EVERTRUST

WinHorizon

Version 1.1, 2025-11-05

Table of Contents

Chapter 1. Installation

1.1. Introduction

Description

WinHorizon is the EverTrust WCCE proxy solution part of EverTrust Horizon suite EverTrust. WinHorizon is powered up by:

- .NET Framework 4.6.1 or higher

This document is specific to WinHorizon version **1.1**.

Scope

This document is an installation procedure detailing how to install WinHorizon on a server.

Out of Scope

This document does not describe how to configure and operate a WinHorizon instance. Please refer to the administration guide for administration related tasks.

1.2. Specifications & Requirements

You have to deploy at by 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 2012 (64-bit);
- Microsoft Windows Server 2012 R2 (64-bit);
- Microsoft Windows Server 2016 (64-bit);
- Microsoft Windows Server 2019 (64-bit).

- Microsoft Windows Server 2022 (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;

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 2012;
- Microsoft Windows Server 2012 R2;
- Microsoft Windows Server 2016;
- Microsoft Windows Server 2019.
- Microsoft Windows Server 2022.

1.3. Installation Procedure

This section details how to install WinHorizon. WinHorizon is made with only one package:

- winhorizon-1.1.msi

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

2. Double-click on **winhorizon-1.1.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. Click **Install**

6. Click **Finish**

The installation results in the creation of:

- EverTrust WinHorizon Configurator application;
- EverTrust WinHorizon service (accessible using **services.msc**).

1.4. 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.

1.5. Troubleshooting

A common issue when installing WinHorizon is that TLS 1.2 is not enabled by default on Windows

Server. This will translate into SSL errors when WinHorizon will try to connect to Horizon.

To solve this, 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.

Chapter 2. Administration

2.1. Introduction

Description

WinHorizon is the EverTrust WCCE proxy solution part of EverTrust Horizon suite EverTrust. WinHorizon is powered up by:

- .NET Framework 4.6.1 or higher

This document is specific to WinHorizon version **1.1**.

Scope

This document is an installation procedure detailing how to configure and operate WinHorizon.

Out of Scope

This document does not describe how to install a WinHorizon instance. Please refer to the installation guide for installation related tasks.

2.2. Prerequisites

- WinHorizon should be installed using WinHorizon installation guide;
- An account with Full Control permissions on Public Key Services (Sites and Services > Services > Public Key Services).
  This account must be able to open sessions on WinHorizon's server. An enterprise administrator account can be used;
- Access to WinHorizon server;
- WinHorizon certificate (PKCS12, PFX format) with proper permissions on WCCE profiles on Horizon side;
- The following flaws should 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

Source	Destination	Port	Description
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

