SOLARWINDS

Serv-U File Server
Administrator Guide

solarwinds

Unexpected Simplicity

Last revised: 5/28/2014

Chapter 3: Server 39

Serv-U File Server Administrator Guide

About SolarWinds

SolarWinds, Inc develops and markets an array of network management, monitoring, and discovery tools to meet the diverse requirements of today’s network management and consulting professionals. SolarWinds products continue to set benchmarks for quality and performance and have positioned the company as the leader in network management and discovery technology. The SolarWinds customer base includes over 45 percent of the Fortune 500 and customers from over 90 countries. Our global business partner distributor network exceeds 100 distributors and resellers.

Conventions

The documentation uses consistent conventions to help you identify items throughout the printed and online library.

Convention	Specifying
Bold	Window items, including buttons and fields
Italics	Book and CD titles, variable names, new terms
`Fixed font`	File and directory names, commands and code examples, text typed by you
Straight brackets, as in [value]	Optional command parameters
Curly braces, as in {value}	Required command parameters

Logical OR, as in value1|value2	Exclusive command parameters where only one of the options can be specified

Serv-U Documentation Library

The following documents are included in the SolarWinds Virtualization Manager documentation library:

Document	Purpose
Administrator Guide	Provides detailed setup, configuration, and conceptual information.
Release Notes	Provides late-breaking information, known issues, and updates. The latest Release Notes can be found at http://www.solarwinds.com.

Technical Support

Have a question and need more help? SolarWinds offers a variety of technical support options. For current product support policies, please refer to the Serv-U Help Desk.

Users who purchased their copy of Serv-U from an official reseller are referred back to their reseller for support. Telephone technical support is available.

If you have lost your registration ID, please visit the Online Customer Service Center.

Free Email Support

Free technical support is available via email to all users. We ask that all users submit their inquiries to http://www.Serv-U.com/support/ for technical support requests.

Knowledge Base

Our Knowledge Base is a dynamic support tool that you can use to research solutions to your questions and problems. Nearly every technical question posed to our technical support team is answered here. The Knowledge Base can provide immediate, informative, step-by-step answers with screenshots to your questions.

Visit http://www.Serv-U.com/kb/ to get answers now.

Sales Support

Sales questions relative to the Serv-U File Server software should be directed to: http://www.Serv-U.com/sales/. Sales representatives can also be reached by calling SolarWinds at +1 (855) 498-4154.

Technical Support options are subject to change without notice at the discretion of SolarWinds.

Contacting SolarWinds

If you have lost your registration ID, please visit the Online Customer Service Center.

You can contact SolarWinds by snail-mail at:

SolarWinds

7171 Southwest Parkway

Bldg 400

Austin, TX 78735

Sales: +1 (855) 498-4154
FAX: +1 (512) 682-9301
Phone: +1 (866) 530-8100

http://www.Serv-U.com/

http://www.Serv-U.com/sales/

http://www.Serv-U.com/support/

For sales inquiries, visit: http://www.Serv-U.com/sales/.

For more information on the Serv-U File Server, visit: http://www.Serv-U.com/.

Chapter 1: Serv-U File Server

Serv-U File Server Overview

Welcome to the Serv-U File Server!

The Serv-U File Server is a multi-protocol file server capable of sending and receiving files from other networked computers through various means. Administrators create accounts for users that allow access to specific files and folders on the server's hard drive or any other available network resource. These access permissions define where and how the users can access the available resources. Serv-U's multi-protocol support means that users can employ whatever access method is available to them when connecting to your server. In addition, Serv-U supports both IPv4 and IPv6 for next-generation networks. The Serv-U File Server supports the following protocols:

- FTP (File Transfer Protocol)
- HTTP (Hyper Text Transfer Protocol)
- FTPS (FTP over SSL)
- HTTPS (HTTP over SSL)*
- SFTP using SSH2 (File Transfer over Secure Shell)*

In addition to Serv-U's excellent support for a large collection of the most popular FTP clients, you can now use your favorite web browser or SSH client to connect and transfer files to and from Serv-U. Server administrators looking to provide a full-featured FTP client to users that may not have an FTP client license of their own can even license FTP Voyager JV - a Java enabled FTP client delivered to the user after logging in to their Serv-U account. For more information about licensing FTP Voyager JV, click here.

The Serv-U File Server maintains the Serv-U brand's legendary feature set and continues to raise the bar for file servers by enabling you to:

- Access files from anywhere
- Share files with friends, family, and clientèle
- Provide employees in the field with a central location to send and receive data files
- Full group support that streamlines user creation and maintenance
- View images in thumbnails and slide shows, generated on-the-fly to minimize bandwidth usage
- Administer the server through a custom-built web interface
- Chat with FTP clients and view session logs in real time
- Customize FTP command responses
- Create custom limits and rules at an extremely granular level to control resource usage on the server
- Connect securely using SSL/TLS or SSH2
- Use 3rd party digital certificates to guarantee the server's identity to clients
- Host multiple domains on the same IP address and port
- Utilize multiple sources of authentication on the same domain (local user database, NT/SAM, ODBC)
- Automatically build the tables necessary for ODBC authentication
- For more information see File Sharing

A Serv-U trial allows you to test Serv-U MFT Server in a non-production environment for a specific period of time. A commercial license or maintenance renewal provides you with free software updates and free technical support via email and/or phone, depending on edition, for the duration of the associated maintenance plan.

**** - Requires Serv-U MFT Server***

Serv-U Editions

Serv-U is available in two editions to support the different needs of different organizations.

Serv-U FTP Server is designed for small businesses and project teams requiring FTPS to secure FTP, scripted transfers, and smaller number of users and domains supported on a single server.

Serv-U MFT Server is designed for businesses of all sizes who need to secure data in transit via SFTP, FTPS or HTTPS. It also adds remote administration through web browsers and the iPad, authentication via Active Directory or a database, clustering and event-driven automation, and branding. It also includes our FTP Voyager JV module for a rich "sync and side-by-side" web client interface.

Both editions ship with FTP, web transfer, and mobile device support. Both editions also support the optional Serv-U Gateway module (a reverse proxy component that prevents “data at rest” in a DMZ segment).

Click here to view a feature-by-feature comparison of each version.

How to Purchase Serv-U

Serv-U is available as a fully functional MFT Server trial for 30 days after the date of initial installation. In order to continue using Serv-U with its full set of features, a Serv-U license must be purchased.

A license can be purchased online at http://www.Serv-U.com/purchase/. Simply choose which edition of the Serv-U File Server is required and the quantity to purchase (discount pricing applies for bulk purchasing). A Serv-U File Server license must be purchased before adding an FTP Voyager JV license to your shopping cart. Licenses of FTP Voyager (our premier FTP client software) may also be bundled at the time of purchase at a substantial discount.

Pricing information can be found at: http://www.Serv-U.com/pricing/.

If you have lost your registration ID, it can be retrieved at: Online Customer Service Center.

Once the purchase has been completed, an email containing the registration details is immediately sent. If it is not received within an hour, check your spam filter to make sure that the email has not been filtered.

Purchase orders can be sent to SolarWinds in one of three ways:

1. E-Mail PO (PDF/JPG/GIF format preferred) to a Sales Representative at http://www.Serv-U.com/sales/.
2. Fax PO to +1 (512) 682-9301
3. Mail directly to SolarWinds:

SolarWinds
7171 Southwest Parkway
Bldg 400
Austin, TX 78735
USA

Chapter 2: Getting Started

System Requirements

This section contains detailed information about the minimum hardware, operating system and browser requirements that have to be met to run Serv-U.

Hardware requirements

Most modern operating systems require higher hardware specifications. Use minimum operating system requirements instead where applicable.

Minimum Hardware	Requirement
CPU	1 GHz+
RAM	256 MB+
Network	10/100 Mbps NIC
Hard drive space	30 MB
Video	128 MB Video RAM

Serv-U's hardware requirements are modest, but our software has been built to take advantage of multicore processors and multiple processor architectures.

The following table lists the requirements in the case of modest traffic: up to 500 configured users and 25 simultaneous transfers.

Recommended Hardware - Modest traffic	Requirement
CPU	2 GHz+ multicore
RAM	2 GB+

Recommended Hardware - Modest traffic	Requirement
Network	10/100/1000 Mbps NIC
Hard drive space	120 GB
Video	128 MB Video RAM

The following table lists the requirements in the case of high traffic: up to 10 000 configured users and 250 simultaneous transfers.

Recommended Hardware - High Traffic	Requirement
CPU	Multiple 3.2 GHz+ multicore
RAM	4 GB+
Network	10/100/1000 Mbps NIC
Hard drive space	120 GB
Video	128 MB Video RAM

Operating system requirements

We recommend the use of Microsoft Windows Server 2008 R2 or Red Hat Enterprise Linux v6 with our Serv-U and Serv-U Gateway deployments, but we also support other Windows and Linux operating systems. 64-bit and 32-bit editions are supported unless otherwise noted (or not available).

Operating system	Requirement
Microsoft Windows	• Windows Server 2012

Operating system	Requirement
	Windows Server 2012 RC2 Windows Server 2008, 2008 SP2, 2008 R2, and 2008 R2 SP1 Windows Server 2003 SP2 and 2003 R2 SP2 Windows XP SP2, Windows Vista, Windows 7, Windows 8, Windows 8.1 for trial purposes
Linux	Red Hat Enterprise Linux (RHEL) v.6.4 Fedora 19 Ubuntu CentOS 6.4 OpenSUSE

Client requirements

The default web browser on many mobile devices can be used to transfer files, work with files and folders, or run Serv-U's web-based management console without any plug-ins. However, Javascript and cookies must be enabled.

We support the following functionality on the following devices.

Device	Supported functionality
Apple iPhone 3+	download, manage and preview files
Apple iPad 1+	download, manage and preview files, run management console
Apple iPod	download, manage and preview files

Device	Supported functionality
Google Android 2.2+	upload, download, manage and preview files
Amazon Kindle Fire	upload, download, manage and preview files
RIM BlackBerry	upload, download, manage and preview files
Microsoft Windows Mobile	upload, download, manage and preview files

The following major browsers are supported with the basic web client, to upload, download, manage, and preview files, and for web administration:

- Microsoft Internet Explorer 8.0+
- Mozilla Firefox - latest two versions
- Safari 5, 7
- Google Chrome - latest version
- Mobile browser

The following database management systems are supported:

- MS SQL 2012, 2012 SP1
- MySQL 5.7.3
- PostgreSQL - latest version

The following LDAP versions are supported:

- Active Directory 2003, 2008, 2012
- Open Directory 4
- OpenLDAP 2.4

The following Java version is supported:

- Java JRE 7

Notes:

- To be able to use Web Client Pro and FTP Voyager JV, Java has to be installed and enabled in the browser.
- Apple Macintosh users must have at least Mac OS X 10.6 installed.

Quick Start Guide

Serv-U has been designed to be simple to configure with the flexibility and control you require to easily share files with others under the best security possible. This Quick Start Guide helps you install the server, create your first domain, and add a user account to the new domain. Once you have completed these steps, you will be able to connect to your new file server and start transferring files.

Installation

If you are installing Serv-U for the first time, follow the instructions on the installation screens to choose the installation directory and configure any desktop shortcuts for quickly accessing the server.

Serv-U supports installation in English, German, Spanish, French, Italian, Serbian, Swedish, Russian, and Simplified and Traditional Chinese. At this point you are selecting only the default language for the Management Console. Users connecting remotely can select any language from the supported languages they want when they connect to Serv-U.

You can also choose to install Serv-U as a system service, meaning that Serv-U is automatically started when the server is started, before any user logs on to the machine. This is useful if Serv-U is run on a dedicated server machine that does not regularly have an interactive user session logged on to it. If Serv-U is not installed as a system service, it has to be manually started after logging in to the server.

If Serv-U is being installed over an existing Serv-U installation, we recommend creating a backup of your original installation folder first. While Serv-U can be safely installed over any existing installations and performs any necessary upgrades to data files and binaries, it is considered good data management practice to back up critical components before upgrading them. If the installation being upgraded is older than version 7.0, you are also prompted with a dialog pointing out some of the critical changes made after version 6 and how these changes affect your administration of the Serv-U File Server.

Once installation is complete, the Serv-U Management Console is started. If you chose not to have the Serv-U Management Console started after installation, you can always launch it by double-clicking on the Serv-U icon in your system tray, or by right-clicking it and selecting **Start Management Console**.

Creating Your First Domain

Once the Management Console has finished loading, you are prompted if you would like to create a new domain if no domains are currently present.

Serv-U domains are collections of users and groups that share common settings, such as transfer rate limitations, service listeners and directory access rules. In most cases, all of your users and settings will exist in the same domain, with no need to create separate domains.

Note: Users sharing the same domain does not mean that all users share access to the same files. Each user in Serv-U has unique permissions to the directories you define, and does not have access to any files or folders unless you explicitly grant them that access.

Click **Yes** to start the domain creation wizard. This wizard can be run at any time by clicking the **+ (New Domain)** button found at the top of the Management Console.

To create a new domain:

1. Click **+ (New Domain)** at the top of the Management Console.
2. Type a unique name and an optional description for the new domain.

Note: The domain name is not visible to any of its users, nor does it affect how the domain is accessed by others. The name serves as an identifier for the domain to make identification and management of the domain easier for administrators. The name must be unique so that Serv-U can distinguish it from other domains on the server.

3. ***If you want the domain to be temporarily unavailable to users while you are configuring it***, deselect **Enable domain.**
4. Click **Next**.
5. Decide whether you want the domain to be a File Transfer Domain, a File Sharing Domain, or both, and then click **Next**.
    - ***If you are setting up a File Transfer Domain only***, perform the following steps:
        a. On the Protocols screen, select the protocols and port numbers the domain should use to provide access to its users, and then click **Next**.

        Note: The standard file sharing protocol is FTP, which operates on the default port of 21. However, you can change any of the available ports to a value of your choosing. If you want to run the server on a non-default port, it is recommended that you use a port above 1024. For more information about the supported protocols in each Serv-U edition, see the documentation about Serv-U editions.

        b. On the IP Listeners screen, specify the IP address that is used to connect to this domain, and then click **Next**.

        Note: ***If you do not specify an address***, Serv-U will use any available IP address on the computer.

        c. On the Encryption screen, select the encryption mode you want to use when storing passwords on the domain.

Note: For more information about password encryption modes, see "Domain Limits and Settings".

d. ***If you want to enable users to recover their passwords***, select the appropriate option.

e. Click **Finish** to create the domain, or click **Back** to modify the settings you specified.

- ***If you are setting up a File Sharing Domain only***, perform the following steps:

  a. On the File Sharing screen, specify the Domain URL, the File Sharing Repository, and whether you want to use Secure URL.

  b. Click **Configure SMTP** to set up an SMTP server. An SMTP server is necessary for sending email notifications, and for events that use email actions.

  Note: The SMTP server can be configured at a later time as well. For more information, see "Serv-U SMTP Configuration".

  c. Click **Next**.

  d. On the IP Listeners screen, specify the IP address that is used to connect to this domain.

  Note: ***If you do not specify an address***, Serv-U will use any available IP address on the computer.

  e. Click **Finish** to create the domain, or click **Back** to modify the settings you specified.

- ***If you are setting up a File Transer and File Sharing Domain***, perform the following steps:

a. On the File Sharing screen, specify the Domain URL, the File Sharing Repository, and whether you want to use Secure URL.

b. Click **Configure SMTP** to set up an SMTP server. An SMTP server is necessary for sending email notifications, and for events that use email actions.

   Note: The SMTP server can be configured at a later time as well. For more information, see "Serv-U SMTP Configuration".

c. Click **Next**.

d. On the Protocols screen, select the protocols and port numbers the domain should use to provide access to its users, and then click **Next**.

   Note: The standard file sharing protocol is FTP, which operates on the default port of 21. However, you can change any of the available ports to a value of your choosing. If you want to run the server on a non-default port, it is recommended that you use a port above 1024. For more information about the supported protocols in each Serv-U edition, see the documentation about Serv-U editions.

e. On the IP Listeners screen, specify the IP address that is used to connect to this domain, and then click **Next**.

   Note: ***If you do not specify an address,*** Serv-U will use any available IP address on the computer.

f. On the Encryption screen, select the encryption mode you want to use when storing passwords on the domain.

   Note: For more information about password encryption modes, see "Domain Limits and Settings".

g. ***If you want to enable users to recover their passwords***, select the appropriate option.

h. Click **Finish** to create the domain, or click **Back** to modify the settings you specified.

There are additional properties you can configure for the domain. For more information about these options, see "Domain Settings".

Creating Your First User Account

After your first domain is created, you are taken to the user's page of the Management Console and asked if you want to create a new user account with the new user wizard. Clicking **Yes** starts the new user account wizard. This wizard can be run at any time by clicking the **Wizard** button on the user account page.

The first step is to provide a unique login ID for the account. This login ID is used to begin the authentication process when connecting to the domain. The login ID must be unique for this domain, however other domains on your server may have an account with the same login ID. To create an anonymous account, specify `anonymous` or `ftp` for the login ID.

At this time, a Full Name and an email address can also be specified for the user account. The Full Name provides a canonical name with which to refer to the user account, and the email address allows Serv-U email notifications and recovered passwords to be sent to the user account. Click **Next** to continue creating the user account.

After specifying a unique login ID, you must also specify a password for the account. The password is the second piece of information required to authenticate a user when they connect to the domain. In order for another person to connect to this domain, they must know the login ID specified in step 1, and this password. It is possible to leave this password blank, however that allows anyone who knows the login ID to access your domain. Click **Next** to continue.

The third step is specifying a home directory for the account. The home directory is the location on the server's hard drive (or accessible network resource) that the user account is placed in upon successful login. Essentially, it is the location you want the user account to use when sending and receiving files on the server. Click **Browse** to browse to a location on your hard drive, or type the location manually. If the user is locked in their home directory, they are not able to access files or folders above the directory structure of their home directory. Additionally, the actual location of their home directory is masked and displayed as "/". Click **Next** to proceed to the final step.

The final step is granting access rights to the user account. Access rights are granted on a per directory basis. However, they can be inherited by all subdirectories contained in an accessible directory. The default access is **Read Only**, which means that the user can list files and folders in their home directory and download them. However, they cannot upload files, create new directories, delete files or folders, or rename files or folders. If **Full Access** is selected, the user is able to do all of these things. After the user is created, these access rights can be configured on a more granular basis by editing the user, and selecting the Directory Access tab. After selecting the directory access rights, click **Finish** to create the user account.

Congratulations! Your Serv-U File Server is now accessible and ready for sharing. You can create more accounts just like this one to share it with other friends, family, or colleagues. Each user can have a different home directory allowing you to share different files with different people. There are many more user configurable options that let you fine-tune an account's access to the server. For more information about these options, see "About User Accounts".

File Sharing

The File Sharing Feature enables your domain users to send or receive files from guests.

To send file sharing invitation emails, you must configure your SMTP settings. This configuration only needs to be set once for the entire server or a domain.

Note: File Sharing is disabled by default.

For more information, see File Sharing.

URL Parameters

Serv-U supports several parameters that can enhance log on in various ways. You can create special login links that allow users to automatically send their Login ID and password, start audio files immediately, and more. To specify these parameters, follow the syntax in the following example:

`http://yourserver.com/?user=admin&password=test`

The following parameters are supported in Serv-U:

- user=username&password=password - Allows the Login ID and password to be sent automatically to Serv-U, bypassing the need to log in. This can be convenient for audio or video, but should not be used for confidential or protected information.
- thumbnail=1 - Starts the Web Client in Thumbnail Mode, showing thumbnails of images.
- slideshow=1 - Starts the Web Client in Slideshow Mode, showing a slideshow of all images.
- playlist=1 - Start the Web Client in media mode, playing audio or video files in order.
- playmedia=1 - Starts the Web Client in media mode, playing video files only.
- dir=`directory` - Specifies what directory to browse to immediately after login.
- file=`file` - Specifies a file to download immediately after login, defaulting in the home directory. If the `dir` parameter is used in conjunction with the `file` parameter, the Web Client attempts to download a file from that folder.

- sortcol=`column` - Specifies the column by which to sort the files in the Web Client. This column accepts the integer values 1-3 for sorting by name, size, or time, respectively.

Server Concepts

The Serv-U File Server makes use of several concepts that aid in the understanding of how to configure and administer your File Server as a single, hierarchical unit. There are four related levels of configuration to the Serv-U File Server: the **Server**, the **Domain**, the **Group**, and the **User**. Of all of these, only the **Group** is optional - all the other levels are mandatory parts of the File Server. An explanation of each level is provided below.

Server

> The server is the basic unit of the Serv-U File Server and the highest level of configuration available. It represents the File Server as a whole and governs the behavior of all domains, groups, and users. The Serv-U File Server ships with a set of default options that can be overridden on a per setting basis. Thus, the server is at the top-level of the hierarchy of configuring Serv-U. domains, groups, and users inherit their default settings from the server. Inherited settings can be overridden at each of these lower levels. However, some settings are exclusive to the server, such as the PASV port range.

Domain

> A server can contain one or more domains. Domains are the interface through which users connect to your File Server and access a specific user account. A domain's settings are inherited from the server. It also defines the collection of settings that all of its groups and user accounts inherit. If a server setting is overridden at the domain level, then all of its groups and user accounts inherit that value as their default value.

Group

> The group is an optional level of extra configuration provided to make it

easier to manage related user accounts that share many of the same settings. By using a group, you can quickly make changes that propagate to more than one user account instead of having to manually configure each one separately. A group inherits all of its default settings from the domain it belongs to. It defines the collection of settings inherited by all users who are a member of the group. Virtually every user level setting can be configured at the group level, or overridden at the user level.

User

The user is at the bottom of the hierarchy. It can inherit its default settings from multiple groups (if it is a member of more than one group) or from its parent domain (if it is not a member of a group or the group does not define a default setting). A user account identifies a physical connection to the File Server and defines the access rights and limitations of that connection. Settings overridden at the user level cannot be overridden elsewhere and are always applied to connections authenticated with that user account.

User Collections

Unlike groups, user collections do not offer any level of configuration to the user accounts they contain. Instead, they simply offer a way to organize users into containers for ease of viewing and administration. For example, collections can be created to organize user accounts based upon group membership, however they must be manually maintained when user accounts change group membership.

Glossary

Listener

A listening service in Serv-U which is configured in a domain to accept incoming FTP, FTPS, SFTP, HTTP or HTTPS connections.

Limit

A configuration option which can be set at the server, domain, group or user level. Limits can be set for password complexity requirements, session timeout, Web Client customization, and more.

Event

A Serv-U event consists primarily of an event type (such as User Login or File Upload Failed), and an Action Type (such as Show Balloon Tip or Send Email). Serv-U events are used to automate behavior and provide greater visibility of important file transfer processes.

Anti-Hammering

A Serv-U feature which allows administrators to block IP addresses who attempt to connect repeatedly with incorrect credentials. By handling only IP addresses who repeatedly fail to log on correctly, anti-hammering allows for smart blocking of bots and hackers.

IP Access Rules

IP Access rules are used in Serv-U to determine who may connect to the server. Rules set up at the server and domain levels define who is allowed to make an initial connection to Serv-U, while rules set up at the group and user levels define who may connect using a given user account.

Directory Access

Directory access encompasses all of the permissions applied to a server, domain, group and user, which grant and deny access to files and folders. Directory access rules are the foundation of file access rights, determining what a user may and may not access, as well as how they may access it.

The Serv-U Management Console

The Serv-U Management Console is designed to provide quick and easy access to the File Server's configuration options in a familiar way. When viewing a configuration page, you can return to the main Management Console page at any time by clicking on the Serv-U File Server logo in the top left corner.

Management Console Layout

The Management Console is presented in an accordion style layout, with an accordion list on the left, and the global dashboard on the right. The accordion menu contains the name of the server on top, and then the list of configured domains. The global dashboard contains the session statistics, the server log, and information about the active sessions.

Click the name of the server or the domain to expand the list of configuration options available for the server or for the particular domain, and then click one of the options.

Domain Administrators only have access to configuring settings and options for their applicable domain and do not have access to the server-level categories displayed to System Administrators.

To return to the global dashboard, click the Serv-U Management Console icon in the top left corner.

Tabbed Configuration Pages

When opening a category from the Management Console, all related sub-category pages are displayed in tabs on the same screen. This allows for quick navigation between related configuration options.

Launching A Web Client

While configuring the Serv-U File Server, an HTTP session can be launched by clicking **Serv-U Products > Web Client** on the top toolbar. If licensed for use, the Web Client is available and runs from within the browser. If licensed for use, FTP Voyager JV can also be launched using the Java Runtime Environment, by clicking **Serv-U Products > FTP Voyager JV**.

User Interface Conventions

The Serv-U File Server uses a consistent method of representing configuration options in a manner that not only convey the current value of the option, but also whether or not that value is the default (or inherited) value. Traditionally, this has been done with something called a tri-state check box. The tri-state check box has two major drawbacks:

1. The default state does not clearly convey the current value of the option. In some versions of Windows, the box is checked with a grey background -

even if the option is not currently enabled.

2. They can only be used to represent binary values, which is to say they can only represent two values - on or off.

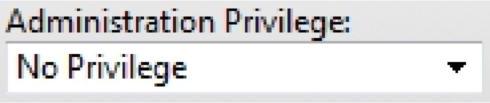
The Serv-U File Server uses a different, easy to understand convention that overcomes these drawbacks. When an option is inheriting its value from a parent, the text of the option is displayed in regular font. The value that is displayed (whether it is a text value or a check box) can change to reflect changes made to the parent where the item is currently inheriting its value.

However, if the value is overriding the default, the text of the value is displayed in **bold**. The value that is currently displayed is always the value of that option, regardless of changes to its parent.

Understanding User Interface Conventions

To better illustrate the user interface conventions, consider the following case file.

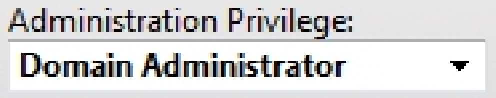
Acme Technology Co. is a computer repair company that maintains a Serv-U File Server providing global access to shared corporate resources to their traveling technicians. Each technician has their own account on the File Server. To facilitate easy administration of the user accounts, the File Server administrator has made each user account a member of the "Technician" group. This group's Administration Privilege is set to **No Privilege** since none of the technicians have any File Server administration duties.



Administration Privilege:

No Privilege

A technician receives a promotion. In addition to his current technician duties, he is also given administration privileges on the File Server so he can assist other technicians with their accounts. The File Server administrator can edit the technician's user account and change the Administration Privilege to **Domain Administrator**. The text of this option turns bold to reflect that it is overriding the default value (No Privilege) that the user account inherits from its membership to the "Technician" group.



Administration Privilege:

Domain Administrator

At a later date, the Administration Privilege can be reverted back to the default value inherited from the "Technician" group by selecting the **Inherit default value** option from the **Administration Privilege** list.

Chapter 3: Server

Server Overview

The Serv-U File Server allows for certain settings to be configured at the server level. When configured at the server level, the settings apply to all users, groups, and domains on the server unless those settings are overridden at a lower level. Settings that can be configured at the server level include: Directory Access rules, IP Access rules, bandwidth limitations, global user accounts (user accounts which can log into any Serv-U Domain), and more. Detailed information about each setting and how it can be configured is listed in the following sections.

Server Details

IP Access Rules

IP Access rules restrict login access to specific IP addresses, ranges of IP addresses, or even a domain name. IP Access rules can be configured at the server, domain, group, and user levels.

IP access rules are applied in the order they are displayed. In this way, specific rules can be placed at the top to allow (or deny) access before a more general rule is applied later on in the list. The arrows on the right side of the list can be used to change the position of an individual rule in the list.

IP Access Masks

IP Access rules use masks to authorize IP addresses and domain names. These masks may contain specific values, ranges and wildcards made up of the following elements.

xxx

An exact match such as `192.168.1.1` (IPv4), `fe80:0:0:0:a450:9a2e:ff9d:a915` (IPv6, long form) or `fe80::a450:9a2e:ff9d:a915` (IPv6, shorthand).

xxx-xxx

A specified range of IP addresses such as `192.168.1.10-19` (IPv4), `fe80:0:0:0:a450:9a2e:ff9d:a915-a9aa` (IPv6, long form), or `fe80::a450:9a2e:ff9d:a915-a9aa` (IPv6, shorthand).

*****

Any valid IP address value such as `192.168.1.*`, which is analogous to `192.168.1.0-255`, or `fe80::a450:9a2e:ff9d:*`, which is analogous to `fe80::a450:9a2e:ff9d:0-ffff`.

?

Any valid character when specifying a reverse DNS name such as `server?.mydomain.com`.

/

The slash separator allows the use of CIDR notation to specify which IP addresses should be allowed or blocked. Common CIDR blocks are `/8 (for 1.*.*.*)`, `/16 (for 1.2.*.*)` and `/24 (for 1.2.3.*)`. CIDR notation also works with IPv6 addresses, such as `2001:db8::/32`.

Caveats

Specific IP addresses listed in Allow rules will not be blocked by anti-hammering. (In other words, they are 'whitelisted'.) However, addresses matched by wildcard or range will be subject to anti-hammering prevention.

Implicit Deny All

Serv-U assumes that connections from any IP address are valid until you add your first IP access rule. After you add that first IP access rule Serv-U assumes that all connections not explicitly allowed should be denied. This is also known as "an implicit 'Deny All' rule". With this in mind, make sure you add a 'wildcard allow' rule (such as `Allow *.*.*.*`) at the end of your IP Access rule list.

Matching All Addresses

Use a mask of `*.*.*.*` to match any IPv4 address. Use a mask of `*:*` to match any IPv6 address. Remember to add Allow ranges for both IPv4 and IPv6 addresses if you use both IPv4 and IPv6 listeners.

DNS Lookup

If a dynamic DNS service is used, then a domain name can be specified in place of an IP address to allow access to clients that travel and do not have a static IP address. Reverse DNS names are also acceptable. If a domain name or reverse DNS rule is created, Serv-U must perform either a reverse DNS look-up or DNS resolution in order to apply these rules. This can cause a slight delay during login depending on the speed of the system's DNS server.

Rule Use During Connection

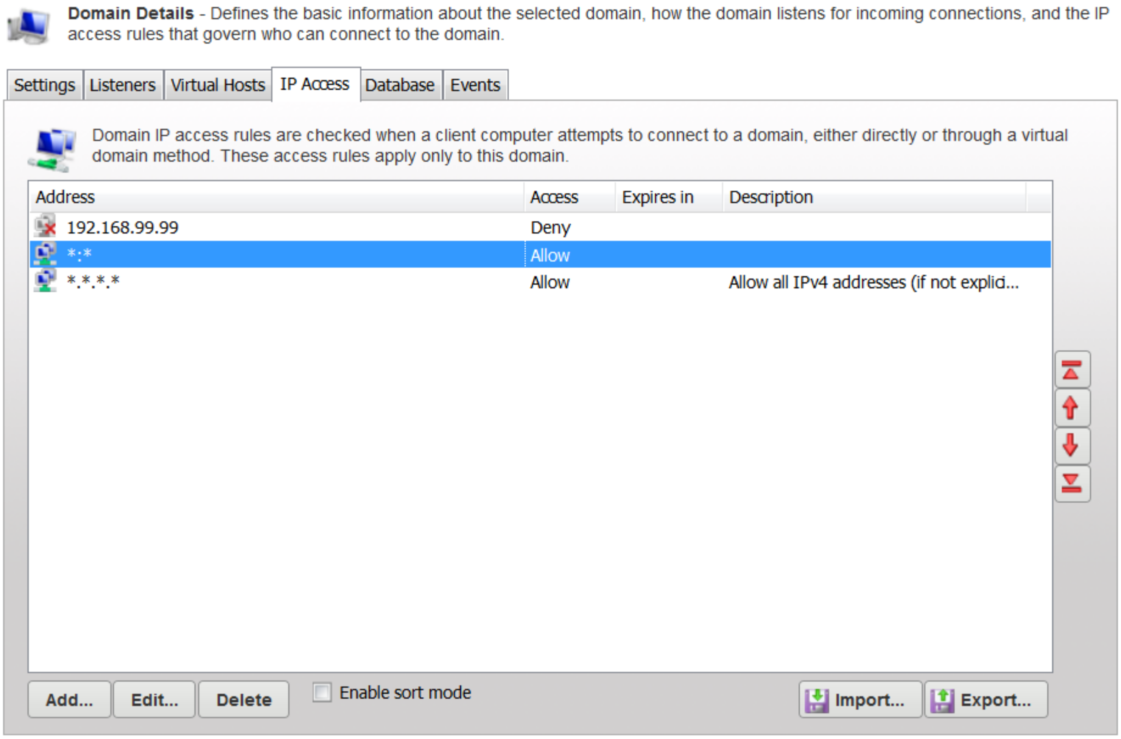
The level at which an IP access rule is specified also defines how far a connection is allowed before being rejected. Server and domain level IP access rules are applied before the Welcome message is sent. Domain level IP access rules are also applied when responding to the HOST command to connect to a virtual domain. Group and user level IP access rules are applied in response to a USER command when the client identifies itself to the server.

Anti-Hammering

Serv-U allows administrators to set up an "anti-hammering policy" that blocks clients who connect and fail to authenticate more than a certain number of times within a certain period of time. These policies can be configured server-wide in **Server Limits and Settings > Server Settings** and domain-wide in **Domain Limits and Settings > Domain Settings**.

IP addresses blocked by anti-hammering rules will appear in your Domain IP Access rules with a value in the **Expires in** column. If you have multiple domains with different listeners, blocked IPs will appear in the domain that contains the listener. (Blocked IP addresses will never appear in the Server IP Access list, even if anti-hammering was set up at the server level.)

The **Expires in** value of the blocked IP will tick down second by second until the entry disappears. You can unblock any blocked IP early by deleting its entry from the list.



Domain Details - Defines the basic information about the selected domain, how the domain listens for incoming connections, and the IP access rules that govern who can connect to the domain.

Domain IP access rules are checked when a client computer attempts to connect to a domain, either directly or through a virtual domain method. These access rules apply only to this domain.

Address	Access	Expires in	Description
192.168.99.99	Deny		
:	Allow		
..*.*	Allow		Allow all IPv4 addresses (if not explici...

☐ Enable sort mode

IP Access List Controls

Enable Sort Mode

This option allows the IP Access list to be sorted numerically rather than in the processing order. Displaying the IP Access list in sort mode will not change the order in which rules are processed. To view rule precedence disable this option. Viewing the IP Access list in numerical order can be a valuable tool when reviewing long lists of access rules to determine if an entry already exists.

Importing/Exporting IP Access Rules

Serv-U IP Access rules can be imported and exported from users, groups, domains, and the server using a standard text-based comma separated values (CSV) file. To export IP Access rules, view the list of rules to export, and then click **Export**, specifying the path and the file name to save the list to. To import IP Access rules, click **Import** and select the file with the rules to be imported. The CSV file must contain the following fields, headers included:

-IP - The IP address, IP range, CIDR block, or domain name for which the rule will apply

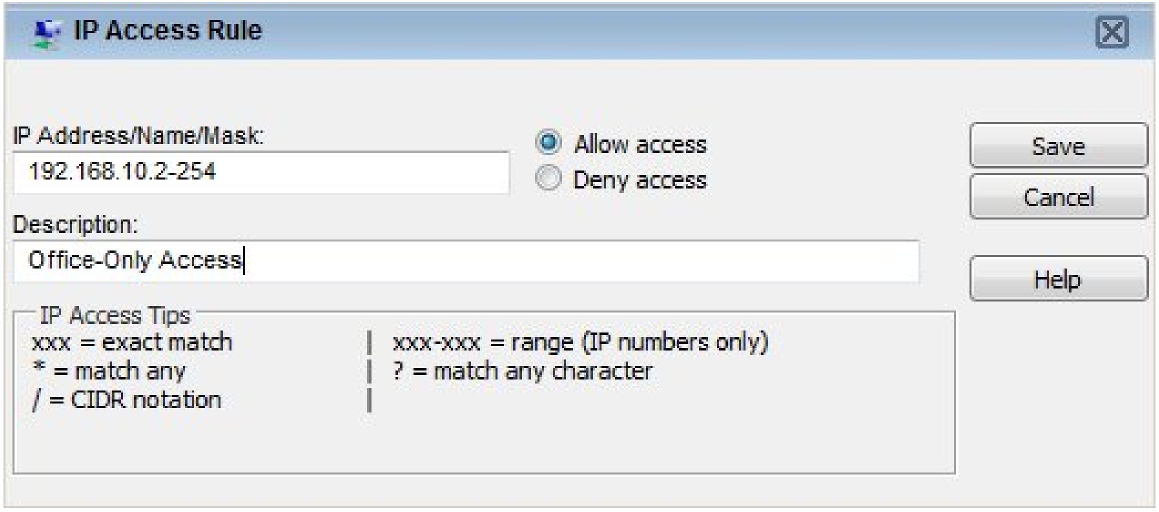
-Allow - Set this value to 0 for Deny, or to 1 for Allow

-Description - A text description of the rule for reference purposes

Examples

Case File - Office-Only Access

A contractor has been hired to work in the office, and only in the office. Office workstations have IP addresses from 192.168.10.2 to 192.168.10.254. The related Serv-U access rule should therefore be `Allow 192.168.10.2-254` (see below), and it should be added to either the contractor's user account or a 'Contractors' group that will contain multiple contractors. (Note that no "Deny" rule is required here because Serv-U provides an implicit 'deny all' at the end of the list.)



IP Address/Name/Mask: 192.168.10.2-254

● Allow access
○ Deny access

Description: Office-Only Access

Case File - Prohibited Machines

Users should normally be able to access Serv-U from anywhere, except from a bank of special internal machines in the IP address range of 192.168.15.100 - 192.168.15.110. The related Serv-U access rules should therefore be `Deny 192.168.15.100-110`, followed by `Allow *.*.*.*`, and these should both be added to either the domain or the server IP Access rules.

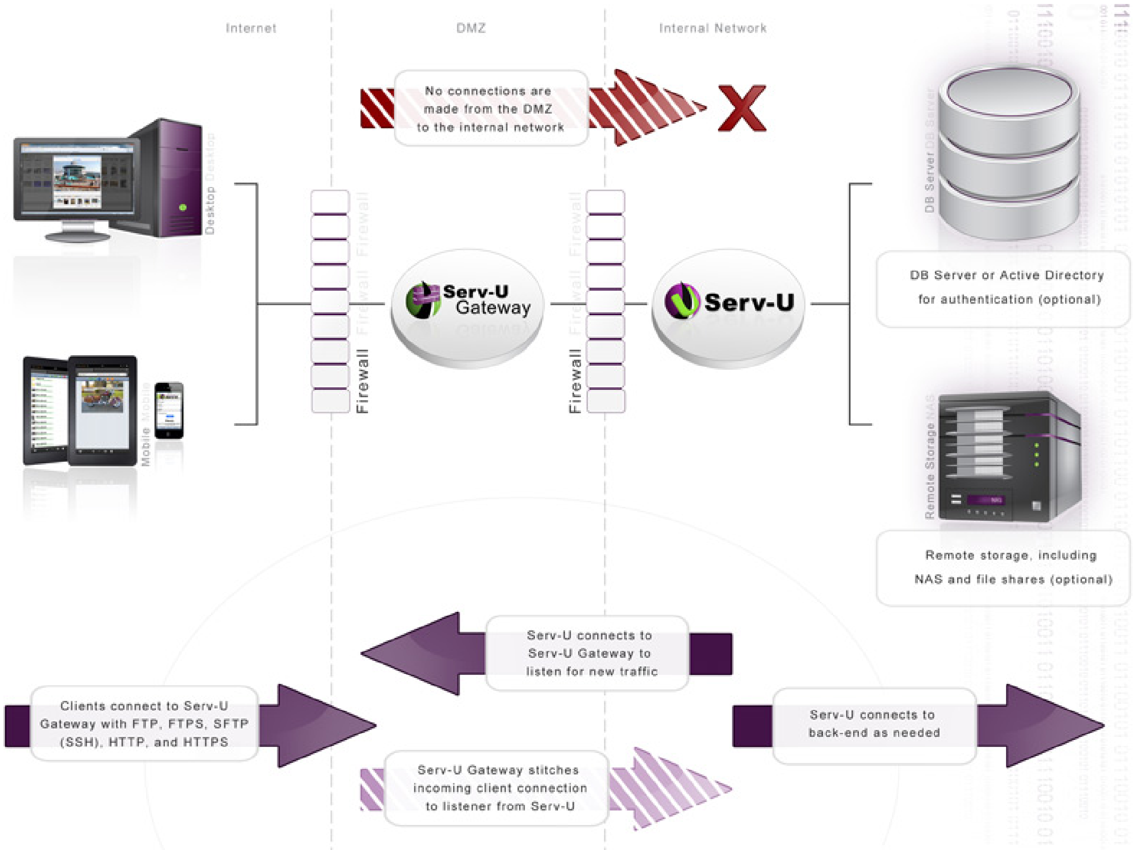
Case File - DNS-based Access Control

The only users allowed to access a Serv-U Domain will be connecting from `*.internal.com` or `*.trustedpartner.com`. The related Serv-U access rules should therefore be `Allow *.internal.com` and `Allow *.trustedpartner.com` (in any order) and these should both be added to the domain IP Access rules. (Note that no "Deny" rule is required here because Serv-U provides an implicit 'deny all' at the end of the list.)

Serv-U Gateway

Serv-U Gateway provides defense in depth to Serv-U deployments.

It acts as a reverse proxy in DMZ segments and prevents your Serv-U deployments from ever storing data in the DMZ or opening connections from the DMZ to the internal network. This type of architecture is essential to meet PCI DSS, managed file transfer and other high-security requirements.


Internet
DMZ
Internal Network
No connections are made from the DMZ to the internal network
Desktop
Mobile
Firewall
Firewall
Serv-U Gateway
Serv-U
DB Server
DB Server or Active Directory for authentication (optional)
Remote Storage
Remote storage, including NAS and file shares (optional)
Serv-U connects to Serv-U Gateway to listen for new traffic
Clients connect to Serv-U Gateway with FTP, FTPS, SFTP (SSH), HTTP, and HTTPS
Serv-U Gateway stitches incoming client connection to listener from Serv-U
Serv-U connects to back-end as needed

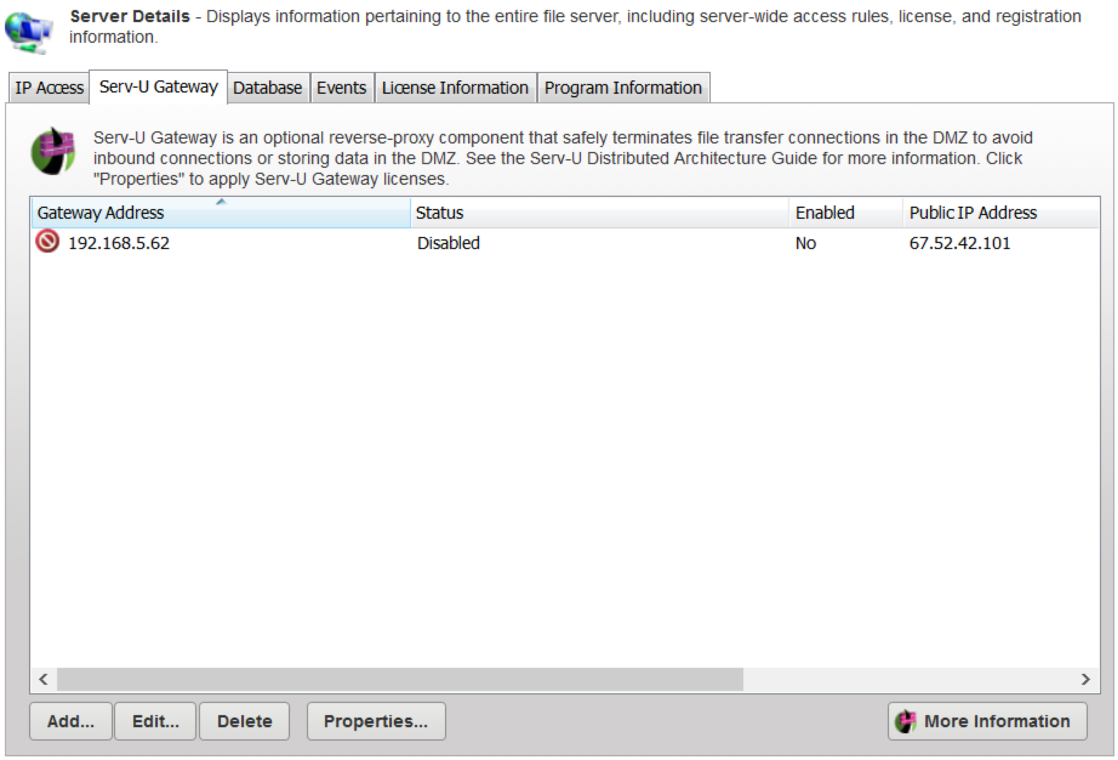
Basic Serv-U MFT Deployment

Deploying Serv-U Gateway

The following documents contain detailed information about the deployment of Serv-U Gateway:

- Serv-U Distributed Architecture Guide - to select the correct architecture
- Serv-U Gateway Installation Instructions
    - For Windows
    - For Linux
- Planning Your Serv-U Gateway Deployment - to develop a project plan for production deployment

Serv-U Gateway Tab



Server Details - Displays information pertaining to the entire file server, including server-wide access rules, license, and registration information.

Serv-U Gateway is an optional reverse-proxy component that safely terminates file transfer connections in the DMZ to avoid inbound connections or storing data in the DMZ. See the Serv-U Distributed Architecture Guide for more information. Click "Properties" to apply Serv-U Gateway licenses.

Gateway Address	Status	Enabled	Public IP Address
192.168.5.62	Disabled	No	67.52.42.101

The Serv-U Gateway tab in the Server Details displays all configured Gateways known to this Serv-U deployment. Serv-U periodically checks on every configured Gateway and displays a brief status message here.

Gateway Address Column

The Gateway Address is the IP address on the Serv-U Gateway that Serv-U uses to communicate with Serv-U Gateway. This should almost always be a private IP address (for example, `10.1.1.5`).

A status icon also appears to the left of the Gateway Address.The Status column shows a brief message to tell you what Serv-U knows about the Gateway's current health.

The icon in the Gateway Address column will change to reflect the current Gateway status.

- The Gateway is ready for connections. (However, the Gateway still needs Listeners to receive connections.)

- Serv-U is checking on the Gateway's status. Another status will appear in a few seconds.
- The Gateway is ready but you are running dangerously close to the end of your trial or updates/support period. You should plan to buy or renew soon, but you may also move on to the next step for now.
- Something is wrong. Select the Gateway entry, and then select **Properties** to find out why you cannot connect to your new Gateway.

Public IP Address Column

The Public IP Address column will either show the IP address file transfer clients should connect to or a blank entry. If a blank entry is present that indicates that the Gateway will automatically pass a list of public IP addresses to Serv-U at runtime.

A private IP address will be in the Public IP Address column if a private IP address was explicitly configured in the Gateway. This will be the case if the Gateway has no public IP addresses, which is common during trials and situations in which the Gateway lives behind NAT (network address translation).

Description Column

The Description column shows any note added to the Gateway configuration. It does not affect behavior in any way.

Buttons

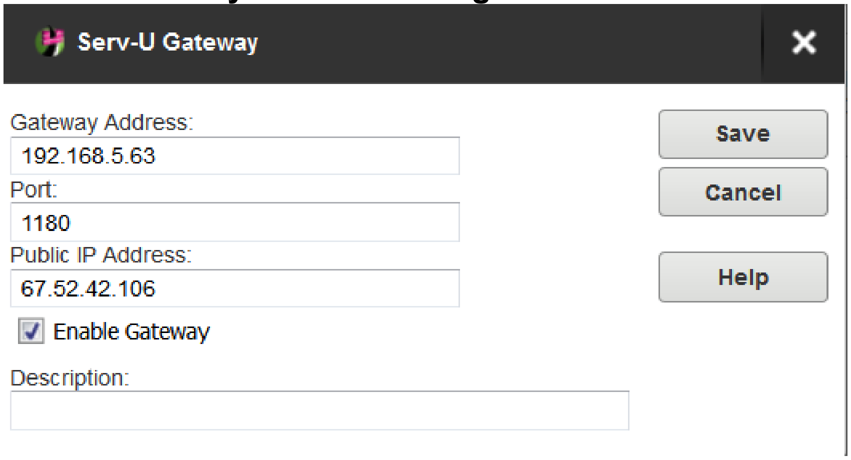
Click **Add** to add new Gateway configurations.

Click **Edit** to edit existing Gateway configurations.

Click **Delete** to delete existing Gateway configurations.

Click **Properties** to view detailed status about and add licenses to existing Gateway configurations. This button only displays complete properties when Serv-U is connected to the Gateway.

Serv-U Gateway Add/Edit Dialog



Gateway Address: 192.168.5.63

Port: 1180

Public IP Address: 67.52.42.106

☑ Enable Gateway

Description:

The Gateway Address is the IP address on the Serv-U Gateway that Serv-U uses to communicate with Serv-U Gateway. This should almost always be a private IP address (for example, `10.1.1.5`).

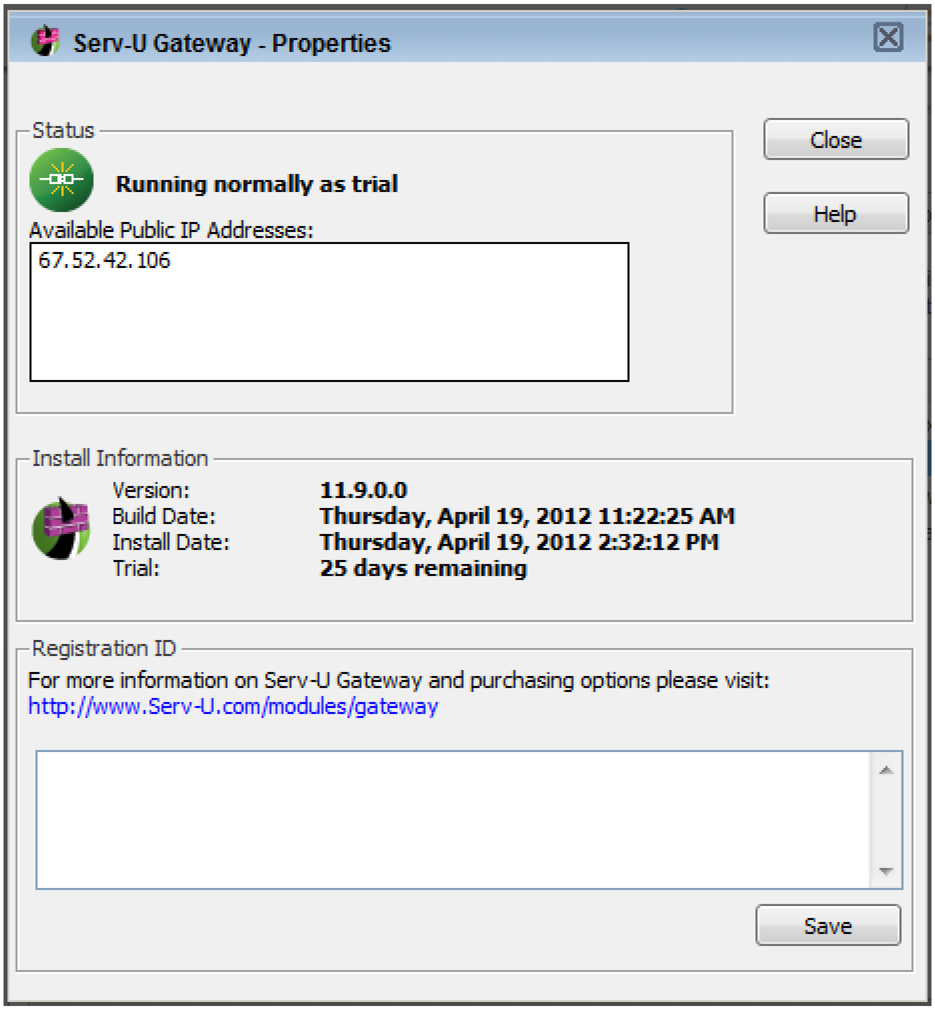
The Port is the TCP port on the Serv-U Gateway that Serv-U uses to communicate with Serv-U Gateway. The default is TCP port 1180.

The Public IP Address field should either contain the IP address file transfer clients should connect to or a blank entry. A blank entry indicates that the Gateway will automatically pass a list of public IP addresses to Serv-U at runtime. A private IP address should be entered in the Public IP Address field if the Gateway has no public IP addresses. This is common during trials and situations in which the Gateway lives behind NAT (network address translation).

The **Enabled Gateway** option is used to turn the Gateway on and off. The default is selected.

The Description is an optional note that describes the Gateway. It has no effect on any behavior.

Serv-U Gateway Properties Dialog



Status

Running normally as trial

Available Public IP Addresses:

67.52.42.106

Install Information

Version: 11.9.0.0

Build Date: Thursday, April 19, 2012 11:22:25 AM

Install Date: Thursday, April 19, 2012 2:32:12 PM

Trial: 25 days remaining

Registration ID

For more information on Serv-U Gateway and purchasing options please visit:

http://www.Serv-U.com/modules/gateway

Status Panel

The large icon here and a status message tell you if the Gateway is running, and whether or not it is running with a trial or commercial license.

The Available Public IP Addresses field contains a list of all the public IP addresses automatically detected on Serv-U Gateway. If a private address has been explicitly configured in the Gateway's **Public IP Address** field, then this field will display a message of "No public IP addresses found on gateway server" and this is normal.

Install Information Panel

This shows the version and build date of the Serv-U Gateway software running on the Gateway, the date Serv-U Gateway was installed or last updated and how many days are left in the evaluation period (if applicable).

Registration ID Panel

Copy and paste your Serv-U Gateway Registration ID (not your Serv-U Registration ID) into this field, and then click **Save** to apply a commercial license to your Serv-U Gateway software.

Database Access

Serv-U enables the use of an ODBC database to store and maintain group and user accounts at both the domain and server levels. The ODBC connections are configured from two locations: **Domain > Domain Details > Database** and **Server > Server Details > Database**. Serv-U can automatically create all of the tables and columns necessary to begin storing users and groups in your database. Because Serv-U uses one set of table names to store its information, individual ODBC connections must be configured for each item which stores details in the database. In other words, the server as well as each domain must have a unique ODBC connection to ensure they are stored separately. To configure a database, follow these steps:

- Create an ODBC connection for Serv-U to use. SolarWinds recommends MySQL, but any database that has an ODBC driver available can be used. Use a System DSN if Serv-U is operating as a system service, or a User DSN if Serv-U is operating as a regular application.
- Open the Serv-U Management Console and browse to the appropriate domain or server database settings. Enter the Data Source Name (DSN), the login ID, and password, and then click **Save**.

If the database connection is being configured for the first time, leave the **Automatically create** options selected. With these options selected, the Serv-U File Server builds the database tables and columns automatically.

SQL Templates

Serv-U uses multiple queries to maintain the databases containing user and group information. These queries conform to the SQL language standards. However, if the database you are using is having problems working with Serv-U, you may need to alter these queries. From the SQL Templates dialog, each query used by Serv-U can be specially tailored to conform to the standards supported by your database.

Warning: Incorrectly editing these SQL queries could cause ODBC support to stop working in Serv-U. Do not edit these queries unless you are comfortable constructing SQL statements and are positive that it is necessary to enable ODBC support with your database software.

User and Group Table Mappings

By default, Serv-U automatically creates and maintains the tables and columns necessary to store user and group information in a database. However, if you are attempting to connect Serv-U to an existing database containing this information, you need to customize the table and column names to conform to the existing database structure. Click **User Table Mappings** or **Group Table Mappings** to get started.

Serv-U stores information for a user or group in 10 separate tables. Only the User/Group Info Table and User/Group Dir Access Table are required. The current table can be changed from the **Object Table** list. The **Attribute** column lists the attributes that are stored in the current table. The **Mapped Database Value** displays the name of the column that attribute is mapped to in the database. The first row always displays the "TableName" and can be used to change the name of the table.

Certain tables where the order of the entries bears significance have a **SortColumn** attribute listed. This column is used to store the order in which rules are applied.

