Installing a Secure FTP Server on Windows using IIS

You may want to install a secure FTP server on Windows either as standalone file storage or to have means of editing your website hosted on IIS (Internet Information Services) web server. In both cases, you can use an optional *FTP Server* component of the IIS. It can be installed standalone or along with a *Web Server*.[1)]

Installing FTP Server

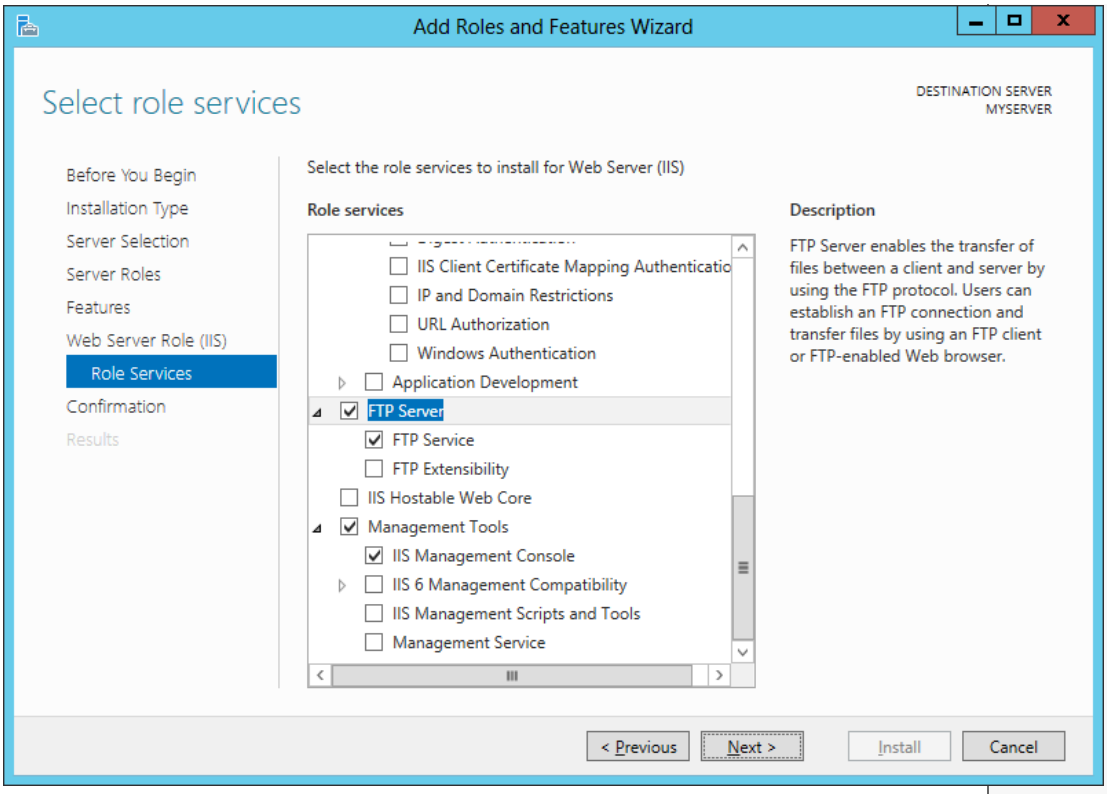
Edit

On Windows Server 2016 and Windows Server 2012

Edit

- In Windows *Server Manager* go to *Dashboard* and run *Manage > Add Roles and Features*.

- In *Add Roles and Features* wizard:
  - Proceed to *Installation Type* step and confirm *Role-based or feature-based installation*.
  - Proceed to *Server Roles* step and check *Web Server (IIS)* role. Note that it is checked already, if you had IIS installed as a Web Server previously. Confirm installing *IIS Management Console* tool.
  - Proceed to *Web Server Role (IIS) > Role Services* step and check *FTP Server* role service. Uncheck *Web Server* role service, if you do not need it.
  - Proceed to the end of the wizard and click *Install*.
  - Wait for the installation to complete.



Skip to the **next step**.

