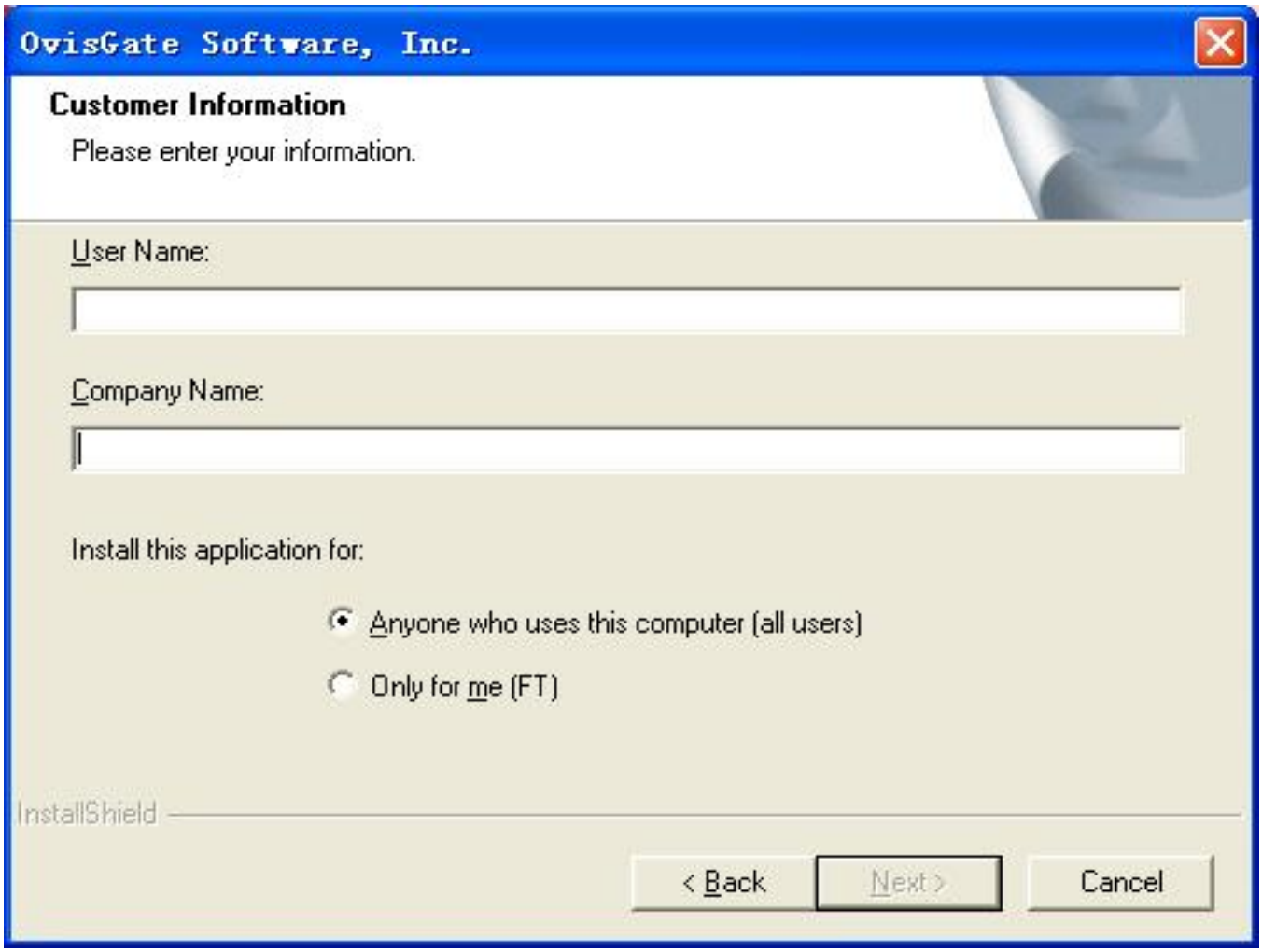
Installation Guide:

Step 1:

This window should appear once the setup is started. Enter in an appropriate user name and company, and then choose the installation type.