Click **Edit** or double-click the column name to edit a value.

When enabled, the table is accessed as needed. In special situations a table that is not being used may be disabled to reduce the number of ODBC (database) calls. For example, if you are not using Ratios and Quotas, the User Ratio-Free Files, Per User Files Ratio, Per User Bytes Ratio, Per Session Files Ratio, and Per Session Bytes Ratio tables may be disabled to prevent unneeded ODBC calls. Use caution when disabling tables as the fields will appear in dialogs, but they will not be saved or loaded. The User Info and Group Info tables cannot be disabled.

Case File - ODBC Authentication

Authentication in the Serv-U File Server can be handled through an ODBC database, allowing for scripted account management and maintenance. In order to make use of ODBC functionality, migrate to ODBC authentication through a database. By storing credentials in settings in a database, accounts can be managed from outside the Serv-U Management Console through scripted database operations which can be built into many existing account provisioning systems. A DSN must first be created in **Control Panel > Administrative Tools > ODBC Data Sources**. Use a System DSN if Serv-U is running as a service or a User DSN if Serv-U is running as an application. Once the proper DSN has been created, specify the Data Source Name, login ID and password, and then click **Save**. Serv-U creates the tables and columns transparently. Database Users and Groups can be managed from the Database Users and Database Groups sections of Serv-U (located near the normal Users and Groups tabs).

Data Source Name Creation in Linux

Database access in Serv-U Linux follows the same method as Serv-U on Windows, with the one change in how Data Source Names are created. In Linux, a DSN can be created after installing the following packages:

- mysql-connector-odbc
- postgressql-odbc
- unixodbc

Note that only the ODBC driver corresponding to the database needs to be installed. If Serv-U is running as a service, the next step is to edit the `/etc/odbc.ini` file, which contains all system-level DSNs. If Serv-U is running as an application, edit the `~/odbc.ini` file instead, and then enter the parameters as follows:

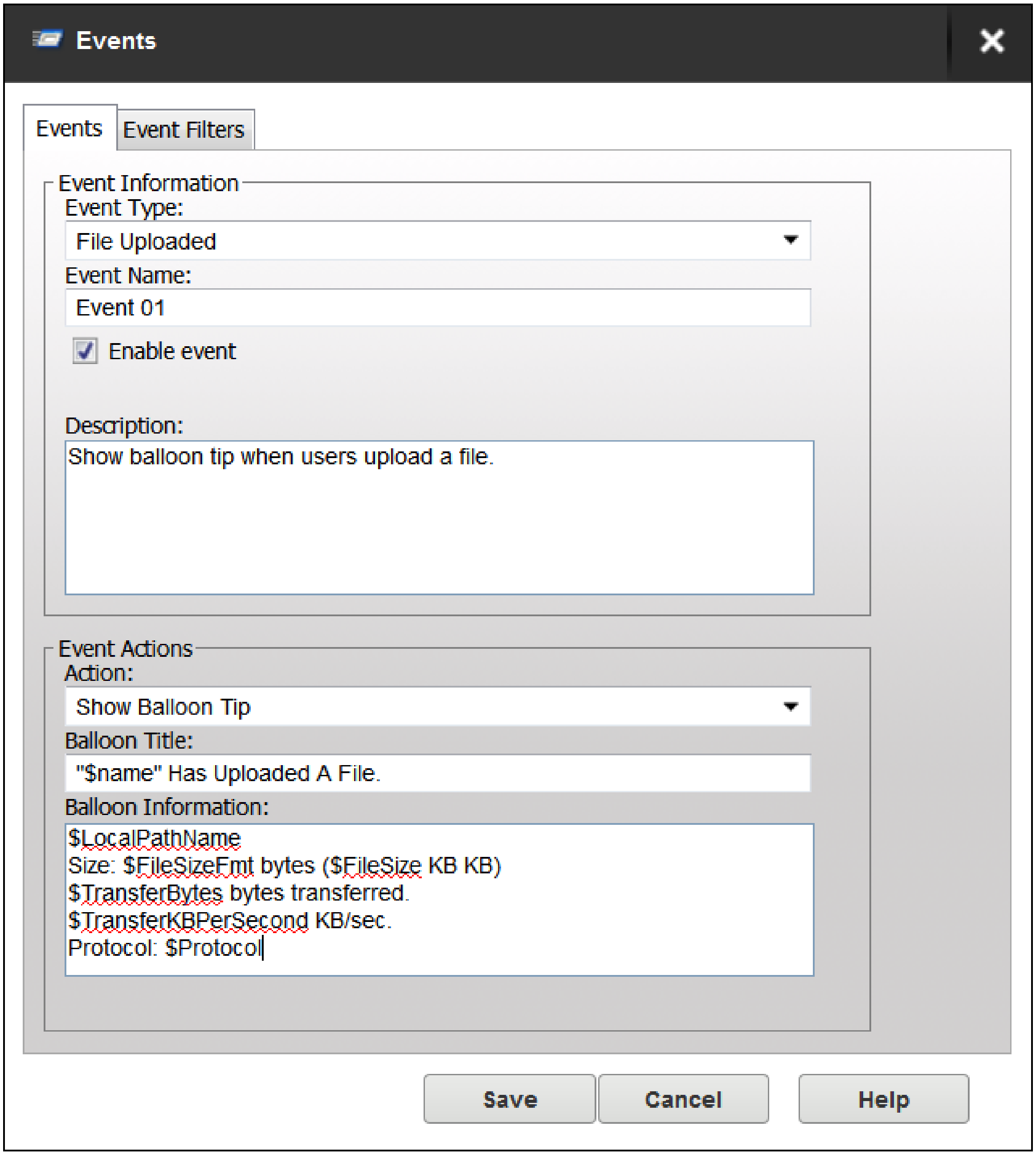
```
[MySQL-test]
Description = MySQL test database
Trace = Off
TraceFile = stderr
Driver = MySQL
SERVER = YOURIPADDRESS
USER = USERNAME
PASSWORD = PASSWORD
PORT = 3306
DATABASE = YOURDATABASE

[PostgreSQL-test]
Description = Test to Postgres
Driver = PostgreSQL
Trace = Yes
TraceFile = sql.log
Database = YOURDATABASE
Servername = YOURIPADDRESS
UserName = USERNAME
Password = PASSWORD
Port = 5432
Protocol = 6.4
ReadOnly = No
RowVersioning = No
ShowSystemTables = No
ShowOidColumn = No
FakeOidIndex = No
ConnSettings =
```

The names in brackets should be adjusted to your needed DSN name string. Finally, test the DSN using the command `isql %DSN% -c -v`.

For further customization, see the Serv-U Database Integration Guide at: http://www.serv-u.com/integration_guide

Serv-U Events



Event Type: File Uploaded

Event Name: Event 01

☑ Enable event

Description:
Show balloon tip when users upload a file.

Action: Show Balloon Tip

Balloon Title: "$name" Has Uploaded A File.

Balloon Information:

```
$LocalPathName
Size: $FileSizeFmt bytes ($FileSize KB KB)
$TransferBytes bytes transferred.
$TransferKBPerSecond KB/sec.
Protocol: $Protocol
```

Serv-U enables the use of event handling which can perform various actions triggered by a list of selected events. The following list contains the actions available to administrators:

Server Events

- Server Start - Triggered by Serv-U starting up, whether by starting the Serv-U service or starting Serv-U as an application.
- Server Stop - Triggered by Serv-U shutting down, whether from service or application-level status. This event will only trigger for graceful stops.

Server and Domain Events

- Domain Start - Triggered by a Serv-U Domain starting, via the **Enable Domain** setting in the **Domain Details > Settings** menu or as part of normal server startup.
- Domain Stop - Triggered by a Serv-U Domain stopping, via the **Enable Domain** setting in the **Domain Details > Settings** menu or as part of normal server startup.
- Session Connection - Triggered by a new TCP session connection.
- Session Disconnect - Triggered by a TCP session disconnection.
- Session Connection Failure - Triggered by a failed session connection attempt.
- Log File Deleted - Triggered by the automatic deletion of a log file, according to logging settings.
- Log File Rotated - Triggered by the automatic rotation of a log file, according to logging settings.
- Listener Success - Triggered by a successful listener connection.
- Listener Stop - Triggered by a stopped listener connection.
- Listener Failure - Triggered by a failed listener connection.
- Gateway Listener Success - Triggered by a successful Gateway listener connection.
- Gateway Listener Stop - Triggered by a stopped Gateway listener connection.

- Gateway Listener Failure - Triggered by a failed Gateway listener connection.
- Permanent Listener Success - Triggered by a successful permanent listener connection.
- Permanent Listener Failure - Triggered by a failed permanent listener connection.
- Permanent Listener Stop - Triggered by a stopped permanent listener connection.
- Permanent Gateway Listener Success - Triggered by a successful permanent Gateway listener connection.
- Permanent Gateway Listener Stop - Triggered by a stopped permanent Gateway listener connection.
- Permanent Gateway Listener Failure - Triggered by a failed permanent Gateway listener connection.
- File Management Rule Success - Triggered when a file management rule is applied, and no errors are encountered.
- File Management Rule Failure - Triggered when a file management rule is applied, and at least one error is encountered.

Server, Domain, User and Group Events

- User Login - Triggered by the login of a user account.
- User Logout - Triggered by the logout of a user account.
- User Login Failure - Triggered by a failed login. A failed login is any connection attempt to Serv-U that fails, whether due to invalid credentials, or a session disconnect before authentication, either due to an incorrect user name, incorrect password, incorrect SSH key pair (for SFTP Public Key Authentication), or any or all of the above.
- User Password Change - Triggered by the change of a password for a user account, either by an administrator or by the user (if permitted).

- User Password Change Failure - Triggered by a failed password change attempt.
- User Enabled - Triggered by the enabling of a user account that was previously disabled.
- User Disabled - Triggered by the disabling of a user account that was previously enabled.
- User Deleted - Triggered by the deletion of a user account by a remote administrator, in an ODBC database, or in the local Management Console.
- User Added - Triggered by the creation of a user account by a remote administrator, in an ODBC database, or in the local Management Console.
- Password Recovery Sent - Triggered by a successful password recovery by an end user or by an administrator.
- Password Recovery Failed - Triggered by a failed password recovery attempt, either due to lack of email address in the user account or lack of permissions.
- Password Stale - Triggered by a stale password, as configured in **Limits & Settings**, that is going to expire.
- User Auto Disable - Triggered by the automatic disabling of a user account, as configured by a user's **Automatically Disable** date.
- User Auto Deleted - Triggered by the automatic deletion of a user account, as configured by a user's **Automatically Delete** date.
- User Pre-disable - Triggered by the upcoming disabling of a user account, as configured in the user's **Automatically Disable** date and the "Days before automatically disabling account to trigger the pre-disable event" limit.
- User Pre-delete - Triggered by the upcoming deletion of a user account, as configured in the user's **Automatically Delete** date and the **Days before automatically deleting account to trigger the pre-delete** event limit.
- User Email Set - Triggered by a user or administrator setting the email address for a user account.

- User Email Set Failure - Triggered by a failed attempt by a user or administrator to set the email address for a user account.
- IP Blocked - Triggered by a failed login attempt due to an IP Access rule.
- IP Blocked Time - Triggered by a failed login attempt due to an IP Access rule that was automatically added by brute force settings, configured in **Domain Limits & Settings** or **Server Limits & Settings**.
- Too Many Sessions - Triggered by more sessions logging on to the server than are permitted, per the **Limits & Settings** for the user account, group, domain, or server.
- Too Many Session On IP - Triggered by more sessions logging on to the server from a specific IP address than are permitted, per the **Limits & Settings** for the user account, group, domain, or server.
- IP Auto Added To Access Rules - Triggered by the automatic addition of an IP Access rule due to a user triggering the "brute force" settings.
- Session Idle Timeout - Triggered by an idle session timeout.
- Session Timeout - Triggered by a session timeout.
- File Uploaded - Triggered by a file uploaded to Serv-U. This event triggers for partial uploads if the upload session terminated with a successful message and no data corruption.
- File Upload Failed - Triggered by a failed file upload to Serv-U.
- File Download - Triggered by a file downloaded from Serv-U.
- File Download Failed - Triggered by a failed file download from Serv-U.
- File Deleted - Triggered by the deletion of a file on the Serv-U server by a user.
- File Moved - Triggered by the moving of a file on the Serv-U server by a user.
- Directory Created - Triggered by the creation of a directory.
- Directory Deleted - Triggered by the deletion of a directory.

- Directory Changed - Triggered by changing the current working directory.
- Directory Moved - Triggered by moving a directory to a new location.
- Over Quota - Triggered by going over disk quota space. The current quota space is shown in the user account, in the **Limits & Settings** menu.
- Over Disk Space - Triggered by exceeding the Max Dir Size configured for a Directory Access rule. The current disk space is shown with the `AVBL FTP` command, or using the **Directory Properties** option in the HTTP/HTTPS Web Client and FTP Voyager JV.

Creating Common Events

Serv-U allows administrators to automatically create a list of the most common events. You can choose to create these common events using email and/or balloon tip actions. Click **Create Common Event** located in the Events tab. Select either the **Send Email** or **Show balloon tip** option for the action you want to be performed on the common events. If you choose to Send Email you must also enter an **To:** address where the events are to be sent.

Note: The **Write to Windows Event Log**, and **Write to Microsoft Message Queue (MSMQ)** options are available for Windows only.

Event Actions

Administrators can select from the following actions that will be executed when an event is triggered:

- Send Email
- Show Balloon Tip*
- Execute Command*
- Write to Windows Event Log (Windows only)*
- Write to Microsoft Message Queue (MSMQ) (Windows only)*

* - Events involving anything other than email may only be configured by Serv-U server administrators.

Email Actions

Email actions can be configured to send emails to multiple recipients and to Serv-U Groups when an event is triggered. To add an email address, enter it in the **To** or **Bcc** fields. To send emails to a Serv-U Group, use the **Group** icon to add or remove Serv-U Groups from the distribution list. Email addresses must be separated by commas or semicolons. Email actions contain a **To**, **Subject** and **Message** parameter. Special variables can be used to send specific data pertaining to the event. For more information about the variables, see "System Variables".

To use email actions, you must first configure SMTP in Serv-U. For information, see "Serv-U SMTP Configuration".

Balloon Tip Actions

Balloon tip actions can be configured to show a balloon tip in the system tray when an event is triggered. Balloon tip actions contain a **Balloon Title** and a **Balloon Message** parameter. Special variables can be used to send specific data pertaining to the event. For more information about the variables, see "System Variables".

Execute Command Actions

Execute command actions can be configured to execute a command on a file when an event is triggered. Execute command actions contain an **Executable Path**, **Command Line Parameters**, and **Completion Wait Time** parameter. For the **Completion Wait Time** parameter, you can enter the number of seconds to wait after starting the executable path. Enter a value of 0 for no waiting.

Note: Any amount of time Serv-U spends waiting delays any processing that Serv-U can perform.

A wait value should only be used to give an external program enough time to perform some operation, such as move a log file before it is deleted (for example, `$LogFilePath` for the Log File Deleted event). Special variables can be used to send specific data pertaining to the event. For more information about the variables, see "System Variables".

Write to Windows Event Log

Writing event messages to a local Windows Event Log allows you to monitor and record Serv-U activity using third-party network management software such as those from HP Openview, SolarWinds, SpiceWorks, and many other vendors. All messages will appear in the Windows Application Log from a source of "Serv-U".

This event has only one field:

- Log Information: The contents of the message to be written into the event log. This is normally either a human-readable message (for example, `filename uploaded by person`) or a machine-readable string (for example, `filename|uploaded|person`), depending on who or what is expected to read these messages. Serv-U system variables are supported in this field. This field may be left blank, but usually should not be left blank.

Write to Microsoft Queue (MSMQ)

Microsoft Message Queuing (MSMQ) is an enterprise technology that lets independent applications communicate quickly and reliably. Serv-U MFT Server can send messages to new or existing MSMQ queues whenever a Serv-U event triggers. Corporations can use this feature to tell enterprise applications that files have arrived, files have been picked up, partners have signed on, or many other activities have just occurred.

These events have the following two fields:

- Message Queue Path: The MSMQ path that addresses the queue. Remote queues can be addressed when a full path (for example, `MessageServer\Serv-U Message Queue`) is specified. Local, public queues on the local machine can be addressed when a full path is not specified (for example, `.\Serv-U Message Queue` or just `Serv-U Message Queue`). If the specified queue does not exist, Serv-U will make its best effort to try to create it. (This normally only works on public queues on the local machine.) Serv-U system variables are supported in this field.

- Message Body: The contents of the message to be sent into the queue. This is normally a text string with a specific format specified by an enterprise application owner or enterprise architect. Serv-U system variables are also supported in this field. This field may be left blank, but usually is not.

Note: Microsoft message queues created in Windows do not grant access to SYSTEM by default, preventing Serv-U from writing events to the queue. In order to correct this, after creating the queue in MSMQ, right-click it, select **Properties**, and then set the permissions so that “SYSTEM” (or the network account under which Serv-U runs) has permission to the queue.

Event Filters

Serv-U Event Filters allow administrators to control to a greater degree when a Serv-U event is triggered. By default, Serv-U Events trigger each time the event occurs. The Event Filter allows events to be triggered only if certain conditions are met. For example, a standard Serv-U Event might trigger an email each time a file is uploaded to the server. However, using an Event Filter, Events can be triggered on a more targeted basis. A File Uploaded event can be configured to only send an email when the file name contains the string `important`, so an email would be sent when the file `Important Tax Forms.pdf` is uploaded but not when random other files are uploaded to the server. Additionally, a File Upload Failed event could be set to run only when the FTP protocol is used, not triggering for failed HTTP or SFTP uploads. This is done by controlling the various variables and values related to the Event and evaluating their results when the event is triggered.

Event Filter Fields

Each Event Filter has the following critical values that must be set:

- Name - This is the name of the filter, used to identify the filter for the event.
- Description (Optional) - This is the description of the event, which may be included for reference.

- Logic - This determines how the filter interacts with other filters for an event. In most cases, AND will be used all filters must be satisfied for the event to trigger. The function of AND is to require that all conditions be met. However, the OR operator can be used if there are multiple possible satisfactory responses (for example, abnormal bandwidth usage of less than 20 KB/s OR greater than 2000 KB/s).
- Filter Comparison - This is the most critical portion of the filter. The Filter Comparison contains the evaluation that must occur for the event to trigger. For example, a filter can be configured so that only the user "admin" triggers the event. In this case, the comparison will be `If $Name = (is equal to) admin`, and the data type will be `string`. For bandwidth, either an "unsigned integer" or "double precision floating point" value would be used.

Event filters also support wildcards when evaluating text strings. The supported wildcards are the following:

- * - The asterisk wildcard matches any text string of any length. For example:
    - An Event Filter that compared the `$FileName` variable to the string `data*` would match files named `data`, `data7`, `data77`, `data.txt`, `data7.txt`, and `data77.txt`.
- ? - The question mark wildcard matches any one character, but only one character. For example:
    - An Event Filter that compared the `$FileName` variable to the string `data?` would match a file named `data7` but not `data`, `data77`, `data.txt`, `data7.txt`, or `data77.txt`.
    - An Event Filter that compared the `$FileName` variable to the string `data?.`* would match files named `data7` and `data7.txt` but not `data`, `data77`, `data.txt`, or `data77.txt`.
    - An Event Filter than compared the `$Name variable` to the string `A????` would match any five-character username starting with `A`.
- [] - The bracket wildcard matches a character against the set of characters inside the brackets. For example:

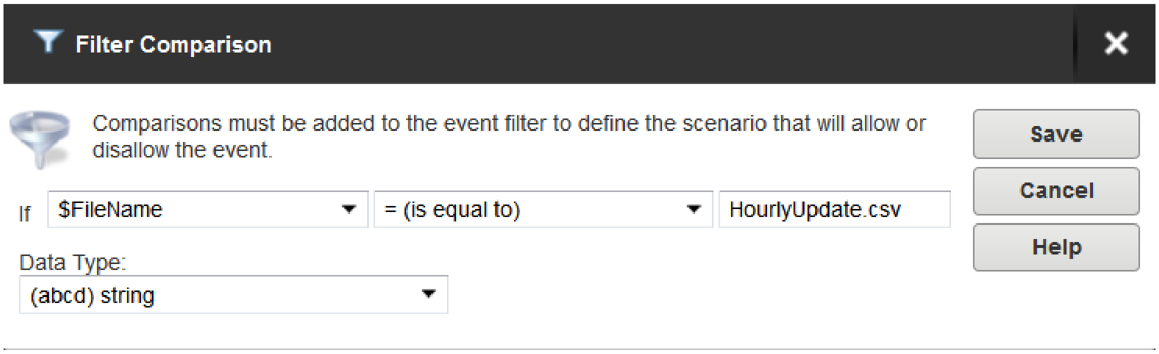
  - An Event Filter that compared the `$FileName` variable to the string `data[687].txt` would match files named `data6.txt`, `data7.txt` and `data8.txt` but not `data5.txt`.
  - An Event Filter that compared the `$LocalPathName` variable to the string `[CD]:\*` would match any file or folder on the `C:` or `D:` drives.

Multiple wildcards can be used in each filter. For example:

- An Event Filter that compared the `$FileName` variable to the string `[cC]:\*.???` would match any file on the `C:` drive that ended in a three letter file extension.
- An Event Filter that compared the `$FileName` variable to the string `?:\*Red[678]\?????.*` would match a file on any Windows drive, contained in any folder whose name contains `Red6`, `Red7` or `Red8`, and that also has a five character file name followed by a file extension of any length.

Using Event Filters

Event filters are used by comparing fields to expected values in the Event Filter menu. The best example is firing an event only when a certain user triggers the action, or when a certain file is uploaded. For example, an administrator may want to fire an email event when the file `HourlyUpdate.csv` is uploaded to the server, but not other files. To do this, a new event can be created in the **Domain Details > Events** menu. The **Event Type** is File Uploaded, and on the Event Filter tab a new filter must be added. The $FileName variable is used and the value is `HourlyUpdate.csv` as shown:

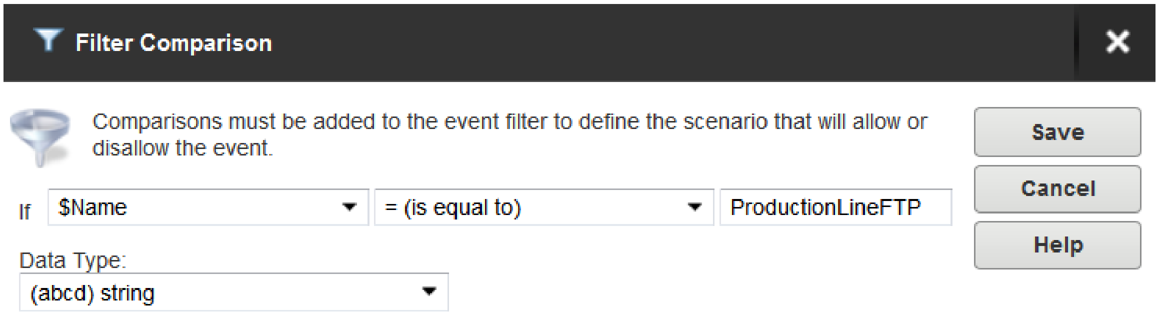


Comparisons must be added to the event filter to define the scenario that will allow or disallow the event.

If $FileName = (is equal to) HourlyUpdate.csv

Data Type: (abcd) string

As another example, it might be necessary to know when a file transfer fails for a specific user account (perhaps one used by an automated process). To perform this task, create a new File Upload Failed event, and then add a new filter. The filter comparison will be `$Name`, and the value to compare would be the username, such as `ProductionLineFTP`:

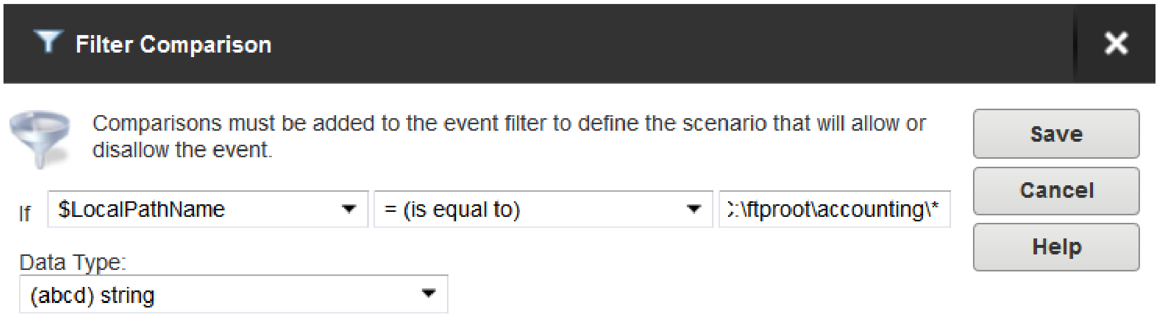


Comparisons must be added to the event filter to define the scenario that will allow or disallow the event.

If $Name = (is equal to) ProductionLineFTP

Data Type: (abcd) string

It is also possible to filter for events based on specific folders, using wildcards. In some cases it may be necessary to trigger events for files uploaded only to a specific folder, such as when an accounting department uploads time-sensitive tax files. To filter based on a folder name, first create a new File Uploaded event in the **Domain Details > Events** menu, and set it to **Send Email**. After specifying the email recipients, subject line, and message content, open the Event Filters tab. Create a new Event Filter, and add the filter comparison `If $LocalPathName = (is equal to) C:\ftproot\accounting\*` with the type of `(abcd) string`. This will cause the event to trigger only for files that are located within `C:\ftproot\accounting\`.



Comparisons must be added to the event filter to define the scenario that will allow or disallow the event.

If $LocalPathName = (is equal to) :\ftproot\accounting\*

Data Type: (abcd) string

License Information

The License Information tab displays the information contained in the current registration ID in use by the Serv-U File Server. If the installation is running in trial mode, then information on the number of trial days remaining is also included. Information contained on this tab includes:

Name

The name associated with the current license.

Email Address

The email address associated with the current license.

Serv-U Edition

The Serv-U Edition that is enabled by the current license. For more information, see "Serv-U Editions".

Copies

The number of concurrent installations allowed by the current license.

Purchase Date

The date the current license was purchased.

Updates

The date through which the current license allows free updates to the latest version. If running as a trial, the number of trial days remaining is displayed.

Additional Products

Additional add-ons for Serv-U and whether or not they are enabled.

Edition Information

Displays the enabled functionality and limitations of the licensed Serv-U Edition.

Registering Serv-U

To register the Serv-U File Server, click **Enter License ID** on the bottom toolbar, and then enter your alphanumeric registration ID. If you have lost your ID, click **Lost ID** for assistance in retrieving it. If you want to purchase an ID, click

Purchase to visit our web site to purchase an ID. To upgrade your Serv-U installation, click **Upgrade License**.

Program Information

The Program Information tab displays information about the current version of Serv-U installed on the server including:

Serv-U File Server Version Number

The full version number for the current installation.

Build Date

The date of the software build for the current installation.

Install Date

The original date that Serv-U was first installed on the computer.

Operating system

Information about the operating system on which Serv-U is installed.

Development Information

Information about the development and localization (if applicable) for the Serv-U File Server.

Contact Information

The contact information for SolarWinds.

Legal Disclaimer

The Serv-U legal disclaimer.

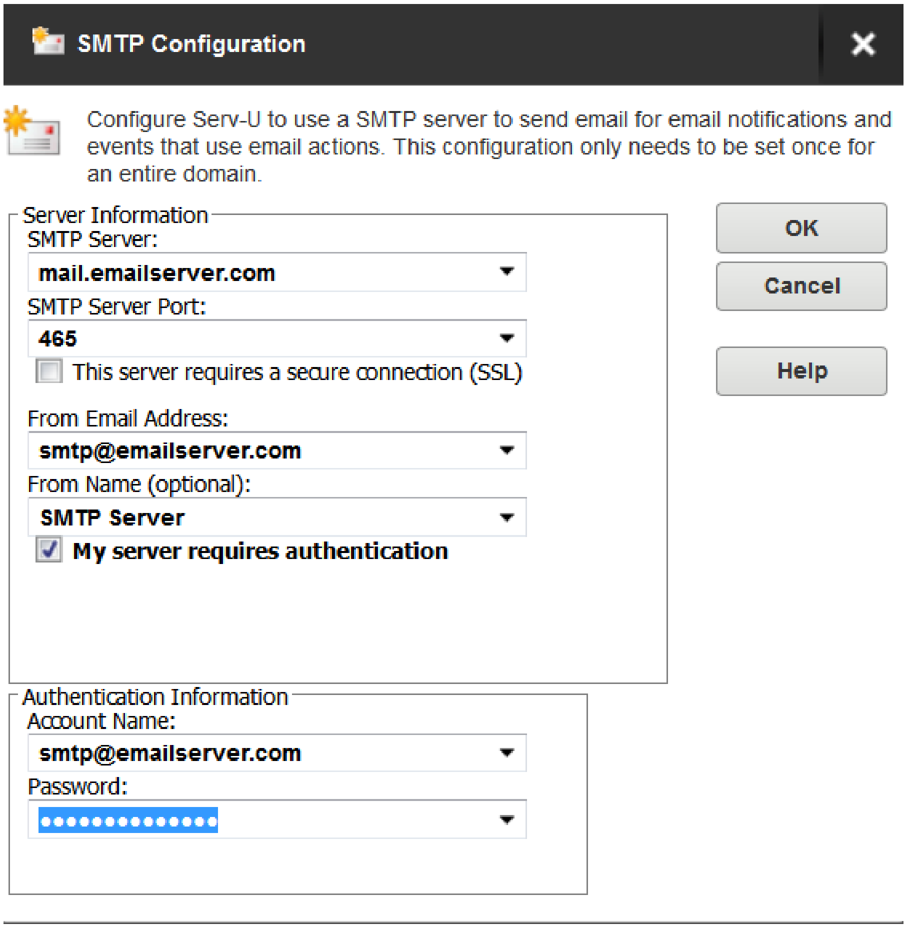
Serv-U SMTP Configuration

Serv-U allows administrators to configure an SMTP connection to send email for events configured to use email actions. SMTP can be configured on the server and/or the domain level. SMTP configuration at the domain level may be inherited from the server level. The SMTP configuration dialog is located in the Events tab in the **Domain Details** and **Server Details** pages.Click **Configure SMTP** to launch the dialog, and then specify the following details:

- SMTP Server - the name or IP address of the SMTP server.
- SMTP Server Port - the port the SMTP server is using.
- From Email Address - the email address to use for the outgoing email.
- From Name (optional) - the name to use for the outgoing email.
- This server requires a secure connection (SSL) - Some SMTP servers require that all incoming connections be encrypted to protect against possible attacks. If your server requires incoming SMTP connections to be encrypted, enable this option. The default port for encrypted SMTP connections is 465. Serv-U supports Implicit SSL only, and does not support Explicit SSL (port 587).
- My server requires authentication - to enable authentication, select this option.

If your SMTP server requires authentication you must enter the following information:

- Account Name - the account name associated with authentication for the SMTP server.
- Password - the password for the account.



Configure Serv-U to use a SMTP server to send email for email notifications and events that use email actions. This configuration only needs to be set once for an entire domain.

Server Information

SMTP Server: mail.emailserver.com

SMTP Server Port: 465

☐ This server requires a secure connection (SSL)

From Email Address: smtp@emailserver.com

From Name (optional): SMTP Server

☑ My server requires authentication

Authentication Information

Account Name: smtp@emailserver.com

Password: ••••••••••••••••

Directory Access Rules

Directory Access Rules

Directory Access rules define the areas of the system that are accessible to user accounts. While traditionally restricted to the user and group levels, Serv-U extends the usage of Directory Access rules to both the domain and server levels through the creation of global Directory Access rules. Directory Access rules specified at the server level are inherited by all users of the File Server. When specified at the domain level, they are only inherited by users belonging to that domain. The traditional rules of inheritance apply where rules specified at a lower level (for example, the user level), override conflicting or duplicates rules specified at a higher level (for example, the server level).

When setting the Directory Access path, the `&#37;USER&#37;`, `&#37;HOME&#37;`, `&#37;USER_FULL_NAME&#37;`, and `&#37;DOMAIN_HOME&#37;` variables are available to simplify the process. For example, use `%HOME%/ftproot/` to create a Directory Access rule that specifies the `ftproot` folder in the user's home directory. Directory access rules specified in this manner are "portable" in the event that the actual home directory changes while maintaining the same subdirectory structure. This leads to less maintenance for the File Server administrator. If the `%USER%` variable is specified in the path, it is replaced with the user's login ID. This variable is useful in specifying a group's home directory to ensure that users inherit a logical and unique home directory. The `&#37;USER_FULL_NAME&#37;` variable can be used to insert the Full Name value into the path (the user must have a "Full Name" specified for this to function). For example, the user "Tom Smith" could use `D:\ftproot\&#37;USER_FULL_NAME&#37;` for `D:\ftproot\Tom Smith`. Finally, the `%DOMAIN_HOME%` macro can also be used to identify the user's home directory. For example, to place a user and their home directory into a common directory use `%DOMAIN_HOME%\%USER%`.

Directory Access rules are applied in the order they are listed. The first rule Serv-U encounters in the list that matches the path of a client's request is the one that is applied for that rule. In other words, if a rule exists that denies access to a particular subdirectory but is listed *below* the rule that grants access to the parent directory, then a user still has access to the subdirectory in question. The arrows on the right side of the Directory Access list are used to rearrange the order in which the rules are applied.

A listing and description of each available directory access permission follows.

File Permissions

Read

Allows users to read (that is, download) files. This permission does not allow users to list the contents of a directory, which is granted by the **List** permission.

Write

Allows users to write (that is, upload) files. This permission does not allow users to modify existing files, which is granted by the **Append** permission.

Append

Allows users to append data to existing files. This permission is normally used to grant users the ability to resume transferring to partially uploaded files.

Rename

Allows users to rename existing files.

Delete

Allows users to delete files.

Execute

Allows users to remotely execute files. Execute access is meant for remotely starting programs and usually applies to specific files. This is a very powerful permission and great care should be used in granting it to users. A user with **Write** and **Execute** permissions can essentially install any program of their choosing on your system.

Directory Permissions

List

Allows users to list the files and subdirectories contained in the directory. Also allows users to list this folder when listing the contents of a parent directory. (See KB #2079 for more information about "blind downloads" and "blind uploads".)

Create

Allows users to create new directories within the directory.

Rename

Allows users to rename existing directories within the directory.

Remove

Allows users to delete existing directories within the directory. **Note:** If the directory contains files, the user also needs to have the **Delete** files permission in order to remove the directory.

Subdirectory Permissions

Inherit

Allows all subdirectories to inherit the same permissions as the parent directory. The **Inherit** permission is appropriate for most circumstances, but if access must be restricted to subfolders (as is the case when implementing Mandatory Access Control), deselect **Inherit** and grant permissions specifically by folder.

Advanced: Access as Windows User (Windows Only)

For a variety of reasons, files and folders may be kept on external servers in order to centralize file storage or provide additional layers of security. In this environment, files can be accessed by the UNC path (`\\servername\folder\`) instead of the traditional `C:\ftproot\folder` path. However, accessing folders stored across the network poses an additional challenge, because Windows services are run under the Local System account by default, which has no access to network resources.

To mitigate this problem for all of Serv-U, it is possible to configure the Serv-U File Server service to run under a network account. The alternative, preferred when many servers exist, or if the Serv-U File Server service needs to run under Local System for security reasons is to configure a Directory Access rule to use a specific Windows User for file access. By clicking the **Advanced** button it is possible to specify a specific Windows user for each individual Directory Access rule. Just like in Windows Authentication, directory access is subject to NTFS permissions, though in this case also to the configured permissions in Serv-U.

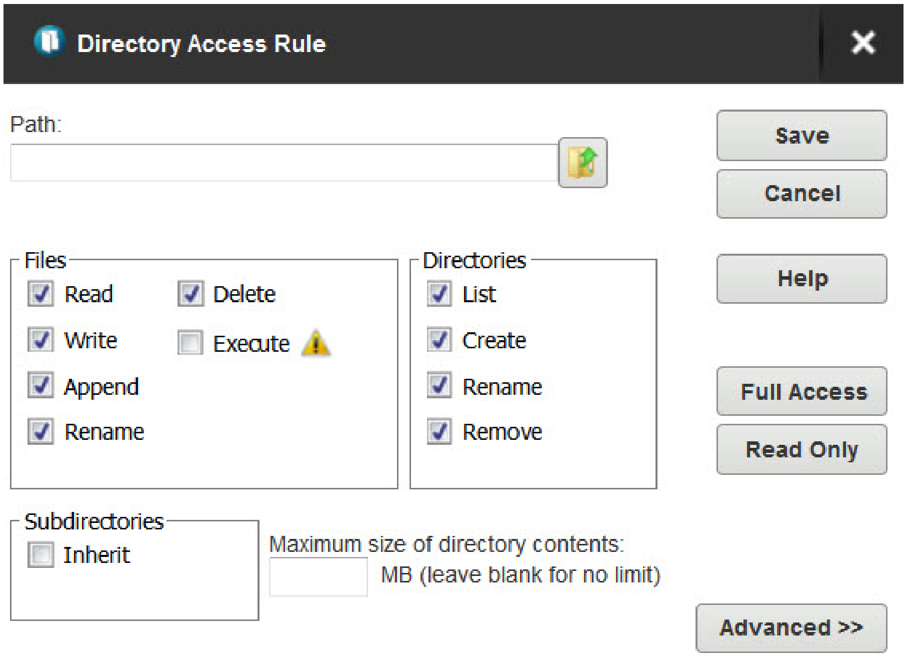
Quota Permissions

Maximum size of directory contents

Setting the maximum size actively restricts the size of the directory contents to the specified value. Any attempted file transfers that cause the directory contents to exceed this value are rejected. This feature serves as an alternative to the traditional quota feature that relies upon tracking all file transfers (uploads and deletions) to calculate directory sizes and is not able to consider changes made to the directory contents outside of a user's File Server activity.

Mandatory Access Control

Serv-U enables the use of Mandatory Access control in cases where users need to be granted access to the same home directory but should not necessarily be able to access the subdirectories below it. To implement Mandatory Access Control at a directory level, disable the **Inherit** permission as shown below (assume the rule applies to `D:\ftproot\`):



Path:

Files
☑ Read
☑ Write
☑ Append
☑ Rename
☑ Delete
☐ Execute

Directories
☑ List
☑ Create
☑ Rename
☑ Remove

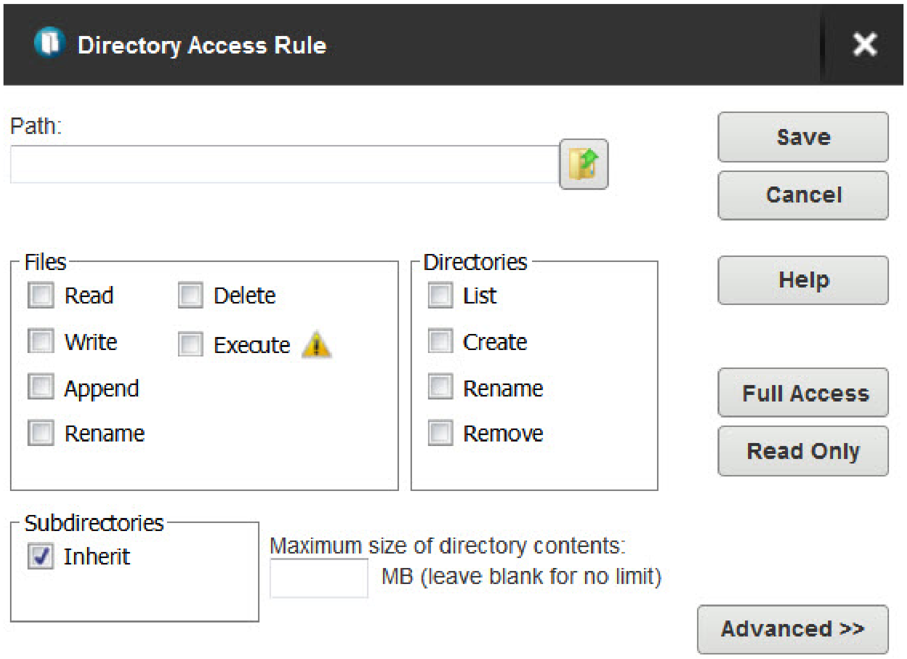
Subdirectories
☐ Inherit

Maximum size of directory contents:
MB (leave blank for no limit)

Now, the user has access to the `ftproot` folder but to no folders below it. Permissions must individually be granted to subfolders that the user needs access to, providing the security of Mandatory Access Control in the Serv-U File Server.

Restricting File Types

If users are using storage space on the Serv-U File Server to store non-work-related files such as MP3 music files, this can be prevented by configuring a Directory Access rule placed **above** the main Directory Access Rule (use the arrows on the right to reorder rules) to prevent MP3 files from being transferred as shown below. In the text entry for the rule, type `*.mp3` and use the permissions shown below:



Path:

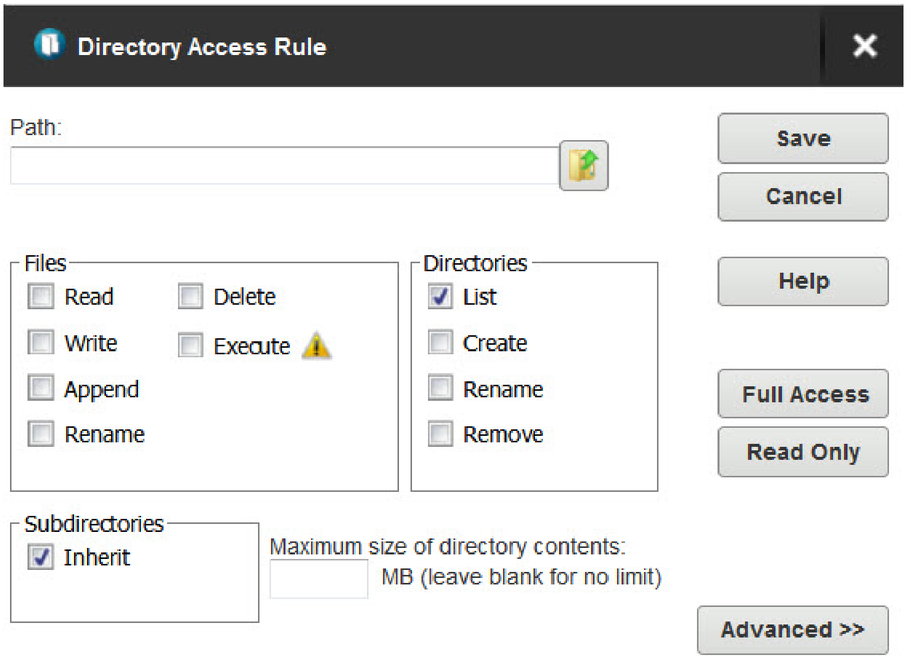
Files
☐ Read
☐ Write
☐ Append
☐ Rename
☐ Delete
☐ Execute

Directories
☐ List
☐ Create
☐ Rename
☐ Remove

Subdirectories
☑ Inherit

Maximum size of directory contents:
MB (leave blank for no limit)

The rule denies permission to any transfer of files with the `.mp3` extension and can be modified to reflect any file extension. Similarly, if accounting employees only need to transfer files with the `.mdb` extension, configure a pair of rules that grants permissions for `.mdb` files but denies access to all other files, as shown below. In the first rule enter the path that should be the user's home directory or directory they need access to, and in the second rule enter the extension of the file that should be accessed (such as `*.mdb`):



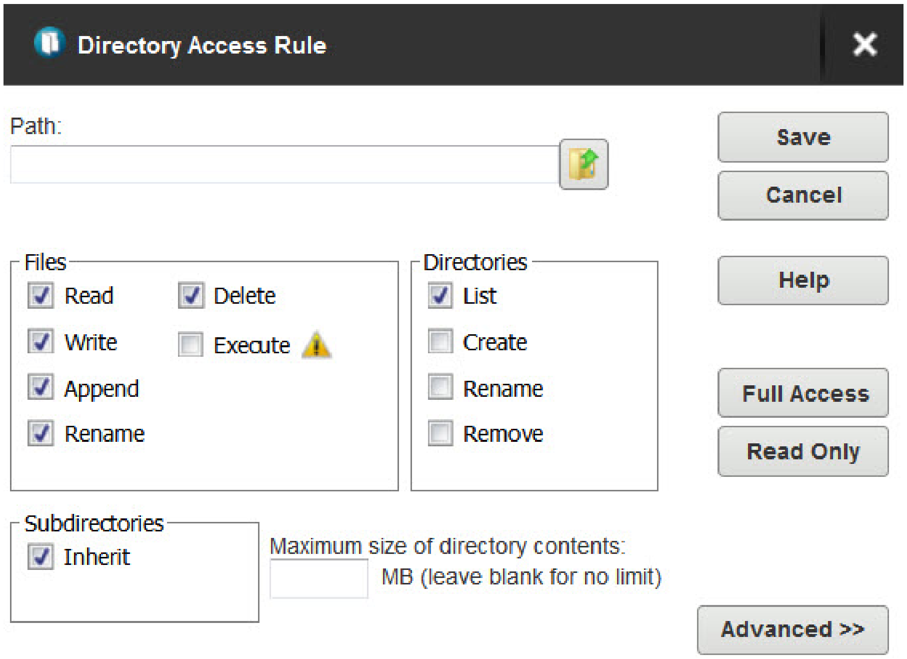
Path:

Files
☐ Read ☐ Delete
☐ Write ☐ Execute ⚠
☐ Append
☐ Rename

Directories
☑ List
☐ Create
☐ Rename
☐ Remove

Subdirectories
☑ Inherit

Maximum size of directory contents:
MB (leave blank for no limit)



Path:

Files
☑ Read ☑ Delete
☑ Write ☐ Execute ⚠
☑ Append
☑ Rename

Directories
☑ List
☐ Create
☐ Rename
☐ Remove

Subdirectories
☑ Inherit

Maximum size of directory contents:
MB (leave blank for no limit)

These rules only allow users to access `.mdb` files within the directories specified, and can be adapted to any file extension or set of file extensions.

Virtual Paths

Virtual Paths allow users to gain access to files and folders outside of their own home directory. A Virtual Path only defines a method of mapping an existing directory to another location on the system to make it visible within a user's accessible directory structure. In order to actually have access to the mapped location, the user must still have a Directory Access rule specified for the physical path of a Virtual Path.

Like Directory Access Rules, Virtual Paths can be configured at the server, domain, group, and user levels. Virtual Paths created at the server level are available for use by all users of the File Server. When created at the domain level, they are only accessible by users belonging to that domain. Serv-U's granular file access controls even allow for Virtual Paths created specifically for individual users or groups.

Physical Path

The physical path is the actual location on the system, or network, that is to be placed in a virtual location accessible by a user. If the physical path is located on the same computer, a full path should be used, such as `D:\inetpub\ftp\public`. A UNC path can also be used, such as `\\Server\share\public`. In order for a Virtual Path to be visible to a user, they must have a Directory Access rule specified for the physical path.

Virtual Path

The virtual path is the location that the physical path should appear in for the user. The `%HOME%` macro is commonly used in the virtual path to place the specified physical path in the home directory of the user. When specifying the virtual path, the last specified directory is used as the name displayed in directory listings to the user. For example, a virtual path of `%HOME%/public` places the specified physical path in a folder named `public` within the user's home directory. A full path without any macros can also be used.

Include in "Maximum Directory Size" calculations

When selected, the Virtual Path is included in Maximum Directory Size calculations. When deselected, the Virtual Path is not included in the Maximum Directory Size calculations. Maximum Directory Size limits the size of directories affecting how much data can be uploaded.

Case File - Using Virtual Paths

A group of web developers have been granted access to the directory `D:\ftproot\examplesite.com\` for web development purposes. The developers also need access to an image repository located at `D:\corpimages\`. To avoid granting the group access to the root D drive, a Virtual Path must be configured so that the image repository *appears* to be contained within their home directory. Within the web developer's group, add a Virtual Path to bring the directory to the users by specifying `D:\corpimages\` as the Physical Path and `D:\ftproot\examplesite.com\corpimages` as the Virtual Path. Be sure to add a group level Directory Access rule for `D:\corpimages\` as well. The developers now have access to the image repository without compromising security or relocating shared resources.

Case File - Creating Relative Virtual Paths

Continuing with the previous example, if the web developer's group home directory is relocated to another drive, not only does the home directory have to be updated, but the Virtual Path also needs to be updated to reflect this change. This can be avoided by using the `%HOME%` macro to create a relative Virtual Path location that eliminates the need to update the path if the home directory changes. Instead of using `D:\ftproot\examplesite.com\corpimages` as the Virtual Path, use `%HOME%\corpimages`. This tells Serv-U to place the `corpimages` Virtual Path within the group's home directory - whatever that may be. If the home directory changes at a later date, the Virtual Path still appears there.

Automated File Management

Using file management rules, you can automatically remove or archive files from the file server. Automated file management rules can be configured at the server and domain level. When specified at the server level, the file management rules are accessible to all users of the file server. When specified at the domain level, they are only accessible to users belonging to that domain.

Depending on the file system, Serv-U uses the creation or change date of files to determine the expiration date. On Windows, the creation date of the file is used to determine when a file is expired. On Linux, the change date is used to determine the expiration date. The change date is updated whenever the file's metadata or index node (inode) is modified. If the contents or attributes (such as the permissions) of the file are modified, the change date is also updated.

Note: The change date is not modified if the file is read from.

The file management rules apply recursively to all files within the folder for which they are configured, and not only to those that have been uploaded through Serv-U. This way it is possible to manage files which are transferred by clients, or which are copied to the folder outside of Serv-U.

The folder structure is not affected by the file management rules. When Serv-U deletes or moves expired files, it leaves the folders themselves intact.

The file management rules run hourly in the background. For this reason, there can be an hour delay before Serv-U deletes or moves an expired file.

To monitor the status of the file management rules, you can configure a File Management Rule Success and a File Management Rule Error event under **Server/Domain Details > Events**. The file management rules continue running even if deleting or moving a single file fails. For more information, see "Serv-U Events".

To define a new file management rule:

1. Navigate to **Directories > File Management**, and then click **Add**.
2. Type the path to the file or folder in the **Directory Path** field, or click **Browse** to navigate to the file or folder.
3. Select the action you want to perform on the file:
    a. If you want to delete the file after it expires, select **Delete file(s) after specified time**.
    b. If you want to move the file after it expires, select **Move file(s) after specified time**, and then specify the folder where you want to move the file in the **Destination Directory Path** field.
4. Specify the number of days after the file creation date when the action should be executed.
5. Click **Save**.

Note: Serv-U regularly and individually checks all the files in the directory for their age, and executes the specified action on the files that meet the age criteria you specify.

Server Limits and Settings

Serv-U offers advanced options which can be used to customize how it can be used as well as ways to apply limits and custom settings to users, groups, domains, and the server in its entirety. The limits stack intelligently, with user settings overriding group settings, group settings overriding domain settings, and domain settings overriding server settings. In addition, limits can be applied only during certain days of the week or times of the day. It is possible to grant exceptions to administrators and restrict specific users more than others, providing total control over the Server. The Limits and Settings in Serv-U are split into the following categories:

- Connection
- Password
- Directory Listing
- Data Transfer
- HTTP
- Email
- File Sharing
- Advanced

To apply a limit, select the appropriate category, click **Add**, select the limit, and then select or enter the value. For example, to disable the **Lock users in home directory** option for a domain, follow these steps:

1. Select **Limits & Settings** in the Serv-U Management Console.
2. Select the **Directory Listing** from the **Limit Type** list.
3. Click **Add**.
4. Select **Lock users in home directory** from the **Limit** list.
5. Deselect the option.
6. Click **Save**.

The limits list displays the current limits applied to the domain. Limits with a light-blue shade to the background are default values. Limits with a white background are values that override the defaults. After completing the above steps, a new Lock users in home directory limit appears in the list that displays "No" for the value. Because of inheritance rules, this option applies to all users in the domain unless overridden at the group or user level. For more information about this method of inheritance, see "User Interface Conventions".

Limits can be deleted by selecting them and clicking **Delete**. To edit an overridden value, select the limit, and then click **Edit**. Default rules cannot be edited or deleted. Create a new limit to override a default one.

To create a limit that is restricted to a specific time of day or days of the week, click **Advanced** on the New / Edit Limit dialog.The additional options allow you to **Apply limit only at this time of day** at which point a start and stop time for the new limit can be entered. To restrict the limit to certain days of the week, deselect the days for which you do not want the limit applied. When a limit is restricted in this way, default values (or the value of other limit overrides) are applied when the time of day or day of the week restrictions are not met for this limit.

The following is a reference of all available **Server** limits, organized by category.

Connection

Maximum number of sessions on server

Specifies the maximum number of concurrent sessions that may be allowed on the entire server.

Maximum sessions per IP address on server

Specifies the maximum number of concurrent sessions that may be opened to the entire server from a single IP address.

Maximum number of sessions per user account

Specifies the maximum number of concurrent sessions that may be opened from a single user account.

Maximum sessions per IP address for user account

Specifies the maximum number of concurrent sessions that a user may open from a single IP address.

Require secure connection before login

Requires that a connection be secure (for example, FTPS, SFTP, or HTTPS), before it is accepted.

Automatic idle connection timeout

Specifies the number of minutes that must pass after the last client data transfer before a session is disconnected for being idle.

Note: Setting the Packet time-out is a requirement for this limit to work. The value of Packet time-out must be less than the value of the Automatic idle connection timeout for the Automatic idle connection timeout to work properly. For information about setting the packet time-out, see "Server Settings".

Automatic session timeout

Specifies the number of minutes a session is allowed to last before being disconnected by the server.

Block anti-timeout schemes

Blocks the use of commands such as "NOOP", which is commonly used to keep FTP Command Channel connections open during long file transfers or other periods of inactivity where no information is being transferred on the control channel. When these are blocked, Serv-U disconnects the client when the connection has been idle, that is, not transferring data for a specified period of time.

Automatically create home directories

Instructs Serv-U whether or not to automatically create the home directory specified when creating a new user account if the directory does not already exist.

Block IP address of timed out session

Specifies the number of minutes for which the IP address of a timed out session is blocked.

Allow X-Forwarded-For to change HTTP connection IP addresses

When enabled, the "X-Forwarded-For" HTTP header parameter changes the IP address of the client for Serv-U. This is useful when all HTTP connections are coming from a proxy server or a load balancer. Proxy servers and load balancers typically append this parameter to the HTTP header so that HTTP servers can identify the actual client IP address and apply security rules as needed.

Require reverse DNS name

Requires that users connecting to the server connect from an IP address that has a valid reverse DNS name, also known as a PTR record. Checks for the existence of a valid PTR record but does not check its contents.

Maximum sessions per IP address on domain

Specifies the maximum number of concurrent sessions that may be opened to the entire domain from the same IP address.

Password

Check anonymous passwords

Specifies whether or not Serv-U should validate email addresses supplied as the password to log in anonymously.

Require complex passwords

Specifies that all user account passwords must contain at least one uppercase and one non-alphabetic character to be considered valid.

Minimum password length

Specifies the minimum number of characters required in a user account's password. Specifying 0 characters indicates that there is no minimum requirement.

Automatically expire passwords

Specifies the number of days a password is valid before it must be changed. Specifying 0 days means passwords never expire.

Allow users to change password

Specifies whether or not users are allowed to change their own passwords.

Mask received passwords in logs

Masks the passwords received from clients from being shown in log files.

Disabling this allows passwords to be displayed in log files, which can be useful for debugging connection problems or auditing user account security.

Password encryption mode

Specifies the level of password encryption on user passwords. The following options are available:

- One-way encryption (more secure) - This option fully encrypts passwords and cannot be reversed. This is the default setting.
- Simple two-way encryption (less secure) - This option encrypts passwords in a reversible format for easy recovery. Use this option when users are expected to take advantage of the Password Recovery utility in the Web Client. In this case it may be desirable to use two-way encryption so that Serv-U does not need to reset their passwords when password recovery is requested.
- No encryption (not recommended) - This option stores passwords in clear text. Using this option may be necessary for integration with legacy systems (especially when using database support).

