

Cisco ISE Web UI

Privileged Session Management (PSM)

Connection Component / Universal Connector

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.

Prerequisites

This connection component requires the Secure Web Application Connectors Framework which comes out of box starting at version 10.2

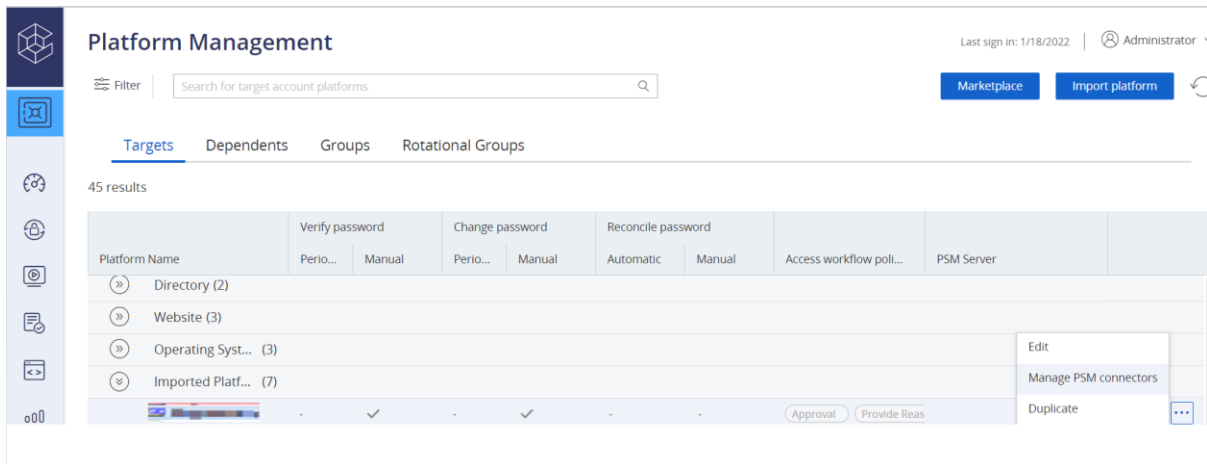
- **You must install the Secure Web Application Connectors Framework before importing this connection component.**
 - **Download the latest version of Secure Web Application Connectors Framework** from: [CyberArk Marketplace > Integrations > Secure Web Application Connectors Framework](#).
 - Please refer to the [Installation documentation](#) for details regarding:
 - *Which browsers are supported.*
 - *The latest browser driver.*
 - *Additional hardening configuration details*
 - **Use the latest version of the Secure Web Application Connectors Framework whenever possible.**

Installation

After installing the **Secure Web Application Connectors Framework**:

V12 or above:

1. Go to the PVWA -> Administration -> Platform Management. Select the necessary platform, select the 3 dots (on the right) and 'Management PSM connectors'



Platform Management

Last sign in: 1/18/2022 | Administrator

Filter: Search for target account platforms

Marketplace Import platform

Targets Dependents Groups Rotational Groups

45 results

Platform Name	Verify password		Change password		Reconcile password		Access workflow poli...	PSM Server
	Perio...	Manual	Perio...	Manual	Automatic	Manual		
Directory (2)								
Website (3)								
Operating Syst... (3)								
Imported Platf... (7)								

Approval Provide Reas Duplicate

2. Select the preferred PSM Server and click 'Next'.
3. Drag and drop **CC-CiscoISEWebUI.zip**

Manage PSM connectors

The platform is configured to use PSM server [PSM Server on AMPM-C067135F3](#)

☒ Show only selected connectors (0)

Search

 **Connector package**
Drag & drop or browse

A1000 Malware Analysis

Prerequisite

This connection component requires the Secure Web Application Connectors Framework. Please download the latest version from the Marketplace [here](#).

Configuration

PVWA UI Admin → Configuration → Options → Configurations → Connection Components → **PSM-CiscoISEWebUI**

Connection Component Parameters (Root Level)

Parameters that define generic settings of the PSM connection component.

