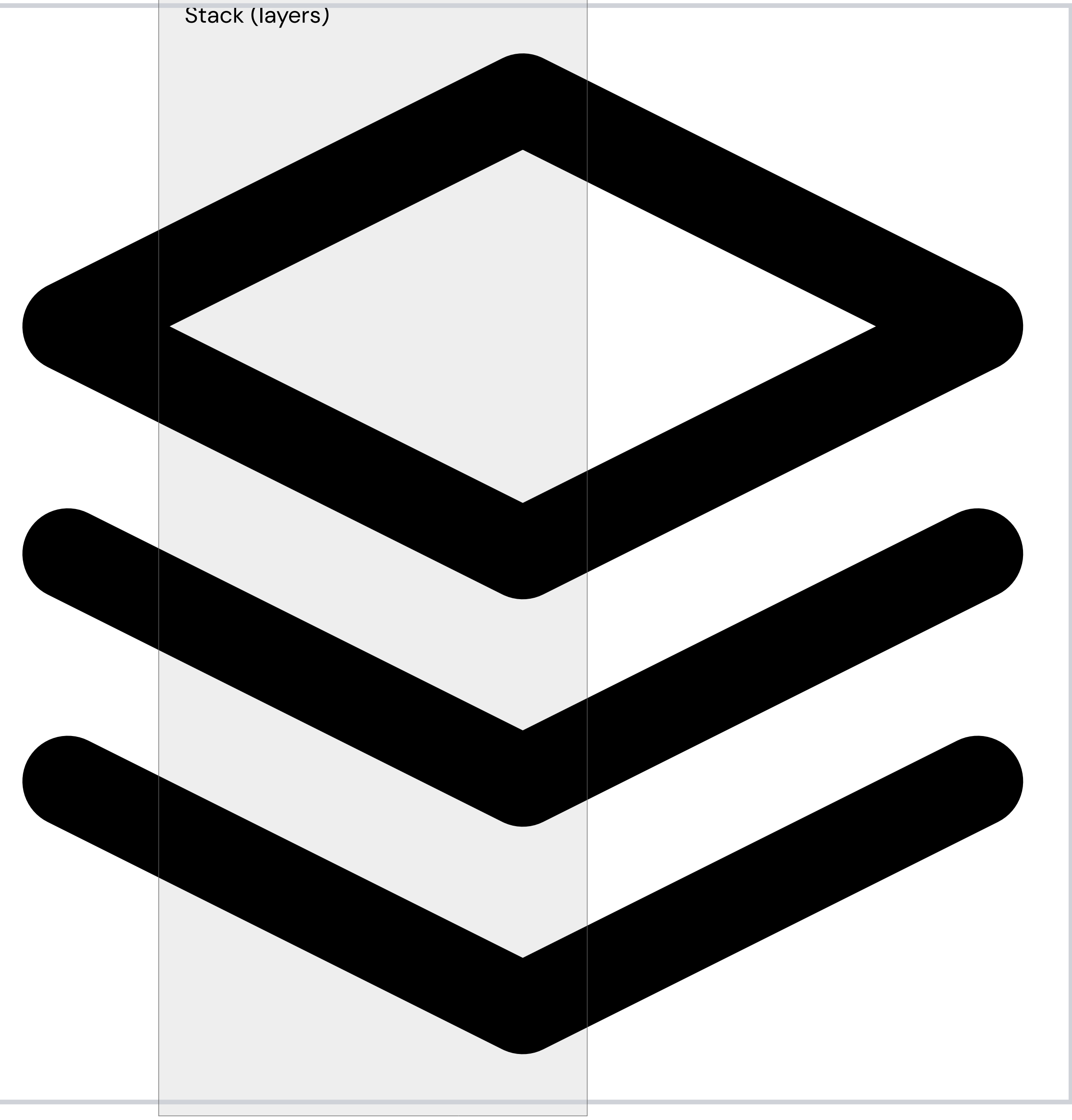
Description	Icon (76px)
Cloud	☁

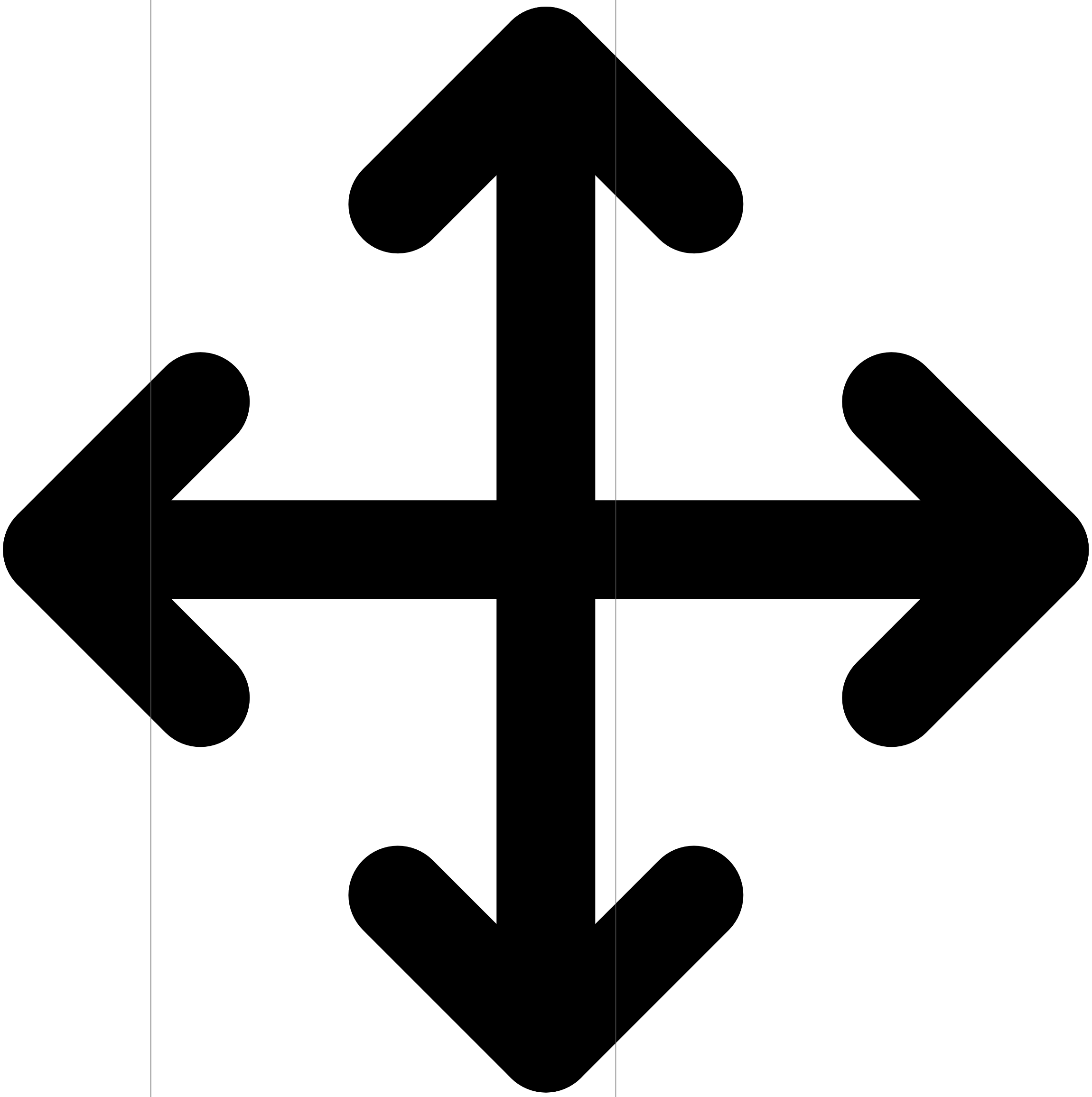
