DEPLOYMENT GUIDE

Fortinet FortiSIEM and CyberArk Integration

Fortinet FortiSIEM and CyberArk Integration

Overview

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network - today and into the future. Only the Fortinet Security Fabric architecture can deliver security features without compromise to address the most critical security challenges, whether in networked, application, cloud or mobile environments. Fortinet ranks #1 in the most security appliances shipped worldwide and more than 400,000 customers trust Fortinet to protect their businesses. Learn more at https://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

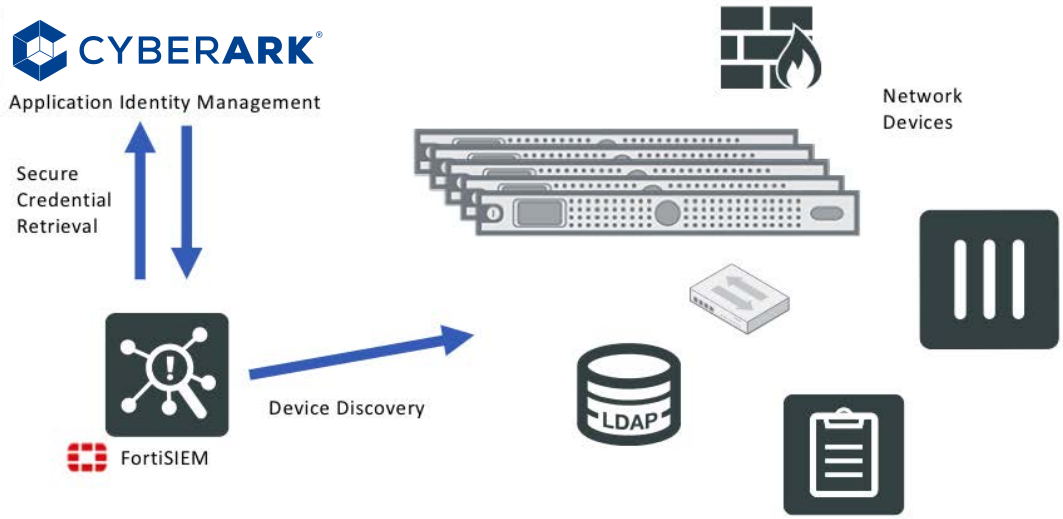
The Application Identity Manager™ (AIM), part of CyberArk's Privileged Account Security solution, eliminates the need to store App2App passwords in applications, scripts or configuration files, and allows these highly-sensitive passwords to be centrally stored, logged and managed with CyberArk's patented Vaulting Technology®. Using AIM, organizations can comply with internal and regulatory requirements for regularly replacing passwords and securely monitoring privileged access across all systems, databases and applications. AIM fully addresses the need to assure the highest availability for applications running the enterprise business, independent of network availability and with the highest performance.

Deployment Prerequisites

1. Fortinet FortiSIEM version 4.6.1 or newer (tested with version 5.0.1)
2. CyberArk Application Identity Manager version 9.9.5 Credential Provider

FORTINET Fabric-Ready

To address the needs of large enterprises, AIM supports a variety of systems, applications, Application Servers, scripts, jobs and more. It provides simple and intuitive tools for eliminating hard coded passwords, as well as a structured framework for addressing the challenges of App2App projects based on CyberArk's vast experience with large enterprise deployments.



