EVERTRUST

# ADCS Connector

Version 1.1, 2025-12-05

# Table of Contents

# Chapter 1. Installation

## 1.1. Introduction

### Description

ADCS Connector is the EverTrust ADCS proxy solution part of EverTrust Horizon suite.

This document is specific to ADCS Connector version **1.1**.

ADCS Connector allows to connect Horizon to Microsoft Active Directory Certificate Services (ADCS) in order to issue certificates from an Active Directory environment.

### Installation

To install ADCS Connector, please refer to the Installation Procedure section.

### Uninstallation

To uninstall ADCS Connector, please refer to the Uninstallation Procedure section.

## 1.2. Specifications & Requirements

You have to deploy ADCS Connector 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;

### Network prerequisites

The following network flows must be opened:

| Source | Destination | Port | Description |
|---|---|---|---|
| HORIZON_IP | ADCS_CONNECTOR_IP | 4443/TCP | Horizon connects to ADCS Connector using mutual SSL authentication |
| ADCS_CONNECTOR_IP | ADCS_IP | 135/TCP, 445/TCP | ADCS Connector connects to ADCS using DCOM/RPC |

# 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 ADCS Connector. ADCS Connector is contained in only one package:

- EverTrust ADCS Connector.1.1.msi

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

**2.** Double-click on **EverTrust ADCS Connector.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 ADCS Connector service (accessible using **services.msc**).

## Configuration

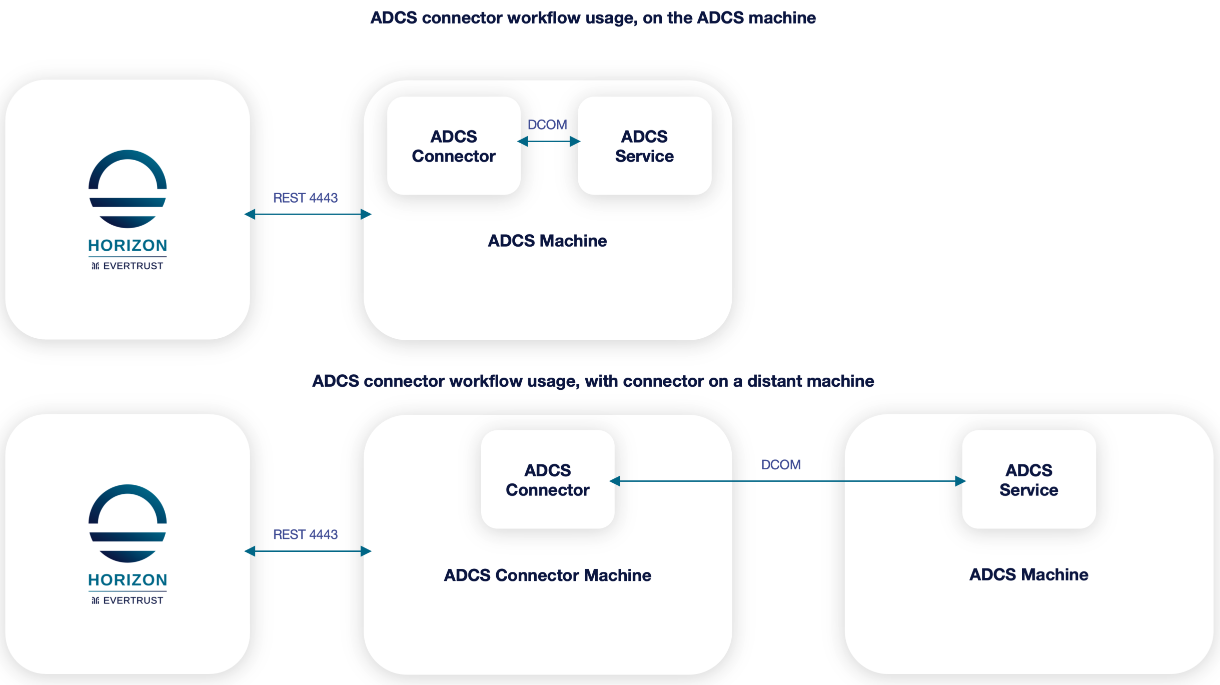
After installation, please refer to the Initial Configuration section to configure ADCS Connector.

