

miniFTP Server

**(FTPS for
Windows 2000, Windows
2003, WindowsXP and Vista)**

This document is protected by Federal Copyright Law and may not be reproduced, transcribed, copied or duplicated by any means without the expressed written permission of:

**Blue Smoke Software
13301 Southwest Highway
Orland Park, IL 60462
(708) 671-0100**

It is believed that the information contained in this manual is accurate, however no responsibility, financial or otherwise will be accepted for any consequence arising out of the use of this material.

Table of Contents

Table of Contents	3
Introduction	4
Scenario	4
Compatibility	4
Installation	5
Activation	11
Configuration.....	12
MODE	15
Authentication Level	15
Require Client Certificate.....	16
Ignore Untrusted Root.....	16
Ignore Invalid Date.....	16
Ignore Invalid Signature	16
Server Certificate.....	16
Port Number	16
Max Idle Time	16
System Name.....	16
Status Response.....	17
Root Directory.....	17
Log Directory	17
Client Usercode	17
Client Password.....	17
Allow Restarts	17
Only Run Service when I am Logged On.....	17
Welcome Message.....	17
Quit Message	17
Starting The Service	18
In Case of Difficulty.....	19
Service Fails to Start.....	19
Clients Can not Connect.....	19
Clients Connect but then Disconnect.....	19
Making Changes to an existing Configuration	19
Supported Client Commands.....	19

Introduction

Blue Smoke Software. has developed a small compact FTP server to serve the needs of many large financial data centers throughout the country. Since Security has become a major concern of all companies, PNCI Software has made this software available to all industries including Health Care and government.

The concept behind miniFTPServer is simple. It was designed for a single data center to be able to distribute files in a timely fashion when Data Center processing was complete. It is the Data Centers desire to send files (or receive files) to (from) remote servers as soon as batch processing is complete regardless of time of day.

Most Secure FTP Servers on the market today are over kill and make it cost prohibited to deploy.

Scenario

A large Banking service center finishes its nightly processing at 2:00 AM. It does processing for over a 1000 branches. Reports need to be at the branches when the branches open early in the morning. Having a central server doesn't fit this requirement, because the clients would need to come in before the branches opened, to pull the files down from the central server and subsequently print them. To put a traditional FTPS server at each location would cost close to ½ million dollars. This is where the miniftpserver comes in. For roughly the same cost as a FTPS client(under \$50) , The Data Center can send the reports as soon as they are ready and even have the reports printed before the branches open and still have the same security benefits of a more expensive server.

Compatibility

miniFTPServer has been tested with many popular FTP Clients including CuteFTP¹ and WS-FTPpro² as well as PNCI Software's FTP Monitor Client in both SECURED mode(SSL) and UNSECURED mode.

¹CuteFTP is a product of GlobalSCAPE

²WS-FTP Pro is a product of IPSwitch Inc.

