2012

Cerberus, LLC

Grant Averett

[CERBERUS FTP SERVER 5.0]

User manual for Cerberus FTP Server 5.0. It contains detailed steps and help on configuring Cerberus FTP Server.

CONTENTS

INTRODUCTION

DESCRIPTION

Cerberus FTP Server provides a secure and reliable file transfer solution for the demanding IT professional or the casual file sharer. Supporting SFTP, FTP/S, and HTTP/S, Cerberus is able to authenticate against Active Directory and LDAP, run as a Windows service, has native x64 support, includes a robust set of integrity and security features and offers an easy-to-use manager for controlling user access to files and file operations.

GUIDE

For additional help and troubleshooting information, take a look at the Cerberus FTP Server FAQ.

You can also access the most recent help documentation online.

MINIMUM SYSTEM REQUIREMENTS

This section describes the minimum hardware and software requirements to install and run Cerberus FTP Server.

HARDWARE REQUIREMENTS

- Pentium class processor (1 GHz or better recommended)
- 256 MB RAM
- XGA or higher-resolution monitor

OPERATING SYSTEMS

CERBERUS FTP SERVER 2.5 AND HIGHER

- Windows 2000 Professional and Server SP4
- Windows XP SP3
- Windows 2003 Server and R2
- Windows Vista SP2
- Windows 7 SP2
- Windows 2008 Server and R2

CERBERUS FTP SERVER 5.0 AND HIGHER

- Windows XP SP3
- Windows 2003 Server and R2
- Windows Vista SP2
- Windows 7 SP2
- Windows 2008 Server and R2

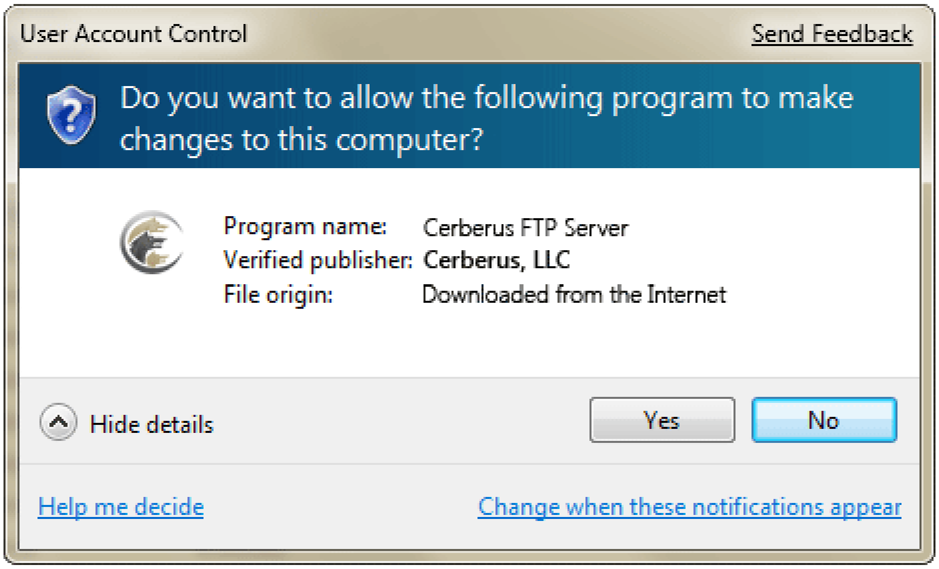
The latest Service Packs for your operating system are **highly** recommended.

INSTALLATION

Close all other programs (recommended) before installing Cerberus FTP Server and make sure that you install it logged in as Administrator or a member of the Administrators group if you are installing it on a Windows NT or higher system.

1. Download the latest version of Cerberus FTP Server from http://www.cerberusftp.com/files/CerberusInstall.exe

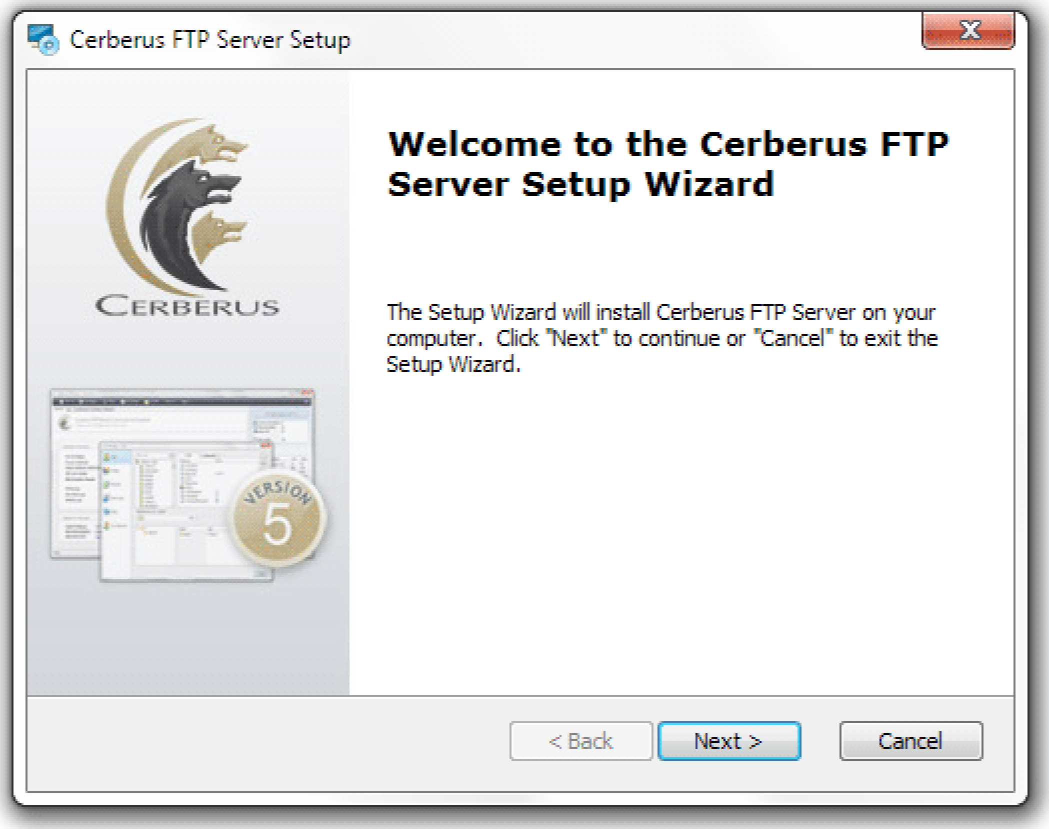
2. Double click or run the **CerberusInstall.exe** self-extracting installer. You may be prompted "Do you want to allow the following program to make changes to this computer" click **Yes** (or **Allow**). Clicking **Yes** will give the Cerberus FTP Server Installer Administrator privileges to install (required on most operating systems).



Do you want to allow the following program to make changes to this computer?

Program name: Cerberus FTP Server
Verified publisher: Cerberus, LLC
File origin: Downloaded from the Internet

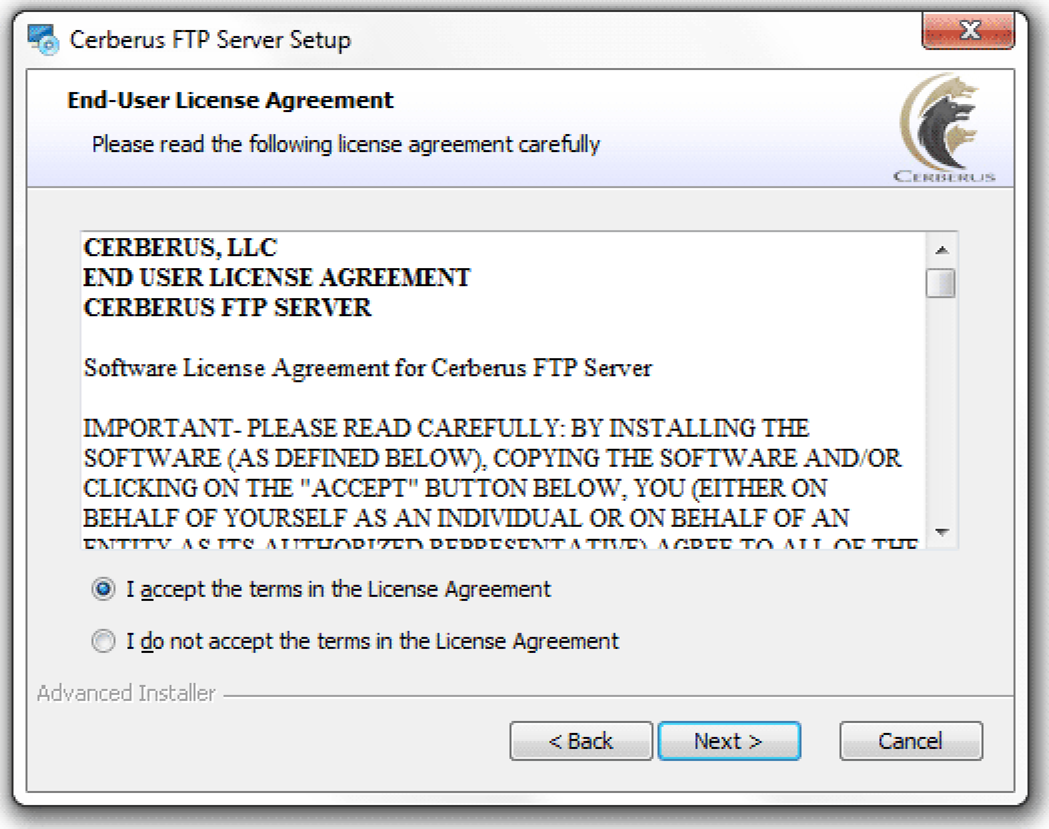
3. You will see the "Welcome to the Cerberus FTP Server Setup" screen. Click **Next**.



Welcome to the Cerberus FTP Server Setup Wizard

The Setup Wizard will install Cerberus FTP Server on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

4. Agree to the licensing agreement to continue. Select the "**I accept the terms in the License Agreement**" button and click **Next**.



Cerberus FTP Server Setup

End-User License Agreement

Please read the following license agreement carefully

CERBERUS, LLC
END USER LICENSE AGREEMENT
CERBERUS FTP SERVER

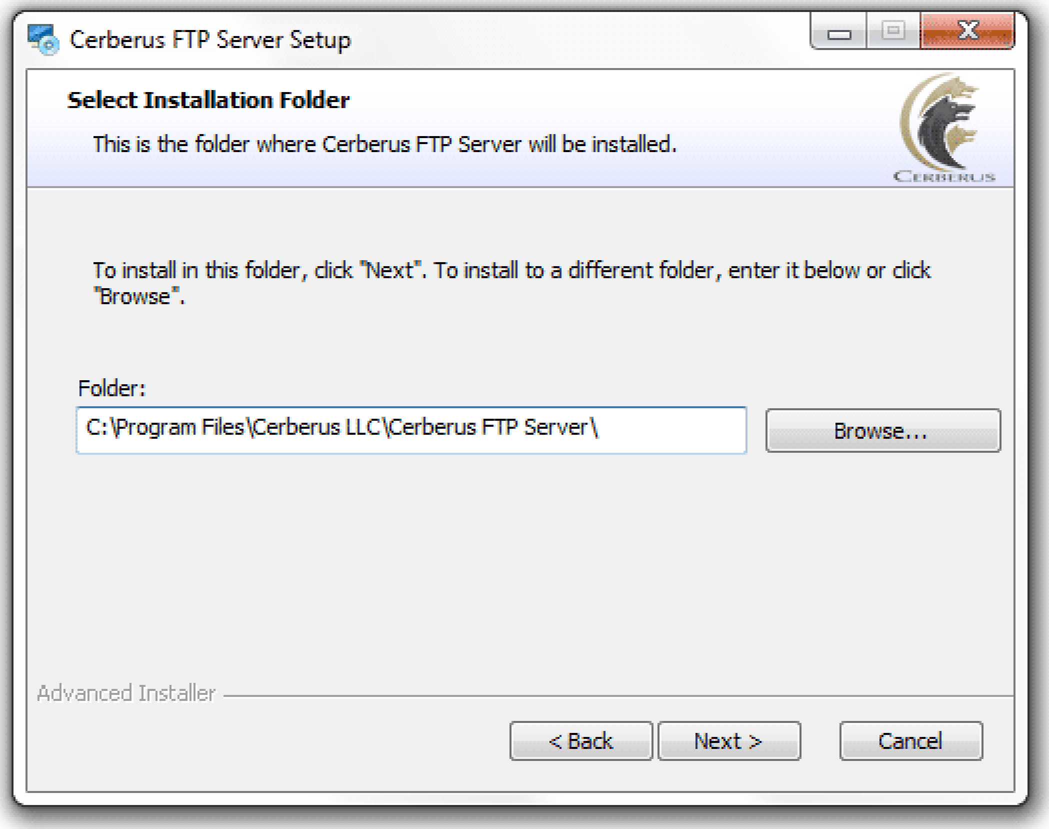
Software License Agreement for Cerberus FTP Server

IMPORTANT- PLEASE READ CAREFULLY: BY INSTALLING THE SOFTWARE (AS DEFINED BELOW), COPYING THE SOFTWARE AND/OR CLICKING ON THE "ACCEPT" BUTTON BELOW, YOU (EITHER ON BEHALF OF YOURSELF AS AN INDIVIDUAL OR ON BEHALF OF AN ENTITY AS ITS AUTHORIZED REPRESENTATIVE) AGREE TO ALL OF THE

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

5. Select an installation folder. Or keep the default path. Click **Next**.



Cerberus FTP Server Setup

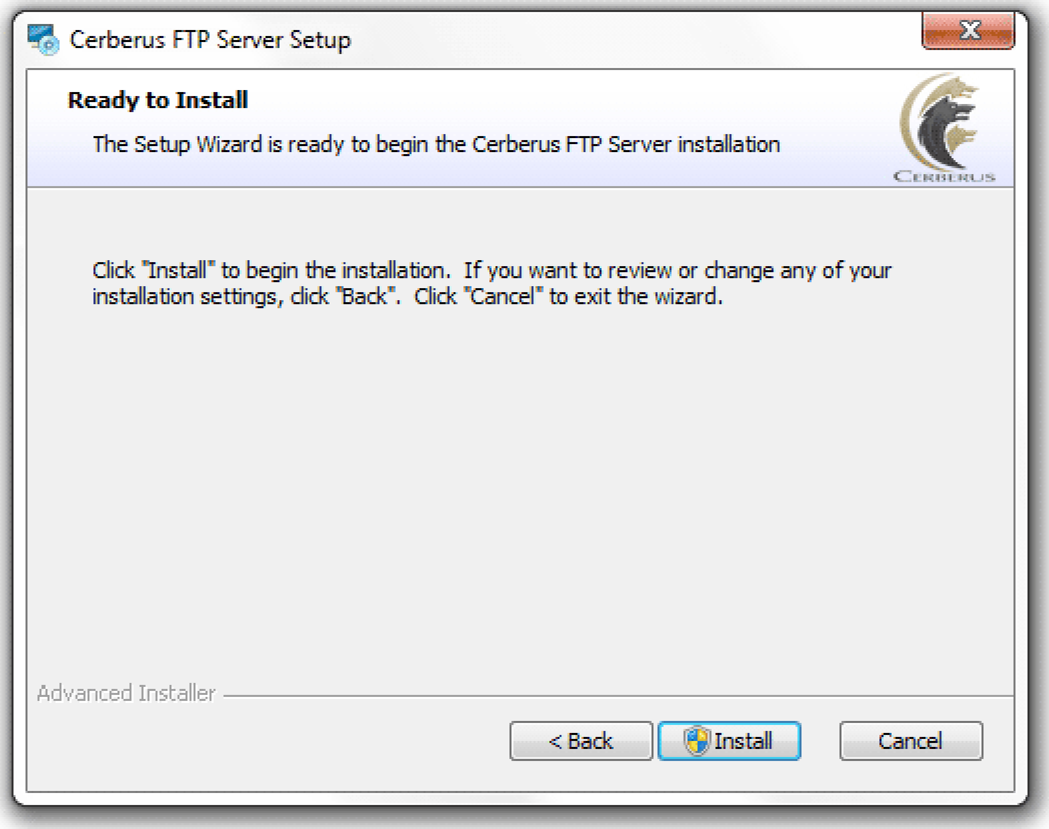
Select Installation Folder

This is the folder where Cerberus FTP Server will be installed.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\Cerberus LLC\Cerberus FTP Server\

6. Confirm your settings and click **Install** to begin installation.



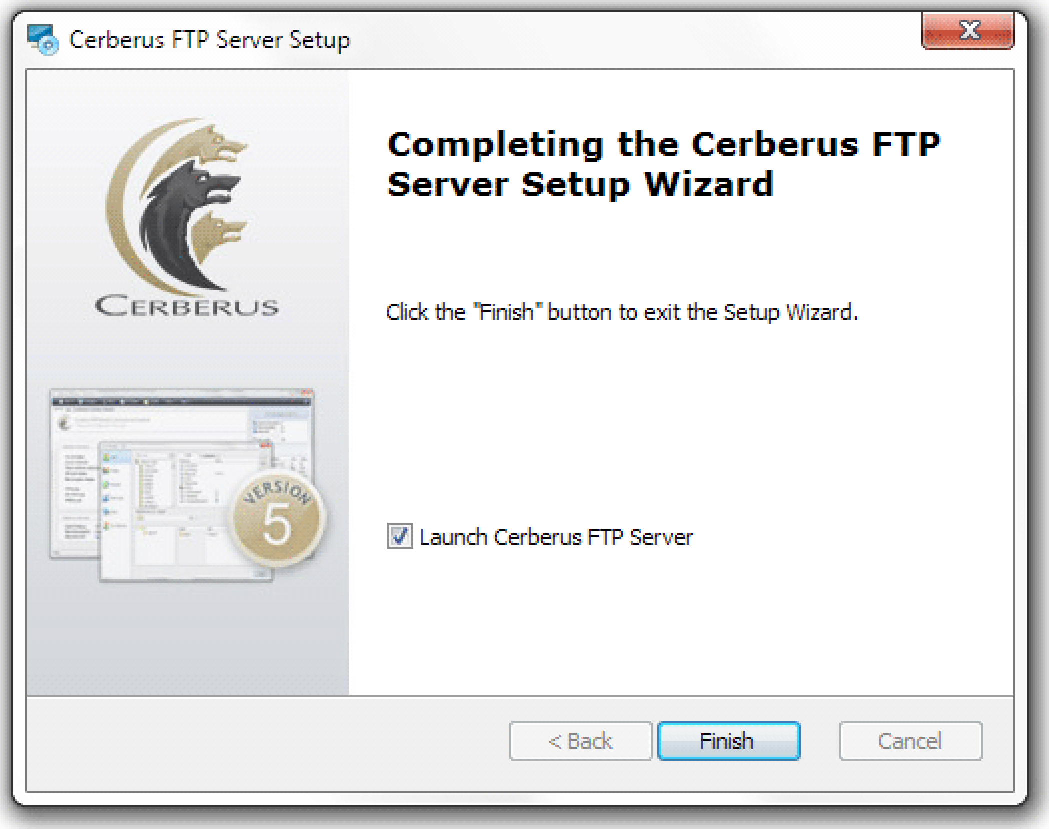
Cerberus FTP Server Setup

Ready to Install

The Setup Wizard is ready to begin the Cerberus FTP Server installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

7. Click **Finish**.



Cerberus FTP Server Setup

Completing the Cerberus FTP Server Setup Wizard

Click the "Finish" button to exit the Setup Wizard.

☑ Launch Cerberus FTP Server

GETTING STARTED - INITIAL SETUP WIZARD

THE WIZARD

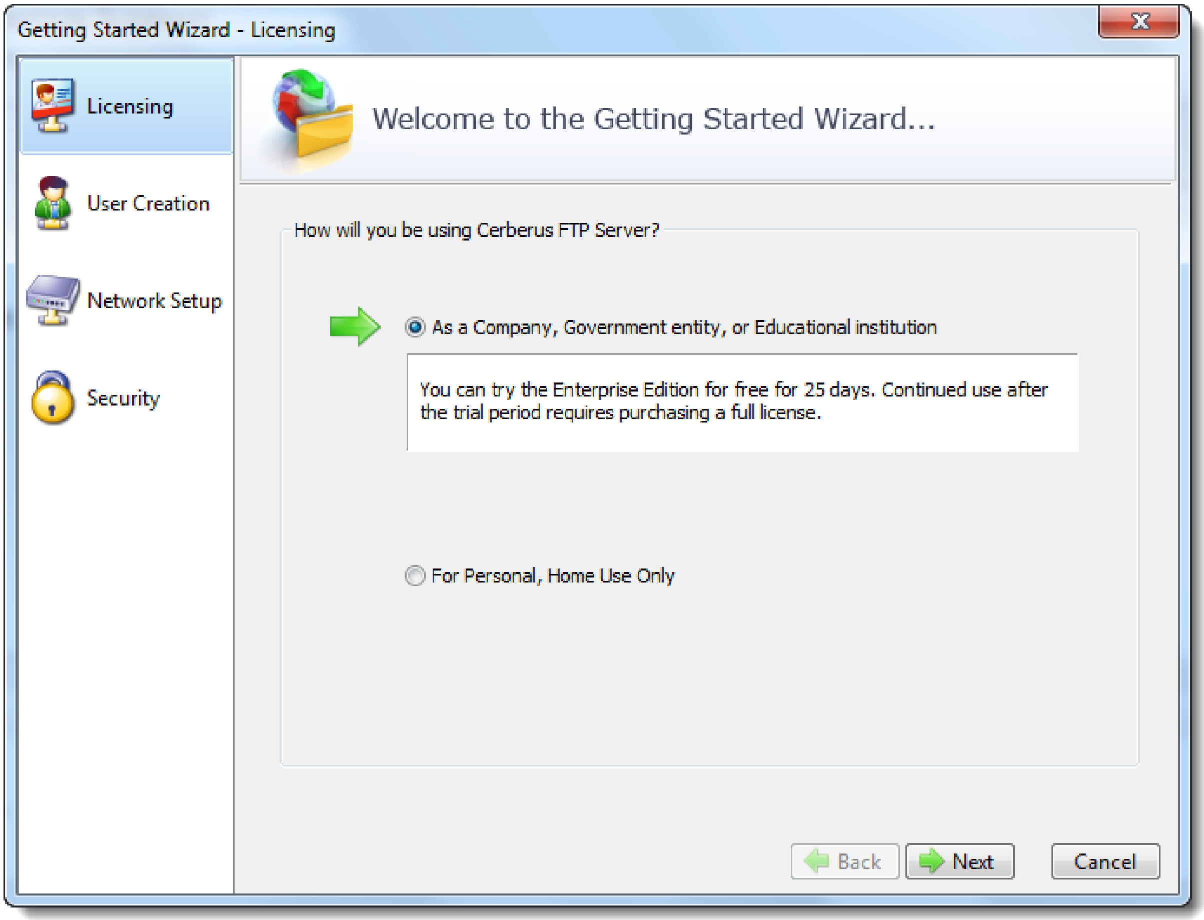
The Getting Started Wizard will appear when you start Cerberus FTP Server for the first time. The wizard is designed to walk you through the basic steps of configuring the server to allow clients to connect. At the end of the Getting Started Wizard your server should be ready to accept connections from FTP, FTPS, SSH SFTP, and HTTP clients.

STEP 1 - LICENSING

The Licensing page allows the administrator to select the licensing option most appropriate for their intended use of Cerberus FTP Server.

- Selecting "**As a Company, Government entity, or Educational institution**" enables a 25 day trial period of the Enterprise edition of Cerberus FTP Server. During the trial period, the server will perform and function as the Enterprise edition. Cerberus FTP Server reverts to the Home edition after the evaluation period expires and a message indicating that the server is unregistered will be added to the server welcome message for each connection. At any time, including after the trial period has expired or even if "For Personal Use" was selected at startup, Cerberus may be turned into the full commercial Personal, Standard, Professional, or Enterprise edition by entering a valid registration code into the license dialog.

- Selecting the "**For Personal, Home Use Only**" option immediately causes Cerberus to function as the Home edition. This license is only permitted for at home, personal use of the FTP server. The Home edition is limited to at most 5 simultaneous FTP or FTPS connections. A message indicating that the server is Cerberus FTP Server Home edition will also appear in the FTP welcome message whenever a client connects to the server. In all other respects, Cerberus FTP Server Home edition is functionally equivalent to the licensed Personal edition.



Welcome to the Getting Started Wizard...

How will you be using Cerberus FTP Server?

● As a Company, Government entity, or Educational institution

You can try the Enterprise Edition for free for 25 days. Continued use after the trial period requires purchasing a full license.

○ For Personal, Home Use Only

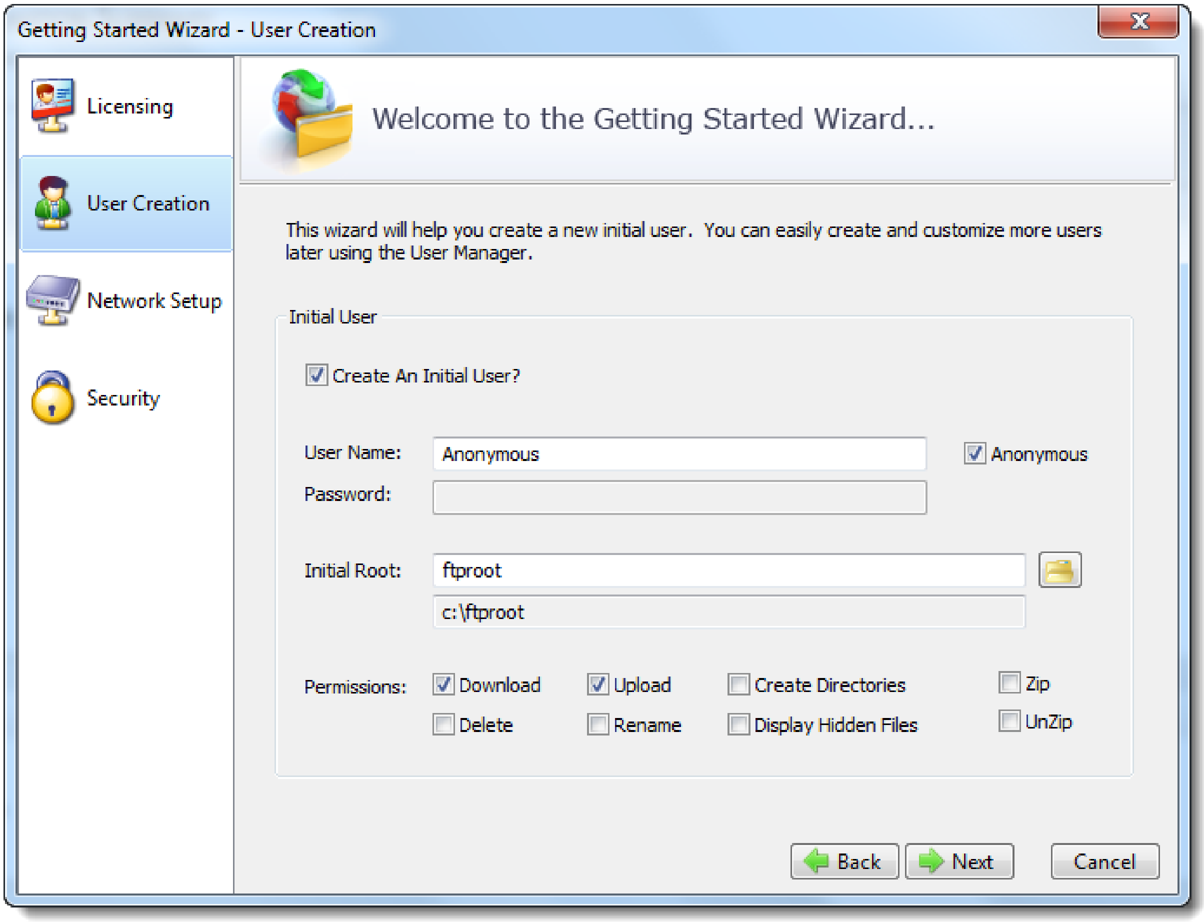
Figure 1 Licensing Page of the Getting Started Wizard

STEP 2 - INITIAL USER CREATION

The User Creation page will allow you to automatically create a simple user account with access to a directory on the local machine. You can use this account to test out your initial connection to the server. You can turn off the creation of the user account by un-checking the "Create an Initial User?" checkbox.

By default, an anonymous user will be created under the User Manager. The default anonymous user will have download and upload-only access to the "C:\ftproot" directory as their root drive. This directory will be created if it does not already exist. Please note, the default settings for the anonymous user allow anyone to connect to your FTP server without specifying a password. Using the default settings, anyone can view and download any file from your "C:\ftproot" directory and any subdirectories of that directory. To disallow anonymous access to Cerberus FTP Server, uncheck the "Create Initial user" box and the anonymous user will not be added.

You can further customize the newly added user, or create and manage additional users, through the User Manager after the "Getting Started" wizard has finished.



Welcome to the Getting Started Wizard...

This wizard will help you create a new initial user. You can easily create and customize more users later using the User Manager.

Initial User

☑ Create An Initial User?

