

RealVNC Client

Privileged Session Management (PSM)

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.

Connecting to RealVNC Client via PSM

The Privileged Session Manager enables organizations to securely launch sessions to remote target systems through controlled, isolated connections, with credentials retrieved from the Enterprise Password Vault and injected without exposing them to the end user. This connector supports the automated launch of the **RealVNC Client** and the secure handling of credential entry during session establishment.

Prerequisite

This PSM Connection Component requires AutoIt3 to be installed on the PSM machine.

Available here: <https://www.autoitscript.com/autoit3/files/archive/autoit/>

The connector requires the correct version of AutoIt3 installed on the PSM server – **3.3.16.1** (or higher)

The RealVNC Client PSM Connector now supports the following **Authentication Types**:

Single sign-on (SSO)

- Windows Domain user (RunAs)
- *Requires adding additional settings to the connector defaults.*
 - o *Carefully read the instructions below. ***

Windows Password (win) = Windows user credentials

- *Windows Local or Windows Domain accounts authorized to connect to the target RealVNC server*

VNC Password (password) = RealVNC Password Authentication.

- o *(Local target VNC host password)*

If using **VNC Password (password)**, the *Real VNC Type* is derived from the *Username* attribute.

(Refer to the corresponding CPM plug-in documentation for more details.)

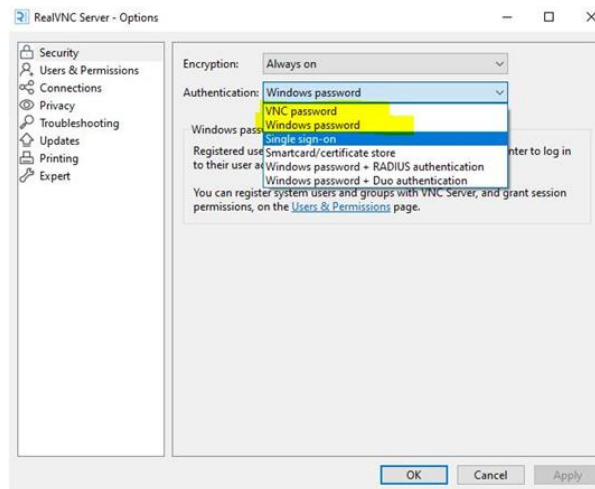
The following VNC Password Types are supported:

‘Password’ default VNC password

‘AdminPassword’ administrative user able to bypass accept/reject prompts.

‘ViewOnlyPassword’ password for a basic user able to observe but not interact.

On the target VNC server (Target host), verify the server authentication setting is compatible with this connection component:



Legacy VNC server targets:

If the target (Non-RealVNC) VNC Server uses the legacy VNC protocol and password, this PSM connector can be used with the corresponding "[RealVNC Server Local Passwords](#)" CPM plugin as long as the target VNC account object is *unmanaged*.

Legacy VNC Passwords that are not RealVNC cannot be managed by the CyberArk Marketplace "[RealVNC Server Local Passwords](#)" CPM plugin; However, the platform provides the required account attributes / File Categories required by this PSM connection component for this type of unmanaged password.

The RealVNC Client PSM connector does **not** support the use of any of the following:

- Multi-Window Mode / Multi-Monitor Support
- RealVNC 'virtual mode' credentials
- RealVNC SmartCard Authentication
- RealVNC with Radius or MFA Authentication
- GuestPassword
- Weakpwd

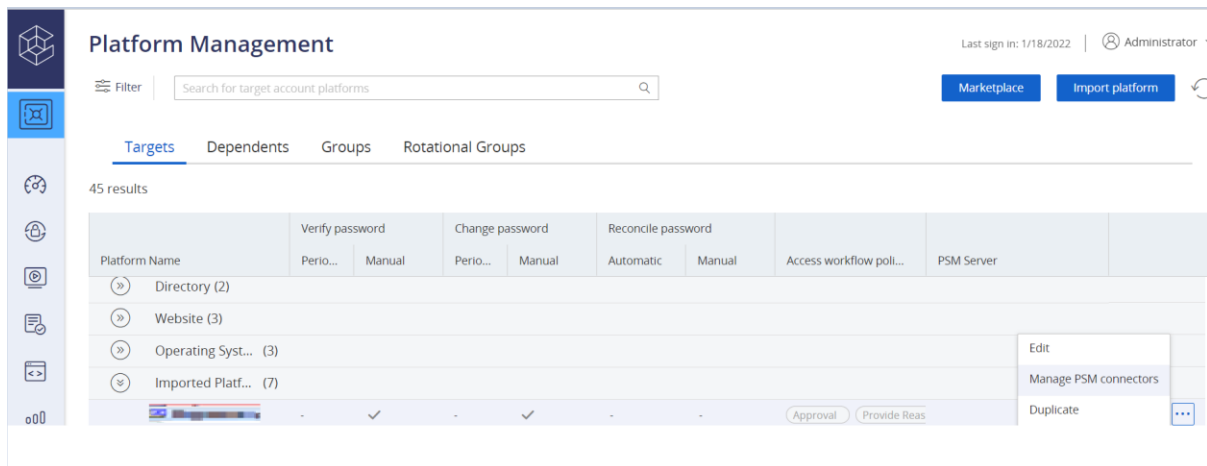
```
-weakpwd Permit the setting of a weak password (less than 6 characters).
          Not recommended.
```

