



Forescout Console 9.1.3 PSM Universal Connector

The CyberArk Password Vault
Version v12.X

Copyright © 1999-2026 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 Forescout 9.1.3 PSM Universal Connector from your CyberArk representative. The following instructions show you how to install it.

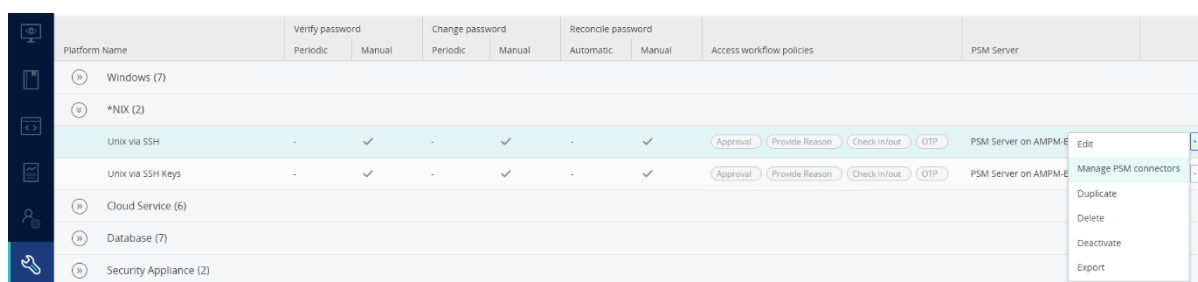
Installing the Forescout 9.1.3 PSM Universal Connector

1. Copy the following files from the installation package to the specified subfolder of the **Privileged Session Manager** installation folder on the PSM machine:

- In the 'components' folder:
ForescoutConsole9_1_3Dispatcher.exe

Import Connection Component (Supported in v12+)

1. In PVWA go to Administration → Options → Platform Management (New UI)
2. Select the platform you are going to add the Connection Component
3. Click on the configuration menu to the far right of the platform row
4. Select "Manage PSM connectors" from the list of options



5. Do one of the following:
 - Click "Connector package Drag & drop or browse" → Find the CC .zip package and click "Open"
 - Drag and drop the CC .zip package into the "Connector package Drag & drop or browse" box.
6. Once imported the CC will automatically be added to the platform you have selected though will be an option within the "Manage PSM connectors" menu for all other platforms.

Create the Connection Component (non v12+ environments)

1. In PVWA go to Administration → Options → Connection Components
2. Select the connection component named "PSM-VNCCClientSample", right-click it and select copy
3. Right-click on "Connection Components" and paste
4. Rename the newly created component by setting "Id" to "PSM-Forescout-9.1.3"



5. Under the new connection component:
 - Modify the configurations mentioned below within “Connection Component Settings” at the relevant/specified configuration level.
6. Click “OK” to save

Configuration

Connection Component Settings

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 Reference
Acceptable Values	String
Default Value	PSM-Forescout-9.1.3

Parameter Name	DisplayName
Description	The name to be displayed in the connection selection. ("click to connect" drop-down on the account view) Reference
Acceptable Values	String
Default Value	Forescout 9.1.3

Target Settings Section

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

Parameter Name	ClientDispatcher
Description	The launcher / automation client that will open the target connection.
Acceptable Values	Path Placeholders are acceptable
Default Value	"{PSMComponentsFolder}\ForescoutConsole9_1_3Dispatcher.exe" "{PSMComponentsFolder}"

Target Settings → Client Specific



Parameter Name	ClientPath
Description	The full path of the target application folder located on the PSM Server.
Acceptable Values	Path Placeholders are acceptable
Default Value	C:\Program Files (x86)\Forescout Console 9.1.3\GuiManager\current

Target Settings → Lock Application Window

Parameter Name	Enable
Description	Whether or not the application window will be locked.
Acceptable Values	Yes, No
Default Value	No

Add the connection component to a platform(non v12+ environments)

1. Go to Administration → Platform Management
2. Select the platform for which you would like to use this connector
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 newly created “Connection Component” to “PSM-Forescout-9.1.3” (update Id field)
6. Click “OK” to save
7. On the PSM server – restart the service “CyberArk Privileged Session Manager” (or wait for several minutes)



Appendix A : Configure AppLocker

If your PSM server is hardened, you will need to make the following configurations in order for Forescout-9.1.3 executable to be excluded from the AppLocker rules:

1. Open Powershell as Administrator from C:\Program Files (x86)\CyberArk\PSM\Hardening
2. Run notepad PSMConfigureAppLocker.xml
3. Towards the end of the PSMConfigureAppLocker.xml file, before the `</AllowedApplications>` tag, add the following lines:

```
<Application Name="Forescout-9.1.3" Type="Exe" Path="Path to Forescout-9.1.3" Method="Hash" />
```

If Forescout-9.1.3 uses Java then also add the following:

```
<Application Name="Java32" Type="Exe" Path="C:\Program Files (x86)\Java\<your installed JRE version>\bin\java.exe" Method="Hash" />

<Application Name="Java64" Type="Exe" Path="C:\Program Files\Java\<your installed JRE version>\bin\java.exe" Method="Hash" />

<Application Name="JavaWS32" Type="Exe" Path="C:\Program Files (x86)\Java\<your installed JRE version>\bin\javaws.exe" Method="Hash" />

<Application Name="JavaWS64" Type="Exe" Path="C:\Program Files\Java\<your installed JRE version>\bin\javaws.exe" Method="Hash" />
```

Possible extra application to allow (depends on specific java web application requirements):

```
<Application Name="JavaLauncher32" Type="Exe" Path="C:\Program Files (x86)\Java\<your installed JRE version>\bin\jp2launcher.exe" Method="Hash" />

<Application Name="JavaLauncher64" Type="Exe" Path="C:\Program Files\Java\<your installed JRE version>\bin\jp2launcher.exe" Method="Hash" />
```

Anytime the Java Runtime Environment is updated on the PSM server, you will need to update this AppLocker file to have updated JRE version values in the file path. Then re-run the PSMConfigureAppLocker.ps1 script to have the new hashes updated. It's also possible to enable AppLocker to whitelist a more generic path instead of individual file hashes. However, this is unadvisable as there are other Java executables that would be included under this path which reduces overall security posture.

4. In the same Powershell window run PSMConfigureAppLocker.ps1

