

# Setup & Configuration Omnissa Horizon

---

document version 5.2

## Content

Content .....	1
1. Prepare Horizon Environment .....	7
1.1 Create DB for Horizon Events .....	7
1.2 Create vCenter Server Account for Horizon .....	8
1.3 Create Domain Account for Horizon .....	8
1.4 Create a Certificate Template for Horizon Connection Server .....	8
1.5 Add Horizon ADMX Templates to GPO.....	11
1.6 AV exclusion list for Horizon.....	11
2. Setup Omnissa Horizon Standard Server .....	12
2.1 Initial Setup.....	12
2.2 Initial Configuration Horizon Console.....	17
2.2.1 License Key .....	17
2.2.2 Event DB.....	18
2.2.3 Add vCenter Server .....	18
2.2.4 Request certificate .....	18
2.2.5 Locked.properties .....	20
2.2.6 Add Domain Accounts.....	21
2.2.7 Optional configuration .....	21
3. Setup Horizon Edge Gateway .....	21
3.1 Requirements .....	21
3.2 Deployment Horizon Edge Gateway.....	22
3.3 Further options for Edge GW .....	25
3.4 Update Horizon Edge Gateway .....	26
4. Setup VMware Horizon Replica Server .....	27
5. Setup VMware Horizon Enrollment Server.....	29
5.1 Preparation CA .....	<b>Fehler! Textmarke nicht definiert.</b>
5.2 (optional) Add Security Group.....	35
5.3 Create Certificate Template for TrueSSO .....	<b>Fehler! Textmarke nicht definiert.</b>

5.4	Certificate Template für Enrollment Server erstellen .....	43
5.5	Enrollment Agent (Computer) Certificate .....	45
5.6	Setup Enrollment Server .....	45
5.6.1	Configure Enrollment Server to prefer local CA.....	48
5.6.2	Configure Connection Servers to enable LB between Enrollment Servers .....	48
5.7	Pairing Connection und Enrollment Server .....	51
5.7.1	Export the Enrollment Service Client Certificate.....	51
5.7.2	Import the Enrollment Service Client Certificate on the Enrollment Server .....	52
5.8	Configure SAML Authentication .....	54
5.9	Configure Connection Server for TrueSSO .....	54
5.10	Setup additional Enrollment Server and enable HA .....	56
5.11	(optional) Setup Sub-CA .....	<b>Fehler! Textmarke nicht definiert.</b>
5.12	Quellen Enrollment Server .....	<b>Fehler! Textmarke nicht definiert.</b>
5.13	Troubleshooting Enrollment Server .....	<b>Fehler! Textmarke nicht definiert.</b>
6.	Key Management Server (KMS) einrichten.....	60
7.	Netzwerklastenausgleich-Manager konfigurieren.....	62
8.	Einrichten eines Load Balancers .....	67
8.1	Einrichten eines Hercules Load Balancers (VMware Virtual Appliance).....	67
8.2	Einrichten eines PEN Load Balancers auf einem Ubuntu Linux .....	68
8.3	Einrichten eines HAProxys auf einem Debian System .....	68
9.	Setup Location-Based Printing.....	69
10.	Setup VMware Unified Access Gateway.....	70
10.1	Requirements .....	70
10.2	Deployment per PS-Script .....	70
10.3	Configuration UAG .....	71
10.4	Troubleshooting UAG .....	72
10.5	Create public certificate for external access .....	72
11.	Upgrade from earlier Horizon versions .....	72
11.1	Update to Horizon 2503 (8.15).....	72
11.1.1	Update Horizon 2503.....	73
11.1.2	Update application partition names .....	74
11.1.3	Update to Horizon 2503.1 .....	75
11.2	Update to Horizon 2412 (8.14).....	76
11.3	Update to Horizon 2406 (8.13).....	76

11.4	Update from Horizon 7 to Horizon 8 .....	77
11.4.1	Given Environment .....	77
11.4.2	Preparation .....	77
11.4.3	Upgrade to Horizon 8.....	78
11.4.4	Cleanup Tasks .....	79
11.4.5	Troubleshooting options.....	80
12.	Common Tasks and Day-2-Operations .....	80
12.1	Auto Upgrade of Horizon Agents.....	80
12.1.1	Preparation for Horizon Subscription .....	80
12.1.2	Preparation for Horizon Term licencing.....	81
12.2	Horizon Group Policies .....	82
12.2.1	Common GPO Settings for Desktop and RDSH Server VMs.....	82
12.2.2	Cleanup-Tasks Horizon.....	82
12.2.3	RDSH Server OU-Level Settings.....	83
12.3	Preparation RDSH Systems.....	83
12.3.1	Prepare RDSH Golden Image for remote access.....	83
12.4	Omnissa Horizon As Built Report.....	83
12.4.1	Requirements .....	83
12.4.2	Generating Report .....	84
12.5	Migration von Komponenten auf andere OS .....	<b>Fehler! Textmarke nicht definiert.</b>
12.5.1	Migration Connection Server auf andere Maschine	<b>Fehler! Textmarke nicht definiert.</b>
13.	Setup und Update VMware AppVolumes.....	86
13.1	Requirements App Volumes.....	86
13.2	Setup App Volumes .....	88
13.3	Initial configuration App Volumes Manager.....	93
13.4	Preparation Provisioning VM.....	98
13.5	Setup App Volumes Agent.....	99
13.6	Update VMware AppVolumes (2.x).....	101
13.7	Post-Tasks AppVolumes .....	105
13.7.1	Add additional App Volumes Manager .....	106
13.7.2	Configure SSL certificate validation for AD .....	107
13.7.3	Anpassungen bei Horizon automatischen Pools.....	108
13.7.4	Dem App Volumes Agent weitere App Volumes Manager hinzufügen .....	109
13.7.5	Replace self-signed certificate .....	110

13.7.6	Establish a multi-instance architecture .....	111
13.8	App Volumes Tools.....	113
13.8.1	Setup App Volumes Tools .....	113
13.8.2	Capture an application.....	114
13.9	Troubleshooting App Volumes .....	114
13.9.1	Replacing/Restoring a single Manager with external SQL DB.....	114
13.9.2	After update, Admin UI is failing.....	115
13.9.3	Omnissa App Volumes order of operation .....	115
14.	Setup Dynamic Environment Manager.....	116
14.1	Prepare Environment for DEM .....	116
14.1.1	Create File Shares .....	116
14.1.2	Import ADMX Templates for DEM .....	117
14.2	File Shares anlegen.....	117
14.3	Setup DEM Management Console.....	118
14.4	Initial DEM Configuration .....	119
14.4.1	Initial configuration DEM Management Console.....	119
14.4.2	Minimum required GPOs for DEM.....	120
14.4.3	Additional (optional) configuration .....	124
14.5	Setup DEM Agent .....	125
14.6	DEM Application Profiler .....	127
14.6.1	Requirements .....	127
14.6.2	Setup Application Profiler .....	127
14.6.3	Using Application Profiler .....	128
14.7	DEM Sync-Tool .....	130
14.7.1	Setup Sync-Tool .....	130
14.7.2	Configuring Sync-Tool .....	131
14.8	DEM Helpdesk Support Tool.....	132
14.8.1	Configuring Helpdesk Support Tool .....	132
14.8.2	Setup Helpdesk Tool .....	133
14.8.3	Using Helpdesk Tool .....	134
14.9	DEM – Appendix and Issues .....	135
14.9.1	MS Edge Settings .....	135
14.9.2	Sonstiges .....	136
14.9.3	Template for Windows Settings (Default) .....	136

15.	Microsoft FSLogix.....	137
15.1	Preparation.....	137
15.2	Setup FSLogix Agent .....	138
15.3	FSLogix GPO-Configuration.....	139
15.4	Additional information .....	139
16.	Horizon Recording .....	139
16.1	Requirements .....	139
16.2	Setup .....	140
16.3	Initial configuration .....	143
17.	Integration in Omnisca Access .....	145
17.1	Setup Omnisca Access Connector .....	145
17.1.1	Upload Connection Server certificate to Omnisca Access Connector.....	149
17.2	Providing Access to Horizon Desktops and Applications in Omnisca Access.....	150
17.2.1	Configure SAML Authentication in Horizon for Omnisca Access Integration .....	151
17.3	Add on-prem AD to Omnisca Access .....	153
17.4	Set Login Preferences in Omnisca Access.....	156
17.5	Create a Virtual App Collection for Horizon .....	156
17.5.1	Assign Pod to Network Ranges .....	158
17.5.2	Define Network Ranges .....	158
18.	2FA for UAG .....	162
18.1	rootPrepare VM for DUO Proxy Service .....	163
18.2	Create Application in DUO.....	164
18.3	Install the Duo Authentication Proxy .....	164
18.4	Configure and Start Authentication Proxy.....	166
18.5	Enroll users for using DUO 2FA.....	168
18.6	Configure UAG for Radius.....	168
18.7	Verify external access per 2FA.....	169
19.	Linux Deployment in Horizon.....	170
19.1	Create a Linux VM in vSphere.....	181
20.	Nacharbeiten .....	184
20.1	Troubleshooting Horizon.....	185
21.	Scripting & Automation .....	187
21.1	S&A Horizon .....	187
21.1.1	FSLogix – create a VHD(X) disk per user AND pool ID OR Hostname.....	187

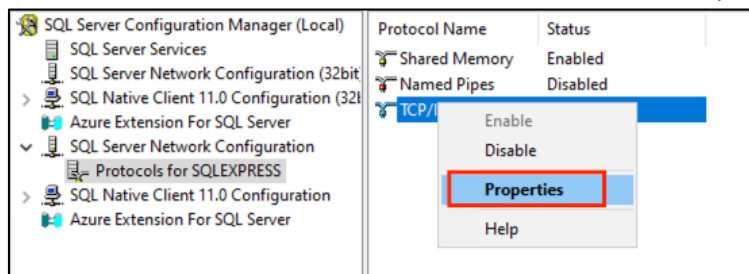
22.	References and KBs .....	191
23.	Table of Revisions .....	193

# 1. Prepare Horizon Environment

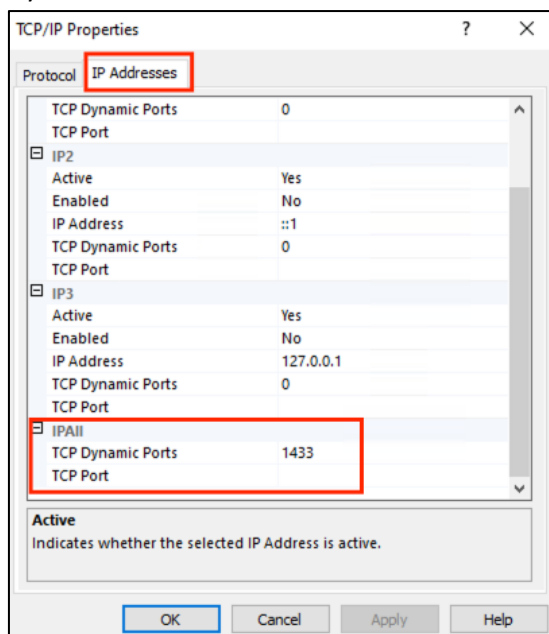
## 1.1 Create DB for Horizon Events

You need a database for recording of the Horizon Events. This must be a MS SQL, Oracle or PostgreSQL database. For testing and PoC purpose you can use a MS SQL Express version also.

- SQL Server Authentication is mandatory!
- Verify that port 1433 is opened for incoming requests in firewall of the SQL server
- In case you want to use MS SQL Express, you had to set the appropriate port, after you created the database
  - Start →SQL Server Configuration Manager, and switch to →SQL Server Network Configuration →Protocols for SQLEXPRESS
  - Select →TCP/IP, click on →Enable. After that, click to →Properties:

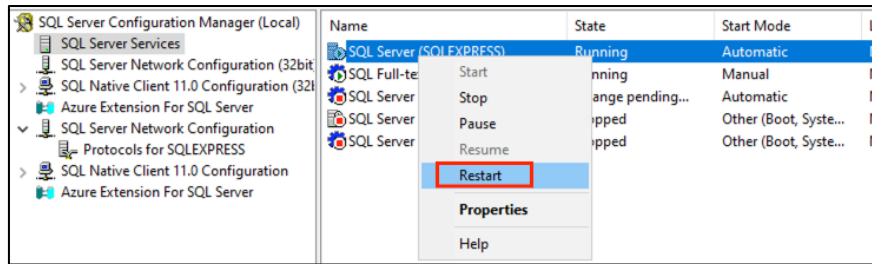


- Go to the tab “IP Addresses” and scroll down to “IPAll”. You can see the given “TCP Dynamic Ports” and set it to the default value “1433”:



- Click →Apply, then →OK

- Finally, you have to restart the “SQL Server (SQLEXPRESS)” Service:



## 1.2 Create vCenter Server Account for Horizon

For communication between Horizon and vCenter, you should create a dedicated role with needed privileges. Adding a dedicated user (AD-User or SSO-User) ensure that only minimum permissions are assigned.

- Privileges Required for the vCenter Server User With Instant Clones, see [here](#)

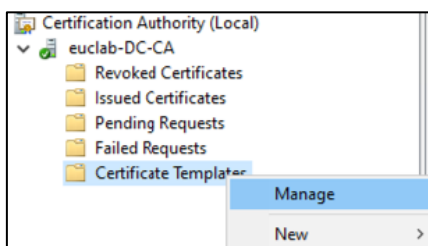
## 1.3 Create Domain Account for Horizon

For every domain which will be used for provisioning machines, a domain account has to be configured. Needed AD-permissions are documented [here](#) (Create a User Account for Instant-Clone Operations).

## 1.4 Create a Certificate Template for Horizon Connection Server

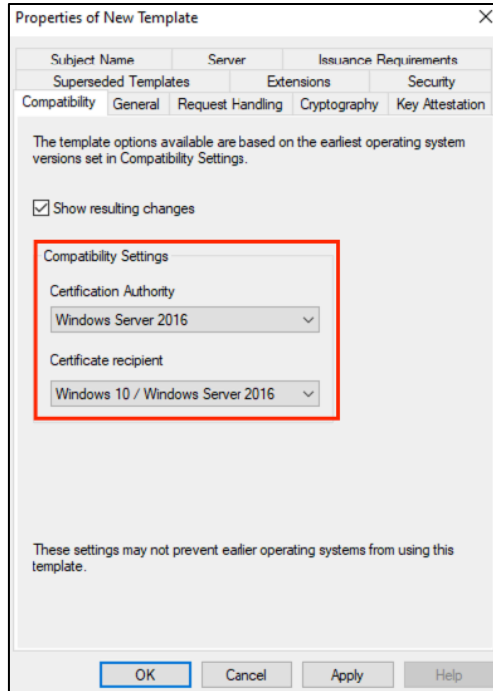
It is recommended to have a dedicated certificate template for Hoizon connection servers as described [here](#).

- On your CA Server, start → Certification Authority Console
- Select → Certificate Templates, and click → Manage to open the “Certificate Templates Console”:

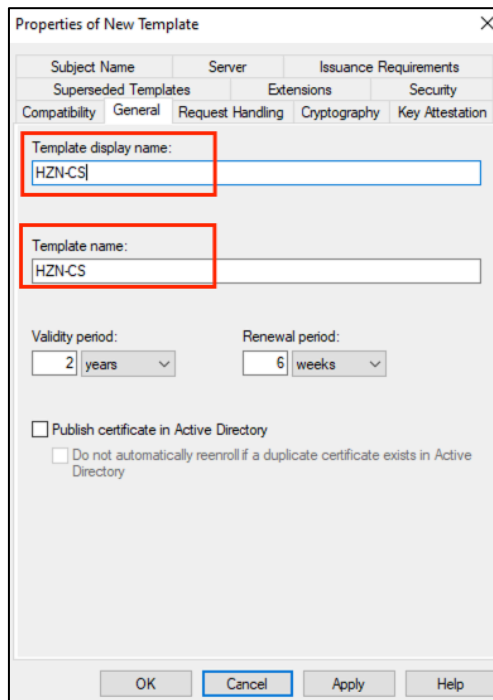


- Select the “Web Server” Template, and click on → Duplicate Template – the properties of the new template pop up

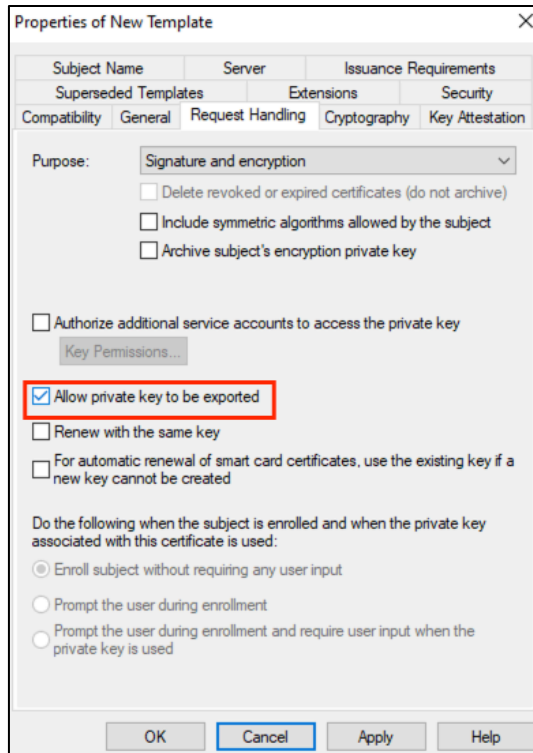
- Under tab →Compatibility set the compatibility settings



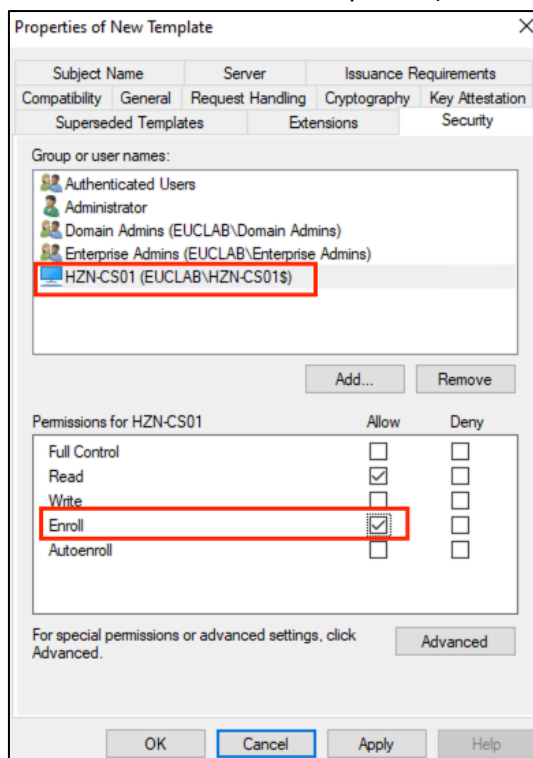
- Under tab →General, set a template display name



- Under tab →Request Handling, “Allow private key to exported”



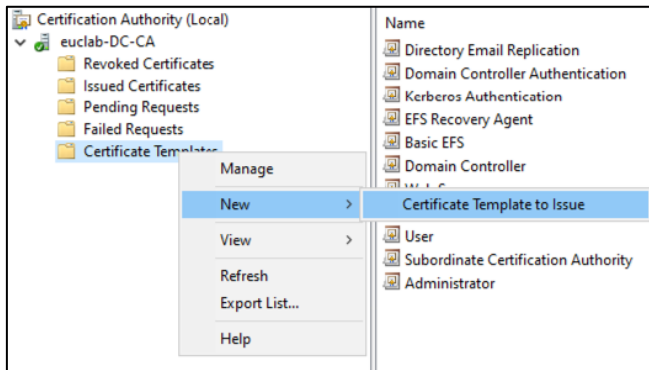
- Under tab →Security add the permission “Enroll” for domain users, or in minimum for the affected domain computers (which are used for Horizon connection servers)



- Submit and click →OK

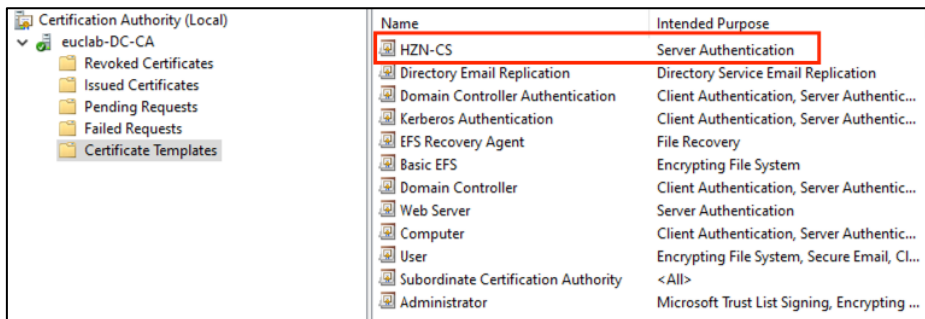
- Close the “Certificate Templates Console” Window

- In the CA, right-click on →Certificate Templates, then →New →Certificate Templates to Issue



- Select the previously created Template, and click →OK.

- Now you should see the new Template



## 1.5 Add Horizon ADMX Templates to GPO

Horizon offers multiple GPO templates. These have to be applied into the existing environment, as described [here](#) (Add a Horizon 8 ADMX Template File to a GPO).

- Copy the .admx files to the %systemroot%\PolicyDefinitions folder on your Active Directory server.
- Copy the language resource (.adml) files from subfolder en-US (or different language folder) to the appropriate subfolder in %systemroot%\PolicyDefinitions\ on your Active Directory server.

## 1.6 AV exclusion list for Horizon

Depending from the AV solution at customer site, consider to set an executable exclusion list for

- Horizon Connection Server

Folder Path	EXE Files
C:\Program Files\Omnissa\Horizon\Server\bin	ws_ConnectionServer.exe ws_dctservice.exe ws_MessageBusService.exe ws_scripthost.exe

	wsm.exe ws_tomcat-service.exe ws_tunnel-service.exe securitygateway.exe ws_dct-service.exe ws_cr-service.exe
--	-----------------------------------------------------------------------------------------------------------------------------

- Horizon Agent

Folder Path	EXE Files
C:\Program Files\Omnissa\Horizon\Agent\bin	wsm.exe wsm_jms.exe ws_script-host.exe SecurityGateway.exe tsdrvdisvc.dll
C:\Program Files\Omnissa\Horizon\Agent\Blast	VMBlastS.exe VMBlastW.exe
C:\Program Files (x86)\Common Files\Omnissa\USB\	omnissa-usbarbitrator64.exe
C:\Program Files\Common Files\Omnissa\ScannerRedirection\	Scanner.exe

- App Volumes Agent

Folder Path	EXE Files
C:\Program Files\Omnissa\AppVolumes\Agent\	svs-service.exe

- DEM Agent

Folder Path	EXE Files
C:\Program Files\Omnissa\DEM\	FlexEngine.exe FlexService.exe Flex+ Self-Support.exe

See the complete overview here, [URL](#)

Also see here: [Antivirus Considerations in a Horizon Environment](#)

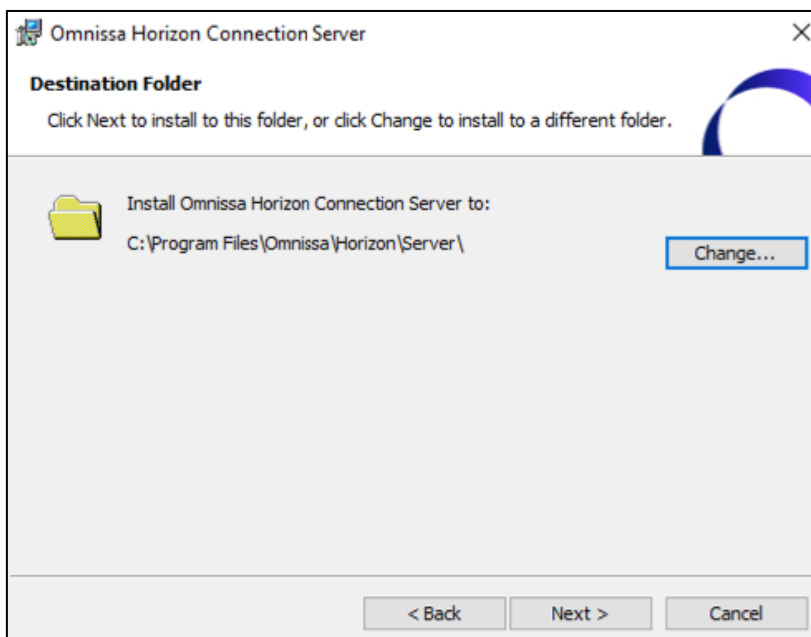
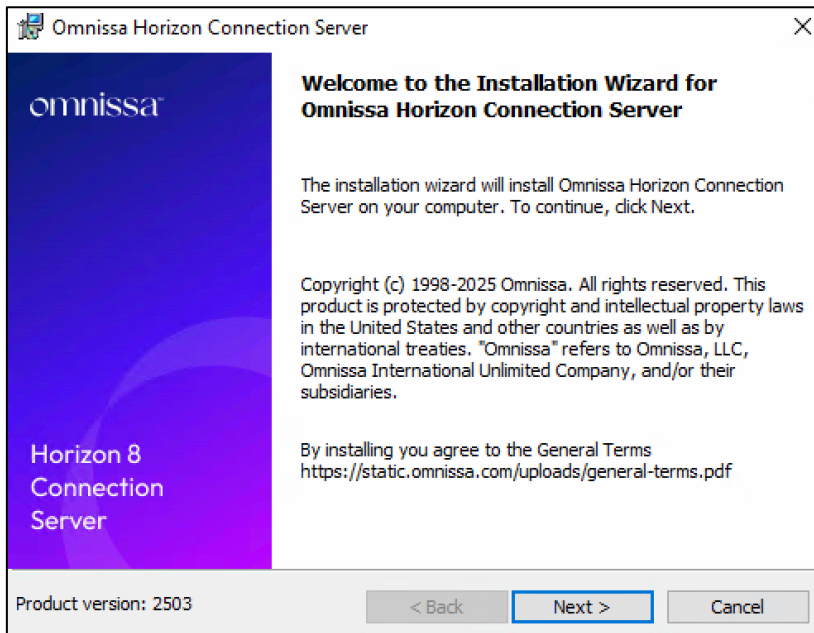
## 2. Setup Omnissa Horizon Standard Server

Version 2503 (8.15)

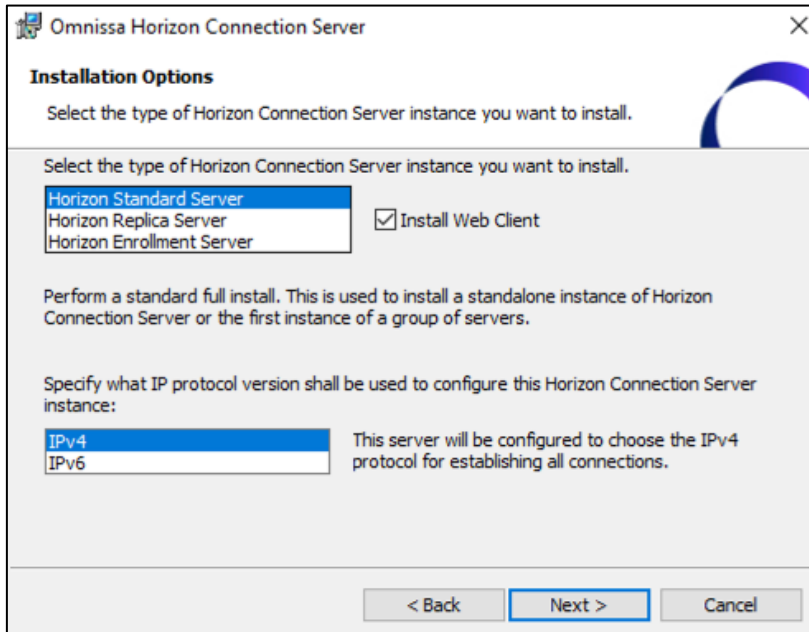
### 2.1 Initial Setup

- Requirements: Windows Server 2016 or higher

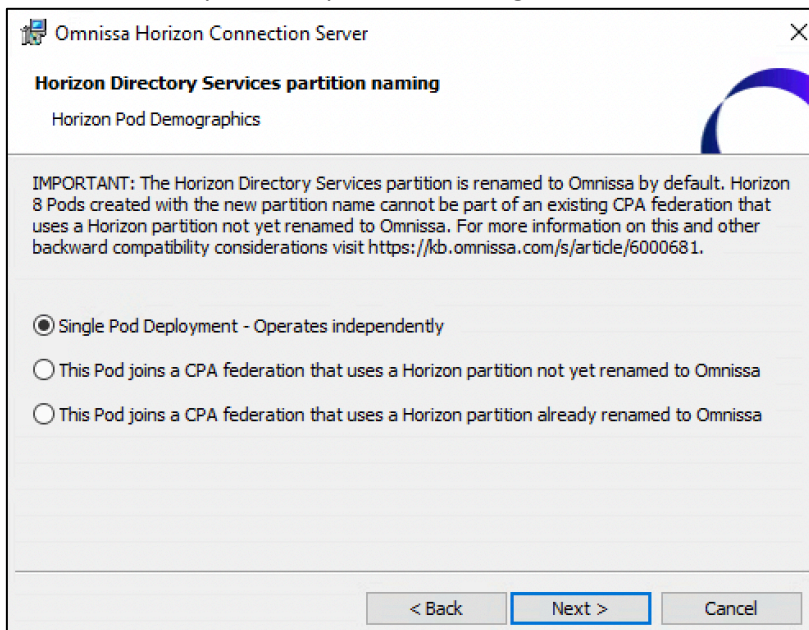
- Setup MS-Updates, VMware Tools
- Horizon Connection Server must be member of AD, and configured with a static IP
- Execute installation:



- Setup Horizon Standard Server:



- Horizon Directory Services partition naming:



- Set password for data recovery:

Omnissia Horizon Connection Server

### Data Recovery

Enter data recovery password details.

This password protects data backups of your Horizon Connection Server. Recovering a backup will require entry of this password.

Enter data recovery password:

Re-enter password:

Enter password reminder (optional):

< Back   Next >   Cancel

- Configure firewall automatically:

Omnissia Horizon Connection Server

### Firewall Configuration

Automatically configure the Windows Firewall to allow incoming TCP protocol connections.

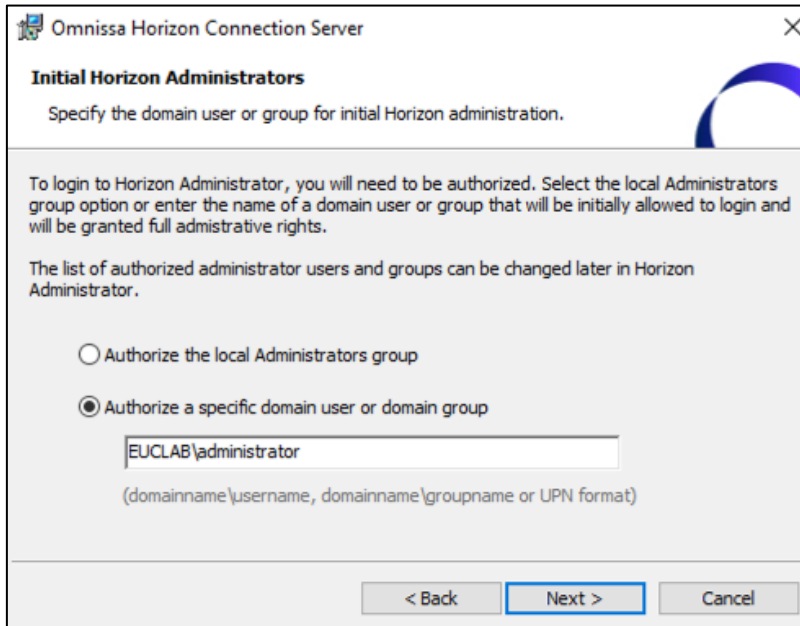
In order for Horizon Connection Server to operate on a network, specific incoming TCP ports must be allowed through the local Windows Firewall service. The incoming TCP ports for the Standard Server are 8009 (AJP13), 80 (HTTP), 443 (HTTPS), 4001 (JMS), 4002 (JMS-SSL), 4100 (JMSIR), 4101 (JMSIR-SSL), 4172 (PCoIP), 8472 (Inter-pod API), and 8443 (Web Client). UDP packets on port 4172 (PCoIP) are allowed through as well.

Configure Windows Firewall automatically

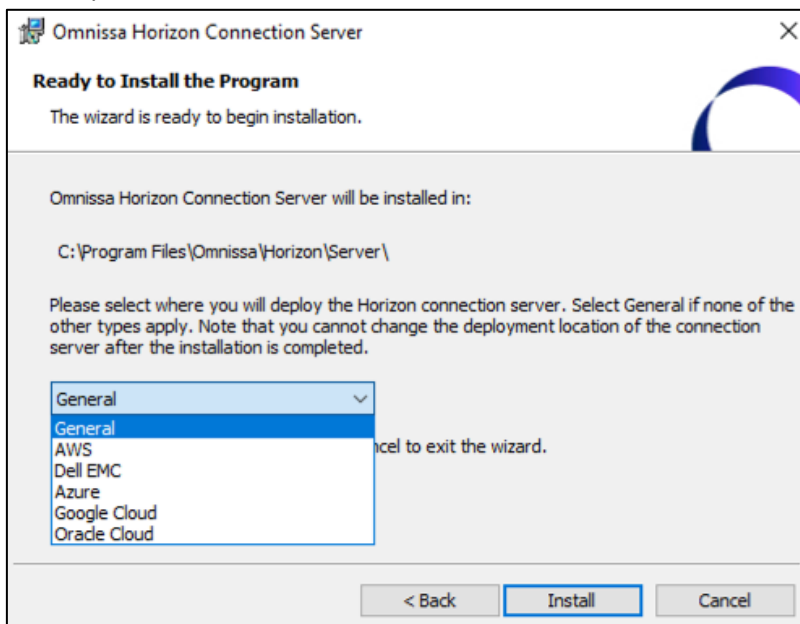
Do not configure Windows Firewall

< Back   Next >   Cancel

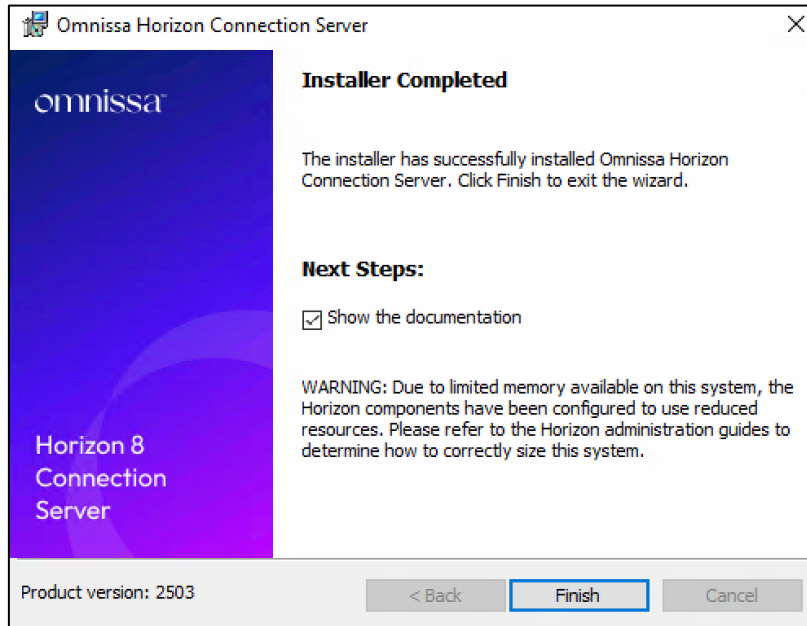
- Specify the authorized user or group for Horizon Console:



- For on-premises, select "General":

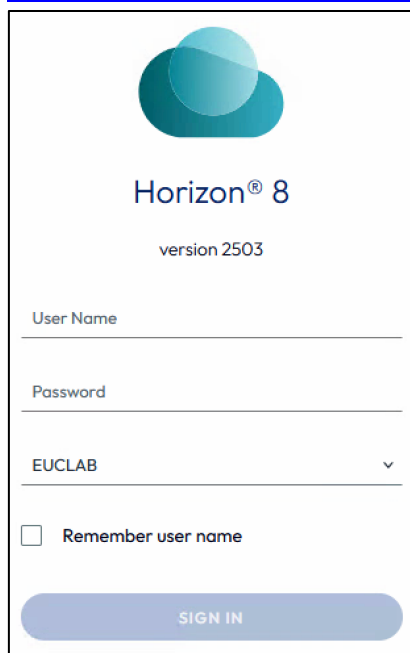


- Finish installation



- Now you can logon to the Horizon Administrator Console:

<https://connectionserver.domain/admin>



## 2.2 Initial Configuration Horizon Console

### 2.2.1 License Key

- Enter license key in Horizon Console under →Settings →Product Licensing and Usage, or configure subscription per Horizon Edge Gateway.

## 2.2.2 Event DB

- Configure Horizon Event Database under →Settings →Event Configuration:

**Edit Event Database**

Asterisk (\*) denotes required field

- \* Database Server: sql.euclab.org
- Database Type: Microsoft SQL Server
- \* Port: 1433
- \* Database Name: HZN-Events
- \* User Name: HZN-DB-Admin
- \* Password: \*\*\*\*\*
- \* Confirm Password: \*\*\*\*\*
- Table Prefix: VE\_

CANCEL OK

## 2.2.3 Add vCenter Server

- Add vCenter Server for provisioning desktops (or RDSH farms) – use the previously created vCenter Server Account for Horizon:

**Add vCenter Server**

1 vCenter Information | 2 Storage | 3 Ready to Complete

Asterisk (\*) denotes required field

- \* Server address: vcso.euclab.org
- \* User Name: hzn-sa@vsphere.local
- \* Password: \*\*\*\*\*

**Servers**

vCenter Servers | Gateways | Connection Servers | Gateway Certificates | App Volumes Managers | Capacity Providers

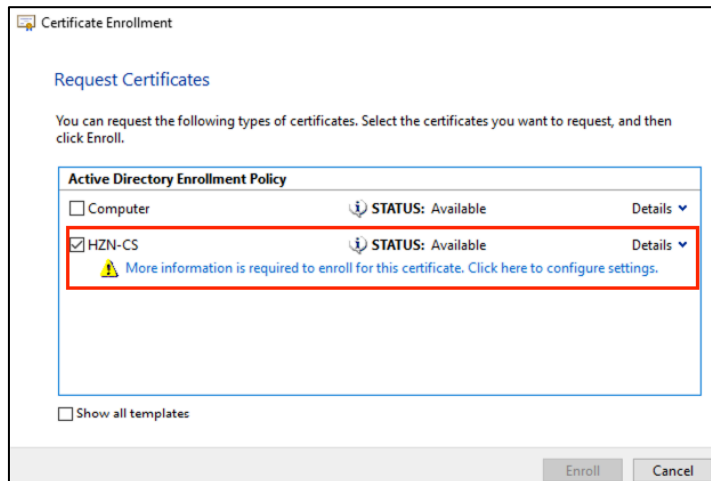
ADD | EDIT | REMOVE | MORE

vCenter Servers	VM Disk Space Reclamation	View Storage Accelerator	Provisioning
vcso.euclab.org(hzn-sa@vsphere.local)	✓		✓

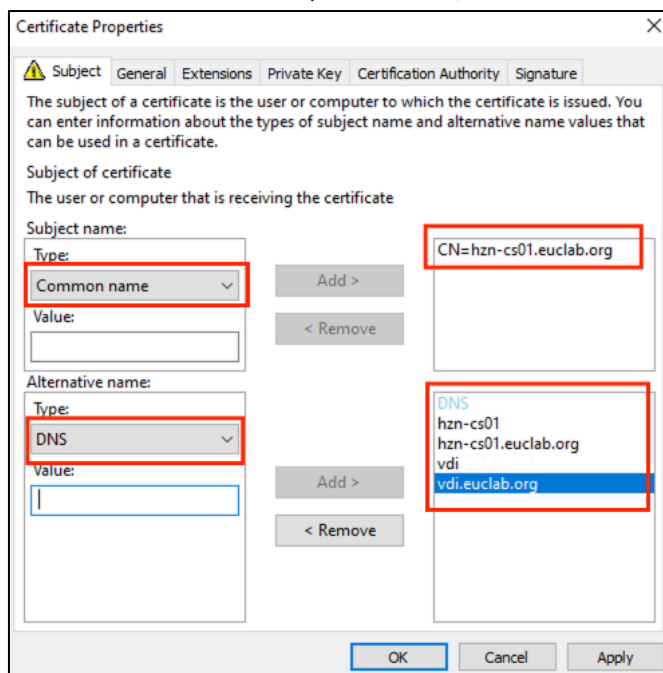
## 2.2.4 Request certificate

- For every Connection Server, request a valid (SAN-)certificate, based on the certificate template for Horizon

- In the MMC, add the certificate snap-in and request a new certificate (under →Personal →Certificates)

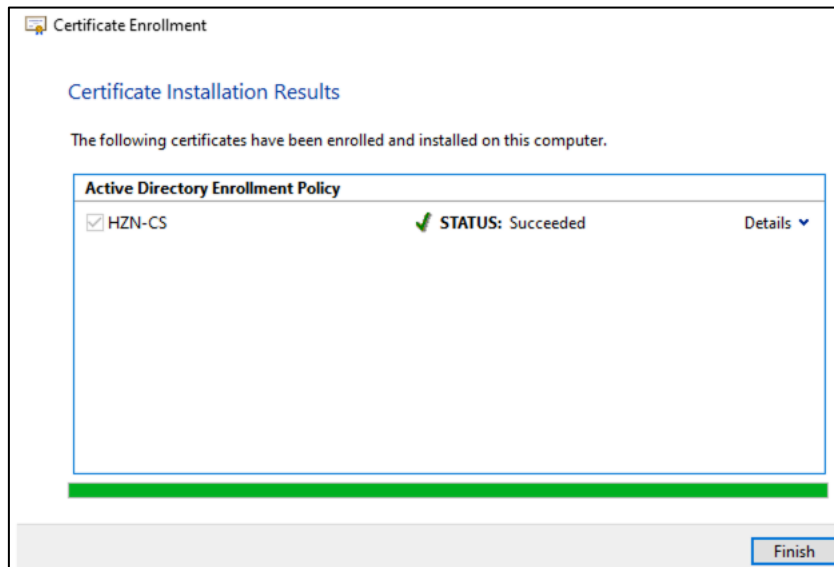


- Click on the “More information is required” link to edit the certificate properties
- Use the FQDN from the connection server as common name, and enter every alternative name as DNS (shortnames, Load Balancer FQDNs etc.)



- Submit with →OK

- Click →Enroll, finished



- The default self-signed certificate still has a friendly name “vdm”. This has to be renamed, and the previously requested certificate has to reflect the friendly name “vdm”.

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
Broker-RESTAuth	Broker-RESTAuth	21/03/2025	<All>	RestAuth-key-pair-...
HZN-CS01.euclab.org	HZN-CS01.euclab.org	24/06/2026	Server Authenticati...	vdm_old
hzn-cs01.euclab.org	euclab-DC-CA	21/03/2026	Server Authenticati...	vdm
PCoIP Security Gateway	VMware Horizon View Gateway R...	19/03/2034	Server Authenticati...	psgsc
PCoIP Security Gateway Contro...	VMware Horizon View Gateway R...	19/03/2034	Client Authentication	psgcc

- Restart “VMware Horizon View Connection Server” Service to take changes effect.

## 2.2.5 Locked.properties

For security reasons, the connection server only allows connections from clients which use the address from the connection itself. See also [here](#) (Cross-Origin Resource Sharing (CORS) with Horizon 8 and loadbalanced HTML5 access) .Connections using (short)names or IP addresses of a load balancer, alias or similar will fail. For that purpose, these URLs have to be recognized in a file called locked.properties

- Go to → C:\Program Files\Omnissa\Horizon\Server\sslgateway\conf  
Create (if not exists) a file “locked.properties” and edit this as following:

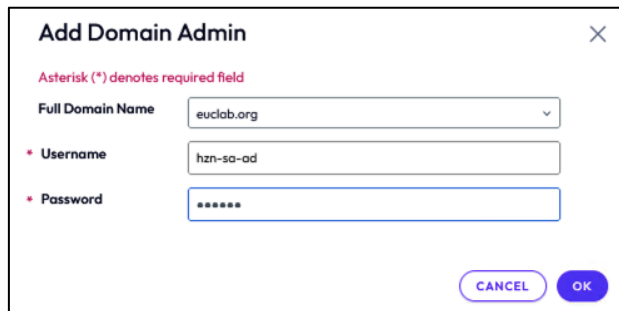
```
checkOrigin=false (optional)
enableCORS=false (optional)
balancedHost=FQDN Load Balancer
portalHost.1=FQDN of a valid URL
portalHost.2=FQDN of a valid URL
portalHost.n=FQDN of a valid URL
```

- Restart “Omnissa Horizon Connection Server” Service to take changes effect.

## 2.2.6 Add Domain Accounts

For every domain which will be used for provisioning machines, a domain account has to be configured. Needed AD-permissions are documented [here](#) (Create a User Account for Instant-Clone Operations).

- Go to →Settings →Domains
- Add needed domain admin accounts



## 2.2.7 Optional configuration

Some initial configuration are recommended, but not mandatory.

- Configure or add roles and permissions for relevant user groups only
  - Create a role within Horizon Console with privilege “Colect Operation Logs” for Troubleshooting.
- Consider Global Settings to edit
  - Horizon Console Settings (timeout, automatic refresh etc.)
  - Client Settings (forcibly disconnect users, send domain list etc.)
- Consider to edit the connection server settings
  - Are secure tunnel needed for HTTPS or Blast gateway?
  - Should backup scheduling be modified?

# 3. Setup Horizon Edge Gateway

Version 2506.1

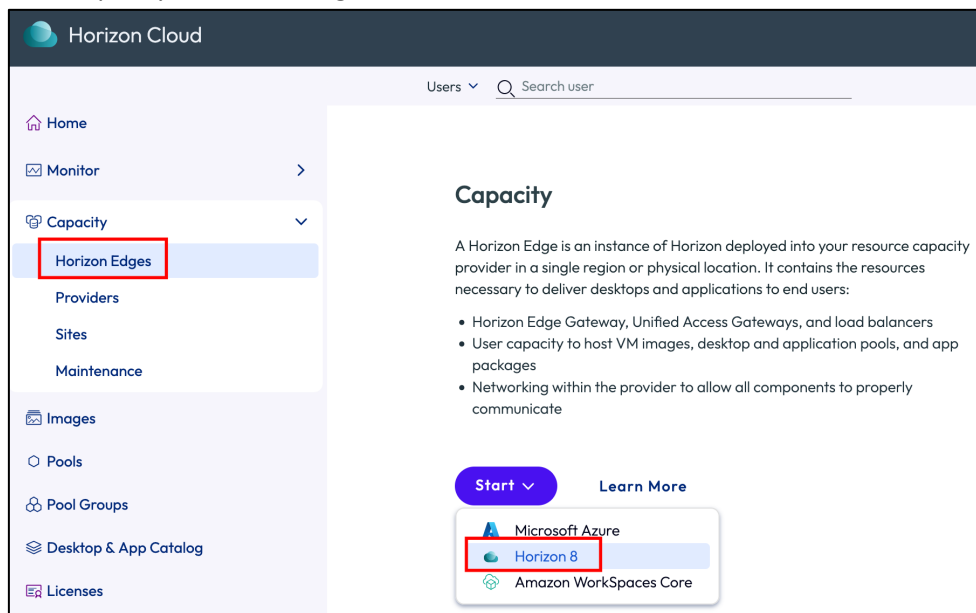
## 3.1 Requirements

- Follow the documentation about needed DNS, ports, and protocols needed for the Horizon Edge Gateway – see [URL](#)
- Additional URLs must be reachable from local deployment, as described [here](#)
- DNS record (forward and reverse DNS) for the Edge Gateway in the local AD

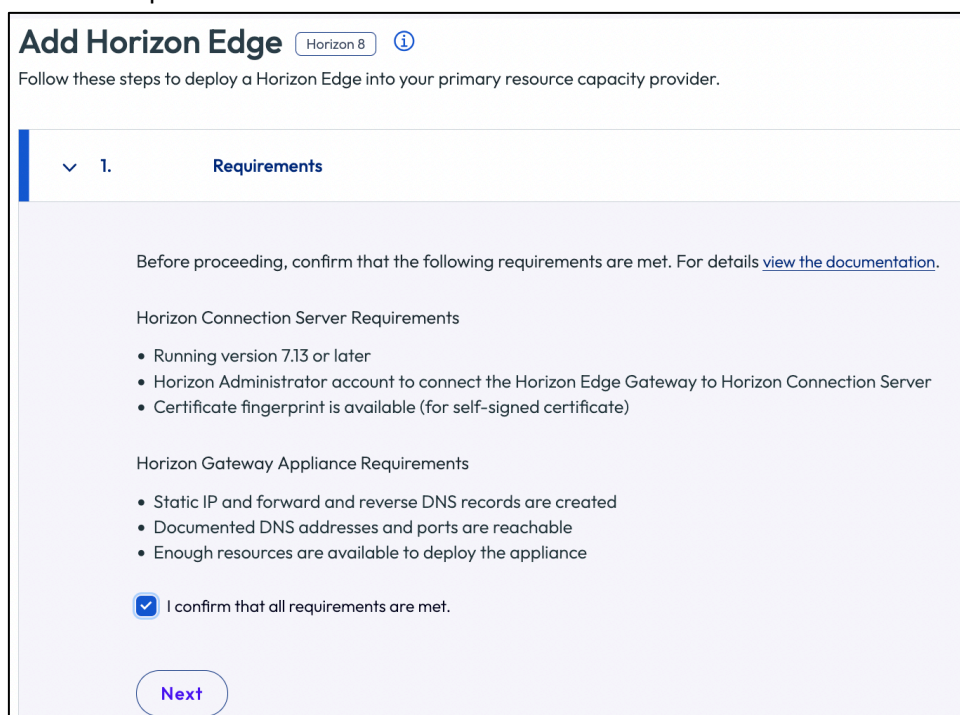
- static ip address
- (optional) define an AD service account with permission to the role “Horizon Cloud Service” – this is needed for the communication between Edge Gateway and Connection Server

## 3.2 Deployment Horizon Edge Gateway

- Login to the Horizon Universal Console ([URL](#) – if needed switch to your organization) and go to →Capacity →Horizon Edges →Start →Horizon 8:



- Confirm Requirements and click →Next



- Set the Name for the Edge Gateway and click →Next

**Add Horizon Edge** Horizon 8 ⓘ

Follow these steps to deploy a Horizon Edge into your primary resource capacity provider.

> ✓ Requirements

▼ 2. General Information

Horizon Edge name  ⓘ

Description (optional)

[Next](#)

- Select Capacity Type and enter Location, and click →Next

▼ 3. Capacity Provider

Capacity type

Location

[Next](#)

- Provide the FQDN of the Edge Gateway, and click →Next

▼ 4. Horizon Edge Gateway

FQDN

Agent Monitoring  ⓘ

[Next](#)

- If not done already, download the actual OVA image, and click →Next

5. Download Horizon Edge Gateway Appliance

Download the image for the Edge Gateway appliance to deploy on your virtualization platform.

Edge Gateway Appliance			
Name	horizon-edge-gw-2506.1.0.ova	File type	Open Virtual Appliance
Release date	August 5, 2025	File size	5809 MB
Build number	237	MD5SUM	ac37b6aa392466d641ffa350d1a33c7
SHA256SUM	cd000e80dccb297ab74f3b65b8cd6eb a94344608c6e625b4f70f53061b20e61 6		

Download

Next

- Deploy the Edge Gateway in your SDDC. You need the pairing code during deployment.

6. Deploy and Pair Horizon Edge Gateway

To deploy the Horizon Edge Gateway appliance and connect to Horizon Cloud Service, follow these steps.

1. Log in to the vCenter administration console and open the appliance deployment wizard.
2. Deploy the appliance and enter the pairing code.

Pairing code:

1. Power on the Horizon Edge Gateway appliance to connect it to Horizon Cloud Service. You can wait for pairing to complete on Server.

**Pairing Code** eyJjb25uZWNOaW9uU3RyaW5nljoiSG9zdE5hbWU9ZWRnZW...

**Pairing Status** ⚠ Not Paired [Refresh](#)

[Save & Close](#) [Next](#)

- You have to enter static network information during the OVF deployment (please use FQDN for hostname). After booting up the deployed appliance, the pairing status should switch to “Paired” (can take some time). Click →Next

6. Deploy and Pair Horizon Edge Gateway

To deploy the Horizon Edge Gateway appliance and connect to Horizon Cloud Service, follow these steps.

1. Log in to the vCenter administration console and open the appliance deployment wizard.
2. Deploy the appliance and enter the pairing code.

Pairing code:

1. Power on the Horizon Edge Gateway appliance to connect it to Horizon Cloud Service. You can wait for pairing to complete on Server.

**Pairing Code** eyJjb25uZWNOaW9uU3RyaW5nljoiSG9zdE5hbWU9ZWRnZW...

**Pairing Status** [Pairing Successful](#)

[Save & Close](#) [Next](#)

- In the last step, you have to enter the information about one of the connection server of the POD. Click →Finish, you have to check and confirm the certificate.

- Now you can see the successful deployed Edge Gateway

Name	Status	Provider Type	Provider Name	Site name	Region	Unified Access Gateway	Horizon Edge Gateway
HZN-EGW	Connected	Horizon 8	HZN-EGW	-	-	Not Configured	Connected

- Additionally, you can check the license type in the Horizon Console of the connection server

- Note – you can still switch between subscription and perpetual/term license indeed. In case of switching (back from perpetual/term to subscription), it can take up to 24 hours, until this will be reflected in the UI of the Horizon Console.

### 3.3 Further options for Edge GW

- Enable SSH Access for Horizon Edge, see [here](#)
  - Divergent from Doc, use this command in the VM console:  
/opt/horizon/bin/configure-adapter.py --sshEnable
  - Type vi /etc/ssh/sshd\_config
  - Change the line PermitRootLogin no to PermitRootLogin yes

- Restart the sshd daemon by running the command `systemctl restart sshd`
- Set customized NTP per CLI
  - `systemctl status systemd-timesyncd`
  - `vi /etc/systemd/timesyncd.conf` and add time servers under [Time]
  - `systemctl restart systemd-timesyncd`
  - `systemctl status systemd-timesyncd`
- If needed, Troubleshooting Horizon 8 Edge Connectivity Issues (92056), see [KB-article](#)

### 3.4 Update Horizon Edge Gateway

New version: 2506.1

- Download latest version via Horizon Cloud Portal

**Horizon Edge Gateway**

i A new version 2506.1.0 is available for upgrade for this Edge Gateway. [View](#)

<b>Version</b>	2412.0.0
<b>FQDN</b>	hzn-egw.euclab.org
<b>Agent Monitoring</b>	<span style="color: green;">✔</span> Enabled
<b>Deployment status</b>	<span style="color: green;">✔</span> Ready
<b>Connectivity status</b>	<span style="color: green;">✔</span> Connected
<b>Appliance</b>	<a href="#" style="color: #0056b3; text-decoration: none;">Download</a>
<b>Pairing code</b>	<a href="#" style="color: #0056b3; text-decoration: none;">Retrieve Code</a>

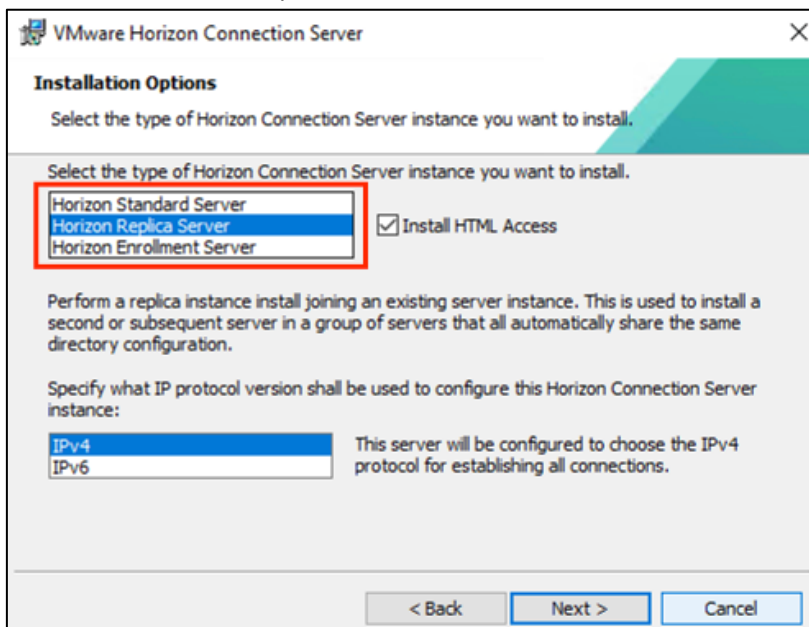
- Shutdown and rename existing Edge Gateway

- Deploy new Edge Gateway as usual (see previous chapter), and verify it in Horizon Cloud

Horizon Edge Gateway	
Version	2506.1.0
FQDN	hzn-egw.euclab.org
Agent Monitoring	✔ Enabled
Deployment status	✔ Ready
Connectivity status	✔ Connected
Appliance	<a href="#">Download</a>
Pairing code	<a href="#">Retrieve Code</a>

## 4. Setup VMware Horizon Replica Server

- Requirements: Windows Server 2016 or higher
- Setup MS-Updates, VMware Tools
- Horizon Connection Server must be member of AD, and configured with a static IP
- Execute installation in the same way as the [Horizon Standard Server](#), but choose Replica Server as Installation Option:



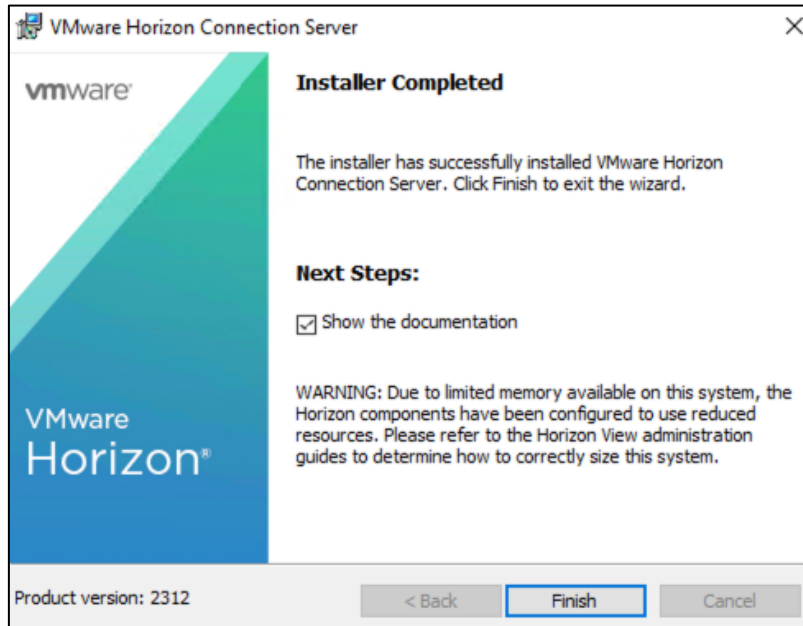
- Enter the FQDN of an existing Connection Server:

The screenshot shows the 'Source Server' configuration window in VMware Horizon. The title bar reads 'VMware Horizon Connection Server'. The main heading is 'Source Server' with the instruction: 'Select an existing Horizon Connection Server instance from which to replicate.' Below this, there is explanatory text: 'A group of Horizon Connection Server instances that share the same configuration data is called a Horizon Connection Server group. Setup will replicate configuration data from an existing server instance. Enter the server name of an existing Horizon Connection Server instance to make this server part of that group. Example server: view.internal.vmware.com.' A text input field labeled 'Server:' contains the value 'hzn-cs01.eudab.org' with a '(hostname or IP address)' label to its right. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- Configure firewall automatically and click →Next →Install:

The screenshot shows the 'Firewall Configuration' window in VMware Horizon. The title bar reads 'VMware Horizon Connection Server'. The main heading is 'Firewall Configuration' with the instruction: 'Automatically configure the Windows Firewall to allow incoming TCP protocol connections.' Below this, there is explanatory text: 'In order for Horizon Connection Server to operate on a network, specific incoming TCP ports must be allowed through the local Windows Firewall service. The incoming TCP ports for the Standard Server are 8009 (AJP13), 80 (HTTP), 443 (HTTPS), 4001 (JMS), 4002 (JMS-SSL), 4100 (JMSIR), 4101 (JMSIR-SSL), 4172 (PCoIP), 8472 (Inter-pod API), and 8443 (HTML Access). UDP packets on port 4172 (PCoIP) are allowed through as well.' There are two radio button options: 'Configure Windows Firewall automatically' (which is selected) and 'Do not configure Windows Firewall'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- Finish installation



- Next step: [Request Certificate](#) for the added replica server

## 5. Setup TrueSSO

Reference – [URL](#)

With the True SSO (single sign-on) feature, after users log in to Omnisia Workspace ONE Access using a smart card or RSA SecurID or RADIUS authentication, or a third-party identity provider using an Unified Access Gateway appliance, users are not required to also enter Active Directory credentials in order to use a virtual desktop or published desktop or application.

