Integrate with CyberArk

Edit

The page covers details of WorkFusion integration with CyberArk products.

CyberArk Central Policy Manager

The integration allows CyberArk to communicate with the Intelligent Automation Cloud to manage the privileged user credentials. With this plugin, the privileged user for WorkFusion will need to log in to the CyberArk Vault to gain access to the credentials to perform their configuration changes. CyberArk will also be able to monitor and report on that activity.

> TIP
>
> For details and integration support, refer to CyberArk CPM documentation.

CyberArk Privileged Session Manager

The integration serves as a jump server between the CyberArk Vault and the Intelligent Automation Cloud. When a privileged user logs in to the Vault, instead of receiving the credentials and then manually logging into the Intelligent Automation Cloud, they will see a link that will connect them without ever seeing the credentials. CyberArk will also be able to record each mouse click and keystroke of the person using the credentials. This is an isolated session, so the user will not be able to use this connection to move laterally throughout the network and the SOC will be able to kill any session that looks suspicious.

> TIP
>
> For details and integration support, refer to CyberArk PSM documentation.

CyberArk Application Access Manager

> NOTE
>
> Since v9.1

The integration enables the storage of automated application passwords and RPA bot passwords in CyberArk AAM.

Prerequisites

CyberArk components installed:

- CyberArk Vault
- CyberArk PrivateArk
- CyberArk PAS (web API)
- CyberArk AIM (Central Credential Provider + Central Credential Provider Web Service)

CyberArk is integrated into the infrastructure:

- Credentials for the automated application are stored in CyberArk safe
- Credentials for RPA bot users are stored in CyberArk safe

> **TIP**
>
> For details, refer to CyberArk AAM documentation.

WorkFusion configuration:

- The Bot Master user is reserved for the startup of the bots and supports the standard Windows authentication mechanism.
- WorkFusion servers are authorized to access CyberArk AIM Web Service

Automate application integrated with CyberArk

Use case: the application being automated is already integrated with CyberArk. In order to access it, RPA bot logic needs to retrieve the password from CyberArk.

To retrieve credentials in bot config, a call to CyberArk API needs to be performed as in the example below.

Expand to see sample bot config

Store RPA infrastructure passwords in CyberArk

Use case: Windows passwords to RPA bot machines are to be stored in CyberArk.

Only bot agents' passwords can be stored in CyberArk. The Bot Master user needs to support the standard authentication mechanism.

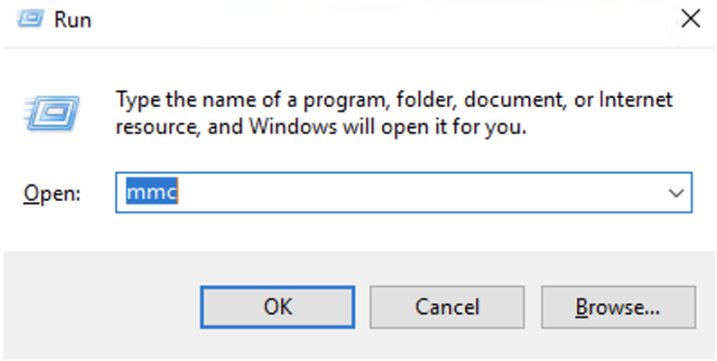
Bot Master user is a "patient 0" which will invoke CyberArk API, retrieve credentials to individual RPA bots, and initiate the startup of the RPA bots.

In the default setup, there is one Bot Master on each RPA server.

