

# Advanced WOL PORTAL with optional SSO Support via SAML 2.0

Manual and Installation Guide

---



Allow remote work from  
anywhere at any time.

---

**Secure Remote Wake-on-LAN Management for  
Enterprise Environments.**

## CONTENT

Overview .....	4
The Basics .....	4
Single Sign-On – Supported Scenario: .....	4
Login to the WOL Portal without SSO .....	5
Manage Users and PCs .....	6
Group Status Overview .....	9
Requirements .....	10
.NET Framework .....	10
Auto Shutdown Manager Server (ASDM) .....	10
Internet Information Services (IIS) .....	10
SSL certificate .....	12
SQL Server .....	13
Database Login .....	13
Installation .....	15
Install the Advanced WOL Portal .....	16
Download the latest Advanced WOL Portal version .....	16
Configuration .....	16
Database Connection String .....	16
Connection to the Auto Shutdown Manager Server .....	17
Allow Remote WOL on the Auto Shutdown Manager Server .....	18
Integration into IIS .....	19
Set required file permissions for logging .....	20
Enable / Disable Logging .....	22
Single Sign-On (SSO) .....	23
Requirements .....	23
Configuration of SAML 2.0 for Single Sign-On (SSO) .....	23
Adding the IdP Metadata .....	24
IdP Configuration for LoginName .....	24
User Login-Name variable .....	28
Active Directory schema extension .....	29

WOLPCNAME Variable Name .....	33
Testing the WOL Portal .....	34
Automatically Import Users from Active Directory .....	35
LEGAL NOTICE .....	36
DISCLAIMER AND LIMITATION OF LIABILITY .....	36
SEVERABILITY CLAUSE.....	36
GOVERNING LAW AND JURISDICTION .....	37
COPYRIGHT AND INTELLECTUAL PROPERTY .....	37

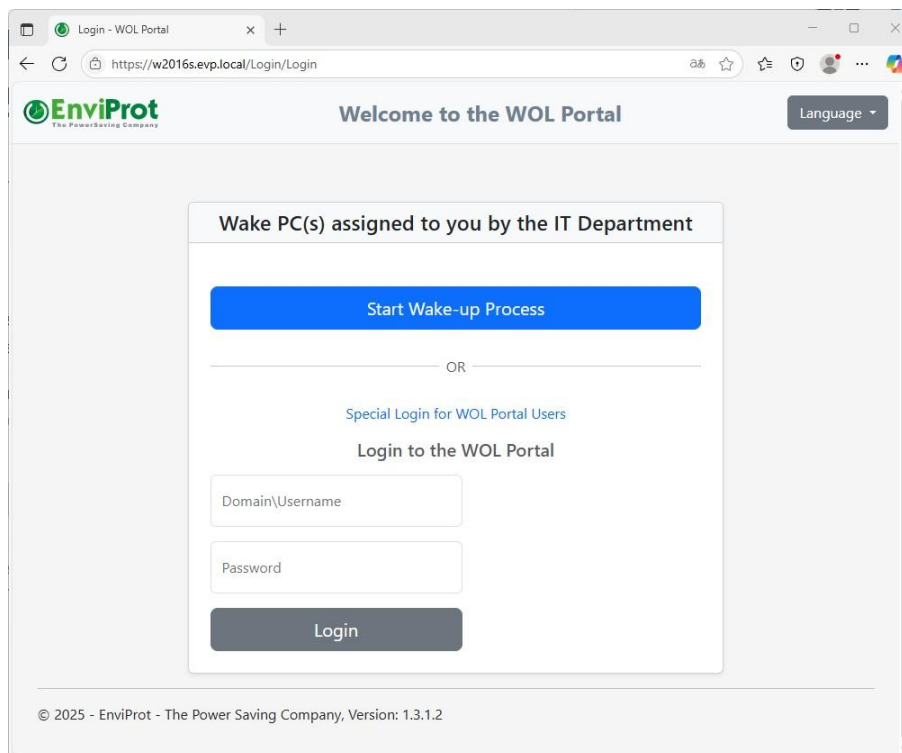
## Overview

### The Basics

The EnviProt Advanced WOL Portal is an extension of the existing Auto Shutdown Manager Server infrastructure. It enables external users to wake their internal corporate PCs in a secure and controlled manner. The Portal is typically hosted within the customer's intranet using **Microsoft IIS**. **Active Directory** is required for user authentication.

#### Single Sign-On – Supported Scenario:

Users first establish a VPN connection from their home PC's **web browser** by logging in to the central **enterprise VPN**, such as GlobalProtect VPN or Fortinet FortiGate. The enterprise VPN uses a **SAML 2.0-compliant Identity Provider (IdP)**, such as AD FS or OneLogin, to verify user authentication. Once successfully authenticated, users can navigate to the WOL Portal and **wake their assigned PC or PCs** with a **single click**.



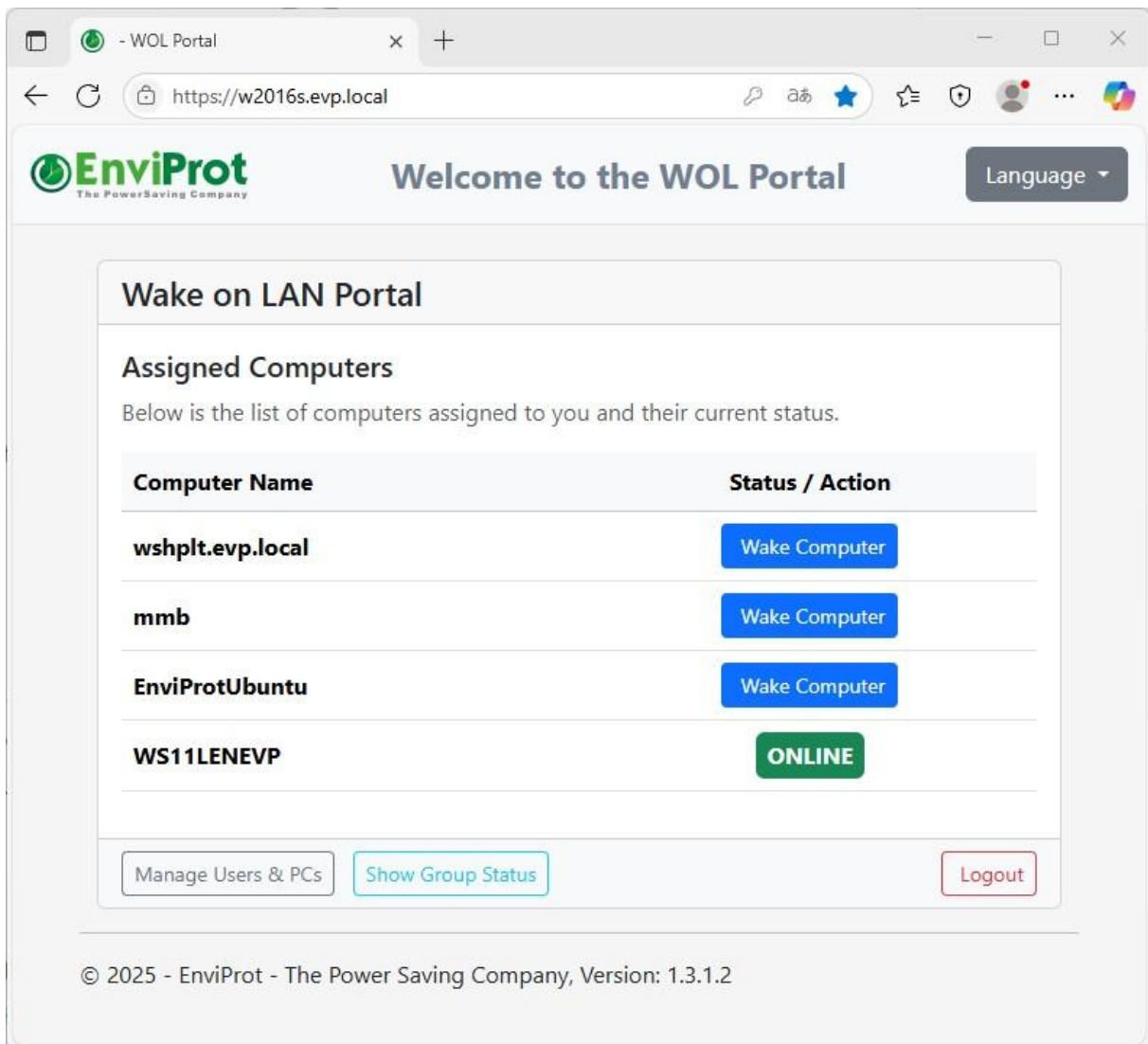
Screenshot 1: The WOL Portal with active Single Sign-On (SSO)

## Login to the WOL Portal without SSO

The first user who logs in to the WOL Portal automatically becomes the initial WOL Portal administrator. Additional administrators can be added by this user.

If Sing Sign-On authentication is not configured, WOL Portal administrators can manually add users and assign PCs to them.

After a user logs on, they see their assigned PCs along with the most recent status information. Depending on their permissions, they may also see the **Manage Users and PCs** and **Show Group Status** buttons, which provide access to additional portal management and diagnostic functions.



The screenshot shows a web browser window with the URL `https://w2016s.evp.local`. The page header includes the EnviProt logo, the text "Welcome to the WOL Portal", and a "Language" dropdown menu. The main content area is titled "Wake on LAN Portal" and "Assigned Computers". It contains a table with the following data:

Computer Name	Status / Action
wshplt.evp.local	Wake Computer
mmb	Wake Computer
EnviProtUbuntu	Wake Computer
WS11LENEVP	ONLINE

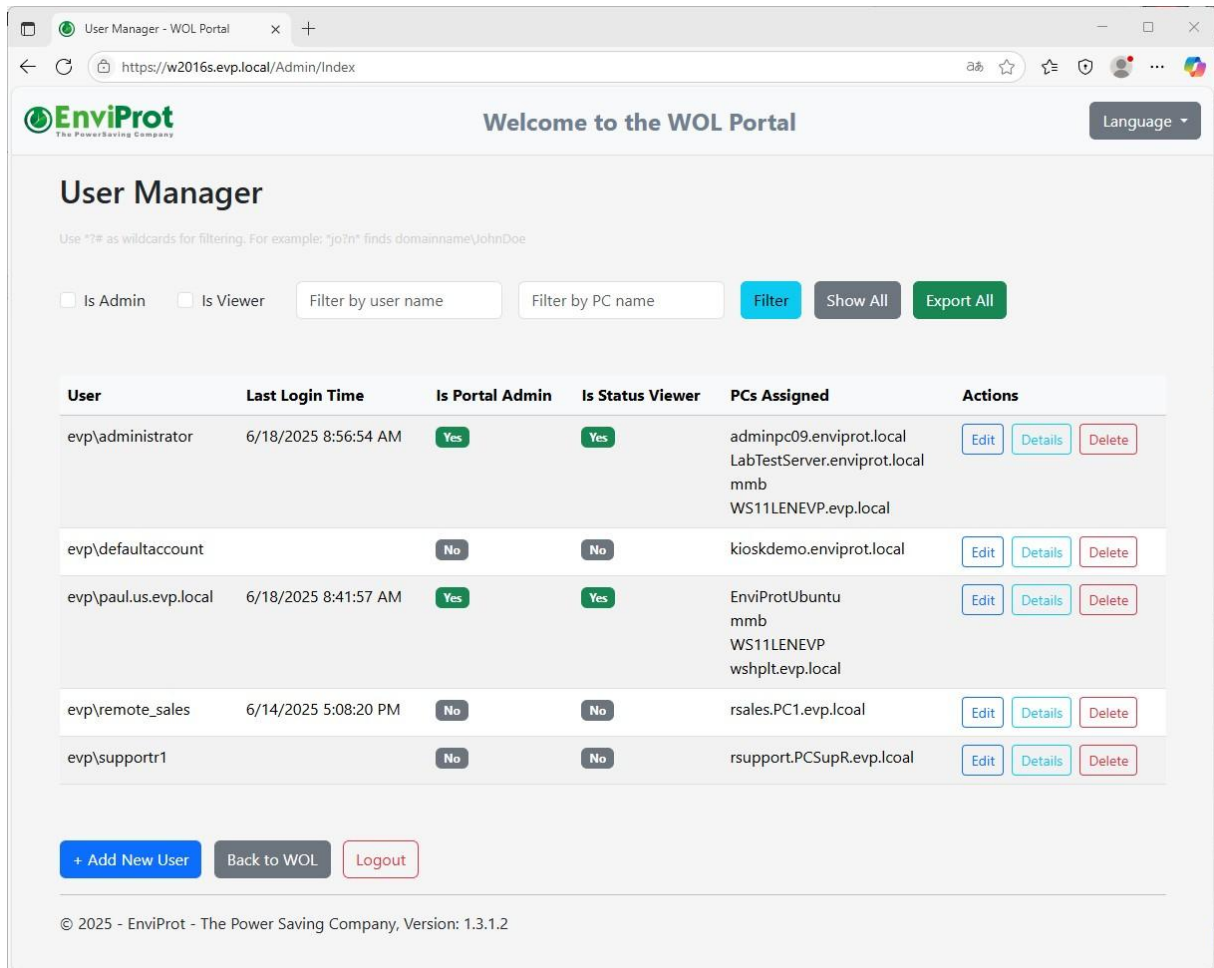
Below the table are three buttons: "Manage Users & PCs", "Show Group Status", and "Logout". The footer text reads: "© 2025 - EnviProt - The Power Saving Company, Version: 1.3.1.2".

