



# Okta Client Credentials Plug-in for the Central Policy Manager

The Cyber-Ark Password Vault  
Version 15.x

**Copyright © 1999-2026 Cyber-Ark Software Ltd. All rights reserved.**

This document contains information and ideas, which are proprietary to Cyber-Ark 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 Cyber-Ark Software Ltd.

EPVEMC07-2-0-1



# Changing Passwords on Okta Client Credentials

The Central Password Manager enables organizations to change passwords automatically on remote machines and store the new passwords in the Enterprise Password Vault, with no human intervention, according to the organizational policy. This plug-in supports the changing of passwords for users on the Okta Client Credentials using the API protocol.

## Prerequisite

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

Managing an Okta client secret for privileged accounts.

The Okta application integration must adhere to the following criteria in order for client secret management to be achieved via this plugin:

- The application integration sign-in method must be configured as "OIDC - OpenID Connect".
- The application type must be set to either "Web Application" or "Native Application". Where client authentication is specified as "Client secret".
- The "Authorization Code" grant type must be enabled.
- The Scope in the platform settings must be assigned to the Authorization Server that is configured for the Application within Okta API settings.

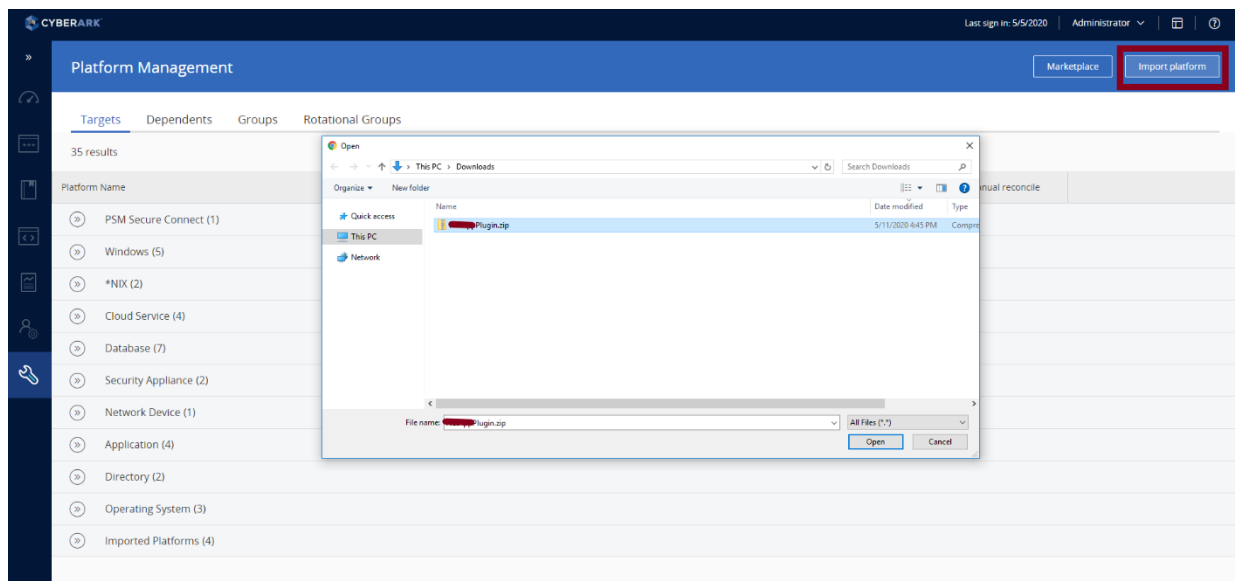


## Installation

You will receive the OktaClientCredentials plug-in zip archive from your CyberArk representative. The following instructions show you how to install it.

### Installing the Okta Client Credentials Plug-in

1. Log in to the PVWA with an administrative account.
2. Go to Administration > Platform Management.
3. Click Import Platform. Upload the OktaClientCredentialsPlugin.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 → OktaClientCredentials → Edit → Automatic Password Management →

| Parameter Name          | Description                                                                              | Value     |
|-------------------------|------------------------------------------------------------------------------------------|-----------|
| UseSSL                  | Whether to use an SSL connection.                                                        | Yes       |
| Port                    | The port used to connect to the target device.                                           | 443       |
| Scope                   | The name of the configured and associated scope to the Authorization server within Okta. | CHANGE_ME |
| AuthorizationServerName | The name of the configured authorization server within Okta.                             | CHANGE_ME |

## Adding OktaClientCredentials Accounts

### Adding Accounts through the Password Vault Web Access

- Create a new OktaClientCredentials account or use an existing one.
  - Client ID is the Client ID found within Okta.
  - Password is the Client Secret found within Okta
  - Address of the Okta server
- Associate a reconcile account to the current user
  - Locate or manually generate an Okta API key for your Okta application and set it as the password value for the Reconcile Account.

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

## General Notes

OktaClientCredentials plug-in supports the following:

- Password verification



- Password change (All changes are resets)
- Password reconciliation