If a user authenticates by using Active Directory credentials, the True SSO feature is not necessary, but you can configure True SSO to be used even in this case, so that the AD credentials that the user provides are ignored and True SSO is used.

The following steps are needed to implement TrueSSO:

1. Set Up an Enterprise Certificate Authority
2. Create Certificate Templates Used with True SSO
3. Install and Set Up an Enrollment Server
4. Pair Connection and Enrollment Server
5. Configure SAML Authentication to Work with True SSO
6. Configure Horizon Connection Server for True SSO

## 5.1 Set Up an Enterprise Certificate Authority

You need an enterprise CA. Best practise ist to implement a sub CA, optional installed on the same system like the Horizon enrollment server, or on a dedicated server system.

Short introduction:

Enabling non-persistent certificate processing can help reduce the CA database growth rate and frequency of database management tasks. Enabling this setting does not prevent the CA from storing issued certificates and it does not prevent general certificate revocation checking.

By default, when you enable non-persistent certificate processing, all issued certificates are still stored in the database. Use this to configure the CA for specific templates for which the CA does not store a copy of issued certificates. Therefore, for this setting to have any affect, you must also configure this setting on the individual certificate template. All out of the box templates have this setting disabled, which means that even if the CA is configured to allow volatile requests it will still store a copy of issued certificates.

TrueSSO requests a new certificate for every new connection. If all of these certificates are kept, eventually the CA will run out of disk space and you will see a degradation of CA performance.

The only practical reason why you need to keep the certificates in the CA database is to allow the administrator to revoke a specific certificate. **Since you can configure a short certificate lifetime for certificates used with True SSO there is no practical requirement to be able to revoke individual certificates used by True SSO.**

True SSO certificates only need to be valid long enough for the logon to complete. The Microsoft Certificate Management console allows you to configure a short one hour life time for a certificate.

If you enable this setting, and you do not change other certificate templates to request that they not be stored in the CA database, only those certificates that True SSO uses are kept out of the CA database.

If you have an existing CA, and do not want to enable this setting for the CA, you can set up additional dedicated CAs exclusively for True SSO and on which you enable the True SSO Certificate template. You can enable the DBFLAGS\_ENABLEVOLATILEREQUESTS setting on these CAs. You can then use the existing CA to issue all other certificates including the Enrollment Certificate required by Horizon Enrollment Server<sup>1</sup>.

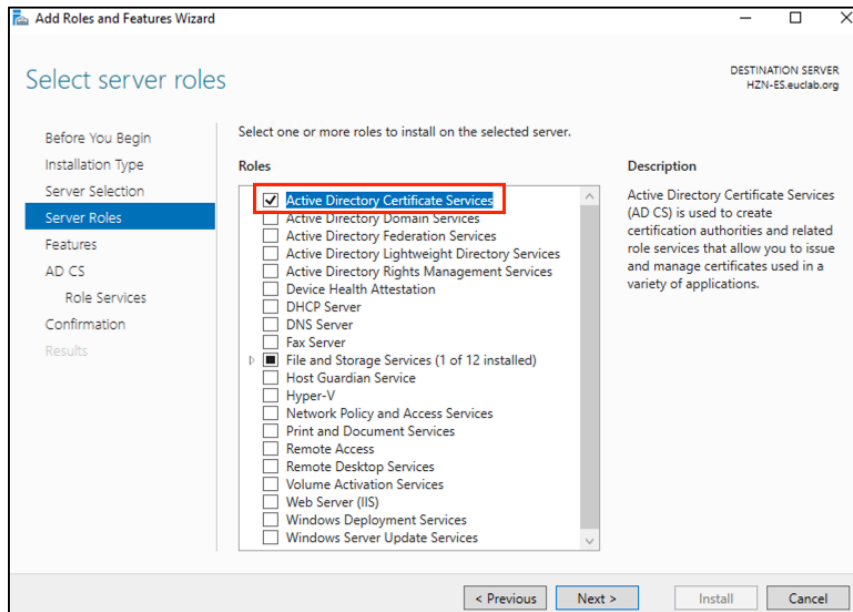
### 5.1.1 Create Sub-CA

In this example, we create a sub CA on the same host which will be used as Enrollment Server.

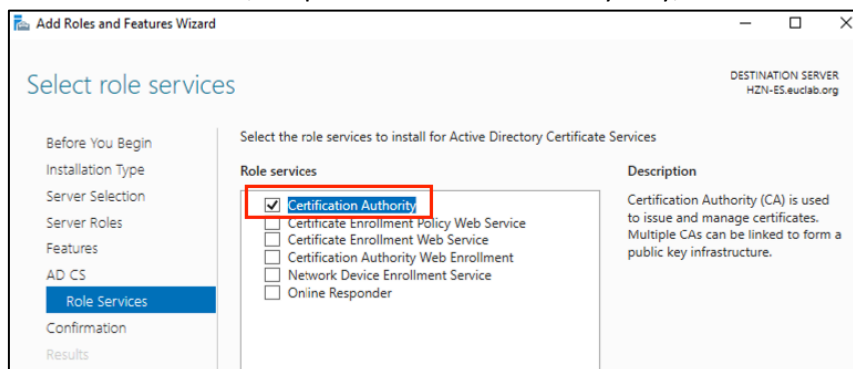
---

<sup>1</sup> Quelle: <https://kb.omnissa.com/s/article/2149312>

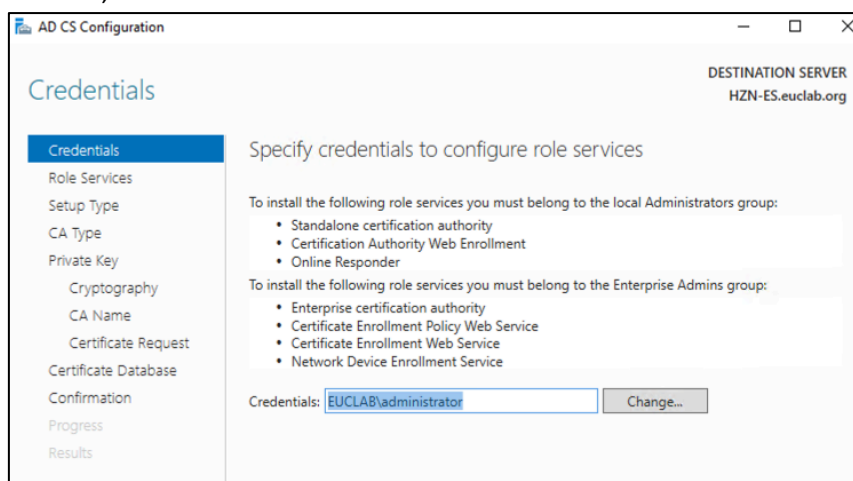
- Add AD CS role and click →Next



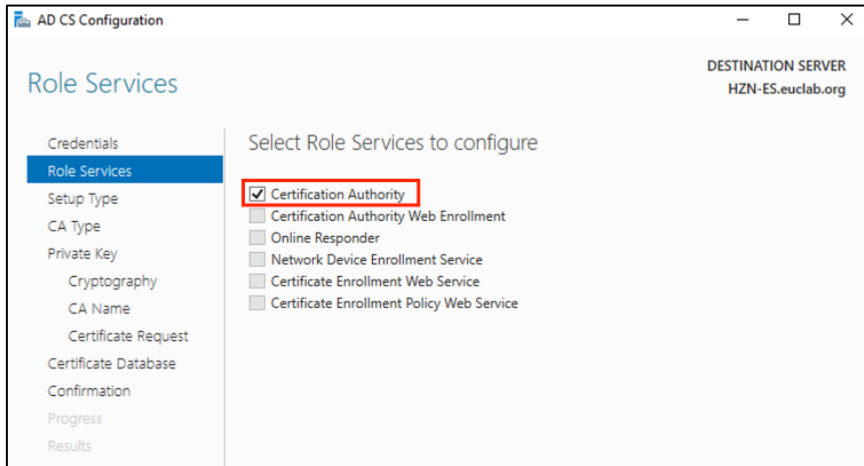
- For the role services, keep the Certificate Authority only, and click →Next, then →Install:



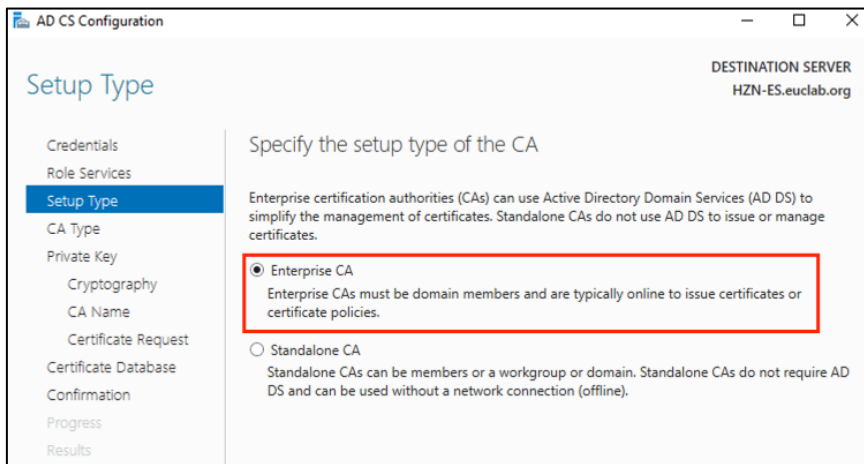
- After installation, proceed with the configuration. Specify credentials to configure role services, and click →Next:



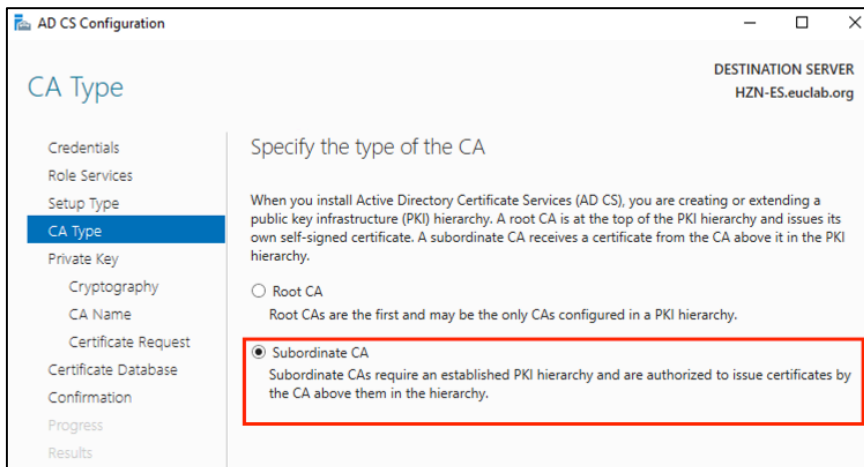
- Select the “Certificate Authority” to configure, and click →Next:



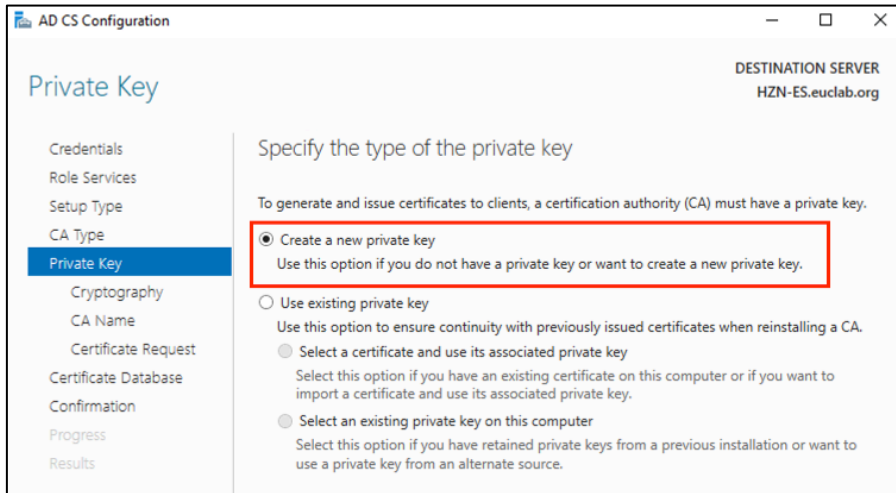
- Chosse “Enterprise CA”, and click →Next:



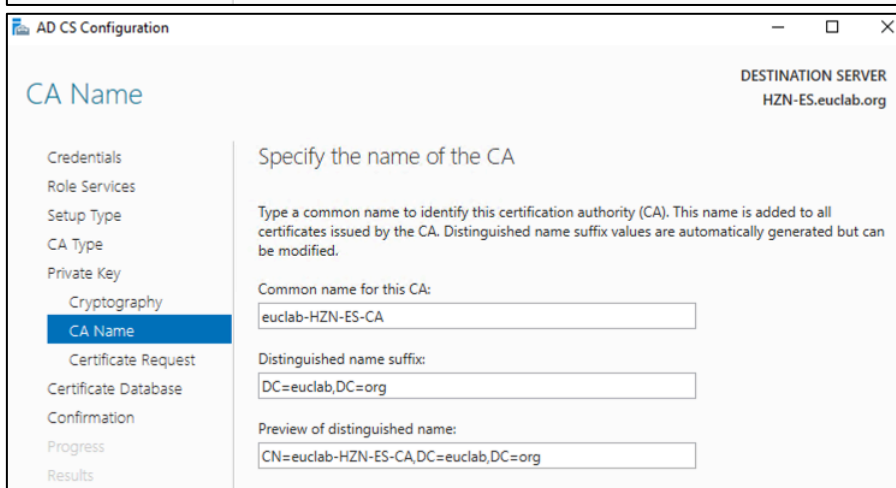
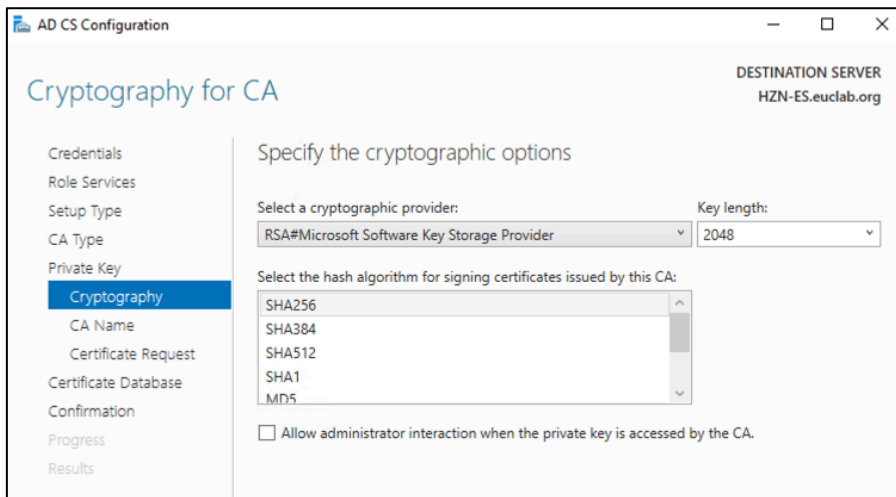
- Choose “Subordinate CA”, and click →Next:



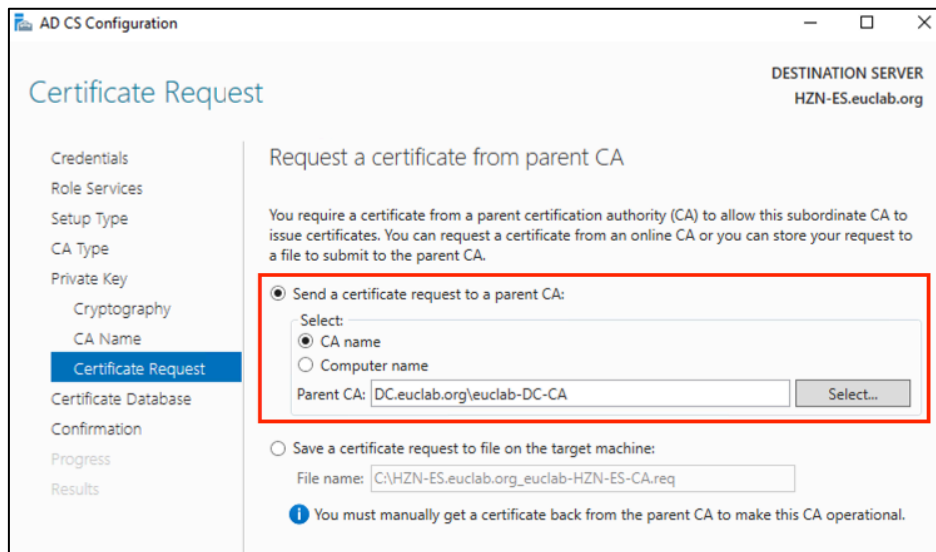
- Choose “Create a new private key”, and click →Next:



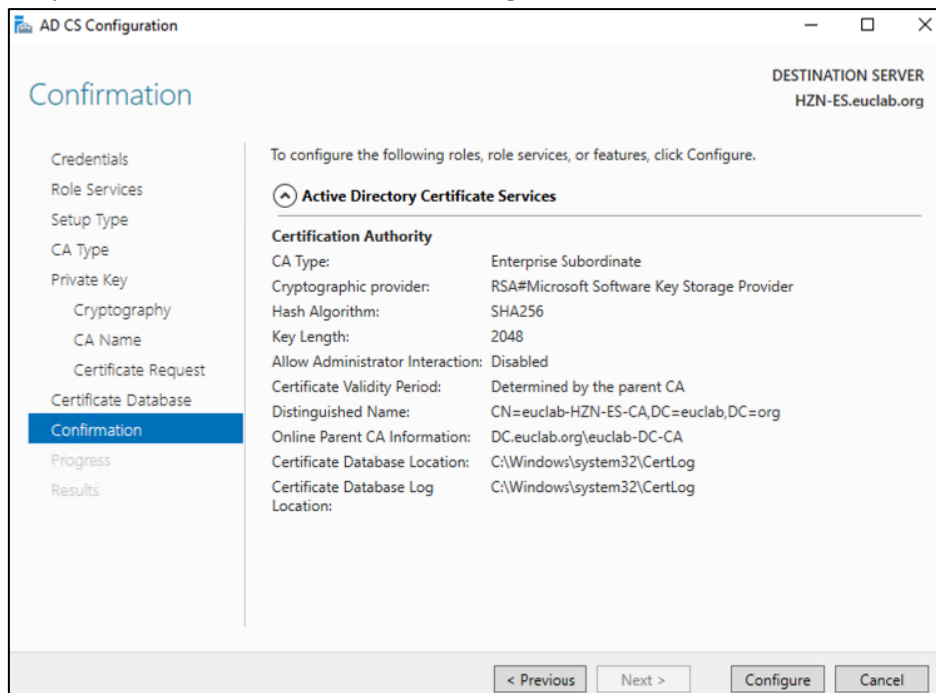
- Keep the default settings for the next two steps:



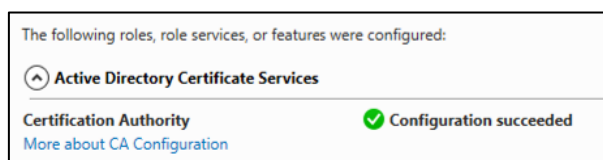
- To allow this Seb CA to issue certificates, you require a certificate from the parent CA. You can send this request to the parent CA directly. Click →Next:



- Keep the rest as default, and click →Configure:



- It should finish after some seconds:



## 5.1.2 Enable non-persistent certificate processing

- Execute the following command to configure the CA for non-persistent certificate processing  
certutil -setreg DBFlags +DBFLAGS\_ENABLEVOLATILEREQUESTS

```
C:\Users\administrator.VEUC>certutil -setreg DBFlags +DBFLAGS_ENABLEVOLATILEREQUESTS
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBFlags:

Old Value:
  DBFlags REG_DWORD = b0 (176)
  DBFLAGS_MAXCACHESIZEX100 -- 10 (16)
  DBFLAGS_CHECKPOINTDEPTH60MB -- 20 (32)
  DBFLAGS_LOGBUFFERSHUGE -- 80 (128)

New Value:
  DBFlags REG_DWORD = 8b0 (2224)
  DBFLAGS_MAXCACHESIZEX100 -- 10 (16)
  DBFLAGS_CHECKPOINTDEPTH60MB -- 20 (32)
  DBFLAGS_LOGBUFFERSHUGE -- 80 (128)
  DBFLAGS_ENABLEVOLATILEREQUESTS -- 800 (2048)
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.

C:\Users\administrator.VEUC>
```

- Enter the following command to prevent a service interruption if the root CA CRL is allowed to expire:

```
certutil -setreg ca\CRLFlags +CRLF_REVCHECK_IGNORE_OFFLINE

C:\Users\administrator.VEUC>certutil -setreg ca\CRLFlags +CRLF_REVCHECK_IGNORE_OFFLINE
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\VEUC-HZN-ES1-CA\CRLFlags:

Old Value:
  CRLFlags REG_DWORD = 2
  CRLF_DELETE_EXPIRED_CRLS -- 2

New Value:
  CRLFlags REG_DWORD = a (10)
  CRLF_DELETE_EXPIRED_CRLS -- 2
  CRLF_REVCHECK_IGNORE_OFFLINE -- 8
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.

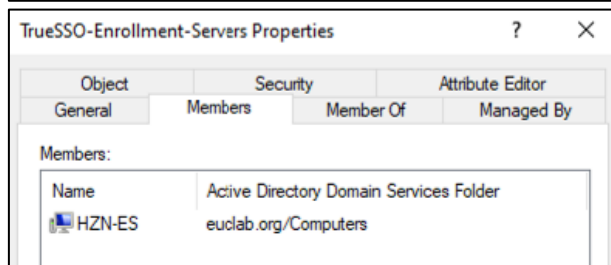
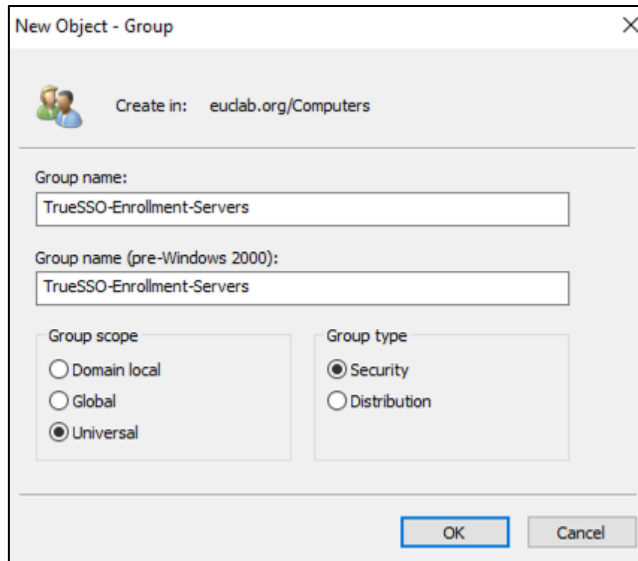
C:\Users\administrator.VEUC>
```

- Enabling CRLF\_REVCHECK\_IGNORE\_OFFLINE setting will depend on the PKI architecture and is not a strict requirement for True SSO. In the unlikely event that the root CRL is inaccessible, set this to avoid revocation check failures.
- Enter the following commands to restart the service:  
sc stop certsvc  
sc start certsvc

## 5.2 (optional) Add Security Group for Enrollment Servers

Create a Security group in the domain (and forest) for the enrollment servers, and add the related computer accounts. This group can be added to the certificate template for TrueSSO later.

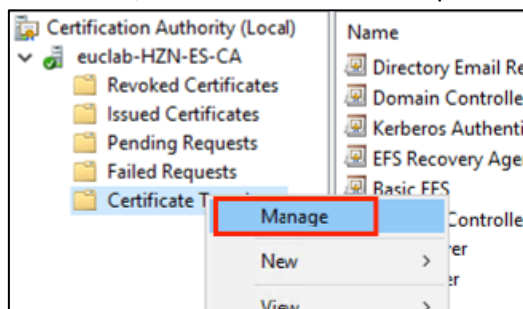
- At the domain controller, add a new Universal Group



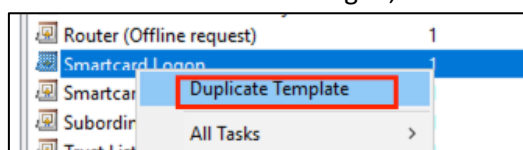
### 5.3 Create Certificate Template used with True SSO

You must create a certificate template that can be used for issuing short-lived certificates, and you must specify which computers in the domain can request this type of certificate.

- On the server with Sub CA installed, open the →Certification Authority
- On the left, select →Certificate Template →Manage



- Look for the →Smartcard Logon, and click →Duplicate Template



- Make the following changes

- **Compatibility** – select appropriate CA and certificate recipient

The screenshot shows the 'Properties of New Template' dialog box with the 'Compatibility' tab selected. The 'Compatibility Settings' section is highlighted with a red box. It contains two dropdown menus: 'Certification Authority' set to 'Windows Server 2008 R2' and 'Certificate recipient' set to 'Windows 8 / Windows Server 2012'. The 'Show resulting changes' checkbox is checked. The dialog also includes tabs for Subject Name, Server, Issuance Requirements, Superseded Templates, Extensions, Security, Request Handling, Cryptography, and Key Attestation. At the bottom, there are buttons for OK, Cancel, Apply, and Help.

- **General** – the default maximum lifetime of a user ticket is 10 hours, so it should be configured similar. The renewal periods should reflect 50%-75% of the validity period.

The screenshot shows the 'Properties of New Template' dialog box with the 'General' tab selected. The 'Template display name' and 'Template name' fields are both set to 'TrueSSO|' and 'TrueSSO' respectively, and are highlighted with red boxes. The 'Validity period' is set to '10 hours' and the 'Renewal period' is set to '6 hours', both highlighted with red boxes. The 'Publish certificate in Active Directory' checkbox is unchecked, and the sub-option 'Do not automatically reenroll if a duplicate certificate exists in Active Directory' is also unchecked. The dialog includes tabs for Subject Name, Server, Issuance Requirements, Superseded Templates, Extensions, Security, Request Handling, Cryptography, and Key Attestation. At the bottom, there are buttons for OK, Cancel, Apply, and Help.

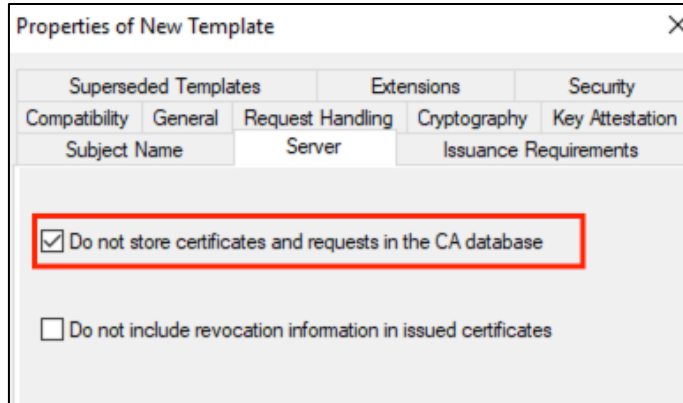
○ Request Handling

The screenshot shows the 'Properties of New Template' dialog box with the 'Request Handling' tab selected. The 'Purpose' dropdown is set to 'Signature and smartcard logon'. Three checkboxes are present: 'Delete revoked or expired certificates (do not archive)', 'Include symmetric algorithms allowed by the subject', and 'Archive subject's encryption private key', all of which are unchecked. Below these, there are three more checkboxes: 'Allow private key to be exported', 'Renew with the same key (\*)', and 'For automatic renewal of smart card certificates, use the existing key if a new key cannot be created'. The last checkbox is checked. Underneath, there are three radio button options for enrollment: 'Enroll subject without requiring any user input', 'Prompt the user during enrollment' (which is selected), and 'Prompt the user during enrollment and require user input when the private key is used'. A note at the bottom states '\* Control is disabled due to compatibility settings.' The 'Cancel' button is highlighted with a red box.

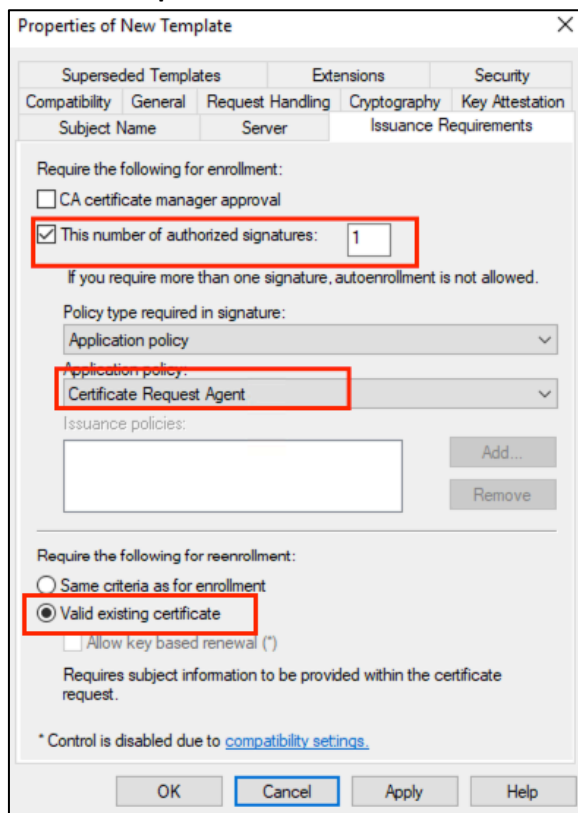
○ Cryptography

The screenshot shows the 'Properties of New Template' dialog box with the 'Cryptography' tab selected. The 'Provider Category' dropdown is set to 'Key Storage Provider' and the 'Algorithm name' dropdown is set to 'RSA'. The 'Minimum key size' is set to '2048'. There are two radio button options: 'Requests can use any provider available on the subject's computer' (which is selected) and 'Requests must use one of the following providers:'. Below this, there is a list of providers: 'Microsoft Software Key Storage Provider', 'Microsoft Platform Crypto Provider', and 'Microsoft Smart Card Key Storage Provider', all of which are unchecked. At the bottom, the 'Request hash' dropdown is set to 'SHA1' and the 'Use alternate signature format' checkbox is unchecked. The 'Cancel' button is highlighted with a red box.

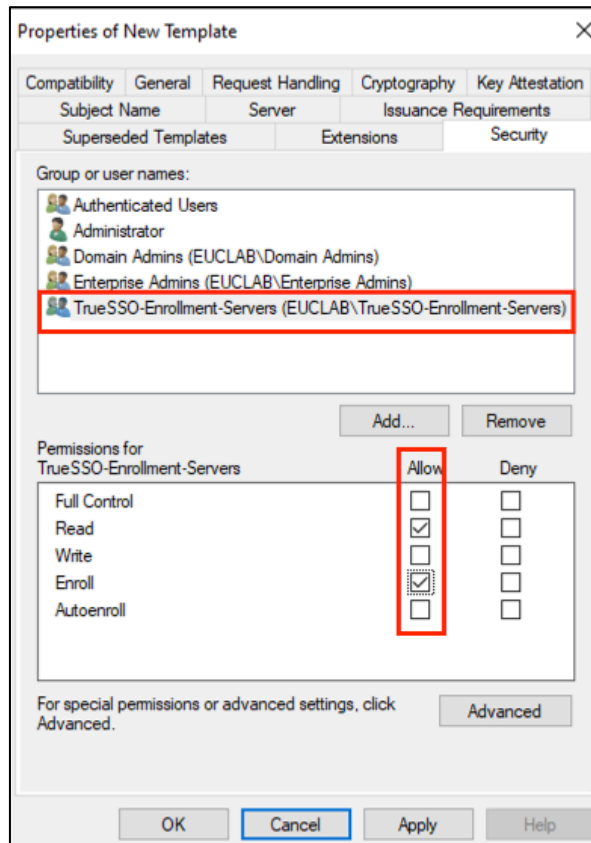
○ **Server**



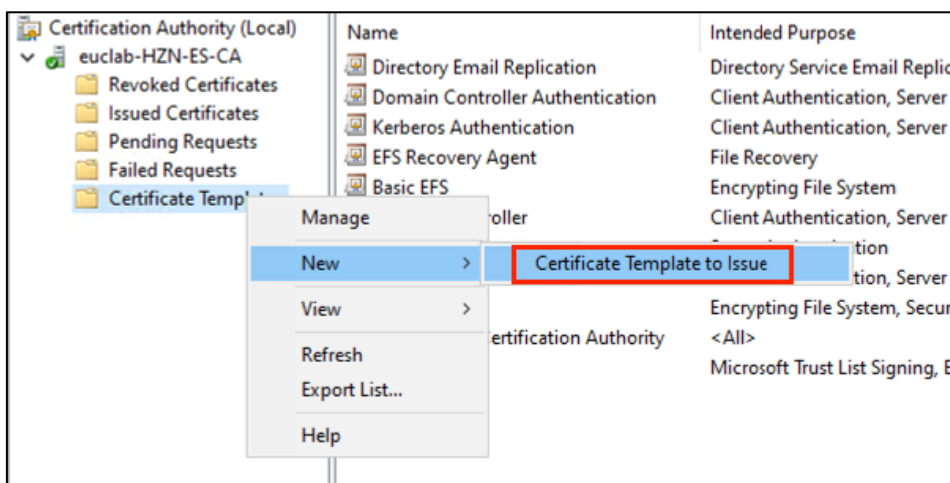
○ **Issuance Requirements**



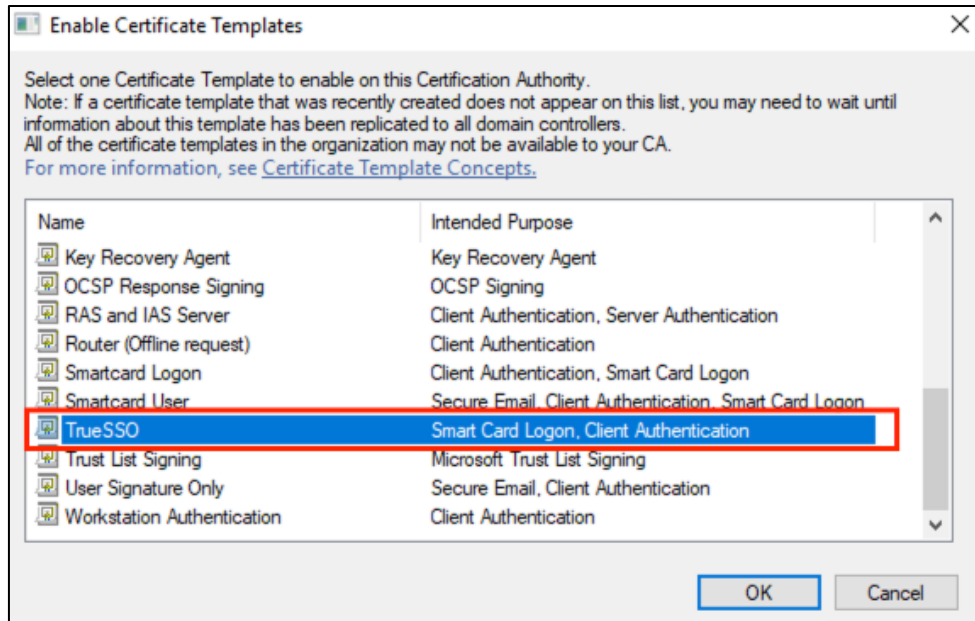
- **Security** – add the security group for the enrollment servers you created before, or select every enrollment server alternatively



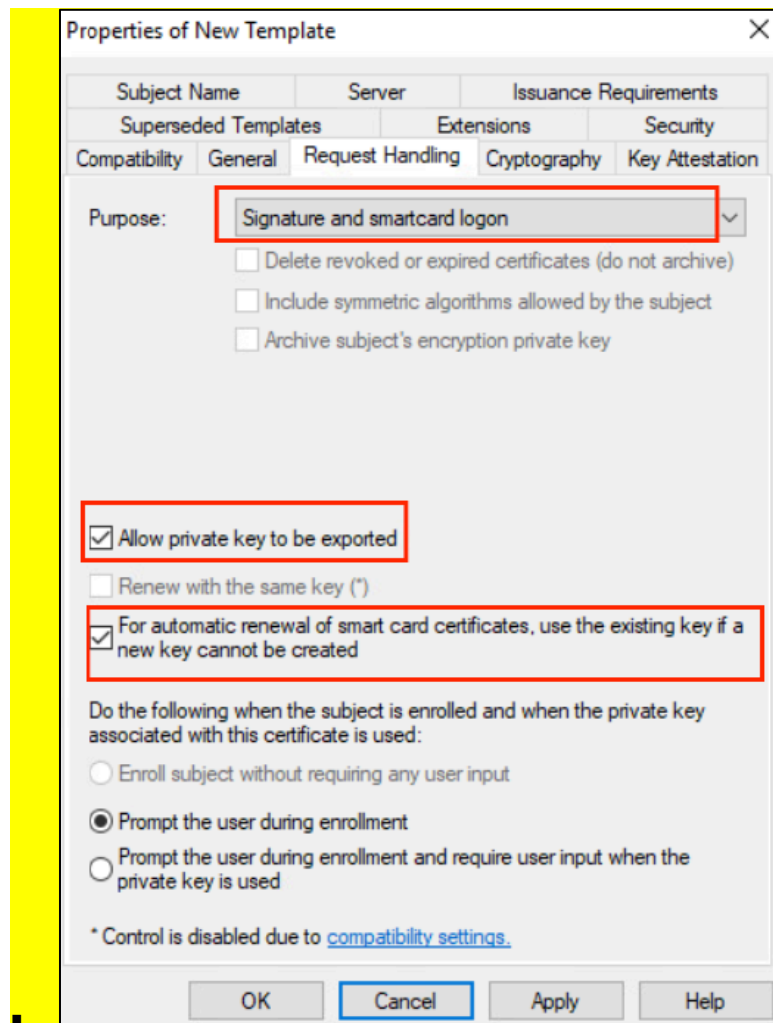
- Submit with →OK
- Close the Certificate Template Console
- Right-click to →Certificate Templates →New →Certificate Template to Issue – this step has to be done on every (Sub-)CA, which is involved to issue user certificates on the template created earlier.



- Select the TrueSSO Template created earlier



- 
- **Request Handling**
  - Purpose: Signature and smartcard logon
  - Set checkbox "Allow private key to be exported"
  - Set checkbox "For automatic renewal of smartcard certificates [...]"



- o **Cryptography**

- Provider Category: Key Storage Provider
- Algorithm name: RSA
- Minimum key size: 2048
- Request hash: SHA256

Properties of New Template

Subject Name    Server    Issuance Requirements

Superseded Templates    Extensions    Security

Compatibility    General    Request Handling    Cryptography    Key Attestation

Provider Category: Key Storage Provider

Algorithm name: RSA

Minimum key size: 2048

Choose which cryptographic providers can be used for requests

Requests can use any provider available on the subject's computer

Requests must use one of the following providers:

Providers:

Microsoft Software Key Storage Provider

Request hash: SHA256

Use alternate signature format

OK    Cancel    Apply    Help

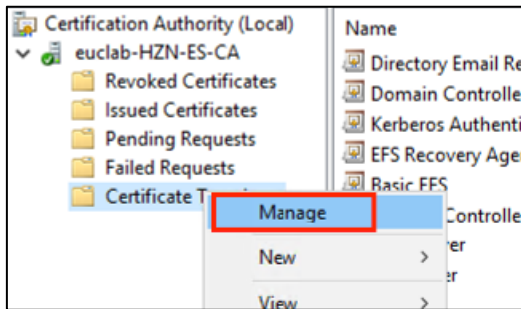
- Certificate Template Console schließen.

- Im Kontext-Menü →Certificate Templates auf →Certificate Template to issue gehen und "True SSO" auswählen.

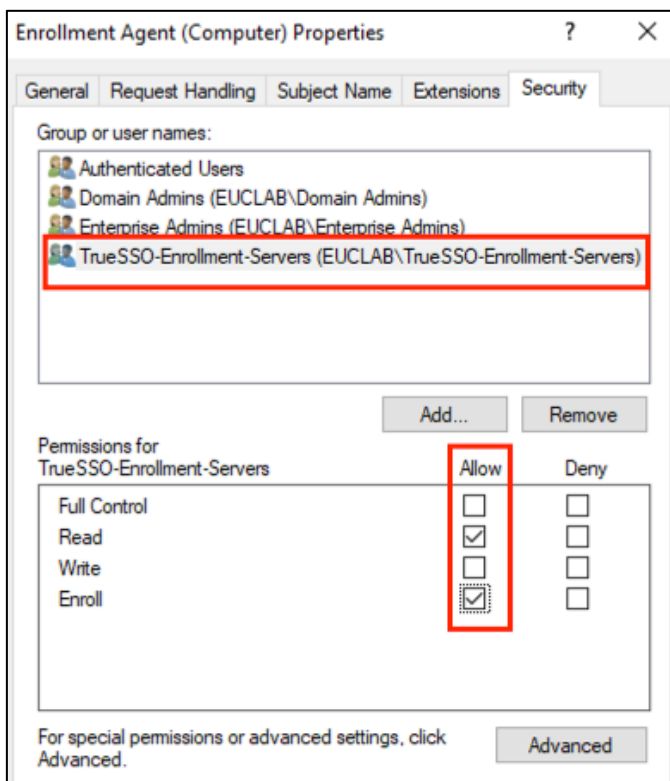
### 5.3.1 Create Certificate Template for Enrollment Server

You have to configure the Enrollment Agent Computer on the machine you are using for the CA. This step is required for all certificate authorities that issue certificates based on this template.

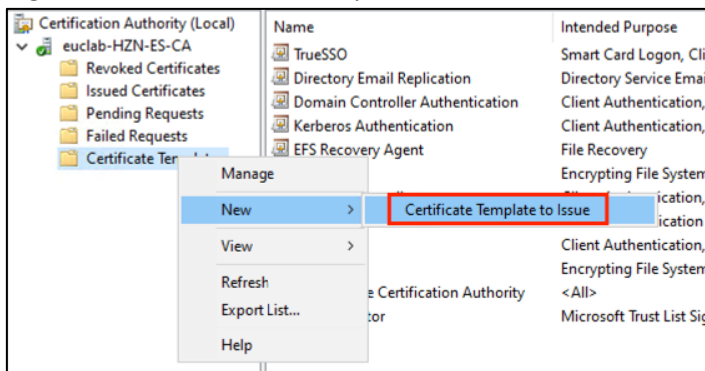
- On the server with (Sub-CA) installed, start CA snapin, and right-click →Certificate Templates, then select →Manage



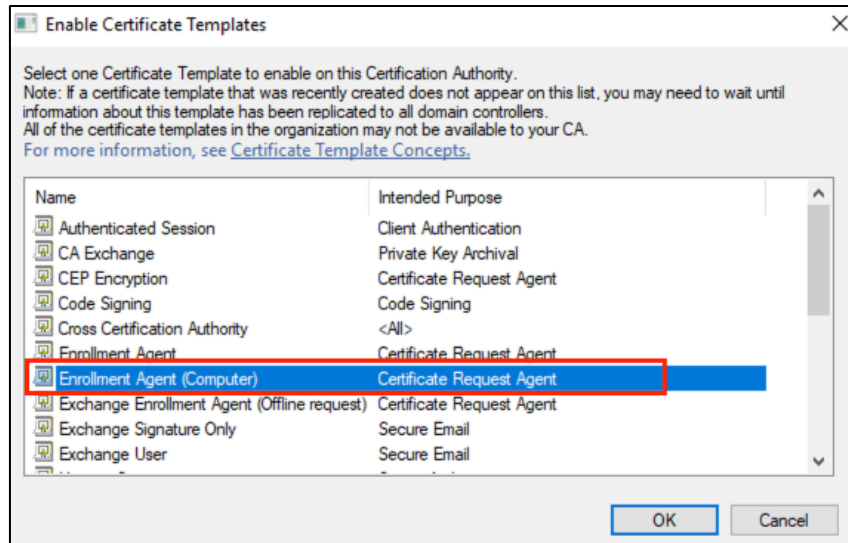
- Select the Template “Enrollment Agent (Computer) and go to →Properties
- In the →Security Tab, add the (previously created) security group for the Enrollment servers (alternatively every single Enrollment server), and add permission to Read and Enroll. Click →OK.



- Close Certificate Template Console
- Right-click on Certificate Template →New →Certificate Template to Issue



- Select “Enrollment Agent (Computer)” and click OK.



## 5.4 Install and set up Enrollment Server

The enrollment server enables a “pure” TrueSSO and supports external logins to Horizon with options apart from the classic one (domain AD username and password). The enrollment server requests short-lived certificates on behalf of the users you specify. These short-term certificates are the mechanism True SSO uses for authentication to avoid prompting users for Active Directory credentials.

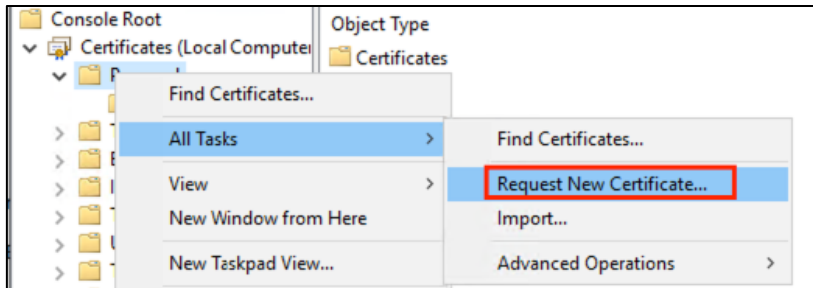
- Requirements
  - Prepared Windows Server OS
  - No other Horizon role installed (like connection server, agent etc.)
  - Domain-joined, static IPv4-address

### 5.4.1 Enrollment Agent (Computer) Certificate

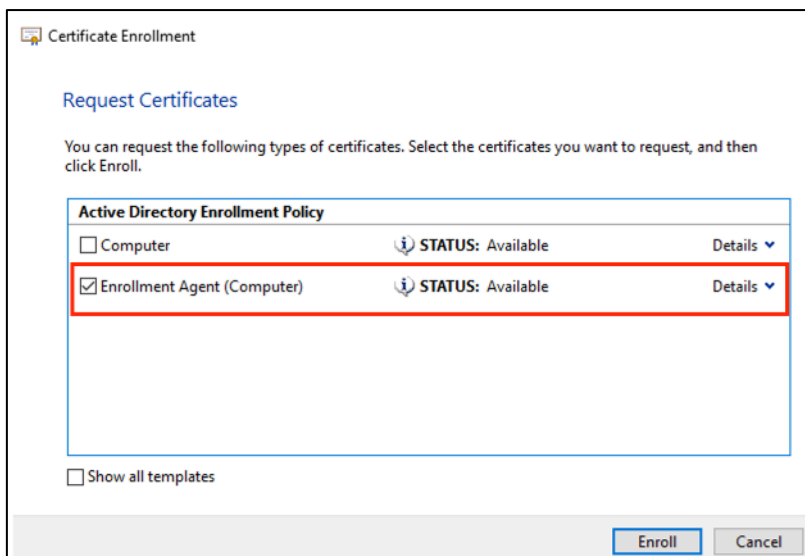
On the enrollment server you need the “Enrollment Agent (Computer)” certificate to authorize the enrollment server to generate certificates on behalf of users.

- Start MMC and add the snap-in “Certificates”, select Computer account

- Right-click the →Personal-folder, and go to →All Tasks →Request New Certificate



- In the →Request Certificates dialog, select the →Enrollment Agent (Computer), and click →Enroll.

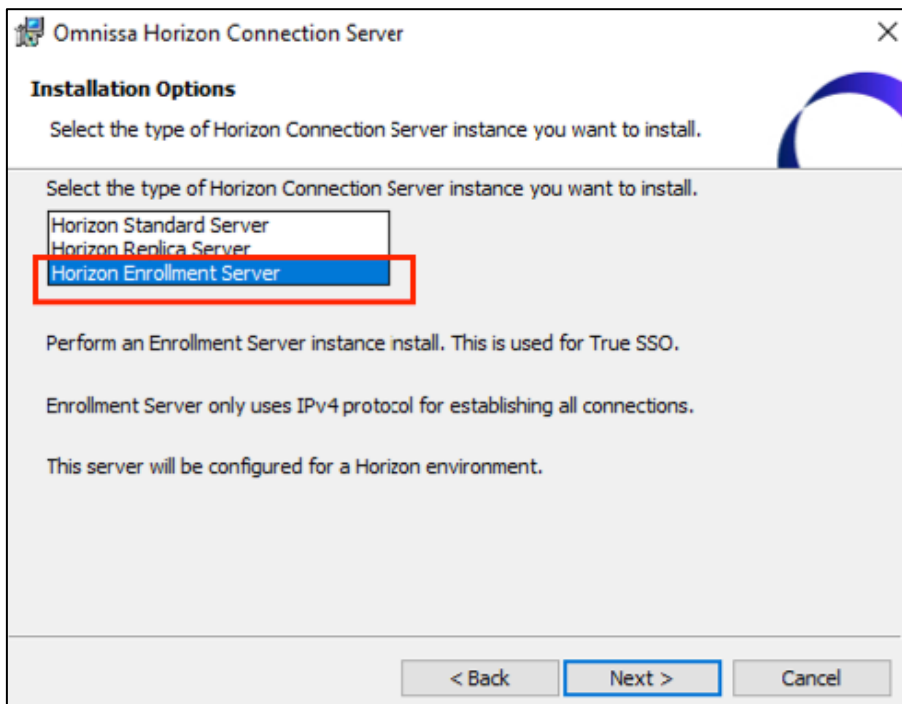


- You can close the MMC now.

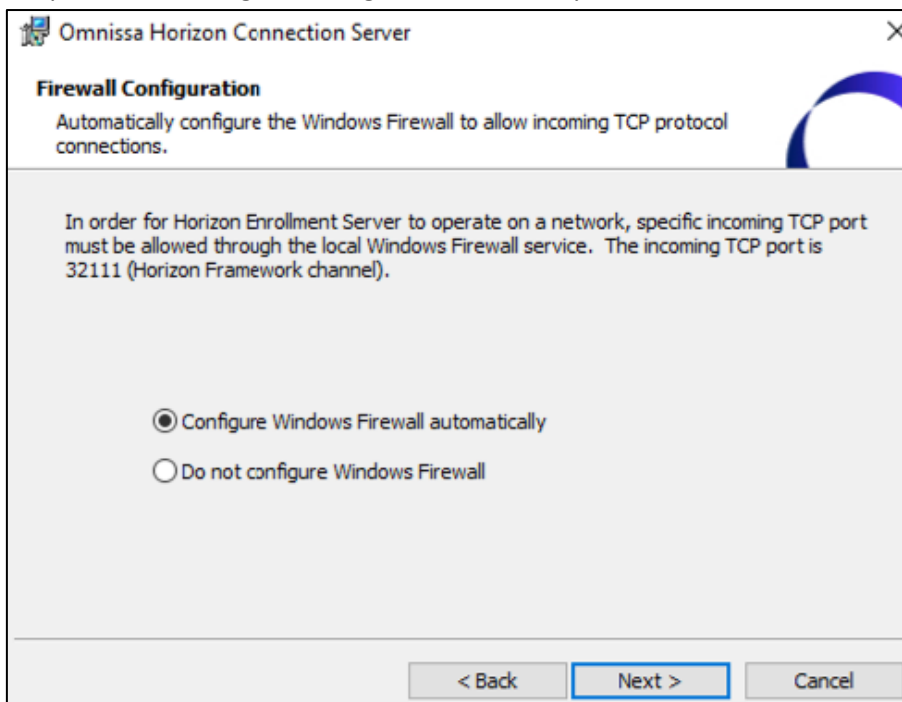
## 5.4.2 Setup Enrollment Server

Version 2503.1

- Execute the installer, and click →Next until you are asked for the Installation Options. Select „Horizon Enrollment Server“, and click →Next:



- Keep Firewall settings to configure automatically, and click →Next, then →Install:



- After finishing setup, reboot the server.

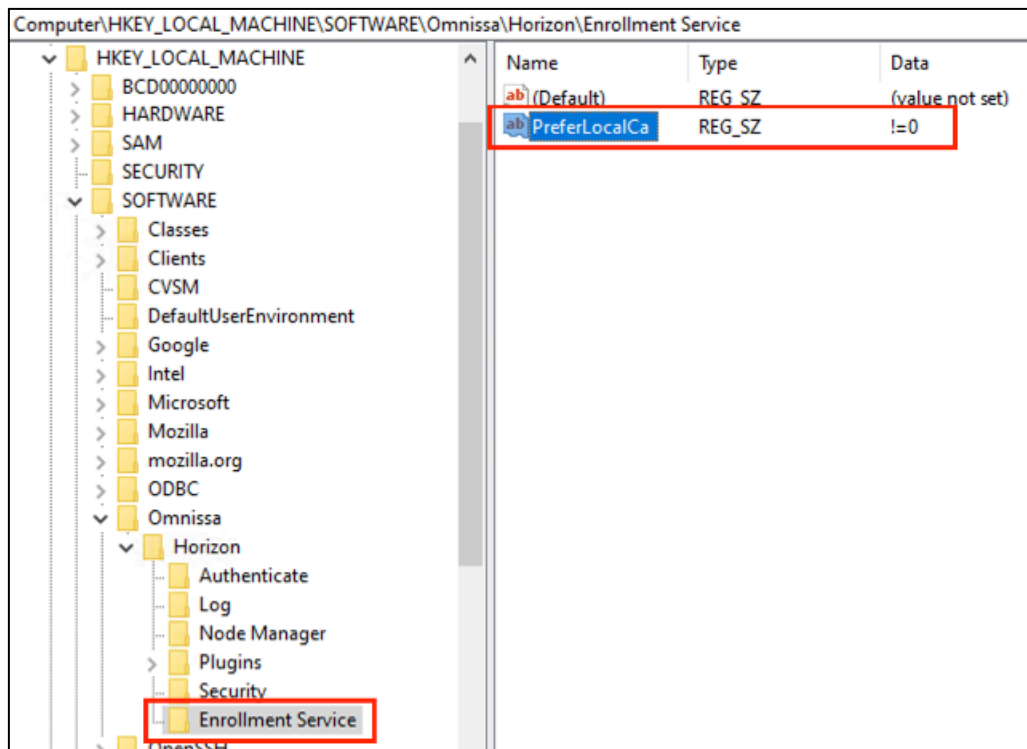
If you installed the enrollment server on the same machine that hosts an enterprise CA, configure the enrollment server to prefer using the local CA (see next sub-chapter). Optionally, if you install and set up more than one enrollment server, configure connection servers to enable load balancing between

the enrollment servers (see sub-chapter after next one).

### 5.4.3 Configure Enrollment Server to prefer local CA

Reference – [URL](#)

- On the enrollment server create the following registry key:  
HKLM\SOFTWARE\Omnissa\Horizon\Enrollment Service
- Add the following key from type “REG\_SZ”: PreferLocalCA
- Enter this value for value TRUE, so the enrollment server will send request to the local CA preferred – only in case it fails, the server will send these to alternate CAs: !=0



### 5.4.4 Configure Connection Servers to enable LB between Enrollment Servers

Reference – [URL](#)

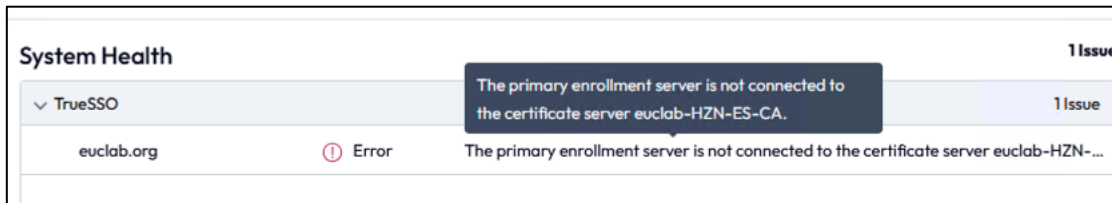
- On one Connection Server, start the ADSI Edit tool

- Expand OU=Properties, select OU=Global, and double-click CN=Common
- Edit the value **pae-NameValuePair**, and add the following value:
  - `cs-view-certssso-enable-es-loadbalance=true`

- Submit with →OK.