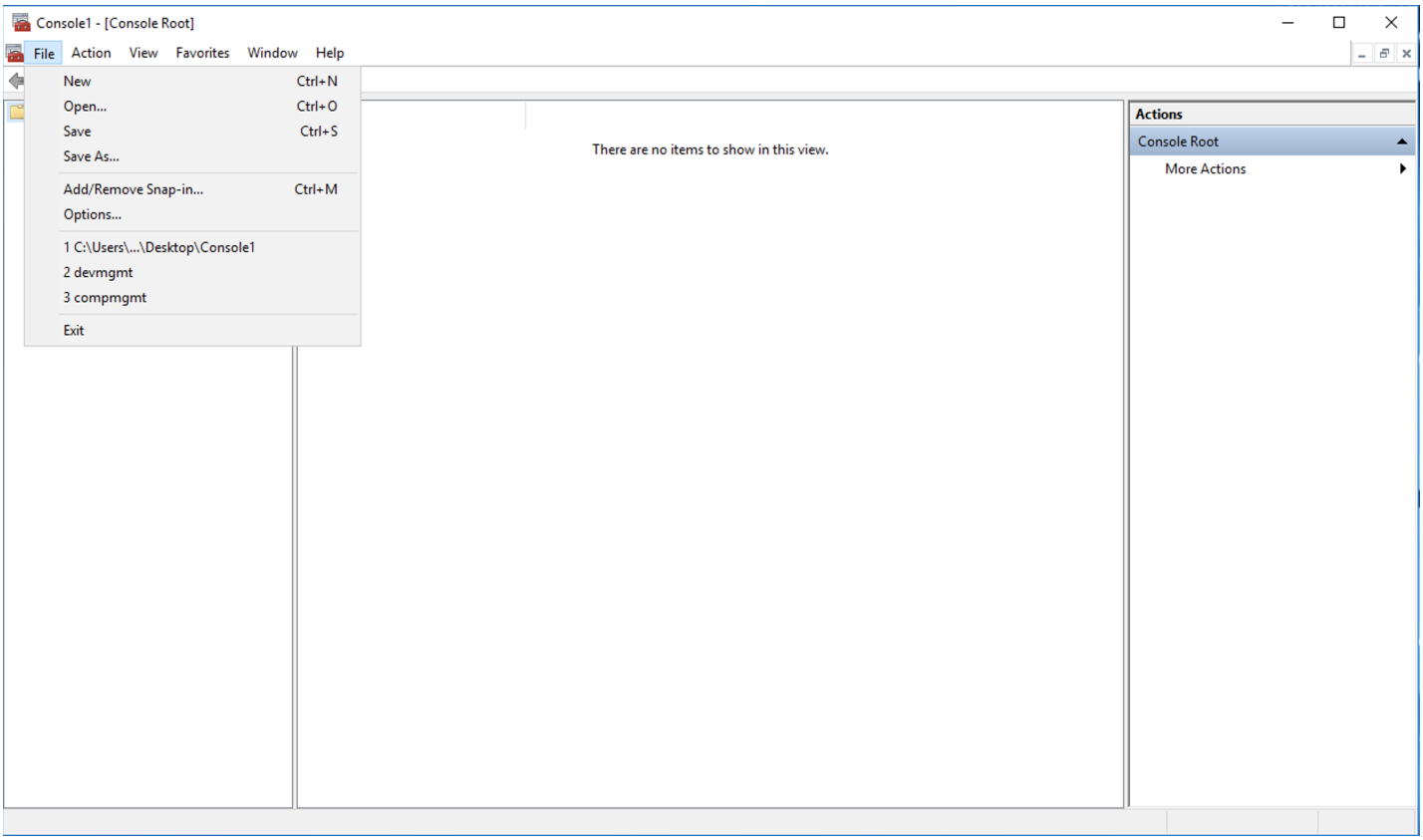
Enable certificate-based authentication with shared user (mTLS)

Log in to an RPA machine as Bot Master and download the certificates provided by CyberArk AIMWebService. Follow the steps below to install the certificate to the RPA machine.

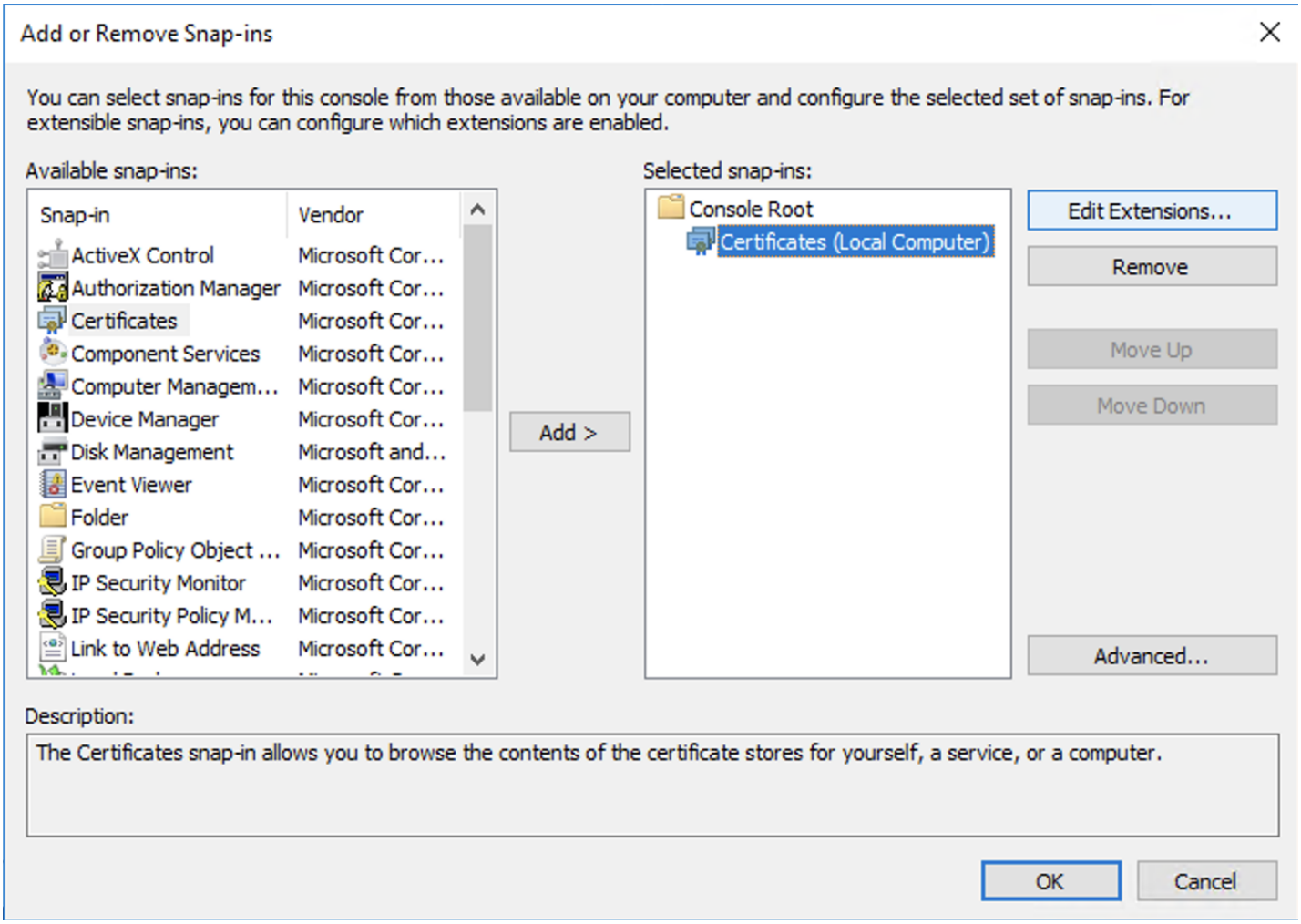
1. Open **Run** (Windows+R) and execute `mmc` (Microsoft Management Console).