User Name: Anonymous ☑ Anonymous

Password:

Initial Root: ftproot

c:\ftproot

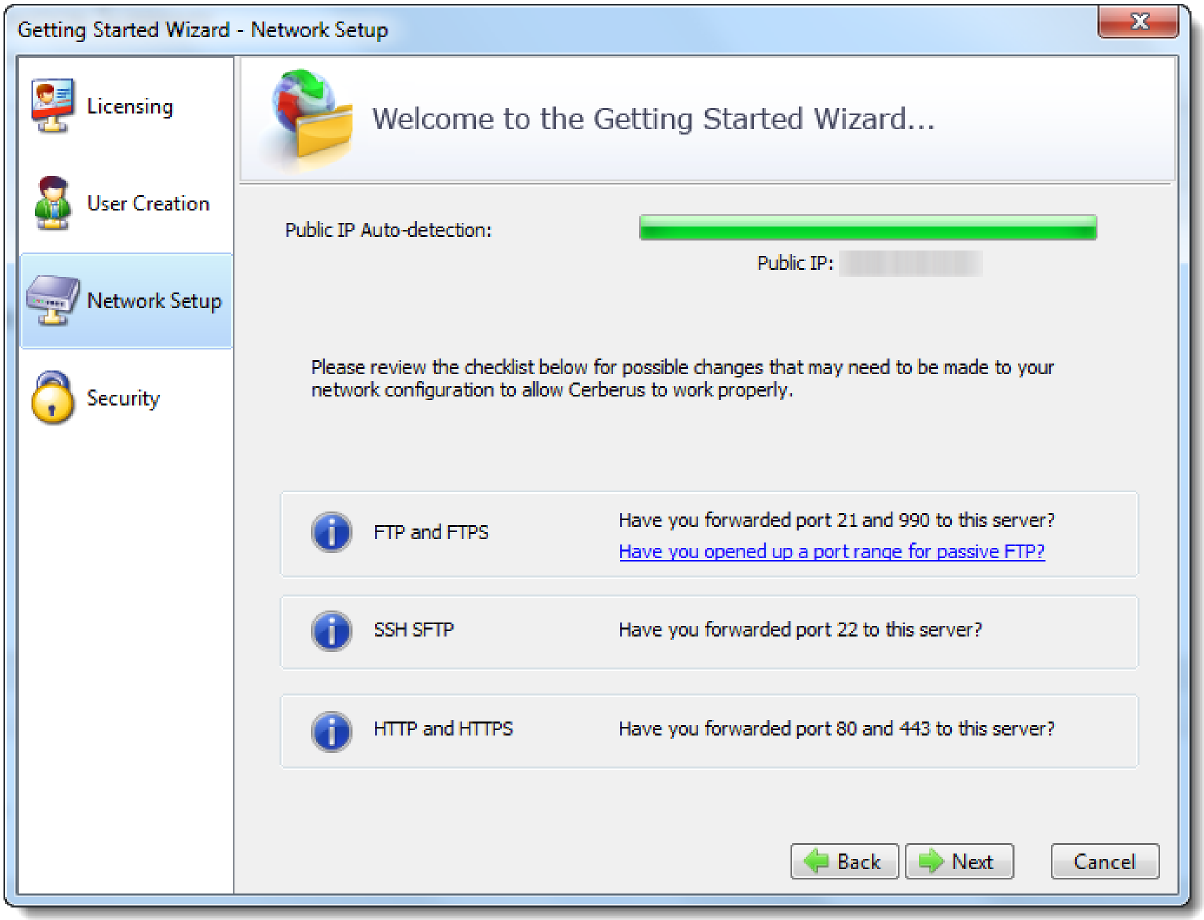
Permissions: ☑ Download ☑ Upload □ Create Directories □ Zip

□ Delete □ Rename □ Display Hidden Files □ UnZip

Figure 2 Initial User Creation

STEP 3 - NETWORK SETUP

The Network Setup screen detects basic network settings and tries to provide advice on any settings changes that need to be made because of the computer's network configuration.



Welcome to the Getting Started Wizard...

Public IP Auto-detection:

Public IP: [redacted]

Please review the checklist below for possible changes that may need to be made to your network configuration to allow Cerberus to work properly.

FTP and FTPS — Have you forwarded port 21 and 990 to this server? Have you opened up a port range for passive FTP?

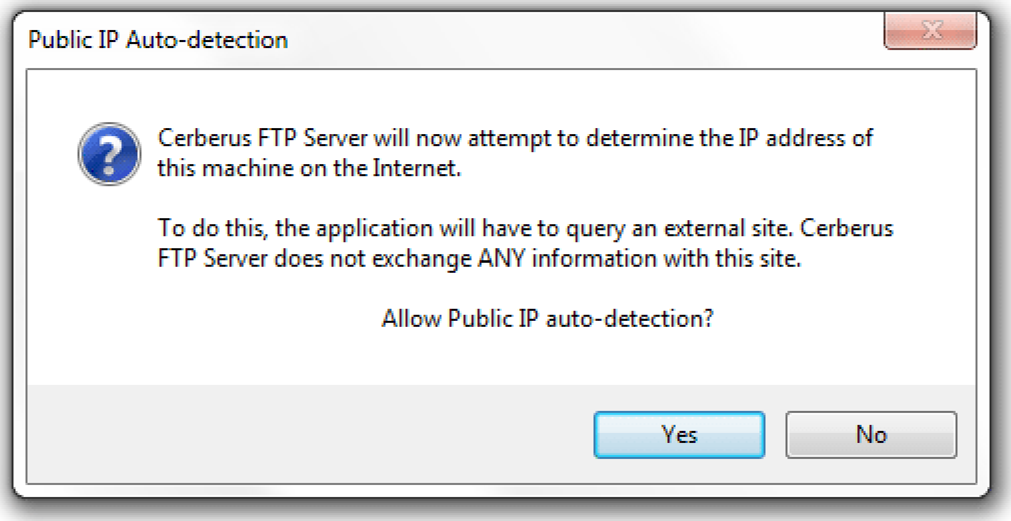
SSH SFTP — Have you forwarded port 22 to this server?

HTTP and HTTPS — Have you forwarded port 80 and 443 to this server?

Figure 3 Network Setup Checklist

PUBLIC IP AUTO-DETECTION FOR PASSIVE MODE FTP

The most complex task in configuring basic FTP access to your server is preparing the machine to accept FTP data connections. Unlike the SSH SFTP or HTTP/S protocols, FTP is complicated by the need for two connections for each client session. The first connection is established when the client initially connects and is used to exchange commands and status between the FTP server and the client. A second connection is created every time a directory listing or file transfer takes place. Whenever a directory listing or file transfer is requested, the FTP server has to respond with an IP address and port that the client can connect over to establish the secondary data connection. To aid the server in determining what IP address to give to the client, the server can be configured to automatically detect the IP address of the server on the Internet and use this IP address when sending the client connection instructions.



Public IP Auto-detection

Cerberus FTP Server will now attempt to determine the IP address of this machine on the Internet.

To do this, the application will have to query an external site. Cerberus FTP Server does not exchange ANY information with this site.

Allow Public IP auto-detection?

Figure 4 Public IP Auto-detection

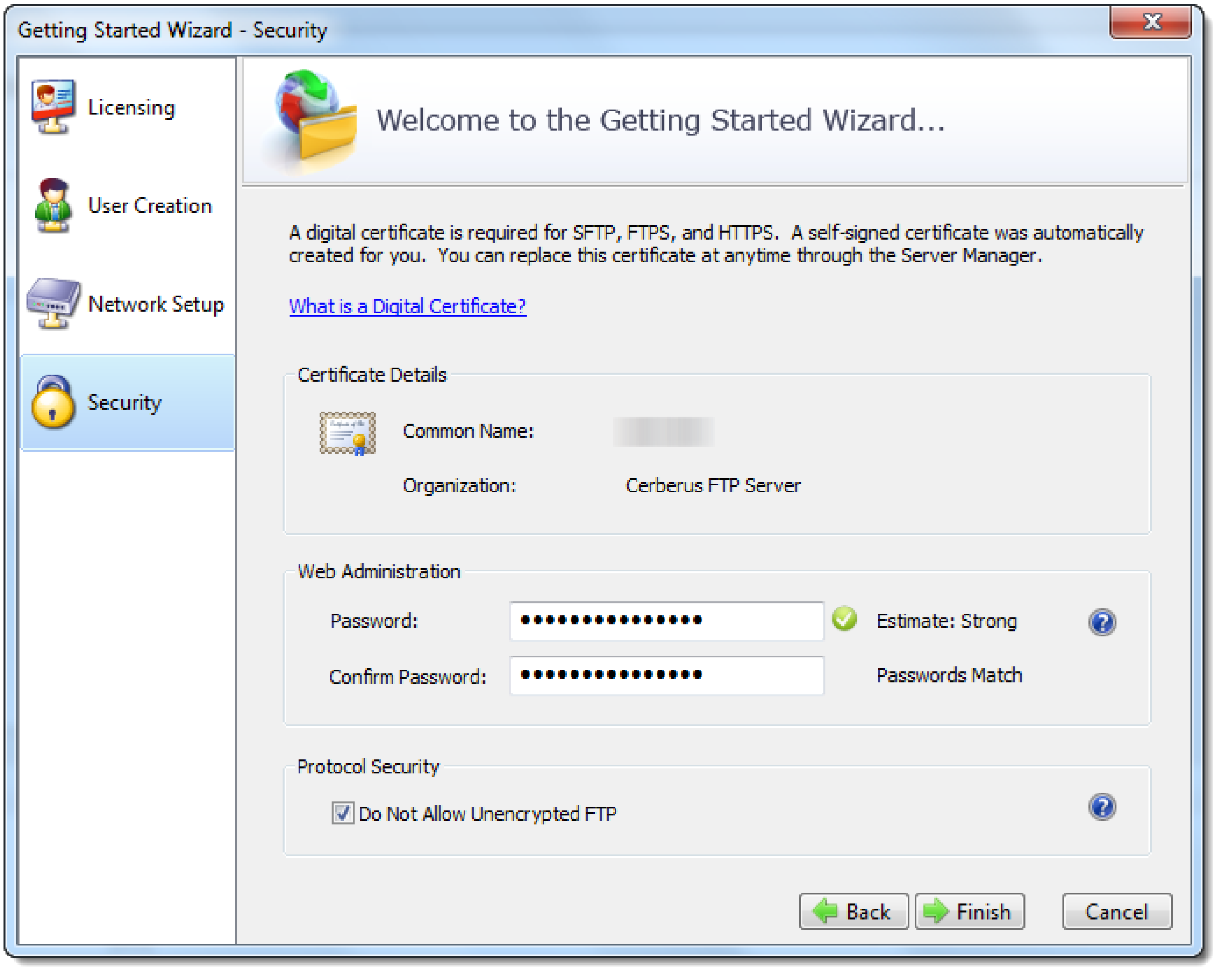
After clicking the Next button on the Network Setup page a dialog prompt will ask whether you want to allow Cerberus to automatically attempt to detect your public IP address. We normally recommend you answer "**Yes**" here. Answering yes will instruct Cerberus to automatically attempt to detect and use the correct external IP address when clients request passive FTP data connections.

STEP 4 – SECURITY

The last page of the Getting Started Wizard will allow the administrator to configure a few basic server security settings.

Cerberus FTP Server fully supports TLSv1/SSLv3 encryption over FTP (FTPS), HTTPS, and SSH SFTP. To enable FTPS, HTTPS, and SSH SFTP support, a digital certificate must be generated for the server. This digital certificate contains the necessary security data to allow the server to establish encrypted connections with clients.

Cerberus FTP Server will automatically generate a new, self-signed certificate for you the first time you run the Getting Started Wizard. You can replace the certificate at any time through the Security page of the Server Manager.



Getting Started Wizard - Security
Licensing
User Creation
Network Setup
Security
Welcome to the Getting Started Wizard...
Back
Finish
Cancel

A digital certificate is required for SFTP, FTPS, and HTTPS. A self-signed certificate was automatically created for you. You can replace this certificate at anytime through the Server Manager.

What is a Digital Certificate?

Certificate Details

Common Name: [redacted]

Organization: Cerberus FTP Server

Web Administration

Password: ••••••••••••••• Estimate: Strong

Confirm Password: ••••••••••••••• Passwords Match

Protocol Security

☑ Do Not Allow Unencrypted FTP

Figure 5 Security page of the Getting Started Wizard

WEB ADMINISTRATION PASSWORD

You also have the option to configure a web administration and remote API access password on the Security Wizard page. You should set a strong password here even if you are not using web administration. Please note that the password strength estimation meter is only meant as a guide. It will flag obviously poor passwords but there is no official weighting system and this meter should only be utilized as a loose guide to improving your password.

PROTOCOL SECURITY

The last option allows you to configure the server to only accept encrypted FTP connections. Normal FTP has no encryption and therefore allows passwords and data to be transmitted unencrypted over a network.

Fortunately, it is possible to establish a normal unencrypted FTP connection and then "upgrade" the connection to secure encryption through special FTP commands (this enhanced protocol is called FTPES). This type of connection depends on the client issuing FTP commands instructing the server to establish encryption before accepting login credentials. However, the client can also continue as a normal FTP connection without enabling encryption. This situation allows for unencrypted connections and presents a security issue for servers.

If you wish to allow FTPES secure connections, but not FTP, then you must instruct the server to require encryption before allowing a connection to proceed.

Checking this option does exactly that. It requires the client upgrade the connection to use encryption before allowing login.

FINAL STEPS

Click the Finish button to complete the Getting Started Wizard. Your server is now ready to accept local network FTP/S, SSH SFTP, or HTTP/S web client connections. Please take a look at the next section for any changes that might need to be made to your firewall or router to allow connection from outside of your local network to reach your server.

GETTING STARTED - NETWORK SETUP

BASIC SETUP SO USERS CAN CONNECT FROM THE INTERNET

FTP connections within your local network usually work without any problems. However, when you want the FTP server to be available outside of your local network, additional steps are often necessary to make the server visible to the outside world. The following steps are usually required to allow Cerberus FTP Server to be accessed from the Internet:

STEP 1 - CONTROL CONNECTION

The control connection port Cerberus FTP Server is listening on needs to be forwarded from your router to the machine hosting Cerberus. The default port that Cerberus listens on is port 21. Consult your router documentation for instructions on how to setup port forwarding. Finishing this step will allow Internet users to establish a connection with your server. The next step is making sure **passive mode** is configured so that directory listings and file transfers work.

STEP 2 - PASSIVE MODE

To allow passive mode to work properly, you must forward the passive range of ports from your router to the machine running Cerberus. See "My IP address begins with 192.168.xxx.xxx. Is there anything special I have to do for people to see my FTP Server on the Internet?" for detailed instructions on how to make sure passive mode is setup properly. If you don't perform this step, users may be able to login but directory listings may hang and timeout.

STEP 3 - FIREWALL

Make sure any firewalls you are running are allowing connections on port 21. Cerberus will automatically attempt to add itself to the Windows Firewall Exception list (you will be prompted to allow this). However, you may still have to manually add an exception to allow port 21 connections into your computer.

ALLOWING EXTERNAL ACCESS TO YOUR SERVER

Depending upon your connection to the Internet, you may need to configure your router or firewall before users outside of your local network can see your FTP server. Communication with an FTP server is done through two connections, a control connection, and a data connection. Ensuring these connections can be established are the two areas where special attention is usually needed.

THE CONTROL CONNECTION

The control connection is always the first connection established with an FTP server. The control connection's purpose is to allow clients to connect and to send commands to the server (and receive server responses). Port **21** is considered the default control connection port, and this is the default port that Cerberus FTP Server will configure your IP interfaces to listen on for new connections. Using the default port is not mandatory - the administrator is free to change the interface to use any free port on the system as the listening port. However, if the administrator is running a software-based firewall, the administrator must be certain that [incoming] connections are not blocked on the port chosen for the control connection. If the port that Cerberus is listening on is blocked, no one will be able to see or connect to the FTP server.

THE DATA CONNECTION

The second type of connection is called the data connection. This is the connection that an FTP server uses to exchange file listings and transfer files on. When an FTP client uses the control connection to instruct Cerberus FTP Server to send a file listing or transfer a file, the actual data exchange takes place on the data connection. The data connection is usually where most of the confusion and problems arise for FTP server administrators.

There are two different ways a data connection can be established between an FTP client and an FTP server. The first is commonly called **active** FTP. In this mode, an FTP client sends the IP address and port that the client is currently listening for data connections on to the FTP server. The client accomplishes this by sending the server a *PORT* command over the control connection. Using the address and port from the *PORT* command, the FTP Server then connects to the client and sends the file or file listing. When using **active** FTP, the administrator has to make sure that port 20 on the machine that Cerberus FTP Server is running on is open for outgoing connections. The reason for this is because when using **active** FTP, the server always establishes connections from port 20. Most firewalls allow outgoing connections automatically, so manually opening up port 20 for outgoing connections is usually not necessary.

The other way to establish a data connection between client and server is to use **passive** FTP. **Passive** mode was introduced to get around common problems with client firewalls. Instead of the FTP server connecting to the FTP client, the client connects to the FTP server using a port previously communicated using the *PASV* command. When a client issues the *PASV* command, the FTP server responds with a port that the server is currently listening on for data communication. Problems occur with **passive** FTP when the firewall that Cerberus FTP Server is running on is blocking the selected ports. To get around this problem, the administrator is required to open up the range of ports that Cerberus has reserved for **passive** FTP connections. You can configure what range of ports Cerberus FTP Sever uses for **passive** FTP mode by looking under the 'Advanced' tab of the Server manager.

Failures during LIST, NLST, MLST, RETR, or STOR operations can usually be attributed to problems with the data connection.

COMMON NETWORK CONFIGURATIONS

A PC running Cerberus FTP Server with access to the Internet often fits into one of two configurations:

CONFIGURATION 1: YOUR COMPUTER IS CONNECTED DIRECTLY TO THE INTERNET

This is the simplest network configuration you can have and usually requires little or no configuration to Cerberus FTP Server to allow full access. This configuration is most common with dial-up, DSL, cable modem, and other broadband users. However, machines connected to the Internet directly often employ a software firewall to provide some protection against unwanted intrusion attempts. While some firewall software can automatically detect an FTP server and properly configure itself, the administrator usually has to manually configure the firewall. See the explanation above about the control and data connection for common ports that have to be allowed through a firewall.

CONFIGURATION 2: YOUR COMPUTER IS CONNECTED TO A ROUTER, AND THE ROUTER IS CONNECTED TO THE INTERNET

Routers usually act as firewalls, so the same problems that can occur in Configuration 1 can occur here. Follow the advice in Configuration 1 to resolve firewall problems.

In addition to the firewall problems that can occur in this network configuration, there is now the problem that the IP address you are using on your machine is not the IP address that the Internet sees for your machine. Other users on the Internet usually see your router's IP address instead of your PC's private address. Routers are devices on your network, just like your PC, and they have their own IP address, and that is the IP address the router tells other computers is your address when you go out on the Internet. When a user attempts to connect to the FTP server, they need to use the Internet-facing IP address of the router (the router is where the connection is really happening), not the private address of the computer Cerberus FTP Server is running on. When the router receives the connection attempt it is then able to forwarded the connection to your computer.

The first thing to check in this configuration is that your router is sending all of the FTP traffic to the computer Cerberus FTP Server is running on. Most routers have a web-based configuration utility that you can use to configure **Port Forwarding**. Specifically, you will want to make sure you forward the control and possible data connection ports to the computer running Cerberus FTP Server.

There is one more problem that crops up in this network configuration. To properly allow **passive** transfer mode, the administrator will have to make sure Cerberus is giving out the router address in response to PASV requests. You can automatically enable this by making sure "WAN IP Auto detection" is enabled in the 'General' tab of the Server Manager. Alternately, you can enter the IP address of the router manually for each interface in the "Use different IP for PASV mode" IP box under the Server manager's 'Interfaces' tab.

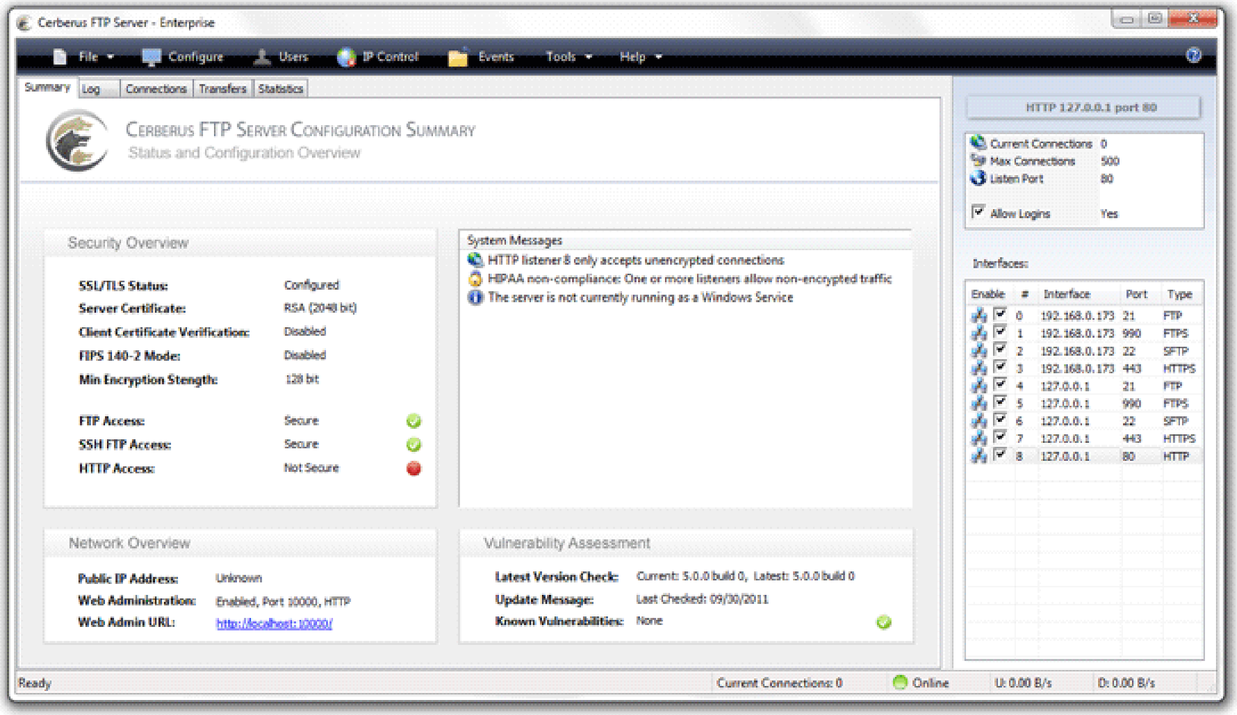
While more complicated network configurations are possible, most users will fall into one of the above configurations.

THE SUMMARY VIEW

UNDERSTANDING THE SUMMARY VIEW

Available in Cerberus FTP Server 5.0, the Summary View provides the administrator with a one page overview of the server's configuration and any potential security issues that may be present.

The server scans the current Cerberus configuration at startup, and every time a configuration change is made, to look for any potential security issues that might result from the current system configuration. System warnings and messages are displayed in the **System Messages** list and each protocol type is given an overall security status indicator.



SSL/TLS Status: Configured
Server Certificate: RSA (2048 bit)
Client Certificate Verification: Disabled
FIPS 140-2 Mode: Disabled
Min Encryption Stength: 128 bit

FTP Access: Secure ✓
SSH FTP Access: Secure ✓
HTTP Access: Not Secure ●

HTTP listener 8 only accepts unencrypted connections
HIPAA non-compliance: One or more listeners allow non-encrypted traffic
The server is not currently running as a Windows Service

Public IP Address: Unknown
Web Administration: Enabled, Port 10000, HTTP
Web Admin URL: http://localhost:10000/

Latest Version Check: Current: 5.0.0 build 0, Latest: 5.0.0 build 0
Update Message: Last Checked: 09/30/2011
Known Vulnerabilities: None ✓

Current Connections 0
Max Connections 500
Listen Port 80

☑ Allow Logins Yes

Enable	#	Interface	Port	Type
☑	0	192.168.0.173	21	FTP
☑	1	192.168.0.173	990	FTPS
☑	2	192.168.0.173	22	SFTP
☑	3	192.168.0.173	443	HTTPS
☑	4	127.0.0.1	21	FTP
☑	5	127.0.0.1	990	FTPS
☑	6	127.0.0.1	22	SFTP
☑	7	127.0.0.1	443	HTTPS
☑	8	127.0.0.1	80	HTTP

Ready   Current Connections: 0   Online   U: 0.00 B/s   D: 0.00 B/s

Figure 6 - The Cerberus FTP Server Summary View

The possible status for each protocol type is:

Secure	All listeners currently active for this protocol type are configured to accept only encrypted connections.
Not Secure	Some or all listeners currently active for this protocol type are configured to allow unencrypted connections.
Disabled	There are no listeners currently active on the server for this protocol.

COMMON SYSTEM MESSAGES

There are generally two types of system messages displayed in the System Messages list - general messages and security messages.

Anytime a protocol is listed as **Not Secure** there will be a system security message detailing the reason. Common system messages, their explanation and resolution, if applicable, are detailed below.

- ***FTP Listener X can allow unencrypted control or data connections***

  Background: Normal FTP has no encryption and therefore allows passwords and data to be transmitted in the clear over a network. To address this security issue, two secure forms of FTP were developed called implicit FTPS and explicit FTPES. Implicit FTPS is very similar to HTTPS and takes place on a completely separate port from typical FTP. Interfaces of this type are always encrypted and considered secure. Explicit FTPES, however, starts on a normal unencrypted FTP connection and is then "upgraded" to a secure connection through special FTP commands. This type of connection depends on the client issuing commands instructing the server to enable encryption. However, the client can also continue as a normal FTP connection without enabling encryption. This situation allows for unencrypted connections and presents a security issue for servers.

  Resolution: To resolve this issue and still allow FTP access there are two possible solutions. One is to remove all FTP listeners and only enable FTPS listeners. FTPS listeners only accept encrypted communications and are considered secure.

  If you wish to also allow FTPES secure connections then you must instruct the server to require encryption before allowing a connection to proceed. To require the FTP listener to require encryption, go to the Interfaces page of the Server Manager and for **each** FTP interface, select the **Require Secure Control** and **Require Secure Data** options.

- ***HTTP Listener X only accepts unencrypted connections***

  Background: Connections of type HTTP are always unencrypted and are therefore very susceptible to inspection on a network. System administrators are encouraged to disable HTTP listeners in favor of secure HTTPS listeners.

  Resolution: To resolve this issue the system administrator must disable any HTTP listeners in the system. HTTPS listeners will not trigger a security issue.

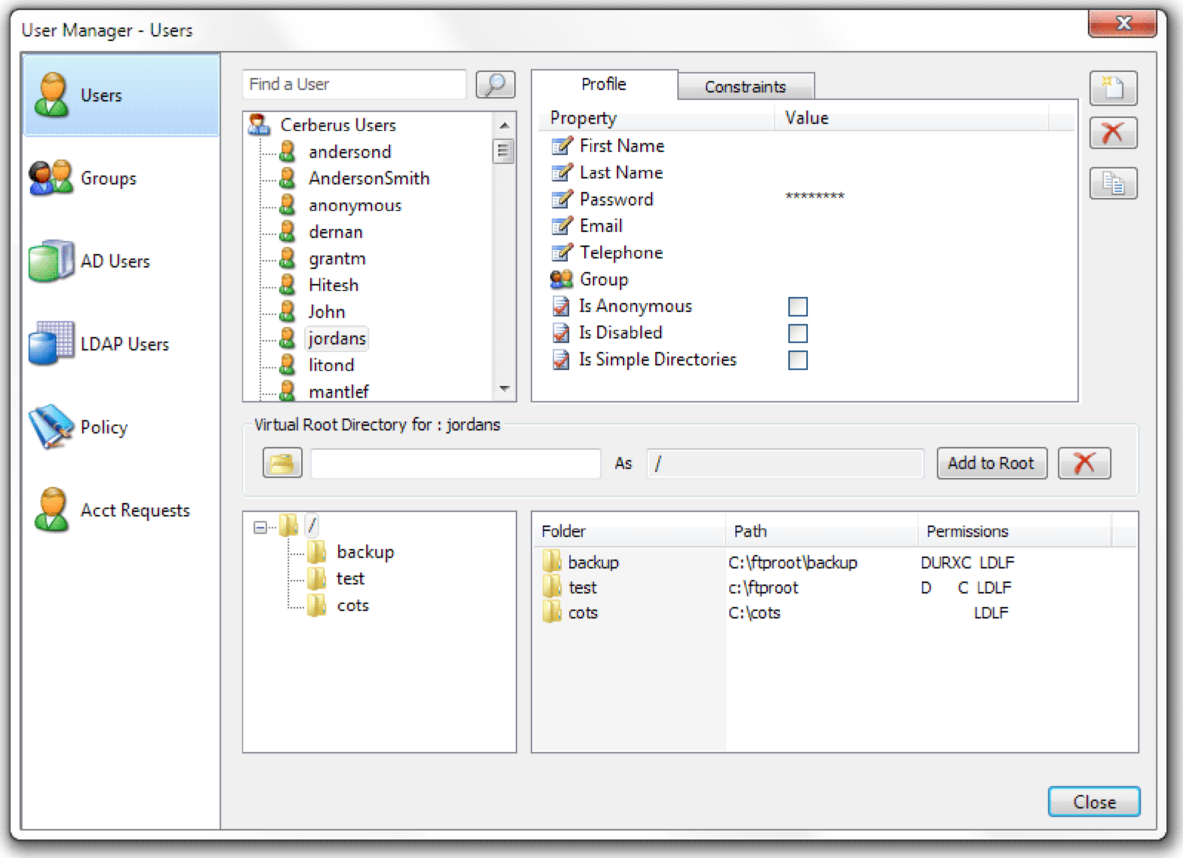
THE USER MANAGER

ABOUT CERBERUS FTP SERVER AUTHENTICATION

Cerberus FTP Server can manage user accounts from three different sources. The first is the default Cerberus FTP Server user database. The Cerberus default user database is displayed in the User List box on the General page of the User Manager. The accounts within the default database are users created just for Cerberus FTP Server. The directions on this page are for adding a user to this default database.

You may also use Cerberus FTP Server to authenticate Active Directory users when the machine hosting Cerberus is part of a domain (or the local NT account database), even if the computer Cerberus FTP Server is installed on is not the domain controller. See the page Active Directory Authentication for more information on how to configure Cerberus to allow authentication of Active Directory domain users.

