

Veritas Appliance Guide for CyberArk Plugin Configuration

Document Version 6

Cohesity™ Appliance Setup for CyberArk™ Plugins

Last updated: 2026-01-14

Legal Notice

Copyright © 2026 Cohesity, Inc. All rights reserved.

© 2026 Cohesity, Inc. All Rights Reserved. Cohesity, the Cohesity Logo and other Cohesity Marks are trademarks of Cohesity, Inc. in the US and/or internationally. The information supplied herein is the confidential and proprietary information of Cohesity and may only be used (a) by the intended recipients and (b) in conjunction with validly licensed Cohesity software and services. Find the terms of Cohesity licenses at www.cohesity.com/agreements.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. COHESITY SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

<https://www.veritas.com/support>

You can manage your Cohesity account information at the following URL:

<https://my.veritas.com>

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Cohesity website.

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Cohesity website.

Cohesity Services and Operations Readiness Tools (SORT)

Cohesity Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1	Introduction	5
	Overview	5
Chapter 2	CyberArk plugin configurations for Flex Appliance	7
	Veritas Flex Appliance Console CPM (GEN1)	7
	Veritas Flex Appliance Console CPM GEN2	9
	Veritas Flex Appliance Shell CPM	12
	Veritas Flex Appliance Primary and Media Instance CPM	13
	Veritas Flex Appliance WORM Instance CPM	15
	Veritas Flex Appliance Console PSM	16
Chapter 3	CyberArk plugin configuration for NetBackup Appliance	19
	Veritas NetBackup Appliance CPM CyberArk Plugin	19
Chapter 4	CyberArk plugin for Remote Management interface	23
	Veritas Remote Management Interface via API CyberArk Plugin	23
Chapter 5	CyberArk plugin configurations for Flex Scale and Access Appliances	26
	Veritas NetBackup Flex Scale and Access Appliance API CyberArk CPM plug-in	26
	Configuration for CyberArk Privileged Session Manager (PSM) for SSH	28

Introduction

This chapter includes the following topics:

- [Overview](#)

Overview

CyberArk is an identity security company that specializes in privileged access management. With the CyberArk application, you can manage user login credentials with the following features:

- Set up password policies.
- Change passwords.
- Reconcile passwords.
- Rotate passwords.

Through the CyberArk application, you can install and configure CyberArk plugins for use with specific Veritas appliances. Each plugin is unique to the appliance platform and the access that you want to allow various users. The following Veritas appliance platforms are supported:

- Veritas Access Appliance
- Veritas Flex Appliance
- Veritas NetBackup Flex Scale Appliance
- Veritas NetBackup Appliance

All installation and configuration takes place in the CyberArk application on their website. CyberArk provides all plugin installation instructions.

About this document

Once you have installed the appropriate plugin for the specific appliance platform, use this document to configure the plugin. The configuration for each plugin is unique. This document provides individual configuration procedures for each plugin.

Note: CyberArk provides instructions for post-configuration operations such as connecting and changing passwords.

About known issues

The following document link describes the currently known issues for all Veritas supported CyberArk plugins:

https://www.veritas.com/support/en_US/article.100066817

https://veritas.com/internal-search/en_US/article.100066817.html

Each listed issue includes a description of the issue, the cause, and how to resolve or work around the issue. For any solution that describes a workaround, check this document periodically to see if a plugin update is available to resolve the issue.

CyberArk plugin configurations for Flex Appliance

This chapter includes the following topics:

- [Veritas Flex Appliance Console CPM \(GEN1\)](#)
- [Veritas Flex Appliance Console CPM GEN2](#)
- [Veritas Flex Appliance Shell CPM](#)
- [Veritas Flex Appliance Primary and Media Instance CPM](#)
- [Veritas Flex Appliance WORM Instance CPM](#)
- [Veritas Flex Appliance Console PSM](#)

Veritas Flex Appliance Console CPM (GEN1)

[Updated plugin; version 1.5]

The Veritas Flex Appliance Console CPM (GEN1) plugin is a CyberArk component. The plugin integrates the Flex Appliance web user interface with CyberArk and lets you manage the Flex Appliance Web Console administrator accounts. It includes the default administrator account along with other configured administrator user accounts with the Web console. The plugin enables the automation to secure privileged access by storing and retrieving privileged Flex admin accounts in the CyberArk password vault.

Note: This GEN1 plugin version is compatible only with Flex Appliance software versions 3.x and 4.x. If you have upgraded a Flex Appliance to version 5.x or later that currently uses this GEN1 plugin version, you must also upgrade the plugin to the GEN2 version. For plugin upgrade details, see the following topic: [Veritas Flex Appliance Console CPM GEN2](#)

The following describes the supported plugin functionality:

- Change the administrator account password.
- Verify the administrator account password.
- Limitations:
 - Reconciliation is not supported.

