



Cisco ISE CLI Admin Plug-in for the Central Policy Manager

The Cyber-Ark Password Vault
Version 12.x

Copyright © 2022 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 Cisco ISE CLI Admin

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 Cisco ISE CLI Admin using the SSH protocol.

Installation

This plug-in uses the newer management engine: **CyberArk.TPC.exe**

Please update **CyberArk.TPC.exe** to the latest version when installing this plug-in.

1. [Download the TPC Zip from the CyberArk Marketplace](#)*

Please note that CyberArk TPC v12 requires the [Microsoft .NET 4.8 Framework](#) to be installed on the CPM.

2. Copy the Zip to the CPM server(s) and extract these files to a temporary location:

- Expect.NET.dll
- Eagle.dll
- CyberArk.TPC.exe.config
- CyberArk.TPC.exe
- CyberArk.Extensions.Utilities.dll
- CyberArk.Extensions.Infra.Common.dll
- CyberArk.Extensions.Contracts.dll
- 3rdPartyLicense.txt
- META-INF folder

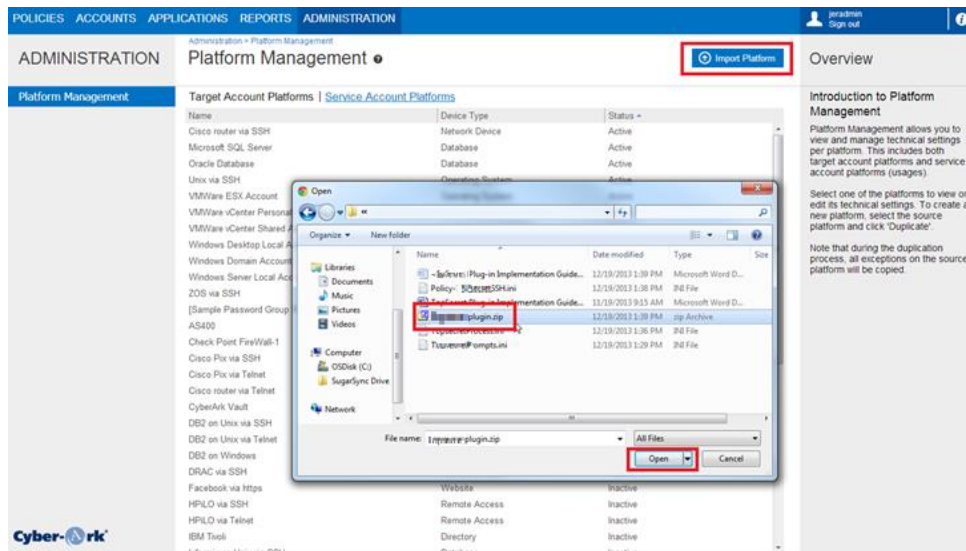
3. Create a backup copy of the existing *C:\Program Files (x86)\CyberArk\Password Manager\bin* directory.
4. Copy the files to: *C:\Program Files (x86)\CyberArk\Password Manager\bin*
5. [Additional instructions and information about CyberArk.TPC.exe are available here](#)**

You will receive the **CiscoISECLIAdminPlugin.zip** archive from your CyberArk representative.



Installing the Cisco ISE CLI Admin Plug-in

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



Platform Configuration

- The following platform settings are given initial default values. Please check that these match your environment or edit them accordingly .

To Edit these values navigate to :

Administration → Platform Management → Cisco ISE CLI Admin → Edit → Automatic Password Management → Additional Policy Settings → Parameters :

Parameter name	Default value	Description
Port	22	Target port
Protocol	SSH	Protocol used
FailOnDisconnectedSession	Yes	Yes: Change / Reconcile actions will fail if there are existing disconnected sessions. No: Actions will not fail if there are existing disconnected sessions, unless MaxSessions policy is exceeded.

Adding CiscoISECLIAdmin Accounts

Adding Accounts through the Password Vault Web Access

- Create a new CiscoISECLIAdmin account or use an existing one.
- Specify the required account properties.
- Associate a reconcile account for the new password object (*required*)

For more information about adding password objects in the Password Vault Web Access, refer to the Privileged Account Security Implementation Guide.

General Notes

- CiscoISECLIAdmin plug-in supports the following:
 - Password Change
 - Password Reconciliation
 - Password verification

