EVERTRUST

WinHorizon

Version 2.0, 2026-02-20

Table of Contents

Chapter 1. Installation

1.1. Introduction

Description

WinHorizon is the EverTrust WCCE proxy solution part of EverTrust Horizon suite.

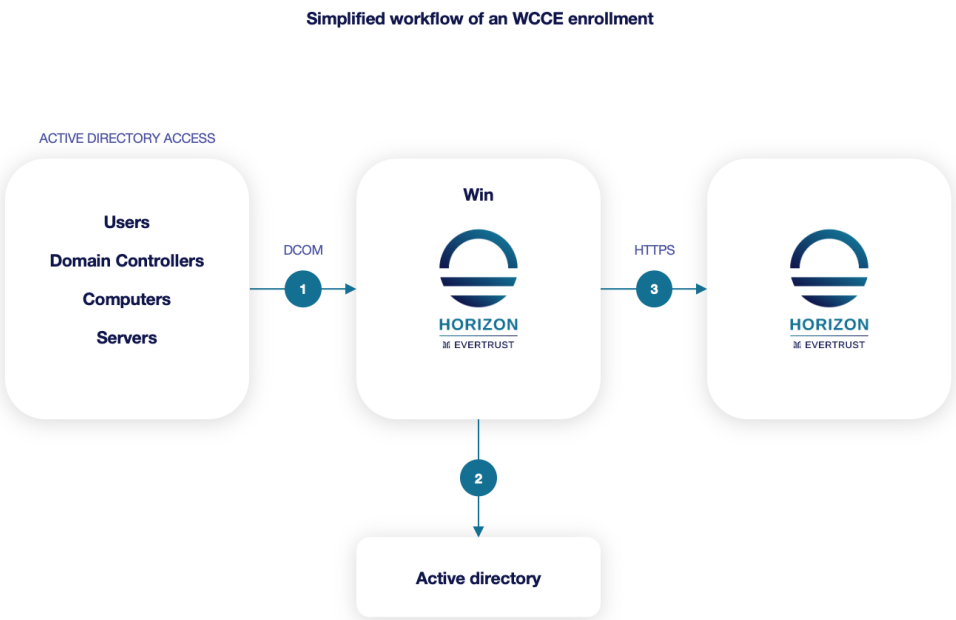
This document is specific to WinHorizon version **2.0**.

WinHorizon allows to connect Horizon to Windows Certificate Enrollment (WCCE) in order to issue certificates from an Active Directory environment.

Managing certificate lifecycle through the WCCE protocol involves up to three components:

- One or more Active Directory assets (domain controller, server, workstation, user) as WCCE Client,
- WinHorizon as the Active Directory enrollment service,
- Horizon as the WCCE proxy.

The protocol paradigm can be described as follows: **Every Windows Active Directory member (machines, users) can use DCOM interfaces to interact with a CA to request certificate enrollment**.



Installation

To install WinHorizon, please refer to the Installation Procedure section.

Uninstallation

To uninstall WinHorizon, please refer to the Uninstallation Procedure section.

1.2. Specifications & Requirements

You have to deploy WinHorizon inside an Active Directory forest.

Requirements

Hardware requirements

The following elements are considered as hardware requirements:

- 50 GB of disk (at least);
- 4 GB of RAM (at least).

Operating system requirements

The operating system should be installed using an english install ISO. The following elements are considered as operating system requirements:

- Microsoft Windows Server 2016 (64-bit);
- Microsoft Windows Server 2019 (64-bit);
- Microsoft Windows Server 2022 (64-bit).
- Microsoft Windows Server 2025 (64-bit).

Active Directory requirements

The following elements are considered as Active Directory system requirements:

- Active Directory Schema version: 30 or higher;
- Domain Controller(s) OS version: Microsoft Windows Server 2003 or higher;
- Forest functional level: Microsoft Windows Server 2003 or higher.

Prerequisites

This section describes the system and software pre-requisites to install WinHorizon.

System prerequisites

The following elements are considered as system pre-requisites:

- Server must be part of a domain of your Active Directory forest;
- Access with administrative privileges to the server mentioned above;

- An account with Full Control permissions on Public Key Services (Sites and Services > Services > Public Key Services) who can open sessions on WinHorizon's server or an enterprise administrator account.

Network prerequisites

The following network flows must be opened:

Source	Destination	Port	Description
`CLIENTS_IP`	`WINHORIZON_IP`	1024-65535/TCP, 1024-65535/UDP, 135/TCP	Clients using DCOM to retrieve certificates through WinHorizon
`WINHORIZON_IP`	`AD_IP`	3269/TCP, 3268/TCP, 389/TCP, 389/UDP, 636/TCP, 88/TCP and 88/UDP	WinHorizon connects to Active Directory component
`WINHORIZON_IP`	`HORIZON_IP`	443/TCP	WinHorizon connects to Horizon instance using mutual SSL authentication
`WINHORIZON_IP`	`CRLDP_IP or OCSP_IP`	80/TCP	WinHorizon retrieves CRL or perform OCSP request

Client prerequisites

To be able to enroll using WCCE protocol through WinHorizon, the client machines must run one of the following operating systems:

- Microsoft Windows 10;
- Microsoft Windows 11;
- Microsoft Windows Server 2016;
- Microsoft Windows Server 2019;
- Microsoft Windows Server 2022.

1.3. Installation Procedure

Installation Procedure

Before proceeding with the installation, please ensure that all the Specifications & Requirements are met.

This section details how to install WinHorizon.

Download the latest version of the package **winhorizon-2.0.msi** from Evertrust Repo repo.evertrust.io

WinHorizon is contained in only one package:

- winhorizon-2.0.msi

1. Log in to the WinHorizon server with **administrative privileges**.

2. Double-click on **winhorizon-2.0.msi**.

3. The welcome screen of the install wizard appears. Click on **Next**.

4. The End-User License Agreement screen of the wizard appears. Click on **Next**.

5. The install location screen appears. Choose your installation location or keep the default.

6. In the event of a product upgrade you will be prompted to choose if you want to keep your previous configuration. If you are doing a fresh install, this step will not appear.

7. A recap screen appears to remind you of your choices. Click **Install**.

8. When the install is successful, click **Finish**. If your installation has failed, you can view the installation logs with the **View Log** button.

The installation results in the creation of:

- EverTrust WinHorizon Configurator application (located in the install directory and named **WinHorizonConfig.exe**);
- EverTrust WinHorizon service (accessible using **services.msc**).

Configuration

After installation, please refer to the Initial Configuration section to configure WinHorizon.

1.4. Initial Configuration

Initial Configuration of WinHorizon

Before proceeding with the setup, please ensure that WinHorizon is correctly installed.

Publishing the Trust Chain

This section details how to publish the trust chain within Active Directory.

If several WinHorizon servers are installed, the procedure detailed in this section must only be executed once. If the trust chain is already published, this procedure does not need to be performed.

1. Launch a 'cmd.exe' using a privileged account (using the 'RunAs' command);

2. Execute the following command to add Root CA:

```
certutil -f -dspublish "C:\<PATH_TO_ROOT_CA_CERTIFICATE>" rootca
```

3. Execute the following command to add Subordinate CA:

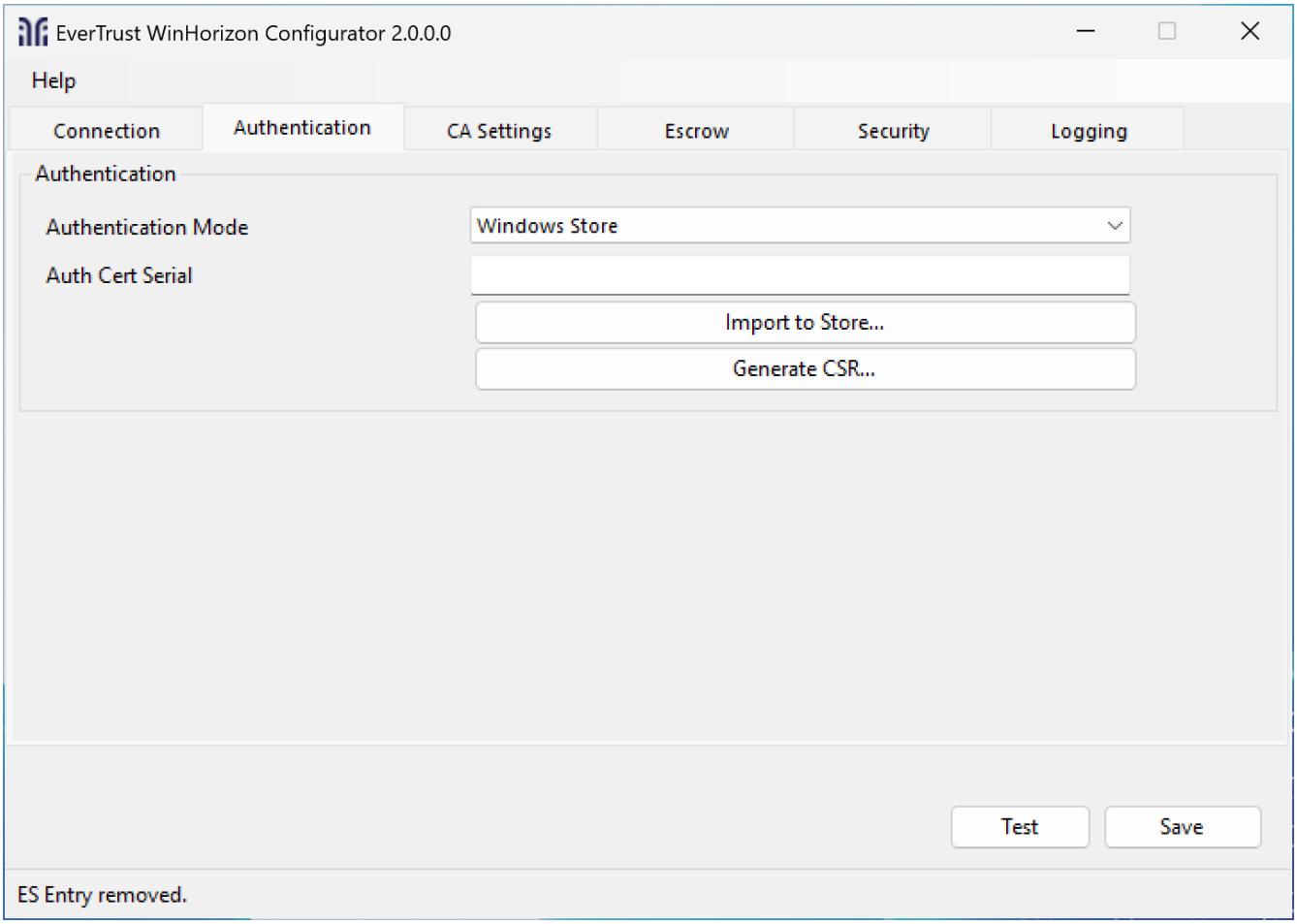
```
certutil -f -dspublish "C:\<PATH_TO_SUBORDINATE_CA_CERTIFICATE>" subca
```