Requirements and prerequisites

The following describes the requirements and tasks that you must perform before you can configure the plugin:

- A configured Flex Appliance with versions 3.x or 4.x with a web interface configured.
- A CyberArk PAM (Privileged Access Manager) solution.
- Download the Veritas Flex Appliance API CPM Plugin from the following CyberArk Marketplace site and install it:
<https://cyberark.my.site.com/mplace/s/#a352J000001I69RQAS-a392J000001og4pQAA>

Configuration

After you have downloaded and installed the plugin, perform the following configuration steps in the application on the CyberArk site.

To configure the plugin for a Flex Appliance administrator account

- 1 Log in to the CyberArk PVWA.
- 2 On the **Account View** page, click **Add account** and do the following:
 - For **Select system type**, click **Imported platforms**.
 - For **Assign to platform**, click **Veritas Flex Appliance Console CPM GEN1**.
 - For **Store in safe**, select where you want to store the configuration. You can also click **Create Safe** to create a new one.
 - For **Define properties**, enter the following:
 - **Address:** Enter the Flex Appliance fully qualified domain name.

- **Username:** Enter the Flex Appliance administrator account username.
 - **Password:** Enter the associated password for the entered Flex Appliance administrator account username.
- 3 For Flex Appliance configurations, add a second user account as described in step 2 as follows:
- For appliances with software versions 3.x, you must add the default administrator user account.
 - For appliances with software versions 4.x, you must add a security administrator user account.
- 4 After adding the second account, associate it with the first account that you added in step 2 as follows:
- In the left column on the **Accounts View** page, select the **Username** that you first added in step 2, then on the right side of the page click **Additional details & actions in classic interface**.
 - When the **Associate Account** dialog appears, select the second user account that you created and click **Associate** to link it with the first user account.

The plugin is designed for use with an SSL certificate. If the target appliance uses a self-signed certificate, you must reconfigure the plugin to use that certificate type as follows:

To reconfigure the plugin to use a self-signed certificate

- 1 Log in to the CyberArk PVWA.
- 2 Navigate to the **Platform Management** page and do the following:
 - Click the platform named **Veritas Flex Appliance API via REST**.
 - On the lower right side, click **Edit**.
 - In the left column, expand **Automatic Password Management** and click **Additional Policy Settings**.
 - In the **Properties** column, click **Use SSL**. Then, in the **Value** column, right-click on **Yes** and select **IgnoreUntrustedCertificate**.

Veritas Flex Appliance Console CPM GEN2

[New plugin; version 1.0]

The Veritas Flex Appliance Console CPM GEN2 plugin is a CyberArk component. The plugin integrates the Flex Appliance web user interface with CyberArk and lets

you manage the Flex Appliance Web Console administrator accounts. It includes the default administrator account along with other configured administrator user accounts with the Web console. The plugin enables the automation to secure privileged access by storing and retrieving privileged Flex admin accounts in the CyberArk password vault.

Note: This GEN2 plugin version is compatible only with Flex Appliance software version 5.x or later. If you have upgraded a Flex Appliance to version 5.x or later that currently uses the GEN1 plugin version, you must also upgrade the plugin to this GEN2 version. For plugin upgrade details, see the section [Upgrade plugin from GEN1 to GEN2 version](#).

The following describes the supported plugin functionality:

- Change the administrator account password.
- Verify the administrator account password.
- Limitations:
 - Reconciliation is not supported.
 - The Flex service account user is not supported by CyberArk.

Requirements and prerequisites

The following describes the requirements and tasks that you must perform before you can configure the plugin:

- A configured Flex Appliance on a compatible version. See the following article for the list of supported versions:
[CyberArk Support for Veritas Appliances](#)
- A CyberArk PAM (Privileged Access Manager) solution.
- Download the Veritas Flex Appliance API CPM Plugin from the following CyberArk Marketplace site and install it:
<https://cyberark.my.site.com/mplace/s/--Veritas>

Configuration

After you have downloaded and installed the plugin, perform the following configuration steps in the application on the CyberArk site.

Note: Use this procedure only to configure the GEN2 plugin version for new Flex Appliance 5.x or later installations.

To configure the plugin for a Flex Appliance administrator account

- 1 Log in to the CyberArk PVWA.
- 2 On the **Account View** page, click **Add account** and do the following:
 - For **Select system type**, click **Imported platforms**.
 - For **Assign to platform**, click **Veritas Flex Appliance Console CPM GEN2**.
 - For **Store in safe**, select where you want to store the configuration. You can also click **Create Safe** to create a new one.
 - For **Define properties**, enter the following:
 - **Address**: Enter the Flex Appliance fully qualified domain name.
 - **Username**: Enter the Flex Appliance administrator account username.
 - **Password**: Enter the associated password for the entered Flex Appliance administrator account username.

Upgrade plugin from GEN1 to GEN2 version

Use this procedure only for a Flex Appliance that has been upgraded from versions 3.x or 4.x to version 5.x or later.