Description	Icon (76px)
Tools	🔧

Description	Icon (76px)
Authorize	🔑

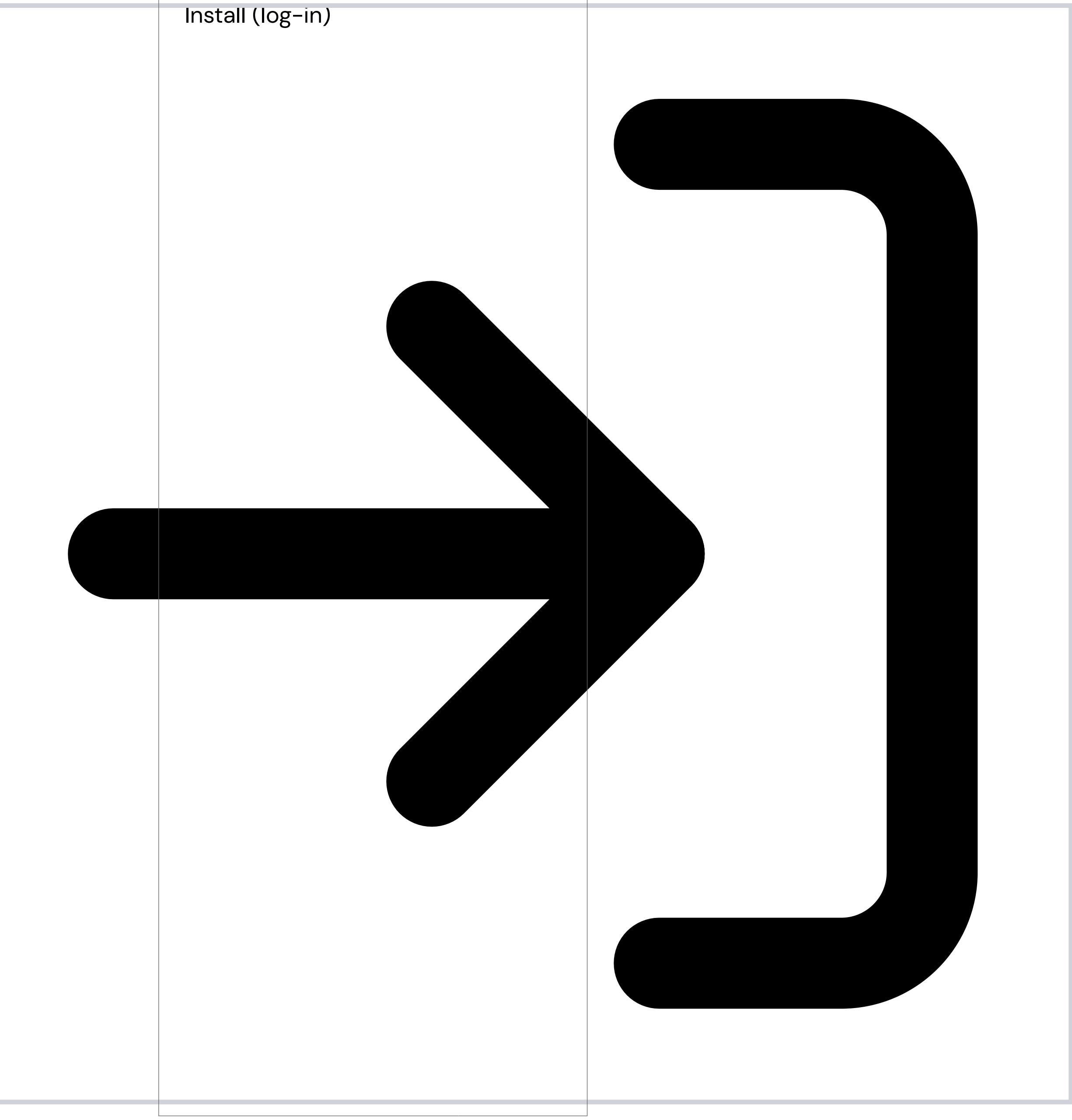