Screenshot 2

## Manage Users and PCs

If you are not using the optional Single Sign-On feature, which manages users and PC assignments through Active Directory attributes, you must **manually add the users** who should have access to the WOL Portal and **assign the PCs** they are **allowed to wake**. A tool that can automatically import users from Active Directory is described later in this document. See: **Automatically Import Users from Active Directory** on page 35.

"Manage Users and PCs" opens the User Manager Console, where user accounts and their assigned PCs can be managed.



**User Manager**

Use \*?# as wildcards for filtering. For example: "jo\*n" finds domainname\JohnDoe

☐ Is Admin ☐ Is Viewer   Filter Show All Export All

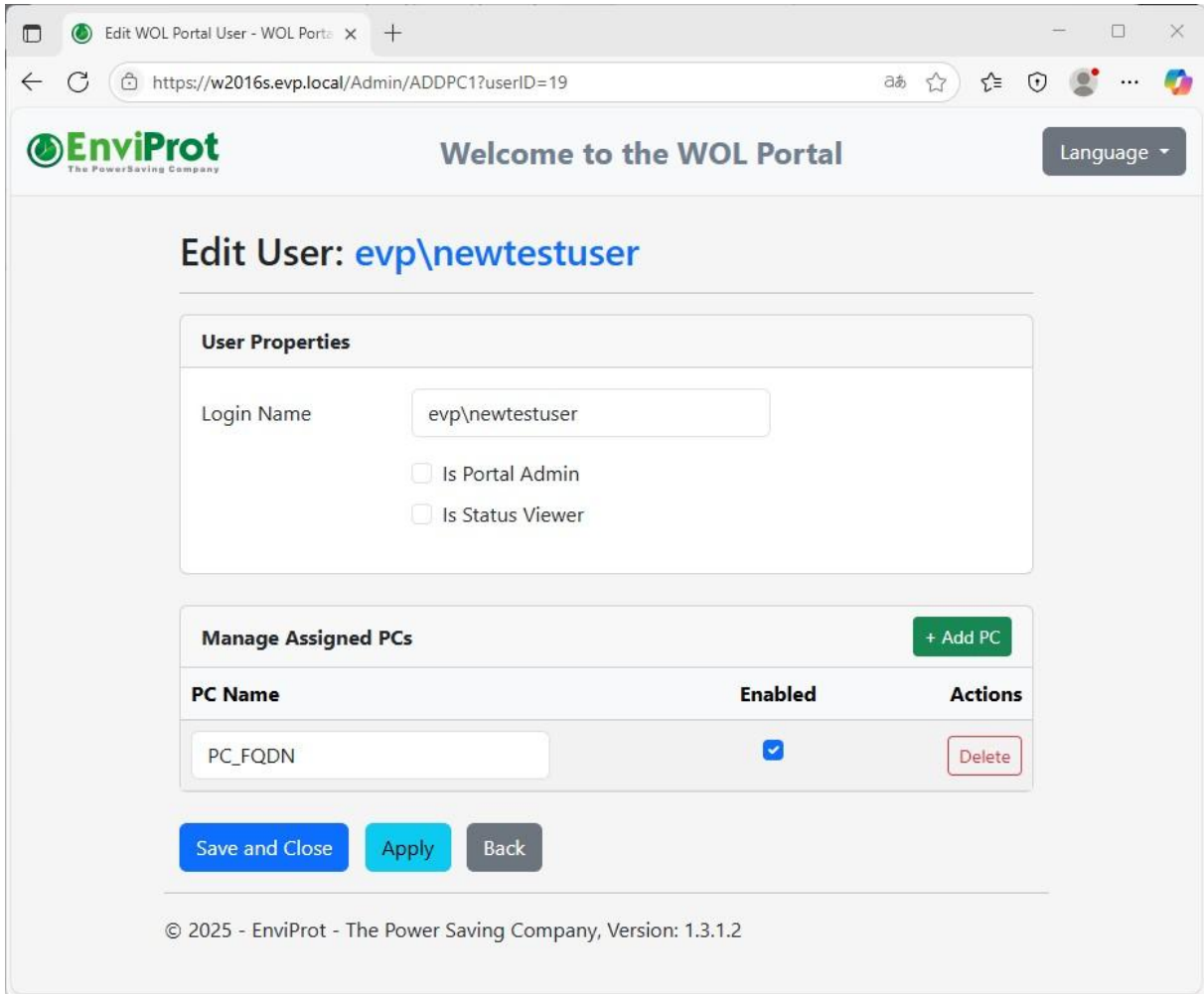
User	Last Login Time	Is Portal Admin	Is Status Viewer	PCs Assigned	Actions
evp/administrator	6/18/2025 8:56:54 AM	Yes	Yes	adminpc09.enviprot.local LabTestServer.enviprot.local mmb WS11LENEVP.evp.local	<a>Edit</a> <a>Details</a> <a>Delete</a>
evp/defaultaccount		No	No	kioskdemo.enviprot.local	<a>Edit</a> <a>Details</a> <a>Delete</a>
evp/paul.us.evp.local	6/18/2025 8:41:57 AM	Yes	Yes	EnviProtUbuntu mmb WS11LENEVP wshplt.evp.local	<a>Edit</a> <a>Details</a> <a>Delete</a>
evp/remote_sales	6/14/2025 5:08:20 PM	No	No	rsales.PC1.evp.lcoal	<a>Edit</a> <a>Details</a> <a>Delete</a>
evp/supportr1		No	No	rsupport.PCSupR.evp.lcoal	<a>Edit</a> <a>Details</a> <a>Delete</a>

+ Add New User Back to WOL Logout

© 2025 - EnviProt - The Power Saving Company, Version: 1.3.1.2

New users can be added, edited, or deleted.

*Edit or assign PCs to the selected user*



The screenshot shows a web browser window with the URL `https://w2016s.evp.local/Admin/ADDPC1?userID=19`. The page header includes the EnviProt logo, the text "Welcome to the WOL Portal", and a "Language" dropdown menu. The main heading is "Edit User: evp\newtestuser".

**User Properties**

Login Name:

☐ Is Portal Admin

☐ Is Status Viewer

**Manage Assigned PCs** + Add PC

PC Name	Enabled	Actions
<input type="text" value="PC_FQDN"/>	<input checked="" type="checkbox"/>	<span>Delete</span>

Save and Close Apply Back

© 2025 - EnviProt - The Power Saving Company, Version: 1.3.1.2

Users will only see PCs that are both assigned to their usernames and marked as enabled.

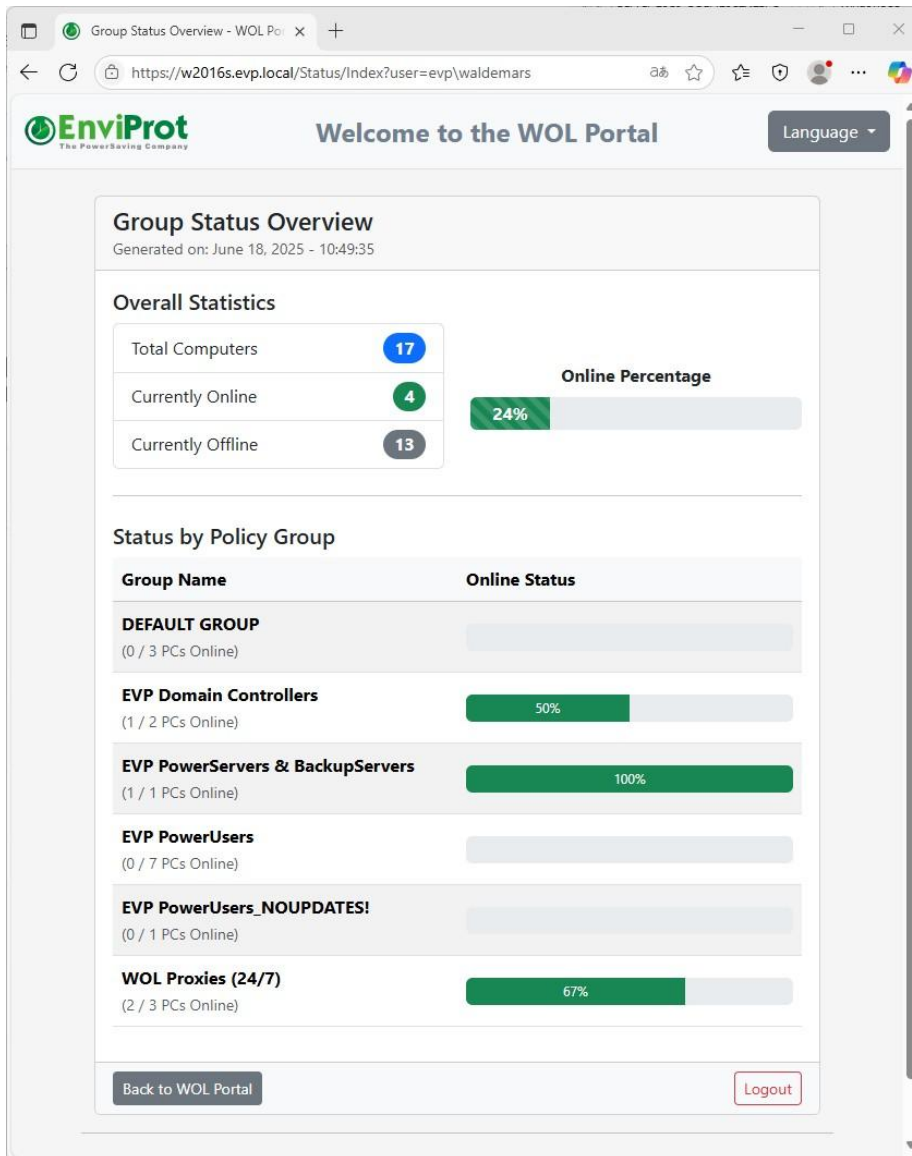
Please ensure that the PC names match those displayed by the Auto Shutdown Manager Server, which are typically shown in **Fully Qualified Domain Name (FQDN)** format.





## Group Status Overview

The Group Status Overview provides a quick summary of how many PCs are powered on or off in each PC group, as configured in the Auto Shutdown Manager Server.



## Requirements

### .NET Framework

The Advanced WOL Portal requires Microsoft .NET Framework 4.8 or newer to be installed. In some cases, when upgrading to the latest .NET Framework version, it may be necessary to re-register it for ASP.NET by running the following command: `aspnet_regiis -i`

Please refer to the official Microsoft documentation for more details.