4. Execute the following command to push new Active Directory schema:

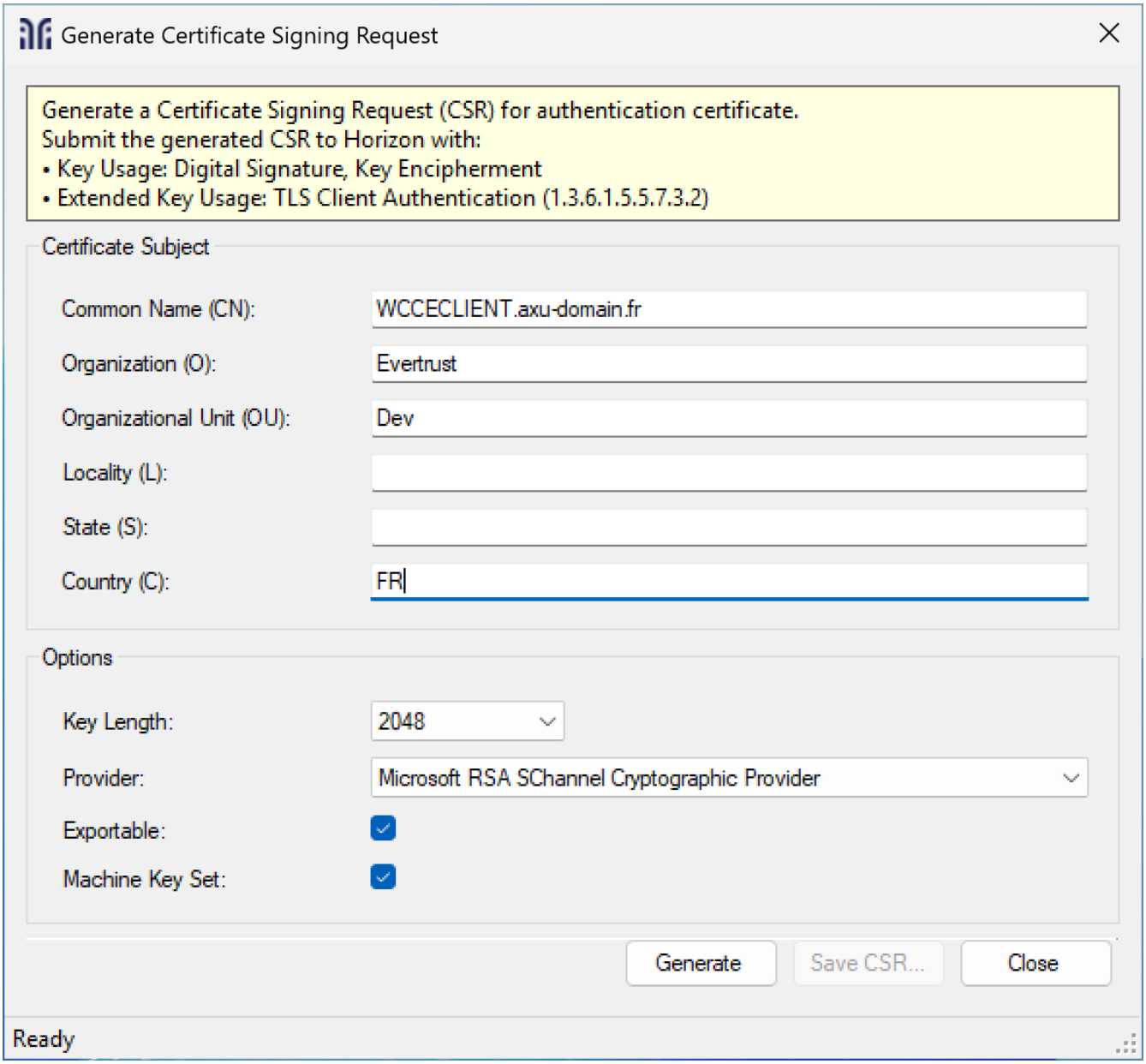
```
certutil -pulse
```

Request WinHorizon Authentication Certificate

Open the EverTrust WinHorizon Configurator and go to the **Authentication** tab.

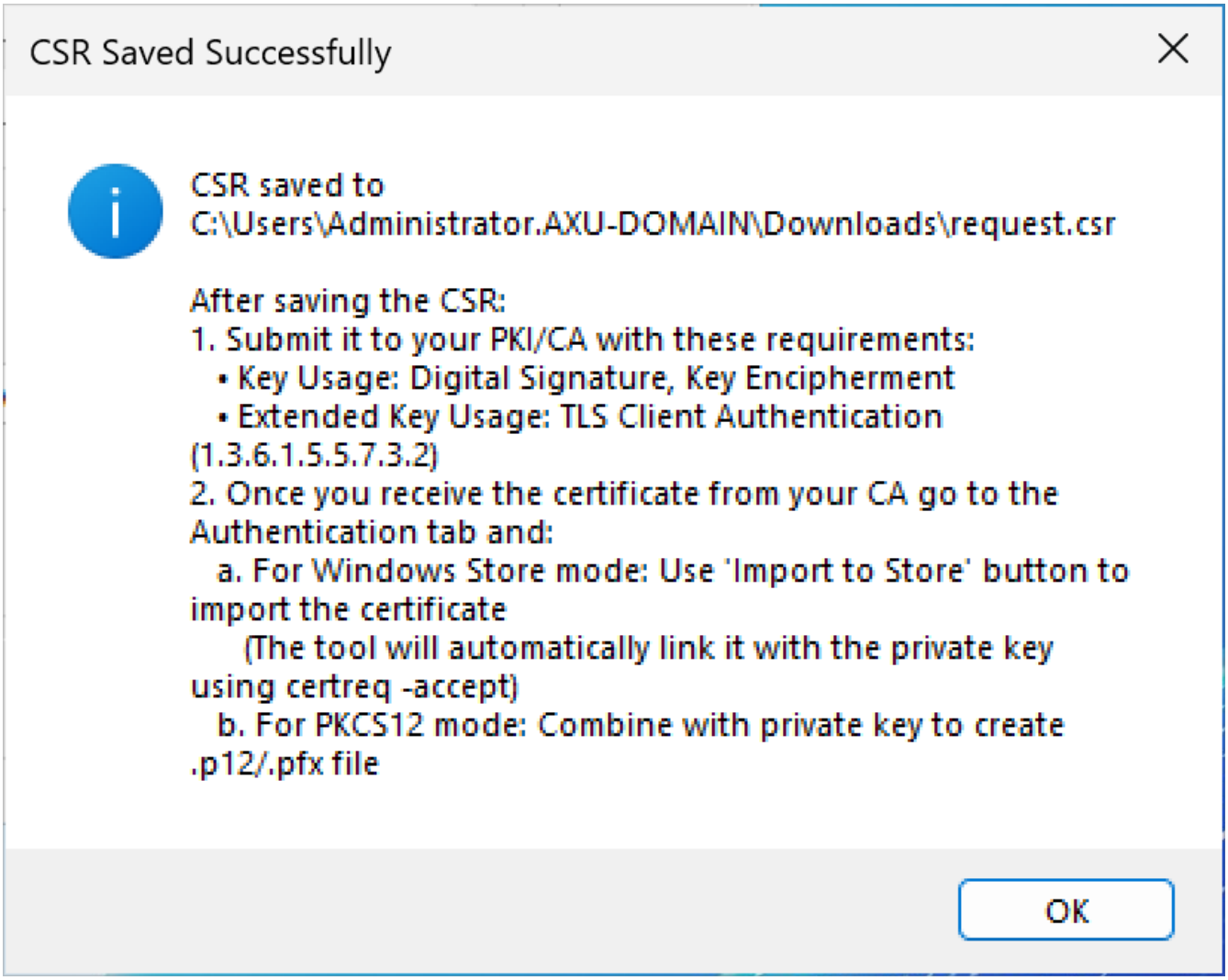


Then click the **Generate CSR** button and fill in the fields you need, leave a field blank if it is not needed (it will not appear in the CSR).



