

CyberArk Privilege Cloud configuration

XM SCM Docs

Table of Contents

Tool information	4
Configuring CyberArk Privilege Cloud with XM SCM	5
Preparing CyberArk Privilege Cloud prerequisites.....	6
Connecting CyberArk Privilege Cloud to SCM	7
Adding a tool to the tool list	8
Connecting a tool to SCM.....	8
Noteworthy CSCs	9

- [Tool information](#)
- [Configuring CyberArk Privilege Cloud with XM SCM](#)
- [Preparing CyberArk Privilege Cloud prerequisites](#)
- [Connecting CyberArk Privilege Cloud to SCM](#)
- [Noteworthy CSCs](#)

Tool information

Here is updated information about the CyberArk Privilege Cloud tool:

- **Tool name:** CyberArk Privilege Cloud
- **Catalog number:** XM-SSPM-2-036
- **Applicable for Core release:** 5.1.1
- **Release date:** 22 May 2025

Configuring CyberArk Privilege Cloud with XM SCM

This procedure describes how to configure CyberArk Privilege Cloud with SCM so that you can manage your CyberArk Privilege Cloud CSCs.

1. [Prepare the CyberArk Privilege Cloud prerequisites.](#)
2. [Connect CyberArk Privilege Cloud to SCM.](#)
3. [Set up the plugin and its parameters.](#)

Preparing CyberArk Privilege Cloud prerequisites

Creating an ISPSS service account

This procedure describes how to create an ISPSS service account, which you need to do to connect CyberArk Privilege Cloud to SCM.

1. In the Identity Administration portal, click **Core Services > Users** and click **Add user**.
2. Enter login credentials and save them for later. The user must have the following checked under **Status**:
 - **Is OAuth confidential client**
 - **Is service user**
 - **Password never expires**
3. Click **Create user**.
4. Click **Core services > Roles**.
5. Click the **SCAApiReadOnly** role, click **Member > Add**, and add the newly created user.
6. Click the **Privilege Cloud Auditors** role, click **Member > Add**, and add the newly created user.

Connecting CyberArk Privilege Cloud to SCM

This procedure describes how to add CyberArk Privilege Cloud to the tool list and start pulling data to the SCM platform.

- ✓ Make sure you have the following from the [Prerequisites](#) above:
 - Authentication URL
 - Username and password for the user you created

Adding a tool to the tool list

1. Log in to SCM as an admin.
2. On the left side, click **System > Tools configuration**.
3. On the top right, click **+ Add tool**.
4. Click the relevant tab (for on-prem tools: **OSPM**, for cloud tools: **SSPM**) and select the relevant information.
5. Click **Save**.
6. In the list of tools, click the tool you just created.
7. In the **General** tab, select **System active** and click **Apply changes**.

The screenshot shows the 'General' tab of a tool configuration page. The interface includes several input fields and checkboxes. The 'System active' checkbox is highlighted with a red circle. Below the form, there are buttons for 'Info', 'Duplicate tool', 'Collect now', 'Clear changes', and 'Apply changes'.

Name	Vendor name	CSC version
[Redacted]	[Redacted]	4.0.0

Tool target score: [Redacted]

Virtual tool: No

Poll interval*: Every 55 minutes ⚙️

Tickets recipients ⓘ
Examples: mail@mail.com, snu:user, sng:group ...

☒ System active ☐ Sequential collect ⓘ

Buttons: Info, Duplicate tool, Collect now, Clear changes, Apply changes

Connecting a tool to SCM

After adding the tool to the tool list, you need to create a database and activate the plugin to start pulling data to SCM by using the following procedure.

1. In the **Datasource** tab, expand the row with the database.
2. In **Database**, enter a name for the database, select **Create database**, and click **Save**.
3. In the **Plugins** tab, expand the plugin and click **Set parameters**.
4. In the **Plugin parameters** dialog box, enter the information you got earlier.
5. Click **Save**.
6. Back in the **Plugins** tab, click **Save**.

You can now pull data to SCM by clicking  (execute) at the end of the row. It may take a few minutes to finish pulling all the data.

Noteworthy CSCs

Due to the information the CyberArk API sends, these CSCs always trigger alerts. You should suppress data you know is irrelevant from these controls.

- Active Target platforms where the 'Perform Periodic Verification' set to 'No'
- Active Target platforms where the 'Allow Manual Reconciliation' set to 'No'
- Active Target platforms where the 'Automatic Reconcile When Unsynced' set to 'No'
- Active Target Platforms where the 'Require Privileged Session Monitoring And Isolation' set to 'No'
- Active Target Platforms where the 'Record And Save Session Activity' set to 'No'
- Active Target Platforms where the 'Require Dual Control Password Access Approval' set to 'No'
- Active Target Platforms where the 'Enforce One time Password Access' set to 'No'
- Active Target Platforms where the 'Require Users To Specify Reason For Access' set to 'No'
- Active Target platforms where the Password Change for 'Perform Automatic Periodic Change' set to 'No'
- Active Target Platforms where the 'Require Password Verification Every XDays' set to Higher than 7 days