## 5.4.5 TrueSSO – Enrollment Server unable to connect to CA

When Enrollment Server and CA are co-hosted on a single VM, you can experience an issue with TrueSSO and Enrollment Server not being able to connect to Certificate Authority, like this<sup>2</sup>:



This is as expected, and we have to force the Enrollment Server service to use NTLM when authenticating to the CA service by adding those registry values:

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Omnissa\Horizon\Enrollment Service\UseNTLMAuthenticationToCa => TRUE
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Omnissa\Horizon\Enrollment Service\UseKerberosAuthenticationToCa => FALSE

Name	Type	Data
(Default)	REG_SZ	(value not set)
PreferLocalCa	REG_SZ	1=0
UseNTLMAuthenticationToCa	REG_SZ	True
UseKerberosAuthenticationToCa	REG_SZ	False

## 5.4.6 Validate TrueSSO with Diagnostic Tool

There is a tool called “TrueSSO ES Diagnostic Tool”, you can use to verify that TrueSSO is working as expected and configured. The tool is command-line-based, and can be downloaded [here](#).

- Execute with /ListEnvironment:

```
C:\INSTALL\TrueSSO ES Diagnostic Tool>es_diag.exe /ListEnvironment
Execute EnrollmentDiags::ListEnvironment:
Connect to the Enrollment Service: localhost
Successfully connected to the Enrollment Server
=====
ES Computer Name   : HZN-ES.euclab.org
ES ApiVersion     : 1.0
-----
Domain
Domain Name       : euclab.org
Forest Name       : euclab.org
Domain State      : Ready
-----
1 Domains
-----
Forest
Forest Name       : euclab.org
Directory State   : OK
TimeSince Last Sync: 3 sec
Enroll Cert Status : Valid
Cert Valid To     : 2027-11-12,09:12:26
```

<sup>2</sup> <https://kb.omnissa.com/s/article/90682>

- Verify that certificates can be requested successfully:

```
C:\INSTALL\TrueSSO ES Diagnostic Tool>es_diag.exe /enrollmenttest /domain:euclab.org /requester:euclab\administrator /template:TrueSSO /caserver:euclab-HZN-ES-CA
Execute EnrollmentDiags::EnrollmentTest:
Connect to the Enrollment Service: localhost
Successfully connected to the Enrollment Server
Configure the enrollment service for the selected domain
Wait up to 30 seconds for the Active Directory to be read
Send Cert-Request(s) to the enrollment service:
Successfully requested a Certificate

Requested : 1, Issued: 1, Failed: 0, Retry: 0
Total Time: 0.285 sec to generate 1 certificates.
Throughput: 3 certificates/second.
Average : 0.285 sec to generate a certificate.

Subject : Administrator
UPN : administrator@euclab.org
SerialNo : 44:00:00:00:0A:95:7B:71:17:1D:F0:B5:87:00:00:00:00:00:0A
UTC Time : 2025-11-13,12:26:33
Valid From: 2025-11-13,12:16:33
Valid To : 2025-11-13,22:16:33
Validity : Certificate is valid

C:\INSTALL\TrueSSO ES Diagnostic Tool>
```

## 5.5 Pair Connection und Enrollment Server

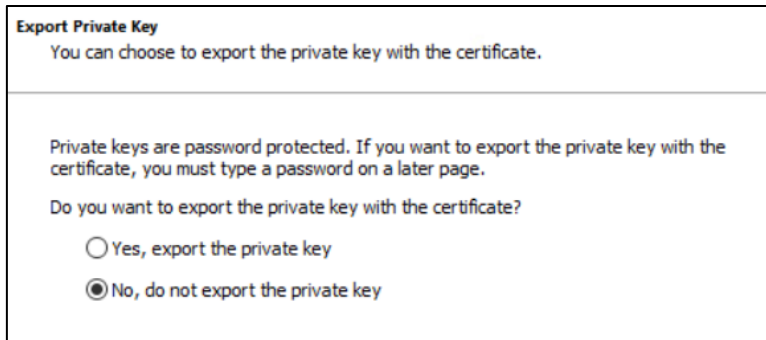
To enable trust between Enrollment Server and Connection Server, you need to export the Ommissa Horizon Certificate from the Connection Servers. The certificate is replicated between all Connection Servers through Horizon LDAP already, so we need to export this from one connection server only. The exported certificate is called a client certificate, because the connection server is a client of the Enrollment Service provided by the enrollment server.

### 5.5.1 Export the Enrollment Service Client Certificate

- On one of the the connection server, start the MMC and add the snap-in “Certificates” (Computer account)
- On the left, go to →Ommissa Horizon Certificates →Certificates, and select on the right the certificate with the friendly name “vdm.ec”

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
broker/hzn-cs01	broker/hzn-cs01	09/07/2026	<All>	ConnectionBroker
broker/hzn-cs01	broker/hzn-cs01	10/01/2026	<All>	ConnectionBroker
fa030a2d-a25c-4d35-b938-ccb1...	fa030a2d-a25c-4d35-b938-ccb142...	12/11/2025	<All>	vdm.enc
fa030a2d-a25c-4d35-b938-ccb1...	fa030a2d-a25c-4d35-b938-ccb142...	12/11/2025	<All>	vdm.enc
fa030a2d-a25c-4d35-b938-ccb1...	fa030a2d-a25c-4d35-b938-ccb142...	19/03/2034	<All>	vdm.ec
PodEndpoint/4c3f48c1-dc79-42...	PodEndpoint/4c3f48c1-dc79-4251...	25/11/2025	<All>	PodEndpoint
PodEndpoint/4c3f48c1-dc79-42...	PodEndpoint/4c3f48c1-dc79-4251...	18/11/2025	<All>	PodEndpoint
router/hzn-cs01	router/hzn-cs01	10/01/2026	<All>	MQRouter
router/hzn-cs01	router/hzn-cs01	09/07/2026	<All>	MQRouter
tunnel/hzn-cs01	tunnel/hzn-cs01	09/07/2026	<All>	Tunnel
tunnel/hzn-cs01	tunnel/hzn-cs01	10/01/2026	<All>	Tunnel

- Export this certificate



**Export Private Key**  
You can choose to export the private key with the certificate.

---

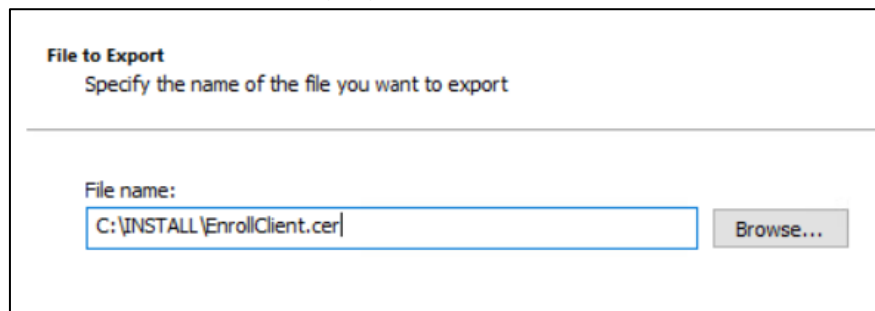
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

Yes, export the private key

No, do not export the private key

- Name it "EnrollClient.cer" (i.e.):



**File to Export**  
Specify the name of the file you want to export

---

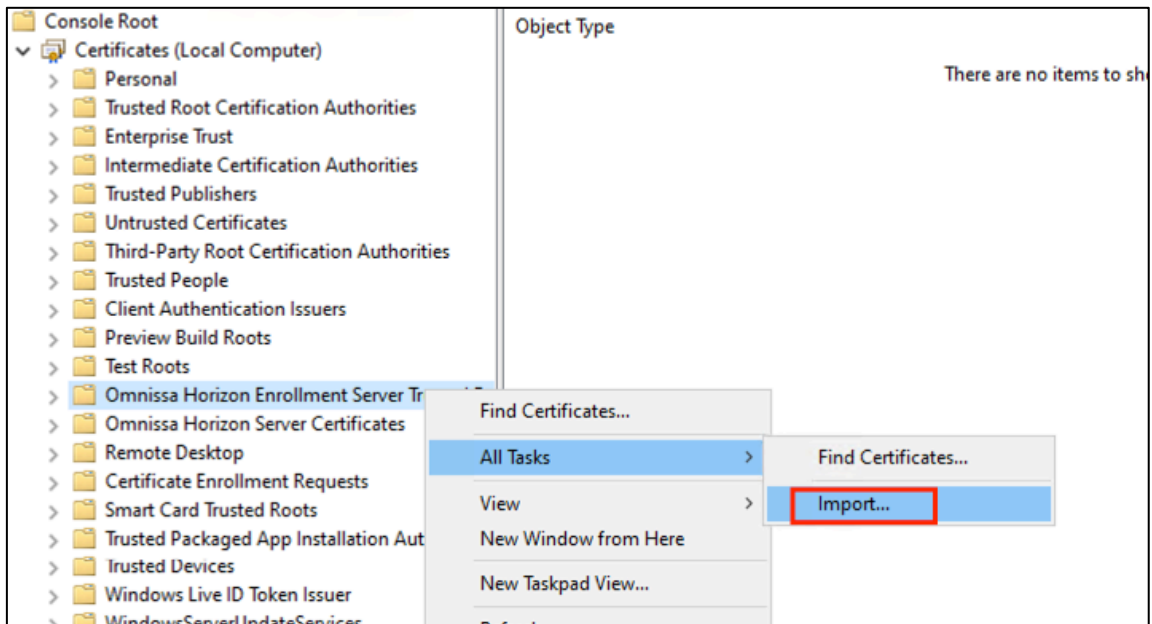
File name:

C:\INSTALL\EnrollClient.cer

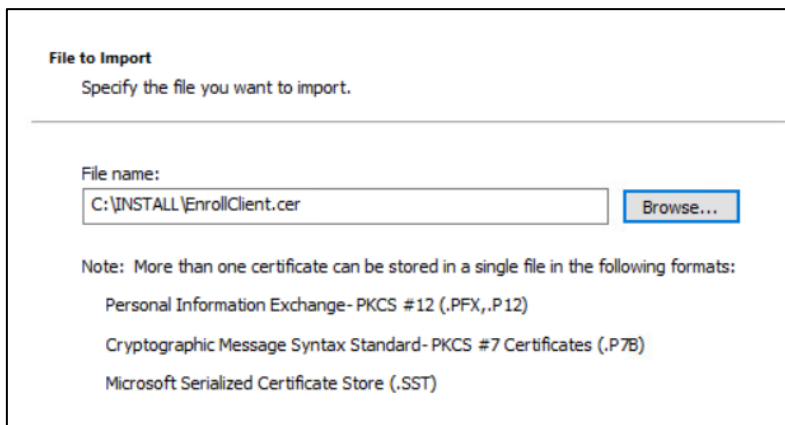
- Copy the cer file to the Enrollment Server.

## 5.5.2 Import the Enrollment Service Client Certificate on the Enrollment Server

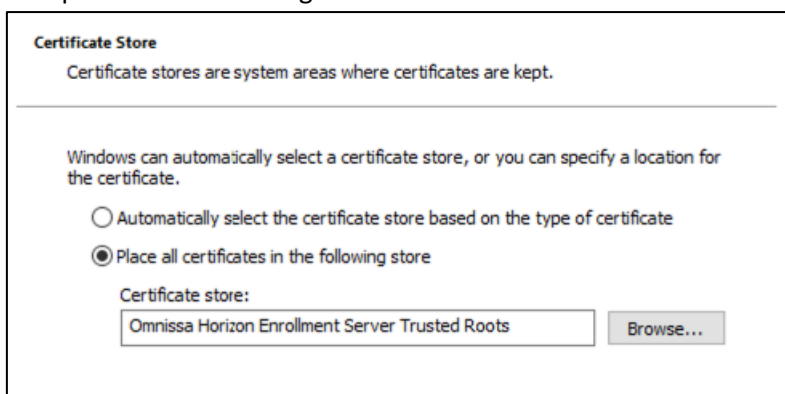
- Start MMC on the Enrollment Server
- On the left, right-click to →Omnissa Horizon Enrollment Server Trusted Roots →All Tasks →Import




- Select the previously copied cer file:



- Accept the default settings and click →Finish:



- After successful import, change the friendly name to “vdm.ec” (not mandatory, but recommended):

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
 e1b2f2f7-0302-4c9a-bc3e-0314...	e1b2f2f7-0302-4c9a-bc3e-031432...	23.02.2032	<All>	vdm.ec

## 5.6 Configure SAML Authentication to work with TrueSSO

With the True SSO feature, users can log in to Omnissa Workspace ONE Access using smart card, RADIUS, or RSA SecurID authentication, and they will no longer be prompted for Active Directory credentials, even when they launch a remote desktop or application for the first time.

- Verify that SSO is enabled in Horizon Console under →Settings →Global Settings
- Verify that Omnissa Access is installed and configured.
- Verify that the root certificate for the signing CA for the SAML server certificate is installed on the connection server host.
- Configure the SAML Authenticator in Horizon, following the guidance from this chapter: [Configure SAML Authentication in Horizon for Omnissa Access Integration](#)
  - Enable TrueSSO Trigger Mode in the SAML Authenticator

If you need to extend the expiration period of the Connection Server metadata so that remote sessions are not terminated after only 24 hours, you can follow this [URL](#).

## 5.7 Configure Horizon Connection Server for TrueSSO

This procedure is required to be performed on only one connection server in a POD to enable or disable TrueSSO.

- Execute cmd as administrator
- Add enrollment server to the global list
  - vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --truesso --environment --add --enrollmentServer enroll-server-fqdn
  - vdmUtil --authAs administrator --authDomain euclab.org --authPassword ##### --truesso --environment --add --enrollmentServer HZN-ES.euclab.org

```
C:\Users\administrator>vdmUtil --authAs administrator --authDomain euclab.org --authPassword ██████████
--truesso --environment --add --enrollmentServer HZN-ES.euclab.org
Enrollment server(s) added to the environment
C:\Users\administrator>
```

- Verify the correct listing of the enrollment server

- o vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --truesso --environment --list --enrollmentServer enroll-server-fqdn --domain domain-fqdn
- o vdmUtil --authAs administrator --authDomain euclab.org --authPassword ##### --truesso --environment --list --enrollmentServer HZN-ES.euclab.org --domain euclab.org

```
C:\Users\administrator>vdmUtil --authAs administrator --authDomain euclab.org --authPassword [REDACTED]
--truesso --environment --list --enrollmentServer HZN-ES.euclab.org --domain euclab.org
True SSO environment info
Enrollment server: hzn-es.euclab.org
Domain: euclab.org
Forest:
  Name: euclab.org
  Enrollment CertState: VALID
  Template(s):
    Name: TrueSSO
    Minimum key length: 2048
    Hash algorithm: SHA1
  Certificate Authority(s):
    Name: euclab-DC-CA
    Name: euclab-HZN-ES-CA
C:\Users\administrator>
```

- Create a TrueSSO connector and enable the connector

- o vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --truesso --create --connector --domain domain-fqdn --template TrueSSO-template-name --primaryEnrollmentServer enroll-server-fqdn --certificateServer ca-common-name --mode enabled
  - *TrueSSO-template-name* is the name of the template shown in the output for the previous command, and *ca-common-name* is the common name of the enterprise certificate authority shown in that output.
- o vdmUtil --authAs administrator --authDomain euclab.org --authPassword ##### --truesso --create --connector --domain euclab.org --template TrueSSO --primaryEnrollmentServer HZN-ES.euclab.org --certificateServer euclab-HZN-ES-CA --mode enabled

```
C:\Users\administrator>vdmUtil --authAs administrator --authDomain euclab.org --authPassword [REDACTED]
--truesso --create --connector --domain euclab.org --template TrueSSO --primaryEnrollmentServer HZN-ES
.euclab.org --certificateServer euclab-HZN-ES-CA --mode enabled
Connector created
Domain: euclab.org
Mode: ENABLED
C:\Users\administrator>
```

- Discover which SAML authenticators are available – these are configured previously in Horizon Console

- o vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --truesso --list --authenticator
- o vdmUtil --authAs administrator --authDomain euclab.org --authPassword ##### --truesso --list --authenticator

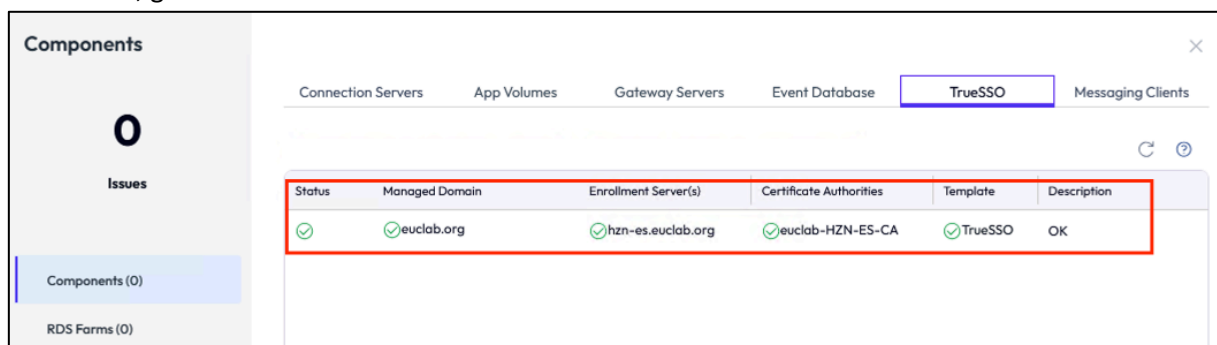
```
C:\Users\administrator>vdmUtil --authAs administrator --authDomain euclab.org --authPassword [REDACTED]
--truesso --list --authenticator
Authenticator(s) found: 2
Name: SAML EUCLAB
True SSO mode: ENABLE_IF_NO_PASSWORD
Name: MS Entra ID
True SSO mode: DISABLED
C:\Users\administrator>
```

- Enable the authenticator to use TrueSSO mode
  - vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --truesso --authenticator --edit --name authenticator-fqdn --truessoMode {ENABLED|ALWAYS}
    - For --truessoMode, use ENABLED if you want True SSO to be used only if no password was supplied when the user logged in to Ommissa Access. In this case if a password was used and cached, the system will use the password. Set --truessoMode to ALWAYS if you want True SSO to be used even if a password was supplied when the user logged in to Ommissa Access.
  - vdmUtil --authAs administrator --authDomain euclab.org --authPassword ##### --truesso --authenticator --edit --name "SAML EUCLAB" --truessoMode ALWAYS

```
C:\Users\administrator>vdmUtil --authAs administrator --authDomain euclab.org --authPassword [REDACTED]
--truesso --authenticator --edit --name "SAML EUCLAB" --truessoMode ALWAYS
Authenticator updated
Name: SAML EUCLAB
True SSO mode: ENABLE ALWAYS
C:\Users\administrator>
```

The True SSO connector is enabled on a pool or cluster for the domain specified. To disable True SSO at the pool level, run `vdmUtil --certsso --edit --connector <domain> --mode disabled`. To disable true SSO for an individual virtual machine, you can use GPO (`vdm_agent.adm`).

Finally, you should see that TrueSSO is implemented, by viewing the Horizon System Health Dashboard, go to →View and validate the status of TrueSSO:

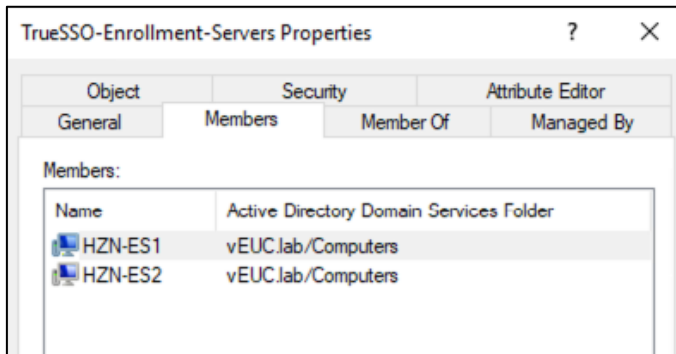


## 5.8 Setup additional Enrollment Server and enable HA

You can add a second Enrollment Server for configuring HA and load distribution.

Preparation on the CA:

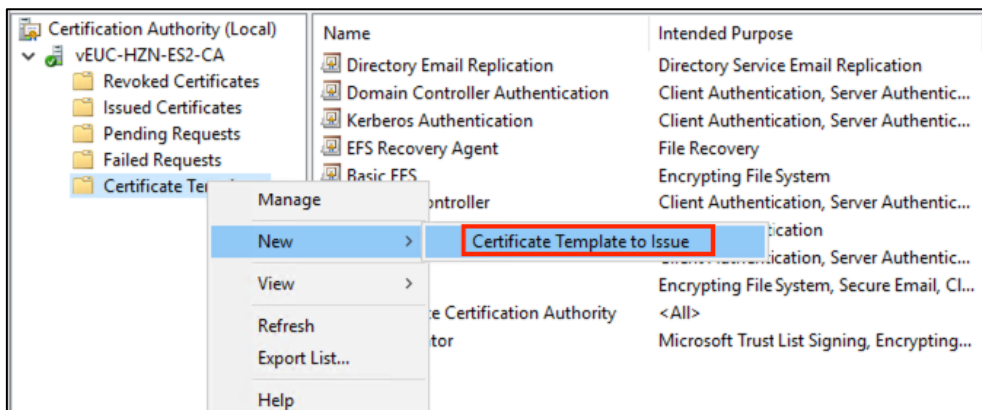
- Add the newly prepared Windows Server to the Security Group, as created in [before](#).



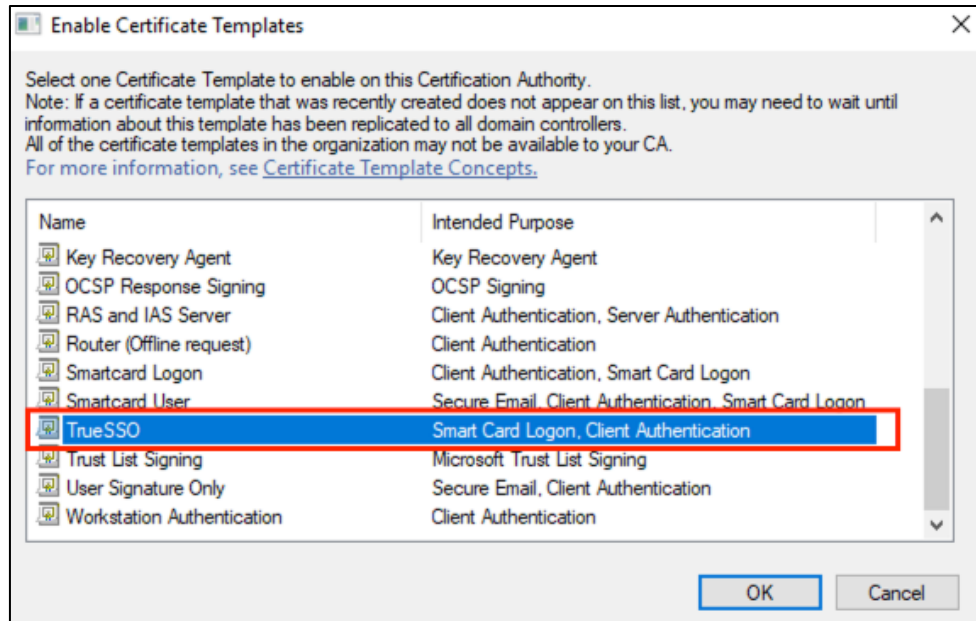
- You can use an existing (Sub-)CA, or create a dedicate one, co-installed, as described [here](#).

On the new designated Enrollment Server with co-installed CA:

- The certificate template for TrueSSO already exists, but we need to issue this template for a new Enrollment Server

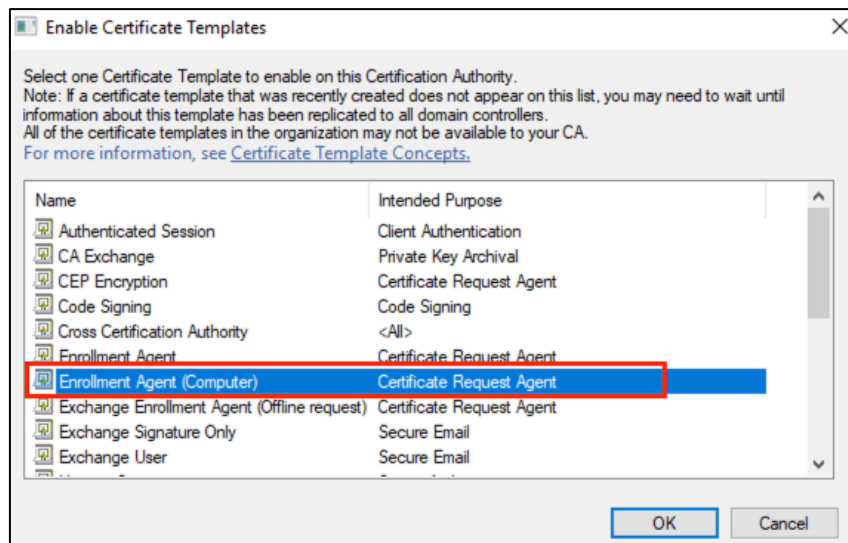


- Select TrueSSO template



- Further, we need to issue a new certificate template for the Enrollment Agent (Computer)

- Select Enrollment Agent (Computer)



- You need to request the “Enrollment Agent (Computer)” certificate to authorize the enrollment server to generate certificates on behalf of users, as described in [here](#).
- Setup **Enrollment Server**, as described in [here](#).
  - Be aware about using local CA and load balancing for the Connection Servers.
- Start the pairing process between Connection Server and the newly installed Enrollment Server, as described in [here](#).
- Configure the Connection Server for TrueSSO with the newly installed Enrollment Server, similar as described in [here](#).

- Add the new Enrollment Server to the global list:

```
vdmUtil --authAs administrator --authDomain vEUC.lab --
authPassword ##### --truesso --environment --add --
enrollmentServer HZN-ES2.vEUC.lab
```

```
C:\Users\administrator.VEUC>vdmUtil --authAs administrator --authDomain vEUC.lab --authPassword [REDACTED] --truesso --envir
onment --add --enrollmentServer HZN-ES2.vEUC.lab
Enrollment server(s) added to the environment
```

- Verify the correct listing of the new Enrollment Server:

```
vdmUtil --authAs administrator --authDomain vEUC.lab --
authPassword ##### --truesso --environment --list --
enrollmentServer HZN-ES2.vEUC.lab --domain vEUC.lab
```

```
C:\Users\administrator.VEUC>vdmUtil --authAs administrator --authDomain vEUC.lab --authPassword [REDACTED] --truesso --envir
onment --list --enrollmentServer HZN-ES2.vEUC.lab --domain vEUC.lab
True SSO environment info
Enrollment server: hzn-es2.veuc.lab
Domain: veuc.lab
Forest:
  Name: vEUC.lab
  Enrollment CertState: NOT_VALID
  Template(s):
    Name: TrueSSO
    Minimum key length: 2048
    Hash algorithm: SHA1
  Certificate Authority(s):
    Name: vEUC-HZN-ES1-CA
    Name: vEUC-HZN-ES2-CA
    Name: vEUC-VEUC-DC-CA
C:\Users\administrator.VEUC>
```

- Edit the existing connector:

```
vdmUtil --authAs administrator --authDomain vEUC.lab --
authPassword ##### --truesso --edit --connector --domain
vEUC.lab --template TrueSSO --secondaryEnrollmentServer HZN-
ES2.vEUC.lab --certificateServer vEUC-HZN-ES1-CA,vEUC-HZN-ES2-
CA --mode enabled
```

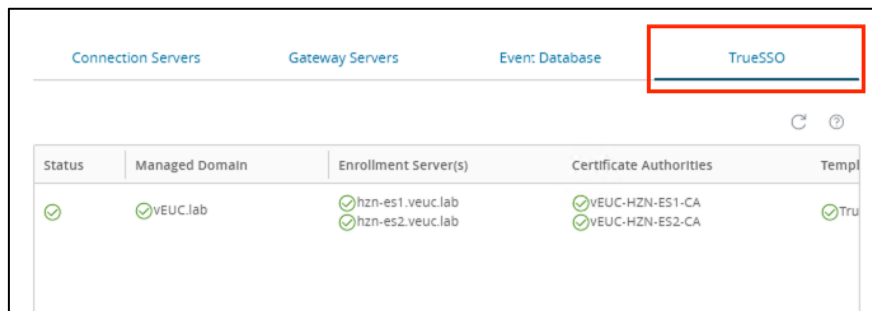
```
C:\Users\administrator.VEUC>vdmUtil --authAs administrator --authDomain vEUC.lab --authPassword [REDACTED] --truesso --edit
--connector --domain vEUC.lab --template TrueSSO --secondaryEnrollmentServer HZN-ES2.vEUC.lab --certificateServer vEUC-H
ZN-ES1-CA,vEUC-HZN-ES2-CA --mode enabled
Connector updated
Domain: vEUC.lab
Mode: ENABLED
C:\Users\administrator.VEUC>
```

- Check settings:

```
vdmUtil --authAs administrator --authDomain vEUC.lab --
authPassword ##### --truesso --list --connector --domain
vEUC.lab
```

```
C:\Users\administrator.VEUC>vdmUtil --authAs administrator --authDomain vEUC.lab --authPassword [REDACTED] --truesso --list
--connector --domain vEUC.lab
Connector found
Domain: vEUC.lab
Primary Enrollment Server: hzn-es1.veuc.lab
Secondary Enrollment Server: hzn-es2.veuc.lab
Template Name: TrueSSO
Mode: ENABLED
Certificate Authority Server(s):
  vEUC-HZN-ES1-CA
  vEUC-HZN-ES2-CA
C:\Users\administrator.VEUC>
```

- You should now see the newly added Enrollment Server and the CA in the dashboard of the Horizon Console:



- Enable load balancing for the Enrollment Servers, if not done already (see [here](#)).

## 5.9 Additional resources for TrueSSO

- VMware Horizon 7 True SSO: Setting Up In a Lab  
<https://blogs.vmware.com/euc/2016/04/true-ss0-setting-up-in-a-lab.html>
- VMware Horizon TrueSSO – Configuration for High Availability and Redundancy  
<https://askaresh.com/2018/04/13/vmware-horizon-truesso-configuration-for-high-availability-and-redundancy/>
- VMware Horizon True SSO with UAG SAML  
<https://www.carlstalhood.com/vmware-horizon-true-ss0-uag-saml/>
- VMware Horizon 7 True SSO: Advanced Features  
<https://blogs.vmware.com/euc/2017/02/horizon-7-ss0-advanced-features.html>
- VMware Horizon True SSO configuration  
<https://nolabnparty.com/en/vmware-horizon-true-ss0-configuration-pt-1/>  
<https://nolabnparty.com/en/vmware-horizon-true-ss0-configuration-pt-2/>
- Enabling and Troubleshooting Omnissa Horizon True SSO  
<https://darrylmiles.blog/2023/08/12/enabling-and-troubleshooting-vmware-horizon-true-ss0/>

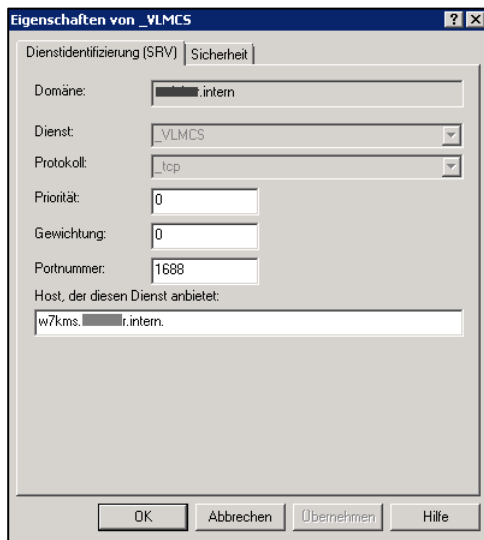
## 6. Key Management Server (KMS) einrichten

Je nach KMS-Kategorie wird der sog. KMS-Host auf einer Windows 7- bzw. auf einer Windows 2008 R2 Maschine eingerichtet. Die Kommunikation zwischen KMS-Host und KMS-Client findet später über TCP Port 1688 statt.

Für eine automatische Aktivierung der KMS-Clients müssen bei Windows 7 mind. 25 Systeme (virtuell/physisch) bzw. bei Windows 2008 R2 mind. 5 Systeme vorhanden sein.

- Installieren des KMS-Schlüssels auf dem KMS-Host per Konsole:  
`cscript c:\windows\system32\slmgr.vbs /ipk <KMS-Schlüssel>`

- Aktivieren des KMS-Schlüssels bei Microsoft  
`cscript c:\windows\system32\slmgr.vbs /ato`
- Im DNS sollte automatisch ein entsprechender Eintrag angelegt werden, zu prüfen mit dem Befehl  
`nslookup -type=srv _vlmcs._tcp.<Domäne>`

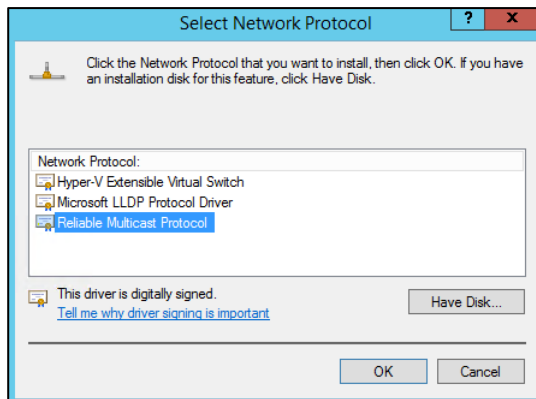


## 7. Netzwerklastenausgleich-Manager konfigurieren

Damit ein Anwender in seinem View-Client nicht beide Adressen (View Connection Server bzw. View Replica Server) vorhalten muss, eignet sich hierfür der MS-eigene Netzwerklastenausgleich. Somit muss der End-Anwender lediglich **eine** Adresse haben, um sich mit einem der Connection Server verbinden zu können.

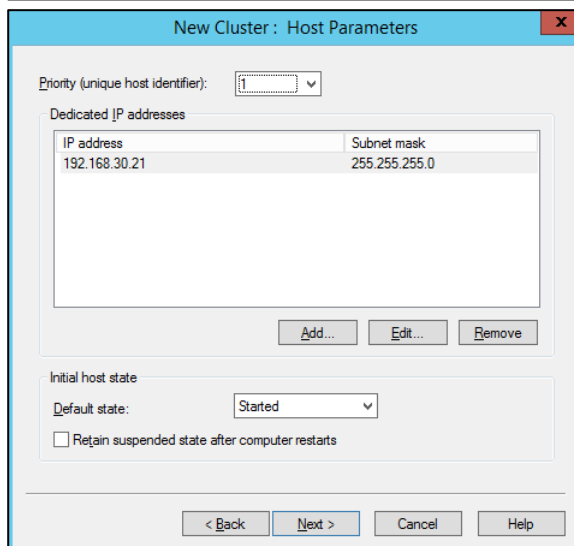
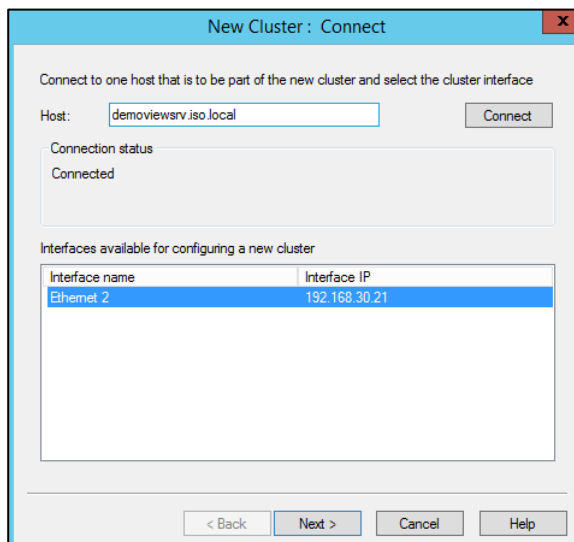
- Im AD wird ein neuer DNS-Eintrag „demoview.iso.local“ vorgenommen, dazu die IP-Adresse statisch hinterlegt.
  - Auf beiden Connection-Servern wird der MS-eigene Netzwerklastenausgleich-Manager konfiguriert (Feature NLB):  
Netzwerklastenausgleich-Cluster „demoview.iso.local“, bestehend aus
    - demoviewsrv.iso.local
    - demoviewreplica.iso.local
  - Somit kann sich der View-Client nun immer mit „demoview.iso.local“ verbinden, unabhängig davon, welcher View Connection Server gerade verfügbar ist.
  
  - Ausgangslage:
    - Ein View Connection Server: demoviewsrv.iso.local
    - Ein View Replica Server: demoviewreplica.iso.local
  
  - Einrichten eines neuen Host-Eintrags im DNS-Manager
    - demoview.iso.local
-

- In den LAN-Eigenschaften **beider** Connection Server das „Reliable Multicast-Protokoll“ installieren:



- Installieren des Netzwerklastenausgleich-Manager (NLB) über die →Verwaltung → Server-Manager, oder alternativ über „*servermanagercmd.exe –install nlb*“ auf beiden Connection Servern
- Auf einem der beiden Connection-Server einen Netzwerklastenausgleich-Cluster hinzufügen:

#### Eingabe des ersten Cluster-Knotens



## Eingabe der Cluster-IP-Adresse

The cluster IP addresses are shared by every member of the cluster for load balancing. The first IP address listed is considered the primary cluster IP address and used for cluster heartbeats.

Cluster IP addresses:

IP address	Subnet mask
192.168.30.20	255.255.255.0

Buttons: Add..., Edit..., Remove

Navigation: < Back, Next >, Cancel, Help

→ Als Clusterausführungsmodus „Multicast“ wählen (zwecks VMotion-Kompatibilität)

Cluster IP configuration

IP address: 192.168.30.20

Subnet mask: 255 . 255 . 255 . 0

Full Internet name: demoview.iso.local

Network address: 03-bf-c0-a8-1e-14

Cluster operation mode

Unicast

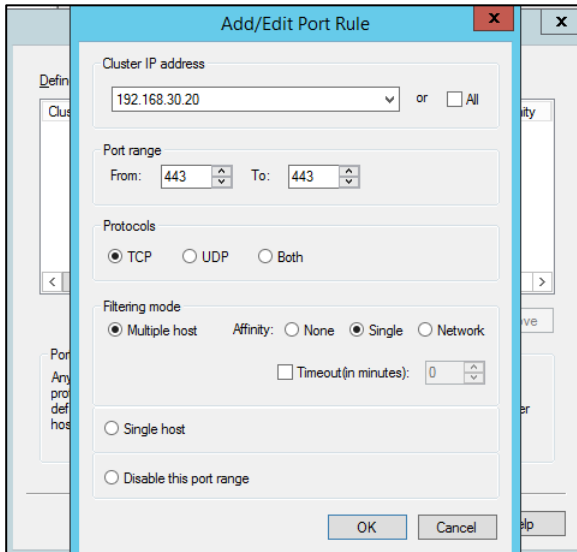
Multicast

IGMP multicast

Navigation: < Back, Next >, Cancel, Help

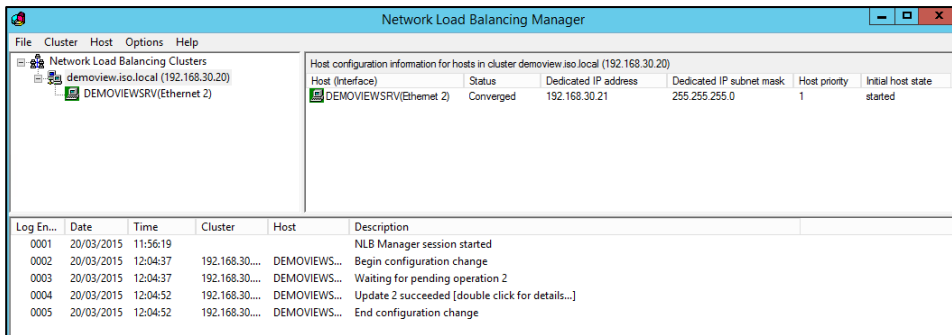
Entfernen der vorhandenen Standard-Portregel,

Hinzufügen einer Portregel, welche lediglich auf eingehenden TCP-Verkehr auf Port 443 hört

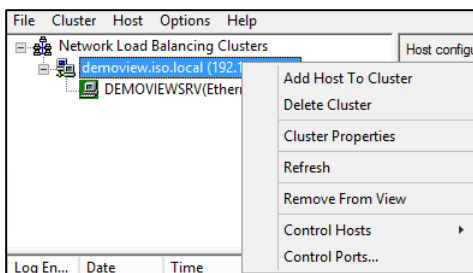


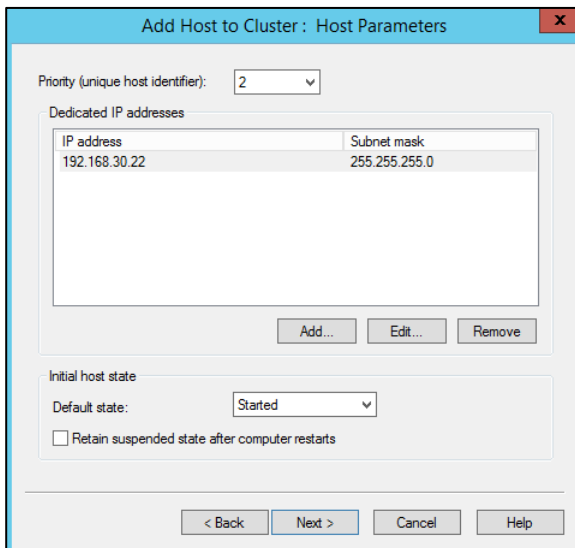
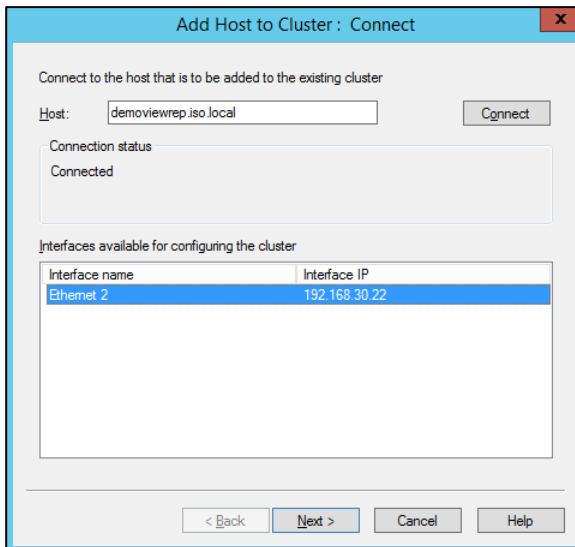
Vorgang abschließen.

- So sieht dann in etwa aus:



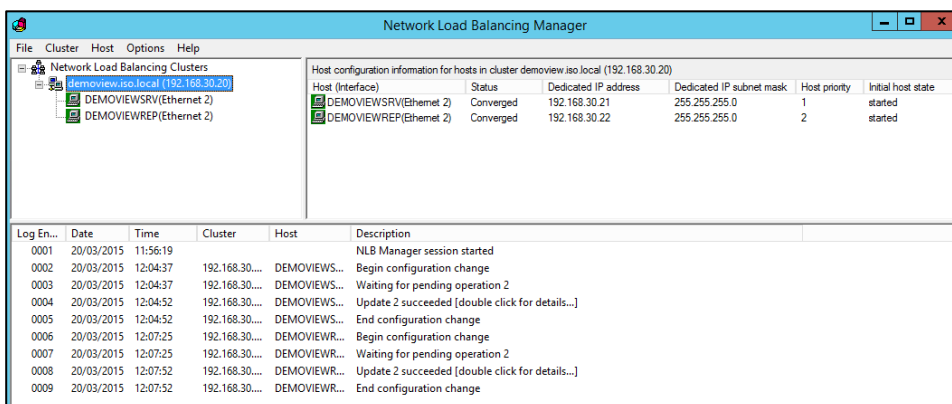
- Weiteren Host (view45replica.iso.local) zum Cluster hinzufügen (ggf. vom zweiten Host machen):





Vorgang abschließen.

- Nach kurzer Wartezeit sieht es dann so aus:



## 8. Einrichten eines Load Balancers

### 8.1 Einrichten eines Hercules Load Balancers (VMware Virtual Appliance)

Alternativ zum Netzwerklastenausgleich à la Microsoft kann auch eine Virtual Appliance namens Hercules zum Einsatz kommen. Diese verteilt eingehende Anfragen an die entsprechenden Connection bzw. Replica-Server.

- Importieren der entsprechenden ovf-Datei
- Start und Login in das Linux-System (User: root, Passwort: root)
- Editieren des LAN-Interfaces:

*vi /etc/network/interfaces*

```
192.168.143.150 - PuTTY
Configure Loopback
auto lo
iface lo inet loopback

# ethernet interface

auto eth0
iface eth0 inet static
address 192.168.143.150
network 192.168.143.0
netmask 255.255.255.0
broadcast 192.168.143.255
gateway 192.168.143.1
```

*Mit ZZ (YY) komme ich aus dem vi wieder heraus.*

- Eintragen der beiden Cluster-Knoten:

*vi /etc/init.d/pen*

```
192.168.143.150 - PuTTY
#!/bin/sh
#
# startup script for pen
# pchaganti@gmail.com

LOGFILE=/var/log/pen.log
PIDFILE=/var/run/pen.pid
CONTROLPORT=8888
CHROOTDIR=/chroot/pen
LBSERVER=192.168.143.150:https
SERVER1=192.168.143.151:https
SERVER2=192.168.143.152:https

case "$1" in
    start)
        if [ -x /bin/pen ] ; then
            echo -n "Starting pen: "
            /bin/pen -C $CONTROLPORT -X -l $LOGFILE -p $PIDFILE $LBSERVER $SERVER1 $SERVER2
            echo "OK"
        fi
        ;;
    stop)
        kill `cat /var/run/pen.pid`
        ;;
    *)
        echo "usage: $0 { start | stop }" >&2
        exit 1
        ;;
endcase
```

Es sind auch mehr als zwei Knoten (SERVER1 & SERVER2) denkbar.

- Neustart der VA – Fertig.

## 8.2 Einrichten eines PEN Load Balancers auf einem Ubuntu Linux

Wer die OpenSource Variante PEN lieber auf einem anderen Linux einrichten möchte, kann dieses zum Beispiel über Ubuntu machen.

- Einrichten einer Ubuntu-VM (hier mit Ubuntu 14.04.2 LTS)
- Konfigurieren einer statischen IP-Adresse
- Setup der VMware-Tools (siehe VMware KB-Artikel 1022525)
  - Mounten der VMware-CD an die VM
  - Extrahieren der VMwareToolsxxxx.tar.gz in einen Ordner
  - Zum Ordner vmware-tools-distrib navigieren und
  - `sudo ./vmware-install.pl -d` ausführen
  - Neustart der VM
- Download der aktuellen PEN-Version (<http://siag.nu/pub/pen/>) und in einen Ordner extrahieren
- `sudo apt-get install pen` ausführen
- Für den Autostart von PEN muss die Datei `/etc/rc.local` editiert werden:

```
# By default this script does nothing.
pen 443 192.168.30.21 192.168.30.22
exit 0
```

→ Hier wird Load Balancing über https mit den beiden IPs 192.168.30.21 und 192.168.30.22 konfiguriert.

- Nun ist die Konfiguration auch Neustart-resistent. Ggf. kontrollieren mit „`ps aux | grep pen`“.
- Bei Bedarf kann der pen service auch regelmäßig neu gestartet werden:
  - GNOME für die grafische Verwaltung installieren:  
`sudo apt-get install gnome`  
`sudo apt install gksu`
  - GNOME ausführen: `gksudo gnome-schedule`
  - Editieren der `/etc/crontab` – hier werden tabellarisch jene Befehle (systemweit) gespeichert, die zu bestimmten Uhrzeiten ausgeführt werden sollen.  
`sudo vi /etc/crontab`
  - Einrichten eines Mailversands postfix:  
`sudo apt-get install postfix`

## 8.3 Einrichten eines HAProxy auf einem Debian System

Der HAProxy ist ein TCP/HTTP Load Balancer und als freie Software unter [www.haproxy.org](http://www.haproxy.org) zum Download verfügbar. Diesen habe ich einmal auf einem Debian-System installiert. Dazu existiert eine dedizierte Anleitung.

## 9. Setup Location-Based Printing

### Voraussetzung

- VMware Integrated Printing Feature im Horizon Agent
- Setup entsprechender Druckertreiber in der Master-VM
- Translation Rules für jeden location-based Drucker
- <https://www.carlstalhood.com/category/vmware-horizon/vmware-horizon-8/> ?

<https://docs.vmware.com/en/VMware-Horizon/2106/horizon-remote-desktop-features/GUID-F599DFBC-1713-44C1-BDD8-F7F54FA58D51.html>

### Install LBP

- Download Horizon GPO Bundle
- installutil.exe C:\vmware-print-lbpsettingui.dll
  - InstallUtil.exe is usually in the Microsoft.NET directory, for example, C:\Windows\Microsoft.NET\Framework64\v4.0.30319
- GPO: →Computer Configuration →Software Settings →LBP UI

### Configure LBP

- The group policy setting is a name translation table that maps printers to remote desktops
- Translation Rules can base on
  - client system's IP address
  - client name
  - client MAC address
  - user's name
  - user's group
- You can specify one translation rule, or a combination of several translation rules, for a specific printer.

Oder per DEM:

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-horizon-view-virtual-printing-location-redirectation.pdf>

## 10. Setup VMware Unified Access Gateway

### 10.1 Requirements

Benötigte Ports von Draußen zur externen IP des UAGs:

- TCP and UDP 443 (includes Blast Extreme)
- TCP and UDP 4172. UDP 4172 must be opened in both directions. (PCoIP)
- TCP and UDP 8443 (for HTML Blast)

Benötigte Ports von der internen IP des UAGs nach Drinnen:

- TCP 443 to internal Connection Servers (through a load balancer)
- TCP and UDP 4172 (PCoIP) to all internal Horizon View Agents. UDP 4172 must be opened in both directions.
- TCP 32111 (USB Redirection) to all internal Horizon View Agents.
- TCP and UDP 22443 (Blast Extreme) to all internal Horizon View Agents.
- TCP 9427 (MMR and CDR) to all internal Horizon View Agents.

Benötigte Ports für die interne Kommunikation zwischen UAG und den Desktops:

- TCP 9443 (REST API)
- TCP 80/443 (Edge Gateway)

### 10.2 Deployment per PS-Script

- Prepare a Windows client computer with VMware OVF Tool (Download [URL](#))
  - `Set-ExecutionPolicy unrestricted`
- If you get an error like this `“.ps1 is not digitally signed. The script will not execute on the system.”` You have to execute hits command:
  - `Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass`

- Customize ini file for setup, example:

```
[General]
name=HZN-UAG1
source=C:\INSTALL\UAG2209.1\euc-unified-access-gateway-22.09.1.0-20812260_OVF10.ova
target=vi://administrator@vsphere.local:PASSWORD@vEUC-VCSA/vEUC-DC/host/vEUC-Cluster/veuc-esxi01.veuc.lab

ds=VDI-Pool
diskMode=thick

netInternet=dvpg-VM-extern
netManagementNetwork=dvpg-VM-Network
netBackendNetwork=dvpg-VM-Network

deploymentOption=twonic
#ip0 is public NIC
ip0=172.16.0.11
netmask0=255.255.255.0
#ip1 is Backend NIC
ip1=192.168.0.36
netmask1=255.255.255.0

dns=192.168.0.10
defaultGateway=192.168.0.253
ntpServers=192.168.0.253

uagName=HZN-UAG1
honorCipherOrder=true
.
[Horizon]
proxyDestinationUrl=https://192.168.0.209
```

- Execute powershell command:
  - .\uagdeploy.ps1 .\setup-HZN-UAG1.ini
  - (optional) .\uagdeploy.ps1 .\setup-HZN-UAG1.ini 'root-password' 'admin-password' no (no stands for participation with CEIP)
- Caution: does an UAG with the same name already exists, the script will delete this before deployment of the new one.

## 10.3 Configuration UAG

- Login to UAG console as root
  - set timezone
  - (optional) configure root password expiration (default is 365 days)
    - chage -l root
    - chage -M 99999 root
- Login to UI per URL https://<FQDN or IP>:9443 as admin
  - configure Horizon Edge settings
  - Upload needed certificate
  - Export config file as JSON and INI
- Enable SSH for UAG

- Open console window, login as root and enter
- `vi /etc/ssh/sshd_config`
- set the line "PermitRootLogin" to yes and save the file
- Restart SSH Service via `service sshd restart`

## 10.4 Troubleshooting UAG

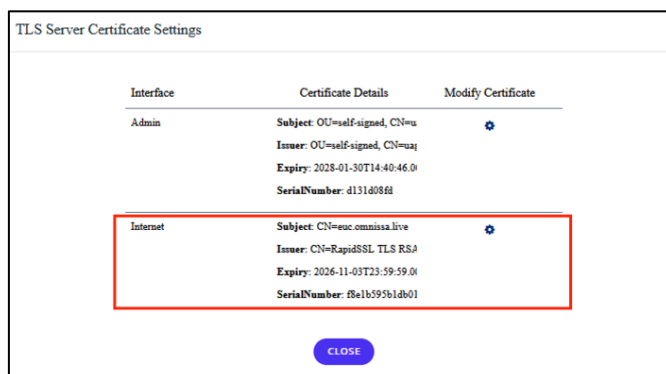
Test port connection between UAG and Connection Server/LB etc:

```
curl -v telnet://target-computer:443
```

## 10.5 Create public certificate for external access

You can create a CSR for UAG, and set the certificate in the UAG UI

- UAG - Generate CSR and Private Key using `uagcertutil` Command, see [here](#)
- Add the public certificate in the UI under → TLS Server Certificate Settings for the Internet interface



## 11. Upgrade from earlier Horizon versions

### 11.1 Update to Horizon 2503 (8.15)

For Term licensing, ensure that you have a valid license key available for Horizon 2412 or higher. For subscription, there is no action needed.

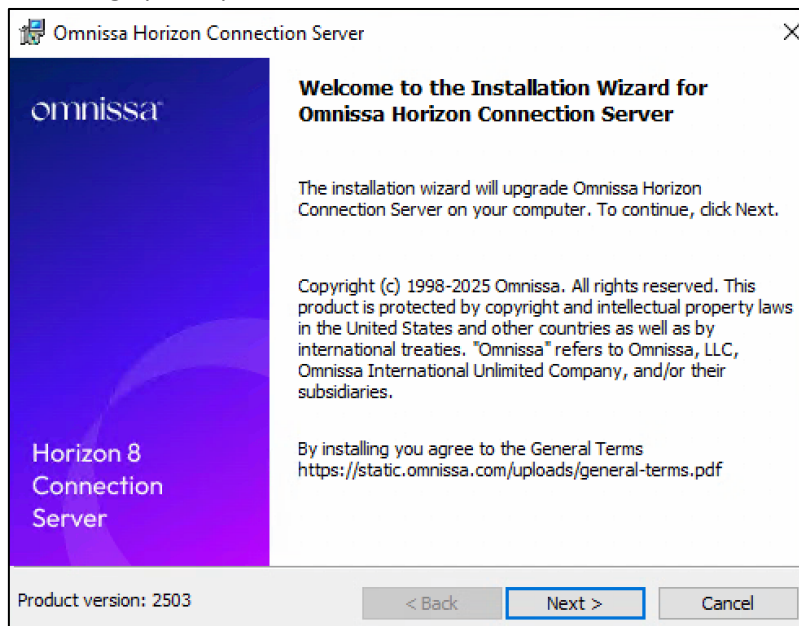
With Horizon 2503, the application partition names in both local and global AD LDS instances have been updated, to reflect the Omnissa naming<sup>3</sup>.

So after updating to Horizon 2503, the Horizon Connection Server application partition names will be updated with a PS-script.

Connection Servers can be updated and kept with the legacy partition name, but they cannot be part of a CPA federation with Connection Servers installed with the new partition name (or vice versa).

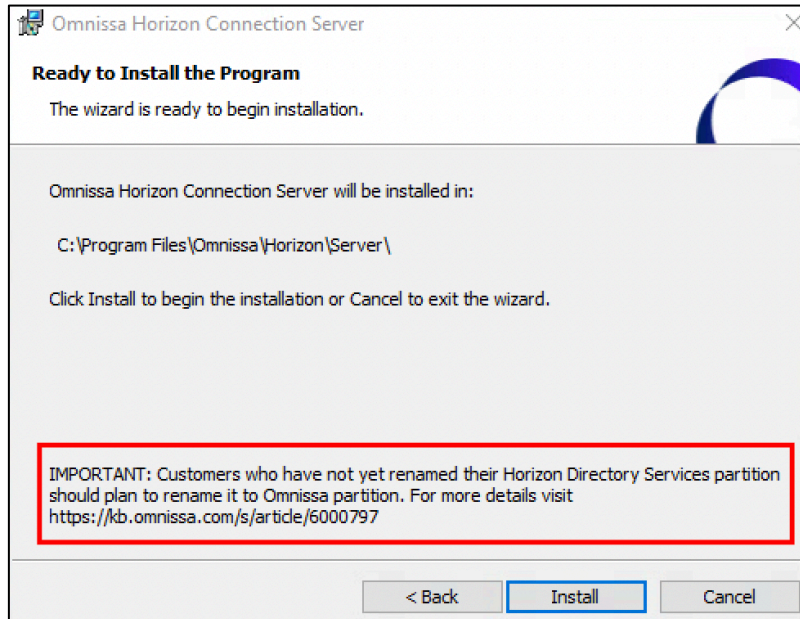
### 11.1.1 Update Horizon 2503

- Executing update process

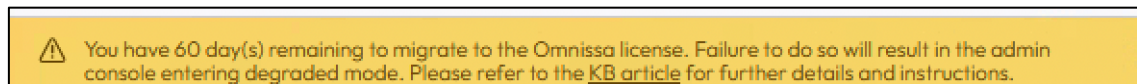


<sup>3</sup> <https://kb.omnissa.com/s/article/6000797>

- Recognize the new program folder



- After finishing the update, you see an alert in the Horizon Console, that the new OmniSSA license key has to be configured (for Term licensing only).