Note: When you change this setting, all user passwords must be reset. Existing passwords are not updated automatically, and must be re-saved to be stored in the new format.

Allow users to recover passwords

If enabled, allows users to recover passwords using the Web Client password recovery utility at the login page.

SSH authentication type

Specifies how SSH authentication is to occur. The following options are available:

- Password and Public Key - requires both a password and a public key (when specified) for login
- Password or Public Key - requires either a password or public key for login

- Public Key Only - requires that a public key is provided for successful login, a password is not allowed
- Password Only - requires that a password is provided for successful login, a public key is not allowed.

Note: The Public Key Only authentication type allows users to log in with a password if they have no SSH key configured in Serv-U. This way the administrator cannot deny access to a user account through misconfiguration.

Days before considering password to be stale

The number of days prior to expiration that a password is to be considered stale. A stale password is a password that is about to expire. An event can be configured to identify when a password is about to expire. This value is the lead-time, in days, before password expiration.

Directory Listing

Hide files marked as hidden from listings

Hides files and folders from directory listings that have the Windows "hidden" system attribute set on them.

Use lowercase for file names and directories

Forces Serv-U to display all file names and directories using lowercase characters, regardless of the actual letter case in use by the file or directory.

Interpret Windows shortcuts as links

Instructs Serv-U to treat all valid .lnk files as the actual destination object. In other words, if a .lnk file points to another file, the destination file is shown in the directory listing instead of the .lnk file itself.

Treat Windows shortcuts as target in links

Instructs Serv-U to treat all valid .lnk (shortcut) files as a UNIX symbolic link.

Lock users in home directory

Locks users into their home directory, and does not allow users to browse above that folder. In addition, their home directory is displayed as "/"

masking the actual physical location.

Allow root ("/") to list drives for unlocked users (Windows Only)

Allows users to change directory to the root ("/") of the system and display all drives on the computer. This option only works when the user is not locked in their home directory.

Hide the compressed state of files and directories

Hides the compressed state of all compressed files and directories being viewed by the user.

Hide the encrypted state of files and directories

Hides the encrypted state of all encrypted files and directories being viewed by the user.

Message file path

Welcome messages are normally displayed once to a user during login to relay important information to users about the file server site. By using a secondary message file, welcome messages can be provided in specific folders to relay additional information. A non-relative path such as `MessageFile.message` can be used as the path. The welcome message will only be displayed when navigating into folders which contain a file matching the specified file name.

Directory listing mask (Windows Only)

Specifies the text string sent to FTP clients for file permissions. Windows does not support traditional file permissions like Unix making this option largely cosmetic, however some clients require a certain mask to operate correctly.

Data Transfer

Maximum upload speed for server

Limits the maximum bandwidth that can be used server-wide for all uploads. Setting a limit of 0 KB/s means unlimited bandwidth.

Maximum download speed for server

Limits the maximum bandwidth that can be used server-wide for all downloads. Setting a limit of 0 KB/s means unlimited bandwidth.

Maximum upload speed per session

Limits the maximum upload bandwidth for each individual session. Setting a limit of 0 KB/s means unlimited bandwidth.

Maximum download speed per session

Limits the maximum download bandwidth for each individual session. Setting a limit of 0 KB/s means unlimited bandwidth.

Maximum upload speed for user accounts

Limits the maximum upload bandwidth shared between all sessions associated with an individual user account. Setting a limit of 0 KB/s means unlimited bandwidth.

Maximum Upload File Size

Restricts the maximum single file size a user can upload to Serv-U. File size is measured in kilobytes.

Maximum download speed for user accounts

Limits the maximum download bandwidth shared between all sessions associated with an individual user account. Setting a limit of 0 KB/s means unlimited bandwidth.

Delete partially uploaded files

Instructs Serv-U to delete incomplete file uploads. If this option is enabled, users are not able to restart interrupted uploads using the REST (Restart) FTP command.

Interpret line feed byte as a new line when in ASCII mode (Windows Only)

When uploading and downloading files using ASCII mode, Serv-U will assume <LF> characters are the same as <CR><LF> end-of-line markers. Most Windows applications expect <CR><LF> to represent a new-line, as does the FTP protocol. However, since the definition of a new-line sequence is not fully defined in Windows, this option allows Serv-U to assume <LF> is the same as <CR><LF>. When uploading in ASCII mode stand-alone <LF> characters are changed to <CR><LF> prior to writing to the file. When downloading in ASCII mode, stand-alone <LF> characters are changed to <CR><LF> prior to sending to the client.

Automatically check directory sizes during upload

Instructs Serv-U to occasionally check the size of directories in which a maximum directory size has been specified. This attribute ensures that Serv-U always has updated directory sizes available instead of having to calculate them at transfer time, which can be a time consuming operation.

File upload access

Specifies the method in which uploaded files are opened while they are being received from a client. The default **Allow read access** means that other clients may attempt to download the file even while it is still being received. **Allow full access** means other clients can read from and write to the file while it is being transferred. To prevent any other client from accessing a file while it is still being transferred, select **Allow no access**.

File download access

Specifies the method in which downloaded files are opened while they are being sent to a client. The default **Allow read access** means that other clients may also attempt to concurrently download the same file. **Allow full access** means other clients can read from and write to the file while it is being sent to another client. To prevent any other client from accessing a file while it is still being sent, select **Allow no access**.

Maximum simultaneous thumbnails

Specifies the maximum number of threads that are dedicated towards generating thumbnail images for HTTP clients and in response to the FTP THUMB command. Generating thumbnails is a CPU intensive operation. Increasing this value too high may cause thumbnails to take longer to generate, even while Serv-U is able to handle more client thumbnail requests concurrently.

HTTP

Warn end users when using old web browsers

When enabled (default) Serv-U will warn users that they are using an outdated browser and should upgrade the browser to take advantage of performance and feature enhancements to improve their experience.

Default language for Web Client

When the end-user connects with an unsupported language, the HTTP Login Page is displayed in English. The default language can be set to any language you want. When connecting to Serv-U using a supported localization of Windows, the native language of Windows is used.

Allow HTTP media playback

The Serv-U Web Client supports fully interactive media playback of audio and video files. This function can be disabled as desired during specific business hours or altogether based on business needs.

Allow browsers to remember login information

The HTTP login page supports a **Remember me** option (not enabled by default) that allows user names to be remembered by the login page. This feature can be disabled for security reasons.

Allow users to change languages

The Serv-U Web Client is supported in many languages, but if users should not be able to select their native language this can be disabled.

Allow users to use Web Client

Serv-U Web Client is enabled by default. Administrators can disallow the use of Serv-U Web Client by disabling this limit.

Allow users to use Web Client Pro

Serv-U Web Client Pro is enabled by default. Administrators can disallow the use of Serv-U Web Client Pro by disabling this limit.

Allow users to use FTP Voyager JV

FTP Voyager JV is enabled by default. Administrators can disallow the use of FTP Voyager JV by disabling this limit.

Maintain file dates and times after uploading (FTP Voyager JV and Web Client Pro only)

When enabled, Serv-U can maintain the last modification date and time of the file when end-users are using FTP Voyager JV or Web Client Pro. When disabled, Serv-U will not set the file's last modification date and time, it will remain the date and time the file was uploaded.

Allow HTTP sessions to change IP address (disabling may cause mobile devices to fail)

The Serv-U Web Client supports the transfer of HTTP sessions if the IP address changes. This option can be disabled but it may cause mobile devices to be disconnected due to frequent IP address changes by these devices.

Hide Serv-U version information in HTTP response headers

When enabled, the version information of Serv-U will be hidden in HTTP and HTTPs response headers. This way a potential security threat arising from the knowledge of the version information can be mitigated.

Allow autocomplete for HTTP login fields

With this limit you can configure whether or not password auto-completion is allowed on the Serv-U login screen. This option is enabled by default.

File Sharing

Require a password for guest access

Specifies whether it is possible to set up a file share where the guest is required to provide a password. When this limit is set to Always or Never, the creator of the file share will not be able to specify this optional setting. When this limit is set to Optional, the user can individually specify in each file share whether or not the guest must provide a password.

Insert passwords within invitation emails

Specifies whether it is possible to set up a file share where the password for the share is included in the invitation email. When this limit is set to Always or Never, the creator of the file share will not be able to specify this optional setting. When this limit is set to Optional, the **Include the password in the email** option can be selected individually in each file share.

Maximum file size guests can upload (per file)

Specifies the file size constraints imposed upon the guest user. If set to 0, there is no file size constraint. In this case, the creator of the file share request can specify the maximum file size in each file share request without an upper limit.

Allow user-defined guest link expiration

When enabled, users will be able to specify link expiration dates individually on the Request Files and Send Files wizards. When disabled, the file share links will expire after the number of days specified in the **Duration before guest link expires** limit.

Duration before guest link expires

Limits the number of days after which a file share link expires if the Allow user-defined guest link expiration limit is disabled.

Notify user after a file is downloaded

Specifies whether the **Notify me when the file(s) have been downloaded** option can be used on the Send Files wizard. When this limit is set to Always or Never, the creator of the file share will not be able to specify this optional setting. When this limit is set to Optional, the user can individually specify in each file share whether to receive notification of the file download.

Notify user after a file is uploaded

Specifies whether the **Notify me when the file(s) have been uploaded** option can be used on the Request Files wizard. When this limit is set to Always or Never, the creator of the file share request will not be able to specify this optional setting. When this limit is set to Optional, the user can individually specify in each file share request whether to receive notification of the file upload.

Send the guest access link to the recipients

Specifies whether the **Automatically send the download/upload link to the guest user(s) in email** option can be used on the Send Files and Request Files wizard. When this limit is set to Always or Never, the user will not be able to specify this optional setting. When this limit is set to Optional, the user can individually specify in each file share or file share request whether to send the access link automatically.

Send the guest access link to the sender

Specifies whether the **Send me an email copy with the download/upload link** option can be used on the Send Files and Request Files wizard. When this limit is set to Always or Never, the user will not be able to specify this optional setting. When this limit is set to Optional, the user can individually specify in each file share or file share request whether to receive an email copy with the download/upload link.

Allow user-defined contact information

When enabled, users will be able to edit their name and email address on the Request Files and Send Files wizards. When disabled, users are not allowed to edit their contact information on the Request Files and Send Files wizards.

Maximum number of files for "Sent" shares

Specifies the maximum number of files users can include in a single file share. If set to 0, the default limit of 20 is used.

Maximum number of files for "Requested" shares

Specifies the maximum number of files users can upload after receiving a file share request. If set to 0, the default limit of 20 is used.

Advanced

Convert URL characters in commands to ASCII

Instructs Serv-U to convert special characters contained in command parameters to plain ASCII text. Certain Web browsers can encode special characters contained in file names and directories when using the FTP protocol. This attribute allows Serv-U to decode these special characters.

Inline out-of-band data

Parse out-of-band socket data into the regular TCP data stream, treating it like normal data. This option is useful to counter denial-of-service attacks that send large amounts of out-of-band (OOB) data to socket stacks that cannot handle large amounts of OOB data.

Send keep alive packets to detect broken connections

Periodically sends keep-alive packets to determine if the socket is still connected.

Disable usage of Nagle algorithm

Disables waiting for the ACK TCP handshake before sending the next packet. This option is typically only used for connections with very large latencies, such as satellite links.

Use adaptive time-out on fast file uploads

Slowly lower packet time-out for consistently fast transfers during file uploads. If the transfer does not complete successfully, adaptive time-outs make it easier to resume the upload since Serv-U recognizes more quickly that the transfer is dead and thus allows access to the file sooner.

Maximum supported SFTP Version

Specifies the maximum version of SFTP permitted for SFTP connections. Serv-U supports SFTP versions 3-6.

Allow rename overwrite

When enabled, (default) Serv-U allows files to be renamed to files where the destination already exists. When disabled, users are not allowed to rename a file or directory to a path name that already exists.

Apply server and domain directory access rules before user and group

The order in which Directory Access Rules are listed has significance in determining the resources that are available to a user or group account. By default, Directory Access Rules specified at the group or user level take precedence over ones specified at the domain and server level. However, there are certain instances where you may want the domain and server level rules to take precedence. Setting this value to "Yes" places the group's and user's Directory Access Rules *below* the server and domain. Please also refer to the "Apply group directory access rules first" setting which is outlined on Group Information.

Days before automatically disabling account to trigger the pre-disable event

The number of days prior to automatically disabling the user account that the pre-disable event should be triggered.

Days before automatically deleting account to trigger the pre-delete event

The number of days prior to automatically deleting the user account that the pre-delete event should be triggered.

Reset user stats after restart

When this limit is enabled the user statistics are reset after a server restart.

Reset group stats after restart

When this limit is enabled the group statistics are reset after a server restart.

Owner ID (user name) for created files and directories (Linux Only)

The user name given to set as the owner of a created file or directory.

Group ID (group name) for created files and directories (Linux Only)

The group name given to set as the owner of a created file or directory.

Server Settings

The **Server Limits & Settings > Settings** tabs allow you to configure basic server settings that affect performance, security, and network connectivity. To configure a setting, type the value you want in the appropriate area, and then click **Save**. This topic contains detailed information about the settings that can be configured.

Connection Settings

Block users who connect more than 'x' times within 'y' seconds for 'z' minutes

Also known as anti-hammering, enabling this option is a method of preventing brute force password guessing systems from using dictionary style attacks to locate a valid password for a user account. Using strong, complex passwords defeats most dictionary attacks. However, enabling this option ensures that Serv-U does not waste time processing connections from these illegitimate sources. When configuring this option, ensure that there is some room available for legitimate users to correct an incorrect password before they are blocked.

When enabled, this option temporarily blocks IP addresses for 'z' minutes that fail to successfully login after 'x' attempts within 'y' seconds. IP addresses blocked in this way can be viewed in the appropriate IP Access rules tab. A successful login resets the counter tracking attempted logins.

Hide server information from SSH identity

After a successful SSH login, the server sends identification information to the client. Normally, this information includes the server name and version number. Enable this option to prevent the information from being given to the client.

Default Web Client

Specifies whether the Web Client or FTP Voyager JV should be used by all HTTP clients by default. A third option (the default option) is to prompt the user for the client they want to use instead. This option is also available at the group and user level.

Client Support Link

The Client Support Link is a powerful feature that allows a direct method of contact to be inserted into the Web Client and FTP Voyager JV in the event that a client requires support or assistance. The basic syntax for this feature is `protocol:path`. This option is highly flexible and allows for any network shortcut to be used, such as:

```
http://www.website.com/support/
```

```
mailto:service@website.com?subject=Serv-U File Server Support
```

```
aim:goim?screenname=ExampleAdminUser&message=I need help with your
Serv-U File Server!
```

Any format can be used as long as the client's machine understands the provided protocol.

Network Settings

Auto-configure firewall through UPnP (Windows Only)

When enabled, Serv-U automatically configures the necessary port forwards in your UPnP-enabled network device (usually a router) so that the File Server is accessible from outside your network. This is particularly useful in enabling PASV mode FTP data transfers.

Packet time-out

Specifies the timeout, in seconds, for a TCP packet transfer. Only very slow networks experiencing high levels of latency may need to change this value from the default 300 seconds.

PASV Port Range

Specifies the inclusive range of ports that Serv-U should use for PASV mode data transfers. Serv-U normally allows the operating system to assign it a random port number when opening a socket for a PASV mode data transfer. This attribute accommodates routers or firewalls that need to know a specific range of ports in advance by restricting Serv-U's PASV port range to a known range. A range of 10 ports is sufficient for the busiest of file servers.

Note: Some NAT routers work differently and may require a larger port range. If Serv-U and clients have troubles listing directories or transferring files, try increasing the port range here and on your router.

Other Settings

Ratio Free Files

Files listed by opening the **Ratio Free Files** button are exempt from transfer ratio limitations on file transfers. Ratio free files specified at the server or domain level are inherited by all their users accounts. For more information, see "Transfer Ratio and Quota Management".

Change Admin Password

The Serv-U Management Console can be password protected when it is launched by double-clicking on the Serv-U system tray icon. When the Management Console is running in this way, the option to change the password becomes available. By default, there is no admin password.

FTP Settings

The Serv-U File Server allows for the customization of the FTP commands that it accepts as well as its responses to FTP commands received. When configuring these options at the server level, all domains inherit these customizations. To customize the FTP behavior for a specific domain, select the appropriate domain, open the FTP Settings tab for the domain, and then click **Use Custom Settings** . At any time, you can click **Use Default Settings** to have the domain revert back to the server's default settings.

Warning: Customizing the FTP behavior in this way is not recommended except for those very familiar with the FTP protocol and its standard and extended command set.

Global Properties

When using custom settings, the **Global Properties** button becomes available.

FTP Responses

Global FTP responses are responses shared amongst most FTP commands, such as the error message sent when a file is not found.

Customizing a global FTP response ensures that the response is used by all other FTP commands rather than having to customize it for each individual FTP command. FTP command responses can contain special macros that allow real-time data to be inserted in to the response. For more information, see "System Variables".

Message File

The server welcome message is sent in addition to the standard "220 Welcome Message" that identifies the server to clients when they first connect. If the **Include response code in text of message file** option is selected, then the 220 response code begins each line of the specified welcome message. To customize the welcome message, enter the path to a text file in **Message File Path** field. Click **Browse** to select a file on the computer. Serv-U opens this file and sends its contents to connecting clients.

Advanced Options

- Block "FTP_bounce" attacks and FXP (server-to-server transfers) - Select this option to block all server-to-server file transfers involving this Serv-U File Server by only allowing file transfers to the IP address in use by the command channel. For more information about FTP_bounce attacks, see CERT advisory CA-97.27.
- Include response code on all lines of multi-line responses - The FTP protocol defines two ways in which a multi-line response can be issued by an FTP server. Some older FTP clients have trouble parsing multi-line responses that do not contain the 3-digit response code on each line. Select this option if your clients are using an FTP client experiencing problems with multi-line responses from Serv-U.
- Use UTF-8 encoding for all sent and received paths and file names - By default, Serv-U treats all file names and paths as UTF-8 encoded strings. It also sends all file names and paths as UTF-8 encoded strings, such as when sending a directory listing. Deselecting this option prevents Serv-U

from UTF-8 encoding these strings. When this option is deselected, UTF-8 is not included in the FEAT command response to indicate to clients that the server is not using UTF-8 encoding.

Editing FTP Commands and Responses

To edit FTP Commands, select the FTP command to edit, and then click **Edit**.

Information

Under the Information tab, basic information about the command is shown along with a link to more information on our website. Each FTP command can also be disabled by selecting the **Disable command** option. Disabled commands are treated as unrecognized commands when they are received from a client.

FTP Responses

Under the FTP Responses tab, all possible FTP responses to the command as issued by the server can be modified by clicking **Edit** for each response. FTP command responses can contain special macros that allow real-time data to be inserted in to the response. For more information, see "System Variables".

Message Files

Certain FTP commands allow a message file to be associated with them. The contents of a message file are sent along with the standard FTP response. In addition, a secondary message file path is available as a default option. This allows for message files to be specified using a path relative to the user's home directory for the Message File. If the first message file is not found, then Serv-U attempts to use the Secondary Message File instead. By specifying an absolute file path in the secondary location, you can ensure that each user receives a message file.

The following FTP commands allow specifying a message file:

- CDUP
- CWD

- QUIT

Managing Recursive Listings

Serv-U supports recursive listings by default, allowing FTP clients to obtain large directory listings with a single command. In some cases, clients may request excessively large directory listings using the -R parameter to the LIST and NLST commands. If performance in Serv-U is being impacted by users requesting excessively large listings, recursive listings can be disabled using the **Allow client to specify recursive directory listings with -R parameter** option.

Advanced Options

Some FTP commands contain advanced configuration options that offer additional ways to configure the behavior of the command. Where available, the configuration option is described in detail in the Management Console. The following FTP commands contain advanced configuration options:

- LIST
- MDTM
- NLST

Case File - Custom FTP Command Response

Users connecting to the server need to know how much quota space is available in a given folder when they have completed a transfer. To do this, edit the response to the STOR command to include a report on available space. By default, the 226 (command successful) response to the STOR command (which stores files on the server) is the following:

```
Transfer complete. $TransferBytes bytes transferred.
$TransferKBPerSecond KB/sec.
```

Modify this to include an extra variable in the following way:

```
Transfer complete. $TransferBytes bytes transferred.
$TransferKBPerSecond KB/sec. Remaining storage space is $QuotaLeft.
```

The last sentence shows the user how much storage space is left at the end of each file upload. The same can be done for the DELE command, so that every time a user deletes a file, their updated quota value, showing an increase in available space, is displayed. This can be done for any FTP command response.

Encryption

Serv-U supports two methods of encrypted data transfer - Secure Socket Layer (SSL) and Secure Shell 2 (SSH2). SSL is used to secure the File Transfer Protocol (FTP) and Hypertext Transfer Protocol (HTTP). SSH2 is a method of securely interacting with a remote system that supports a method of file transfer commonly referred to as SFTP. Despite its name, SFTP does not have anything in common with the FTP protocol itself.

In order for each method of encryption to work, a certificate and/or private key must be supplied. SSL requires the presence of both, while SSH2 only requires a private key. If you do not possess either of these required files, Serv-U can create them for you.

Encryption options specified at the server level are automatically inherited by all domains. Any encryption options specified at the domain level automatically overrides the corresponding server-level option. Certain configuration options are only available to the server.

When creating SSL/TLS, SSH, and HTTPS encrypted domains within Serv-U, it is important to know that encrypted domains cannot share listeners. Because SSL/TLS and SSH encryption is based on encrypting traffic sent between IP addresses, each domain must have unique listeners in order to operate properly. In the case that multiple encrypted domains are created that share listeners, the domain created first takes precedence causing other encrypted domains to fail to function properly. To operate multiple encrypted domains, modify the listeners of each domain to ensure they listen on unique port numbers.

Configuring SSL for FTPS and HTTPS

To use an existing certificate:

1. Obtain an SSL certificate and private key file from a certificate authority.
2. Place these files in a secured directory in the server.
3. Use the appropriate **Browse** button to select both the certificate and private key files.
4. If a CA (Certificate Authority) PEM file has been issued, enter or browse to the file.
5. Enter the password used to encrypt the private key file.
6. Click **Save**.

If the provided file paths and password are all correct, Serv-U begins using the certificate immediately to secure FTPS and HTTPS connections using the provided certificate. If the password is incorrect or Serv-U cannot find either of the provided files, an error message is displayed that explains the encountered error.

To create a new certificate:

1. Click **Create Certificate**.
2. Specify the **Certificate Set Name** that is used to name each of the files Serv-U creates.
3. Specify the output path where the created files are to be placed. In most cases, the installation directory is a safe location (for example, `C:\ProgramData\RhinoSoft\Serv-U\`).
4. Specify the city or town in which the server or corporation is located.
5. Specify the state (if applicable) in which the server or corporation is located.
6. Specify the 2-digit country code for the country in which the server or corporation is located.
7. Specify the password used to secure the private key.

8. Specify the full organization name.
9. Specify the common name of the certificate. The IP address or the Fully Qualified Domain Name (FQDN) that users use to connect must be listed here. **Note:** If the Common Name is not the IP address or FQDN used by clients to connect, clients may be prompted that the certificate does not match the domain name they are connecting to.
10. Specify the business unit the server resides in.
11. Specify the key length in bits.
12. Click **Create** to complete the certificate creation.

Serv-U creates three files using the provided information: A self-signed certificate (.crt) that can be used immediately on the server but is not authenticated by any known certificate authority, a certificate request (.csr) that can be provided to a certificate authority for authentication, and a private key file (.key) that is used to secure both certificate files. It is extremely important that the private key be kept in a safe and secure location. If your private key is compromised, then your certificate can be used by malicious individuals.

Viewing the certificate

To view the SSL certificate once it is configured, click **View Certificate**. All identifying information about the certificate, including the dates during which the certificate is valid, are displayed in a new dialog.

Advanced SSL Options

The advanced SSL options can only be configured at the server level. All domains inherit this behavior, which cannot be individually overridden.

- Enable low-security SSL ciphers - Select this option to enable low-security SSL ciphers to be used. Some older or international clients may not support today's best SSL ciphers. Because these ciphers are considered insecure by today's computing standards, Serv-U does not accept these ciphers by default.

- Disable SSLv2 support - There are several different versions of SSL supported by Serv-U. An older version, SSLv2, has documented security weaknesses that make it less secure than SSLv3 and TLS. However, it may be necessary to support SSLv2 for compatibility with exported clients or old client software. Select this option to disable support for the older SSLv2 protocol.
- SSL Ciphers - By default, the low security SSL ciphers are disabled for use by the server. To enable these ciphers select **Enable low-security SSL ciphers**. These ciphers are listed in the third column under **SSL Ciphers**. All other SSL ciphers are enabled by default. If your specific security needs dictate that only certain ciphers can be used, you can individually disable unwanted ciphers by deselecting the corresponding options.

FIPS Options

Enable FIPS 140-2 mode - FIPS 140-2 is a set of rigorously tested encryption specifications set by the National Institute of Standards and Technology (NIST). Enabling FIPS 140-2 mode limits Serv-U to encryption algorithms certified to be FIPS 140-2 compliant and ensures the highest level of security for encrypted connections.

SFTP (Secure File Transfer over SSH2)

To use an existing private key

1. Obtain a private key file.
2. Place the private key file in a secured directory in the server. Use **Browse** in Serv-U to select the file.
3. Enter the password for the private key file.
4. Click **Save**.

To create a private key:

1. Click **Create Private Key**.
2. Enter the name of the private key (for example, `MyDomain Key`), which is also used to name the storage file.
3. Enter the output path of the certificate (for example, `C:\ProgramData\RhinoSoft\Serv-U\`).
4. Select the Key Type (default of DSA is preferred, but RSA is available).
5. Select the Key Length (default of 1024 bits provides best performance, 2048 bits is a good median, while 4096 bits provides best security).
6. Enter the password to use for securing the private key file.

SSH Ciphers and MACs

By default, all supported SSH ciphers and MACs (Message Authentication Codes) are enabled for use by the server. If your specific security needs dictate that only certain ciphers or MACs can be used, you can individually disable unwanted ciphers and MACs by deselecting the appropriate ciphers or MACs.

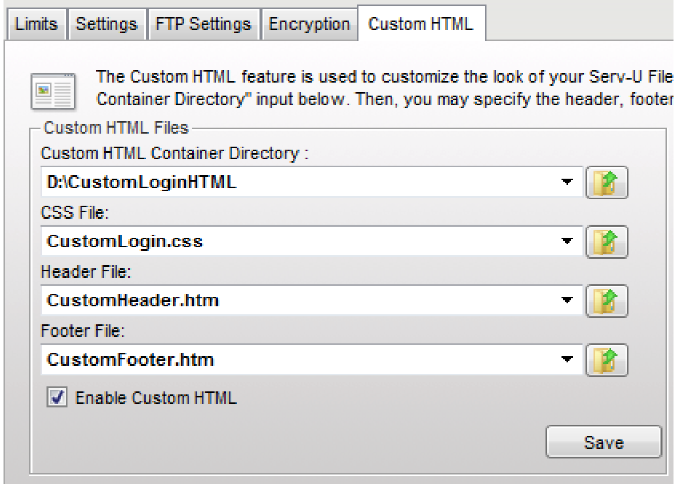
Custom HTML

Serv-U supports custom HTML for the HTTP/HTTPS login pages. This feature allows experienced web developers to design their login experience to show off their exclusive brand and design the page to match existing business themes. Basic branding (custom logo and limited text changes) is also available. For more information, see "Domain Settings".

The Custom HTML feature operates by allowing a web developer to provide a custom header and custom footer for the HTTP/HTTPS login page, while the main Login Form is automatically inserted between the content defined in the Header File and Footer File. The Custom HTML interface also uses a CSS file which defines the style used in the Login Form. This CSS file can also be used to define custom CSS styles, containers, other CSS formatting as needed.

Several branding samples are automatically unpacked to your installation folder (for example, `C:\Program Files\RhinoSoft\Serv-U\Custom HTML Samples`) when Serv-U is installed. Serv-U KB #2054 has step-by-step instructions to explore the current set of samples and build your own branding.

The fields used by the Custom HTML feature are the following:



The Custom HTML feature is used to customize the look of your Serv-U File
Container Directory" input below. Then, you may specify the header, footer

Custom HTML Container Directory : D:\CustomLoginHTML

CSS File: CustomLogin.css

Header File: CustomHeader.htm

Footer File: CustomFooter.htm

☑ Enable Custom HTML

- Custom HTML Container Directory - This directory contains all of the files used by the Custom HTML, including all images, the Header File, the Footer File, and the CSS file. Subdirectories in this folder are allowed.
- CSS File - This .CSS file contains all the styles, containers, and other formatting that will be used throughout the Header File and Footer File, as well as the styles that will be used by the Login Form.
- Header File - This .HTM file contains the content for the HTML header content that will be inserted before the Login Form.
- Footer File - This .HTM file contains the content for the HTML footer content that will be inserted after the Login Form.
- Enable Custom HTML - The Custom HTML will not be used by Serv-U until this option is enabled.

Most Custom HTML interfaces will include custom images, which requires Serv-U to know where the images are being kept. To universalize this storage location, Serv-U requires the use of the `&#37;25CUSTOM_HTML_DIR&#37;25` tag in paths referencing images. This has the further benefit of avoiding changes to HTML when the container storing the HTML files and images is changed, because the path only has to be defined once in the **Custom HTML Container Directory** field. The tag is used as follows:

```
<img src="/&#37;25CUSTOM_HTML_DIR&#37;25/images/image.png" alt="My
Image">
```

File Share

The File Sharing feature allows your domain users to send or receive files from guests.

Note: File Sharing is disabled by default. You must select the relevant option to enable it.

To send file sharing invitation emails, you must configure your SMTP settings. This configuration only needs to be set once for the entire server or a domain.

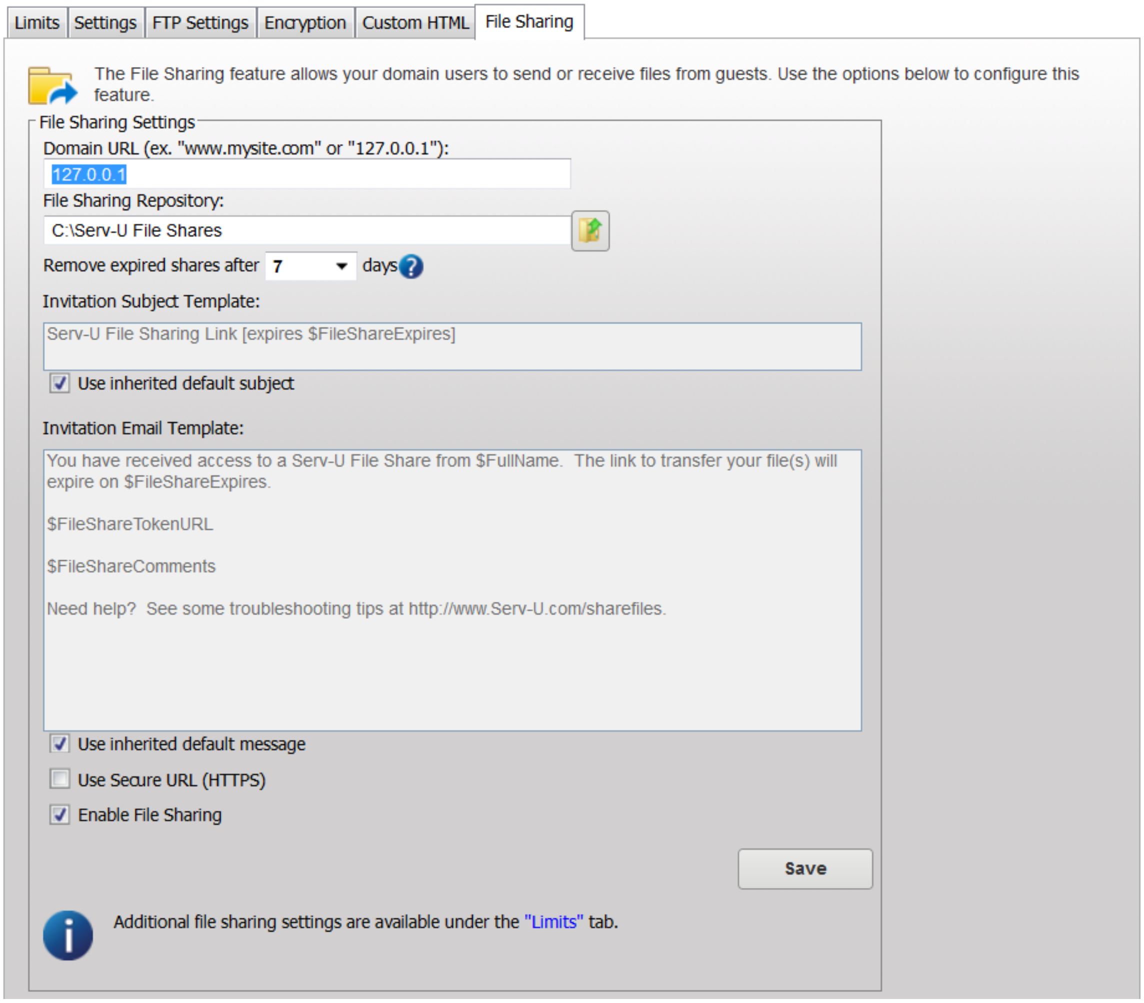
Click here to view common Administrator FAQs:

http://www.solarwinds.com/documentation/kbLoader.aspx?kb=4771

To enable file sharing:

1. Navigate to Server Limits and Settings > File Sharing.
2. Type the address for the Domain URL.
3. Type the location of the File Sharing Repository.
4. Select the number of days until the shares expire.
5. Select whether you want to use the inherited default email invitation subject, or customize your own. ***If the option is deselected***, you can type in a custom email invitation subject.
6. Select whether you want to use the inherited default email notification message, or customize your own. ***If the option is deselected***, you can type in a custom message.
7. Select **Enable File Sharing**.

8. If it is not configured yet, configure your SMTP to be able to send and receive notification emails. For more information, see "Serv-U SMTP Configuration".
9. Click **Save**.



The File Sharing feature allows your domain users to send or receive files from guests. Use the options below to configure this feature.

File Sharing Settings

Domain URL (ex. "www.mysite.com" or "127.0.0.1"): 127.0.0.1

File Sharing Repository: C:\Serv-U File Shares

Remove expired shares after 7 days

Invitation Subject Template: Serv-U File Sharing Link [expires $FileShareExpires]

☑ Use inherited default subject

Invitation Email Template:

You have received access to a Serv-U File Share from $FullName. The link to transfer your file(s) will expire on $FileShareExpires.

$FileShareTokenURL

$FileShareComments

Need help? See some troubleshooting tips at http://www.Serv-U.com/sharefiles.

☑ Use inherited default message

☐ Use Secure URL (HTTPS)

☑ Enable File Sharing

Additional file sharing settings are available under the "Limits" tab.

Server Activity

The Server Activity > Sessions, and Domain Activity > Sessions tabs display the current File Server session activity. When viewing the Sessions page from the server, all connected sessions from all domains are displayed. When viewed while administering a domain, only that domain's current sessions are displayed. From this page, an overall picture of the current activity on the File Server can be seen. In addition, individual sessions can be viewed including their current status, connection state, and transfer information.

To view the detailed information on a specific session, select the session. The **Active Session Information** group is populated with the details of the currently highlighted session. This information is frequently updated to provide you with an accurate and up-to-date snapshot of that session's activities.

Depending upon the type of connection made by that session (for example, FTP, HTTP, or SFTP), certain additional functions are available.

Disconnect

Any type of session can be disconnected at any time by clicking **Disconnect**. Click this button to bring up another dialog with additional options for how the disconnect should be performed. The following disconnect options are available:

- Disconnect - Immediately disconnects the session. Another session can be immediately established by the disconnected client. This is also known as "kicking" the user.
- Disconnect and ban IP for - Immediately disconnects the session and bans their IP address for the specified number of minutes, preventing them from immediately reconnecting.
- Disconnect and block IP permanently - Immediately disconnects the session and adds a deny IP access rule for their IP address, preventing them from ever reconnecting from the same IP address.

When disconnecting a session from the Server Session view, an additional option is available called **Apply IP rule to**. This option allows you to select where you would like the temporary or permanent IP ban to be applied - for the entire server or just the domain the session is connected to.

In addition to disconnecting the session, the user account in use by the session can also be disabled by selecting **Disable user account**.

If the current session is using the FTP protocol, a message can be sent to the user before disconnecting them by typing it in the **Message to user** field. This option is not available for HTTP or SFTP sessions as neither protocol defines a method for chatting with users.

Spy & Chat

Any type of session can be spied on by clicking **Spy & Chat** or double-clicking on a session from the list. Spying on a user displays all the detailed information normally visible by highlighting the session, but also includes a complete copy of the session's log since it first connected to the file server. This allows an administrator to browse the log and view all actions taken by the session's user.

If the current session is using the FTP protocol, additional options are available for chatting with the user. The **Chat** group shows all messages sent to and received from the session since beginning to "spy" on the session. To send a message to the session, type the message text in the **Message Content** field, and then click **Send**. When a message is received from the session, it is automatically displayed here.

Note: Not all FTP clients support chatting with system administrators. The command used to send a message to the server is `SITE MSG`. In order for a client to receive messages, the client application must be capable of receiving unsolicited responses from the server (instead of just discarding them).

Broadcast

A message can be sent to all currently connected FTP sessions by clicking **Broadcast**. Sending a message via broadcast is equivalent to opening the **Spy & Chat** dialog to each individual FTP session and sending it a chat message.

Abort

If a session is performing a file transfer, the file transfer can be terminated without disconnecting the session by clicking **Abort**. After confirming the abort command, the current file transfer for that session is terminated by the server. Some clients, especially FTP and SFTP clients, may automatically restart the aborted transfer making it appear that the abort failed. If this is the case, try disconnecting the session instead.

Server and Domain Statistics

The Server Activity > Statistics and Domain Activity > Statistics pages show detailed statistics on the use of the server for use in benchmarking and records keeping. Statistics viewed at the server level are an aggregate of those accumulated by all domains on the server. Statistics viewed for an individual domain are for that domain only. The displayed information includes the following:

Session Statistics

Current Sessions

The number of sessions currently connected.

Total Sessions

The total number of sessions that have connected since being placed online.

24 Hrs Sessions

The number of sessions that have connected in the past 24 hours.

Highest Num Sessions

The highest number of concurrent sessions that has been recorded since being placed online.

Average Session Length

The average length of time a session has remained connected.

Longest Session

The longest recorded time for a session.

Login Statistics

These statistics can apply to either a domain or the entire server depending on the statistics currently being viewed. Login statistics differ from session statistics because they apply to a login (providing a login ID and password) as opposed to connecting and disconnection.

Logins

The total number of successful logins.

Average Duration Logged In

The average login time for all sessions.

Last Login Time

The last recorded valid login time (not the last time a connection was made).

Last Logout Time

The last recorded valid logout time.

Most Logged In

The highest number of users logged in concurrently.

Currently Logged In

The number of sessions currently logged in.

Transfer Statistics

Download Speed

Cumulative download bandwidth currently being used.

Upload Speed

Cumulative upload bandwidth currently being used.

Downloaded

The total amount of data, and number of files, downloaded since being placed online.

Uploaded

The total amount of data, and number of files, uploaded since being placed online.

Average Download Speed

The average download bandwidth used since being placed online.

Average Upload Speed

The average upload bandwidth used since being placed online.

User & Group Statistics

The User & Group Statistics pages show detailed statistics based on individual user or group activity. Statistics viewed for a user or group are for that user or group only. The displayed information includes the following:

Session Statistics

Current Sessions

The number of sessions currently connected.

24 Hrs Sessions

The number of sessions that have connected in the past 24 hours.

Total Sessions

The total number of sessions that have connected since being placed online.

Highest Num Sessions

The highest number of concurrent sessions that has been recorded since being placed online.

Avg. Session Length

The average length of time a session has remained connected.

Longest Session

The longest recorded time for a session.

Login Statistics

These statistics can apply to either a user or a group of users depending on the statistics currently being viewed. Login statistics differ from session statistics because they apply to a login (providing a login ID and password) as opposed to connecting and disconnection.

Logins

The total number of successful logins.

Last Login Time

The last recorded valid login time (not the last time a connection was made).

Last Logout Time

The last recorded valid logout time.

Logouts

The total number of logouts.

Most Logged In

The highest number of simultaneously logged in sessions.

Longest Duration Logged In

The longest amount of time a session was logged in.

Currently Logged In

The number of sessions currently logged in.

Average Duration Logged In

The average login time for all sessions.

Shortest Login Duration Seconds

The shortest amount of time a session was logged in.

Transfer Statistics

Download Speed

Cumulative download bandwidth currently being used.

Upload Speed

Cumulative upload bandwidth currently being used.

Average Download Speed

The average download bandwidth used since being placed online.

Average Upload Speed

The average upload bandwidth used since being placed online.

Downloaded

The total amount of data, and number of files, downloaded since being placed online.

Uploaded

The total amount of data, and number of files, uploaded since being placed online.

Save Statistics

User and group statistics can be saved directly to a CSV file for programmatic analysis and review. In order to save statistics to a file, first select the user or group you want to generate a statistics file for, and then click **Save Statistics** on the bottom of the page.

Server & Domain Log

The Server Activity > Log and Domain Activity > Log tabs show logged activity for the server or domain.

The Server Log shows File Server startup, configuration, and shutdown information. It does not show domain activity information. To activity logs, view the appropriate domain's log instead. In addition to status information about libraries, licensing, and the current build that is logged when the File Server is first starts, the Server Log also contains information about all domain listener status, Universal Plug-and-Play (UPnP) status information, and PASV port range status. The information contained in the Server Log is also saved to a text file located in the installation directory that is named `Serv-U-StartupLog.txt`. This file is replaced each time the Serv-U File Server is started.

The Domain Log contains information about and activity pertaining to the currently administered domain only. This includes the status of the domain's listeners and any configured activity log information. For more information about the types of activity information that can be placed in the Domain Log, see "Configuring Domain Logs".

Information contained in the log can be highlighted by clicking and dragging the mouse cursor over the appropriate portion of the log. Once highlighted, the selected portion can be copied to the clipboard.

Freeze Log

Select this option to temporarily pause the refreshing of the log. This is useful on busy systems so a certain section of the log can be highlighted and copied before it scrolls out of view. Once finished, deselect the option to resume the automatic updating of the log.

Select All

Click this button to automatically freeze the log and highlight all currently displayed log information so that it can be copied to the clipboard.

Clear Log

When the log has become too large for you to view at once, click this button to erase the currently displayed log information. Only log information received after clicking the button is displayed.

Legend

To make viewing the different components of the log easier, each different type of logged message is color-coded for quick identification. Clicking this shows the legend in a draggable dialog. Drag the legend dialog to a convenient location so it can be used for reference while browsing the log.

Filter Log

To quickly find and read through specific sections of the log, it can be filtered based upon a search string. Click this button to bring up the Filter Log dialog. Provide a search string, and then click **Filter** to refresh the log to only display log entries containing the search string. To view the entire contents of the log again, open the Filter Log dialog, and then click **Reset**.

Download Log

To download the full log file from Serv-U, click **Download Log**. If you have permission to download the file your web browser will prompt you to choose a location to save the file, or begin downloading the file automatically.

Chapter 4: Domain

Domain Overview

At the core of the Serv-U File Server is the Serv-U domain. At the most basic level, a Serv-U domain is set of user accounts and listeners that allow users to connect to the server to access files and folders. Serv-U domains can also be configured further to restrict access based on IP address, limit bandwidth usage, enforce transfer quotas, and more. Virtually every setting available at the server level can be overridden for each individual domain. Careful advanced planning allows you to specify an acceptable level of default options at the server level to minimize the amount of configuration required for a domain.

Serv-U can support any number of domains on the File Server. Domains can share listeners, or they can each be hosted on a unique IP address if the system has multiple IP addresses. However, the maximum number of domains that can be created on an installation is dictated by the license. For more information about the different editions of Serv-U, see "Serv-U Editions".

When running a new installation of the Serv-U File Server for the first time, you are prompted to create your first domain using the New Domain Wizard. Follow the instructions on each page of the wizard to get your first domain created. For more information, see "Quick Start Guide".

Managing Domains

The domain currently being managed is always displayed in the header of each page next to the **+ (New Domain)** button. To change the active domain, click the domain name in the accordion menu on the left, and then select one of the available options.

If supported by your license, you can create another new domain at any time by clicking **+ (New Domain)** on the console page. After changing the active domain, the current page automatically reloads to reflect the new active domain's settings.

To delete a domain and all of its users and groups, navigate to **Domain > Domain Details**, and then click **Delete Domain**.

Warning: This action cannot be undone.

Domain Details

Domain Name and Description

Each domain must be uniquely identified with a domain name. If a name is provided that is not unique, an error message is shown indicating that a unique name is required for each domain. The domain name is used purely for administrative purposes and is not visible or accessible to users.

In addition, each domain can have additional descriptive information associated with it through the description. Like the domain name, the description text is also only available to users with administrative access. This field is useful for describing the purpose of the domain or summarizing the resources made available by the domain's existence on the File Server.

Domains can be temporarily disabled by deselecting the **Enable domain** option. While disabled, the domain is completely inaccessible to all users. The domain still exists on the File Server, all settings are preserved, and it can still be administered while it is disabled. To make the domain accessible to users again, select **Enable domain**.

After making changes to any of the above domain settings, click **Save** to apply the changes.

Domain Home Directory

System Administrators can limit the disk space available to a domain by configuring a home directory for the domain and specifying a maximum size. The domain's home directory does not affect user directory access rules, nor does it restrict the paths that are available to a user in any way. However, in order to calculate the amount of disk space in use by a domain, Serv-U must know the root directory under which it expects all domain files to be stored.

To specify the domain home directory, enter a path in the **Domain Home Directory** field, or click **Browse**to select a path. When creating a Domain Administrator account for this domain, it is suggested that their home directory be the same, which ensures that all users of the domain are placed in a subdirectory of the domain's home directory. Enter the amount of disk space, in megabytes (MB), available to the domain in the **Maximum Size** field. Leaving this field blank or entering "0" does not impose a maximum size on the domain. When a limit is imposed, any upload that would cause this maximum size to be exceeded is rejected by the server.

Click **Save** to apply these changes.

Note: Calculating the amount of disk space in use by a domain can be a time consuming operation depending on the directory structure.

Domain Listeners

The Serv-U File Server offers a highly configurable interface for enabling the different file sharing protocols on a domain. Listeners are added, edited, and deleted using the appropriately labeled button. Each domain can listen on multiple ports and IP addresses by adding a listener bound to the IP address and port you want. In addition to selecting these connection attributes for a listener, a file sharing protocol must also be selected. Serv-U supports IPv4 and IPv6 simultaneously, so to offer services to both IPv4 and IPv6 users a listener must be created both for an IPv4 address and an IPv6 address. A listing and short description of the file sharing protocols supported by the Serv-U File Server follows.

FTP - File Transfer Protocol

FTP is the traditional protocol for transferring files over the Internet. It normally operates on the default port 21. Traditionally, FTP is handled in plain-text, however, SSL connections are explicitly supported through the use of the AUTH command.

FTPS - File Transfer Protocol using SSL

FTPS is identical to FTP, however connecting to a listener configured for FTPS means that an SSL connection is required before any protocol communication is performed. This is commonly referred to as Implicit FTPS, which normally takes place on the default port 990.

SFTP - Secure File Transfer Using SSH2

SFTP is a secure method of transferring files through a secure shell session. It performs all protocol communications and data transfers over the same port eliminating the need to open multiple ports in firewalls as is commonly required when using FTP. SFTP sessions are always encrypted. SFTP operates on the default port 22.

HTTP - Hypertext Transfer Protocol

HTTP is the protocol used to browse websites. It is also a simple method for downloading and transferring files. One benefit to adding an HTTP listener to a domain is the availability of the Web Client, which allows users to transfer files to and from your File Server without the need for a standalone client. HTTP traditionally operates on port 80.

HTTPS - Hypertext Transfer Protocol using SSL

HTTPS is identical to HTTP except all communications are secured using SSL. Like FTPS, a secure connection is implied when connecting to a listener running the HTTPS protocol. The default port for HTTPS is 443.

Adding a Listener

After clicking **Add**, the listener configuration dialog is shown. After configuring each of the listener options, click **Save** to add the listener to the domain.

Type

Select the file sharing protocol that is to be supported by this listener. Each listener can only support a single protocol. To add more file sharing protocols to the domain, create new listeners for each protocol. A brief description of the supported file sharing protocols is found above.

IP Address

A listener can be bound to a single IP address by entering it here. Serv-U supports both IPv4 and IPv6 addresses. If the File Server does not have an external IP address (for example, it is behind a router), this field can be left blank. If no IP address is specified, you must select the option to either listen on all available IPv4 addresses or all IPv6 addresses. Unless you are running a purely IPv6 network, it is recommended to use IPv4 addresses and add IPv6 listeners as needed.

PASV IP Address or Domain Name (FTP ONLY)

If the listener is supporting the FTP protocol, this additional field is available to specify a separate IP address to use for PASV mode data transfers. Entering an IP address here ensures that PASV mode works properly on both unsecured and secured connections. If the File Server does not have an external IP address, try using a dynamic DNS service and entering your DNS domain name in this field. Serv-U resolves your DNS domain name to ensure it always has the proper external IP address for PASV command responses.

Use only with SSL connections

This option allows the PASV IP Address or domain name to only be used for SSL connections where it is always necessary to provide the PASV IP Address to connecting clients. When this option is enabled, the IP Address specified for PASV mode will not be provided to clients connecting via non-SSL FTP.

Use with LAN connections

Normally, Serv-U does not use the PASV IP Address for connections coming from the Local Area Network (computers on the same network as Serv-U). When this option is enabled, the PASV IP Address is also used for LAN connections.

Port

The default port for the selected protocol is automatically provided. However, any port between 1 and 65535 can be used. When using a non-standard port, clients must know the proper port in advance when attempting to connect to the domain. If using a non-standard port, it is recommended that you use a value above 1024 to prevent potential conflicts.

Enable listener

A listener can be temporarily disabled by deselecting this option. While disabled, listeners are displayed with a different icon in the list.

Pure Virtual Domains

Serv-U supports the ability for multiple domains to "share" the same listeners. In other words, one domain can possess the necessary listener configurations while the other domain "piggybacks" on the first one. In this way, the second domain exists in a virtual way. To have a domain "piggyback" on the listener configurations of existing domains, leave the listener list blank for the domain. The "piggybacking" domain needs to have at least one virtual host defined for it. For more information, see "Virtual Hosts".

This method of "piggybacking" only works with the FTP and HTTP protocols as they are the only two file sharing protocols that specify a method for identifying the specific host after a connection is established. For FTP connections, the client must issue a HOST command to identify the specific domain. For HTTP connections, the browser automatically handles providing the necessary host header to Serv-U based on the domain name used to establish the HTTP connection.

Virtual Hosts

Virtual Hosts provide a way for multiple domains to share the same IP and Listener port numbers. Normally, each domain listener must use a unique IP address and port number combination. With Virtual Hosts, it is possible to host multiple domains on a system that only has one unique IP address without having to use non-standard port numbers. The domains can share the same listeners by proper implementation of Virtual Hosts. This feature is only available when the current license supports hosting multiple domains.

To configure Virtual Hosts for a domain, click **Add** under **Domain Details > Virtual Hosts**, and then type in the Virtual Host name for the domain. The Virtual

Host name is usually the fully qualified domain name used to connect to the domain such as `ftp.Serv-U.com`.

The method used by a client to connect to a specific Virtual Host depends on the protocol being used to connect to Serv-U.

FTP

FTP users can use one of two methods to connect to a specific Virtual Host. If supported by the FTP client, the HOST command can be issued to Serv-U before login to identify the Virtual Host. Otherwise, the virtual host can be provided with the login ID in the following format: `virtual_host_name|login ID`. The Virtual Host name is entered first, followed by the vertical bar character ('|'), then the login ID.

SFTP

SFTP users who want to connect to a specific virtual host must use the specially crafted login ID format as described above in the FTP section.

HTTP

For HTTP users, the browser automatically provides Serv-U with the hostname used to reach the site allowing Serv-U to identify the Virtual Host from the fully qualified domain name entered into the browser's navigation bar.

Case File - Virtual Hosts

Multiple domains are being configured on the same server, which has one IP address and two Fully Qualified Domain Names (FQDN) pointing to it. Because users connecting to both domains must use port 21 for connections, configure Virtual Hosts on each domain so that Serv-U can distinguish between requests for the two domains. After setting up the same listener properties on each domain, open the Virtual Hosts tab, click **Add**, and then type in the FQDN that clients should use to connect to the domain (such as `ftp.Serv-U.com`).

After connecting to the server with FTP, users can send a `HOST ftp.Serv-U.com` command to connect to the appropriate domain on the File Server. FTP and SFTP users can also identify the Virtual Host through their login ID of `ftp.Serv-`

`U.com|login ID`. If connecting via HTTP, users can connect to this domain by visiting `http://ftp.Serv-U.com`.

Server Details

IP Access Rules

IP Access rules restrict login access to specific IP addresses, ranges of IP addresses, or even a domain name. IP Access rules can be configured at the server, domain, group, and user levels.

IP access rules are applied in the order they are displayed. In this way, specific rules can be placed at the top to allow (or deny) access before a more general rule is applied later on in the list. The arrows on the right side of the list can be used to change the position of an individual rule in the list.

IP Access Masks

IP Access rules use masks to authorize IP addresses and domain names. These masks may contain specific values, ranges and wildcards made up of the following elements.

xxx

An exact match such as `192.168.1.1` (IPv4), `fe80:0:0:0:a450:9a2e:ff9d:a915` (IPv6, long form) or `fe80::a450:9a2e:ff9d:a915` (IPv6, shorthand).

xxx-xxx

A specified range of IP addresses such as `192.168.1.10-19` (IPv4), `fe80:0:0:0:a450:9a2e:ff9d:a915-a9aa` (IPv6, long form), or `fe80::a450:9a2e:ff9d:a915-a9aa` (IPv6, shorthand).

*****

Any valid IP address value such as `192.168.1.*`, which is analogous to `192.168.1.0-255`, or `fe80::a450:9a2e:ff9d:*`, which is analogous to `fe80::a450:9a2e:ff9d:0-ffff`.

?

Any valid character when specifying a reverse DNS name such as `server?.mydomain.com`.

/

The slash separator allows the use of CIDR notation to specify which IP addresses should be allowed or blocked. Common CIDR blocks are `/8 (for 1.*.*.*)`, `/16 (for 1.2.*.*)` and `/24 (for 1.2.3.*)`. CIDR notation also works with IPv6 addresses, such as `2001:db8::/32`.

Caveats

Specific IP addresses listed in Allow rules will not be blocked by anti-hammering. (In other words, they are ‘whitelisted’.) However, addresses matched by wildcard or range will be subject to anti-hammering prevention.

Implicit Deny All

Serv-U assumes that connections from any IP address are valid until you add your first IP access rule. After you add that first IP access rule Serv-U assumes that all connections not explicitly allowed should be denied. This is also known as "an implicit 'Deny All' rule". With this in mind, make sure you add a 'wildcard allow' rule (such as `Allow *.*.*.*`) at the end of your IP Access rule list.

Matching All Addresses

Use a mask of `*.*.*.*` to match any IPv4 address. Use a mask of `*:*` to match any IPv6 address. Remember to add Allow ranges for both IPv4 and IPv6 addresses if you use both IPv4 and IPv6 listeners.

DNS Lookup

If a dynamic DNS service is used, then a domain name can be specified in place of an IP address to allow access to clients that travel and do not have a static IP address. Reverse DNS names are also acceptable. If a domain name or reverse DNS rule is created, Serv-U must perform either a reverse DNS look-up or DNS resolution in order to apply these rules. This can cause a slight delay during login depending on the speed of the system's DNS server.