On Windows Server 2008 R2

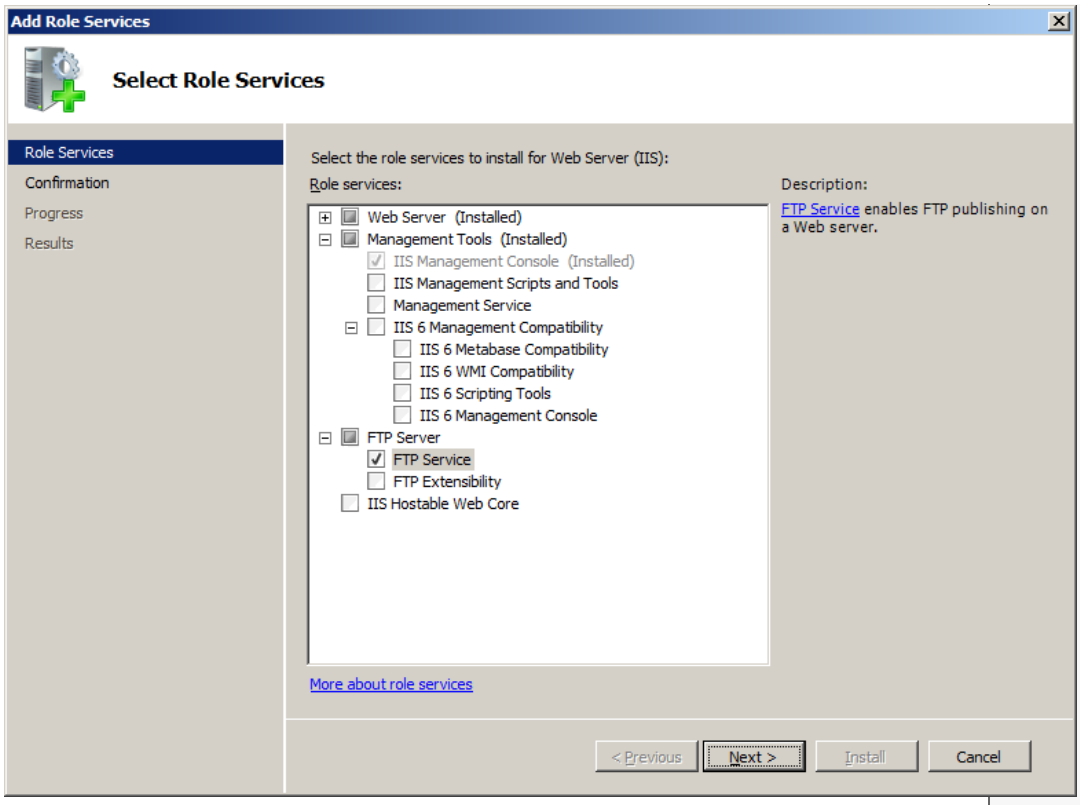
Edit

If you do not have IIS installed yet:

- In Windows *Server Manager* go to *Roles* node and in *Roles Summary* panel click *Add Roles*.
- In *Add Roles* wizard:
  - Proceed to *Server Roles* step and check *Web Server (IIS)* role.
  - Proceed to *Role Services* step and check *FTP Server > FTP Service* role service. Uncheck *Web Server* role service, if you do not need it. Make sure *Management Service > IIS Management Console* role service is checked.
  - Proceed to the end of the wizard and click *Install*.
  - Wait for the installation to complete.

If you have IIS installed already (i.e. as a Web Server):