Different from update to 2412, the locked.properties file will be kept automatically, and moved to the new folder structure (C:\Program Files\OmniSSA\Horizon\Server\sslgateway\conf\locked.properties).

### 11.1.2 Update application partition names

A maintenance window is needed for the update of the application partition names. The PS-script "OmniSSAHorizonPartitionMigration-v1" needs to be executed on one Connection Server per POD. This script updates the local, but as well the global AD LDS instance.

After execution, the OmniSSA Horizon Connection Server service has to be stopped on all Connection Servers within a POD. Only once the service on all servers is in the stopped state can it be started again, to reflect the changes.

- Open Powershell as Administrator
- Set Execution Policy to "RemoteSigned"

- Execute the PS-Script “OmnissaHorizonPartitionMigration-v2” – depending from the size of the environment, the first execution can take between some minutes and half an hour.

```

Administrator: Windows PowerShell
===== Script to migrate OmnisshZeDS application partition =====
Disclaimer : Before executing this script, it is essential to upgrade the Horizon environment to Version 2503 or later.
If you're using Omnissh Access with the Horizon 8 deployment, ensure the Omnissh Access connector is upgraded to a version that supports the new partition name.
The migration operation must be performed during the designated maintenance window. During this period, actions such as pool creation, maintenance tasks, configuration changes, entitlements, and launching desktop or application pools should not be performed.
Before initiating the migration process, verify that there are no replication issues within the Horizon environment. You can check the replication status on the dashboard in the Horizon Console.
For more information refer KB article https://kb.omnissh.com/s/article/6000797?lang=en\_US
=====
Press '1' To initiate ADAM Partition Migration
Press '2' To perform cleanup operation
Press '3' To quit
Please select the option :

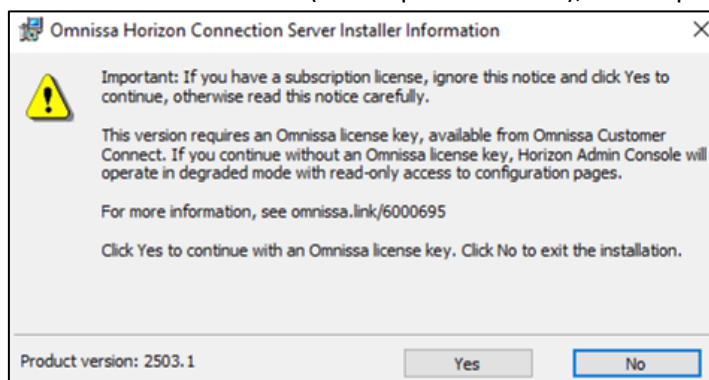
```

- After finishing the script, stop Omnissh Horizon Connection Server service on all Connection Servers in the affected POD.
- Only when Services are stopped, they can be started again.
- If you have additional PODs, repeat the procedure accordingly.

As from now on, the new partition name “DC=vdi,DC=horizon,DC=internal” for local AD LDS application partition, and “DC=vdiglobal,DC=horizon,DC=internal” for global AD LDS replication is active. The PS-Script also can be used to cleanup the old partition name. This should be considered after a waiting time the environment runs stable and without any issues.

### 11.1.3 Update to Horizon 2503.1

- Check the kind of license (subscription vs. term), before proceed



- Click Next and (finally) finish

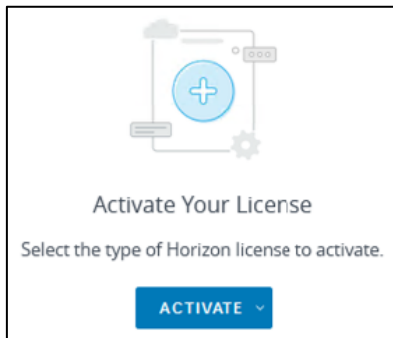


## 11.2 Update to Horizon 2412 (8.14)

- For Term licensing, ensure that you have a valid license key available for Horizon 2412. For subscription, there is no action needed.
- Before updating to 2412, make a copy of the locked.properties file – after the update this has to be placed again.
  - See C:\Program Files\VMware\VMware View\Server\sslgateway\conf\locked.properties in the existing installation
  - Copy it to C:\Program Files\Omnisssa\Horizon\Server\sslgateway\conf\locked.properties
- In Horizon 2412 there is a known bug, that lets get the connection server into degraded mode after 60 days – see this [KB](#) for a workaround.

## 11.3 Update to Horizon 2406 (8.13)

- After updating the first connection server, you have to re-activate the license. So prepare to have the license key available after upgrade directly.



## 11.4 Update from Horizon 7 to Horizon 8

### 11.4.1 Given Environment

- Multiple Horizon 7.13.x Connection Servers on a supported OS (for Horizon 7 and Horizon 8) within a Horizon POD

### 11.4.2 Preparation<sup>4</sup>

- Verify that none of the following features are still in use
  - Composer Linked Clones
  - Persistent Disks
  - Persona Management
- Update Horizon Client to Version 8.x
- Verify Health Status in Horizon Console Dashboard
- Check successful replication to other replica servers
  - `repadmin.exe /showrepl localhost:389`  
`DC=vdi,DC=vmware,DC=int`
- Document global settings in Horizon Console
- Verify that Horizon 8 license is available
- Check for C:\Program Files\VMware\VMware View\Server\sslgateway\conf\locked.properties
- Disable provisioning for affected vCenter Server
- Create actual backup from one Connection Server for the View LDAP configuration per Horizon Console
  - Default folder: C:\ProgramData\VMware\VDM\backups
  - Verify that you have the data recovery password

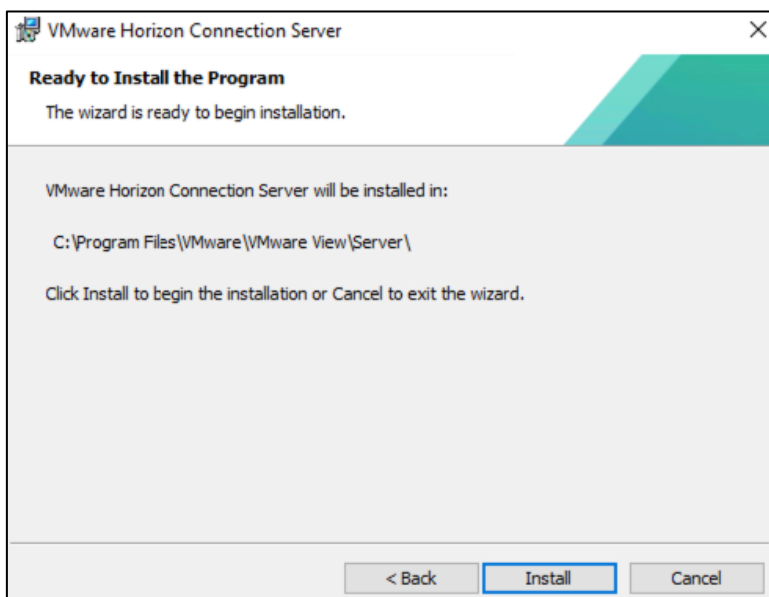
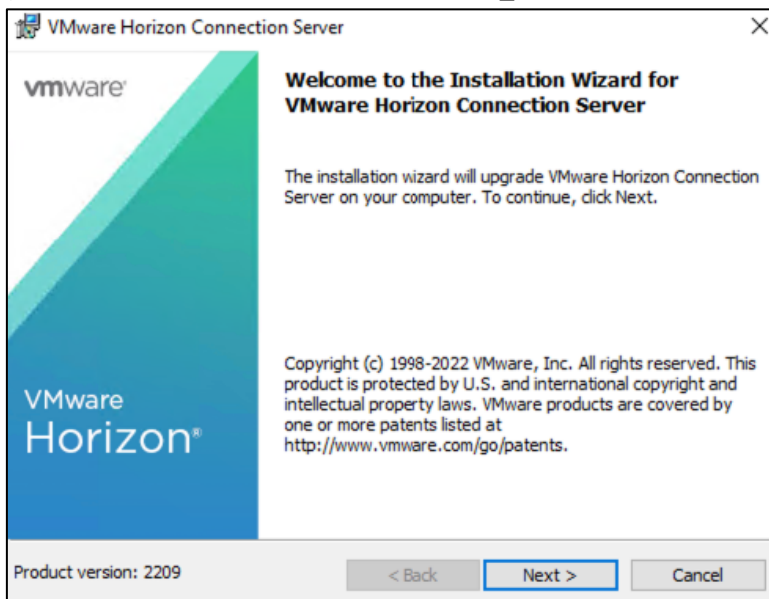
<sup>4</sup> Followed by [VMware Horizon 8 Upgrade Overview](#)

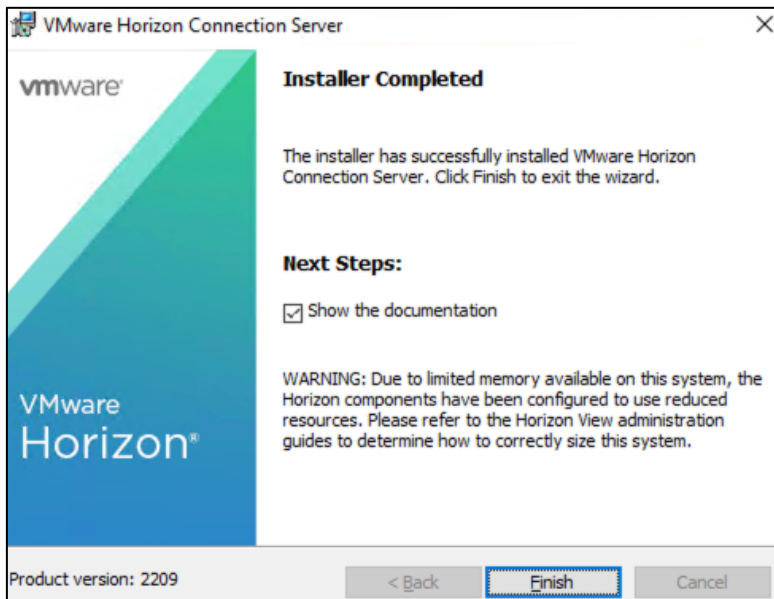
- (optional) create backup from one Connection Server per vdmexport.exe
  - `vdmexport.exe -f HorizonExport.LDF`
- Take an online snapshot from the one Connection Server which was used before for creating the LDAP backup

### 11.4.3 Upgrade to Horizon 8

- Disable the Connection Server which will be upgraded first (in Horizon Console)
- Run the installer for Horizon 8 setup

(VMware-Horizon-Connection-Server-x86\_64-8.7.0-20649599.exe)





- Verify that **VMware Horizon View Connection Server** Service is started after the upgrade
- Login to the Horizon Console from upgraded Connection Server and enter a valid Horizon 8 license key.
- Enable the upgraded Connection Server in Horizon Console.
- Verify that login to the upgraded Connection Server is successful
  
- Repeat the upgrade for each replicated Connection Server within the POD, and run the Horizon 8 installer
  - Verify that login to the upgraded Connection Server is successful after the upgrade
- Verify Health Status in Horizon Console Dashboard
- Verify that vCenter Server icon is green in Horizon Console
  - If not, check for an invalid certificate, and accept the thumbprint of the untrusted certificate
- Enable Provisioning for vCenter Servers
  
- Copy actual GPO-Templates (admx files) to folder C:\Windows\PolicyDefinitions on a domain controller, additional the adml files to folder C:\Windows\PolicyDefinitions\en-US.

#### 11.4.4 Cleanup Tasks

- Take a backup of the newly upgraded Horizon LDAP database (per vdmexport, or per Horizon Console)
- Consolidate snapshots which are taken before the upgrade

### 11.4.5 Troubleshooting options

- Create a Replicated Group After Reverting Connection Server to a Snapshot
  - See [URL](#)
- Maybe you will see a warning message in the dashboard for the upgraded connection servers like “unrecognized request detected”
  - This is a known issue in Horizon 2209, as described in [KB90398](#)
  - Warning message can be ignored, and will disappear after a while (minutes)

## 12. Common Tasks and Day-2-Operations

### 12.1 Auto Upgrade of Horizon Agents

Following types of desktop agents can be updated automatically - since Horizon 2506 Horizon-, App Volumes- and DEM-agents can be updated with this method:

- An automated desktop pool using full clones
- A manual desktop pool
- Manual RDSH farms

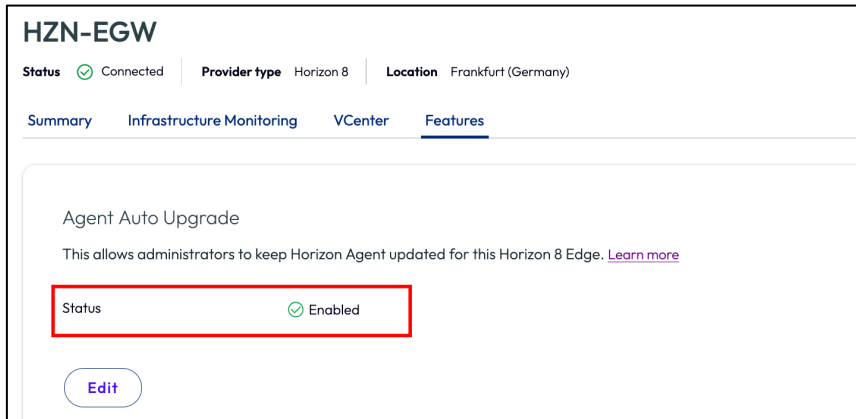
So instant clone desktops are NOT supported.

Generally, this feature is available for Horizon subscription (Edge Gateway needed), but also for Term licensing (“Edgeless”). See [“Auto Upgrade of Horizon Agents and other Supported Agents”](#)

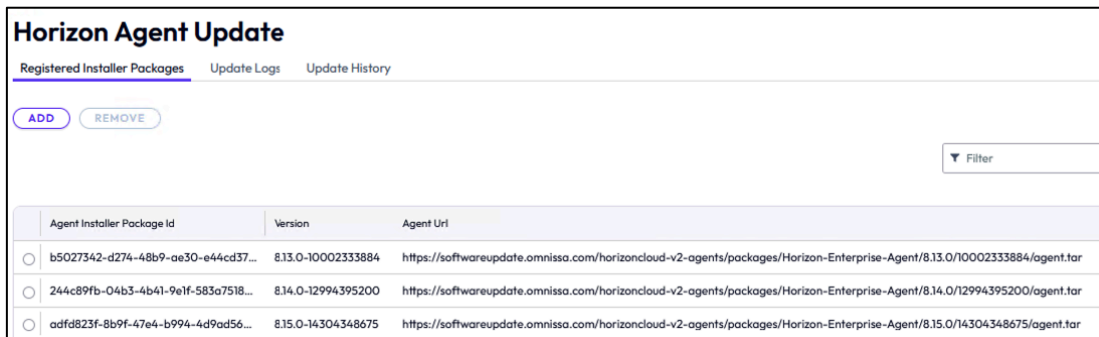
#### 12.1.1 Preparation for Horizon Subscription

- Login to Horizon Cloud Console → Horizon Edges → Select the affected Edge and click on → Features

- Edit **Agent Auto Upgrade** and set Status to **Enabled**

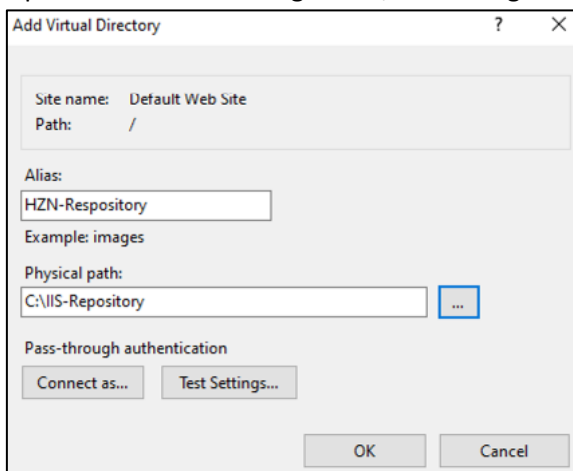


- In Horizon Console, after some moments, you should see the installer packages, which are added automatically



## 12.1.2 Preparation for Horizon Term licencing

- Create and install a web server, like MS Internet Information Services (IIS) (server role)
- Add a folder to the web server, and add needed installer files for agents (exe and json)
- Open Web Server Management, and configure a virtual directory (here MS IIS)



- For MS IIS, enable Direct Browsing, further select "Require SSL" to allow https

- Edit the json file from the Agent installer, and insert the thumbprint from the Web Server certificate as “checksum” in the file (as otherwise the server certificate for metadata file URL is not trusted).
- In the Horizon Console, under →Horizon Agents, add the URL for the json file as following:  
https://FQDN-WebServer/Virtual Directory/Omnissa-Horizon-Agent-x86\_64-xxxx-8.xx-xxxxxx.exe-metadata.json
- The installer package(s) are listed now:

The screenshot shows the 'Horizon Agent Update' interface. It has three tabs: 'Registered Installer Packages' (selected), 'Update Logs', and 'Update History'. Below the tabs are 'ADD' and 'REMOVE' buttons. A 'Filter' dropdown is on the right. The table below lists two packages:

Agent Installer Package Id	Version	Agent Url
5895545e-24d1-44d2-81f8-54d1bd29...	8.16.0-16560454767	https://dc.euclab.org/HZN-Repository/Omnissa-Horizon-Agent-x86_64-2506-8.16.0-16560454767.exe
b700ee51-171b-453f-95ed-34c00259...	8.15.1-16832928916	https://dc.euclab.org/HZN-Repository/Omnissa-Horizon-Agent-x86_64-25031-8.15.1-16832928916.exe

## 12.2 Horizon Group Policies

### 12.2.1 Common GPO Settings for Desktop and RDSH Server VMs

Configures common settings per GPO

- Computer Configuration > Policies > Administrative Templates > System > Group Policy
  - Configure user Group Policy loopback processing mode = Enabled (Mode: Replace) - **loopback replace ensures that only user settings for the VM’s OU are applied to the session.**
  - Configure Logon Script Delay = Disabled
- Computer Configuration > Policies > Administrative Templates > System > Logon
  - Show first sign-in animation = Disabled
  - Always wait for the network at computer startup and logon = Enabled
- User Configuration > Policies > Administrative Templates > Start Menu and Taskbar
  - Remove and prevent access to the Shut Down, Restart, Sleep and Hibernate commands = Enabled
  - Add Logoff to the Start Menu = Enabled

### 12.2.2 Cleanup-Tasks Horizon

- Delete orphaned cp-replica or cp-template entries
  - See Instant-Clone Maintenance Utilities, [URL](#)

- Located under C:\Program Files\Omnissa\Horizon\Server\tools\bin

### 12.2.3 RDSH Server OU-Level Settings

Configure RDS-specific values per GPO

- Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Licensing
  - Use the specified Remote Desktop license server = Enabled
  - Hide notifications about RD Licensing problems that affect the RD Session Host Server = Enabled
  - Set the Remote Desktop license mode = Enabled
- Computer Configuration > Policies > Administrative Templates > System > User Profiles
  - Delete cached copies of roaming profiles = Enabled

## 12.3 Preparation RDSH Systems

### 12.3.1 Prepare RDSH Golden Image for remote access

- Add Domain Users to the local group Remote Desktops Users on the RDSH golden image

## 12.4 Omnissa Horizon As Built Report

There are some scripts available to create a simple but comprehensive Report about an existing Horizon POD environment.

See Source and Documentation here:

<https://github.com/AsBuiltReport/AsBuiltReport.VMware.Horizon/tree/dev>

### 12.4.1 Requirements

Use Powershell:

- VMware PowerCLI 13.2  
`Install-Module -Name VMware.PowerCLI -RequiredVersion 13.2.0.227463535`
  - VMware removed the "VMware.VimAutomation.HorizonView" in latest versions, so newer versions are not compatible.

---

<sup>5</sup> <https://www.powershellgallery.com/packages/VMware.PowerCLI/13.2.0.22746353>

- AsBuiltReport.VMware.Horizon Module  
Install-module AsBuiltReport.VMware.Horizon

## 12.4.2 Generating Report

Use Powershell:

- Generate a Horizon As Built Report for Horizon Connection Server 'hzn-cs01.euclab.org' using specified credentials. Export report to HTML & DOCX formats. Use default report style. Append timestamp to report filename. Save reports to 'C:\INSTALL'

```
New-AsBuiltReport -Report VMware.Horizon -Target 'hzn-
cs01.euclab.org' -Username 'administrator@euclab.org' -Password
'VMware1!' -Format Html,Word -OutputFolderPath 'C:\INSTALL' -
Timestamp
```

Other examples can be found [here](#).

## 12.5 Omnissa Horizon Accelerator – Horizon 8

The „Omnissa Horizon Accelerator – Horizon 8“ is a daily health check script. The script is a comprehensive PowerShell automation tool designed to perform daily health checks for VMware vCenter and Horizon environments. It generates detailed HTML reports covering infrastructure health, performance metrics, and operational status.

### Prerequisites

- Installed VMware PowerCLI Module
  - See readme.md file from Accelerator tool
- (optional) installed Send-MailKitMessage Module (if you want to send the report automatically)
- Installed Horizon Powershell Module
  - See <https://developer.omnissa.com/horizon-powercli/> for further instructions
  - See <https://github.com/euc-oss/euc-samples/tree/main/Horizon-Samples/Omnissa.Horizon.Helper>

The executable “Horizon8.exe” connects with vCenter and Horizon, and offers status for the following items:

- vCenter
  - Datastore utilization and connection status

- host compute utilization
- VMHost alerts, VM alerts, vCenter alerts
- Horizon
  - View Web client response
  - Health status connection server
  - Horizon Event DB status
  - Horizon license information
  - Horizon vCenter
  - Horizon UAG web client response
  - UAG certificate expiry

## 12.6 Replace vCenter Machine SSL certificate

Follow this approach “**vCert - Scripted vCenter expired certificate replacement**”

<https://knowledge.broadcom.com/external/article/385107/vcert-scripted-vcenter-expired-certific.html>

### Connect to vCenter Server via WinSCP

Run WinSCP and define the new session with these instructions:

- File protocol: SFTP
- Host name: The vCenter or ESXi FQDN or IP address.
- Port number: 22
- User name: root
- Password: <the root account password>
  - Click Advanced
  - Select SFTP
  - In SFTP server, replace the default with this: shell /usr/libexec/sftp-server  
This option is better than changing the bash of vCenter as it will not bring risks on changing the vCenter Photon OS settings.  
With this option, WinSCP will not return the error:  
"Received too large (1433299822 B) SFTP packet. Max supported packet size is 1024000 B. The error is typically caused by message printed from startup script (like .profile). The message may start with "Unkn". Cannot initialize SFTP protocol. Is the host running an SFTP server?"

- Click Login.

Source: <https://knowledge.broadcom.com/external/article/403632/how-to-upload-or-download-files-to-or-fr.html>

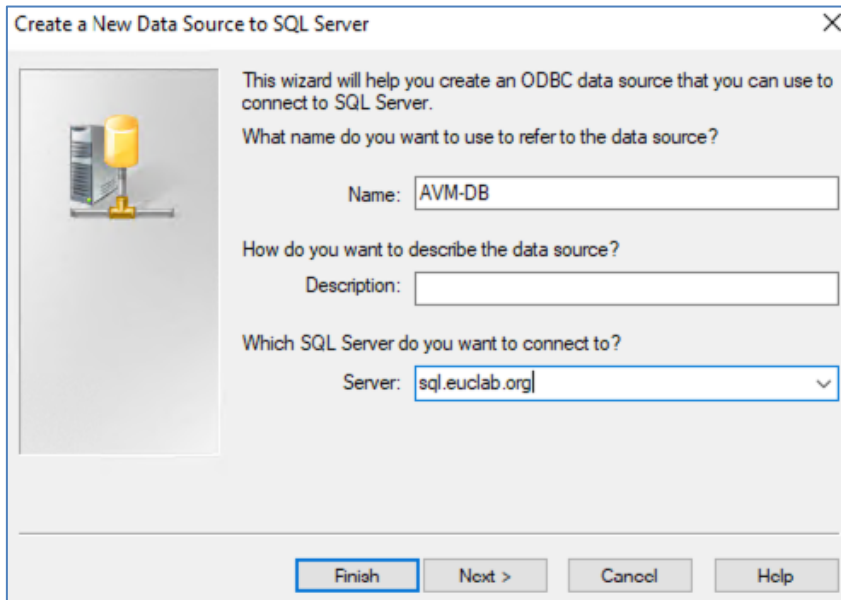
For Custom CA-signed certificate (via <https://<CA-FQDN>/certsrv>), use DER encoded format.

## 13. Setup und Update Omnissa AppVolumes

Version 2312.2

### 13.1 Requirements App Volumes

- For the first App Volumes Manager, create a SQL DB for App Volumes
- Create ODBC (64-bit) connection on the desired App Volumes Server



Create a New Data Source to SQL Server

This wizard will help you create an ODBC data source that you can use to connect to SQL Server.

What name do you want to use to refer to the data source?

Name:


How do you want to describe the data source?

Description:

Which SQL Server do you want to connect to?

Server:

Create a New Data Source to SQL Server



How should SQL Server verify the authenticity of the login ID?

With Windows NT authentication using the network login ID.

With SQL Server authentication using a login ID and password entered by the user.

To change the network library used to communicate with SQL Server, click Client Configuration.

Client Configuration...


Connect to SQL Server to obtain default settings for the additional configuration options.

Login ID: HZN-DB-Admin

Password: ●●●●●●●●

< Back Next > Cancel Help

Create a New Data Source to SQL Server



Change the default database to:

AVM-DB

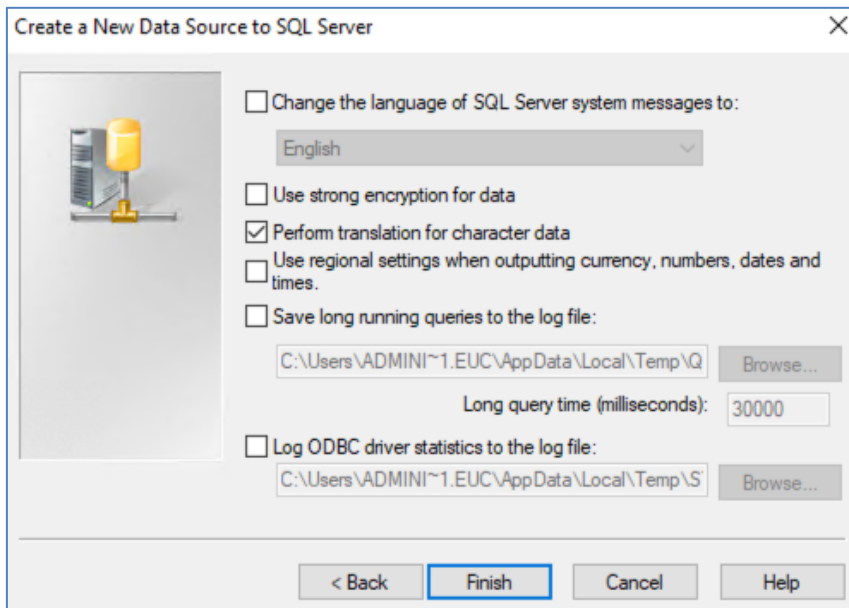
Attach database filename:

Use ANSI quoted identifiers.

Use ANSI nulls, paddings and warnings.

Use the failover SQL Server if the primary SQL Server is not available.

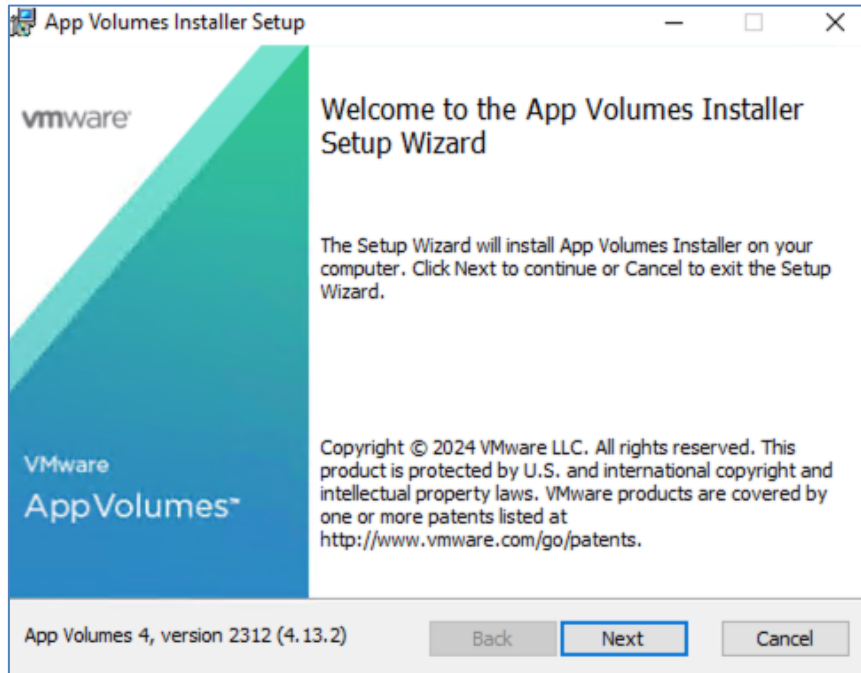
< Back Next > Cancel Help



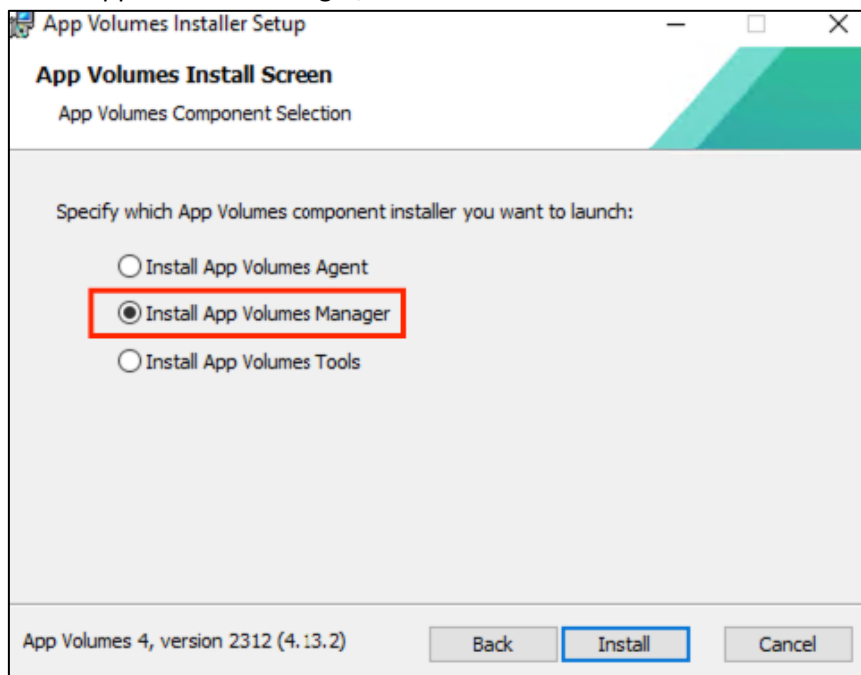
- Create a Service Account for communication between App Volumes and AD (consider to choose a dedicated account per App Volumes instance!), with sufficient permissions, as described [here](#). In summary, these permissions are needed:
  - Has read access to the Active Directory domain
  - Administrator privileges are not required
  - Has a password that does not expire

## 13.2 Setup App Volumes

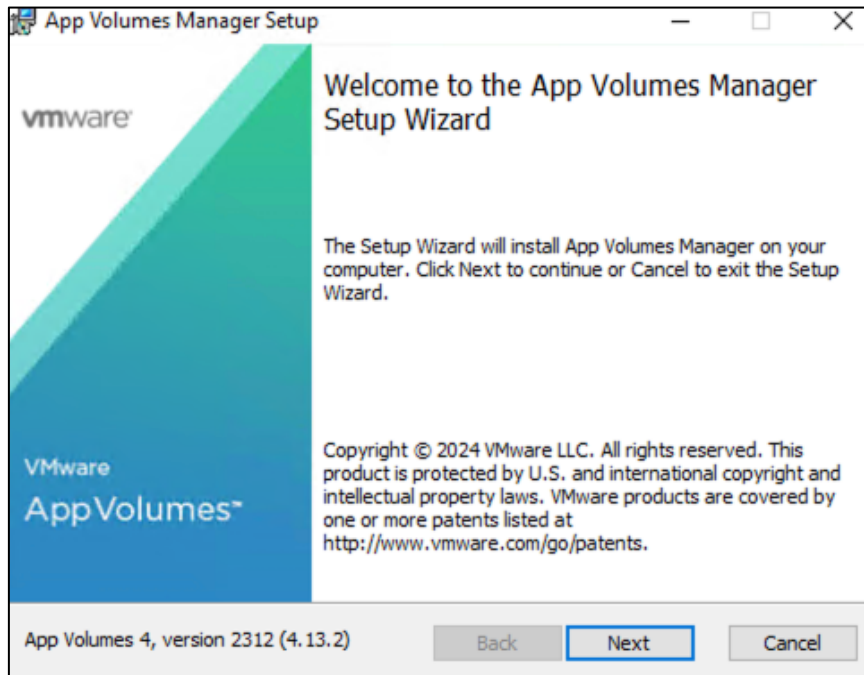
- Execute setup process, and click →Next:



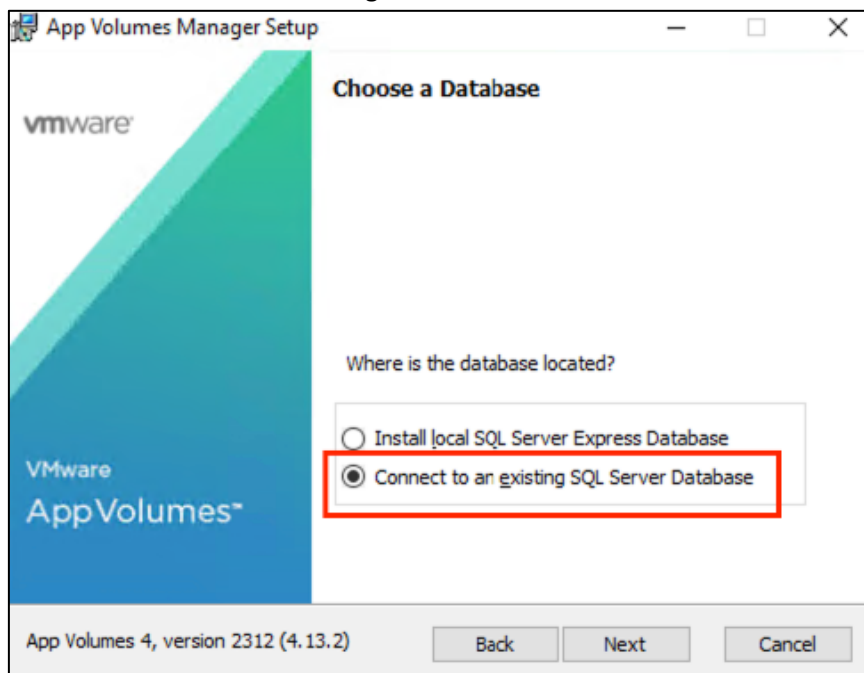
- Select App Volumes Manager, and click →Install:



- After a few seconds, click →Next:



- Select to connect to an existing SQL Server Database:



- Enter appropriate information, and deselect SQL Server certificate validation:

App Volumes Manager Setup

### Database Server

Select database server and authentication method

Choose local or remote database server to use:

SQL.euclab.org Browse...

Connect using:

Windows Integrated Authentication (automatically use this server's SYSTEM account)

Server authentication using the Login ID and password below

Login ID: HZN-DB-Admin

Password: [masked]

Name of database catalog to use or create:

AVM-DB Browse...

Overwrite existing database (if any)  Enable SQL Server certificate validation

App Volumes 4, version 2312 (4.13.2) Back Next Cancel

- Edit port options, if needed, and consider to allow connections over HTTP:

App Volumes Manager Setup

### Choose Network Ports and Security options

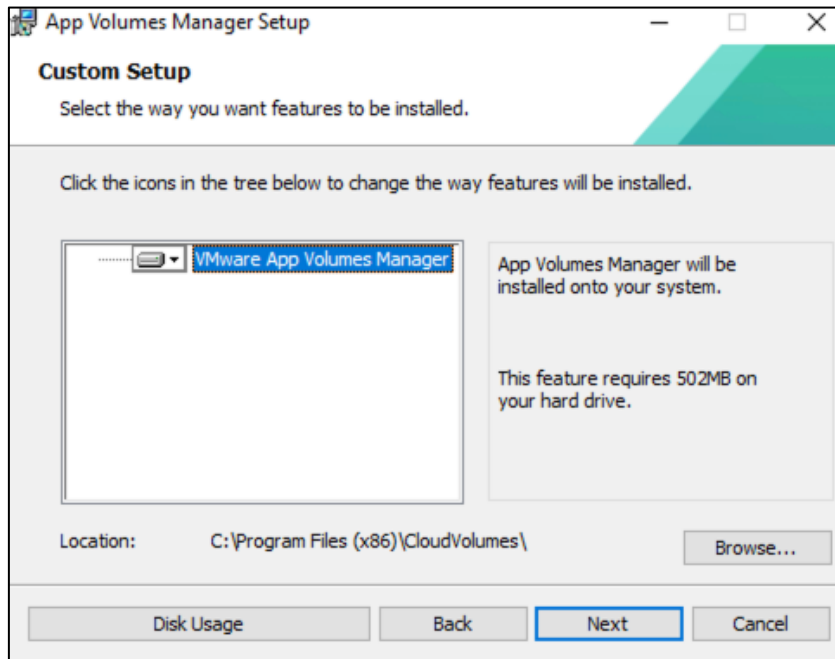
HTTP Port: 80 HTTPS Port: 443

Allow connections over HTTP (insecure)

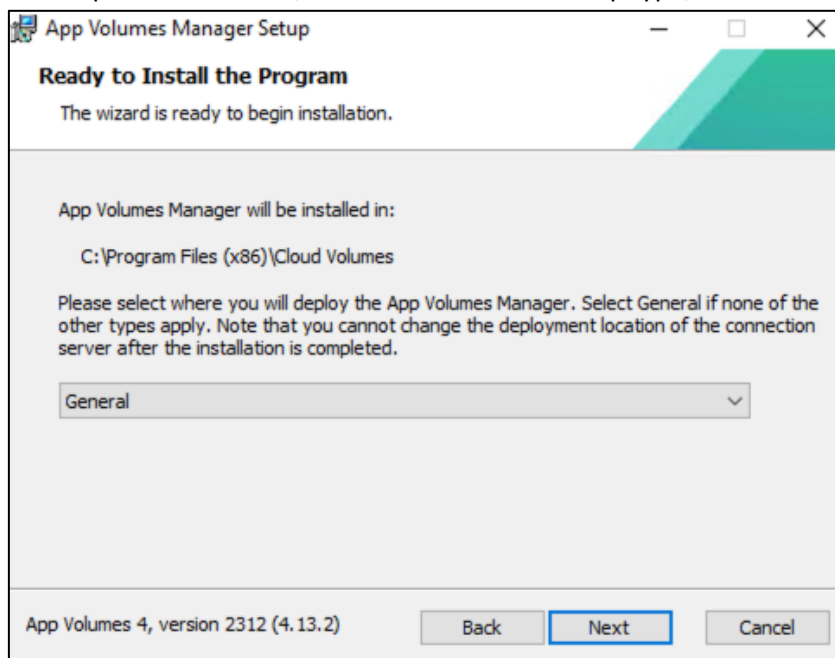
These ports will be allowed through the Windows Firewall

App Volumes 4, version 2312 (4.13.2) Back Next Cancel

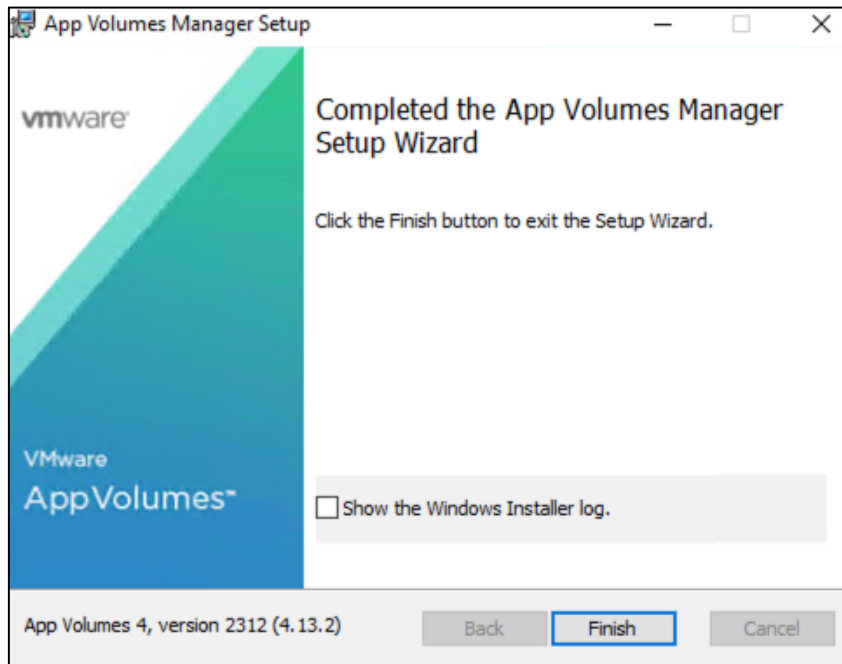
- Confirm the default setup path:



- For on-prem installation, choose “General” as setup type, and start installation:

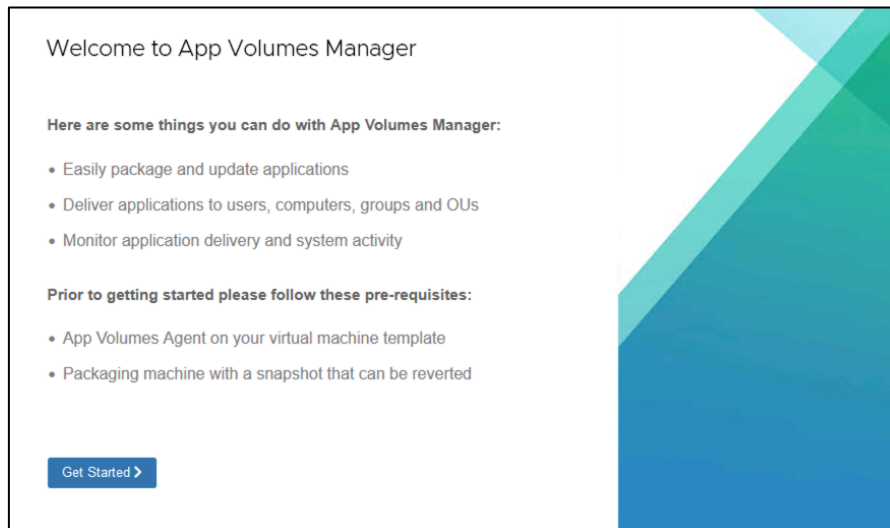


- Finished after some minutes



### 13.3 Initial configuration App Volumes Manager

- Open App Volumes Manager UI: <https://FQDN> – you will see the “Get Started” page. Click on →Get Started:



- Edit the license information, and upload the license file from the setup:

VMware App Volumes™

License | AD Domains | Admin Roles | Machine Managers | Storage | Settings

### License Information

A valid license issued by VMware is required to use this management console.

Upload the VMware App Volumes license key file to activate this product.

App Volumes License File:  VMware\_App\_Volu...\_License\_v4.key

- Register AD Domain:

VMware App Volumes™

License | AD Domains | Admin Roles | Machine Managers | Storage | Settings

### Register Active Directory Domain

Active Directory Domain Name:  Fully qualified Active Directory domain name  
Example: vmware.com

Domain Controller Hosts:  This may be left blank (to use any Domain Controller)  
Example: ad\_server.vmware.com, 10.107.XX.XXX, 10.107.XXX.XX

LDAP Base:  This may be left blank (to use all of Active Directory)  
Example: OU=engineering,DC=vmware,DC=com

Username:  This may be a user with read-only access  
Example: administrator

Password:  Password is stored encrypted

Security:  Requires corresponding ActiveDirectory configuration  
 Disable certificate validation (insecure)

Port:  This may be left blank (to use default port)

- Consider to disable certificate validation – you can edit this later.

- Click →Next:

VMware App Volumes™

License | AD Domains | Admin Roles | Machine Managers | Storage | Settings

### Active Directory Domains

App Volumes uses Active Directory to assign applications to users, computers, groups, and OUs.

Important Information:

- The credentials you provide are stored encrypted.
- The service accounts you provide only require read access.
- Ensure the service accounts you provide do not require periodic password reset.

Show 10

Domain	Netbios	Base	Username	Security	Port	
euclab.org	EUCLAB		avm-sa-ad	LDAPS	636	<input type="checkbox"/>

Showing 1 to 1 of 1 domains   1

- Assign administrative role to the appropriate AD group:

VMware App Volumes™

License AD Domains **Admin Roles** Machine Managers Storage Settings

### Administrator Roles

Roles grant administrative privileges to the members of Active Directory groups.

Important information:

- Only users in these groups will be able to login to the Manager.

Role: Administrators

Search Domain: All

Search Groups: administrators Contains Search

Search all domains in the Active Directory forest

Choose Group: EUCLABAdministrators

Assign

- You can manage and assign additional roles later. Click →Next:

VMware App Volumes™

License AD Domains **Admin Roles** Machine Managers Storage Settings

### Administrator Roles

Assign Role Manage Roles

Roles grant administrative privileges to the members of Active Directory groups.

Important information:

- Only users in these groups will be able to login to the Manager.

Show 10 Filter

Group	Role
EUCLABAdministrators	Administrators

Showing 1 to 1 of 1 role assignments

First Previous 1 Next Last

Next

- Register the “Machine Manager” (vCenter Server). You should create a dedicated user and role in vSphere, as described [here](#).

VMware App Volumes™

License | AD Domains | Admin Roles | **Machine Managers** | Storage | Settings

### Machine Managers

Register and configure in-guest services or leverage the performance of VMware vCenter Servers to deliver volumes.

Type:

Hostname:  **vCenter Hostname**  
Example: server.your-domain.local

Username:  **vCenter Service Account Username**  
Note: You may use a local account for better performance

Password:  **vCenter Service Account Password**  
Note: Password is stored encrypted

Fast Attach:  Enable Fast Attach for VMDK packages **Requires VMware vSphere version 8.0 update 2 or later**

Mount ESXi:  Issue mount operations to ESXi servers **When mounting, connect directly to ESXi servers**

Mount Local:  Use local copies of volumes **Prioritize volumes available on locally attached storage when possible  
Increases IO performance by distributing utilization (unnecessary on VSAN)**

Mount Queue:  Use queues for mount operations **Use shared queues to store and process mount requests  
Decreases the number of active connections to vCenter and ESXi servers**

Mount Async:  Use asynchronous mount operations **Wait for the mount request completion in the background  
Increases Manager server throughput (requires queues)**

Mount Throttle:  Throttle concurrent mount operations **Limits the number of actively processing mount requests  
Decreases load on vCenter/ESXi servers (requires queues)**

**Maximum number of concurrent mount operations per queue  
Each vCenter/ESXi server uses a queue per Manager process**

[Save](#)

- Click Next:

VMware App Volumes™

License | AD Domains | Admin Roles | **Machine Managers** | Storage | Settings

### Machine Managers

[Register Machine Manager](#)

Register and configure in-guest services or leverage the performance of VMware vCenter Servers to deliver volumes.

Show 10

Host	Username	Type	
+	vcsa.euclab.org	avm-sa@vsphere.local	VMware vCenter <input type="checkbox"/>

Showing 1 to 1 of 1 machine managers

First Previous 1 Next Last

[Next](#)

- Select an appropriate datastore for packages and writables:

VMware App Volumes™

License | AD Domains | Admin Roles | Machine Managers | **Storage** | Settings

**Storage** Upload Templates Rescan

Configure storage options for Packages, Writable Volumes, and AppStacks.

Important Information:

- Use storage that is accessible to all virtual machine host servers.
- Local host storage may be used, but volumes will only be attached for VMs on that host.

**Packages**

Default Storage Location:    
Type: NFS - Share Mode: Shared

Default Storage Path:

Templates Path:

**Writable Volumes**

Default Storage Location:    
Type: NFS - Share Mode: Shared

Default Storage Path:

Templates Path:

Default Backup Path:

Next

- Upload the templates, and confirm the default settings to finish the wizard:

VMware App Volumes™

License | AD Domains | Admin Roles | Machine Managers | **Storage** | Settings

**Upload Templates**

Upload the volumes packaged with this Manager to the selected datastore.  
 Credentials for an ESX host with access to the selected datastore are needed to convert the uploaded volumes to thin format.

Storage:

Host:

ESX Username:

ESX Password:

Show 10

Filename	Type	Destination	Exists	
template_workstation.vmdk	Package	appvolumes/packages_templates	No	<input checked="" type="checkbox"/>
template_profile_only_workstation.vmdk	Profile Only	appvolumes/writables_templates	No	<input checked="" type="checkbox"/>
template_uia_plus_profile_workstation.vmdk	UIA + Profile	appvolumes/writables_templates	No	<input checked="" type="checkbox"/>
template_uia_only_workstation.vmdk	UIA Only	appvolumes/writables_templates	No	<input checked="" type="checkbox"/>

Showing 1 to 4 of 4 Templates First Previous 1 Next Last

Skip Upload

## 13.4 Preparation Provisioning VM

Try to keep the provisioning VM (more or less) identical as the golden master for Horizon pools (or RDSH farms), see [References](#)

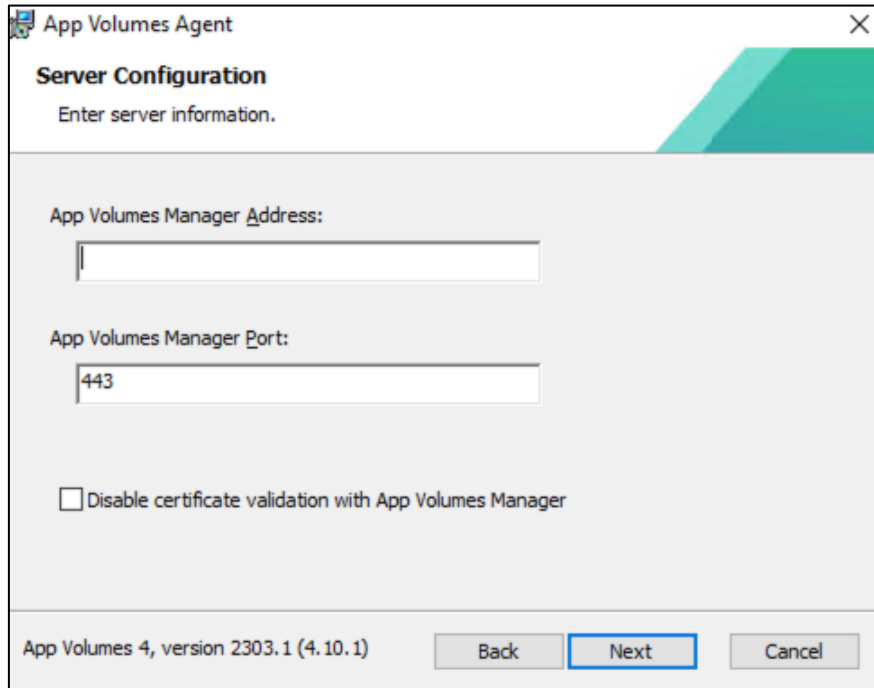
- Domain joined in the same AD as the target computers
- No Horizon Agent installed
- OS optimized

Setup App Volumes Agent

- Execute Installation file

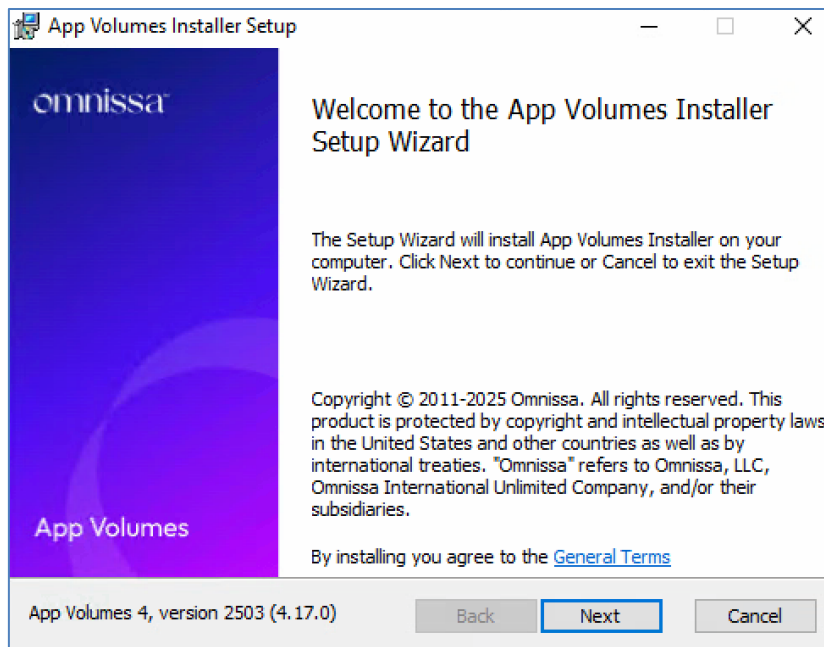


- Enter FQDN from App Volumes Manager (or from LB)

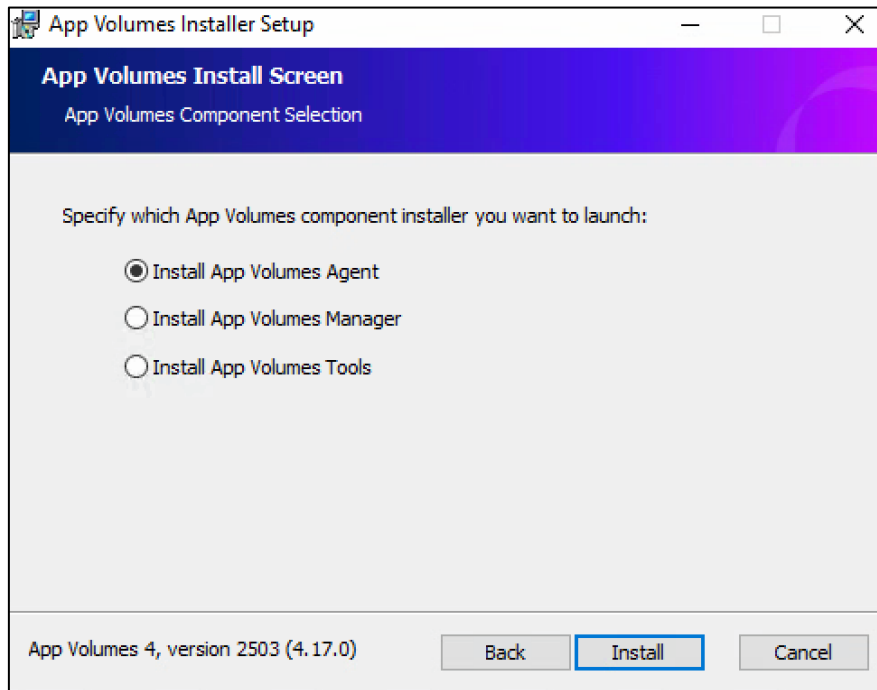


## 13.5 Setup App Volumes Agent

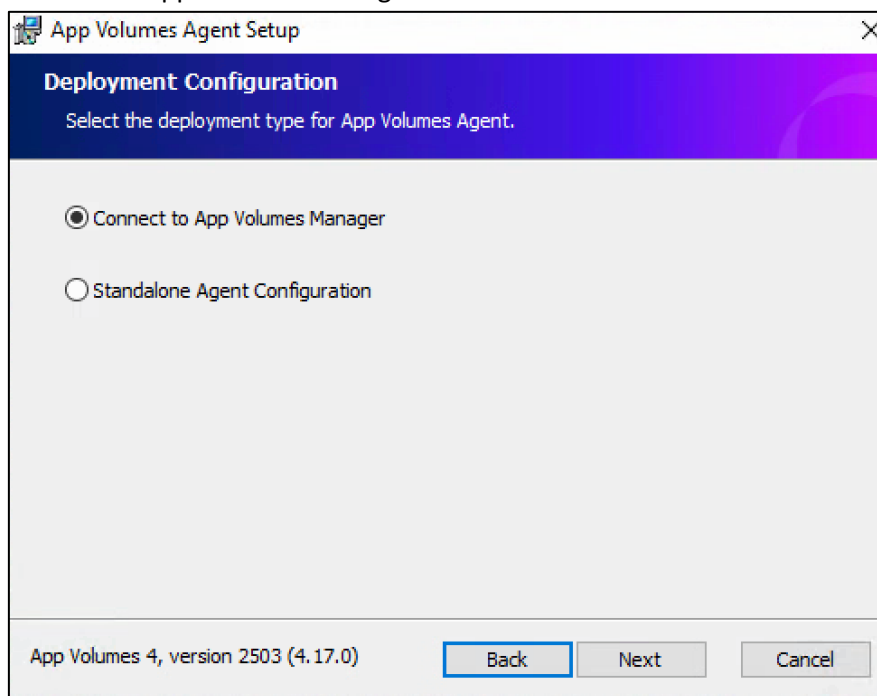
- Execute installation file



- Select App Volumes Agent



- Connect to App Volumes Manager



- Standalone Configuration is needed, if you intend to setup the Agent on a Windows endpoint directly (not virtual).

- Enter FQDN from App Volumes Manager (or from LB)

The screenshot shows the 'App Volumes Agent' window with the 'Server Configuration' tab selected. The window title is 'App Volumes Agent'. The header bar is blue with the text 'Server Configuration' and 'Enter server information.' below it. The main area contains three input fields: 'App Volumes Manager Address:' (empty), 'App Volumes Manager Port:' (containing '443'), and a checkbox labeled 'Disable certificate validation with App Volumes Manager' which is currently unchecked. At the bottom, there is a footer with the text 'App Volumes 4, version 2503 (4.17.0)' and three buttons: 'Back', 'Next' (highlighted with a blue border), and 'Cancel'.