### Auto Shutdown Manager Server (ASDM)

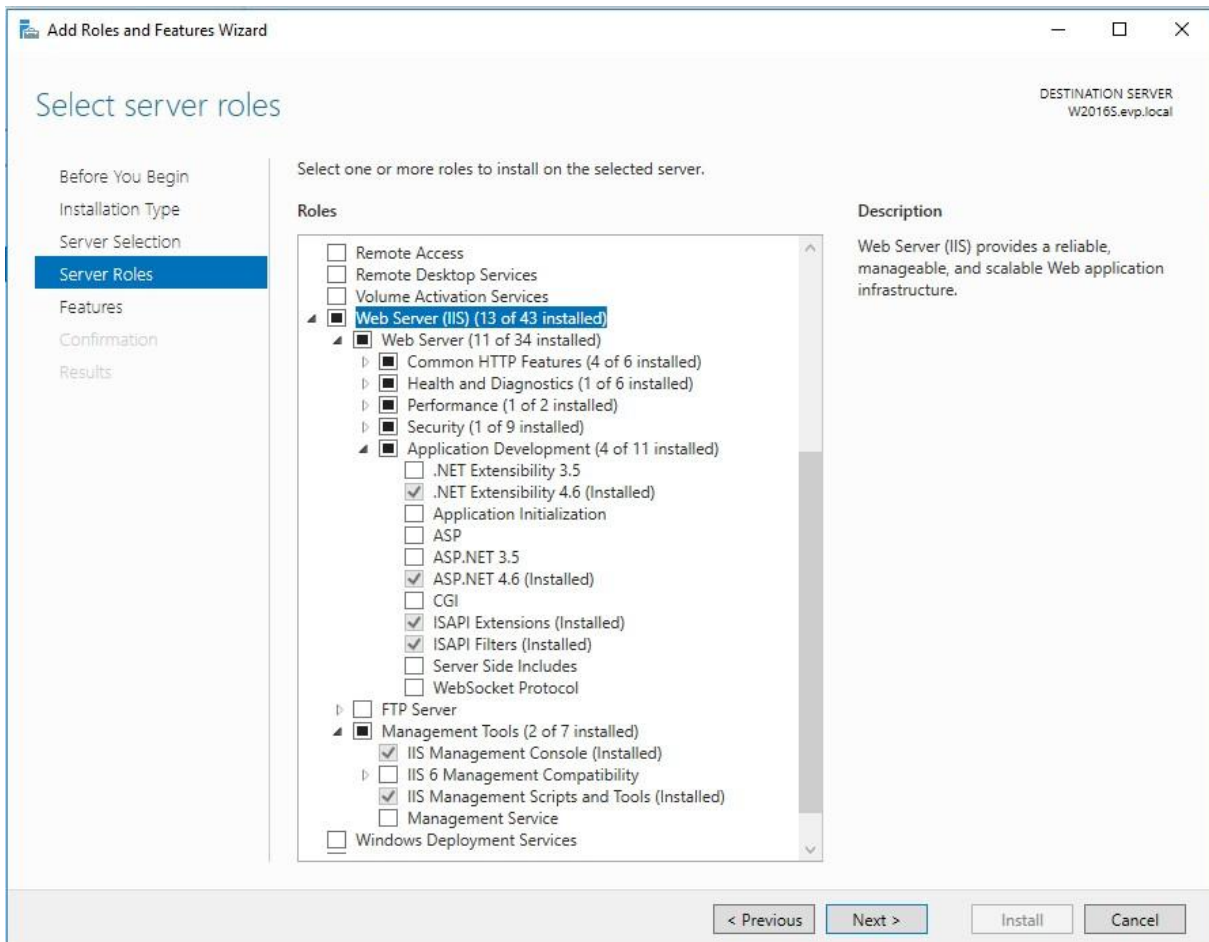
The EnviProt **Auto Shutdown Manager Server version 5.7.4.x** or newer (recommended) is required for full compatibility with this portal. All Wake-on-LAN (WOL) requests are forwarded to the Auto Shutdown Manager Server, which then processes the final WOL action using its robust WOL infrastructure — including WOL proxies and other supporting components.

Older ASDM versions may still function, but some features may not be supported.

### Internet Information Services (IIS)

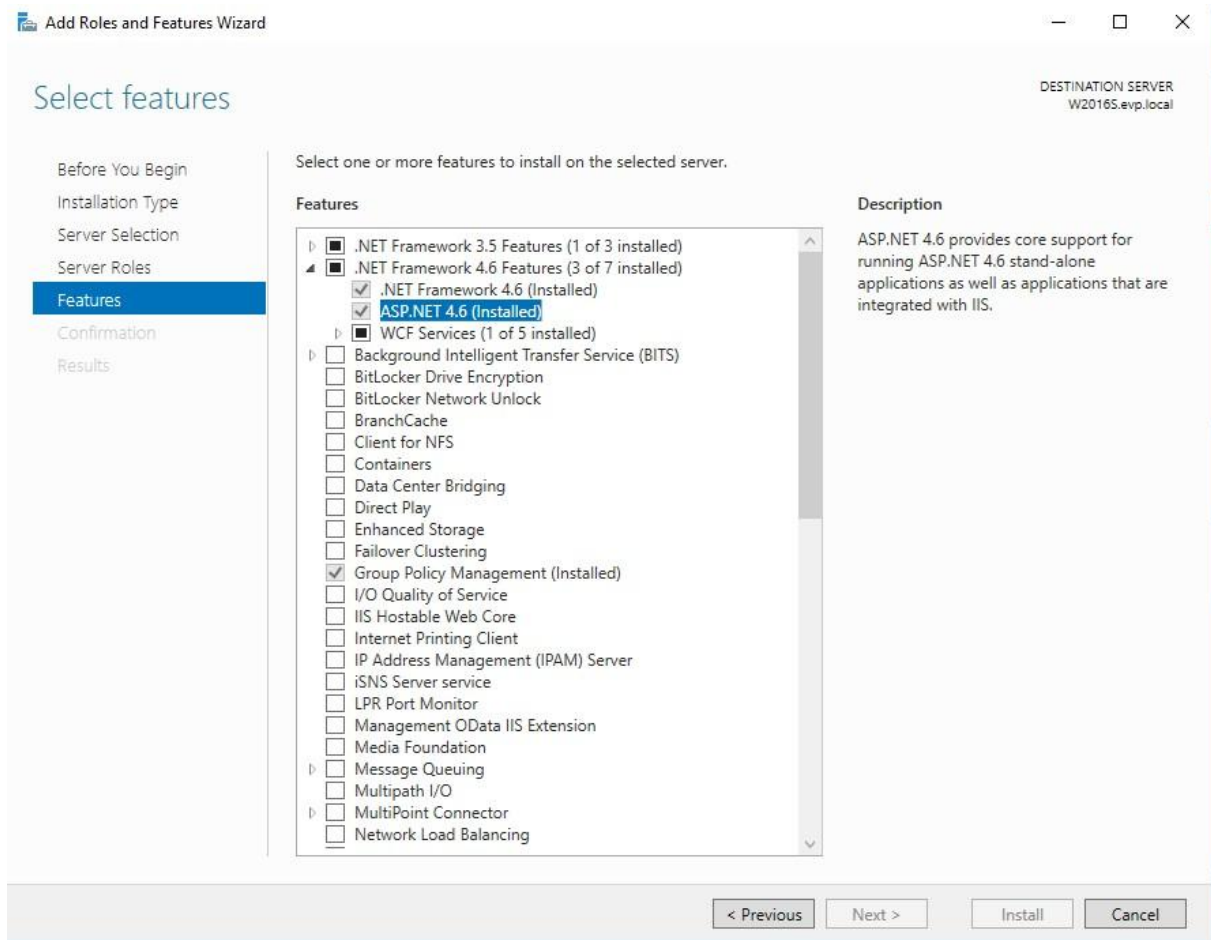
Microsoft IIS must be running on Windows Server 2016 or newer.

IIS must be installed and enabled on your intranet, including the **Application Development** role services required for the latest version of .NET as show in the screenshot below:



Note that the .NET Framework must be updated to version 4.8 or later, even if the server does not display it.

**Important:** Please also ensure that the **ASP.NET 4.x** s feature is enabled:



For detailed instructions and best practices on installing and securely operating the IIS infrastructure, please refer to the official guidelines and recommendations provided by Microsoft.

## SSL certificate

For security reasons, the Advanced WOL Portal requires the use of the HTTPS protocol.

For security reasons, the Advanced WOL Portal requires the use of the HTTPS protocol.

If an official SSL certificate is not available, you can generate a self-signed certificate. In this case, the certificate must be distributed and trusted on all client devices. Otherwise, users will still be able to access the portal but will encounter a security warning due to the untrusted self-signed certificate. When creating a self-signed SSL certificate, make sure to include the parameter **-KeyUsage DigitalSignature**.

Example: Open PowerShell as an administrator and enter:

```
New-SelfSignedCertificate -FriendlyName AnyNAME -DnsName  
your.server.address -KeyUsage DigitalSignature -NotAfter (Get-  
Date).AddYears(3)
```

## SQL Server

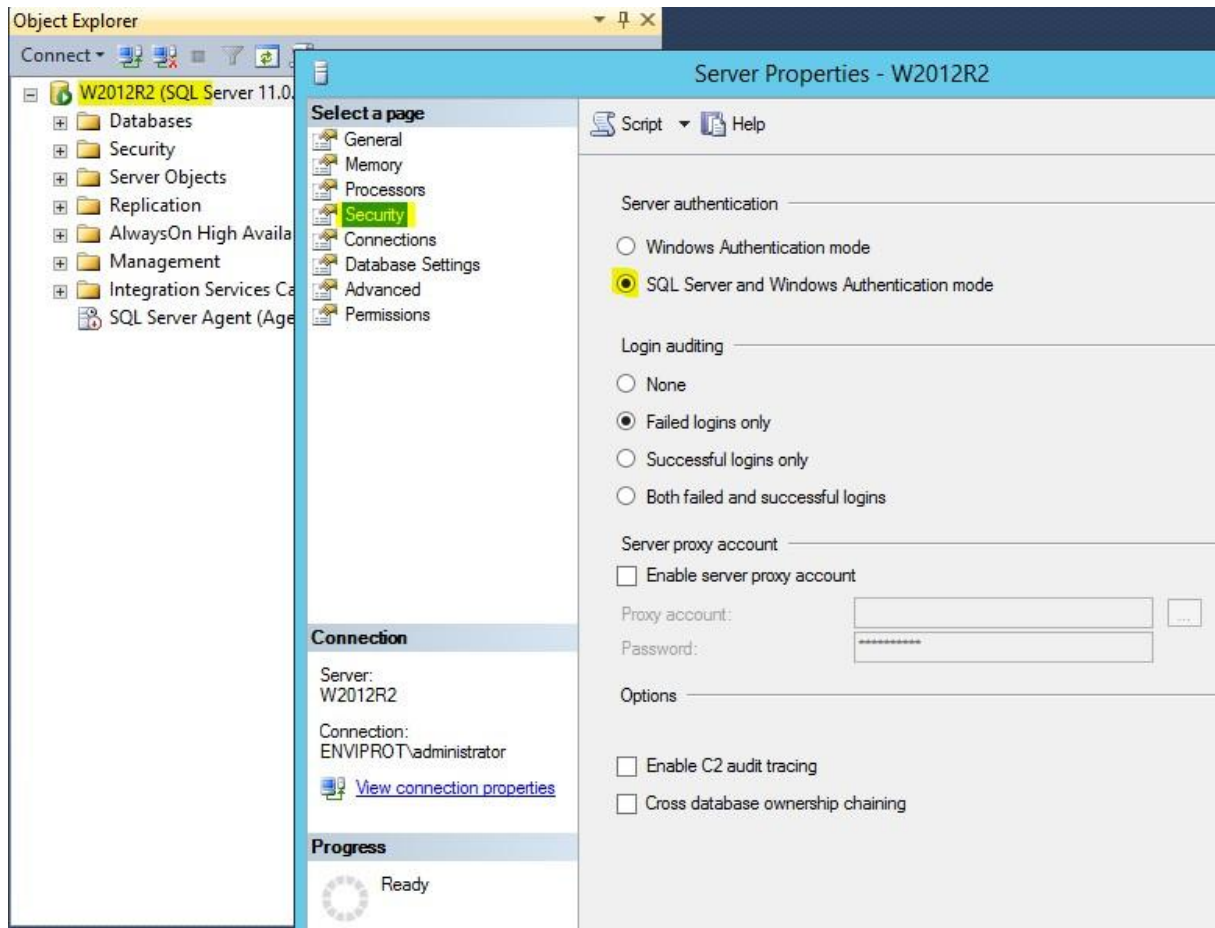
Microsoft SQL (Express) Server 2016 or newer is required.