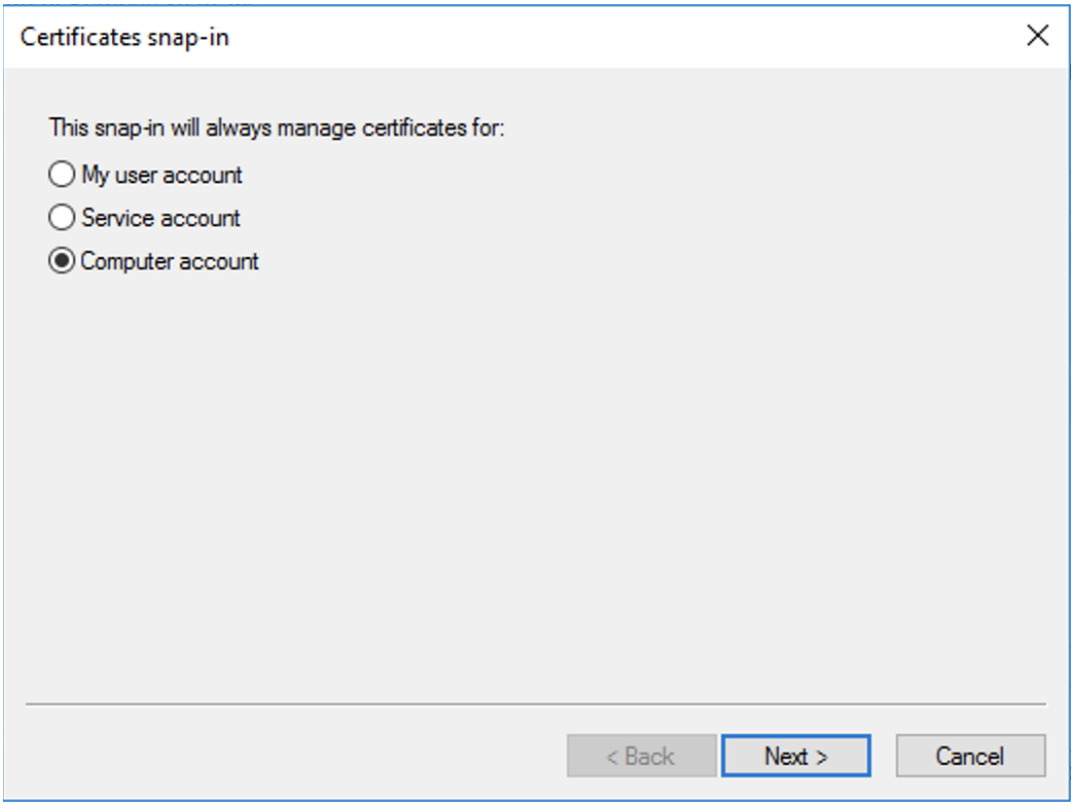
2. In the MMC application, click on **File > Add/Remove Snap-in** (Ctrl+M).