Description	Icon (76px)
API	

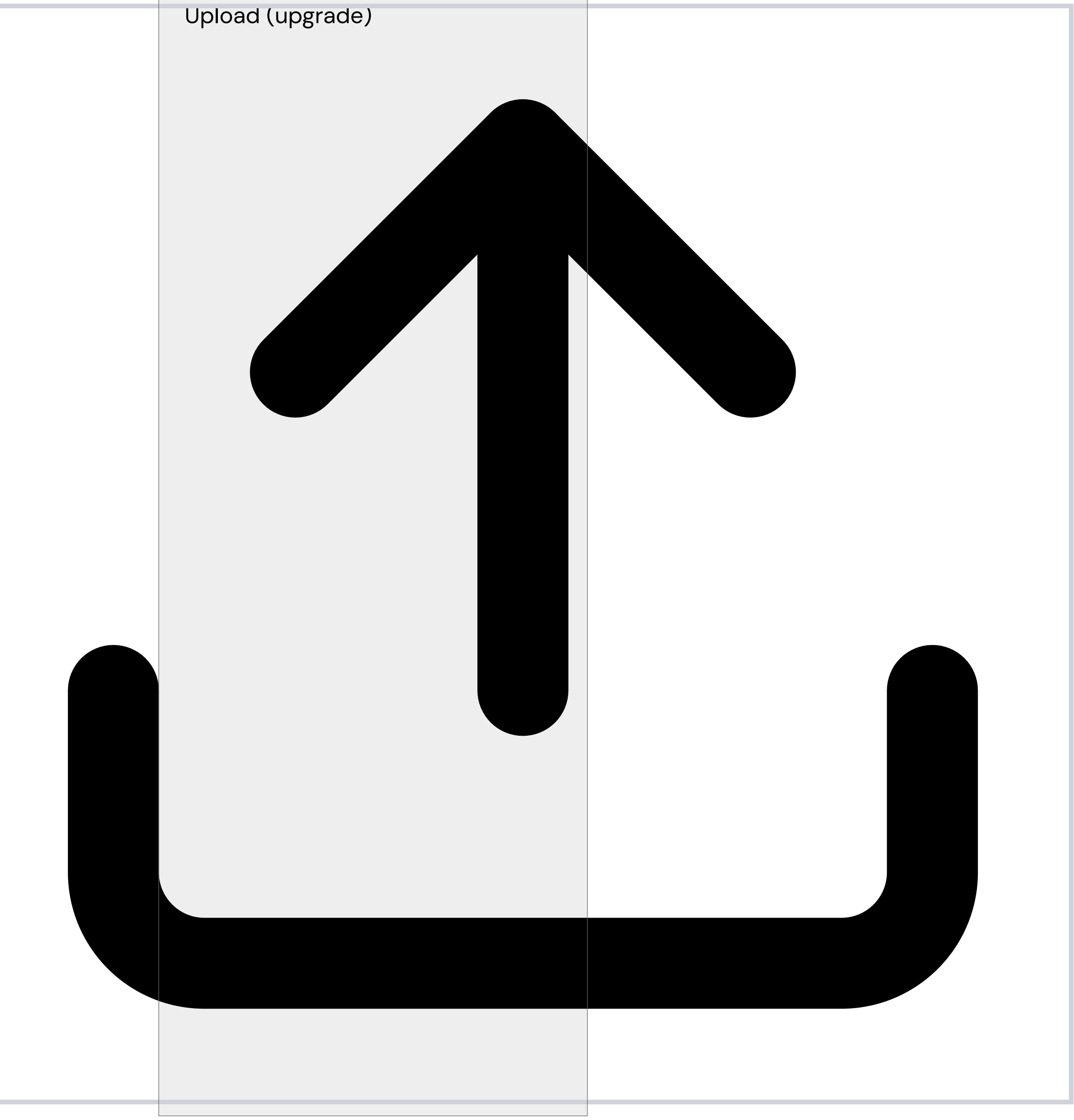
Description	Icon (76px)