- Select the type of machine for app delivery (default non-persistent enabled)

The screenshot shows the 'App Volumes Agent Setup' window with the 'Machine Type' tab selected. The window title is 'App Volumes Agent Setup'. The header bar is blue with the text 'Machine Type'. Below the header, there is a paragraph of text: 'The following setting is intended for environments with non-persistent virtual desktop infrastructure (VDI), where user data and installed applications do not persist across sessions.' Below this text is a checkbox labeled 'Non-persistent or multi-session machines' which is checked. Underneath the checkbox is a note: 'Leave this option unchecked if the machine retains user data and settings on the operating system disk.' At the bottom, there is a footer with the text 'App Volumes 4, version 2503 (4.17.0)' and three buttons: 'Back' (highlighted with a blue border), 'Next', and 'Cancel'.

- Reboot VM.

## 13.6 Update VMware AppVolumes (2.x)

- Das Update ist mit Downtime von AppVolumes verbunden!

- Unassign aller Volumes (Detach aller Volumes)
- Backup der SQL-DB des AppVolumes-Managers.  
I.d.R. ist auf dem Windows-System eine MS SQL-Express-Instanz installiert. Ggf. das SQL Server Management Studio installieren, um die DB („svmanager\_production“) mit Bordmitteln zu sichern.
- Snapshot der VM des App Volumes Managers

- Ein direktes Update ist ab der Version 2.12 möglich über die Installationsroutine

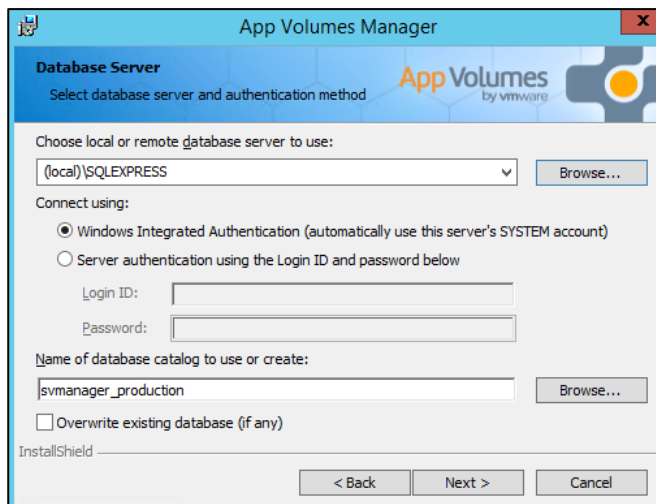


- Existiert eine ältere Version, muss diese erst deinstalliert(!) werden über die Systemsteuerung
- Darauf achten NICHT die SQL Express Instanz zu deinstallieren

- Aufruf der Installationsroutine des neuen App Volumes Manager



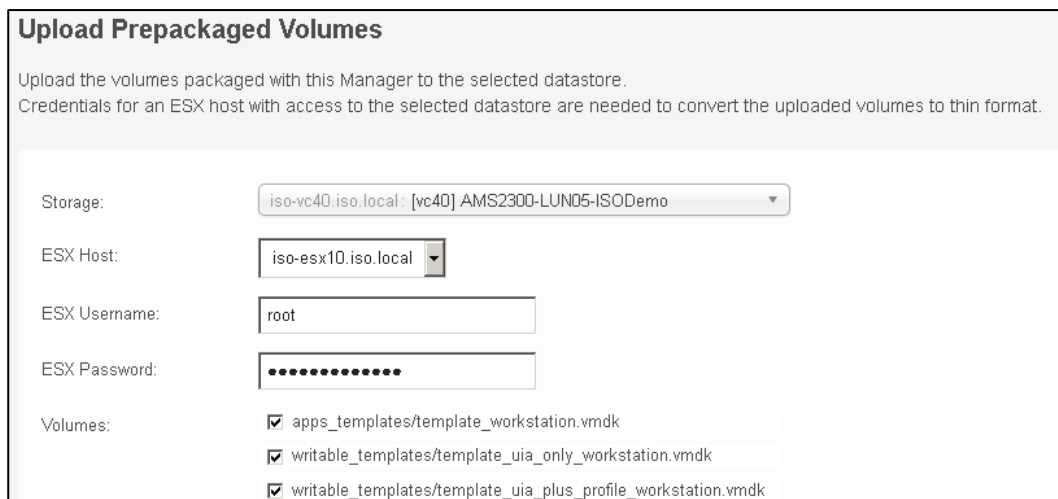
- Auswahl der vorhandenen MS SQL Express Datenbank



- Nach erfolgter Installation über das Web-Portal einloggen:  
<https://fqdn-app-volumes-manager/login>
  - Wechseln zu →Configuration →Machine Managers
    - Für jeden hier hinterlegten Host in die →Details gehen und das Zertifikat akzeptieren

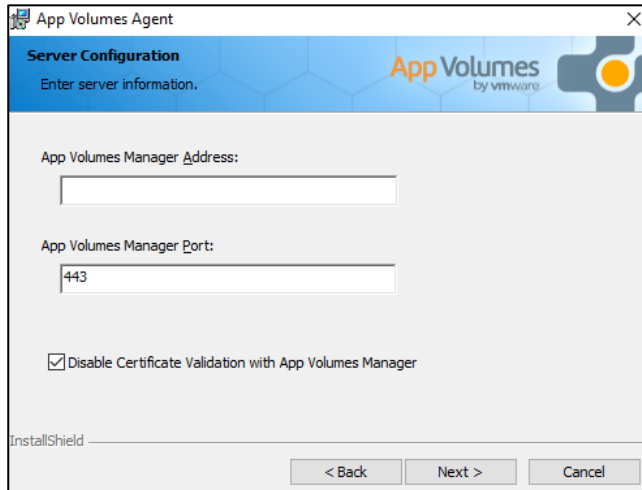



- Upgrade der App Volumes Templates
  - Im App Volumes Manager wechseln zu →Configuration →Storage
  - Klick auf →Upload Prepackaged Volumes



- Mit Klick auf →Upload bestätigen.
- Ab hier kann der Betrieb ggf. wieder aufgenommen werden (heisst die unter der Vorgänger-Version erstellten AppStacks können weiterhin genutzt werden).  
Dazu müssen die Volumes wieder „assigned“ werden.  
Empfohlen wird jedoch nun das Update des App Volumes Agent.
  - Update App Volumes Agent
    - Auf den sog. „Target VMs“ (Parent VMs, Master VMs) muss der alte App Volumes Agent deinstalliert, anschließend der aktuelle installiert werden. Dabei bitte den

Haken setzen bei „Disable Certificate Validation with App Volumes Manager“:



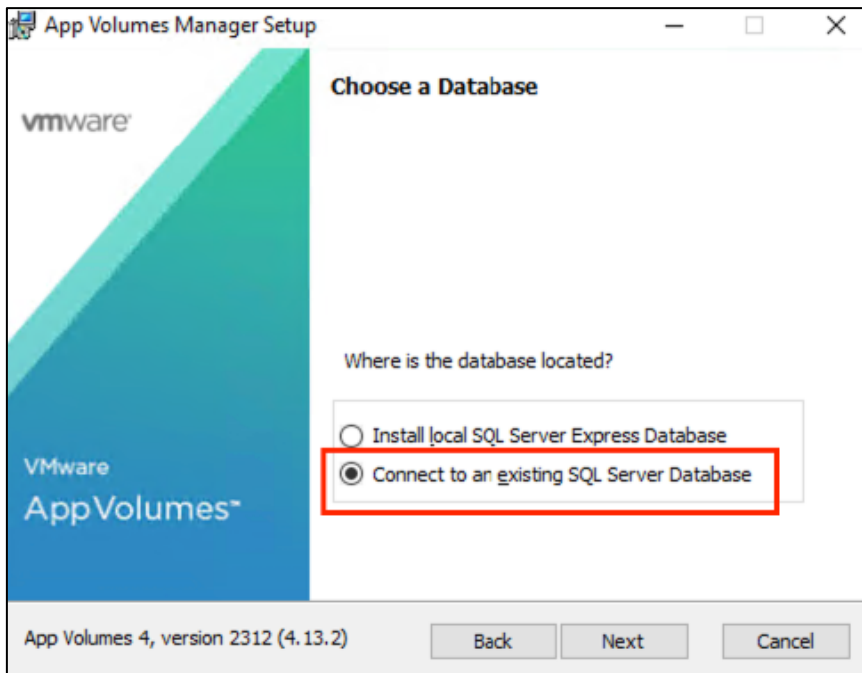
- Falls die Target VM nach der Installation des aktuellen Agenten eine Fehlermeldung produziert („Unable to contact App Volumes Manager. Virtualization is disabled“) kann das an einem falschen Port liegen, über welchen der Agent versucht den Manager zu erreichen. Default ist Port 443. Ebenso kann es aber auch sein, dass Manager und Agent nicht identisch konfiguriert sind bzgl. der SSL-Kommunikation. Siehe auch [VMware KB-Artikel 2148178](#).
  - Falls beim **Manager** während der Installation ausschließlich HTTPS konfiguriert wurde, kann HTTP auch nachträglich konfiguriert werden:  
<https://docs.vmware.com/en/VMware-App-Volumes/2.12/com.vmware.appvolumes.user.doc/GUID-3CE54D86-5EFF-40CD-BOCC-47066CE2E768.html>
    - Eine funktionierende [nginx.conf](#) (HTTP und HTTPS)  
  
nginx.conf
  - Ebenso kann beim **Agenten** der Port sowie die SSL-Validierung nachträglich geändert werden per Registry:  
<https://docs.vmware.com/en/VMware-App-Volumes/2.12/com.vmware.appvolumes.user.doc/GUID-794F658B-9332-4340-92CB-BEFA760DDA01.html>
- Nacharbeiten
  - Neu-Erstellen (Recompose) der Desktop-Pools
  - Re-Assign der Volumes
  - Konsolidieren des Snapshots des App Volumes Managers

## 13.7 Post-Tasks AppVolumes

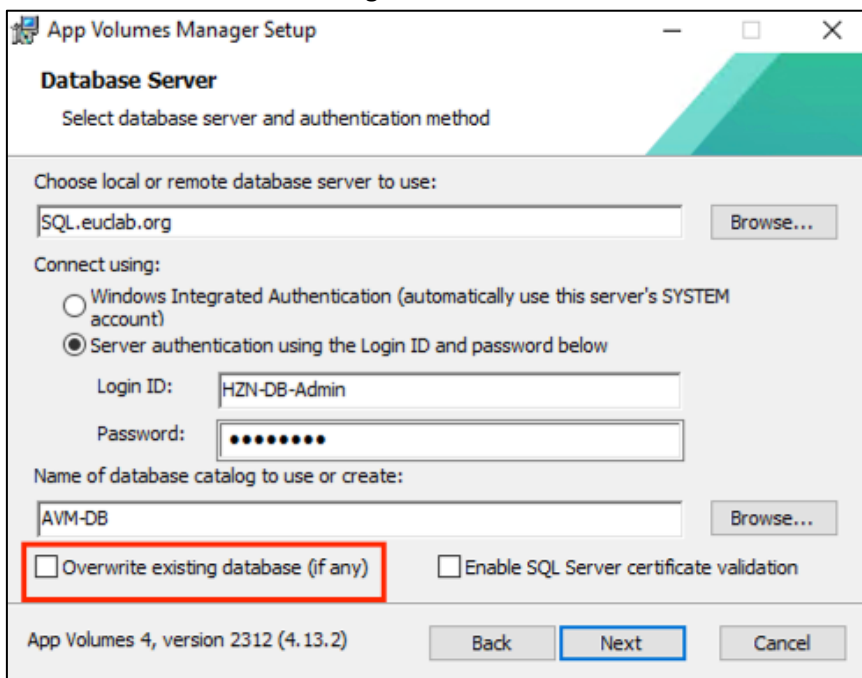
### 13.7.1 Add additional App Volumes Manager

You can add additional App Volumes Manager to the same instance for HA and workload distribution purpose.

- Follow the instructions similar to installing the first App Volumes Manager, as described [here](#).
- Similar, select to connect to an existing SQL Server Database:



- Ensure that "Overwrite existing database" is NOT selected:



- Keep the rest as described already, and finish installation.
- Accessing the UI from the newly installed App Volumes Manager, it has to be registered with one of the existing Manager:

VMware App Volumes™

### Register App Volumes Manager Server

The current App Volumes Manager server is unregistered. Please specify the address of a registered App Volumes Manager server and login credentials.

Registered Manager Address:  (?)

Username:

Password:

Domain:

- Finally, this can be verified under →Configuration →Managers (at one of the managers):

VMware App Volumes™

EUCLAB\Administrator Logout

INVENTORY DIRECTORY INFRASTRUCTURE ACTIVITY CONFIGURATION

License AD Domains Admin Roles Machine Managers Storage Managers Settings

### App Volumes Manager Servers

App Volumes Manager servers that have been seen by this instance of App Volumes.

Show 10 Filter

Manager	Version	Status	First Seen	Last Seen
AVM01	App Volumes 4, version 2312 (4.13.2.15)	Registered	Jul 19 2024	Jul 22 2024
AVM02	App Volumes 4, version 2312 (4.13.2.15)	Registered	Jul 23 2024	Jul 23 2024

Showing 1 to 2 of 2 App Volumes Manager Servers

First Previous 1 Next Last

## 13.7.2 Configure SSL certificate validation for AD

For a secure communication between App Volumes and AD over LDAPS, you can enable certificate validation. You need the appropriate root certificate from your CA per App Volumes Manager, as described [here](#) (Configure CA Certificates in App Volumes Manager).

- On system, which holds the CA, execute this command to export the root certificate:
 

```
certutil -ca.cert adCA.cer
```

  - This shows the root certificate, and exports it as cer file (the name caAD.cer is mandatory)
  - If needed, you can convert cer file to pem file with openssl:
 

```
openssl x509 -inform der -in adCA.cer -out adCA.pem
```
- In App Volumes Manager, domain controller host names that are specified in the domain controller hosts field must match the certificate host names
- Copy the adCA.pem file to every App Volumes Manager into this directory:
 

```
C:\Program Files (x86)\Cloud Volumes\Manager\config
```

- Restart the App Volumes Manager service (for every affected AVM)
- In AVM console, edit the AD domain configuration, and enable certificate validation

The screenshot shows the VMware App Volumes console interface. The main navigation bar includes 'INVENTORY', 'DIRECTORY', 'INFRASTRUCTURE', 'ACTIVITY', and 'CONFIGURATION'. The 'CONFIGURATION' tab is active, and the 'AD Domains' sub-tab is selected. The page title is 'Edit Active Directory Domain'. The configuration form includes the following fields and options:

- Active Directory Domain Name:** euclab.org (Fully qualified Active Directory domain name, Example: vmware.com)
- Domain Controller Hosts:** dc.euclab.org (This may be left blank to use any Domain Controller, Example: ad\_server.vmware.com, 10.107.XX.XXX, 10.107.XX.XXX)
- LDAP Base:** (This may be left blank to use all of Active Directory, Example: OU=engineering,DC=vmware,DC=com)
- Username:** avm-sa-ad (This may be a user with read-only access, Example: administrator)
- Password:** (Password is stored encrypted)
- Security:** Secure LDAP (LDAPS) (Requires corresponding ActiveDirectory configuration)
- Disable certificate validation (insecure)** (This checkbox is highlighted with a red box in the original image)
- Port:** 636 (This may be left blank to use default port)

Buttons for 'Cancel' and 'Update' are located at the bottom of the form.

### 13.7.3 Anpassungen bei Horizon automatischen Pools

- In Zusammenhang mit automatisch provisionierten Desktops in Horizon View kann es ggf. zu „unliebsamen Überschneidungen“ kommen, wenn der App Volumes Agent bereits mit dem App Volumes Manager kommuniziert, obwohl die Anpassung eines neu provisionierten Desktops noch nicht abgeschlossen ist. Dieses Verhalten tritt vor allem auf, wenn in den Assignments der AppStacks Computerkonten anstelle Benutzerkonten hinterlegt sind!

Als Workaround empfiehlt sich, den App Volumes Agent Dienst in der Parent VM (alternativ Template) auf manuell zu stellen. In der Anpassung muss dann jeweils ein Skript ausgeführt werden, damit der App Volumes Agent nach erfolgter Anpassung des Desktops wieder auf automatisch gestartet werden kann.

- Bei Quickprep:

The screenshot shows the 'QuickPrep verwenden' configuration form. It includes the following fields and examples:

- Name des Ausschaltskripts:** (Field with a help icon)
- Parameter des Ausschaltskripts:** (Field with a help icon, Example: p1 p2 p3)
- Name des nach der Synchronisierung ausgeführten Skripts:** c:\post-script.cmd (Field with a help icon)
- Parameter des nach der Synchronisierung ausgeführten Skripts:** (Field with a help icon, Example: p1 p2 p3)

```
svservice.cmd.txt - Editor
Datei Bearbeiten Format Ansicht ?
echo on
sc config svservice start=auto
net start svservice
```

- Bei Sysprep:

Anpassung-Win10-AL - Wird bearbeitet

1 Eigenschaften  
2 Registrierungsinformationen  
3 Computername  
4 Windows-Lizenz  
5 Administrator Kennwort  
6 Zeitzone  
7 Einmaliges Ausführen  
8 Netzwerk  
9 Arbeitsgruppe oder Domäne  
10 Betriebssystemoptionen  
11 Bereit zum Abschließen

### Administrator Kennwort

Legen Sie die Optionen für Kennwort und automatische Anmeldung fest.

Kennwort:

Kennwort bestätigen:

Automatisch als Administrator anmelden

Anzahl der automatischen Anmeldeversuche: 2

Anpassung-Win10-AL - Wird bearbeitet

1 Eigenschaften  
2 Registrierungsinformationen  
3 Computername  
4 Windows-Lizenz  
5 Administrator Kennwort  
6 Zeitzone  
7 Einmaliges Ausführen  
8 Netzwerk  
9 Arbeitsgruppe oder Domäne  
10 Betriebssystemoptionen  
11 Bereit zum Abschließen

### Einmaliges Ausführen

Geben Sie die Befehle ein, die bei der Einrichtung ausgeführt werden sollen.

<Einen neuen Befehl eingeben>

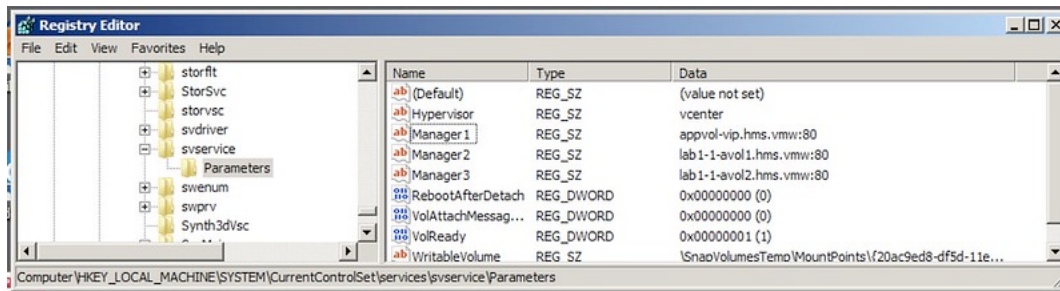
sc config svservice start=auto  
net start svservice

Nach erfolgter Fertigstellung muss der Desktop einmal durchgestartet werden (da der lokale Administrator angemeldet ist).

### 13.7.4 Dem App Volumes Agent weitere App Volumes Manager hinzufügen

Der App Volumes Agent kann mehr als nur einen App Volumes Manager abfragen, falls der bei der Installation angegebene nicht erreichbar ist. Dies geschieht per Registry-Eintrag:

HKLM\System\CurrentControlSet\services\svservice\parameters



### 13.7.5 Replace self-signed certificate

- For the App Volumes Manager, create a valid certificate, signed by your CA. Ensure that the private key is exportable. If the Agent uses a load balancer instead of the App Volume Manager, use the LB FQDN for the CN (common name), and all valid FQDNs as DNS.
- Extract the pfx file via openssl into a crt-file and the key-file
  - Extract the private key
 

```
openssl pkcs12 -in avm01-cert.pfx -nocerts -out avm01-cert-key.key
```

    - You will be prompted for the import password, as well as for the passphrase password to create.
  - Extract the certificate
 

```
openssl pkcs12 -in avm01-cert.pfx -clcerts -out avm01-cert.crt
```

    - You will be asked for the import password, as well as for the passphrase
  - Decrypt the private key
 

```
openssl rsa -in avm01-cert-key.key -out avm01-cert-decrypt.key
```
- On the App Volumes Manager OS, copy the decrypted key file and the crt file into the folder "C:\Program Files (x86)\CloudVolumes\Manager\nginx\conf"
- Modify the nginx.conf in the same folder and edit the ssl\_certificate as well as the ssl\_certificate\_key variables, reflecting the file names for your crt and key file

```
server {
    server_name 0.0.0.0;
    listen 3443 ssl;
    listen [::]:3443 ssl;
    listen 443 ssl;
    listen [::]:443 ssl;

    ssl_certificate avm01-cert.crt;
    ssl_certificate_key avm01-cert-decrypt.key;
    ssl_session_cache builtin:1000;
    ssl_session_timeout 5m;
}
```

- Restart the App Volumes Manager service

## 13.7.6 Establish a multi-instance architecture

Verion: 2503

To ensure replication of packages, markers and assignments between site, multi-instance architecture can be established. You can add multiple target instances to a given source instance.

### 13.7.6.1. Add instance target

- On source App Volumes Manager, go to →Infrastructure →Instances, and click to “Add Target”:

The screenshot shows the 'Add App Volumes Instance Target' form. At the top, there are tabs for 'Machines', 'Storages', 'Storage Groups', and 'Instances'. The form title is 'Add App Volumes Instance Target' with a subtitle 'Add App Volumes instance target to keep application data and assignments synchronized'. The form fields are: 'Secure Address' (text input with 'avm02.euclab.org'), 'Username' (text input with 'administrator'), 'Password' (password input with masked characters), 'Domain' (dropdown menu with 'EUCLAB'), 'Application Package Import' (checkbox checked), 'Package Symmetry Assurance' (checkbox checked), 'Synchronize Markers' (checkbox checked), and 'Synchronize Assignments' (checkbox checked). At the bottom, there are 'SAVE' and 'CANCEL' buttons.

- Keep in mind, that synchronization between source and target is unidirectional. Synchronization takes place from Source to Target only.
- After adding the target, you can verify the configuration on both instances:
  - Source:

The screenshot shows the 'Instance Details' page for AVM01. It includes fields for Name, URL, GUID, and Created. Below, there is a 'Related Instance' section with a table showing the configuration of the target instance AVM02.

Name	Host	Type	Status	Last Synchronized
> AVM02	avm02.euclab.org:443	Target	Active	0 Never

- Target:

**Instance Details** EDIT

Name: AVM02  
 URL: https://AVM02.euclab.org:443  
 GUID: 83877bba-8c0a-4ea8-a258-0dacfc12970f  
 Created: Jul 24 2024

**Related Instance**

Show 10 ↻ Filter

Name	Host	Type	Status	↻	Last Synchronized	☐
> AVM01	AVM01.euclab.org:443	Source	Active	0	Never	☐

Showing 1 to 1 of 1 Instances First Previous 1 Next Last

### 13.7.6.2. Setup package replication

You need a shared NFS datastore to replicate packages between sites and App Volumes instances.

- Set the shared NFS datastore for replication as **non-attachable** under →Infrastructure →Storages, so packages can be replicated to and from this datastore, but prevents packages being mounted from this datastore. Repeat this step for all App Volumes instances.
- Mark the NFS datastore for replication as **read-only** for the target App Volumes instance
- Create a Storage Group under →Infrastructure →Storage Groups for the source as well as for the target App Volumes Manager
  - Select the “local default datastore” and the NFS datastore used for replication
  - **Do not select “Automatically Import Application Packages”!**
  - Select “Automatically Replicate Application Packages”

**Create Storage Group**

You can directly choose storage to be included or specify a name prefix so new matching storage is automatically added.

Group Name:

**Application Packages**

Automation:

- Automatically Import Application Packages (?)
- Automatically Replicate Application Packages (?)

Stages to Replicate:

- All (?)
- New
- Tested
- Published
- Retired

**Writable Volumes**

Distribution Strategy:  (?)

Template Storage:

**Storage**

Selection Method:

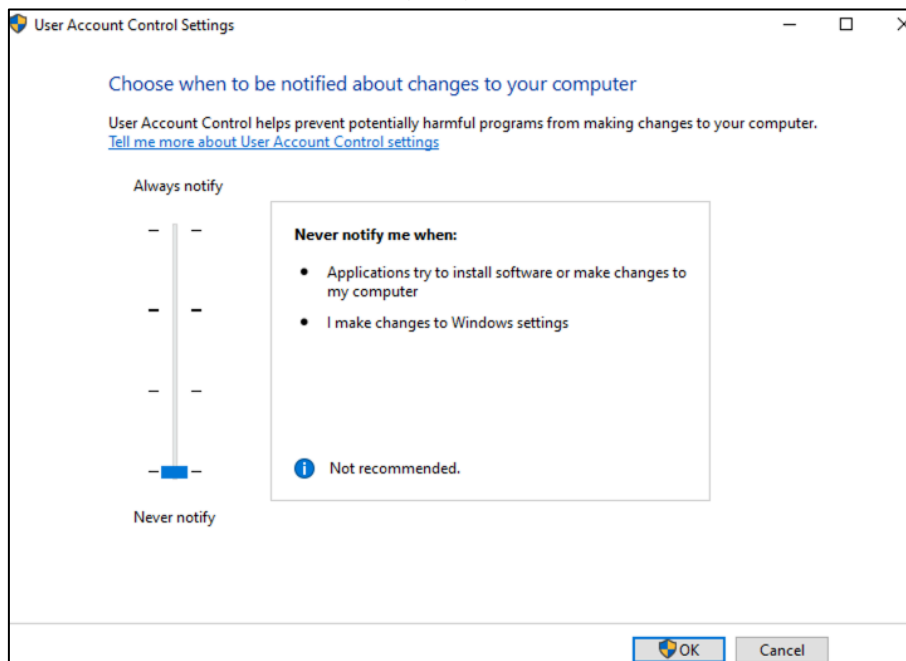
## 13.8 App Volumes Tools

### 13.8.1 Setup App Volumes Tools

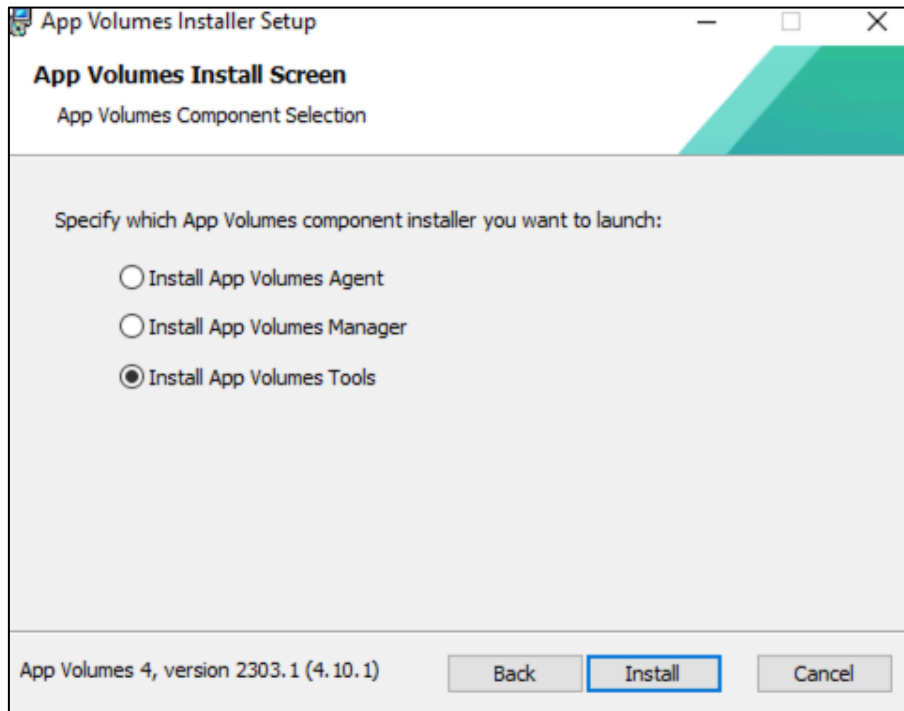
To use automation in conjunction with application package deployment, you can use the App Volumes Tools, released in version 2103.

You can install them on a clean Windows Desktop OS machine – verify that no other App Volumes component is installed.

- Execute VMware OS Optimization Tool
- Deactivate User Account Control (UAC):



- Execute the installation process, and choose the App Volumes Tools:



- Take an offline snapshot, you can revert after every capture process.

<https://roderikdeblock.com/automate-the-complete-capturing-process-using-app-volumes-tools/>

## 13.8.2 Capture an application

- Place the application you want to setup, into a local install folder

## 13.9 Troubleshooting App Volumes

### 13.9.1 Replacing/Restoring a single Manager with external SQL DB

In case of loss of a single App Volumes Manager with an external SQL DB (DB backup available), you can install a fresh App Volumes Manager, and connect this with the existing SQL DB.

During first login to the UI the wizzard asks for registration of App Volumes Manager – however, there is no additional manager who can execute this:

### Register App Volumes Manager Server

The current App Volumes Manager server is unregistered. Please specify the address of a registered App Volumes Manager server and login credentials.

Registered Manager Address:  (?)

Username:

Password:

Domain:  ▼

Workaround:

- Stop App Volumes Manager Service
- Login to the SQL server, load the SQL server Management Studio and navigate to the table **dbo.manager\_services**
- Delete the entry from the already registered App Volumes Manager
- Once the entry is deleted restart the AVM service and test accessing the AVM console again
- You have to check (or re-enter) license details, AD connectivity, vCenter connectivity

### 13.9.2 After update, Admin UI is failing

In some cases, after upgrading an App Volumes Manager, the Admin UI is failing (getting timeout). However, the upgrade finished successful, and the App Volumes Manager service is up and running.

- In svmanager\_server.log, you find an antry like this:
  - `nginx: [emerg] unknown directive "ssl" in C:\Program Files (x86)\CloudVolumes\Manager\nginx/conf/nginx.conf:`
- After the update, check the nginx.conf file, located here:  
C:\Program Files (x86)\CloudVolumes\Manager\nginx\conf\
- Edit the nginx.conf
  - Change "listen 443;" to "listen 443 ssl;" in server configuration
  - Comment out "ssl on;" by keeping "#" at the stating of the line (#ssl on;)
- Restart of the App Volumes Manager service not needed, but recommended

### 13.9.3 Omnissa App Volumes order of operation

Detailed explanation about the order of operation for App Volumes Manager, as well as for the User logon: [KB2143163](#)

## 14. Setup Dynamic Environment Manager

We are using the AD mode.

### 14.1 Prepare Environment for DEM

#### 14.1.1 Create File Shares

We need the following shares for DEM:

- DEM Configuration Share (i.e. \\FS\DEMconfig)
  - Share permissions – **Everyone** must have **Change** permissions
  - NTFS Security permissions
    - Administrators must have **Full Control** permissions applied to **This folder, subfolders and files**
    - End users must have **Read & execute** permissions applied to **This folder, subfolders and files**
    - (optional) If you want to use DEM also for computer environment settings, remote computer accounts must also have **Read & execute** permissions applied to **This folder, subfolders and files**
- DEM Profile Archives Share (i.e. \\FS\DEMprofiles) for storing personal (application-)settings
  - Share permissions - **Everyone** must have **Change** permissions
    - (optional) Helpdesk staff using the optional Helpdesk Support Tool must have **Full Control** permissions applied
  - NTFS Security permissions – for each user at his first login an own folder has to be created, and the user can use his own folder only
    - For Administrators and Helpdesk Staff, **Full Control** applied to **This folder, subfolders and files**
    - For End users: **Create folders / append data** applied to **This folder only**
    - (optional) If you want to use DEM also for computer environment settings, remote computer accounts must also have **Create folders / append data** permissions applied to **This folder only**
    - For **Creator Owner: Full Control** applied to **Subfolders and files only**
- (optional) DEM User Share (i.e. \\FS\userdata) for roaming user profile (partial or complete)

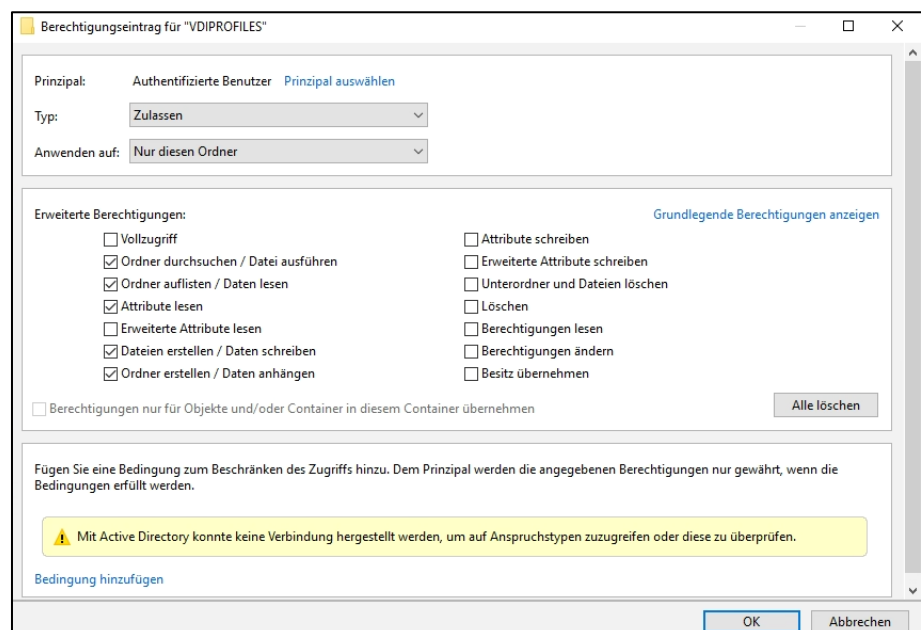
## 14.1.2 Import ADMX Templates for DEM

Add the DEM specific ADMX templates to the GPO environment

- Copy the .admx files to the %systemroot%\PolicyDefinitions folder on your Active Directory server.
- Copy the language resource (.adml) files from subfolder en-US (or different language folder) to the appropriate subfolder in %systemroot%\PolicyDefinitions\ on your Active Directory server.

## 14.2 File Shares anlegen

- \\FS\DEMConfig - Share für die DEM Konfiguration
  - NTFS Security Berechtigungen:
    - Administrators must have full permissions
    - End users must have Read and Execute permissions
  - Falls Computer-based ADMX Settings konfiguriert werden sollen, müssen "Domain Computers" Read Permission haben auf dem Config Share
- \\FS\DEMprofiles - Share für die user-spezifischen Applikationseinstellungen
  - For the share the **Everyone** group must have **Change** permissions applied
  - NTFS Security Berechtigungen:
    - For DEM Admins and Help Desk: Full control, applied to this folder, sub folders and files
    - For End Users: Create folders and append data, applied to this folder only **AND read and execute to this folder only**
    - For Creator owner: Full control, applied to sub folders and files only
- \\FS\DEMuserdata - Share für Profil-Umleitungen (optional)
  - NTFS Security Berechtigungen:
    - For authenticated users:

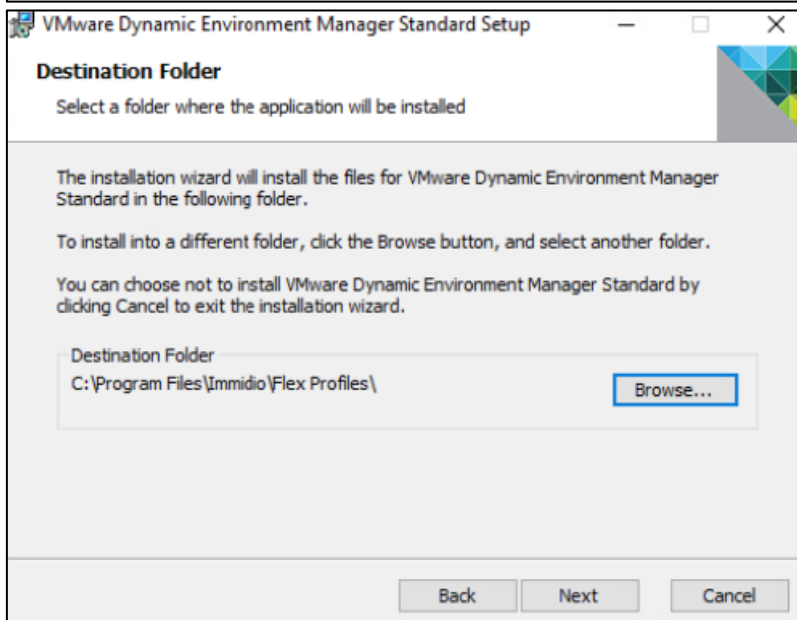
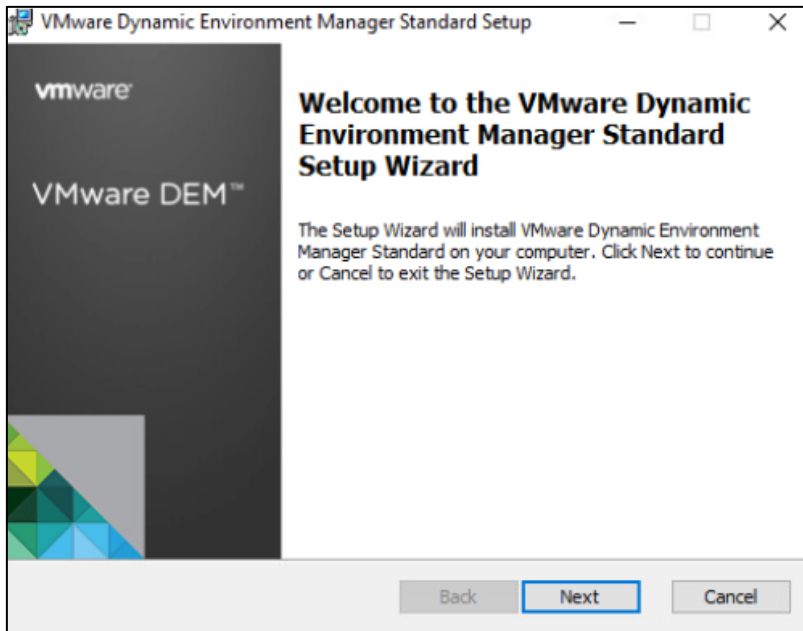


- For DEM Admins: Full control, applied to this folder, sub folders and files
- For End Users: Read and execute, Create Folders, to this folder only
- For Creator owner: Full control, applied to sub folders and files only

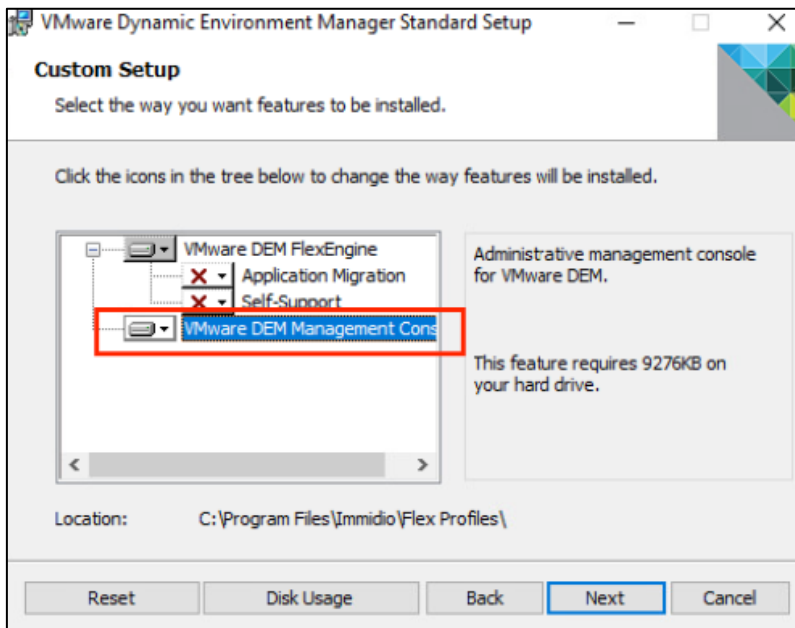
## 14.3 Setup DEM Management Console

Version 2312.

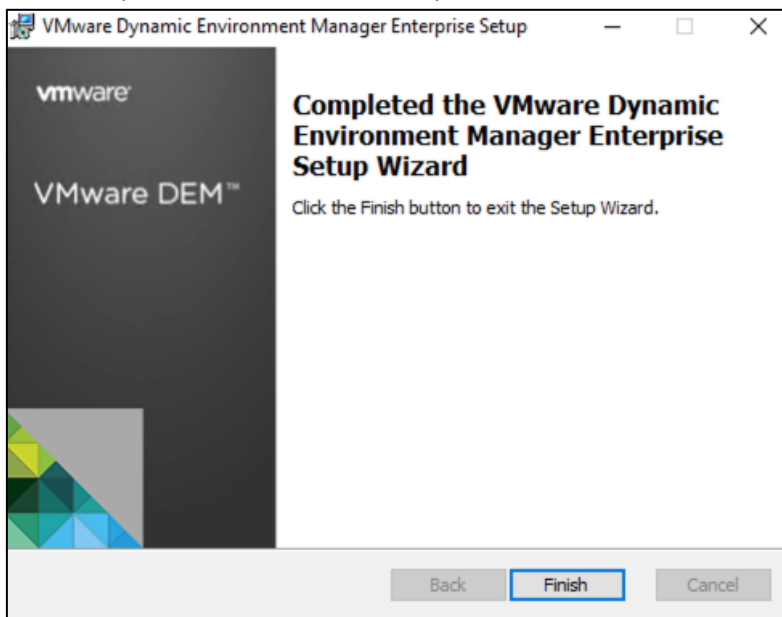
- Execute setup:



- Choose custom setup, then activate the DEM Management Console, and deactivate the DEM FlexEngine:



- Start setup, takes a few seconds only:

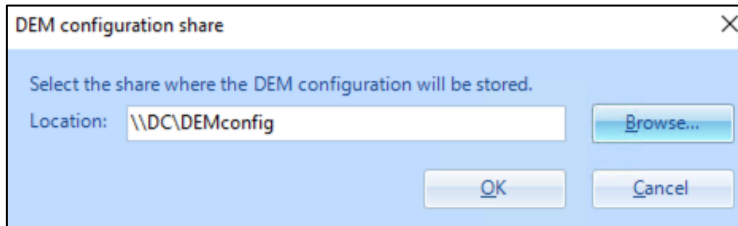


## 14.4 Initial DEM Configuration

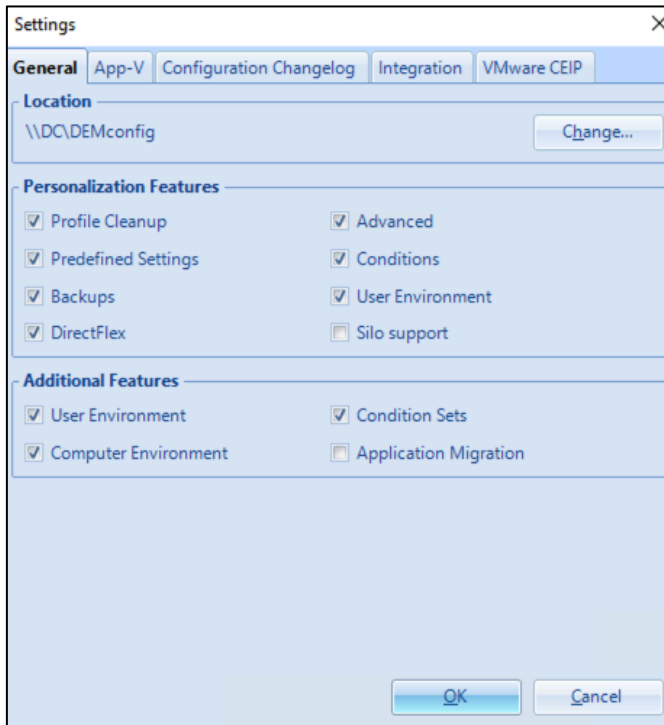
### 14.4.1 Initial configuration DEM Management Console

- Start DEM Management Console – at first start, you can (optional) activate Workspace ONE UEM integration. This can be configured later.

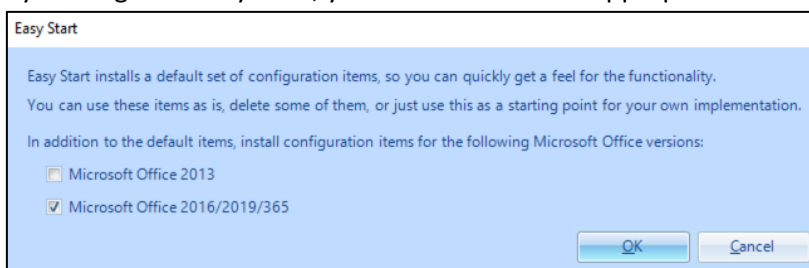
- Configure DEM configuration share



- Under →Configure →Settings, you should configure general DEM features



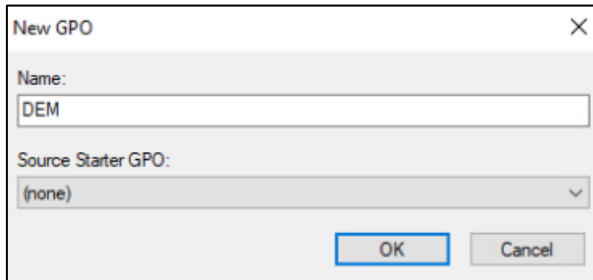
- By clicking to →Easy Start, you should choose an appropriate set of configuration items



## 14.4.2 Minimum required GPOs for DEM

Some requirements have to be configured in minimum.

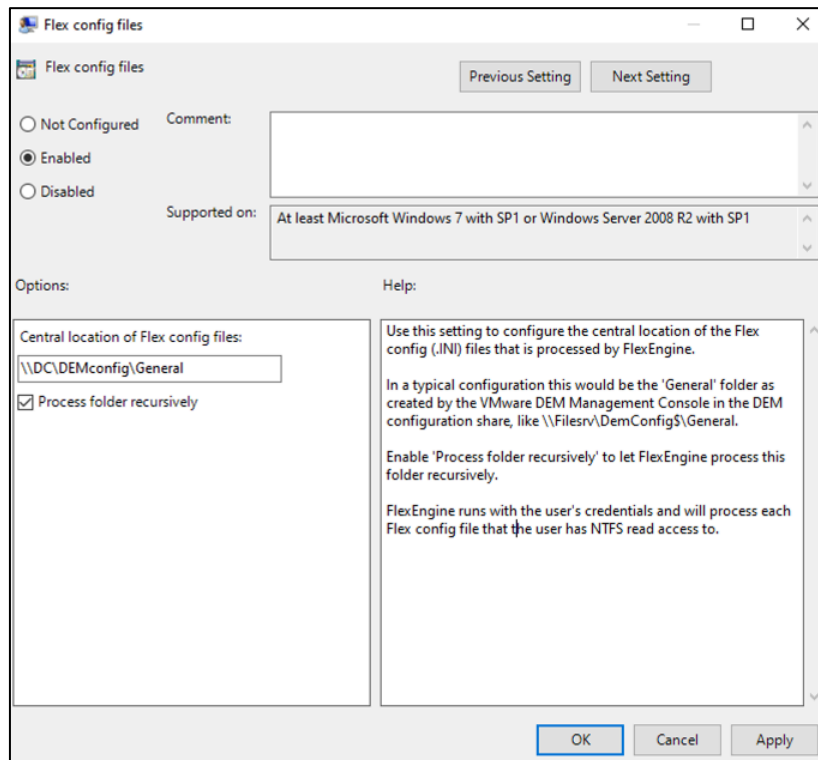
- Create a new GPO for DEM:



This GPO will be applied for the OU which is used by DEM-Users. That means here are User Configuration settings applied. Is there a need for Computer Configuration settings (i.e. RDSH farms), it is mandatory to enable loopback processing (described later).

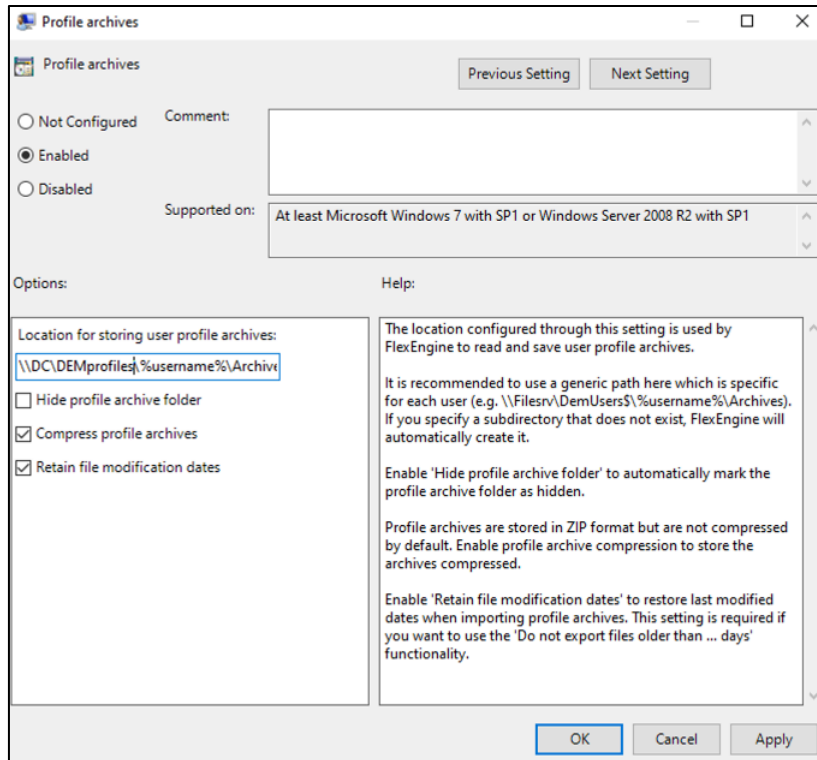
- Edit the new GPO and switch to →User Configuration →Policies →Administrative Templates →VMware DEM →FlexEngine

- **Flex config files**



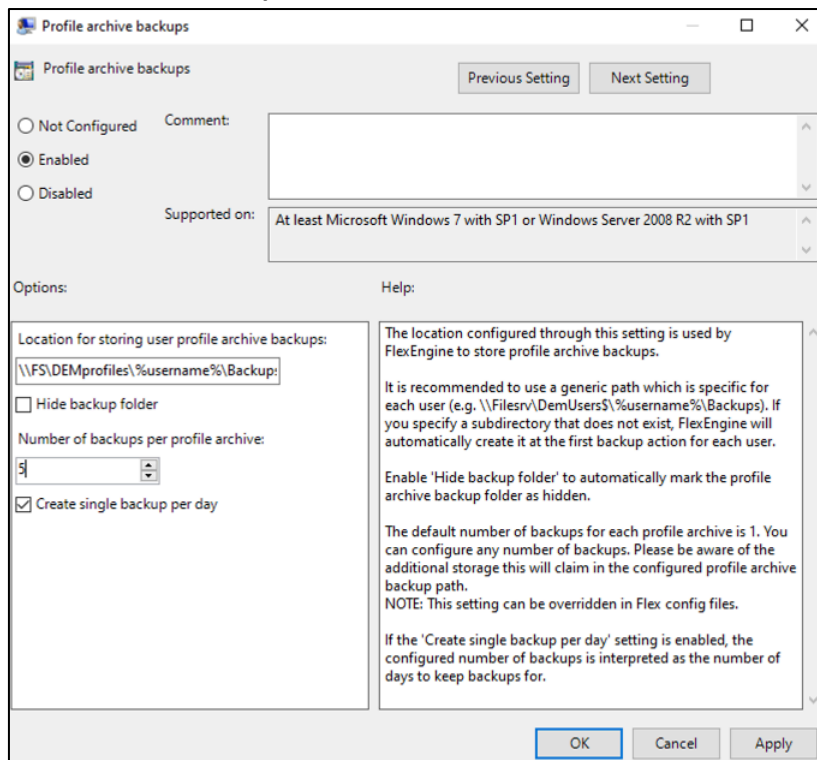
- Enabled
- Central location of Flex config files: \\FS\DEMConfig\General
- Check mark for “Process folder recursively”

○ **Profile archives**



- Enabled
- Location for storing user profile archives:  
\\FS\DEMprofiles\%username%\archives
- Check mark for “Compress profile archives” and for „Retain file modification dates“

○ **Profile archive backups**

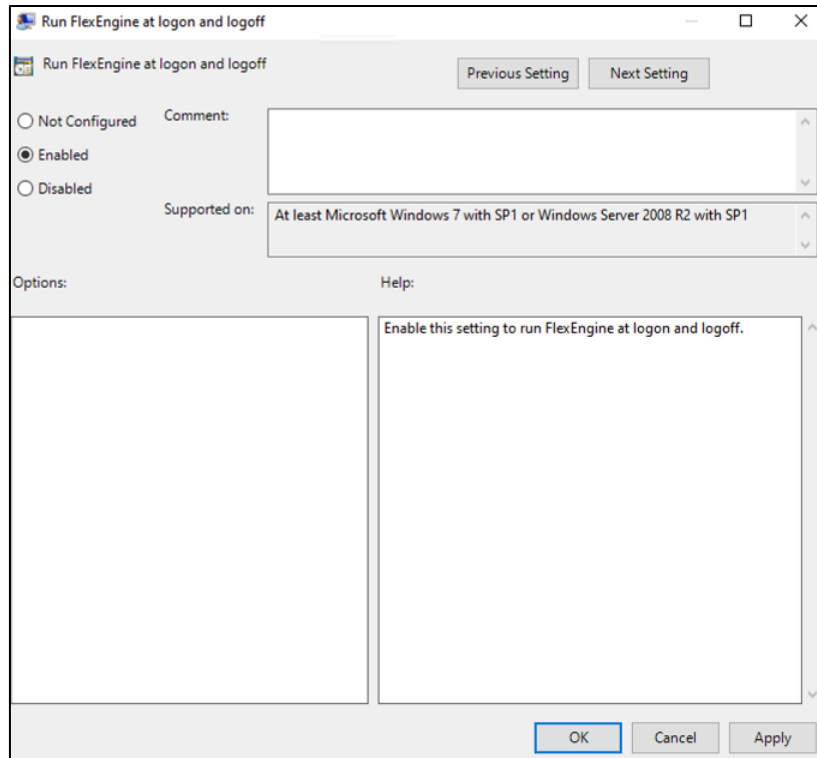


- Enabled
- Location for storing user profile archive backups:  
\\FS\DEMprofiles\%username%\backups
- Number of backups per profile archive
- Check mark for “Create single backup per day”

○ **FlexEngine logging**

- Enabled
- Path and file name of log file:  
\\FS\DEMprofiles\%username%\Logs\FlexEngine.log
- Log level: Warn (Debug for PoC)
- Maximum log file size in kB: 512

- **Run FlexEngine at logon and logoff**



- Enabled
  - **This GPO is recommended to enable since DEM 2111.**
  - For DEM settings until 2106, see [here](#).
- If you need to manage **computer objects** in OUs, you need to switch to →Computer Configuration →Policies →Administrative Templates →System →Group Policy, and set **Configure user Group Policy loopback processing mode** to “Enabled”
  - In case you want to implement DEM with computer environment settings, you should configure a registry setting to make the DEM configuration path available for the computer object.
    - See official documentation [here](#).

