



QxEDGE™ - CyberArk Vault Integration Guide

Introduction

The guide provides instructions to integrate the CyberArk Digital Vault with the Crypto4A QxEDGE™ - HSM as a Platform.

This enables the use of the Crypto4A Quantum Assured Security Module (QASM™), a next generation HSM that is fully integrated into the Crypto4A QxEDGE™, as the root of trust for multiple instances (up to 3) of the CyberArk Vault that can be installed on separate confidential compute Processing Engines (PEs) contained as part of the Crypto4A QxEDGE™.

Integration Steps

Install KVM on the QxEDGE™

By default QxEDGE™ does not ship with KVM, but it needs to be installed to support the Windows-based CyberArk Server:

```
sudo apt update
sudo apt install qemu-kvm libvirt-bin bridge-utils virtinst virt-manager
```

Check the installation was successful and KVM is active:

```
sudo systemctl is-active libvirtd
```

Add user to kvm group:

```
sudo usermod -aG libvirt $USER
sudo usermod -aG kvm $USER
```

Install Windows Server and CyberArk Server

It is highly recommended that a QEMU-KVM image with Microsoft Windows Server and CyberArk Digital Vault is first created outside the QxEDGE™ and then loaded onto one of the QxEDGE™ PE's. This greatly simplifies the installation process. The QEMU-KVM image should be uploaded to the /var directory, e.g. /var/vm. Please refer to the CyberArk documentation for details on how to install the Digital Vault.

Configure X11 and access virt-manager

It is convenient to access the KVM virt-manager to manage the virtual machine, as well as accessing the Windows GUI. To do so, one can enable X11 access to the PE's inside a QxEDGE™.

In /etc/ssh/sshd_config, add the following lines:

```
X11Forwarding yes
X11DisplayOffset 10
X11UseLocalhost yes
```

Login to the PE with X11 enabled:

```
ssh -X <username>@<IP address>
```

Start the KVM manager:

```
virt-manager
```

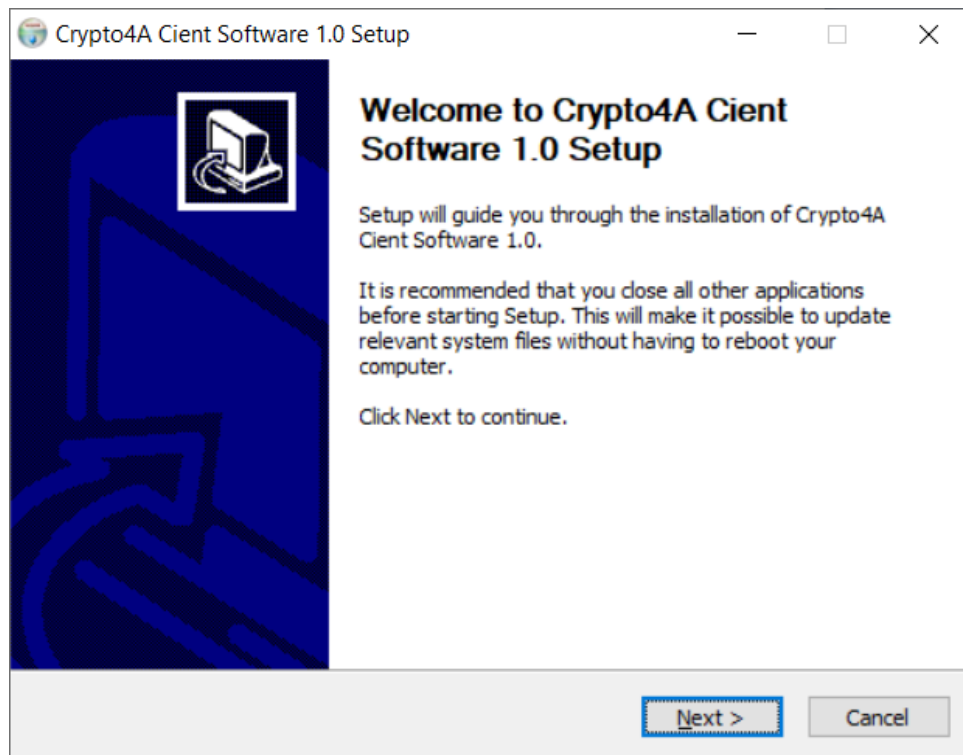
Create Virtual Machine

Create a VM with an existing KVM image with Windows Server and CyberArk server. Choose the right CPU cores and memory size when creating the VM. After the VM is created, start the Windows Server.

