

Delete External Users Implementation Guide

21 Nov 2021

Overview

About the Script

This script is designed to delete external vault users from the database based on a specific directory map. A typical use case might be that a new directory map was added for end users that require a different authentication method. In this use case, the users need to be added to the new group in LDAP and the present external users need to be deleted from the vault database. This can become a tedious task if there are more than just a handful of users.

Support

This script is not supported by CyberArk. By using the script, you agree to the disclaimer (shown when the script is executed).

Pre-Requisites

Before preparation for use, ensure the following is in place

Environment

- Vault environment
 - Supported version: Any. This has been tested with vault version 12.2
- PowerShell
 - Version 7
- ExportVaultData
 - Part of the script depends on a CSV file created from CyberArk's ExportVaultData utility. More information on ExportVaultData is located [here](#)

Knowledge

The end user should have the following pre-requisite knowledge

- Vault
 - ExportVaultData usage
 - Familiarity with fundamental vault concepts and operation

Implementation

Installation

The script is in two parts

- DelExtUser.ps1
- DelExtUserEnv.ps1

The scripts can be placed in any folder; however, they must be in the same folder. There is no installation wizard necessary.

Operation

Preparation

1. Before each execution of the script, generate a new users file with ExportVaultData
2. Note the full URL of a PVWA, i.e., <https://somehost.domain.com/PasswordVault>
3. If multiple LDAP directories have been configured, note the domain of the desired LDAP directory maps to work with.

Syntax

It is strongly recommended to generate a CSV file with ExportVaultData each time the script is to be executed

./DelExtUser.ps1 <Path to ExportVaultData CSV file>

Environment Variables

The 'DelExtUserEnv.ps1' contains variables that are initialized. While most of these *should not be changed*, there is one variable, '\$exclList' that can be changed. This is a PowerShell array that contains usernames that which under no circumstances should be deleted. A default list could be entered, i.e., tsawyer, vaultadmin, vaultuser. During the operation of the script there is an opportunity to edit this list.

Test Mode

The script can be executed in test mode. Test mode simulates what actions will be taken in the database, but not actually deleting the users from the database. This is strongly recommended before making any changes.

Miscellaneous

Known Issues

When the script is exited, there is an error stating that the Logoff method has failed, however the session token cannot be reused.