

# McAfee Vulnerability Manager and Cyber-Ark integration

McAfee Vulnerability Manager 7.0.6 (and later) can be configured to use Cyber-Ark for secure scan credential storage. This guide contains the procedures needed to integrate these products.

McAfee Vulnerability Manager and Cyber-Ark are separate applications. You must make sure both are installed, configured, and working properly before attempting to integrate the two applications.

---

## Install Cyber-Ark provider

The Cyber-Ark provider must be installed on all McAfee Vulnerability Manager scan engines that must access the vault for passwords during scanning.

Make sure the Cyber-Ark provider is correctly provisioned to access the Cyber-Ark vault that will store the user credentials.

By default, McAfee Vulnerability Manager uses Foundstone as the Application ID to connect to the vault. This application ID must be provisioned with the appropriate security access to the vault.

You can customize the application ID used by each scan engine. To change the application ID, you can edit a registry value on each scan engine.

- For 32-bit systems: REG\_SZ:  
SOFTWARE\Foundstone\FSScanEngine\CyberArkAppID
- For 64-bit systems: REG\_SZ:  
SOFTWARE\Wow6432Node\Foundstone\FSScanEngine\CyberArkAppID

The scan engine will try to locate the Provider SDK DLL. If the DLL is installed in an unusual location, you can specify the location by editing a registry value on each scan engine.

- For 32-bit systems: REG\_SZ:  
SOFTWARE\Foundstone\FSScanEngine\CyberArkPath
- For 64-bit systems: REG\_SZ:  
SOFTWARE\Wow6432Node\Foundstone\FSScanEngine\CyberArkPath

---

## Register McAfee Vulnerability Manager in Cyber-Ark

The McAfee Vulnerability Manager application ID must be provisioned with the correct security privileges to access the vault(s) that store scan credentials.

By default, McAfee Vulnerability Manager uses Foundstone as the Application ID to connect to the vault. If needed, you can change the application ID (see the previous topic).

---

## Enable Cyber-Ark credentials

To use Cyber-Ark in McAfee Vulnerability Manager, you must enable the user interface elements that allow the entry of Cyber-Ark credentials when creating a scan or credential set.

- 1 Open the *config.ini* file on the enterprise manager server.
  - For a 32-bit system: \Program Files\Foundstone\portal\include\config.ini.
  - For a 64-bit system: \Program Files(x86)\Foundstone\portal\include\config.ini.
- 2 Type `CyberArk = 1` somewhere in the file. You can add this line at the bottom of the *config.ini* file.
- 3 Save the file.

---

## Add Cyber-Ark credentials to a scan

Adding Cyber-Ark credentials to a scan can be done directly in the Scan Editor or by referencing a Credential Set that uses Cyber-Ark.

- 1 Select **Cyber Ark** for each credential to be added where the password is stored in a Cyber-Ark vault.
- 2 Specify the name of the vault where the password is stored in the **Cyber Ark Safe** field.
- 3 Specify the name of the object that stores the password in the **Object Name** field.
- 4 For some object types, Cyber-Ark can store login names/account names in addition to passwords. To use the user name stored in Cyber-Ark, select **vault** and leave the **User ID** field blank.