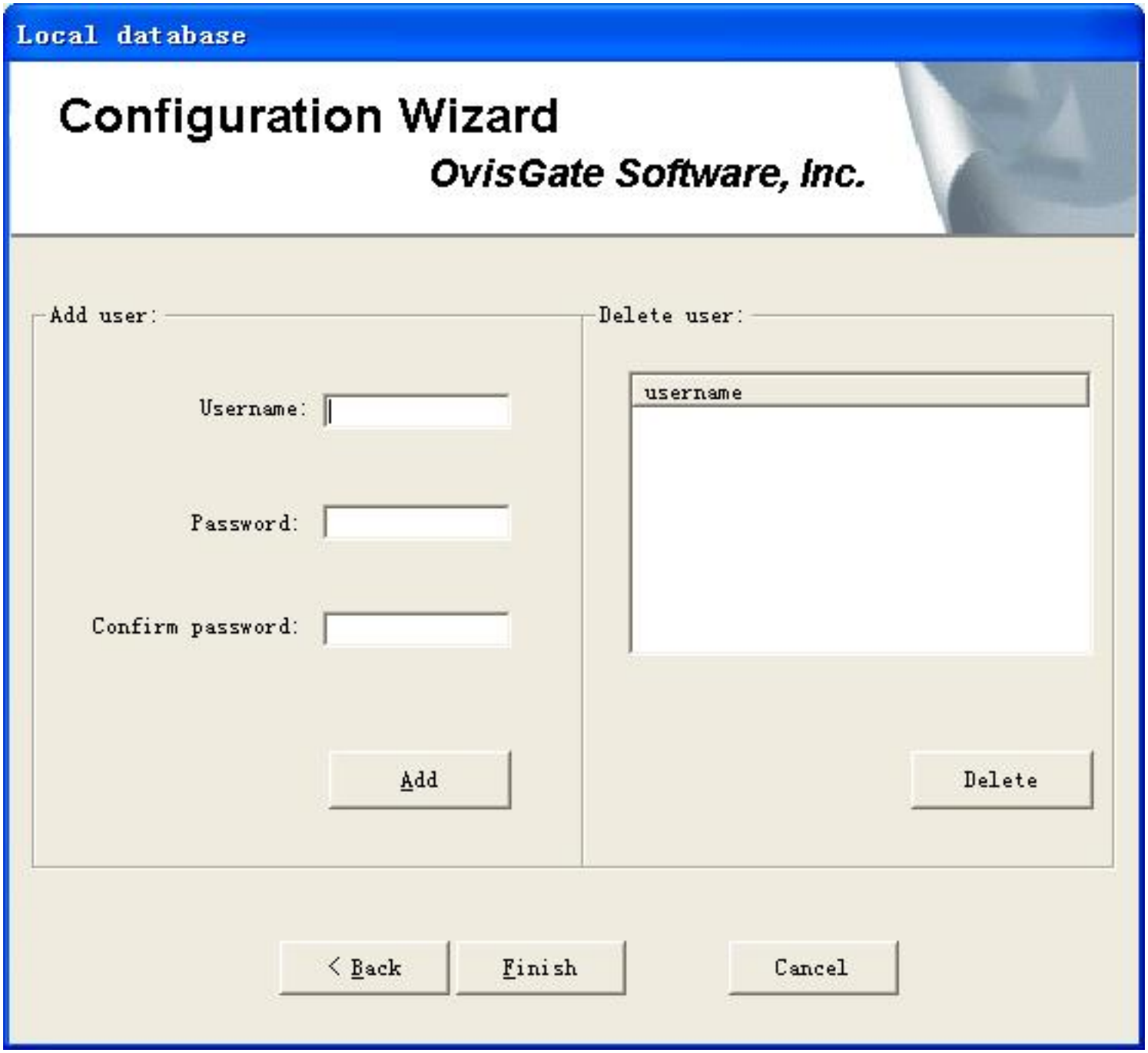


Step 2:

Here you should choose the type of "User Authentication" user wish to use.
Note: you must have a Radius, LDAP or Domain server in place in order to use those options.