To upgrade users from the GEN1 platform to the GEN2 platform, there is no need to recreate the users in CyberArk. CyberArk provides the ability to change platforms. Whenever a Flex Appliance is upgraded to version 5.x or later, you must also upgrade those existing appliance users to the GEN2 platform.

Note the following when upgrading to the GEN2 platform:

- Linked-Account Security Admin is not required for the Veritas Flex Appliance Console CPM GEN2 platform. If Linked-Account Security Admin was set previously for the GEN1 platform, the GEN2 platform ignores it.
- During the change of platforms, it is not necessary to clear the Linked-Account.
- You must upgrade the platform for each user account.

To upgrade the plugin from GEN1 to the GEN2 version

- 1 Log in to the CyberArk PVWA.
- 2 On the **Accounts View** page, locate the Flex Appliance user account and click **Edit**.
- 3 Change the platform for the selected user as follows:
 - On the **Edit Account** page, click the checkmark next to **Assigned to Platform**.

- Change the platform by selecting **Veritas Flex Appliance Console via API GEN2**.
 - When the **Change platform** popup appears, click **Change**.
 - Click **Save**.
- 4 Return to the **Accounts View** page to verify that **VeritasFlexApplianceAPIGEN2** appears in the **Platform ID** column.

The plugin is designed for use with an SSL certificate. If the target appliance uses a self-signed certificate, you must reconfigure the plugin to use that certificate type as follows:

To reconfigure the plugin to use a self-signed certificate

- 1 Log in to the CyberArk PVWA.
- 2 Navigate to the **Platform Management** page and do the following:
 - Click the platform named **Veritas Flex Appliance API via REST**.
 - On the lower right side, click **Edit**.
 - In the left column, expand **Automatic Password Management** and click **Additional Policy Settings**.
 - In the **Properties** column, click **Use SSL**. Then, in the **Value** column, right-click on **Yes** and select **IgnoreUntrustedCertificate**.

Veritas Flex Appliance Shell CPM

[Updated plugin; version 1.2]

The Veritas Flex Appliance Shell CPM plugin is a CyberArk component. The plugin provides a solution to manage the password of all Flex shell user accounts on a configured Flex Appliance.

The following describes the supported plugin functionality:

- Change the host admin account password.
- Verify the host admin account password.
- Starting with plugin version 1.1, the plugin supports password updates/changes for user accounts with an expired password.
- Limitations:
 - This plugin only supports the configured host admin accounts on a Flex appliance.
 - This plugin does not support to reconcile the host admin account password.

Requirements and prerequisites

The following describes the requirements and tasks that you must perform before you can configure the plugin:

- A configured Flex Appliance on a compatible version. See the following article for the list of supported versions:
[CyberArk Support for Veritas Appliances](#)
- A CyberArk PAM (Privileged Access Manager) solution.
- Download the plugin from the following CyberArk Marketplace site and install it:
<https://cyberark-customers.force.com/mplace/s/##a352J000000rgi7QAA-a392J000001jYe9QAE>

Configuration

After you have downloaded and installed the plugin, perform the following configuration steps in the application on the CyberArk site.

To configure the plugin for a Flex Appliance host admin account

- 1 Log in to the CyberArk PVWA.
- 2 On the **Account View** page, click **Add account** and do the following:
 - For **Select system type**, click **Imported platforms**.
 - For **Assign to platform**, click **Veritas Flex Appliance Shell via SSH**.
 - For **Store in safe**, select where you want to store the configuration. You can also click **Create Safe** to create a new one.
 - For **Define properties**, enter the following:
 - **Address**: Enter the Flex Appliance fully qualified domain name.
 - **Username**: Enter the Flex Appliance host admin account username.
 - **Password**: Enter the associated password for the entered Flex Appliance host admin account username.

Veritas Flex Appliance Primary and Media Instance CPM

[Updated plugin; version 1.1]

The Veritas Flex Appliance Primary and Media Instance CPM is a CyberArk plugin component. It provides a solution to manage the password of a primary or media user instance of a configured NetBackup server on a Flex Appliance.

The following describes the supported plugin functionality:

- Change the user account password.
- Verify the user account password.
- Reconcile the user account password, when necessary.
- Limitation:
Support assistance is required to enable the reconcile feature for this plugin.
Contact Veritas Technical Support and refer them to article number 100056201.

Prerequisites and requirements

The following describes the requirements and tasks that you must perform before you can configure the plugin:

- A configured NetBackup instance on a compatible version. See the following article for the list of supported versions:
[CyberArk Support for Veritas Appliances](#)
- A CyberArk PAM (Privileged Access Manager) solution.

Configuration

After you have downloaded and installed the plugin, perform the following configuration steps in the application on the CyberArk site.