Installation

You will receive the CC-PSMRealVNCClient-v1.5.zip archive from your CyberArk representative. The following instructions show you how to install it.

V12 or above:

1. Navigate and authenticate to the PVWA Web UI as an admin user.
2. Go to the PVWA → Administration → Platform Management. Select the necessary platform, select the 3 dots (on the right) and 'Management PSM connectors'



3. Select the preferred PSM Server and click 'Next'.
4. Drag and drop **CC-PSMRealVNCClient-v1.5.zip**

Manage PSM connectors

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

☐ Show only selected connectors (0)

 Connector package
Drag & drop or browse

A1000 Malware Analysis

Configuration

PVWA UI Admin → Configuration → Options → Configurations → Connection Components → **PSM-RealVNC715**

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-RealVNC715

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	RealVNC Client v7.15.1

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

Parameter Name	ClientDispatcher
Description	The launcher / automation client that will open the target connection.
Acceptable Values	"{PSMComponentsFolder}\PSMRealVNCClientDispatcher.exe" "{PSMComponentsFolder}"

Parameter Name	ConnectionComponentInitTimeout
Description	Time allowed for the connection component to initialize, in milliseconds. 0 means infinitely.
Acceptable Values	Positive integer in milliseconds
Default Value	60000

Target Settings section

Target Settings → Client Specific

Parameter Name	ExeFullPath
Description	The full path of where the target application exe file is located on the PSM Server.
Acceptable Values	Path
Default Value	C:\Program Files\RealVNC\VNC Viewer\vncviewer.exe

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

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 (Legacy)

If the connection component wasn't added using the instructions in the section above:

Installation 12 *xor above*, the legacy method for adding the connector to a platform is detailed below:

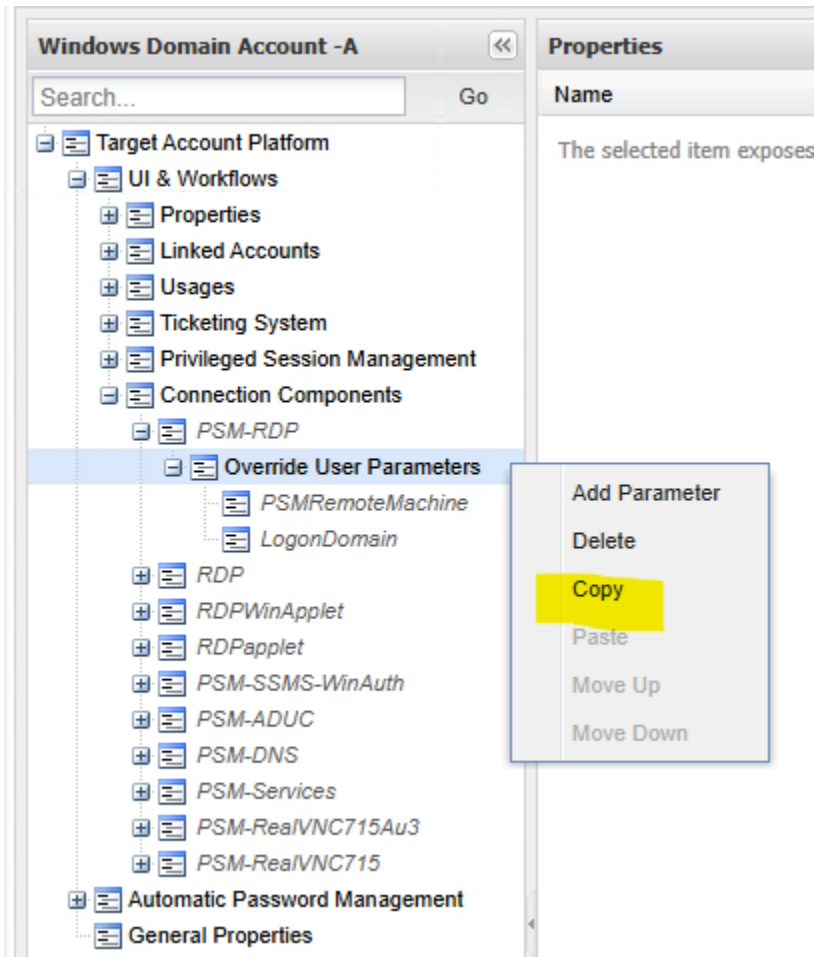
1. Go to Administration → Platform Management
2. Select the platform you would like to add this connector to
3. Click “Edit”
4. Go to “UI & Workflows” →
 - Right-click → “Add Privileged Session Management” (it may be grayed out if the platform already has it configured)
 - If there is no “Connection Components” then Right-click → “Add Connection Components”
 - “Connection Components” → Add Connection Component
5. Rename the newly created “Connection Component” to “PSM-RealVNC715” (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)