Finally, users can also be authenticated against an LDAP service. See the section on configuring Cerberus for LDAP authentication for more information.



Cerberus Users
- andersond
- AndersonSmith
- anonymous
- dernan
- grantm
- Hitesh
- John
- jordans
- litond
- mantlef

Property	Value
First Name	
Last Name	
Password	********
Email	
Telephone	
Group	
Is Anonymous	□
Is Disabled	□
Is Simple Directories	□

Virtual Root Directory for : jordans

As /

/
- backup
- test
- cots

Folder	Path	Permissions
backup	C:\ftproot\backup	DURXC LDLF
test	c:\ftproot	D C LDLF
cots	C:\cots	LDLF

Figure 7 - The Cerberus FTP Server User Manager- Users page

NOTE: Active Directory and LDAP authentication are only available in the Professional and Enterprise editions of Cerberus FTP Server.

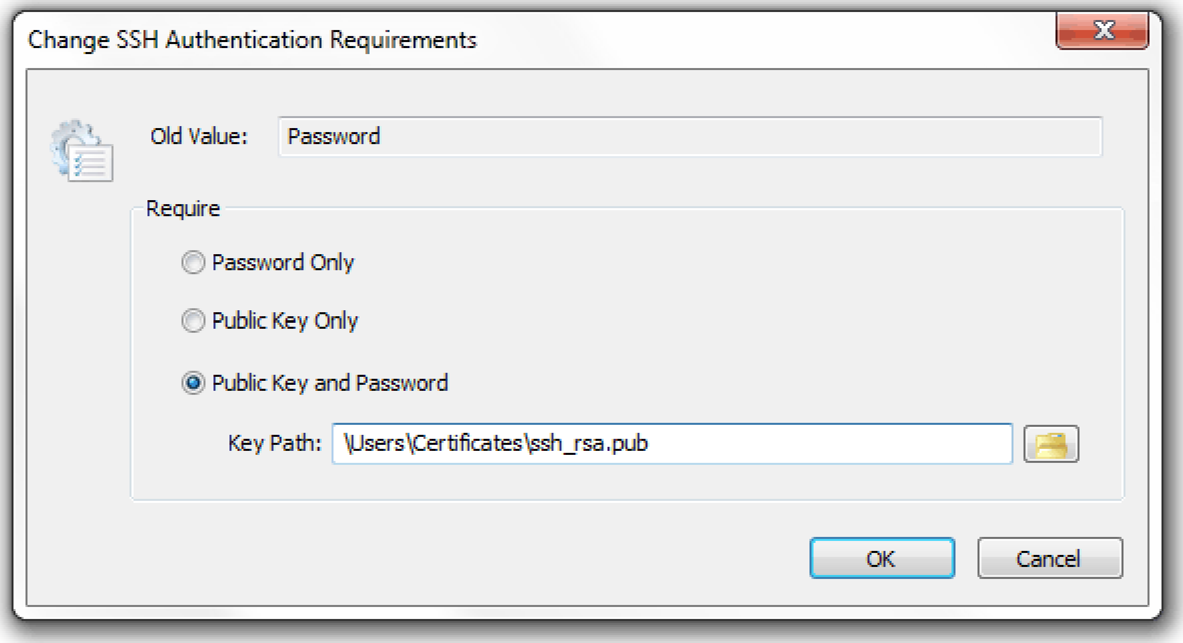
ADDING A NEW USER

Users can be added and modified in the Cerberus FTP Server user database by opening up the **User Manager** and selecting the **Users** tab. To add a user, select the **New** button from the button group along the right side of the page. A new user will appear under the user list box. The newly created user will already be in rename mode, so simply type in the new name of the user. All user names must be unique and are case insensitive. Once you have entered the new user name, press enter to commit the change. The user can then be configured by clicking on the user's name in the user list box.

A list of configurable properties for that user will appear in the list box to the right of the user. Those properties are:

Password	The password for the user. **Note**: The Password always displays as 7 (*) characters.
Group	A Cerberus FTP Server Group that this user belongs to.
Is Anonymous	If checked, the user password is ignored and the user can be logged in using any password.
Is Simple Directories	In simple directory mode the administrator can only assign one directory to represent the virtual directory for a user. See below for an explanation of this setting.
Is Disabled	Determines whether the account can login or not. A disabled account cannot login into the server.
Simultaneous Logins	The maximum number of connections this user can make to the server at the same time.
Require Secure Control	(Applies to FTP only) If enabled, this user can only login to the server using a secure TLS/SSL encrypted connection.
Require Secure Data	(Applies to FTP only) If enabled, file transfers will only be allowed over secure TLS/SSL encrypted connections.

Disable After Date	If a date is set here then the account will become disabled after the date specified. **Note**: The granularity of the timer is 30 minutes. The account will be disabled within 30 minutes of the time set.
Allow Protocols to Login	Controls which protocols a user is allowed to login with. If a protocol is not checked then the user will not be allowed to login using that protocol.
SSH Authentication	Determines the authentication requirements for logging into an SFTP interface. Valid options are: - **Password Only**: Require only a password for authentication. - **Public Key Only**: Require only a valid public key for authentication - **Public Key and Password**: Require both a valid public key and a valid password for authenticating a user



Change SSH Authentication Requirements

Old Value: Password

Require

○ Password Only

○ Public Key Only

● Public Key and Password

Key Path: \Users\Certificates\ssh_rsa.pub

Figure 8 The SSH Authentication Method dialog under the User Manager

CONFIGURING A USER FOR SSH PUBLIC KEY AUTHENTICATION

The procedure for configuring a user for SSH Public Key Authentication in Cerberus FTP Server is:

1. Open the Cerberus FTP Server **User Manager**. The default page is the **Users** tab.

2. Select the User from the **Cerberus User Accounts** list that you wish to configure for Public Key Authentication.
3. Double-click on the **SSH Authentication Method** property for the selected user. The **Change SSH Authentication Requirements** dialog will appear.
4. Select the **Public Key Only** or **Public Key and Password** radio option. The **Key Path** edit box and file selection button will become visible/enabled.
5. Select the folder button next the **Key Path** edit box. A file selection dialog box will appear.
6. Select the public key file you wish to use for the selected user. Press **Open** button to select the file.
7. Press **OK** button on the Change **SSH Authentication Requirements** dialog to close and save the new SSH authentication settings.
8. Press the **Close** button on the **User Manager** to save the changes to the selected user.

THE VIRTUAL DIRECTORY SYSTEM

The virtual directory (VD) system allows the administrator to attach any directory or drive to the root. When a client requests the root directory from the server, the VDs you specify are sent to the client. The client can also navigate to any of the VD directories' subdirectories. The VD system takes care of all path translation.

Security settings can be specified for each virtual directory. All subdirectories under the VD inherit the security settings of the VD.

There are 2 modes that a user account can operate in with respect to the virtual file system. The two modes are simple and standard mode.

SIMPLE VIRTUAL DIRECTORY MODE

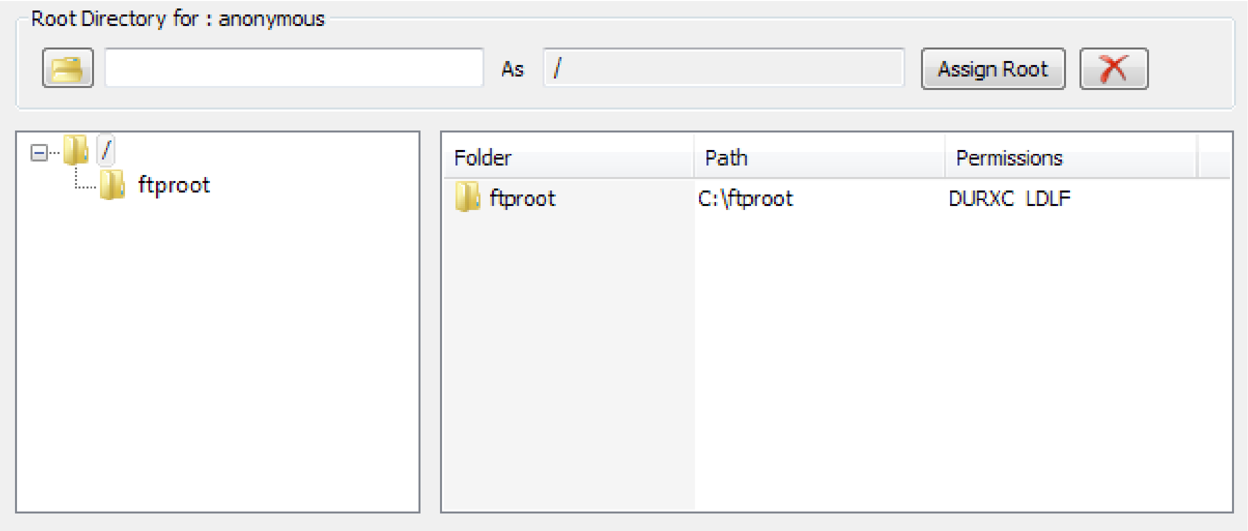
When a user account uses simple directory mode, the administrator can only assign one directory to represent the virtual directory for that user. Instead of that directory being seen as a subdirectory off of the root, the virtual directory selected will be the directory the user is placed in when they first log into the server. In other words, the directory selected as the virtual root directory will be the root directory.

STANDARD VIRTUAL DIRECTORY MODE

In standard mode (the **Simple Directories** option is un-checked), the administrator may add as many directories as virtual directories to a user account as desired. The directories selected will appear as subdirectories off of the root when the designated user logs into the server.

A VIRTUAL DIRECTORY MODE EXAMPLE

Let's take a user with one simple virtual directory called **ftproot** that maps to **C:\ftproot**.



Folder	Path	Permissions
ftproot	C:\ftproot	DURXC LDLF

Figure 9 Virtual Directory Settings for a User

In **Simple Directory** mode, the remote root directory that the user sees, "/", is mapped directly to **C:\ftproot** on the server. The actual virtual directory name is ignored (you can think of it as always being named "/"). The user will see all files and folders in **C:\ftproot** listed in their root directory. They can upload and download files directly into the root directory and they will be uploaded or downloaded to **C:\ftproot** on the server.

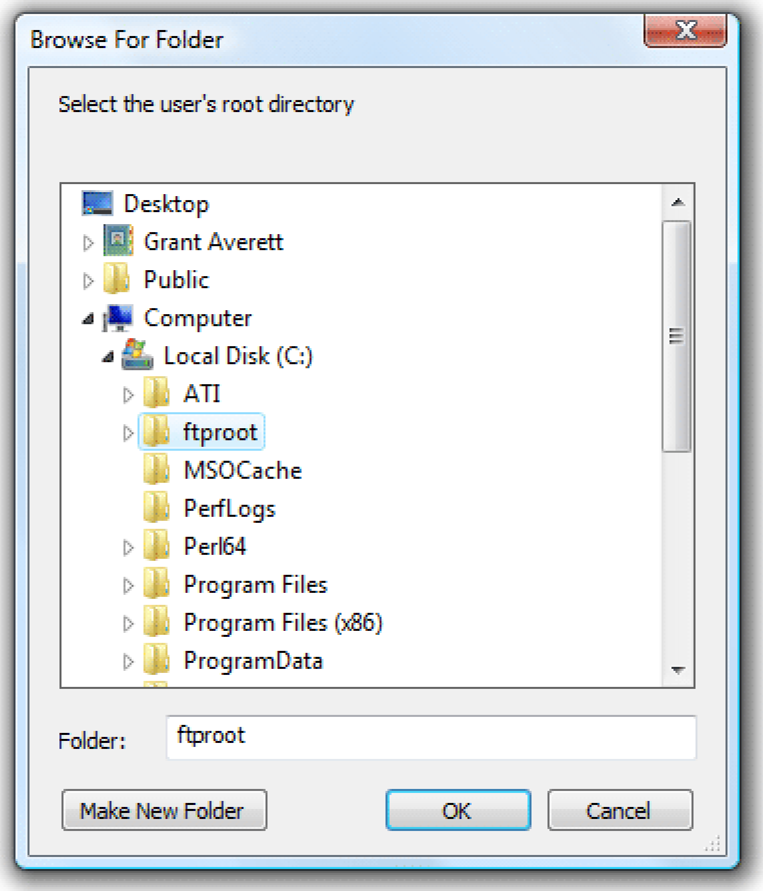
When not in simple directory mode, the root directory "**/**" doesn't map to anything. Instead, the root directory "**/**" becomes a virtual file system that you can attach sub-directories to. When not in simple directory mode, you can add as many virtual directories to a user account as you like and the virtual directory name will become a sub-directory in the virtual root. However, you have to change to that sub-directory before you can upload or download anything. If you try to upload a file to the root folder "**/**" then the operation is invalid because the path "**/**" doesn't map directly to a folder on the server. You would need to specify the path **/ftproot** to upload or download files from the virtual directory **ftproot**.

ADDING A VIRTUAL DIRECTORY TO A USER ACCOUNT

Each user can be assigned different virtual directories. A virtual directory is added to a user account by using the User Manager, pictured above. To add a virtual directory to a user, first:

1. Select the user in the "User List."
2. Next, click on the button labeled "**...**". This button is located below the "User List" list box, in the "Virtual Directory" group. Once you have clicked on the "..." button, a "**Browse for Folder**" dialog will appear.
3. Navigate to the directory you wish to add and press the "**OK**" button on the dialog box. The directory you selected should appear in the edit box to the right of the "**...**" button.
4. Finally, select the "**Add to Root**" (this button will be labeled "**Assign as Root**" in simple mode) button located to the right of the "**...**" button.

   The directory should appear in the "Virtual Root directory" list box. To configure the newly added directory, click on the directory name in the list box. The directory's permission options should appear in the list box to the right of the directory list. Place a check beside any permission that you would like to grant to the virtual directory and all of that directory's subdirectories.



Browse For Folder

Select the user's root directory

Folder: ftproot

Figure 10 Virtual Directory Browse for Files

VIRTUAL DIRECTORY PERMISSIONS

Each virtual directory that you add for a user can have a separate and distinct set of access permissions. The settings applied to a top level virtual directory filter down to all of that root directory's subdirectories.

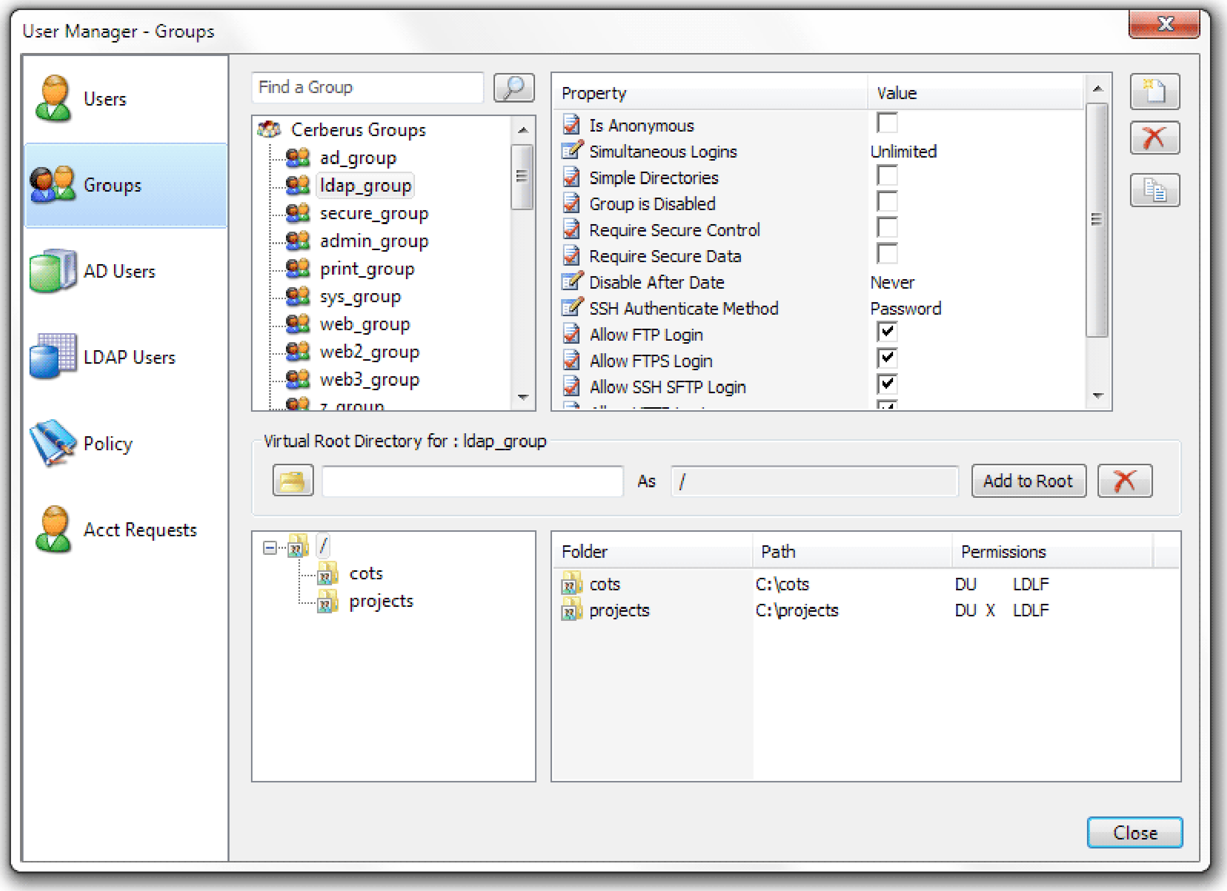
Permissions can only be assigned at the top, root level.

CERBERUS GROUP ACCOUNTS

ABOUT GROUPS

Cerberus FTP Server has supported groups since version 3.0. This simplifies administration by letting you assign permissions once to the group instead of multiple times to each individual user. You can add Virtual Directories and basic user settings to a group and have users inherit those permissions. By default, when a user is assigned a group that group's settings override the default user settings. You will see the user settings grayed out and the actual value displayed for each grayed setting is the value of the group that user belongs to.

The exception is the virtual directory list. The user's virtual directories are a union of the group's virtual directories and any virtual directories you add to the user.



Property	Value
Is Anonymous	☐
Simultaneous Logins	Unlimited
Simple Directories	☐
Group is Disabled	☐
Require Secure Control	☐
Require Secure Data	☐
Disable After Date	Never
SSH Authenticate Method	Password
Allow FTP Login	☑
Allow FTPS Login	☑
Allow SSH SFTP Login	☑

Virtual Root Directory for : ldap_group

As /

/
cots
projects

Folder	Path	Permissions
cots	C:\cots	DU LDLF
projects	C:\projects	DU X LDLF

Figure 11 The Cerberus FTP Server User Manager- Groups page

OVERRIDING GROUP SETTINGS FOR A USER

You can always over-ride the group settings by right-clicking on a user in the User Manager and select the "Override Group" to assign a value different from the group value. From that point on that user setting will be "disconnected" from the group setting. You can revert back to the group setting by right-clicking on the user and selecting "Default to Group".

ADDING A NEW GROUP

A single group can be added and modified in the Cerberus FTP Server database by opening up the User Manager and selecting the **Groups** tab. To add a group, select "New" from the button to the right of the "Cerberus Group Accounts" group box. A new group will appear under the group list box. The newly created group will already be in rename mode, so simply type in the new name of the group. All group names must be unique and are case insensitive. Once you have entered the new group name, press "enter" to commit the change. The group can then be configured by clicking on the group name in the group list box. A list of configurable properties for that group will appear in the list box to the right of the group.

Those properties are:

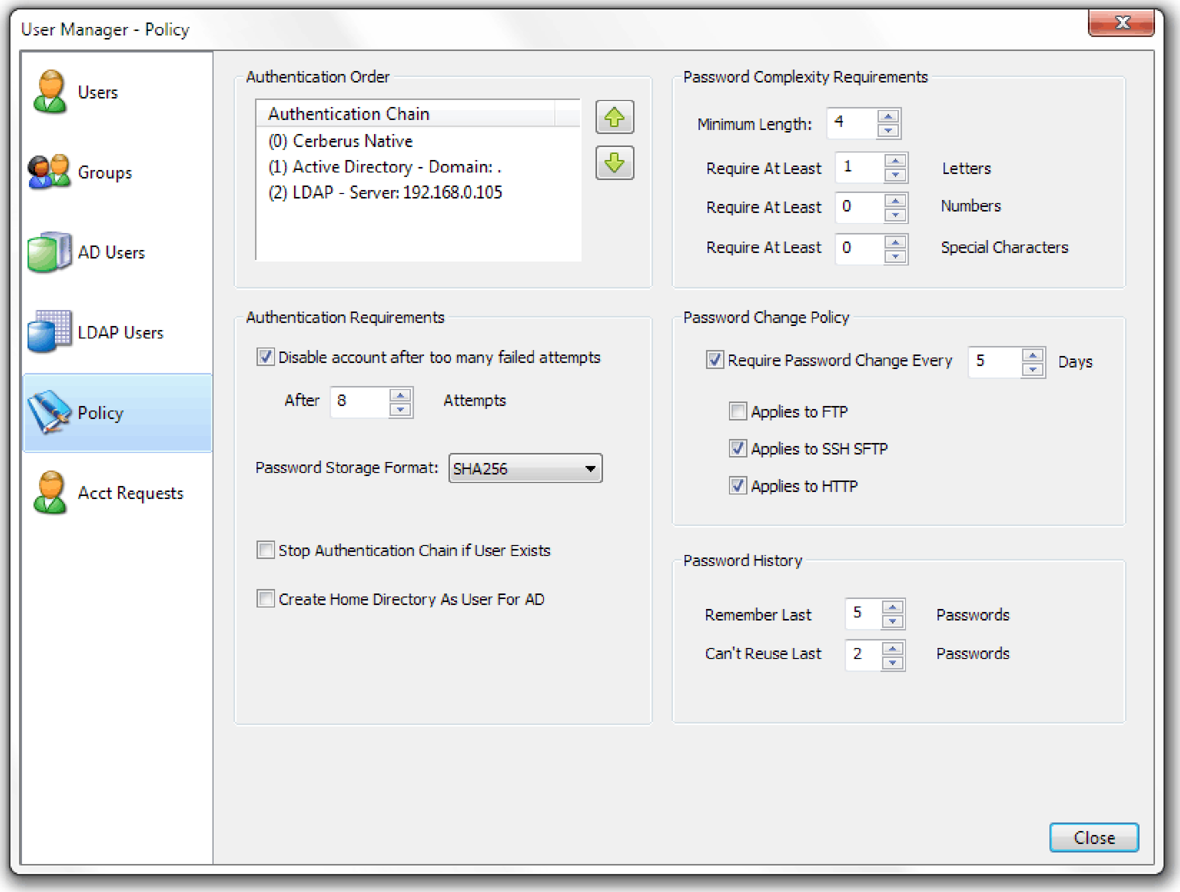
Is Anonymous	If checked, the password for any user that is part of this group is ignored and the user can be logged in using any password.
Is Simple Directories	In simple directory mode the administrator can only assign one directory to represent the virtual directory for a user that is a member of this group.
Is Disabled	Determines whether the account can login or not. A disabled account cannot login to the server.
Simultaneous Logins	The maximum number of connections this user can make to the server at the same time.
Require Secure Control	(Applies to FTP only) If enabled, members of this group can only login to the server using a secure TLS/SSL encrypted connection.
Require Secure Data	(Applies to FTP only) If enabled, members of this group can only initiate file transfers over secure TLS/SSL encrypted connections.
Disable After Date	If a date is set here then the group will become disabled after the date specified. All users that are members of this group will also become disabled. **Note**: The granularity of the timer is 30 minutes. The account will be disabled within 30 minutes of the time set.

Allow Protocols to Login	Controls which protocols a member of this group is allowed to login with. If a protocol is not checked then the user will not be allowed to login using that protocol.
SSH Authentication	Determines the SSH authentication requirements for users that are members of this group. Valid options are: • **Password Only**: Require only a password for authentication. • **Public Key Only**: Require only a valid public key for authentication • **Public Key and Password**: Require both a valid public key and a valid password for authenticating a user

USER POLICY SETTINGS

AUTHENTICATION ORDER

Cerberus FTP Server can authenticate against several different types of data sources. The current possible authentication sources include the Native user system, Active Directory (AD), and LDAP. You can have multiple AD and LDAP servers configured and Cerberus will checked each one and attempt to match a username and password. Cerberus will try each authentication source in order until a successful authentication occurs or until all sources fail authentication.



Authentication Order

Authentication Chain
(0) Cerberus Native
(1) Active Directory - Domain: .
(2) LDAP - Server: 192.168.0.105

Authentication Requirements

☑ Disable account after too many failed attempts

After 8 Attempts

Password Storage Format: SHA256

☐ Stop Authentication Chain if User Exists

☐ Create Home Directory As User For AD

Password Complexity Requirements

Minimum Length: 4
Require At Least 1 Letters
Require At Least 0 Numbers
Require At Least 0 Special Characters

Password Change Policy

☑ Require Password Change Every 5 Days

☐ Applies to FTP
☑ Applies to SSH SFTP
☑ Applies to HTTP

Password History

Remember Last 5 Passwords
Can't Reuse Last 2 Passwords

Figure 12 User Manager Policy Page

The order that authentication sources are checked is determined by the Authentication Order list box. You can move authentication sources up and down in order depending upon your needs.

AUTHENTICATION REQUIREMENTS

The Disable Account and Password Storage Format options only apply to Cerberus Native accounts.

Disable Account After x Failed Attempts	The Native account becomes disabled if x number of consecutive failed login attempts. The counter is reset on a successful login.
Password Storage Format	This is the method Cerberus uses to store password information. Options are MD5, SHA1, SHA256, and SHA512. All options are salted and are performed using FIPS compliant crypto routines if the server is in FIPS mode.
Stop Authentication Chain if User Exists	If a user is found in an authentication source but the password is incorrect, don't proceed to check the other authentication sources. Just fail the authentication request.
Create Home Directory as User For AD	This setting influences how home directories are created for AD users when the default virtual directory mapping mode in AD is set to Global Home/%username% mode. Normally, Cerberus creates the home directory while under the service account. If this option is enabled, Cerberus will impersonate the AD user before creating the directory. This ensures the home directory is owned by the AD user instead of the service account.

PASSWORD COMPLEXITY REQUIREMENTS

These settings only apply to Cerberus Native accounts.

Minimum Length	The password must be at least x characters long.
Require at Least x Letters	The password must contain at least x count of letters.
Require at Least x Numbers	The password must contain at least x count of numbers.
Require at Least x Special Characters	The password must contain at least x count of special characters (ex, %, $, #).

PASSWORD CHANGE POLICY

These settings only apply to Cerberus Native accounts.

Require Password Change Every X Days - The server will require that native account passwords be changed this number of days.

Applied to FTP	When checked, this policy is enforced for FTP/S account access. Note, FTP does not have a standard way of changing or prompting the user to change an account password. Cerberus supports a common extension that allows changing the user password using the **SITE PSWD *oldpassword newpassword*** command.
Applies to SSH SFTP	When checked, this policy is enforced for SSH SFTP account access. SSH has a standard method of allowing users to change their passwords but many SFTP clients do not implement it.

Applies to HTTP	When checked, this policy is enforced for HTTP/S account access.

PASSWORD HISTORY

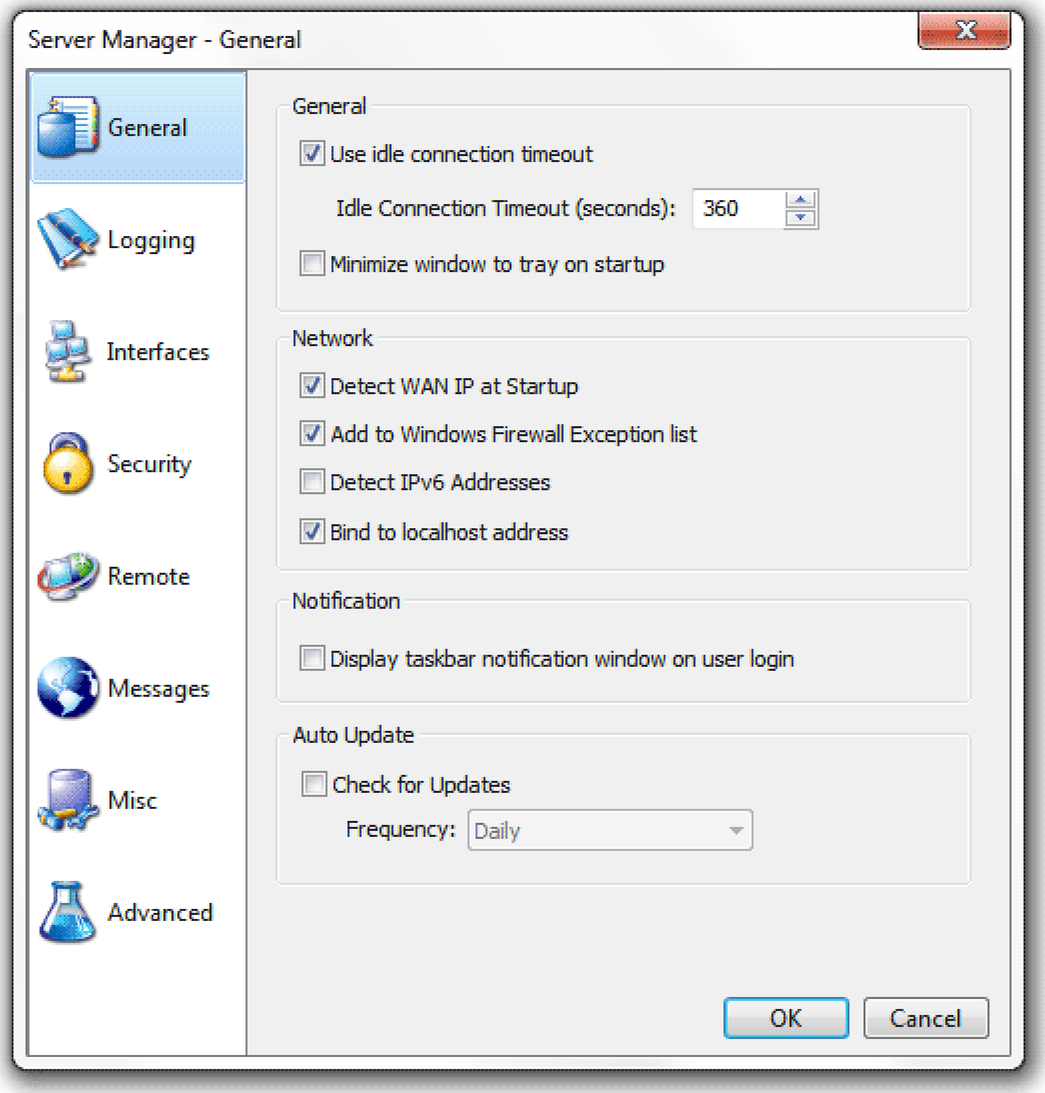
These settings only apply to Cerberus Native accounts.