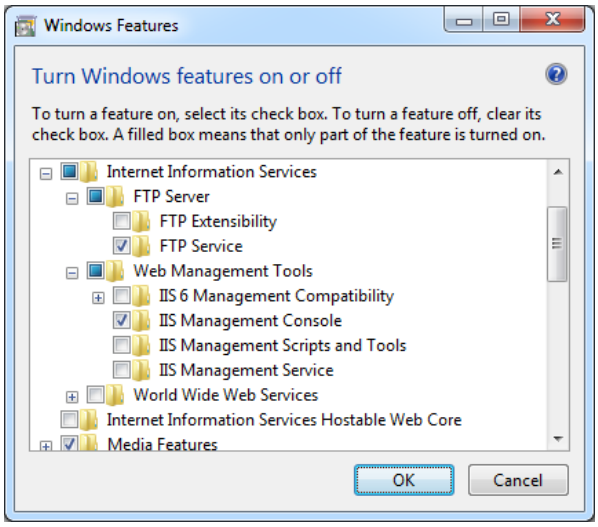
- In Windows *Server Manager* go to *Roles* node and in *Web Server (IIS) > Role Services* panel click *Add Role Services*.
- In *Add Role Services* wizard:
  - Check *FTP Server > FTP Service* role service.
  - Make sure that *Management Service > IIS Management Console* is checked.
  - Confirm with *Next* button.
  - Proceed to the end of the wizard and click *Install*.
  - Wait for the installation to complete.



Skip to the **next step**.

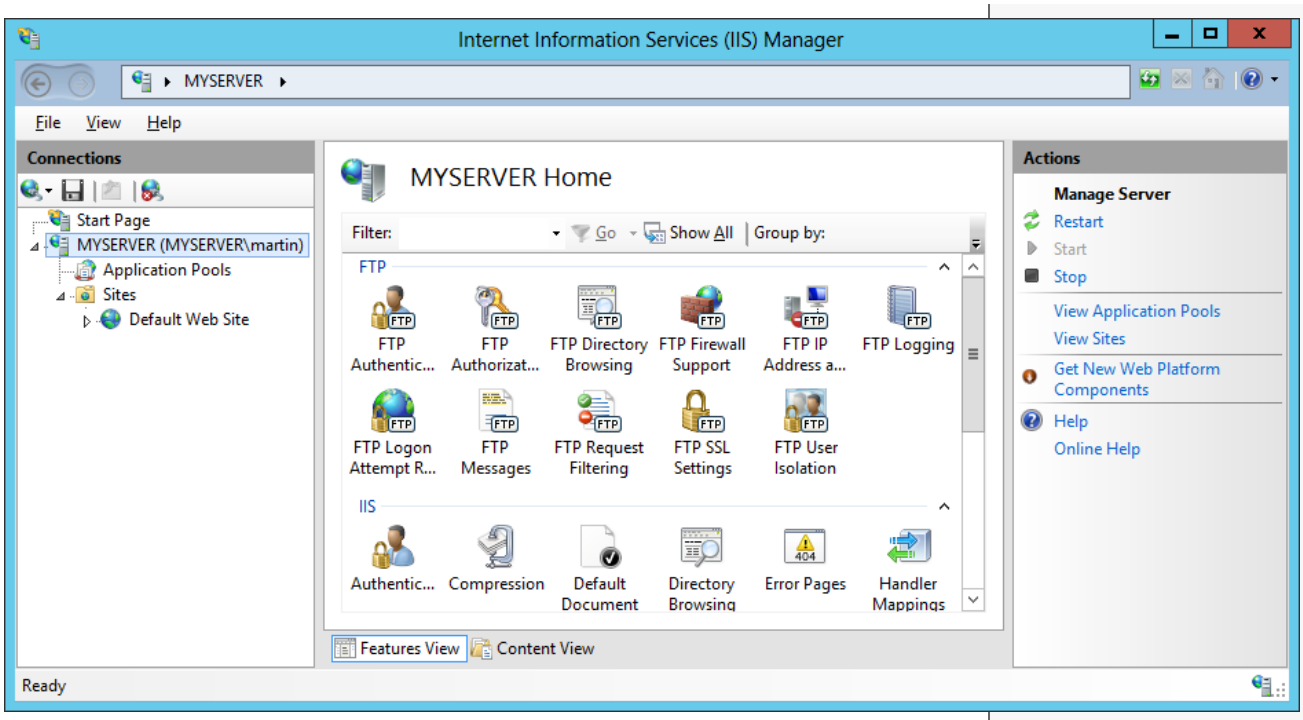
On Windows Desktop (Windows 10, Windows 8, Windows 7 and Windows Vista)

- Go to *Control Panel > Programs > Program and Features > Turn Windows features on or off*.
- On a *Windows Features* window:
  - Expand *Internet Information Services > FTP Server* and check *FTP Service*.
  - Expand *Internet Information Services > Web Management Tools* and check *IIS Management Console*, if it is not checked yet.
  - Confirm with *OK* button.
  - Wait for the installation to complete.