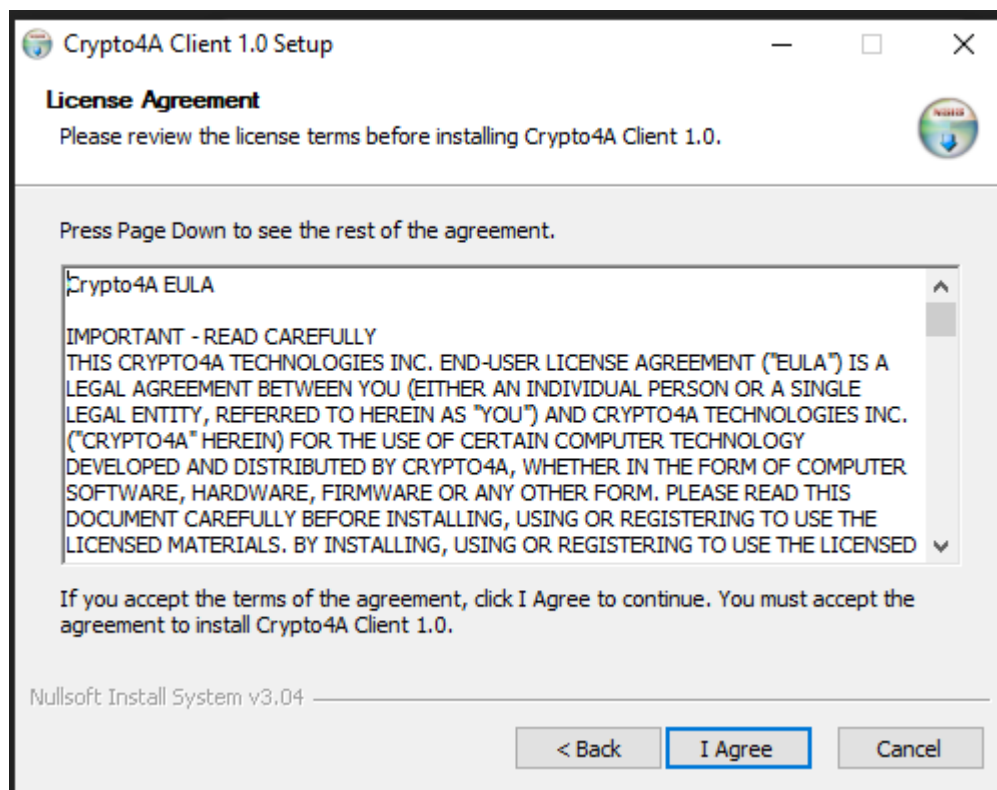
Connect to QASM™ using spa-fwd

The Windows server needs a secure channel to communicate with the QASM™. Crypto4A provides a Windows installer package that contains spa-fwd and a PKCS#11 library that is used to enable communication between the Digital Vault and the QASM™.