Rule Use During Connection

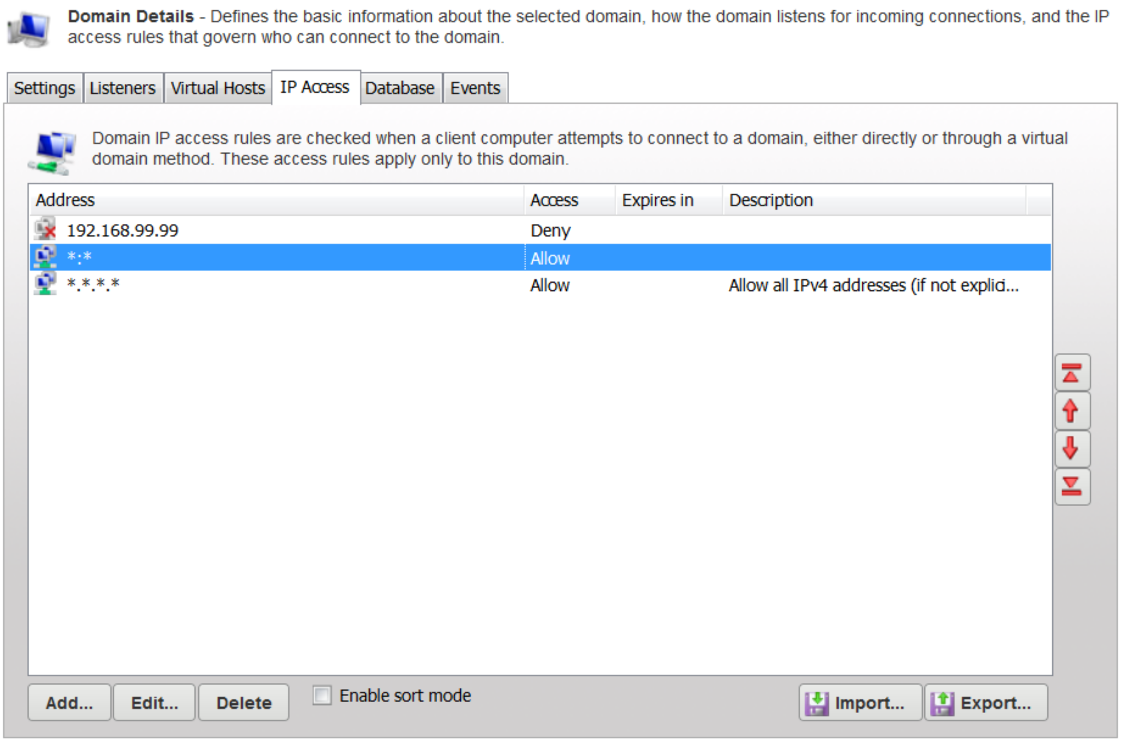
The level at which an IP access rule is specified also defines how far a connection is allowed before being rejected. Server and domain level IP access rules are applied before the Welcome message is sent. Domain level IP access rules are also applied when responding to the HOST command to connect to a virtual domain. Group and user level IP access rules are applied in response to a USER command when the client identifies itself to the server.

Anti-Hammering

Serv-U allows administrators to set up an "anti-hammering policy" that blocks clients who connect and fail to authenticate more than a certain number of times within a certain period of time. These policies can be configured server-wide in **Server Limits and Settings > Server Settings** and domain-wide in **Domain Limits and Settings > Domain Settings**.

IP addresses blocked by anti-hammering rules will appear in your Domain IP Access rules with a value in the **Expires in** column. If you have multiple domains with different listeners, blocked IPs will appear in the domain that contains the listener. (Blocked IP addresses will never appear in the Server IP Access list, even if anti-hammering was set up at the server level.)

The **Expires in** value of the blocked IP will tick down second by second until the entry disappears. You can unblock any blocked IP early by deleting its entry from the list.



Domain Details - Defines the basic information about the selected domain, how the domain listens for incoming connections, and the IP access rules that govern who can connect to the domain.

Domain IP access rules are checked when a client computer attempts to connect to a domain, either directly or through a virtual domain method. These access rules apply only to this domain.

Address	Access	Expires in	Description
192.168.99.99	Deny		
:	Allow		
..*.*	Allow		Allow all IPv4 addresses (if not explici...

IP Access List Controls

Enable Sort Mode

This option allows the IP Access list to be sorted numerically rather than in the processing order. Displaying the IP Access list in sort mode will not change the order in which rules are processed. To view rule precedence disable this option. Viewing the IP Access list in numerical order can be a valuable tool when reviewing long lists of access rules to determine if an entry already exists.

Importing/Exporting IP Access Rules

Serv-U IP Access rules can be imported and exported from users, groups, domains, and the server using a standard text-based comma separated values (CSV) file. To export IP Access rules, view the list of rules to export, and then click **Export**, specifying the path and the file name to save the list to. To import IP Access rules, click **Import** and select the file with the rules

to be imported. The CSV file must contain the following fields, headers included:

-IP - The IP address, IP range, CIDR block, or domain name for which the rule will apply

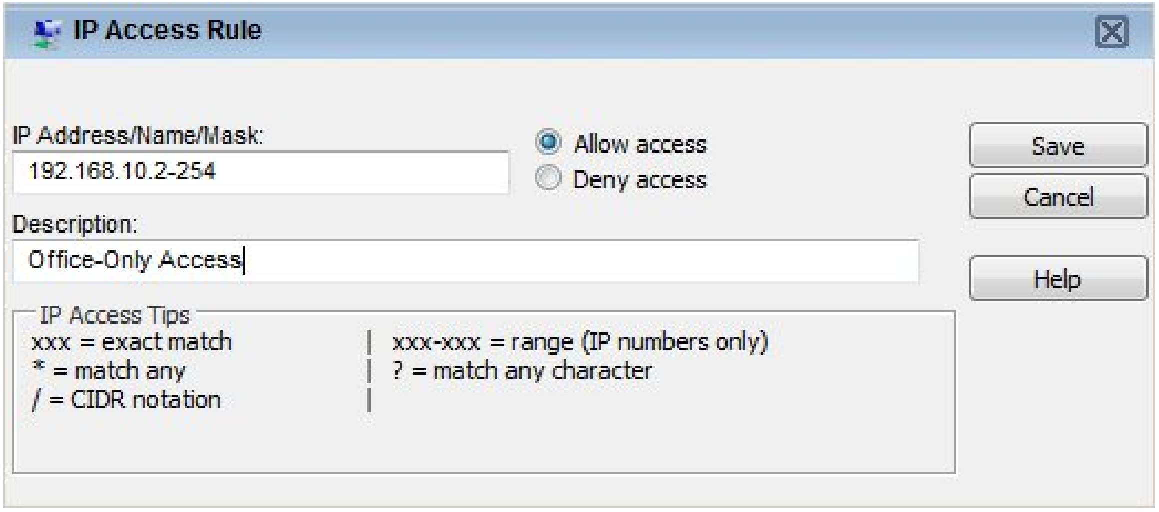
-Allow - Set this value to 0 for Deny, or to 1 for Allow

-Description - A text description of the rule for reference purposes

Examples

Case File - Office-Only Access

A contractor has been hired to work in the office, and only in the office. Office workstations have IP addresses from 192.168.10.2 to 192.168.10.254. The related Serv-U access rule should therefore be `Allow 192.168.10.2-254` (see below), and it should be added to either the contractor's user account or a 'Contractors' group that will contain multiple contractors. (Note that no "Deny" rule is required here because Serv-U provides an implicit 'deny all' at the end of the list.)



IP Address/Name/Mask: 192.168.10.2-254

● Allow access
○ Deny access

Description: Office-Only Access

IP Access Tips
xxx = exact match | xxx-xxx = range (IP numbers only)
* = match any | ? = match any character
/ = CIDR notation |

Case File - Prohibited Machines

Users should normally be able to access Serv-U from anywhere, except from a bank of special internal machines in the IP address range of 192.168.15.100 -

192.168.15.110. The related Serv-U access rules should therefore be `Deny 192.168.15.100-110`, followed by `Allow *.*.*.*`, and these should both be added to either the domain or the server IP Access rules.

Case File - DNS-based Access Control

The only users allowed to access a Serv-U Domain will be connecting from `*.internal.com` or `*.trustedpartner.com`. The related Serv-U access rules should therefore be `Allow *.internal.com` and `Allow *.trustedpartner.com` (in any order) and these should both be added to the domain IP Access rules. (Note that no "Deny" rule is required here because Serv-U provides an implicit 'deny all' at the end of the list.)

Database Access

Serv-U enables the use of an ODBC database to store and maintain group and user accounts at both the domain and server levels. The ODBC connections are configured from two locations: **Domain > Domain Details > Database** and **Server > Server Details > Database**. Serv-U can automatically create all of the tables and columns necessary to begin storing users and groups in your database. Because Serv-U uses one set of table names to store its information, individual ODBC connections must be configured for each item which stores details in the database. In other words, the server as well as each domain must have a unique ODBC connection to ensure they are stored separately. To configure a database, follow these steps:

- Create an ODBC connection for Serv-U to use. SolarWinds recommends MySQL, but any database that has an ODBC driver available can be used. Use a System DSN if Serv-U is operating as a system service, or a User DSN if Serv-U is operating as a regular application.
- Open the Serv-U Management Console and browse to the appropriate domain or server database settings. Enter the Data Source Name (DSN), the login ID, and password, and then click **Save**.

If the database connection is being configured for the first time, leave the

Automatically create options selected. With these options selected, the Serv-U File Server builds the database tables and columns automatically.

SQL Templates

Serv-U uses multiple queries to maintain the databases containing user and group information. These queries conform to the SQL language standards. However, if the database you are using is having problems working with Serv-U, you may need to alter these queries. From the SQL Templates dialog, each query used by Serv-U can be specially tailored to conform to the standards supported by your database.

Warning: Incorrectly editing these SQL queries could cause ODBC support to stop working in Serv-U. Do not edit these queries unless you are comfortable constructing SQL statements and are positive that it is necessary to enable ODBC support with your database software.

User and Group Table Mappings

By default, Serv-U automatically creates and maintains the tables and columns necessary to store user and group information in a database. However, if you are attempting to connect Serv-U to an existing database containing this information, you need to customize the table and column names to conform to the existing database structure. Click **User Table Mappings** or **Group Table Mappings** to get started.

Serv-U stores information for a user or group in 10 separate tables. Only the User/Group Info Table and User/Group Dir Access Table are required. The current table can be changed from the **Object Table** list. The **Attribute** column lists the attributes that are stored in the current table. The **Mapped Database Value** displays the name of the column that attribute is mapped to in the database. The first row always displays the "TableName" and can be used to change the name of the table.

Certain tables where the order of the entries bears significance have a **SortColumn** attribute listed. This column is used to store the order in which rules are applied.

Click **Edit** or double-click the column name to edit a value.

When enabled, the table is accessed as needed. In special situations a table that is not being used may be disabled to reduce the number of ODBC (database) calls. For example, if you are not using Ratios and Quotas, the User Ratio-Free Files, Per User Files Ratio, Per User Bytes Ratio, Per Session Files Ratio, and Per Session Bytes Ratio tables may be disabled to prevent unneeded ODBC calls. Use caution when disabling tables as the fields will appear in dialogs, but they will not be saved or loaded. The User Info and Group Info tables cannot be disabled.

Case File - ODBC Authentication

Authentication in the Serv-U File Server can be handled through an ODBC database, allowing for scripted account management and maintenance. In order to make use of ODBC functionality, migrate to ODBC authentication through a database. By storing credentials in settings in a database, accounts can be managed from outside the Serv-U Management Console through scripted database operations which can be built into many existing account provisioning systems. A DSN must first be created in **Control Panel > Administrative Tools > ODBC Data Sources**. Use a System DSN if Serv-U is running as a service or a User DSN if Serv-U is running as an application. Once the proper DSN has been created, specify the Data Source Name, login ID and password, and then click **Save**. Serv-U creates the tables and columns transparently. Database Users and Groups can be managed from the Database Users and Database Groups sections of Serv-U (located near the normal Users and Groups tabs).

Data Source Name Creation in Linux

Database access in Serv-U Linux follows the same method as Serv-U on Windows, with the one change in how Data Source Names are created. In Linux, a DSN can be created after installing the following packages:

- mysql-connector-odbc
- postgressql-odbc
- unixodbc

Note that only the ODBC driver corresponding to the database needs to be installed. If Serv-U is running as a service, the next step is to edit the `/etc/odbc.ini` file, which contains all system-level DSNs. If Serv-U is running as an application, edit the `~/odbc.ini` file instead, and then enter the parameters as follows:

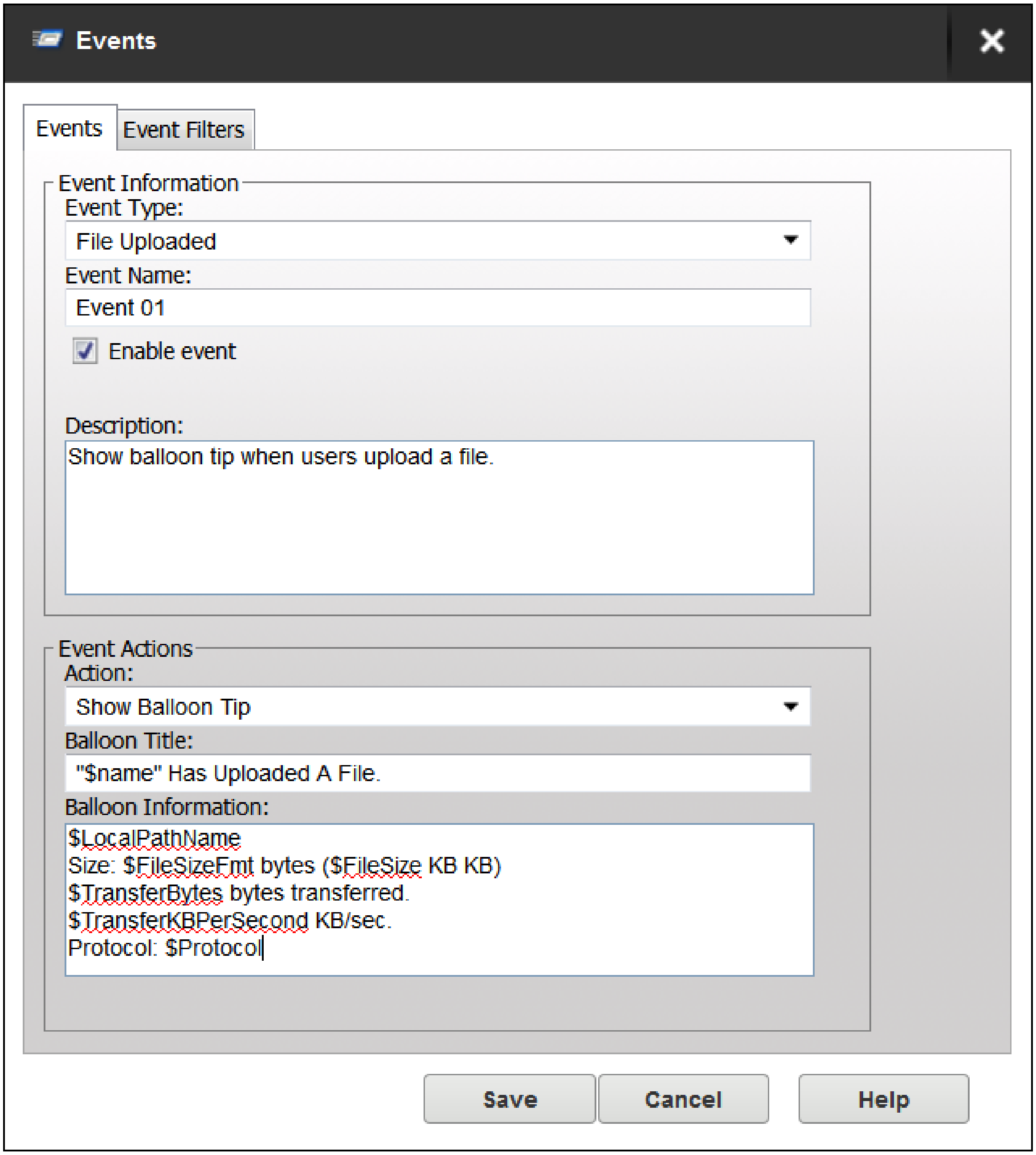
```
[MySQL-test]
Description = MySQL test database
Trace = Off
TraceFile = stderr
Driver = MySQL
SERVER = YOURIPADDRESS
USER = USERNAME
PASSWORD = PASSWORD
PORT = 3306
DATABASE = YOURDATABASE

[PostgreSQL-test]
Description = Test to Postgres
Driver = PostgreSQL
Trace = Yes
TraceFile = sql.log
Database = YOURDATABASE
Servername = YOURIPADDRESS
UserName = USERNAME
Password = PASSWORD
Port = 5432
Protocol = 6.4
ReadOnly = No
RowVersioning = No
ShowSystemTables = No
ShowOidColumn = No
FakeOidIndex = No
ConnSettings =
```

The names in brackets should be adjusted to your needed DSN name string. Finally, test the DSN using the command `isql %DSN% -c -v`.

For further customization, see the Serv-U Database Integration Guide at: http://www.serv-u.com/integration_guide

Serv-U Events



Event Type: File Uploaded

Event Name: Event 01

☑ Enable event

Description: Show balloon tip when users upload a file.

Action: Show Balloon Tip

Balloon Title: "$name" Has Uploaded A File.

Balloon Information:
$LocalPathName
Size: $FileSizeFmt bytes ($FileSize KB KB)
$TransferBytes bytes transferred.
$TransferKBPerSecond KB/sec.
Protocol: $Protocol

Serv-U enables the use of event handling which can perform various actions triggered by a list of selected events. The following list contains the actions available to administrators:

Server Events

- Server Start - Triggered by Serv-U starting up, whether by starting the Serv-U service or starting Serv-U as an application.
- Server Stop - Triggered by Serv-U shutting down, whether from service or application-level status. This event will only trigger for graceful stops.

Server and Domain Events

- Domain Start - Triggered by a Serv-U Domain starting, via the **Enable Domain** setting in the **Domain Details > Settings** menu or as part of normal server startup.
- Domain Stop - Triggered by a Serv-U Domain stopping, via the **Enable Domain** setting in the **Domain Details > Settings** menu or as part of normal server startup.
- Session Connection - Triggered by a new TCP session connection.
- Session Disconnect - Triggered by a TCP session disconnection.
- Session Connection Failure - Triggered by a failed session connection attempt.
- Log File Deleted - Triggered by the automatic deletion of a log file, according to logging settings.
- Log File Rotated - Triggered by the automatic rotation of a log file, according to logging settings.
- Listener Success - Triggered by a successful listener connection.
- Listener Stop - Triggered by a stopped listener connection.
- Listener Failure - Triggered by a failed listener connection.
- Gateway Listener Success - Triggered by a successful Gateway listener connection.
- Gateway Listener Stop - Triggered by a stopped Gateway listener connection.

- Gateway Listener Failure - Triggered by a failed Gateway listener connection.
- Permanent Listener Success - Triggered by a successful permanent listener connection.
- Permanent Listener Failure - Triggered by a failed permanent listener connection.
- Permanent Listener Stop - Triggered by a stopped permanent listener connection.
- Permanent Gateway Listener Success - Triggered by a successful permanent Gateway listener connection.
- Permanent Gateway Listener Stop - Triggered by a stopped permanent Gateway listener connection.
- Permanent Gateway Listener Failure - Triggered by a failed permanent Gateway listener connection.
- File Management Rule Success - Triggered when a file management rule is applied, and no errors are encountered.
- File Management Rule Failure - Triggered when a file management rule is applied, and at least one error is encountered.

Server, Domain, User and Group Events

- User Login - Triggered by the login of a user account.
- User Logout - Triggered by the logout of a user account.
- User Login Failure - Triggered by a failed login. A failed login is any connection attempt to Serv-U that fails, whether due to invalid credentials, or a session disconnect before authentication, either due to an incorrect user name, incorrect password, incorrect SSH key pair (for SFTP Public Key Authentication), or any or all of the above.
- User Password Change - Triggered by the change of a password for a user account, either by an administrator or by the user (if permitted).

- User Password Change Failure - Triggered by a failed password change attempt.
- User Enabled - Triggered by the enabling of a user account that was previously disabled.
- User Disabled - Triggered by the disabling of a user account that was previously enabled.
- User Deleted - Triggered by the deletion of a user account by a remote administrator, in an ODBC database, or in the local Management Console.
- User Added - Triggered by the creation of a user account by a remote administrator, in an ODBC database, or in the local Management Console.
- Password Recovery Sent - Triggered by a successful password recovery by an end user or by an administrator.
- Password Recovery Failed - Triggered by a failed password recovery attempt, either due to lack of email address in the user account or lack of permissions.
- Password Stale - Triggered by a stale password, as configured in **Limits & Settings**, that is going to expire.
- User Auto Disable - Triggered by the automatic disabling of a user account, as configured by a user's **Automatically Disable** date.
- User Auto Deleted - Triggered by the automatic deletion of a user account, as configured by a user's **Automatically Delete** date.
- User Pre-disable - Triggered by the upcoming disabling of a user account, as configured in the user's **Automatically Disable** date and the "Days before automatically disabling account to trigger the pre-disable event" limit.
- User Pre-delete - Triggered by the upcoming deletion of a user account, as configured in the user's **Automatically Delete** date and the **Days before automatically deleting account to trigger the pre-delete** event limit.
- User Email Set - Triggered by a user or administrator setting the email address for a user account.

- User Email Set Failure - Triggered by a failed attempt by a user or administrator to set the email address for a user account.
- IP Blocked - Triggered by a failed login attempt due to an IP Access rule.
- IP Blocked Time - Triggered by a failed login attempt due to an IP Access rule that was automatically added by brute force settings, configured in **Domain Limits & Settings** or **Server Limits & Settings**.
- Too Many Sessions - Triggered by more sessions logging on to the server than are permitted, per the **Limits & Settings** for the user account, group, domain, or server.
- Too Many Session On IP - Triggered by more sessions logging on to the server from a specific IP address than are permitted, per the **Limits & Settings** for the user account, group, domain, or server.
- IP Auto Added To Access Rules - Triggered by the automatic addition of an IP Access rule due to a user triggering the "brute force" settings.
- Session Idle Timeout - Triggered by an idle session timeout.
- Session Timeout - Triggered by a session timeout.
- File Uploaded - Triggered by a file uploaded to Serv-U. This event triggers for partial uploads if the upload session terminated with a successful message and no data corruption.
- File Upload Failed - Triggered by a failed file upload to Serv-U.
- File Download - Triggered by a file downloaded from Serv-U.
- File Download Failed - Triggered by a failed file download from Serv-U.
- File Deleted - Triggered by the deletion of a file on the Serv-U server by a user.
- File Moved - Triggered by the moving of a file on the Serv-U server by a user.
- Directory Created - Triggered by the creation of a directory.
- Directory Deleted - Triggered by the deletion of a directory.

- Directory Changed - Triggered by changing the current working directory.
- Directory Moved - Triggered by moving a directory to a new location.
- Over Quota - Triggered by going over disk quota space. The current quota space is shown in the user account, in the **Limits & Settings** menu.
- Over Disk Space - Triggered by exceeding the Max Dir Size configured for a Directory Access rule. The current disk space is shown with the `AVBL FTP` command, or using the **Directory Properties** option in the HTTP/HTTPS Web Client and FTP Voyager JV.

Creating Common Events

Serv-U allows administrators to automatically create a list of the most common events. You can choose to create these common events using email and/or balloon tip actions. Click **Create Common Event** located in the Events tab. Select either the **Send Email** or **Show balloon tip** option for the action you want to be performed on the common events. If you choose to Send Email you must also enter an **To:** address where the events are to be sent.

Note: The **Write to Windows Event Log**, and **Write to Microsoft Message Queue (MSMQ)** options are available for Windows only.

Event Actions

Administrators can select from the following actions that will be executed when an event is triggered:

- Send Email
- Show Balloon Tip*
- Execute Command*
- Write to Windows Event Log (Windows only)*
- Write to Microsoft Message Queue (MSMQ) (Windows only)*

* - Events involving anything other than email may only be configured by Serv-U server administrators.

Email Actions

Email actions can be configured to send emails to multiple recipients and to Serv-U Groups when an event is triggered. To add an email address, enter it in the **To** or **Bcc** fields. To send emails to a Serv-U Group, use the **Group** icon to add or remove Serv-U Groups from the distribution list. Email addresses must be separated by commas or semicolons. Email actions contain a **To**, **Subject** and **Message** parameter. Special variables can be used to send specific data pertaining to the event. For more information about the variables, see "System Variables".

To use email actions, you must first configure SMTP in Serv-U. For information, see "Serv-U SMTP Configuration".

Balloon Tip Actions

Balloon tip actions can be configured to show a balloon tip in the system tray when an event is triggered. Balloon tip actions contain a **Balloon Title** and a **Balloon Message** parameter. Special variables can be used to send specific data pertaining to the event. For more information about the variables, see "System Variables".

Execute Command Actions

Execute command actions can be configured to execute a command on a file when an event is triggered. Execute command actions contain an **Executable Path**, **Command Line Parameters**, and **Completion Wait Time** parameter. For the **Completion Wait Time** parameter, you can enter the number of seconds to wait after starting the executable path. Enter a value of 0 for no waiting.

Note: Any amount of time Serv-U spends waiting delays any processing that Serv-U can perform.

A wait value should only be used to give an external program enough time to perform some operation, such as move a log file before it is deleted (for example, `$LogFilePath` for the Log File Deleted event). Special variables can be used to send specific data pertaining to the event. For more information about the variables, see "System Variables".

Write to Windows Event Log

Writing event messages to a local Windows Event Log allows you to monitor and record Serv-U activity using third-party network management software such as those from HP Openview, SolarWinds, SpiceWorks, and many other vendors. All messages will appear in the Windows Application Log from a source of "Serv-U".

This event has only one field:

- Log Information: The contents of the message to be written into the event log. This is normally either a human-readable message (for example, `filename uploaded by person`) or a machine-readable string (for example, `filename|uploaded|person`), depending on who or what is expected to read these messages. Serv-U system variables are supported in this field. This field may be left blank, but usually should not be left blank.

Write to Microsoft Queue (MSMQ)

Microsoft Message Queuing (MSMQ) is an enterprise technology that lets independent applications communicate quickly and reliably. Serv-U MFT Server can send messages to new or existing MSMQ queues whenever a Serv-U event triggers. Corporations can use this feature to tell enterprise applications that files have arrived, files have been picked up, partners have signed on, or many other activities have just occurred.

These events have the following two fields:

- Message Queue Path: The MSMQ path that addresses the queue. Remote queues can be addressed when a full path (for example, `MessageServer\Serv-U Message Queue`) is specified. Local, public queues on the local machine can be addressed when a full path is not specified (for example, `.\Serv-U Message Queue` or just `Serv-U Message Queue`). If the specified queue does not exist, Serv-U will make its best effort to try to create it. (This normally only works on public queues on the local machine.) Serv-U system variables are supported in this field.

- Message Body: The contents of the message to be sent into the queue. This is normally a text string with a specific format specified by an enterprise application owner or enterprise architect. Serv-U system variables are also supported in this field. This field may be left blank, but usually is not.

Note: Microsoft message queues created in Windows do not grant access to SYSTEM by default, preventing Serv-U from writing events to the queue. In order to correct this, after creating the queue in MSMQ, right-click it, select **Properties**, and then set the permissions so that “SYSTEM” (or the network account under which Serv-U runs) has permission to the queue.

Event Filters

Serv-U Event Filters allow administrators to control to a greater degree when a Serv-U event is triggered. By default, Serv-U Events trigger each time the event occurs. The Event Filter allows events to be triggered only if certain conditions are met. For example, a standard Serv-U Event might trigger an email each time a file is uploaded to the server. However, using an Event Filter, Events can be triggered on a more targeted basis. A File Uploaded event can be configured to only send an email when the file name contains the string `important`, so an email would be sent when the file `Important Tax Forms.pdf` is uploaded but not when random other files are uploaded to the server. Additionally, a File Upload Failed event could be set to run only when the FTP protocol is used, not triggering for failed HTTP or SFTP uploads. This is done by controlling the various variables and values related to the Event and evaluating their results when the event is triggered.

Event Filter Fields

Each Event Filter has the following critical values that must be set:

- Name - This is the name of the filter, used to identify the filter for the event.
- Description (Optional) - This is the description of the event, which may be included for reference.

- Logic - This determines how the filter interacts with other filters for an event. In most cases, AND will be used all filters must be satisfied for the event to trigger. The function of AND is to require that all conditions be met. However, the OR operator can be used if there are multiple possible satisfactory responses (for example, abnormal bandwidth usage of less than 20 KB/s OR greater than 2000 KB/s).
- Filter Comparison - This is the most critical portion of the filter. The Filter Comparison contains the evaluation that must occur for the event to trigger. For example, a filter can be configured so that only the user "admin" triggers the event. In this case, the comparison will be `If $Name = (is equal to) admin`, and the data type will be `string`. For bandwidth, either an "unsigned integer" or "double precision floating point" value would be used.

Event filters also support wildcards when evaluating text strings. The supported wildcards are the following:

- * - The asterisk wildcard matches any text string of any length. For example:
    - An Event Filter that compared the `$FileName` variable to the string `data*` would match files named `data`, `data7`, `data77`, `data.txt`, `data7.txt`, and `data77.txt`.
- ? - The question mark wildcard matches any one character, but only one character. For example:
    - An Event Filter that compared the `$FileName` variable to the string `data?` would match a file named `data7` but not `data`, `data77`, `data.txt`, `data7.txt`, or `data77.txt`.
    - An Event Filter that compared the `$FileName` variable to the string `data?.`* would match files named `data7` and `data7.txt` but not `data`, `data77`, `data.txt`, or `data77.txt`.
    - An Event Filter than compared the `$Name variable` to the string `A????` would match any five-character username starting with `A`.
- [] - The bracket wildcard matches a character against the set of characters inside the brackets. For example:

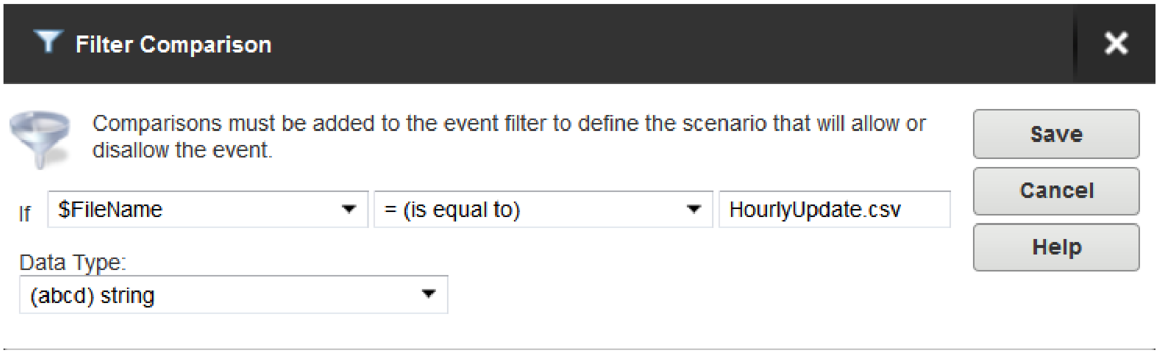
- An Event Filter that compared the `$FileName` variable to the string `data [687].txt` would match files named `data6.txt`, `data7.txt` and `data8.txt` but not `data5.txt`.
- An Event Filter that compared the `$LocalPathName` variable to the string `[CD]:\*` would match any file or folder on the `C:` or `D:` drives.

Multiple wildcards can be used in each filter. For example:

- An Event Filter that compared the `$FileName` variable to the string `[cC]:\*.???` would match any file on the `C:` drive that ended in a three letter file extension.
- An Event Filter that compared the `$FileName` variable to the string `?:\*Red [678]\?????.*` would match a file on any Windows drive, contained in any folder whose name contains `Red6`, `Red7` or `Red8`, and that also has a five character file name followed by a file extension of any length.

Using Event Filters

Event filters are used by comparing fields to expected values in the Event Filter menu. The best example is firing an event only when a certain user triggers the action, or when a certain file is uploaded. For example, an administrator may want to fire an email event when the file `HourlyUpdate.csv` is uploaded to the server, but not other files. To do this, a new event can be created in the **Domain Details > Events** menu. The **Event Type** is File Uploaded, and on the Event Filter tab a new filter must be added. The $FileName variable is used and the value is `HourlyUpdate.csv` as shown:

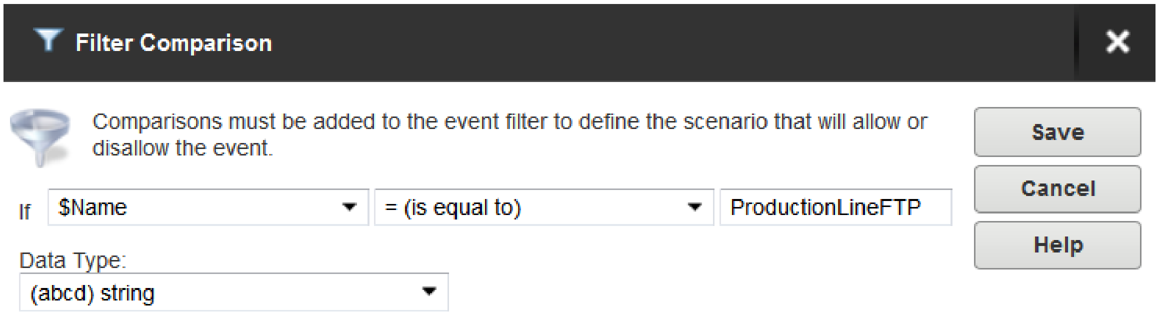


Comparisons must be added to the event filter to define the scenario that will allow or disallow the event.

If $FileName = (is equal to) HourlyUpdate.csv

Data Type: (abcd) string

As another example, it might be necessary to know when a file transfer fails for a specific user account (perhaps one used by an automated process). To perform this task, create a new File Upload Failed event, and then add a new filter. The filter comparison will be `$Name`, and the value to compare would be the username, such as `ProductionLineFTP`:

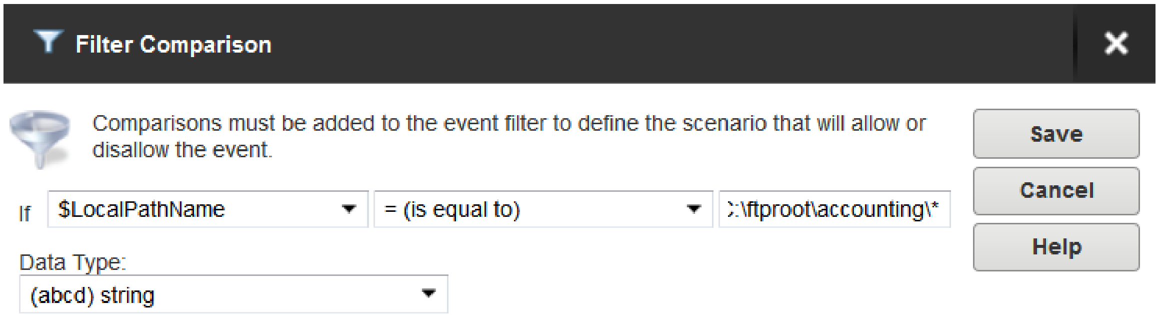


Comparisons must be added to the event filter to define the scenario that will allow or disallow the event.

If $Name = (is equal to) ProductionLineFTP

Data Type: (abcd) string

It is also possible to filter for events based on specific folders, using wildcards. In some cases it may be necessary to trigger events for files uploaded only to a specific folder, such as when an accounting department uploads time-sensitive tax files. To filter based on a folder name, first create a new File Uploaded event in the **Domain Details > Events** menu, and set it to **Send Email**. After specifying the email recipients, subject line, and message content, open the Event Filters tab. Create a new Event Filter, and add the filter comparison `If $LocalPathName = (is equal to) C:\ftproot\accounting\*` with the type of `(abcd) string`. This will cause the event to trigger only for files that are located within `C:\ftproot\accounting\`.



Comparisons must be added to the event filter to define the scenario that will allow or disallow the event.

If $LocalPathName = (is equal to) :\ftproot\accounting\*

Data Type: (abcd) string

Serv-U SMTP Configuration

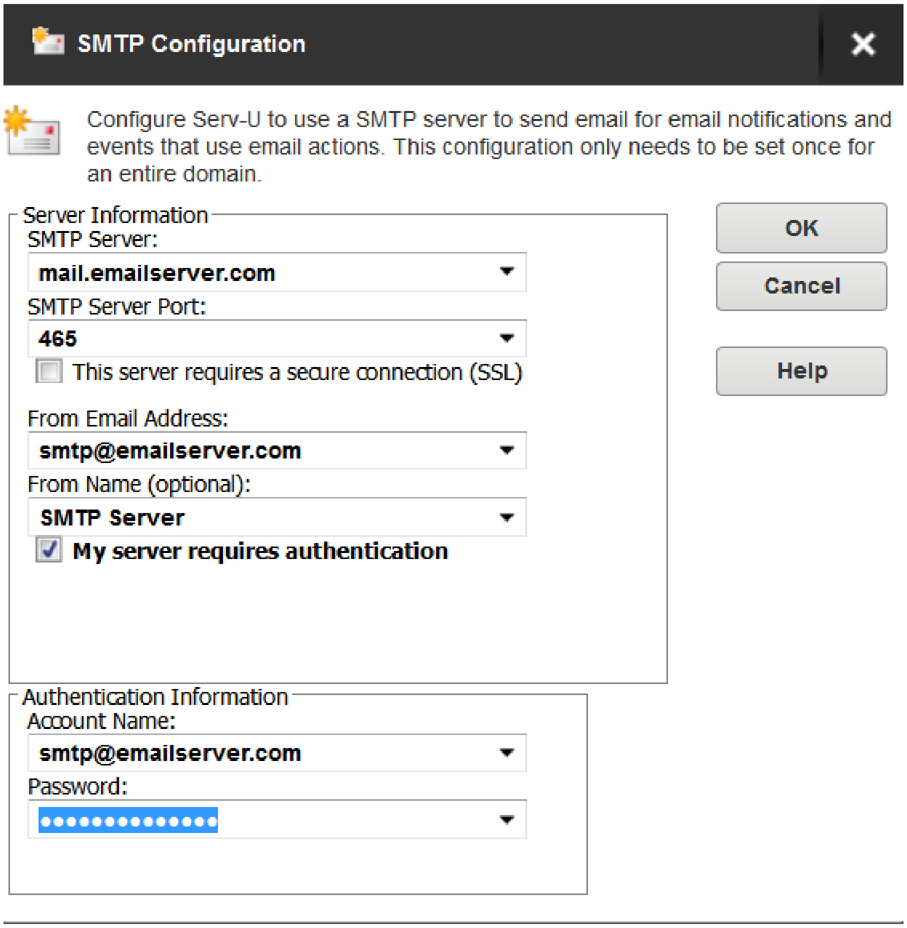
Serv-U allows administrators to configure an SMTP connection to send email for events configured to use email actions. SMTP can be configured on the server and/or the domain level. SMTP configuration at the domain level may be inherited from the server level. The SMTP configuration dialog is located in the Events tab in the **Domain Details** and **Server Details** pages.Click **Configure SMTP** to launch the dialog, and then specify the following details:

- SMTP Server - the name or IP address of the SMTP server.
- SMTP Server Port - the port the SMTP server is using.
- From Email Address - the email address to use for the outgoing email.
- From Name (optional) - the name to use for the outgoing email.
- This server requires a secure connection (SSL) - Some SMTP servers require that all incoming connections be encrypted to protect against possible attacks. If your server requires incoming SMTP connections to be encrypted, enable this option. The default port for encrypted SMTP connections is 465. Serv-U supports Implicit SSL only, and does not support Explicit SSL (port 587).
- My server requires authentication - to enable authentication, select this option.

If your SMTP server requires authentication you must enter the following information:

- Account Name - the account name associated with authentication for the SMTP server.

- Password - the password for the account.



Configure Serv-U to use a SMTP server to send email for email notifications and events that use email actions. This configuration only needs to be set once for an entire domain.

Server Information

SMTP Server: mail.emailserver.com

SMTP Server Port: 465

☐ This server requires a secure connection (SSL)

From Email Address: smtp@emailserver.com

From Name (optional): SMTP Server

☑ My server requires authentication

Authentication Information

Account Name: smtp@emailserver.com

Password: ••••••••••••••

Directory Access Rules

Directory Access Rules

Directory Access rules define the areas of the system that are accessible to user accounts. While traditionally restricted to the user and group levels, Serv-U extends the usage of Directory Access rules to both the domain and server levels through the creation of global Directory Access rules. Directory Access rules specified at the server level are inherited by all users of the File Server. When specified at the domain level, they are only inherited by users belonging to that domain. The traditional rules of inheritance apply where rules specified at a lower level (for example, the user level), override conflicting or duplicates rules specified at a higher level (for example, the server level).

When setting the Directory Access path, the `&#37;USER&#37;`, `&#37;HOME&#37;`, `&#37;USER_FULL_NAME&#37;`, and `&#37;DOMAIN_HOME&#37;` variables are available to simplify the process. For example, use `%HOME%/ftproot/` to create a Directory Access rule that specifies the `ftproot` folder in the user's home directory. Directory access rules specified in this manner are "portable" in the event that the actual home directory changes while maintaining the same subdirectory structure. This leads to less maintenance for the File Server administrator. If the `%USER%` variable is specified in the path, it is replaced with the user's login ID. This variable is useful in specifying a group's home directory to ensure that users inherit a logical and unique home directory. The `&#37;USER_FULL_NAME&#37;` variable can be used to insert the Full Name value into the path (the user must have a "Full Name" specified for this to function). For example, the user "Tom Smith" could use `D:\ftproot\&#37;USER_FULL_NAME&#37;` for `D:\ftproot\Tom Smith`. Finally, the `%DOMAIN_HOME%` macro can also be used to identify the user's home directory. For example, to place a user and their home directory into a common directory use `%DOMAIN_HOME%\%USER%`.

Directory Access rules are applied in the order they are listed. The first rule Serv-U encounters in the list that matches the path of a client's request is the one that is applied for that rule. In other words, if a rule exists that denies access to a particular subdirectory but is listed *below* the rule that grants access to the parent directory, then a user still has access to the subdirectory in question. The arrows on the right side of the Directory Access list are used to rearrange the order in which the rules are applied.

A listing and description of each available directory access permission follows.

File Permissions

Read

Allows users to read (that is, download) files. This permission does not allow users to list the contents of a directory, which is granted by the **List** permission.

Write

Allows users to write (that is, upload) files. This permission does not allow users to modify existing files, which is granted by the **Append** permission.

Append

Allows users to append data to existing files. This permission is normally used to grant users the ability to resume transferring to partially uploaded files.

Rename

Allows users to rename existing files.

Delete

Allows users to delete files.

Execute

Allows users to remotely execute files. Execute access is meant for remotely starting programs and usually applies to specific files. This is a very powerful permission and great care should be used in granting it to users. A user with **Write** and **Execute** permissions can essentially install any program of their choosing on your system.

Directory Permissions

List

Allows users to list the files and subdirectories contained in the directory. Also allows users to list this folder when listing the contents of a parent directory. (See KB #2079 for more information about "blind downloads" and "blind uploads".)

Create

Allows users to create new directories within the directory.

Rename

Allows users to rename existing directories within the directory.

Remove

Allows users to delete existing directories within the directory. **Note:** If the directory contains files, the user also needs to have the **Delete** files permission in order to remove the directory.

Subdirectory Permissions

Inherit

Allows all subdirectories to inherit the same permissions as the parent directory. The **Inherit** permission is appropriate for most circumstances, but if access must be restricted to subfolders (as is the case when implementing Mandatory Access Control), deselect **Inherit** and grant permissions specifically by folder.

Advanced: Access as Windows User (Windows Only)

For a variety of reasons, files and folders may be kept on external servers in order to centralize file storage or provide additional layers of security. In this environment, files can be accessed by the UNC path (`\\servername\folder\`) instead of the traditional `C:\ftproot\folder` path. However, accessing folders stored across the network poses an additional challenge, because Windows services are run under the Local System account by default, which has no access to network resources.

To mitigate this problem for all of Serv-U, it is possible to configure the Serv-U File Server service to run under a network account. The alternative, preferred when many servers exist, or if the Serv-U File Server service needs to run under Local System for security reasons is to configure a Directory Access rule to use a specific Windows User for file access. By clicking the **Advanced** button it is possible to specify a specific Windows user for each individual Directory Access rule. Just like in Windows Authentication, directory access is subject to NTFS permissions, though in this case also to the configured permissions in Serv-U.

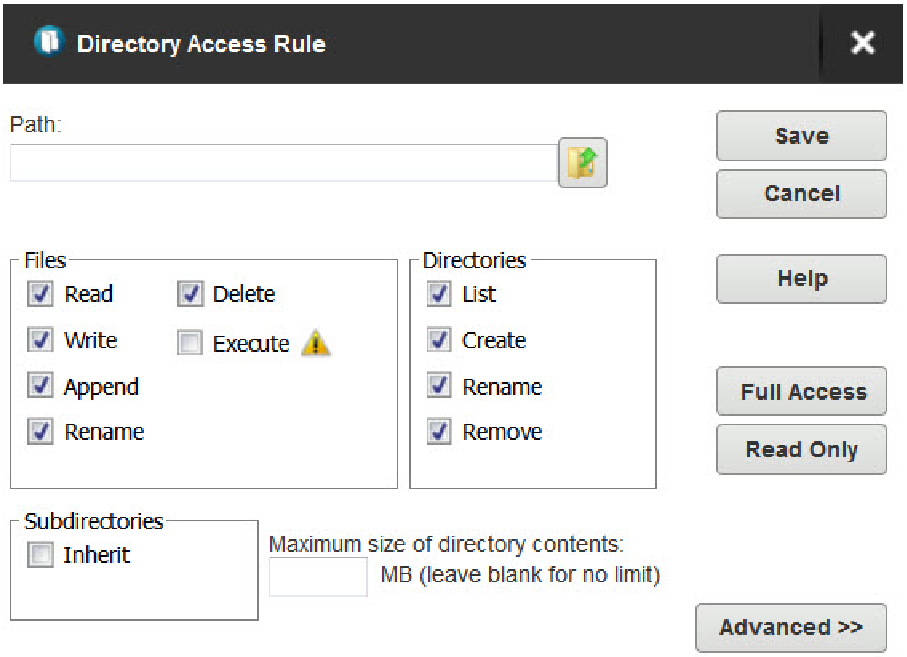
Quota Permissions

Maximum size of directory contents

Setting the maximum size actively restricts the size of the directory contents to the specified value. Any attempted file transfers that cause the directory contents to exceed this value are rejected. This feature serves as an alternative to the traditional quota feature that relies upon tracking all file transfers (uploads and deletions) to calculate directory sizes and is not able to consider changes made to the directory contents outside of a user's File Server activity.

Mandatory Access Control

Serv-U enables the use of Mandatory Access control in cases where users need to be granted access to the same home directory but should not necessarily be able to access the subdirectories below it. To implement Mandatory Access Control at a directory level, disable the **Inherit** permission as shown below (assume the rule applies to `D:\ftproot\`):



Path:

Files
☑ Read
☑ Delete
☑ Write
☐ Execute
☑ Append
☑ Rename

Directories
☑ List
☑ Create
☑ Rename
☑ Remove

Subdirectories
☐ Inherit

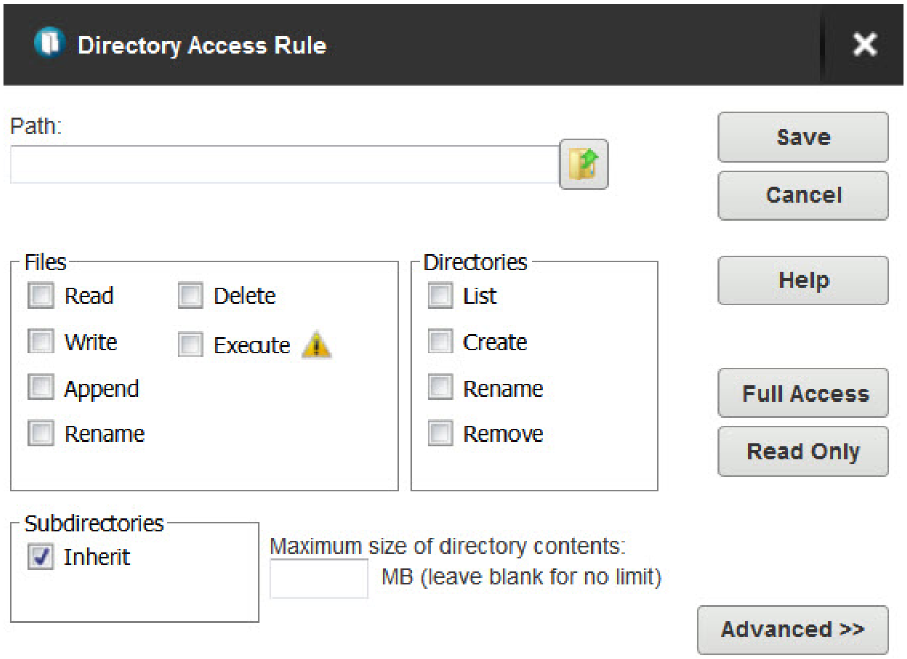
Maximum size of directory contents:
MB (leave blank for no limit)

Now, the user has access to the `ftproot` folder but to no folders below it.

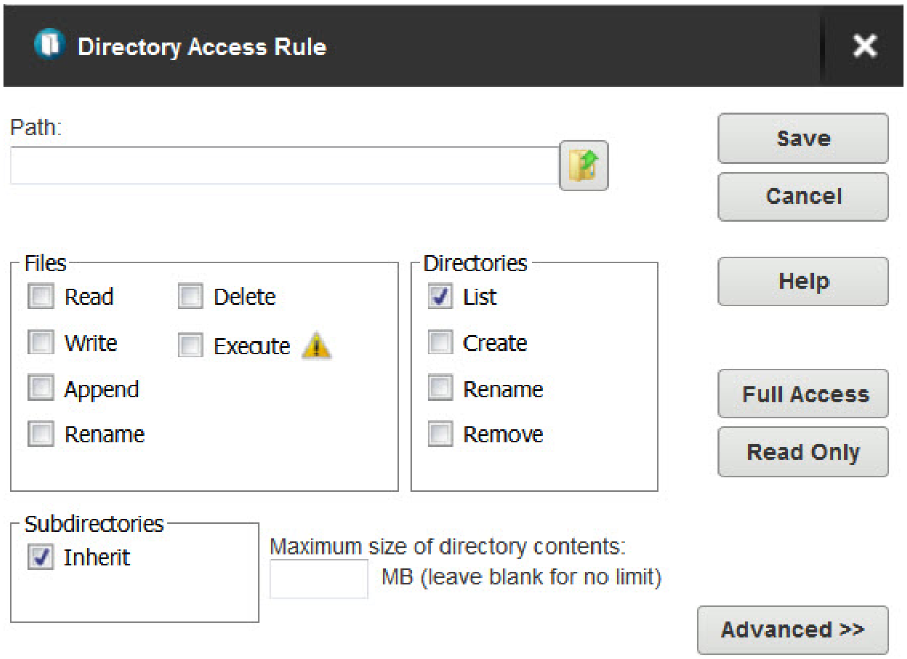
Permissions must individually be granted to subfolders that the user needs access to, providing the security of Mandatory Access Control in the Serv-U File Server.

Restricting File Types

If users are using storage space on the Serv-U File Server to store non-work-related files such as MP3 music files, this can be prevented by configuring a Directory Access rule placed **above** the main Directory Access Rule (use the arrows on the right to reorder rules) to prevent MP3 files from being transferred as shown below. In the text entry for the rule, type `*.mp3` and use the permissions shown below:



The rule denies permission to any transfer of files with the `.mp3` extension and can be modified to reflect any file extension. Similarly, if accounting employees only need to transfer files with the `.mdb` extension, configure a pair of rules that grants permissions for `.mdb` files but denies access to all other files, as shown below. In the first rule enter the path that should be the user's home directory or directory they need access to, and in the second rule enter the extension of the file that should be accessed (such as `*.mdb`):



Directory Access Rule

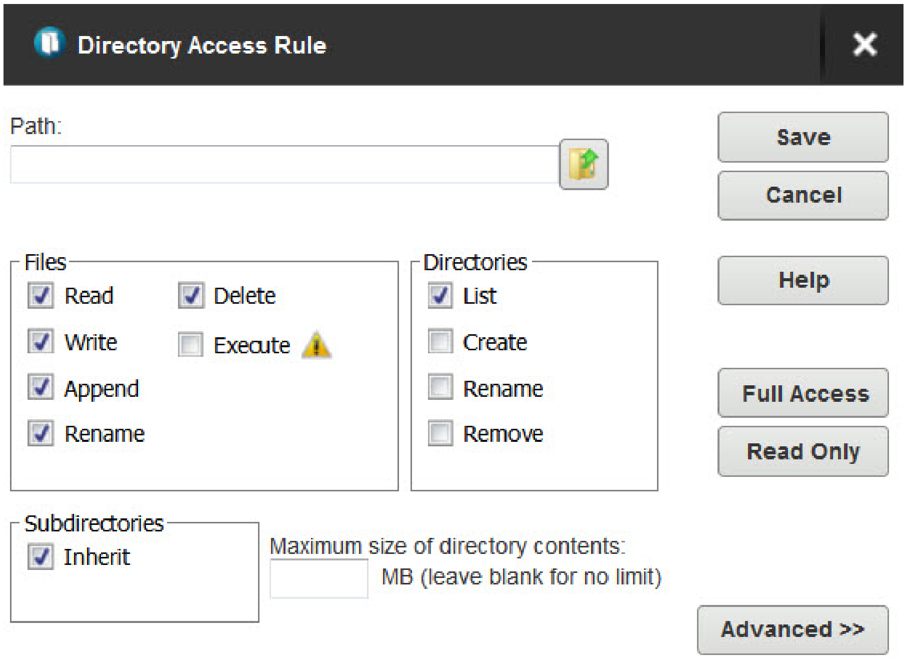
Path:

Files
☐ Read
☐ Write
☐ Append
☐ Rename
☐ Delete
☐ Execute

Directories
☑ List
☐ Create
☐ Rename
☐ Remove

Subdirectories
☑ Inherit

Maximum size of directory contents:
MB (leave blank for no limit)



Directory Access Rule

Path:

Files
☑ Read
☑ Write
☑ Append
☑ Rename
☑ Delete
☐ Execute

Directories
☑ List
☐ Create
☐ Rename
☐ Remove

Subdirectories
☑ Inherit

Maximum size of directory contents:
MB (leave blank for no limit)

These rules only allow users to access `.mdb` files within the directories specified, and can be adapted to any file extension or set of file extensions.

Virtual Paths

Virtual Paths allow users to gain access to files and folders outside of their own home directory. A Virtual Path only defines a method of mapping an existing directory to another location on the system to make it visible within a user's accessible directory structure. In order to actually have access to the mapped location, the user must still have a Directory Access rule specified for the physical path of a Virtual Path.

Like Directory Access Rules, Virtual Paths can be configured at the server, domain, group, and user levels. Virtual Paths created at the server level are available for use by all users of the File Server. When created at the domain level, they are only accessible by users belonging to that domain. Serv-U's granular file access controls even allow for Virtual Paths created specifically for individual users or groups.

Physical Path

The physical path is the actual location on the system, or network, that is to be placed in a virtual location accessible by a user. If the physical path is located on the same computer, a full path should be used, such as `D:\inetpub\ftp\public`. A UNC path can also be used, such as `\\Server\share\public`. In order for a Virtual Path to be visible to a user, they must have a Directory Access rule specified for the physical path.

Virtual Path

The virtual path is the location that the physical path should appear in for the user. The `%HOME%` macro is commonly used in the virtual path to place the specified physical path in the home directory of the user. When specifying the virtual path, the last specified directory is used as the name displayed in directory listings to the user. For example, a virtual path of `%HOME%/public` places the specified physical path in a folder named `public` within the user's home directory. A full path without any macros can also be used.

Include in "Maximum Directory Size" calculations

When selected, the Virtual Path is included in Maximum Directory Size calculations. When deselected, the Virtual Path is not included in the Maximum Directory Size calculations. Maximum Directory Size limits the size of directories affecting how much data can be uploaded.