The WOL Portal will create and use a database named “**WOLPortal**”.

### Database Login

If you don't want to use your own DB Login, the WOLPortal Database will be created by the **Portal IIS APPPOOL\YourAppPoolName** account automatically, for example IIS APPPOOL\WOLPORTAL.

If you want to use your **own database user**, you can create a dedicated database login in SQL Server Management Studio (Management Studio → YourSQLServer → Security → Logins). In this case, make sure that the SQL Server is configured to support both **SQL Server and Windows Authentication** modes:



To demonstrate this, we created a new login named ASDMS:

Login Properties - ASDMS

Select a page

- General
- Server Roles
- User Mapping
- Securables
- Status

Script ? Help

Login name: ASDMS

Securables: Search...

Name	Type
W2016S\SQLEXPRESS2019	Server

Connection

Server:  
W2016S\SQLEXPRESS2019

Connection:  
WS11LENEVP\waldemars

[View connection properties](#)

Progress

Ready

Permissions for W2016S\SQLEXPRESS2019:

Explicit Effective

Permission	Grantor	Grant	With Grant	Deny
Connect SQL		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Connect SQL	sa	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Control server		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Create any database		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Create availability group		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Create DDL event not...		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Create endpoint		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OK Cancel

**Important:** If the required permission “**Create any database**” is not granted, the database will not be created, and database error messages will occur.

**Important:** Make sure to remember the login name and password for later use.

## Installation

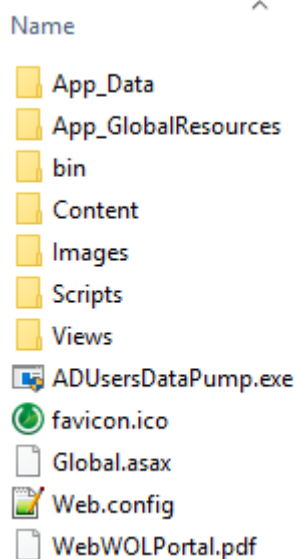
Please ensure that IIS, SQL Server, and the required .NET Framework are installed and running. For more information, refer to the Requirements section above.

## Install the Advanced WOL Portal

### Download the latest Advanced WOL Portal version

If not already done, please download the **Advanced WOL Portal ZIP** file from <https://www.enviprot.com/downloads>. Extract the ZIP file and copy its contents to a new IIS inetpub\wwwroot folder, for example:

```
C:\inetpub\wwwroot\WolportalSAML
```



The integration into IIS will be discussed later.

## Configuration

### Database Connection String

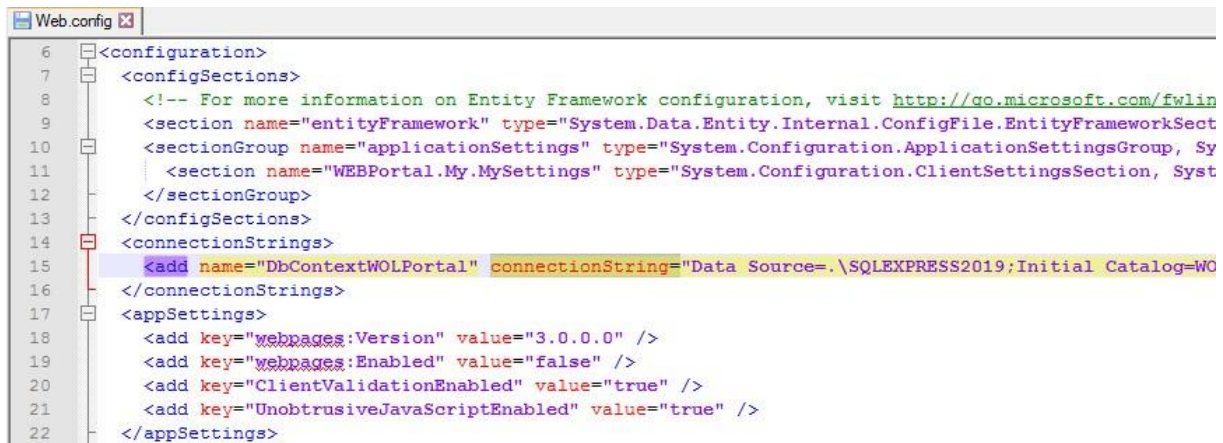
The connection string is required for the Portal to create and access the database properly. As mentioned under Requirements-> SQL Server, please ensure that all requirements are met. Open the **Web.config** file using a text editor of your choice, running in **administrator** mode. Navigate to the following section:

```
<connectionStrings>
  <add name="DbContextWOLPortal" connectionString="..." />
</connectionStrings>
```



Modify the connection details to match your database configuration. By default — as an example — the setting points to the local host and expects a SQL Server instance named SQLEXPRESS2019 (.\SQLEXPRESS2019). Tip: You can list your local DB instances with:

```
SqlLocalDB.exe info.
```



```
Web.config
6 <configuration>
7   <configSections>
8     <!-- For more information on Entity Framework configuration, visit http://go.microsoft.com/fwlink
9     <section name="entityFramework" type="System.Data.Entity.Internal.ConfigFile.EntityFrameworkSect
10    <sectionGroup name="applicationSettings" type="System.Configuration.ApplicationSettingsGroup, Sy
11    <section name="WEBPortal.My.MySettings" type="System.Configuration.ClientSettingsSection, Syst
12    </sectionGroup>
13  </configSections>
14  <connectionStrings>
15    <add name="DbContextWOLPortal" connectionString="Data Source=.\SQLEXPRESS2019;Initial Catalog=WOL
16  </connectionStrings>
17  <appSettings>
18    <add key="webpages:Version" value="3.0.0.0" />
19    <add key="webpages:Enabled" value="false" />
20    <add key="ClientValidationEnabled" value="true" />
21    <add key="UnobtrusiveJavaScriptEnabled" value="true" />
22  </appSettings>
```

If you configured your **own database login**, for example named “WOLPORTALUSER”, you need to modify the connection string by setting **Integrated Security=False** and adding the ‘**User Id=**’ and ‘**Password=**’ parameters as shown below:

```
<add name="DbContextWOLPortal"
      connectionString="Data Source=.\SQLEXPRESS2019;
      Initial Catalog=WOLPortal; User Id=WOLPORTALUSER;Password=ThePassword;
      Integrated Security=False" providerName="System.Data.SqlClient"
/>
```

Please note: There is a space between User and Id in the connection string (User Id — not UserId)

## Connection to the Auto Shutdown Manager Server

Still in the Web.config file, search for the ASDMServer attribute.

```
<setting name="ASDMServer" serializeAs="String">
```

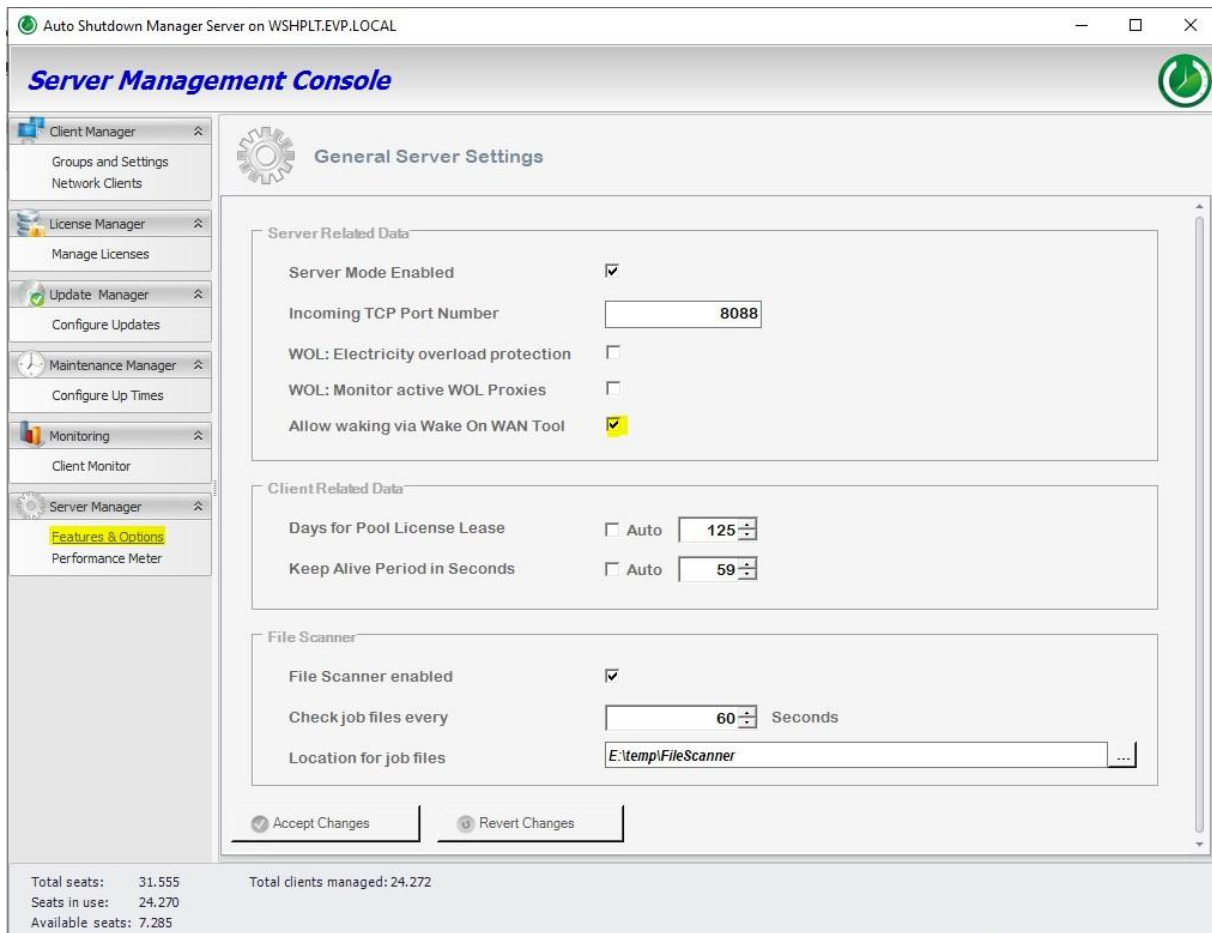
In that section, as shown below, enter the DNS name or IP address of your Auto Shutdown Manager Server. The example server name “**asdmctrl**” should be replaced with the actual address of your server.