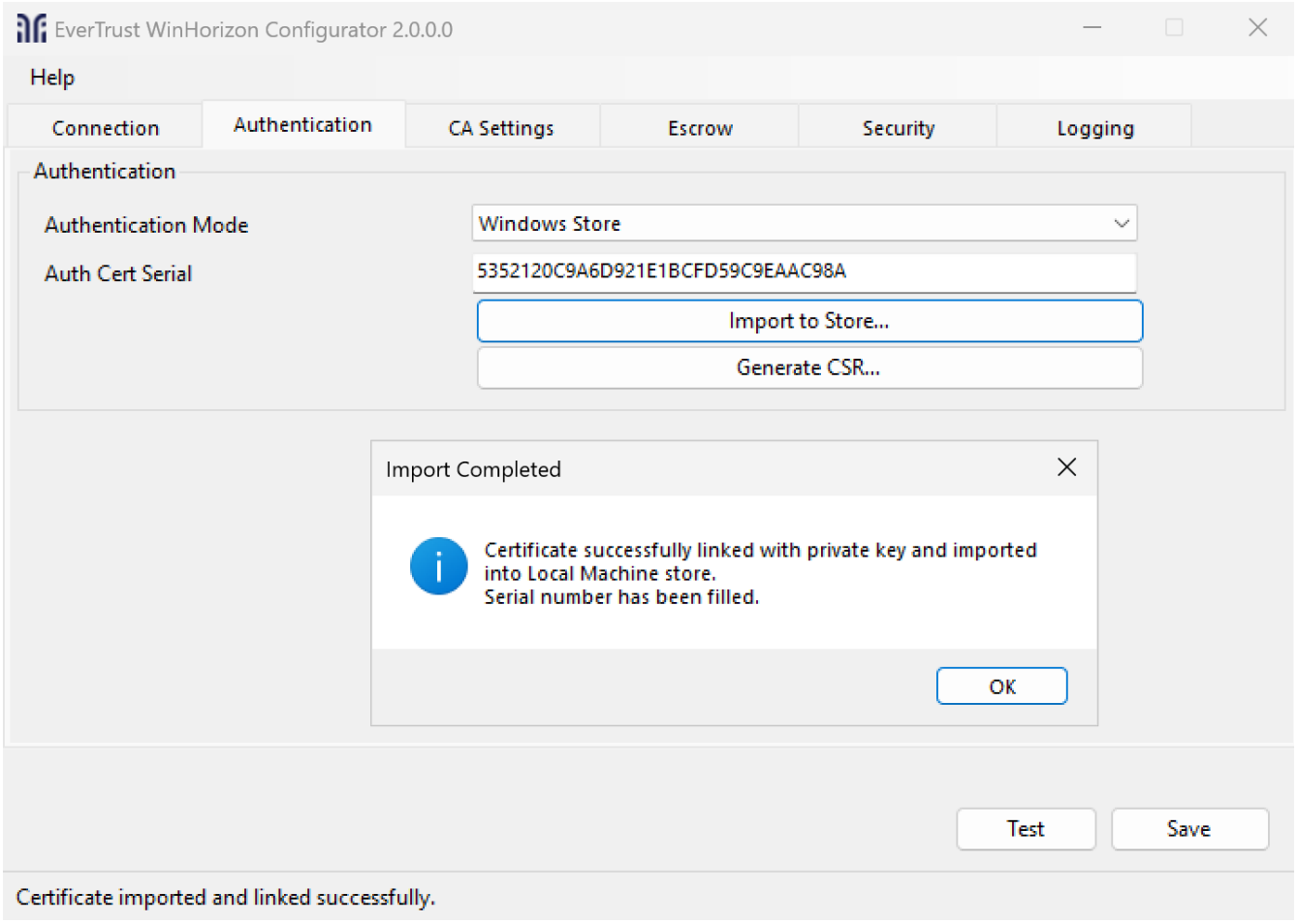
We recommend leaving the options as default.

When you have completed all the necessary fields, click the **Generate** button and then use the **Save CSR** button to save the CSR somewhere you can find it.



Use this CSR to sign the certificate with your PKI / CA and download the newly created certificate in PEM format.

After downloading the certificate, go back to the Authentication tab, click the **Import Certificate** button and choose the certificate.



Check that you are in the "Windows store" authentication mode.

After a successful import, you should see a confirmation message as well as the serial number being filled in the specific field. If the import errors out, the serial will also be filled, but you will need to reconcile the request or restart the authentication certificate step.

Don’t close the configurator since it will be needed afterward.

TLS 1.2 Configuration

Before proceeding, you need to activate TLS v1.2. To enable TLS 1.2, please add the following registry entries:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\WinHttp]
      "DefaultSecureProtocols" = (DWORD): 0xAA0
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet
Settings\WinHttp]
      "DefaultSecureProtocols" = (DWORD): 0xAA0

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v2.0.50727]
      "SystemDefaultTlsVersions" = dword:00000001
```