2.3. Active Directory Configuration

Publishing trust chain

This section details how to publish the trust chain within Active Directory. If several WinHorizon servers are installed or, 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 the 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
```

Microsoft Certificate Template creation

Create/Update the Microsoft Certificate Template using the privileged account and Certificate Templates' snap-in (through MMC).

EverTrust advises to duplicate existing Microsoft Certificate Template in order to create new ones consumed by WinHorizon:

- Duplicate the **Kerberos Authentication** template if you want to issue **Domain Controllers** certificate (compliant with Kerberos requirements);
- Duplicate the **Workstation Authentication** template if you want to issue **Machines** certificates (Workstation, server);
- Duplicate the **SmartCard Logon** template if you want to issue **User authentication** certificates.

Please ensure that template ACLs are properly configured. WinHorizon requires each template it manages to have at least the permission **Read** for the group **Authenticated Users**. Moreover, EverTrust recommends to create AD local groups and grant **Read/Enroll/Auto enroll** rights on proper Microsoft Certificate Template. Adding assets on group will automatically grant proper permissions on Microsoft Certificate Template.

Enabling Auto Enrollment through a GPO

On Windows hosts, Auto Enrollment is enabled through GPO settings. These GPO settings can be added to an existing GPO or a dedicated GPO can be created regarding this usage. This GPO must be mapped on the Active Directory forest so that machine (Domain Controllers, Computers, Servers, Users) targeted by auto enrollment receive this GPO.

1. Launch the Group **Policy Management console**;

2. Edit or create a GPO regarding Auto Enrollment;

3. Browse to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies**:

4. Edit the **Certificate Services Client – Auto-Enrollment** settings;

5. Specify the following settings:

- Configuration Model: **Enabled**;
- Check **Renew expired certificates, update pending certificates, and remove revoke certificates**;
- Check **Update certificates that use certificate templates**;
- Leave the other settings with default value.

And hit the **OK** button.

6. Ensure that this GPO is linked to an OU targeting the machines where auto enrollment must be enabled.

Regarding specific AD attributes

All of the AD attributes that map to a supported attribute in the RFC 5280 are natively supported by WinHorizon. Moreover, the following attributes can be consumed and re-mapped through the Horizon CSR data mapping feature:

- company
- department
- displayName
- employeeNumber
- employeeId
- samAccountName
- title

If you plan on using these attributes' values in your certificates through WinHorizon, it is important to note that WinHorizon fetches the attributes' values from the Global Catalog component of the AD and not from the LDAP. This means that if you edit these attributes through the "Active Directory Users and Groups" or through ADSI Edit in LDAP mode, the value of the aforementioned attributes will have to be manually replicated using the following steps:

1. Ensure that you have an account with Enterprise Admin and Schema Admin permission in the AD;
2. Start the MMC with the aforementioned permissions and load the "Active Directory Schema" snap-in;
3. In the "Attributes" folder, search for the attribute that you plan on using through WinHorizon (ex. employeeNumber) then right click and open its **Properties**;
4. Check the **Replicate this attribute to the Global Catalog** box then click **Apply**;
5. Open a cmd prompt with Enterprise Admin permissions then run the following command: **repadmin /syncall**

The userPrincipalName (UPN), objectGUID (GUID) and securityID (SID) are retrieved as expected by WinHorizon without having to do these extra steps.

2.4. WinHorizon server configuration

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;

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.

EverTrust WinHorizon Configurator

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

2. Fill the following fields:

- **Horizon URL**:
  Enter the Horizon instance URL to connect to. Should end with **/api/v1** Example: https://horizon.evertrust.fr/api/v1

WinHorizon uses a certificate to authenticate on Horizon. There are two ways to store this certificate. Firstly store it as PKCS12 in **C:\ProgramData\EverTrust\WinHorizon\clientCertificate.p12**. Secondly import PKCS12 in Microsoft Certificate store.

- **PKCS12 Password** (if WinHorizon certificate is stored as PKCS12 file) Password of the PKCS12.
- **Auth Cert Serial** (if WinHorizon certificate is stored in Microsoft Certificate Store) Certificate serial number of the WinHorizon certificate stored in the Microsoft Certificate Store.

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

- **CA Name**:
  CA Name will be used as **cn**.
- **WinHorizon Hostname**:
  WinHorizon Hostname will be used as **dNSHostName**.
- **Internet Ports** :
  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, this section must be followed.

3. Click on **Add ES Entry** and import the CA certificate file that has signed the WinHorizon Certificate.

4. Click on **Template**. A wizard 'Certificate Template' appears.

5. Write down each template managed by the WinHorizon instance separate by **;** . Click **Ok**. Example: EverTrustDomainController;EverTrustIIS;EverTrustUser;EverTrustServer.

6. Click on **Save**

WinHorizon service restart

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

2. Restart the **WinHorizon** service:

2.5. Restricting Internet Ports

To restrict the range of ports used by WinHorizon from 1024-65535 to a chosen range, in this example 5000-6000, follow these steps:

1. **Add** the Internet key under: **HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc**
2. Under the Internet key (**HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Internet**), add the values "Ports" (MULTI_SZ), "PortsInternetAvailable" (REG_SZ), and "UseInternetPorts" (REG_SZ). For example, the new registry key appears as follows:
    a. **Ports**: *REG_MULTI_SZ*: 5000-6000
    b. **PortsInternetAvailable**: *REG_SZ*: Y
    c. **UseInternetPorts**: *REG_SZ*: Y
3. Set **"Use Internet Ports"** to "YES" in WinHorizon and save the configuration
4. Restart the server. All applications (including WinHorizon) that use RPC dynamic port allocation use ports 5000 through 6000, inclusive.