The default port is 8088 and can usually remain unchanged unless your configuration requires a different port.

```
<applicationSettings>
  <WEBPortal.My.MySettings>
    <setting name="ASDMServer" serializeAs="String">
      <value>asdmctrl</value>
    </setting>
    <setting name="ASDMPort" serializeAs="String">
      <value>8088</value>
    </setting>
  </WEBPortal.My.MySettings>
</applicationSettings>
</configuration>
```

### Allow Remote WOL on the Auto Shutdown Manager Server

Finally, make sure that the Auto Shutdown Manager Server is configured to allow remote WOL waking:



Auto Shutdown Manager Server on WSHP.LT.EVP.LOCAL

### Server Management Console

- Client Manager
  - Groups and Settings
  - Network Clients
- License Manager
  - Manage Licenses
- Update Manager
  - Configure Updates
- Maintenance Manager
  - Configure Up Times
- Monitoring
  - Client Monitor
- Server Manager
  - Features & Options
  - Performance Meter

### General Server Settings

**Server Related Data**

- Server Mode Enabled ☒
- Incoming TCP Port Number
- WOL: Electricity overload protection ☐
- WOL: Monitor active WOL Proxies ☐
- Allow waking via Wake On WAN Tool ☒

**Client Related Data**

- Days for Pool License Lease ☐ Auto
- Keep Alive Period in Seconds ☐ Auto

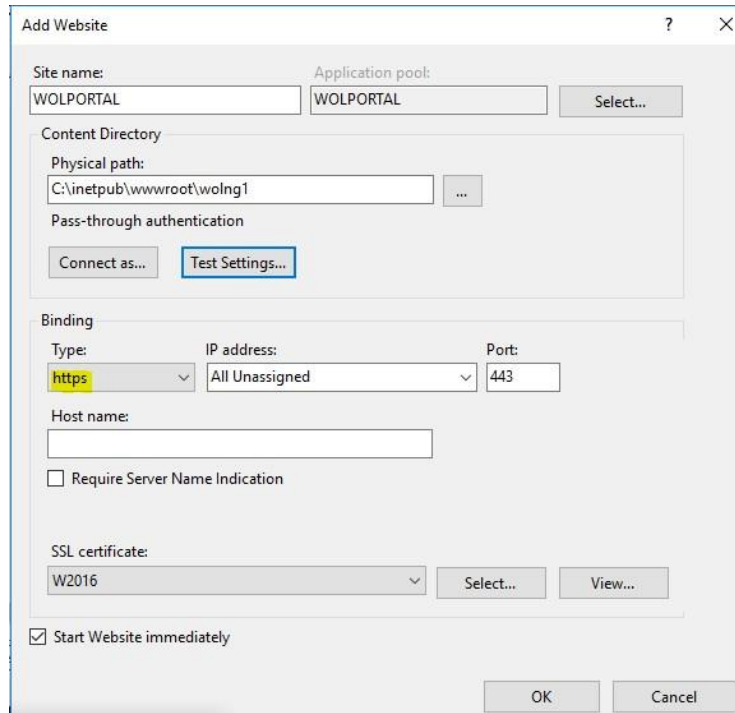
**File Scanner**

- File Scanner enabled ☒
- Check job files every  Seconds
- Location for job files

Total seats: 31.555  
 Seats in use: 24.270  
 Available seats: 7.285  
 Total clients managed: 24.272

## Integration into IIS

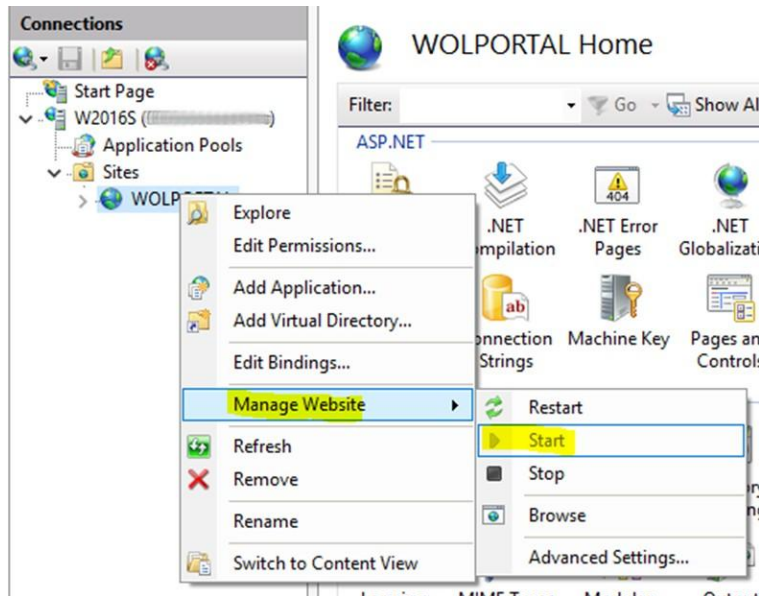
Open Internet Information Services (IIS) Manager and create a new website.



The screenshot shows the 'Add Website' dialog box in IIS Manager. The 'Site name' field is set to 'WOLPORTAL'. The 'Application pool' dropdown is set to 'WOLPORTAL'. The 'Content Directory' section shows the 'Physical path' as 'C:\inetpub\wwwroot\wolng1'. The 'Binding' section shows 'Type' as 'https', 'IP address' as 'All Unassigned', and 'Port' as '443'. The 'Host name' field is empty. The 'Require Server Name Indication' checkbox is unchecked. The 'SSL certificate' dropdown is set to 'W2016'. The 'Start Website immediately' checkbox is checked. The 'OK' and 'Cancel' buttons are at the bottom right.

Make sure to select HTTPS for the binding and choose your SSL certificate (see Requirements section for details).

Also, ensure that the site is started and running.



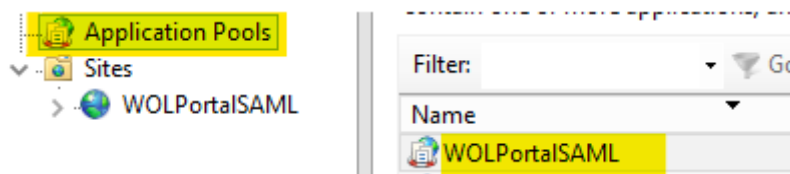
### Set required file permissions for logging

The IIS Service has by default no write rights into the any of the portal folders.

To allow logging to be written into the App\_data folder -which is strongly recommended the write permissions must be granted.

Here is a step-by-step guide:

Open the IIS Manager -> **Application Pools** dialog, and find the application pool used by your site (for example: **WOLPortalSAML**).

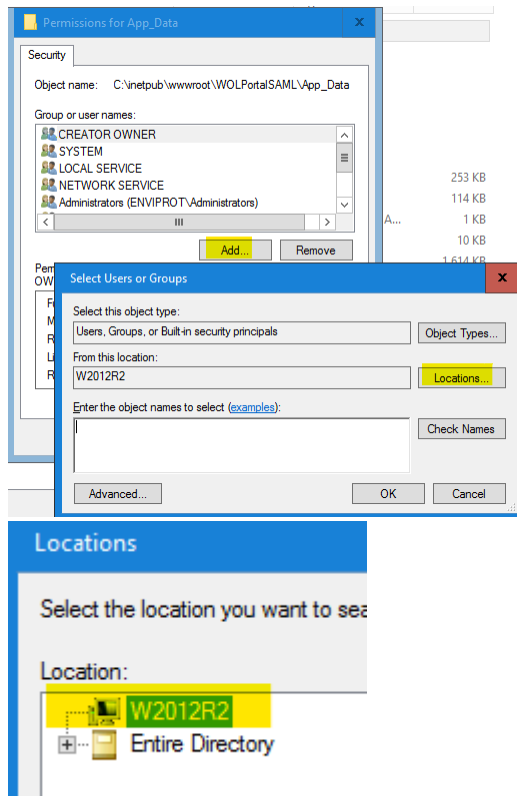


This is usually the same name as your Site name.

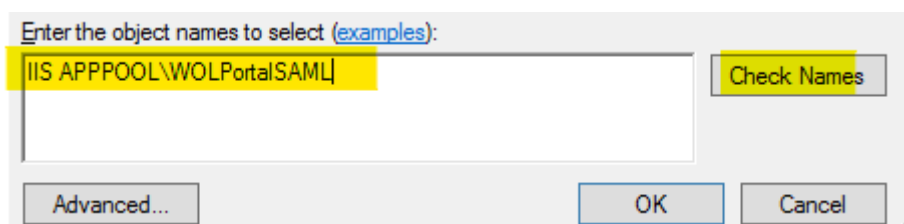
Note the name of the application pool.

1. Open File Explorer and navigate to the application's root directory. It is usually located under **C:\inetpub\wwwroot\WOLPortalSAML**
2. Find the "App\_Data" sub-folder (for example: `C:\inetpub\wwwroot\WOLPORTAL\AppData`).
3. Right-click the App\_Data folder and select Properties
4. Open the Security tab.

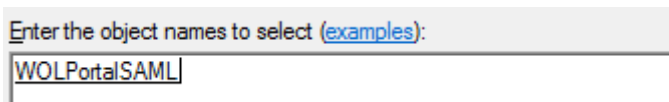
5. Click Edit...
6. Click Add...
7. **IMPORTANT:** Click **Locations...** and select your **local computer** (should be the very top entry)



8. In the "Enter the object enter: IIS APPPOOL\WOLPortalSAML (replace WOLPortalSAML with the name of your application pool name if different)



Click **Check Names** to resolve it and finally OK to close the dialog.

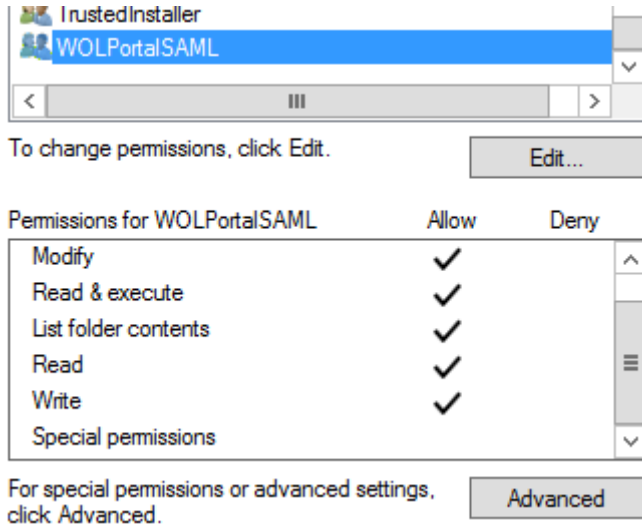


8a. If the above account is unavailable, select IIS\_IUSRS instead and grant add **Modify (Modify, Read, Write, etc.)** permissions

8b. Only for testing purposes, you can also grant permissions to "Everyone", but this is not recommended for production environments.

9. Click OK

10. Back in the Security dialog select **Full Control** (or at least LIST, READ, WRITE, MODIFY) for the newly added WOLPortalSAML account and click OK to apply the changes.



The App-Data content cannot be accessed via the browser.

## Enable / Disable Logging

The WOL Portal generates a log file that records key events. The file is named “WOLPortalLogDATECODE.txt” and is located in the **App\_Data** folder within the root directory of the portal installation. Logging can be enabled or disabled in the Web.config file under the following section:

```
<setting name="EnableEvpDebugLogger" serializeAs="String">
  <value>True</value>
</setting>
```

**Tip:** If logging is **not working**, please check the section “Set required file permissions for logging” on page 20.

**Important:** It is **strongly recommended** to **enable logging**, at least during the initial operation of the WOL Portal. Logging helps verify that the configuration is correct and that all functions work as expected. It is also essential when requesting support from EnviProt in case any issues occur.

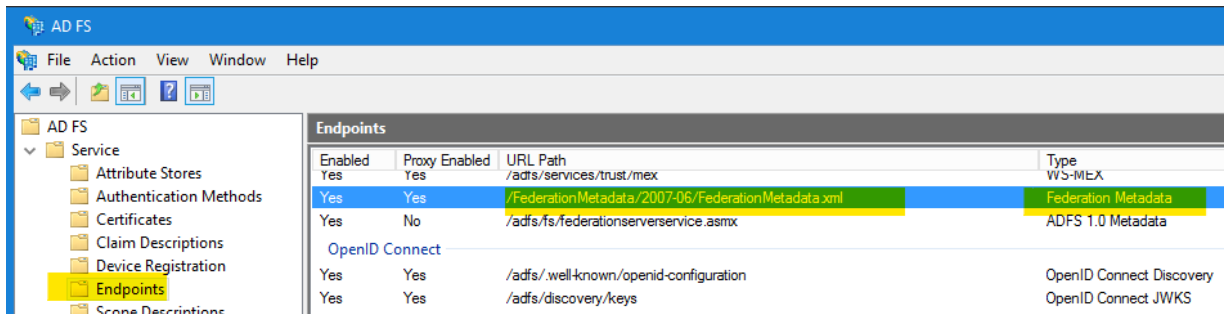
## Single Sign-On (SSO)

SSO is an optional feature of the Advanced WOL Portal that allows remote users, already authenticated through their corporate VPN system, to wake their office PCs directly from a web browser with a single click—without the need for an additional login.

### Requirements

- EnviProt Advanced WOL Portal Release **1.3** or later.
- **SAML 2.0–compliant** Identity Provider (IdP), such as AD FS or OneLogin
- **Endpoint** URL for your **IdP’s metadata**, for example (AD FS):  
<https://your.IdP.host/FederationMetadata/2007-06/FederationMetadata.xml>

In AD FS for example, you can find out the Endpoint of the Metadata provider like this:



Enabled	Proxy Enabled	URL Path	Type
Yes	Yes	/ads/services/trust/mex	WS-MEX
Yes	Yes	/FederationMetadata/2007-06/FederationMetadata.xml	Federation Metadata
Yes	No	/ads/fs/federationserverservice.asmx	ADFS 1.0 Metadata
OpenID Connect			
Yes	Yes	/ads/.well-known/openid-configuration	OpenID Connect Discovery
Yes	Yes	/ads/discovery/keys	OpenID Connect JWKS

- **Endpoint** URL for the EnviProt **Advanced WOL Portal metadata**:  
<https://your.wolportal.host/auth/Metadata>  
 Tip: You will need this metadata URL to configure the WOL Portal as a Relying Party Trust in your Identity Provider (IdP).
- Configured **Claim Issuance Policy** in your IdP to provide the **User-Principal-Name** (UPN) attribute (see below).
- **Active Directory** access with a **custom attribute** added to the **user object class** to store the PCs assigned to each user for Wake-on-LAN (see below).