Remember Last X Passwords	Cerberus will save a secure hash of the last specified number of passwords that the user has used.
Can't Reuse Last X Passwords	Cerberus will prevent a user from changing their password to any password used within the specified history count.

GENERAL SETTINGS

CONFIGURING GENERAL SETTINGS

The general settings page contains options for connection timeout, network detection, login notifications, and auto-update settings.



Server Manager - General

General

☑ Use idle connection timeout

Idle Connection Timeout (seconds): 360

□ Minimize window to tray on startup

Network

☑ Detect WAN IP at Startup

☑ Add to Windows Firewall Exception list

□ Detect IPv6 Addresses

☑ Bind to localhost address

Notification

□ Display taskbar notification window on user login

Auto Update

□ Check for Updates

Frequency: Daily

Figure 13 General page

GENERAL

The general settings page contains options for connection timeout and hiding the main Cerberus window.

- **Use idle connection timeout** - Controls whether idle connections should be terminated after a period of inactivity.
    - **Idle Connection Timeout (seconds)** - How long a connection can remain idle without being terminated.
- **Minimize window to tray on startup** - If selected, Cerberus FTP Server will start hidden when windows starts up. Only the tray icon will appear. You can restore the graphical interface by double-clicking on the Cerberus tray icon, or right-clicking on the tray icon and selecting "Show/Hide Server"

NETWORK

This section allows an administrator to change general network settings.

- **Detect WAN IP at Startup** - If enabled, Cerberus will attempt to detect the external address that Internet computers see for connecting to the network this machine is located on. This is usually the external router address. Enabling this option is important for ensuring passive connections work correctly.
- **Add to Windows Firewall Exception List** - If selected, Cerberus FTP Server will attempt to add itself to the Windows Firewall Exception list. This setting is disabled on operating systems that do not support the Windows Firewall (Windows 2000 and below).
- **Detect IPv6 Addresses** - If selected, Cerberus FTP Server will attempt to detect any IPv6 addresses that the system has initialized. You can leave this setting disabled if you are not using IPv6.
- **Minimize window to tray on startup** - Selecting this option will make Cerberus bind to localhost address (127.0.0.1).

NOTIFICATION

This section allows an administrator to change user login notification settings.

- **Display taskbar notification window on user login** - If enabled, Cerberus will display a small notification window on the bottom-right corner of the desktop whenever a user attempts to login to the server.

CONFIGURING LOGGING SUPPORT

AUDITING

Cerberus FTP Server provides comprehensive logging of all file and user operations and provides both on-screen logging, file logging, and Syslog support. File-based logging can be managed through an XML configuration file that can control nearly all aspects of how log data is written to a file.

LOG FILE LOCATION

Cerberus FTP Server logging is implemented through the Apache Log4cxx framework, a robust logging package modeled after the popular log4j Java logging package. The default configuration logs up to 5000KB of data to a single file and then rolls over to a new log file. The past 10 log files are kept by default but log file size, naming, and history are all completely configurable through the log4j.xml file.

The log file is located at the following location:

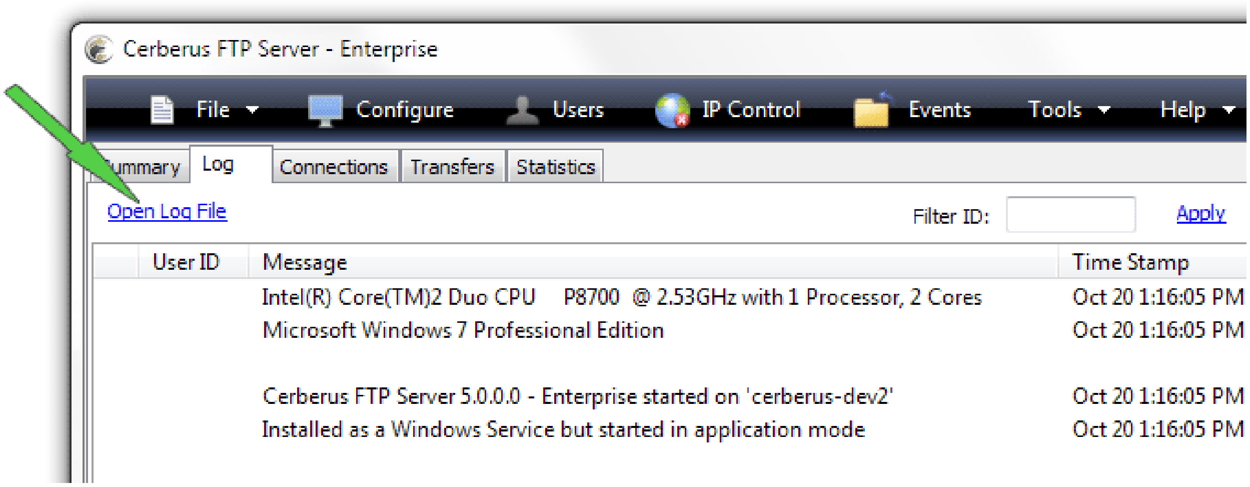
ON WINDOWS VISTA, WINDOWS 2008 AND ABOVE

C:\ProgramData\Cerberus LLC\Cerberus FTP Server\log

ON WINDOWS 2003, XP, AND 2000

C:\Documents and Settings\All Users\Application Data\Cerberus LLC\Cerberus FTP Server\log

You can also open the log file by simply clicking on the **Open Log File** link on the **Log** tab of the main user interface console as demonstrated below:



User ID	Message	Time Stamp
	Intel(R) Core(TM)2 Duo CPU P8700 @ 2.53GHz with 1 Processor, 2 Cores	Oct 20 1:16:05 PM
	Microsoft Windows 7 Professional Edition	Oct 20 1:16:05 PM
	Cerberus FTP Server 5.0.0.0 - Enterprise started on 'cerberus-dev2'	Oct 20 1:16:05 PM
	Installed as a Windows Service but started in application mode	Oct 20 1:16:05 PM

Figure 14 Logging console

CONFIGURING LOGGING

The **log4j.xml** configuration file is one level above in the "Cerberus FTP Server" folder. An example log4j.xml file is below.

There is an example of a size-based log appenders which roll over after the log file reaches a certain maximum size and that limit the number of log files that are kept. These types of loggers are limited to at most 13 saved log files.

There is also daily log file appender example (with no maximum number of kept log file limits), and a Syslog log appender example.

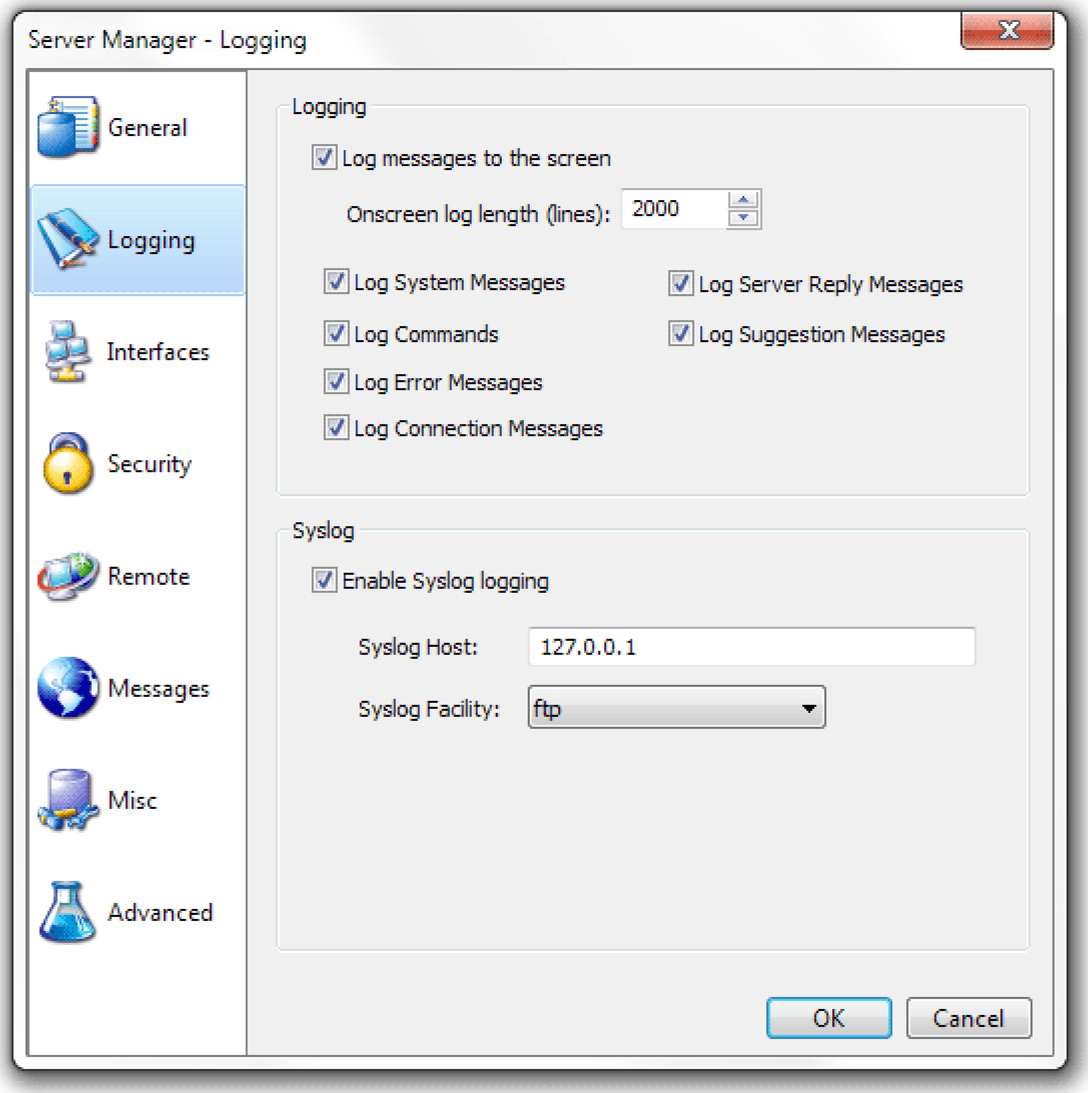
```
<?xml version="1.0" encoding="UTF-8" ?>
<log4j:configuration xmlns:log4j='http://logging.apache.org/' debug="false">

        <appender name="FILE" class="org.apache.log4j.rolling.RollingFileAppender">
                <rollingPolicy class="org.apache.log4j.rolling.FixedWindowRollingPolicy" >
                        <param name="activeFileName" value="log/server.log" />
                        <param name="fileNamePattern" value="log/server.%i.log" />
                        <param name="minIndex" value="1" />
                        <param name="maxIndex" value="5" />
                </rollingPolicy>
                <triggeringPolicy class="org.apache.log4j.rolling.SizeBasedTriggeringPolicy">
                        <param name="maxFileSize" value="5000KB" />
                </triggeringPolicy>
                <layout class="org.apache.log4j.PatternLayout">
                        <param name="ConversionPattern"
                                value="[%d{yyyy-MM-dd HH:mm:ss}]:%7.7p [%6.6x] - %m%n" />
                </layout>
        </appender>

        <appender name="ERROR_FILE" class="org.apache.log4j.rolling.RollingFileAppender">
                <rollingPolicy class="org.apache.log4j.rolling.FixedWindowRollingPolicy">
                        <param name="activeFileName" value="log/server_error.log"/>
```

```
                              <param name="fileNamePattern" value="log/server_error.%i.log"/>
                    </rollingPolicy>
                    <triggeringPolicy class="org.apache.log4j.rolling.SizeBasedTriggeringPolicy">
                              <param name="maxFileSize" value="5000KB"/>
                    </triggeringPolicy>
                    <layout class="org.apache.log4j.PatternLayout">
                              <param name="ConversionPattern" value="[%d{yyyy-MM-dd
HH:mm:ss}]:%7.7p [%6.6x]
                                        - %m%n"/>
                    </layout>
                    <filter class="org.apache.log4j.varia.LevelRangeFilter">
                              <param name="LevelMin" value="ERROR" />
                    </filter>
          </appender>



          <root>
                    <level value="INFO" class="org.apache.log4j.xml.XLevel" />
                    <appender-ref ref="FILE"/>
                    <appender-ref ref="ERROR_FILE"/>
          </root>
 </log4j:configuration>
```

Possible values for the **<level value="LEVEL" class="org.apache.log4j.xml.XLevel" />** tag's ***level*** parameter are:

- TRACE
- DEBUG
- INFO
- WARN
- ERROR

SCREEN LOGGING SETTINGS



Logging

☑ Log messages to the screen

Onscreen log length (lines): 2000

☑ Log System Messages

☑ Log Commands

☑ Log Error Messages

☑ Log Connection Messages

☑ Log Server Reply Messages

☑ Log Suggestion Messages

Syslog

☑ Enable Syslog logging

Syslog Host: 127.0.0.1

Syslog Facility: ftp

Figure 15 Logging settings page

In addition to the file-based log, Cerberus also displays the current log output to the graphical user interface while the server is running. Options for the screen-based logging can be controlled through the Logging settings tab of the Server Manager.

Log messages to screen	Enable logging messages to the screen
Onscreen log length	The number of lines of on screen logging that should be saved

SYSLOG SUPPORT

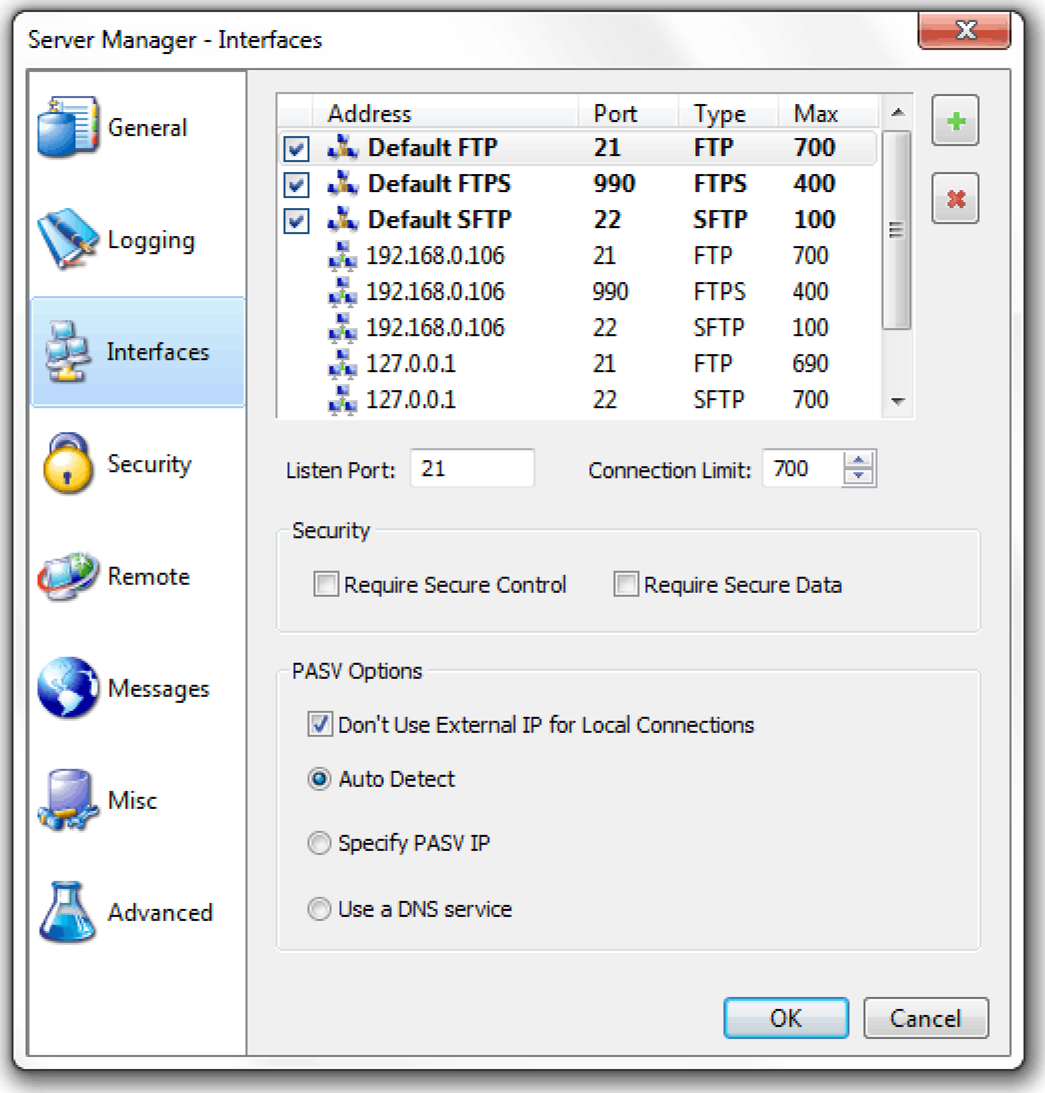
Cerberus FTP Server 5.0 supports Syslog integration from the logging page.

Enable Syslog logging	Enable syslog logging
Syslog Host	The address of the machine hosting the syslog server.
Syslog Facility	The syslog facility value that should be associated with the syslog events.

CONFIGURING INTERFACES

INTERFACES

An interface is simply an IP address that the FTP Server is listening on. It can be an IPv4 or IPv6 address. The "Default" interface represents the settings that will be applied for newly detected interfaces. There are several different parameters that each interface can have:



Server Manager - Interfaces

	Address	Port	Type	Max
☑	**Default FTP**	**21**	**FTP**	**700**
☑	**Default FTPS**	**990**	**FTPS**	**400**
☑	**Default SFTP**	**22**	**SFTP**	**100**
	192.168.0.106	21	FTP	700
	192.168.0.106	990	FTPS	400
	192.168.0.106	22	SFTP	100
	127.0.0.1	21	FTP	690
	127.0.0.1	22	SFTP	700

Listen Port: 21   Connection Limit: 700

Security

□ Require Secure Control   □ Require Secure Data

PASV Options

☑ Don't Use External IP for Local Connections

● Auto Detect

○ Specify PASV IP

○ Use a DNS service

Figure 16 Interfaces page of the Server Manager

TYPES OF LISTENERS

There are five types of listeners that you can add to an IP address. **FTP listeners**, **FTPS listeners**, **SSH2 File Transfer Protocol (SFTP) listeners**, **HTTP** and **HTTPS listeners**. The first two allow regular FTP as well as different forms of secure FTP while the SSH2 SFTP listener is for establishing connections over the SFTP protocol (a completely different protocol from FTP, despite the similar name). The HTTP and HTTPS listeners allow web client connections to the server using either the unsecure HTTP protocol or encrypted HTTPS protocol.

There are two types of secure FTP connections possible, FTPS and FTPES. FTPS is usually referred to as implicit FTP with TLS/SSL security. Its closest analog is HTTPS. It is basically the FTP protocol over a TLS/SSL secured connection. This form of secure FTP is deprecated but widely supported and still in use. This is what a Cerberus FTP Server **FTPS listener** is for and this type of listener typically listens on port 990. Note, the settings "Require Secure Control" and "Require Secure Data" are meaningless for this type of listener. Connections established to an FTPS listener can only be established securely.

FTPES, which is often referred to as **explicit FTP** with TLS/SSL security, is a modification of the FTP protocol that starts out over an insecure, normal FTP connection and is then upgraded to a secure connection through FTP command extensions during login. This is the preferred method of secure FTP because it allows SPI firewalls to know that there is FTP traffic occurring on the connection. You establish FTPES sessions using a normal Cerberus FTP Server **FTP listener**, typically over port 21. Both unencrypted FTP and explicit TLS/SSL connections can be established to this type of listener. You cannot establish an implicit FTPS connection over this type of listener.

ADDING A NEW INTERFACE

Cerberus FTP Server 4.0 and higher supports adding multiple listening interfaces for a given IP address. The only requirement is that the listener be on a unique IP/port combination. You can add an FTP, FTPS (for implicit secure FTP only), SSH2 SFTP, and HTTP or HTTPS listener.

Select the ✚ icon next to the interface list box to add a new interface. A new dialog box will appear to ask for the interface details (interface IP, type, and port combination). Selecting the "X" icon will prompt you to delete the selected interface listener.

INTERFACE SETTINGS

Listen Port	The port that this interface will listen on for the control connection
Max Connections	The maximum number of simultaneous connections that can connect to this interface
Require Secure Control	If enabled, only secure control connection will be allowed. This is required to protect passwords from compromise on unsecured networks.

Require Secure Data	If enabled, only secure data connections will be allowed. All directory listings and file transfers will be required to be encrypted.
Don't Use External IP for Passive connections	If enabled, local area network connections will receive the internal IP address instead of the public IP.
Passive Options	• **Auto Detect** - If WAN IP auto detection is enabled then use the WAN IP for the PASV command, otherwise use the interface's IP. • **Specify PASV IP** - Allows the administrator to specify what IP address is returned in response to a PASV command • **Use a DNS service** - Allows use of DNS names like www.cerberusftp.com. The address specified will be examined at regular intervals and the IP address that represents that DNS name will be used in PASV commands.

THE "DEFAULT" INTERFACES

There is a Default interface for each type of listener (FTP, implicit FTPS, SFTP, HTTP, and HTTPS). When a new interface (IP address) is detected, that interface will receive an FTP, FTPS and SFTP listener and each of those listeners will be assigned the values of the appropriate "Default" interface at the time of detection. For example, If the "Default FTP" interface was defined to be on port 21, then when a new interface is detected for the first time it will receive an FTP listener on port 21 with the values of the Default FTP interface. Those settings then become the settings for the newly detected interface. Note that the new interface's settings are not linked to the "Default" interface in any way. The "Default" interface simply represents the values that newly detected interfaces will be initialized with. Changing the values of the "Default" interface wouldn't change any values on existing or previously detected interfaces.

For example, when you first install Cerberus FTP Server, the "Default FTP" interface is set to port 21 (the default FTP listening port) and all interfaces detected during that first start will receive FTP listeners with that port value. If you later change the "Default FTP" interface settings then that change will have no effect on existing interfaces.

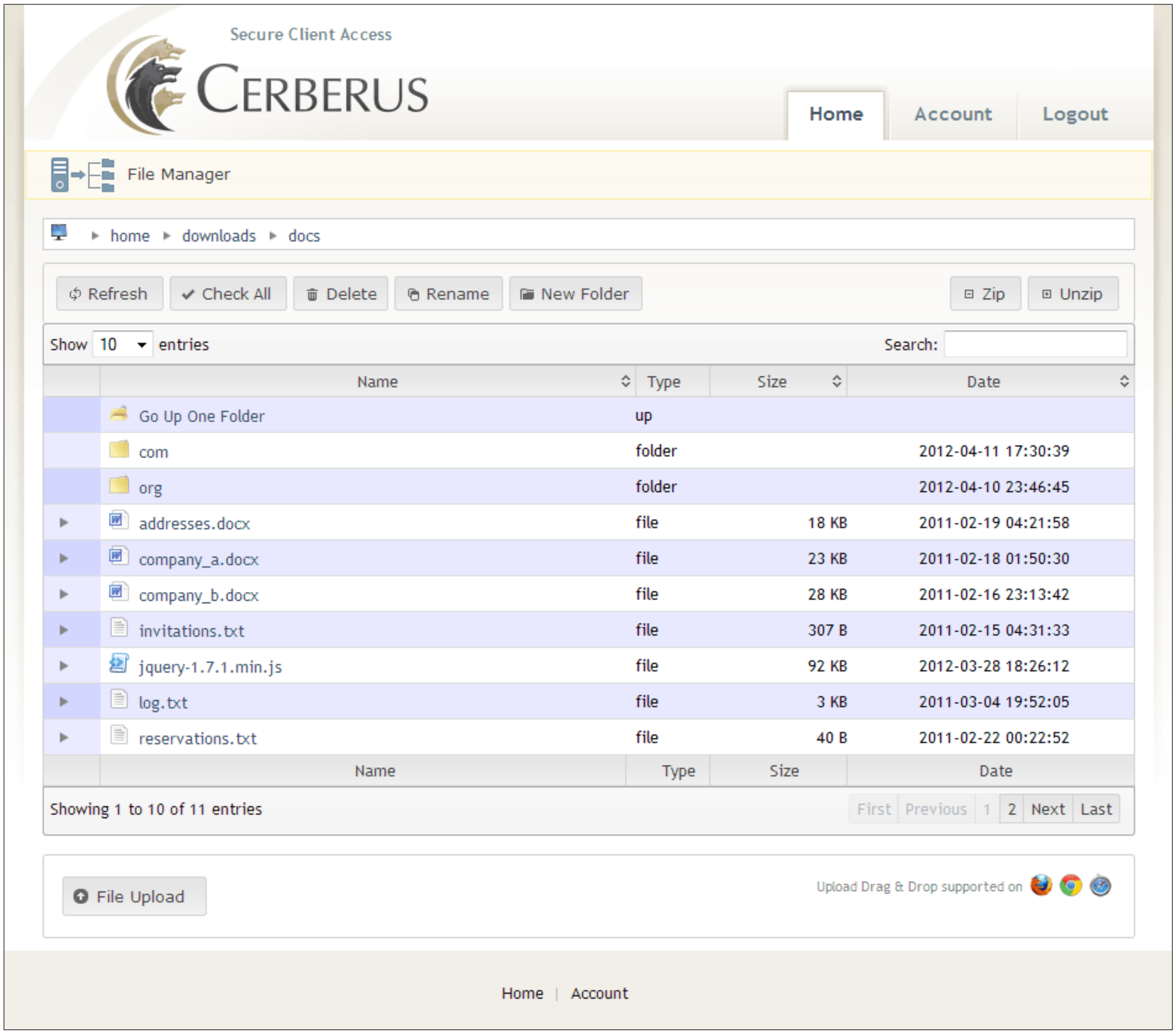
It is also worth noting that Cerberus remembers the settings for interfaces that were previously detected but might have changed. For servers that have dynamic addresses that constantly change or cycle between a range of addresses, Cerberus will "remember" the old values and apply those instead of the "Default" settings if that interface address is later detected again.

Un-checking the box next to each Default interface will disable automatic listener activation for that interface type when a new interface is detected.

THE HTTP/S WEB CLIENT

Available in Cerberus FTP Server 5.0 Enterprise edition, the HTTP/S web client capability allows any user with access to a common web browser to easily connect to the server to perform file operations (uploading, downloading, deleting, renaming, creating directories, and zipping and unzipping files and directories) using a web browser.

The web client is a native web application that requires no plug-ins or external tools to use. The web client relies on HTML and JavaScript for all of its functionality and will run on any modern web browser.



Name	Type	Size	Date
Go Up One Folder	up		
com	folder		2012-04-11 17:30:39
org	folder		2012-04-10 23:46:45
addresses.docx	file	18 KB	2011-02-19 04:21:58
company_a.docx	file	23 KB	2011-02-18 01:50:30
company_b.docx	file	28 KB	2011-02-16 23:13:42
invitations.txt	file	307 B	2011-02-15 04:31:33
jquery-1.7.1.min.js	file	92 KB	2012-03-28 18:26:12
log.txt	file	3 KB	2011-03-04 19:52:05
reservations.txt	file	40 B	2011-02-22 00:22:52

Showing 1 to 10 of 11 entries

Figure 17 Cerberus FTP Server 5.0 Web Client

Additional Web Client features include:

- Fully tested against IE 7.0+, Firefox 18+, Chrome 20+, Safari 4.0+, Opera 9.0+, iPhone, and the iPad.
- No file size limitations and can efficiently handle file uploads and downloads of any size.
- Multiple, simultaneous file upload and upload drag and drop support in Firefox, Safari, and Chrome

- Confirmation dialogs for file deleting, zipping, and unzipping.
- Web-based with no software to install for end users

ADDING AN HTTP/S LISTENER

The Cerberus FTP Server web client can be accessed by adding an HTTP or HTTPS listener to Cerberus FTP Server's listener list. You can add a new HTTP/S listener from the **Interfaces** page of the **Server Manager**.

