
Cisco ISE Non-Admin Users via API - (WSCchains)

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 Cisco ISE Non-Admin Users via API - (WSChains)

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 Non-Admin Users via API - (WSChains) using the REST API

Prerequisite

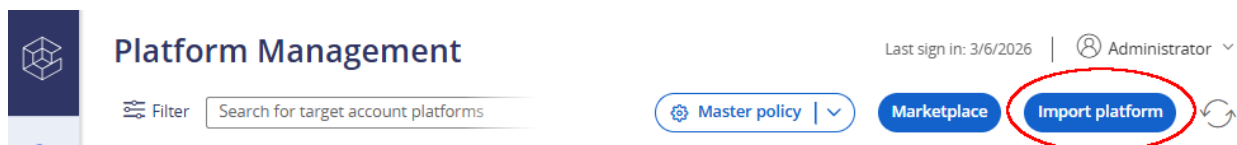
This plugin runs on the Terminal Plugin Controller (TPC) engine. It can be found on the Marketplace [here](#).

Installation

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

Installing the Cisco ISE Non-Admin Users via API - (WSChains) Plug-in

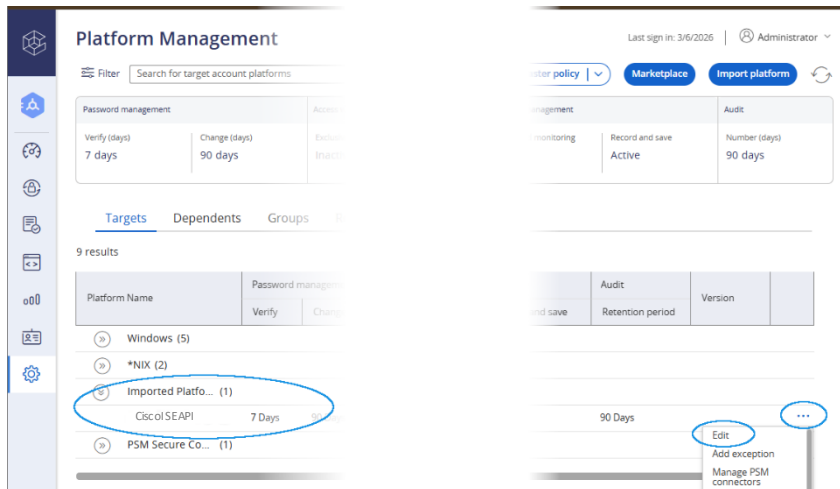
1. Log in to the PVWA with an administrative account.
2. Go to Administration > Platform Management.
3. Click Import Platform. Upload the CiscolSEAPIPlugin.zip file.



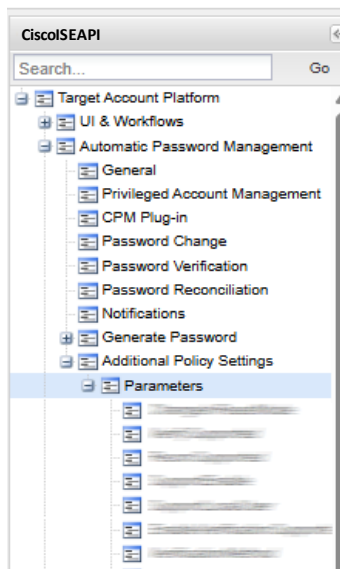
Platform Configuration

Please check that the following platform settings match your environment.

The settings can be modified by navigating to (PVWA UI) → Administration → Platform Management → CiscoISEAPI → ... → **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
ChainsFilePath	Configuration file of REST call logic	bin\CiscoISEAPIChains.xml
Port	The port used to connect to the target device.	443
Debug	Whether to create a debug log. Useful for troubleshooting.	No

Adding CiscoISEAPI Accounts

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

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

More Information

For information about managing platforms and password objects in the Password Vault Web:

[Limit platforms to specific Safes](#)

[Manage platforms](#)