```
      "SchUseStrongCrypto" = dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
      "SystemDefaultTlsVersions" = dword:00000001
      "SchUseStrongCrypto" = dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727]
      "SystemDefaultTlsVersions" = dword:00000001
      "SchUseStrongCrypto" = dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v4.0.30319]
      "SystemDefaultTlsVersions" = dword:00000001
      "SchUseStrongCrypto" = dword:00000001
```

You can also directly download this .reg file and execute it on the concerned server. Note that it has the .txt extension to not be flagged as dangerous by antiviruses but if you want to use it, you will have to give it back the .reg extension.

Active Directory Configuration

To access the Microsoft Certificate Template, you should install Remote Server Administration Tools (RSAT). If it's not on your windows server, you can follow the steps below to install it:

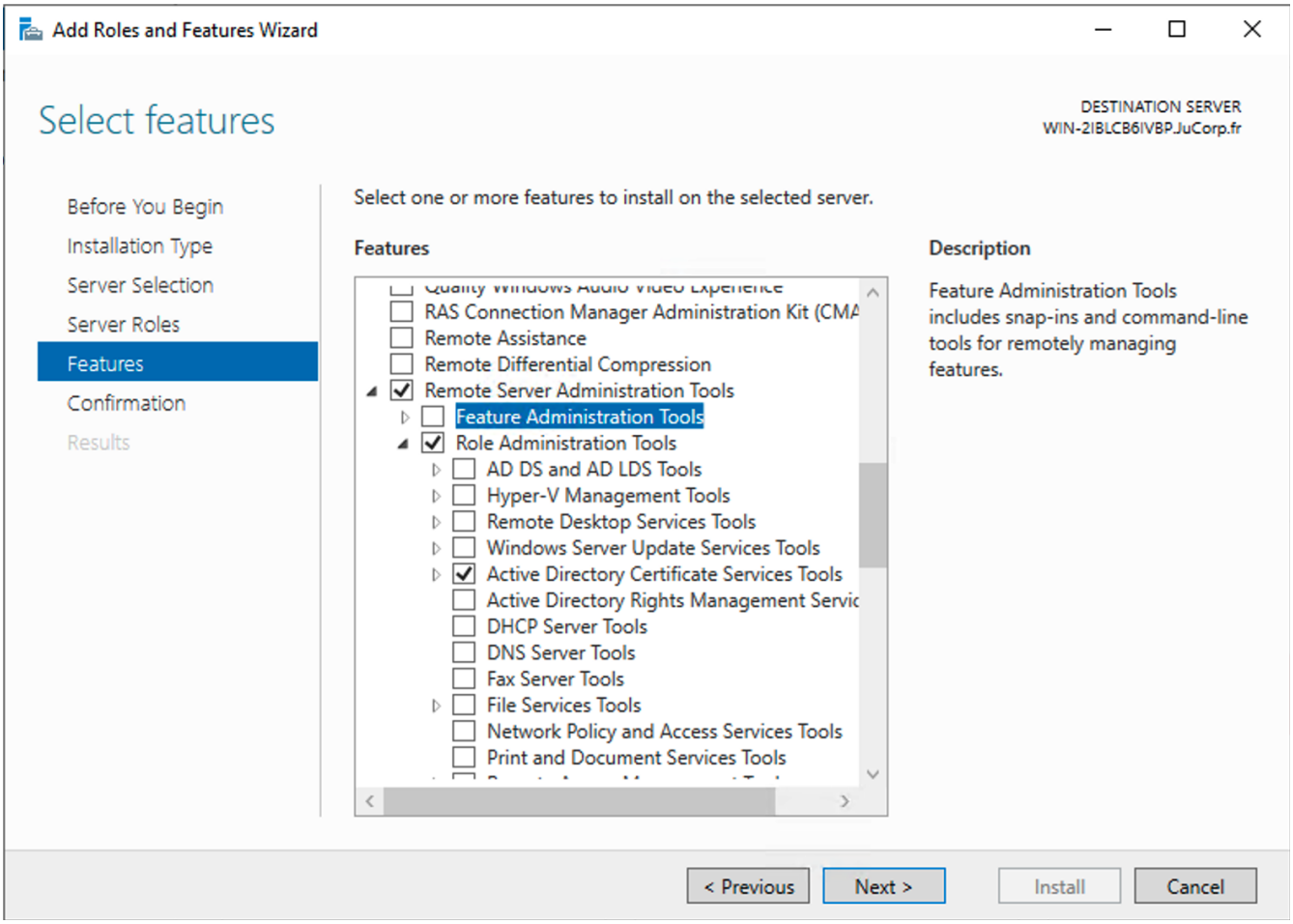
1. Open the **Server Manager** tool.

2. Select **Manage** > **Add Roles and Features**.

3. Select **Features** and expand **Remote Server Administration Tools** > **Role Administration Tools** > **Active Directory Certificate Services Tools**.

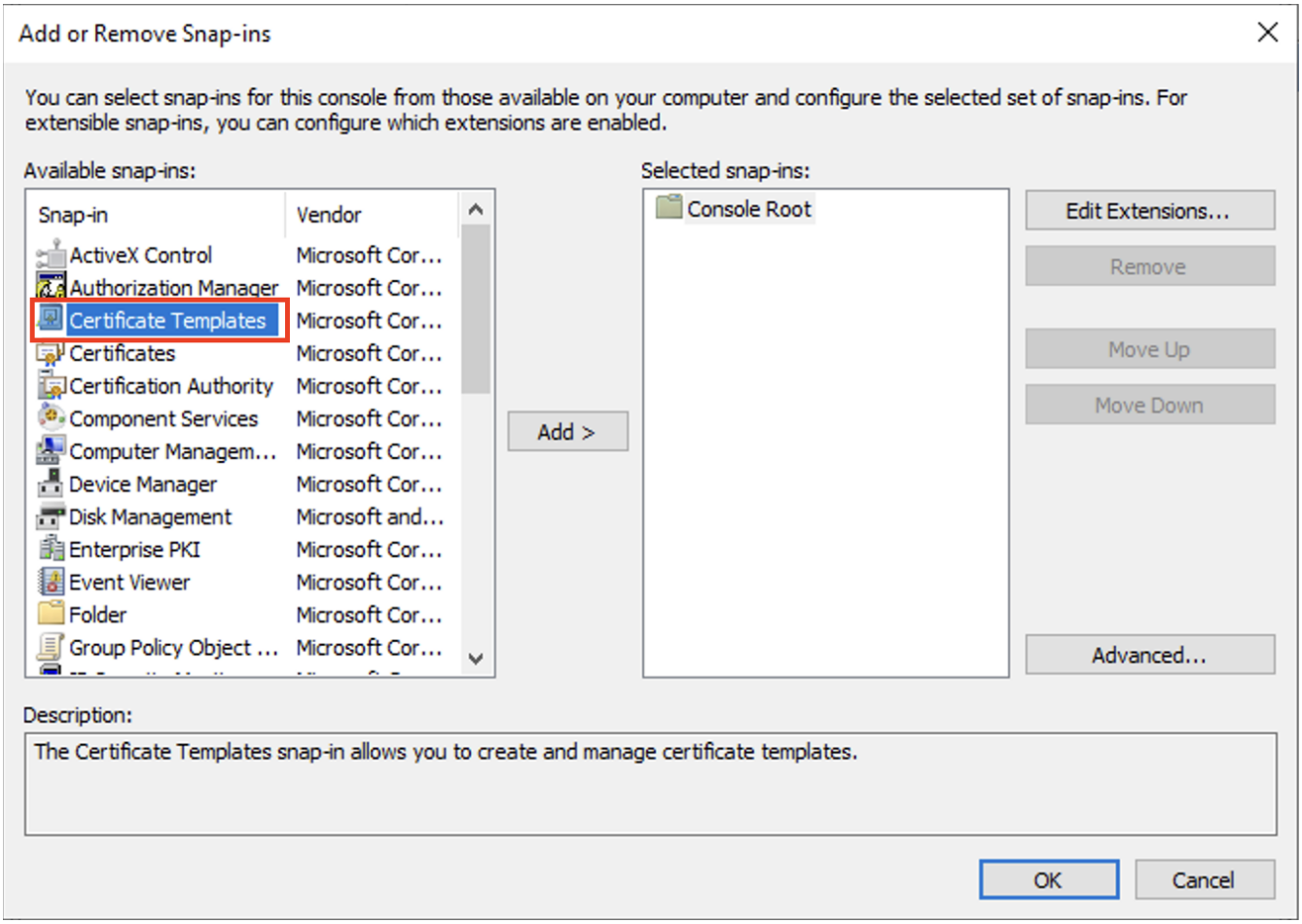
4. Select **Certification Authority Management Tools**.

5. Select **Next** and then select **Install**.

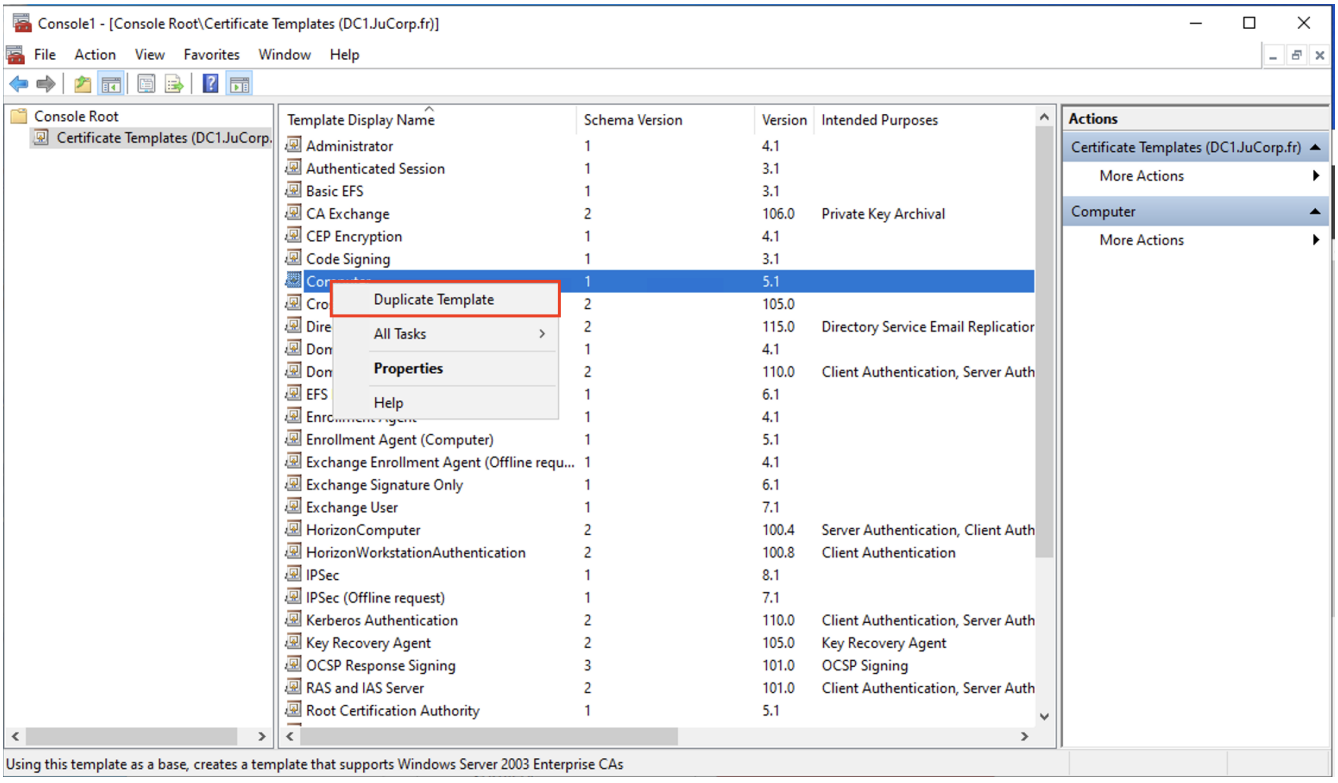


Configure Certificate Templates

To update or create Certificate template, you need to press `Win + R` and execute `mmc.exe`. Select **File** > **Add/Remove Snap-in**.



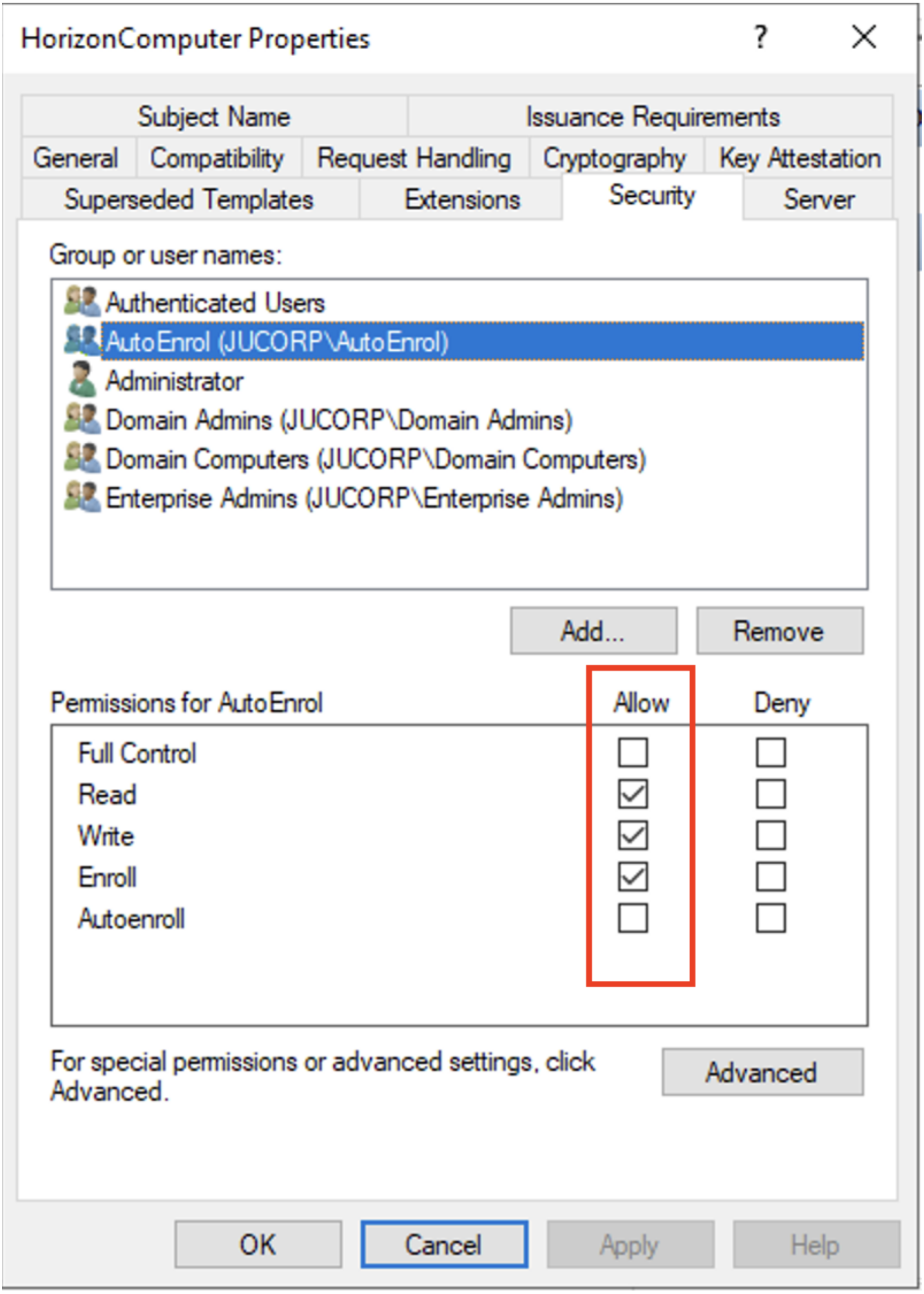
Click on **Certificate templates**, you should see all the templates available in the forest. EVERTRUST advises to duplicate existing Microsoft Certificate Template in order to create new ones consumed by WinHorizon.



Don't configure template names with spaces and take notes of the template