AWS (box)	

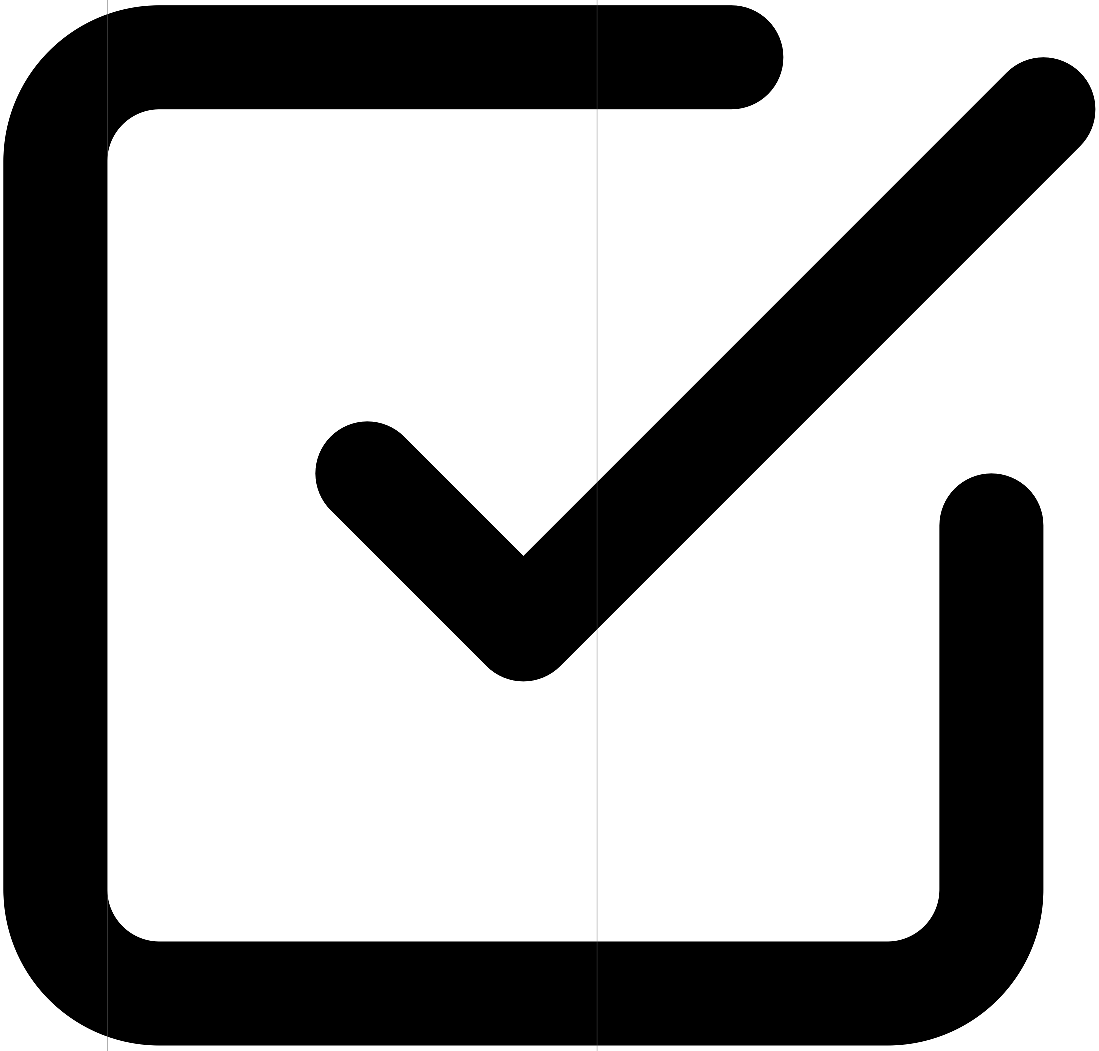
Description	Icon (76px)
Stack (layers)	