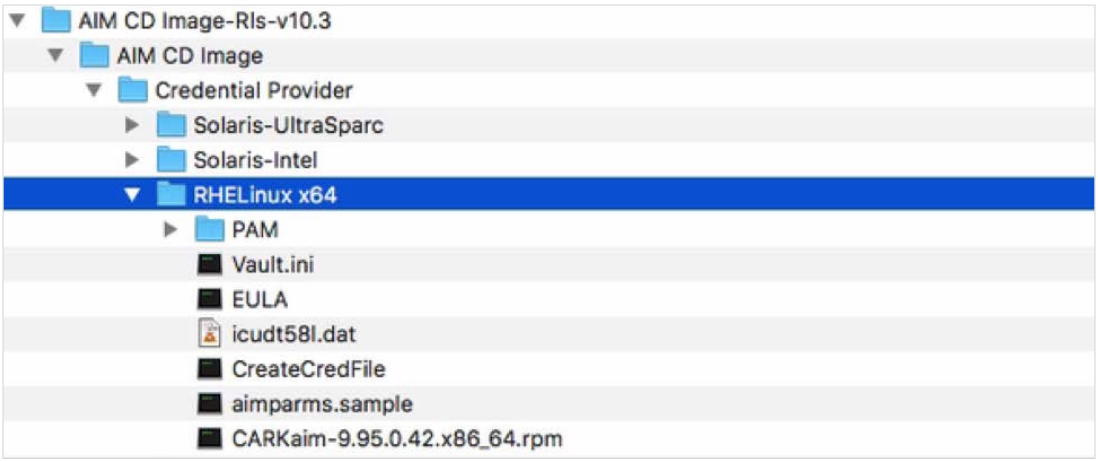
FortiSIEM Configuration_Install CyberArk Credential Power

Install the redhat-lsb package on FortiSIEM before installing the Credential Provider.

Note: you may also be required to install Dependencies prior to redhat-lsb.

```
Last login: Fri Jun 15 14:43:01 2018 from 10.101.32.254
[root@FSM-5 ~]# yum install redhat-lsb
Loaded plugins: fastestmirror
Setting up Install Process
Loading mirror speeds from cached hostfile
 * base: os-pkgs.fortisiem.fortinet.com
 * extras: os-pkgs.fortisiem.fortinet.com
 * updates: os-pkgs.fortisiem.fortinet.com
base                                                     | 3.6 kB     00:00
extras                                                   | 2.9 kB     00:00
updates                                                  | 2.9 kB     00:00
Package redhat-lsb-4.0-7.el6.centos.x86_64 already installed and latest version
Nothing to do
[root@FSM-5 ~]#
```

Download the Credential Provider Software from CyberArk. The installation files will look like this:



Create a new directory for the installation files.

Copy the following installation files to this directory:

CARKaim-9.50-<build number>.i386.rpm – The Linux installation packages

CreateCredFile – The CyberArk utility that creates credentials files

Vault.ini – The Vault parameter file

aimparms.sample – A sample of the parameter file used for installation

EULA – The Credential Provider end user license agreement.

icudt42b.dat – A file required to run the CreateCredFile utility

Open Vault.ini and enter the correct Address and Port, similar to the example below. Save the file when done.

```
VAULT = "Demo Vault"
ADDRESS=services-useast.skytap.com
PORT=29951

#------------------------------------
# Additional parameters (optional)
#------------------------------------

TIMEOUT=8                       - Seconds to wait for a Vault to respond to a request

#VAULTDN=                                - Vault's Distinguished Name (PKI Authentication)

#Proxy server connection settings  - cannot be used together with BEHINDFIREWALL
#---------------------------------
#PROXYTYPE=HTTP                  - Possible values - HTTP, HTTPS, SOCKS4, SOCKS5
#PROXYADDRESS=192.33.44.55       - Proxy server IP address (mandatory when using proxy server)
#PROXYPORT=8081                  - Proxy server IP Port
#PROXYUSER=xxx                   - User for Proxy server if NTLM authentication is required
#PROXYPASSWORD=yyy               - Password for Proxy server if NTLM authentication is required
#PROXYAUTHDOMAIN=NT_DOMAIN_NAME  - Domain for Proxy server if NTLM authentication is required

#BEHINDFIREWALL=NO               - Accessing the Cyber-Ark vault via a Firewall.

#USEONLYHTTP1=NO                 - Use only HTTP 1.0 protocol. Valid either with proxy settings Or with BEHINDFIREWALL

#NUMOFRECORDSPERSEND=15          - Number of file records that require an acknowledgement from the Vault server
#NUMOFRECORDSPERCHUNK=15         - Number of file records to transfer together in a single TCP /IP send/receive operation
#ENHANCEDSSL=NO                  - Enhanced SSL based connection (port 443) is required

#PREAUTHSECUREDSESSION=NO            - Enable pre authentication secured session
#TRUSTSSC=NO                           - Trust self-sign certificates in pre authentication secured session
#ALLOWSSCFOR3PARTYAUTH=NO            - Are self-sign certificates allowed for 3rd party authentication (like RADIUS)

#PROXYCREDENTIALS=                       - Instead of specifying proxy user and clear text proxy password, they can be given in the
 file pointed by this parameter
```

Edit the aimparms.sample file as follows.

