**Remote Windows Agent Installation**

This document will take the user through the steps necessary to install and setup their remote Windows agent.

The user will need:

* The Remote Windows Agent installer
* The SSL certificates from the servers that will be making calls to the agent. (.pfx or .p12 files)

Once the customer has downloaded ***RemoteWindowsAgentInstaller.exe***, they just have to run the executable. The installer will go through these steps:

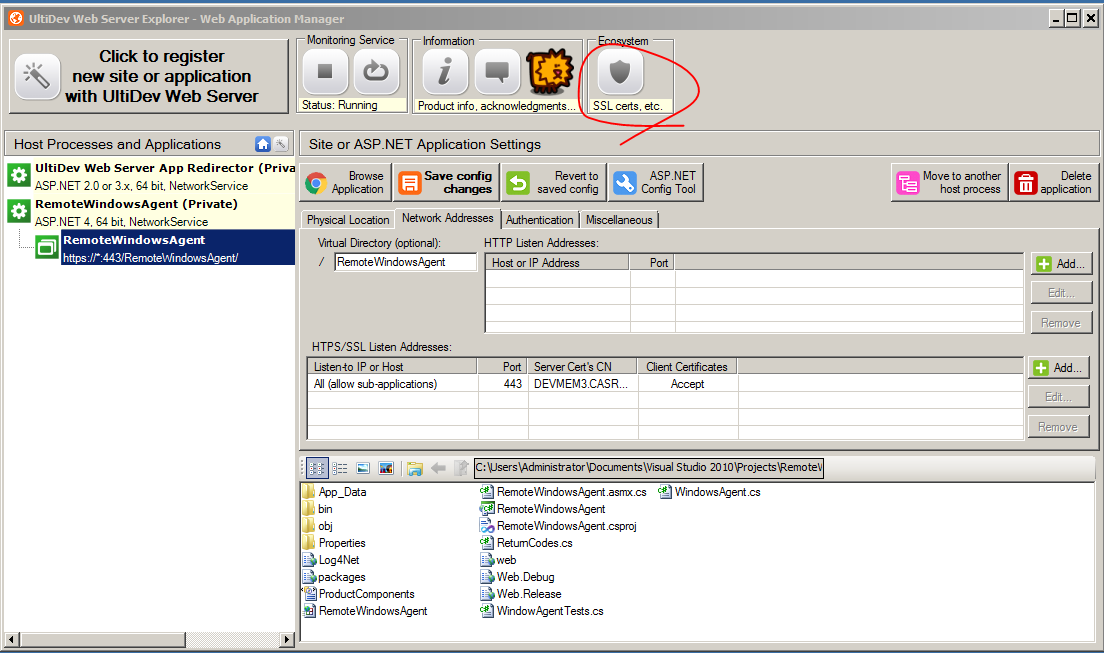
1. Check that .NET Framework 4.0 is installed
   1. If it is not, the executable will install it.
2. Install UltiDev’s Web Server Pro
   1. The user will have to accept terms of use to continue with the installation.
3. Install the files needed to setup the application on Web Server Pro.
   1. These will be located at ***C:\Program Files (x86)\Avatier\RemoteWindowsAgent***

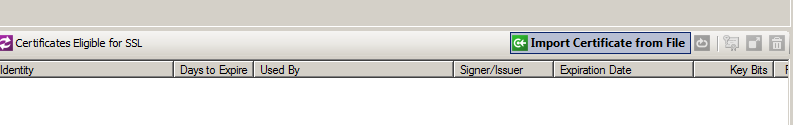
*Note* that if the executable installs .NET for the user, the user will need to use Windows Update to install updates and patches for .NET and then reboot. If the user does not update, they may see errors in later steps during setup.

After the installer has run, the user can now open up Web Server Pro and continue the setup process.

Web App Explorer Setup

The first thing the user will need to do is register their SSL certificates with the server following these steps:

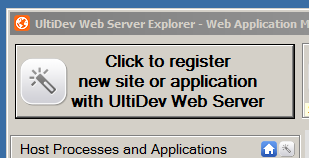
1. Open UtilDev Web App Explorer. The link will be in the start menu. The window will look like the one below.
2. Click the shield icon that is circled in the image above.
3. Click import from file to import your .pfx or .p12 files.



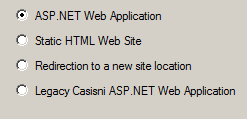
1. It is best to make the certificate’s private key non-exportable.
2. Repeat this until all certificates are added.

Now that the SSL certificates are in place, the user can begin to register the application.

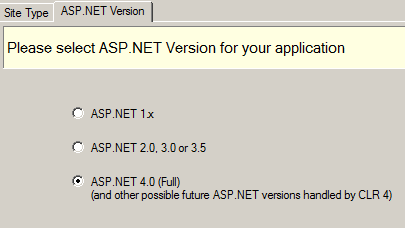
1. In order to start setup, click the large registration button in the top left of the UtilDev Web App Explorer window.