> names you will be using with WinHorizon. They will be needed in the WinHorizon configurator.

To check the authorizations on the different templates, you can right click on a template and choose properties. WinHorizon requires each template it manages to have at least the permission Read for the group Authenticated Users.

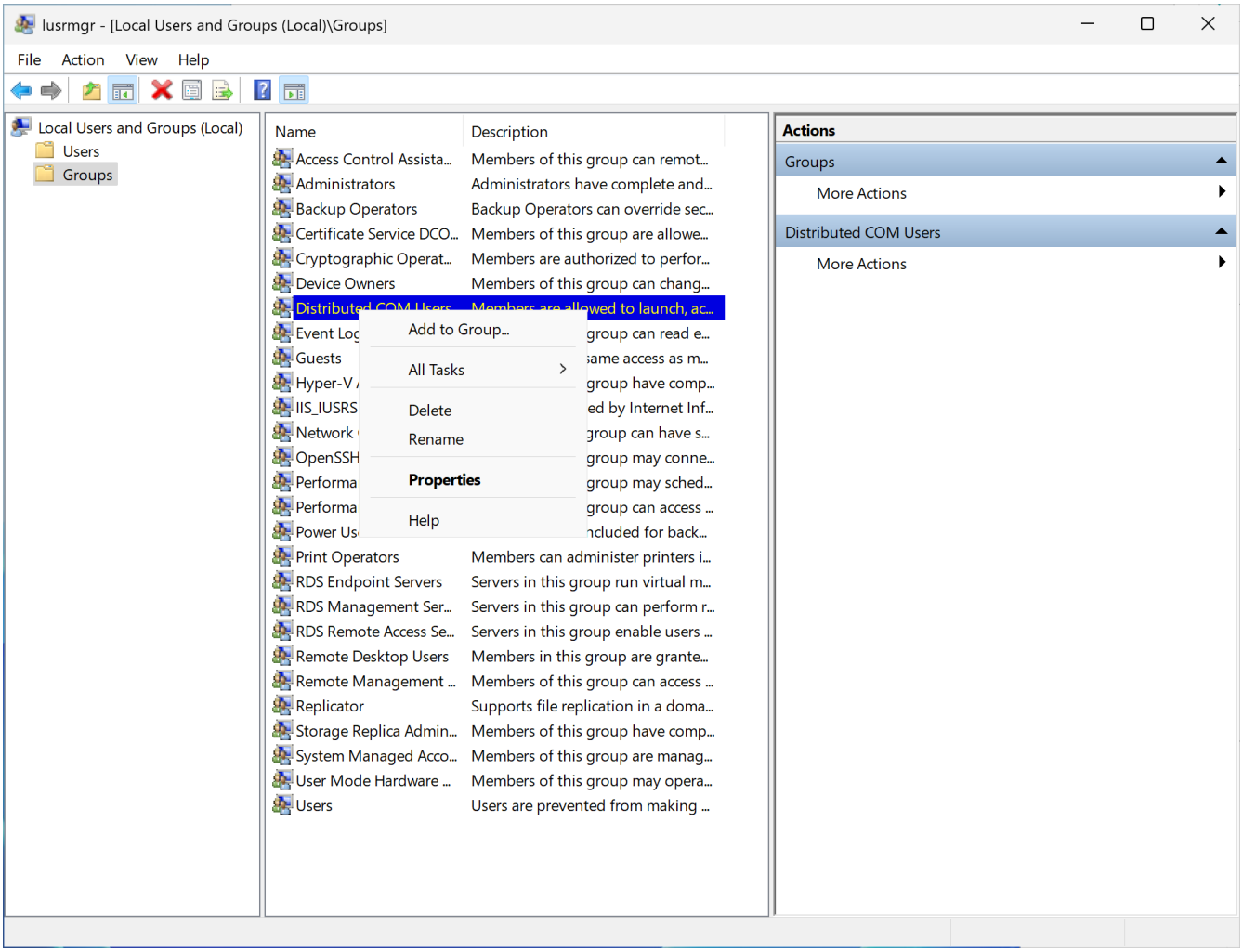


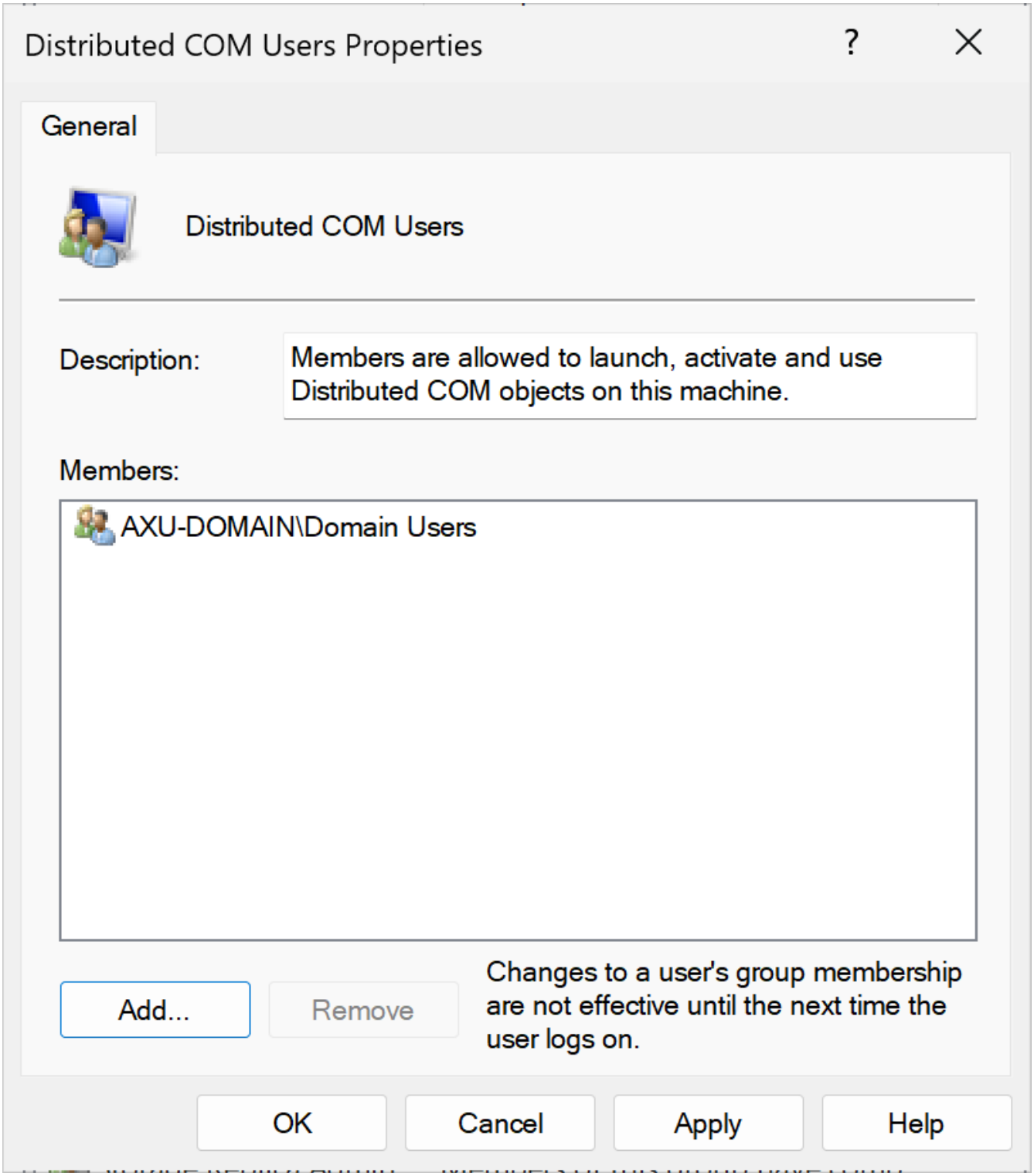
Moreover, EverTrust recommends creating AD local groups and grant `Read/Enroll/Auto enroll` rights on proper Microsoft Certificate.

For more details, please refer to the Active Directory Configuration section in the administration guide.

Enable Distributed COM Users

To enroll from any Windows device, you should follow the next steps. Based on the security group(s) that you assigned to your template (for example, "**Domain Users**"), add the same security group(s) to the "**Distributed COM Users**" local group on the machine using the `lusrmgr.msc` utility.

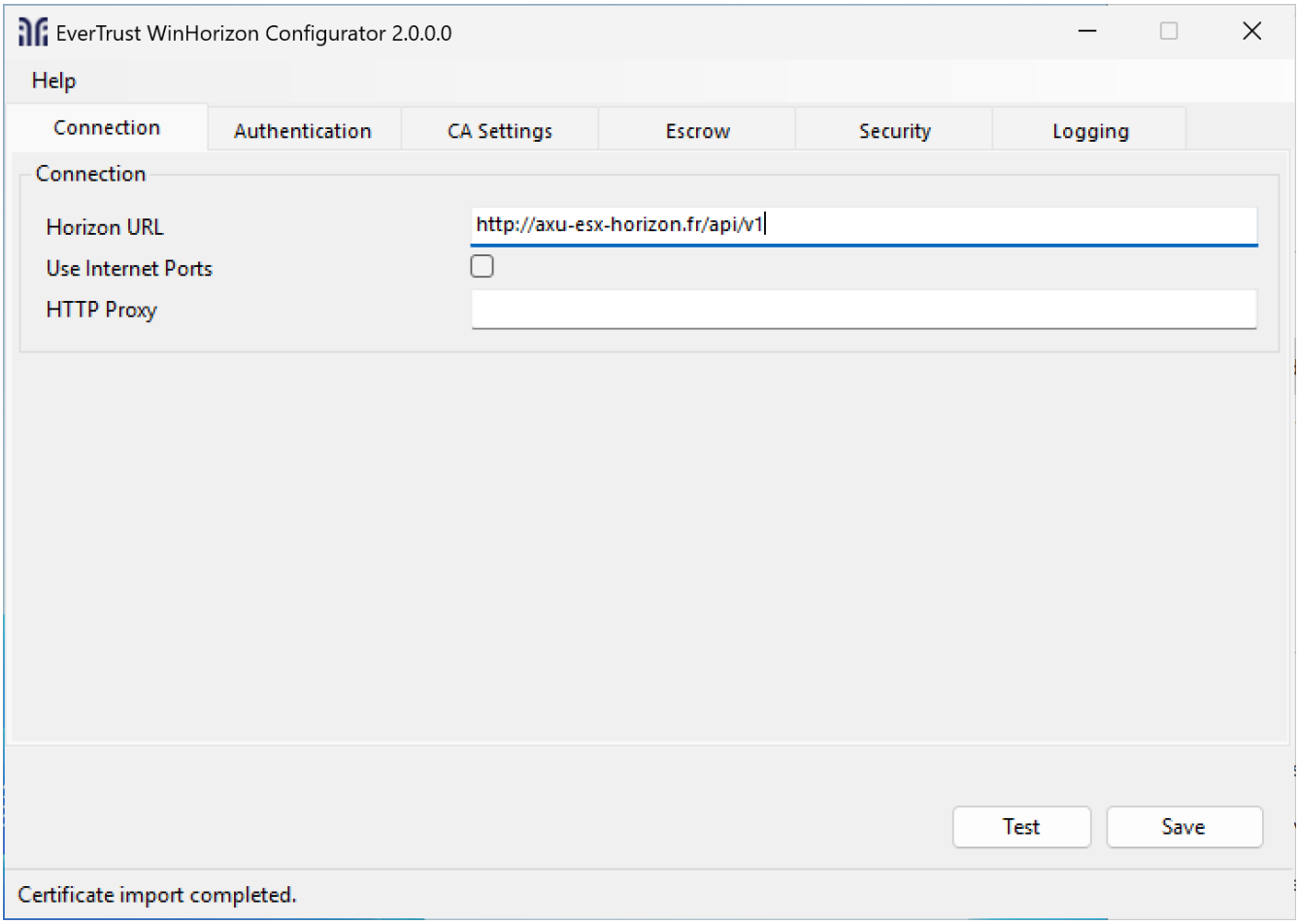




Don't forget to manage WinHorizon's **Microsoft Defender Firewall**.

WinHorizon Configurator - Connection Settings

Go back to the WinHorizon Configurator and go to the **Connection** tab.

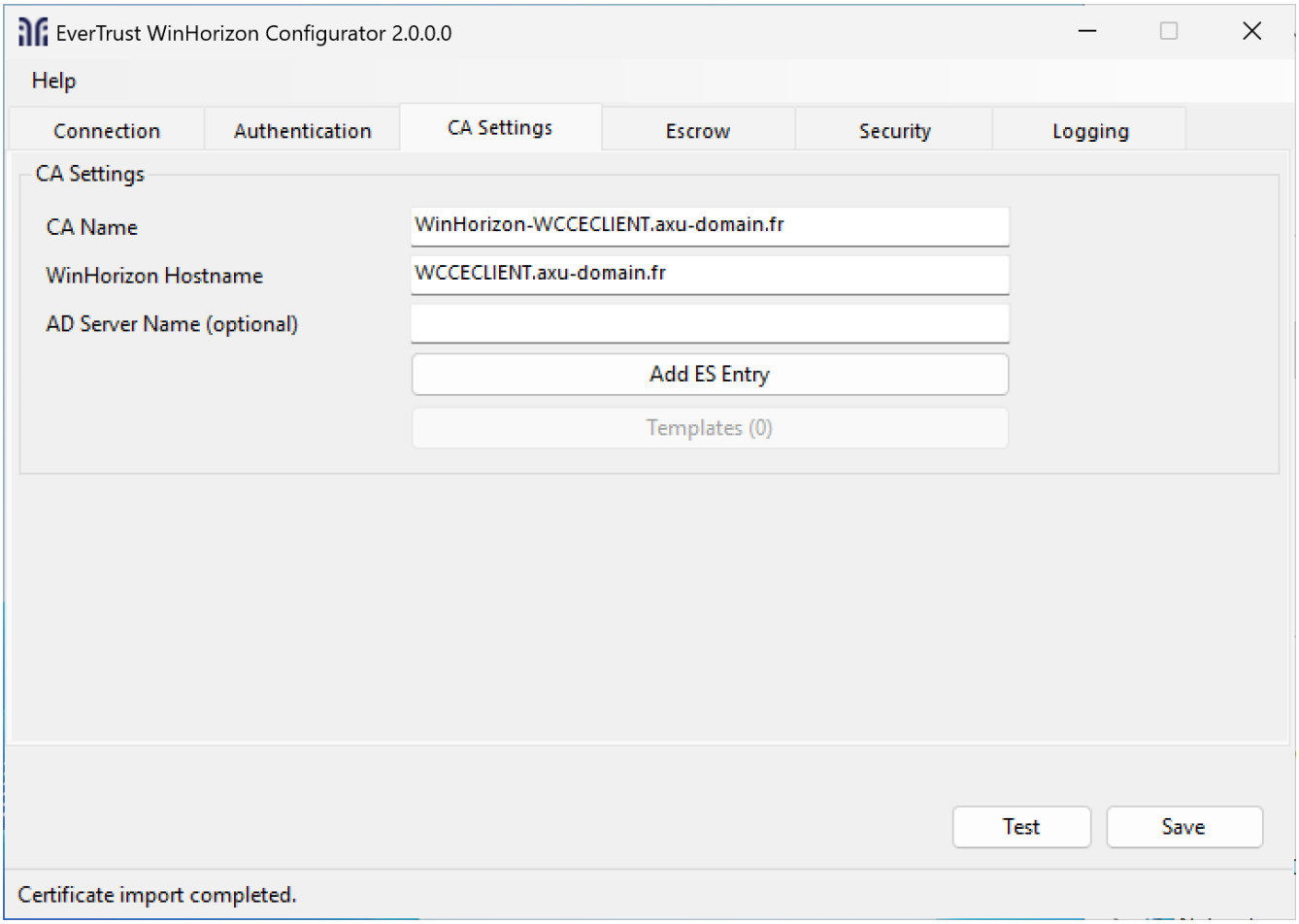


Fill the fields with your horizon URL suffixed with **/api/v1**.

Furthermore, if you need a proxy to reach Horizon, fill in the proxy URL as well.

WinHorizon Configurator - CA Settings

After filling the connection information, go to the **CA Settings** tab.



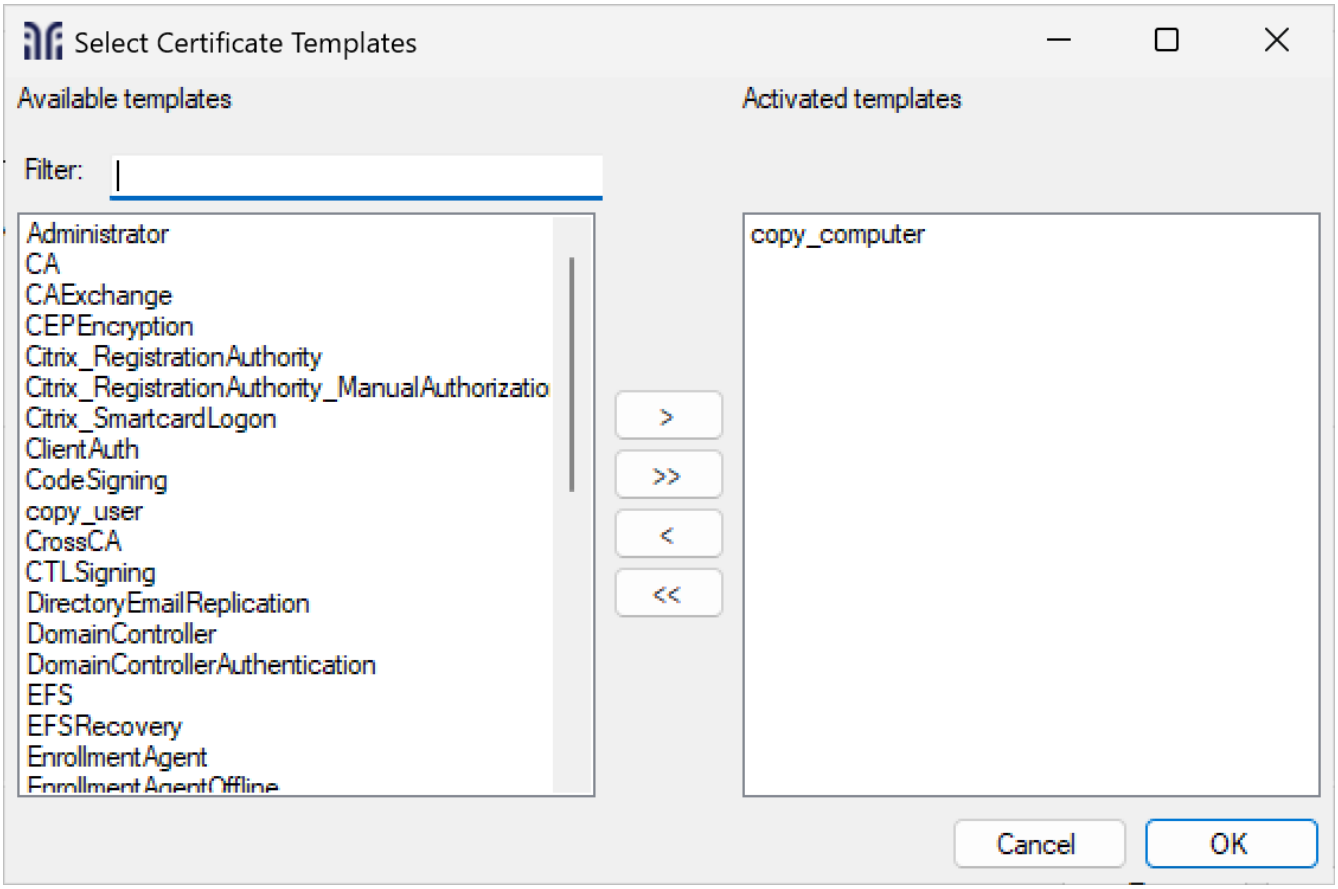
Fill in the **CA Name** value if it is not already filled.

It is not recommended to edit the hostname since it is already based on your machine FQDN.

Click **Add ES Entry** and import the CA certificate file that has signed the WinHorizon Certificate, most likely the Technical CA.

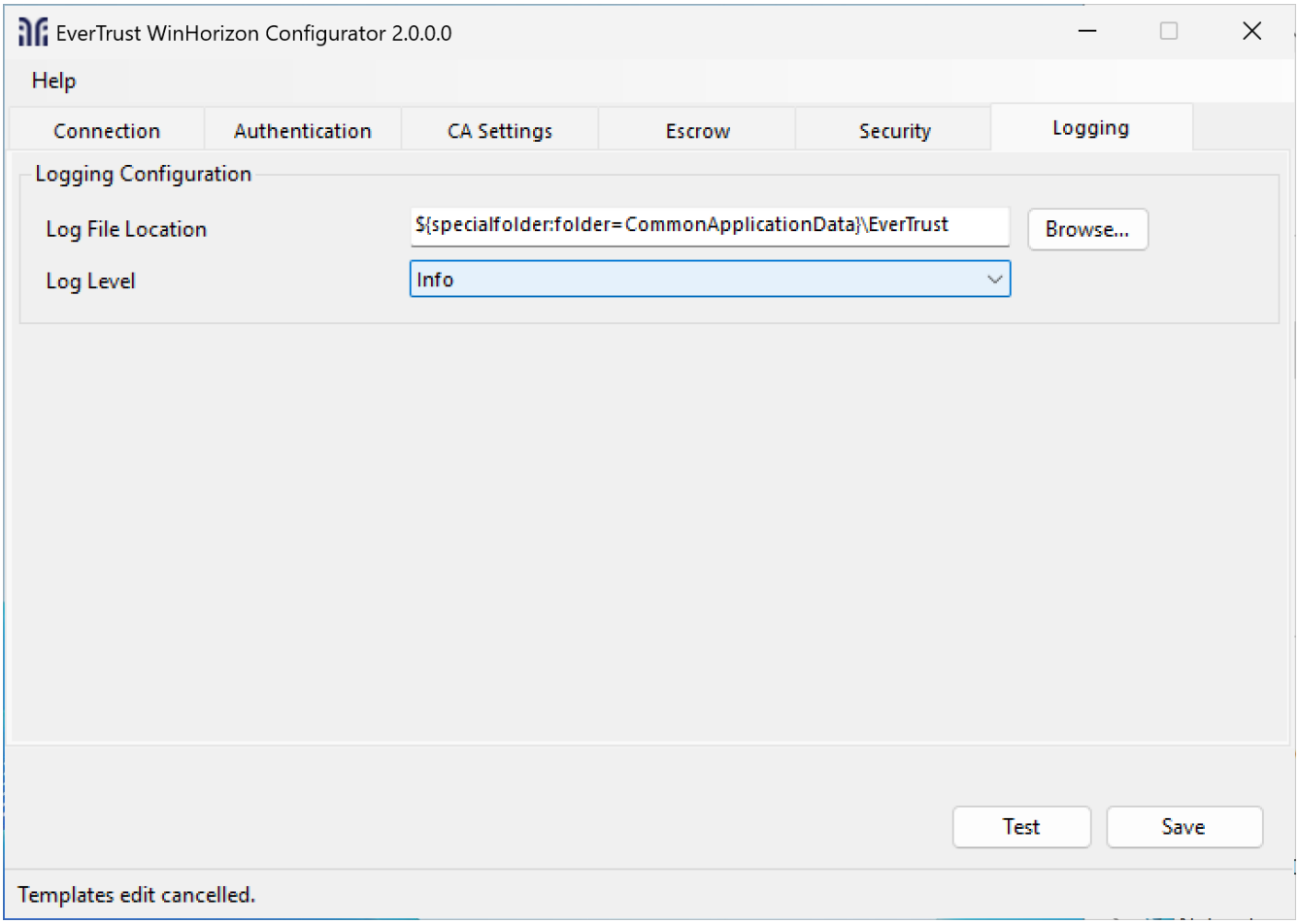