# 1.4. Initial Configuration

## Initial Configuration of the ADCS Connector

Before proceeding with the setup, please ensure that the ADCS Connector program is correctly installed and stopped.

> The connector can be installed on the ADCS server itself or on another machine in the same domain. For the latter, install the Remote Server Administration Tools (RSAT) for Active Directory Certificate Services on that machine. You can use the server manager to add the feature "AD CS and AD LDS Tools" under "Remote Server Administration Tools" > "Role Administration Tools" > "AD CS Tools"



ADCS connector workflow usage, on the ADCS machine

ADCS connector workflow usage, with connector on a distant machine

## TLS Certificate

Enroll a TLS Web Server certificate with the "Server Authentication" and a SAN DNS that will have the DNS name you are going to use for this ADCS machine and import it in the certificate store of the ADCS machine.

Retrieve the hash of that certificate through certlm.msc. Be careful as some special characters may be copied alongside with the hash, so ensure that you get rid of them should they be present.

## Connector Configuration

Edit the `C:\Program Files\EverTrust\ADCSConnector\EverTrustADCSConnector.exe.config` file and paste the previously copied hash to be the value of the "CertHash" line, then save the file.

> ℹ Please don't copy the file from one installation to another as the content may differ from one version to another.

## Network Configuration

Ensure that the port 4443 is opened in the firewall of this machine and that the machine can indeed be reached from the Horizon machine.

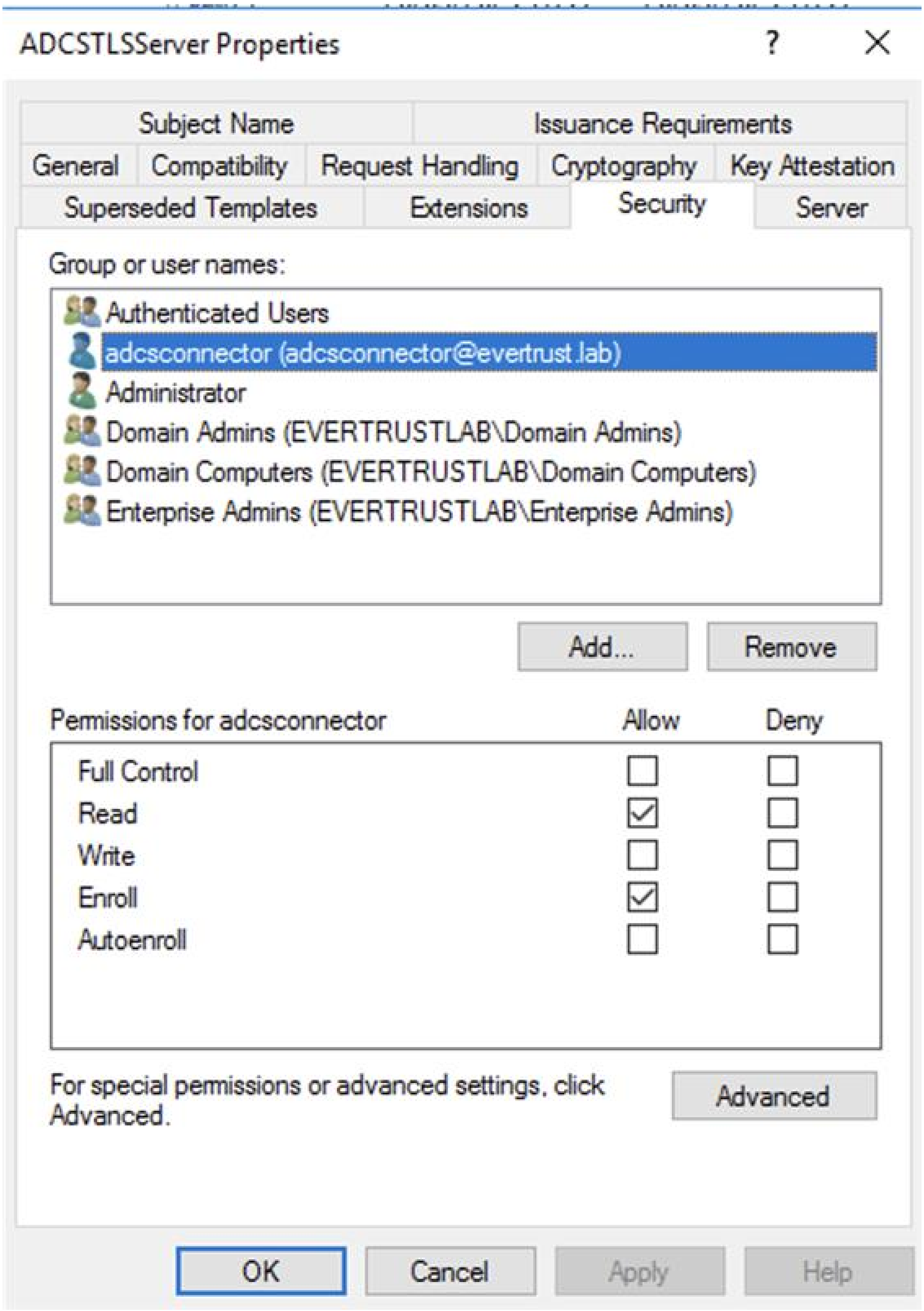
Using `services.msc`, start the "EverTrust ADCS Connector" service. To see whether the service started successfully, start Internet Explorer and go to `https://localhost:4443/api/certificate`. This should download a JSON file that says "OK" if everything is good.