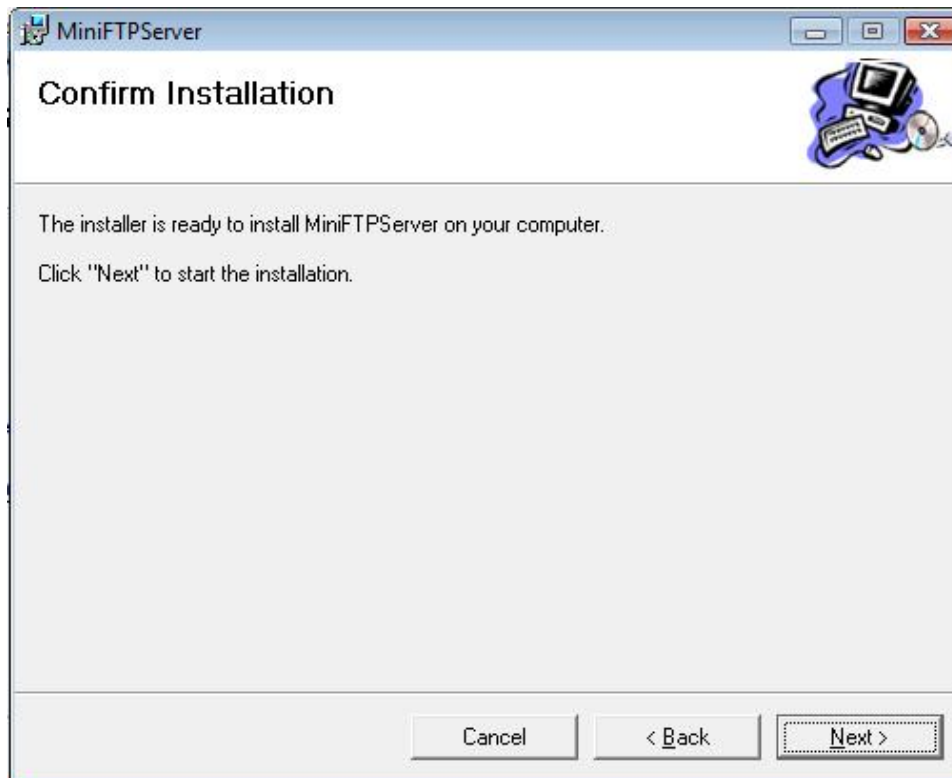
Installation

Installation begins by executing the Setup.exe file. If you are installing this product on a VISTA machine, be sure to execute the Setup.exe and not just the .msi file. Vista requires the Setup file to handle UAC (User Account Control) properly. The form below should appear.



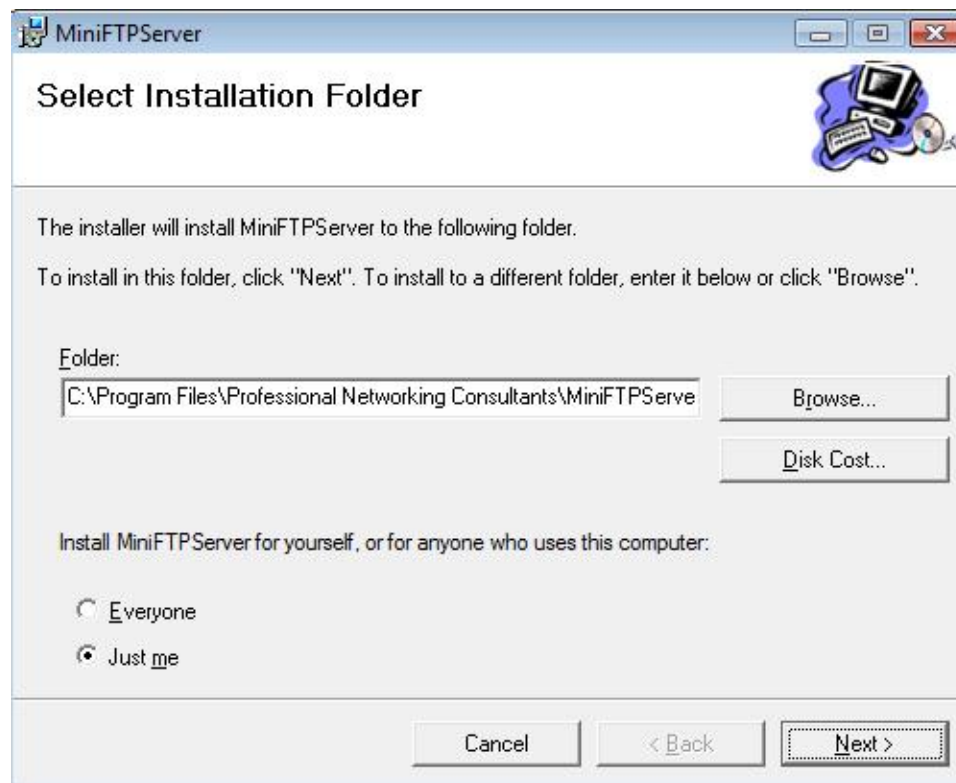
Click the Next> Button to continue with the Installation

At this point you can confirm the installation parameters.