To be able to add the Enrollment service entry to the Active Directory you need permissions to manage them.

Click **Templates** to add the templates your WinHorizon will serve.



WinHorizon Configurator - Logging

Then you can setup the service logs in the Logging tab.



After the complete configuration is done, click **Save** and restart the WinHorizon service.

If you want to save this configuration, you can export this registry key: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\EverTrust\WinHorizon`

Next Steps

After configuring WinHorizon, you can go back to setting up your WCCE forest and profiles.

1.5. Uninstallation Procedure

Uninstalling WinHorizon

Uninstalling WinHorizon consists in uninstalling:

- The EverTrust WinHorizon service;
- The EverTrust WinHorizon configuration application.

1. Log in to the WinHorizon server with **administrative privileges**.

2. Open the **Control Panel**

3. In the **Programs** section, click **Uninstall** a program.

4. Search **EverTrust WinHorizon**.

5. Once found click **Uninstall**

Clean up

1. Log in to the WinHorizon server with **administrative privileges**.

2. Delete the **%USERPROFILE%\Program Files\EverTrust** directory.

3. Delete the **%USERPROFILE%\ProgramData\EverTrust** directory.

4. If WinHorizon certificate has been stored on Microsoft Certificate store, remove the **private key** and the associated **certificate**.

WinHorizon certificate revocation

Ask a Horizon administrator to revoke the WinHorizon certificate used to authenticate on Horizon.

Chapter 2. Administration

2.1. Active Directory Configuration

Installing Remote Server Administration Tools (RSAT)

To access the Microsoft Certificate Template, you should install Remote Server Administration Tools (RSAT). If it's not on your windows server, you can follow the steps below to install it:

1. Open the **Server Manager** tool.

2. Select **Manage** > **Add Roles and Features**.