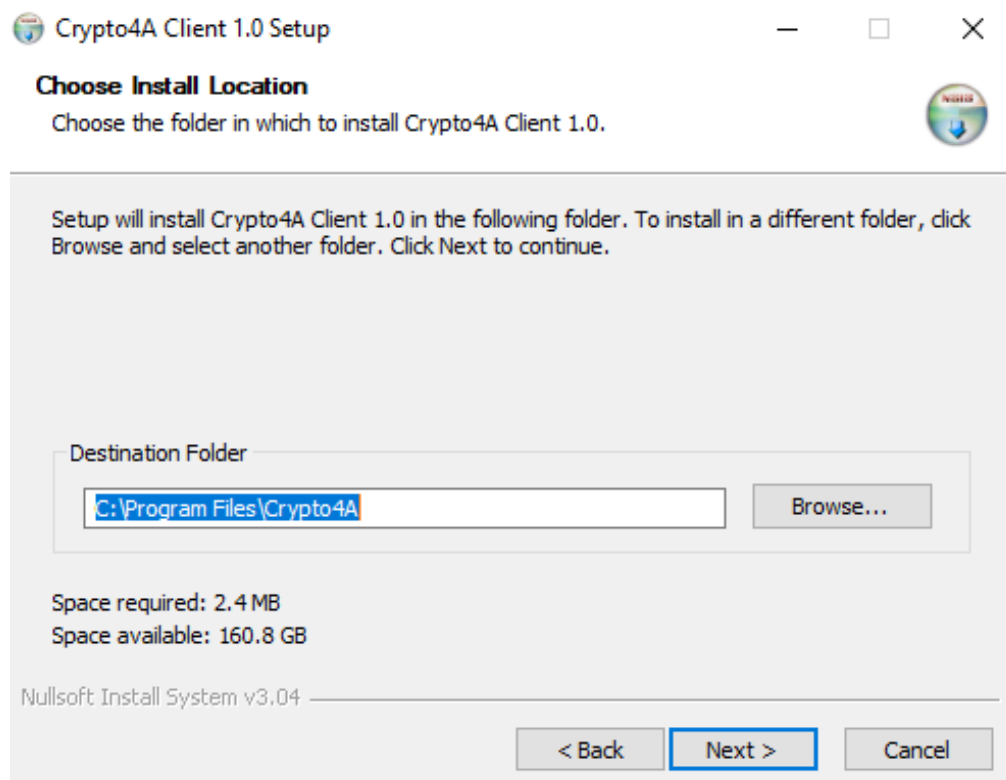
Install the Crypto4A spa-fwd package in the Windows server by double clicking the installer.



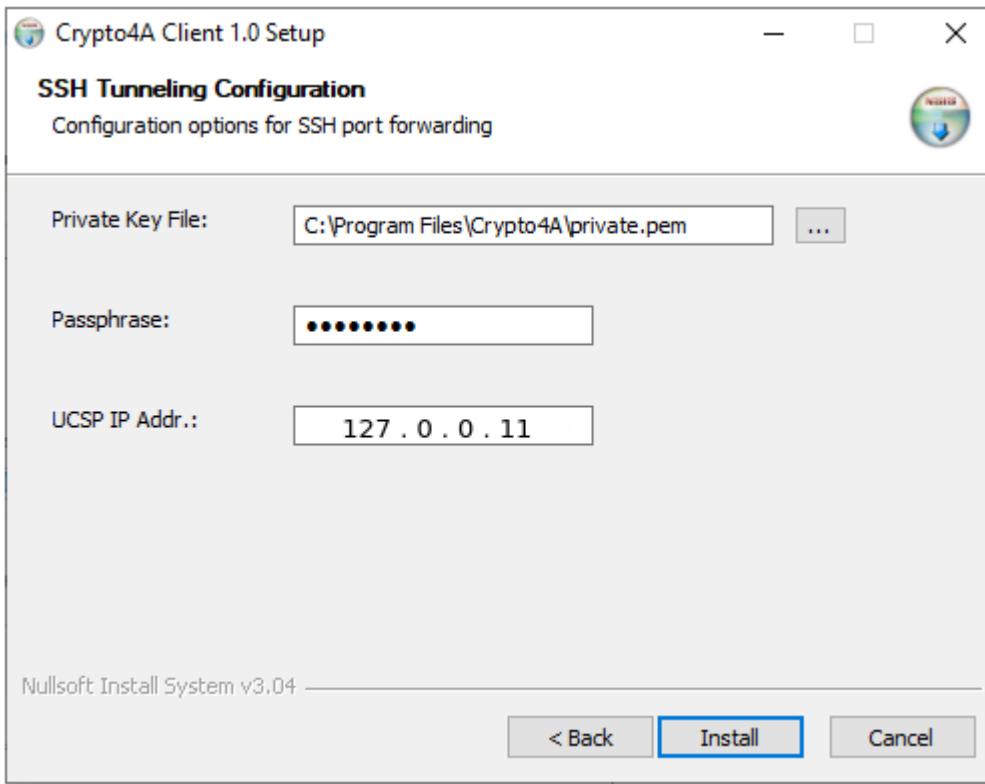
Click "Next".



Click "I Agree"



The default installation location is C:\Program Files\Crypto4A. Select a Destination folder (the default should be fine) and click "Next". The installation wizard will install the files (including PKCS#11 DLL) in the destination folder.