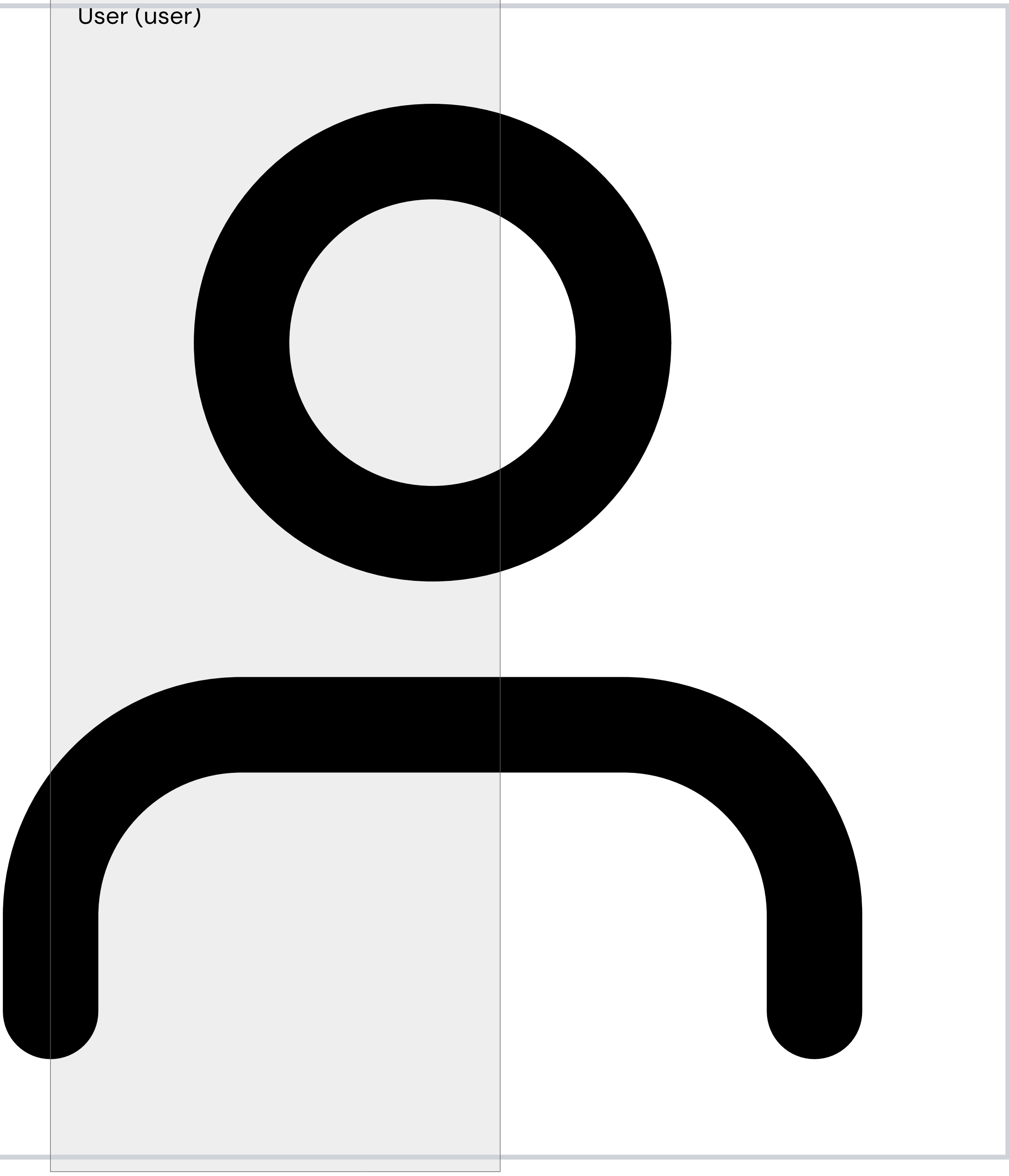
Description	Icon (76px)
Move (move)	