To configure the plugin for a Flex Primary or Media Instance via SSH

- 1 Log in to the CyberArk PVWA.
- 2 On the **Account View** page, click **Add account** and do the following:
 - For **Select system type**, click **Imported platforms**.
 - For **Assign to platform**, click **Veritas Flex Primary or Media Instance via SSH**.
 - For **Store in safe**, select where you want to store the configuration. You can also click **Create Safe** to create a new one.
 - For **Define properties**, enter the following:
 - **Address**: Enter the Flex Appliance fully qualified domain name.
 - **Username**: Enter the NetBackup username.
 - **Password**: Enter the associated password for the entered NetBackup username.

Veritas Flex Appliance WORM Instance CPM

[Updated plugin; version 1.1]

The Veritas Flex Appliance WORM Instance CPM is a CyberArk plugin component. It supports password verification and change for the built-in msdpadm and MSDP user (non-msdpadm) login accounts configured on a WORM instance.

Requirements and prerequisites

The following describes the requirements and tasks that you must perform before you can configure the plugin:

- A configured WORM instance on a compatible version. See the following article for the list of supported versions:
[CyberArk Support for Veritas Appliances](#)
- A CyberArk PAM (Privileged Access Manager) solution.
- Download the Veritas Flex Appliance WORM Instance CPM plugin from the following CyberArk Marketplace site and install it:
<https://cyberark-customers.force.com/mplace/s/#a35Ht000000rtwZIAQ-a39Ht000003SejFIAS>
- Limitations:
 - Although the **Reconcile** option is available with this plugin, this functionality is not supported. Password change restrictions for the msdpadm and MSDP user accounts on a WORM instance prevent reconciliation. Any attempt to use the **Reconcile** option fails and displays an error message.
 - To change the passwords for MSDP user accounts, you must associate the built-in msdpadm account as the Instance Administrator Account for each of the configured MSDP user accounts in CyberArk. The "Association" section describes the procedure.

Configuration

After you have downloaded and installed the plugin, perform the following configuration steps in the application on the CyberArk site.

Note: You can use this procedure to configure either msdpadm or MSDP users that are configured on WORM instances.

To configure the plugin for a Flex Appliance WORM Instance to manage msdpadm or MSDP users

- 1 Log in to the CyberArk PVWA.
- 2 On the **Account View** page, click **Add account** and do the following:

- For **Select system type**, click **Imported platforms**.
- For **Assign to platform**, click **Veritas Flex Appliance WORM Instance via SSH**.
- For **Store in safe**, select where you want to store the configuration. You can also click **Create Safe** to create a new one.
- For **Define properties**, enter the following:
 - **Address**: Enter the Flex Appliance fully qualified domain name.
 - **Username**: Enter the msdpadm or MSDP username.
 - **Password**: Enter the associated password for the entered msdpadm or MSDP username.

Association

After you have added any MSDP user accounts, you must associate each one with the built-in msdpadm account as the Instance Administrator Account. This task is required as it enables you to verify and change the passwords for MSDP user accounts.

To associate the built-in msdpadm account as the Instance Administrator Account for a configured MSDP user account

- 1 On the **Accounts View** page:
 - On the left side of the page, select the appropriate msdp user account.
 - On the upper right side of the page, click **Select Additional details & actions in classic interface**.
- 2 On the **Account Details** page, on the upper right side of the page, click **Associate** for the **Instance Administrator Account**.

Veritas Flex Appliance Console PSM

The Veritas Flex Appliance Console PSM is a CyberArk plugin component. The plugin enables you to initiate, monitor, and record privileged login sessions, and usage of administrative and user accounts for the web user passwords that are stored in a CyberArk password vault. A Remote Desktop connection starts up in Windows and records the entire session.

Requirements and prerequisites

The following describes the requirements and tasks that you must perform before you can configure the plugin:

- A configured Flex Appliance on a compatible version. See the following article for the list of supported versions:
[CyberArk Support for Veritas Appliances](#)
- A standard CyberArk Marketplace account to download the plugin.
- A CyberArk PAM (Privileged Access Manager) solution.
- Download the Veritas Flex Appliance Console PSM Plugin from the following CyberArk Marketplace site and install it:
<https://cyberark-customers.force.com/mplace/s/#a352J000001169RQAS-a392J000001og4pQAA>
- Limitations:
For the best experience and to avoid errors on the CyberArk website, use Google Chrome version 109.0.5414.129 (64-bit).

Architecture

The PSM uses the password from a vault for the user logons. A Remote Desktop Session is invoked to log in. The login is fully automatic as it matches the form elements in the Web UI login and then clicks on **Login**. The architecture uses the standard CyberArk architecture where it records the sessions that are stored in the vault.

Configuration

After you have downloaded and installed the plugin, perform the following configuration steps in the application on the CyberArk site.