Click the Next > Button to continue.

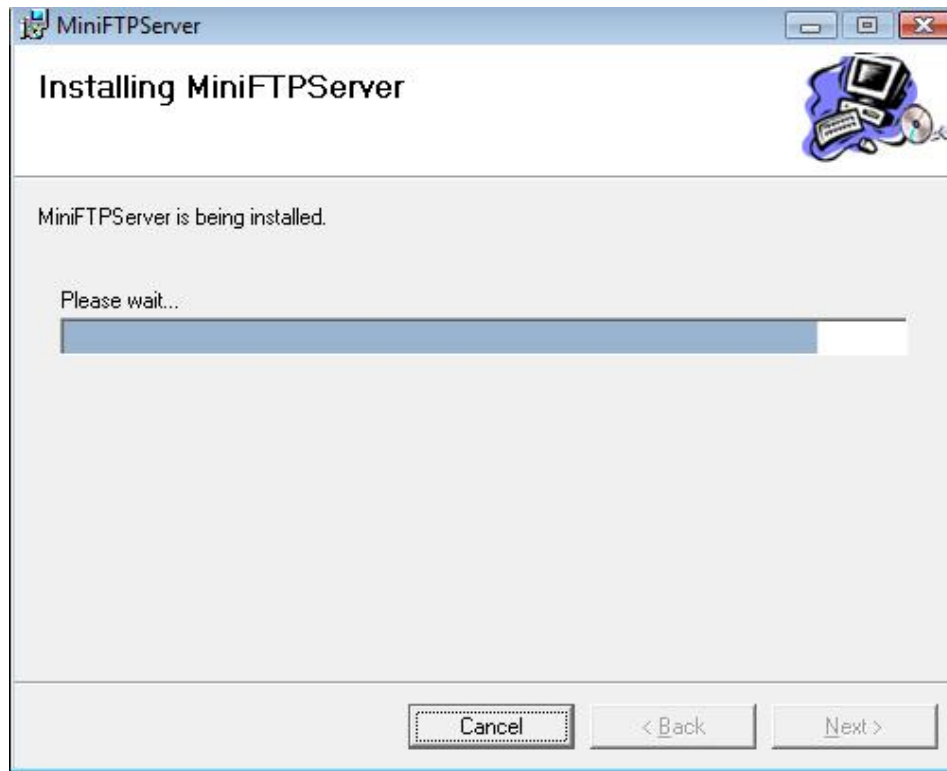
Select the destination folder to install the software to.



Although miniFTPServer runs as a service, the configuration and activation utilities run as foreground tasks, thus select “Just me” .

Click the Next > button to continue.

The installer will begin loading the program files and a progress dialog like the one below will be displayed.

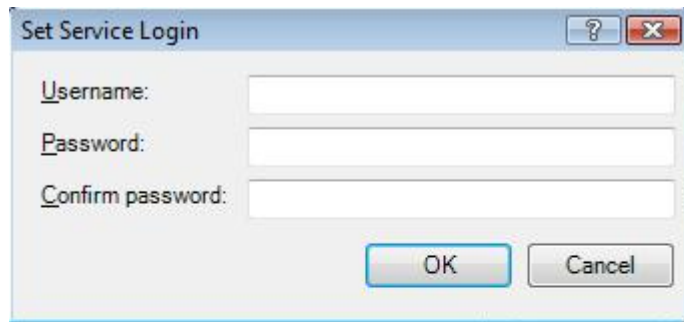


During the final phase of installation, you will be requested to specify the User name and password that the miniFTPServer Service will run under.