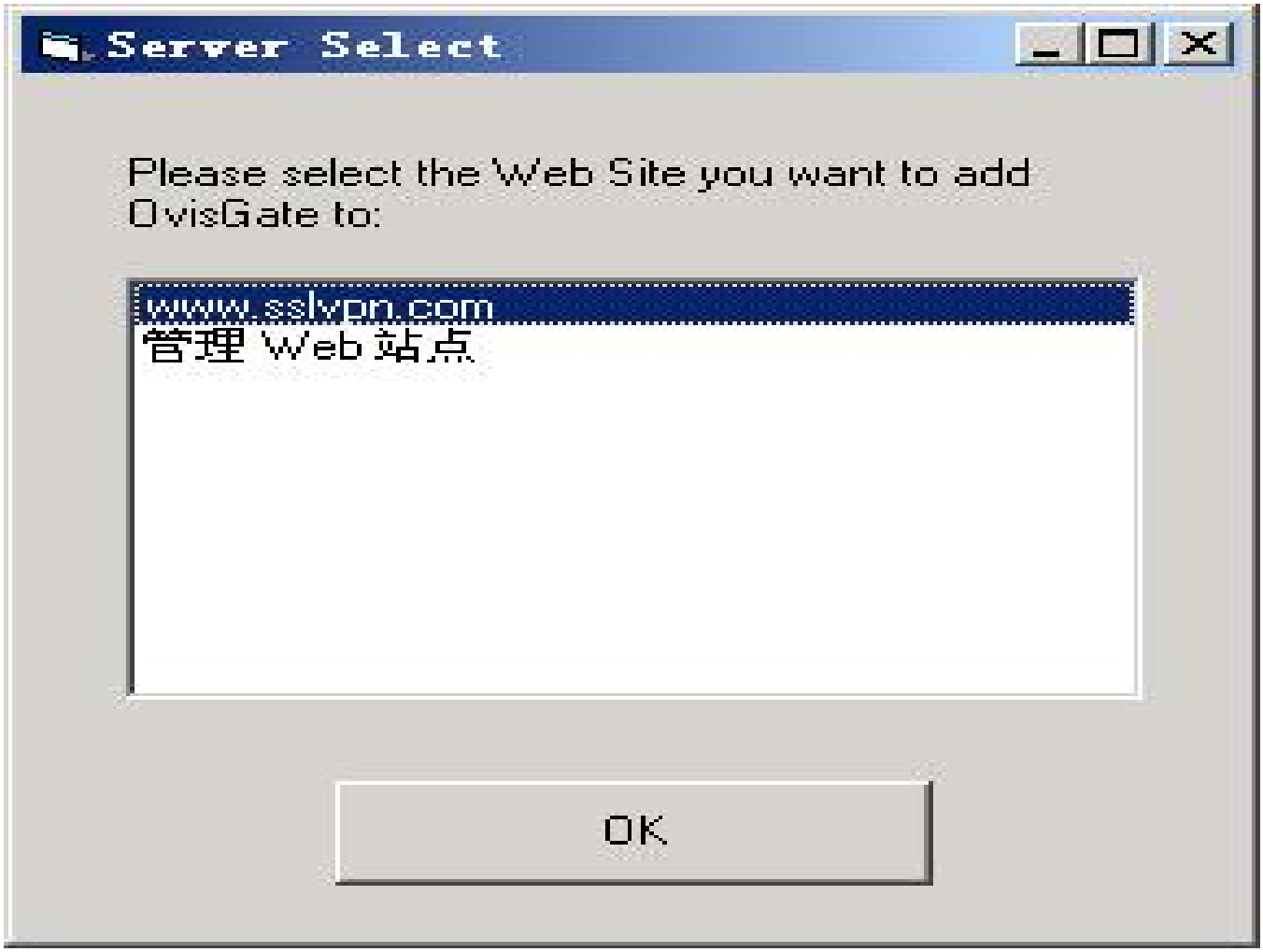
Step 3:

You need to follow the specific instructions for each specific User Authentication type. For Example, if "Local Database" is chosen, you would add users by inputting unique usernames and passwords into their respective fields. Once added the username will appear in the list to the right.