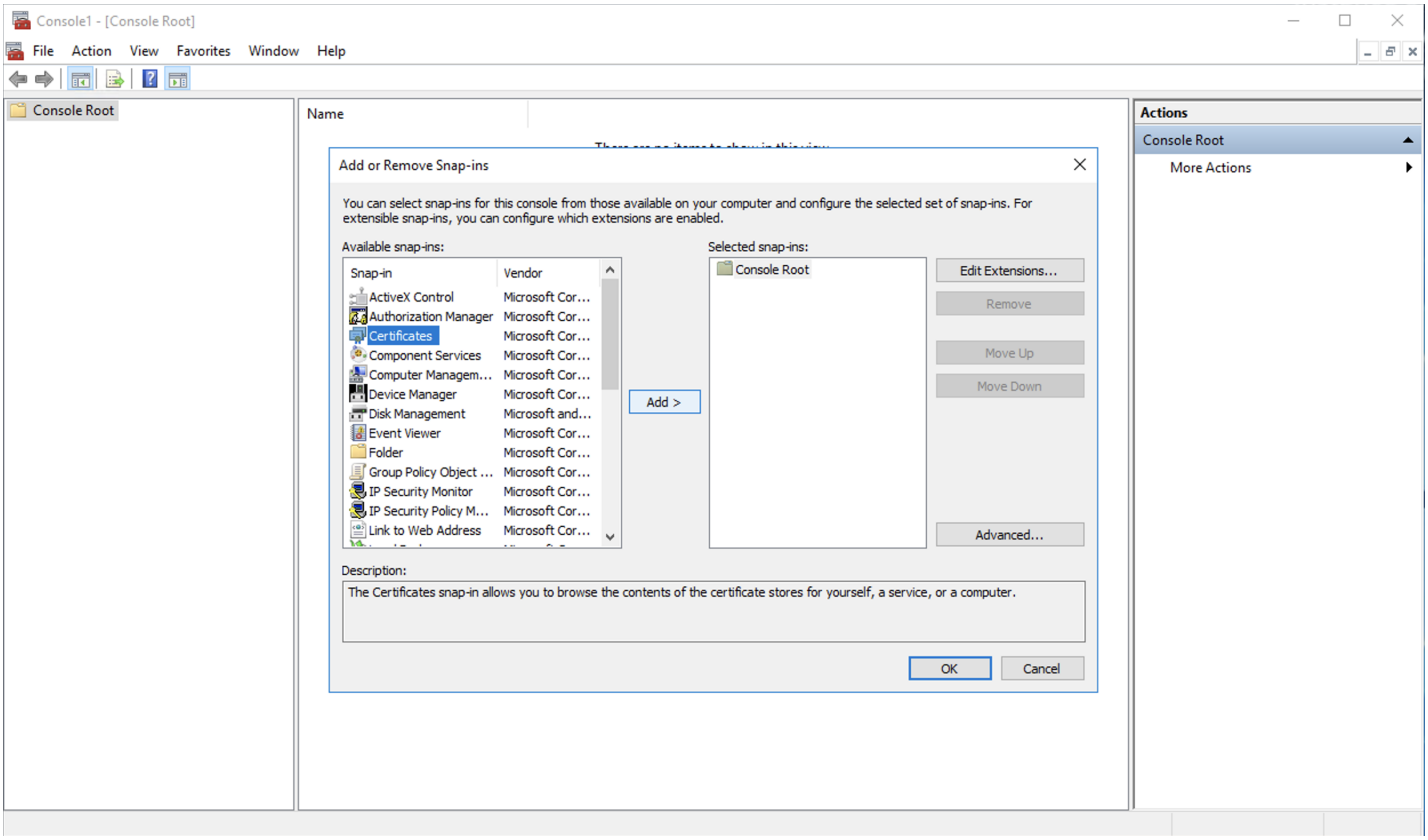
3. Select **Certificate** in the left column.