NOTE:

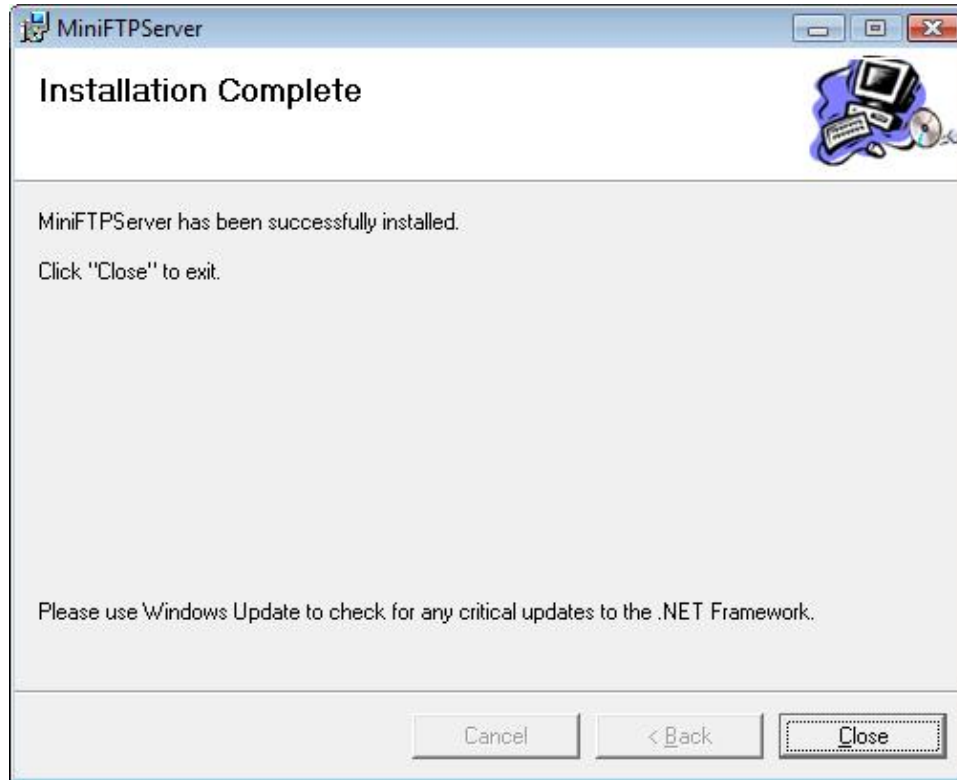
This should be the account you are currently running under now, otherwise miniFTPServer will not be able to find the Certificate you specify if you are running in secured mode.

Also specify the local machine name in the usercode field.
(i.e. LENSVISTA\LSMITH) LSMITH should be the account you are running the installation under now and should have administrator rights.



The image shows a Windows-style dialog box titled "Set Service Login". It contains three text input fields: "Username:", "Password:", and "Confirm password:". Below the fields are two buttons: "OK" and "Cancel". The dialog box has a standard Windows window border with a question mark icon and a close button (X) in the top right corner.

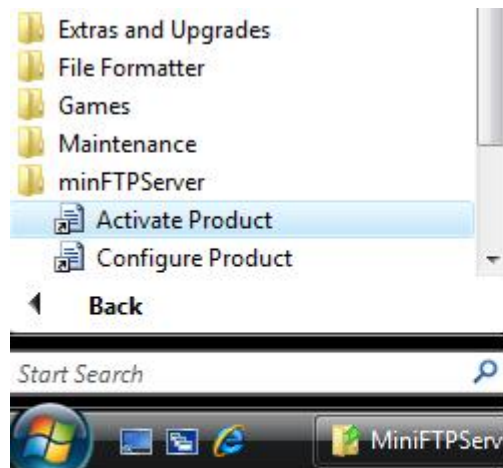
The installation is now complete, you are ready to move on to the Activation stage.



Click the Close Button

Activation

From the program files menu, Select miniFTPServer>ActivationWizard.