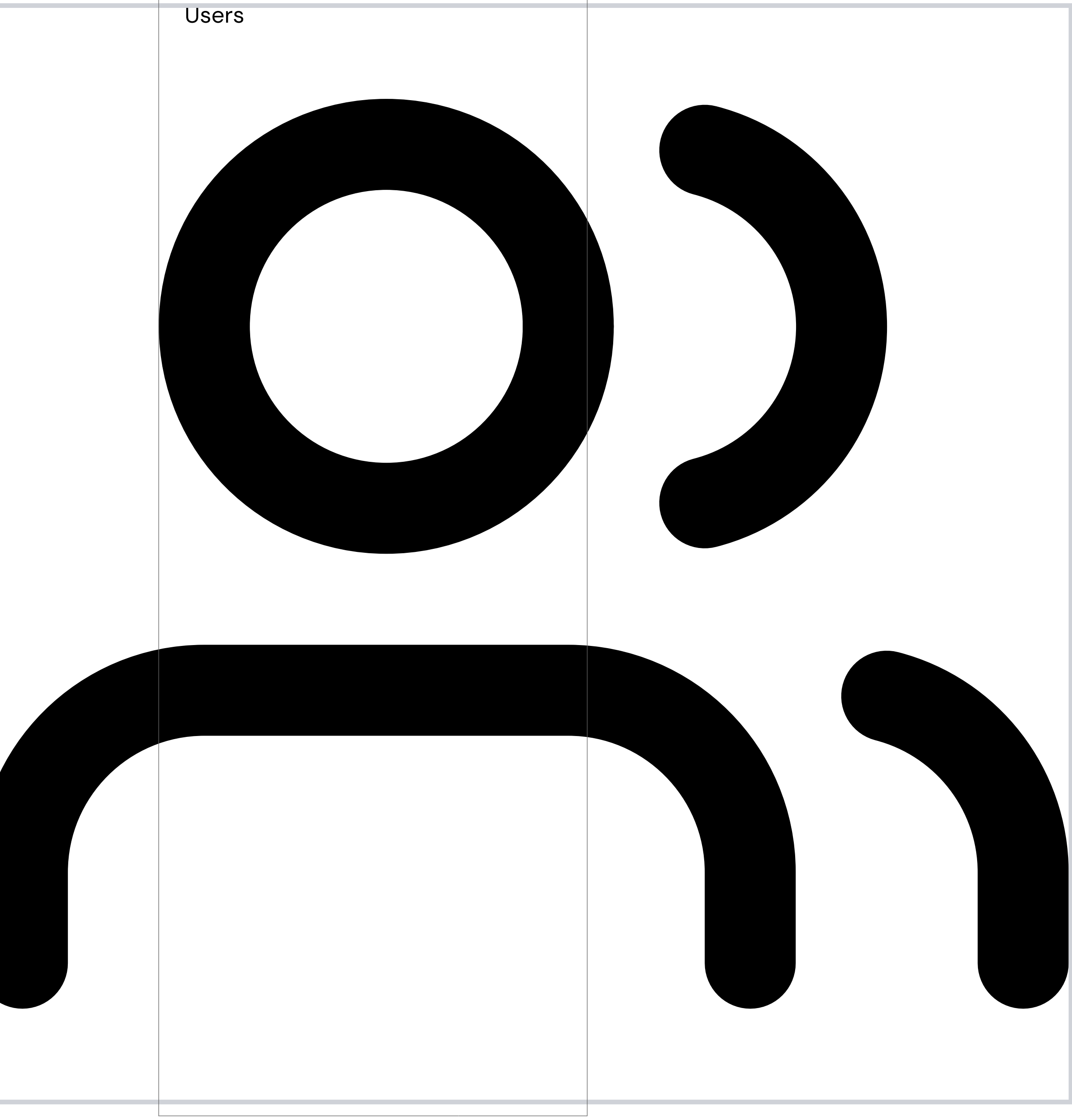
Description	Icon (76px)
Update (refresh-cw)	↻