### 14.4.3 Additional (optional) configuration

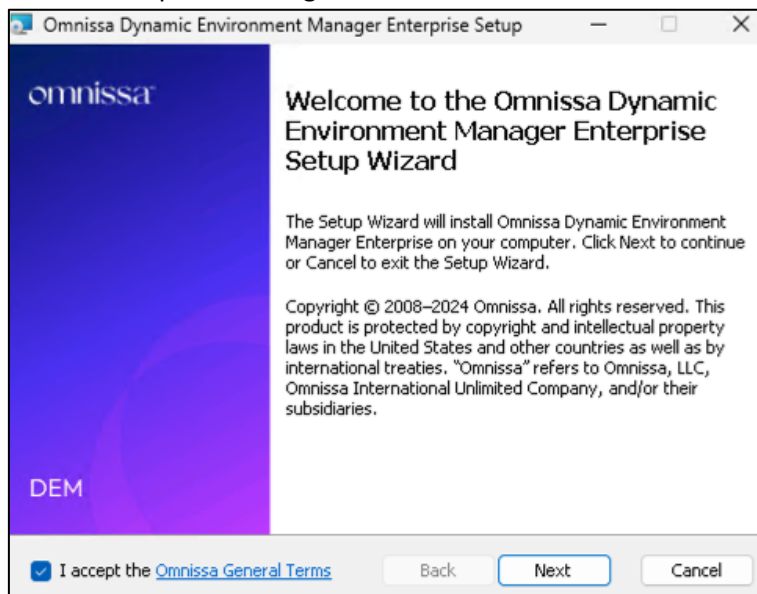
Depending from the use case, you can edit or add specific configuration options:

- **File Type Associations**
  - <https://ivandemes.com/managing-file-type-associations-fta-natively-using-dynamic-environment-manager/>
  - <https://kb.vmware.com/s/article/83679>
- **Available Application Templates**

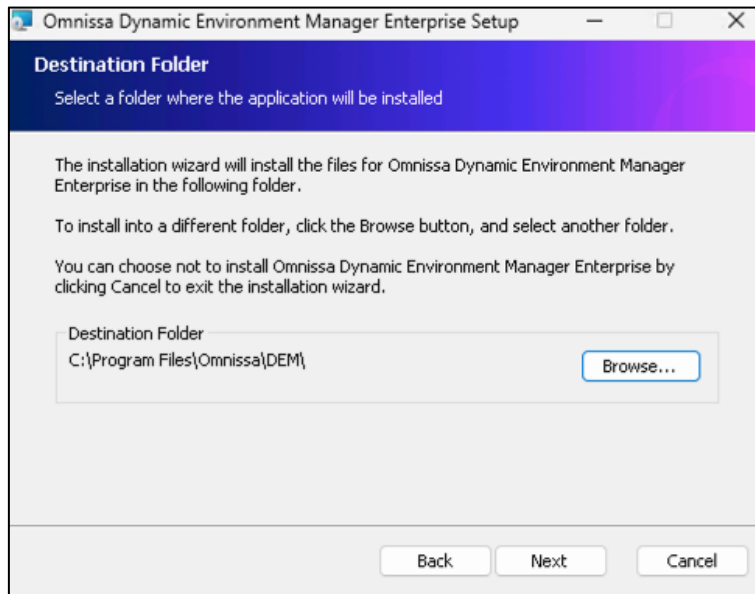
- <https://ivandemes.com/vmware-uem-9-5-introduces-the-vmware-marketplace-for-templates/>
  - <https://www.ivandemes.com/uemtemplates/alluemtemplates.php>
  - <https://communities.vmware.com/t5/Dynamic-Environment-Manager/tkb-p/3026>
- **Predefined Settings**
    - <http://vlenzker.net/2016/12/vmware-uem-predefined-settings-basic-concepts/>

## 14.5 Setup DEM Agent

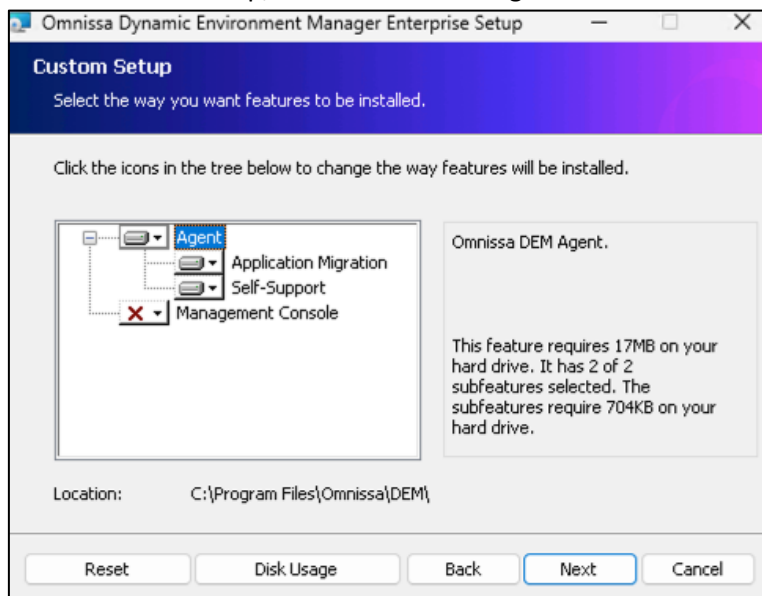
- Execute setup for DEM Agent:



- Select default destination folder

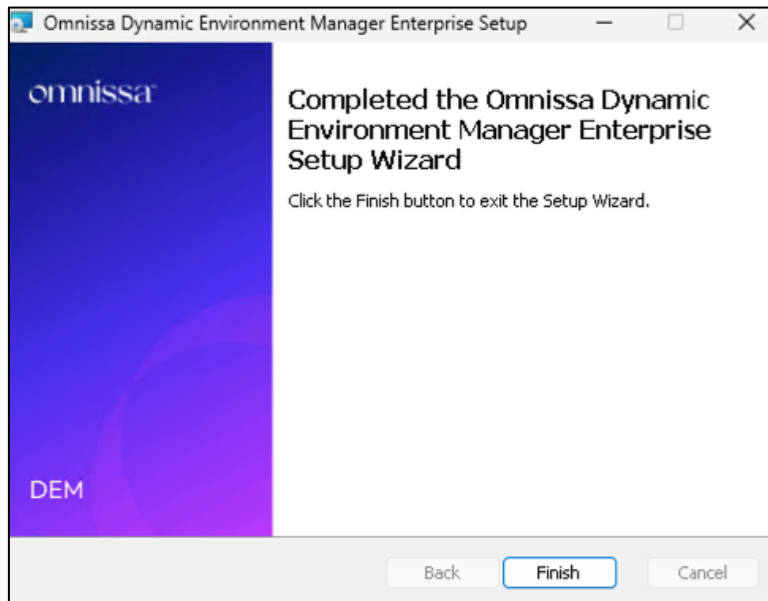


- Choose custom setup, and confirm DEM Agent



- Proceed with installation. As long as the Horizon agent is installed already on this machine, no specific DEM license is needed.

- Setup takes a few seconds only



## 14.6 DEM Application Profiler

Version 2506

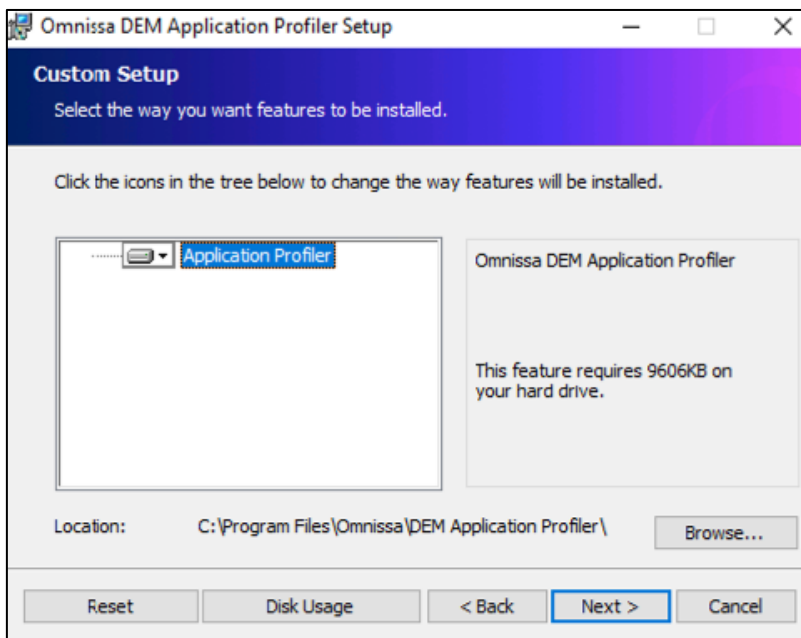
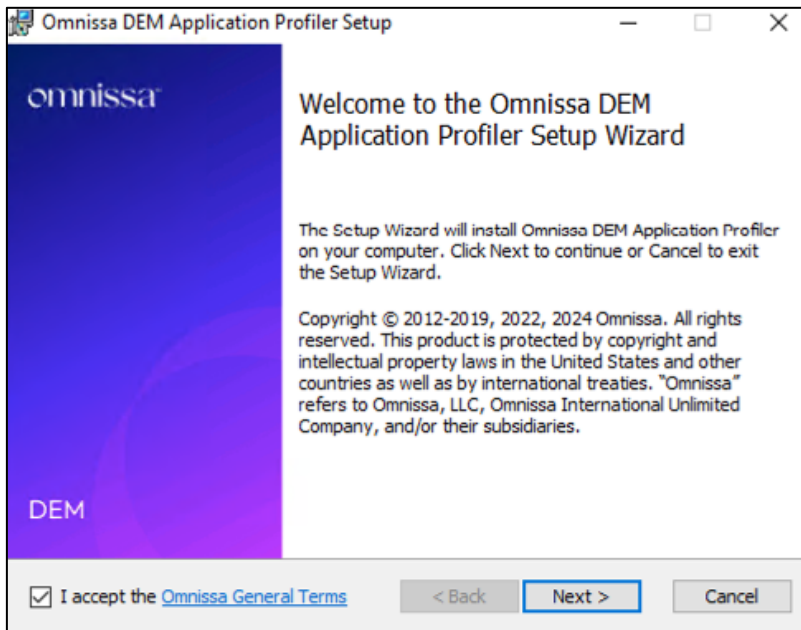
If you have to create profiles for applications which are not “known” by DEM (or a template isn’t present already), you can use the Application Profiler to create application profiles.

### 14.6.1 Requirements

- Use an OS which is similar (or identical) to the environment in which the applications will take place (or the DEM agent will be deployed)
- Use a dedicated VM, without DEM Agent installed.

### 14.6.2 Setup Application Profiler

- Run the installer - VMware DEM Application Profiler xxxx 10.xx x64.msi (part of the download for DEM)

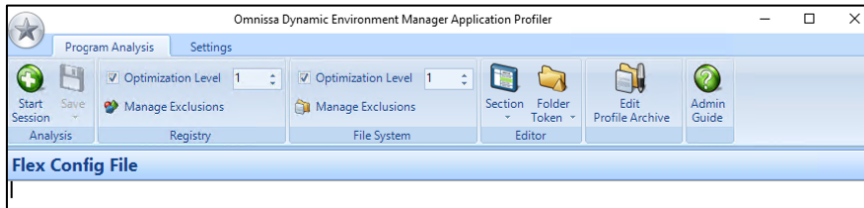


- Create a final snapshot you can revert to, after a new application was profiled.

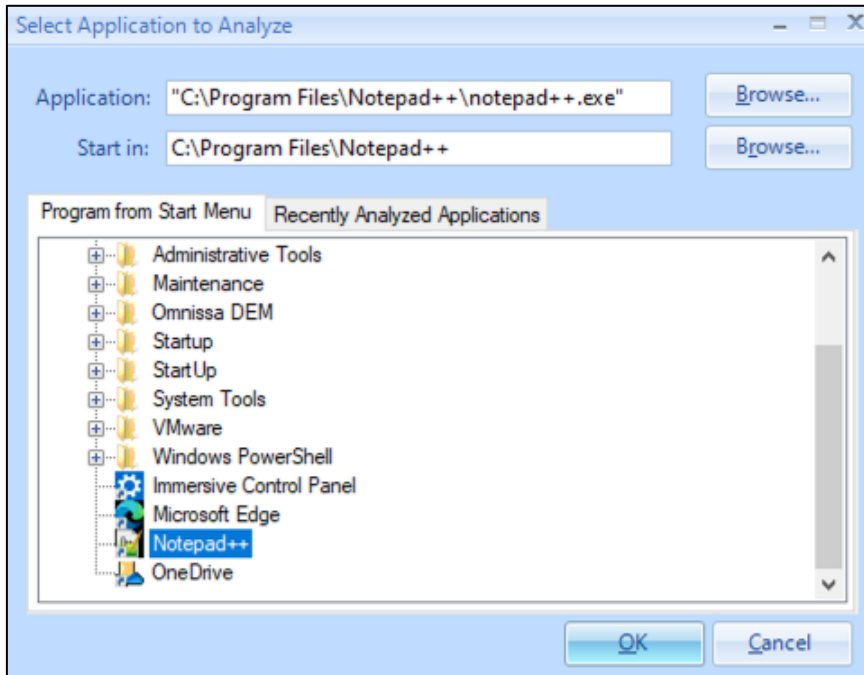
### 14.6.3 Using Application Profiler

- Consider to have a snapshot before installation and profiling, to keep a clean machine you can revert to.
- Install the application which should be profiled (i.e. FormatFactory, PDF24)

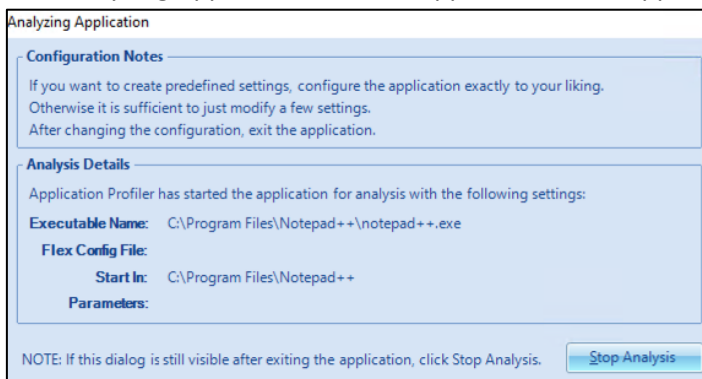
- Start Application Profiler



- Click →Start Session. Browse to the Application you want to profile

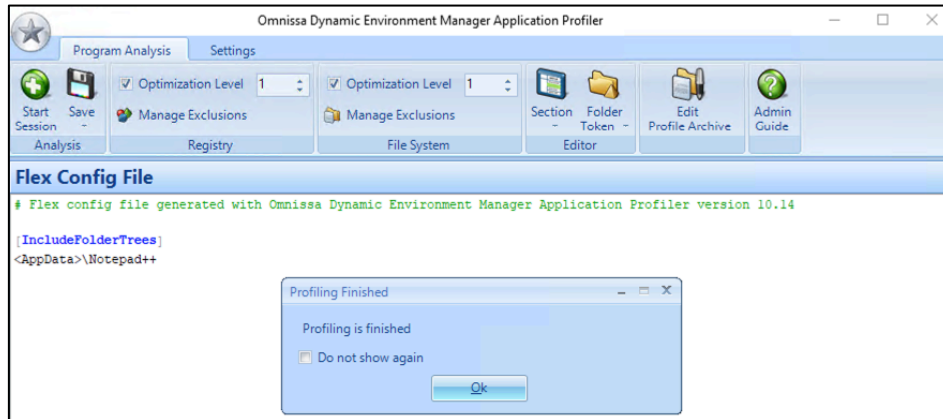


- The Analyzing Application window appears, and the application starts

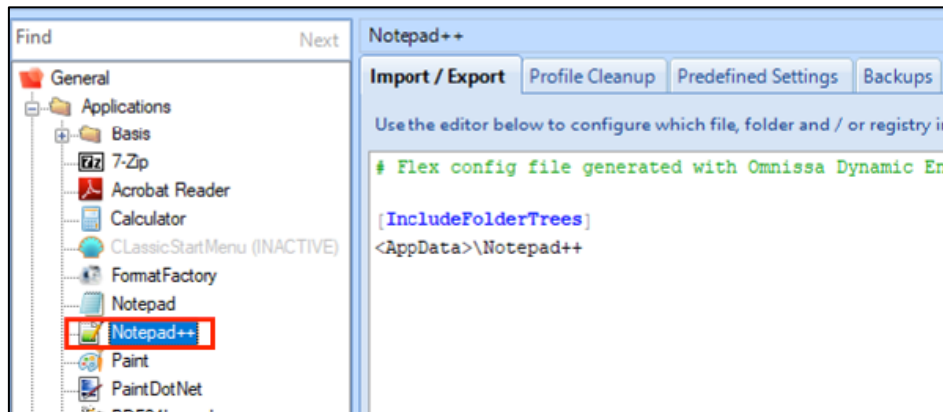


- Make the necessary changes within the application, then exit the application

- The Application Profiler UI shows the results of the analysis



- Click on →Save to save the Config File. You also can save config file with predefined settings (or predefined settings only).
- Copy the created files to the DEM Config Folder for Applications, after a tree refresh you will see it in UI



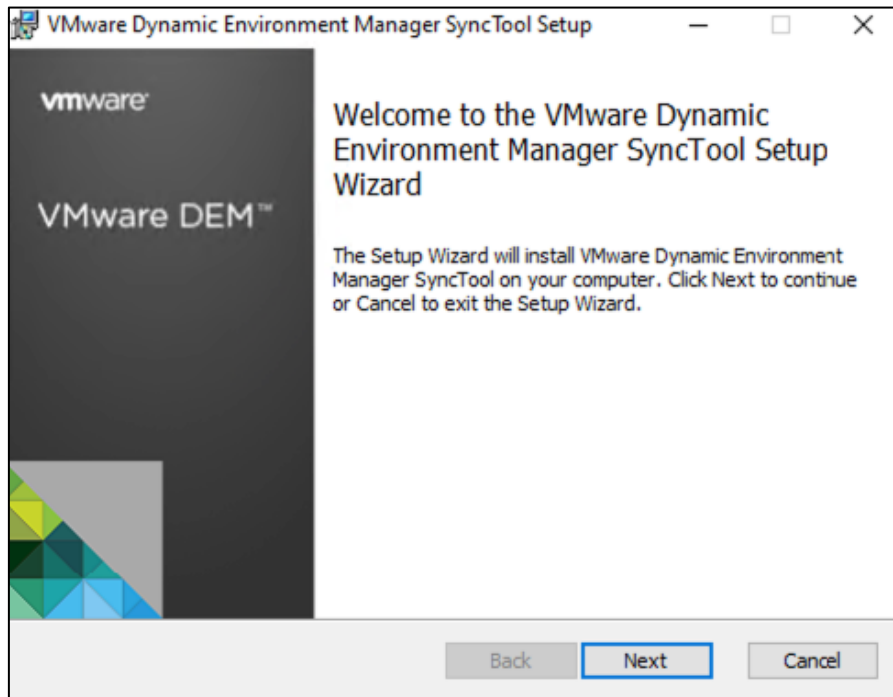
## 14.7 DEM Sync-Tool

In an existing DEM configuration, the Sync-Tool can be installed as an additional DEM feature on the same machine as the FlexEngine (DEM Agent).

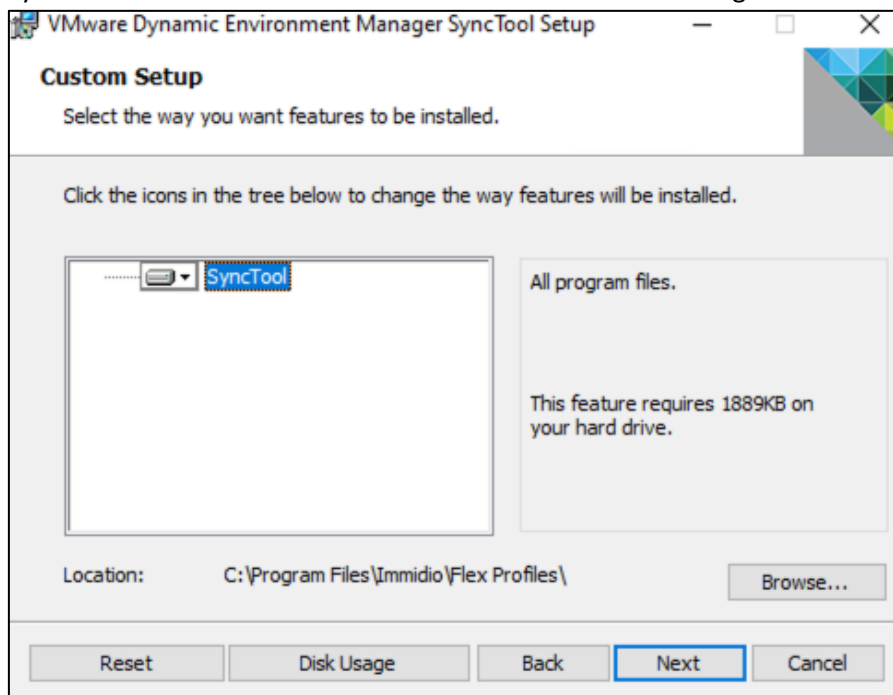
Syn-Tool offers to sync the DEM configuration itself, but also the User DEM-Profiles (Application Settings) for Offline-Usage.

### 14.7.1 Setup Sync-Tool

- Execute installer file



- Sync-Tool has to be installed in the same folder as the FlexEngine



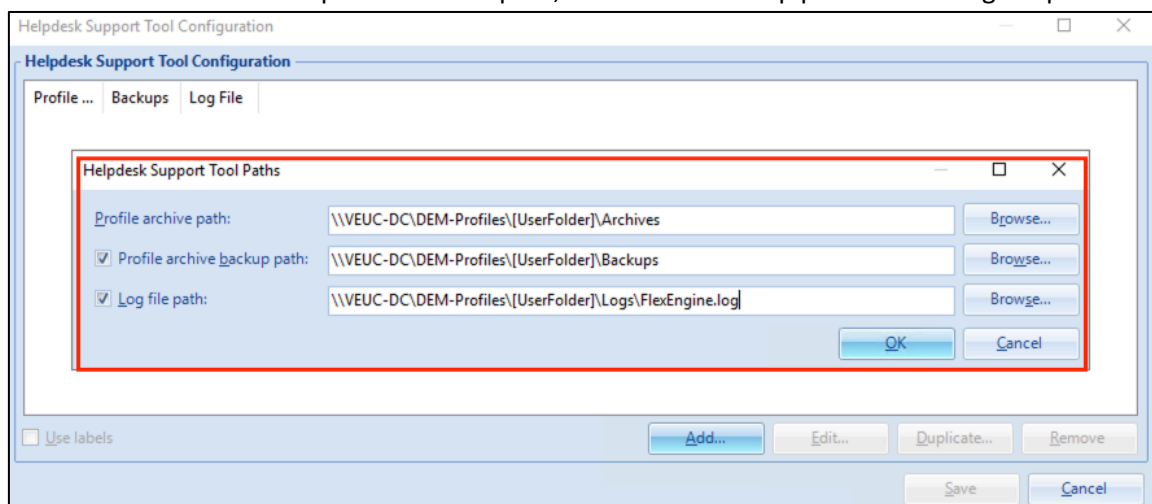
## 14.7.2 Configuring Sync-Tool

- Administrative Templates “VMware DEM.admx” and “VMware DEM SyncTool.admx” have to be copied in the PolicyDefinitions Folder (C:\Windows\PolicyDefinitions) on domain controller, if they do not exist already.
- You can use the existing GPO for DEM, or create a dedicated one for Sync-Tool. If Sync-Tool is not installed on the target VM (Golden Master), Sync-Tool GPO settings are ignored. So it can be used in parallel within one GPO.
- (optional) you have to set up a license file in DEM Management Console, if Horizon Agent is not in place on the machine the Sync tool is installed.

## 14.8 DEM Helpdesk Support Tool

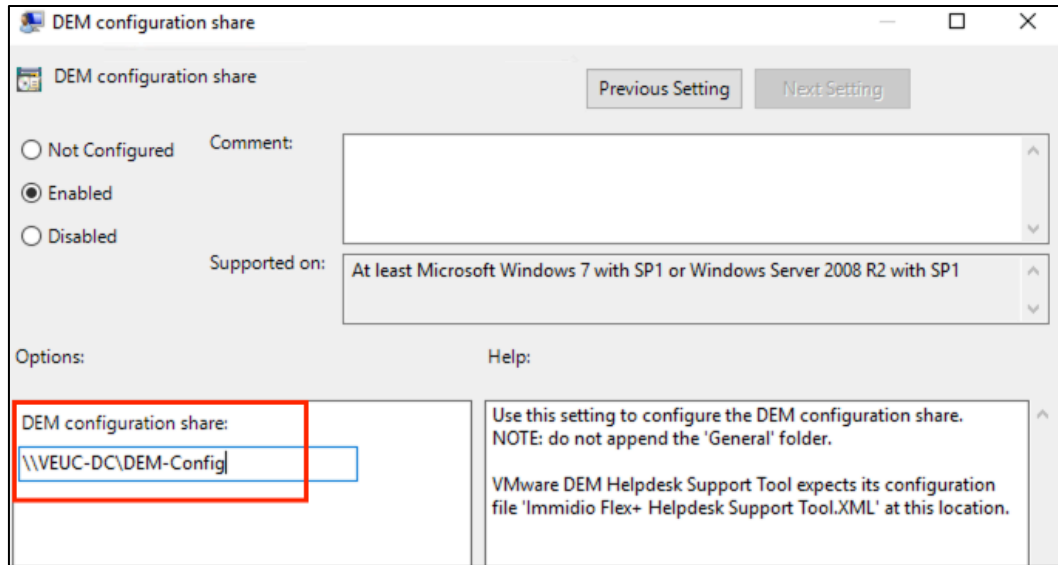
### 14.8.1 Configuring Helpdesk Support Tool

- Start DEM Management Console, and go to →Star →Configure Helpdesk Support Tool
- Click →Add and enter the profile archive path, the archive backup path and the log file path

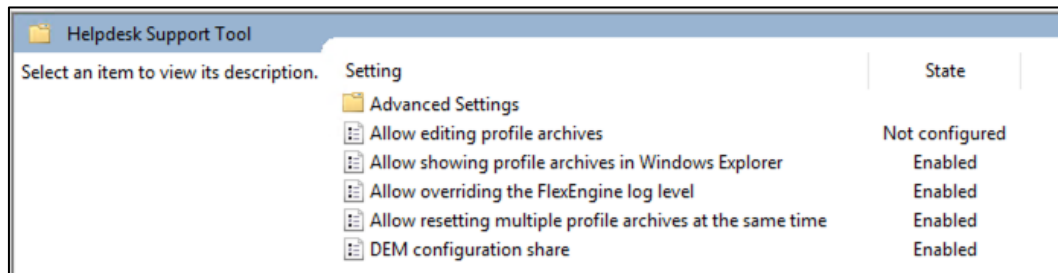


- In case of users which are distributed across different file servers, you can configure multiple UNC paths, using (creating) a Immidio Flex+ Helpdesk Support Tool.xml file. Also you can use multiple Labels to organize and manage different locations.
- After click on →OK, in the DEM-Config share the config file “Immidio Flex+ Helpdesk Support Tool.xml” will be created.
- Create dedicated GPO for Helpdesk Account(s), using administrative Template under →User Configuration\Administrative Templates\VMware DEM\Helpdesk Support Tool.

- DEM configuration share – the share to the previously created xml config file

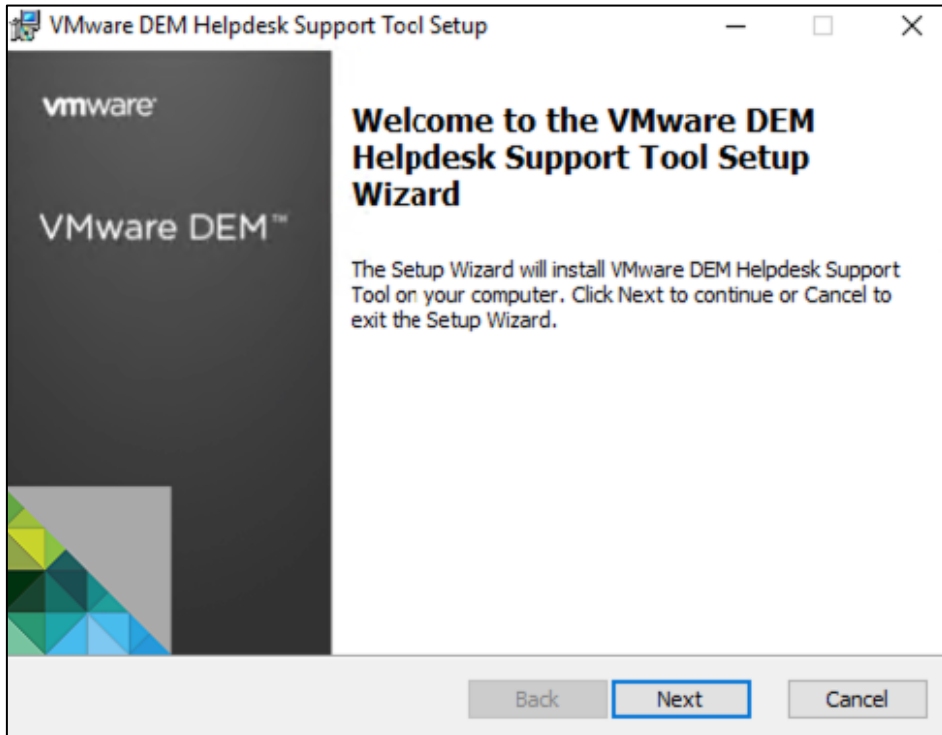


- As an example, you can configure these setting as default, see doc [here](#):

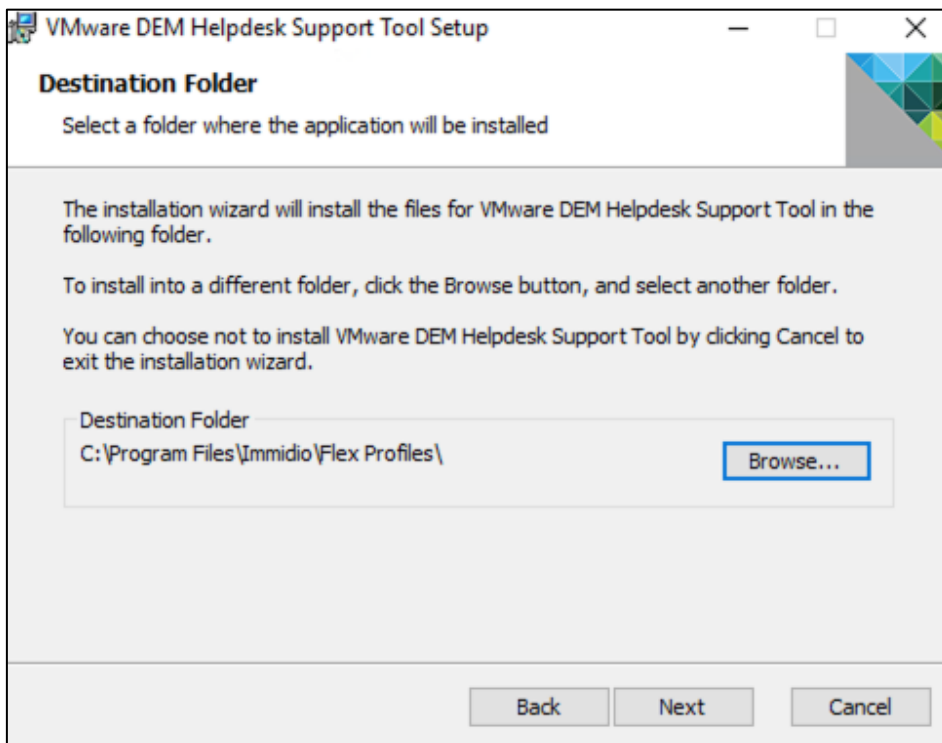


## 14.8.2 Setup Helpdesk Tool

- Execute the Helpdesk-Installer on a dedicated machine

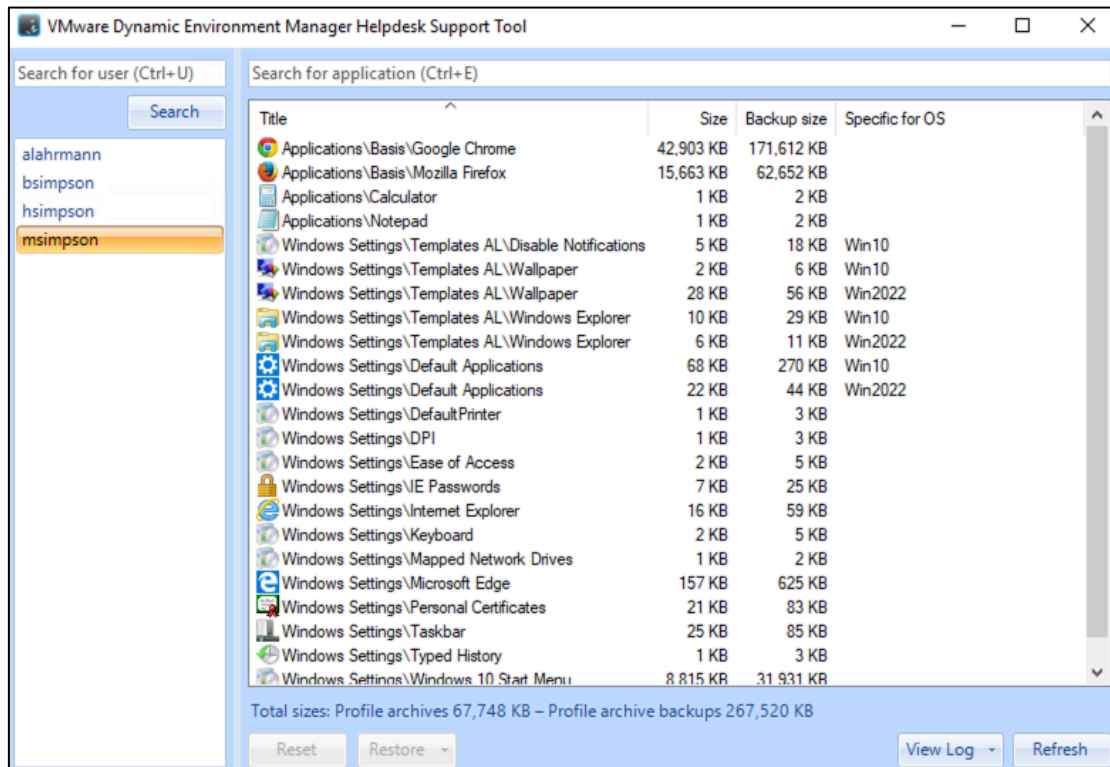


- Use default installation folder



### 14.8.3 Using Helpdesk Tool

- Start → Helpdesk Support Tool, and enter (partially) username in the search field



## 14.9 DEM – Appendix and Issues

### 14.9.1 MS Edge Settings

[IncludeRegistryTrees]

HKCU\Software\Microsoft\Edge

[IncludeFiles]

<LocalAppData>\Microsoft\Edge\User Data\First Run

<LocalAppData>\Microsoft\Edge\User Data\Local State

<AppData>\Microsoft\Edge\User Data\Default\profile.pb

[IncludeFolderTrees]

<LocalAppData>\Microsoft\Edge\User Data\Default

[ExcludeFolderTrees]

<LocalAppData>\Microsoft\Edge\User Data\Default\Cache

<LocalAppData>\Microsoft\Edge\User Data\Default\Code Cache

<LocalAppData>\Microsoft\Edge\User Data\Default\GPUCache

<LocalAppData>\Microsoft\Edge\User Data\Default\IndexedDB

<LocalAppData>\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage

<LocalAppData>\Microsoft\Edge\User Data\Default\Service Worker\ScriptCache

## 14.9.2 Sonstiges

Roaming “nicht-typischer” Ordner auf LW C:

Import/Export

<C-Drive>\ProgramData\CSP client.components Windows\%username%\set\[EXPAND ENV VARS]

<https://docs.vmware.com/en/VMware-Dynamic-Environment-Manager/2106/com.vmware.dynamic.environment.manager-adminguide/GUID-537E02E3-4814-42F9-8D0F-0418D76DD84D.html>

## 14.9.3 Template for Windows Settings (Default)

Saved under \Documents\VMware Horizon\DEM\DEM-Windows-Settings-Templates.zip

Already present, but expanded:

- Personal Certificates
- Screensaver (if not disabled by OSOT)

Windows Common Setting (Expanded)

- DPI
- DefaultPrinter (divergent from default expansion)
- Keyboard
- Mapped Network Drives
- Mouse
- Taskbar
- Typed History – history for IE and Windows Explorer

Customized

- Cookies
- Credentials Manager - saves credentials for network drives
- Window Colors - Saves individual window colors

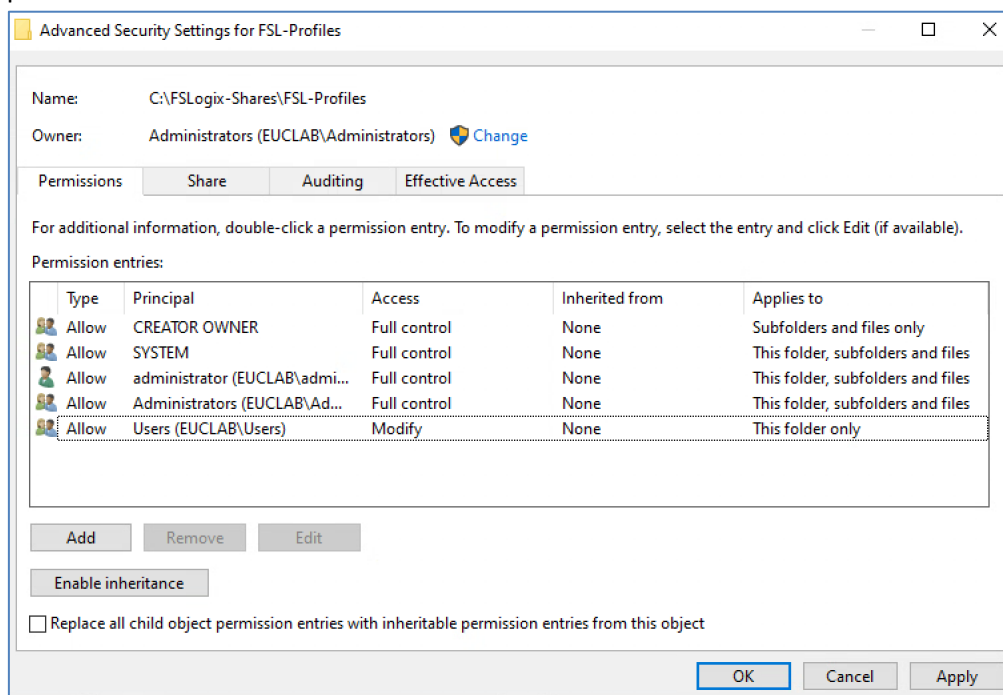
- Jump List - Saves preview for task list and startmenu for the recently used docs, files etc.
- Num Lock Status – saves num lock status
- Startup – roaming for startup folder
- VisualEffects
- Wallpaper
- Windows Explorer
- EdgeChromium
- Disable Notifications

## 15. Microsoft FSLogix

Version 25.09 (3.25.822.19044)

### 15.1 Preparation

- Configure a SMB-Share to store the FSLogix VHD(X) files for the users, and add needed permissions:



**Tabelle 1: The table outlines the recommended ACL(s) to be configured.**

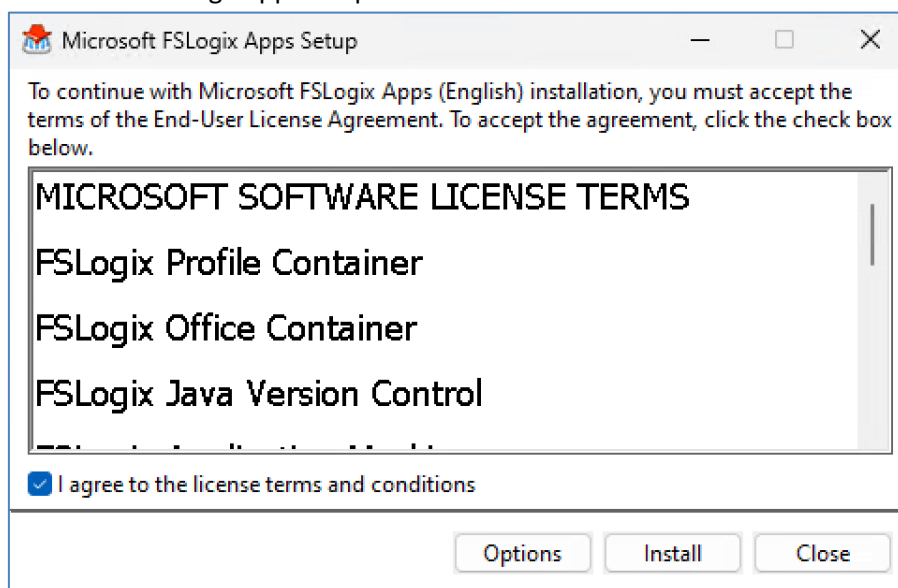
Principal	Access	Applies to	Description
-----------	--------	------------	-------------

CREATOR OWNER	Modify (Read / Write)	Subfolders and files only	Ensures the profile directory created by the user has the correct permissions only for that user.
EUCLAB\Domain Admins	Full Control	This folder, subfolders and files	Replace with your organizations group used for administrative purposes.
EUCLAB\Domain Users	Modify (Read / Write)	This folder only	Enables authorized users to create their profile directory. Replace with organizational users who need access to create profiles.

- Copy the GPO Templates into the appropriate folder
  - fslogix.admx to %systemroot%\policyDefinitions
  - fslogix.adml to %systemroot%\policyDefinitions\en-us

## 15.2 Setup FSLogix Agent

- Execute the FSLogixAppsSetup.exe



## 15.3 FSLogix GPO-Configuration

- FSLogix is managed via **Computer-GPO** under →Computer Configuration then →Administrative Templates then →FSLogix
- **Important:** Group Policy settings stored under HKEY\_LOCAL\_MACHINE\SOFTWARE\FSLogix are considered preferences and NOT policies. This means that if a Group Policy is either removed or the setting is changed to Not Configured, the registry setting will remain on the virtual machine.  
This primarily affects settings related to Apps, Logging and Profiles. ODFC settings are located under HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\FSLogix\ODFC and will correctly reset themselves under the above circumstances.
- FSLogix **profile** containers are a complete roaming profile solution for virtual environments. The profile container (single container), redirects the entire Windows user profile into a VHD stored on a storage provider.  
The profile container is inclusive of all the benefits and uses found in the ODFC container.
- FSLogix **ODFC containers** are a subset to the profile container and are used to redirect specific Microsoft 365 app data into a VHD stored on a storage provider.
  - Using the ODFC container in a single container configuration is recommended with third party roaming profile solutions.
  - Using the ODFC container in a dual container configuration isn't necessary or recommended.

## 15.4 Additional information

- During logoff of the user-session a VHD disk compaction is executed automatically, to decrease the size of the VHD(X) file
  - For that reason, the Windows server “Optimize Drives” (defragsvc) has to be set to automatic in the golden image, if modified previously by VMware OSOT.

# 16. Horizon Recording

Version 1.12.0, see [documentation](#)

## 16.1 Requirements

### Horizon Recording Server

- MS Windows Server OS, static IP, Domain joined

- VM hardware: 4x vCPUs, 8GB RAM, dedicated HDD for recordings (if local)
- Local or shared NTFS for recordings
- TCP port 9443 for incoming requests has to be opened (for Web UI and Horizon Agent)

### Horizon Agent

- Needs Windows 10 Build 1909 or higher (or Windows Server OS for RDSH Farms)

### Omnissa Horizon 2106 or higher

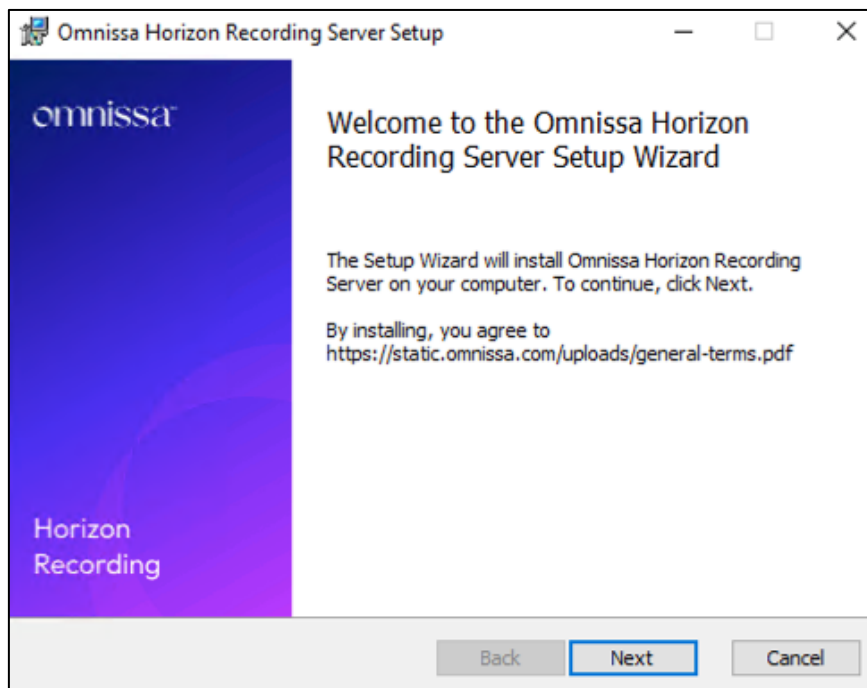
### Notices

- Only Blast sessions can be recorded
- If an user has multiple displays, for every display one recording file will be created
- If notification message will be edited, a service restart for the agent is needed

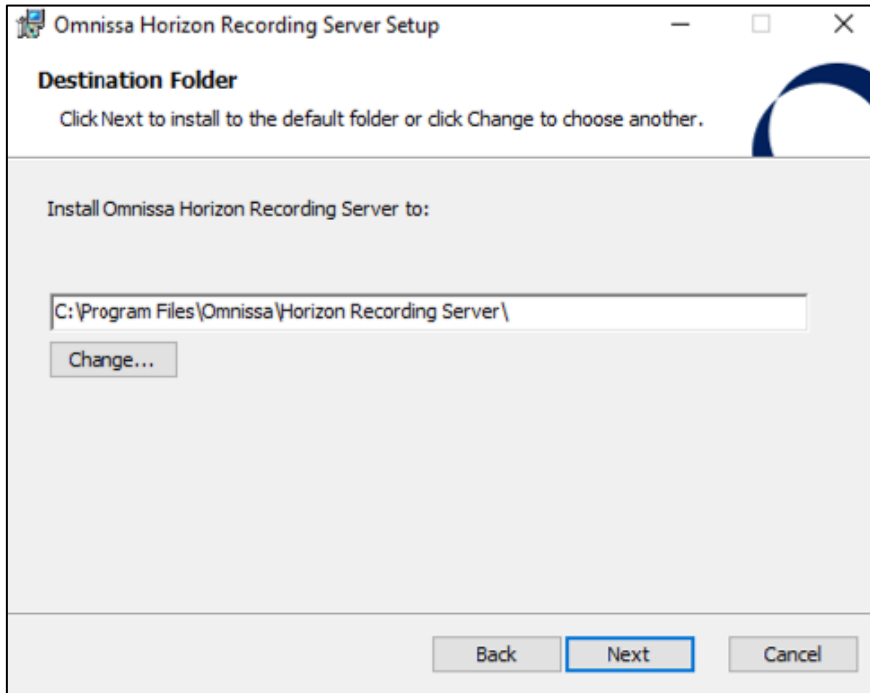
## 16.2 Setup

### Setup Recording Server

- Execute Installer



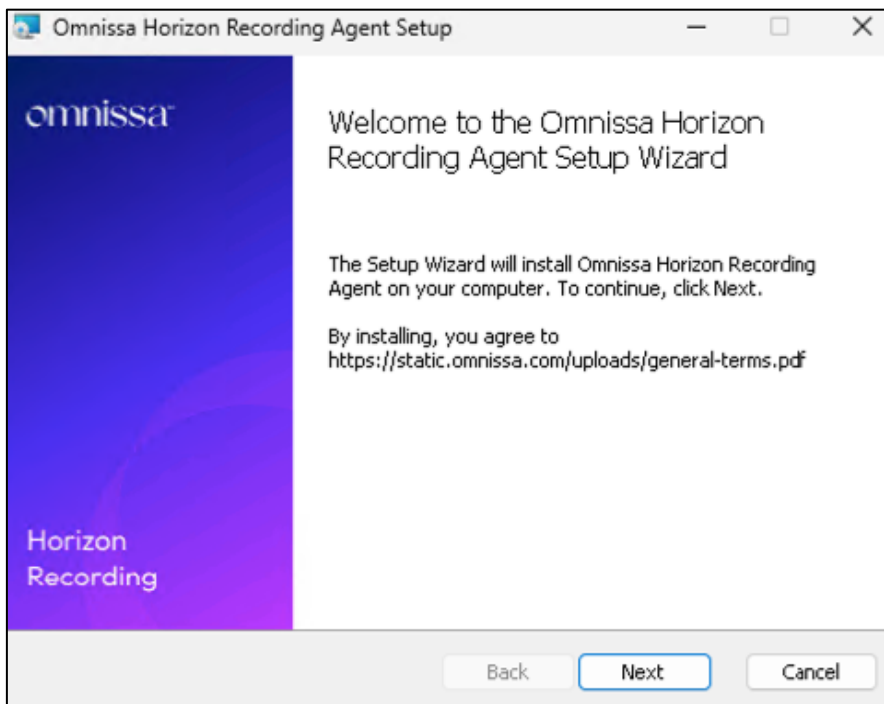
- Validate setup folder



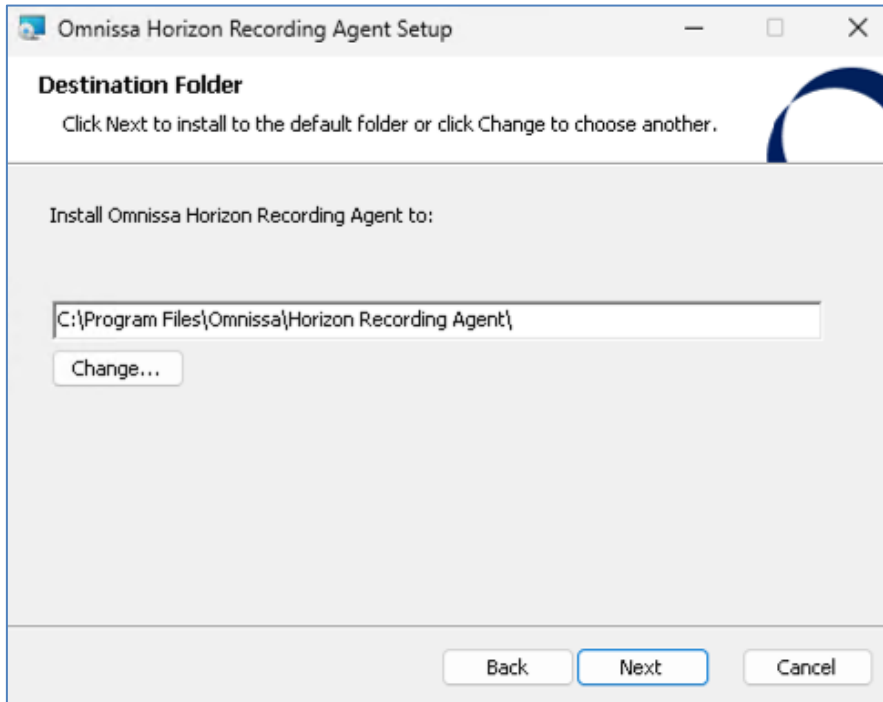
- Next and Finish

## Setup Recording Agent

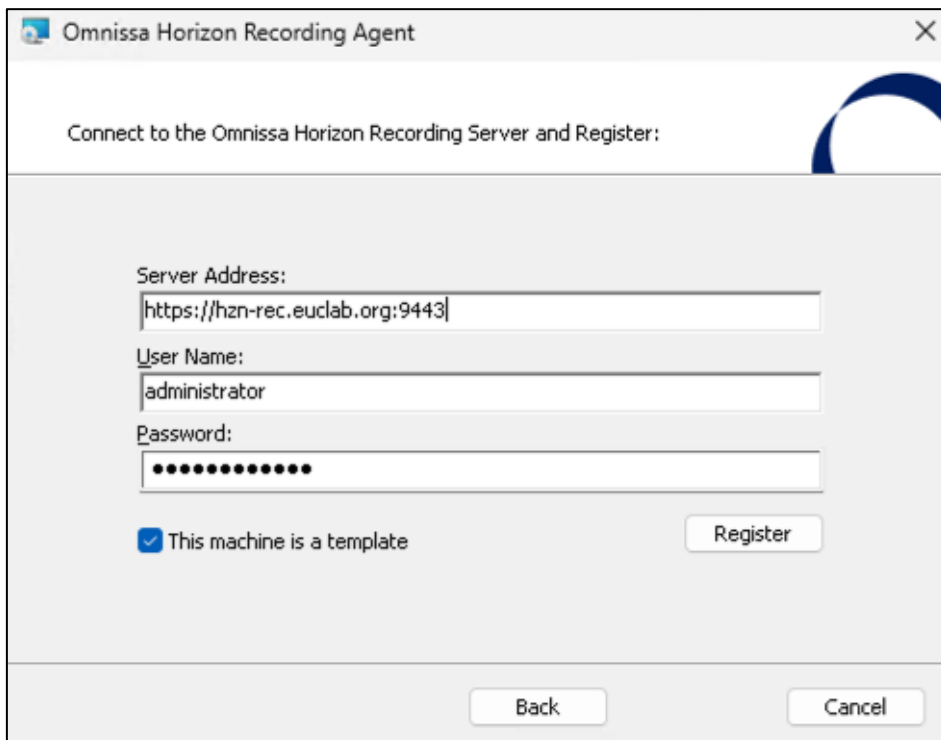
- Execute Installer



- Validate setup folder

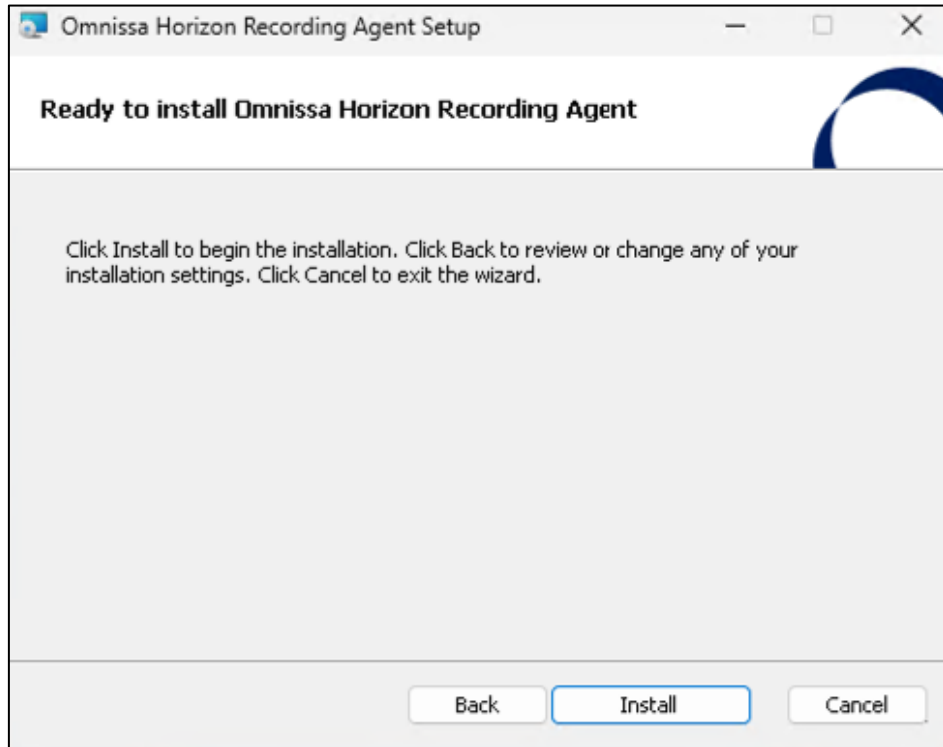


- Enter server address "https://<FQDN or IP>:9443", the admin account for the UI, and enable the template option, if it is a golden image or similar. Click on →Register



- If the certificate is untrusted, you have to submit this in a pop-up window

- Start installation



- The settings of the agent are stored in the Registry:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Omnissa\Horizon\Blast\Recording Agent

## 16.3 Initial configuration

- Login to the Admin UI: <https://<FQDN or IP>:9443>
  - Default Login for Administrator: Administrator / Recording123
  - Default Login for Viewer: Viewer / Recording456
- Go to → Administrator → Manage Agents
  - Here you can see the registered agent from the golden image VM

Registered Machines:					
<input type="checkbox"/>	Name:	Type:	Last Seen:	Version:	Horizon Version:
<input type="checkbox"/>	WIN10-GM	Template	9/23/24, 11:27 AM	1.11.0	8.13.0

Manage Columns Item

- Go to → Administrator → Service Settings to configure general items

- Authentication Settings – LDAPS integration (mandatory, if you would add AD groups for recording)

General	LDAPS Integration
Enable LDAPS Integration:	<input checked="" type="checkbox"/>
LDAPS URL:	euclab.org <small>The url or fqdn of the LDAPS server you wish to use: e.g: "exampledomain.local"</small>
Bind User DN:	CN=sa-hzn-rec,cn=users,DC=euclab,DC=org <small>The LDAP user account DN. e.g: "CN=BindUser,cn=users,DC=exampledomain,DC=local"</small>
Bind User Password:	•••••••• <small>The LDAPS user password.</small>
Search Base:	DC=euclab,DC=org <small>The root location to search from. "e.g: DC=exampledomain,DC=local"</small>
Administrative Group DN:	CN=RecordingAdmins,CN=Users,DC=euclab,DC=org <small>The DN of the LDAP Group you wish to assign administrative access to this console. e.g: "CN=RecordingAdmins,CN=Users,DC=euclab,DC=org"</small>
Viewer User Group DN:	CN=RecordingUsers,CN=Users,DC=euclab,DC=org <small>The DN of the LDAP Group you wish to assign user (viewer) access to this console. e.g: "CN=RecordingUsers,CN=Users,DC=euclab,DC=org"</small>
Advanced:	
User Search Filter:	(&(objectClass=user)(objectClass=person)(UserPrincipalName={0})) <small>The LDAP user search filter, dont change this unless required, the default is: "(&amp;(objectClass=user)(objectClass=person)(UserPrincipalName={0}))"</small>
Group Search Filter:	(&(ObjectClass=group)(distinguishedName={0})) <small>The LDAP group search filter, dont change this unless required, the default is: "(&amp;(ObjectClass=group)(distinguishedName={0}))"</small>
<b>TEST CONFIGURATION</b>	

- Agent Settings
  - Notification message etc.

- Recording Criteria

Recording Criteria:

Session Types:  Record Local Sessions  
 Record Remote Sessions (Through UAG)

Groups to Record:

	Group Name	SID
<input type="radio"/>	Simpsons	S-1-5-21-2847478624-3711033770-2204177024-1140

Manage Columns Items per page 10  1 - 1 of 1 Items

- Server Settings

- DB connection type
- Recording Storage Folder
- Encryption
- Retention Settings (Default 14 days)
- etc.

## 17. Horizon Integration in Omnissa Access

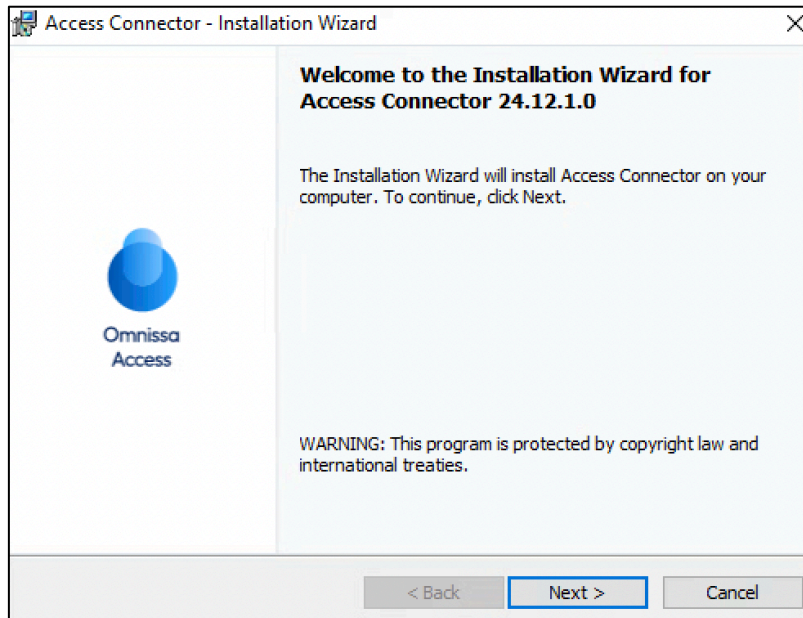
You can integrate Web apps and Virtual Apps (like Horizon applications and desktops) with Omnissa® Access™ to make these apps and desktops available to end users in the Omnissa® Intelligent Hub app and portal. Omnissa Access provides multi-factor authentication, conditional access, and single sign-on to the apps.