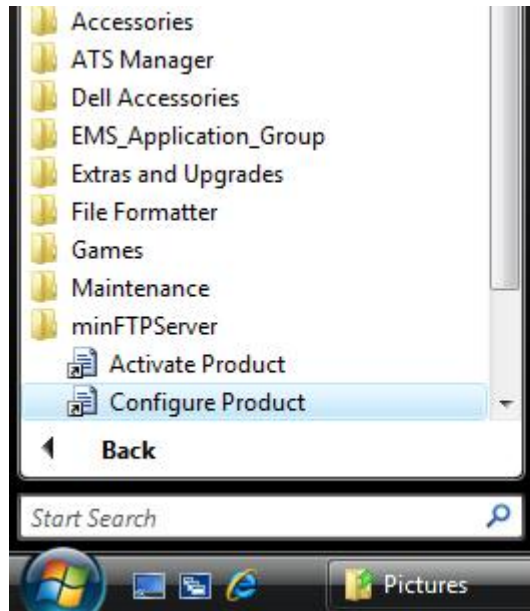
Follow the step by step prompts to either activate a trial or purchase.

If you purchased this product a Confirmation Number should have been emailed to you. Enter, the confirmation when prompted.

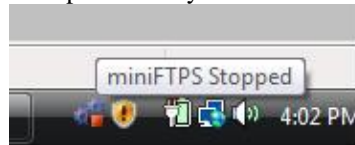
NOTE: Make sure you are running this program on the machine you wish to Activate. If the machine that you wish to activate does not have internet access, the activation wizard will return a machine specific string you can email to LICENSES@BLUESMOKESOFTWARE.COM from another machine that does have access to the internet. Be sure to include your confirmation string if you are requesting a purchase key.

Configuration

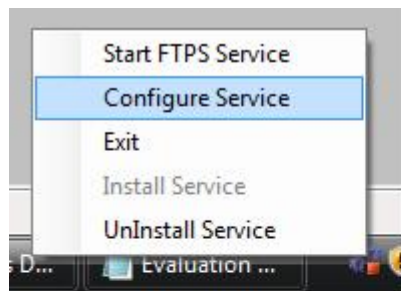
From the Program Files Menu, select miniFTPServer > Configure Product.



A two-gear red box icon should appear in the System Tray. When you move the mouse over it, the tooltip should say “miniFTPS Stopped”



Right click on the Icon and select “Configure Service” from the pop-up menu.



miniFTPServer

The Main configuration dialog will appear.

The screenshot shows the 'Server Configuration' dialog box. It is divided into several sections:

- Mode:** Two radio buttons are present: 'Un-Secured' (unselected) and 'Secured (SSL)' (selected).
- Port Number:** A text box containing '990'.
- Max Idle Time(minutes):** A text box containing '10'.
- System Name:** A text box containing 'Big Bopper'.
- Status Response:** A text box containing 'Ready'.
- Root Directory:** A text box containing 'c:\miniftpservs' with a browse button (>).
- Log Directory:** A text box containing 'c:\logs' with a browse button (>).
- Welcome Message:** A text box containing 'Welcome to PNC's FTP Server'.
- Quit Message:** A text box containing 'Good Byte!'.
- Secure Mode Options:** A section containing:
 - Authentication Level:** A dropdown menu set to 'Explicit Normal (Default)'. A checkbox for 'Require Client Certificate' is present and unchecked.
 - Server Certificate:** A dropdown menu set to 'SN=303a00003039 - Issuer=Professional-Networking'. Below it are three unchecked checkboxes: 'Ignore Untrusted Root', 'Ignore Invalid Date', and 'Ignore Invalid Signature'.
- Client Signon:** A section containing:
 - User Code:** A text box containing 'DEMO'.
 - Password:** A text box containing '****'.
 - Two checkboxes: 'Allow Restarts' (unchecked) and 'Only Run Service When I am Logged On' (checked).

At the bottom right, there are 'OK' and 'Cancel' buttons.

MODE

Unsecured – behaves like a standard FTP server.
Secured- uses SSL protocol.

Authentication Level

Constant	Description
None	No encryption is used.
SecureData	The data is encrypted with SSL.
ImplicitControl	The control connection is always encrypted with SSL.
ImplicitNormal	The maximum security setting.
ExplicitControl	The control connection is encrypted with SSL after an initial login.
ExplicitNormal	Everything is encrypted after the certificate is sent. This is used by many vendors including CuteFTP and WS_FTP pro.(This is the Default)
HashLogin	Encrypts and salts the password, using 256-bit AES to ensure stronger protection over a clear connection..
FirewallReady	Enables Secure FTP communications over a Firewall. This will only work in conjunction with PNC's FTP Monitor pairing.
ExplicitAutoControl	Explicit is used if possible; otherwise no encryption is used on the control connection.

