



Genetec Config Tool Videounit Usage Plug-in for the Central Policy Manager

The CyberArk Password Vault
Version 11.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

Changing Passwords on Genetec Config Tool Videounit Usage

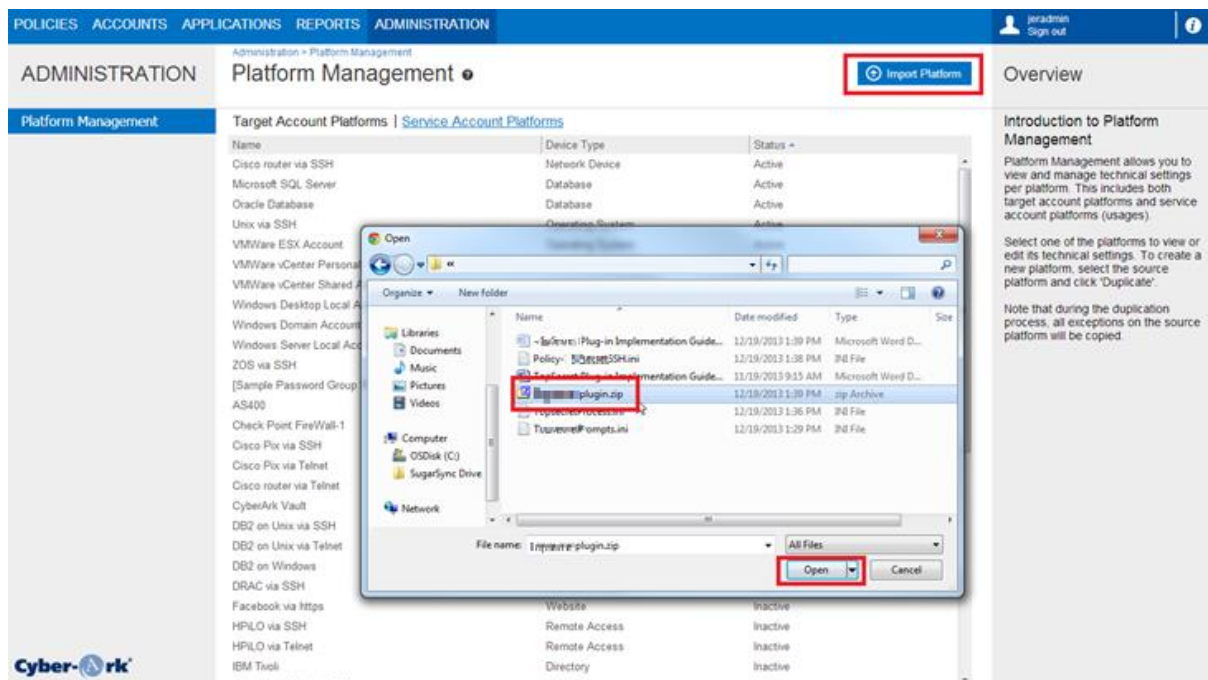
The Central Password Manager enables organizations to change passwords automatically on remote machines and store the new passwords in the Enterprise Password Vault, with no human intervention, according to the organizational policy. This plug-in supports the changing of passwords for users on the Genetec Config Tool Videounit Usage using the HTTP protocol.

Installation

You will receive the GenetecConfigToolVideounitUsage plug-in zip archive from your CyberArk representative. The following instructions show you how to install it.

Installing the Genetec Config Tool Videounit Usage Plug-in

1. Log into the PVWA with an administrative account.
2. Go to Administration > Platform Management.
3. Click Import Platform. Upload the GenetecConfigToolVideounitUsagePlugin.zip file.



Platform Configuration

- The following platform settings are given initial default values. Please check that these match your environment or edit them accordingly.

To Edit these values navigate to:

Administration → Platform Management → Genetec Config Tool Videounit Usage
→ Edit → Automatic Password Management → Additional Policy Settings →

Parameters:

Parameter name	Default value	Allowed values	Description
ChainsFilePath	bin\GenetecConfigToolVideounitUsageChains.xml	A valid path on CPM server(s)	Configuration file of REST call logic
UseSSLForHTTP	IgnoreUntrustedCertificate	Yes, No, IgnoreUntrustedCertificate	Whether or not an SSL connection will be used to connect to the remote device.
Address	CHANGE_ME	Hostname or IPv4	The address of the target machine. See General Notes section for additional information.
BaseURI	WebSdk	Same value as configured in Config Tool	Value specified in WebSDK role in Config Tool
ApplicationID	CHANGE_ME	A valid application ID	An Application ID value retrieved from Genetec Security Center SDK certificate

To Edit these values navigate to:

Administration → Platform Management → Genetec Config Tool Videounit Usage
→ Edit → Automatic Password Management → Additional Policy Settings:

Parameter name	Default value	Allowed values	Description
Port	-1	A numeric value	The port used to connect to the remote machine. Set the value to '-1' to avoid using the port.



Configuring the Platform Policy Vault Web Access

- Go to 'Administration' -> 'Platform Management' and update the existing (master) platform policy.
- Right click on 'UI & Workflows' and select 'Add Usages', right click on Usages and select 'Add Usage'. Rename the new usage to: GenetecConfigToolVideounitUsage
- Go to 'Automatic Password Management' -> 'General' and set SearchForUsages to **Yes**
- Click "OK" (bottom right) to save these changes

Adding GenetecConfigToolVideounitUsage Accounts

Adding Accounts through the Password Vault Web Access

- Create a new GenetecConfigToolVideounitUsage account or use an existing one.
- Specify the required account properties.
- Associate a required logon account for the new password object.

For more information about adding password objects in the Password Vault Web Access, refer to the Privileged Account Security Implementation Guide.

General Notes

1. GenetecConfigToolVideounitUsage usage plug-in supports the following:
 - Password change
2. The logon account is required for password change.
 - The logon account must have permissions to authenticate to Genetec REST API.
3. When specifying a value for an address, set it to be without protocol and port. These values are set on policy level (port by **Port** property and protocol by **UseSSLForHTTP** property).
For example:
 - 127.0.0.1 – is an address in a proper format.
 - https://127.0.0.1:443 – is an address in an improper format, and needs to be changed.