To configure the plugin for a Flex Appliance with a configured web interface

- 1 Log in to the CyberArk PVWA and verify that the **Record and save session activity** is **Active**, as follows:
 - After logging in, on the left side of the main page, click the **Policies** icon, then click **Policies > Master Policy**.
 - In the **Master Policy** window, click the arrow next to **Session Management** to expand it and verify that **Record and save session activity** is **Active**.
 - If it is not active, on the lower right of the window, click **Edit Settings** and change it to **Active**.
- 2 Verify that the IP address of the PSM server you want to connect to is correct, as follows:
 - On the left side of the main page, click the **Administration** icon, then click **Configuration Options > Options**.

- In the left column of the **Options** window, expand **Privileged Session Management > Configured PSM Servers > Connection Details > Servers** to verify the IP address.
- 3** Set the **EnforceCertificateValidation** option to **No**, as follows:
- In the left column of the **Options** window, expand **Connection Components**.
 - Scroll down and expand **PSM-VeritasFlexApplianceWeb > Target Settings > Web Form Settings**.
 - In the **Properties** section, in the **Value** column, set **EnforceCertificateValidation** to **No**, then click **Apply**.
- 4** Add the ID value of **PSM-VeritasFlexApplianceWeb** as a connection component, as follows:
- In the left column of the **Options** window, scroll down and click **PSM-VeritasFlexApplianceWeb**.
 - In the **Properties** section, in the first row for the ID, click and drag to highlight the ID in the **Value** column, then right-click and select **Copy**.
 - On the left side of the main page, click the **Administration** icon, then click **Platform Management > Veritas Flex Appliance API Via REST > Edit**.
 - Click on the following elements in the order as shown:
 Right click on **UI & Workflows** and select **Add Privileged Session Management**.
 Right click again on **UI & Workflows** and select **Add Connection Components**.
 Right click on **Connection Components** and select **Add Connection Component**.
 Paste the ID content, then click **Apply** and **OK**.
- 5** Restart the Cyber-Ark Privileged Session Manager as follows:
- Navigate to **Services [Local]**, right-click on **Cyber-Ark Privileged Session Manager** and select **Restart**.

CyberArk plugin configuration for NetBackup Appliance

This chapter includes the following topics:

- [Veritas NetBackup Appliance CPM CyberArk Plugin](#)

Veritas NetBackup Appliance CPM CyberArk Plugin

The Veritas NetBackup Appliance CPM Plugin is a CyberArk component. It supports password management for the built-in administrator and maintenance users along with verification, change, and reconciliation for all standard local user login accounts existing on a Veritas NetBackup Appliance.

The following describes the supported plugin functionality:

- Verify the administrator or the maintenance user password.
- Change the following account passwords:
 - Administrator (built-in admin user and other user accounts with administrator privileges)
 - Maintenance user
 - NetBackup CLI users
 - Standard local users (such as nbasecadmin)
- Reconcile the user password, when necessary.

- **Limitation:**
The reconcile feature requires that you first add the appliance maintenance user account to CyberArk, and then associate it with an appliance administrator account. After completing the plugin configuration procedure, see the following:
See [the section called “Enable reconciliation”](#) on page 20.

Requirements and prerequisites

The following describes the requirements and tasks that you must perform before you can configure the plugin:

- A configured NetBackup Appliance with software versions 3.3.x or later.
- A CyberArk PAM (Privileged Access Manager) solution.
- Download the Veritas NetBackup Appliance CPM Plugin from the following CyberArk Marketplace site and install it:
<https://cyberark-customers.force.com/mplace/s/#a352J00000003MU8QAM-a392J0000002KuEoQAK>

Configuration

After you have downloaded and installed the plugin, perform the following configuration steps in the application on the CyberArk site.

To configure the plugin for the Veritas NetBackup Appliance CPM

- 1 Log in to the CyberArk PVWA.
- 2 On the **Account View** page, click **Add account** and do the following:
 - For **Select system type**, click **Imported platforms**.
 - For **Assign to platform**, click **Veritas NetBackup via SSH**.
 - For **Store in safe**, select where you want to store the configuration. You can also click **Create Safe** to create a new one.
 - For **Define properties**, enter the following:
 - **Address**: Enter the appliance fully qualified domain name.
 - **Username**: Enter the administrator or the maintenance user username.
 - **Password**: Enter the associated password for the entered administrator or the maintenance username.

Enable reconciliation

To enable password reconciliation for an account, the following tasks are required:

- Create a new user with administrator privileges on the appliance, then add that user to CyberArk.
- Add the NetBackup Appliance maintenance user account to CyberArk.

- Associate the new administrator user account as the **Logon Account** for the current user account.
- Associate the maintenance user account as the **Reconcile Account** for the current user account.

To enable reconciliation for the Veritas NetBackup Appliance CPM plugin

- 1 On the NetBackup Appliance, create a new local user with the administrator privileges.
- 2 Add the new administrator user account to CyberArk as follows:
 - On the CyberArk PVWA, click **Add Account**.
 - On the **Add account** page, enter the required information in the following fields:

Address - the NetBackup Appliance address or host name.

Username - the new appliance administrator user account.

Password - the password for the administrator user account.