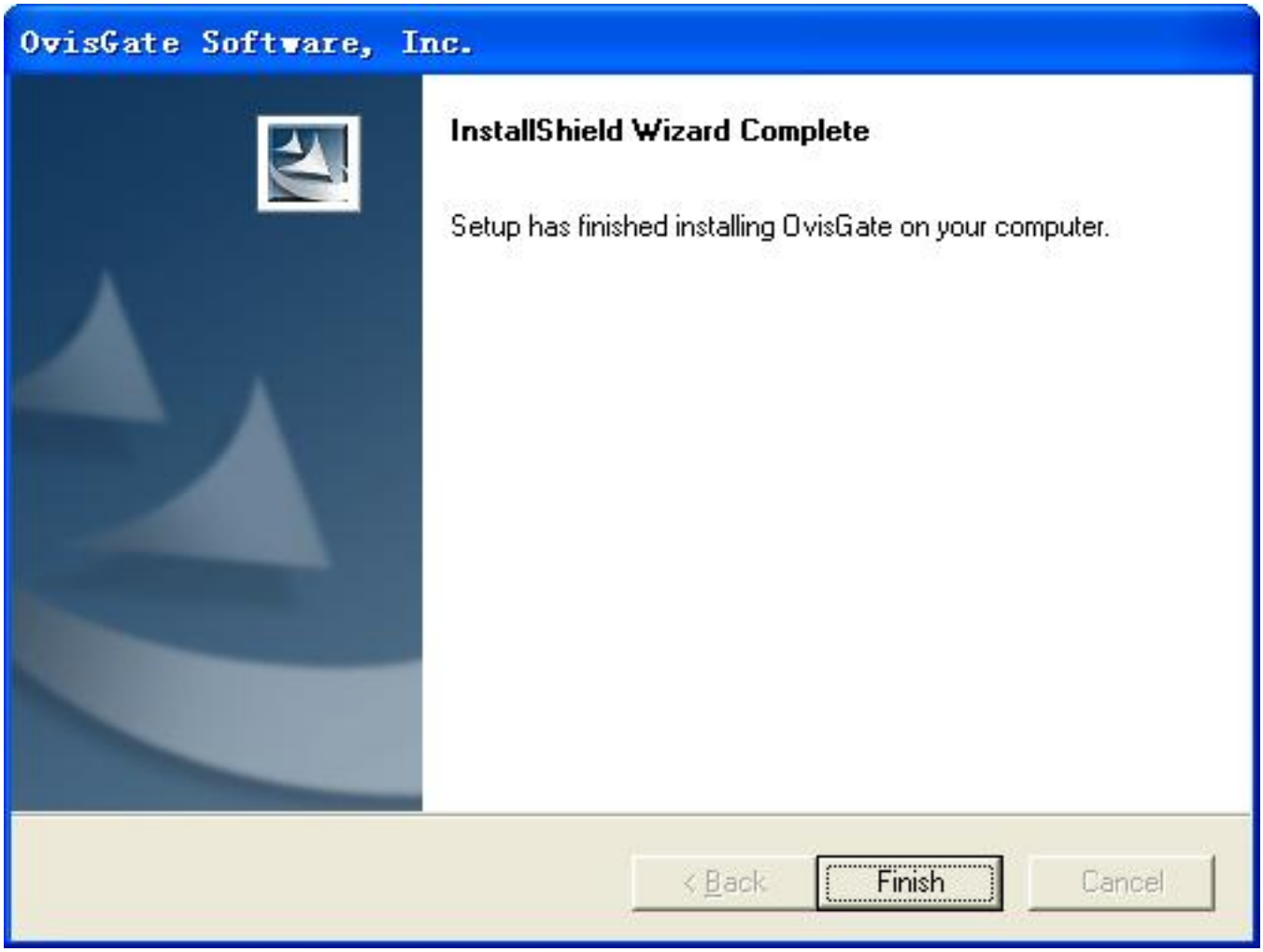


Step 4:

Select the site for OvisGate.



Step 5:
Finish the installation.



Step 6:

Configuration

After installation, you should do some configuratation, this subject is refered on "Admin guide"

Step 7:

Open specfic ports for OvisGate.

