



Snowflake Plugins for the Central Policy Manager

The CyberArk Password Vault
Version 12.x

Copyright © 1999-2025 CyberArk Software Ltd. All rights reserved.

This document contains information and ideas, which are proprietary to CyberArk Software Ltd. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, without the prior written permission of CyberArk Software Ltd.

EPVEMC07-2-0-1



Changing Credentials on Snowflake

The Central Password Manager enables organizations to change credentials automatically on remote machines and store the new credentials in the Enterprise Password Vault, with no human intervention, according to the organizational policy. These plugins support the changing of credentials for users on the Snowflake using the REST API protocol.

Snowflake Credentials

Snowflake plugins support the following types of credentials on Snowflake:

1. [Keys \(also referred as key pair\)](#)
2. [PATs \(programmatic access tokens\)](#)
3. [Passwords \(via ALTER USER command\)](#)

Pre-requisites

REST API Platform

1. Download and install the [REST API Platform](#) from Marketplace
 - If you already have an older version installed, remove the platform and install the newest version from Marketplace.

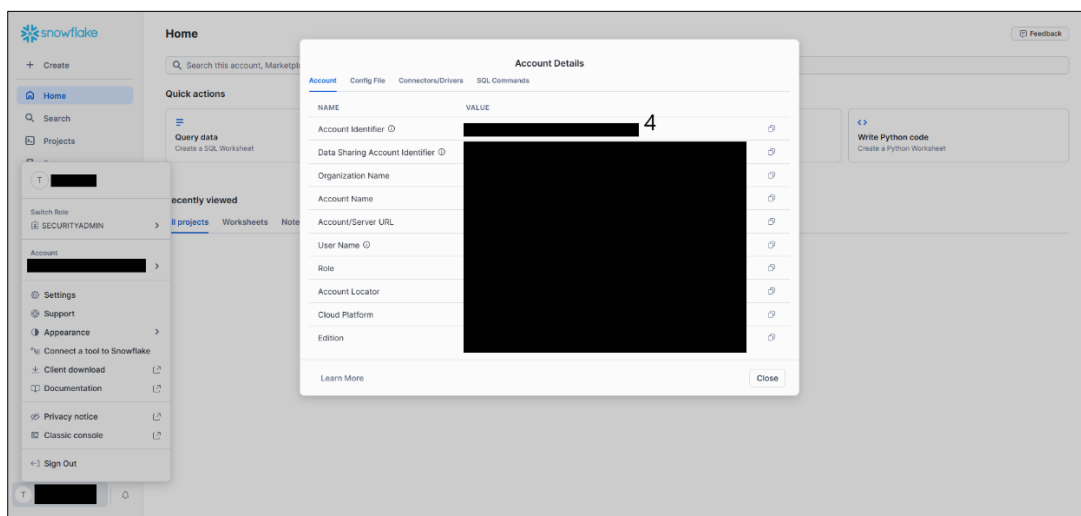
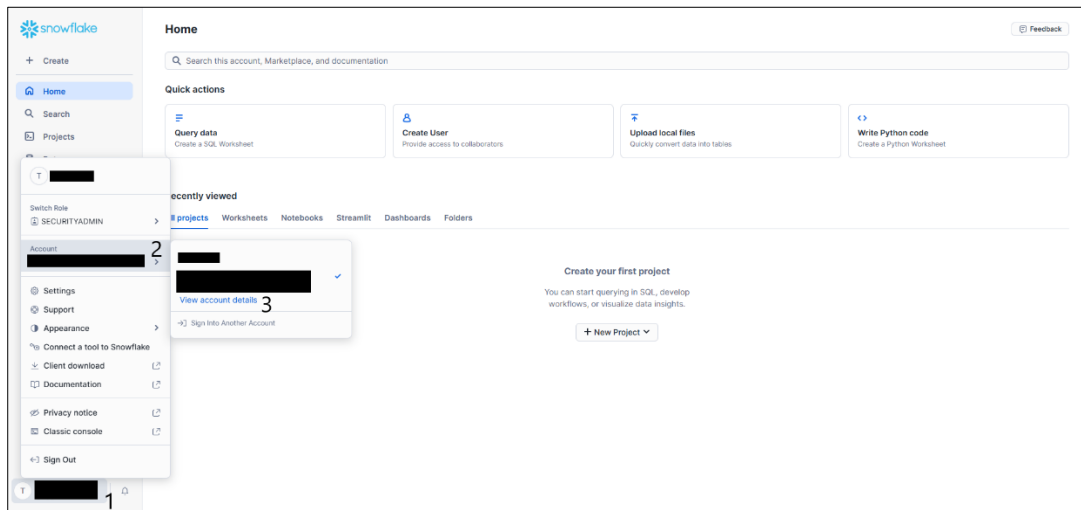
Reconcile Account

2. All Snowflake plugins require a reconcile account to function correctly. Absence of linked reconcile account or missing setup (listed below) will result in failed Change and Reconcile.
 - Reconcile account must have a Snowflake role with at least OWNERSHIP privilege for target account/s (or higher role). See [Snowflake documentation](#) for more details.
 - Reconcile account must have **Key** as its credential (not PAT nor password). As result, the reconcile account must be set per instructions for Snowflake Keys Plugin.
 - The only exception to this rule is the Snowflake Keys plugin, where target account can Change its own Key. In that use case, make sure to give the target account same privileges as reconcile account to allow Key Change.