AcceptCyberArkEULA should be set to yes

Uncomment (remove the # symbol) from the beginning of the CreateVaultEnvironment line

LicensedProducts should be set to AIM

CredFilePath should be set to the full path of the admin.cf file (created in the next step)

VaultFilePath should be set to the full path of the Vault.ini file

Save the aimparms.sample file. It should look something like this:

```
[Main]
AcceptCyberArkEULA=Yes
#CreateVaultEnvironment=yes
LicensedProducts=AIM
CredFilePath=/root/cyberark/admin.cf
VaultFilePath=/root/cyberark/Vault.ini
OverrideExistingConfFile=yes
AppProviderUserLocation=Applications

### In Repair/Upgrade the following parameters will be read from the existing "/etc/opt/CARKaim/conf/basic_appprovider.conf"
### file unless they are uncommented and contain different values
#AppProviderConfSafe=AppProviderConf
#MainAppProviderConfFile=main_appprovider.conf.linux.<version>
#MainOPMConfFile=main_opm.conf.linux.<version>
#AppProviderUser=Prov_<host_name>
#OPMUser=OPM_<host_name>
#PIMConfigurationSafe=PVWAConfig
#PIMConfigurationFolder=Root
#PIMPVConfigurationFileName=PVConfiguration.xml
#PIMPoliciesConfigurationFileName=Policies.xml
###

[AIM]
CacheLevel=persistent
CacheRefreshInterval=3

[PIMSu]
PIMSuCacheLevel=persistent
PIMSuCacheRefreshInterval=3
~
~
~
~
~
~
```

Copy the aimparms.sample file to /var/tmp/aimparms:

```
[root@FSM-5 aim]# cp aimparms.sample /var/tmp/aimparms
```

Enter the following to specify the administrative user that will create the Vault environment during installation:

./CreateCredFile admin.cf Password

Enter the Username and Password when prompted.

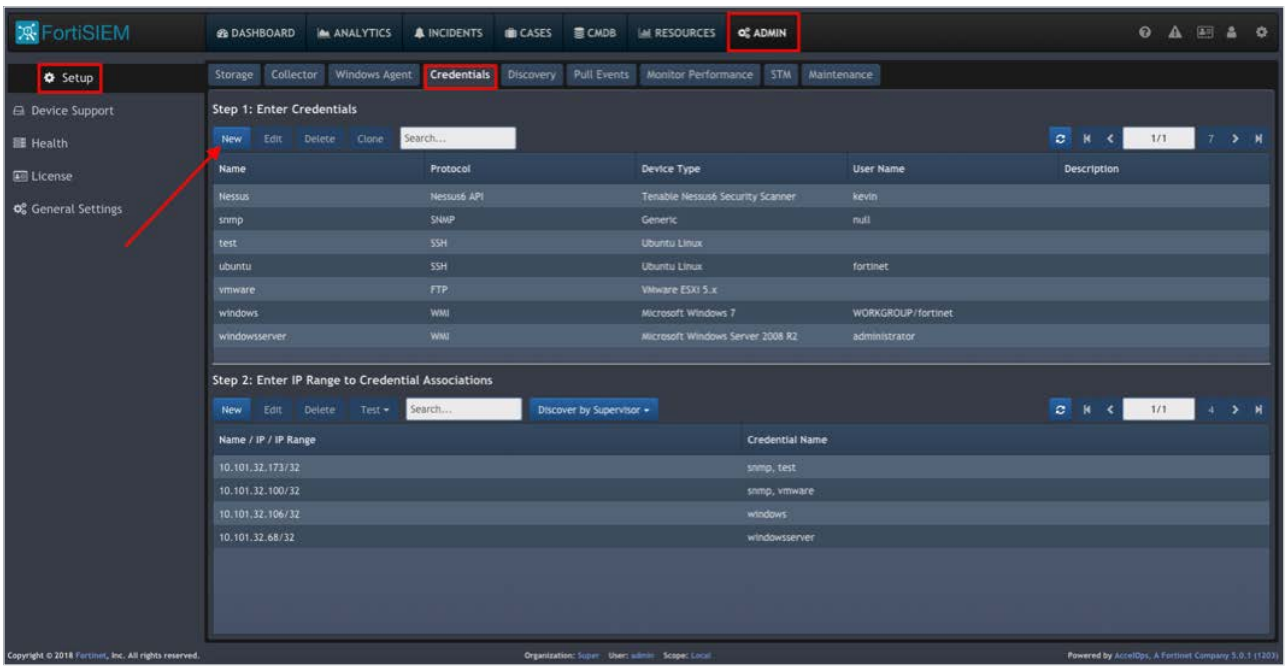
```
[root@FSM-5 cyberark]# ./CreateCredFile admin.cf Password
Vault Username [Administrator] ==>
Vault Password (will be encrypted in credential file) ==>
Disable wait for DR synchronization before allowing password change (yes/no) [No] ==>
External Authentication Facility (LDAP/Radius/No) [No] ==>
Restrict to Application Type [optional] ==>
Restrict to Executable Path [optional] ==>
Restrict to current machine IP (yes/no) [No] ==>
Restrict to current machine hostname (yes/no) [No] ==>
Restrict to OS User name [optional] ==>
Display Restrictions in output file (yes/no) [No] ==>

Command ended successfully
[root@FSM-5 cyberark]#
```