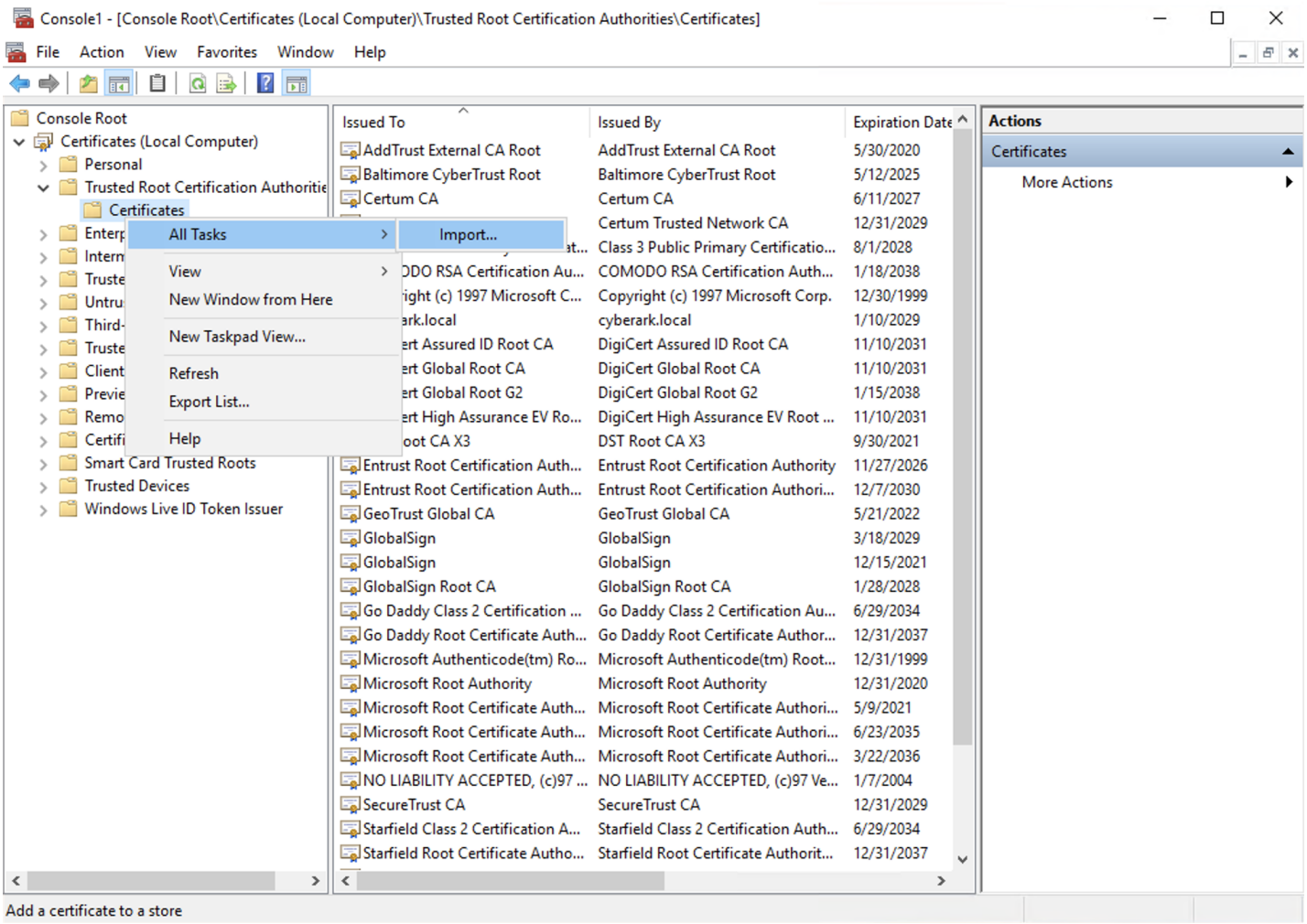
4. Select **Computer account** in the popup.