Account Identifier

3. All credentials require **Account Identifier** property to function properly. Here are the instructions on finding that value.
 - **Account Identifier** property consists of the name of the account prefixed by its organization (e.g. myorg-account123). More details in Snowflake documentation about [Account identifiers](#).
 - Navigate to Snowflake app homepage and follow the steps in the screenshots:



Snowflake Keys Plugin

Installation

The following instructions show you how to install the Snowflake Keys Plugin.

Pre-requisites

1. Generate the keys.
 - Use PuTTYgen (third-party tool) to generate a private key (set **RSA** as key type and **2048** as number of bits).
 - PuTTYgen can be downloaded [here](#).
 - Export the private key as OpenSSH key without passphrase (in PuTTYgen, **Conversions > Export OpenSSH key**) as file with .p8 file extension.
 - Generate a public key using OpenSSL command-line tool:

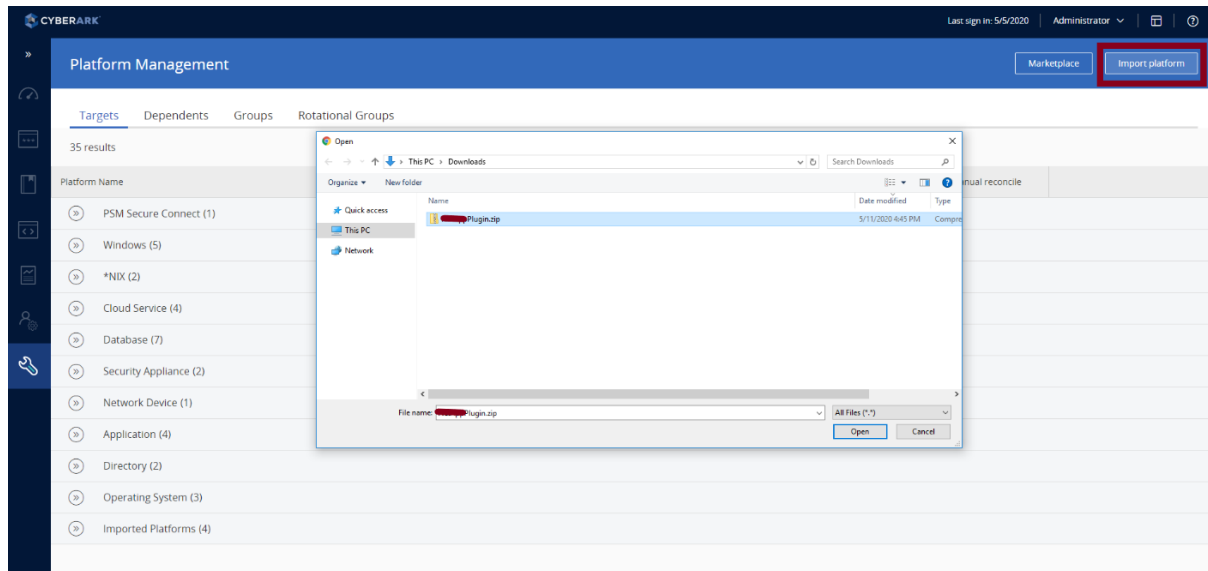
```
openssl rsa -in <private key>.p8 -pubout -out <public key>.pub
```

 - OpenSSL command-line tool can be downloaded as part of [Git for Windows](#).
 - Alternatively, it can be downloaded directly from [OpenSSL website](#) (for advanced users only).
2. Grant the privilege to assign a public key to a Snowflake user by following [Grant the privilege to assign a public key to a Snowflake user](#) section in Snowflake's documentation. Only the linked section needs to be completed – other sections are not required.
3. Assign the public key to a Snowflake user by following [Assign the public key to a Snowflake user](#) section in Snowflake's documentation. Only the linked section needs to be completed – other sections are not required.



Installing the Snowflake Keys Plugin

1. Log in to the PVWA with an administrative account.
2. Go to Administration > Platform Management.
3. Click Import Platform. Upload the SnowflakeKeysPlugin.zip file.