Confirm password

Click **Add**.

- 3 Add the appliance maintenance user account to CyberArk as follows:
 - On the CyberArk PVWA, click **Add Account**.
 - On the **Add account** page, enter the required information in the following fields:

Address - the NetBackup Appliance address or host name.

Username - the appliance maintenance user account.

Password - the password for the maintenance user account.

Confirm password

Click **Add**.

- 4 Associate the new administrator user account with the appliance maintenance user account as follows:
 - On the **Accounts View** page, select the new NetBackup Appliance administrator account that you added. Then, in the upper right corner, click **Additional details & actions classic interface**.
 - On the **Account Details** page that appears, in the box on the right side of the page, for **Logon Account**, click **Associate**. In the popup window that appears, select the new NetBackup Appliance administrator account and click **Associate**.
 After the popup window closes, in the same box on the right side of the page, for **Reconcile Account**, click **Associate**. In the popup window that

appears, select the NetBackup Appliance maintenance account and click **Associate**.

CyberArk plugin for Remote Management interface

This chapter includes the following topics:

- [Veritas Remote Management Interface via API CyberArk Plugin](#)

Veritas Remote Management Interface via API CyberArk Plugin

[Marketplace document updates only]

The Veritas Remote Management Interface via API Plugin is a CyberArk component. The plugin is supported for the following Veritas appliances that use the IPMI platform:

- Access Appliance
- Flex Appliance
- NetBackup Appliance

The following describes the supported plugin functionality:

- Verify that the sysadmin and other account passwords are valid.
- Change the password of sysadmin account.
- Reconcile, or use an associated account to change the password of the sysadmin account.

Requirements and prerequisites

The following describes the requirements and tasks that you must perform before you can configure the plugin:

- The supported Veritas appliances must use one of the following Intel BMC firmware versions:
 - Intel BMC FW Rev 1.90.0CF6E935
 - Intel BMC FW Rev 2.37.1f190479
 - Intel BMC FW Rev 2.48.89b32e0d
 - Intel BMC FW Rev 2.86.2da97d3f
 - Intel BMC FW Rev 2.88.79ef9f8b
 - Intel BMC FW Rev 2.88.c7c905f1
 - Intel BMC FW Rev 2.88.e172ff67
 - Intel BMC FW Rev 2.88.e5f45b9c
 - Intel BMC FW Rev 2.89.7e3b728b
 - Intel BMC FW Rev 2.91.8a19dcde
 - Intel BMC FW Rev 2.92.9CAAE307
 - Intel BMC FW Rev 2.92.76E25E1D

To upgrade to the appropriate Intel BMC firmware version for your appliance, click the following link for instructions about how to update the appliance firmware:

https://www.veritas.com/content/support/en_US/downloads/update.UPD966809
- A CyberArk PAM (Privileged Access Manager) solution.
- Download the Veritas Remote Management Interface via API Plugin from the following CyberArk Marketplace site and install it:

<https://cyberark-customers.force.com/mplace/s/#a35Ht000000rtweIAA-a39Ht000003SejKIAS>

Configuration

After you have downloaded and installed the plugin, perform the following configuration steps in the application on the CyberArk site.

To configure the plugin for the Veritas Remote Management Interface via API

- 1 Log in to the CyberArk PVWA.
- 2 On the **Account View** page, click **Add account** and do the following:
 - For **Select system type**, click **Imported platforms**.
 - For **Assign to platform**, click **Veritas Remote Management Interface via API**.
 - For **Store in safe**, select where you want to store the configuration. You can also click **Create Safe** to create a new one.

- For **Define properties**, enter the following:
 - **Address**: Enter the appliance fully qualified domain name.
 - **Username**: Enter the sysadmin username.
 - **Password**: Enter the associated password for the entered sysadmin username.

The plugin is designed for use with an SSL certificate. If the target appliance uses a self-signed certificate, you must reconfigure the plugin to use that certificate type as follows:

To reconfigure the plugin to use a self-signed certificate

- 1 Log in to the CyberArk PVWA.
- 2 Navigate to the **Platform Management** page and do the following:
 - Click the platform named **Veritas Remote Management Interface via API**.
 - On the lower right side, click **Edit**.
 - In the left column, expand **Automatic Password Management** and click **Additional Policy Settings**.
 - In the **Properties** column, click **Use SSL**. Then, in the **Value** column, right-click on **Yes** and select **IgnoreUntrustedCertificate**.

CyberArk plugin configurations for Flex Scale and Access Appliances

This chapter includes the following topics:

- [Veritas NetBackup Flex Scale and Access Appliance API CyberArk CPM plug-in](#)
- [Configuration for CyberArk Privileged Session Manager \(PSM\) for SSH](#)

Veritas NetBackup Flex Scale and Access Appliance API CyberArk CPM plug-in

The Veritas NetBackup Flex Scale and Access Appliance API CPM Plugin is a CyberArk component. The plugin integrates the NetBackup Flex Scale and Access Appliance user interfaces with CyberArk and lets you manage the user accounts on those appliances. The following describes the supported plugin functionality:

- Change or verify passwords for the following NetBackup Flex Scale Appliance user accounts: all local users, maintenance, and all NetBackup users.
- Change or verify passwords for the following Access Appliance user accounts: primary, local, and maintenance.
- Limitations:
 - Reconciliation is not supported.