Opening IIS Manager

- Go to *Control Panel > System and Security > Administrative Tools* and open *Internet Information Services (IIS) Manager*.
- Navigate to your Windows server node.



Creating Certificate for the FTPS Server

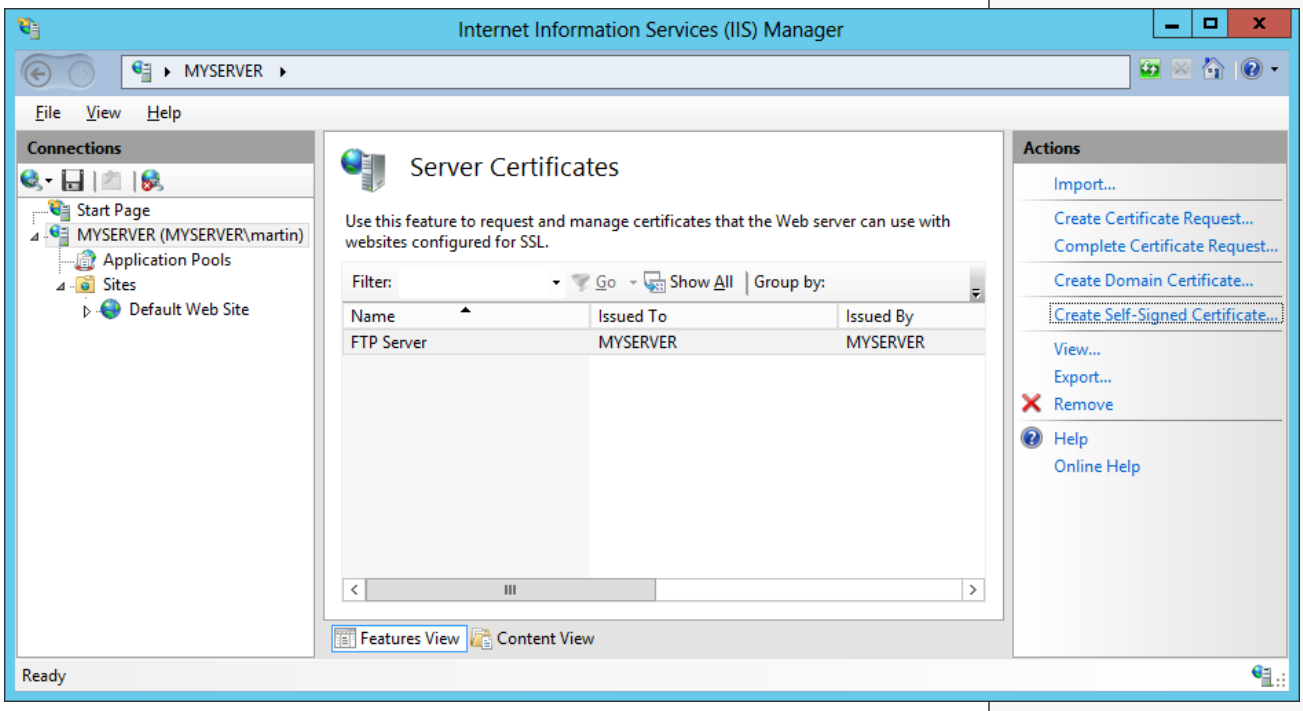
You need a TLS/SSL certificate to secure your FTPS server. Ideally you should acquire the certificate from a certificate authority.

You may also create a self-signed certificate locally, but in such case users of your FTPS server **will be warned**, when connecting to the server.

To create the self-signed certificate:

- In *IIS Manager*, open *IIS > Server Certificates*.
- Click on *Create Self-Signed Certificate* action.
- Specify a certificate name (e.g. “FTP Server”) and submit with *OK*.