## Template & Permissions

Create a new certificate template on the ADCS (or use an existing one) that the connector will use to enroll the certificates.

Create a technical account to manage the connector:

- Give it the right to enroll on the previously created template



ADCSTLSServer Properties

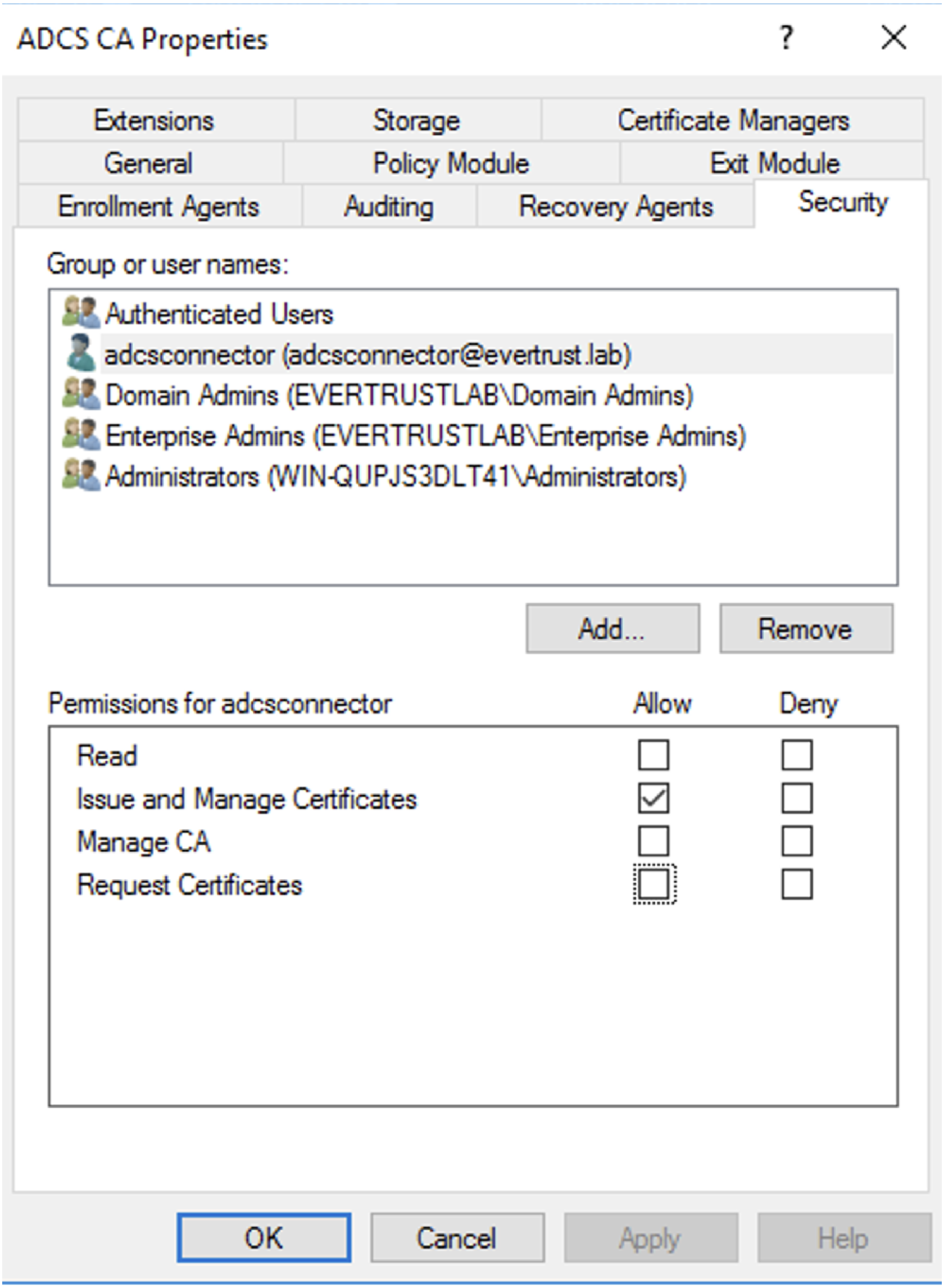
Group or user names:

- Authenticated Users
- adcsconnector (adcsconnector@evertrust.lab)
- Administrator
- Domain Admins (EVERTRUSTLAB\Domain Admins)
- Domain Computers (EVERTRUSTLAB\Domain Computers)
- Enterprise Admins (EVERTRUSTLAB\Enterprise Admins)

| Permissions for adcsconnector | Allow | Deny |
|---|---|---|
| Full Control | □ | □ |
| Read | ☑ | □ |
| Write | □ | □ |
| Enroll | ☑ | □ |
| Autoenroll | □ | □ |

For special permissions or advanced settings, click Advanced.

- Give it the right to `Issue and Manage Certificates` on the ADCS



Group or user names:

- Authenticated Users
- adcsconnector (adcsconnector@evertrust.lab)
- Domain Admins (EVERTRUSTLAB\Domain Admins)
- Enterprise Admins (EVERTRUSTLAB\Enterprise Admins)
- Administrators (WIN-QUPJS3DLT41\Administrators)

| Permissions for adcsconnector | Allow | Deny |
|---|---|---|
| Read | □ | □ |
| Issue and Manage Certificates | ☑ | □ |
| Manage CA | □ | □ |
| Request Certificates | □ | □ |

## Enrollment Agent

Create an enrollment agent certificate and export it as PKCS#12. This certificate will be the one used to sign the CMC messages from Horizon.

After configuring the ADCS Connector, you can go back and proceed with the creation of the MSADCS PKI Connector in Horizon.

# 1.5. Uninstallation Procedure

## Uninstalling ADCS Connector

Uninstalling ADCS Connector consists in uninstalling:

- The EverTrust ADCS Connector service;

**1.** Log in to the ADCS Connector server with **administrative privileges**.

**2.** Open the **Control Panel**

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

**4.** Search **EverTrust ADCS Connector**.

**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 ADCS Connector TLS certificate has been stored on Microsoft Certificate store, remove the **private key** and the associated **certificate**.

## ADCS Connector certificate revocation

Ask a Horizon administrator to revoke the ADCS Connector TLS certificate.

# Chapter 2. Release notes

## 2.1. ADCS Connector 1.1.0 release notes

Here are the release notes for EverTrust ADCS Connector v[object Object], released on 2025-12-02. For the installation and upgrade procedure, please refer to the Installation and Upgrade guide.

### New Features

- Service no longer requires the technical account to have login permissions on the machine where the connector is installed.

### Enhancements

`[None]`

### Bug Fixes

- The ADCS Connector service can now be upgraded without requiring uninstallation of the previous version.

### Known defects

`[None]`