To add a new HTTP or HTTPS listener:

1. Open the Server Manager
2. Select the **Interfaces** page
3. Select the "plus" icon next to the interface list box to add a new interface. The "Add New Listener" dialog box will appear to ask for the interface details (interface IP, type, and port combination)
4. Select the IP address that you want to listen for connections on
5. Select the interface type (HTTP or HTTPS for web client access)
6. Enter the port you wish to listen on. Cerberus will automatically pre-populate the port with the default port for the type of listener you are adding
7. Press the **Add** button to add the listener

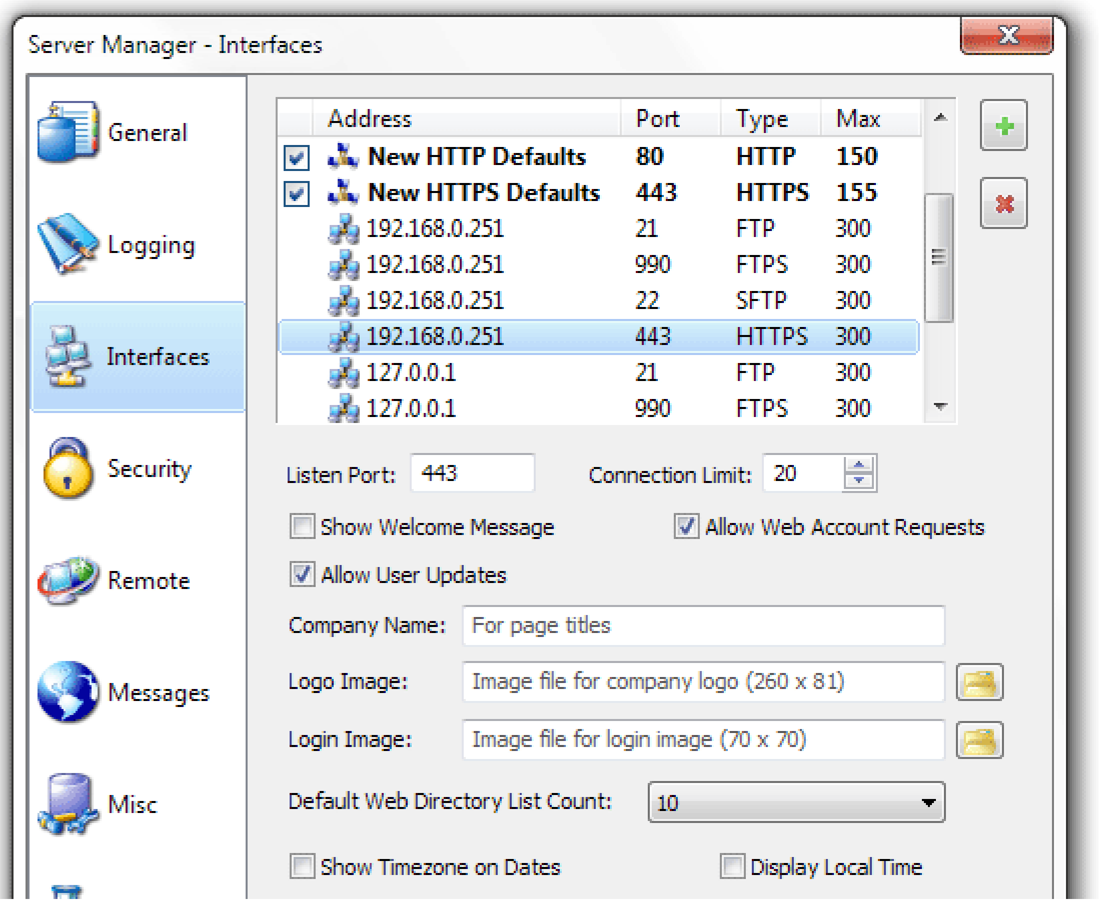
The listener should now be added to the Interfaces list. Press **Ok** to close the Server Manager and save you changes.

WEB CLIENT CUSTOMIZATIONS

The HTTP/S web client can be customized in several ways. Options for changing the default settings are discussed in the following sections.

CHANGING THE COMPANY LOGO AND LOGIN IMAGE

You can easily change the company logo displayed on the web client by specifying your own logo file.



	Address	Port	Type	Max
☑	**New HTTP Defaults**	**80**	**HTTP**	**150**
☑	**New HTTPS Defaults**	**443**	**HTTPS**	**155**
	192.168.0.251	21	FTP	300
	192.168.0.251	990	FTPS	300
	192.168.0.251	22	SFTP	300
	192.168.0.251	443	HTTPS	300
	127.0.0.1	21	FTP	300
	127.0.0.1	990	FTPS	300

Listen Port: 443 Connection Limit: 20

□ Show Welcome Message ☑ Allow Web Account Requests

☑ Allow User Updates

Company Name: For page titles

Logo Image: Image file for company logo (260 x 81)

Login Image: Image file for login image (70 x 70)

Default Web Directory List Count: 10

□ Show Timezone on Dates □ Display Local Time

Figure 18 Cerberus FTP Server 5.0 HTTP Listener

1. Go to the Interfaces page of the Server Manager
2. Select the HTTP/S interface you wish to change (not the default interface)
3. Press the file selection button across from the Logo Image edit box
4. Select the image file you wish to use and press Ok. The preferred image size is 260x81.

The login image displayed on the login page is also customizable using the same procedure as for the company logo. The preferred login image size is 70x70 pixels.

CHANGING THE LOGIN WELCOME MESSAGE

If you select the **Show Welcome Message** option for the HTTP/S listener then the server welcome message is displayed next to the login credentials box when a client logs in on that listener. This message can be customized from the **Messages** page of the **Server Manager**.

FURTHER WEB CLIENT CUSTOMIZATIONS

The HTTP/S web client can be further customized by modifying the underlying template files. However, any changes made to those template files will be overwritten whenever Cerberus FTP Server is upgraded. We are working on ways to allow more permanent and lasting changes to the web client. The relevant template files are in:

C:\Program Files\Cerberus LLC\Cerberus FTP Server\webadmin

and

C:\Program Files\Cerberus LLC\Cerberus FTP Server\webadmin\client

The client-index.tpl file is probably the best place to start for modifying the overall look of the web client. A restart of the underlying Cerberus FTP Server Windows Service is required before any changes to these files will take effect.

WEB ACCOUNT REQUESTS

ALLOWING USERS TO REQUEST ACCOUNTS THROUGH THE WEB

Starting with Cerberus FTP Server 5.0 Enterprise edition, users can now request new accounts through the HTTP/S Web Client. A "Request a New Account" link will appear on the login page if the administrator decides to allow web account requests.

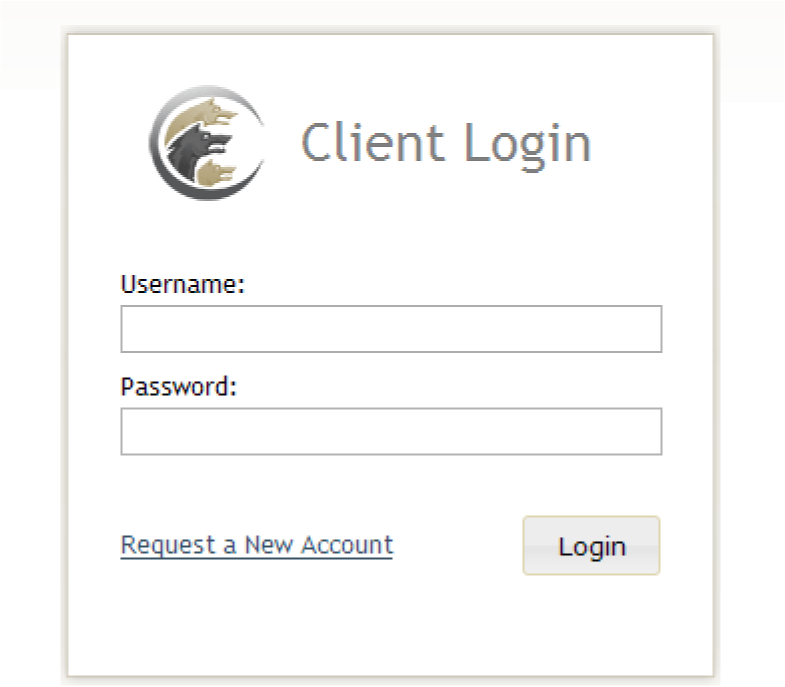
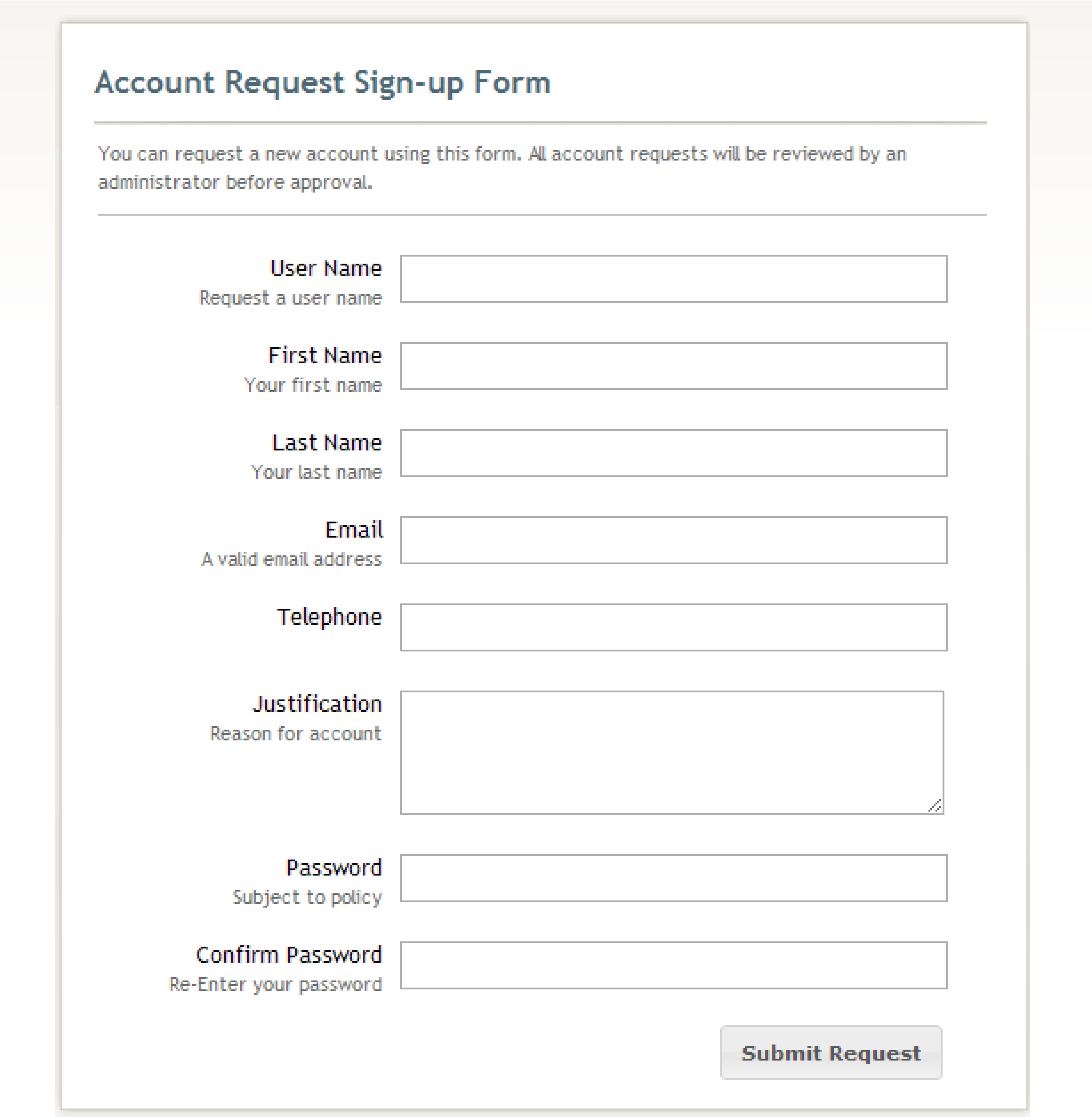


Figure 19 HTTP/S Login Page with "Request a New Account" Link

REQUESTING A NEW ACCOUNT

The account request page allows a user to submit a request for a new account to the Cerberus FTP Server system administrator. Event Rules can be enabled on the server to automatically email the administrator whenever a new account request is made.



Account Request Sign-up Form

You can request a new account using this form. All account requests will be reviewed by an administrator before approval.

User Name
Request a user name

First Name
Your first name

Last Name
Your last name

Email
A valid email address

Telephone

Justification
Reason for account

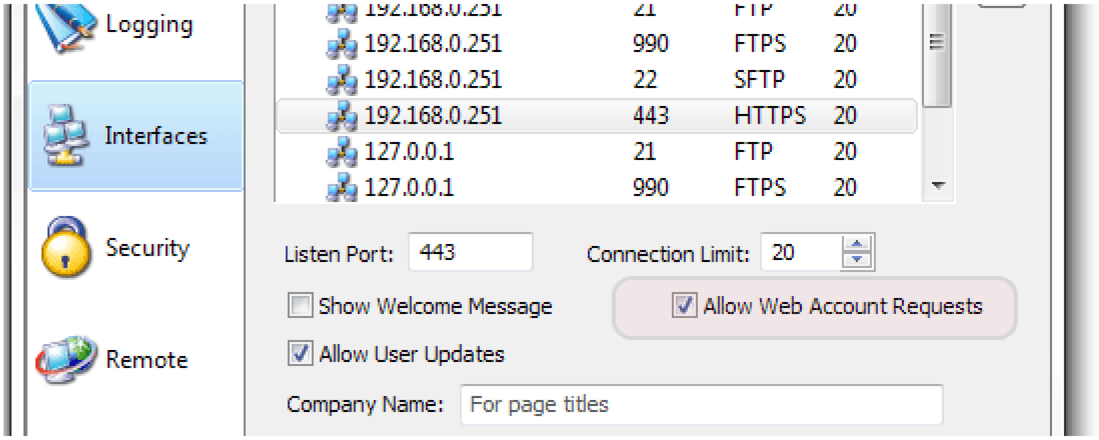
Password
Subject to policy

Confirm Password
Re-Enter your password

Figure 20 Web Client Account Request Page

ENABLING OR DISABLING ACCOUNT REQUESTS

The link can be enabled or disabled for any HTTP or HTTPS listener by selecting that listener in the Interfaces page of the Server Manager.



192.168.0.251	21	FTP	20
192.168.0.251	990	FTPS	20
192.168.0.251	22	SFTP	20
192.168.0.251	443	HTTPS	20
127.0.0.1	21	FTP	20
127.0.0.1	990	FTPS	20

Listen Port: 443

Connection Limit: 20

☐ Show Welcome Message

☑ Allow Web Account Requests

☑ Allow User Updates

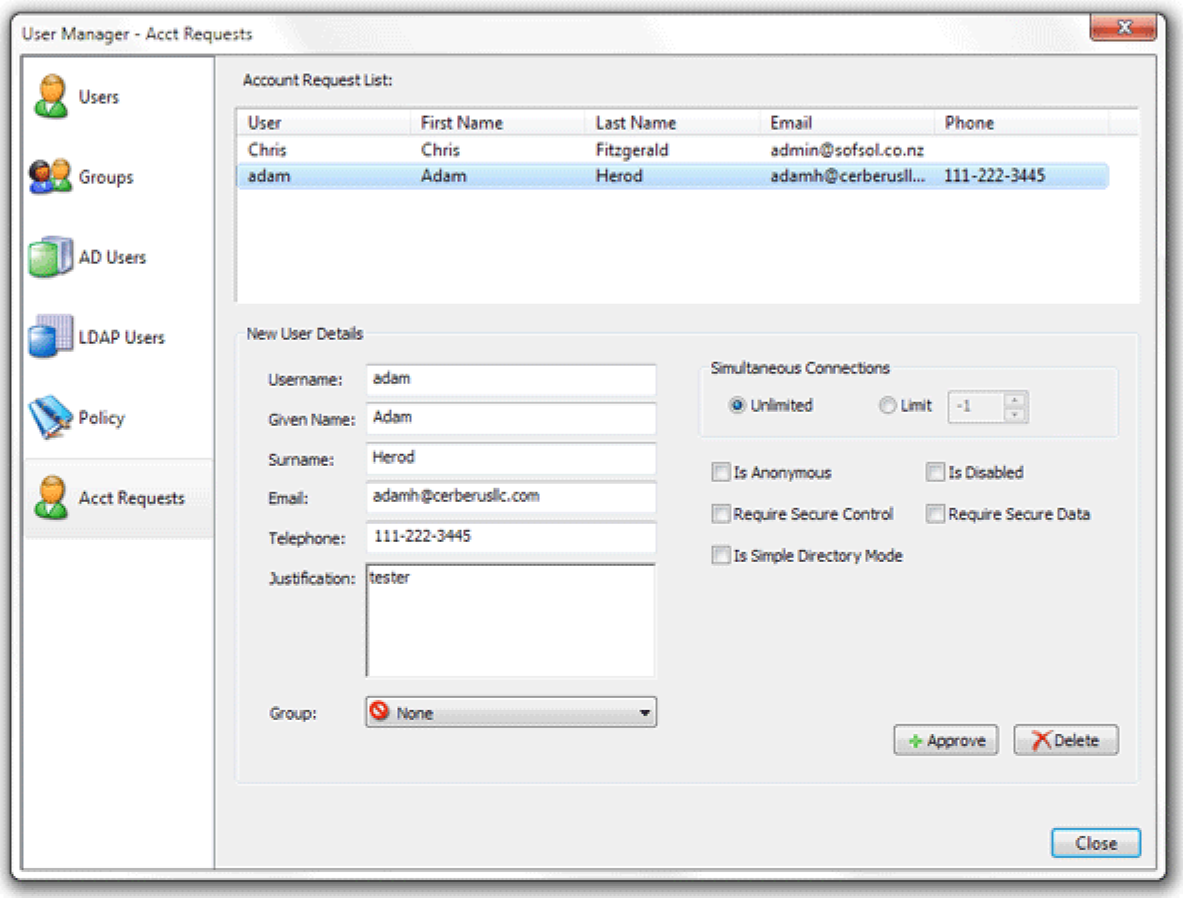
Company Name: For page titles

Figure 21 Web Client Account Request Page

APPROVING OR DENYING ACCOUNT REQUESTS

Administrators can view pending account requests through both the **Account Requests** page of the **User Manager** in the Cerberus GUI, or through the Account Requests administrator web page. Accounts can be approved or denied through either method by selecting an account and using the **Approve** or **Delete** button.

Approved accounts are automatically created and activated in the **Users** page of the **User Manager** and can be further customized there.



Account Request List:

User	First Name	Last Name	Email	Phone
Chris	Chris	Fitzgerald	admin@sofsol.co.nz	
adam	Adam	Herod	adamh@cerberusll...	111-222-3445

New User Details

Username: adam

Given Name: Adam

Surname: Herod

Email: adamh@cerberusllc.com

Telephone: 111-222-3445

Justification: tester

Group: None

Simultaneous Connections

● Unlimited ○ Limit -1

□ Is Anonymous □ Is Disabled

□ Require Secure Control □ Require Secure Data

□ Is Simple Directory Mode

Figure 22 The Cerberus FTP Server Account Request Page of the User Manager

SECURITY SETTINGS

CONFIGURING SECURITY SETTINGS

The security settings page allows the administrator to configure all aspects of Cerberus FTP Server SSL/TLS security. To enable TLS/SSL connections between FTP clients and the server, you need a server certificate and a private key.

DIGITAL CERTIFICATE SUPPORT

Cerberus FTP Server 4.0 and higher supports RSA, DSA and Elliptical Curve (EC) keys. Support for elliptical curve ciphers with FTPS requires a special Elliptical Curve Cryptography (ECC) build of Cerberus FTP Server.

There are generally two options for obtaining a digital certificate (with private key).

1. You can generate your own self-signed certificate using the Cerberus **Create Cert** button.
2. You can obtain a certificate from a recognized Certificate Authority

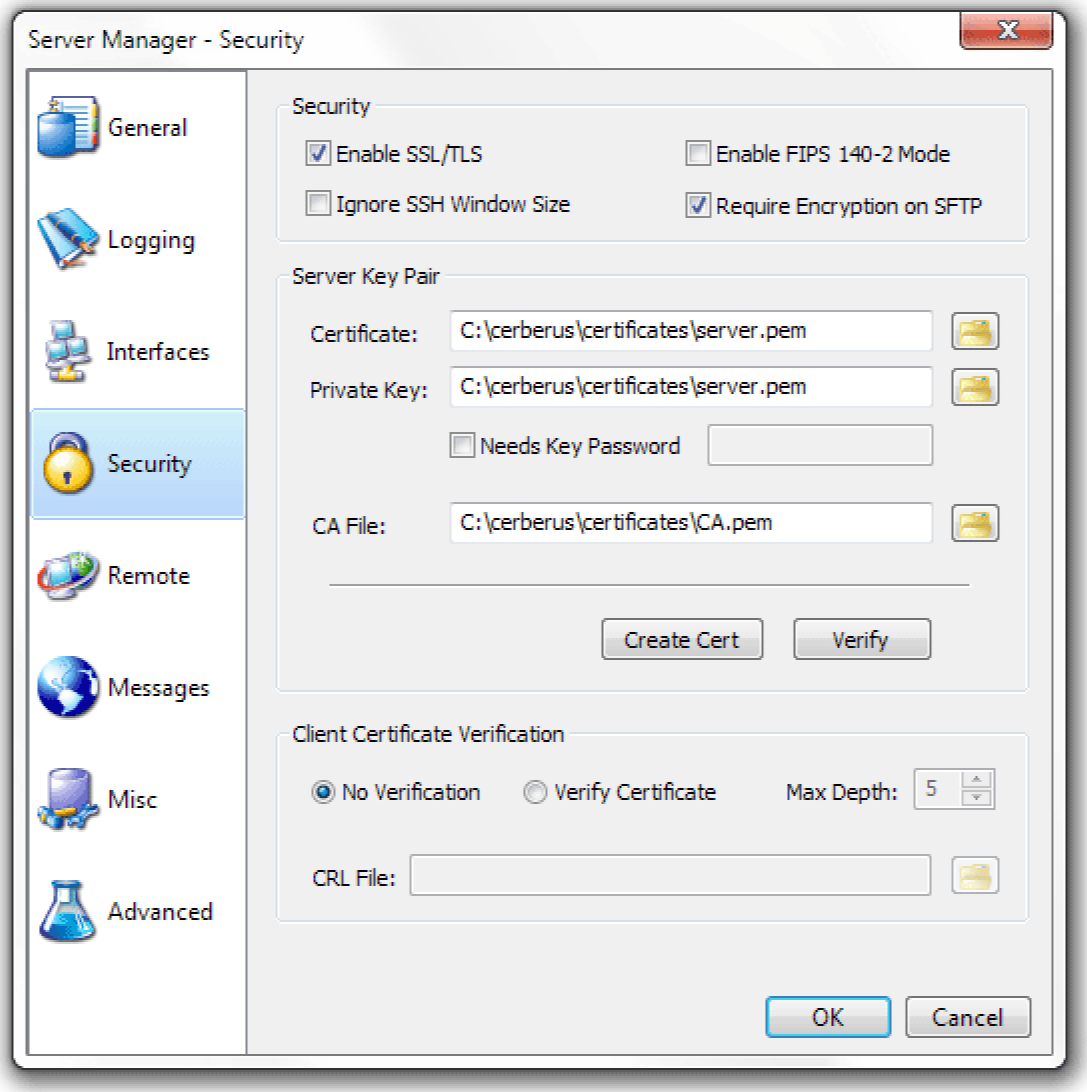
Which is more appropriate really depends upon your goals. If you just want to make sure that client and server connections are securely encrypted then a self-signed certificate is all you need. It has the benefit of being easily created through Cerberus and completely free. Just click the **Create Cert** button, fill in the certificate details in the dialog that appears, press the Ok button and that should be all you have to do. A self-signed certificate will be created and Cerberus will be automatically configured to use it.

If your goal is to make sure that your clients can verify that the server they are connecting to is legitimate and to ensure they don't see any warning messages about being "unable to verify the server" then using a certificate signed by a trusted certificate authority is required. You will have to contact one of the recognized Certificate Authorities such as Comodo, Thawte, Verisign or one of the many other recognized Certificate Authorities and request a server certificate (for a price).

A note about secure connections: Cerberus supports FTP/S, FTPES, SFTP, and HTTPS encryption. To establish a secure connection you must connect to the server with a client that supports one of those secure methods. For secure FTPES, FTPS, or SFTP, this will require a dedicated FTP client, not a web browser. No web browsers natively support any type of secure FTP.

ABOUT CERTIFICATE AUTHORITIES

You only need to worry about setting up and validating against a certificate authority if you (the server) want to authenticate the certificates coming from your FTPS and HTTPS clients. If you aren't concerned with verifying your FTPS and HTTPS clients using certificates then you can safely ignore all of the certificate authority configuration information. Just select the "No verification" setting (the default). Note: Client certificate verification is completely separate from SSH SFTP public key authentication. SSH SFTP public key authentication is configured on a per user basis.



Security

☑ Enable SSL/TLS ☐ Enable FIPS 140-2 Mode

☐ Ignore SSH Window Size ☑ Require Encryption on SFTP

Server Key Pair

Certificate: C:\cerberus\certificates\server.pem

Private Key: C:\cerberus\certificates\server.pem

☐ Needs Key Password

CA File: C:\cerberus\certificates\CA.pem

Client Certificate Verification

● No Verification ○ Verify Certificate Max Depth: 5

CRL File:

Figure 23 Security settings page of the Server Manager

TLS/SSL SECURITY

Cerberus uses the settings here for all secure connections.

SECURITY OPTIONS

These are basic TLS/SSL settings applicable to secure client FTPS, HTTPS and SSH connections and encrypted HTTPS SOAP messages.

Enable Explicit TLS/SSL	This must be enabled to allow secure access to the server. NOTE: A certificate and private key must be available before TLS/SSL encryption will be available.
Enable FIPS 140-2 Mode	Engaged the FIPS 140-2 certified encryption module for Cerberus FTP Server. Selecting this option enables encryption using only FIPS 140-2

	certified algorithms. ONLY AVAILABLE IN THE PROFESSIONAL AND ENTERPRISE EDITIONS.
Ignore SSH Window Size	Some SFTP clients do not correctly request an increase in the SSH channel window size. Enabling this option will allow those connections to continue even after exceeding the available channel window space.
Require Encryption on SFTP	Although most clients won't request an unencrypted connection, the SSH protocol does allow it. Check this option to disallow unencrypted SSH connections.
Public Certificate	The full path to your public certificate. The public certificate is exchanged with the client during TLS/SSL encryption and is examined by the client to verify the server.
Private Key	This is the server's private key. The private key is used to encrypt messages to the client. The client can use the server's public key to decrypt messages encrypted with the server's private key. The private key is not sent to the client. If your public and private key are in the same file then set this path to be the same as the Public Certificate. *NOTE*: The public and private key can be in the same file. If your public and private key are in the same file then set this path to the same path as your Public Certificate path. Cerberus understands both DER and PEM encoded certificate formats.
Needs Key Password	Check this option if the digital certificate is encrypted.
Password	The key password used to decrypt your digital certificate.
Create Cert	Cerberus will generate a Self-Signed Certificate that will allow encrypted connections.
Verify	Cerberus will attempt to verify that the certificate at the Public and Private key path is recognized and readable with the given password.

CLIENT CERTIFICATE VERIFICATION

Cerberus FTP Server can be configured to require FTPS and HTTPS clients to verify themselves using digital certificates. When given a Certificate Authority certificate list, Cerberus will verify that the client certificate is signed and valid for the given Certificate Authorities. Cerberus will also make sure the certificate hasn't been revoked if a CRL is specified. This feature is only available in Cerberus FTP Server Professional and Enterprise edition and currently only applies to FTPS, FTPES, and HTTPS connections.

- **No Verification** - This is the default option. Cerberus will not require nor will it verify digital certificates
- **Verify Certificate** - Cerberus will attempt to verify that the certificate presented by the client is signed and valid. It will compare the certificate against the certificate authorities present in the CA Certificates File. Any FTPS connection attempts without a valid certificate will be denied when this option is selected.
- **CA File** - A file containing a PEM-encoded list of Certificate Authorities with which to verify client certificates against.

ADDITIONAL CLIENT CERTIFICATE VERIFICATION OPTIONS

Cerberus can be configured to provide additional post-verification client certificate checking. Specifically, you can require the certificate common name to match the FTP username. This option is currently only exposed via the **settings.xml** configuration file and can be controlled through the following security tag

<verifyClientCommonName>true</verifyClientCommonName>

Set this option to true to enable certificate common name to FTP username checking.

TLS/SSL CIPHER SELECTION

The ciphers that Cerberus uses during secure connection negotiation can be controlled through a text string in the Cerberus FTP Server **settings.xml** configuration file. The

<cipherListString>ALL:!LOW:@STRENGTH</cipherListString>

element follows the same cipher string format as the OpenSSL ciphers string.

DSA CERTIFICATES AND EPHEMERAL DIFFIE-HELLMAN KEYS

Cerberus FTP Server 4.0.3 and higher includes support for DSA certificates. Unlike RSA certificates, DSA certificates cannot be used for key exchange and require additional Diffie-Hellman (DH) parameters during key exchange.

DH parameters are computationally very expensive to generate and it isn't feasible (or necessary) to generate those parameters in real-time. Cerberus FTP Server includes DH parameters for 512, 1024, 2048, and 4096 bit keys. The parameters were pre-generated using strong sources of pseudo-random entropy and are used during DH key exchange to generate new, temporary keys for each SSL session.

Cerberus looks for the DH parameter files in the **C:\ProgramData\Cerberus LLC\Cerberus FTP Server\certificates** directory. You can freely replace the included parameter files with your own, pre-generated versions if you desire. If the existing files are deleted, Cerberus will attempt to re-create the missing files during startup by generating new ones. This can take a *very* long time and Cerberus will appear to hang during startup while the files are generated. Deleting the existing DH parameter files is **not recommended**.