Note that Microsoft Azure Windows servers created on the old Azure Management portal manage.windowsazure.com come with a self-signed certificate, so you do not need to create one.



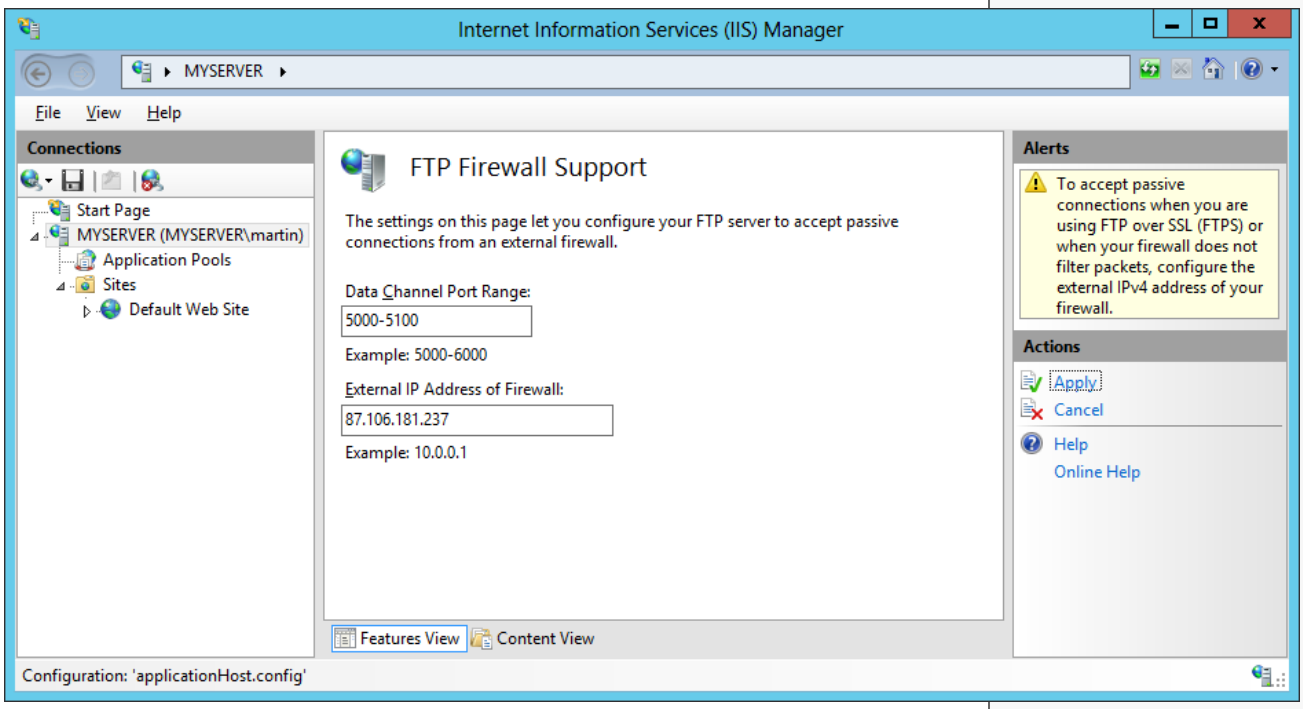
Servers behind external Firewall/NAT

If your server is behind an external firewall/NAT, you need to tell the FTP server its external IP address, to allow passive mode connections.

- In *IIS Manager*, open *FTP > FTP Firewall Support*.
- Specify your server's external IP address.
  For **Microsoft Azure Windows servers** you will find the external IP address:
  - On the new Azure Portal portal.azure.com: IP address: in *Public IP address* section in *Essentials* panel;
  - On the old Azure Management Portal manage.windowsazure.com: in *Public virtual IP (VIP) address* section on *Quick glance* sidebar of your instance dashboard; or as a *Public IP* on the instance desktop.