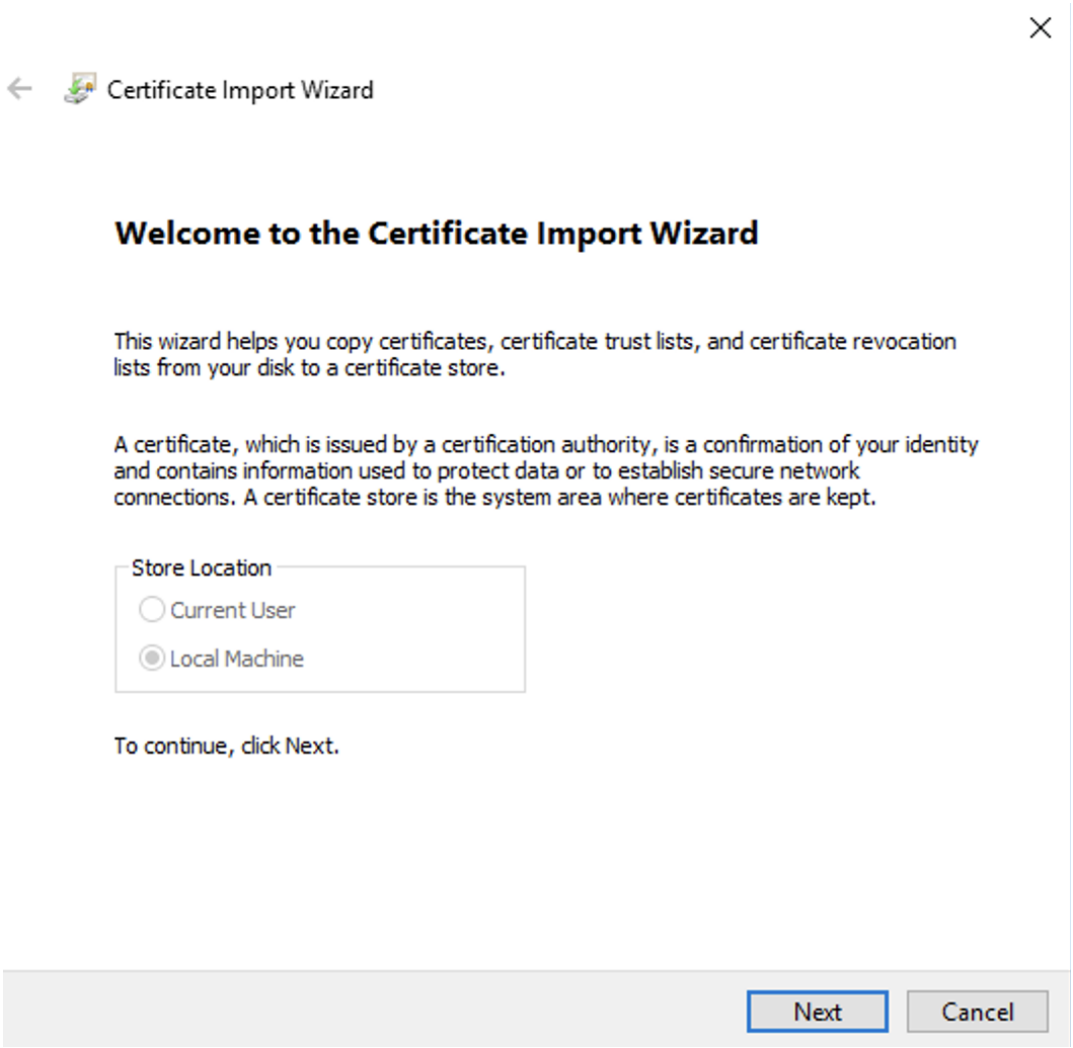


5. Click **Next** and then **OK** to create **Certificates** for your local computer.

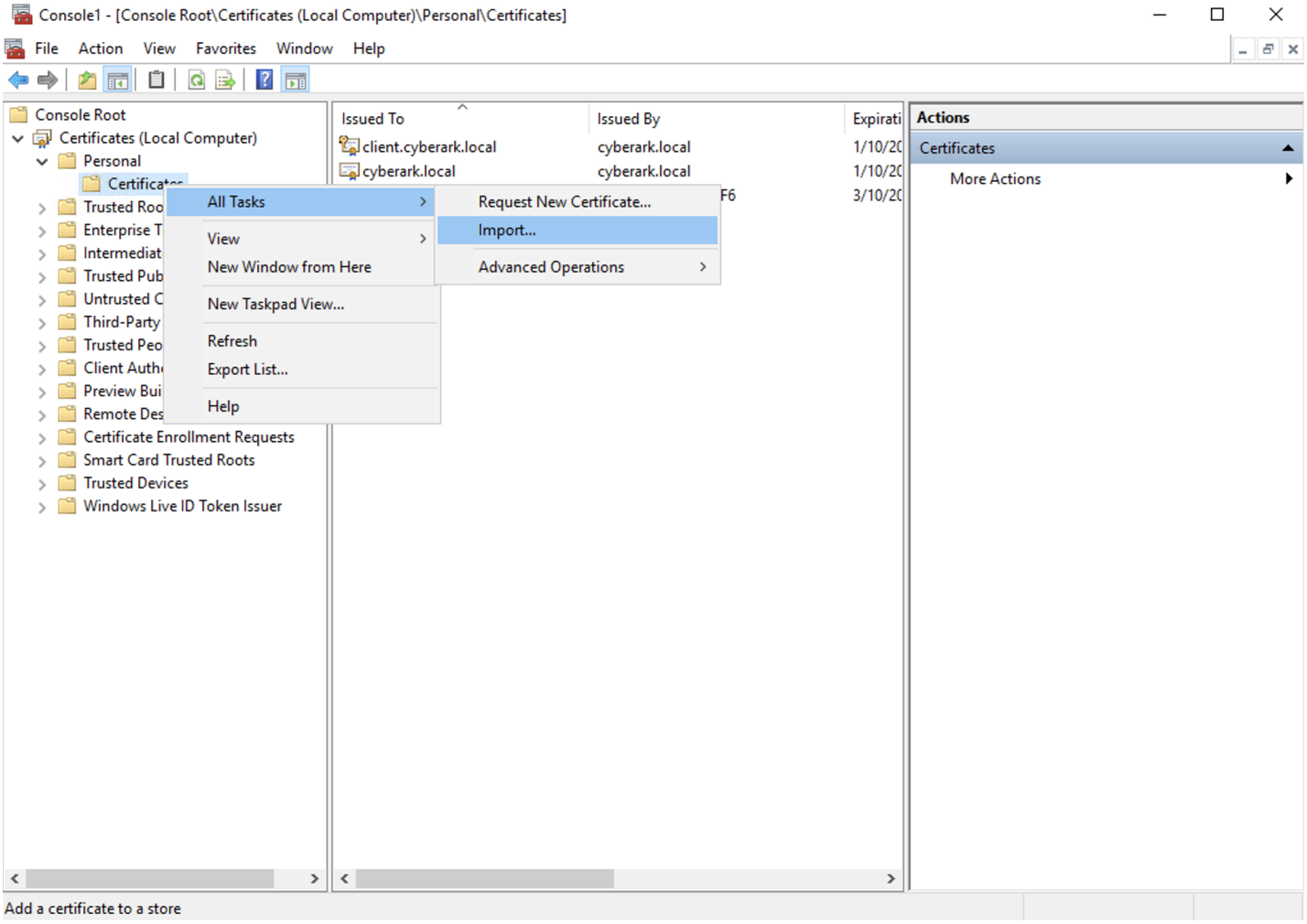


6. Expand **Trusted Root Certification Authorities** inside the **Certificates** folder and right-click on **Certificates** to import the root certificate provided.