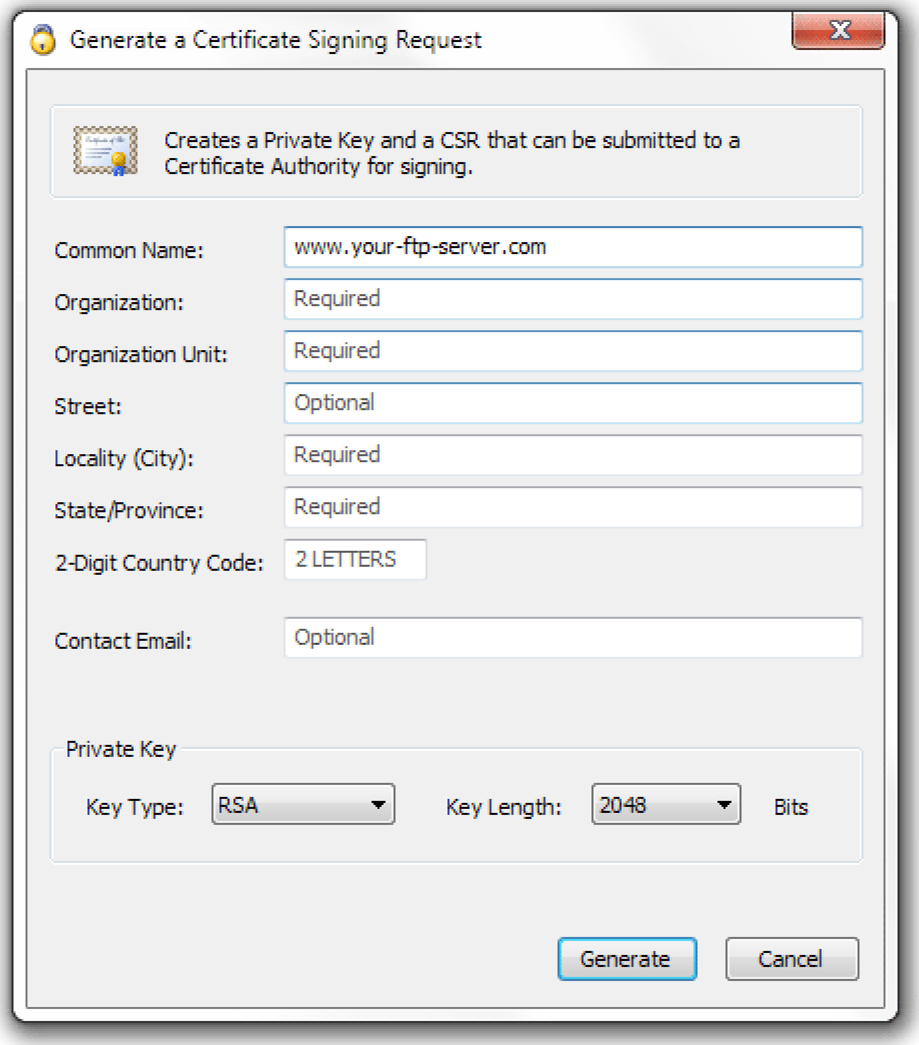
ELLIPTICAL CURVE CERTIFICATES

Cerberus FTP Server 4.0.3 and higher includes support for elliptical curve (EC) certificates. Cerberus FTP Server 4.0.9 and higher support Elliptic Curve Diffie-Hellman (ECDH) key agreement, Elliptic Curve Digital Signature Algorithm (ECDSA), and elliptic curve public keys for SSH SFTP as specified in RFC 5656. Only the required NIST curves at 256, 384, and 521 bits with uncompressed points are currently supported. Please see this page for more information on elliptical curve cryptography support

CERTIFICATE SIGNING REQUEST

CREATING A CERTIFICATE SIGNING REQUEST

The first step in requesting a certificate from a Certificate Authority (CA) is usually creating what is called a Certificate Signing Request (CSR). Cerberus FTP Server 5.0 and higher allow you to easily create a CSR using a simple wizard. You can start the CSR Wizard by opening the Tools menu and selecting the Generate a CSR menu item.



Generate a Certificate Signing Request

Creates a Private Key and a CSR that can be submitted to a Certificate Authority for signing.

Common Name: www.your-ftp-server.com

Organization: Required

Organization Unit: Required

Street: Optional

Locality (City): Required

State/Province: Required

2-Digit Country Code: 2 LETTERS

Contact Email: Optional

Private Key

Key Type: RSA

Key Length: 2048 Bits

Figure 24 Certificate Signing Request Wizard

Fill in all of the required fields for the CSR and then press the Generate button. After you select the Generate button a directory selection dialog will appear to allow you to specify a directory to save the private key and certificate signing request.

Make sure you save both the private key file, and the CSR file. You will need both of these files.

SUBMITTING YOUR CSR TO A CERTIFICATE AUTHORITY

You will submit the CSR file to your CA and keep the private key file. Once your CA has approved your CSR they will issue you a signed public certificate file. This signed public certificate file from your CA and the private key file, created during your certificate signing request, together represent your server public and private key pair.

The CA will usually provide several different format options for the signed public certificate. The preferred format is a PEM-formatted certificate (the same format Apache web server uses). PEM is also called a Base64 encoded DER certificate. You can tell if a certificate is in this format by opening it in a text editor, and looking for the beginning and ending lines "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----".

ASSIGNING YOUR CERTIFICATE AND PRIVATE KEY IN CERBERUS FTP SERVER

The final step involves assigning the signed public certificate file and private key file as your public key pair in the Security page of the Server Manager.

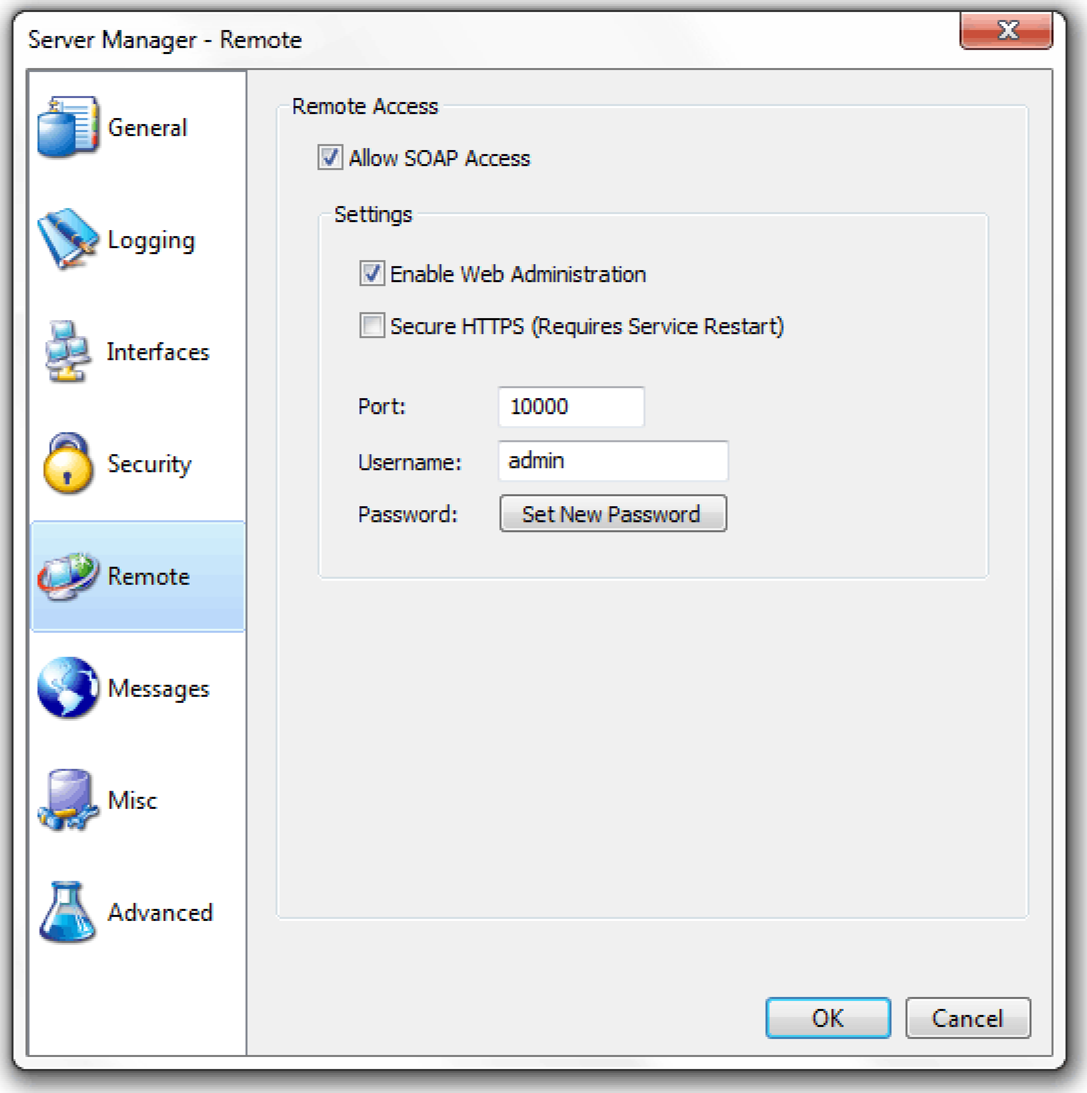
1. Open the **Server Manager** by selecting the **Configuration** -> **Server Manager** item from the main menu.
2. Select the **Security** page.
3. Under the Server Key Pair group, click the file selection button next to the **Certificate** edit control.
4. A file open dialog will appear that will allow you to select the public certificate provided from your certificate authority.
5. Under the Server Key Pair group, click the file selection button next to the **Private Key** edit control.
6. A file open dialog will appear that will allow you to select the server's private key. This file was generated when you first created your CSR.
7. Most CAs provide a CA bundle file that contains all of the intermediate CA certificates leading up to your signed certificate. If your CA provides a CA bundle file, download and assign that file to the CA File field.

REMOTE SETTINGS

CONFIGURING REMOTE SETTINGS

The remote settings page allows the administrator to configure web administration access and remote Application Programming Interface (API) access to Cerberus FTP Server. Cerberus allows remote access to the server administrator via a web browser-based interface and via the normal Cerberus FTP Server Graphical User Interface (GUI) when running in Windows Service mode.

For software developers, Cerberus exposes several APIs for controlling all aspects of the server using the SOAP web services.



☑ Allow SOAP Access

☑ Enable Web Administration

□ Secure HTTPS (Requires Service Restart)

Port: 10000

Username: admin

Password:

Figure 25 Remote settings page of the Server Manager

REMOTE ACCESS

The remote access settings control HTTP and HTTPS web and SOAP access to Cerberus FTP Server. When Cerberus is running as a Windows Service, the GUI connects to and communicates with the Cerberus service through a remote access API called SOAP. The Cerberus service listens for SOAP connections on the **Port** specified under the Remote Settings page. That port must be available for Cerberus to listen on or the GUI will be unable to connect to the service.

- **Allow SOAP Access** - Enable SOAP-based access. SOAP is an API for connecting programmatically to the server.
    - ***NOTE:*** This must be enabled to be able to access the server user interface when running as a Windows Service.
- **Secure HTTP (HTTPS)** - Select this option to allow only secure HTTPS connections for the web administration and SOAP access
- **Port** - The port that the SOAP service and web admin pages will be served from.
- **Username** - The username used to access the web administration page.
- **Password** - The password used to access the web administration page.
    - ***NOTE:*** This is also the username and password used when accessing Cerberus as a Windows Service from the Cerberus GUI. Normally, administrators won't be prompted for this password and the GUI will automatically connect to the service whenever it is started.

WEB ADMINISTRATION

The web admin capability does not have the full feature set of the local Windows user interface but does provide a large subset. We will be adding more features with every minor release until it mirrors the local graphical user interface.

- **Enable Web Access** - Allow a server administrator to connect and configure Cerberus FTP Server using the built-in web-based interface.

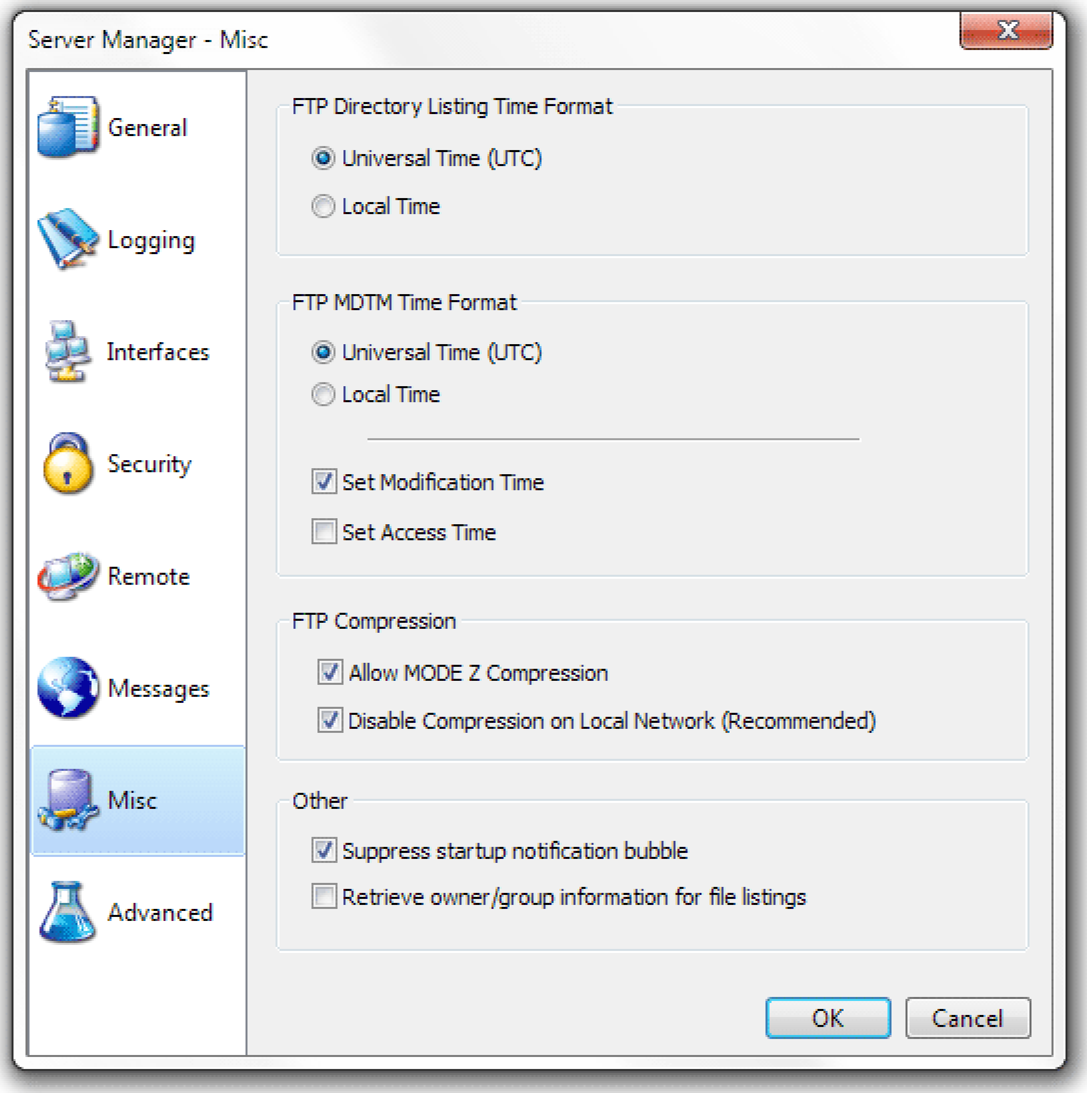
The Standard and Professional edition include a web administration feature and can be enabled by:

1. Select the **Remote** tab of the Server Manager
2. Check **Allow SOAP Access**
3. If you would like to enable secure web access, check **Secure HTTP (HTTPS)**
4. Check **Enable Web Access**
5. Enter the **Username** and **Set New Password** for the remote admin account. This is the username and password you will use to login to the web administration console
6. Shutdown and Restart Cerberus FTP Server
7. Open your web browser on the machine running Cerberus FTP Server and go to http://localhost:10000/ or https://localhost:10000/ if you selected **Secure HTTP (HTTPS)**

MISCELLANEOUS SETTINGS

CONFIGURING MISCELLANEOUS SETTINGS

The miscellaneous settings page contains options that do not fit well into any other category.



Server Manager - Misc

FTP Directory Listing Time Format

● Universal Time (UTC)

○ Local Time

FTP MDTM Time Format

● Universal Time (UTC)

○ Local Time

☑ Set Modification Time

☐ Set Access Time

FTP Compression

☑ Allow MODE Z Compression

☑ Disable Compression on Local Network (Recommended)

Other

☑ Suppress startup notification bubble

☐ Retrieve owner/group information for file listings

Figure 26 Miscellaneous Settings Page of the Server Manager

FTP DIRECTORY LISTING TIME FORMAT

This setting determines the time zone format for the file list returned in response to the LIST and NLST commands. Most clients expect dates and times to be UTC format.

- **Universal Time (UTC)** - The default, send file date/time in UTC format.
- **Local Time** - Send file date/time in local time.

FTP MDTM TIME FORMAT

The FTP command, MODIFICATION TIME (MDTM), can be used to determine when a file in the server file system was last modified. This command has existed in many FTP servers for many years, as an adjunct to the REST command for STREAM mode. As a result, this command is widely available.

This command is also frequently used in a non-standard fashion to set file modification times. Cerberus supports both the standard MDTM command for retrieving file times and the non-standard use for setting the date/time on a file.

NOTE: Settings dates and times required FTP client support. There is often a setting that has to be enabled in many FTP clients before an uploaded or downloaded file will have its date/time set. Consult your FTP client documentation on how to enable this setting. Cerberus automatically supports setting a file date/time without any additional configuration.

- **Universal Time (UTC)** - Most FTP clients expect the MDTM command to process date/time values in UTC format and this is the default. Selecting this option will cause Cerberus to interpret and send dates in UTC format.
- **Local Time** - Interpret and send dates in local time (not RFC compliant).
- **Set Modification Time** - When clients attempt to use the non-standard MDTM extension to set a date/time for a file, this setting determines whether the file modification time will be set
- **Set Access Time** - When clients attempt to use the non-standard MDTM extension to set a date/time for a file, this setting determines whether the file access time will be set

FTP COMPRESSION

Cerberus FTP Server 5.0 and higher support MODE Z compression for FTP directory listings, uploads and downloads.

- **Allow MODE Z Compression** - If checked, MODE Z compression will be enabled for clients that request it.
- **Disable Compression on Local Network (Recommended)** - The benefits of compression on the local network can often times be outweighed by the time it takes to compress that data. It is recommended that compression be disabled for local network connections.

OTHER

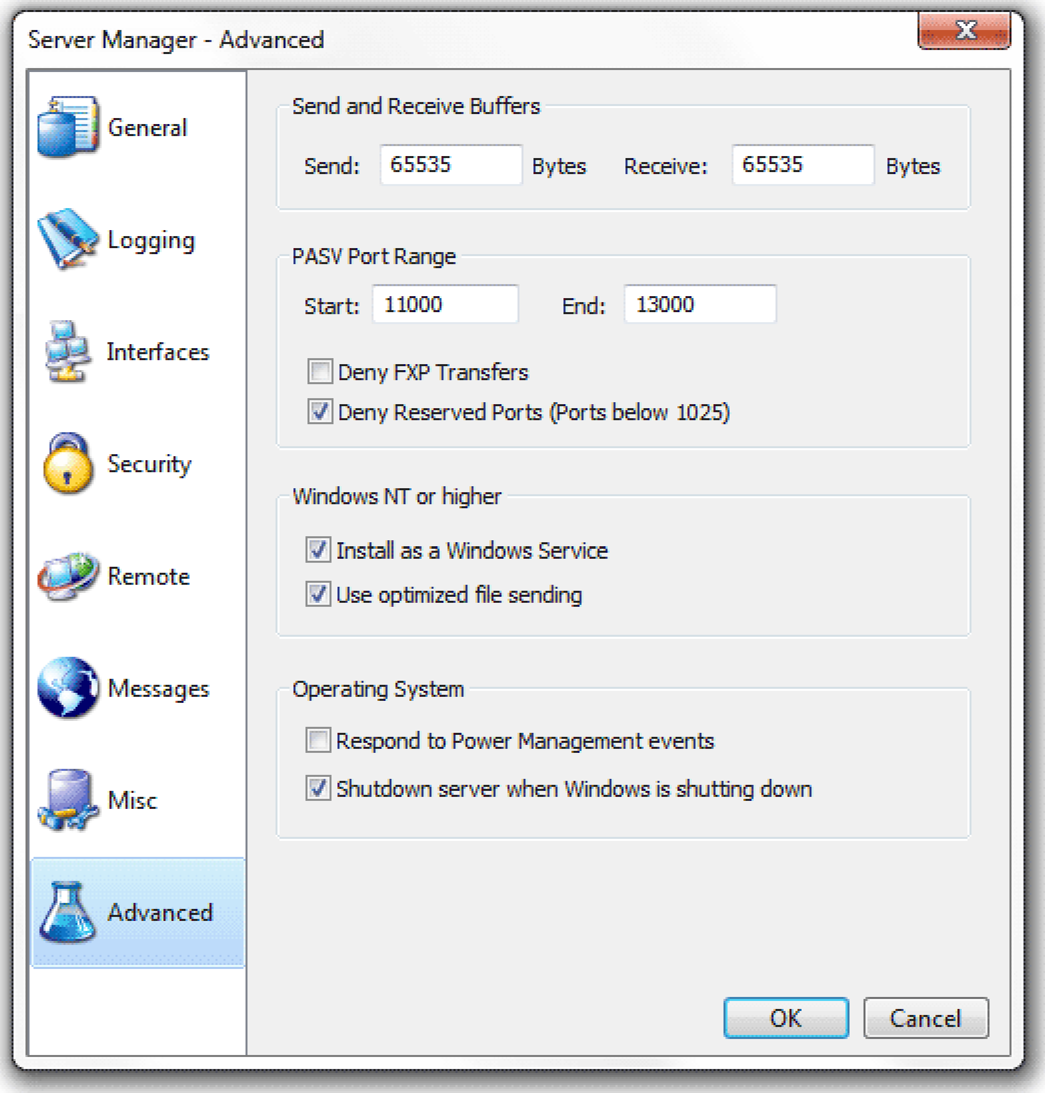
These are settings that don't fit anywhere else.

- **Suppress Startup Notification Bubble** - If checked, the tooltip bubble that is displayed with the Cerberus GUI will not be displayed when the GUI is first started.
- **Retrieve Owner/Group information for file listings** - Includes the owner and group of each file in responses to the LIST and NLST command. NOTE: This will slow down file listings.

ADVANCED SETTINGS

CONFIGURING ADVANCED SETTINGS

The advanced settings page contains options for passive mode, running as a Windows Service, network buffers, and power management.



Server Manager - Advanced

Send and Receive Buffers

Send: 65535 Bytes Receive: 65535 Bytes

PASV Port Range

Start: 11000 End: 13000

□ Deny FXP Transfers

☑ Deny Reserved Ports (Ports below 1025)

Windows NT or higher

☑ Install as a Windows Service

☑ Use optimized file sending

Operating System

□ Respond to Power Management events

☑ Shutdown server when Windows is shutting down

Figure 27 Advanced page of the Server Manager

SEND AND RECEIVE BUFFERS

These settings control the size of the buffers used for data transfers. Cerberus will read and write packets of this size for send and receive operations.

- **Send** - Number of bytes to send at once.
- **Receive** - Number of bytes to receive at once.

PASV PORT RANGE

These settings control passive FTP options.

- **Start** - First port in the port range to use for passive connections.
- **End** - Last port to use for passive connections before wrapping back around to the **Start** port.
- **Deny FXP Transfers** - File eXchange Protocol (FXP) is a method of data transfer which uses the FTP protocol to transfer data from one remote server to another (inter-server) without routing this data through the client's connection. Conventional FTP involves a single server and a single client; all data transmission is done between these two. In the FXP session, a client maintains a standard FTP connection to two servers, and can direct either server to connect to the other to initiate a data transfer.
- **Deny Reserved Ports** - Don't allow passive or active port requests below port 1024.

WINDOWS NT

These settings are only available on Windows NT and higher.

- **Install as a Windows Service** - If enabled, installs Cerberus FTP Server as a Windows Service. After selecting this option and pressing "Ok" to close the Server Manager the user may be prompted for an account with permissions to add a service to the system.
    - ***IMPORTANT:*** Remote access using SOAP must be enabled for the administrator to be able to access the GUI when running as a Windows Service. If you haven't already enabled Remote access then selecting INSTALL AS WINDOWS Service will automatically enable it and prompt you for a remote access password.
- **Use optimized file sending** - Uses the built-in Windows API for fast file sending.

OPERATING SYSTEM

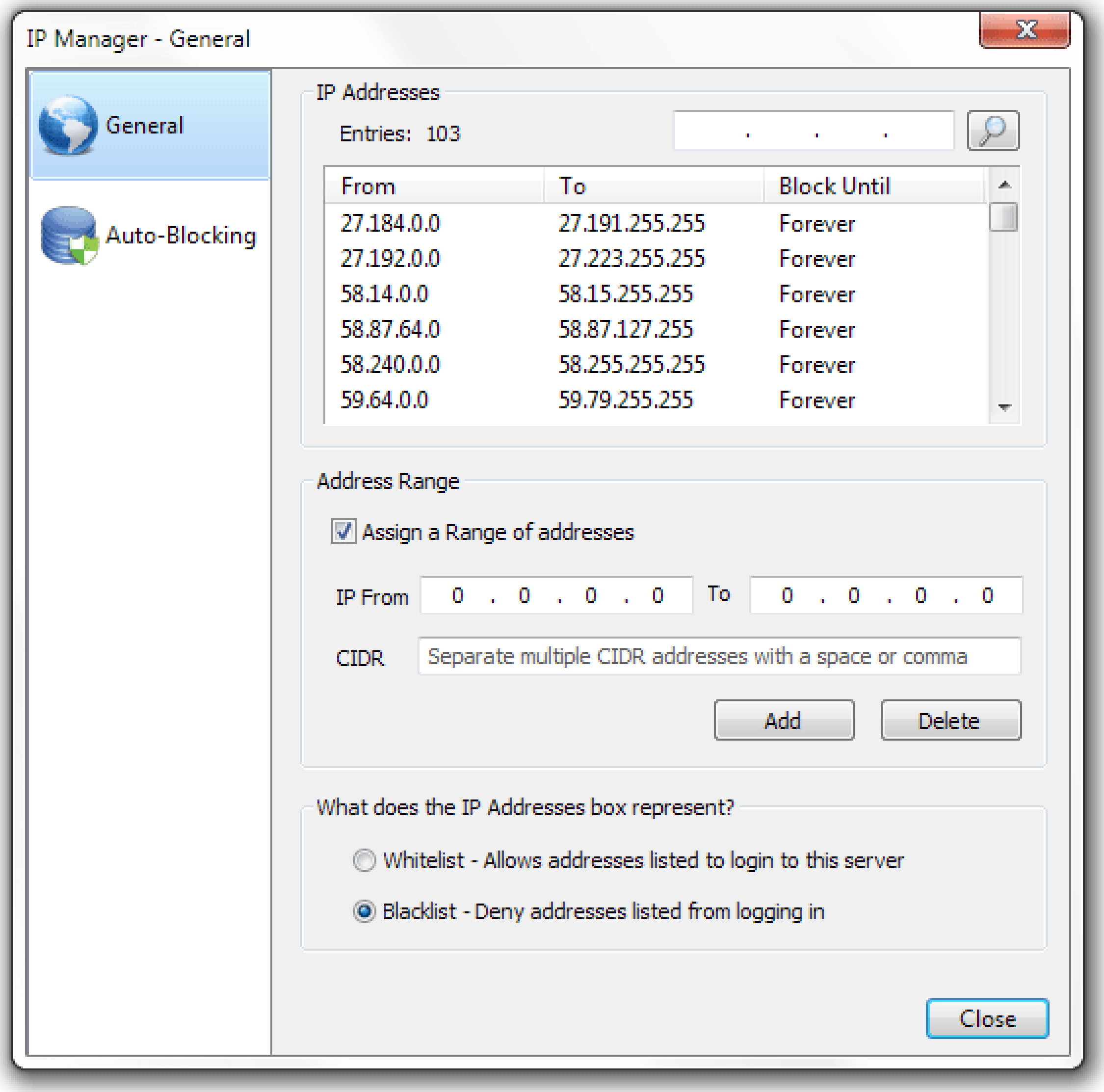
These settings control how the server responds to certain operating system events.

- **Respond to power management events** - If enabled, Cerberus will attempt to gracefully shutdown and startup in response to power suspend and resume events. May allow more graceful recovery from suspending and resuming the system.
- **Shutdown Server when Windows is shutting down** - Detects operating system shutdown or restarts and tries to gracefully terminate all connections and ensure all server settings are saved.

THE IP MANAGER

THE "GENERAL" PAGE

The Cerberus FTP Server IP Manager allows an administrator to selectively allow or deny access to the FTP server based upon IP address. The IP manager functions in one of two policy modes, either denying any IP addresses listed from logging into Cerberus FTP Server (functioning as a Blacklist), or only allowing IP addresses listed to log in (a Whitelist). The policy mode is controlled by a radio button at the bottom of the "General" tab page.



Entries: 103

From	To	Block Until
27.184.0.0	27.191.255.255	Forever
27.192.0.0	27.223.255.255	Forever
58.14.0.0	58.15.255.255	Forever
58.87.64.0	58.87.127.255	Forever
58.240.0.0	58.255.255.255	Forever
59.64.0.0	59.79.255.255	Forever

☑ Assign a Range of addresses

IP From 0 . 0 . 0 . 0 To 0 . 0 . 0 . 0

CIDR Separate multiple CIDR addresses with a space or comma

What does the IP Addresses box represent?

○ Whitelist - Allows addresses listed to login to this server

● Blacklist - Deny addresses listed from logging in

Figure 28 General page of the IP Manager

The IP list shows the IP address or IP address range and how long that address or address range is blocked for. Possible options for block time are "Forever" (Blacklist mode), "Never" (Whitelist mode), or a date/time value. If a date/time value is present, the IP address or IP address range is blocked from connecting until that date/time has elapsed (Blacklist or Whitelist mode). You can change how long an IP address entry is blocked for by right-clicking on that IP entry and selecting "Change Time" from the menu that appears.