### Configuration of SAML 2.0 for Single Sign-On (SSO)

The WOL Portal requires two key pieces of information to operate correctly with SSO:

#### 1) Who is the currently signed-in user?

- This information — the user's name (UPN) — is provided by the Identity Provider (IdP) as a variable. The default variable name is **LoginName**.
- This is required to verify that the user is valid and to identify who is initiating the Wake-on-LAN request.

## 2) Which PC(s) should be awakened?

- This information is stored in the user object's custom attribute. The default attribute name is **WOLPCNAME**. It can contain one or more comma-separated PC FQDNs, such as user1pc1.your.domain, user1pc2.your.domain
- Therefore, this custom attribute must be added to the Active Directory schema (see the how-to steps below).

## Adding the IdP Metadata

In the **Web.config** file in your WOL Portal installation directory, search for the **SamlIdPMetadataURL** setting.

```
<setting name="SamlIdPMetadataURL" serializeAs="String">  
  <value>https://w2016s.evp.local/FederationMetadata/2007-06/FederationMetadata.xml</value>  
</setting>
```

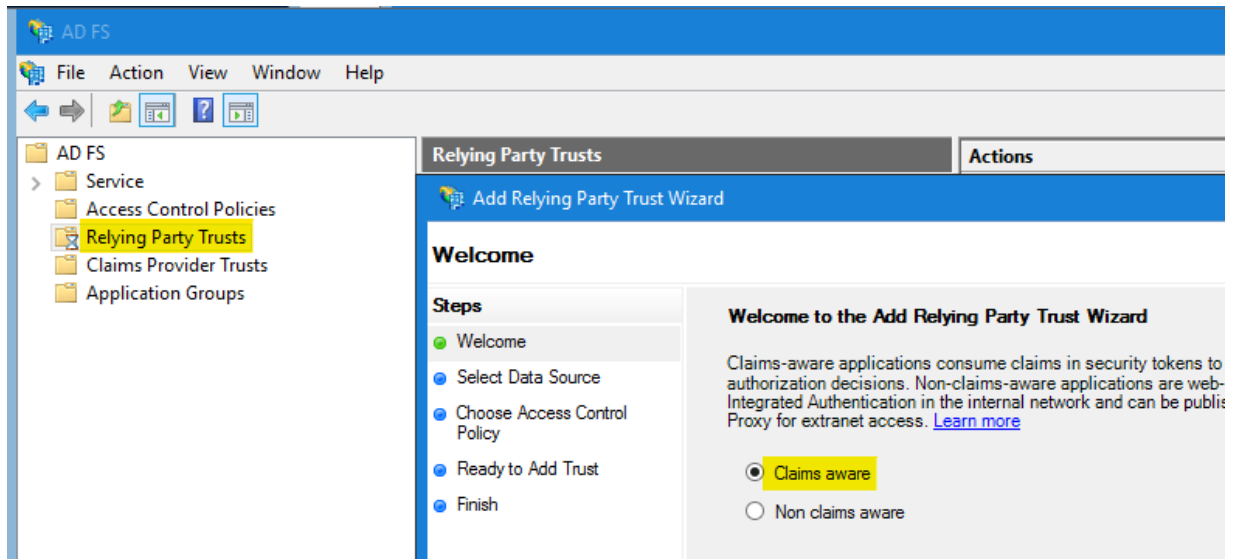
In the **<value>** field, enter the URL of your Identity Provider's (IdP) metadata, as shown in the example above.

## IdP Configuration for LoginName

In the example below, Microsoft Active Directory Federation Services (AD FS) is used to demonstrate the basic integration process.



Open AD FS Management from the **Server Manager** → **Tools** menu, right-click **Relying Party Trusts**, and select **Add Relying Party Trusts...** The following dialog will appear:



Keep the default setting **Claims aware** and click **Start**.

In the next dialog, enter the URL of your WOL Portal metadata as described under Requirements above and click Next:

## Add Relying Party Trust Wizard



## Select Data Source

## Steps

- Welcome
- Select Data Source
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

- ☒ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

- ☐ Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

[Browse...](#)

- ☐ Enter data about the relying party manually

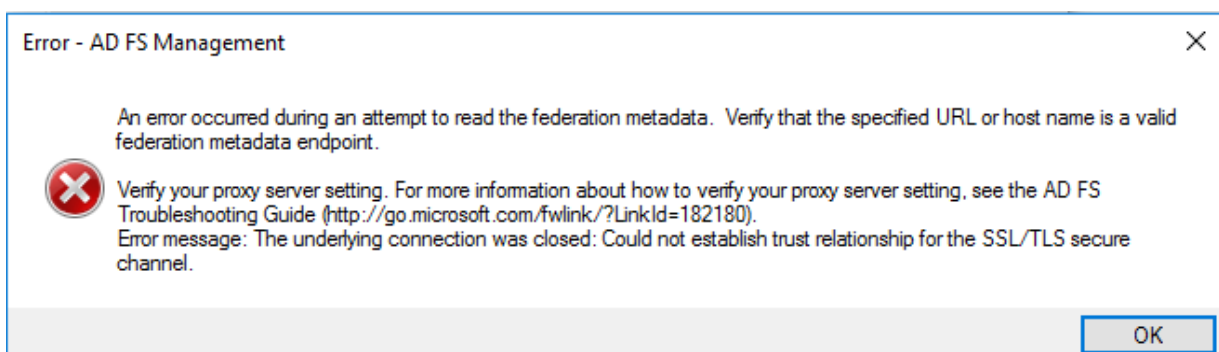
Use this option to manually input the necessary data about this relying party organization.

< Previous

Next >

Cancel

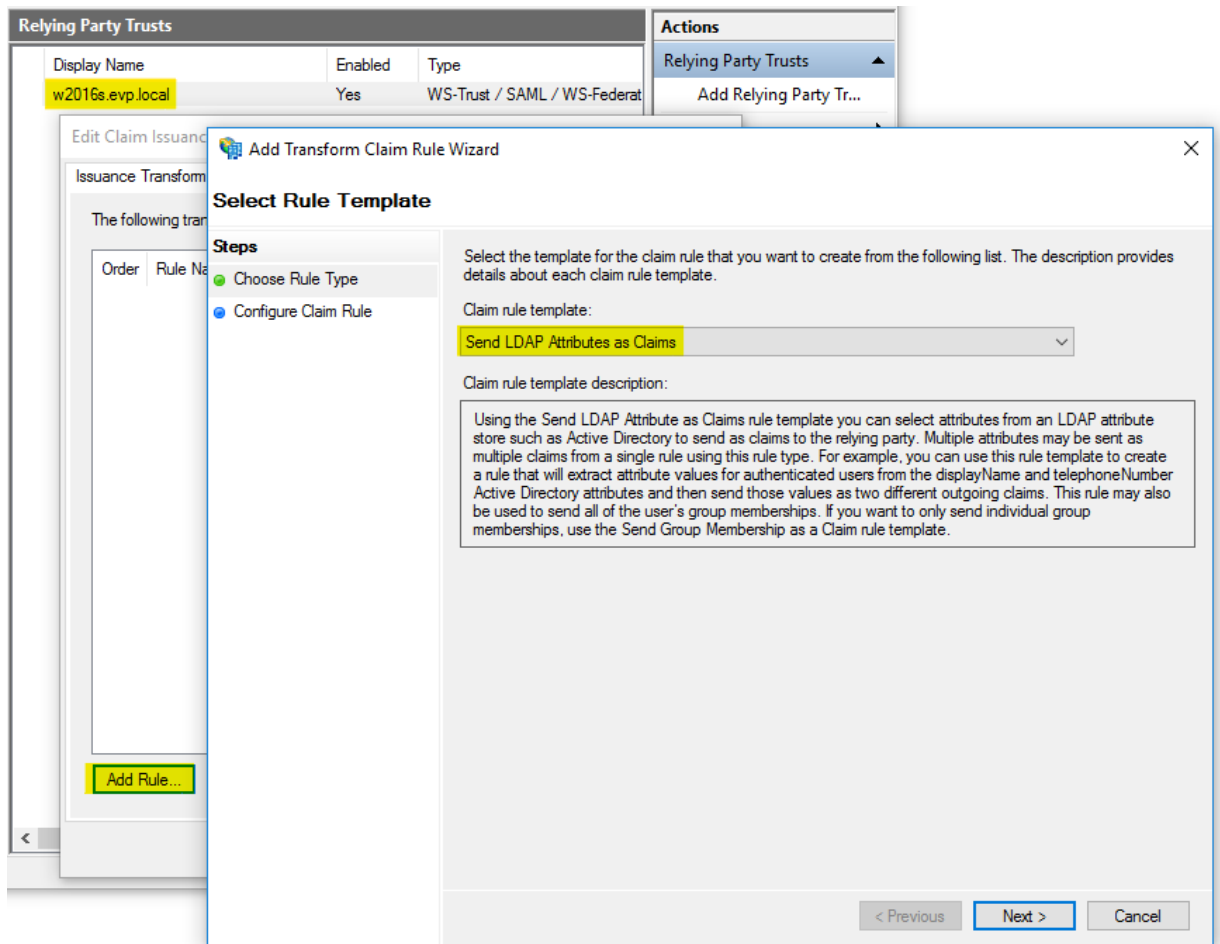
If you encounter an error such as “**An error occurred during an attempt to read the federation metadata...**,” even though the URL is correct, check the **server’s SSL certificate**.



To **verify** a possible SSL issue, open a **web browser** on the server and paste the **same URL**. The browser should either download the **Metadata.xml** file or display a descriptive error message indicating the problem.

When the metadata has been added successfully, enter the **Display name**, then click Next. If needed, adjust the permissions or keep the default setting **Permit everyone**, then click Next again and finally Close the dialog.

Now, a new entry should appear. Right-click on it and select **Edit Claim Issuance Policy** → **Add Rule**. Make sure **Send LDAP Attributes as Claims** is selected, then click **Next**.



In the next “Configure Rule” dialog, enter a descriptive claim rule name of your choice and set **Active Directory** as the attribute store. From the **LDAP Attribute** list, select **User-Principal-Name**, then **IMPORTANT**: type **LoginName** as the **Outgoing Claim Type**, and click Finish.

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	User-Principal-Name ▼	LoginName ▼
*	▼	▼

Make note of the variable name specified in the “Outgoing Claim Type” field (**LoginName** in our example), as this value must be referenced in the subsequent configuration. The WOL Portal depends on this claim variable to obtain the user's login name during the SAML authentication process. This login name serves as a key identifier and is essential for the portal to query the corresponding custom Active Directory (AD) attribute—configured by your IT department—that contains the list of PC names assigned to each individual user (as described further below).

### User Login-Name variable

**LoginName** is just a variable name and can be changed if needed.

To do so: open the **Web.config** file in your WOL Portal installation directory, search for **SamlUPNIdPAttributeName**, and adjust the value as required:

```
<setting name="SamlUPNIdPAttributeName" serializeAs="String">
    <value>LoginName</value>
</setting>
```

With this final step, you have successfully completed the IdP preparation.

## Active Directory schema extension

Step-by-step guide to adding a custom attribute to the Active Directory schema to store the PCs that each user can wake.

Note: The following steps are provided as examples without any warranty or guarantee. Perform all changes in a test environment first and at your own risk.