Case File - Using Virtual Paths

A group of web developers have been granted access to the directory `D:\ftproot\examplesite.com\` for web development purposes. The developers also need access to an image repository located at `D:\corpimages\`. To avoid granting the group access to the root D drive, a Virtual Path must be configured so that the image repository *appears* to be contained within their home directory. Within the web developer's group, add a Virtual Path to bring the directory to the users by specifying `D:\corpimages\` as the Physical Path and `D:\ftproot\examplesite.com\corpimages` as the Virtual Path. Be sure to add a group level Directory Access rule for `D:\corpimages\` as well. The developers now have access to the image repository without compromising security or relocating shared resources.

Case File - Creating Relative Virtual Paths

Continuing with the previous example, if the web developer's group home directory is relocated to another drive, not only does the home directory have to be updated, but the Virtual Path also needs to be updated to reflect this change. This can be avoided by using the `%HOME%` macro to create a relative Virtual Path location that eliminates the need to update the path if the home directory changes. Instead of using `D:\ftproot\examplesite.com\corpimages` as the Virtual Path, use `%HOME%\corpimages`. This tells Serv-U to place the `corpimages` Virtual Path within the group's home directory - whatever that may be. If the home directory changes at a later date, the Virtual Path still appears there.

Automated File Management

Using file management rules, you can automatically remove or archive files from the file server. Automated file management rules can be configured at the server and domain level. When specified at the server level, the file management rules are accessible to all users of the file server. When specified at the domain level, they are only accessible to users belonging to that domain.

Depending on the file system, Serv-U uses the creation or change date of files to determine the expiration date. On Windows, the creation date of the file is used to determine when a file is expired. On Linux, the change date is used to determine the expiration date. The change date is updated whenever the file's metadata or index node (inode) is modified. If the contents or attributes (such as the permissions) of the file are modified, the change date is also updated.

Note: The change date is not modified if the file is read from.

The file management rules apply recursively to all files within the folder for which they are configured, and not only to those that have been uploaded through Serv-U. This way it is possible to manage files which are transferred by clients, or which are copied to the folder outside of Serv-U.

The folder structure is not affected by the file management rules. When Serv-U deletes or moves expired files, it leaves the folders themselves intact.

The file management rules run hourly in the background. For this reason, there can be an hour delay before Serv-U deletes or moves an expired file.

To monitor the status of the file management rules, you can configure a File Management Rule Success and a File Management Rule Error event under **Server/Domain Details > Events**. The file management rules continue running even if deleting or moving a single file fails. For more information, see "Serv-U Events".

To define a new file management rule:

1. Navigate to **Directories > File Management**, and then click **Add**.
2. Type the path to the file or folder in the **Directory Path** field, or click **Browse** to navigate to the file or folder.
3. Select the action you want to perform on the file:
    a. If you want to delete the file after it expires, select **Delete file(s) after specified time**.
    b. If you want to move the file after it expires, select **Move file(s) after specified time**, and then specify the folder where you want to move the file in the **Destination Directory Path** field.
4. Specify the number of days after the file creation date when the action should be executed.
5. Click **Save**.

Note: Serv-U regularly and individually checks all the files in the directory for their age, and executes the specified action on the files that meet the age criteria you specify.

Domain Limits and Settings

Serv-U offers advanced options which can be used to customize how it can be used as well as ways to apply limits and custom settings to users, groups, domains, and the server in its entirety. The limits stack intelligently, with user settings overriding group settings, group settings overriding domain settings, and domain settings overriding server settings. In addition, limits can be applied only during certain days of the week or times of the day. It is possible to grant exceptions to administrators and restrict specific users more than others, providing total control over the server. The Limits and Settings in Serv-U are split into the following categories:

- Connection
- Password
- Directory Listing
- Data Transfer
- HTTP
- Email
- File Sharing
- Advanced

To apply a limit, select the appropriate category, click **Add**, select the limit, and then select or enter the value. For example, to disable the **Lock users in home directory** option for a domain, follow these steps:

1. Select Domain Limits & Settings from the Serv-U Management Console.
2. Select **Directory Listing** from the **Limit Type** list.
3. Click **Add**.
4. Select **Lock users in home directory** from the **Limit**list.
5. Deselect the option.
6. Click **Save**.

The limits list displays the current limits applied to the domain. Limits with a light-blue shade to the background are default values. Limits with a white background are values that override the defaults. After completing the above steps, a new **Lock users in home directory** limit appears in the list that displays "No" for the value. Because of inheritance rules, this option applies to all users in the domain unless overridden at the Group or User level. For more information on this method of inheritance, see "User Interface Conventions".

Limits can be deleted by selecting them, and then clicking **Delete**. To edit an overridden value, select the limit, and then click **Edit**. Default rules cannot be edited or deleted. Create a new limit to override a default one.

To create a limit that is restricted to a specific time of day or days of the week, click **Advanced** on the New / Edit Limit dialog. The additional options allow you to **Apply limit only at this time of day** at which point a start and stop time for the new limit can be entered. To restrict the limit to certain days of the week, deselect the days for which you do not want to apply the limit. When a limit is restricted in this way, default values (or the value of other limit overrides) are applied when the time of day or day of the week restrictions are not met for this limit.

The following is a reference of all available domain limits, organized by category.

Connection

Maximum number of sessions on domain

Specifies the maximum number of concurrent sessions that may be allowed on the current domain.

Maximum sessions per IP address on domain

Specifies the maximum number of concurrent sessions that may be opened to the current domain from a single IP address.

Maximum number of sessions per user account

Specifies the maximum number of concurrent sessions that may be opened from a single user account.

Maximum sessions per IP address for user account

Specifies the maximum number of concurrent sessions that a user may open from a single IP address.

Require secure connection before login

Requires that a connection be secure (for example, FTPS, SFTP, or HTTPS), before it is accepted.

Automatic idle connection timeout

Specifies the number of minutes that must pass after the last client data transfer before a session is disconnected for being idle.

Note: Setting the Packet time-out is a requirement for this limit to work. The value of Packet time-out must be less than the value of the Automatic idle connection timeout for the Automatic idle connection timeout to work properly. For information about setting the packet time-out, see "Server Settings".

Automatic session timeout

Specifies the number of minutes a session is allowed to last before being disconnected by the server.

Block anti-timeout schemes

Blocks the use of commands such as "NOOP", which is commonly used to keep FTP Command Channel connections open during long file transfers or other periods of inactivity where no information is being transferred on the control channel. When these are blocked, Serv-U disconnects the client when the connection has been idle, that is, not transferring data, for a specified period of time.

Automatically create home directories

Instructs Serv-U on whether or not to automatically create the home directory specified when creating a new user account if the directory does not already exist.

Block IP address of timed out session

Specifies the number of minutes for which the IP address of a timed out session is blocked.

Allow X-Forwarded-For to change HTTP connection IP addresses

When enabled, the "X-Forwarded-For" HTTP header parameter changes the IP address of the client for Serv-U. This is useful when all HTTP connections are coming from a proxy server or a load balancer. Proxy servers and load balancers typically append this parameter to the HTTP header so that HTTP servers can identify the actual client IP address and apply security rules as needed.

Require reverse DNS name

Requires that users connecting to the server connect from an IP address that has a valid reverse DNS name, also known as a PTR record. Checks for the existence of a valid PTR record but does not check its contents.

Password

Check anonymous passwords

Specifies whether or not Serv-U should validate email addresses supplied as the password to login anonymously.

Require complex passwords

Specifies that all user account passwords must contain at least one uppercase and one non-alphabetic character to be considered valid.

Minimum password length

Specifies the minimum number of characters required in a user account's password. Specifying 0 characters indicates that there is no minimum requirement.

Automatically expire passwords

Specifies the number of days a password is valid before it must be changed. Specifying 0 days means passwords never expire.

Allow users to change password

Specifies whether or not users are allowed to change their own passwords.

Mask received passwords in logs

Masks the passwords received from clients from being shown in log files. Disabling this allows passwords to be displayed in log files, which can be useful for debugging connection problems or auditing user account security.

Password encryption mode

Specifies the level of password encryption on user passwords. The following options are available:

- One-way encryption (more secure) - This option fully encrypts passwords and cannot be reversed. This is the default setting.
- Simple two-way encryption (less secure) - This option encrypts passwords in a reversible format for easy recovery. Use this option when users are expected to take advantage of the Password Recovery utility in the Web Client. In this case it may be desirable to use two-way encryption so that Serv-U does not need to reset their passwords when password recovery is requested.
- No encryption (not recommended) - This option stores passwords in clear text. Using this option may be necessary for integration with legacy systems (especially when using database support).

Note: When you change this setting, all user passwords must be reset. Existing passwords are not updated automatically, and must be re-saved to be stored in the new format.

Allow users to recover password

If enabled, allows users to recover passwords using the Web Client password recovery utility at the login page.

SSH authentication type

Specifies how SSH authentication is to occur. Options include: "Password and Public Key" - requires both a password and a public key (when specified) for login; "Password or Public Key" - requires either a password or public key for login; "Public Key Only" - requires that a public key is provided for successful login, a password is not allowed; "Password Only" - requires that a password is provided for successful login, a public key is not allowed.

Days before considering password to be stale

The number of days prior to expiration that a password is to be considered stale. A stale password is a password that is about to expire. An event can be configured to identify when a password is about to expire. This value is the lead-time, in days, before password expiration.

Directory Listing

Hide files marked as hidden from listings

Hides files and folders from directory listings that have the Windows "hidden" system attribute set on them.

Use lowercase for file names and directories

Forces Serv-U to display all file names and directories using lowercase characters, regardless of the actual letter case in use by the file or directory.

Interpret Windows shortcuts as links

Instructs Serv-U to treat all valid .lnk files as the actual destination object. In other words, if a .lnk file points to another file, the destination file is shown in the directory listing instead of the .lnk file itself.

Treat Windows shortcuts as target in links

Instructs Serv-U to treat all valid .lnk (shortcut) files as a UNIX symbolic link.

Lock users in home directory

Locks users into their home directory, and does not allow Users to browse above that folder. In addition, their home directory is displayed as "/" masking the actual physical location.

Allow root ("/") to list drives for unlocked users (Windows Only)

Allows users to change directory to the root ("/") of the system and display all drives on the computer. This option only works when the user is not locked in their home directory.

Use natural language sorting for sorted listings

By default, Serv-U uses natural language sorting for a more intuitive sort order. However, some clients may prefer ASCII sorting. Serv-U supports both sort orders.

Hide the compressed state of files and directories

Hides the compressed state of all compressed files and directories being viewed by the user.

Hide the encrypted state of files and directories

Hides the encrypted state of all encrypted files and directories being viewed by the user.

Message file path

Welcome messages are normally displayed once to a user during login to relay important information to users about the file server site. By using a secondary message file, welcome messages can be provided in specific folders to relay additional information. A non-relative path such as `MessageFile.message` can be used as the path. The welcome message will only be displayed when navigating into folders which contain a file matching the specified file name.

Data Transfer

Maximum upload speed for domain

Limits the maximum bandwidth that can be used domain-wide for all uploads. Setting a limit of 0 KB/s means unlimited bandwidth.

Maximum download speed for domain

Limits the maximum bandwidth that can be used domain-wide for all downloads. Setting a limit of 0 KB/s means unlimited bandwidth.

Maximum upload speed per session

Limits the maximum upload bandwidth for each individual session. Setting a limit of 0 KB/s means unlimited bandwidth.

Maximum download speed per session

Limits the maximum download bandwidth for each individual session. Setting a limit of 0 KB/s means unlimited bandwidth.

Maximum upload speed for user accounts

Limits the maximum upload bandwidth shared between all sessions associated with an individual User account. Setting a limit of 0 KB/s means unlimited bandwidth.

Maximum upload file size

Restricts the maximum single file size a user can upload to Serv-U. The file size is measured in kilobytes.

Maximum download speed for user accounts

Limits the maximum download bandwidth shared between all sessions associated with an individual user account. Setting a limit of 0 KB/s means unlimited bandwidth.

Delete partially uploaded files

Instructs Serv-U to delete incomplete file uploads. If this option is enabled, users are not able to restart interrupted uploads using the REST (Restart) FTP command.

Interpret line feed byte as a new line when in ASCII mode (Windows Only)

When uploading and downloading files using ASCII mode, Serv-U will assume <LF> characters are the same as <CR><LF> end-of-line markers. Most Windows applications expect <CR><LF> to represent a new-line, as does the FTP protocol. However, since the definition of a new-line sequence is not fully defined in Windows, this option allows Serv-U to assume <LF> is the same as <CR><LF>. When uploading in ASCII mode stand-alone <LF> characters are changed to <CR><LF> prior to writing to the file. When downloading in ASCII mode, stand-alone <LF> characters are changed to <CR><LF> prior to sending to the client.

Automatically check directory sizes during upload

Instructs Serv-U to occasionally check the size of directories in which a maximum directory size has been specified. This attribute ensures that Serv-U always has updated directory sizes available instead of having to calculate them at transfer time, which can be a time consuming operation.

HTTP

Warn end users when using old web browsers

When enabled (default) Serv-U will warn users that they are using an outdated browser and should upgrade the browser to take advantage of performance and feature enhancements to improve their experience.

Default language for Web Client

When the end-user connects with an unsupported language, the HTTP Login Page is displayed in English. The default language can be set to any language you want. When connecting to Serv-U using a supported localization of Windows, the native language of Windows is used.

Allow HTTP media playback

The Serv-U Web Client supports fully interactive media playback of audio and video files. This function can be disabled as desired during specific business hours or altogether based on business needs.

Allow browsers to remember login information

The HTTP login page supports a Remember me option (not enabled by default) that allows usernames to be remembered by the login page. This feature can be disabled for security reasons.

Allow users to change languages

The Serv-U Web Client is supported in many languages, but if users should not be able to select their native language this can be disabled.

Allow users to use Web Client

Serv-U Web Client is enabled by default. Administrators can disallow the use of Serv-U Web Client by disabling this limit.

Allow users to use Web Client Pro

Serv-U Web Client Pro is enabled by default. Administrators can disallow the use of Serv-U Web Client Pro by disabling this limit.

Allow users to use FTP Voyager JV

FTP Voyager JV is enabled by default. Administrators can disallow the use of FTP Voyager JV by disabling this limit.

Maintain file dates and times after uploading (FTP Voyager JV and Web Client Pro only)

When enabled, Serv-U can maintain the last modification date and time of the file when end-users are using FTP Voyager JV or Web Client Pro. When disabled, Serv-U will not set the file's last modification date and time, it will remain the date and time the file was uploaded.

Allow HTTP sessions to change IP address (disabling may cause mobile devices to fail)

The Serv-U Web Client supports the transfer of HTTP sessions if the IP address changes. This option can be disabled but it may cause mobile devices to be disconnected due to frequent IP address changes by these devices.

Hide Serv-U version information in HTTP response headers

When enabled, the version information of Serv-U will be hidden in HTTP and HTTPs response headers. This way a potential security threat arising from the knowledge of the version information can be mitigated.

Allow autocomplete for HTTP login fields

With this limit you can configure whether or not password auto-completion is allowed on the Serv-U login screen. This option is enabled by default.

File Sharing

Require a password for guest access

Specifies whether it is possible to set up a file share where the guest is required to provide a password. When this limit is set to Always or Never, the creator of the file share will not be able to specify this optional setting. When this limit is set to Optional, the user can individually specify in each file share whether or not the guest must provide a password.

Insert passwords within invitation emails

Specifies whether it is possible to set up a file share where the password for the share is included in the invitation email. When this limit is set to Always or Never, the creator of the file share will not be able to specify this optional setting. When this limit is set to Optional, the **Include the password in the email** option can be selected individually in each file share.

Maximum file size guests can upload (per file)

Specifies the file size constraints imposed upon the guest user. If set to 0, there is no file size constraint. In this case, the creator of the file share request can specify the maximum file size in each file share request without an upper limit.

Allow user-defined guest link expiration

When enabled, users will be able to specify link expiration dates individually on the Request Files and Send Files wizards. When disabled, the file share links will expire after the number of days specified in the **Duration before guest link expires** limit.

Duration before guest link expires

Limits the number of days after which a file share link expires if the Allow user-defined guest link expiration limit is disabled.

Notify user after a file is downloaded

Specifies whether the **Notify me when the file(s) have been downloaded** option can be used on the Send Files wizard. When this limit is set to Always or Never, the creator of the file share will not be able to specify this optional setting. When this limit is set to Optional, the user can individually specify in each file share whether to receive notification of the file download.

Notify user after a file is uploaded

Specifies whether the **Notify me when the file(s) have been uploaded** option can be used on the Request Files wizard. When this limit is set to Always or Never, the creator of the file share request will not be able to specify this optional setting. When this limit is set to Optional, the user can individually specify in each file share request whether to receive notification of the file upload.

Send the guest access link to the recipients

Specifies whether the **Automatically send the download/upload link to the guest user(s) in email** option can be used on the Send Files and Request Files wizard. When this limit is set to Always or Never, the user will not be able to specify this optional setting. When this limit is set to Optional, the user can individually specify in each file share or file share request whether to send the access link automatically.

Send the guest access link to the sender

Specifies whether the **Send me an email copy with the download/upload link** option can be used on the Send Files and Request Files wizard. When this limit is set to Always or Never, the user will not be able to specify this optional setting. When this limit is set to Optional, the user can individually specify in each file share or file share request whether to receive an email copy with the download/upload link.

Allow user-defined contact information

When enabled, users will be able to edit their name and email address on the Request Files and Send Files wizards. When disabled, users are not allowed to edit their contact information on the Request Files and Send Files wizards.

Maximum number of files for "Sent" shares

Specifies the maximum number of files users can include in a single file share. If set to 0, the default limit of 20 is used.

Maximum number of files for "Requested" shares

Specifies the maximum number of files users can upload after receiving a file share request. If set to 0, the default limit of 20 is used.

Advanced

Convert URL characters in commands to ASCII

Instructs Serv-U to convert special characters contained in command parameters to plain ASCII text. Certain web browsers can encode special characters contained in file names and directories when using the FTP protocol. This attribute allows Serv-U to decode these special characters.

Maximum supported SFTP version

Specifies the maximum version of SFTP permitted for SFTP connections. Serv-U supports SFTP versions 3-6.

Allow rename overwrite

When enabled (default) Serv-U allows files to be renamed to files where the destination already exists. When disabled users are not allowed to rename a file or directory to a path name that already exists.

Apply server and domain directory access rules before user and group

The order in which Directory Access Rules are listed has significance in determining the resources that are available to a user or group account. By default, Directory Access Rules specified at the group or user level take precedence over ones specified at the domain and server level. However, there are certain instances where you may want the domain and server level rules to take precedence. Setting this value to "Yes" places the group's and user's Directory Access Rules *below* the server and domain. Please also refer to the "Apply group directory access rules first" setting which is outlined in Group Information.

Days before automatically disabling account to trigger the pre-disable event

The number of days prior to automatically disabling the user account that the pre-disable event should be triggered.

Days before automatically deleting account to trigger the pre-delete event

The number of days prior to automatically deleting the user account that the pre-delete event should be triggered.

Owner ID (user name) for created files and directories (Linux Only)

The user name given to set as the owner of a created file or directory.

Group ID (group name) for created files and directories (Linux Only)

The group name given to set as the owner of a created file or directory.

Reset user stats after restart

When this limit is enabled the user stats are reset after a server restart.

Reset group stats after restart

When this limit is enabled the group stats are reset after a server restart.

Domain Settings

The **Domain Limits and Settings > Settings** tab allows you to configure basic domain settings that affect performance, security, and network connectivity. To configure a setting, specify the value you want in the appropriate area, and then click **Save**. The following sections provide more information about the settings that can be configured.

Connection Settings

Block users who connect more than 'x' times within 'y' seconds for 'z' minutes

Also known as anti-hammering, enabling this option is a method of preventing brute force password guessing systems from using dictionary style attacks to locate a valid password for a user account. Using strong, complex passwords defeats most dictionary attacks. However, enabling this option ensures that Serv-U does not waste time processing connections from these illegitimate sources. When configuring this option, ensure that there is some room available for legitimate users to correct an incorrect password before they are blocked.

When enabled, this option temporarily blocks IP addresses for 'z' minutes that fail to successfully login after 'x' attempts within 'y' seconds. IP addresses blocked in this way can be viewed in the appropriate IP Access rules tab. A successful login resets the counter tracking attempted logins.

Hide server information from SSH identity

After a successful SSH login, the server sends identification information to the client. Normally, this information includes the server name and version number. Enable this option to prevent the information from being given to the client.

Default Web Client

Specifies whether the Web Client or FTP Voyager JV should be used by all HTTP clients by default. A third option (the default option) is to prompt the user for the client they want to use instead. This option is also available at the group and user level.

Client Support Link

The Client Support Link is a powerful feature that allows a direct method of contact to be inserted into the Web Client and FTP Voyager JV in the event that a client requires support or assistance. The basic syntax for this feature is `protocol:path`. This option is highly flexible and allows for any network shortcut to be used, such as the following:

```
http://www.website.com/support/
mailto:service@website.com?subject=Serv-U File Server Support
aim:goim?screenname=ExampleAdminUser&message=I need help with your Serv-
U File Server!
```

Any format can be used as long as the client's machine understands the provided protocol.

Custom HTTP Settings

Basic branding (custom logo and limited text changes) is implemented using the Custom HTTP Settings. Advanced branding is also available. For more information, see "Custom HTML".

For step-by-step instructions for applying your own logo and customizing the text all end users will see on the login screen, see the KB article "Serv-U Web Client Customization (Basic Branding)", http://www.serv-u.com/kb/1781/ServU-Web-Client-Customization-Basic-Branding.

Specify a custom logo to be displayed on the login and Web Client pages

Dimensions for custom logos must have a width of 400 pixels and a height of 100 pixels. If a logo does not meet this criteria an error message will appear when you attempt to save the logo.

Note: JPEG images which use CMYK instead of RGB encoding may not work properly in certain browsers. Test your logo image to make sure it is displayed properly in all browsers.

To add a logo, click **Browse** next to **Custom Logo Path**, and then select the path to your logo. Click **Save** and the logo will appear below the **Custom Logo Path** field. To delete a custom logo, clear the path in the **Custom Logo Path** field, and then click **Save**.

HTTP Login Title Text (no HTML)

Provide text to be used as the title of the HTTP login and Web Client pages.

HTTP Login Page Text

Provide any custom login page text you want in this area. This text can be HTML-formatted, including links, images, and standard formatting like italics, bold, underline, alignment and more.

HTTP Client Interface Background (CSS Only)

Provide a custom CSS background style for the Web Client, File Sharing and FTP Voyager JV landing page. This style follows the CSS background shorthand standard. The "background:" string is assumed so it does not need to be entered here. The format for a CSS background is `color url('/&#37;CUSTOM_HTML_DIR&#37;/images/yourimage.png') repeat-type horizontal-alignment vertical-alignment`.

The `&#37;CUSTOM_HTML_DIR&#37;` must be used in conjunction with the Custom HTML settings. Custom HTML must be enabled and a Custom HTML Container Directory must be specified.

The following examples provide a reference:

- `#0b16f8 url('/&#37;CUSTOM_HTML_DIR&#37;/images/Header01.png') no-repeat right top`
- `#FFFFFF url('/&#37;CUSTOM_HTML_DIR&#37;/images/MyLogoTile.png') repeat-x left top`
- `red (this example uses no image)`
- `url('/&#37;CUSTOM_HTML_DIR&#37;/images/MyHeader.png') no-repeat center top (this example uses no custom color)`

Password Recovery Email Message

Send email messages to users with their login credentials using this customizable password recovery message.

The password recovery email message has a simple default subject and message with the user's login ID and password. This message will be sent if the user has a valid email address recorded in Serv-U. Users may request this message from the Serv-U login page.

Administrators can also send this message to users using the **Recover Password** button under domain users and global users in the Management Console.

Integration DLL / Shared Library

For information about writing an Integration DLL or Shared Library, see the Serv-U Integration Sample DLL installed with Serv-U in the `Serv-U Integration Sample DLL` sub-directory. The Integration API is documented in this sample.

Other Settings

Ratio Free Files

Files listed by clicking **Ratio Free Files** are exempt from Transfer Ratio limitations on file transfers. Ratio free files specified at the server or domain level are inherited by all their users accounts. For more information about ratio free files, see "Transfer Ratio and Quota Management".

FTP Settings

The Serv-U File Server allows for the customization of the FTP commands that it accepts as well as its responses to FTP commands received. When configuring these options at the server level, all domains inherit these customizations. To customize the FTP behavior for a specific domain, select the appropriate domain, open the FTP Settings tab for the domain, and then click **Use Custom Settings** . At any time, you can click **Use Default Settings** to have the domain revert back to the server's default settings.

Warning: Customizing the FTP behavior in this way is not recommended except for those very familiar with the FTP protocol and its standard and extended command set.

Global Properties

When using custom settings, the **Global Properties** button becomes available.

FTP Responses

Global FTP responses are responses shared amongst most FTP commands, such as the error message sent when a file is not found. Customizing a global FTP response ensures that the response is used by all other FTP commands rather than having to customize it for each individual FTP command. FTP command responses can contain special macros that allow real-time data to be inserted in to the response. For more information, see "System Variables".

Message File

The server welcome message is sent in addition to the standard "220 Welcome Message" that identifies the server to clients when they first connect. If the **Include response code in text of message file** option is selected, then the 220 response code begins each line of the specified welcome message. To customize the welcome message, enter the path to a text file in **Message File Path** field. Click **Browse** to select a file on the computer. Serv-U opens this file and sends its contents to connecting clients.

Advanced Options

- Block "FTP_bounce" attacks and FXP (server-to-server transfers) - Select this option to block all server-to-server file transfers involving this Serv-U File Server by only allowing file transfers to the IP address in use by the command channel. For more information about FTP_bounce attacks, see CERT advisory CA-97.27.
- Include response code on all lines of multi-line responses - The FTP protocol defines two ways in which a multi-line response can be issued by

an FTP server. Some older FTP clients have trouble parsing multi-line responses that do not contain the 3-digit response code on each line. Select this option if your clients are using an FTP client experiencing problems with multi-line responses from Serv-U.

- Use UTF-8 encoding for all sent and received paths and file names - By default, Serv-U treats all file names and paths as UTF-8 encoded strings. It also sends all file names and paths as UTF-8 encoded strings, such as when sending a directory listing. Deselecting this option prevents Serv-U from UTF-8 encoding these strings. When this option is deselected, UTF-8 is not included in the FEAT command response to indicate to clients that the server is not using UTF-8 encoding.

Editing FTP Commands and Responses

To edit FTP Commands, select the FTP command to edit, and then click **Edit**.

Information

Under the Information tab, basic information about the command is shown along with a link to more information on our website. Each FTP command can also be disabled by selecting the **Disable command** option. Disabled commands are treated as unrecognized commands when they are received from a client.

FTP Responses

Under the FTP Responses tab, all possible FTP responses to the command as issued by the server can be modified by clicking **Edit** for each response. FTP command responses can contain special macros that allow real-time data to be inserted in to the response. For more information, see "System Variables".

Message Files

Certain FTP commands allow a message file to be associated with them. The contents of a message file are sent along with the standard FTP response. In addition, a secondary message file path is available as a default option. This allows for message files to be specified using a path relative to the user's home directory for the Message File. If the first message file is not found, then Serv-U attempts to use the Secondary Message File instead. By specifying an absolute file path in the secondary location, you can ensure that each user receives a message file.

The following FTP commands allow specifying a message file:

- CDUP
- CWD
- QUIT

Managing Recursive Listings

Serv-U supports recursive listings by default, allowing FTP clients to obtain large directory listings with a single command. In some cases, clients may request excessively large directory listings using the -R parameter to the LIST and NLST commands. If performance in Serv-U is being impacted by users requesting excessively large listings, recursive listings can be disabled using the **Allow client to specify recursive directory listings with -R parameter** option.

Advanced Options

Some FTP commands contain advanced configuration options that offer additional ways to configure the behavior of the command. Where available, the configuration option is described in detail in the Management Console. The following FTP commands contain advanced configuration options:

- LIST
- MDTM
- NLST

Case File - Custom FTP Command Response

Users connecting to the server need to know how much quota space is available in a given folder when they have completed a transfer. To do this, edit the response to the STOR command to include a report on available space. By default, the 226 (command successful) response to the STOR command (which stores files on the server) is the following:

```
Transfer complete. $TransferBytes bytes transferred.
$TransferKBPerSecond KB/sec.
```

Modify this to include an extra variable in the following way:

```
Transfer complete. $TransferBytes bytes transferred.
$TransferKBPerSecond KB/sec. Remaining storage space is $QuotaLeft.
```

The last sentence shows the user how much storage space is left at the end of each file upload. The same can be done for the DELE command, so that every time a user deletes a file, their updated quota value, showing an increase in available space, is displayed. This can be done for any FTP command response.

Encryption

Serv-U supports two methods of encrypted data transfer - Secure Socket Layer (SSL) and Secure Shell 2 (SSH2). SSL is used to secure the File Transfer Protocol (FTP) and Hypertext Transfer Protocol (HTTP). SSH2 is a method of securely interacting with a remote system that supports a method of file transfer commonly referred to as SFTP. Despite its name, SFTP does not have anything in common with the FTP protocol itself.

In order for each method of encryption to work, a certificate and/or private key must be supplied. SSL requires the presence of both, while SSH2 only requires a private key. If you do not possess either of these required files, Serv-U can create them for you.

Encryption options specified at the server level are automatically inherited by all domains. Any encryption options specified at the domain level automatically overrides the corresponding server-level option. Certain configuration options are only available to the server.

When creating SSL/TLS, SSH, and HTTPS encrypted domains within Serv-U, it is important to know that encrypted domains cannot share listeners. Because

SSL/TLS and SSH encryption is based on encrypting traffic sent between IP addresses, each domain must have unique listeners in order to operate properly. In the case that multiple encrypted domains are created that share listeners, the domain created first takes precedence causing other encrypted domains to fail to function properly. To operate multiple encrypted domains, modify the listeners of each domain to ensure they listen on unique port numbers.

Configuring SSL for FTPS and HTTPS

To use an existing certificate:

1. Obtain an SSL certificate and private key file from a certificate authority.
2. Place these files in a secured directory in the server.
3. Use the appropriate **Browse** button to select both the certificate and private key files.
4. If a CA (Certificate Authority) PEM file has been issued, enter or browse to the file.
5. Enter the password used to encrypt the private key file.
6. Click **Save**.

If the provided file paths and password are all correct, Serv-U begins using the certificate immediately to secure FTPS and HTTPS connections using the provided certificate. If the password is incorrect or Serv-U cannot find either of the provided files, an error message is displayed that explains the encountered error.

To create a new certificate:

1. Click **Create Certificate**.
2. Specify the **Certificate Set Name** that is used to name each of the files Serv-U creates.
3. Specify the output path where the created files are to be placed. In most cases, the installation directory is a safe location (for example, `C:\ProgramData\RhinoSoft\Serv-U\`).

4. Specify the city/town in which the server or corporation is located.
5. Specify the state (if applicable) in which the server or corporation is located.
6. Specify the 2-digit country code for the country in which the server or corporation is located.
7. Specify the password used to secure the private key.
8. Specify the full organization name.
9. Specify the common name of the certificate. The IP address or the Fully Qualified Domain Name (FQDN) that users use to connect must be listed here. **Note**: If the Common Name is not the IP address or FQDN used by clients to connect, clients may be prompted that the certificate does not match the domain name they are connecting to.
10. Specify the business unit the server resides in.
11. Specify the key length in bits.
12. Click **Create** to complete the certificate creation.

Serv-U creates three files using the provided information: A self-signed certificate (.crt) that can be used immediately on the server but is not authenticated by any known certificate authority, a certificate request (.csr) that can be provided to a certificate authority for authentication, and a private key file (.key) that is used to secure both certificate files. It is extremely important that the private key be kept in a safe and secure location. If your private key is compromised, then your certificate can be used by malicious individuals.

Viewing the certificate

To view the SSL certificate once it is configured, click **View Certificate**. All identifying information about the certificate, including the dates during which the certificate is valid, are displayed in a new dialog.

SFTP (Secure File Transfer over SSH2)

To use an existing private key:

1. Obtain a private key file.
2. Place the private key file in a secured directory in the server. Use **Browse** in Serv-U to select the file.
3. Enter the password for the private key file.
4. Click **Save**.

To create a private key:

1. Click **Create Private Key**.
2. Enter the name of the private key, (for example, `MyDomain Key`), which is also used to name the storage file.
3. Enter the output path of the certificate, (for example, `C:\ProgramData\RhinoSoft\Serv-U\`).
4. Select the Key Type (default of DSA is preferred, but RSA is available).
5. Select the Key Length (default of 1024 bits provides best performance, 2048 bits is a good median, while 4096 bits provides best security).
6. Enter the password to use for securing the private key file.

SSH Ciphers and MACs

By default, all supported SSH ciphers and MACs (Message Authentication Codes) are enabled for use by the server. If your specific security needs dictate that only certain ciphers or MACs can be used, you can individually disable unwanted ciphers and MACs by deselecting the appropriate ciphers or MACs.

Custom HTML

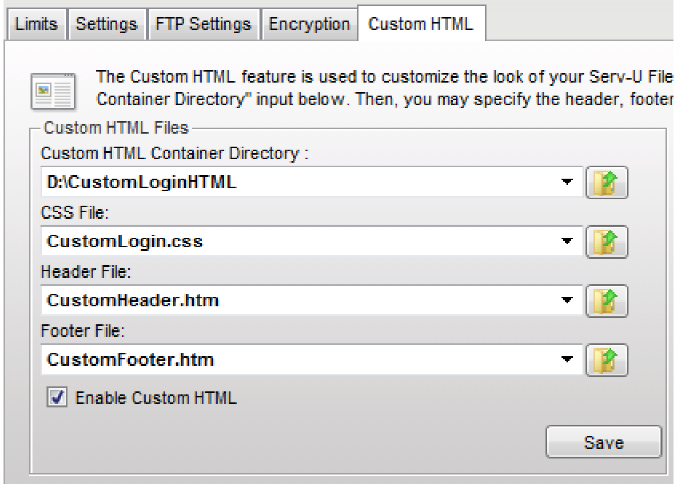
Serv-U supports custom HTML for the HTTP/HTTPS login pages. This feature allows experienced web developers to design their login experience to show off their exclusive brand and design the page to match existing business themes.

Basic branding (custom logo and limited text changes) is also available. For more information, see "Domain Settings".

The Custom HTML feature operates by allowing a web developer to provide a custom header and custom footer for the HTTP/HTTPS login page, while the main Login Form is automatically inserted between the content defined in the Header File and Footer File. The Custom HTML interface also uses a CSS file which defines the style used in the Login Form. This CSS file can also be used to define custom CSS styles, containers, other CSS formatting as needed.

Several branding samples are automatically unpacked to your installation folder (for example, `C:\Program Files\RhinoSoft\Serv-U\Custom HTML Samples`) when Serv-U is installed. Serv-U KB #2054 has step-by-step instructions to explore the current set of samples and build your own branding.

The fields used by the Custom HTML feature are the following:



The Custom HTML feature is used to customize the look of your Serv-U File
Container Directory" input below. Then, you may specify the header, footer

Custom HTML Container Directory : D:\CustomLoginHTML

CSS File: CustomLogin.css

Header File: CustomHeader.htm

Footer File: CustomFooter.htm

☑ Enable Custom HTML

- Custom HTML Container Directory - This directory contains all of the files used by the Custom HTML, including all images, the Header File, the Footer File, and the CSS file. Subdirectories in this folder are allowed.
- CSS File - This .CSS file contains all the styles, containers, and other formatting that will be used throughout the Header File and Footer File, as well as the styles that will be used by the Login Form.

- Header File - This .HTM file contains the content for the HTML header content that will be inserted before the Login Form.
- Footer File - This .HTM file contains the content for the HTML footer content that will be inserted after the Login Form.
- Enable Custom HTML - The Custom HTML will not be used by Serv-U until this option is enabled.

Most Custom HTML interfaces will include custom images, which requires Serv-U to know where the images are being kept. To universalize this storage location, Serv-U requires the use of the `&#37;25CUSTOM_HTML_DIR&#37;25` tag in paths referencing images. This has the further benefit of avoiding changes to HTML when the container storing the HTML files and images is changed, because the path only has to be defined once in the **Custom HTML Container Directory** field. The tag is used as follows:

```
<img src="/&#37;25CUSTOM_HTML_DIR&#37;25/images/image.png" alt="My
Image">
```

File Share

The File Sharing feature allows your domain users to send or receive files from guests.

Note: File Sharing is disabled by default. You must select the relevant option to enable it.

To send file sharing invitation emails, you must configure your SMTP settings. This configuration only needs to be set once for the entire server or a domain.

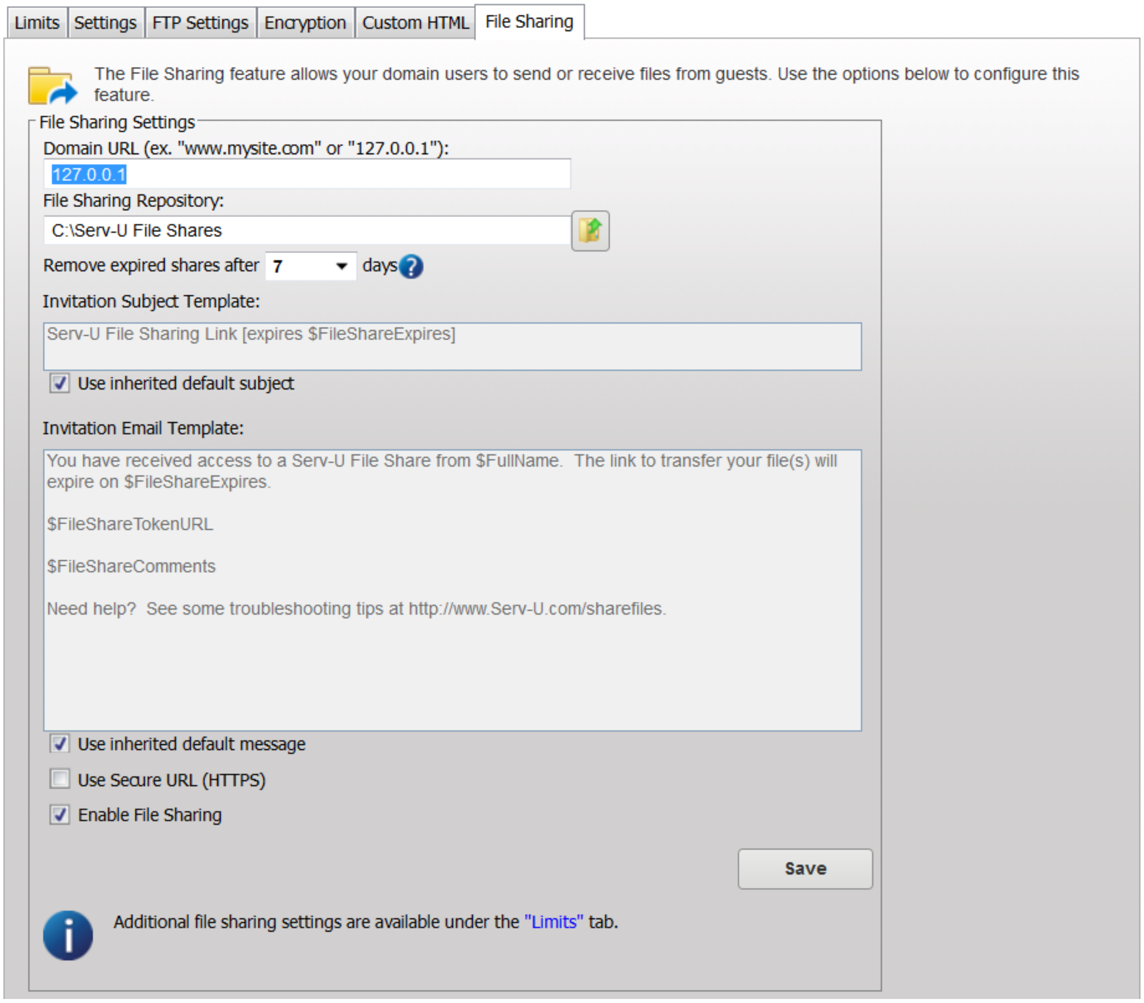
Click here to view common Administrator FAQs:

http://www.solarwinds.com/documentation/kbLoader.aspx?kb=4771

To enable file sharing:

1. Navigate to Server Limits and Settings > File Sharing.
2. Type the address for the Domain URL.
3. Type the location of the File Sharing Repository.

4. Select the number of days until the shares expire.
5. Select whether you want to use the inherited default email invitation subject, or customize your own. ***If the option is deselected***, you can type in a custom email invitation subject.
6. Select whether you want to use the inherited default email notification message, or customize your own. ***If the option is deselected***, you can type in a custom message.
7. Select **Enable File Sharing**.
8. If it is not configured yet, configure your SMTP to be able to send and receive notification emails. For more information, see "Serv-U SMTP Configuration".
9. Click **Save**.



The File Sharing feature allows your domain users to send or receive files from guests. Use the options below to configure this feature.

File Sharing Settings

Domain URL (ex. "www.mysite.com" or "127.0.0.1"): 127.0.0.1

File Sharing Repository: C:\Serv-U File Shares

Remove expired shares after 7 days

Invitation Subject Template: Serv-U File Sharing Link [expires $FileShareExpires]

☑ Use inherited default subject

Invitation Email Template:

You have received access to a Serv-U File Share from $FullName. The link to transfer your file(s) will expire on $FileShareExpires.

$FileShareTokenURL

$FileShareComments

Need help? See some troubleshooting tips at http://www.Serv-U.com/sharefiles.

☑ Use inherited default message

☐ Use Secure URL (HTTPS)

☑ Enable File Sharing

Additional file sharing settings are available under the "Limits" tab.

Server Activity

The Server Activity > Sessions, and Domain Activity > Sessions tabs display the current File Server session activity. When viewing the Sessions page from the server, all connected sessions from all domains are displayed. When viewed while administering a domain, only that domain's current sessions are displayed. From this page, an overall picture of the current activity on the File Server can be seen. In addition, individual sessions can be viewed including their current status, connection state, and transfer information.

To view the detailed information on a specific session, select the session. The **Active Session Information** group is populated with the details of the currently highlighted session. This information is frequently updated to provide you with an accurate and up-to-date snapshot of that session's activities.

Depending upon the type of connection made by that session (for example, FTP, HTTP, or SFTP), certain additional functions are available.

Disconnect

Any type of session can be disconnected at any time by clicking **Disconnect**. Click this button to bring up another dialog with additional options for how the disconnect should be performed. The following disconnect options are available:

- Disconnect - Immediately disconnects the session. Another session can be immediately established by the disconnected client. This is also known as "kicking" the user.
- Disconnect and ban IP for - Immediately disconnects the session and bans their IP address for the specified number of minutes, preventing them from immediately reconnecting.
- Disconnect and block IP permanently - Immediately disconnects the session and adds a deny IP access rule for their IP address, preventing them from ever reconnecting from the same IP address.

When disconnecting a session from the Server Session view, an additional option is available called **Apply IP rule to**. This option allows you to select where you would like the temporary or permanent IP ban to be applied - for the entire server or just the domain the session is connected to.

In addition to disconnecting the session, the user account in use by the session can also be disabled by selecting **Disable user account**.

If the current session is using the FTP protocol, a message can be sent to the user before disconnecting them by typing it in the **Message to user** field. This option is not available for HTTP or SFTP sessions as neither protocol defines a method for chatting with users.

Spy & Chat

Any type of session can be spied on by clicking **Spy & Chat** or double-clicking on a session from the list. Spying on a user displays all the detailed information normally visible by highlighting the session, but also includes a complete copy of the session's log since it first connected to the file server. This allows an administrator to browse the log and view all actions taken by the session's user.

If the current session is using the FTP protocol, additional options are available for chatting with the user. The **Chat** group shows all messages sent to and received from the session since beginning to "spy" on the session. To send a message to the session, type the message text in the **Message Content** field, and then click **Send**. When a message is received from the session, it is automatically displayed here.

Note: Not all FTP clients support chatting with system administrators. The command used to send a message to the server is `SITE MSG`. In order for a client to receive messages, the client application must be capable of receiving unsolicited responses from the server (instead of just discarding them).

Broadcast

A message can be sent to all currently connected FTP sessions by clicking **Broadcast**. Sending a message via broadcast is equivalent to opening the **Spy & Chat** dialog to each individual FTP session and sending it a chat message.

Abort

If a session is performing a file transfer, the file transfer can be terminated without disconnecting the session by clicking **Abort**. After confirming the abort command, the current file transfer for that session is terminated by the server. Some clients, especially FTP and SFTP clients, may automatically restart the aborted transfer making it appear that the abort failed. If this is the case, try disconnecting the session instead.

Server and Domain Statistics

The Server Activity > Statistics and Domain Activity > Statistics pages show detailed statistics on the use of the server for use in benchmarking and records keeping. Statistics viewed at the server level are an aggregate of those accumulated by all domains on the server. Statistics viewed for an individual domain are for that domain only. The displayed information includes the following:

Session Statistics

Current Sessions

The number of sessions currently connected.

Total Sessions

The total number of sessions that have connected since being placed online.

24 Hrs Sessions

The number of sessions that have connected in the past 24 hours.

Highest Num Sessions

The highest number of concurrent sessions that has been recorded since being placed online.

Average Session Length

The average length of time a session has remained connected.

Longest Session

The longest recorded time for a session.

Login Statistics

These statistics can apply to either a domain or the entire server depending on the statistics currently being viewed. Login statistics differ from session statistics because they apply to a login (providing a login ID and password) as opposed to connecting and disconnection.

Logins

The total number of successful logins.

Average Duration Logged In

The average login time for all sessions.

Last Login Time

The last recorded valid login time (not the last time a connection was made).

Last Logout Time

The last recorded valid logout time.

Most Logged In

The highest number of users logged in concurrently.

Currently Logged In

The number of sessions currently logged in.

Transfer Statistics

Download Speed

Cumulative download bandwidth currently being used.

Upload Speed

Cumulative upload bandwidth currently being used.

Downloaded

The total amount of data, and number of files, downloaded since being placed online.

Uploaded

The total amount of data, and number of files, uploaded since being placed online.

Average Download Speed

The average download bandwidth used since being placed online.

Average Upload Speed

The average upload bandwidth used since being placed online.

User & Group Statistics

The User & Group Statistics pages show detailed statistics based on individual user or group activity. Statistics viewed for a user or group are for that user or group only. The displayed information includes the following:

Session Statistics

Current Sessions

The number of sessions currently connected.

24 Hrs Sessions

The number of sessions that have connected in the past 24 hours.

Total Sessions

The total number of sessions that have connected since being placed online.

Highest Num Sessions

The highest number of concurrent sessions that has been recorded since being placed online.

Avg. Session Length

The average length of time a session has remained connected.

Longest Session

The longest recorded time for a session.

Login Statistics

These statistics can apply to either a user or a group of users depending on the statistics currently being viewed. Login statistics differ from session statistics because they apply to a login (providing a login ID and password) as opposed to connecting and disconnection.

Logins

The total number of successful logins.

Last Login Time

The last recorded valid login time (not the last time a connection was made).

Last Logout Time

The last recorded valid logout time.

Logouts

The total number of logouts.

Most Logged In

The highest number of simultaneously logged in sessions.

Longest Duration Logged In

The longest amount of time a session was logged in.

Currently Logged In

The number of sessions currently logged in.

Average Duration Logged In

The average login time for all sessions.

Shortest Login Duration Seconds

The shortest amount of time a session was logged in.

Transfer Statistics

Download Speed

Cumulative download bandwidth currently being used.

Upload Speed

Cumulative upload bandwidth currently being used.

Average Download Speed

The average download bandwidth used since being placed online.

Average Upload Speed

The average upload bandwidth used since being placed online.

Downloaded

The total amount of data, and number of files, downloaded since being placed online.

Uploaded

The total amount of data, and number of files, uploaded since being placed online.

Save Statistics

User and group statistics can be saved directly to a CSV file for programmatic analysis and review. In order to save statistics to a file, first select the user or group you want to generate a statistics file for, and then click **Save Statistics** on the bottom of the page.

Server & Domain Log

The Server Activity > Log and Domain Activity > Log tabs show logged activity for the server or domain.

The Server Log shows File Server startup, configuration, and shutdown information. It does not show domain activity information. To activity logs, view the appropriate domain's log instead. In addition to status information about libraries, licensing, and the current build that is logged when the File Server is first starts, the Server Log also contains information about all domain listener status, Universal Plug-and-Play (UPnP) status information, and PASV port range status. The information contained in the Server Log is also saved to a text file located in the installation directory that is named `Serv-U-StartupLog.txt`. This file is replaced each time the Serv-U File Server is started.

The Domain Log contains information about and activity pertaining to the currently administered domain only. This includes the status of the domain's listeners and any configured activity log information. For more information about the types of activity information that can be placed in the Domain Log, see "Configuring Domain Logs".

Information contained in the log can be highlighted by clicking and dragging the mouse cursor over the appropriate portion of the log. Once highlighted, the selected portion can be copied to the clipboard.

Freeze Log

Select this option to temporarily pause the refreshing of the log. This is useful on busy systems so a certain section of the log can be highlighted and copied before it scrolls out of view. Once finished, deselect the option to resume the automatic updating of the log.

Select All

Click this button to automatically freeze the log and highlight all currently displayed log information so that it can be copied to the clipboard.

Clear Log

When the log has become too large for you to view at once, click this button to erase the currently displayed log information. Only log information received after clicking the button is displayed.

Legend

To make viewing the different components of the log easier, each different type of logged message is color-coded for quick identification. Clicking this shows the legend in a draggable dialog. Drag the legend dialog to a convenient location so it can be used for reference while browsing the log.

Filter Log

To quickly find and read through specific sections of the log, it can be filtered based upon a search string. Click this button to bring up the Filter Log dialog. Provide a search string, and then click **Filter** to refresh the log to only display log entries containing the search string. To view the entire contents of the log again, open the Filter Log dialog, and then click **Reset**.

Download Log

To download the full log file from Serv-U, click **Download Log**. If you have permission to download the file your web browser will prompt you to choose a location to save the file, or begin downloading the file automatically.

Configuring Domain Logs

The Serv-U File Server allows for a great deal of customization in logging domain events and activity. Logging is broken into two sections: File and Screen. To enable a logging option, select the appropriate option in the File or Screen column. When an option is selected from the File column, the appropriate logging information is saved to the specified log file if **Enable logging to file** is selected.

When an option is selected from the Screen column, then the event is displayed in the log when viewed from the Serv-U Management Console. The log can be configured to show as much or as little information as you want. After configuring the logging options you want, click **Save** to save the changes.

Logging to File Settings

Log file path

The log file must be given a name before information can be saved to a file. Click **Browse** to select an existing file or directory location for the log file. The log file path supports certain wildcard characters as outlined below. Wildcard characters referencing the date applies to the day that the log file is created. When combined with the **Automatically rotate log file** option, wildcards provide an automatic way to archive domain activity for audits, such as those required by HIPAA. The available wildcard characters are the following:

- %H - The hour of the day (24-hour clock)
- %D - The current day of the month
- %M - The name of the current month
- %N - The numeric value of the current month (1-12)
- %Y - The 4-digit value of the current year, (for example, 2014)
- %X - The 2-digit value of the current year, (for example, 14 for 2014)
- %S - The name of the domain whose activity is being logged

Enable logging to file

Select this option to enable Serv-U to begin saving log information to the file specified in the **Log file path**. If this option is not selected, Serv-U does not log any information to the file, regardless of the individual options selected in the File column.

Automatically rotate log file

To ensure that log files remain a manageable size and can be easily referenced during auditing, Serv-U supports the ability to automatically rotate the log file on a regular basis. By specifying a **Log file path** containing wildcards referencing the current date, Serv-U can rotate the log file and create a unique file name every hour, day, week, month, or year.

Purge Old Log Files

Serv-U supports the ability to automatically purge old log files by setting a maximum number of files to keep and/or a maximum size limit in megabytes. Setting these options to "0" means the setting is unlimited and the limit is not applied.

Warning: Log files are purged based only on the current log file path name and purged approximately every 10 minutes. Log file variables are replaced with Windows wildcard values used to search for matching files. For example:

`C:\Logs\%Y:%N:%D %S Log.txt` is searched for `C:\Logs\????:??:?? * Log.txt`

`C:\Logs\%Y:%M:%D %S Log.txt` is searched for `C:\Logs\????:*:?? * Log.txt`

`C:\Logs\%S\%Y:%M:%D Log.txt` is searched for `C:\Logs\--DomainName--\????:*:?? Log.txt`

Log variables are wildcarded in the following way:

%D --> ??
%N --> ??
%M --> *
%Y --> ????
%X --> ??
%S --> *

Anything matching the wildcarded path name can be purged. Use caution: it is best practice to place log files into a single directory to avoid unexpected file deletion.

Do Not Log IPs

Serv-U supports the ability to specify IP addresses that are exempt from logging. Activity from these IP addresses is not logged to the location specified by the rule - the Screen, a File, or both. This is useful to exempt IP addresses for administrators that may otherwise generate a lot of logging information that can obfuscate domain activity from regular users. It can also be used to save on log space and reduce overhead. Click **Do Not Log IPs**, and then add IP addresses as appropriate.

Chapter 5: Users

About User Accounts

A user account is required in order to provide access to the File Server. At its most basic level, a user account defines login credentials (that is, login ID and password), a home directory, and a set of Directory Access Rules that define the areas of the system accessible to the user and the actions they can perform in those locations. Each active session on the File Server has a user account associated with it that identifies the client to the administrator.

User accounts can be defined in various ways on the Serv-U File Server, including the following:

- **Domain Users** - Defined at the domain level, Domain Users can only log in to the domain under which they are created.
- **Global Users** - Defined at the server level, Global Users are accounts that can log in to any domain on the File Server.
- **Database Users** - Available at both the server and domain level, Database Users are stored in an external database accessible through ODBC and supplement the local account database.
- **Windows Users** - Defined at the domain level, Windows Users use the credentials and often, the home directories, of Windows accounts from the local machine or Windows domain controller (including Active Directory). Windows Users only work on Windows, and require a Serv-U MFT Server license.
- **LDAP Users** - Defined at the domain level, LDAP Users use the credentials and often, the email and other attributes, of LDAP accounts from a remote LDAP server. Unlike Windows Users, LDAP Users work on both Windows and Linux, and may access LDAP servers (including Active Directory and

OpenLDAP) in any accessible domain. LDAP Users require a Serv-U MFT Server license.

Since user accounts can be assigned at the various levels with the same login ID, a hierarchy is used by Serv-U to determine which account takes precedence. The user account types listed above are listed in the order of precedence. Where user accounts can be specified at both the domain and server levels, the domain level account always takes precedence over the server one.

When creating users, consider what kind of access they need, and select the appropriate location for the user account accordingly - time and effort can be saved by entering such settings at the server level to remove the need for multiple user accounts at the domain level.

In Serv-U MFT Server, user accounts can be organized into collections in order to make account management more logical and organized. This can be useful when managing all users from a department or physical location. For example, all users in the accounting department can be placed in a collection named `Accounting`, or all users at an office in Topeka can be placed in a collection named `Topeka Users`.

To create a collection, click **Add** in the **Select user collection** grouping on the Users window. In the new dialog, type the name of your collection, and then click **Save**. Users can now be added this new collection by selecting it and clicking **Add** button below the User list. To move a user from one collection to another, click **Move** below the User list and select the destination collection for the highlighted user accounts. Collections can also be renamed or deleted using the appropriate button.

Warning: When deleting a collection, all user accounts contained in that collection are deleted, too. If you want to keep the user accounts, be sure to move them before deleting the collection.

By default, all users are created in the **General** user collection.

New User Wizard

A wizard is available to assist in creating a new user account. Click **Wizard** on the Users page to open the wizard. The New User Wizard walks you through the 4 steps required to create a user account with the minimum number of required attributes. Once created, the user can be edited to configure more advanced settings such as group membership or additional Directory Access rules. For more information about using the New User Wizard, see the "Quick Start Guide".