Platform Configuration

- Please check that the following default platform settings match your environment.
- They can be modified by navigating to Administration → Platform Management → Snowflake Keys via REST API → Edit → Automatic Password Management → Additional Policy Settings → Parameters

Parameter Name	Description	Value
UseSSL	Setting this property to yes will create a REST API request using HTTPS and validate a proper certificate is used. Setting this property to no will create a REST API request using HTTP. Setting this property to ignoreuntrustedcertificates will create a REST API request using HTTPS but does not require a valid certificate.	Yes
Port	The port used to connect to the target device. Setting its value to -1 will let the port to be set based on the HTTP protocol (80 for HTTP and 443 for HTTPS).	-1



Adding Snowflake Keys Accounts

Adding Accounts through the Password Vault Web Access

- Create a new Snowflake Keys account or use an existing one.
- Specify the required account properties.
 - See the [Account Identifier](#) section for **Account Identifier** setup.
- Associate a reconcile account for the new password object.
 - See the [Reconcile Account](#) section for reconcile and target accounts setup.

For more information about adding password objects in the Password Vault Web Access, refer to the online documentation [here](#).

General Notes

Snowflake Keys plugin supports the following:

- Key Verify
- Key Change
 - Target account must have the same privileges as reconcile account for a successful Key Change.
- Key Reconcile



Snowflake PATs Plugin

Installation

The following instructions show you how to install the Snowflake PATs Plugin.

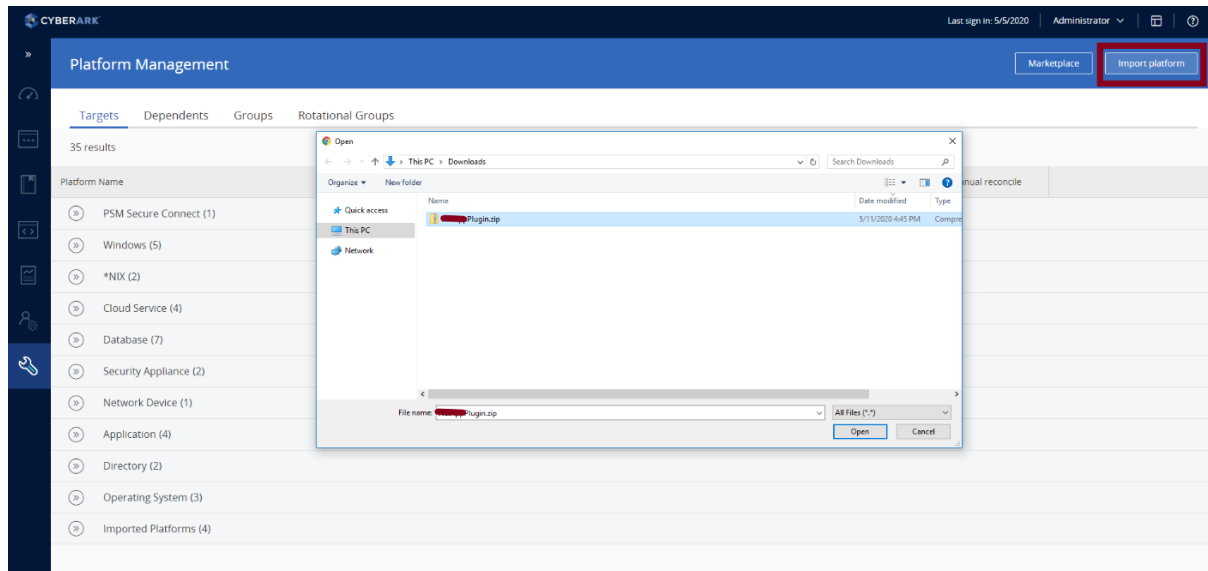
Pre-requisites

1. Generate the PAT via Snowflake web interface.
2. Set an active [network policy](#) on the account or user.
 - You can confirm that a network policy is correctly set when you no longer see the **Missing network policy** warning in the PATs section.



Installing the Snowflake PATs Plugin

1. Log in to the PVWA with an administrative account.
2. Go to Administration > Platform Management.
3. Click Import Platform. Upload the SnowflakePATsPlugin.zip file.