Install the Credential Provider for RHELinux x64

```
[root@FSM-5 aim]# rpm -i CARKaim-9.95.0.42.x86_64.rpm
Installation process is starting...
Searching for optional parameters...
Parameter [AppProviderUser] was set to its default value: [Prov_FSM-5]
Parameter [OPMUser] was set to its default value: [OPM_FSM-5]
Parameter [AppProviderConfSafe] was set to its default value: [AppProviderConf]
Parameter [MainAppProviderConfFile] was set to its default value: [main_appprovider.conf.linux.9.95]
Parameter [MainOPMConfFile] was set to its default value: [main_opm.conf.linux.9.95]
Parameter [PIMConfigurationSafe] was set to its default value: [PVWAConfig]
Parameter [PIMConfigurationFolder] was set to its default value: [Root]
Parameter [PIMPVConfigurationFileName] was set to its default value: [PVConfiguration.xml]
Parameter [PIMPoliciesConfigurationFileName] was set to its default value: [Policies.xml]
Creating Vault environment...
Creating environment for AIM...
Starting Cyber-Ark Application Password Provider...
Cyber-Ark Application Password Provider was started successfully.
Installation process was completed successfully.
[root@FSM-5 aim]#
```

FortiSIEM Configuration – Device Discovery Example

From the FortiSIEM GUI go to Admin > Setup > Credentials and click New

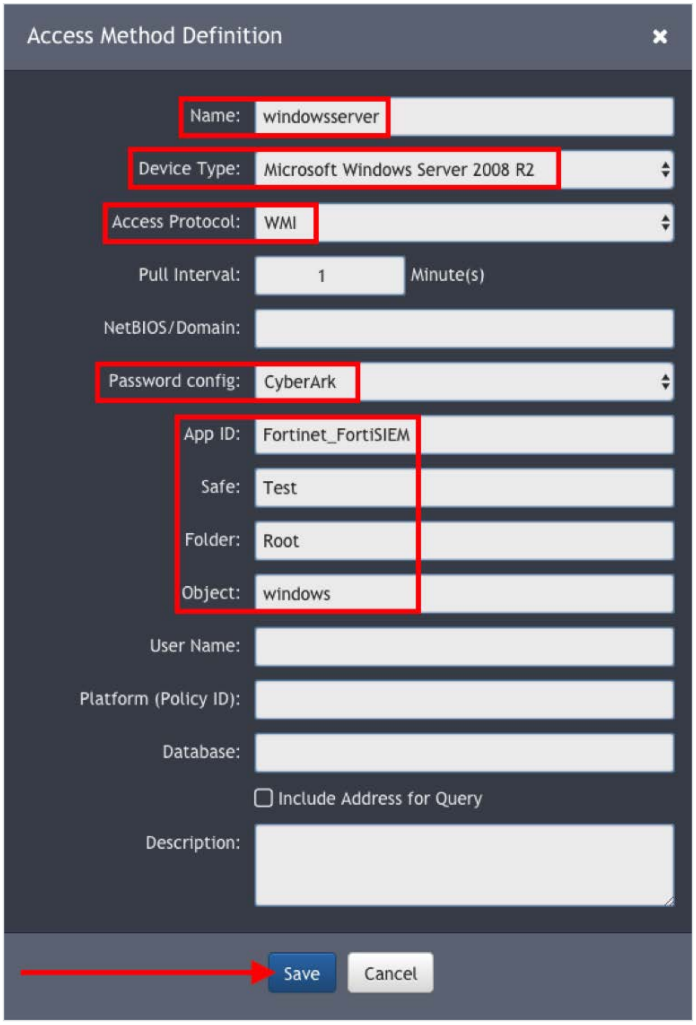


Give it a Name. Select the Device Type from the drop-down menu, in this example a Windows Server. Set the Access Protocol to WMI.

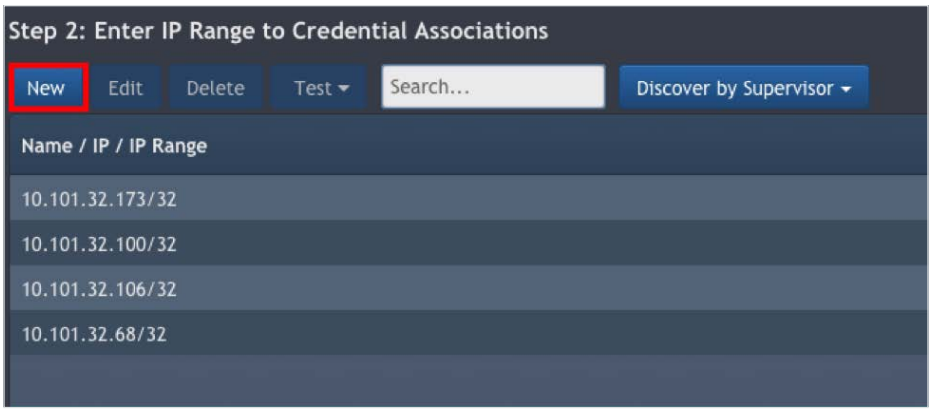
For the Password config change from the default of Manual to CyberArk.

You must configure the App ID, Safe, Folder and Object specific to your CyberArk account. Note that the Object is referred to as a Name in CyberArk.

Click Save.



Test Credential Retrieval in Step 2 – First click New.

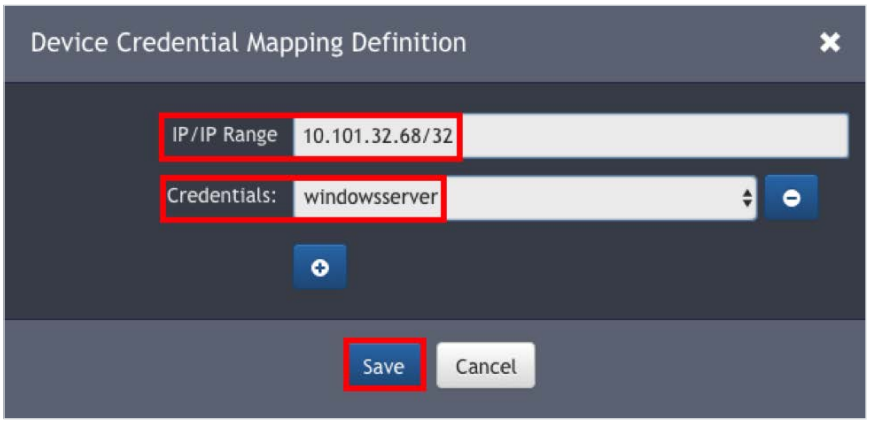


Enter the Name, IP Address or IP Range of a device you want to test. In this example it's a single IP address, 10.101.32.68.

