



Dell PowerScale OneFS ** Central Policy Manager (CPM) Plug-in Implementation Guide

CyberArk Privilege Access Manager / Identity Security Platform - Versions 12.x or higher

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.

Changing Passwords on Dell PowerScale OneFS

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 Dell PowerScale OneFS using the Protocol protocol.

Prerequisite

This plugin runs on the Terminal Plugin Controller (TPC) engine found on the Marketplace [here](#).

Requirements:

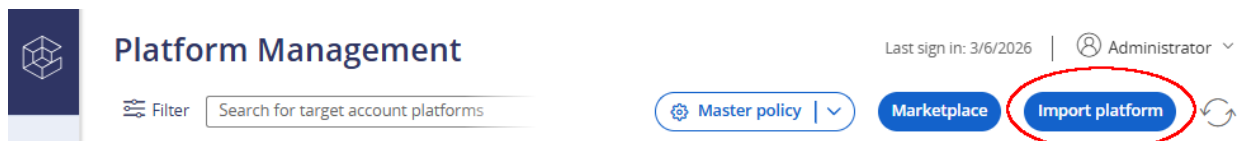
- The target account must reside in the OneFS built-in System file provider (Isa-file-provider:System)
- SSH access must be enabled on the target account via the ISI_PRIV_LOGIN_SSH privilege
- To use admin as a reconcile account for root, sudo permission must be granted for both /usr/bin/isi **AND** /usr/bin/isi_for_array via command: isi_visudo:
admin ALL=(ALL) NOPASSWD:/usr/bin/isi_for_array, /usr/bin/isi
- The OneFS cluster must be running a version that supports isi auth users reset-password

Installation

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

Installing the Dell PowerScale OneFS Plug-in

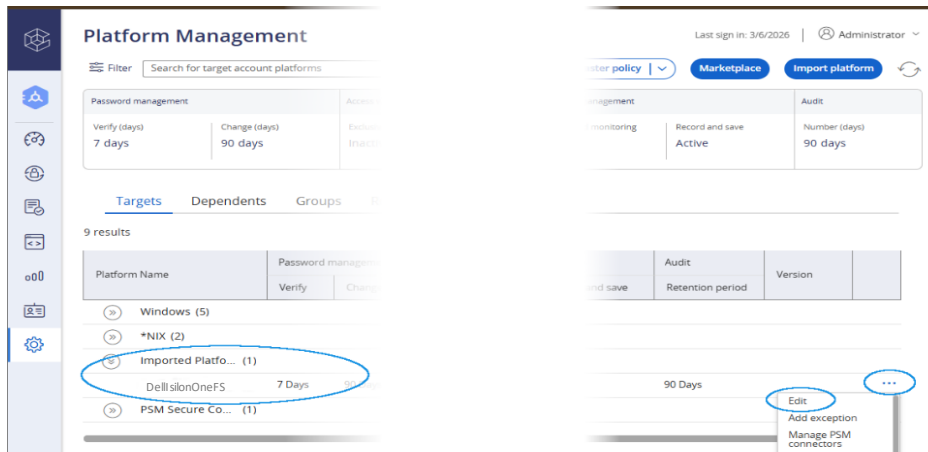
1. Log in to the PVWA with an administrative account.
2. Go to Administration > Platform Management.
3. Click Import Platform. Upload the DellPowerScaleOneFSPlugin.zip file.



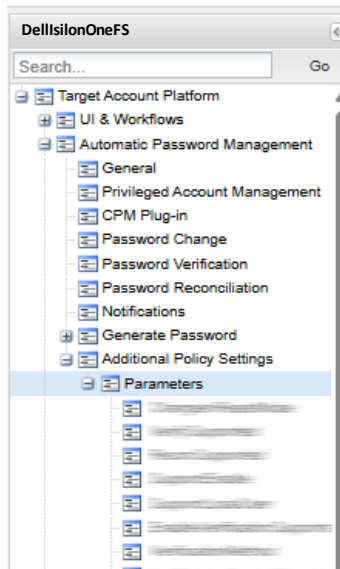
Platform Configuration

Please check that the following platform settings match your environment.

The settings can be modified by navigating to (PVWA UI) → Administration → Platform Management → DellPowerScaleOneFS → ... → **Edit**



Automatic Password Management → Additional Policy Settings → Parameters



Parameter Name	Description	Value
Protocol	The protocol employed to connect to the target device.	SSH
Port	The port used to connect to the target device.	22
InterruptActiveSessions	Controls whether to proceed if an active SSH session is detected during ReconcilePass.	No
RotateAndEnableDisabledAccounts	Controls whether to proceed if the account is disabled. This will enable the target account.	No
RotateAndUnlockLockedAccounts	Controls whether to proceed if the account is locked. This will unlock the target account.	No
SleepBetweenConnectionsSec	Optional sleep interval in seconds between connections.	5

Adding DellPowerScaleOneFS Accounts

Adding Accounts through via the Password Vault Web Access (PVWA) UI:

- [Create a new DellPowerScaleOneFS account or use an existing one.](#)
- [Specify the required account properties.](#)
- [Associate a reconcile account with the new password object](#)

More Information

For more information about managing platforms and password objects in the Password Vault Web Access, refer to the online documentation:

[Limit platforms to specific Safes](#)

[Manage platforms](#)

General Notes

DellPowerScaleOneFS plug-in supports the following:

- Password change
- Password verification
- Password reconciliation

Password Self-Reconciliation:

Password reconciliation using a self-reconcile path (when the reconcile account matches the target account, aka: 'root' as reconcile associated to 'root' target) bypasses temporary password generation and performs a direct password change using the stored reconcile credential.

**** Note regarding legacy Isilon branding:** Dell now brands the platform as PowerScale and the OS as OneFS. Current documentation is generally published as PowerScale OneFS, although some support URLs, product identifiers, and legacy hardware references still retain Isilon naming.