ADDING A SINGLE IP ADDRESS TO THE IP MANAGER POLICY

IP addresses can be managed individually, or whole ranges of addresses can be affected by the current policy. To add a single address to the current policy, make sure the "Assign a range of addresses" check box is unselected. Then, enter the IP address you wish to add to the first IP address box. Finally, click the "Add" button immediately below the IP address box.

ADDING A RANGE OF IP ADDRESSES TO THE IP MANAGER POLICY

To add a range of addresses, first ensure the "Assign a range of addresses" check box is selected. Then, enter the beginning IP address in the "IP From" box and the ending IP address in the "IP To" box. The range will be interpreted as a contiguous range of addresses to block or allow. Finally, click the **Add** button immediately below the IP address box.

CIDR SUPPORT

You can also enter a range of IP addresses in CIDR notation using the CIDR edit box. You can enter one CIDR range or multiple CIDR ranges. To enter multiple CIDR ranges, separate each CIDR range with a space or comma. The CIDR address will be converted to a contiguous range and added to the IP Manager list.

DELETING A IP ADDRESSES FROM THE CURRENT POLICY

To delete either an IP address or range of IP addresses from the current policy, select the item from the "IP Addresses" list view box. Once selected, press the Delete button. You can also select and delete multiple items at once from the IP manager by ctrl or shift-clicking multiple items in the list box. NOTE: You can also delete an IP address or a range of IP addresses by right-clicking on the selected IP and selecting "Delete" from the menu that appears.

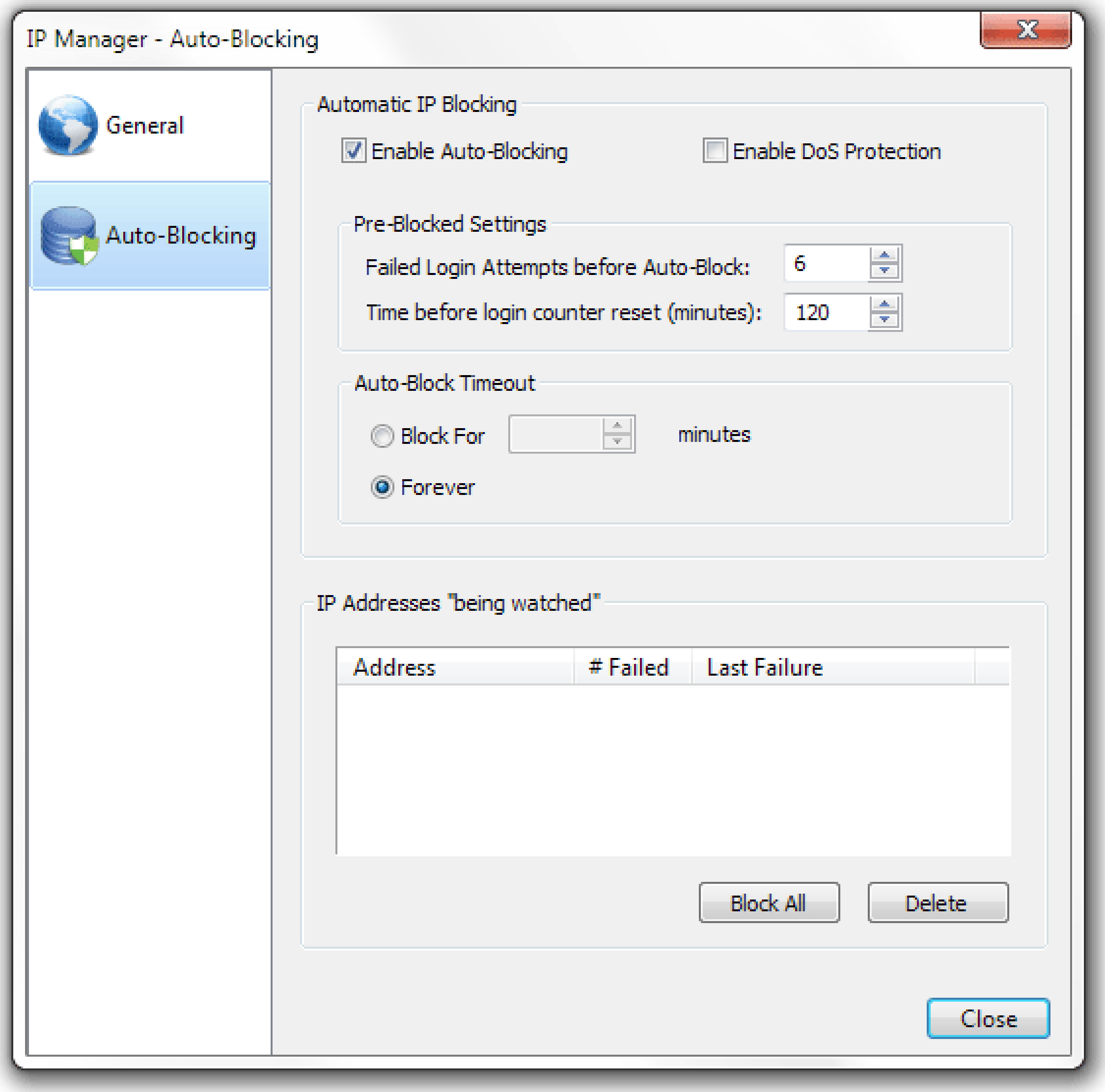
SEARCHING FOR AN IP ADDRESS

You can use the "Find" button at the top of the IP list box to search for an IP address in the list box. The "Find" button will select the first IP address or range of IP addresses containing the IP address you are searching for.

THE "AUTO-BLOCKING" PAGE

The other use for the IP manager is the ability to configure an auto-blocking policy for the FTP server. Administrators can use the auto-blocking policy to help prevent DoS (Denial of Service) and brute force password guessing. If the auto-blocking policy is enabled, a user that continually fails to log into the server will be blocked from trying after a certain number of failed attempts. The number of failed attempts and the length of time the IP address will be blocked from attempting to log in can be configured from the "Auto-Blocking" page.

When **Enable Auto-Blocking** is enabled a failed attempt is logged whenever a user enters an incorrect password or tries to login with an invalid username. If **Enable DoS Protection** is selected then any attempt to connect to the server will be counted towards auto-blocking, even if the connection doesn't attempt to authenticate. This can helpful in preventing DoS attacks that try to tie up connections and overwhelm the server. However, a successful login from an IP address resets the "Failed login attempts" counter to zero for the IP address.



Automatic IP Blocking

☑ Enable Auto-Blocking ☐ Enable DoS Protection

Pre-Blocked Settings

Failed Login Attempts before Auto-Block: 6

Time before login counter reset (minutes): 120

Auto-Block Timeout

○ Block For minutes

● Forever

IP Addresses "being watched"

Address	# Failed	Last Failure

Figure 29 Auto-blocking page of the IP Manager

The number of failed login attempts can be configured from the **Pre-Blocked Settings** frame. The **Time before login counter reset** edit control can be used to set the amount of time that must elapse before the **Failed login attempt** counter is reset.

The length of time an address is blocked can be configured using the **Auto-Block Timeout** setting. Select the Forever radio button to block a flagged IP address indefinitely, or select the "Block for X minutes" radio button to set the length of time the address is blocked. Once an address is blocked, the timeout period must elapse before the address is allowed to log in again.

IP addresses that have recently failed logins, but have not yet exceeded the **Failed login attempt** threshold, are displayed in the **IP Addresses being "watched"** list view. You can freely delete an address from the list view. Deleting the address has the effect of resetting the **Failed Login attempt** counter for that address to zero.

DIFFERENCES IN AUTO-BLOCKING BETWEEN BLACKLIST MODE AND WHITELIST MODE

How auto-blocking works differs depending upon whether the IP manager is functioning in Blacklist or Whitelist mode. If the IP manager is functioning as a Blacklist (denying addresses listed in the IP manager), then whenever a connection exceeds the failed login attempt threshold, that connection's IP address is added to the deny list.

Auto-blocking works differently for Whitelist mode (allowing only addresses listed to login to the server). In Whitelist mode, whenever a failed login attempt exceeds the failed login threshold, the IP address is either removed from the IP manager's list of allowed IP addresses (if auto-blocking is set to block failed logins forever) or blocked for the Auto-Block Timeout period. The exception is if the IP address is part of a range of IP addresses. If an IP address is part of a range of allowed IP addresses, that range is not deleted.

THE EVENT MANAGER

ABOUT EVENT RULES

Available in Cerberus FTP Server 5.0 Enterprise edition, the Event Manager allows an administrator to configure email notification, perform file operation or batch file actions, and carry out certain server operations based off of server events.

Event rules are based on the simple premise that an event occurs that triggers an action. There are several different rule types and for each rule type there is a corresponding event that can trigger that rule. For example, a File Transfer Event rule has a file upload or download event as an event trigger. You can further control if that even triggers the rule by specifying additional conditions that must exist before the rule's actions are taken.

For example, suppose you have a folder in which customers can drop files. You can set up an event rule that monitors that folder, and when someone uploads a file into that folder, moves it into another folder and then sends an e-mail to anyone you specify informing them that a file has been moved.

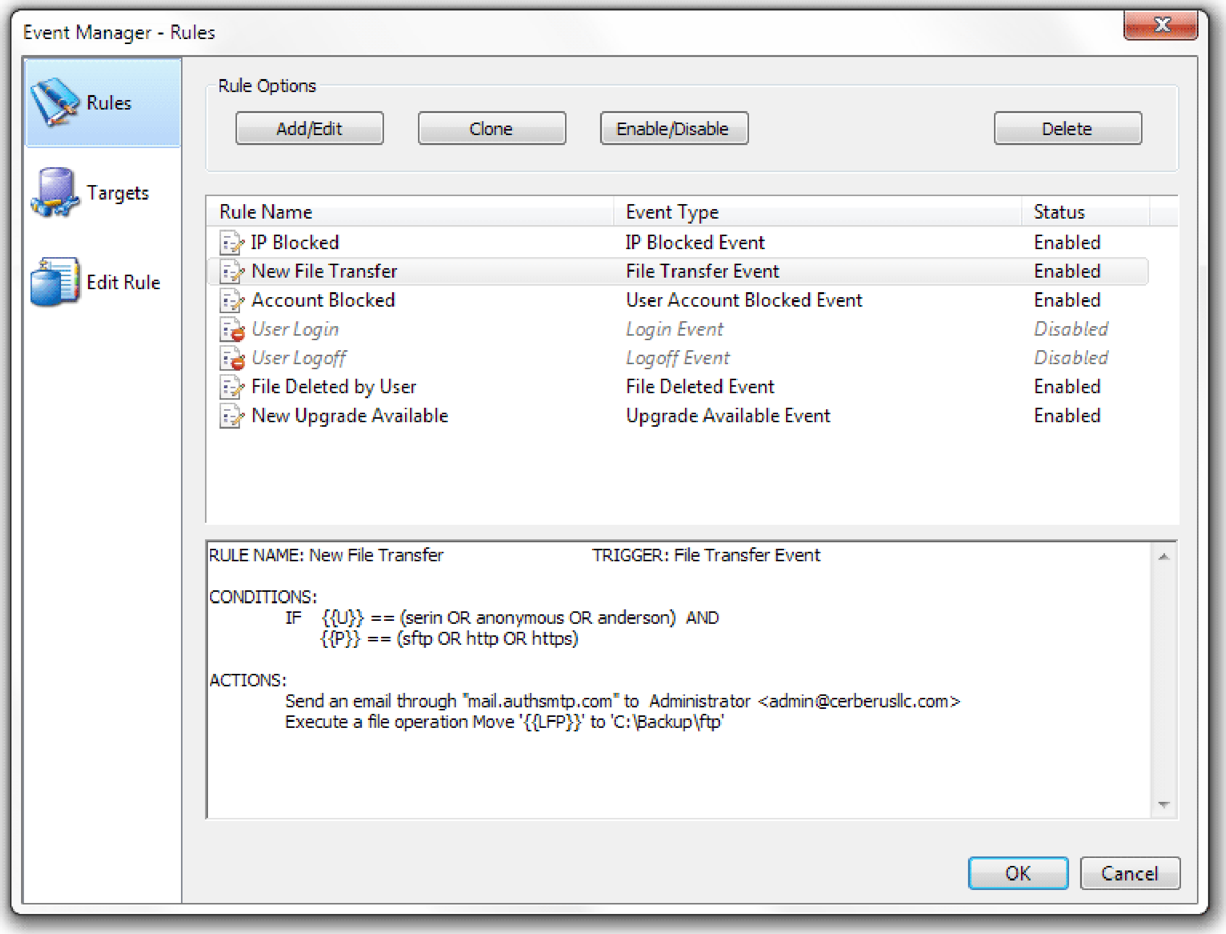
You can also set up a rule that only moves particular files. For example, you can configure the rule to move only the files that end in .zip, or you can route particular files to different folders.

An event rule consists of a triggering event, any optional conditions affecting that event, and the resulting actions that are carried out. You can modify your rules any time in the event manager.

THE RULES PAGE

The Rules page provides an overview of all of the rules you have added. From this page you can Add, Delete, Clone, or Enable and Disable a rule.

You can enable or disable a rule from this page. Whenever a rule is disabled, that rule is no longer checked whenever the system generates an event that would normally trigger the rule.



Rule Name	Event Type	Status
IP Blocked	IP Blocked Event	Enabled
New File Transfer	File Transfer Event	Enabled
Account Blocked	User Account Blocked Event	Enabled
User Login	*Login Event*	*Disabled*
User Logoff	*Logoff Event*	*Disabled*
File Deleted by User	File Deleted Event	Enabled
New Upgrade Available	Upgrade Available Event	Enabled

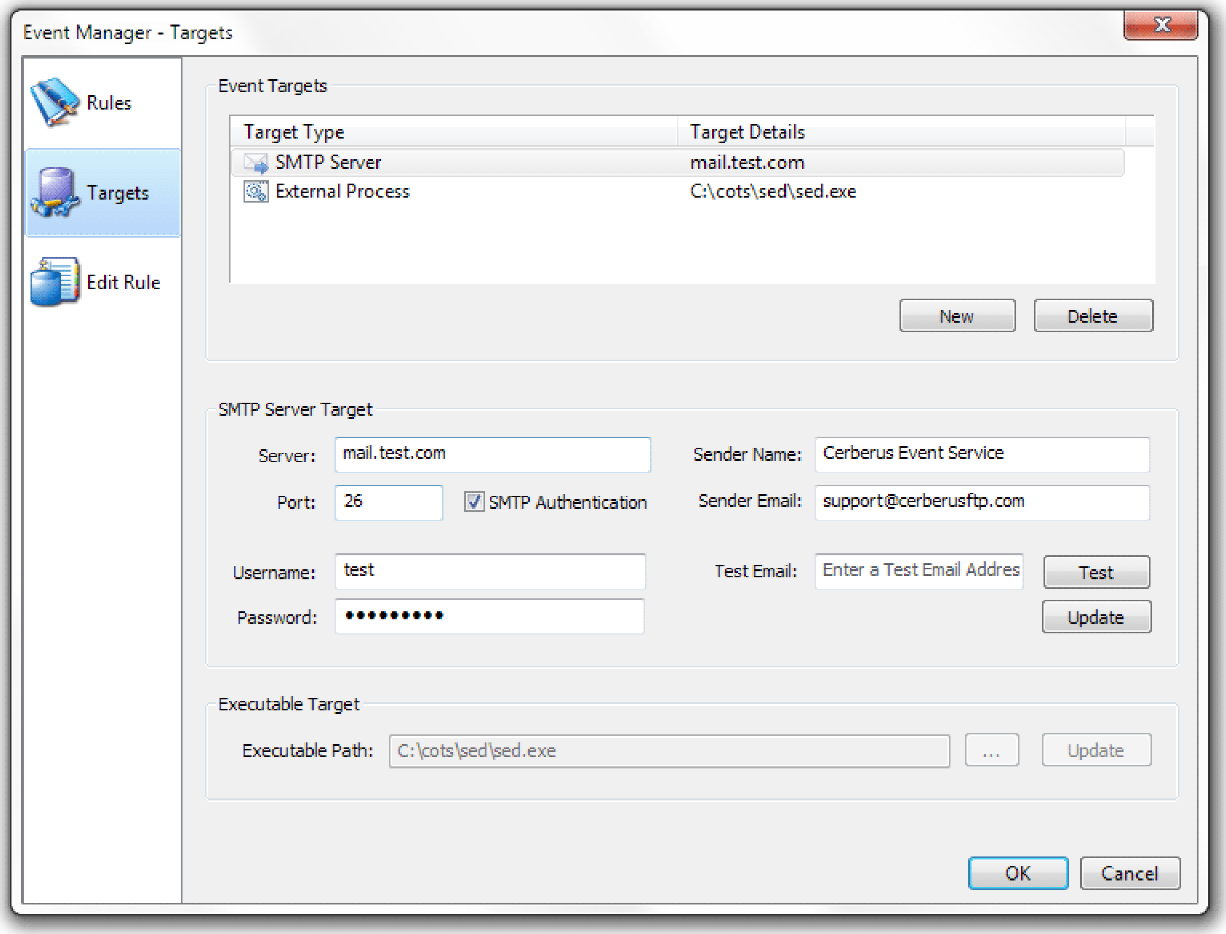
```
RULE NAME: New File Transfer                    TRIGGER: File Transfer Event

CONDITIONS:
         IF    {{U}} == (serin OR anonymous OR anderson)  AND
               {{P}} == (sftp OR http OR https)

ACTIONS:
         Send an email through "mail.authsmtp.com" to  Administrator <admin@cerberusllc.com>
         Execute a file operation Move '{{LFP}}' to 'C:\Backup\ftp'
```

Figure 30 Rules List page of the Event Manager

When you select a rule from the Rules list you see a summary of the rule's conditions and actions in the summary edit box.

THE TARGETS PAGE

The Rule Targets page allows an administrator to add email servers and executable files as event targets. Before an email server or executable file can be selected as an action in an event rule, the SMTP server or file path has to first be added to the targets list.



Event Targets

Target Type	Target Details
SMTP Server	mail.test.com
External Process	C:\cots\sed\sed.exe

SMTP Server Target

Server: mail.test.com

Port: 26 ☑ SMTP Authentication

Username: test

Password: •••••••••

Sender Name: Cerberus Event Service

Sender Email: support@cerberusftp.com

Test Email: Enter a Test Email Addres

Executable Target

Executable Path: C:\cots\sed\sed.exe

Figure 31 The Event Target page of the Event Manager

Rules can be associated with the SMTP and executable files and when an SMTP server or executable file path is updated here, all rules that use that target will automatically be updated to reflect the new settings.

SMTP SERVER TARGETS

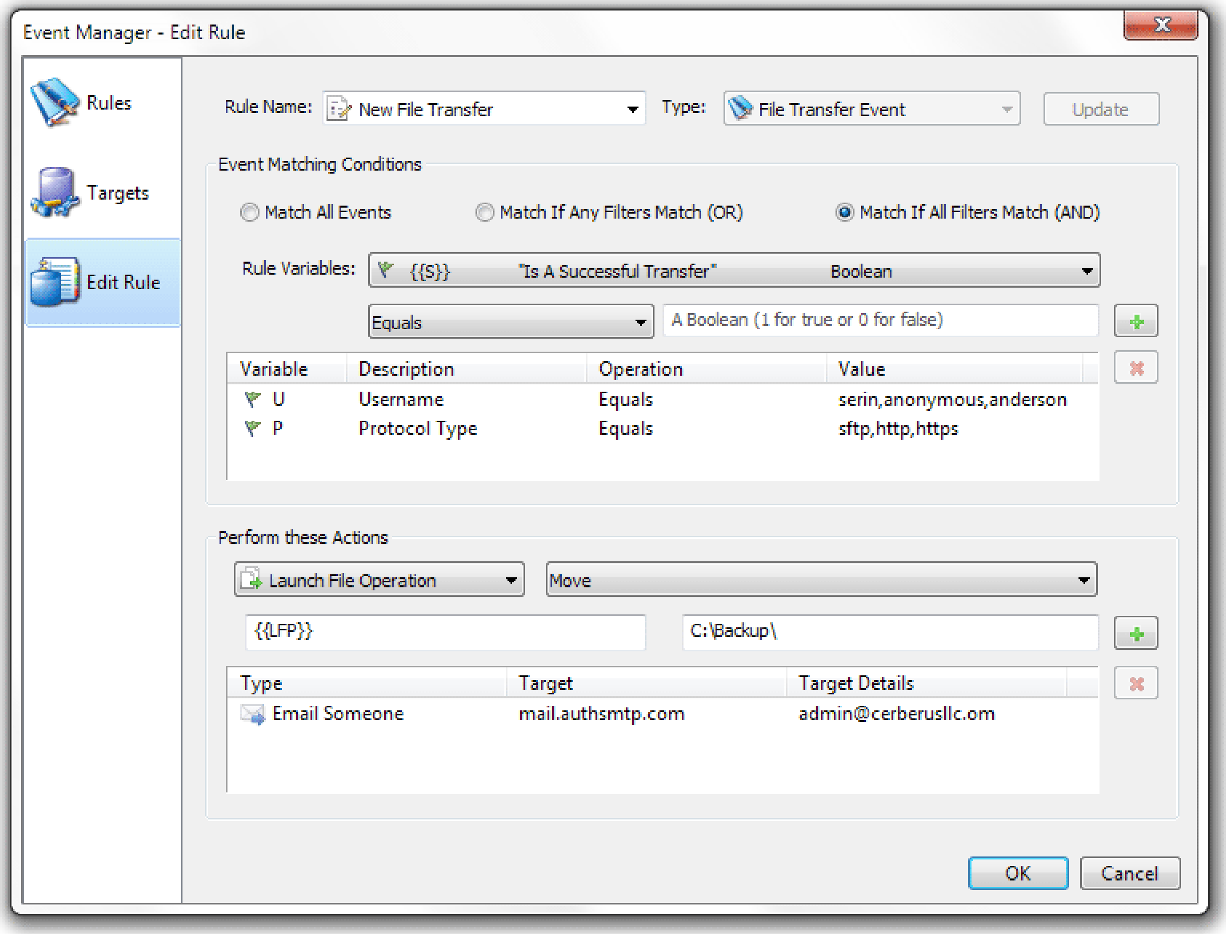
You can add SMTP servers using the SMTP Server Target box. Cerberus currently supports the SMTP protocol, including SMTP with SSL encryption and STARTTLS. If your server requires it, SMTP server credentials can be configured by selecting the **SMTP Authentication** checkbox.

EXECUTABLE TARGETS

Cerberus can be configured to launch an .exe, .bat, or .com file as an action for any event. Just select a file path and press the "Add" button to make an executable target available for selection when adding and editing rules. Command line options for the executable are specified on a per action basis from the rule editing page.

THE EDIT RULE PAGE

Rule creation and editing is done using the Edit Rule page.



Event Manager - Edit Rule

Rule Name: New File Transfer

Type: File Transfer Event

Event Matching Conditions

○ Match All Events ○ Match If Any Filters Match (OR) ● Match If All Filters Match (AND)

Rule Variables: {{S}} "Is A Successful Transfer" Boolean

Equals

A Boolean (1 for true or 0 for false)

Variable	Description	Operation	Value
U	Username	Equals	serin,anonymous,anderson
P	Protocol Type	Equals	sftp,http,https

Perform these Actions

Launch File Operation

Move

{{LFP}}

C:\Backup\

Type	Target	Target Details
Email Someone	mail.authsmtp.com	admin@cerberusllc.om

Figure 32 Rule Editing in the Event Manager

AVAILABLE EVENT RULE TYPES

A rule is defined by the type of event that triggers it. Each rule has a single event type associated with it. When that event occurs, any rules associated with that event type are triggered. The following rule event types are available:

- File Transfer Event
- IP Blocked Event
- User Account Blocked Event
- User Disable Date Elapsed
- New Account Request Event
- Login Event
- Logoff Event
- File Deleted Event
- File Move/Copy Event
- Upgrade Available Event

ADDING NEW RULE OR EDITTING AN EXISTING RULE

To add a **new** rule:

1. Open the Rule Name combo box.
2. Select the New Rule option. Type a name in the combo box for your new rule. The Event Type combo box should become enabled.
3. From the event Type combo box, select the event type you wish to trigger this rule.
4. Press the Add button to add the new rule.

To add edit an **existing** rule:

1. Open the Rule Name combo box.
2. Select the name of the existing rule you wish to edit. The Event Matching Conditions and Perform these Actions sections should become enabled.

ADDING RULE CONDITIONS

A rule's actions are carried out whenever that rule's event trigger happens. For example, a Login Event rule will be triggered whenever a user logs into the server. Conditions (also called filters) can be placed on rules to further modify if an event matches a rule. For example, a Login Event rule can have a filter placed on it that requires the username of the user logging in to match a specific name or be in a list of names before the rule's actions are invoked. There are three modes that influence how conditions or filters are applied.

RULE MATCHING MODES

The three rule matching modes are:

- **Match All Events** - This rule will always be triggered whenever the rule's event occurs.
- **Match If Any Filters Match** - This rule will be triggered whenever the rule's event occurs and if **any** of the conditions listed are fulfilled
- **Match If All Filters Match** - This rule will only be triggered whenever the rule's event occurs and if **all** of the conditions listed are fulfilled

RULE VARIABLES

Each event type has specific variables that can be used as part of a condition or action. A rule condition consists of a variable, a comparison operation to perform on that variable, and a set of values to compare the variable to. For example, an IP Blocked event has an **{{IP}}** variable associated with it that contains the IP address that was blocked. You can use the variable in a condition to help decide if the event should trigger the rule.

You can determine what rule variables are available for each event type by looking in the **Rule Variables** combo box.

CONDITION OPERATIONS

A condition is basically a comparison operation of an event variable to a set of values. The comparison operations you can perform are detailed below:

- > (Greater than or Equal To)
- ≥ (Greater than)
- < (Less than)
- ≤ (Less than or Equal To)
- = (Equal To)
- != (Not Equal To)
- Contains
- Starts with
- Ends with
- Regular Express match

Once a comparison operation is selected, you can enter the values to compare to in the edit box to the right of the comparison combo box. Multiple values can be entered by separating the values with a comma. Each value is checked and if any are a match then the condition is considered fulfilled (or true).

ADDING RULE ACTIONS

When an event matches all of the conditions of a rule then the rule actions are carried out. The current rule actions allow an administrator to:

- Send an email message
- Launch an external process
- Perform a file copy, move, delete or directory create or delete operation

Each action can have optional parameters such as the email name and address to send a message to, or the path from and path to for a file move or copy operation. In addition, rule variables can be specified as parameters for the external processes command line or file operation parameters. You can use a rule variable as a parameter and when the rule is actually triggered, the variable's value will be substituted for the variable. You specify variables by enclosing the variable in double brackets, i.e. **{{U}}**.

LDAP AUTHENTICATION

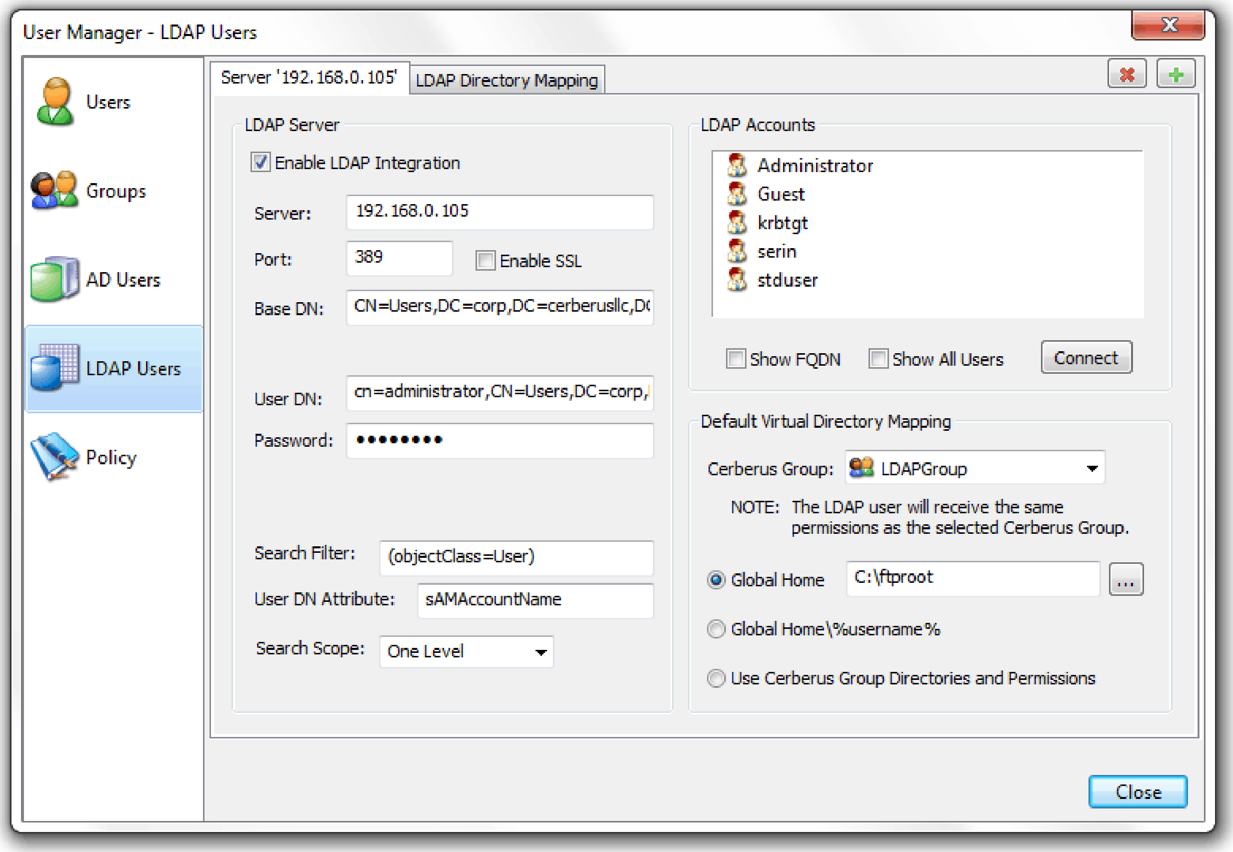
Cerberus FTP Server Professional is able to authenticate users against LDAP directory services. The **Lightweight Directory Access Protocol**, or **LDAP**, is an application protocol for querying and modifying directory services running over TCP/IP.