Description	Icon (76px)
Install (log-in)	

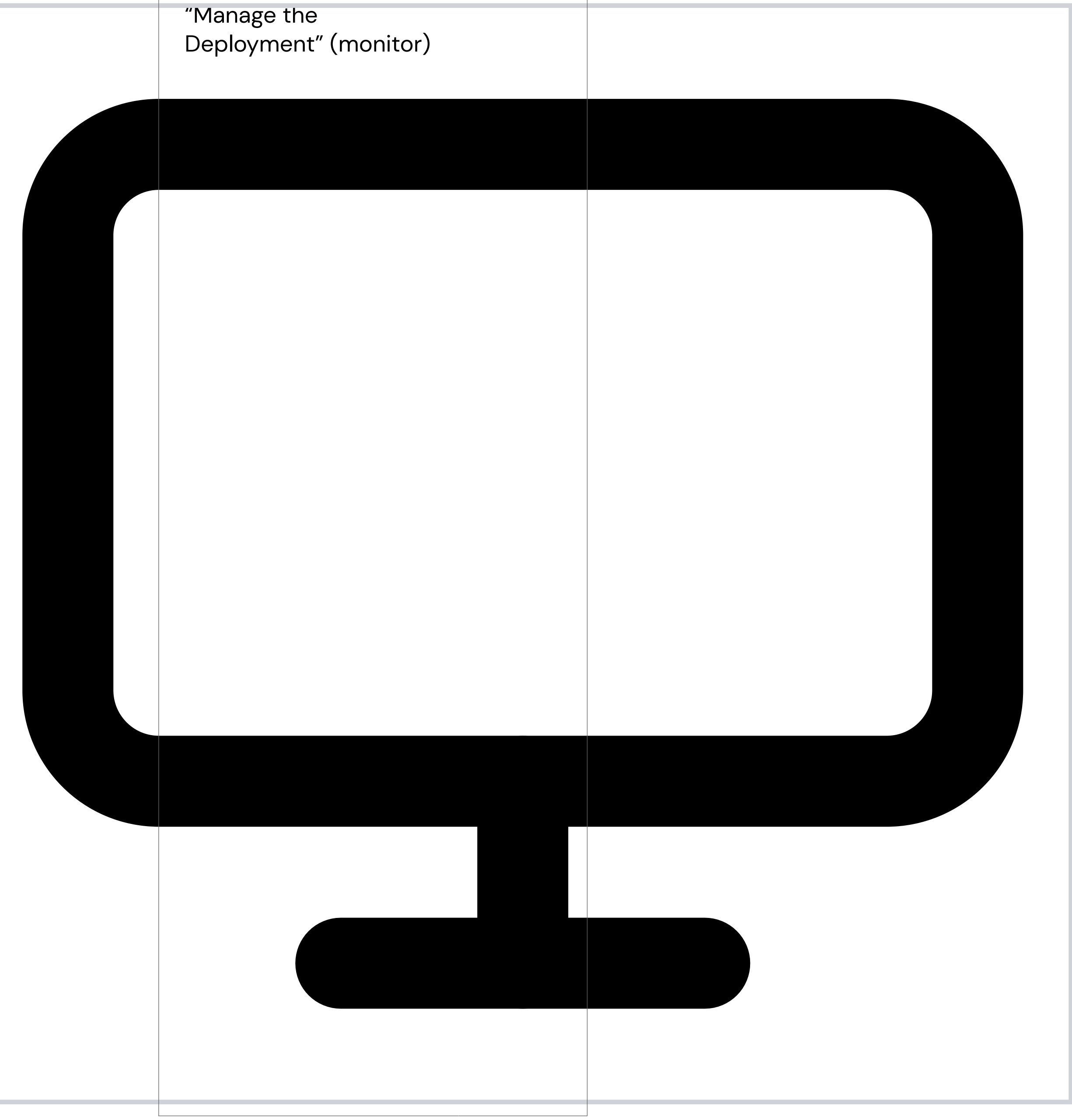
Description	Icon (76px)
Upload (upgrade)	

Description	Icon (76px)
Require (check-square)	

Description	Icon (76px)
User (user)	