3. Select **Features** and expand **Remote Server Administration Tools** > **Role Administration Tools** > **Active Directory Certificate Services Tools**.

4. Select **Certification Authority Management Tools**.

5. Select **Next** and then select **Install**.

Certificate Template Configuration

To update or create Certificate template, you need to press `Win + R` and execute `mmc.exe`. Select **File** > **Add/Remove Snap-in**.

Click on **Certificate templates**, you should see all the templates available in the forest. EVERTRUST advises to duplicate existing Microsoft Certificate Template in order to create new ones consumed by WinHorizon.

Don't configure template names with spaces and take notes of the template names you will be using with WinHorizon. They will be needed in the WinHorizon configurator.

To check the authorizations on the different templates, you can right click on a template and choose properties. WinHorizon requires each template it manages to have at least the permission Read for the group Authenticated Users.

Moreover, EverTrust recommends creating AD local groups and grant `Read/Enroll/Auto enroll` rights on proper Microsoft Certificate.

Enabling Auto Enrollment through a GPO

You need to enable GPO to enable auto-enrollment. For detailed instructions on enabling auto-enrollment through a GPO, please refer to the Microsoft documentation or your organization's Active Directory configuration guidelines.

Publishing the Trust Chain

This section details how to publish the trust chain within Active Directory.

If several WinHorizon servers are installed, the procedure detailed in this section must only be executed once. If the trust chain is already published, this procedure does not need to be performed.

1. Launch a 'cmd.exe' using a privileged account (using the 'RunAs' command);

2. Execute the following command to add Root CA:

```
certutil -f -dspublish "C:\<PATH_TO_ROOT_CA_CERTIFICATE>" rootca
```

3. Execute the following command to add Subordinate CA:

```
certutil -f -dspublish "C:\<PATH_TO_SUBORDINATE_CA_CERTIFICATE>" subca
```

4. Execute the following command to push new Active Directory schema:

```
certutil -pulse
```

2.2. WinHorizon Configuration

Prerequisites

Before configuring WinHorizon, ensure that you have published your trust chain like described in the Publishing the Trust Chain section.

Updating the local built-in 'Distributed COM Users' group

For Domain Controllers and computers to be able to enroll (i.e. contact the DCOM service on the WinHorizon server), they need to be members of the built-in local group 'Distributed COM Users'.

1. Access the WinHorizon server (local console or Terminal Services) using a local administrator account;

2. Launch the 'Local User and Groups' management console using `lusrmgr.msc`;

3. Edit the built-in group 'Distributed COM Users';

4. Add the groups that should be able to enroll/auto enroll:

- For Domain Controllers: Domain Controllers;

- For workstation: Domain Computers.

Based on the security group(s) that you assigned to your template (for example, "**Domain Users**"), add the same security group(s) to the "**Distributed COM Users**" local group on the machine.

Don’t forget to manage WinHorizon’s **Microsoft Defender Firewall**.

EverTrust WinHorizon Configurator

Authentication Tab

1. Search and start the **EverTrust WinHorizon configurator** application using Domain **Administrator account**.

2. Go to the **Authentication** tab.

3. Click the **Generate CSR** button and fill in the fields you need, leave a field blank if it is not needed (it will not appear in the CSR).

We recommend leaving the options as default.

4. When you have completed all the necessary fields, click the **Generate** button and then use the **Save CSR** button to save the CSR somewhere you can find it.

5. Use this CSR to sign the certificate with your PKI / CA and download the newly created certificate in PEM format.

6. After downloading the certificate, go back to the Authentication tab, click the **Import Certificate** button and choose the certificate.

Check that you are in the "Windows store" authentication mode.

7. After a successful import, you should see a confirmation message as well as the serial number being filled in the specific field.

Connection Tab

Fill the following fields in the **Connection** tab:

- **Horizon URL**: Enter the Horizon instance URL to connect to. Should end with **/api/v1** Example: https://horizon.evertrust.fr/api/v1
- **Proxy URL** (if needed): If you need a proxy to reach Horizon, fill in the proxy URL as well.

CA Settings Tab

WinHorizon is registered as an **Enrollment Service** in Active Directory. **CA Name** and **WinHorizon Hostname** are used to create the Enrollment Service entry.

Fill the following fields:

- **CA Name**: CA Name will be used as **cn**.
- **WinHorizon Hostname**: WinHorizon Hostname will be used as **dNSHostName**.

It is not recommended to edit the hostname since it is already based on your machine FQDN.

1. Click on **Add ES Entry** and import the CA certificate file that has signed the WinHorizon Certificate, most likely the Technical CA.

To be able to add the Enrollment service entry to the Active Directory you need permissions to manage them.

2. Click on **Templates** to add the templates your WinHorizon will serve.

3. Write down each template managed by the WinHorizon instance separated by ;. Click **OK**. Example: EverTrustDomainController;EverTrustIIS;EverTrustUser;EverTrustServer.

Internet Ports Configuration

WinHorizon uses the port 135 as management port and then affects a port for each client. By default, the port is randomly chosen between 1024 and 65535 but if the option is turned on, the port range can be restricted.

To restrict this range to specific ports, additional DCOM configuration may be required.

Logging Tab

Configure the service logs in the **Logging** tab according to your organization's requirements.

Saving Configuration

1. After the complete configuration is done, click **Save**.

If you want to save this configuration, you can export this registry key: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\EverTrust\WinHorizon`

WinHorizon service restart

1. Access the Services Management Console (services.msc).

2. Restart the **WinHorizon** service.

2.3. Testing & Validation

This section details how to test and validate your WinHorizon installation and configuration.

ADSI Test

Use the ADSI edit tool to verify that WinHorizon is properly registered in Active Directory.

1. Launch **ADSI Edit** from Administrative Tools or by running `adsiedit.msc`.

2. Connect to your configuration partition.

3. Navigate to **Configuration** > **Services** > **Public Key Services** > **Enrollment Services**.

4. Verify that you can see your WinHorizon enrollment service entry in the list.

If WinHorizon appears in the enrollment services, this confirms that it has been properly registered in Active Directory.

Manual Certificate Enrollment Test

To test certificate enrollment manually through WinHorizon:

1. Launch the Certificate Manager by running `certlm.msc`.

2. Navigate to **Personal** > **Certificates**.

3. Right-click and select **All Tasks** > **Request New Certificate**.

4. Follow the Certificate Enrollment wizard: - Click **Next** on the initial screen - Select the appropriate certificate template that has been configured for WinHorizon - Complete the enrollment process

5. Verify that the certificate is successfully issued and appears in your personal certificate store.

Troubleshooting Common Issues

Certificate Enrollment Fails

If certificate enrollment fails, check the following:

- Verify that the WinHorizon service is running
- Check that the client machine is a member of the appropriate Active Directory groups
- Ensure that the certificate template permissions are correctly configured
- Verify network connectivity between client and WinHorizon server

DCOM Connection Issues

If clients cannot connect to WinHorizon via DCOM:

- Verify that the client groups are added to the "Distributed COM Users" group
- Check Windows Firewall settings on the WinHorizon server
- Ensure that the required network ports are open (135/TCP and dynamic RPC ports)

Horizon Connectivity Issues

If WinHorizon cannot connect to Horizon:

- Verify the Horizon URL configuration
- Check that TLS 1.2 is properly enabled
- Validate the WinHorizon authentication certificate
- Test network connectivity to the Horizon server on port 443

Log Files and Diagnostics

WinHorizon logs can be found in the Windows Event Viewer and in the configured log directory. Check these logs for detailed error information when troubleshooting issues.

The WinHorizon service logs important events related to:

- Service startup and configuration
- Certificate enrollment requests
- Communication with Horizon
- Active Directory operations
- DCOM connection attempts