First, **add a custom attribute** to the Active Directory schema on the **user object class**:

- 1) Log on using an account that is a member of the **Schema Admins** group (membership in **Domain Admins** is not sufficient).
- 2) Register the Active Directory Schema snap-in (run as Administrator on a domain controller):
  - **regsvr32 schmmgmt.dll**
- 3) Open the **mmc.exe** → **File** → **Add/Remove Snap-in...** → **Active Directory Schema** → **Add** → **OK**.
- 4) In Active Directory Schema, expand **Attributes** → right-click **Attributes** → **Create Attribute**.
- 5) Common Name: **WOLPCNAME**
- 6) Enter your organization's enterprise OID.  
For testing reasons, you can generate random numbers for the last parts.  
1.2.840.113556.1.8000.xxxxxxxx.xxxxxxxx
- 7) Syntax: Case-Insensitive String for text
- 8) If you plan to add multiple PCs, consider increasing the **Maximum** length value accordingly.
- 9) Click OK. (This writes the new attribute to the schema.)
- 10) Inside **Attributes** search for the attribute name (**WOLPCNAME**) and double-click it.

11) Click on Replicate this attribute to the Global Catalog

Name	Syntax	Status	Descr
WOLPCNAME	Case Insensitive String	Active	FQDN

Console Root  
 Active Directory Schema [W20...]  
   Classes  
   Attributes

WOLPCNAME Properties

**General**

WOLPCNAME

Description: FQDN

Common Name: WOLPCNAME

X.500 OID: 1.2.840.113556.1.8000.2554.48181.34000.60331

Syntax and Range

Syntax: Case Insensitive String

Minimum: 1

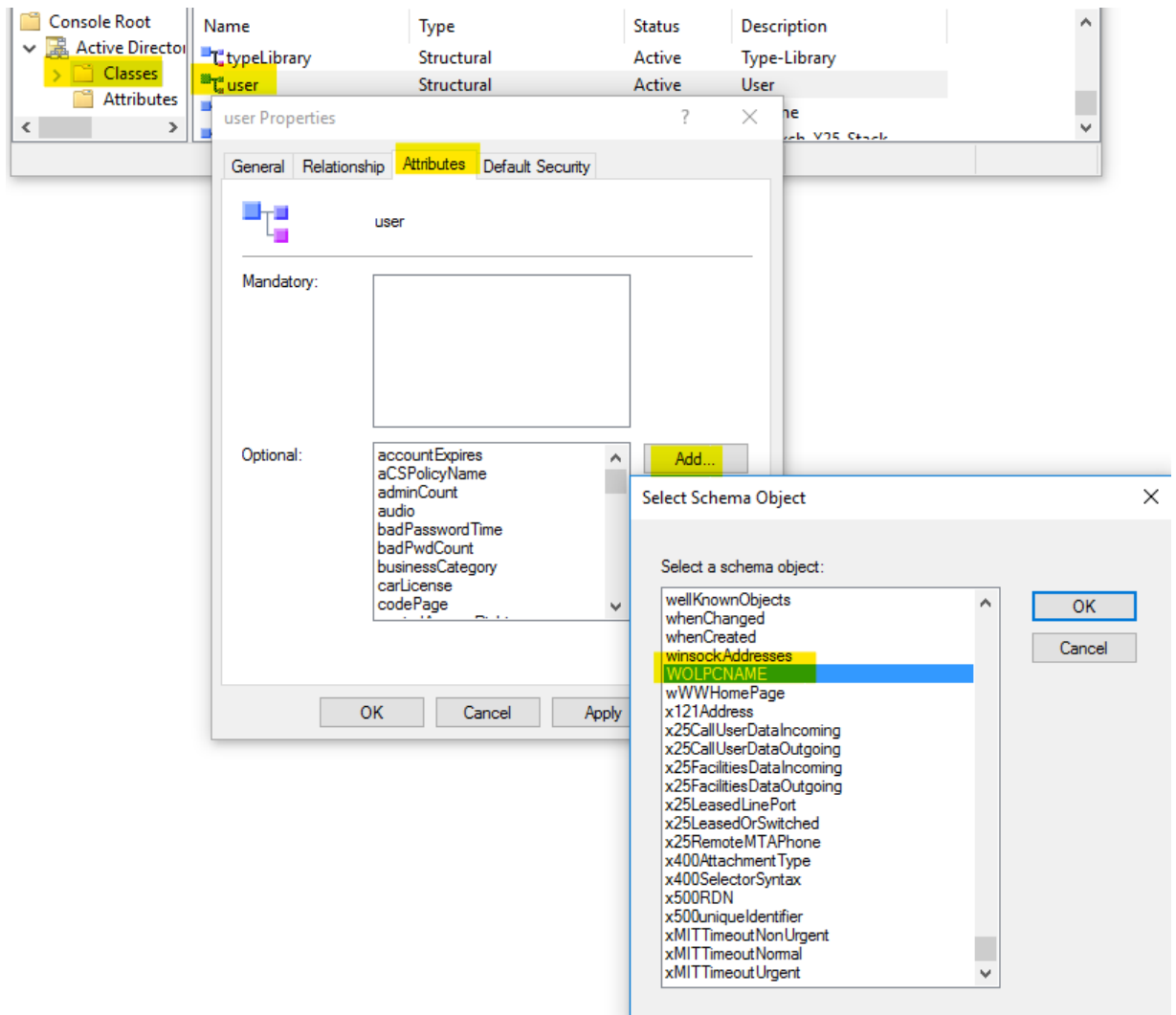
Maximum: 4096

This attribute is single-valued.

☒ Attribute is active  
☐ Index this attribute  
☐ Ambiguous Name Resolution (ANR)  
☒ Replicate this attribute to the Global Catalog  
☐ Attribute is copied when duplicating a user  
☐ Index this attribute for containerized searches

OK Cancel Apply Help

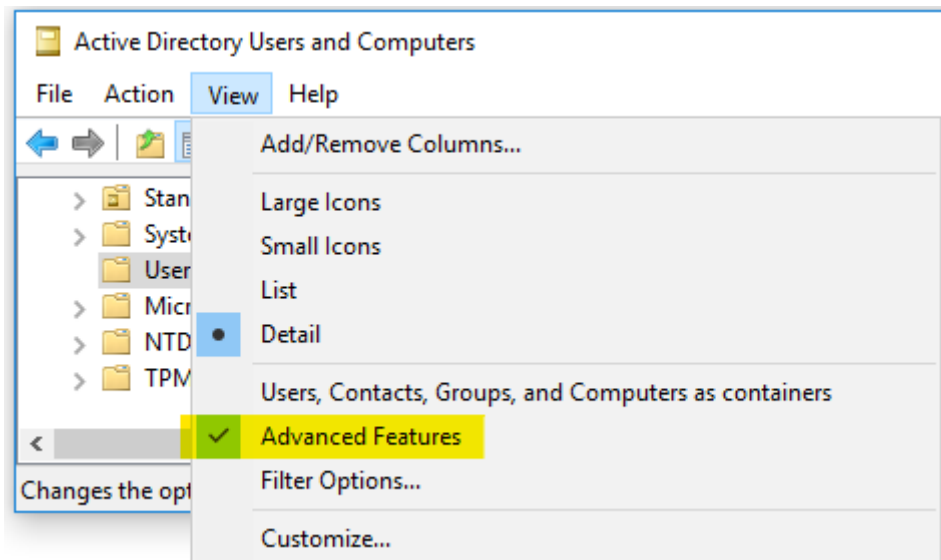
12) Now add the attribute to the user object class: click on **Classes**.



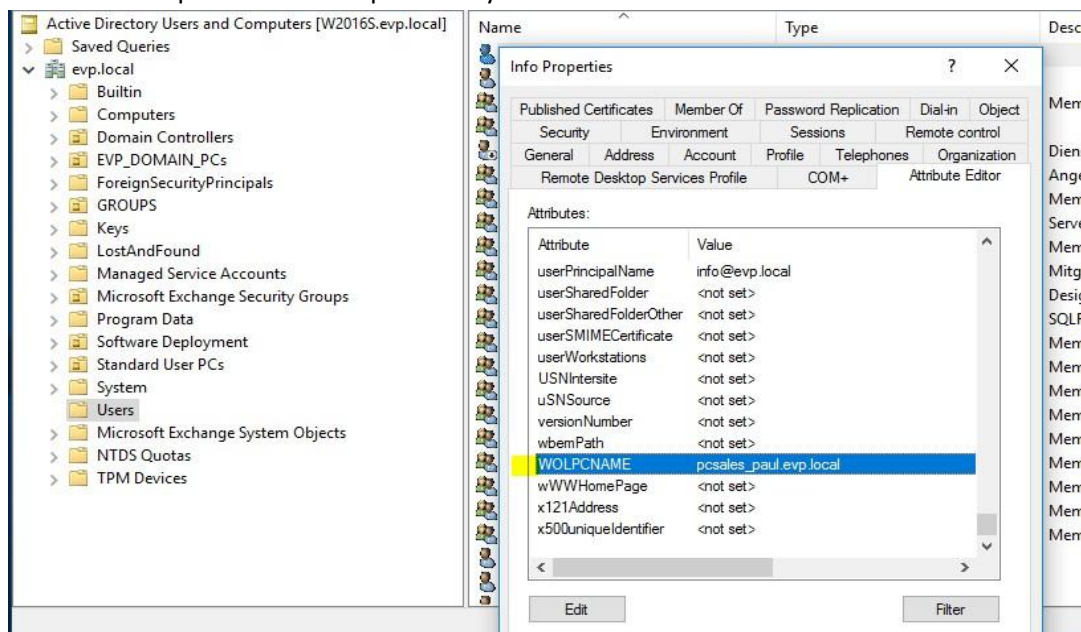
13) Right-click on **user**, then select **Properties -> Attributes -> Add**

14) Select the **WOLPCNAME** attribute from the list-> **OK -> OK -> DONE**

15) Verify the result: Open **Active Directory Users and Computers**, go to **View**, and make sure **Advanced Features** is enabled:



16) Right-click any user (for example, your own account) and select **Properties** → **Attribute Editor**. The **WOLPCNAME** attribute should now appear in the list. Here you can enter the user's PC name or multiple PC names separated by commas.



**Important:** The PC names must be entered exactly as they appear in the **Auto Shutdown Manager MMC** → **Client Details**. Typically, this is the fully qualified domain name (FQDN), for example: **w2016s.evp.local**



**Server Management Console**

Client Manager | Auto Group Assignment | Client Overview | Client Energy Profiles

Search filter:  v [X] [Y]

Clients found: 3 ☐ Show clients with technical problems ☐ WOL Pending

PC Name	Last connected	Number of own Seats	Number of Pool Seats	Release	Group	Remote WOL Address	Remote WOL Port
EnviProtUbuntu	16.12.2020 10:57:26	0	1	5.6.3.10	WOL Proxies		
wshplt.evp.local	16.12.2020 10:57:16	49590	0	5.6.8.31	EVP PowerServer		
W2016S.evp.local	16.12.2020 10:57:16	1	0	5.6.8.31	EVP Domain Controllers		

**Right Click** (indicated by a red arrow pointing to the 'W2016S.evp.local' row)

**Client Details for W2016S.evp.local**

MAC / BCA	00-0C-29-CD-79-C3	Manufacturer	VMware, Inc.	Physical Memory	2,0 GB
Release	5.6.8.31	PC Model	VMware Virtual Platform	# Processors	1
Power Supply State	Safe	PC System Type	Desktop	Energy Saved	0 kWh
Thermal State	Safe	Sleep Mode Support	Yes	Last IP Address	192.168.10.10
AD Groups	4	Client ID	3fda4087-f327-44ac-aa89-8ae5ad4f758a		

**Tip:** In the **Auto Shutdown Manager Server MMC** → **Network Clients** → **Clients Overview**, right-click the **Client Details for ...** field to copy the PC name to the **clipboard**. Other details, such as MAC addresses, manufacturer information, and similar data, can also be copied in the same way.