Platform Configuration

- Please check that the following default platform settings match your environment.
- They can be modified by navigating to Administration → Platform Management → Snowflake PATs via REST API → Edit → Automatic Password Management → Additional Policy Settings → Parameters

Parameter Name	Description	Value
UseSSL	Setting this property to yes will create a REST API request using HTTPS and validate a proper certificate is used. Setting this property to no will create a REST API request using HTTP. Setting this property to ignoreuntrustedcertificates will create a REST API request using HTTPS but does not require a valid certificate.	Yes
Port	The port used to connect to the target device. Setting its value to -1 will let the port to be set based on the HTTP protocol (80 for HTTP and 443 for HTTPS).	-1



Adding Snowflake PATs Accounts

Adding Accounts through the Password Vault Web Access

- Create a new Snowflake PATs account or use an existing one.
- Specify the required account properties.
 - **PAT Name** must be in ALL CAPS (on both account level and in Snowflake), otherwise the plugin will fail.
 - See the [Account Identifier](#) section for **Account Identifier** setup.
- Associate a required reconcile account for the new password object.
 - See the [Reconcile Account](#) section for mandatory setup.

For more information about adding password objects in the Password Vault Web Access, refer to the online documentation [here](#).

General Notes

Snowflake PATs plugin supports the following:

- PAT Verify
 - Set an active [network policy](#) on the account or user.
- PAT Change
- PAT Reconcile



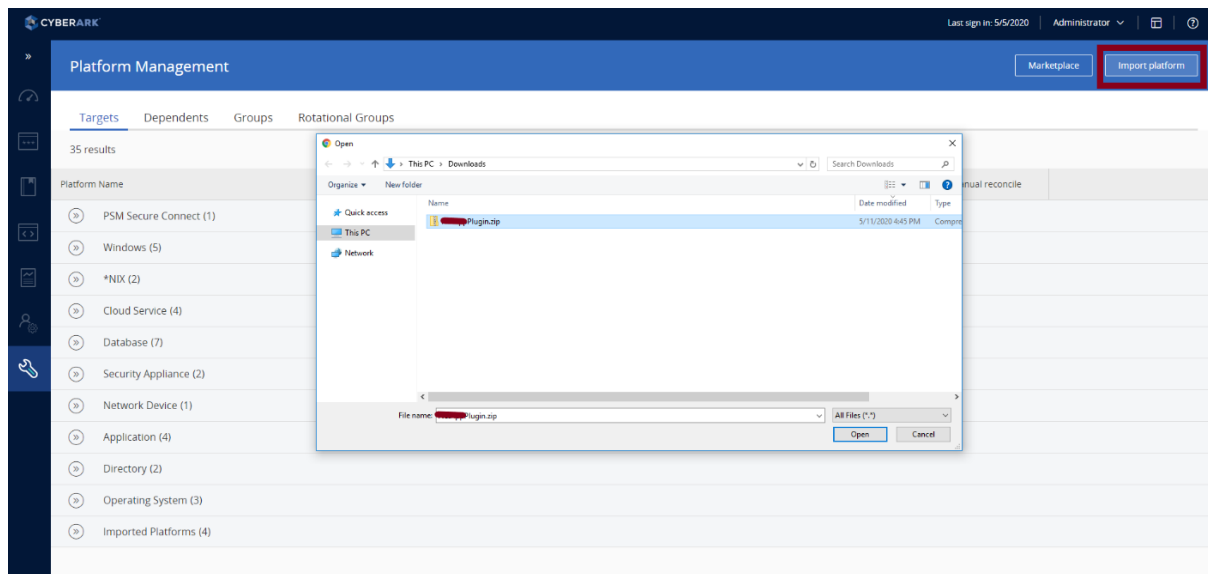
Snowflake Passwords Plugin

Installation

The following instructions show you how to install the Snowflake Passwords Plugin.

Installing the Snowflake Passwords Plugin

4. Log in to the PVWA with an administrative account.
5. Go to Administration > Platform Management.
6. Click Import Platform. Upload the SnowflakePasswordsPlugin.zip file.



Platform Configuration

- Please check that the following default platform settings match your environment.
- They can be modified by navigating to Administration → Platform Management → Snowflake Passwords via REST API → Edit → Automatic Password Management → Additional Policy Settings → Parameters

Parameter Name	Description	Value
UseSSL	Setting this property to yes will create a REST API request using HTTPS and validate a proper certificate is used. Setting this property to no will create a REST API request using HTTP. Setting this property to ignoreuntrustedcertificates will create a REST API request using HTTPS but does not require a valid certificate.	Yes
Port	The port used to connect to the target device. Setting its value to -1 will let the port to be set based on the HTTP protocol (80 for HTTP and 443 for HTTPS).	-1



Adding Snowflake Passwords Accounts

Adding Accounts through the Password Vault Web Access

- Create a new Snowflake Passwords account or use an existing one.
- Specify the required account properties.
 - See the [Account Identifier](#) section for **Account Identifier** setup.
- Associate a required reconcile account for the new password object.
 - See the [Reconcile Account](#) section for mandatory setup.

For more information about adding password objects in the Password Vault Web Access, refer to the online documentation [here](#).

General Notes

Snowflake Passwords plugin supports the following:

- Password Change
- Password Reconcile