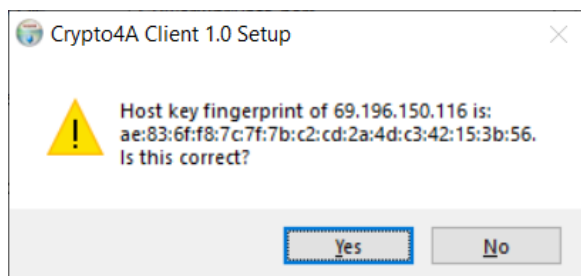


The **Private Key File** is the name of the passphrase-protected SSH key file to be used to connect securely to an SSH service running on a network-accessible QxEDGE™. Use a private key given by the QxEDGE™ administrator.

The **Passphrase** is the password which was used to protect the private key file when it was generated.

The **UCSP IP Address** (QxEDGE™) value is 127.0.0.11

Click the “Install” button, and it becomes “Check ...”, as the wizard is checking the connection with the QASM™. After a few seconds, a dialog should pop up:



It shows the QASM™ host key fingerprint. Check that the fingerprint is as expected to make sure it is connected to the correct host. Click “Yes” if the fingerprint is correct.

After another few seconds, the wizard will finish configuring the port forwarding and the installation is done.

Configuring HSM Key Management

Please see the following instructions for details on configuring HSM key management:

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/configuring-HSM-Key-Management.htm>

Make sure that the Vault Server is not running before configuring the HSM and importing the key.

In DBParm.ini, configure the **AllowNonStandard FWAddresses** parameter to open the Firewall and allow access to the HSM device:

```
AllowNonStandardFWAddresses=[127.0.0.1],Yes,1024:inbound/tcp,1024:outbound/tcp
```

Configure the PKCS#11 provider DLL and specify it in the **PKCS11ProviderPath** parameter in DBParm.ini:

```
PKCS11ProviderPath=C:\Program Files\Crypto4A\libpkcs11.dll
```

Save the DBParm.ini and close it.

The QASM™ does not require a PIN/passphrase but one still needs to be set up as part of the integration. From a windows command prompt, run the following command:

```
CAVaultManager SecureSecretFiles /SecretType HSM /Secret <hsmpincode>
```

(The PIN/passcode can be any 4-digit number)

Open DBParm.ini to check that the HSMPinCode parameter was added with the encrypted value of the PIN/passcode.

Import Server Key

The server key can be generated in the HSM, but this requires the re-encryption of the CyberArk database. It is recommended that the server key be imported into the HSM as this does not require re-encryption and is much faster.

Please run the following command to load the server key into the HSM using key wrapping which is required by the QxEDGE™:

```
CAVaultManager.exe LoadServerKeyToHSM /WrapKey
```

Check the command output to make sure that the key importation is successful. Open the DBParm.ini file again and change the ServerKey parameter to:

```
ServerKey=HSM
```

Re-start CyberArk server and make sure there are no error messages.

Port forwarding/Proxy from QxEDGE™ to Windows Server

The Windows Server is a guest OS inside QxEDGE™. To allow incoming connections to the Windows server and the CyberArk server, we need to set up port forwarding, so that the QxEDGE™ host can forward the request to CyberArk server. This can be done through iptables forwarding, or running a proxy server.

The easiest way is to use a proxy server such as “simpleproxy”:

```
sudo apt-get install -y simpleproxy
```

To start the proxy server:

```
simpleproxy -L 0.0.0.0:1858 -R 192.168.122.216:1858
```

The ip address 192.168.122.216 is the Windows server ip address, and should be replaced with the actual one.

The “simpleproxy” can be run inside a Linux screen session, or as a linux service.

To run it as a service, create a file /etc/systemd/system/simpleproxy.service with the following content:

```
[Unit]
Description=Simple Proxy for CyberArk
After=network.target
StartLimitIntervalSec=0

[Service]
Type=simple
Restart=always
RestartSec=1
User=sshuser
```

```
ExecStart=/usr/bin/simpleproxy -L 0.0.0.0:1858 -R 192.168.122.216:1858
```

```
[Install]
```

```
WantedBy=multi-user.target
```

Make sure the “User” field and the ip address for simpleproxy (ExecStart) are of the correct values.

To start the service:

```
sudo systemctl start simpleproxy
```

To stop the service:

```
sudo systemctl start simpleproxy
```

Complete

This completes the steps for the integration of the CyberArk Digital vault with the Crypto4A QxEDGE™. For additional information please contact us directly or by emailing support@crypto4A.com.