



CYBERARK®

Commvault CommCell with Automated MFA PSM Universal Connector

CyberArk Privileged Access Management
Versions 12.x

Copyright © 2026 CyberArk Software Ltd. 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.

EPVEMC07-2-0-1



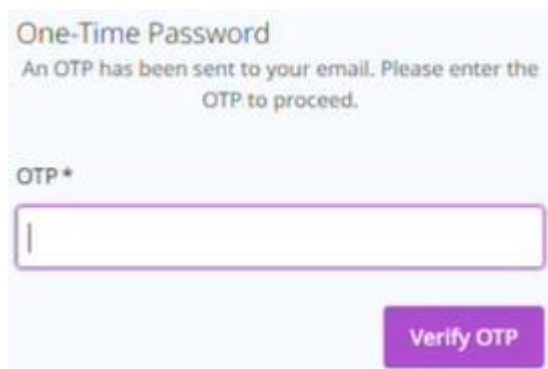
Installation

You will receive the Commvault CommCell with Automated MFA PSM Universal Connector from your CyberArk representative. The following instructions show you how to install it.

Prerequisites

In order to automate the CommCell MFA login process, you need to obtain the MFA key that is provided by CommCell. This MFA Key must be onboarded into CyberArk as a separate account. To obtain this MFA Key, the following steps must be performed:

1. Once MFA has been setup for the account, manually login with the target account username and password (or use the CommCell with Manual MFA PSM Connector).
2. If the following screen appears, you will need to enter the OTP code that is sent to the associated email:

A screenshot of a web-based One-Time Password (OTP) verification screen. The title is "One-Time Password". Below the title, it says "An OTP has been sent to your email. Please enter the OTP to proceed." There is a text input field labeled "OTP*" with a single vertical line cursor inside. Below the input field is a purple button labeled "Verify OTP".

3. After logging in the first time, a QR code will be displayed as well as the MFA Key. Copy the value of the Key, as it will need to be onboarded into the vault:



Account: [REDACTED]:AutomaticMFAUser1

Key: V5F [REDACTED] 4

4. If you are unable to obtain the MFA Key, please refer to the Commvault documentation or reach out to your Commvault contact for more details.

Once the MFA Key has been obtained, create a new account through PVWA and store the MFA Key value into the password field. Note that the PSM connector will only retrieve the MFA Key value and the rest of the details of this account are unused by the PSM Connector.

This newly created MFA Key account will need to be associated as a linked logon account to the target account.



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

It is recommended to use the latest version of the Secure Web Application Connectors Framework whenever possible.

- A supported browser must be installed. For more information, see [Supported browsers](#) below.
- The latest browser driver must be installed for all browsers that you use. For more information, see [Supported browsers](#) below.
- Microsoft Edge requires further hardening configuration. For details, see [PSM Hardening Tasks](#).
- CPM plugins require .NET Framework 4.8. If you are using an older version of the CPM, .NET Framework 4.8 must be installed on the CPM machine as well.
- Latest version of Secure Web Application Connectors Framework, download from [CyberArk Marketplace > Integrations > Secure Web Application Connectors Framework](#).



Connection Component Settings

[Documentation Reference link](#)

https://docs.cyberark.com/pam-self-hosted/latest/en/content/pasimp/psm_webapplication.htm

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	CommvaultCommCellWithAutomatedMFA

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	Commvault CommCell with Automated MFA

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

Parameters that define specific target machines settings. These parameters can be overridden at the platform or account level.