When behind an external firewall, you need to open ports for data connections (obviously in addition to opening an FTP port 21 and possibly an implicit TLS/SSL FTP port 990). You won't probably want to open whole default port range 1024-65535. In such case, you need to tell the FTP server to use only the range that is opened on the firewall. Use a *Data Channel Port Range* box for that. Any time you change this range, you will need to **restart FTP service**. *Learn how to open ports on Microsoft Azure.*

Click *Apply* action to submit your settings.



Some external firewalls are able to monitor FTP control connection and automatically open and close the data connection ports as needed. So you do not need to have whole port range opened all the time, even when not in use. This won't work with the secure FTPS as the control connection is encrypted and the firewall cannot monitor it.

Windows Firewall Rules

An internal Windows firewall is automatically configured with rules for the ports 21, 990 and 1024-65535, when IIS FTP server is installed.

The rules are not enabled initially though some versions of Windows.[2)] To enable or change the rules, go to *Control Panel > System and Security > Windows Firewall > Advanced Settings > Inbound Rules* and locate three "FTP server" rules. If the rules are not enabled, click on *Actions > Enable Rule*.

Restarting FTP Service

While the internal Windows firewall is automatically configured to open FTP ports when FTP server is installed, this change does not seem to apply, until FTP service is restarted. The same is true for changing data channel port range.

To restart FTP service go to *Control Panel > System and Security > Administrative Tools* and open *Services*. Locate *Microsoft FTP Service* and click *Restart service*.[3)]

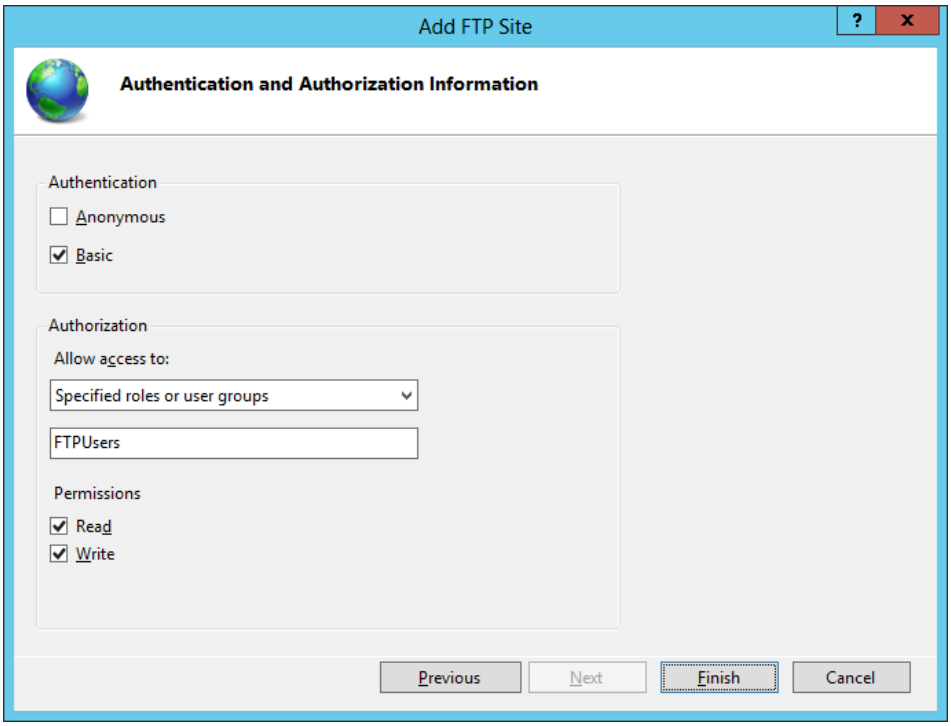
Adding FTP Site

To a Web Site

If you want to add FTP server to manage your web site remotely, locate your web site node in *IIS Manager* and:

- Click *Add FTP Publishing* action.
- In *Add FTP Site Publishing* wizard:
  - On an initial *Binding and SSL Settings* step, select *Require SSL* to disallow non-encrypted connections and select your certificate.
  - On *Authentication and Authorization Information* step, select *Basic* authentication and make sure *Anonymous* authentication is not selected. Select which users (Windows accounts) you allow to connect to the server with what permissions. You can choose *All users* or select only some. Do not select *Anonymous users*.
  - Submit with *Finish* button.