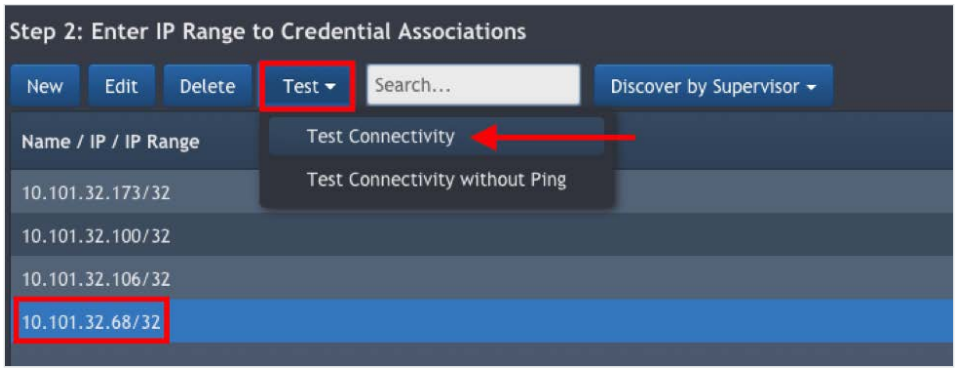
For Credentials select the Name defined in the previous step.

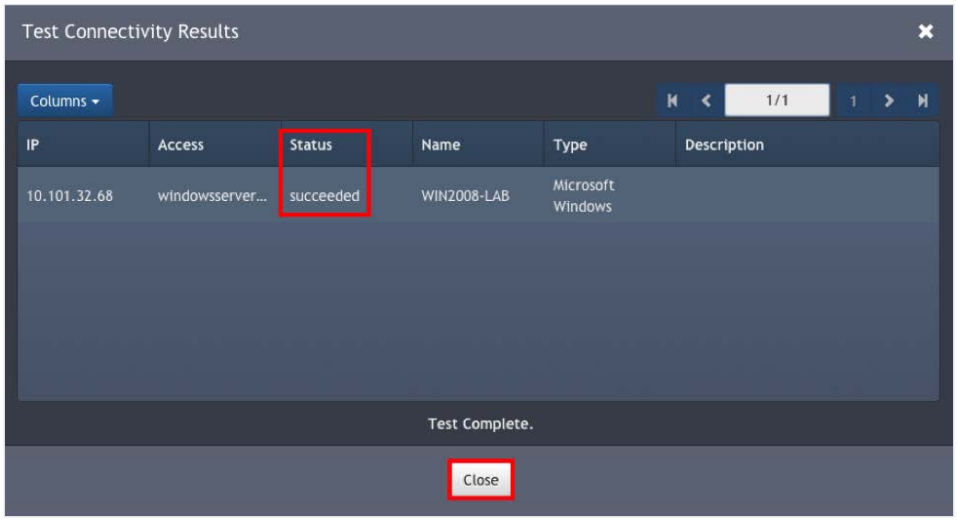
Click Save.

Note: The username, password and type of device should already be configured in CyberArk.



Highlight the new entry and click Test > Test Connectivity.





Click Close.

Congratulations, you're done!

Conclusion

You are now ready to use the CyberArk Application Identity Manager with FortiSIEM. Use CyberArk to securely provide admin credentials when FortiSIEM is discovering network devices.

FortiSIEM User Guide: https://docs.fortinet.com/uploaded/files/4438/fortisiem-5-0-1-user-guide-html.pdf

FortiSIEM External Systems Configurations Guide:
https://docs.fortinet.com/uploaded/files/4340/fortisiem-external-systems configurationguide.pdf

FortiSIEM User Guide: https://docs.fortinet.com/uploaded/files/4438/fortisiem-5-0-1-user-guide-html.pdf

CyberArk Credential Provider and ASCP Implementation Guide:

https://support.cyberark.com/SFE/directaccess.ashx?pageid=downloadfile&Safe=CyberArk+Documentation&Folder=Root%5cPAS+and+SIM%5cRelease-Specific%5cV9.9%5cPAS&Name=Credential+Provider+and+ASCP+Implementation+Guide.pdf

July 10, 2019 1:04 AM

440593-0-0-EN

D:\Fortinet\Deployment Guide\CyberArk\DG - Fortinet and CyberArk V1