User Template

While the New User Wizard offers a way to quickly create a user account with the minimum number of required attributes, most File Server administrators have a collection of settings they want all user accounts to abide by. Groups are the best way to accomplish this task, however there are times when it may not be the course of action you want.

Serv-U allows an administrator to configure a template for new user accounts by clicking **Template**. Once opened, the template user can be configured just like any other user account, with the exception of a login ID. After these settings are saved to the template, all new user accounts that are manually created are done so with their default settings set to those found within the template.

Copying User Accounts

User templates offer a way for large numbers of users to be created with the same settings. In cases where only the settings of a single user must be duplicated or there is a need for multiple user templates, use **Copy** to create a copy of a user account lacking only the username and the password. To copy a user, select the user account and choose **Copy**.

Recover Password

Serv-U supports password recovery both through the Management Console and through the Web Client. For password recovery to be available, the SMTP options for the server or domain must be configured, and the user account must have an email address listed. To use password recovery from the Management Console, select a user account, and then click **Recover Password**. If the password is stored using one-way encryption, the password will be reset and the new password will be sent to the user's email address. If the password is stored using two-way encryption or no encryption, the original password will be sent by email.

Password Recovery from the Web Client requires that the **Allow users to recover password** limit be enabled for the user account. Once this option is enabled, users can use the Recover Password option in the Web Client. Password Recovery from the Web Client otherwise works the same as from the Management Console.

Importing/Exporting User Accounts

User accounts can be imported and exported using the **Import** and **Export** options. Click **Export** to export all users in either the current domain/server or the current Collection to a comma-separated values file (CSV file) which can be viewed in Excel and analyzed by database engines, among other things. Additionally, by creating a CSV file using the same format as the export it is possible to import lists of users from CSV files into Serv-U.

List Filtering on User & Group IDs

In larger deployments of Serv-U, the user list can grow very large. In order to easily find a specific user account, Serv-U supports filtering user and group lists by login ID using input from the administrator. Wildcards are also supported:

- Use the "*" parameter to filter for Users/Group login IDs when the whole ID is unknown (for example, `*Department`, `*Admin*`, `Tech*`).
- Use the "?" parameter when a specific character is unknown (for example, `????Lastname`, `Firstname???`).
- Use the "[]" parameter when a specific character is unknown but should contain one of the specified characters in the brackets (for example, `[utr]sername`, `User[fmn]ame`).

User Information

A user account consists of many attributes and settings. The User Information tab contains general information about the user account including login credentials, the home directory, and the type of account. This topic provides detailed information about each of the available attributes.

Login ID

The login ID is provided by the client as one part of authenticating the session to the File Server. In addition to the login ID, clients must provide a password to complete authentication. Login IDs must be unique for each account specified at that level. Login IDs may not contain any of the following special characters: \ / < > | : ? *.

Note: There are two special login IDs: `Anonymous` and `FTP`. These login IDs are synonymous with one another and can be used for guests on your File Server. These users do not require a password, which should be left blank in this case. Instead, Serv-U requires users who log on with one of these accounts to provide their email address to complete the login process.

Full Name

The full name of the account is available to specify additional identifying information about the account. It is not used by clients when they log in.

Password

The password is the second item required for a session to be authenticated with the File Server. The password should be kept a secret and not shared with anyone other than the person that owns the account. A strong password contains at least 6 characters including a mix of upper and lowercase letters and at least one number. Restrictions can be placed on the length and complexity of passwords through limits. For more information about password limits, see "Limits and Settings".

Additionally, you can generate a new random password for a user by clicking the **Lock** icon next to the **Password**. This new password will follow the defined password length requirements. By default, all passwords are 8 characters long and are complex. If the Minimum Password Length is equal to or less than four characters, the password will be four characters long - otherwise, generated passwords will follow the specified domain value.

Administration Privilege

A user account can be granted one of the following types of administrative privileges:

- No Privilege
- Group Administrator
- Domain Administrator
- System Administrator

The value of this attribute can be inherited through group membership. A user account with No Privilege is a regular user account that can only log in to transfer files to and from the File Server. The Serv-U Management Console is not available to these User accounts.

A Group Administrator can only perform administrative duties relating to their primary group (the group that is listed first in their Groups memberships list. They can add, edit, and delete users which are members of their primary group, as well as assign permissions at or below the level of the Group Administrator. They may not make any other changes.

A Domain Administrator can only administrative duties for the Domain to which their account belongs. A Domain Administrator is also restricted from performing domain-related activities that may affect other domains. The domain-related activities that may *not* be performed by Domain Administrators consist of configuring their domain listeners or configuring ODBC database access for the domain.

A System Administrator has the ability to perform any File Server administration activity including creating and deleting domains, user accounts, or even updating the File Server's license. A user account with System Administrator privileges that is logged in through HTTP remote administration can essentially administer the server as if they had physical access to the machine.

Serv-U also supports read-only administrator accounts which can allow administrators to log in and view configuration options at the domain or server level, greatly aiding remote problem diagnosis when working with outside parties. Read-only administrator privileges are identical to their full-access equivalents, except that they cannot change any settings or create, delete or edit user accounts.

Note: When configuring a user account with administrative privileges, take care in specifying their home directory. An administrator with a home directory other than "\" (root) that is locked in their home directory may not use file paths outside of their home directory when configuring the File Server.

Home Directory

The home directory for a user account is where the user is placed immediately after logging in to the File Server. Each user must have a home directory assigned to it, although it can be specified at the group level if the user is a member of a group. Home directories must be specified using a full path including the drive letter or UNC share name. If the home directory is not found, Serv-U can be configured to create it.

When specifying the home directory, the `%USER%` macro can be used to insert the login ID in to the path. This is used mostly to configure a default home directory at the group level or within the new user template to ensure that all new users have a unique home directory. When combined with a Directory Access Rule for `%HOME%`, a new user can be configured with a unique home directory and the proper access rights to that location with a minimal amount of effort.

The `%DOMAIN_HOME%` macro can also be used to identify the user's home directory. For example, to place a user's home directory into a common location use `%DOMAIN_HOME%\%USER%`.

The home directory can be specified as "\" (root) in order to grant system-level access to a user, allowing them the ability to access all system drives. In order for this to work properly, the user must not be locked in their home directory.

SSH Public Key Path

The SSH public key can be used to authenticate a user when logging into the the Serv-U File Server. The public key path should point to the key file in a secured directory on the server. This path can include the following macros:

%HOME% - The Home Directory of the user account
%USER% - The Login ID, used if the public key will have the Login ID as part of the file name
%DOMAIN_HOME% - The Home Directory the Domain, set in **Domain Details > Settings**, used if the keys will be in a central folder relative to the domain Home Directory

Examples:

```
%HOME%\SSHpublic.pub
```

```
%HOME%\%USER%.pub
%DOMAIN_HOME%\SSHKeys\%USER%.pub
```

For information about creating an SSH key pair, see "SFTP (Secure File Transfer over SSH2) for Users and Groups".

Account Type

By default, all accounts are permanent and exist on the File Server until they are manually deleted or disabled. An account can be configured to be automatically disabled or even deleted on a specified date by configuring the Account Type. After selecting the appropriate type, the **Account Expiration Date** control appears. Click on the calendar or expiration date to select when the account should be disabled or deleted.

Default Web Client

If your Serv-U license enables the use of FTP Voyager JV, then users connecting to the File Server through HTTP can choose which client they want to use after logging in. Instead of asking users which client they want to use, a default client can also be specified. If this option is changed, it overrides the option specified at the server or domain level. It can also be inherited by a user through group membership. Use the **Inherit default value** option to reset it to the appropriate default value.

Email Address

Serv-U events can use the **Email Address** field when sending email notifications to groups, and password recovery using the Web Client requires an email address to send a recovered password to a user. Type an email address here to allow email notifications or password recovery for the user account.

Lock user in home directory

A user that is locked in their home directory may not access paths above their home directory. In addition, the actual physical location of their home directory is masked as Serv-U always reports it as "/" (root). The value of this attribute can be inherited through group membership.

Enable account

Deselect this option to disable the current account. Disabled accounts remain on the File Server but cannot be used to log in. To re-enable the account, select the **Enable account** option again.

Always allow login

Enabling this option means that the user account is always permitted to log in, regardless of restrictions placed upon the File Server such as maximum number of sessions. It is useful as a fail-safe in order to ensure that critical system administrator accounts can always remotely access the File Server under all conditions. As with any option that allows bypassing access rules, care should be taken in granting this ability. The value of this attribute can be inherited through group membership.

Note: Enabling the Always Allow Login option does not override IP access rules. If both options are defined, the IP access rules prevail.

Description

The description allows for the entry of additional notes that are only visible by administrators.

Availability

This feature limits when users can connect to this server. Limitations can be placed on the time of day as well as the day of the week. When logging in outside the specified available times users are presented a message that the user account is currently unavailable.

Welcome Message

The welcome message is a message that is traditionally sent to the FTP client during a successful user login. Serv-U extends this ability to HTTP so that users accessing the File Server through the Web Client or FTP Voyager JV also receive the welcome message. This feature is not available to users logging in via SFTP over SSH2 because SSH2 does not define a method for sending general text information to the user.

The welcome message can contain general information about the server's status, a special message for the user, disclaimers, or other legal notices. There are two ways to configure a welcome message. The first method involves specifying the path to a file containing the welcome message in the **Message File Path** field. Use **Browse** to select an existing file on the system.

As an alternative, the text of the welcome message can be explicitly provided to Serv-U in the space provided. In order to override an explicit welcome message at the user level, select the **Override inherited group welcome message** option first. The provided text is then sent to the user instead of the contents of the file specified in the **Message File Path** field.

These values can be inherited by the user through group membership.

System variables are also available which can be used in the welcome message. For a comprehensive list of the available system variables, see "System Variables".

Directory Access Rules

Directory Access Rules

Directory Access rules define the areas of the system that are accessible to user accounts. While traditionally restricted to the user and group levels, Serv-U extends the usage of Directory Access rules to both the domain and server levels through the creation of global Directory Access rules. Directory Access rules specified at the server level are inherited by all users of the File Server. When specified at the domain level, they are only inherited by users belonging to that domain. The traditional rules of inheritance apply where rules specified at a lower level (for example, the user level), override conflicting or duplicates rules specified at a higher level (for example, the server level).

When setting the Directory Access path, the `&#37;USER&#37;`, `&#37;HOME&#37;`, `&#37;USER_FULL_NAME&#37;`, and `&#37;DOMAIN_HOME&#37;` variables are available to simplify the process. For example, use `%HOME%/ftproot/` to create a Directory Access rule that specifies the `ftproot` folder in the user's home directory. Directory access rules specified in this manner are "portable" in the event that the actual home directory changes while maintaining the same subdirectory structure. This leads to less maintenance for the File Server administrator. If the `%USER%` variable is specified in the path, it is replaced with the user's login ID. This variable is useful in specifying a group's home directory to ensure that users inherit a logical and unique home directory. The `&#37;USER_FULL_NAME&#37;` variable can be used to insert the Full Name value into the path (the user must have a "Full Name" specified for this to function). For example, the user "Tom Smith" could use `D:\ftproot\&#37;USER_FULL_NAME&#37;` for `D:\ftproot\Tom Smith`. Finally, the `%DOMAIN_HOME%` macro can also be used to identify the user's home directory. For example, to place a user and their home directory into a common directory use `%DOMAIN_HOME%\%USER%`.

Directory Access rules are applied in the order they are listed. The first rule Serv-U encounters in the list that matches the path of a client's request is the one that is applied for that rule. In other words, if a rule exists that denies access to a particular subdirectory but is listed *below* the rule that grants access to the parent directory, then a user still has access to the subdirectory in question. The arrows on the right side of the Directory Access list are used to rearrange the order in which the rules are applied.

A listing and description of each available directory access permission follows.

File Permissions

Read

Allows users to read (that is, download) files. This permission does not allow users to list the contents of a directory, which is granted by the **List** permission.

Write

Allows users to write (that is, upload) files. This permission does not allow users to modify existing files, which is granted by the **Append** permission.

Append

Allows users to append data to existing files. This permission is normally used to grant users the ability to resume transferring to partially uploaded files.

Rename

Allows users to rename existing files.

Delete

Allows users to delete files.

Execute

Allows users to remotely execute files. Execute access is meant for remotely starting programs and usually applies to specific files. This is a very powerful permission and great care should be used in granting it to users. A user with **Write** and **Execute** permissions can essentially install any program of their choosing on your system.

Directory Permissions

List

Allows users to list the files and subdirectories contained in the directory. Also allows users to list this folder when listing the contents of a parent directory. (See KB #2079 for more information about "blind downloads" and "blind uploads".)

Create

Allows users to create new directories within the directory.

Rename

Allows users to rename existing directories within the directory.

Remove

Allows users to delete existing directories within the directory. **Note:** If the directory contains files, the user also needs to have the **Delete** files permission in order to remove the directory.

Subdirectory Permissions

Inherit

Allows all subdirectories to inherit the same permissions as the parent directory. The **Inherit** permission is appropriate for most circumstances, but if access must be restricted to subfolders (as is the case when implementing Mandatory Access Control), deselect **Inherit** and grant permissions specifically by folder.

Advanced: Access as Windows User (Windows Only)

For a variety of reasons, files and folders may be kept on external servers in order to centralize file storage or provide additional layers of security. In this environment, files can be accessed by the UNC path (`\\servername\folder\`) instead of the traditional `C:\ftproot\folder` path. However, accessing folders stored across the network poses an additional challenge, because Windows services are run under the Local System account by default, which has no access to network resources.

To mitigate this problem for all of Serv-U, it is possible to configure the Serv-U File Server service to run under a network account. The alternative, preferred when many servers exist, or if the Serv-U File Server service needs to run under Local System for security reasons is to configure a Directory Access rule to use a specific Windows User for file access. By clicking the **Advanced** button it is possible to specify a specific Windows user for each individual Directory Access rule. Just like in Windows Authentication, directory access is subject to NTFS permissions, though in this case also to the configured permissions in Serv-U.

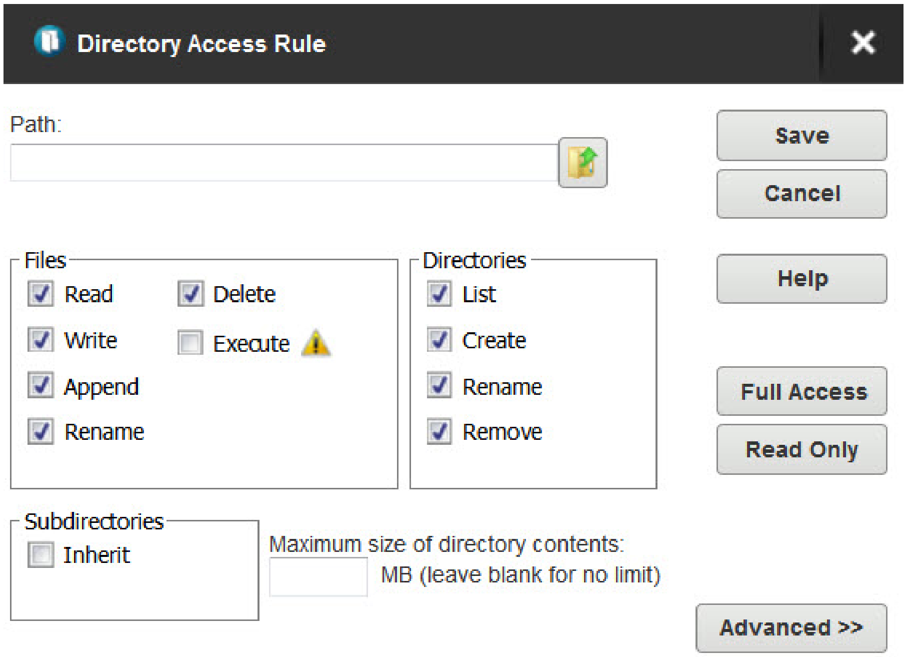
Quota Permissions

Maximum size of directory contents

Setting the maximum size actively restricts the size of the directory contents to the specified value. Any attempted file transfers that cause the directory contents to exceed this value are rejected. This feature serves as an alternative to the traditional quota feature that relies upon tracking all file transfers (uploads and deletions) to calculate directory sizes and is not able to consider changes made to the directory contents outside of a user's File Server activity.

Mandatory Access Control

Serv-U enables the use of Mandatory Access control in cases where users need to be granted access to the same home directory but should not necessarily be able to access the subdirectories below it. To implement Mandatory Access Control at a directory level, disable the **Inherit** permission as shown below (assume the rule applies to `D:\ftproot\`):



Path:

Files
☑ Read
☑ Write
☑ Append
☑ Rename
☑ Delete
☐ Execute

Directories
☑ List
☑ Create
☑ Rename
☑ Remove

Subdirectories
☐ Inherit

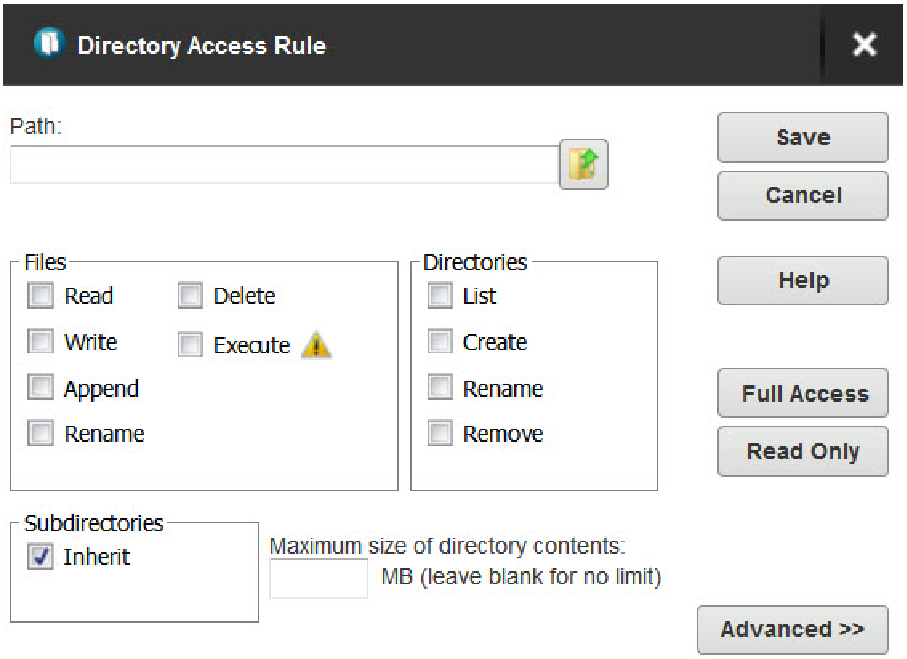
Maximum size of directory contents:
MB (leave blank for no limit)

Now, the user has access to the `ftproot` folder but to no folders below it.

Permissions must individually be granted to subfolders that the user needs access to, providing the security of Mandatory Access Control in the Serv-U File Server.

Restricting File Types

If users are using storage space on the Serv-U File Server to store non-work-related files such as MP3 music files, this can be prevented by configuring a Directory Access rule placed **above** the main Directory Access Rule (use the arrows on the right to reorder rules) to prevent MP3 files from being transferred as shown below. In the text entry for the rule, type `*.mp3` and use the permissions shown below:



Path:

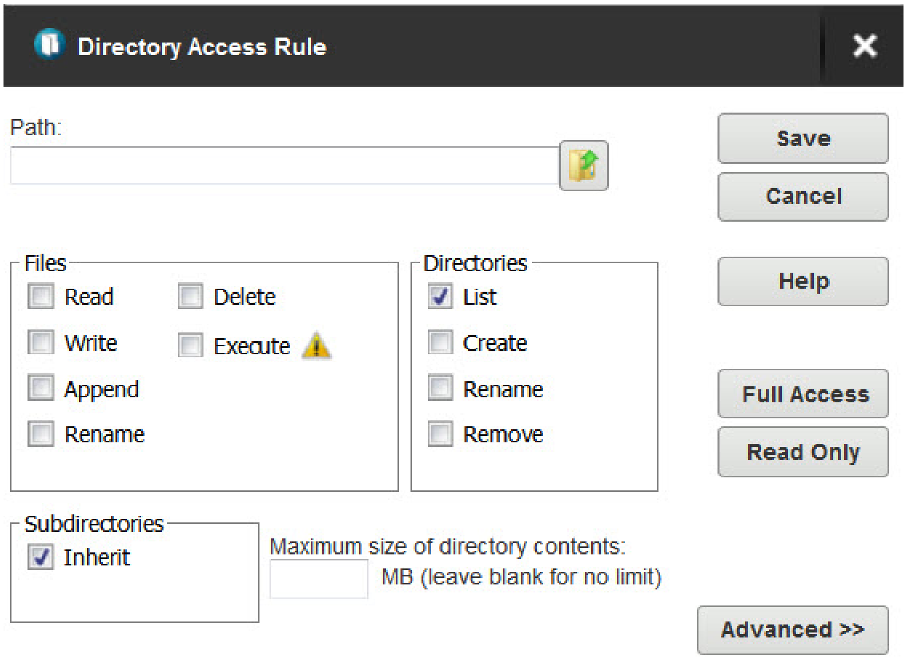
Files
☐ Read
☐ Delete
☐ Write
☐ Execute
☐ Append
☐ Rename

Directories
☐ List
☐ Create
☐ Rename
☐ Remove

Subdirectories
☑ Inherit

Maximum size of directory contents:
MB (leave blank for no limit)

The rule denies permission to any transfer of files with the `.mp3` extension and can be modified to reflect any file extension. Similarly, if accounting employees only need to transfer files with the `.mdb` extension, configure a pair of rules that grants permissions for `.mdb` files but denies access to all other files, as shown below. In the first rule enter the path that should be the user's home directory or directory they need access to, and in the second rule enter the extension of the file that should be accessed (such as `*.mdb`):



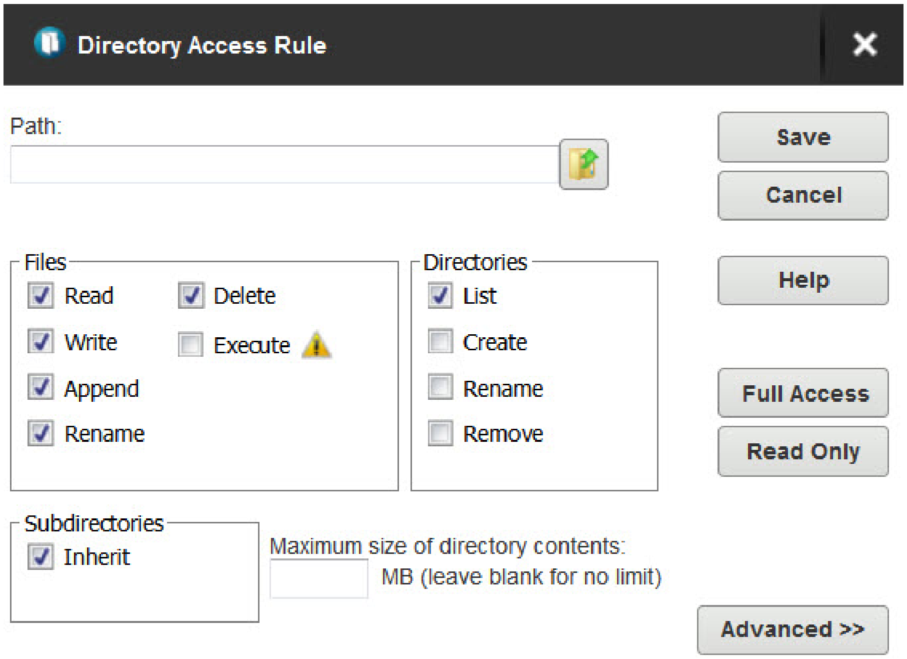
Path:

Files
☐ Read
☐ Write
☐ Append
☐ Rename
☐ Delete
☐ Execute

Directories
☑ List
☐ Create
☐ Rename
☐ Remove

Subdirectories
☑ Inherit

Maximum size of directory contents:
MB (leave blank for no limit)



Path:

Files
☑ Read
☑ Write
☑ Append
☑ Rename
☑ Delete
☐ Execute

Directories
☑ List
☐ Create
☐ Rename
☐ Remove

Subdirectories
☑ Inherit

Maximum size of directory contents:
MB (leave blank for no limit)

These rules only allow users to access `.mdb` files within the directories specified, and can be adapted to any file extension or set of file extensions.

Virtual Paths

Virtual Paths allow users to gain access to files and folders outside of their own home directory. A Virtual Path only defines a method of mapping an existing directory to another location on the system to make it visible within a user's accessible directory structure. In order to actually have access to the mapped location, the user must still have a Directory Access rule specified for the physical path of a Virtual Path.

Like Directory Access Rules, Virtual Paths can be configured at the server, domain, group, and user levels. Virtual Paths created at the server level are available for use by all users of the File Server. When created at the domain level, they are only accessible by users belonging to that domain. Serv-U's granular file access controls even allow for Virtual Paths created specifically for individual users or groups.

Physical Path

The physical path is the actual location on the system, or network, that is to be placed in a virtual location accessible by a user. If the physical path is located on the same computer, a full path should be used, such as `D:\inetpub\ftp\public`. A UNC path can also be used, such as `\\Server\share\public`. In order for a Virtual Path to be visible to a user, they must have a Directory Access rule specified for the physical path.

Virtual Path

The virtual path is the location that the physical path should appear in for the user. The `%HOME%` macro is commonly used in the virtual path to place the specified physical path in the home directory of the user. When specifying the virtual path, the last specified directory is used as the name displayed in directory listings to the user. For example, a virtual path of `%HOME%/public` places the specified physical path in a folder named `public` within the user's home directory. A full path without any macros can also be used.

Include in "Maximum Directory Size" calculations

When selected, the Virtual Path is included in Maximum Directory Size calculations. When deselected, the Virtual Path is not included in the Maximum Directory Size calculations. Maximum Directory Size limits the size of directories affecting how much data can be uploaded.

Case File - Using Virtual Paths

A group of web developers have been granted access to the directory `D:\ftproot\examplesite.com\` for web development purposes. The developers also need access to an image repository located at `D:\corpimages\`. To avoid granting the group access to the root D drive, a Virtual Path must be configured so that the image repository *appears* to be contained within their home directory. Within the web developer's group, add a Virtual Path to bring the directory to the users by specifying `D:\corpimages\` as the Physical Path and `D:\ftproot\examplesite.com\corpimages` as the Virtual Path. Be sure to add a group level Directory Access rule for `D:\corpimages\` as well. The developers now have access to the image repository without compromising security or relocating shared resources.

Case File - Creating Relative Virtual Paths

Continuing with the previous example, if the web developer's group home directory is relocated to another drive, not only does the home directory have to be updated, but the Virtual Path also needs to be updated to reflect this change. This can be avoided by using the `%HOME%` macro to create a relative Virtual Path location that eliminates the need to update the path if the home directory changes. Instead of using `D:\ftproot\examplesite.com\corpimages` as the Virtual Path, use `%HOME%\corpimages`. This tells Serv-U to place the `corpimages` Virtual Path within the group's home directory - whatever that may be. If the home directory changes at a later date, the Virtual Path still appears there.

Configuring User and Group Logs

The Serv-U File Server allows for a great deal of customization in logging user and group events and activity. To enable a logging option, select the appropriate option in the **Log Message Options** grouping. When an option is selected, the appropriate logging information is saved to the specified log file if the **Enable logging to file** option is selected. The log can be configured to show as much or as little information as you want. After configuring the logging options you want, click **Save** to save the changes.

Logging to File Settings

Log file path

The log file must be given a name before information can be saved to a file. Click **Browse** to select an existing file or directory location for the log file. The log file path supports certain wildcard characters as outlined below. Wildcard characters referencing the date apply to the day that the log file is created. When combined with the **Automatically rotate log file** option, wildcards provide an automatic way to archive activity for audits, such as those required by HIPAA. The available wildcard characters are the following:

- %H - The hour of the day (24-hour clock)
- %D - The current day of the month
- %M - The name of the current month
- %N - The numeric value of the current month (1-12)
- %Y - The 4-digit value of the current year (for example, 2014)
- %X - The 2-digit value of the current year (for example, 14 for 2014)
- %S - The name of the domain whose activity is being logged
- %G - The name of the group whose activity is being logged
- %L - The name of the login ID whose activity is being logged
- %U - The full name of the user whose activity is being logged

Enable logging to file

Select this option to enable Serv-U to begin saving log information to the file specified in the **Log file path**. If this option is not selected, Serv-U does not log any information to the file, regardless of the individual options selected in the **Log Message Options** grouping.

Automatically rotate log file

To ensure that log files remain a manageable size and can be easily referenced during auditing, Serv-U supports the ability to automatically rotate the log file on a regular basis. By specifying a **Log file path** containing wildcards referencing the current date, Serv-U can rotate the log file and create a unique file name every hour, day, week, month, or year.

Purge Old Log Files

Serv-U supports the ability to automatically purge old log files by setting a maximum number of files to keep and/or a maximum size limit in megabytes. Setting these options to `0` means the setting is unlimited and the limit is not applied.

Warning: Log files are purged based only on the current log file path name, and are purged approximately every 10 minutes. Log file variables are replaced with Windows wildcard values used to search for matching files. For example:

`C:\Logs\%Y:%N:%D %S Log.txt` is searched for `C:\Logs\????:??:?? * Log.txt`

`C:\Logs\%Y:%M:%D %S Log.txt` is searched for `C:\Logs\????:*:?? * Log.txt`

`C:\Logs\%S\%Y:%M:%D Log.txt` is searched for `C:\Logs\--DomainName--\????:*:?? Log.txt`

`C:\Logs\%G\%Y:%M:%D Log.txt` is searched for `C:\Logs\--GroupName--\????:*:?? Log.txt`

`C:\Logs\%L\%Y:%M:%D Log.txt` is searched for `C:\Logs\--LoginID--\????:*:?? Log.txt`

`C:\Logs\%U\%Y:%M:%D Log.txt` is searched for `C:\Logs\--UserFullName--\????:*:?? Log.txt`

Log variables are wildcarded in the following way:

%H --> ??
%D --> ??

%N --> ??
%M --> *
%Y --> ????
%X --> ??
%S --> *
%G --> *
%L --> *
%U --> *

Anything matching the wildcarded path name can be purged. Use caution. It is best practice to place log files into a single directory to avoid unexpected file deletion.

Do Not Log IPs

Serv-U supports the ability to specify IP addresses that are exempt from logging. Activity from these IP addresses is not logged. This is useful to exempt IP addresses for administrators that may otherwise generate a lot of logging information that can obfuscate domain activity from regular users. It can also be used to save on log space and reduce overhead. Click **Do Not Log IPs**, and then add IP addresses as appropriate.

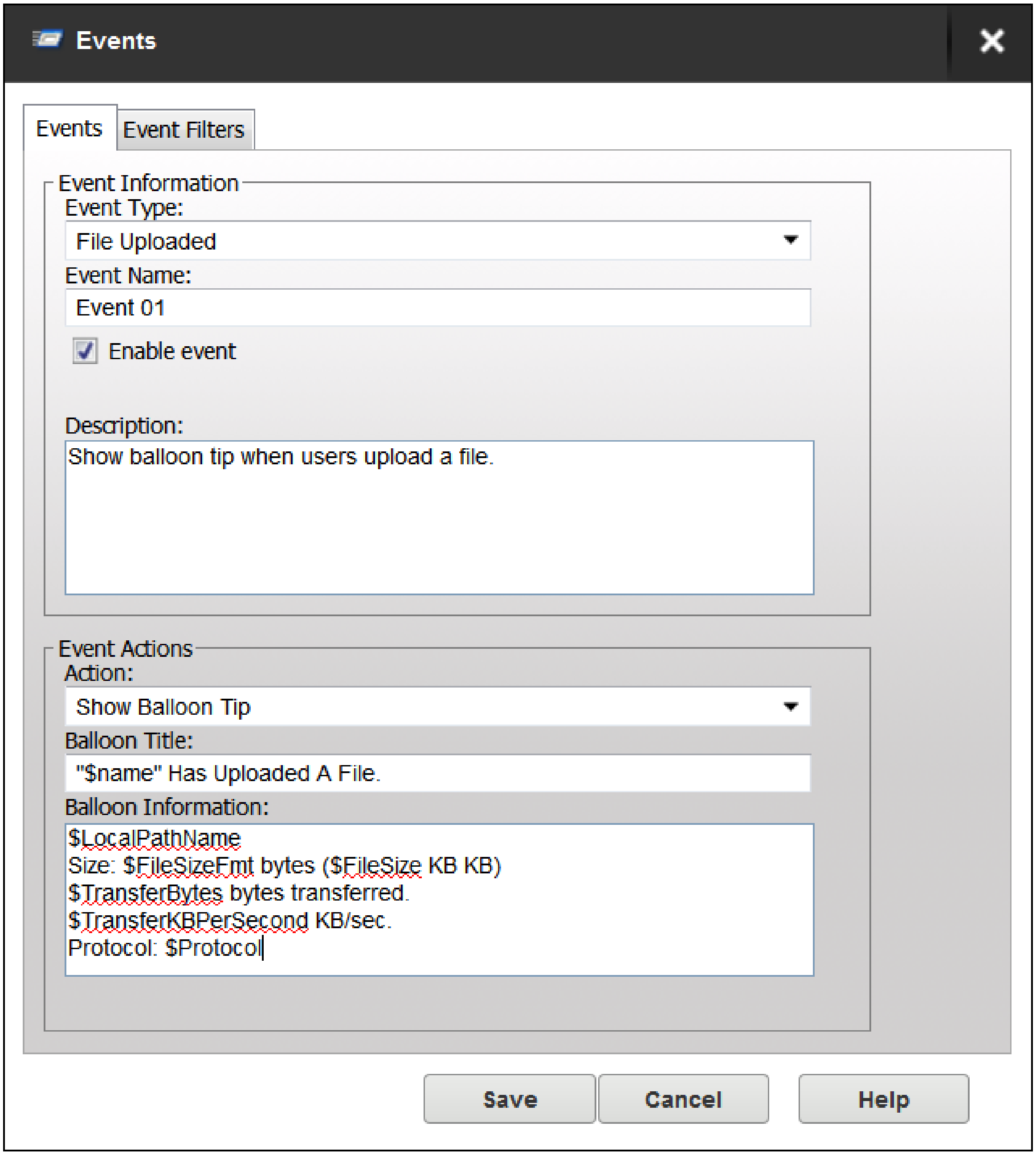
Group Memberships

A user can be a member of any number of groups. Groups provide a convenient way of applying a base set of user attributes and settings to multiple users. For more information about configuring groups, see "About Groups".

Because a user can be a member of multiple groups, the order in which group memberships are presented is important. The first group membership for a user encountered by Serv-U for a user that provides a value for an attribute is the value that is used. Use the arrows on the right side of the group membership list to arrange the order of group memberships as desired.

Use the left and right arrow buttons to add additional group memberships to the user, or remove the user from the selected groups, respectively.

Serv-U Events



Event Information

Event Type: File Uploaded

Event Name: Event 01

☑ Enable event

Description: Show balloon tip when users upload a file.

Event Actions

Action: Show Balloon Tip

Balloon Title: "$name" Has Uploaded A File.

Balloon Information:

```
$LocalPathName
Size: $FileSizeFmt bytes ($FileSize KB KB)
$TransferBytes bytes transferred.
$TransferKBPerSecond KB/sec.
Protocol: $Protocol
```

Serv-U enables the use of event handling which can perform various actions triggered by a list of selected events. The following list contains the actions available to administrators:

Server Events

- Server Start - Triggered by Serv-U starting up, whether by starting the Serv-U service or starting Serv-U as an application.
- Server Stop - Triggered by Serv-U shutting down, whether from service or application-level status. This event will only trigger for graceful stops.

Server and Domain Events

- Domain Start - Triggered by a Serv-U Domain starting, via the **Enable Domain** setting in the **Domain Details > Settings** menu or as part of normal server startup.
- Domain Stop - Triggered by a Serv-U Domain stopping, via the **Enable Domain** setting in the **Domain Details > Settings** menu or as part of normal server startup.
- Session Connection - Triggered by a new TCP session connection.
- Session Disconnect - Triggered by a TCP session disconnection.
- Session Connection Failure - Triggered by a failed session connection attempt.
- Log File Deleted - Triggered by the automatic deletion of a log file, according to logging settings.
- Log File Rotated - Triggered by the automatic rotation of a log file, according to logging settings.
- Listener Success - Triggered by a successful listener connection.
- Listener Stop - Triggered by a stopped listener connection.
- Listener Failure - Triggered by a failed listener connection.
- Gateway Listener Success - Triggered by a successful Gateway listener connection.
- Gateway Listener Stop - Triggered by a stopped Gateway listener connection.

- Gateway Listener Failure - Triggered by a failed Gateway listener connection.
- Permanent Listener Success - Triggered by a successful permanent listener connection.
- Permanent Listener Failure - Triggered by a failed permanent listener connection.
- Permanent Listener Stop - Triggered by a stopped permanent listener connection.
- Permanent Gateway Listener Success - Triggered by a successful permanent Gateway listener connection.
- Permanent Gateway Listener Stop - Triggered by a stopped permanent Gateway listener connection.
- Permanent Gateway Listener Failure - Triggered by a failed permanent Gateway listener connection.
- File Management Rule Success - Triggered when a file management rule is applied, and no errors are encountered.
- File Management Rule Failure - Triggered when a file management rule is applied, and at least one error is encountered.

Server, Domain, User and Group Events

- User Login - Triggered by the login of a user account.
- User Logout - Triggered by the logout of a user account.
- User Login Failure - Triggered by a failed login. A failed login is any connection attempt to Serv-U that fails, whether due to invalid credentials, or a session disconnect before authentication, either due to an incorrect user name, incorrect password, incorrect SSH key pair (for SFTP Public Key Authentication), or any or all of the above.
- User Password Change - Triggered by the change of a password for a user account, either by an administrator or by the user (if permitted).

- User Password Change Failure - Triggered by a failed password change attempt.
- User Enabled - Triggered by the enabling of a user account that was previously disabled.
- User Disabled - Triggered by the disabling of a user account that was previously enabled.
- User Deleted - Triggered by the deletion of a user account by a remote administrator, in an ODBC database, or in the local Management Console.
- User Added - Triggered by the creation of a user account by a remote administrator, in an ODBC database, or in the local Management Console.
- Password Recovery Sent - Triggered by a successful password recovery by an end user or by an administrator.
- Password Recovery Failed - Triggered by a failed password recovery attempt, either due to lack of email address in the user account or lack of permissions.
- Password Stale - Triggered by a stale password, as configured in **Limits & Settings**, that is going to expire.
- User Auto Disable - Triggered by the automatic disabling of a user account, as configured by a user's **Automatically Disable** date.
- User Auto Deleted - Triggered by the automatic deletion of a user account, as configured by a user's **Automatically Delete** date.
- User Pre-disable - Triggered by the upcoming disabling of a user account, as configured in the user's **Automatically Disable** date and the "Days before automatically disabling account to trigger the pre-disable event" limit.
- User Pre-delete - Triggered by the upcoming deletion of a user account, as configured in the user's **Automatically Delete** date and the **Days before automatically deleting account to trigger the pre-delete** event limit.
- User Email Set - Triggered by a user or administrator setting the email address for a user account.

- User Email Set Failure - Triggered by a failed attempt by a user or administrator to set the email address for a user account.
- IP Blocked - Triggered by a failed login attempt due to an IP Access rule.
- IP Blocked Time - Triggered by a failed login attempt due to an IP Access rule that was automatically added by brute force settings, configured in **Domain Limits & Settings** or **Server Limits & Settings**.
- Too Many Sessions - Triggered by more sessions logging on to the server than are permitted, per the **Limits & Settings** for the user account, group, domain, or server.
- Too Many Session On IP - Triggered by more sessions logging on to the server from a specific IP address than are permitted, per the **Limits & Settings** for the user account, group, domain, or server.
- IP Auto Added To Access Rules - Triggered by the automatic addition of an IP Access rule due to a user triggering the "brute force" settings.
- Session Idle Timeout - Triggered by an idle session timeout.
- Session Timeout - Triggered by a session timeout.
- File Uploaded - Triggered by a file uploaded to Serv-U. This event triggers for partial uploads if the upload session terminated with a successful message and no data corruption.
- File Upload Failed - Triggered by a failed file upload to Serv-U.
- File Download - Triggered by a file downloaded from Serv-U.
- File Download Failed - Triggered by a failed file download from Serv-U.
- File Deleted - Triggered by the deletion of a file on the Serv-U server by a user.
- File Moved - Triggered by the moving of a file on the Serv-U server by a user.
- Directory Created - Triggered by the creation of a directory.
- Directory Deleted - Triggered by the deletion of a directory.

- Directory Changed - Triggered by changing the current working directory.
- Directory Moved - Triggered by moving a directory to a new location.
- Over Quota - Triggered by going over disk quota space. The current quota space is shown in the user account, in the **Limits & Settings** menu.
- Over Disk Space - Triggered by exceeding the Max Dir Size configured for a Directory Access rule. The current disk space is shown with the `AVBL FTP` command, or using the **Directory Properties** option in the HTTP/HTTPS Web Client and FTP Voyager JV.

Creating Common Events

Serv-U allows administrators to automatically create a list of the most common events. You can choose to create these common events using email and/or balloon tip actions. Click **Create Common Event** located in the Events tab. Select either the **Send Email** or **Show balloon tip** option for the action you want to be performed on the common events. If you choose to Send Email you must also enter an **To:** address where the events are to be sent.

Note: The **Write to Windows Event Log**, and **Write to Microsoft Message Queue (MSMQ)** options are available for Windows only.

Event Actions

Administrators can select from the following actions that will be executed when an event is triggered:

- Send Email
- Show Balloon Tip*
- Execute Command*
- Write to Windows Event Log (Windows only)*
- Write to Microsoft Message Queue (MSMQ) (Windows only)*

* - Events involving anything other than email may only be configured by Serv-U server administrators.

Email Actions

Email actions can be configured to send emails to multiple recipients and to Serv-U Groups when an event is triggered. To add an email address, enter it in the **To** or **Bcc** fields. To send emails to a Serv-U Group, use the **Group** icon to add or remove Serv-U Groups from the distribution list. Email addresses must be separated by commas or semicolons. Email actions contain a **To**, **Subject** and **Message** parameter. Special variables can be used to send specific data pertaining to the event. For more information about the variables, see "System Variables".

To use email actions, you must first configure SMTP in Serv-U. For information, see "Serv-U SMTP Configuration".

Balloon Tip Actions

Balloon tip actions can be configured to show a balloon tip in the system tray when an event is triggered. Balloon tip actions contain a **Balloon Title** and a **Balloon Message** parameter. Special variables can be used to send specific data pertaining to the event. For more information about the variables, see "System Variables".

Execute Command Actions

Execute command actions can be configured to execute a command on a file when an event is triggered. Execute command actions contain an **Executable Path**, **Command Line Parameters**, and **Completion Wait Time** parameter. For the **Completion Wait Time** parameter, you can enter the number of seconds to wait after starting the executable path. Enter a value of 0 for no waiting.

Note: Any amount of time Serv-U spends waiting delays any processing that Serv-U can perform.

A wait value should only be used to give an external program enough time to perform some operation, such as move a log file before it is deleted (for example, `$LogFilePath` for the Log File Deleted event). Special variables can be used to send specific data pertaining to the event. For more information about the variables, see "System Variables".

Write to Windows Event Log

Writing event messages to a local Windows Event Log allows you to monitor and record Serv-U activity using third-party network management software such as those from HP Openview, SolarWinds, SpiceWorks, and many other vendors. All messages will appear in the Windows Application Log from a source of "Serv-U".

This event has only one field:

- Log Information: The contents of the message to be written into the event log. This is normally either a human-readable message (for example, `filename uploaded by person`) or a machine-readable string (for example, `filename|uploaded|person`), depending on who or what is expected to read these messages. Serv-U system variables are supported in this field. This field may be left blank, but usually should not be left blank.

Write to Microsoft Queue (MSMQ)

Microsoft Message Queuing (MSMQ) is an enterprise technology that lets independent applications communicate quickly and reliably. Serv-U MFT Server can send messages to new or existing MSMQ queues whenever a Serv-U event triggers. Corporations can use this feature to tell enterprise applications that files have arrived, files have been picked up, partners have signed on, or many other activities have just occurred.

These events have the following two fields:

- Message Queue Path: The MSMQ path that addresses the queue. Remote queues can be addressed when a full path (for example, `MessageServer\Serv-U Message Queue`) is specified. Local, public queues on the local machine can be addressed when a full path is not specified (for example, `.\Serv-U Message Queue` or just `Serv-U Message Queue`). If the specified queue does not exist, Serv-U will make its best effort to try to create it. (This normally only works on public queues on the local machine.) Serv-U system variables are supported in this field.

- Message Body: The contents of the message to be sent into the queue. This is normally a text string with a specific format specified by an enterprise application owner or enterprise architect. Serv-U system variables are also supported in this field. This field may be left blank, but usually is not.

Note: Microsoft message queues created in Windows do not grant access to SYSTEM by default, preventing Serv-U from writing events to the queue. In order to correct this, after creating the queue in MSMQ, right-click it, select **Properties**, and then set the permissions so that “SYSTEM” (or the network account under which Serv-U runs) has permission to the queue.

Event Filters

Serv-U Event Filters allow administrators to control to a greater degree when a Serv-U event is triggered. By default, Serv-U Events trigger each time the event occurs. The Event Filter allows events to be triggered only if certain conditions are met. For example, a standard Serv-U Event might trigger an email each time a file is uploaded to the server. However, using an Event Filter, Events can be triggered on a more targeted basis. A File Uploaded event can be configured to only send an email when the file name contains the string `important`, so an email would be sent when the file `Important Tax Forms.pdf` is uploaded but not when random other files are uploaded to the server. Additionally, a File Upload Failed event could be set to run only when the FTP protocol is used, not triggering for failed HTTP or SFTP uploads. This is done by controlling the various variables and values related to the Event and evaluating their results when the event is triggered.

Event Filter Fields

Each Event Filter has the following critical values that must be set:

- Name - This is the name of the filter, used to identify the filter for the event.
- Description (Optional) - This is the description of the event, which may be included for reference.

- Logic - This determines how the filter interacts with other filters for an event. In most cases, AND will be used all filters must be satisfied for the event to trigger. The function of AND is to require that all conditions be met. However, the OR operator can be used if there are multiple possible satisfactory responses (for example, abnormal bandwidth usage of less than 20 KB/s OR greater than 2000 KB/s).
- Filter Comparison - This is the most critical portion of the filter. The Filter Comparison contains the evaluation that must occur for the event to trigger. For example, a filter can be configured so that only the user "admin" triggers the event. In this case, the comparison will be `If $Name = (is equal to) admin`, and the data type will be `string`. For bandwidth, either an "unsigned integer" or "double precision floating point" value would be used.

Event filters also support wildcards when evaluating text strings. The supported wildcards are the following:

- * - The asterisk wildcard matches any text string of any length. For example:
  - An Event Filter that compared the `$FileName` variable to the string `data*` would match files named `data`, `data7`, `data77`, `data.txt`, `data7.txt`, and `data77.txt`.
- ? - The question mark wildcard matches any one character, but only one character. For example:
  - An Event Filter that compared the `$FileName` variable to the string `data?` would match a file named `data7` but not `data`, `data77`, `data.txt`, `data7.txt`, or `data77.txt`.
  - An Event Filter that compared the `$FileName` variable to the string `data?.`* would match files named `data7` and `data7.txt` but not `data`, `data77`, `data.txt`, or `data77.txt`.
  - An Event Filter than compared the `$Name variable` to the string `A????` would match any five-character username starting with `A`.
- [] - The bracket wildcard matches a character against the set of characters inside the brackets. For example:

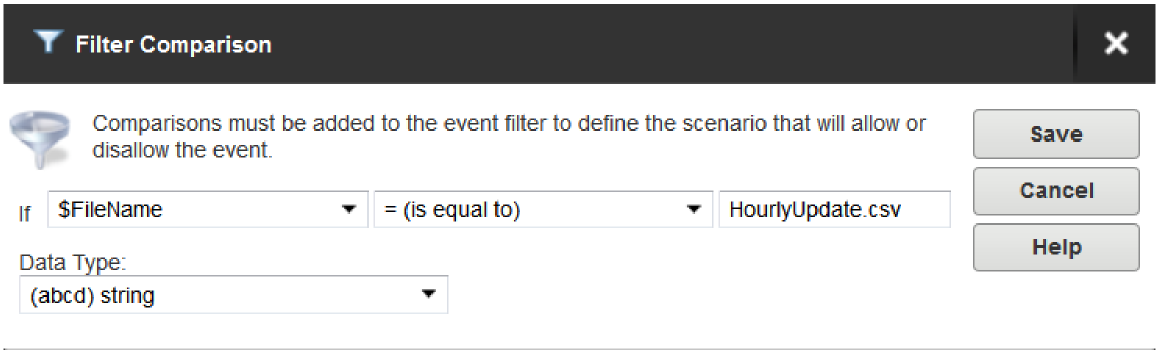
- An Event Filter that compared the `$FileName` variable to the string `data [687].txt` would match files named `data6.txt`, `data7.txt` and `data8.txt` but not `data5.txt`.
- An Event Filter that compared the `$LocalPathName` variable to the string `[CD]:\*` would match any file or folder on the `C:` or `D:` drives.

Multiple wildcards can be used in each filter. For example:

- An Event Filter that compared the `$FileName` variable to the string `[cC]:\*.???` would match any file on the `C:` drive that ended in a three letter file extension.
- An Event Filter that compared the `$FileName` variable to the string `?:\*Red [678]\?????.*` would match a file on any Windows drive, contained in any folder whose name contains `Red6`, `Red7` or `Red8`, and that also has a five character file name followed by a file extension of any length.

Using Event Filters

Event filters are used by comparing fields to expected values in the Event Filter menu. The best example is firing an event only when a certain user triggers the action, or when a certain file is uploaded. For example, an administrator may want to fire an email event when the file `HourlyUpdate.csv` is uploaded to the server, but not other files. To do this, a new event can be created in the **Domain Details > Events** menu. The **Event Type** is File Uploaded, and on the Event Filter tab a new filter must be added. The $FileName variable is used and the value is `HourlyUpdate.csv` as shown:

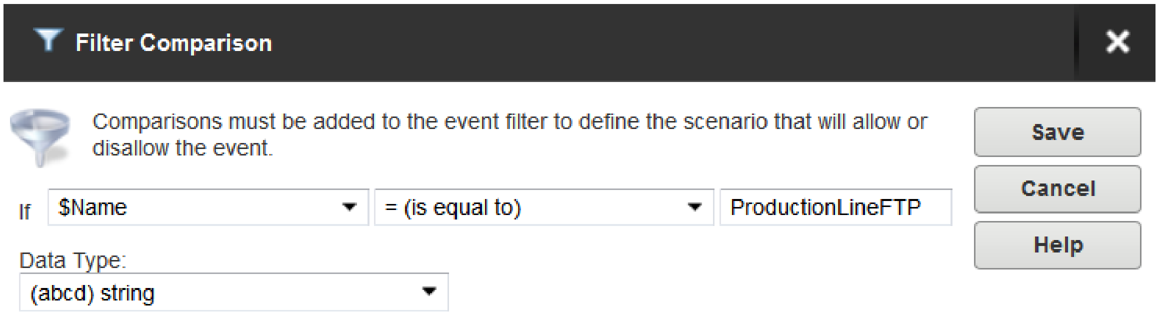


Comparisons must be added to the event filter to define the scenario that will allow or disallow the event.

If $FileName = (is equal to) HourlyUpdate.csv

Data Type: (abcd) string

As another example, it might be necessary to know when a file transfer fails for a specific user account (perhaps one used by an automated process). To perform this task, create a new File Upload Failed event, and then add a new filter. The filter comparison will be `$Name`, and the value to compare would be the username, such as `ProductionLineFTP`:

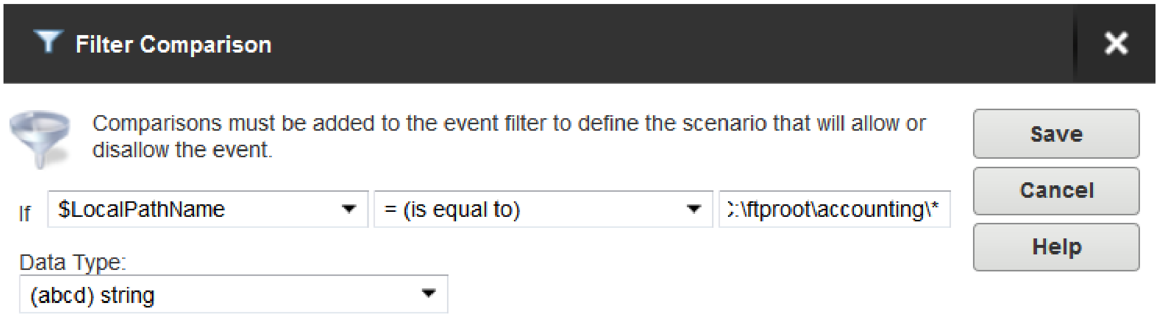


Comparisons must be added to the event filter to define the scenario that will allow or disallow the event.

If $Name = (is equal to) ProductionLineFTP

Data Type: (abcd) string

It is also possible to filter for events based on specific folders, using wildcards. In some cases it may be necessary to trigger events for files uploaded only to a specific folder, such as when an accounting department uploads time-sensitive tax files. To filter based on a folder name, first create a new File Uploaded event in the **Domain Details > Events** menu, and set it to **Send Email**. After specifying the email recipients, subject line, and message content, open the Event Filters tab. Create a new Event Filter, and add the filter comparison `If $LocalPathName = (is equal to) C:\ftproot\accounting\*` with the type of `(abcd) string`. This will cause the event to trigger only for files that are located within `C:\ftproot\accounting\`.



Comparisons must be added to the event filter to define the scenario that will allow or disallow the event.

If $LocalPathName = (is equal to) :\ftproot\accounting\*

Data Type: (abcd) string

Server Details

IP Access Rules

IP Access rules restrict login access to specific IP addresses, ranges of IP addresses, or even a domain name. IP Access rules can be configured at the server, domain, group, and user levels.

IP access rules are applied in the order they are displayed. In this way, specific rules can be placed at the top to allow (or deny) access before a more general rule is applied later on in the list. The arrows on the right side of the list can be used to change the position of an individual rule in the list.

IP Access Masks

IP Access rules use masks to authorize IP addresses and domain names. These masks may contain specific values, ranges and wildcards made up of the following elements.

xxx

An exact match such as `192.168.1.1` (IPv4), `fe80:0:0:0:a450:9a2e:ff9d:a915` (IPv6, long form) or `fe80::a450:9a2e:ff9d:a915` (IPv6, shorthand).

xxx-xxx

A specified range of IP addresses such as `192.168.1.10-19` (IPv4), `fe80:0:0:0:a450:9a2e:ff9d:a915-a9aa` (IPv6, long form), or `fe80::a450:9a2e:ff9d:a915-a9aa` (IPv6, shorthand).

*****

Any valid IP address value such as `192.168.1.*`, which is analogous to `192.168.1.0-255`, or `fe80::a450:9a2e:ff9d:*`, which is analogous to `fe80::a450:9a2e:ff9d:0-ffff`.

?

Any valid character when specifying a reverse DNS name such as `server?.mydomain.com`.

/

The slash separator allows the use of CIDR notation to specify which IP addresses should be allowed or blocked. Common CIDR blocks are `/8 (for 1.*.*.*)`, `/16 (for 1.2.*.*)` and `/24 (for 1.2.3.*)`. CIDR notation also works with IPv6 addresses, such as `2001:db8::/32`.

Caveats

Specific IP addresses listed in Allow rules will not be blocked by anti-hammering. (In other words, they are ‘whitelisted’.) However, addresses matched by wildcard or range will be subject to anti-hammering prevention.

Implicit Deny All

Serv-U assumes that connections from any IP address are valid until you add your first IP access rule. After you add that first IP access rule Serv-U assumes that all connections not explicitly allowed should be denied. This is also known as "an implicit 'Deny All' rule". With this in mind, make sure you add a 'wildcard allow' rule (such as `Allow *.*.*.*`) at the end of your IP Access rule list.