- The plugin cannot verify or change passwords for accounts when the target appliance is offline, especially if the appliance management console is running on it. Once the management console is operational again, the plugin functionality can be reinstated.
- IPMI users, multifactor authentication configured users, and remote users are not supported.

Requirements and prerequisites

The following describes the requirements and tasks that you must perform before you can configure the plugin:

- A configured NetBackup Flex Scale Appliance with software versions 3.2 and later, or a configured Veritas Access Appliance with software versions 8.2 and later.
- A CyberArk PAM (Privileged Access Manager) solution.
- CyberArk CPM (Central Policy Manager) configuration.
- Users must complete their first appliance logon and change their default passwords before they can be added to the CyberArk password vault.
- Download the Veritas NetBackup Flex Scale/Access Appliance API CPM Plugin from the following CyberArk Platform site and install it:
<https://cyberark.my.site.com/mplace/s/#--Veritas>

Configuration

After you have downloaded and installed the plugin, perform the following configuration steps in the application on the CyberArk site.

To configure the plugin for a NetBackup Flex Scale or Access Appliance administrator account

- 1 Log on to the CyberArk PVWA.
- 2 On the **Accounts View** page, click **Add account** and do the following:
 - For **Select system type**, click **Imported platforms**.
 - For **Assign to platform**, click **Veritas NetBackup Flex Scale or Access Appliance API via REST**.
 - For **Store in safe**, select where you want to store the configuration. You can also click **Create Safe** to create a new one.
 - For **Define properties**, enter the following:

Address: Enter the NetBackup Flex Scale or Access Appliance fully qualified domain name.

Username: Enter the NetBackup NetBackup Flex Scale or Access Appliance administrator account username.

Password: Enter the associated password for the entered NetBackup Flex Scale or Access Appliance administrator account username.

The plugin is designed for use with an SSL certificate. If the target appliance uses a self-signed certificate, you must reconfigure the plugin to use that certificate type as follows:

To reconfigure the plugin to use a self-signed certificate

- 1 Log on to the CyberArk PVWA.
- 2 Navigate to the **Platform Management** page and do the following:
 - Click once on the platform named **Veritas NetBackup Flex Scale or Access Appliance API via REST**. Then, on the lower-right side of the page, click **Edit**.
 - In the left column, expand **Automatic Password Management** and click **Additional Policy Settings**.
 - In the **Properties** column, click **Use SSL**. Then, in the **Value** column, right-click on **Yes** and select **IgnoreUntrustedCertificate**.

Configuration for CyberArk Privileged Session Manager (PSM) for SSH

The CyberArk Privileged Session Manager (PSM) supports management of web user passwords for the following Veritas appliances:

- NetBackup Flex Scale Appliance
- Veritas Access Appliance

Note: The console IP, all nodes, and NetBackup WORM are supported. However, NetBackup primary and media instances are not supported.

PSM lets you initiate, monitor, and record privileged login sessions, and usage of administrative and user accounts for the associated account passwords that are stored in a CyberArk password vault. Additionally, the entire user login session is recorded.

Requirements and pre-requisites

The following describes the requirements and tasks that you must perform before you can configure the PSM:

- A configured NetBackup Flex Scale Appliance with software versions 3.2 and later, or a configured Veritas Access Appliance with software versions 8.2 and later.
- A CyberArk PAM (Privileged Access Manager) solution.
- A completed CPM configuration.
- Limitations:
 For the best experience and to avoid errors on the CyberArk website, use Google Chrome versions 109.0.5414.129 (64-bit) and later.

Architecture

The PSM uses the password from a vault for the user logins to initiate an SSH session. The architecture uses the standard CyberArk architecture where it records the sessions that are stored in the vault.

Configuration

You can use one of the following methods to configure the PSM for SSH:

- PSM-SSH method - when a user logs in, this method starts a Remote Desktop connection, and records the entire login session.
- PSMP SSH method - this method requires a dedicated Linux machine that is accessible from the environment. Documentation links are available on the CyberArk website and are included in the procedure that describes this configuration method.

To configure PSM-SSH

- 1 Log in to the CyberArk PVWA.
- 2 Navigate to the following page:

Administration > Configuration Options > Options > Connection Components

Click the **+** symbol to expand and view the component contents. Then, right-click on **PSM-SSH** and click **Copy**.

- 3 Right-click on **Connection Components** and select **Paste Connection Component**.