Edit the connection component platform settings:

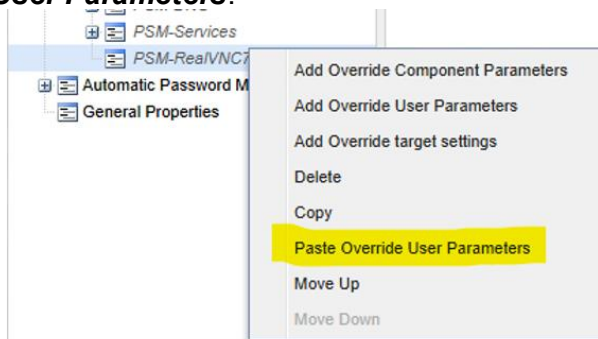
1. Go to Administration → Platform Management
2. Select the target platform you added this connector to
3. Click “Edit”

Windows Domain / SSO platforms:

1. Go to “UI & Workflows” → “Connection Components” → “PSM-RDP”
2. **Right click** and **Copy** the **Override User Parameters** from the default PSM-RDP connection component:



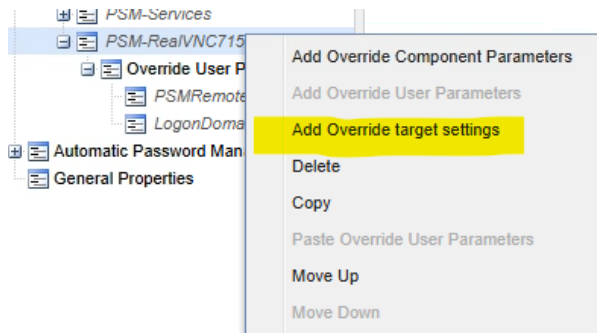
3. **Right click** on the **PSM-RealVNC715** Connection Component and Paste the **Override User Parameters**.



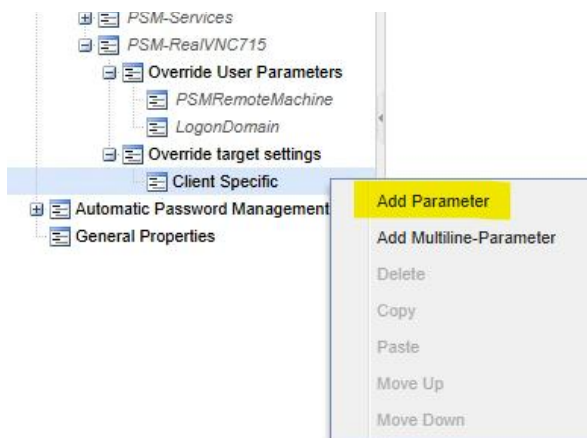
4. (Continue with the instructions below)

All Platform types:

1. **Right click on the PSM-RealVNC715 Connection Component select 'Add Override target settings'**



2. Expand the new **Override target settings**
3. **Right click Client Specific**
4. Select **Add Parameter**



Windows Local and Windows Domain platforms:

Add new parameter **"AuthType"** with value **"win"**

Properties	
Name	Value
• Name	AuthType
• Value	win

SSO platforms:

Add new parameter **"AuthType"** with value **"sso"**

RealVNC (local / password) or other VNC platforms:

Add new parameter **"AuthType"** with value **"password"**

5. **Click OK to save the platform changes.**
6. Wait for the PSM configuration file update / refresh interval to pass. *10 minutes by default.*

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/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/Configure_Applocker.htm