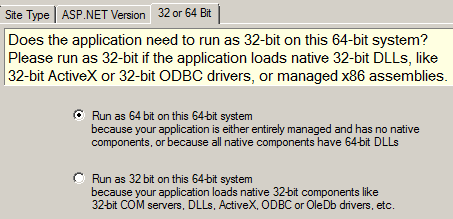
1. The application will be an APS.NET web app

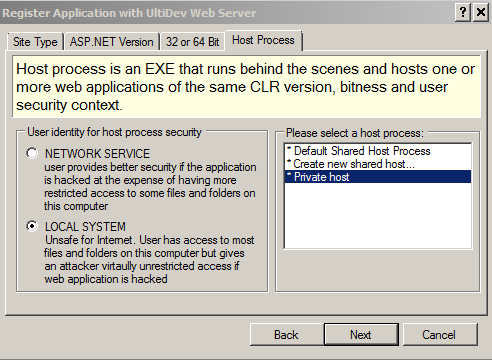


1. The application will run on ASP.NET 4.0(full)

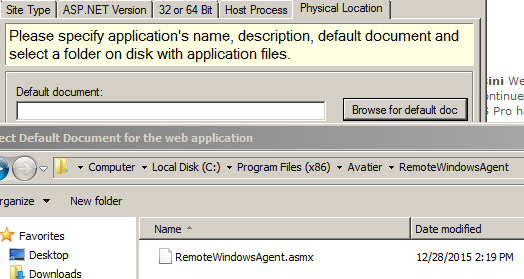


1. Run the application as 64-bit

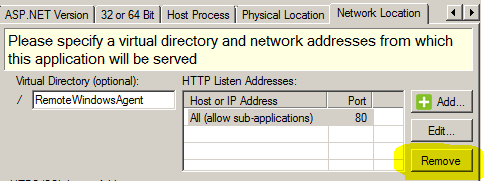


1. The application will be a LOCAL service running on a private host.

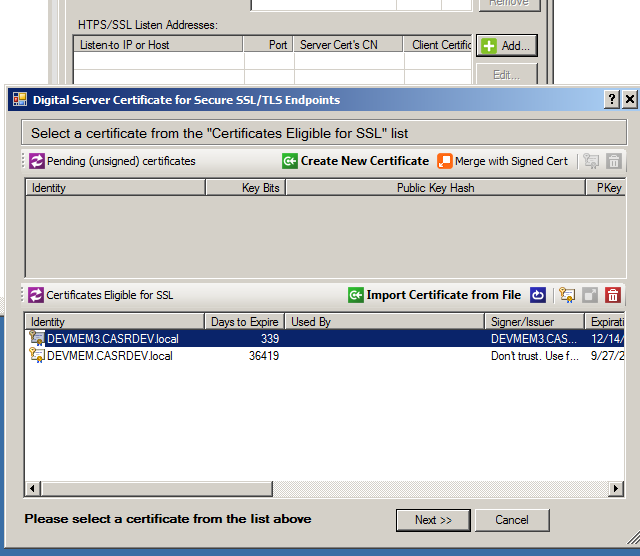
1. The default document will be C:\Program Files (x86)\Avatier\RemoteWindowsAgent\RemoteWindowsAgent.asmx. The other fields will auto fill.



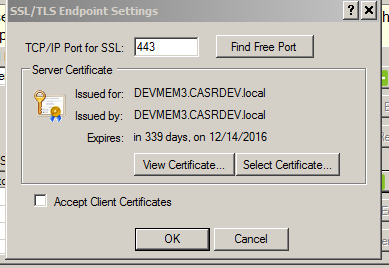
1. Click the item under HTTP listener ports and delete it.



1. Now under HTTPS listener ports, click add.

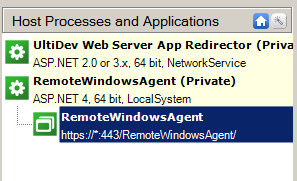


1. Select the SSL certificate you wish to use and hit next.
2. Choose the port you wish to use, or have the server find one for you. and hit ok.



1. Repeat this process until you have added all of the server certificates that are needed. Then click next.
2. Leave the authentication as anonymous.
3. Leave the default settings in other settings and click finish.

Once all of these steps are completed inside of the Web Application Explorer the user should see the service in the list on the left, and the icon should be green to indicate that it is running.



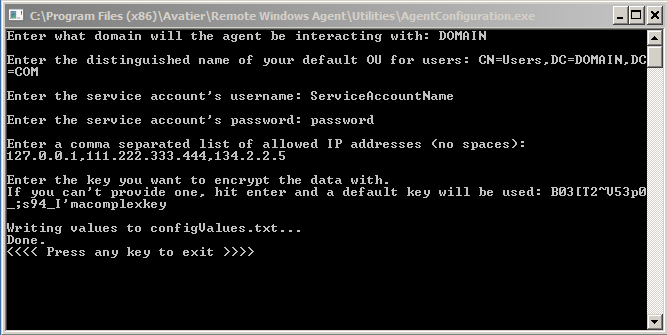
**Running Agent Configuration Executable**

Now the user needs to configure the web service so that it can communicate with Active Directory.

The configuration executable is located in:

**C:\Program Files (x86)\Avatier\Remote Windows Agent\Utilities**

Run the executable and enter the values requested.

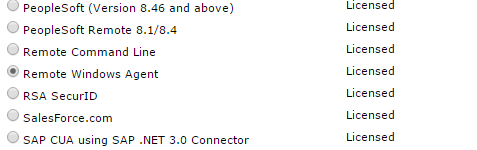


Upon receiving the next SOAP request, the agent will take up and store the new values in an encrypted form and delete the text file.

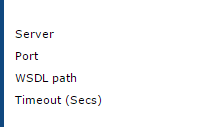
**Configuring AIMS**

The user should now be ready to go and configure their connector in AIMS to point at this agent.

In the connectors list, add a Remote Windows Agent connection.



Edit the new connector and give it the desired configuration options for these config options



Below is a sample setup.