The new component should now appear in the expanded list of components: **PSM-SSH**. To rename the component do the following:

- Click once on the new **PSM-SSH** component.
- In the right pane of the page, in the first row at the top of the page for the **ID**, change the component name where it appears in the **Value** column on the right. For example: **PSM-NBFSAA**.

- Right-click the new component name and select **Copy**.
- 4 Navigate to **Administration > Platform Management**.
- 5 On the page with the list of **Target Account Platforms**, do the following:
 - Locate the CPM PSM name to add PSM support and click on it once.
 - In the lower-right corner of the page, click **Edit**.
- 6 In the left column of the page, do the following:
 - Right-click on **UI & Workflows** and select **Add Privileged Session Management**.
 - Right-click again on **UI & Workflows** and select **Add Connection Components**.
 - Right-click on **Connection Components** and select **Add Connection Component**.
 - Paste the Id content that you copied in step 3.
 - In the lower-right corner of the page, click **Apply**, then click **OK**.
- 7 Right-click on the new PSM to ensure that both the **Privileged Session Management** and **Connection Components** menus appear.
- 8 To add the override functionality, do the following:
 - In the left column of the page, right-click on the PSM and select **Add Override User Parameters**.

Note: Do not select **Add Override Component Parameters**.

- Right-click on the PSM again and select **Add Parameter**.
- On the **Properties** side of the page, at the top of the page for **Name**, enter `PSMRemoteMachine` into the **Value** column.
- On the **Properties** side of the page, for **Type**, enter the following into the **Value** column:
`CyberArk.PasswordVault.Web.TransparentConnection.RemoteMachineUserParameter,`
`CyberArk.PasswordVault.Web`
- In the upper-left corner of the page, click **Apply**, then click **OK**.
- 9 Restart the CyberArk Password Manager as follows:
 - Navigate to **Services (Local)**.

- Right-click on **CyberArk Password Manager** and select **Restart**.
- 10** Log in to CyberArk Password Manager and do the following:
- Navigate to the **Accounts View** page.
 - Select a user account to connect to a machine and click **Connect**.
 - When prompted, add the IP address for the machine to allow the user to access it.

To configure PSMP SSH

- 1** Contact your CyberArk representative to obtain the PSMP software.
- 2** Install the PAMP software on your Linux machine.
- 3** Set up PSM for SSH on your Linux machine as follows:
 - Download the PSM for SSH software from the following site:
<https://cyberark.my.site.com/mplace/s/#software-aK4Ht000000fxT4KAI->
 - Obtain the necessary documentation from the following site:
<https://docs.cyberark.com/PAS/Latest/en/Content/PASIMP/...>
- 4** Log in to the CyberArk PVWA and navigate to the following page:
Administration > Platform Management > Veritas NetBackup Flex Scale or Access Appliance API via REST > Connection Components. In the lower-right corner of the page, click **Edit**.
- 5** Right-click on **UI & Workflows** and select **Add Privileged Session Management**. On the **Properties** side of the page, verify that the **Value** for **PrivilegedSSO** is set to **Yes**.
- 6** In the left column of the page, right-click **UI & Workflows** and select **Add Connection Components**.
- 7** In the left column of the page, right-click **Connection Component** and select **Add Connection Component**.
 On the **Properties** side of the page, in the **Value** column for the **Id**, change the name of the newly added component to **PSMP-SSH**.
- 8** To use one account to connect to multiple target machines, complete the following tasks to add the **Override User Parameter**, as in the previous procedure.
 - In the left column of the page, right-click on the **PSMP-SSH** component and select **Add Override User Parameters**.

Note: Do not select **Add Override Component Parameters**.

- Right-click on **Override User Parameters** and select **Add Parameter**.
 - On the **Properties** side of the page, at the top of the page for **Name**, enter `PSMRemoteMachine` into the **Value** column.
 - On the **Properties** side of the page, for **Type**, enter the following into the **Value** column:
`CyberArk.PasswordVault.Web.TransparentConnection.RemoteMachineUserParameter,`
`CyberArk.PasswordVault.Web`
 - In the upper-left corner of the page, click **Apply**, then click **OK**.
- 9** You are now ready to connect to the NetBackup Flex Scale or Access Appliances in the Linux environment. Use the following connection string to connect:

```
ssh <vault_login_user>@<cyberark_account_name>#<IP/FQDN>@<targetmachine>
#targetport@<vaultuserpassword>@<PSMPserverIP/FQDN>
```

Where *vault_login_user* is the administrator that logs into the PVWA and *cyberark_account_name* is the Access Appliance or NetBackup Flex Scale user login account name.

Note: The *IP/FQDN* parameter for the *cyberark_account_name* must match the target machine context exactly as it appears in the PVWA. For example, to use an IP address instead of a machine name in the PVWA, you must also use the IP address in the string. This same rule applies in the reverse situation whereas if you use a machine name in the string, you must also use the machine name in the PVWA. The concept here is to match the values. Name resolution does not work or apply here.