### 17.1 Setup Omnissa Access Connector

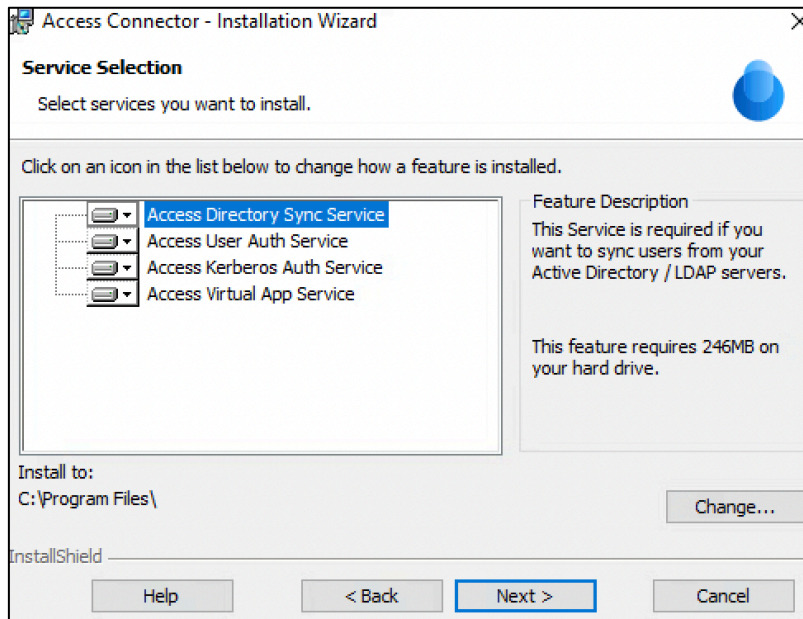
Version 24.12.1

The Omnissa Access connector integrates with on-premises infrastructure such as Active Directory, RSA SecurID, and Horizon for user authentication, directory integration, and virtual app integration<sup>6</sup>.

- Prepare Windows Server OS (AD-joined)
- Execute the Omnissa Access Conector Installer

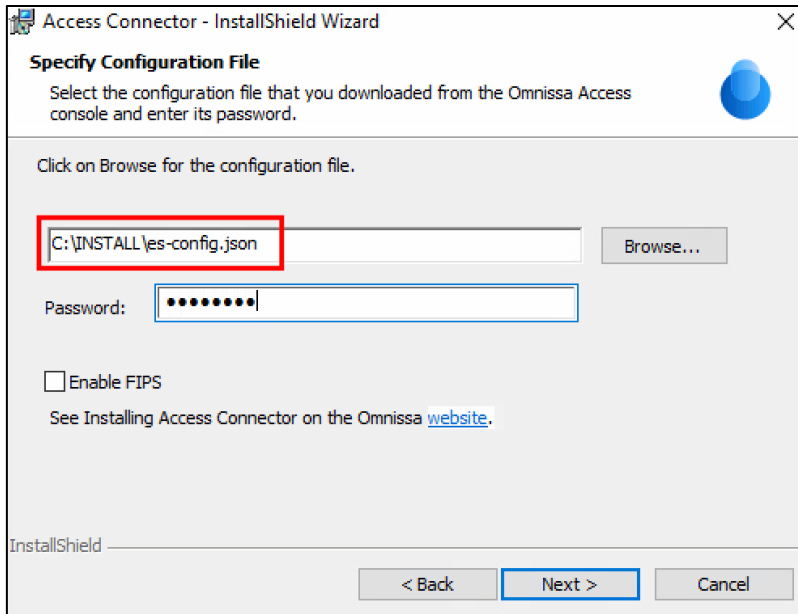


- Select the services you need (typically all of them):

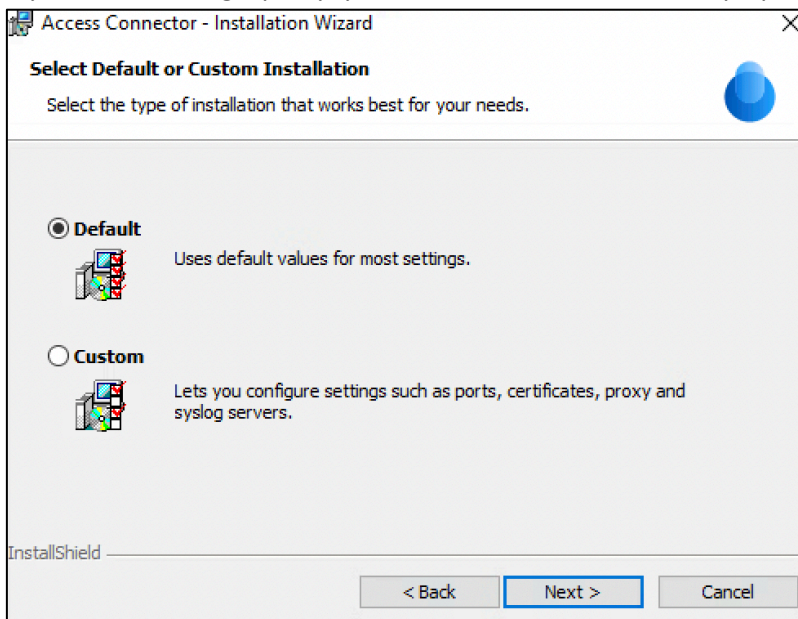


- The configuration (es-config.json) file which is needed, can be generated in the **Omnissa Access Console** via →Omnissa Connect Portal →Access →Integrations →Connectors →New

<sup>6</sup> Omnissa Access Connector Systems Requirements, see [here](#)



- If you are not using a proxy, you can choose the default setup option



- You need to specify a service account, which is part of the Domain Admins group. After installation is complete, this account can be removed from Domain Admins. For Kerberos Auth Service, the following special characters are the only ones which are supported:

! ( & % @ / = ? \* , . #

**Specify Service Account**

Specify the user name and password of the domain account that will be used to run the Kerberos Auth Service and the Virtual App Service.

The user account must be in the form DOMAIN\Username.

User name:  
eudab\sa-acc-con Browse...

Password:  
●●●●●●●●

< Back Next > Cancel

- Click → Install to start the installation

**Ready to Install the Program**

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

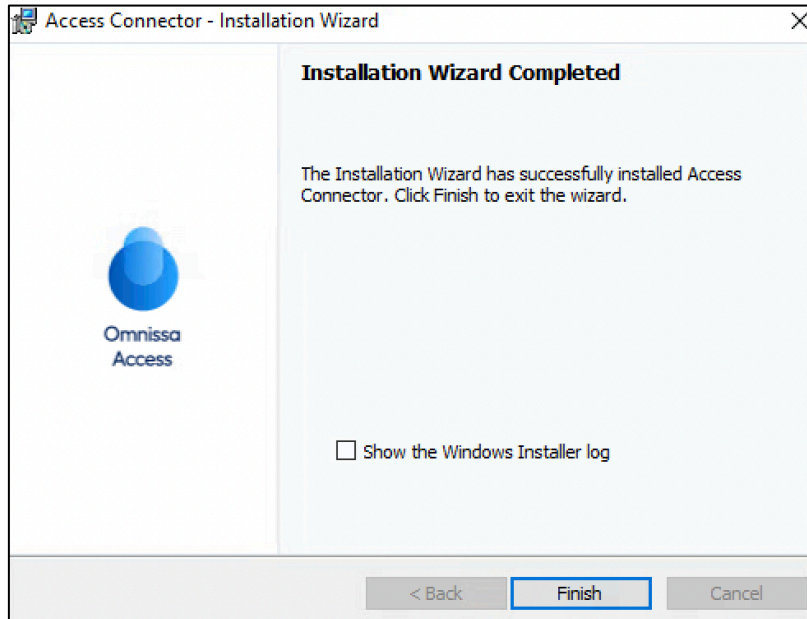
**Installed/Configured Application**

AccessUserAuthService : Configured on Port 8090	Proxy Server : Not Configured
AccessDirectorySyncService : Configured on Port 8080	Syslog Server : Not Configured
AccessVirtualAppService : Configured on Port 8008	
AccessKerberosAuthService : Configured on Port 443	

SSL Certificate : Self-Signed

< Back Install Cancel

- When installation finished, you have to check, if these services are up and running:



- Access Directory Sync Service
  - Access User Auth Service
  - Access Kerberos Auth Service
  - Access Virtual App Service
- In the Omnissa Access Console, refresh the list and verify the the newly installed Connector is shown accordingly

Connectors					
The Omnissa Access connector integrates with on-premises infrastructure such as Active Directory, RSA SecurID, and Horizon for user authentication, Directory integration, and integration.					
New		Manage			
	Host	Enterprise Service	Status	Health	Version
○	OMN-ACC-CON.euclab.org	Directory Sync	Active	⊙	24.12.1.0
		Kerberos Auth	Active	⊙	24.12.1.0
		User Auth	Active	⊙	24.12.1.0
		Virtual App	Active	⊙	24.12.1.0

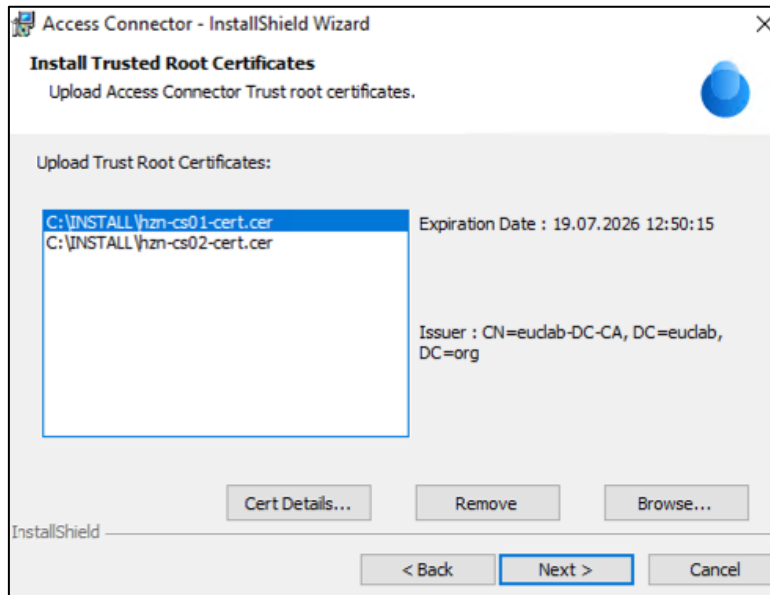
### 17.1.1 Upload Connection Server certificate to Omnissa Access Connector

Reference – [URL](#)

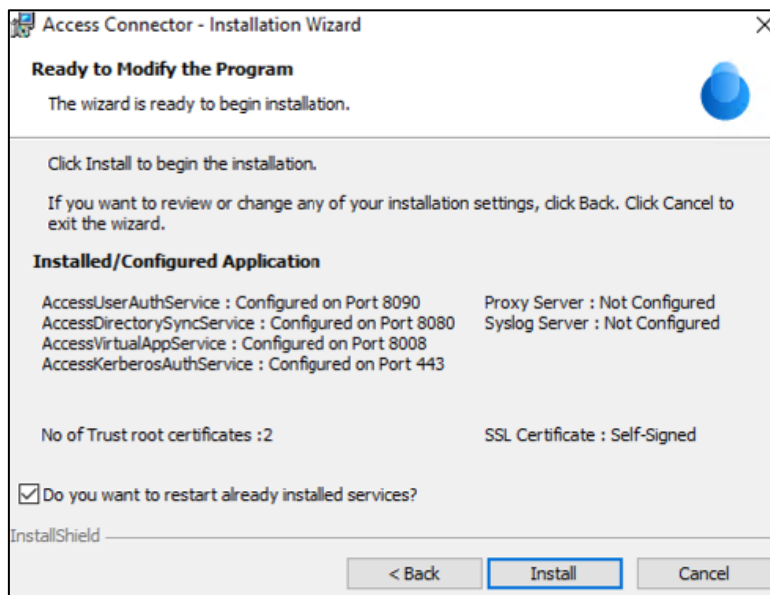
If the Horizon servers have self-signed certificates, you must upload the certificate chain to the Omnissa Access connector instances on which the Virtual App service is installed to establish trust between the connectors and the Horizon servers.

- Export the certificate(s) from the connection server(s) as cer- or pem-file.

- Execute the Omnissa Access Connector Installer again, select Add/Remove Services, and click Next, until you get the windows to →Upload Trust Root Certificates



- Click →Next until the last step, and enable the option to restart already installed services. Finish with →Install



## 17.2 Providing Access to Horizon Desktops and Applications in Omnissa Access

Reference – [URL](#)

Integrating Omnissa Horizon® with the Omnissa Access service lets you provide users the ability to access their assigned Horizon desktops and applications from the Omnissa Intelligent Hub app or portal. You can integrate independent Horizon pods, which consist of Horizon Connection Server instances, and pod federations, which contain multiple pods and can span multiple sites and data centers.

You deploy and manage desktop and application pools in the Horizon Console. You also create user assignments for Active Directory users and groups in Horizon, not in Omnisia Access. You must sync these users and groups to the Omnisia Access service from Active Directory before setting up the integration with Horizon.

To integrate Horizon pods and pod federations with Omnisia Access, you create virtual apps collections in the Omnisia Access console. A collection contains the configuration information for the pods and pod federation, sync settings, and other settings. You then sync the collection, which propagates Horizon resources and assignments to Omnisia Access.

In the Omnisia Access console, you can view the Horizon desktops and applications. You can also view user and group assignments for these desktops and applications.

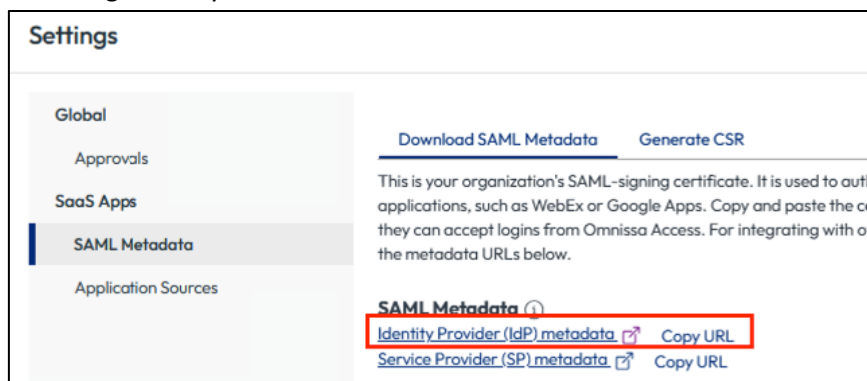
## 17.2.1 Configure SAML Authentication in Horizon for Omnisia Access Integration

Reference – [URL](#)

SAML authentication allow users to launch Horizon desktops and applications using single sign-on. When SAML authentication is configured, users logged into the Intelligent Hub app or portal can launch their remote Horizon desktops and applications without going through a second login procedure.

You must configure SAML authentication on at least one Horizon Connection Server instance in a pod. The best practice is to configure SAML authentication on all instances in the pod. It is NOT required to configure SAML authentication in the UAG!

- Get the **SAML Metadata** – in **Omnisia Access Console**, go to →Resources →Web Apps →Settings. Here you can find the SAML Metadata for the IdP Provider:



- In **Horizon Console**, go to →Settings →Servers →Connection Servers. Select the Connection Server you want to configure for SAML Authentication, and click to the tab →Authentication, to add the SAML Authenticator as **Allowed** or **Required**.
  - **Allowed** means, that a user which connects to the public URL from the UAG, is authenticated through this UAG, and the session is established accordingly, without using Omnisia Access for authentication. Alternatively, a user can connect and authenticate against the Omnisia Access hub, and then establish a Horizon session through the UAG.

- **Required** means, that a user which connects to the public URL from the UAG, is always forwarded to the Omnissa Access hub, and needs to authenticate, before establishing the Horizon session through the UAG.
- Click on →Manage SAML Authenticators and click →Add
  - Paste the Metadata URL you copied from the Omnissa Access Console

- If TrueSSO is implemented, you also need to set TrueSSO Trigger Mode to „Enabled“ or „Always“
  - Enabled – is user entered a password and it is cached, this will be used. Otherwise TrueSSO will be used.
  - Always – TrueSSO will be used always, independent if a user password gets cached or not.
- If you set the „Delegation of authentication to Horizon (SAML 2.0 Authenticator)“ to „Required“, also enable the check box for the „Workspace ONE mode“ in the Authenticator settings:

Enabled for Connection Server  
 Require Encrypted Assertion ⓘ  
 **Workspace ONE Mode** ⓘ  
 IDP Should Authenticate User Every Time ⓘ

## 17.3 Add on-prem AD to Omnisca Access

Reference – [URL](#)

You can integrate your enterprise directory with Omnisca Access to sync users and groups to the Omnisca Access service. Omnisca Access supports integration with Active Directory and with LDAP directories such as OpenLDAP.

When you integrate a directory, a limited number of user and group attributes, specified by the administrator, are synced to the Omnisca Access service. User passwords and any attributes other than the ones specified by the administrator are not synced.

- In Omnisca Access Console, go to →Settings →User Attributes, and select the user attributes that are required

- Add one custom attribute named objectGuid under →Custom Attributes

Custom Attributes

Add your own attributes to sync to the directory. Go to the directory's attributes page to map these attributes.

Name

objectGuid

+ Add Row

- Click →Save when finished
- Go to →Integrations →Directories and click →Add Directory, and select →Active Directory.
  - Enter Directory Name
  - Select **Active Directory over LDAP**, if you plan to connect to a single Active Directory domain environment.
  - Select **Active Directory over IWA**, if you plan to connect to a multi-domain or multi-forest Active Directory environment.

1 Directory Information

Directory Name \*

Type

Active Directory over LDAP

Active Directory over Integrated Windows Authentication

- Configure Directory

2 Configure Directory

### Directory Sync and Authentication

Select at least one active Directory Sync host that syncs users from Active Directory to the Ommissa Access directory.

Directory Sync Hosts \*  OMN-ACC-CON.euclab.org (Active)

Authentication Method

Set up password authentication for this directory

Add authentication methods later

User Authentication Hosts \*  OMN-ACC-CON.euclab.org (Active)

User Name \*

External ID \*   
Enter the attribute to use as the unique identifier of users in the Ommissa Access directory.

Server Location  This directory supports DNS server location

Encryption  Require STARTTLS for all connections

SSF Integration  No

- Enter the DN from which to start account searches
- Enter the CN of the user account that can search for users – this account needs the following permissions:
  - Read
  - Read All Properties
  - Read Permissions

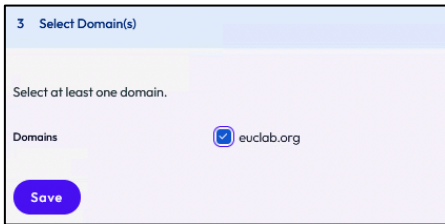
Bind User Details

Base DN \*   
Enter the DN from which to start account searches, for example OU=myUnit,DC=myCorp,DC=com

Bind User DN \*   
Enter the account that can search for users, for example CN=user1,CN=Users,OU=myUnit,DC=myCorp,DC=com.

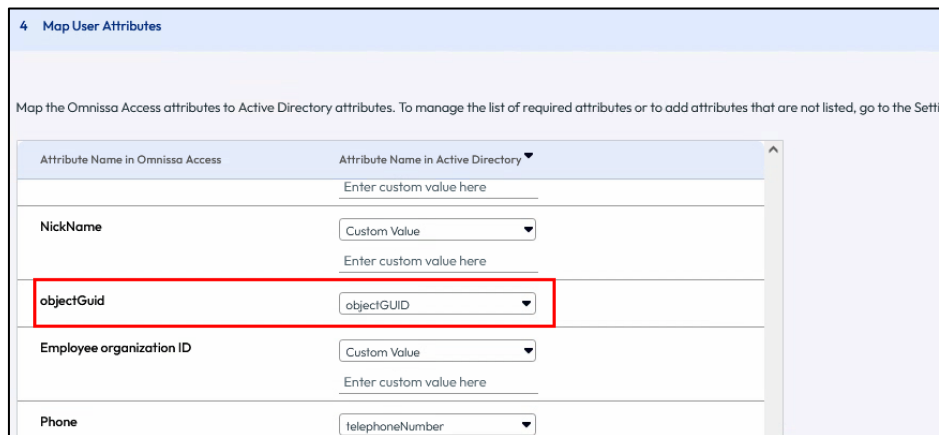
Bind User Password \*   
Enter your Active Directory bind account password.

- Select Domain



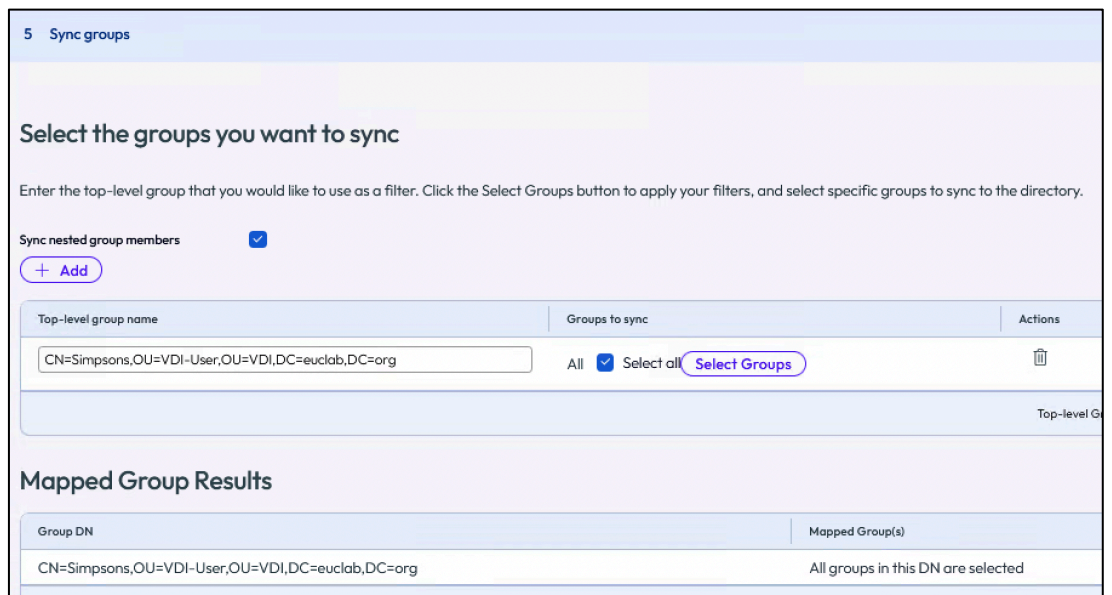
- Map User Attributes

- Set the **objectGUID** equivalent between Omnissa Access attributes and Active Directory attributes. Click →Save.



- Sync groups

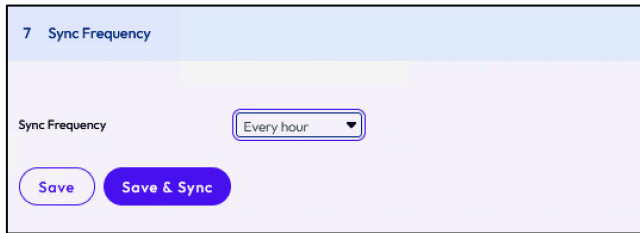
- Add all AD-groups you want to sync from AD to Omnissa Access. Enter the CN of the AD-group. Only group names are synced to the directory. Users that are members of the group are not synced to the directory until the group is entitled to an application or the group name is added to an access policy rule. Click →Save.



- Sync users

- You can select users you want to sync

- Configure the sync frequency



7 Sync Frequency

Sync Frequency

## 17.4 Set Login Preferences in Omnisia Access

- In Omnisia Access Console, go to →Settings →Login Preferences, and enable →**Object GUID attribute for Horizon Virtual App Collection**
- If only one domain is in use, you also can disable the setting →**Show system domain on login page**. The only configured domain will be used then.
- If you are using password-based authentication in Omnisia Access and have NOT implemented TrueSSO, you can go to and enable →**Cache passwords**, to achieve SSO functionality for Horizon. Otherwise the user gets prompted for his password again, when he click on a Horizon resource.

## 17.5 Create a Virtual App Collection for Horizon

Reference – [URL](#)

To integrate Omnisia Horizon desktops and applications with the Omnisia Access service, you create virtual apps collections. These types of integrations require you to install the Virtual App service, a component of the Omnisia Access connector (should be done already [here](#)).

- In Omnisia Access Console, go to →Resources →Virtual App Collections and click →New
- Select Horizon

- Enter a proper name and select the existing Connector

**New Horizon Collection**

- 1 Connector
- 2 Pod And Federation
- 3 Configuration
- 4 Summary

**Connector**

Name \*

HZN EUCLAB

Connector

Select the connectors to use to sync this collection. If multiple connectors are available, you can add them and arrange them in fallback order. One active connector is required.

1. OMN-ACC-CON.euclab.org (active)

Cancel Next

- Add at least one existing Pod. Optionally, you can add CPA configuration as well

**New Horizon Collection**

- 1 Connector
- 2 Pod And Federation
- 3 Configuration
- 4 Summary

**Pod and Federation**

Add or modify pods. If a pod has multiple Horizon Connection Servers, you only need to add it once providing information for any of the Horizon Connection Servers within the pod.

Horizon Connection Server	Username	Smart Card Authentication	True SSO	Sync Local Assignments
HZN-CS01.euclab.org	administrator	Disabled	Disabled	Enabled

+ Add A Pod

Have you enabled Cloud Pod Architecture for any of the pods added above?

Yes

Cancel Back Next

- If you have TrueSSO configured in your Horizon Pod, you should enable True SSO for the added Pod.

- Setup default configuration, like sync frequency, Safeguard Threshold Limits and so on

**New Horizon Collection**

- 1 Connector
- 2 Pod And Federation
- 3 Configuration
- 4 Summary

**Configuration**

Sync

Sync Frequency

Hourly

Sync Duplicate Apps ⓘ

Yes

Safeguard Thresholds Limits

Set up safeguards thresholds that help limit the usage of the server resources when syncing apps, desktops, and assignments. When thresholds are less than 100% the remaining changes will be synced in subsequent sync.

Cancel Back Next

- Save the configuration, after some moments you should see the Virtual App Collection

Virtual Apps Collections  
Add and configure virtual app collections for each type of integration.

New Edit Sync Delete

	Name	Source Type	Sync Frequency	Sync Status
<input type="radio"/>	<a href="#">HZN EUCLAB</a>	Horizon	Hourly	Completed

### 17.5.1 Assign Pod to Network Ranges

As the added Pod for the Virtual App Collection should be accessible from external, you have to assign the Pod to existing or newly created Network Ranges.

If you need to access Horizon resources through Omnissa Access from internal, you need to create a dedicated Network Range. See [next](#) chapter.

- In Omnissa Access, go to →Resources →Virtual App Collections, and select the Virtual App you just created
- Click on →Network Ranges, and select the default →ALL RANGES

Virtual Apps Collections > HZN EUCLAB

Overview Network Ranges

Add

Name	Description
ALL RANGES	A network for all ranges

- Scroll down to “Pod and Federation”, and change the →Client Access FQDN to the external URL under the UAG is reachable from:

Pod and Federation

Pod	Client Access FQDN ⓘ	Port	Wrap Artifact in JWT ⓘ	Audience in JWT ⓘ
hzn-cs01.euclab.org	euc.omnissa.live	443	<input checked="" type="checkbox"/> No	Add

- Click →Save

### 17.5.2 Define Network Ranges

- To define a new Network Range (for internal access i.e.), go to →Resources →Policies and click on →Network Ranges and →Add Network Range

- To assign this newly created Network Range to a Pod, go to →Resources →Virtual Apps Collections, and select the target Virtual App. Go to →Network Ranges, and select the newly created Network Range

Name	Description
ALL RANGES	A network for all ranges
Omnissa Access Internal	Access to Horizon Resources through Omnissa Access internally

- Scroll down and verify that the internal FQDN for the affected Connection Server is configured:

Pod	Client Access FQDN	Port	Wrap Artifact in JWT	Audience in JWT
hzn-cs01.euclab.org	hzn-cs01.euclab.org	443	No	

- Click →Save

## 17.6 (Optional) Implementing Omnissa Pass as MFA

Omnissa Pass is a MFA solution, available as part of Omnissa Access. It is available as **Basic** (includes time-based one-time code passcodes = TOTP), and **Advanced** (includes phishing resistant protections as well as support for FIDO2 passkey credentials additionally).

## 17.6.1 Prepared by Admin

- In **Omnissa Access**, go to →Integrations →Authentication Methods, select →Pass App and click →Configure
  - Enable Omnissa Pass, and configure the settings, as needed.
- Go to →Integrations →Identity Providers, select the →Build-in Provider. Confirm that the Build-in provider is activated, and under “Authentication Methods”, enable →Pass App

Identity Provider Name	Authentication Methods	Directory	Network Ranges	Type	Status
<a href="#">System Identity Provider</a>	Password (Local Directory)	System Directory	ALL RANGES	Built-in	Activated
<a href="#">Built-in</a>	Token Auth Adapter Pass App	EUCLAB.ORG	ALL RANGES	Built-in	Activated
<a href="#">IDP for EUCLAB.ORG</a>	Password (cloud deployment)	EUCLAB.ORG	ALL RANGES	Built-in	Activated
<a href="#">MS Entra ID SAML</a>	entraMFA	EUCLAB.ORG	Mobile	SAML	Activated

Select which authentication methods the IdP will use to authenticate users.

Select All

Password (Local Directory)  Token Auth Adapter

Pass App

- Go to →Resources →Policies. Select the default policy, or create a new one. Add a policy rule, and configure it on your needs. To the existing authentication (like “Password (cloud deployment)”), add another authentication called “Omnissa Pass App”, and submit with →Save:

**Edit Policy Rule**

and user is registering Omnissa Pass •  No

and user accessing content using magic link •  No

Then perform this action: Authenticate using...

then the user may authenticate using • Password (cloud deployment)

AND

Omnissa Pass App

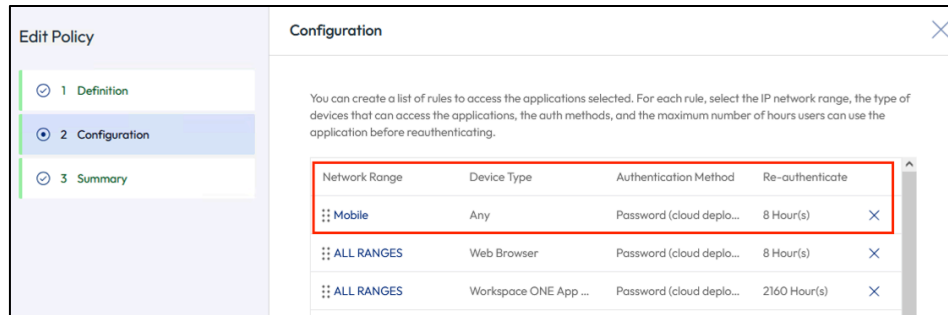
Add

Add Authentication

Add Fallback Method

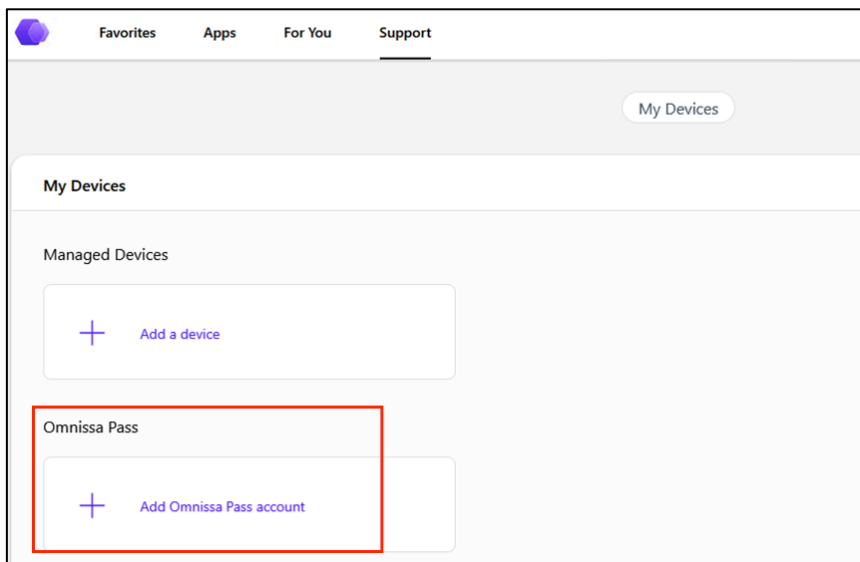
Cancel Save

- Move the newly created policy rule to the top of the list, and click →Save:

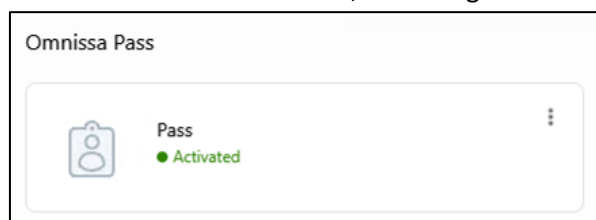


## 17.6.2 Prepared by End User

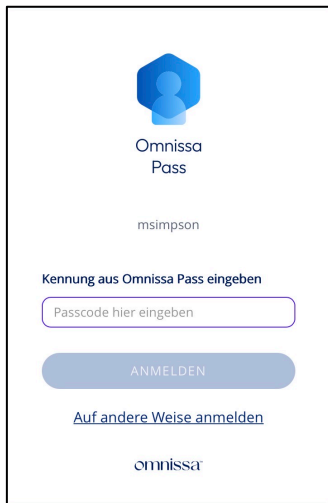
- To get Omnissa Pass working, the end user needs to download the app “Omnissa Pass” to his mobile device
- To add an account to the Omnissa Pass App, the end user needs to login to his Workspace One Hub, go to →Support, and “Add Omnissa Pass account”



- The end user needs to add an account and then scan the shown QR-code via Omnissa Pass App.
- After the account was added, it is recognized in the Hub:



- After the user is logged in via Omnissa Access, now he will be prompted for the MFA from Omnissa Pass:



The screenshot shows the Omnissa Pass login interface. At the top is the Omnissa Pass logo, a blue hexagon with a person icon. Below it, the text 'Omnissa Pass' is displayed. The username 'msimpson' is shown. A prompt 'Kennung aus Omnissa Pass eingeben' is followed by a text input field containing 'Passcode hier eingeben'. Below the input field is a blue button labeled 'ANMELDEN'. At the bottom, there is a link 'Auf andere Weise anmelden' and the Omnissa logo.

## 18. 2FA for UAG with DUO

Simple example of a 2FA-integration with Horizon UAG and DUO

Two-Factor Authentication for VMware Horizon View (VDI)

<https://duo.com/docs/vmwareview>

<https://duo.com/docs/authproxy-reference>

To integrate Duo with your VMware View Server, you will need to install a local Duo proxy service on a machine within your network. This Duo proxy server will receive incoming RADIUS requests from your UAG, contact your existing local LDAP/AD to perform primary authentication, and then contact Duo's cloud service for secondary authentication.

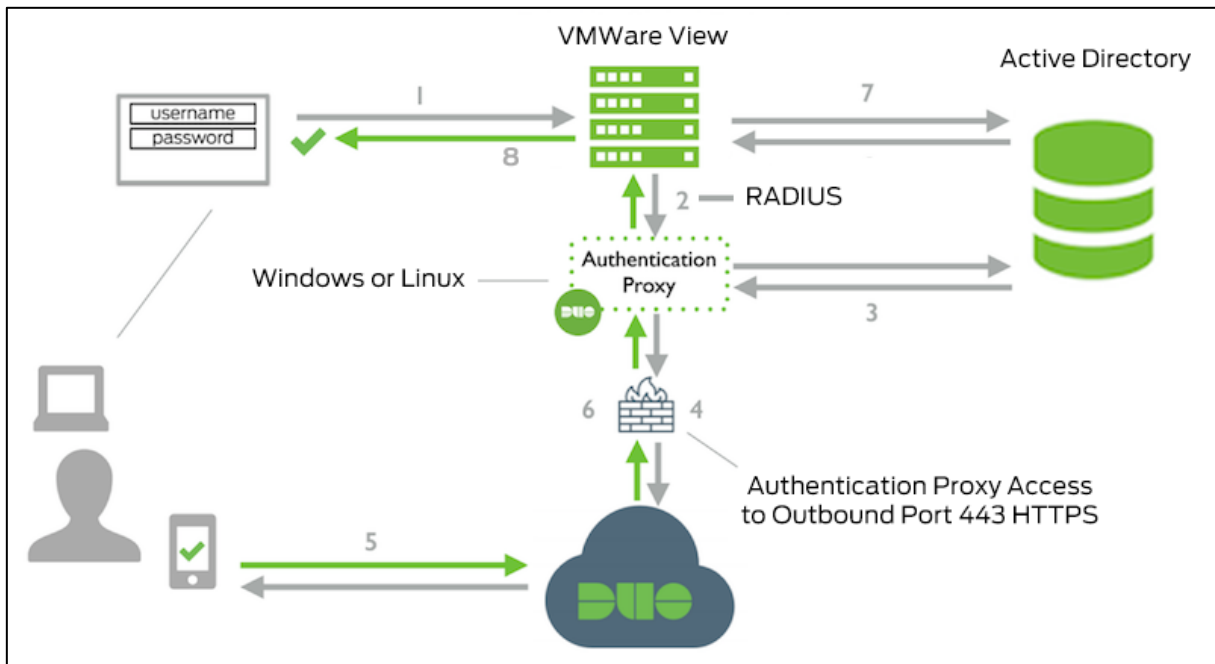


Figure 1: Network flow for DUO 2FA

You need a DUO admin account, see <https://admin.duosecurity.com/>

## 18.1 Prepare VM for DUO Proxy Service

- Setup Ubuntu Desktop 24.04 LTS<sup>7</sup>
- VM should have at least 1x CPU, 4GB RAM.
- Configure static IP address
- Install VMware Tools
  - Open Terminal and execute the following commands:

```
sudo apt install open-vm-tools
sudo apt install open-vm-tools-desktop open-vm-tools
```
  - Reboot the OS per `reboot`
  - Verify installation: `|lsmod | grep vmw`
- (optional) enable SSH access
  - Setup SSH:

```
sudo apt update
sudo apt install openssh-server
```
  - Check Status SSH: `sudo systemctl status ssh`
  - Make sure that firewall port is open for SSH: `sudo ufw allow ssh`
  - Allow SSH access for specific user:
    - Edit the file `/etc/ssh/sshd_config` and add this line:

```
AllowUsers username
```

<sup>7</sup> <https://ubuntu.com/download/desktop>

- Reload the configuration: `sudo service ssh reload`

## 18.2 Create Application in DUO

- Login to Duo Admin Panel ([URL](#))
- Go to →Applications and click on →Protect an Application
- Select “VMware View” and click on →Protect

Application	Protection Type	
 VMware View	2FA	<a href="#">Documentation</a> <a href="#">Protect</a>

- Copy the information about **Integration key**, **Secret key** and **API hostname** to a safe place. You need these information later for the setup of the DUO Proxy Service.

[Dashboard](#) > [Applications](#) > VMware View

### VMware View

See the [VMware Horizon View documentation](#) to integrate Duo into your VMware Horizon with View deployment.

#### Details

Integration key	<code>DIEHJHOY0Y1P6GT3UU6R</code>	<a href="#">Copy</a>
Secret key	<code>.....dnip</code>	<a href="#">Copy</a>
Don't write down your secret key or share it with anyone.		
API hostname	<code>api-ddeb61e9.duosecurity.com</code>	<a href="#">Copy</a>

## 18.3 Install the Duo Authentication Proxy

- Ensure that Perl and a compiler toolchain are installed:  
`sudo apt-get install build-essential libffi-dev perl zlib1g-dev`
- Download the most recent Authentication Proxy for Unix:  
`wget --content-disposition`

<https://dl.duosecurity.com/duoauthproxy-latest-src.tgz>

```
ubuntu@DUO2FA:~$ wget --content-disposition https://dl.duosecurity.com/duoauthproxy-latest-src.tgz
--2024-08-27 11:28:03-- https://dl.duosecurity.com/duoauthproxy-latest-src.tgz
Resolving dl.duosecurity.com (dl.duosecurity.com)... 52.85.92.60, 52.85.92.76, 52.85.92.87, ...
Connecting to dl.duosecurity.com (dl.duosecurity.com)|52.85.92.60|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 45054245 (43M) [application/x-tar]
Saving to: 'duoauthproxy-6.4.1-src.tgz'

duoauthproxy-6.4.1-src.tgz      100%[=====>] 42.97M  20.7MB/s   in 2.1s

2024-08-27 11:28:06 (20.7 MB/s) - 'duoauthproxy-6.4.1-src.tgz' saved [45054245/45054245]

ubuntu@DUO2FA:~$
```

- Extract the Authentication Proxy files and build it as follows:  
tar xzf duoauthproxy-6.4.1-src.tgz  
cd duoauthproxy-version-src  
make
- Install the authentication proxy (as root):  
cd duoauthproxy-build  
sudo ./install
  - Default user will be created to run the Authentication Proxy (duo\_authproxy\_svc) as well as a default user group (duo\_authproxy\_grp)

```
Create an initialization script to run the proxy upon startup? [Yes/no] Yes
Skipping SELinux module installation due to requirements not being met
Created symlink /etc/systemd/system/multi-user.target.wants/duoauthproxy.service - /etc/systemd/system/duoauthproxy.service.
Created service script at /etc/systemd/system/duoauthproxy.service

Installation completed. Before starting the Authentication Proxy,
Please edit the configuration file at:

/opt/duoauthproxy/conf/authproxy.cfg

○ ubuntu@DUO2FA:~/duoauthproxy-6.4.1-src/duoauthproxy-build$
```

### 18.3.1 Update Duo Authentication Proxy

Update from 6.4.1 to 6.6.0

To upgrade the Duo Authentication Proxy, simply download the most recent version and install it over your currently running version. The installer preserves your current configuration, log files, and encryption when upgrading to the latest release<sup>8</sup>.

- Switch to root  
su
- Check Duo Authentication Proxy version  
/opt/duoauthproxy/bin/authproxycctl version
- Download the most recent Authentication Proxy for Unix:  
wget --content-disposition  
<https://dl.duosecurity.com/duoauthproxy-latest-src.tgz>
- The most recent Authentication Proxy version may have additional prerequisites beyond those installed for your current running version. You can install (or verify the presence of) these by running this command:  
sudo apt-get install build-essential libssl-dev libffi-dev
- Extract the Authentication Proxy files and build it as follows:  
tar xzf duoauthproxy-6.6.0-src.tgz

<sup>8</sup> <https://duo.com/docs/authproxy-reference#upgrading-the-proxy>

```
cd duoauthproxy-version-src
make (will take a few moments)
```

- Install the authentication proxy

```
cd duoauthproxy-build
sudo ./install
```

```
ubuntu@DUO2FA:~/duoauthproxy-6.6.0-src/duoauthproxy-build$ sudo ./install
In what directory do you wish to install the Duo Authentication Proxy?
[/opt/duoauthproxy]

Enter the name of a user account under which the Authentication Proxy should be run. We recommend a non-privileged and locked down account.
Or you can press <Enter> and our default locked down user will be created for you:
[duo_authproxy_svc]

Enter the name of a group under which the Authentication Proxy logs will be readable. Or press <Enter> and a default group will be created for you:
[duo_authproxy_grp]

Preparing for upgrade installation...
Removing initscript...
Removed "/etc/systemd/system/multi-user.target.wants/duoauthproxy.service".
Preserving old installation...

Copying files... Done.

Create an initialization script to run the proxy upon startup? [Yes/no] Yes
Skipping SELinux module installation due to requirements not being met
Created symlink /etc/systemd/system/multi-user.target.wants/duoauthproxy.service - /etc/systemd/system/duoauthproxy.service.
Created service script at /etc/systemd/system/duoauthproxy.service

Applying config and logs from old installation...
Removing old installation...
Upgrade complete.

Installation completed. Before starting the Authentication Proxy,
Please edit the configuration file at:
/opt/duoauthproxy/conf/authproxy.cfg
```

- Check Duo Authentication Proxy version  
`/opt/duoauthproxy/bin/authproxycctl version`
- Check Duo Authentication Proxy Service  
`/opt/duoauthproxy/bin/authproxycctl status`
- Start Duo Authentication Proxy Service  
`/opt/duoauthproxy/bin/authproxycctl start`

## 18.4 Configure and Start Authentication Proxy

The Duo Authentication Proxy configuration file is named `authproxy.cfg`, and is located in the `conf` subdirectory of the proxy installation. With default installation paths, the proxy configuration file will be located at `/opt/duoauthproxy/conf/authproxy.cfg`.

- Edit `authproxy.cfg`  
`sudo nano /opt/duoauthproxy/conf/authproxy.cfg`
  - `ad_client` section

```
[ad_client]
host=dc.euclab.org
service_account_username=sa-duoservice
service_account_password=VMware1!
search_dn=DC=euclab,DC=org
```

- radius\_server\_challenge section

```
[radius_server_challenge]
ikey=DIEHJHOY0Y1P6GT3UU6R
skey=*****PP79Gic2Rrcng2xdnip
api_host=api-ddeb6le9.duosecurity.com
radius_ip_1=192.168.188.36
radius_secret_1=VMware!VMware!
failmode=safe
client=ad_client
port=1812
```

- radius\_ip = IP address of the Connection Server or UAG

- in case of troubleshooting, edit the main section accordingly for debug mode

```
[main]
debug=true
log_dir=log
log_max_files=6
log_max_size=10485760
```

- default for debug mode is 'false'
- Log files are located under /opt/duoauthproxy/log

- Start the Authentication Proxy

sudo /opt/duoauthproxy/bin/authproxycctl start

```
ubuntu@DUO2FA:~$ sudo /opt/duoauthproxy/bin/authproxycctl start
Running a validation of your configuration...
[info] Testing section 'ad_client' with configuration:
[info] {'host': 'dc.euclab.org',
       'search_dn': 'DC=euclab,DC=org',
       'service_account_password': '*****',
       'service_account_username': 'sa-duoservice'}
[info] There are no configuration problems
[info] -----
[info] Testing section 'radius_server_challenge' with configuration:
[info] {'api_host': 'api-ddeb6le9.duosecurity.com',
       'client': 'ad_client',
       'failmode': 'safe',
       'ikey': 'DIEHJHOY0Y1P6GT3UU6R',
       'port': '1812',
       'radius_ip_1': '192.168.188.36',
       'radius_secret_1': '*****',
       'skey': '*****[40]'}
[info] There are no configuration problems
[info] -----
[info] SUMMARY
[info] No issues detected

The results have also been logged in /opt/duoauthproxy/log/connectivity_tool.log

Checking updates for Duo Authentication Proxy...
[info] No updates detected. Your Duo Authentication Proxy is up to date.
ubuntu@DUO2FA:~$
```

- Verify that service is running via
  - sudo /opt/duoauthproxy/bin/authproxycctl start

- Verify functionality via Connectivity Tool:

sudo /opt/duoauthproxy/bin/authproxy\_connectivity\_tool

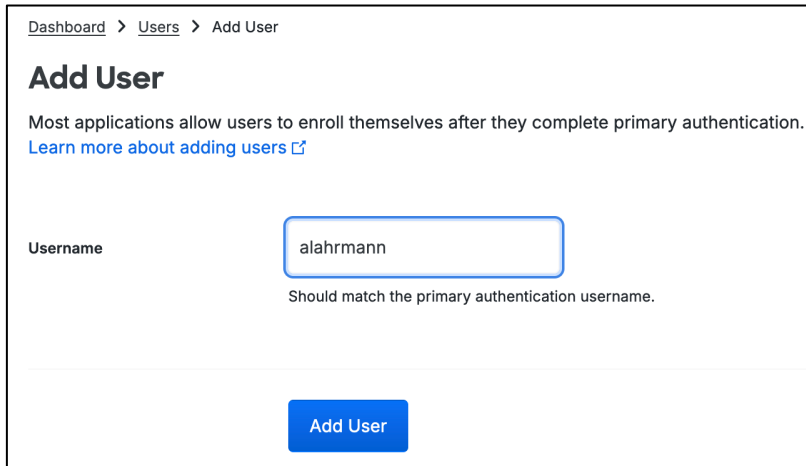
- You can check the status of the service also this way:

- sudo systemctl status duoauthproxy

## 18.5 Enroll users for using DUO 2FA

With DUO Free Edition, users from local AD cannot synced automatically to Duo Cloud Service. So users have to be added manually in Duo Admin Panel ([URL](#)).

- Click on →Users →Add User on the left to add a user manually



Dashboard > Users > Add User

### Add User

Most applications allow users to enroll themselves after they complete primary authentication. [Learn more about adding users](#)

Username

Should match the primary authentication username.

[Add User](#)

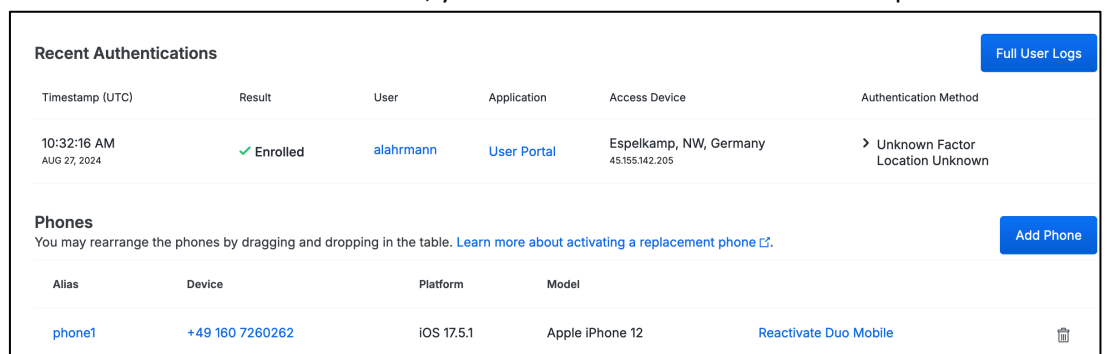
- Enter user's mail address

- Once generated, click on →Send Enrollment Email on the top right



Logs | [Send Enrollment Email](#) | [Send to Trash](#)

- User will get the enrollment URL via mail
  - When user has finished enrollment, you can see the details in DUO Admin portal



Recent Authentications						<a href="#">Full User Logs</a>
Timestamp (UTC)	Result	User	Application	Access Device	Authentication Method	
10:32:16 AM AUG 27, 2024	✓ Enrolled	alahrmann	User Portal	Espelkamp, NW, Germany 45.155.142.205	> Unknown Factor Location Unknown	

Phones				<a href="#">Add Phone</a>
Alias	Device	Platform	Model	
phone1	+49 160 7260262	iOS 17.5.1	Apple iPhone 12	<a href="#">Reactivate Duo Mobile</a>

## 18.6 Configure UAG for Radius

- Configure RADIUS as Authentication Setting

**RADIUS**

Enable RADIUS

Authentication Type: PAP

Shared secret \* [REDACTED]

Number of attempts to RADIUS server \* 3

Server Timeout In Seconds \* 30

RADIUS Server Host name \* 192.168.188.24

Authentication Port \* 1812

More ▾

Save Cancel

## 18.7 Verify external access per 2FA

- Launch Horizon Client (here from iOS), and enter username and (AD-)password

**VMware Horizon**

<https://lahrmann.noip.me>

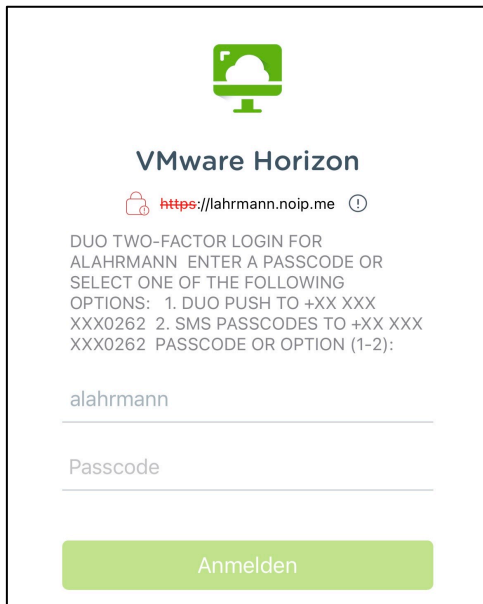
GEBEN SIE IHREN RADIUS  
BENUTZERNAMEN UND PASSWORT EIN.

alahrmann

Passwort

Anmelden

- You can choose now between (1) Duo Push per App or (2) SMS passcode. Alternatively, you can enter the passcode from Duo app directly.



The screenshot shows a login page for VMware Horizon. At the top is a green icon of a monitor with a cloud. Below it, the text reads "VMware Horizon" and "https://lahrmann.noip.me". The main heading is "DUO TWO-FACTOR LOGIN FOR ALAHRMANN ENTER A PASSCODE OR SELECT ONE OF THE FOLLOWING OPTIONS: 1. DUO PUSH TO +XX XXX XXX0262 2. SMS PASSCODES TO +XX XXX XXX0262 PASSCODE OR OPTION (1-2):". There are two input fields: one for the username "alahrmann" and one for the "Passcode". A green button at the bottom is labeled "Anmelden".

## 19. Add MS Entra ID as IdP to Omnisca Access

Reference – [URL](#)

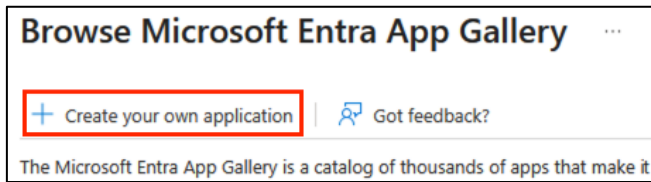
In the Omnisca Access console, you can configure **Microsoft Entra ID MFA** as the secondary authentication method for any supported primary authentication methods in the Omnisca Access service. You configure Microsoft **Entra ID as an identity provider (IDP)** in the Omnisca Access console and then you configure an **Omnisca Access authentication access policy rule** that makes Microsoft Entra ID MFA the secondary authentication method in the rule.

You then configure an **Entra conditional access policy in the Microsoft Entra admin center** to apply the access controls to manage how the secondary authentication is implemented after Omnisca Access primary authentication is completed.

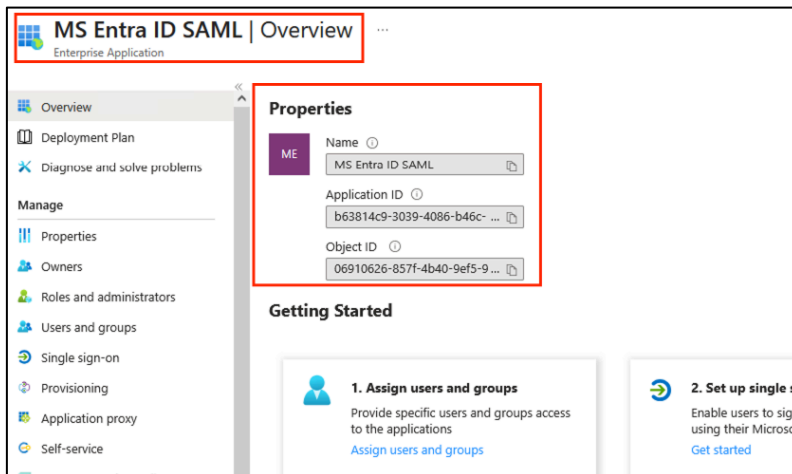
Users use their existing authentication method to log in to Omnisca Access and are then prompted for the Microsoft Entra ID MFA without an additional Entra ID login prompt.

### 19.1 Create Enterprise Application in Entra ID

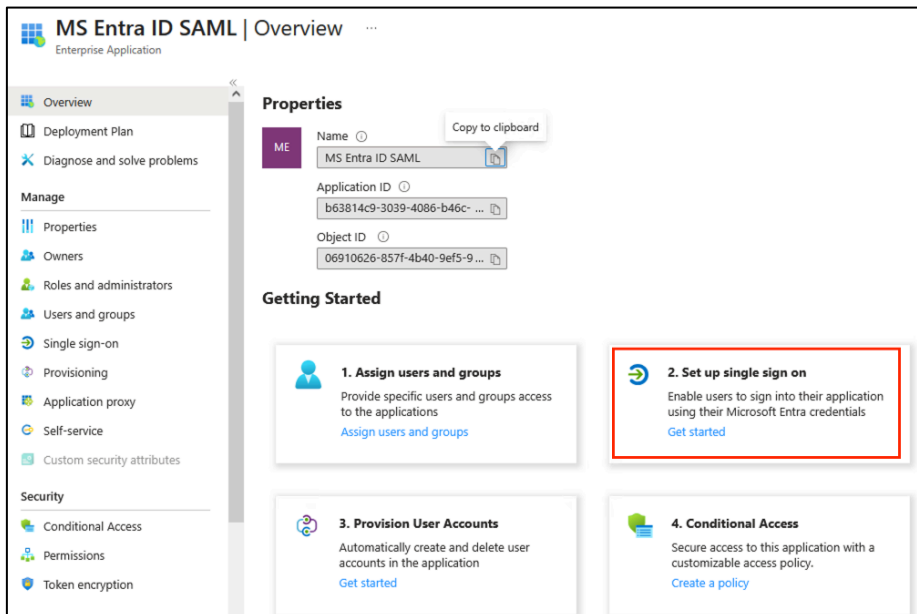
- In **MS Entra admin center**<sup>9</sup>, go to →Entra ID →Enterprise apps →All applications and click →New application →Create your own application



- Set a name and choose “Integrate any other application you don’t find in the gallery (Non-gallery)”
- In the end of the process you should see the new application



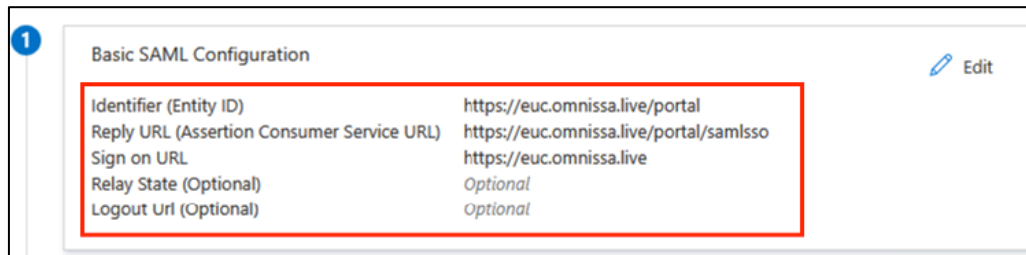
- Select the previously created enterprise application, and go to →Set up single sign on



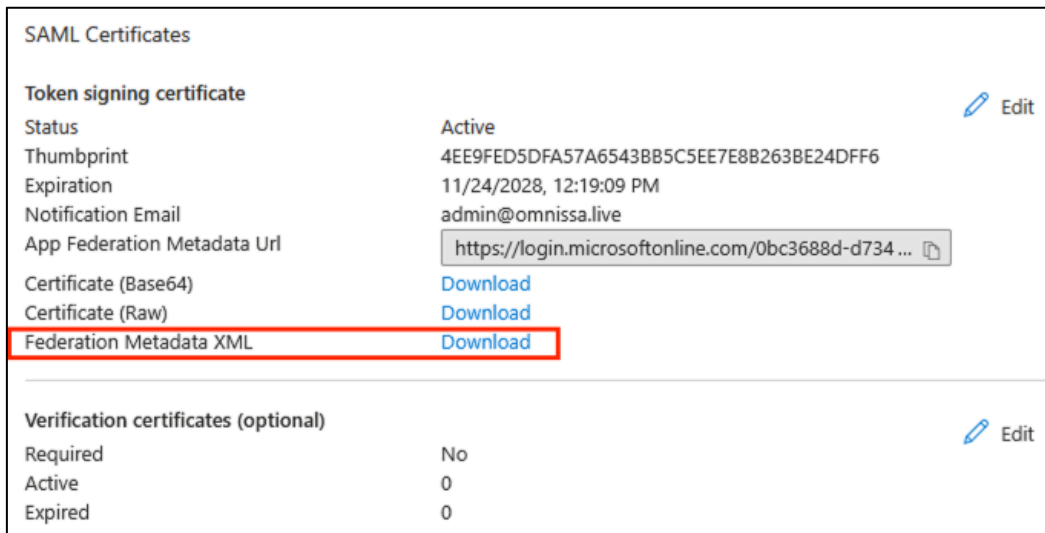
- Select →SAML
- You need to configure the “**Basic SAML configuration**”, and add the following fields:

<sup>9</sup> <https://entra.microsoft.com>

- **Identifier:** https://HORIZON\_UAG\_FQDN/portal  
(i.e. https://euc.omnissa.live/portal)
- **Reply URL:** https://HORIZON\_UAG\_FQDN/portal/samlSso  
(i.e. https://euc.omnissa.live/portal/samlSso)
- **Sign on URL:** https://HORIZON\_UAG\_FQDN  
(i.e. https://euc.omnissa.live)
- Click →Save



- Under →SAML Certificates, you now can download the IdP metadata:



## 19.2 Configure Entra ID as IdP in Omnissa Access

- In **Omnissa Access**, go to →Integrations →Identity Providers, click →Add and select SAML IDP
- Configure the settings for SAML IDP
  - General Information (Identity Provider Name and Type)

- Under Identity Provider Metadata, enter the content from the previously downloaded xml file and click →Process IdP Metadata

**SAML Metadata**

SAML metadata is used to establish trust with the IdP.