General Notes

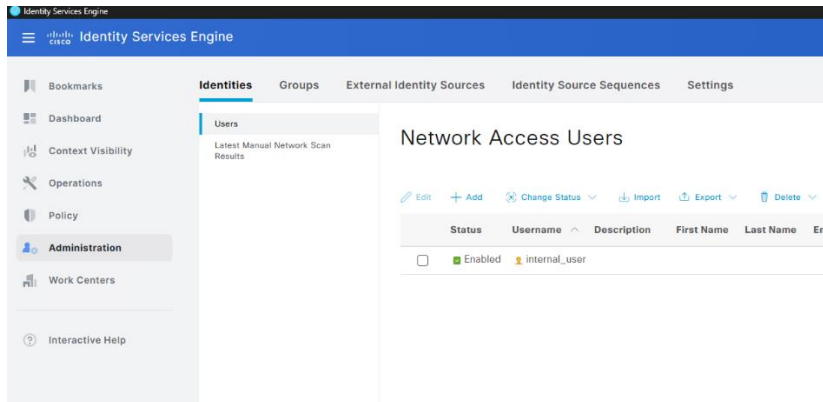
CiscoISEAPI plug-in supports the following:

- Password change (via reconciliation)

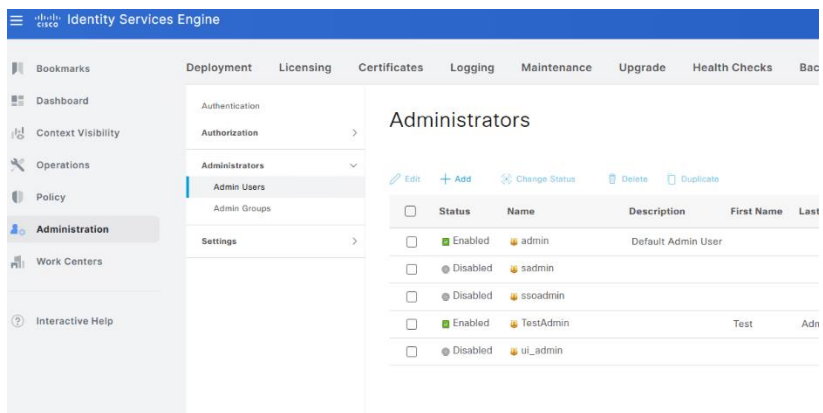
- Password reconciliation (Requires associated reconcile account - default)
- Please Note: Password policies must be aligned between Cisco and CyberArk for the plug-in to function correctly.

Clarification of plug-in purpose:

This Plug-in manages the users listed HERE (example):



This Plug-in DOES NOT manage the users listed here (example):



This Plug-in DOES NOT manage the users listed here (example):

```
cyberarkise/admin#show running-config | include "username"
no-username
username admin password hash $6$wG0a5/IYiMQuZmTs$5yOctMDh9aHZPB1WeE0QR2Hv
NUJ7qd5YrM/ role admin
username cli_admin password hash $6$PZxMddnv03S7X9HP$13DpwV1D9LKDPAY2mwNm
r8Ab4k7b5qbFEPl role admin
username cli_admin rec password hash $6$AHHwldICEepkSiJT$VjX0QUwlekfQMuuF
a4ZwQOxM3ZwOg5ek4VI role admin
username cli_rec_admin password hash $6$zkJU3AqWjWNJ3z76$zr/YqwQe.Qk01yoKd
kbFL.QIAWj1HI9DxjH. role admin
username dummy_admin password hash $6$0K/YOTbvZ6EPoowuSHISE69lmQFdImx4wdv
AvJpa5FG9vjclUjh/ role admin
username fuzz_admin password hash $6$UgdMvVftTVKtCnII$g5Tv/uSHttry/.FFlbyz
V6ifeqppejg42Mz. role admin
username poc_admin password hash $6$IJX7fCvEaNvE2t$XABJsJKBLM8pJWERZBGn
t/108XbbmAGJf21 role admin
username useradmin password hash $6$49/Jwx5CE58dwDJ.$xcFYAuvXQ7DFgE2zuH9h
MacfsgdVFmSimW1 role admin
cyberarkise/admin#
```

© 2026 CyberArk (a Palo Alto Networks Company)