Description	Icon (76px)
Users	

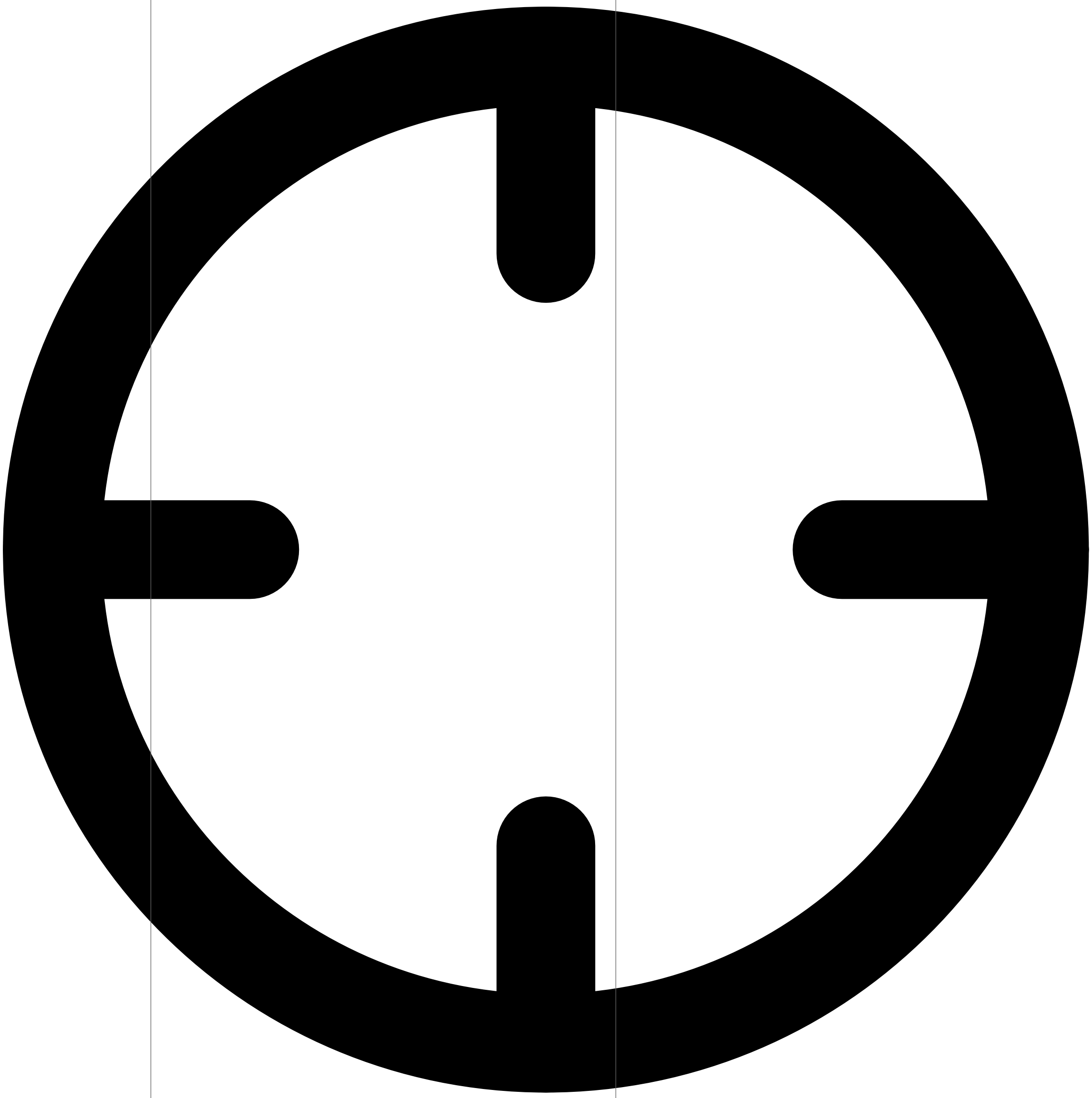
Description	Icon (76px)
Configuring Options (settings)	⚙

Description	Icon (76px)
“Manage the Deployment” (monitor)	

Description	Icon (76px)
"Swagger" (code)	< >

Description	Icon (76px)
Contact Support (help-circle)	❔

Description	Icon (76px)
(star)	☆

Description	Icon (76px)
Watermark (crosshair)	

Description	Icon
Important	❗

Description	Icon
Note (option to use FontAwesome \f15c)	📄

Description	Icon
Tip	💡

Description	Icon
Search bar icon (portal)	🔍

Description	Icon
Warning	⚠