Matching All Addresses

Use a mask of `*.*.*.*` to match any IPv4 address. Use a mask of `*:*` to match any IPv6 address. Remember to add Allow ranges for both IPv4 and IPv6 addresses if you use both IPv4 and IPv6 listeners.

DNS Lookup

If a dynamic DNS service is used, then a domain name can be specified in place of an IP address to allow access to clients that travel and do not have a static IP address. Reverse DNS names are also acceptable. If a domain name or reverse DNS rule is created, Serv-U must perform either a reverse DNS look-up or DNS resolution in order to apply these rules. This can cause a slight delay during login depending on the speed of the system's DNS server.

Rule Use During Connection

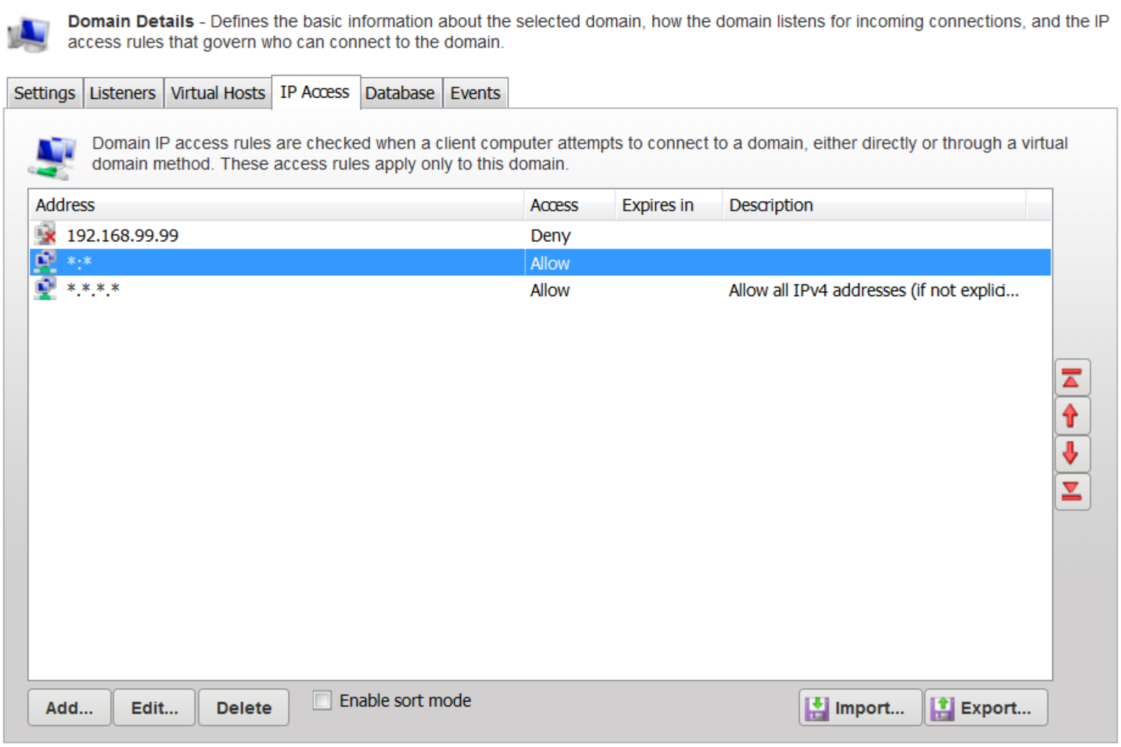
The level at which an IP access rule is specified also defines how far a connection is allowed before being rejected. Server and domain level IP access rules are applied before the Welcome message is sent. Domain level IP access rules are also applied when responding to the HOST command to connect to a virtual domain. Group and user level IP access rules are applied in response to a USER command when the client identifies itself to the server.

Anti-Hammering

Serv-U allows administrators to set up an "anti-hammering policy" that blocks clients who connect and fail to authenticate more than a certain number of times within a certain period of time. These policies can be configured server-wide in **Server Limits and Settings > Server Settings** and domain-wide in **Domain Limits and Settings > Domain Settings**.

IP addresses blocked by anti-hammering rules will appear in your Domain IP Access rules with a value in the **Expires in** column. If you have multiple domains with different listeners, blocked IPs will appear in the domain that contains the listener. (Blocked IP addresses will never appear in the Server IP Access list, even if anti-hammering was set up at the server level.)

The **Expires in** value of the blocked IP will tick down second by second until the entry disappears. You can unblock any blocked IP early by deleting its entry from the list.



Domain Details - Defines the basic information about the selected domain, how the domain listens for incoming connections, and the IP access rules that govern who can connect to the domain.

Domain IP access rules are checked when a client computer attempts to connect to a domain, either directly or through a virtual domain method. These access rules apply only to this domain.

Address	Access	Expires in	Description
192.168.99.99	Deny		
:	Allow		
..*.*	Allow		Allow all IPv4 addresses (if not explici...

☐ Enable sort mode

IP Access List Controls

Enable Sort Mode

This option allows the IP Access list to be sorted numerically rather than in the processing order. Displaying the IP Access list in sort mode will not change the order in which rules are processed. To view rule precedence disable this option. Viewing the IP Access list in numerical order can be a valuable tool when reviewing long lists of access rules to determine if an entry already exists.

Importing/Exporting IP Access Rules

Serv-U IP Access rules can be imported and exported from users, groups, domains, and the server using a standard text-based comma separated values (CSV) file. To export IP Access rules, view the list of rules to export, and then click **Export**, specifying the path and the file name to save the list to. To import IP Access rules, click **Import** and select the file with the rules

to be imported. The CSV file must contain the following fields, headers included:

-IP - The IP address, IP range, CIDR block, or domain name for which the rule will apply

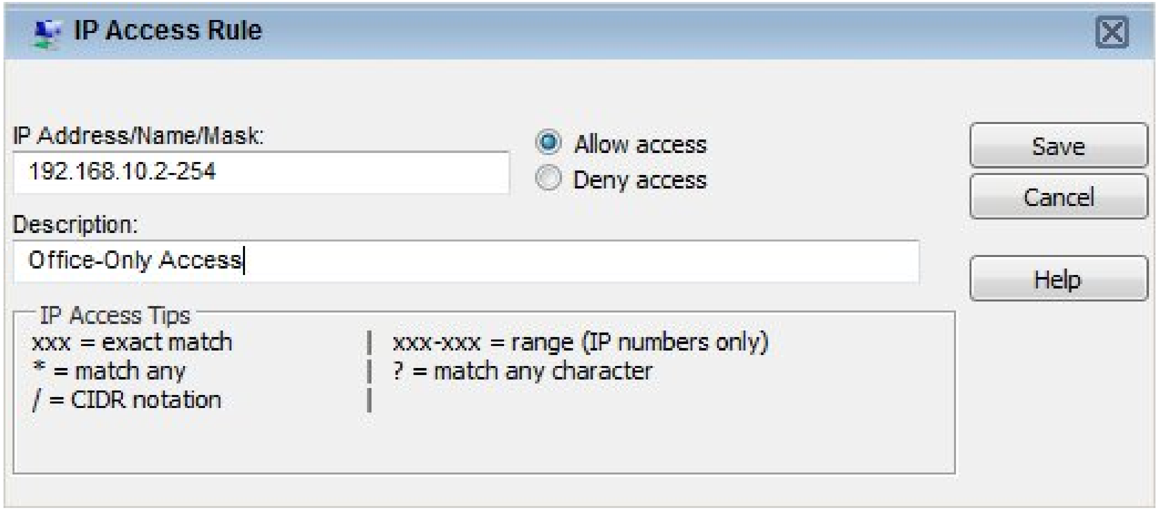
-Allow - Set this value to 0 for Deny, or to 1 for Allow

-Description - A text description of the rule for reference purposes

Examples

Case File - Office-Only Access

A contractor has been hired to work in the office, and only in the office. Office workstations have IP addresses from 192.168.10.2 to 192.168.10.254. The related Serv-U access rule should therefore be `Allow 192.168.10.2-254` (see below), and it should be added to either the contractor's user account or a 'Contractors' group that will contain multiple contractors. (Note that no "Deny" rule is required here because Serv-U provides an implicit 'deny all' at the end of the list.)



IP Address/Name/Mask: 192.168.10.2-254

● Allow access
○ Deny access

Description: Office-Only Access

Case File - Prohibited Machines

Users should normally be able to access Serv-U from anywhere, except from a bank of special internal machines in the IP address range of 192.168.15.100 -

192.168.15.110. The related Serv-U access rules should therefore be `Deny 192.168.15.100-110`, followed by `Allow *.*.*.*`, and these should both be added to either the domain or the server IP Access rules.

Case File - DNS-based Access Control

The only users allowed to access a Serv-U Domain will be connecting from `*.internal.com` or `*.trustedpartner.com`. The related Serv-U access rules should therefore be `Allow *.internal.com` and `Allow *.trustedpartner.com` (in any order) and these should both be added to the domain IP Access rules. (Note that no "Deny" rule is required here because Serv-U provides an implicit 'deny all' at the end of the list.)

Limits and Settings

Serv-U offers advanced options which can be used to customize how it may be used as well as ways to apply limits and custom settings to **Users**, **Groups**, **Domains**, and the **Server** in its entirety. The limits stack intelligently, with user settings overriding group settings, group settings overriding domain settings, and domain settings overriding server settings. In addition, limits can be applied only during certain days of the week or times of the day. It is possible to grant exceptions to administrators and restrict specific users more than others, providing total control over the server. The Limits and Settings in Serv-U are split into the following categories:

- Connection
- Password
- Directory Listing
- Data Transfer
- HTTP
- Email

- File Sharing
- Advanced

To apply a limit, select the appropriate category, click **Add**, select the limit, and then select or enter the value. For example, to disable the **Lock users in home directory** option for a domain, follow these steps:

- Select **Domain > Domain Limits & Settings** from the Serv-U Management Console.
- Select **Directory Listing** from the **Limit Type** list.
- Click **Add**.
- Select **Lock users in home directory** from the **Limit** list.
- Deselect the option.
- Click **Save**.

The limits list displays the current limits applied to the domain. Limits with a light-blue shade to the background are default values. Limits with a white background are values that override the defaults. After completing the above steps, a new **Lock users in home directory** limit appears in the list that displays "No" as the value. Because of inheritance rules, this option applies to all users in the domain unless overridden at the group or user level. For more information about this method of inheritance, see "User Interface Conventions".

Limits can be deleted by selecting them and clicking **Delete**. To edit an overridden value, select the limit, and then click **Edit**. Default rules cannot be edited or deleted. Create a new limit to override a default one.

To create a limit that is restricted to a specific time of day or days of the week, click **Advanced** from the New / Edit Limit dialog. The additional options allow you to Apply limit only at this time of day at which point a start and stop time for the new limit can be entered. To restrict the limit to certain days of the week, deselect the days for which you do not want to apply the limit. When a limit is restricted in this way, default values (or the value of other limit overrides) are applied when the time of day or day of the week restrictions are not met for this limit.

The following is a reference of all available user limits, organized by category.

Connection

Maximum number of sessions per user account

Specifies the maximum number of concurrent sessions that may be opened from a single User account.

Maximum sessions per IP address for user account

Specifies the maximum number of concurrent sessions that a User may open from a single IP address.

Require secure connection before login

Requires that a connection be secure (for example, FTPS, SFTP, or HTTPS), before it is accepted.

Automatic idle connection timeout

Specifies the number of minutes that must pass after the last client data transfer before a session is disconnected for being idle.

Note: Setting the Packet time-out is a requirement for this limit to work. The value of Packet time-out must be less than the value of the Automatic idle connection timeout for the Automatic idle connection timeout to work properly. For information about setting the packet time-out, see "Server Settings".

Automatic session timeout

Specifies the number of minutes a session is allowed to last before being disconnected by the Server.

Block anti-timeout schemes

Blocks the use of commands such as "NOOP", which is commonly used to keep FTP Command Channel connections open during long file transfers or other periods of inactivity where no information is being transferred on the control channel. When these are blocked, Serv-U disconnects the client when the connection has been idle, that is, not transferring data, for a specified period of time.

Block IP address of timed out session

Specifies the number of minutes for which the IP address of a timed out session is blocked.

Allow FTP and FTPS connections

Allows the user to connect using the FTP and FTPS protocols. Deselect **Allow FTP and FTPS connections** to disable the FTP and FTPS protocols.

Allow SFTP connections

Allows the user to connect using the SFTP protocol. Deselect **Allow SFTP connections** to disable the SFTP protocol.

Allow HTTP and HTTPS connections

Allows the user to connect using the HTTP and HTTPS protocols. Deselect **Allow HTTP and HTTPS connections** to disable the HTTP and HTTPS protocols.

Password

Require complex passwords

Specifies that all user account passwords must contain at least one uppercase and one non-alphabetic character to be considered valid.

Minimum password length

Specifies the minimum number of characters required in a user account's password. Specifying 0 characters indicates that there is no minimum requirement.

Automatically expire passwords

Specifies the number of days a password is valid before it must be changed. Specifying 0 days means passwords never expire.

Allow users to change password

Specifies whether or not users are allowed to change their own passwords.

Mask received passwords in logs

Masks the passwords received from clients from being shown in log files. Disabling this allows passwords to be displayed in log files, which can be useful for debugging connection problems or auditing user account security.

SSH authentication type

Specifies how SSH authentication is to occur. Options include: "Password and Public Key" - requires both a password and a public key (when specified) for login; "Password or Public Key" - requires either a password or public key for login; "Public Key Only" - requires that a public key is provided for successful login, a password is not allowed; "Password Only" - requires that a password is provided for successful login, a public key is not allowed.

Allow users to recover password

If enabled, allows users to recover passwords using the Web Client password recovery utility at the login page.

FTP password type

All passwords are stored in an encrypted, irreversible state in Serv-U's configuration files (unless the File Server is configured to not encrypt stored passwords through a password limit). In addition to the **Regular Password** option, two additional types of password storage are available for accounts that use the FTP protocol: **MD4** and **MD5 OTP S/KEY** passwords. This type of password setting allows the user to log in via FTP without sending the password to the File Server as plain text. These options only apply to the FTP protocol. Setting this option does not affect a user's ability to log in through other protocols.

Days before considering password to be stale

The number of days prior to expiration that a password is to be considered "stale". A stale password is a password that is about to expire. An event can be configured to identify when a password is about to expire. This value is the lead-time, in days, before password expiration.

Directory Listing

Hide files marked as hidden from listings

Hides files and folders from directory listings that have the Windows "hidden" system attribute set on them.

Use lowercase for file names and directories

Forces Serv-U to display all file names and directories using lowercase characters, regardless of the actual letter case in use by the file or directory.

Interpret Windows shortcuts as links

Instructs Serv-U to treat all valid .lnk files as the actual destination object. In other words, if a .lnk file points to another file, the destination file is shown in the directory listing instead of the .lnk file itself.

Treat Windows shortcuts as target in links

Instructs Serv-U to treat all valid .lnk (shortcut) files as a UNIX symbolic link.

Allow root ("/") to list drives for unlocked users (Windows Only)

Allows users to change directory to the root ("/") of the system and display all drives on the computer. This option only works when the user is not locked in their home directory.

Hide the compressed state of files and directories

Hides the compressed state of all compressed files and directories being viewed by the user.

Hide the encrypted state of files and directories

Hides the encrypted state of all encrypted files and directories being viewed by the user.

Message file path

Welcome messages are normally displayed once to a user during login to relay important information to users about the file server site. By using a secondary message file, welcome messages can be provided in specific folders to relay additional information. A non-relative path such as `MessageFile.message` can be used as the path. The welcome message will only be displayed when navigating into folders which contain a file matching the specified file name.

Data Transfer

Maximum upload speed per session

Limits the maximum upload bandwidth for each individual session. Setting a limit of 0 KB/s means unlimited bandwidth.

Maximum download speed per session

Limits the maximum download bandwidth for each individual session. Setting a limit of 0 KB/s means unlimited bandwidth.

Maximum upload speed for user accounts

Limits the maximum upload bandwidth shared between all sessions associated with an individual user account. Setting a limit of 0 KB/s means unlimited bandwidth.

Maximum upload file size

Restricts the maximum single file size a user can upload to Serv-U. File size measured in kilobytes.

Maximum download speed for user accounts

Limits the maximum download bandwidth shared between all sessions associated with an individual user account. Setting a limit of 0 KB/s means unlimited bandwidth.

Delete partially uploaded files

Instructs Serv-U to delete incomplete file uploads. If this option is enabled, users are not able to restart interrupted uploads using the REST (Restart) FTP command.

Interpret line feed byte as a new line when in ASCII mode (Windows Only)

When uploading and downloading files using ASCII mode, Serv-U will assume <LF> characters are the same as <CR><LF> end-of-line markers. Most Windows applications expect <CR><LF> to represent a new-line, as does the FTP protocol. However, since the definition of a new-line sequence is not fully defined in Windows, this option allows Serv-U to assume <LF> is the same as <CR><LF>. When uploading in ASCII mode stand-alone <LF> characters are changed to <CR><LF> prior to writing to the file. When downloading in ASCII mode, stand-alone <LF> characters are changed to <CR><LF> prior to sending to the client.

Automatically check directory sizes during upload

Instructs Serv-U to occasionally check the size of directories in which a maximum directory size has been specified. This attribute ensures that Serv-U always has updated directory sizes available instead of having to calculate them at transfer time, which can be a time consuming operation.

HTTP

Default language for Web Client

When the end-user connects with an unsupported language, the HTTP Login Page is displayed in English. The default language can be set to any language. When connecting to Serv-U using a supported localization of Windows, the native language of Windows is used.

Allow HTTP media playback

The Serv-U Web Client supports fully interactive media playback of audio and video files. This function can be disabled as desired during specific business hours or altogether based on business needs.

Allow browsers to remember login information

The HTTP login page supports a "Remember me" option (not enabled by default) that allows user names to be remembered by the login page. This feature can be disabled for security reasons.

Allow users to change themes

The Serv-U Web Client supports visual themes to change the look and feel of the Web Client and HTTP login page. This feature is visual only and has no impact on security or functionality. This option can be disabled for business needs.

Allow users to change languages

The Serv-U Web Client is supported in many languages, but if users should not be able to select their native language this can be disabled.

Allow users to use Web Client Pro

Serv-U Web Client Pro is enabled by default. Administrators may disallow the use of Serv-U Web Client Pro by disabling this limit.

Allow users to use FTP Voyager JV

FTP Voyager JV is enabled by default. Administrators may disallow the use of FTP Voyager JV by disabling this limit.

Maintain file dates and times after uploading (FTP Voyager JV and Web Client Pro only)

When enabled, Serv-U can maintain the last modification date and time of the file when end-users are using FTP Voyager JV or Web Client Pro. When disabled, Serv-U will not set the file's last modification date and time, it will remain the date and time the file was uploaded.

Allow HTTP sessions to change IP address (disabling may cause mobile devices to fail)

The Serv-U Web Client supports the transfer of HTTP sessions if the IP address changes. This option can be disabled but it may cause mobile devices to be disconnected due to frequent IP address changes by these devices.

File Sharing

Require a password for guest access

Specifies whether it is possible to set up a file share where the guest is required to provide a password. When this limit is set to Always or Never, the creator of the file share will not be able to specify this optional setting.

When this limit is set to Optional, the user can individually specify in each file share whether or not the guest must provide a password.

Insert passwords within invitation emails

Specifies whether it is possible to set up a file share where the password for the share is included in the invitation email. When this limit is set to Always or Never, the creator of the file share will not be able to specify this optional setting. When this limit is set to Optional, the **Include the password in the email** option can be selected individually in each file share.

Maximum file size guests can upload (per file)

Specifies the file size constraints imposed upon the guest user. If set to 0, there is no file size constraint. In this case, the creator of the file share request can specify the maximum file size in each file share request without an upper limit.

Allow user-defined guest link expiration

When enabled, users will be able to specify link expiration dates individually on the Request Files and Send Files wizards. When disabled, the file share links will expire after the number of days specified in the **Duration before guest link expires** limit.

Duration before guest link expires

Limits the number of days after which a file share link expires if the Allow user-defined guest link expiration limit is disabled.

Notify user after a file is downloaded

Specifies whether the **Notify me when the file(s) have been downloaded** option can be used on the Send Files wizard. When this limit is set to Always or Never, the creator of the file share will not be able to specify this optional setting. When this limit is set to Optional, the user can individually specify in each file share whether to receive notification of the file download.

Notify user after a file is uploaded

Specifies whether the **Notify me when the file(s) have been uploaded** option can be used on the Request Files wizard. When this limit is set to

Always or Never, the creator of the file share request will not be able to specify this optional setting. When this limit is set to Optional, the user can individually specify in each file share request whether to receive notification of the file upload.

Send the guest access link to the recipients

Specifies whether the **Automatically send the download/upload link to the guest user(s) in email** option can be used on the Send Files and Request Files wizard. When this limit is set to Always or Never, the user will not be able to specify this optional setting. When this limit is set to Optional, the user can individually specify in each file share or file share request whether to send the access link automatically.

Send the guest access link to the sender

Specifies whether the **Send me an email copy with the download/upload link** option can be used on the Send Files and Request Files wizard. When this limit is set to Always or Never, the user will not be able to specify this optional setting. When this limit is set to Optional, the user can individually specify in each file share or file share request whether to receive an email copy with the download/upload link.

Allow file sharing

Specifies whether the user is allowed to use file sharing.

Allow user-defined contact information

When enabled, users will be able to edit their name and email address on the Request Files and Send Files wizards. When disabled, users are not allowed to edit their contact information on the Request Files and Send Files wizards.

Maximum number of files for "Sent" shares

Specifies the maximum number of files users can include in a single file share. If set to 0, the default limit of 20 is used.

Maximum number of files for "Requested" shares

Specifies the maximum number of files users can upload after receiving a file share request. If set to 0, the default limit of 20 is used.

Advanced

Convert URL characters in commands to ASCII

Instructs Serv-U to convert special characters contained in command parameters to plain ASCII text. Certain browsers can encode special characters contained in file names and directories when using the FTP protocol. This attribute allows Serv-U to decode these special characters.

Maximum Supported SFTP Version

Specifies the maximum version of SFTP permitted for SFTP connections. Serv-U supports SFTP versions 3-6.

Allow Rename Overwrite

When enabled (default) Serv-U allows files to be renamed to files where the destination already exists. When disabled users are not allowed to rename a file or directory to a path name that already exists.

Apply server and domain directory access rules before user and group

The order in which Directory Access Rules are listed has significance in determining the resources that are available to a user or group account. By default, Directory Access Rules specified at the group or user level take precedence over ones specified at the domain and server level. However, there are certain instances where you may want the domain and server level rules to take precedence. Setting this value to "Yes" places the group's and user's Directory Access Rules *below* the server and domain. Please also refer to the "Apply group directory access rules first" setting which is outlined on Group Information.

Days before automatically disabling account to trigger the pre-disable event

The number of days prior to automatically disabling the user account that the pre-disable event should be triggered.

Days before automatically deleting account to trigger the pre-delete event

The number of days prior to automatically deleting the user account that the pre-delete event should be triggered.

Owner ID (user name) for created files and directories (Linux Only)

The user name given to set as owner of a created file or directory.

Group ID (group name) for created files and directories (Linux Only)

The group name given to set as owner of a created file or directory.

Reset user stats after restart

When this limit is enabled, the user stats are reset after a server restart.

Transfer Ratio and Quota Management

Transfer Ratios and Quotas are just one of the many ways in which file transfers are managed on the Serv-U File Server. The following sections provide more information about their usage.

Transfer Ratio

Transfer ratios are a convenient way of encouraging file sharing on your File Server. By specifying an appropriate transfer ratio setting, you can grant "credits" to the user for transferring a specified number of bytes or complete files. This is commonly used to grant a user the ability to download 'x' megabytes of data or files for every 'y' megabytes of data or files that they upload.

To enable transfer ratios for the current user account, click **Ratios & Quotas** on the User Information tab of the User Properties window, and then select **Enable transfer ratio**. Select the appropriate type of ratio to impose on the user account. Ratios can be tracked in terms of megabytes or complete files. They can also be tracked per session established or for all sessions established by the user account.

The ratio itself is configured by assigning a numeric value to both the Uploads and Downloads side of the ratio. For example, a 3/1 ratio that is counting files over all sessions means that the user account must upload 3 files in order to have the ability to download 1 file. The current credit for the user account is displayed in the **Credit** field. This value is the current value and can be initialized to a non-zero value to grant the user initial credits.

Quota

Quotas are another way to limit the amount of data that is transferred by a user account. When a **Maximum** quota value is assigned to the user, they are not able to use more disk space than that value. The **Current** field shows how much disk space is currently being used by the user account. When initially configuring a quota, both fields must be filled in. From that point on, Serv-U tracks the file uploads and deletions made by the user and updates the current value as appropriate.

Note: One considerable drawback to using quotas is that in order for the current value to remain accurate, changes must not be made to the contents of the directories that are accessible by the user account outside of Serv-U. Because these changes take place outside of a File Server connection, Serv-U cannot track them and update the current quota value. As an alternative to quotas, consider imposing a maximum size on the contents of a directory when specifying the Directory Access rules for the user account. For more information about this option, see "Directory Access Rules".

Ratio Free Files

Files listed in the ratio free file list are exempt from any imposed transfer ratios. In other words, if a user must upload files in order to earn credits towards downloading a file, a file that matches an entry in this list can always be downloaded by users, even if they have no current credits. This is commonly used to make special files, such as a readme or a directory information file, always accessible to users.

The `*` and `?` wildcard characters can be used when specifying a ratio free file. Using `*` specifies a wildcard of any kind of character and any length. For example, entering `*.txt` makes any file with a `.txt` extension free for download, regardless of the actual filename. A `?` can be used to represent a single character within the filename or directory. Finally, full paths can be specified using standard directory paths such as `C:\ftproot\common\` (in Windows) or `/var/ftpfiles/shared/` (in Linux).

In addition, full or relative paths can be used when making an entry. If a full path is used when specifying a filename, then only that specific file is exempt from transfer ratios. If a relative path is used, such as entering just `readme.txt`, then the provided file is exempt from transfer ratios regardless of the directory it is located in.

Windows Authentication

By enabling Windows authentication, users can log in to Serv-U using their Windows login credentials as provided by the local Windows account database or a specific Windows Domain Server (Active Directory). When logging in using their Windows account, users are placed in the home directory for their Windows account eliminating the need to manually specify a home directory.

To enable Windows authentication, select **Enable Windows authentication**. To authenticate to Active Directory or a Windows Domain Server, enter a specific domain name in this field and ensure your Serv-U computer is a member of that domain. If the system is a member of a Windows Domain, the domain name can be entered in this field to have user logins authorized by the Domain Server. After changing this field, click **Save** to apply the changes.

Use Windows User Group home directory instead of account home directory

By default, Serv-U uses the Windows account's home directory when a client logs in using a Windows User account. Enabling this option causes Serv-U to use the home directory specified in the Windows User Group instead. If no home directory is specified at the group level, then the Windows User account's home directory is still used.

Configure Windows User Group

Windows User accounts are not visible or configurable on an individual basis in Serv-U. To aid in configuring the many advanced options of a local user account, all Windows user accounts are a member of a special Windows User Group. Click **Configure Windows User Group** to configure this group just like a normal group. All settings configured in this Group are inherited by Windows User accounts. This feature can be used to add IP access rules, specify bandwidth limitations, or add additional Directory Access rules.

For more information, see "About Groups".

Windows User Permissions

By default, Windows and Active Directory user accounts do not require any Directory Access rules to be configured because Serv-U automatically applies their NTFS permissions to their login sessions. This way, administrators do not need to configure specific permissions beyond those already defined on the network, saving time and documentation.

Note: In some cases Windows may cache Directory Access rules for a short period of time. If an important NTFS permissions change is made that requires immediate application, restarting the Serv-U service can force Windows to provide the updated permissions to the Serv-U File Server.

LDAP Authentication

By enabling LDAP authentication, users can log in to Serv-U using login credentials as provided by a remote LDAP server, such as Active Directory or OpenLDAP. LDAP users can use a home directory from their LDAP account, eliminating the need to manually specify a home directory.

To enable LDAP authentication, select **Enable LDAP authentication** under **Users > LDAP Authentication**.

LDAP User home folders are normally pulled from the "Home Directory" LDAP attribute specified in your LDAP Server configuration. The service account Serv-U runs as should have full permission to the root folder of all LDAP User folders. For example, if your LDAP User home folders are similar to `\\usernas\homefolders\username` and Serv-U is running as a service on Windows as `servu`, then the Windows `servu` user should have full permissions to `\\usernas\homefolders`.

Use LDAP User Group home directory instead of the account home directory

By default, Serv-U uses the LDAP account's home directory (that is, the value of the "Home Folder" attribute) when an LDAP User logs in. Enabling this option causes Serv-U to use the home directory specified in the Default LDAP User Group instead. If no home directory is specified at the group level, then the LDAP account's home directory is still used. However, if no home directory is defined at the user, group, domain, or system level, and none is available from the LDAP server, the user will not be allowed to sign on.

LDAP Login ID suffix

The **LDAP Login ID suffix** field is used to send fully qualified Login IDs to the LDAP server. A typical value in an Active Directory environment might be `@mydomain.com`. After changing this field, click **Save** to apply the change.

Differences Between Windows Users and LDAP Users

Windows and LDAP Users are similar in many ways but there are a number of important differences that can help you decide which type of user is right for your environment.

Use Windows users if the following conditions apply:

- You only want to access one Windows machine or domain (per Serv-U domain)
- You want each end user to see that user's home folders and enjoy that user's NTFS permissions. Serv-U uses impersonation so that it respects the Windows directory access rules. The Windows directory access rules can

be supplemented with directory access rules defined in Serv-U. For more information about directory access rules, see "Directory Access Rules".

Use LDAP users if the following conditions apply:

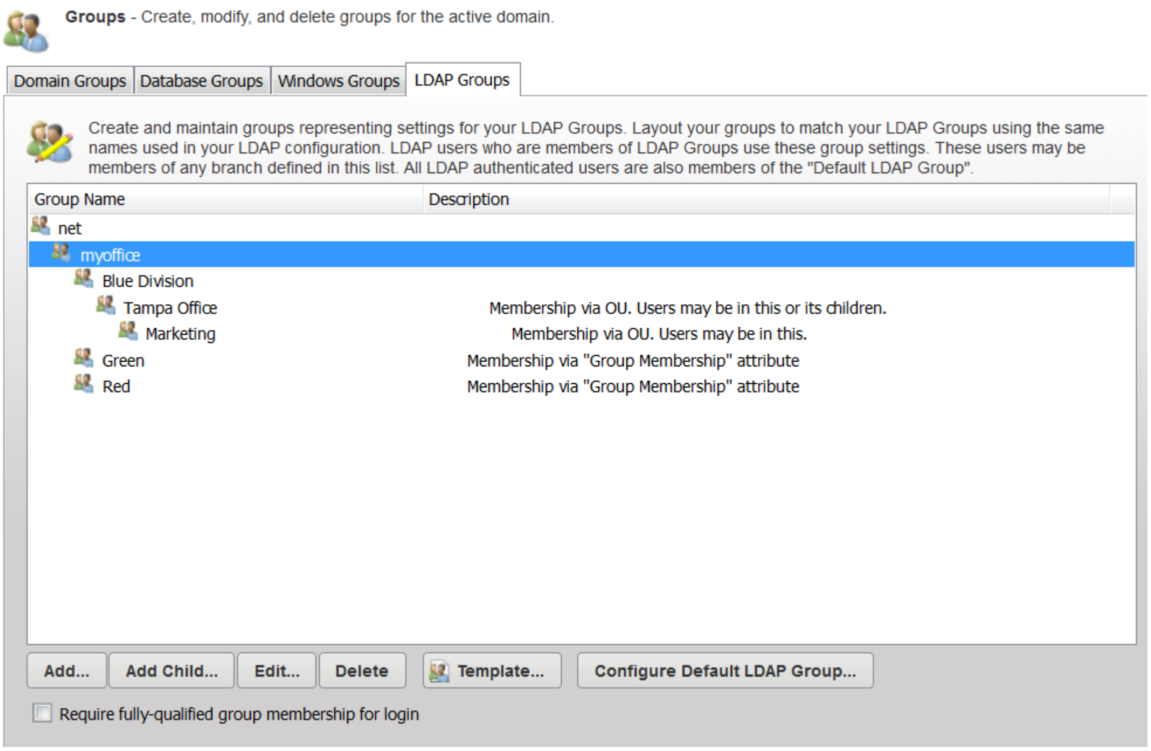
- You want to deploy Serv-U on Linux
- You want to be able to access more than one Windows domain
- You want to be able to access different Windows domains
- You do not care about natively incorporating NTFS permissions. It is not possible to pull directory access rules from LDAP directly, but you can define Serv-U directory access rules for LDAP users. For more information about directory access rules, see "Directory Access Rules".

LDAP User Groups

LDAP User accounts are not visible or configurable on an individual basis in Serv-U, but LDAP Group membership can be used to apply common permissions and settings such as IP restrictions and bandwidth throttles.

All LDAP Users are members of a special Default LDAP Group. Click **Configure Default LDAP Group** under **Users > LDAP Authentication** or under **Groups > LDAP Groups** to configure this group just like a normal Serv-U group. For information about the configuration options available at the group level, see "Groups".

LDAP Users can also be members of individual LDAP Groups. Click **Configure LDAP Groups** under **Users > LDAP Authentication** to configure these groups just like normal Serv-U groups.



Groups - Create, modify, and delete groups for the active domain.

Create and maintain groups representing settings for your LDAP Groups. Layout your groups to match your LDAP Groups using the same names used in your LDAP configuration. LDAP users who are members of LDAP Groups use these group settings. These users may be members of any branch defined in this list. All LDAP authenticated users are also members of the "Default LDAP Group".

Group Name	Description
net	
myoffice	
Blue Division	
Tampa Office	Membership via OU. Users may be in this or its children.
Marketing	Membership via OU. Users may be in this.
Green	Membership via "Group Membership" attribute
Red	Membership via "Group Membership" attribute

☐ Require fully-qualified group membership for login

LDAP Group membership

In order for Serv-U to match users up to the appropriate user groups, the entire hierarchy, including the Distinguished Name (DN) must be recreated in the user group hierarchy.

LDAP Users are also added to any LDAP Groups whose names appear in "Group Membership" attributes defined on the **LDAP Authentication** page. For example, if the Group Membership field is configured to be `grp` and an LDAP user record has both `grp=Green` and `grp=Red` attributes, Serv-U will associate that LDAP User with both the "Red" and "Green" LDAP Groups.

Membership in one or more LDAP groups is required if the **Require fully-qualified group membership for login** option is selected on the **Groups > LDAP Groups** page. If this option is selected, and LDAP Users cannot be matched up to at least one LDAP Group, they will not be allowed to sign on. In this case it is possible that Serv-U successfully authenticates to the LDAP server, and then rejects the user login because the user is not a member of any group.

For more information about group permissions and settings, see "About Groups".

LDAP Server Configuration

Serv-U requires administrators to define one or more LDAP Servers before LDAP authentication will work. LDAP Servers are configured on the **Users > LDAP Authentication** page in the Serv-U Management Console.

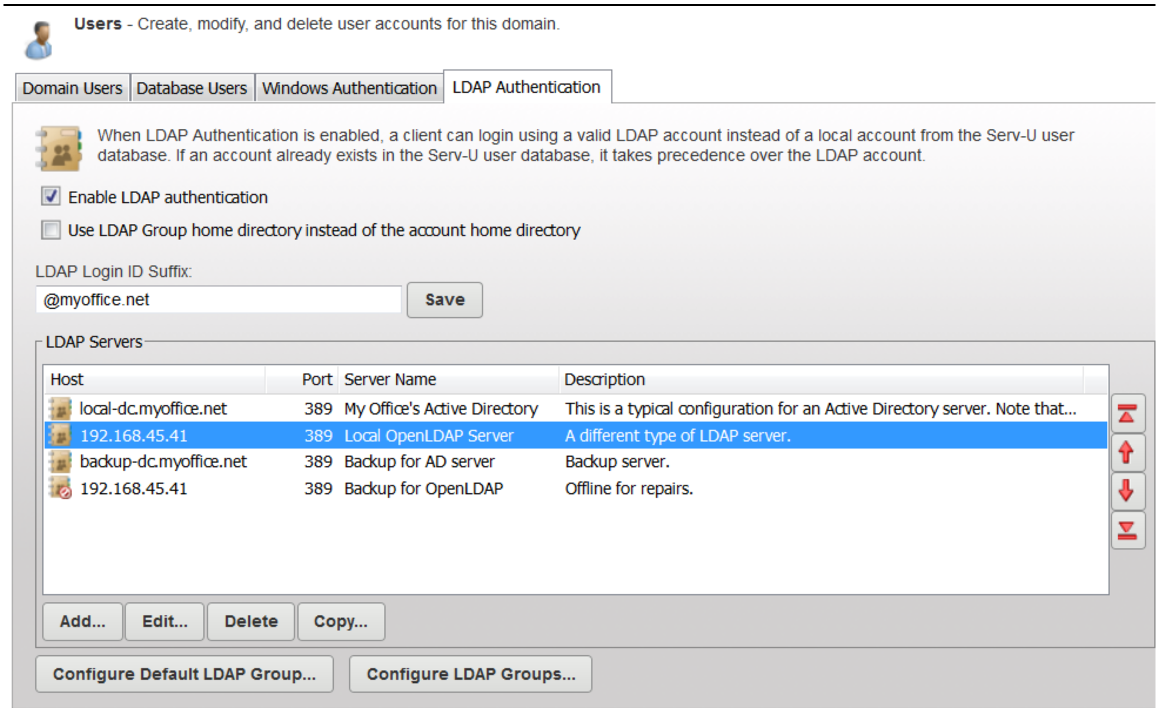
List of LDAP Servers

Administrators can define more than one LDAP Server if they want Serv-U to try a backup server in case the primary LDAP server is down, or if they want to try LDAP credentials against different LDAP servers with different sets of users.

Authentication is attempted against the list of LDAP servers from top to bottom. During login, the first LDAP server that approves a set of credentials will be the server from which the associated LDAP user will draw its full name, email address and other attributes. After attempting a login against the first LDAP server, Serv-U will try each LDAP server in the list until it either encounters a successful login, or it encounters an unsuccessful login paired with an authoritative response from the LDAP server that the attempted LoginID exists on that LDAP server. (In other words, the preceding LDAP servers need to have either been unresponsive or report that they had no knowledge of the LDAP User for login attempts to be made to LDAP servers lower on the list.)

Serv-U tries each available LDAP server, even if the login credentials fail. The error log provides detailed information of any possible connection failure.

Note: The error log contains information about the last LDAP server Serv-U contacted.



Users - Create, modify, and delete user accounts for this domain.

When LDAP Authentication is enabled, a client can login using a valid LDAP account instead of a local account from the Serv-U user database. If an account already exists in the Serv-U user database, it takes precedence over the LDAP account.

☑ Enable LDAP authentication

☐ Use LDAP Group home directory instead of the account home directory

LDAP Login ID Suffix: @myoffice.net

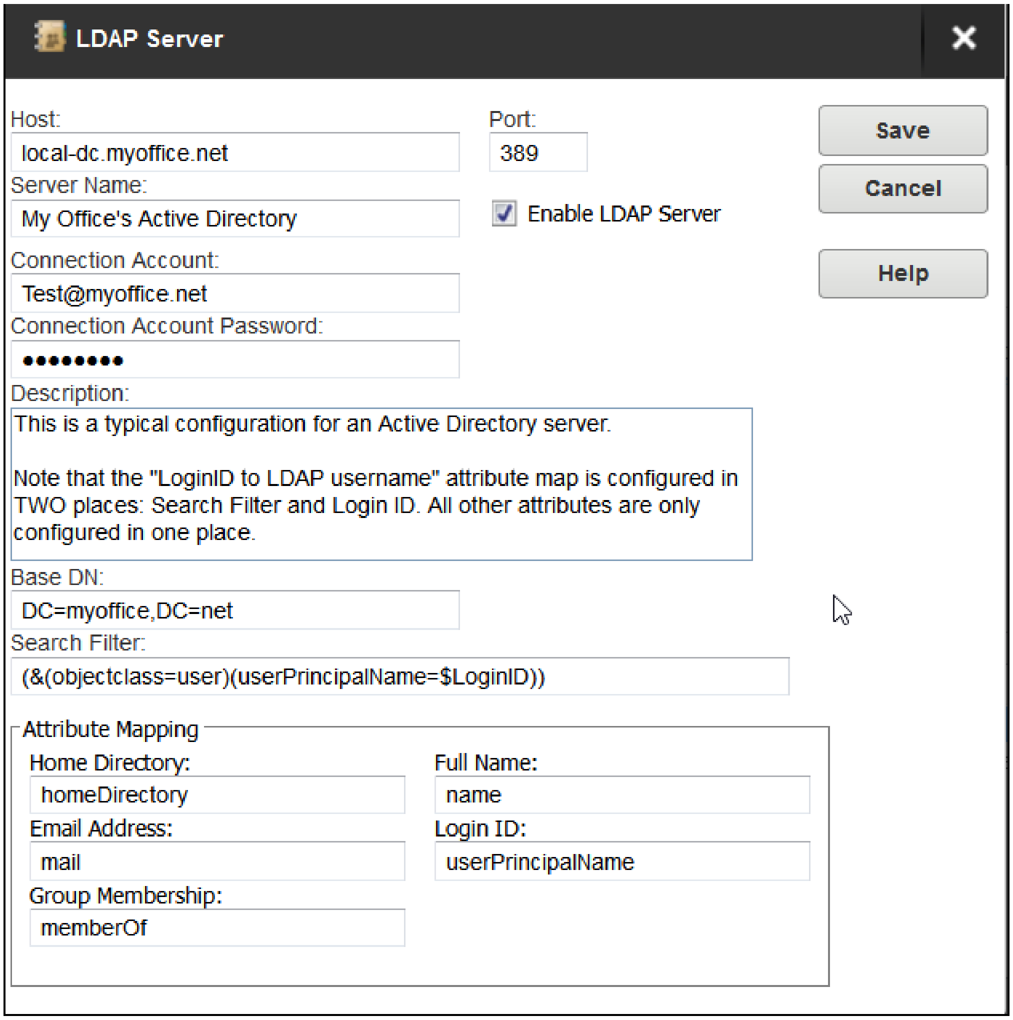
LDAP Servers

Host	Port	Server Name	Description
local-dc.myoffice.net	389	My Office's Active Directory	This is a typical configuration for an Active Directory server. Note that...
192.168.45.41	389	Local OpenLDAP Server	A different type of LDAP server.
backup-dc.myoffice.net	389	Backup for AD server	Backup server.
192.168.45.41	389	Backup for OpenLDAP	Offline for repairs.

Use the **Add**, **Edit**, **Delete**, and **Copy** buttons to work with individual LDAP server entries. When there are multiple LDAP server entries in the list, selecting any entry will reveal **move up**, **move down**, **move to top**, and **move to bottom** ordering arrows on the right side of the dialog.

LDAP Server Configuration

The LDAP Server configuration dialog is displayed when you click **Add**, **Edit**, or **Copy** on the LDAP Servers list.



Host: local-dc.myoffice.net
Port: 389
Server Name: My Office's Active Directory
☑ Enable LDAP Server
Connection Account: Test@myoffice.net
Connection Account Password: ●●●●●●●●●
Description: This is a typical configuration for an Active Directory server.

Note that the "LoginID to LDAP username" attribute map is configured in TWO places: Search Filter and Login ID. All other attributes are only configured in one place.

Base DN: DC=myoffice,DC=net
Search Filter: (&(objectclass=user)(userPrincipalName=$LoginID))

Attribute Mapping
Home Directory: homeDirectory
Full Name: name
Email Address: mail
Login ID: userPrincipalName
Group Membership: memberOf

The LDAP Server Configuration dialog contains the following fields:

- **Host:** The hostname or IP address of the LDAP server. This may be IPv4 or IPv6, but it is always required.
- **Port:** The TCP port on which the LDAP server is listening. This will often be 389.
- **Server Name:** This required field should contain a short description of this LDAP server. We recommend briefly describing the domain and type of LDAP server (for example, `Tampa Office OpenLDAP`).

- **Connection Account**: The username of the account that is used to execute queries against the LDAP server. Provide the account name complete with the UPN suffix. Serv-U does not automatically apply the UPN suffix for the name you provide here.
- **Connection Account Password**: The password belonging to the account that is used to execute queries against the LDAP server.

  Note: If the Connection Account credentials are not supplied, then the credentials that are being authenticated are used.

- **Enable LDAP Server:** Select this option to enable the LDAP server. Disabled LDAP servers will be skipped over during LDAP authentication if you have configured multiple LDAP servers. LDAP authentication will stop working if you disable all your configured LDAP servers.
- **Description**: An optional field in which you can write more notes about your LDAP server.
- **Base DN:** Use this required field to provide the Base DN (or search DN) of the main node in your LDAP server. This is usually similar to the domain name over which your LDAP server has authority. For example, if your LDAP server provides information about your `myoffice.net` domain, this value can be `DC=myoffice,DC=net`.
- **Search Filter:** This required field is used to tell Serv-U how to match incoming LoginIDs ("usernames") to specific LDAP Server entries. `$LoginID` must be included somewhere in this field. During authentication Serv-U will replace this variable with the LDAP User's LoginID (and LDAP Login ID suffix, if specified). The value of the search filter will vary between different types of LDAP servers, and may even vary between different LDAP servers of the same type (depending on the specific schema your LDAP administrator has implemented). For Active Directory LDAP servers, a value of `(&(objectClass=user)(userPrincipalName=$LoginID))` is recommended. Consult with your local LDAP administrator or use an LDAP client (for

example, Softerra LDAP Browser or Apache Directory Studio) to find and test the right value for your LDAP server before deploying into production.

- **Attribute Mapping - Home Directory:** This optional field assigns the value of the named LDAP user entry attribute as your LDAP Users' home directory. A typical value on Active Directory is `homeDirectory`.
- **Attribute Mapping - Full Name:** This optional field assigns the value of the named LDAP user entry attribute as your LDAP Users' full name. A typical value on Active Directory is `name`.
- **Attribute Mapping - Email Address:** This optional field assigns the value of the named LDAP user entry attribute as your LDAP Users' email address. A typical value on Active Directory is `mail`.
- **Attribute Mapping - Login ID:** This optional field assigns the value of the named LDAP user entry attribute as your LDAP Users' login ID (username). A typical value on Active Directory is `userPrincipalName`. This value will almost always match the value paired with `$LoginID`in your Search Filter.
- **Attribute Mapping - Group Membership:** This optional field uses all the values found in the named LDAP attribute as additional LDAP Group membership assigments. For example, if this is configured as `grp` and an LDAP user record has both `grp=Green` and `grp=Red` attributes, Serv-U will associate that LDAP User with both the "Red" and "Green" LDAP Groups. A typical value on Active Directory is `memberOf`.

To test the connection to the LDAP server, log in with an LDAP user. If the connection fails, the log files of Serv-U will provide detailed information about the reason for the failure.

Note: Active Directory and OpenLDAP users are configured in the same way. In the case of OpenLDAP, the user account must have permission to connect to the OpenLDAP database.

The possible error messages are the following:

- An unknown LDAP authentication error has occurred. Please double-check your LDAP configuration - This message signifies a generic issue when the LDAP server does not return any specific error.
- An unknown LDAP authentication error has occurred. The error code returned by the LDAP server was %d - This message signifies a specific LDAP error. The error code returned by the LDAP server can be used to find the specific LDAP error.
- LDAP server returned zero or multiple user records matching the account credentials - This message either indicates that the provided user name is wrong (if zero accounts are returned), or it indicates a problem with the search filter (if multiple accounts are returned).
- Authenticated external user "%s" rejected because group membership is required and no matching Serv-U group was found. A list of all known groups for this user follows.
- No group memberships found. If group membership is expected, double-check the "Group Membership" attribute map for your LDAP configuration in Serv-U.
- No LDAP servers are defined or enabled.
- Unable to initialize LDAP server.
- The connection credentials in the LDAP server configuration have been rejected by the LDAP server.
- The user credentials were rejected by the LDAP server.
- The LDAP server is unavailable to Serv-U.
- The connection credentials in the LDAP server configuration do not have permission to run queries.
- The search filter string in the LDAP server configuration was rejected by the LDAP server.

The following error messages relate to issues with accessing an account's home directory, and are not LDAP specific:

- Error logging in user "%s", permission denied by Serv-U access rules to access home dir "%s"
- Error logging in user "%s", the device for home dir "%s" is not ready
- Error logging in user "%s", could not access home dir "%s"; the error returned by the operating system was %d
- Error logging in user "%s", permission denied by the operating system to access home dir "%s"

SFTP (Secure File Transfer over SSH2) for Users and Groups

Using an Existing Public Key

1. Obtain a public key file.
2. Place the public key file in a secured directory in the server, and then use **Browse** in Serv-U to select the file.
3. Click **Save**.

Creating a Key Pair

1. Click **Manage Keys**.
2. Click **Create Key**.
3. Type the name of the key pair (for example, `MyKey`), which is also used to name the storage file.
4. Type the output directory of the certificate (for example, `C:\ProgramData\RhinoSoft\Serv-U\`).
5. Select the Key Type (default of DSA is preferred, but RSA is available).
6. Select the Key Length (default of 1024 bits provides best performance, 2048 bits is a good median, while 4096 bits provides best security).

7. Enter the password to use for securing the key file.
8. Click **Create**.

Creating Multiple Keys Per User

For the purposes of public key authentication, you can associate multiple public keys with a user account.

To create multiple keys for an account:

1. Click **Manage Keys**.
2. Click **Add Key**, and then specify the Key Name and the Key Path.

When authenticating a client, Serv-U will check all the keys you provide here. If authenticating against one key fails, Serv-U proceeds to check the next key.

Chapter 6: Groups

About Groups

Groups are a method of sharing common configuration options with multiple user accounts. Configuring a group is just like configuring a user account. Virtually every configuration option available for a user account can be set at the group level. In order for a user to inherit a group's settings, it must be a member of the group. Permissions and attributes inherited by a user through group membership can still be overridden at the user level. A user can be a member of multiple groups in order to acquire multiple collections of permissions, such as directory or IP access rules.

Like user accounts, groups can be created at multiple different levels, including:

- Global Groups
- Domain Groups
- Database Groups - available at both the server and domain levels
- Windows Groups

However, groups are only available to user accounts that are defined at the same level. In other words, a global user (that is, a user defined at the server level) can only be a member of a global group. Likewise, a user defined for a specific domain can only be a member of a group also created for that domain. This restriction also applies to groups created in a database in that only users created within a database at the same level can be members of those groups.

Use the **Add**, **Edit**, and **Delete** buttons to manage the available groups.

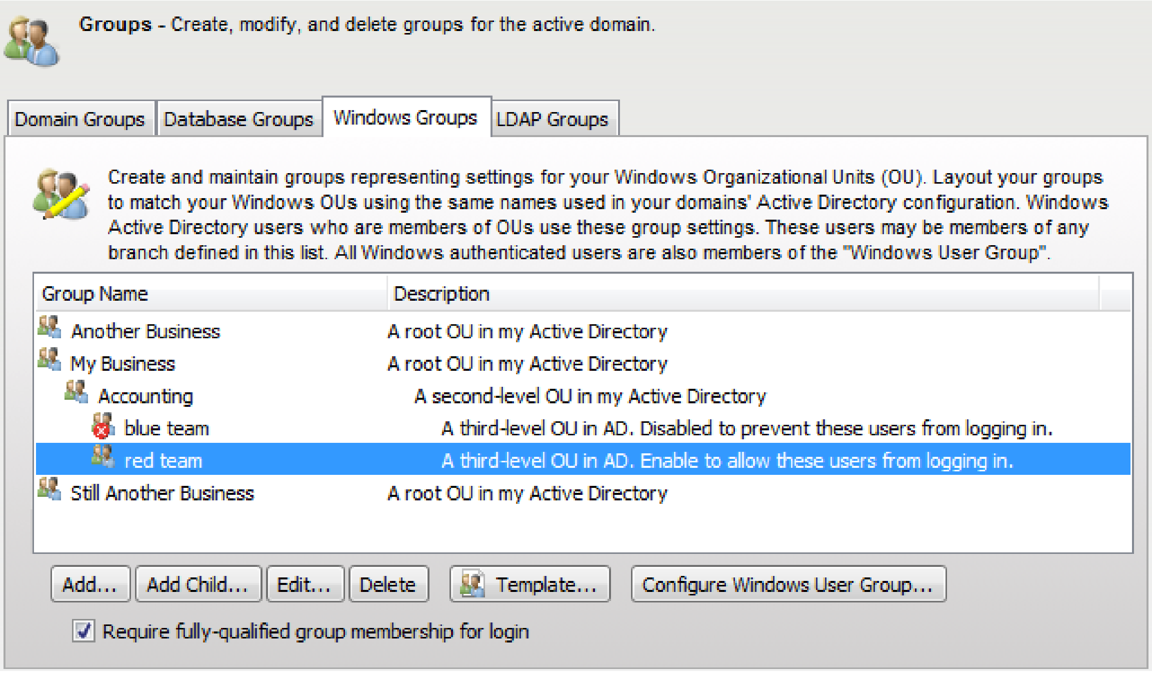
Group Template

Serv-U allows an administrator to configure a template for creating new groups by clicking **Template**. Once opened, the template group can be configured just like any other group object, with the exception of giving it a name. After these settings are saved to the template, all new groups are created with their default settings set to those found within the template. This is a great way to configure some basic settings that you want all of your groups to use by default to save you time when creating new groups.

Windows Groups (Windows Only)

Window Groups are used to apply common permissions and settings such as IP restrictions and bandwidth throttles to Windows Users.

All Windows Users are members of the Default Windows Group. Additional Windows Groups can be created to assign different permissions and settings to different groups of Windows Users.



Groups - Create, modify, and delete groups for the active domain.

Create and maintain groups representing settings for your Windows Organizational Units (OU). Layout your groups to match your Windows OUs using the same names used in your domains' Active Directory configuration. Windows Active Directory users who are members of OUs use these group settings. These users may be members of any branch defined in this list. All Windows authenticated users are also members of the "Windows User Group".

Group Name	Description
Another Business	A root OU in my Active Directory
My Business	A root OU in my Active Directory
Accounting	A second-level OU in my Active Directory
blue team	A third-level OU in AD. Disabled to prevent these users from logging in.
red team	A third-level OU in AD. Enable to allow these users from logging in.
Still Another Business	A root OU in my Active Directory

☑ Require fully-qualified group membership for login

Windows Group membership is determined by the hierarchical OU (organizational unit) membership of each Windows User. For example, a user in the **My Business > Accounting > red team** OU tree would be a member of the **My Business > Accounting > red team** Windows Group on Serv-U, if that group exists. (Visually, "My Business" would be the top Windows Group, "Accounting" would be an indented child Windows Group under that, and "red team" would be an indented child under "Accounting".)

Membership in one or more Windows Groups is required if the **Require fully-qualified group membership for login** option is selected on the Windows Groups page. If this option is selected and Windows Users cannot be matched up to at least one Windows Group, they will not be allowed to log in.

Windows Groups are only available when Serv-U is running on Windows, Serv-U has an MFT Server license, and Windows Authentication has been enabled under **Domain Users > Windows Authentication**.

Search for "Windows Authentication" in the Serv-U Knowledge Base to find current articles and tips about Windows Authentication and Windows Groups.