Identity Provider Metadata (URL or XML)

```

eIixZ+pkIQWso2YofnzyWQD5TsGOBBZP>5IHPJspMIPnLmMNSBOGE2A25y+IleWdOyymbG7Xudl6Uu6a
wA6lyKj6BxZ5i4wr7gutlUdfDnExRLPLF50lir</X509Certificate></X509Data></KeyInfo></
KeyDescriptor><SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://login.microsoftonline.com/Obc3688d-d734-41ca-b0f1-0e2b7dd68adb/saml2" /
><SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://login.microsoftonline.com/Obc3688d-d734-41ca-b0f1-0e2b7dd68adb/saml2" /
><SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://
login.microsoftonline.com/Obc3688d-d734-41ca-b0f1-0e2b7dd68adb/saml2" /></
IDPSSODescriptor></EntityDescriptor>

```

Process IdP Metadata

- Under “Binding Protocol”, select →HTTP Redirect

**SAML Metadata**

Binding Protocol: HTTP Redirect

SAML metadata is used to establish trust with the IdP.

Identity Provider Metadata (URL or XML)

```

eIixZ+pkIQWso2YofnzyWQD5TsGOBBZP>5IHPJspMIPnLmMNSBOGE2A25y+IleWdOyymbG7Xudl6Uu6a
wA6lyKj6BxZ5i4wr7gutlUdfDnExRLPLF50lir</X509Certificate></X509Data></KeyInfo></
KeyDescriptor><SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://login.microsoftonline.com/Obc3688d-d734-41ca-b0f1-0e2b7dd68adb/saml2" /
><SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://login.microsoftonline.com/Obc3688d-d734-41ca-b0f1-0e2b7dd68adb/saml2" /
><SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://
login.microsoftonline.com/Obc3688d-d734-41ca-b0f1-0e2b7dd68adb/saml2" /></
IDPSSODescriptor></EntityDescriptor>

```

Process IdP Metadata

- Enable “Send Subject in SAML Request (when available)”

Name ID Policy in SAML Request: urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

Send Subject in SAML Request (when available)

Use Name ID format mapping for Subject

- Select the users which can authenticate using this IdP

**Users**

Select which users can authenticate using this IdP. Choose from the available directories from the list below.

EUCLAB.ORG

- Select the networks this IdP can be accessed from (typically no internal networks)

**Network**

Select which networks this IdP can be accessed from. Choose from the available network ranges from the list below.

ALL RANGES

EUCLAB internal network

- Enter the authentication method with the given SAML context and a description for end users

**Authentication Methods**

Select which authentication methods the IdP will use to authenticate users.

Authentication Method	SAML Context	Description
entraMFA	urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified	<input type="checkbox"/> Custom Enter Entra ID MFA

## 20. Configure Horizon - UAG with MS Entra ID as IdP

Reference – [URL](#)

Prerequisites:

- A Microsoft Entra user account with an active subscription. If you don't already have one, you can Create an [account for free](#). (just a personal Microsoft account is not sufficient!)
- In Entra ID, create a service account which has the “Hybrid Identity Administrator” role assigned.

### 20.1 Add custom domain name to Entra ID tenant

Reference – [URL](#)

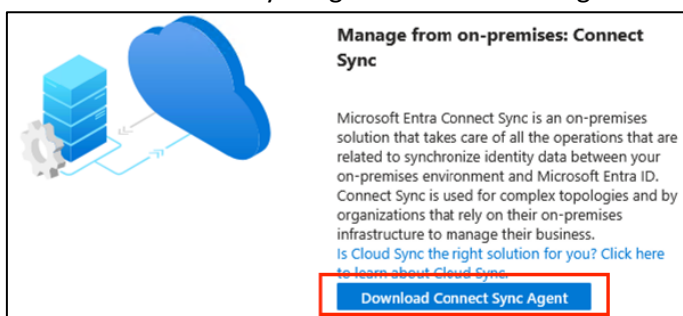
Microsoft Entra tenants come with an initial domain name like domainname.onmicrosoft.com. You can't change or delete the initial domain name, but you can add your organization's DNS name as a custom domain name and set it as primary. By adding your domain name, you can add user names that are familiar to your users, such as alain@contoso.com.

### 20.2 Sync on-prem AD with MS Entra ID

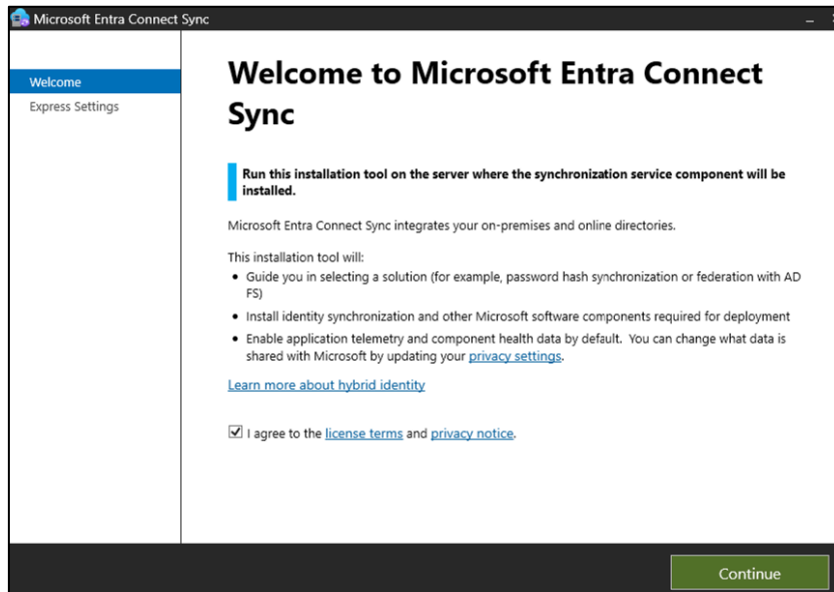
MS Entra Connect Sync, Version 2.5.79.0

With a MS Entra Connect Sync server AD users and groups can be synced between an on-prem AD and the Entra ID.

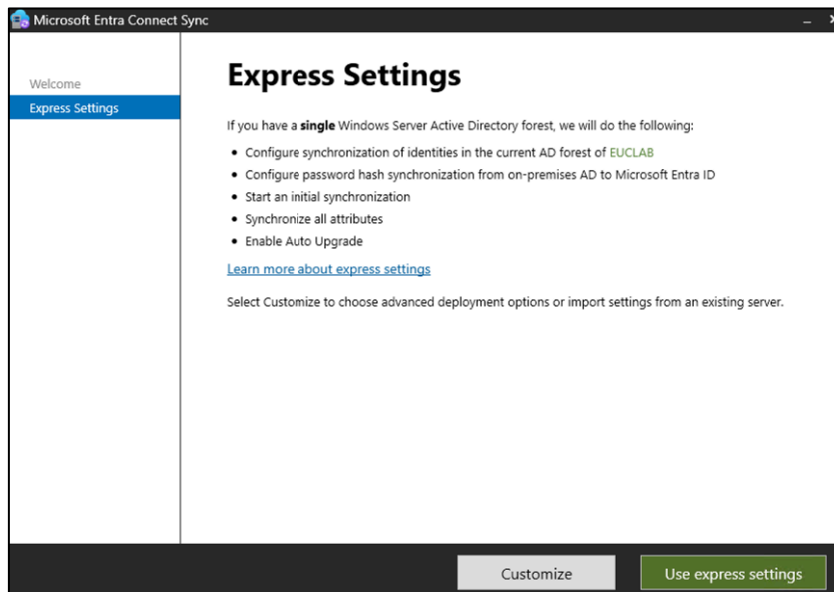
- In MS Entra admin center, go to →Entra ID →Entra Connect →Get started, and click on “Download Connect Sync Agent” under →Manage from on-premises: Connect Sync.



- You need a prepared MS Windows Server (at least 2016), domain-joined. Execute the installer file "AzureADConnect.msi".



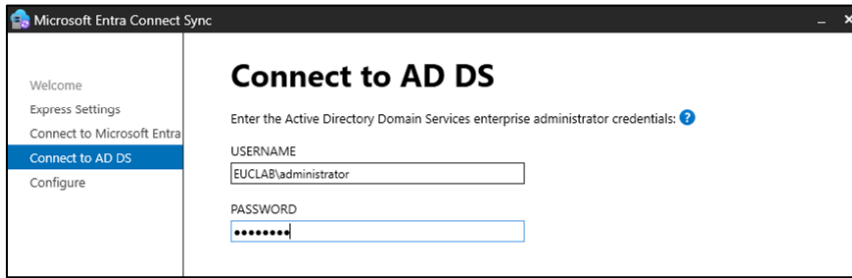
- You can use express settings for a single AD



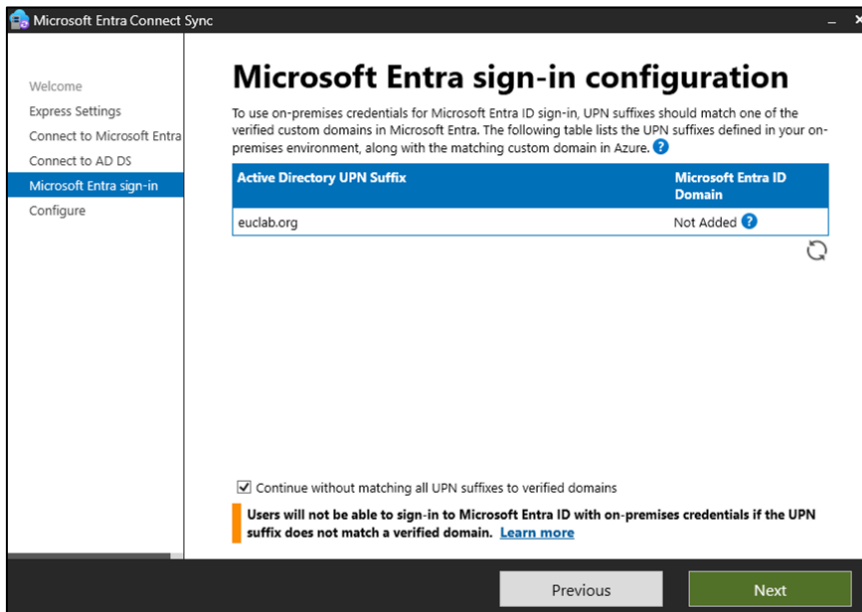
- Enter the username for your MS Entra ID Hybrid Identity Administrator account, and click →Next



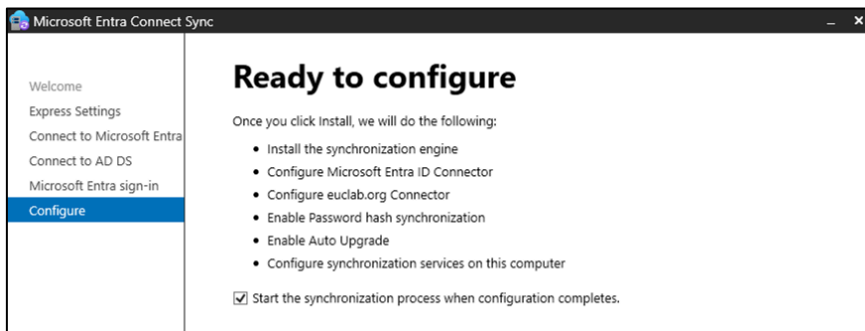
- Enter the credentials of you on-prem AD administrator, and click →Next



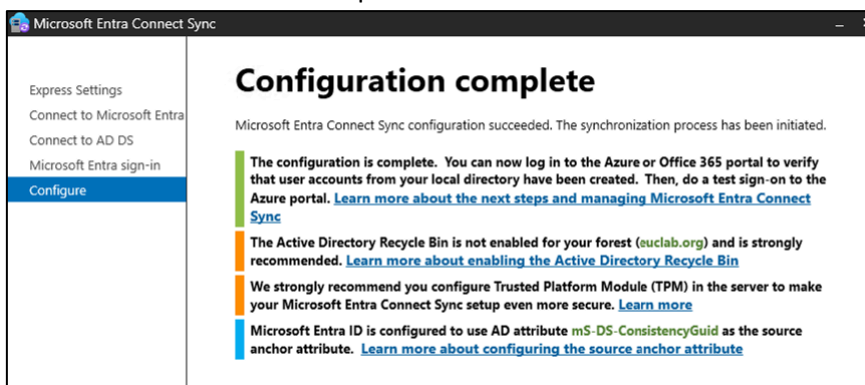
- Continue without matching app UPN suffixes to verified domains



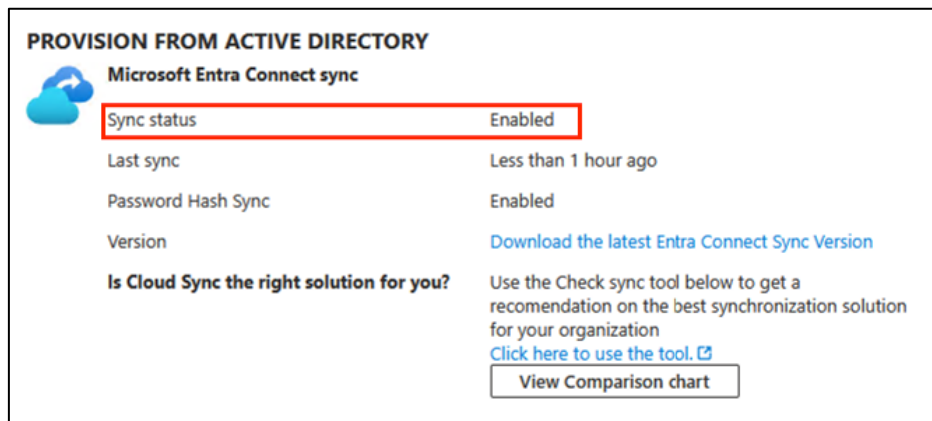
- Click →Install



- It takes a few minutes to complete



- You can check the functionality in MS Entra admin center under →Entra ID →Entra Connect →Connect Sync

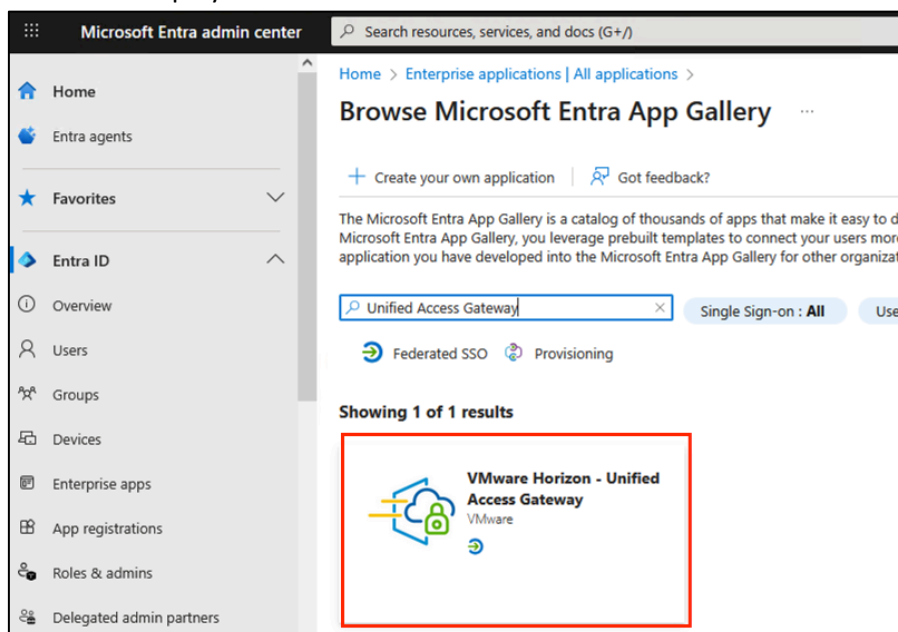


- Also you can verify synchronization if on-prem AD users and groups are shown under →Entra ID →User now. Be aware, that the UPN is different from the on-prem AD!

## 20.3 Add UAG in MS Entra from the gallery

We need the UAG as managed SaaS, and add this from the gallery.

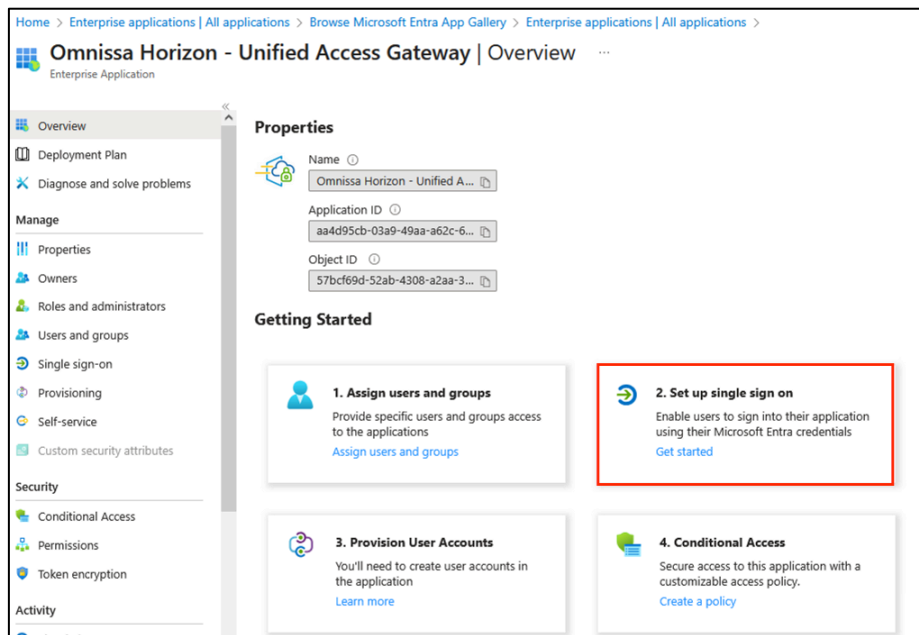
- In **MS Entra admin center**<sup>10</sup>, go to →Entra ID →Enterprise apps →All applications and click →New application and search and select for “Unified Access Gateway” – it takes a few seconds to deploy:



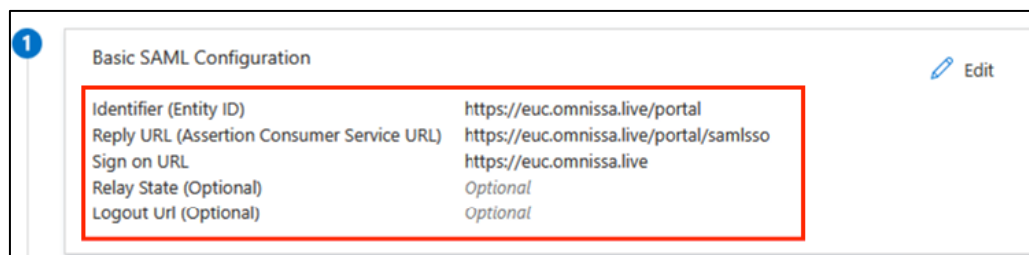
<sup>10</sup> <https://entra.microsoft.com>

## 20.4 Configure MS Entra SSO for the UAG

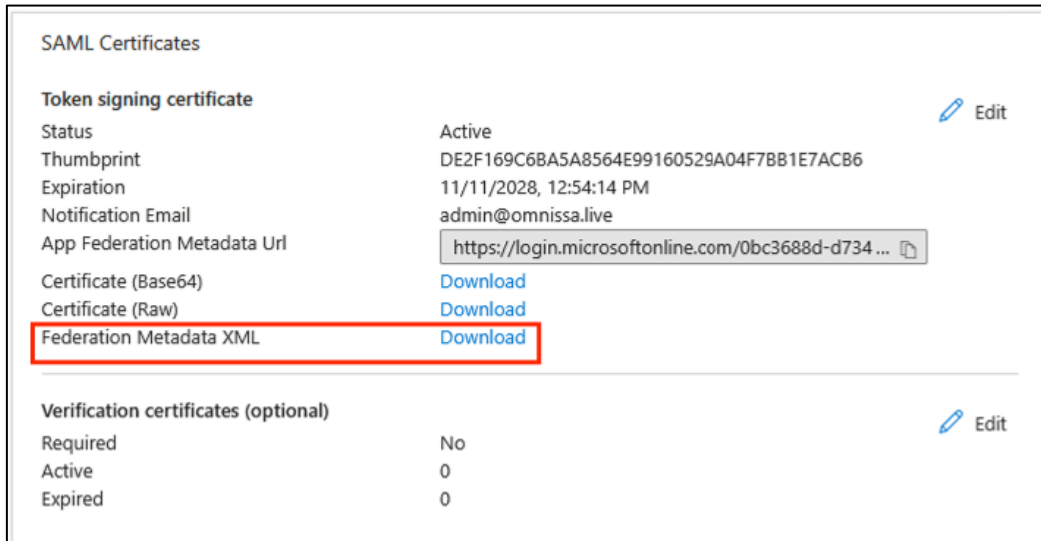
- Select the previously created enterprise application, and go to →Set up single sign on



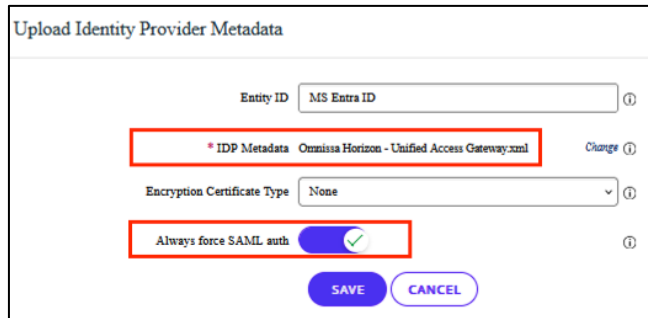
- Select →SAML
- You need to configure the “Basic SAML configuration”, and add the following fields:
  - **Identifier:** https://HORIZON\_UAG\_FQDN/portal  
(i.e. https://euc.ommissa.live/portal)
  - **Reply URL:** https://HORIZON\_UAG\_FQDN/portal/samlso  
(i.e. https://euc.ommissa.live/portal/samlso)
  - **Sign on URL:** https://HORIZON\_UAG\_FQDN  
(i.e. https://euc.ommissa.live)
  - Click →Save



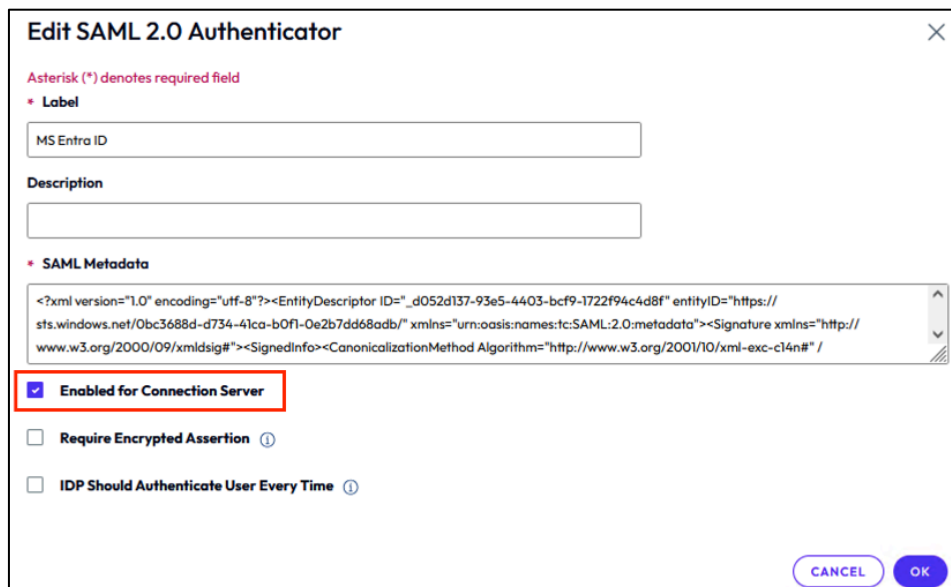
- Under →SAML Certificates, you now can download the IdP metadata:



- You need this metadata, to upload them to the UAG under →Advanced Settings →Identity Bridging Settings →Upload Identity Provider Metadata:



- Furthermore, you need to add this metadata for the Connection Server(s), in the Horizon Console under →Settings →Servers →Connection Servers, select one Connection Server, go to →Edit →Authentication, and click on →Manage SAML Authenticators. Add the ifnroamtion you have downloaded previously from MS Entra admin center:

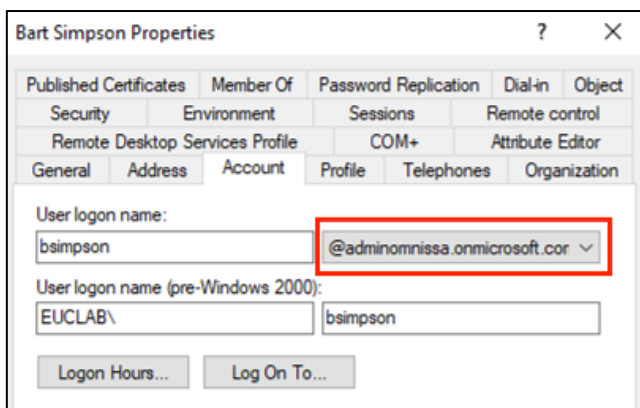
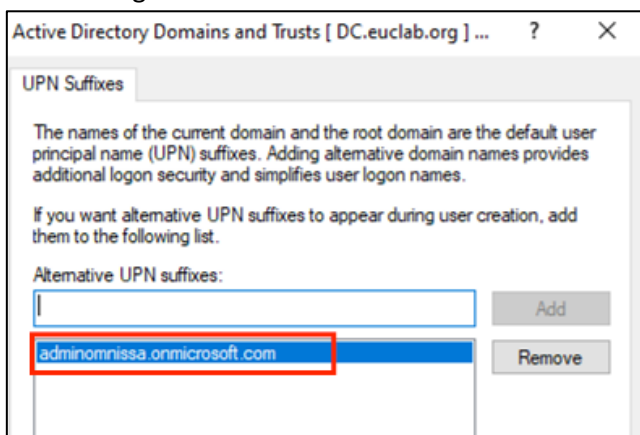


- To add users and groups, select the enterprise application again, and go to →Assign users and groups, then click →Add user/group

## 20.5 Open concern

When UAG and Horizon is configured with Entra ID as IdP, there is are two major concerns.

1. All AD users are synced from on-prem Active Directory (without filtering specific users/groups only).
2. Additionally, for every user a new UPN in the format *username@domain.onmicrosoft.com* is created in Entra ID. To use these UPNs for login via UAG, in the on-prem domain this “alternative UPN suffix” needs to be added in the →Active Directory Domains and Trusts, and the AD-users need to be configured to use this alternative UPN:



Actually, SSO is not usable, as after successful authentication against UAG, the user can select his Horizon session, but gets prompted for the AD credentials again during the login.

## 21. Linux Deployment in Horizon

## 21.1 Create a Linux VM in vSphere

Done with Red Hat Enterprise Linux Workstation 8.10

- Verify System Requirements for Horizon Agent for Linux, see [URL](#)
- Install Linux OS
  - Check network connectivity (DNS, GW, DHCP etc.)
  - Set hostname as FQDN (<https://access.redhat.com/solutions/5444941>)
    - hostname
    - hostnamectl
    - hostnamectl set-hostname FQDN
- Prepare Linux VM for cloning as golden image ([URL](#))
  - To make sure that desktop users are added to the local Remote Desktop Users group of the virtual machine, create a restricted Remote Desktop Users group in Active Directory
  - **Map the Linux machine's host name to 127.0.0.1 in the /etc/hosts file?**

```
[root@gm-rhel8x admin]# cat /etc/hosts
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4 gm-rhel8x
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6 gm-rhel8x
[root@gm-rhel8x admin]#
```

```
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4 gm-rhel8x gm-rhel8x.euclab.org
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6 gm-rhel8x gm-rhel8x.euclab.org
```
  - Install service packs and updates to the guest Linux distribution
  - If needed, manually install OVT (Open VMware Tools) on the machine
  - Verify that `virbr0` is deactivated
    - `sudo virsh net-destroy default`
    - `sudo virsh net-undefine default`
    - `sudo service libvirt restart`
  - check DNS between Linux OS and Horizon Connection Server
  - Configure the Linux machine to run in graphical mode by default
    - `sudo systemctl set-default graphical.target`
  - Install `libXScrnSaver`
    - `sudo yum install libXScrnSaver11`
  - Install Linux Dependency Packages for Horizon Agent, see [URL](#)
    - `sudo yum install libappindicator-gtk3`
    - `sudo yum install nss-tools`
- Install Horizon Agent, [URL](#)
  - Extract the `tar.gz` file on a local folder
  - Run the `install_viewagent.sh` script – command line option [here](#)
    - `sudo ./install_viewagent.sh`
  - Reboot Linux VM
  - Check status of Horizon Agent
    - `sudo service viewagent status`
- Configure SSSD Offline Domain Join ([URL](#))
  - Ensure that the golden image uses the same domain as the instant clones
  - Check that DNS lookup of AD is resolving

---

<sup>11</sup> Not documented yet (but requested by Agent installer)

- dig +short SRV \_ldap.\_tcp.addomain.test
  - dig +short SRV \_kerberos.\_tcp.addomain.test
  - dig +short SRV \_kerberos.\_udp.addomain.test
- Discovering and joining an AD Domain using SSSD ([URL](#)) - Connecting to AD using POSIX ID mapping
  - Install the following packages
 

```
yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli krb5-workstation
```
- To display information for a specific domain, run `realm discover` and add the name of the domain you want to discover
  - `realm discover ad.example.com`

```
[root@qm-rhel8x admin]# realm discover euclab.org
euclab.org
type: kerberos
realm-name: EUCLAB.ORG
domain-name: euclab.org
configured: no
server-software: active-directory
client-software: sssd
required-package: oddjob
required-package: oddjob-mkhomedir
required-package: sssd
required-package: adcli
required-package: samba-common-tools
[root@qm-rhel8x admin]#
```

- Configure the local RHEL system with the `realm join` command
  - `realm join ad.example.com`
- You can check again now
  - `realm discover ad.example.com`

```
[root@qm-rhel8x admin]# realm discover euclab.org
euclab.org
type: kerberos
realm-name: EUCLAB.ORG
domain-name: euclab.org
configured: kerberos-member
server-software: active-directory
client-software: sssd
required-package: oddjob
required-package: oddjob-mkhomedir
required-package: sssd
required-package: adcli
required-package: samba-common-tools
login-formats: %U@euclab.org
login-policy: allow-realm-logins
[root@qm-rhel8x admin]#
```

- Check that you can login with a domain account

- Check the `/etc/sss/sss.conf` configuration file, that it includes the proper DNS name of the AD domain, as follows:

```
[sss]
domains = euclab.org
config_file_version = 2
services = nss, pam

[domain/euclab.org]
ad_domain = euclab.org
krb5_realm = EUCLAB.ORG
realmd_tags = manages-system joined-with-adcli
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
```

- Modify the `/etc/krb5.conf` configuration file to use only the rc4-hmac encryption algorithm
  - To ensure that Horizon Agent recognizes the Linux VM as domain-joined using SSSD authentication, add/edit the following line to the `/etc/omnissa/viewagent-custom.conf` configuration file
    - `OfflineJoinDomain=sss`
  - Check and edit the `/etc/krb5.conf` file, and add/edit this entry:
    - `default_realm = DOMAIN.COM`
- Power off the Golden Master and take a snapshot
- 
- Prepare a Linux Machine for Remote Desktop Deployment, see [URL](#)
    - Add hostname (short and FQDN) to the `/etc/hosts` file

```
127.0.0.1    RHEL-GM810 RHEL-GM810.euclab.org localhost
localhost.localdomain localhost4 localhost4.localdomain4
```
  - Install Linux Dependency Packages for Horizon Agent, see [URL](#)

```
sudo yum install libappindicator-gtk3
sudo yum install nss-tools
```
  - Install the Horizon Agent (use the rpm file), see [URL](#)
  - After installing Horizon Agent, install libXScrnSaver

```
sudo yum install libXScrnSaver
```
  - You can check the agent service status

```
sudo service viewagent status
```
  - Add machine to domain ([URL](#))

```
realm join --user=[domain user account] [domain name]
```

    - You can check the domain status

```
realm list
```

- Switch to root user  
su
- Disable root login per SSH - Open the /etc/ssh/sshd\_config and set PermitRootLogin to no

## 22. Nacharbeiten

Eingeschränkte Rechte im vCenter und in der AD für den View Composer nötig:

AD-Account für den View Composer:

<https://docs.vmware.com/en/VMware-Horizon-7/7.10/horizon-installation/GUID-3446495C-FEC8-425C-AFF8-A6CAABA5E973.html>

Ferner muss dieser AD-Account administrative Rechte auf dem Composer Server haben

vCenter User bzw. Rolle

<https://docs.vmware.com/en/VMware-Horizon-7/7.10/horizon-installation/GUID-467F552F-3034-4917-A985-B5E5FEC5C68F.html>

Getestet und läuft.

View Composer and Instant Clone Privileges Required for the vCenter Server User

<https://docs.vmware.com/en/VMware-Horizon-7/7.12/horizon-installation/GUID-467F552F-3034-4917-A985-B5E5FEC5C68F.html>

Example of Filtering to Exclude Domains

<https://docs.vmware.com/en/VMware-Horizon-7/7.13/horizon-administration/GUID-FD0A107B-9F2C-45A5-B0CE-D3793BD2C3B0.html>

<https://kb.vmware.com/s/article/2006292>

Configure CA Certificates in App Volumes Manager

<https://docs.vmware.com/en/VMware-App-Volumes/2103/app-volumes-admin-guide/GUID-4EA6EF73-7800-4241-9162-2C407AC4AA7A.html>

Troubleshooting Horizon 7 Server Certificate Revocation Checking

<https://docs.vmware.com/en/VMware-Horizon-7/7.13/horizon-administration/GUID-EF771194-AE61-49D1-8424-ADB1D0CA0859.html>

Configuring Certificate Revocation Checking on Server Certificates

<https://docs.vmware.com/en/VMware-Horizon-7/7.13/horizon-installation/GUID-D1190AE8-1677-4637-9345-BEE0F39507DF.html>

## 22.1 Troubleshooting Horizon

Instant-Clone Maintenance Utilities

IcCleanup.cmd – Tool um interne VMs zu identifizieren und zu löschen. Hierbei können vor allem die Abhängigkeiten der internen VMs untereinander sichtbar gemacht werden.

<https://docs.vmware.com/en/VMware-Horizon-7/7.13/virtual-desktops/GUID-6025D684-2E05-4857-9C24-18F16DDC38FD.html>

After updating Horizon View to 8.3, the Web browser access doesn't work anymore

<https://www.comdivision.com/blog/horizon-view-upgrade-8-3-2106>

<https://kb.vmware.com/s/article/85801>

When connecting to a Horizon View virtual machine using Blast, SSL Session is invalid

<https://kb.vmware.com/s/article/2088354>

Certificate issue connecting to VDI per HTML

<https://communities.vmware.com/t5/Horizon-Desktops-and-Apps/Certificate-issue-connecting-to-VDI/td-p/494117>

**Use Case: Sessions per HTML Client sollen nicht getunnelt werden – nach erfolgreichem Login erscheint jeweils eine Zertifikatsfehlermeldung**

- CS verwendet bereits DNS anstatt IP adressen
- Wildcard-Zertifikat für Horizon Agent
  - <https://www.petenetlive.com/KB/Article/0001128>

- <https://robbieroberts.wordpress.com/2014/04/04/creating-a-wildcard-webserver-certificate-with-your-internal-microsoft-ca/>

c. -->Funktioniert nun:

i. <https://kb.vmware.com/s/article/2088354>

ii. Wichtig: Der Thumbprint in der Registry muss mit Leerzeichen hinterlegt werden (wie im Beispiel des KB-Artikels)

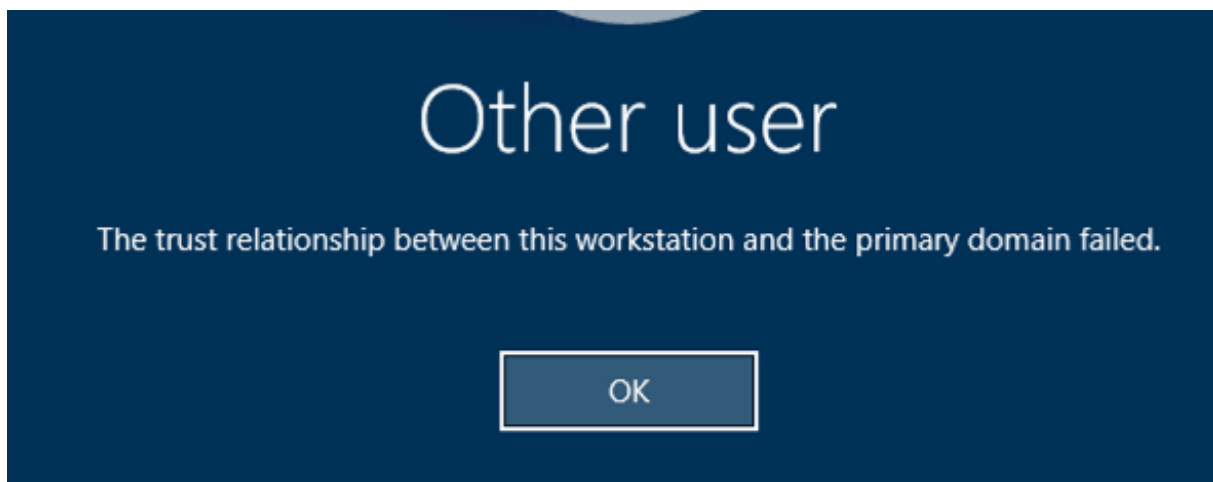
Administration dashboard in VMware Horizon reports the error: Server's certificate cannot be checked (2000063)

<https://kb.vmware.com/s/article/2000063>

**Reset 120 day RDS Grace period on Windows Server 2016, 2019, 2022**

<https://www.virtualizationhowto.com/2020/10/reset-120-day-rds-grace-period-on-2016-and-2019/>

**The trust relationship between this workstation and the primary domain failed.**



See <https://learn.microsoft.com/en-us/answers/questions/1284756/fix-broken-trust-relationship-without-local-admin>

- disconnect the machine from network
- log in with the domain admin credentials
- reconnect the machine to the network
- run the following command from Windows Powershell:  
Reset-ComputerMachinePassword

## 23. Scripting & Automation

### 23.1 S&A Horizon

#### 23.1.1 FSLogix – create a VHD(X) disk per user AND pool ID OR Hostname

If a user should get more than one FSLogix disk, you can create a PS-script, like this – it will get the pool ID AND/Or Hostname, and set it to an environment variable:

```
# -----
# hzn-post-sync.ps1 script
#
# This script reads a registry value to determine the Horizon Pool ID,
# creates a persistent system environment variable, and notifies the system
# of the change.
#
# Modifications:
# - Added logging functionality to C:\temp\fslogixmap.txt.
# - The entire script is now wrapped in a try/catch block to ensure all
# output and errors are captured in the log file, even if the script fails.
# -----

# Define the path for the log file
$logFilePath = "C:\temp\fslogixmap.txt"

# Ensure the log directory exists
if (-not (Test-Path -Path "C:\temp")) {
    New-Item -Path "C:\temp" -ItemType Directory -Force | Out-Null
}

# Start the transcript to capture all console output to the log file
Start-Transcript -Path $logFilePath -Append

try {
    Write-Host "--- Script execution started at $(Get-Date) ---"

    # --- Read the registry value
    $regPath = "HKLM:SOFTWARE\Omnissa\Horizon\Node Manager"
    $regName = "Server Pool DN"

    try {
        Write-Host "Reading registry key: $regPath\$regName"
        $fullValue = (Get-ItemProperty -Path $regPath -Name
$logName).$regName
        Write-Host "Successfully read registry value: '$fullValue'"
    } catch {
        Write-Error "Unable to read registry key $regPath\$regName"
        exit 1
    }

    # --- Extract PoolID (after cn= and before the first comma)
    if ($fullValue -match "cn=(^[^,]+)") {
        $poolID = $matches[1]
        Write-Host "Extracted PoolID: '$poolID'"
    } else {
```

```

        Write-Error "Unable to extract poolID from '$fullValue'"
        exit 1
    }

    # --- Write persistent system environment variable
    Write-Host "Setting system environment variable HZNPoolID to '$poolID'"
    Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Session
Manager\Environment" `
        -Name "HZNPoolID" -Value $poolID

    # --- Notify Windows that environment variables changed
    Write-Host "Notifying Windows of environment variable change..."
    $signature = @"
[DllImport("user32.dll", SetLastError=true)]
public static extern IntPtr SendMessageTimeout(IntPtr hWnd, int Msg, IntPtr
wParam, string lParam, uint fuFlags, uint uTimeout, out IntPtr lpdwResult);
"@
    $SendMessageTimeout = Add-Type -MemberDefinition $signature -Name
"Win32SendMessageTimeout" -Namespace Win32Functions -PassThru
    $HWND_BROADCAST = [IntPtr]0xffff
    $WM_SETTINGCHANGE = 0x1A
    $result = [IntPtr]::Zero
    $SendMessageTimeout::SendMessageTimeout($HWND_BROADCAST,
$WM_SETTINGCHANGE, [IntPtr]::Zero, "Environment", 2, 5000, [ref]$result) |
Out-Null

    Write-Host "System Variable HZNPoolID defined as '$poolID'"

    # Get the hostname
    $hostname = $env:COMPUTERNAME

    # Keep only the first 4 characters (safe handling if shorter)
    if ($hostname.Length -ge 4) {
        $shortHostname = $hostname.Substring(0,6)
    } else {
        $shortHostname = $hostname
    }

    # Save into permanent System Environment Variable (requires admin rights)
    [System.Environment]::SetEnvironmentVariable('ShortHost', $shortHostname,
'Machine')

    Write-Output "Shortened hostname saved system-wide as 'ShortHost':
$shortHostname"

} catch {
    # Catch any unexpected errors during script execution and write them to
the transcript.
    Write-Error "An unexpected error occurred during script execution:"
    Write-Error $_
} finally {
    # This block ensures the transcript is stopped, even if an error
occurred.
    Write-Host "--- Script execution finished at $(Get-Date) ---"
    Stop-Transcript
}

```

This should be executed via cmd-file (and placed as post-synchronization-script in the desktop pool settings in Horizon Console:

```

@echo off
REM -- hzn-post-sync.cmd script

REM --- Set Log file path
set "LogFile=C:\Temp\hzn_post_sync_log.txt"

REM --- Start Logging - overwrite any existing log file
echo [START] hzn-post-sync.cmd execution started on %date% at %time% >
"%LogFile%"
echo. >> "%LogFile%"

REM --- Get current PowerShell ExecutionPolicy
echo Getting current PowerShell ExecutionPolicy... >> "%LogFile%"
for /f "usebackq delims=" %%P in (`powershell -Command "Get-
ExecutionPolicy"`) do (
    set "SavedPolicy=%%P"
)

echo Saved ExecutionPolicy: %SavedPolicy% >> "%LogFile%"

REM --- Set a temporary ExecutionPolicy (example: RemoteSigned)
echo Setting temporary ExecutionPolicy to Unrestricted... >> "%LogFile%"
powershell -Command "Set-ExecutionPolicy Unrestricted -Force" >>
"%LogFile%" 2>&1

echo Temporary ExecutionPolicy set to Unrestricted >> "%LogFile%"
echo. >> "%LogFile%"

REM --- Running PowerShell Script to Get Pool ID
echo Running PowerShell Script C:\Temp\fslogix\hzn-post-sync.ps1... >>
"%LogFile%"
powershell -File C:\Temp\fslogix\hzn-post-sync.ps1 >> "%LogFile%" 2>&1
REM The '2>&1' part above redirects standard error (2) to standard output
(1)
REM and then appends both to the log file.

echo. >> "%LogFile%"

REM --- Restore the original ExecutionPolicy
echo Restoring original ExecutionPolicy: %SavedPolicy%... >> "%LogFile%"
powershell -Command "Set-ExecutionPolicy %SavedPolicy% -Force" >>
"%LogFile%" 2>&1

echo Original ExecutionPolicy restored to %SavedPolicy% >> "%LogFile%"
echo. >> "%LogFile%"
echo [END] hzn-post-sync.cmd execution finished on %date% at %time% >>
"%LogFile%"

shutdown -r -t 0

```

The last step is the configure the FSLogix GPO in order to specify where to create the VHD(X) files – under →Computer Configurations\Policies\Administrative Templats\FsLogix\Profile Containers\Container and Directory Naming

**Tabelle 2: For Pool ID environment variable**

GPO Key	GPO Settings	Details
---------	--------------	---------

SID Directory Name Pattern	%HZNPoolID%.%userdomain%	Use POOL ID and Users domain, i.e. : MYPOOL_MYDOMAIN
SID Directory Name Match	%HZNPoolID%.%userdomain%	Need to be the same as Name Pattern
VHD Name Pattern	Profile_%username%.%profileversion%	Use Profile_ as prefix and then username and profile version
VHD Name Match	Profile_%username%.%profileversion%*	Ask to look for any containers with prefix set by pattern
Volume Type (VHD,VHDX)	VHDX	Specify to use VHDX container

**Tabelle 3: For Hostname environment variable**

GPO Key	GPO Settings	Details
SID Directory Name Pattern	%shortHostname%.%userdomain%	Use hostname prefix and Users domain ex : HOSTNA_DOMAIN
SID Directory Name Match	%shortHostname%.%userdomain%	Need to be the same as Name Pattern
VHD Name Pattern	Profile_%username%.%profileversion%	Use Profile_ as prefix and then username and profile version
VHD Name Match	Profile_%username%.%profileversion%*	Ask to look for any containers with prefix set by pattern
Volume Type (VHD,VHDX)	VHDX	Specify to use VHDX container

Now, as the environment variable is created at the time of the deployment of the VM, FSLogix GPO will use it to create/usr the right folder and container.

Reference: <https://my-virt.alfadir.net/index.php/2025/09/24/create-fslogix-based-on-pool-id-or-hostname-prefix/>

### Horizon As Built Report

<https://github.com/AsBuiltReport/AsBuiltReport.VMware.Horizon>

### PowerCLI Script to Horizon Desktop Pool machine counts & provisioning type

<https://www.retouw.nl/2022/03/26/powercli-script-to-horizon-desktop-pool-machine-counts-provisioning-type/>

## 24. References and KBs

EUC Component	Reference	URL
Horizon	Create a User Account for Instant-Clone Operations	<a href="https://docs.vmware.com/en/VMware-Horizon/2312/horizon-installation/GUID-E91881F4-F8C0-48A5-A1A4-61577E287E29.html">https://docs.vmware.com/en/VMware-Horizon/2312/horizon-installation/GUID-E91881F4-F8C0-48A5-A1A4-61577E287E29.html</a>
Horizon	Privileges Required for the vCenter Server User With Instant Clones	<a href="https://docs.omnissa.com/de-DE/bundle/Horizon8InstallUpgrade/page/PrivilegesRequiredforthevCenterServerUserWithInstantClones.html">https://docs.omnissa.com/de-DE/bundle/Horizon8InstallUpgrade/page/PrivilegesRequiredforthevCenterServerUserWithInstantClones.html</a>
Horizon	Generating a certificate template and generating/renewing certificate for Horizon connection server	<a href="https://kb.vmware.com/s/article/80314">https://kb.vmware.com/s/article/80314</a>
Horizon	Cross-Origin Resource Sharing (CORS) with Horizon 8 and loadbalanced HTML5 access	<a href="https://kb.vmware.com/s/article/85801">https://kb.vmware.com/s/article/85801</a>
Horizon	Add a Horizon 8 ADMX Template File to a GPO	<a href="https://docs.vmware.com/en/VMware-Horizon/2312/horizon-remote-desktop-features/GUID-633FB6A2-206E-40A2-A72B-0FD28823EBCA.html">https://docs.vmware.com/en/VMware-Horizon/2312/horizon-remote-desktop-features/GUID-633FB6A2-206E-40A2-A72B-0FD28823EBCA.html</a>
Horizon	Horizon Cloud Pod (CPA) : After an upgrade to Horizon 8.7 or 8.8 (2209, 2212) with CPA, A Connection Server randomly goes offline and requires a service restart (92558)	<a href="https://kb.vmware.com/s/article/92558">https://kb.vmware.com/s/article/92558</a>
Horizon	Purging old data from the Horizon Events Database (2150309)	<a href="https://kb.vmware.com/s/article/2150309">https://kb.vmware.com/s/article/2150309</a>

Horizon	Instant-Clone Maintenance Utilities	<a href="https://docs.omnissa.com/bundle/Desktops-and-Applications-in-HorizonV2406/page/InstantCloneMaintenanceUtilities.html">https://docs.omnissa.com/bundle/Desktops-and-Applications-in-HorizonV2406/page/InstantCloneMaintenanceUtilities.html</a>
Horizon	Configuring Domains and Trust Relationships for Microsoft Active Directory	<a href="https://docs.omnissa.com/de-DE/bundle/Horizon8InstallUpgrade/page/ConfiguringDomainsandTrustRelationshipsforMicrosoftActiveDirectory.html">https://docs.omnissa.com/de-DE/bundle/Horizon8InstallUpgrade/page/ConfiguringDomainsandTrustRelationshipsforMicrosoftActiveDirectory.html</a>
Horizon	Providing Secondary Credentials for Administrators Using the -T Option	<a href="https://docs.omnissa.com/de-DE/bundle/Horizon-AdministrationV2406/page/ProvidingSecondaryCredentialsforAdministratorsUsingthe-TOption.html">https://docs.omnissa.com/de-DE/bundle/Horizon-AdministrationV2406/page/ProvidingSecondaryCredentialsforAdministratorsUsingthe-TOption.html</a>
Horizon Edge Gateway	Add and Deploy a Horizon 8 Edge	<a href="https://docs.omnissa.com/bundle/HorizonCloudServicesUsingNextGenGuide/page/DeployaHorizonEdgeforUsewithHorizon8DeploymentsandtheHorizonCloudService-next-genControlPlane.html">https://docs.omnissa.com/bundle/HorizonCloudServicesUsingNextGenGuide/page/DeployaHorizonEdgeforUsewithHorizon8DeploymentsandtheHorizonCloudService-next-genControlPlane.html</a>
Horizon CLI	Automating VMware Horizon 8 with VMware PowerCLI	<a href="https://blogs.vmware.com/euc/2023/01/vmware-horizon-8-powercli.html">https://blogs.vmware.com/euc/2023/01/vmware-horizon-8-powercli.html</a>
Horizon CLI	Horizon Powershell Module	<a href="https://developer.omnissa.com/horizon-powercli/">https://developer.omnissa.com/horizon-powercli/</a>
Horizon CLI	Advance Deprecation Announcement for Horizon View API and Replacement with REST API	<a href="https://kb.omnissa.com/s/article/6000139?lang=en_US">https://kb.omnissa.com/s/article/6000139?lang=en_US</a>
Horizon Recording	Using Horizon Recording	<a href="https://docs.omnissa.com/de-DE/bundle/Desktops-and-Applications-in-HorizonV2312/page/UsingHorizonRecording.html">https://docs.omnissa.com/de-DE/bundle/Desktops-and-Applications-in-HorizonV2312/page/UsingHorizonRecording.html</a>
App Volumes	App Volumes User Accounts and Credentials	<a href="https://docs.vmware.com/en/VMware-App-Volumes/2312/app-volumes-install-guide/GUID-6D6AB71B-5632-4C32-8AAF-21DF3B333808.html">https://docs.vmware.com/en/VMware-App-Volumes/2312/app-volumes-install-guide/GUID-6D6AB71B-5632-4C32-8AAF-21DF3B333808.html</a>
App Volumes	Best Practices for Provisioning Virtual Machines and Applications	<a href="https://docs.vmware.com/en/VMware-App-Volumes/2303/app-volumes-admin-guide/GUID-BCC67C19-AC5C-4D25-9F1B-9BE8536A2909.html">https://docs.vmware.com/en/VMware-App-Volumes/2303/app-volumes-admin-guide/GUID-BCC67C19-AC5C-4D25-9F1B-9BE8536A2909.html</a>
App Volumes	Create a Custom vCenter Server Role	<a href="https://docs.omnissa.com/bundle/AppVolumesAdminGuideV2503/page/CreateaCustomvCenterServerRole.html">https://docs.omnissa.com/bundle/AppVolumesAdminGuideV2503/page/CreateaCustomvCenterServerRole.html</a>
App Volumes	Configure CA Certificates in App Volumes Manager	<a href="https://docs.omnissa.com/de-DE/bundle/AppVolumesAdminGuideV2503/page/ConfigureCACertificatesinAppVolumesManager.html">https://docs.omnissa.com/de-DE/bundle/AppVolumesAdminGuideV2503/page/ConfigureCACertificatesinAppVolumesManager.html</a>

App Volumes	Replace the App Volumes Default Self-Signed Certificate	<a href="https://docs.omnissa.com/de-DE/bundle/AppVolumesAdminGuideV2503/page/ReplacetheAppVolumesDefaultSelf-SignedCertificate.html">https://docs.omnissa.com/de-DE/bundle/AppVolumesAdminGuideV2503/page/ReplacetheAppVolumesDefaultSelf-SignedCertificate.html</a>
App Volumes	Creating a new App Volumes AppStack template VMDK changing the default size of 20 GB (also valid for Writables)	<a href="https://kb.vmware.com/s/article/2116022?lang=en_us">https://kb.vmware.com/s/article/2116022?lang=en_us</a>
App Volumes	Pruning the VMware App Volumes SQL database (2132454)	<a href="https://kb.vmware.com/s/article/2132454">https://kb.vmware.com/s/article/2132454</a>
DEM	Configure Dynamic Environment Manager	<a href="https://blog.yahyazahedi.com/2022/12/11/configure-dynamic-environment-manager/">https://blog.yahyazahedi.com/2022/12/11/configure-dynamic-environment-manager/</a>
DEM	Configuring Helpdesk Support Tool	<a href="https://docs.vmware.com/en/VMware-Dynamic-Environment-Manager/2309/com.vmware.dynamic.environment.manager-helpdesk/GUID-B2F834F5-CC85-4BD0-BCF7-F4269298DA2C.html">https://docs.vmware.com/en/VMware-Dynamic-Environment-Manager/2309/com.vmware.dynamic.environment.manager-helpdesk/GUID-B2F834F5-CC85-4BD0-BCF7-F4269298DA2C.html</a>
DEM	VMware Dynamic Environment Manager (DEM) 2312 by Carl Stalhood	<a href="https://www.carlstalhood.com/vmware-user-environment-manager/comment-page-1">https://www.carlstalhood.com/vmware-user-environment-manager/comment-page-1</a>
UAG	Generate CSR and Private Key using uagcertutil Command	<a href="https://docs.omnissa.com/de-DE/bundle/UnifiedAccessGatewayDeployandConfigureV2503/page/GenerateCSRandPrivateKeyusinguagcertutilCommand.html">https://docs.omnissa.com/de-DE/bundle/UnifiedAccessGatewayDeployandConfigureV2503/page/GenerateCSRandPrivateKeyusinguagcertutilCommand.html</a>
FSLogix	FSLogix documentation	<a href="https://learn.microsoft.com/en-us/fslogix/">https://learn.microsoft.com/en-us/fslogix/</a>

## 25. Table of Revisions

Date	Modified/Added Section	Comment
07.11.2025	Added Chapter 17 – Integration in Omnissa Access	
12.11.2025	Reviewed and added chapter 5 about TrueSSO	
19.11.2025	Add chapter 12.5 - 12.5 Omnissa Horizon Accelerator – Horizon 8	
14.01.2026	Add chapter 18.3.1 Update Duo Authentication Proxy	