Your secure FTPS server is now running and can be **connected to**.



Standalone FTP Site

If you want to add a standalone FTP server to store/exchange files, locate *Sites* node (folder) of your Windows server in *IIS Manager* and:

- Click *Add FTP Site* action.
- In *Add FTP Site* wizard:
  - On an initial *Site Information* step, give a name to your FTP site (if it's the only site you are going to have, simple "FTP site" suffice) and specify a path to a folder on your server's disk that is going to be accessible using FTP.
  - On a *Binding and SSL Settings* step, select *Require SSL* to disallow non-encrypted connections and select your certificate.
  - On *Authentication and Authorization Information* step, select *Basic* authentication and make sure *Anonymous* authentication is not selected. Select which users (Windows accounts) you allow to connect to the server with what permissions. You can choose *All users* or select only some. Do not select *Anonymous users*.
  - Submit with *Finish* button.

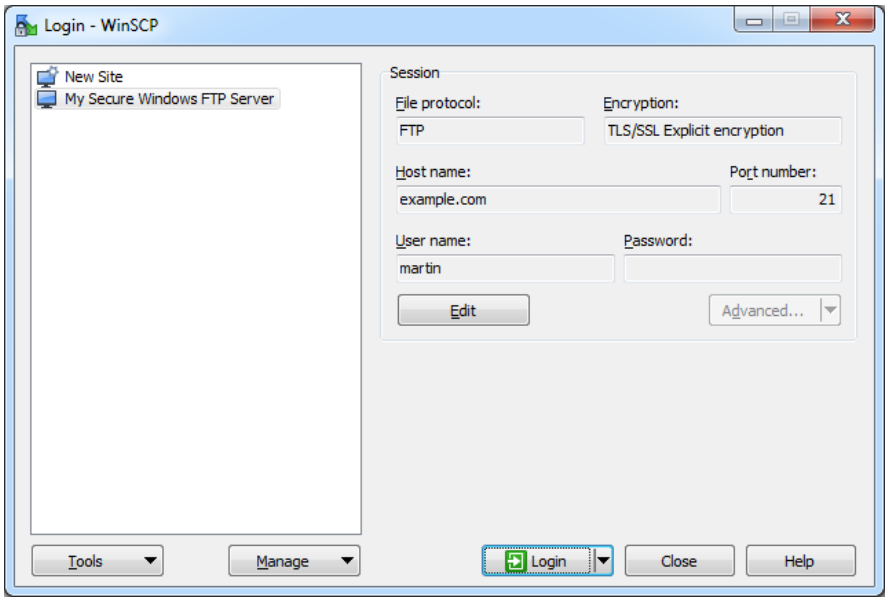
Your secure FTPS server is now running and can be **connected to**.

Connecting to Your FTPS Server

For connecting to a Microsoft Azure Windows instance, see a specific guide.

Start WinSCP. **Login Dialog** will appear. On the dialog:

- Select *FTP* protocol and *TLS/SSL Explicit encryption*.
- Enter your Windows server hostname to *Host name* field. Avoid using an IP address to allow WinSCP to verify that the host name matches with host the server's certificate was issued to (not applicable to self-signed certificates).
- Specify username and password of Windows account you want to connect with (when using domain accounts, you need to specify full username with format `domain\username`).
- You may want to **save your session details** to a site so you do not need to type them in every time you want to connect. Press *Save* button and type site name.
- Press *Login* to connect.
- If you are using **self-signed certificate**, you will be prompted to **accept it**.



Further reading

- Guide to **installing secure FTP server on Microsoft Azure using IIS**;
- Guide to **Installing SFTP/SSH Server on Windows using OpenSSH**;
- Guide to **uploading files to FTPS server**;
- Guide to **automating operations** (including upload).

1) This guide is partially based on article **Setting up a Passive FTP Server in Windows Azure VM**.
2) The rules are enabled initially on Windows Server 2016.
3) Try restarting whole system, if a service restart does not help.

guide_windows_ftps_server.txt · Last modified: 2017-04-11 by martin