Client Specific

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

Parameter Name	WaitForElementActionableTimeout
Description	The maximum number of seconds to wait for the target element to be interactable before timing out and failing execution. If this parameter is not specified, the system uses the value of the ActionTimeout parameter (default value = 10).
Acceptable Values	Positive integer
Default Value	5

Parameter Name	BrowserDriverCommandTimeout
Description	The maximum number of seconds to wait for the browser to complete the command.
Acceptable Values	Positive integer
Default Value	60

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	5



Parameter Name	WaitForFrameLoadDelay
Description	The maximum delay in seconds when focusing on an iFrame without Attribute to enable the frame to load. If this parameter is not specified, the system uses the value of the ActionTimeout parameter
Acceptable Values	Positive integer
Default Value	5

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	BrowserPath
Description	Path to the browser exe file
Acceptable Values	Full Path
Default Value	C:\Program Files\Google\Chrome\Application\chrome.exe

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

Parameter Name	TransparentBackground
Description	Determines whether the ProgressBar background is transparent.
Acceptable Values	Yes, No
Default Value	Yes



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

Parameter Name	EnableTrace
Description	Whether to display the application during the login process. This parameter should be used for debug purposes only.
Acceptable Values	Yes, No
Default Value	No

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}



Parameter Name	WebFormFields
Description	List of login actions to perform.
Acceptable Values	List of commands.
Default Value	username>{Username} continuebtn>(Button)(SearchBy=Id) loginbtn> (Failure) (SearchBy=id)(Message="MFA has not been complete yet for this account") password>{Password}(SearchBy=Name) Continue>(Button)(SearchBy=Text) Run Generate_TOTP_MFA_Code (MFADeviceSecret={LogonAccount\password}) tfaPin > &MFACode& (searchby=id) Login > (button) (searchby=text) nav-search-field>(Validation)

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	No

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 “CommvaultCommCellWithAutomatedMFA” (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.

All AppLocker rules are defined in the **PSMConfigureAppLocker.xml** file in the **PSM installation folder → Hardening**.

- If your environment includes executables that must be allowed, in addition to those that are built-in to the PSM installation, such as PSM Universal Connectors executables, you must edit this file to add rules that will allow these executables.
- If you have connectors deployed using shared universal connector deployment on multiple PSM servers they will be updated automatically in the AppLocker rules. For details, see [Deploy Universal Connectors on multiple PSM servers](#). Associated executables are automatically updated in the AppLocker rules, but DLL dependencies must be added manually.
- Beginning in version 12.2.4, DLL files are allowed only when located with the allowed executables. If your environment includes DLL files that are not located with the allowed executables, you must add them to the **PSMConfigureAppLocker.xml** file.
- Reference:

https://docs.cyberark.com/pam-self-hosted/latest/en/content/pas%20inst/configure_applocker.htm

If your PSM server is hardened and AppLocker is enabled, you will need to perform the following configuration changes so the CyberArk Secure Web Application Connectors Framework dependencies will be allowed to run:

Open Powershell as Administrator from:

```
C:\Program Files (x86)\Cyberark\PSM\Hardening
```

1. Run: `notepad PSMConfigureAppLocker.xml`
2. For Google Chrome, add the following lines to the bottom of the `PSMConfigureAppLocker.xml` file, above the `</AllowedApplications>` tag.

```
<Application Name="Chrome" Type="Exe" Path="C:\Program Files  
(x86)\Google\Chrome\Application\chrome.exe" Method="Publisher" />
```



```
<Application Name="ChromeDriver" Type="Exe" Path="C:\Program Files  
(x86)\CyberArk\PSM\Components\chromedriver.exe" Method="Hash" />
```

3. For Microsoft Edge, add the following lines to the bottom of the PSMConfigureAppLocker.xml file, above the </AllowedApplications> tag.

```
<Application Name="Edge" Type="Exe" Path=" "C:\Program Files  
(x86)\Microsoft\Edge\Application\msedge.exe" Method="Publisher" />
```

```
<Application Name="EdgeDriver" Type="Exe" Path="C:\Program Files  
(x86)\CyberArk\PSM\Components\msedgedriver.exe" Method="Hash" />
```

Note: You may need to change the path(s) listed above to match your environment.

In the same Powershell window run:

```
PSMConfigureAppLocker.ps1
```

Following a successful completion of the script, **reboot the PSM server** to apply the AppLocker changes.

