

FireMon / CyberArk Integration

Integration summary for CyberArk Vault Server with FireMon Security Manager

Name of Integration

FireMon Credential Integration

Vendor Product Name

FireMon Security Manager

FireMon Security Manager integrates seamlessly with CyberArk Vault Server, enhancing secure credential management for network security devices. As a leader in firewall policy management, cloud security operations, and cyber asset discovery, FireMon helps organizations streamline security and compliance efforts.

Integration Highlights

FireMon Security Manager leverages CyberArk to centralize credential management, enabling immediate, authenticated device access through the CyberArk Vault. This integration simplifies configuration retrieval and policy automation across your environment, maintaining seamless functionality.

Requirements from your CyberArk Admin

- URL of your CyberArk instance
- Valid App ID and Safe
- Client certificate and password

Once configured, you can migrate devices to reference CyberArk Vault credentials for streamlined access management across all system and device levels.

Integration Process

To learn more about configuring your CyberArk instance to communicate with Security Manager, please refer to CyberArk documentation.

- https://docs.cyberark.com/credential-providers/latest/en/content/ccp/configure_ccpwindows.htm
- https://docs.cyberark.com/credential-providers/latest/en/content/ccp/configure_ccpwindows.htm#RESTAPI
- <https://docs.cyberark.com/credential-providers/latest/en/content/ccp/calling-the-web-service-using-rest.htm>

Notes

- Currently, Security Manager only tests that the connection is correct when it retrieves credentials in CyberArk for a device (during device setup or retrieval). During device setup, it always tests that the CyberArk account exists.

- The URL for CyberArk is typically **<https://<Client> CyberArk DNS Name>/AIMWebService/api/Accounts?AppID=<CyberArk application id>&Query=safe=<Client safe_name>;Object=**
- Credentials not prefixed with the CyberArk keyword (the default is **cyberark://**) will be treated as the actual credential, and Security Manager will not call CyberArk to get the value.
- **Cache**—CyberArk instances cache credentials for up to 25 minutes. This means retrievals from a device that has a password change will not work for up to 25 minutes. Each on-prem client instance will similarly affect retrieval.
- **Accounts**—Each credential is stored as an "Account" in CyberArk. Although passwords can be stored with user names, we cannot point directly to the credentials and ask it to retrieve the user name and password. Each credential (user name, password, SSH key) must be stored independently in CyberArk and configured in the Administration module.
- **Safe**—Each credential belongs to a "safe" (think of a folder or category). Only a single safe is currently supported since the entire Security Manager domain is tied to one safe. However, you can use different safes provided they are associated with other domains, and the devices whose credentials are in different safes are in different domains.

Open the Security Intelligence Platform

First, you must set up Security Manager to utilize CyberArk as an authentication method.

If your CyberArk instance is hosted, CyberArk is responsible for providing the host name, app ID, and safe.

1. Log in to the Security Intelligence Platform and open the Administration module.
2. On the toolbar, select **Settings > Security Manager**.
3. Scroll to the **Identity Management** section.
4. From the **Select Identity Management Tool** list, choose **CyberArk**.
5. You will need to provide:
 - The URL for the CyberArk instance.
 - The CyberArk token. This token (cyberark://) allows us to differentiate between a CyberArk identifier and an actual credential value.

Credentials not prefixed with the CyberArk keyword (the default is **cyberark://**) will be treated as the actual credential, and Security Manager will not call CyberArk to get the value.

 - Upload the CyberArk client certificate.
 - The Certificate Password for the CyberArk client certificate.
6. Click **Save**.

After setting up identity management for CyberArk, you must configure devices to use the new authentication method for retrievals.

To configure devices, you'll need to choose one of the following:

- Complete a device CSV to import. The template has been updated to include a column for CyberArk.
- Add a new device
- Update an existing device

Refer to the Administration User Guide for detailed device process documentation.

1. On the toolbar, select **Device > Devices** or **Management Stations**.
2. Select the device or management station you added or want to edit to use CyberArk for retrieval authentication.

3. In **Device Settings / Authentication:**

- In the **Username** field, enter the username used in CyberArk for the device.
- In the **Password** field, enter the password used in CyberArk for the device.

If each required field of the credential (username, password, SSH Key etc) is stored in a different CyberArk account, then the device settings will have:

```
username: cyberark://<account name where username is stored>
password: cyberark://<account name where password is stored>
```

If the credential is stored in the same CyberArk account, then the device settings will have:

```
username: cyberark://<account name where username is stored>:username
password: cyberark://<account name where password is stored>:password
```

Note: As seen in the above example, a colon is the only delimiter character allowed.

4. Click **Save**.