### WOLPCNAME Variable Name

If you want to use a different variable name for the WOL PCs attribute, open the **Web.config** file in your WOL Portal installation directory and search for **WOLPCsADAttributeName**.

```
<setting name="WOLPCsADAttributeName" serializeAs="String">
    <value>WOLPCNAME</value>
</setting>
```

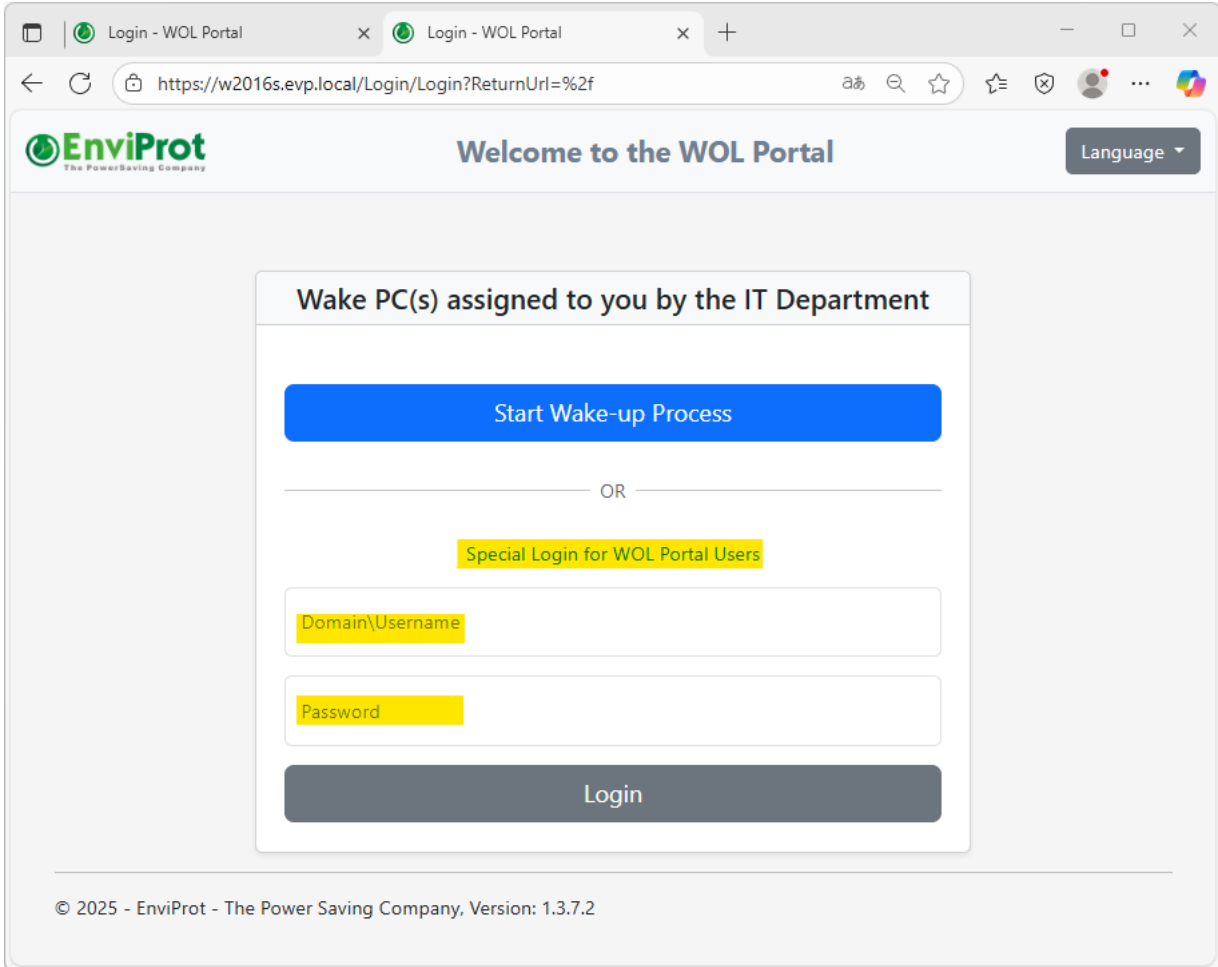
In the **<value>** field, enter the name of your custom Active Directory attribute (in this example, **WOLPCNAME**).

**Note:** If you change this value here, you must update the Active Directory schema accordingly, as described in the steps above.

Additional SAML-related settings can be overridden if required; however, it is recommended to keep the default values unless a specific configuration change is necessary.

## Testing the WOL Portal

To test the portal, open the site in a web browser, click on **Special Login for WOL Portal Users**, and log in using your **domain credentials**.



The screenshot shows a web browser window with two tabs labeled "Login - WOL Portal". The address bar shows the URL "https://w2016s.evp.local/Login/Login?ReturnUrl=%2f". The page header includes the EnviProt logo, the text "Welcome to the WOL Portal", and a "Language" dropdown menu. The main content area features a box titled "Wake PC(s) assigned to you by the IT Department". Inside this box, there is a blue button labeled "Start Wake-up Process". Below this button is a horizontal line with the word "OR" in the center. Underneath the line is a yellow button labeled "Special Login for WOL Portal Users". Below this button are two input fields: the first is labeled "Domain\Username" and the second is labeled "Password". At the bottom of the box is a grey button labeled "Login". The footer of the page contains the text "© 2025 - EnviProt - The Power Saving Company, Version: 1.3.7.2".

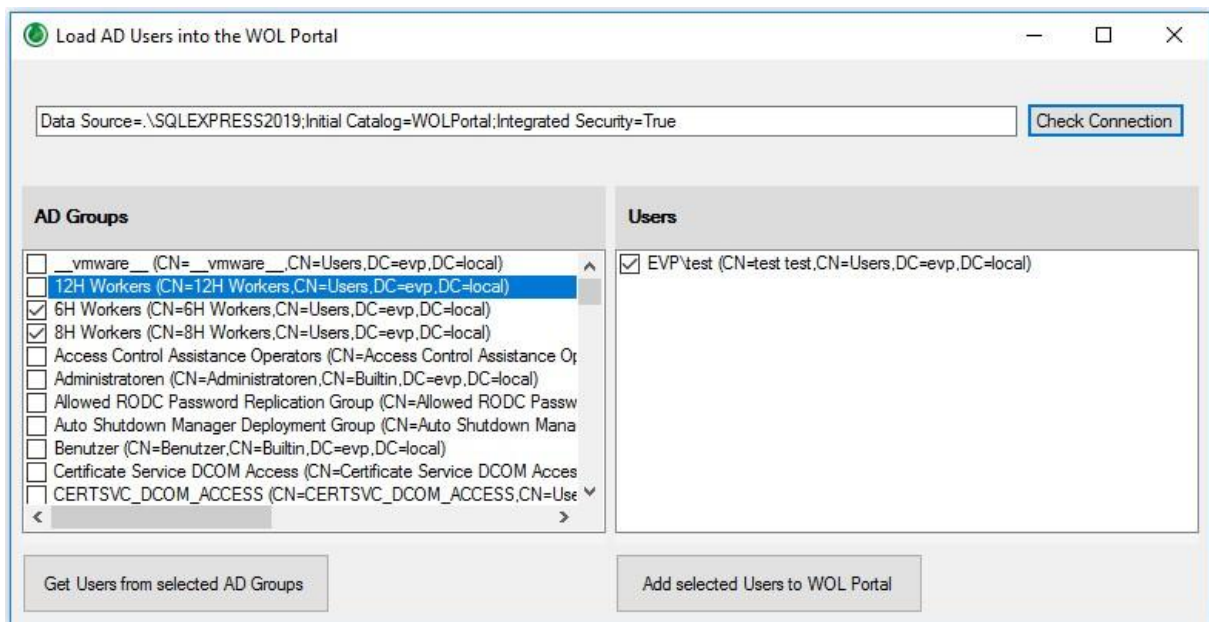
**Important: The first user to log in to the WOL Portal will automatically be assigned as the initial WOL Portal Administrator.** Additional administrators and users can be added, edited, or deleted as needed.

SSO users do not need to be added or configured as WOL Portal users; however, they can be if required—for example, to assign additional PCs that are not used on a daily basis. Their primary PC assignments are managed through Active Directory.

## Automatically Import Users from Active Directory

If the optional Single Sign-On (SSO) feature is not used, users and their associated computers must be manually configured by the WOL Portal administrator. Both modes can be combined. Users can use SSO for their primary, day-to-day PCs, while other PCs can be assigned directly within the WOL Portal.

The same ZIP file that contains the WOL Portal software also includes a tool named **ADUsersDataPump.exe**. This tool allows you to easily **import** multiple **users** directly from **Active Directory** into the WOL Portal and is especially useful for bulk imports from specific AD groups.



First, enter the same connection string that was configured during the WOL Portal setup, and click **Check Connection** to verify that a connection to the database can be established.

Next, select the Active Directory groups from which you want to import users, and click **Get Users from Selected AD Groups**.

A list of all users from the selected AD groups will be displayed. Deselect any users you do not want to import, then click **Add Selected Users to WOL Portal** to start the import process.

If you have questions, ideas, or improvement requests, contact us at [support@enviprot.com](mailto:support@enviprot.com)

## LEGAL NOTICE

### DISCLAIMER AND LIMITATION OF LIABILITY

THIS SOFTWARE IS PROVIDED "AS IS" WITHOUT ANY EXPRESS, IMPLIED, OR STATUTORY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT. THE ENTIRE RISK ARISING FROM THE INSTALLATION, CONFIGURATION, OPERATION, AND USE OF THE SOFTWARE REMAINS WITH THE USER.

ALTHOUGH THE SOFTWARE HAS BEEN CAREFULLY DEVELOPED AND EXTENSIVELY TESTED, IT MAY STILL CONTAIN DEFECTS, ERRORS, OR BUGS. THE DEVELOPER AND DISTRIBUTOR MAKE NO REPRESENTATIONS OR WARRANTIES THAT THE SOFTWARE WILL OPERATE WITHOUT INTERRUPTION, BE ERROR-FREE, OR MEET ANY SPECIFIC PERFORMANCE OR SECURITY REQUIREMENTS.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE DEVELOPER AND DISTRIBUTOR SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY, OR PUNITIVE DAMAGES, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF DATA, BUSINESS INTERRUPTION, UNAUTHORIZED ACCESS, HACKING, OR CRIMINAL MISUSE OF THE WOL PORTAL OR RELATED SYSTEMS, EVEN IF THE DEVELOPER OR DISTRIBUTOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

ALL RISK ASSOCIATED WITH THE INSTALLATION, CONFIGURATION, OPERATION, AND USE OF THIS SOFTWARE LIES SOLELY WITH THE USER. USERS ARE STRONGLY ADVISED TO TEST THE SOFTWARE IN THEIR OWN ENVIRONMENT BEFORE DEPLOYING IT IN PRODUCTION SYSTEMS. IF YOU DO NOT AGREE TO THESE TERMS, DO NOT INSTALL OR USE THE SOFTWARE.

NOTHING IN THIS LIMITATION SHALL EXCLUDE OR RESTRICT LIABILITY WHERE SUCH EXCLUSION OR RESTRICTION IS PROHIBITED BY APPLICABLE LAW, INCLUDING LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM NEGLIGENCE OR WILFUL MISCONDUCT.

### SEVERABILITY CLAUSE

IF ANY PROVISION OF THIS DISCLAIMER OR LIMITATION OF LIABILITY IS HELD TO BE INVALID OR UNENFORCEABLE UNDER APPLICABLE LAW, THE REMAINING

PROVISIONS SHALL REMAIN IN FULL FORCE AND EFFECT. THE INVALID OR UNENFORCEABLE PROVISION SHALL BE REPLACED BY A VALID PROVISION THAT MOST CLOSELY REFLECTS THE ORIGINAL INTENT AND PURPOSE OF THE INVALID PROVISION.

## **GOVERNING LAW AND JURISDICTION**

THIS AGREEMENT AND ANY DISPUTE OR CLAIM ARISING OUT OF OR IN CONNECTION WITH IT SHALL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE FEDERAL REPUBLIC OF GERMANY, EXCLUDING ITS CONFLICT-OF-LAW RULES. THE EXCLUSIVE PLACE OF JURISDICTION FOR ALL DISPUTES ARISING FROM OR IN CONNECTION WITH THIS SOFTWARE SHALL BE STUTTGART, GERMANY.

## **COPYRIGHT AND INTELLECTUAL PROPERTY**

ALL RIGHTS, TITLE, AND INTEREST IN AND TO THIS SOFTWARE, INCLUDING ALL CODE, DOCUMENTATION, AND RELATED MATERIALS, REMAIN THE EXCLUSIVE PROPERTY OF THE DEVELOPER OR ITS LICENSORS. UNAUTHORIZED REPRODUCTION, DISTRIBUTION, OR MODIFICATION OF THE SOFTWARE OR ANY PART THEREOF IS STRICTLY PROHIBITED.