If OvisGate server is befind the firewall, you must map these ports on the firewall to OvisGate server, the ports OvisGate service need are:

80: for HTTP access
443:for HTTPS access
6616: the OvisGate service port

Step 8:

If you wish to use an HTTPS Connection, you will need to setup a Security Certificate. OvisGate comes standard with a temporary certificate that may be used if you do not have your own certificate, you can import this temporary certificate to secure your Web sites by following these steps below:
(it refers to MSDN article:How to Import a Server Certificate for Use in Internet Information Services 5.0, and we have added some comments.)

In order to complete this operation, you must have a backup of the server certificate (and private key) contained in a PFX file.(It is **ovisgate.PFX** in the package, and the password is **ovisgate**)

You must also have access to the Certificates snap-in and have it set to view computer certificates from the local computer (though this can be done remotely).

In order to view the Certificates store on the local computer, perform the following steps:

1. Click **Start**, and then click **Run**.
2. Type "MMC.EXE" (without the quotation marks) and click **OK**.
3. Click **Console** in the new MMC you created, and then click **Add/Remove Snap-in**.
4. In the new window, click **Add**.
5. Highlight the **Certificates** snap-in, and then click **Add**.
6. Choose the **Computer** option and click **Next**.
7. Select **Local Computer** on the next screen, and then click **OK**.
8. Click **Close** , and then click **OK**.
9. You have now added the Certificates snap-in, which will allow you to work with any certificates in your computer's certificate store. You may want to save this MMC for later use.

Now that you have access to the Certificates snap-in, you can import the server certificate into you computer's certificate store by following these steps:

1. Open the Certificates (Local Computer) snap-in and navigate to **Personal**, and then **Certificates**.

Note: Certificates may not be listed. If it is not, that is because there are no certificates installed.

2. Right-click **Certificates** (or **Personal** if that option does not exist.)
3. Choose **All Tasks**, and then click **Import**.
4. When the wizard starts, click **Next**. Browse to the PFX file you created containing your server certificate and private key.(We package our temporary PFX file in the zip file named as "**ovisgate.PFX**") Click **Next**.
5. Enter the password you gave the PFX file when you created it. (The password is **ovisgate** in our PFX file **ovisgate.PFX**)
6. Click **Next**, and then choose the Certificate Store you want to save the certificate to. You should select **Personal** because it is a Web server certificate. If you included the certificates in the certification hierarchy, it will also be added to this store.
7. Click **Next**. You should see a summary of screen showing what the wizard is about to do. If this information is correct, click **Finish**.
8. You will now see the server certificate for your Web server in the list of Personal Certificates. It will be denoted by the common name of the server (found in the subject section of the certificate).

Now that you have the certificate backup imported into the certificate store, you can enable Internet Information Services 5.0 to use that certificate (and the corresponding private key). To do this, perform the following steps:

1. Open the Internet Services Manager (under Administrative Tools) and navigate to the Web site you want to enable secure communications (SSL/TLS) on.
2. Right-click on the site and click **Properties**.
3. You should now see the properties screen for the Web site. Click the **Directory Security** tab.
4. Under the **Secure Communications** section, click **Server Certificate**.
5. This will start the Web Site Certificate Wizard. Click **Next**.
6. Choose the **Assign an existing certificate** option and click **Next**.
7. You will now see a screen showing that contents of your computer's personal certificate store. Highlight your Web server certificate (denoted by the common name), and then click **Next**.
8. You will now see a summary screen showing you all the details about the certificate you are installing. Be sure that this information is correct or you may have problems using SSL or TLS in HTTP communications.
9. Click **Next**, and then click **OK** to exit the wizard.

You should now have an SSL/TLS-enabled Web server.

This is a **TEMPORARY CERTIFICATE**. You should obtain your own, permanent certificate. For information on obtaining your own certificate visit:

1. Microsoft Knowledge Base Article - 228821:Generating a Certificate Request File Using the Certificate Wizard in IIS 5.0
2. Microsoft Knowledge Base Article - 228836:Installing a New Certificate with Certificate Wizard for Use in SSL/TLS