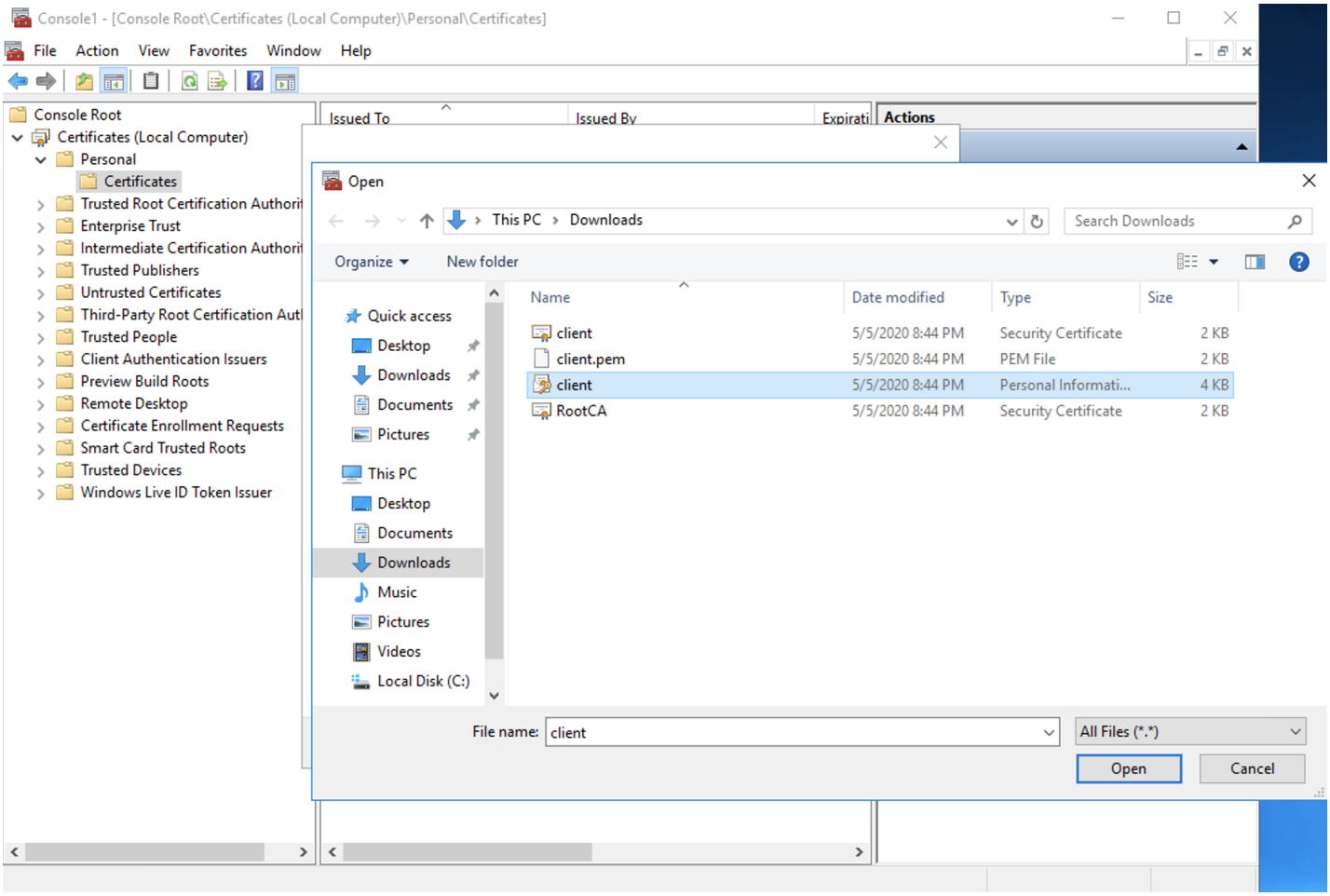

Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Certificates
Enterp
Intern
Truste
Untru
Third-
Truste
Client
Previe
Remo
Certifi
Smart Card Trusted Roots
Trusted Devices
Windows Live ID Token Issuer
All Tasks
View
New Window from Here
New Taskpad View...
Refresh
Export List...
Help
Import...
Issued To
Issued By
Expiration Date
AddTrust External CA Root AddTrust External CA Root 5/30/2020
Baltimore CyberTrust Root Baltimore CyberTrust Root 5/12/2025
Certum CA Certum CA 6/11/2027
Certum Trusted Network CA 12/31/2029
Class 3 Public Primary Certificatio... 8/1/2028
COMODO RSA Certification Au... COMODO RSA Certification Auth... 1/18/2038
ight (c) 1997 Microsoft C... Copyright (c) 1997 Microsoft Corp. 12/30/1999
ark.local cyberark.local 1/10/2029
ert Assured ID Root CA DigiCert Assured ID Root CA 11/10/2031
ert Global Root CA DigiCert Global Root CA 11/10/2031
ert Global Root G2 DigiCert Global Root G2 1/15/2038
ert High Assurance EV Ro... DigiCert High Assurance EV Root ... 11/10/2031
oot CA X3 DST Root CA X3 9/30/2021
Entrust Root Certification Auth... Entrust Root Certification Authority 11/27/2026
Entrust Root Certification Auth... Entrust Root Certification Authori... 12/7/2030
GeoTrust Global CA GeoTrust Global CA 5/21/2022
GlobalSign GlobalSign 3/18/2029
GlobalSign GlobalSign 12/15/2021
GlobalSign Root CA GlobalSign Root CA 1/28/2028
Go Daddy Class 2 Certification ... Go Daddy Class 2 Certification Au... 6/29/2034
Go Daddy Root Certificate Auth... Go Daddy Root Certificate Author... 12/31/2037
Microsoft Authenticode(tm) Ro... Microsoft Authenticode(tm) Root... 12/31/1999
Microsoft Root Authority Microsoft Root Authority 12/31/2020
Microsoft Root Certificate Auth... Microsoft Root Certificate Authori... 5/9/2021
Microsoft Root Certificate Auth... Microsoft Root Certificate Authori... 6/23/2035
Microsoft Root Certificate Auth... Microsoft Root Certificate Authori... 3/22/2036
NO LIABILITY ACCEPTED, (c)97 ... NO LIABILITY ACCEPTED, (c)97 Ve... 1/7/2004
SecureTrust CA SecureTrust CA 12/31/2029
Starfield Class 2 Certification A... Starfield Class 2 Certification Auth... 6/29/2034
Starfield Root Certificate Autho... Starfield Root Certificate Authorit... 12/31/2037
Actions
Certificates
More Actions
Add a certificate to a store


Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
Store Location
Current User
Local Machine
To continue, click Next.
Next
Cancel

7. Expand **Personal** inside the **Certificates** folder and right-click on **Certificates** to import the PFK file.



8. Right-click on the imported certificate and select **Open**.



9. Navigate to the **Details** tab and note down the value for **Thumbprint**. This will be used while connecting to the CyberArk service from the PowerShell script you are going to create.

Retrieve credentials from CyberArk using PowerShell

Bot Master will retrieve credentials from CyberArk using PowerShell.

First, the script needs to be written and tested with pure PowerShell.

Example variables and parameters:

```
param([string] $baseURL, [string] $appId, [string] $safe, [string] $objectName,
[string] $certificateThumbprint)

# Variables
$serverAddress = 'localhost'

# Param example
#$baseURL = 'https://cyberarkserver:port'
#$appId = 'WorkFusion'
#$safe = 'WorkFusionBot'
```

Copy

```
#$objectName = 'WF-Bot-Test'
#$certificateThumbprint = '023A534542CB2454'
```

1. Create a header object to set `Content-Type` .

```
$headers = New-Object "System.Collections.Generic.Dictionary[[String],[String]]"
$headers.Add('Content-Type','application/x-www-form-urlencoded')
```

Copy

2. Set security settings for an HTTPS request.

```
[Net.ServicePointManager]::SecurityProtocol = "tls12, tls11, tls"
```

Copy

3. Retrieve the added certificate using the passed certificate thumbprint.

```
$cert = Get-ChildItem -Path Cert:\CurrentUser\My\$certificateThumbprint
```

Copy

4. Make a GET request to CyberArk.

```
$response = Invoke-WebRequest "$baseURL/AIMWebService/api/Accounts?
AppID=$appId&Safe=$safe&Object=$objectName" -Method 'GET' -Headers $headers -
Certificate $cert
```

Copy

5. Convert the response content to a JSON object.

```
$responseObj = $response.Content | ConvertFrom-Json
```

Copy

6. Cache credentials in the Windows security storage for the server.

```
cmdkey /add:$serverAddress /user:$userName /pass:$password
```

Copy

7. Start an RDP session.

```
mstsc /v:$serverAddress
```

Copy

Use the PowerShell script to start bot agent RDP session

To configure a bot agent to use credentials from CyberArk, do as follows.

1. Modify the following configuration in **{INSTALL_DIR}\wfagent\conf\wfagent-hub.yml** for 9.x, and **{INSTALL_DIR}\bot-agent\conf\bot-agent-master.yml** for 10.x.

   Configuration to modify:

   Copy

   ```
   - id: rdp0
     expression: "cmd /c start /wait node0.RDP"
     directory: "rdp"
     enabled: "${environment.node0_enabled:true}"
   ```

2. Place the PowerShell script created in the previous step to **{INSTALL_DIR}\wfagent\bin** for 9.x, and **{INSTALL_DIR}\bot-agent\bin** for 10.x. The modified configuration will look like below.

   Modified configuration:

   Copy

   ```
   - id: rdp0
     expression: "cmd /c start /wait powershell .\\rdp_connection.ps1 -baseURL
   https://cyberarkserver:port -appId WorkFusion -safe WorkFusionBot -objectName
   workfusion-bot-1 -certificateThumbprint 023423AC43535BA23434"
     tag: "rdp"
     directory: "bin"
     enabled: "${environment.node0_enabled:true}"
   ```

> **NOTE**
>
> The script can be placed wherever you wish inside **wfagent/bot-agent**. Make sure the directory is mentioned in the .yml file.

3. Perform these modification steps for each bot configuration with their corresponding CyberArk Object Name.