---

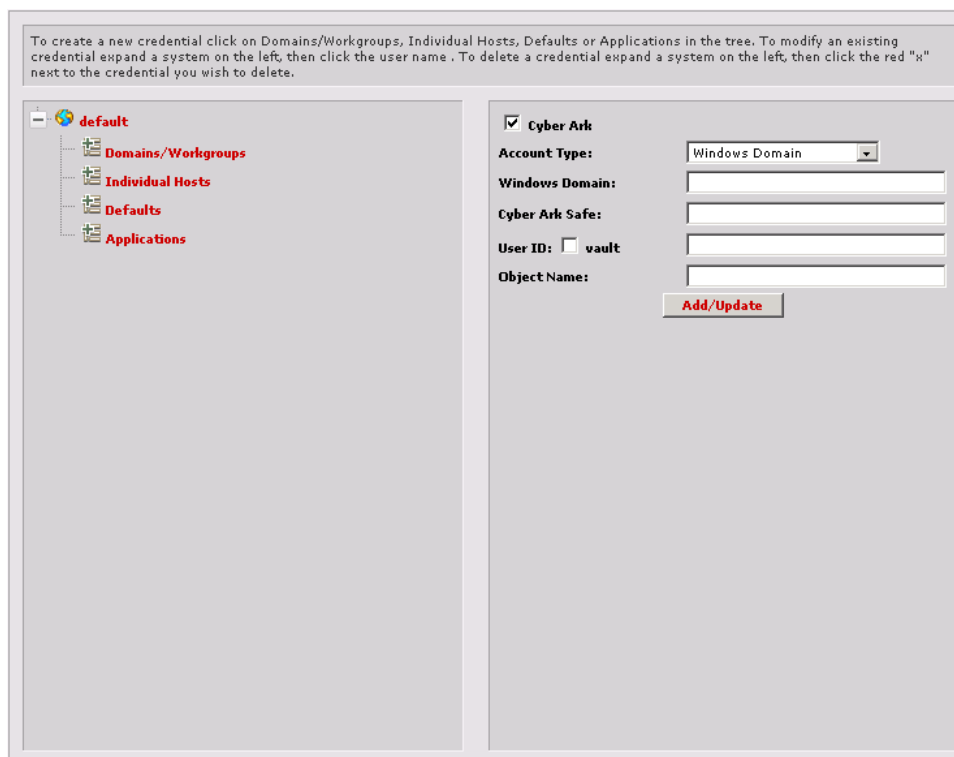
## Use folders in Cyber-Ark vaults

For passwords stored in folders in a vault, the full path to the object must be specified in the Object Name field. For example, if an object called **Admin** is stored in a folder in the vault called **Windows**, the Object Name in McAfee Vulnerability Manager would be:

`root\Windows\Admin`

The name of the root folder (by default **root**) is required if the object is stored in a sub-folder, but is not required if the object is stored in the root folder. The root folder must not be preceded by a slash.

To create a new credential click on Domains/Workgroups, Individual Hosts, Defaults or Applications in the tree. To modify an existing credential expand a system on the left, then click the user name. To delete a credential expand a system on the left, then click the red "x" next to the credential you wish to delete.



The screenshot shows a web-based interface for managing credentials. On the left, a tree view under 'default' contains four folders: 'Domains/Workgroups', 'Individual Hosts', 'Defaults', and 'Applications'. On the right, a configuration panel for 'Cyber Ark' is displayed. It includes a checked checkbox for 'Cyber Ark', a dropdown menu for 'Account Type' set to 'Windows Domain', and four text input fields for 'Windows Domain', 'Cyber Ark Safe', 'User ID', and 'Object Name'. The 'User ID' field has a 'vault' checkbox. An 'Add/Update' button is located at the bottom right of the configuration panel.

Figure 1: Selecting Cyber-Ark for Windows Domain

To create a new credential click on Domains/Workgroups, Individual Hosts, Defaults or Applications in the tree. To modify an existing credential expand a system on the left, then click the user name . To delete a credential expand a system on the left, then click the red "X" next to the credential you wish to delete.

- default
  - Domains/Workgroups
  - Individual Hosts
  - Defaults
  - Applications

☒ **Cyber Ark**

**Account Type:** Shell Individual Host

**Shell Individual Host:**

**Cyber Ark Safe:**

**User ID:** ☐ vault

**Object Name:**

**Shell Options**

**Protocol**

☒ SSHv2 Only ☐ SSHv2 or SSHv1

☐ SSHv2, SSHv1, or Telnet

**Security**

☒ Certificate Only

☐ Certificate or Password

**Privileged Access**

☐ None ☒ root ☐ sudo

☒ Cyber Ark

**Cyber Ark Safe:**

**User ID (Optional):** ☐ vault

**Object Name:**

**Add/Update**

Figure 2: Selecting Cyber-Ark for Shell Credentials

For Shell credentials, you can include Cyber Ark information for root or non-root users. To add Cyber Ark information for non-root users, select the **Cyber Ark** checkbox above the *Account Type*. To add Cyber Ark information for root users, select the **Cyber Ark** checkbox under **Privileged Access**. You can specify Cyber Ark root and non-root user information in the same credential.