Administrators can easily integrate Cerberus and LDAP or LDAPS (Secure LDAP). All you need are a few parameters describing the LDAP service.

WHAT DO I NEED TO USE LDAP AUTHENTICATION?

An LDAP service and some information about the server hosting the LDAP service:

Server	This parameter is the FQDN or IP address of the LDAP server to search.
Port	The network port of the LDAP server.
Enable SSL	This checkbox determines whether the connection to the LDAP server is encrypted. The LDAP server must support encryption for this to work. Port 389 is the default port for unencrypted LDAP and port 636 is the default LDAPS port.
Base DN	The distinguished name to use as the search base.
User DN	The FDN of an account with read privileges to the LDAP server.
Password	The password for the User DN account. This password is encrypted when saved.
User DN attribute	The name of the uid attribute for a user in the directory.



User Manager - LDAP Users

LDAP Server

☑ Enable LDAP Integration

Server: 192.168.0.105

Port: 389 □ Enable SSL

Base DN: CN=Users,DC=corp,DC=cerberusllc,D(

User DN: cn=administrator,CN=Users,DC=corp,

Password: ••••••••

Search Filter: (objectClass=User)

User DN Attribute: sAMAccountName

Search Scope: One Level

LDAP Accounts

- Administrator
- Guest
- krbtgt
- serin
- stduser

□ Show FQDN □ Show All Users

Default Virtual Directory Mapping

Cerberus Group: LDAPGroup

NOTE: The LDAP user will receive the same permissions as the selected Cerberus Group.

● Global Home C:\ftproot

○ Global Home\%username%

○ Use Cerberus Group Directories and Permissions

Figure 33 Configuration page for LDAP Authentication

OTHER LDAP DIALOG OPTIONS

The LDAP Accounts list box that enumerates LDAP accounts is only meant as an aid in determining if your LDAP connection is configured correctly. If you can get a successful listing of user accounts then those accounts should be accessible to Cerberus during authentication. Some additional display options are detailed below:

Show FQDN	Display the fully qualified domain name of each enumerated object. **Note:**This setting has no effect on actual LDAP authentication.
Show All Users	If this option is checked, every account will be retrieved and enumerated in the LDAP Accounts list box. This can take a very long time if there are a large number of users. **Note:** This setting has no effect on actual LDAP authentication.

SETTING UP ACTIVE DIRECTORY AUTHENTICATION

The following steps detail the procedure for enabling LDAP Authentication to verify credentials against Active Directory. The steps are similar for connecting to other LDAP servers, such as OpenLDAP or ApacheDS.

1. Change the LDAP Server and Port attribute in the User Manager, LDAP Users tab to the host name and port number of the Active Directory:

   - e.g., Server: hostname.domain.com or 192.168.0.100
   - Port: 389

2. Change the Base DN to the proper base for the Active Directory.

   Simply specifying the base suffix will not work in this attribute. For Active Directory, it would usually be the cn=Users plus suffixes e.g.: for domain corp.cerberusllc.com

   CN=Users,DC=corp,DC=cerberusllc,DC=com

   or

   CN=Users,DC=corp,DC=cerberusllc,DC=local

3. Change the DN for the User DN bind attribute to a user with the right to read the Active Directory.

   Anonymous access to the Active Directory is not allowed, so a bind account is needed. It is simply an account for Active Directory that has read ability on the attribute to which the user will authenticate. An example might be **cn=administrator,CN=Users,DC=corp,DC=cerberusllc,DC=local**. Enter the password for the user account.

4. Change the User Naming Attribute.

   This attribute is the one that the LDAP module will search for in Active Directory and attempt to match against the supplied FTP username. It is often the UID attribute on many LDAP servers. For example, if users login using their Common Name, the value of this attribute would be CN. For Active Directory, the login name is usually mapped to **sAMAccountName**, as it is the attribute in Active Directory most like UID. For Active Directory, it is usually best to specify **sAMAccountName**, as it is the attribute in Active Directory most like UID.

5. Change the User Entry Search Filter.

   This string is an LDAP search string used to locate and filter the account in Active Directory. It should correspond to the attribute with which people use to log in.

   e.g., **(objectClass=User)**

   The above filter will include on search entities that have the object class **User**. DO NOT attempt to add the uid search attribute here. Cerberus will automatically append an attribute filter to select the correct account based on the User Naming Attribute.

I.e., if the User Naming Attribute is sAMAccountName, Cerberus will automatically create a string like

(&(objectClass=User)(sAMAccountName=FTPUSER)

where FTPUSER is the name of the user that attempted login.

6. Set the search scope.

   This setting controls how deep into the directory to search for users. This setting combined with the Base DN and Search Filter determines which users are matched for authentication.

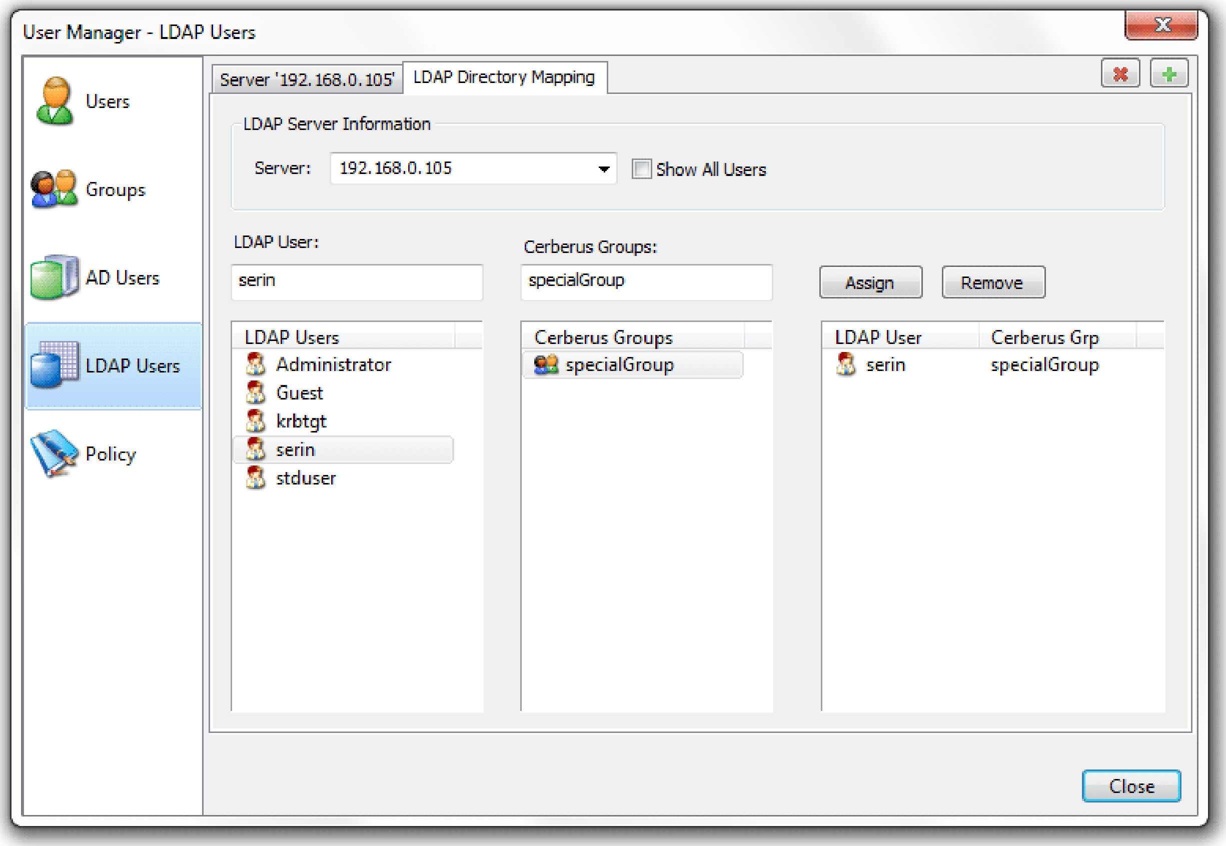
   One Level is usually the best setting for typical Active Directory configurations.

7. Verify that the settings are correct by clicking the "Test Connection" button. You should see the user DNs from Active Directory that are able to log in to Cerberus FTP Server.
8. Select a Cerberus FTP Group to represent the virtual directories and permissions for LDAP users. Note that the **isAnonymous** and **isDisabled** setting on the group are ignored.

Cerberus FTP Server is now configured for authentication against an LDAP server (Active Directory, in this case).

LDAP USER MAPPING

If you wish to customize the directory and permission mappings for individual LDAP users then you can do so through the LDAP Directory Mapping tab. You can select individual LDAP accounts and map them to Cerberus group accounts. This mapping will override the default Cerberus Group and directory mapping specified for all LDAP users on the LDAP server page.



Server: 192.168.0.105 ☐ Show All Users

LDAP User: serin

Cerberus Groups: specialGroup

LDAP Users
Administrator
Guest
krbtgt
serin
stduser

Cerberus Groups
specialGroup

LDAP User	Cerberus Grp
serin	specialGroup

Figure 34 Configuration page for LDAP User to Cerberus Group Mapping

CREATING AN LDAP USER TO CERBERUS GROUP MAPPING

Mappings between an LDAP User and a Cerberus Group can be achieved by selecting an LDAP user (or simply typing the name of the LDAP user in the edit box) and then selecting a Cerberus Group. Select the Assign button and a mapping entry will be placed in the mapping list box to indicate the LDAP user will now have the same constraints and virtual directory mappings as the selected Cerberus Group.

REMOVING AN LDAP MAPPING

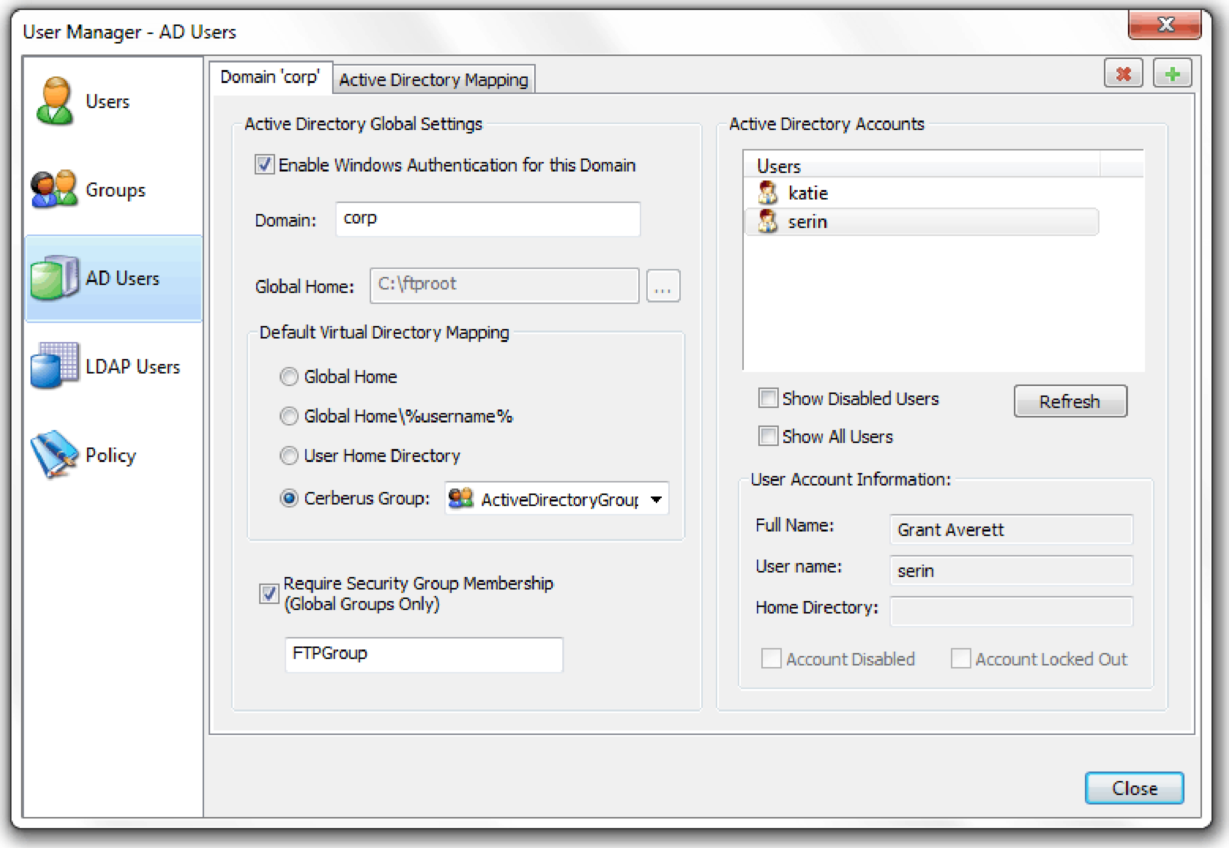
To remove a mapping, simply select the mapped entry and press the Remove button.

ACTIVE DIRECTORY AUTHENTICATION

ABOUT ACTIVE DIRECTORY INTEGRATION

Cerberus FTP Server Professional and Enterprise editions are able to authenticate users on an NT domain (or the local NT account database), even if the computer Cerberus FTP Server is installed on is not the domain controller. The domain may be a pre-Windows 2000 domain (NT4), a domain configured to use Active Directory, or the local system account database (use "." as the domain for authenticating against local machine accounts). However, the machine Cerberus FTP Server is running on must be a member of the domain you wish to authenticate users against.

Configuring Cerberus to use Active Directory authentication simply requires enabling Active Directory authentication and telling the server the name of the domain to authenticate against. The rest of the configuration is automatic. Users are able to FTP into the server using the same username and password they use to log into their workstations on the domain. For the purpose of access to files and folders, the FTP user has the same access as the Active Directory user with the same name. All operations on the server by the user are carried out while impersonating the Active Directory user.



Active Directory Global Settings

☑ Enable Windows Authentication for this Domain

Domain: corp

Global Home: C:\ftproot

Default Virtual Directory Mapping

○ Global Home

○ Global Home\%username%

○ User Home Directory

● Cerberus Group: ActiveDirectoryGrouj

☑ Require Security Group Membership (Global Groups Only)

FTPGroup

Active Directory Accounts

Users
- katie
- serin

□ Show Disabled Users

□ Show All Users

User Account Information:

Full Name: Grant Averett

User name: serin

Home Directory:

□ Account Disabled □ Account Locked Out

Figure 35 Active Directory Authentication page

Important Security Consideration: There is an exception to impersonation for Active Directory authentication when using SFTP and only **Public Key only** SSH authentication. The Active Directory user can still be authenticated with Public Key only authentication but the Active Directory user cannot be impersonated. Only **Password** or **Public Key and Password** SSH authentication methods support AD user impersonation.

To allow Active Directory authentication, you will need to check the **Enable Windows Authentication for this Domain** checkbox under the User Manager's **AD Users** tab. Once checked, Cerberus will attempt to authenticate users from the domain listed in the Domain edit box.

Active Directory accounts are always configured for simple directory mode (See Adding users for more information about simple mode) if any mode other than "Cerberus Group" is selected for the Default Virtual Directory Mapping mode.

The Default Virtual Directory Mapping modes work as follows:

Global Home	Every NT account will use the directory specified under the "Global Home" edit box as the FTP root, the user's home directory, or a subdirectory off of a common root directory that is the same as the user's name.
Global Home\%username%	Every NT account will use a subdirectory off of the "Global Home" directory that is the same as the account's name.
User Home Directory	Every NT account will use that account's home directory as the FTP root.
Cerberus Group	The specified Cerberus Group will be used to determine what directories and what settings to apply to the Active Directory user when they login, including any security requirements associated with the group.

ACTIVE DIRECTORY FTP SECURITY GROUP

Optionally, you can also configure a Security Group for FTP users. This will cause Cerberus FTP Server to check that the Active Directory user is a member of the listed Active Directory Global security group before allowing login. If selected, only members of the security group will be allowed to login.

AUTHENTICATING AGAINST MORE THAN ONE ACTIVE DIRECTORY DOMAIN

Cerberus FTP Server can be configured to authenticate against multiple domains. Select the **AD Users** page of the User Manager and select the ✚ icon in the top right corner. This will add a new domain tab to the AD User page. This new domain tab can be configured the same way as the default Active Directory domain tab.

UNDERSTANDING WINDOWS AUTHENTICATION

Active Directory user authentication is intended for experienced system administrators that understand the NT security model. Novice users, or users wishing to avoid the details of Windows security, should leave Windows Authentication disabled and stick with native Cerberus FTP Server users.

Note: The Cerberus FTP Server account database is always checked for a user before the NT account database is checked. If there is user with the same name in both databases, the Cerberus FTP Server user will be the only one authenticated against. To ensure that the NT user is checked, delete the Cerberus user.

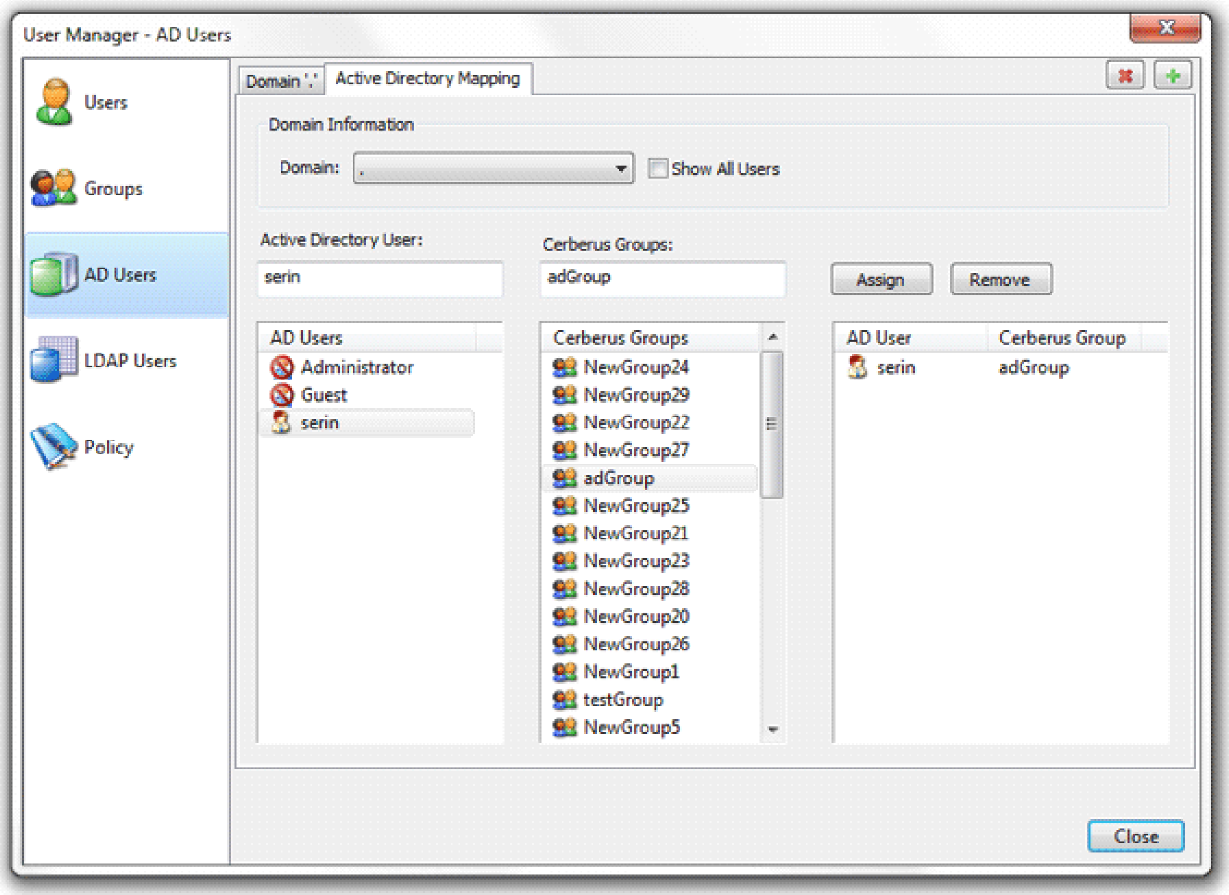
THE "GUEST" ACCOUNT

In NT, the **Guest** account lets people log on to an NT computer when they don't have a personal account defined on the computer, in the computer's domain, or in any of the domains that the computer's domain trusts. Like the Administrator account, the **Guest** account is a built-in account with a fixed SID; although you can rename the account, it can't--by default--be deleted. Unlike the Administrator account, the **Guest** account doesn't require a password for logon, which is why it's disabled by default. A **Guest** account re-enabled by mistake would pose a significant security hole.

To help guards against this potential security hole, an administrator cannot enable Cerberus FTP Server's Windows authentication integration if the **Guest** account is enabled.

ACTIVE DIRECTORY USER TO CERBERUS GROUP MAPPING

By default, all AD users are assigned the same virtual directories and permissions. These defaults are configured on the Domain tab of the AD Users page. However, if you wish to customize the directory and permission mappings for individual AD users then you can do so through the **AD Directory Mapping** tab. You can select individual AD accounts and map them to Cerberus group accounts. This mapping will override the default Cerberus Group and directory mapping specified for all AD users on the AD Users page.



Domain: .

☐ Show All Users

Active Directory User: serin

Cerberus Groups: adGroup

AD Users
Administrator
Guest
serin

Cerberus Groups
NewGroup24
NewGroup29
NewGroup22
NewGroup27
adGroup
NewGroup25
NewGroup21
NewGroup23
NewGroup28
NewGroup20
NewGroup26
NewGroup1
testGroup
NewGroup5

AD User	Cerberus Group
serin	adGroup

Figure 36 Configuration page for AD User to Cerberus Group Mapping

CREATING AN AD USER TO CERBERUS GROUP MAPPING

Mappings between an AD User and a Cerberus Group can be achieved by first selecting an AD domain. Then, select an AD user from the AD Users list box (or simply type the name of the AD user in the edit box) and then select a Cerberus Group. Select the **Assign** button and a mapping entry will be placed in the mapping list box to indicate the AD user will now have the same constraints and virtual directory mappings as the selected Cerberus Group.

REMOVING AN AD MAPPING

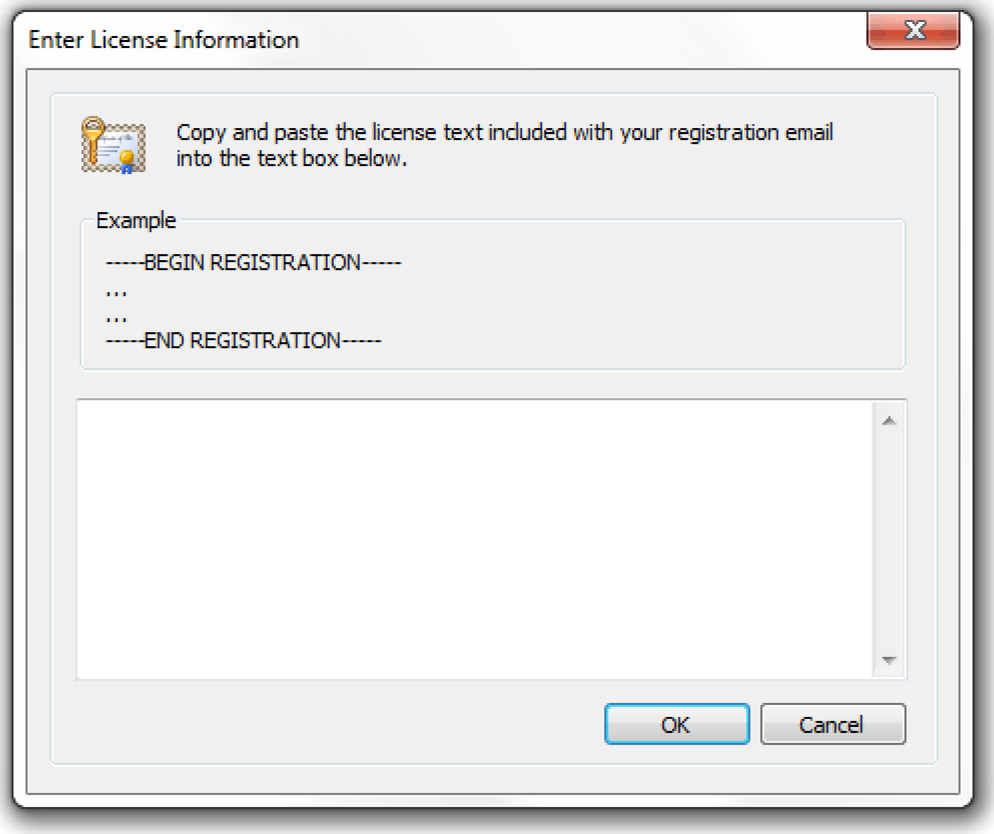
To remove a mapping, simply select the mapped entry and press the **Remove** button.

ENTERING A LICENSE FOR CERBERUS FTP SERVER

THE REGISTRATION DIALOG BOX

Using Cerberus FTP Server for commercial use past the 25 day evaluation period requires a license key. Once you have purchased and received a license key, you need to enter the license key details in the registration dialog box.

To open the registration dialog box, go to the **Help** menu and select the **Enter License Data...** menu item. A box similar to the one below will prompt you to enter your registration code. Open your license email and copy everything starting at and including "-----BEGIN REGISTRATION-----" all the way until and including "-----END REGISTRATION-----". Paste the copied text into the large edit box.



Copy and paste the license text included with your registration email into the text box below.

Example

```
-----BEGIN REGISTRATION-----
...
...
-----END REGISTRATION-----
```

Figure 37 License registration dialog box

Press the OK button. Another dialog box will appear, after you press enter, to inform you of correct or incorrect registration information. Please note that a service restart is required after entering a new license key. Cerberus will prompt you to restart after successfully entering a new license key.

Once you have successfully registered Cerberus FTP Server, the "About" dialog box will display the registration contact name, company name, purchase date, and for how long the license entitles the user to free upgrades.

WEB SERVICES CONTROL

AVAILABLE FEATURES

Programmers can now access most of Cerberus FTP Server's common functions through a new Web Services interface. These services use SOAP 1.2 over HTTP or HTTPS and do not require a separate HTTP server. Cerberus FTP Server's implementation of Web Services includes a built-in, lightweight HTTP stack.

The following functionality is available through the Web Services API:

- Listing the current Cerberus FTP Server user and group accounts
- Adding new users or groups and modifying existing users and groups
- Deleting users or groups
- Retrieving user or group information
- Adding new virtual directories or modifying existing directories for a given user or group
- Deleting a virtual directory for a given user or group
- Getting the server's current started or stopped status
- Stopping or Starting the server
- Retrieving server statistics
- Retrieving and modifying interface details
- List, terminating, and blocking active connections
- Retrieving and saving configuration information

Refer to the included Ceberus.wsdl file for specifics on the Web Services interface to these functions. You can view an example Cerberus.wsdl online here. Always refer to the actual WSDL included with the Cerberus distribution you are using for the latest definitions.

There is an example .NET project available here: NetSoapClient.zip

ACCESS URL

Make sure you enable SOAP access from the Remote settings page on the Server Manager. You can access the SOAP service WSDL on your local machine at the URL http://localhost:10000/wsdl/Cerberus.wsdl.

Make sure you have **Enable Web Administration** selected to view the actual WSDL. If Web Administration is not enabled you will still be able to use the WSDL to develop SOAP services but you won't be able to use the built-in web server to view the WSDL using the URL link. The WSDL is located in the installation directory where Cerberus is installed.

SECURITY CONSIDERATIONS

By default, Cerberus FTP Server's Web Services access is turned off. Before allowing Web Services access to Cerberus FTP Server, you should be well aware of the security implication that this entails. While it is the user's responsibility to be knowledgeable of Web Services and the risks associated with using them, here are some reminders:

- Make sure the port you are running the Web service on is properly locked down. If you are only using Web Services to communicate between programs on the same machine, the port Cerberus is running the Web Services on shouldn't be accessible from outside of the local machine.
- When using Web Services, remember that anyone with access to the port that the Web Services is running on can send service requests to Cerberus FTP Server. This can represent a serious security risk. Make sure you set a strong Remote access password.
- HTTP, the backbone of Cerberus FTP Server's Web Services, transmits information as unencrypted text. Anything you send over HTTP has the potential to be intercepted and read. Cerberus also has the option of using SSL/TLS support for Web Services over HTTPS. Using HTTPS instead of HTTP significantly increased the security of any data transmitted.

Cerberus FTP Server uses the gSOAP toolkit to implement Web Services. You can find out more about gSOAP at the gSOAP home page.

COMMAND SUPPORT

FTP COMMANDS SUPPORTED

The following FTP commands are supported by Cerberus FTP Server:

- ABOR
- ACCT
- ADAT
- ALLO
- APPE
- AUTH
- CCC
- CDUP
- CLNT
- CSID
- CWD
- DELE
- EPSV
- EPRT
- FEAT
- HASH
- HELP
- LANG
- LIST
- MDTM
- MFMT
- MFCT
- MKD
- MODE
- MLSD
- MLST
- MLSD
- NLST
- NOOP
- OPTS
- P@SV
- PASS
- PASV
- PBSZ
- PWD
- PORT

- PROT
- QUIT
- REIN
- RETR
- REST
- RMD
- RMDA
- RNFR
- RNFT
- SITE
- SIZE
- STOR
- STOU
- STRU
- SYST
- TYPE
- USER
- XCRC
- XCUP
- XPWD
- XMD5
- XMKD
- XSHA1
- XSHA256
- XSHA512
- XRMD