Parameter Name	ID
Description	A unique ID that identifies the connection component
Acceptable Values	String
Default Value	PSM-CiscoISEWebUI

Parameter Name	DisplayName
Description	The name to be displayed in the connection selection. ("click to connect" drop-down on the account view)
Acceptable Values	String
Default Value	Cisco ISE Web UI

Parameter Name	DisableRemoteApp
Description	Enable / Disable RDS RemoteApp Experience remote applications with the same look and feel as local applications.
Acceptable Values	Yes/No
Default Value	No

Parameter Name	authentication level:i
Description	Defines the server authentication level settings in the RDP file. 0: If server authentication fails, connect to the computer without warning. 1: If server authentication fails, don't establish a connection. 2: If server authentication fails, show a warning, and choose to connect or refuse the connection. 3: No authentication requirement specified. Note: Some PSM server environments require this to be set to 1 or 2. If this is not required, delete this parameter.
Acceptable Values	0,1,2,3
Default Value	3

Target Settings section

Target Settings → Client Specific

Parameter Name	ActionTimeout
Description	The maximum number of seconds to wait for an action to complete.
Acceptable Values	Positive integer
Default Value	20

Parameter Name	WaitForElementIsNotVisibleTimeout
Description	The maximum number of seconds to wait for the target element to no longer be visible in the browser before timing out and moving to the next step. If this parameter is not specified, the system uses the value of the ActionTimeout parameter.
Acceptable Values	Positive integer
Default Value	2

Parameter Name	PageLoadTimeout
Description	The maximum number of seconds to wait for an action to complete.
Acceptable Values	Positive integer
Default Value	5

Parameter Name	DriverFolder
Description	Folder containing the browser driver.
Acceptable Values	Full Path
Default Value	C:\Program Files (x86)\CyberArk\PSM\Components

Parameter Name	MinimizeBrowserWhenLoading
Description	Determines whether the browser is minimized when connecting to the desired URL.
Acceptable Values	Yes, No
Default Value	Yes

Parameter Name	RunValidations
Description	Specifies if the (validation)action(s) defined in WebFormFields run. If set to "Yes", validations are required.
Acceptable Values	Yes, No
Default Value	Yes

Web Form Settings

All Web Form settings and parameters can include dynamic parameter placeholders such as {address} or {username}. These placeholders are replaced with the value of the corresponding account attribute or platform parameter.

Parameter Name	LogonURL
Description	Specify the URL of the target application login page.
Acceptable Values	URL
Default Value	https://{address}/admin/login.jsp

Parameter Name	WebFormFields
Description	List of login actions to perform.
Acceptable Values	List of commands.
Default Value	username>(button)(searchBy=name) username>{username}(searchBy=name) password>(button)(searchBy=name) password>{password}(searchBy=name) Login>(button)(searchBy=Text) //a^[@class="navbar-logo">^(Validation)(searchBy=XPath)

Parameter Name	EnforceCertificateValidation
Description	Enable or disable validation of target website certificates used by this connector. To connect to a local web application with an invalid certificate, such as LAN applications with self-signed certificates. specify No .
Acceptable Values	Yes, No
Default Value	Yes

Parameter Name	DriverFolder
Description	The folder where the browser driver is located.
Acceptable Values	Full path
Default Value	C:\Program Files (x86)\CyberArk\PSM\Components

Add the connection component to a platform

1. Go to Administration -> Platform Management
2. Select the platform you would like to add this connector to
3. Click "Edit"
4. Go to "UI & Workflows" ->
 - Right-click -> "Add Privileged Session Management" (it may be grayed out if the platform already has it configured)
 - If there is no "Connection Components" then Right-click -> "Add Connection Components"
 - "Connection Components" → Add Connection Component
5. Rename the newly created "Connection Component" to "PSM-CiscoISEWebUI" (update Id field)
6. Click "OK" to save
7. On the PSM server – restart the service "CyberArk Privileged Session Manager" (or wait until the refresh interval has passed)

Configure AppLocker

The PSM installation includes an AppLocker script which enables PSM users to invoke internal PSM applications, mandatory Windows applications, and 3rd party external applications that are used as clients in the PSM.

If your PSM server is hardened and AppLocker is enabled, you will need to perform the configuration changes outlined in the Secure Web Application Connectors Framework documentation.

Please refer to the [Secure Web Application Connectors Framework Installation documentation](#) for more information.