Require Client Certificate

If this option is checked the Client is required to send a certificate to the server for authentication.

Ignore Untrusted Root

This option is used in conjunction with Require Client Certificate. It will tell the server to allow the use of the client certificate if the issuing authority can not be verified. (Useful if using a test certificate)

Ignore Invalid Date

This option is used in conjunction with Require Client Certificate. It will tell the server to allow the use of the client certificate if the Certificate is out of date. (Useful if using a test certificates)

Ignore Invalid Signature

This option is used in conjunction with Require Client Certificate. It will tell the server to allow the use of the client certificate even if the Certificate has not been properly signed. (Useful if using a test certificates)

Server Certificate

This control will display all certificates in the current logged on user's store. Remember the service should be running under the same user code in order for it to see the same certificates. Select the certificate that the service should use during authentication process.

Port Number

Specifies the port that the miniFTPServer Service will be listening on.

Max Idle Time

Specifies the amount of time a connection can remain idle (in Minutes) before the Server disconnects it.

System Name

The system Name that is returned to a client SYST command.

Status Response

The response that is returned to a client STAT command.

Root Directory

The root directory represents the lowest level a remote user attached to miniFTPServer can traverse to. This Directory represents a CWD of "/" to the remote user.

Log Directory

All client actions are recorded to a log file. This specifies the directory where the log files are kept. The user is responsible for periodic maintenance of this directory.

Client Usercode

This is the Usercode the client signs on with. (USER command)

Client Password

This is the Password the Client signs on with (PASS command)

Allow Restarts

With this option selected, if a transfer is interrupted the client can specify a REStart.

Only Run Service when I am Logged On.

With this option selected the service will automatically start when the user signs on and will stop when the user signs off.

Note:

If you would like the service running all the time, from the control panel select administrative tools >services > miniFTPS. And change the startup to automatic. This should be done only after configuration is complete.

Welcome Message

This message is returned when the client first signs on.

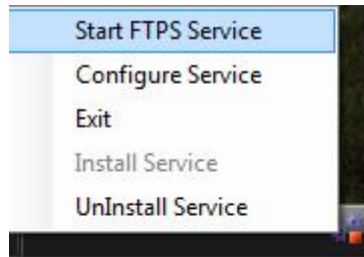
Quit Message

This message is returned to the client when the session is terminated (QUIT).

Press the OK button to save the newly selected options.

Starting The Service

The service now ready to be started. Right click on Icon and select “Start Service From PopUp Menu”



The service should go Running. And the Icon should change to a green box as illustrated below.



In Case of Difficulty

Service Fails to Start

If the service fails to start, check the application Log for a possible explanation.

Most common reasons are the Trial Key expired or the Service can not find the Certificate.

Clients Can not Connect

If the service starts but clients fail to connect, make sure the firewall is allowing incoming connects on the port number specified in the configuration. By default Windows Vista and Server 2003 along with many other firewalls either Software or Hardware firewalls disable most ports.

Clients Connect but then Disconnect

If the Client connects but then disconnects, Usually this is caused by a mismatch of authentication levels between the Client and Server. These must match.

Also verify the client is using the correct usercode and password.

Making Changes to an existing Configuration

If the service is currently running, Stop the Service (Right click, Select Stop Service)
Then Right Click select Configure Service make changes using configure dialog as described above.

Save changes and Right Click and Select Start Service. Changes will only take effect after the service is stopped and restarted.

Supported Client Commands

USER	PASS	CWD	CDUP	SMNT	QUIT
REIN	PORT	PASV	TYPE	STRU	MODE
RETR	STOR	STOU	APPE	ALLO	REST
RNFR	RNTO	ABOR	DELE	RMD	MKD
PWD	LIST	NLST	SITE	SYST	STAT
HELP	NOOP	SIZE			