Configure Windows User Group (Windows Only)

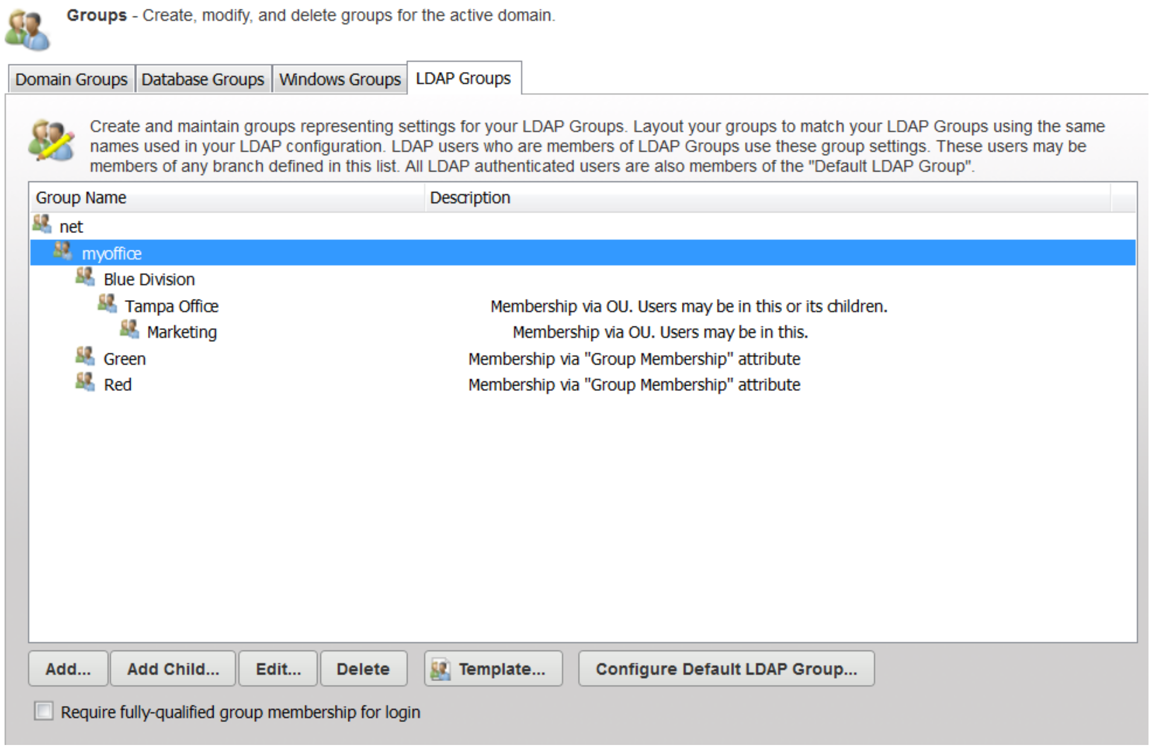
Administrators have the ability to allow clients to log in to the File Server using the local Windows user database or one that is made accessible through a domain server. These user accounts do not exist in the local Serv-U user database and cannot be configured on an individual basis. To aid in configuring these accounts, all users logged in through this method belong to the Default Windows User Group. Clicking this button allows this group to be configured like normal. However, changes that are made to this group only apply to Windows User accounts.

LDAP User Groups

LDAP user accounts are not visible or configurable on an individual basis in Serv-U, but LDAP Group membership can be used to apply common permissions and settings such as IP restrictions and bandwidth throttles.

All LDAP users are members of a special Default LDAP Group. Click **Configure Default LDAP Group** under **Users > LDAP Authentication** or under **Groups > LDAP groups** to configure this group just like a normal Serv-U group.

LDAP users can also be members of individual LDAP Groups. Click **Configure LDAP Groups** under **Users > LDAP Authentication** to configure these groups just like normal Serv-U groups.



Groups - Create, modify, and delete groups for the active domain.

Create and maintain groups representing settings for your LDAP Groups. Layout your groups to match your LDAP Groups using the same names used in your LDAP configuration. LDAP users who are members of LDAP Groups use these group settings. These users may be members of any branch defined in this list. All LDAP authenticated users are also members of the "Default LDAP Group".

Group Name	Description
net	
myoffice	
Blue Division	
Tampa Office	Membership via OU. Users may be in this or its children.
Marketing	Membership via OU. Users may be in this.
Green	Membership via "Group Membership" attribute
Red	Membership via "Group Membership" attribute

☐ Require fully-qualified group membership for login

LDAP Group membership

In order for Serv-U to match users up to the appropriate user groups, the entire hierarchy, including the Distinguished Name (DN) must be recreated in the user group hierarchy.

LDAP users are also added to any LDAP Groups whose names appear in "Group Membership" attributes defined on the **LDAP Authentication** page. For example, if the Group Membership field is configured to be `grp` and an LDAP user record has both `grp=Green` and `grp=Red` attributes, Serv-U will associate that LDAP user with both the "Red" and "Green" LDAP groups.

Membership in one or more LDAP groups is required if the **Require fully-qualified group membership for login** option is selected on the **Groups > LDAP Groups** page. If this option is selected, and LDAP users cannot be matched up to at least one LDAP Group, they will not be allowed to sign on. In this case it is possible that Serv-U successfully authenticates to the LDAP server, and then rejects the user login because the user is not a member of any group.

For more information about LDAP authentication, see "LDAP Authentication".

Group Information

Virtually every attribute available for a user account can be configured at the group level. Group level settings are inherited by the group members and can be overridden at the user level. The Group Information tab contains general information about the group including the name, home directory, and the default administrative privilege for group members. The following sections contain detailed information about each of the available attributes.

Group Name

The group name is a unique identifier that must be unique for each group specified at that level (server or domain). Group names may not contain any of the following special characters: \ / < > | : ? *.

Home Directory

The home directory for a user account is where the user is placed immediately after logging in to the File Server. Each user must have a home directory assigned to it, although the home directory can be specified at the group level if the user is a member of a group. Home directories must be specified using a full path including the drive letter or UNC share name. If the home directory is not found, Serv-U can be configured to create it.

When specifying the home directory, the `%USER%` macro can be used to insert the login ID into the path. This is used mostly to configure a default home directory at the group level or within the new user template to ensure that all new users have a unique home directory. When combined with a Directory Access Rule for `%HOME%`, a new user can be configured with a unique home directory and the proper access rights to that location with a minimal amount of effort.

The `%DOMAIN_HOME%` macro can also be used to identify the user's home directory. For example, to place a user's home directory into a common location, use `%DOMAIN_HOME%\%USER%`.

The home directory can be specified as "\" (root) in order to grant system-level access to a user, allowing them the ability to access all system drives. In order for this to work properly, the user must not be locked in their home directory.

Administration Privilege

A user account can be granted one of the following types of administrative privileges:

- No Privilege
- Group Administrator
- Domain Administrator
- System Administrator

The value of this attribute can be inherited through group membership.

A user account with No Privilege is a regular user account that can only log in to transfer files to and from the File Server. The Serv-U Management Console is not available to these user accounts.

A Group Administrator can only perform administrative duties relating to their primary group (the group that is listed first in their Groups memberships list. They can add, edit, and delete users which are members of their primary group, as well as assign permissions at or below the level of the Group Administrator. They may not make any other changes.

A Domain Administrator can only perform administrative duties for the domain to which their account belongs. A Domain Administrator is also restricted from performing domain-related activities that may affect other domains. The domain-related activities that may *not* be performed by

Domain Administrators consist of configuring their domain listeners or configuring ODBC database access for the domain.

A System Administrator can perform any File Server administration activity including creating and deleting domains, user accounts, or even updating the File Server's license. A user account with System Administrator privileges that is logged in through HTTP remote administration can essentially administer the server as if they had physical access to the machine.

Default Web Client

If your Serv-U license enables the use of FTP Voyager JV, then users connecting to the File Server through HTTP can choose which client they want to use after logging in. Instead of asking users which client they want to use, a default client can also be specified. If this option is changed, it overrides the option specified at the server or domain level. It can also be inherited by a user through group membership. Use the **Inherit default value** option to reset it to the appropriate default value.

Lock user in home directory

A user that is locked in their home directory may not access paths above their home directory. In addition, the actual physical location of their home directory is masked as Serv-U always reports it as "/" (root). The value of this attribute can be inherited through group membership.

Apply group directory access rules first

The order in which Directory Access Rules are listed has significance in determining the resources that are available to a user account. By default, Directory Access Rules specified at the group level take precedence over ones specified at the user level. However, there are certain instances where you may want the user level rules to take precedence. Deselect this option to place the Group's Directory Access Rules *below* the user's.

Always allow login

Enabling this option means that the user account is always permitted to log in, regardless of restrictions placed upon the File Server such as maximum number of sessions. It is useful as a fail-safe in order to ensure that critical system administrator accounts can always remotely access the File Server under all conditions. As with any option that allows bypassing access rules, care should be taken in granting this ability. The value of this attribute can be inherited through group membership.

Note: Enabling the Always Allow Login option does not override IP access rules. If both options are defined, the IP access rules prevail.

Description

The description allows for the entry of additional notes that are only visible by administrators.

Availability

This feature limits when users can connect to this server. Limitations can be placed on the time of day as well as the day of the week. When attempting to log in outside the specified available times, users are presented with a message that the user account is currently unavailable.

Directory Access Rules

Directory Access Rules

Directory Access rules define the areas of the system that are accessible to user accounts. While traditionally restricted to the user and group levels, Serv-U extends the usage of Directory Access rules to both the domain and server levels through the creation of global Directory Access rules. Directory Access rules specified at the server level are inherited by all users of the File Server. When specified at the domain level, they are only inherited by users belonging to that domain. The traditional rules of inheritance apply where rules specified at a lower level (for example, the user level), override conflicting or duplicates rules specified at a higher level (for example, the server level).

When setting the Directory Access path, the `&#37;USER&#37;`, `&#37;HOME&#37;`, `&#37;USER_FULL_NAME&#37;`, and `&#37;DOMAIN_HOME&#37;` variables are available to simplify the process. For example, use `%HOME%/ftproot/` to create a Directory Access rule that specifies the `ftproot` folder in the user's home directory. Directory access rules specified in this manner are "portable" in the event that the actual home directory changes while maintaining the same subdirectory structure. This leads to less maintenance for the File Server administrator. If the `%USER%` variable is specified in the path, it is replaced with the user's login ID. This variable is useful in specifying a group's home directory to ensure that users inherit a logical and unique home directory. The `&#37;USER_FULL_NAME&#37;` variable can be used to insert the Full Name value into the path (the user must have a "Full Name" specified for this to function). For example, the user "Tom Smith" could use `D:\ftproot\&#37;USER_FULL_NAME&#37;` for `D:\ftproot\Tom Smith`. Finally, the `%DOMAIN_HOME%` macro can also be used to identify the user's home directory. For example, to place a user and their home directory into a common directory use `%DOMAIN_HOME%\%USER%`.

Directory Access rules are applied in the order they are listed. The first rule Serv-U encounters in the list that matches the path of a client's request is the one that is applied for that rule. In other words, if a rule exists that denies access to a particular subdirectory but is listed *below* the rule that grants access to the parent directory, then a user still has access to the subdirectory in question. The arrows on the right side of the Directory Access list are used to rearrange the order in which the rules are applied.

A listing and description of each available directory access permission follows.

File Permissions

Read

Allows users to read (that is, download) files. This permission does not allow users to list the contents of a directory, which is granted by the **List** permission.

Write

Allows users to write (that is, upload) files. This permission does not allow users to modify existing files, which is granted by the **Append** permission.

Append

Allows users to append data to existing files. This permission is normally used to grant users the ability to resume transferring to partially uploaded files.

Rename

Allows users to rename existing files.

Delete

Allows users to delete files.

Execute

Allows users to remotely execute files. Execute access is meant for remotely starting programs and usually applies to specific files. This is a very powerful permission and great care should be used in granting it to users. A user with **Write** and **Execute** permissions can essentially install any program of their choosing on your system.

Directory Permissions

List

Allows users to list the files and subdirectories contained in the directory. Also allows users to list this folder when listing the contents of a parent directory. (See KB #2079 for more information about "blind downloads" and "blind uploads".)

Create

Allows users to create new directories within the directory.

Rename

Allows users to rename existing directories within the directory.

Remove

Allows users to delete existing directories within the directory. **Note:** If the directory contains files, the user also needs to have the **Delete** files permission in order to remove the directory.

Subdirectory Permissions

Inherit

Allows all subdirectories to inherit the same permissions as the parent directory. The **Inherit** permission is appropriate for most circumstances, but if access must be restricted to subfolders (as is the case when implementing Mandatory Access Control), deselect **Inherit** and grant permissions specifically by folder.

Advanced: Access as Windows User (Windows Only)

For a variety of reasons, files and folders may be kept on external servers in order to centralize file storage or provide additional layers of security. In this environment, files can be accessed by the UNC path (`\\servername\folder\`) instead of the traditional `C:\ftproot\folder` path. However, accessing folders stored across the network poses an additional challenge, because Windows services are run under the Local System account by default, which has no access to network resources.

To mitigate this problem for all of Serv-U, it is possible to configure the Serv-U File Server service to run under a network account. The alternative, preferred when many servers exist, or if the Serv-U File Server service needs to run under Local System for security reasons is to configure a Directory Access rule to use a specific Windows User for file access. By clicking the **Advanced** button it is possible to specify a specific Windows user for each individual Directory Access rule. Just like in Windows Authentication, directory access is subject to NTFS permissions, though in this case also to the configured permissions in Serv-U.

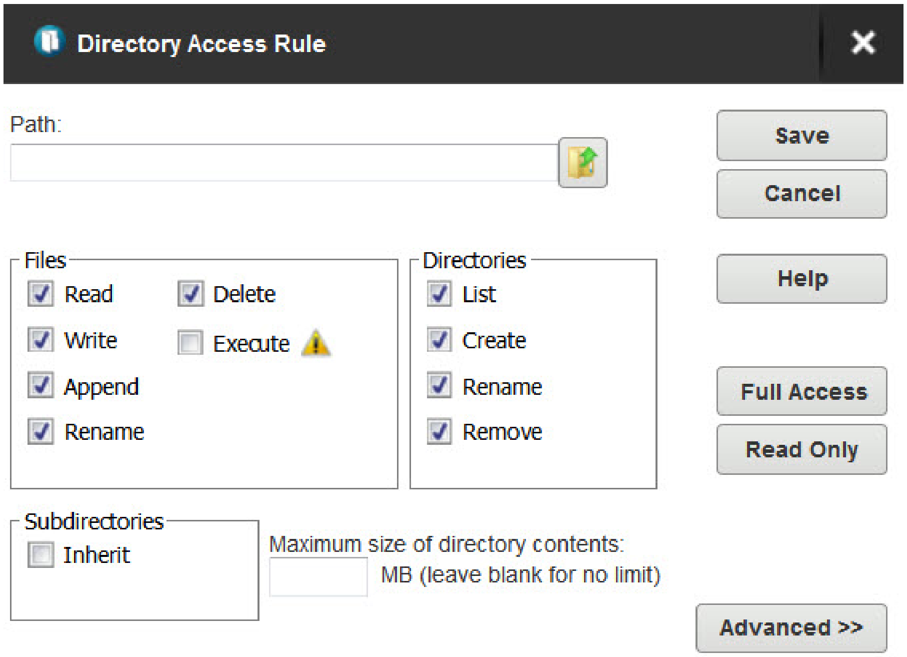
Quota Permissions

Maximum size of directory contents

Setting the maximum size actively restricts the size of the directory contents to the specified value. Any attempted file transfers that cause the directory contents to exceed this value are rejected. This feature serves as an alternative to the traditional quota feature that relies upon tracking all file transfers (uploads and deletions) to calculate directory sizes and is not able to consider changes made to the directory contents outside of a user's File Server activity.

Mandatory Access Control

Serv-U enables the use of Mandatory Access control in cases where users need to be granted access to the same home directory but should not necessarily be able to access the subdirectories below it. To implement Mandatory Access Control at a directory level, disable the **Inherit** permission as shown below (assume the rule applies to `D:\ftproot\`):



Directory Access Rule

Path:

Files
☑ Read
☑ Write
☑ Append
☑ Rename
☑ Delete
☐ Execute

Directories
☑ List
☑ Create
☑ Rename
☑ Remove

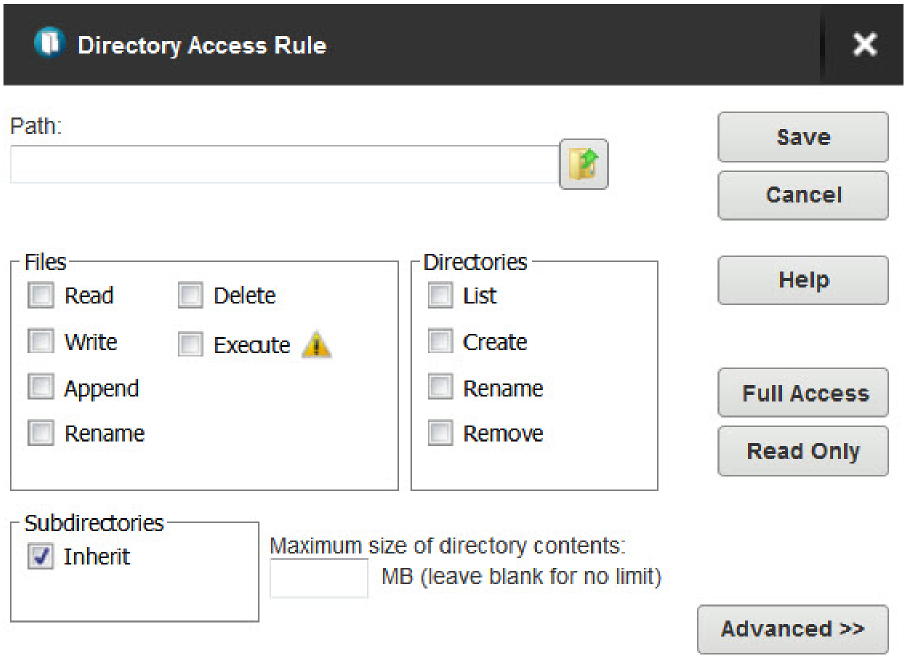
Subdirectories
☐ Inherit

Maximum size of directory contents:
MB (leave blank for no limit)

Now, the user has access to the `ftproot` folder but to no folders below it. Permissions must individually be granted to subfolders that the user needs access to, providing the security of Mandatory Access Control in the Serv-U File Server.

Restricting File Types

If users are using storage space on the Serv-U File Server to store non-work-related files such as MP3 music files, this can be prevented by configuring a Directory Access rule placed **above** the main Directory Access Rule (use the arrows on the right to reorder rules) to prevent MP3 files from being transferred as shown below. In the text entry for the rule, type `*.mp3` and use the permissions shown below:



Path:

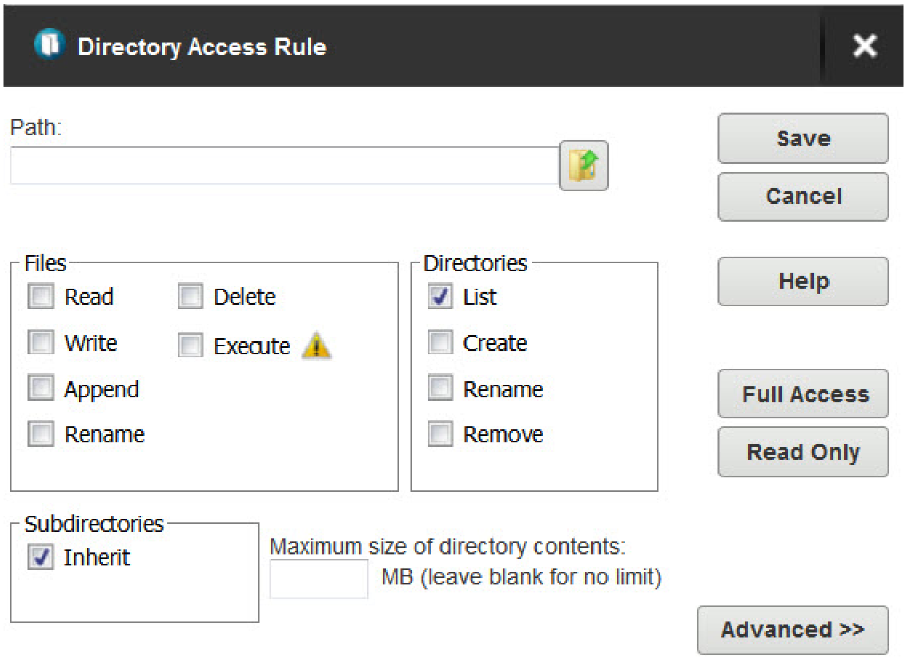
Files
☐ Read ☐ Delete
☐ Write ☐ Execute
☐ Append
☐ Rename

Directories
☐ List
☐ Create
☐ Rename
☐ Remove

Subdirectories
☑ Inherit

Maximum size of directory contents:
MB (leave blank for no limit)

The rule denies permission to any transfer of files with the `.mp3` extension and can be modified to reflect any file extension. Similarly, if accounting employees only need to transfer files with the `.mdb` extension, configure a pair of rules that grants permissions for `.mdb` files but denies access to all other files, as shown below. In the first rule enter the path that should be the user's home directory or directory they need access to, and in the second rule enter the extension of the file that should be accessed (such as `*.mdb`):



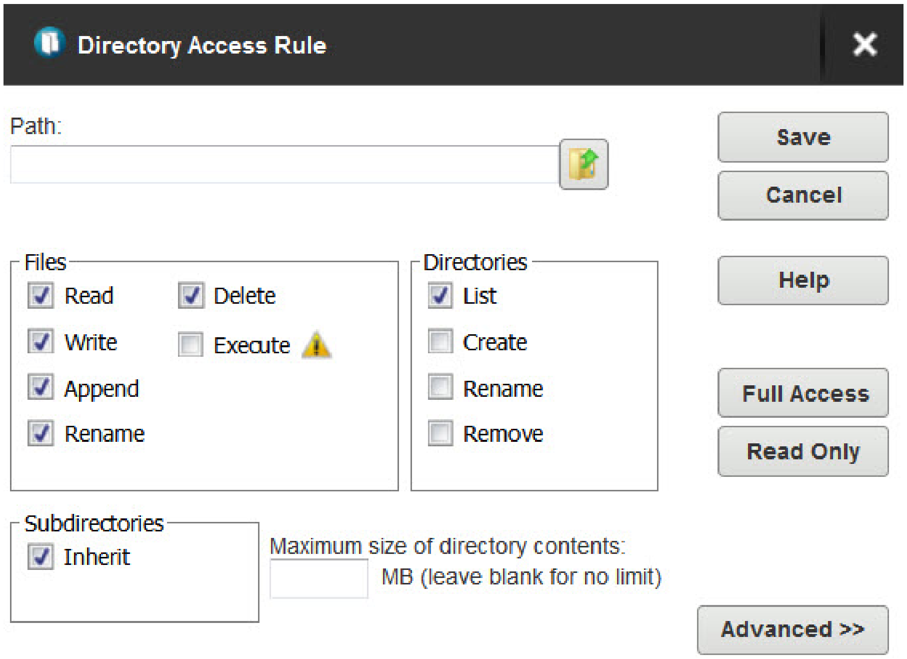
Path:

Files
☐ Read ☐ Delete
☐ Write ☐ Execute ⚠
☐ Append
☐ Rename

Directories
☑ List
☐ Create
☐ Rename
☐ Remove

Subdirectories
☑ Inherit

Maximum size of directory contents:
MB (leave blank for no limit)



Path:

Files
☑ Read ☑ Delete
☑ Write ☐ Execute ⚠
☑ Append
☑ Rename

Directories
☑ List
☐ Create
☐ Rename
☐ Remove

Subdirectories
☑ Inherit

Maximum size of directory contents:
MB (leave blank for no limit)

These rules only allow users to access `.mdb` files within the directories specified, and can be adapted to any file extension or set of file extensions.

Virtual Paths

Virtual Paths allow users to gain access to files and folders outside of their own home directory. A Virtual Path only defines a method of mapping an existing directory to another location on the system to make it visible within a user's accessible directory structure. In order to actually have access to the mapped location, the user must still have a Directory Access rule specified for the physical path of a Virtual Path.

Like Directory Access Rules, Virtual Paths can be configured at the server, domain, group, and user levels. Virtual Paths created at the server level are available for use by all users of the File Server. When created at the domain level, they are only accessible by users belonging to that domain. Serv-U's granular file access controls even allow for Virtual Paths created specifically for individual users or groups.

Physical Path

The physical path is the actual location on the system, or network, that is to be placed in a virtual location accessible by a user. If the physical path is located on the same computer, a full path should be used, such as `D:\inetpub\ftp\public`. A UNC path can also be used, such as `\\Server\share\public`. In order for a Virtual Path to be visible to a user, they must have a Directory Access rule specified for the physical path.

Virtual Path

The virtual path is the location that the physical path should appear in for the user. The `%HOME%` macro is commonly used in the virtual path to place the specified physical path in the home directory of the user. When specifying the virtual path, the last specified directory is used as the name displayed in directory listings to the user. For example, a virtual path of `%HOME%/public` places the specified physical path in a folder named `public` within the user's home directory. A full path without any macros can also be used.

Include in "Maximum Directory Size" calculations

When selected, the Virtual Path is included in Maximum Directory Size calculations. When deselected, the Virtual Path is not included in the Maximum Directory Size calculations. Maximum Directory Size limits the size of directories affecting how much data can be uploaded.

Case File - Using Virtual Paths

A group of web developers have been granted access to the directory `D:\ftproot\examplesite.com\` for web development purposes. The developers also need access to an image repository located at `D:\corpimages\`. To avoid granting the group access to the root D drive, a Virtual Path must be configured so that the image repository *appears* to be contained within their home directory. Within the web developer's group, add a Virtual Path to bring the directory to the users by specifying `D:\corpimages\` as the Physical Path and `D:\ftproot\examplesite.com\corpimages` as the Virtual Path. Be sure to add a group level Directory Access rule for `D:\corpimages\` as well. The developers now have access to the image repository without compromising security or relocating shared resources.

Case File - Creating Relative Virtual Paths

Continuing with the previous example, if the web developer's group home directory is relocated to another drive, not only does the home directory have to be updated, but the Virtual Path also needs to be updated to reflect this change. This can be avoided by using the `%HOME%` macro to create a relative Virtual Path location that eliminates the need to update the path if the home directory changes. Instead of using `D:\ftproot\examplesite.com\corpimages` as the Virtual Path, use `%HOME%\corpimages`. This tells Serv-U to place the `corpimages` Virtual Path within the group's home directory - whatever that may be. If the home directory changes at a later date, the Virtual Path still appears there.

Configuring User and Group Logs

The Serv-U File Server allows for a great deal of customization in logging user and group events and activity. To enable a logging option, select the appropriate option in the **Log Message Options** grouping. When an option is selected, the appropriate logging information is saved to the specified log file if the **Enable logging to file** option is selected. The log can be configured to show as much or as little information as you want. After configuring the logging options you want, click **Save** to save the changes.

Logging to File Settings

Log file path

The log file must be given a name before information can be saved to a file. Click **Browse** to select an existing file or directory location for the log file. The log file path supports certain wildcard characters as outlined below. Wildcard characters referencing the date apply to the day that the log file is created. When combined with the **Automatically rotate log file** option, wildcards provide an automatic way to archive activity for audits, such as those required by HIPAA. The available wildcard characters are the following:

- %H - The hour of the day (24-hour clock)
- %D - The current day of the month
- %M - The name of the current month
- %N - The numeric value of the current month (1-12)
- %Y - The 4-digit value of the current year (for example, 2014)
- %X - The 2-digit value of the current year (for example, 14 for 2014)
- %S - The name of the domain whose activity is being logged
- %G - The name of the group whose activity is being logged
- %L - The name of the login ID whose activity is being logged
- %U - The full name of the user whose activity is being logged

Enable logging to file

Select this option to enable Serv-U to begin saving log information to the file specified in the **Log file path**. If this option is not selected, Serv-U does not log any information to the file, regardless of the individual options selected in the **Log Message Options** grouping.

Automatically rotate log file

To ensure that log files remain a manageable size and can be easily referenced during auditing, Serv-U supports the ability to automatically rotate the log file on a regular basis. By specifying a **Log file path** containing wildcards referencing the current date, Serv-U can rotate the log file and create a unique file name every hour, day, week, month, or year.

Purge Old Log Files

Serv-U supports the ability to automatically purge old log files by setting a maximum number of files to keep and/or a maximum size limit in megabytes. Setting these options to `0` means the setting is unlimited and the limit is not applied.

Warning: Log files are purged based only on the current log file path name, and are purged approximately every 10 minutes. Log file variables are replaced with Windows wildcard values used to search for matching files. For example:

`C:\Logs\%Y:%N:%D %S Log.txt` is searched for `C:\Logs\????:??:?? * Log.txt`

`C:\Logs\%Y:%M:%D %S Log.txt` is searched for `C:\Logs\????:*:?? * Log.txt`

`C:\Logs\%S\%Y:%M:%D Log.txt` is searched for `C:\Logs\--DomainName--\????:*:?? Log.txt`

`C:\Logs\%G\%Y:%M:%D Log.txt` is searched for `C:\Logs\--GroupName--\????:*:?? Log.txt`

`C:\Logs\%L\%Y:%M:%D Log.txt` is searched for `C:\Logs\--LoginID--\????:*:?? Log.txt`

`C:\Logs\%U\%Y:%M:%D Log.txt` is searched for `C:\Logs\--UserFullName--\????:*:?? Log.txt`

Log variables are wildcarded in the following way:

%H --> ??
%D --> ??

%N --> ??
%M --> *
%Y --> ????
%X --> ??
%S --> *
%G --> *
%L --> *
%U --> *

Anything matching the wildcarded path name can be purged. Use caution. It is best practice to place log files into a single directory to avoid unexpected file deletion.

Do Not Log IPs

Serv-U supports the ability to specify IP addresses that are exempt from logging. Activity from these IP addresses is not logged. This is useful to exempt IP addresses for administrators that may otherwise generate a lot of logging information that can obfuscate domain activity from regular users. It can also be used to save on log space and reduce overhead. Click **Do Not Log IPs**, and then add IP addresses as appropriate.

Group Members

The user accounts that are members of the currently selected group are displayed on this tab. It can be used to get a quick overview of what users are currently inheriting the group's settings at this time. Currently, users cannot be added or removed from the group using this interface. Adding or removing a group membership must be done from the appropriate user's account properties window.

A user account can be granted one of four types of administrative privileges:

- No Privilege
- Group Administrator

- Domain Administrator
- System Administrator

The value of this attribute can be inherited through group membership. A user account with No Privilege is a regular user account that can only log in to transfer files to and from the File Server. The Serv-U Management Console is not available to these user accounts.

A Group Administrator can only perform administrative duties relating to their primary group (the group that is listed first in their groups memberships list). They can add, edit, and delete users which are members of their primary group, as well as assign permissions at or below the level of the Group Administrator. They may not make any other changes.

A Domain Administrator can only perform administrative duties for the domain to which their account belongs. A Domain Administrator is also restricted from performing domain-related activities that may affect other domains. The domain-related activities that may not be performed by Domain Administrators consist of configuring their domain listeners or configuring ODBC database access for the domain.

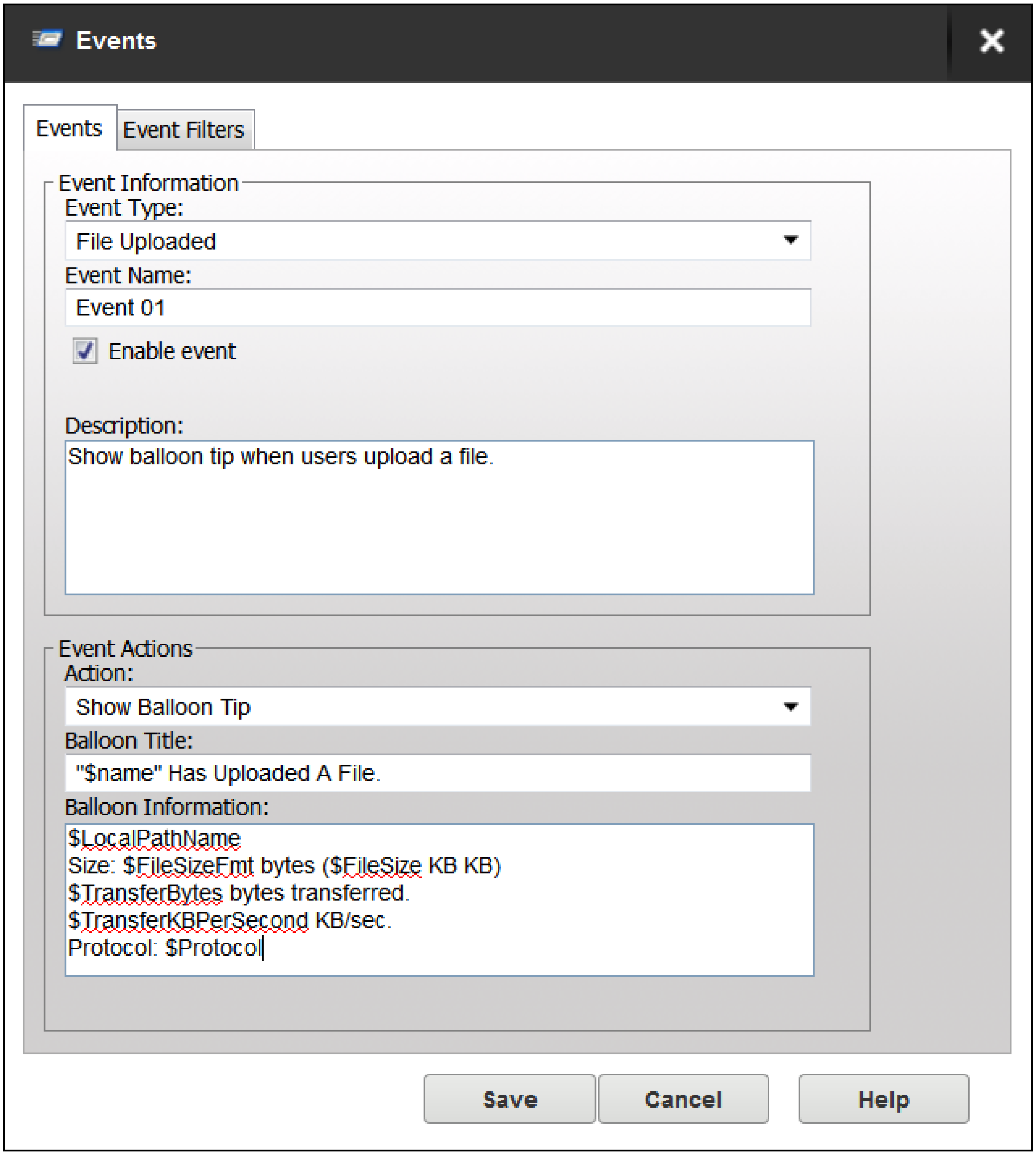
A System Administrator has the ability to perform any File Server administration activity including creating and deleting domains, user accounts, or even updating the File Server's license. A user account with System Administrator privileges that is logged in through HTTP remote administration can essentially administer the server as if they had physical access to the machine.

Serv-U also supports read-only administrator accounts which can allow administrators to log in and view configuration options at the domain or server level, greatly aiding remote problem diagnosis when working with outside parties. Read-only administrator privileges are identical to their full-access equivalents, except that they cannot change any settings or create, delete or edit user accounts.

Note: When configuring a user account with administrative privileges, take care in specifying their home directory. An administrator with a home directory other than

"\" (root) that is locked in their home directory may not use file paths outside of their home directory when configuring the File Server.

Serv-U Events



Event Type: File Uploaded

Event Name: Event 01

☑ Enable event

Description: Show balloon tip when users upload a file.

Action: Show Balloon Tip

Balloon Title: "$name" Has Uploaded A File.

Balloon Information:

```
$LocalPathName
Size: $FileSizeFmt bytes ($FileSize KB KB)
$TransferBytes bytes transferred.
$TransferKBPerSecond KB/sec.
Protocol: $Protocol
```

Serv-U enables the use of event handling which can perform various actions triggered by a list of selected events. The following list contains the actions available to administrators:

Server Events

- Server Start - Triggered by Serv-U starting up, whether by starting the Serv-U service or starting Serv-U as an application.
- Server Stop - Triggered by Serv-U shutting down, whether from service or application-level status. This event will only trigger for graceful stops.

Server and Domain Events

- Domain Start - Triggered by a Serv-U Domain starting, via the **Enable Domain** setting in the **Domain Details > Settings** menu or as part of normal server startup.
- Domain Stop - Triggered by a Serv-U Domain stopping, via the **Enable Domain** setting in the **Domain Details > Settings** menu or as part of normal server startup.
- Session Connection - Triggered by a new TCP session connection.
- Session Disconnect - Triggered by a TCP session disconnection.
- Session Connection Failure - Triggered by a failed session connection attempt.
- Log File Deleted - Triggered by the automatic deletion of a log file, according to logging settings.
- Log File Rotated - Triggered by the automatic rotation of a log file, according to logging settings.
- Listener Success - Triggered by a successful listener connection.
- Listener Stop - Triggered by a stopped listener connection.
- Listener Failure - Triggered by a failed listener connection.
- Gateway Listener Success - Triggered by a successful Gateway listener connection.

- Gateway Listener Stop - Triggered by a stopped Gateway listener connection.
- Gateway Listener Failure - Triggered by a failed Gateway listener connection.
- Permanent Listener Success - Triggered by a successful permanent listener connection.
- Permanent Listener Failure - Triggered by a failed permanent listener connection.
- Permanent Listener Stop - Triggered by a stopped permanent listener connection.
- Permanent Gateway Listener Success - Triggered by a successful permanent Gateway listener connection.
- Permanent Gateway Listener Stop - Triggered by a stopped permanent Gateway listener connection.
- Permanent Gateway Listener Failure - Triggered by a failed permanent Gateway listener connection.
- File Management Rule Success - Triggered when a file management rule is applied, and no errors are encountered.
- File Management Rule Failure - Triggered when a file management rule is applied, and at least one error is encountered.

Server, Domain, User and Group Events

- User Login - Triggered by the login of a user account.
- User Logout - Triggered by the logout of a user account.
- User Login Failure - Triggered by a failed login. A failed login is any connection attempt to Serv-U that fails, whether due to invalid credentials, or a session disconnect before authentication, either due to an incorrect user name, incorrect password, incorrect SSH key pair (for SFTP Public Key Authentication), or any or all of the above.

- User Password Change - Triggered by the change of a password for a user account, either by an administrator or by the user (if permitted).
- User Password Change Failure - Triggered by a failed password change attempt.
- User Enabled - Triggered by the enabling of a user account that was previously disabled.
- User Disabled - Triggered by the disabling of a user account that was previously enabled.
- User Deleted - Triggered by the deletion of a user account by a remote administrator, in an ODBC database, or in the local Management Console.
- User Added - Triggered by the creation of a user account by a remote administrator, in an ODBC database, or in the local Management Console.
- Password Recovery Sent - Triggered by a successful password recovery by an end user or by an administrator.
- Password Recovery Failed - Triggered by a failed password recovery attempt, either due to lack of email address in the user account or lack of permissions.
- Password Stale - Triggered by a stale password, as configured in **Limits & Settings**, that is going to expire.
- User Auto Disable - Triggered by the automatic disabling of a user account, as configured by a user's **Automatically Disable** date.
- User Auto Deleted - Triggered by the automatic deletion of a user account, as configured by a user's **Automatically Delete** date.
- User Pre-disable - Triggered by the upcoming disabling of a user account, as configured in the user's **Automatically Disable** date and the "Days before automatically disabling account to trigger the pre-disable event" limit.
- User Pre-delete - Triggered by the upcoming deletion of a user account, as configured in the user's **Automatically Delete** date and the **Days before automatically deleting account to trigger the pre-delete** event limit.

- User Email Set - Triggered by a user or administrator setting the email address for a user account.
- User Email Set Failure - Triggered by a failed attempt by a user or administrator to set the email address for a user account.
- IP Blocked - Triggered by a failed login attempt due to an IP Access rule.
- IP Blocked Time - Triggered by a failed login attempt due to an IP Access rule that was automatically added by brute force settings, configured in **Domain Limits & Settings** or **Server Limits & Settings**.
- Too Many Sessions - Triggered by more sessions logging on to the server than are permitted, per the **Limits & Settings** for the user account, group, domain, or server.
- Too Many Session On IP - Triggered by more sessions logging on to the server from a specific IP address than are permitted, per the **Limits & Settings** for the user account, group, domain, or server.
- IP Auto Added To Access Rules - Triggered by the automatic addition of an IP Access rule due to a user triggering the "brute force" settings.
- Session Idle Timeout - Triggered by an idle session timeout.
- Session Timeout - Triggered by a session timeout.
- File Uploaded - Triggered by a file uploaded to Serv-U. This event triggers for partial uploads if the upload session terminated with a successful message and no data corruption.
- File Upload Failed - Triggered by a failed file upload to Serv-U.
- File Download - Triggered by a file downloaded from Serv-U.
- File Download Failed - Triggered by a failed file download from Serv-U.
- File Deleted - Triggered by the deletion of a file on the Serv-U server by a user.
- File Moved - Triggered by the moving of a file on the Serv-U server by a user.

- Directory Created - Triggered by the creation of a directory.
- Directory Deleted - Triggered by the deletion of a directory.
- Directory Changed - Triggered by changing the current working directory.
- Directory Moved - Triggered by moving a directory to a new location.
- Over Quota - Triggered by going over disk quota space. The current quota space is shown in the user account, in the **Limits & Settings** menu.
- Over Disk Space - Triggered by exceeding the Max Dir Size configured for a Directory Access rule. The current disk space is shown with the `AVBL FTP` command, or using the **Directory Properties** option in the HTTP/HTTPS Web Client and FTP Voyager JV.

Creating Common Events

Serv-U allows administrators to automatically create a list of the most common events. You can choose to create these common events using email and/or balloon tip actions. Click **Create Common Event** located in the Events tab. Select either the **Send Email** or **Show balloon tip** option for the action you want to be performed on the common events. If you choose to Send Email you must also enter an **To:** address where the events are to be sent.

Note: The **Write to Windows Event Log**, and **Write to Microsoft Message Queue (MSMQ)** options are available for Windows only.

Event Actions

Administrators can select from the following actions that will be executed when an event is triggered:

- Send Email
- Show Balloon Tip*
- Execute Command*
- Write to Windows Event Log (Windows only)*
- Write to Microsoft Message Queue (MSMQ) (Windows only)*

* - Events involving anything other than email may only be configured by Serv-U server administrators.

Email Actions

Email actions can be configured to send emails to multiple recipients and to Serv-U Groups when an event is triggered. To add an email address, enter it in the **To** or **Bcc** fields. To send emails to a Serv-U Group, use the **Group** icon to add or remove Serv-U Groups from the distribution list. Email addresses must be separated by commas or semicolons. Email actions contain a **To**, **Subject** and **Message** parameter. Special variables can be used to send specific data pertaining to the event. For more information about the variables, see "System Variables".

To use email actions, you must first configure SMTP in Serv-U. For information, see "Serv-U SMTP Configuration".

Balloon Tip Actions

Balloon tip actions can be configured to show a balloon tip in the system tray when an event is triggered. Balloon tip actions contain a **Balloon Title** and a **Balloon Message** parameter. Special variables can be used to send specific data pertaining to the event. For more information about the variables, see "System Variables".

Execute Command Actions

Execute command actions can be configured to execute a command on a file when an event is triggered. Execute command actions contain an **Executable Path**, **Command Line Parameters**, and **Completion Wait Time** parameter. For the **Completion Wait Time** parameter, you can enter the number of seconds to wait after starting the executable path. Enter a value of 0 for no waiting.

Note: Any amount of time Serv-U spends waiting delays any processing that Serv-U can perform.

A wait value should only be used to give an external program enough time to perform some operation, such as move a log file before it is deleted (for example, `$LogFilePath` for the Log File Deleted event). Special variables can be used to send specific data pertaining to the event. For more information about the variables, see "System Variables".

Write to Windows Event Log

Writing event messages to a local Windows Event Log allows you to monitor and record Serv-U activity using third-party network management software such as those from HP Openview, SolarWinds, SpiceWorks, and many other vendors. All messages will appear in the Windows Application Log from a source of "Serv-U".

This event has only one field:

- Log Information: The contents of the message to be written into the event log. This is normally either a human-readable message (for example, `filename uploaded by person`) or a machine-readable string (for example, `filename|uploaded|person`), depending on who or what is expected to read these messages. Serv-U system variables are supported in this field. This field may be left blank, but usually should not be left blank.

Write to Microsoft Queue (MSMQ)

Microsoft Message Queuing (MSMQ) is an enterprise technology that lets independent applications communicate quickly and reliably. Serv-U MFT Server can send messages to new or existing MSMQ queues whenever a Serv-U event triggers. Corporations can use this feature to tell enterprise applications that files have arrived, files have been picked up, partners have signed on, or many other activities have just occurred.

These events have the following two fields:

- Message Queue Path: The MSMQ path that addresses the queue. Remote queues can be addressed when a full path (for example, `MessageServer\Serv-U Message Queue`) is specified. Local, public queues on the local machine can be addressed when a full path is not specified (for example, `.\Serv-U Message Queue` or just `Serv-U Message Queue`). If the specified queue does not exist, Serv-U will make its best effort to try to create it. (This normally only works on public queues on the local machine.)

Serv-U system variables are supported in this field.

- Message Body: The contents of the message to be sent into the queue. This is normally a text string with a specific format specified by an enterprise application owner or enterprise architect. Serv-U system variables are also supported in this field. This field may be left blank, but usually is not.

Note: Microsoft message queues created in Windows do not grant access to SYSTEM by default, preventing Serv-U from writing events to the queue. In order to correct this, after creating the queue in MSMQ, right-click it, select **Properties**, and then set the permissions so that “SYSTEM” (or the network account under which Serv-U runs) has permission to the queue.

Event Filters

Serv-U Event Filters allow administrators to control to a greater degree when a Serv-U event is triggered. By default, Serv-U Events trigger each time the event occurs. The Event Filter allows events to be triggered only if certain conditions are met. For example, a standard Serv-U Event might trigger an email each time a file is uploaded to the server. However, using an Event Filter, Events can be triggered on a more targeted basis. A File Uploaded event can be configured to only send an email when the file name contains the string `important`, so an email would be sent when the file `Important Tax Forms.pdf` is uploaded but not when random other files are uploaded to the server. Additionally, a File Upload Failed event could be set to run only when the FTP protocol is used, not triggering for failed HTTP or SFTP uploads. This is done by controlling the various variables and values related to the Event and evaluating their results when the event is triggered.

Event Filter Fields

Each Event Filter has the following critical values that must be set:

- Name - This is the name of the filter, used to identify the filter for the event.
- Description (Optional) - This is the description of the event, which may be included for reference.

- Logic - This determines how the filter interacts with other filters for an event. In most cases, AND will be used all filters must be satisfied for the event to trigger. The function of AND is to require that all conditions be met. However, the OR operator can be used if there are multiple possible satisfactory responses (for example, abnormal bandwidth usage of less than 20 KB/s OR greater than 2000 KB/s).
- Filter Comparison - This is the most critical portion of the filter. The Filter Comparison contains the evaluation that must occur for the event to trigger. For example, a filter can be configured so that only the user "admin" triggers the event. In this case, the comparison will be `If $Name = (is equal to) admin`, and the data type will be `string`. For bandwidth, either an "unsigned integer" or "double precision floating point" value would be used.

Event filters also support wildcards when evaluating text strings. The supported wildcards are the following:

- * - The asterisk wildcard matches any text string of any length. For example:
  - An Event Filter that compared the `$FileName` variable to the string `data*` would match files named `data`, `data7`, `data77`, `data.txt`, `data7.txt`, and `data77.txt`.
- ? - The question mark wildcard matches any one character, but only one character. For example:
  - An Event Filter that compared the `$FileName` variable to the string `data?` would match a file named `data7` but not `data`, `data77`, `data.txt`, `data7.txt`, or `data77.txt`.
  - An Event Filter that compared the `$FileName` variable to the string `data?.`* would match files named `data7` and `data7.txt` but not `data`, `data77`, `data.txt`, or `data77.txt`.
  - An Event Filter than compared the `$Name variable` to the string `A????` would match any five-character username starting with `A`.
- [] - The bracket wildcard matches a character against the set of characters inside the brackets. For example:

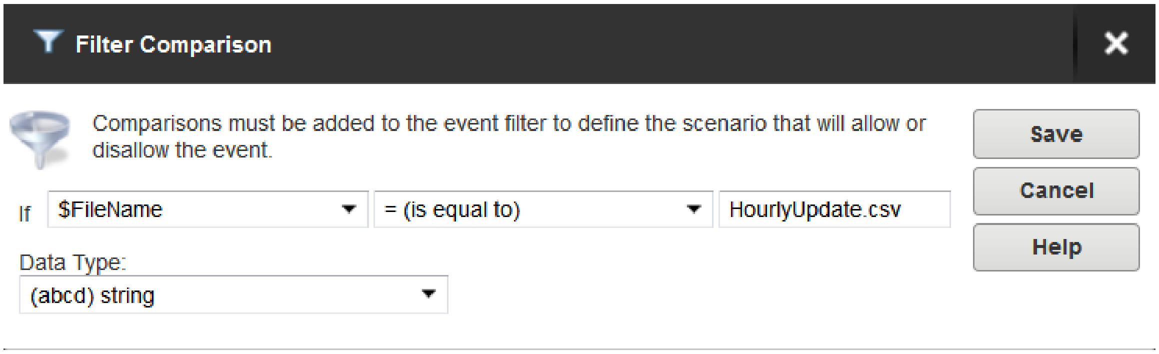
  - An Event Filter that compared the `$FileName` variable to the string `data [687].txt` would match files named `data6.txt`, `data7.txt` and `data8.txt` but not `data5.txt`.
  - An Event Filter that compared the `$LocalPathName` variable to the string `[CD]:\*` would match any file or folder on the `C:` or `D:` drives.

Multiple wildcards can be used in each filter. For example:

- An Event Filter that compared the `$FileName` variable to the string `[cC]:\*.???` would match any file on the `C:` drive that ended in a three letter file extension.
- An Event Filter that compared the `$FileName` variable to the string `?:\*Red [678]\?????.*` would match a file on any Windows drive, contained in any folder whose name contains `Red6`, `Red7` or `Red8`, and that also has a five character file name followed by a file extension of any length.

Using Event Filters

Event filters are used by comparing fields to expected values in the Event Filter menu. The best example is firing an event only when a certain user triggers the action, or when a certain file is uploaded. For example, an administrator may want to fire an email event when the file `HourlyUpdate.csv` is uploaded to the server, but not other files. To do this, a new event can be created in the **Domain Details > Events** menu. The **Event Type** is File Uploaded, and on the Event Filter tab a new filter must be added. The $FileName variable is used and the value is `HourlyUpdate.csv` as shown:



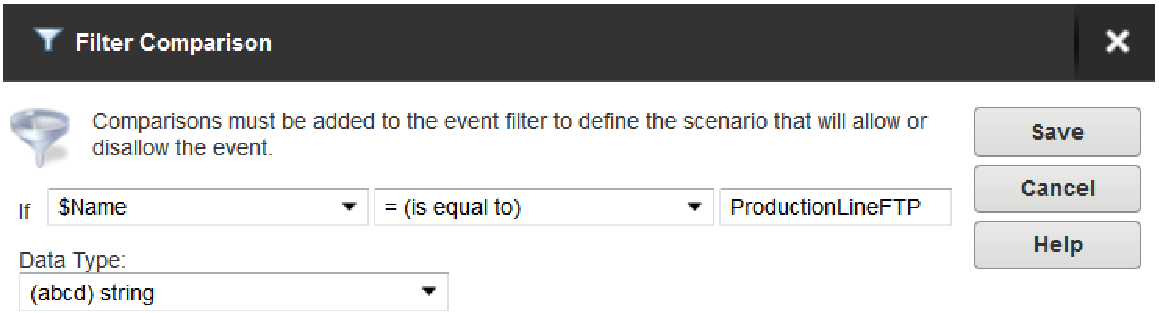
Filter Comparison

Comparisons must be added to the event filter to define the scenario that will allow or disallow the event.

If $FileName = (is equal to) HourlyUpdate.csv

Data Type: (abcd) string

As another example, it might be necessary to know when a file transfer fails for a specific user account (perhaps one used by an automated process). To perform this task, create a new File Upload Failed event, and then add a new filter. The filter comparison will be `$Name`, and the value to compare would be the username, such as `ProductionLineFTP`:

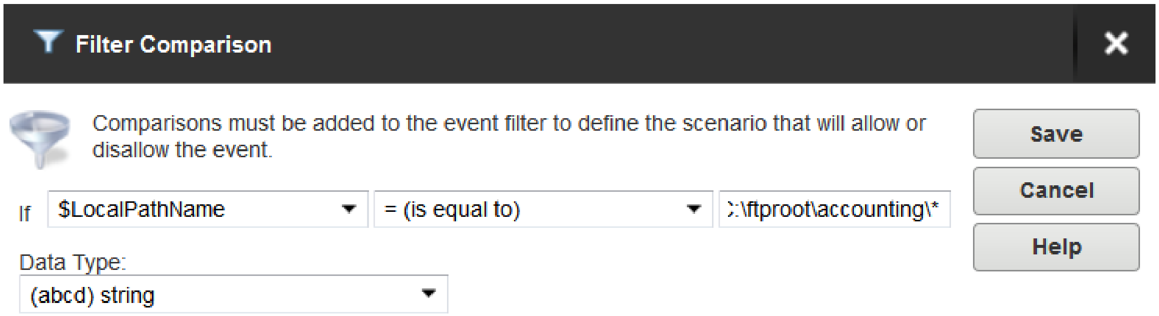


Comparisons must be added to the event filter to define the scenario that will allow or disallow the event.

If $Name = (is equal to) ProductionLineFTP

Data Type: (abcd) string

It is also possible to filter for events based on specific folders, using wildcards. In some cases it may be necessary to trigger events for files uploaded only to a specific folder, such as when an accounting department uploads time-sensitive tax files. To filter based on a folder name, first create a new File Uploaded event in the **Domain Details > Events** menu, and set it to **Send Email**. After specifying the email recipients, subject line, and message content, open the Event Filters tab. Create a new Event Filter, and add the filter comparison `If $LocalPathName = (is equal to) C:\ftproot\accounting\*` with the type of `(abcd) string`. This will cause the event to trigger only for files that are located within `C:\ftproot\accounting\`.



Comparisons must be added to the event filter to define the scenario that will allow or disallow the event.

If $LocalPathName = (is equal to) :\ftproot\accounting\*

Data Type: (abcd) string

Server Details

IP Access Rules

IP Access rules restrict login access to specific IP addresses, ranges of IP addresses, or even a domain name. IP Access rules can be configured at the server, domain, group, and user levels.

IP access rules are applied in the order they are displayed. In this way, specific rules can be placed at the top to allow (or deny) access before a more general rule is applied later on in the list. The arrows on the right side of the list can be used to change the position of an individual rule in the list.

IP Access Masks

IP Access rules use masks to authorize IP addresses and domain names. These masks may contain specific values, ranges and wildcards made up of the following elements.

xxx

An exact match such as `192.168.1.1` (IPv4), `fe80:0:0:0:a450:9a2e:ff9d:a915` (IPv6, long form) or `fe80::a450:9a2e:ff9d:a915` (IPv6, shorthand).

xxx-xxx

A specified range of IP addresses such as `192.168.1.10-19` (IPv4), `fe80:0:0:0:a450:9a2e:ff9d:a915-a9aa` (IPv6, long form), or `fe80::a450:9a2e:ff9d:a915-a9aa` (IPv6, shorthand).

*****

Any valid IP address value such as `192.168.1.*`, which is analogous to `192.168.1.0-255`, or `fe80::a450:9a2e:ff9d:*`, which is analogous to `fe80::a450:9a2e:ff9d:0-ffff`.

?

Any valid character when specifying a reverse DNS name such as `server?.mydomain.com`.

/

The slash separator allows the use of CIDR notation to specify which IP addresses should be allowed or blocked. Common CIDR blocks are `/8 (for 1.*.*.*)`, `/16 (for 1.2.*.*)` and `/24 (for 1.2.3.*)`. CIDR notation also works with IPv6 addresses, such as `2001:db8::/32`.

Caveats

Specific IP addresses listed in Allow rules will not be blocked by anti-hammering. (In other words, they are ‘whitelisted’.) However, addresses matched by wildcard or range will be subject to anti-hammering prevention.

Implicit Deny All

Serv-U assumes that connections from any IP address are valid until you add your first IP access rule. After you add that first IP access rule Serv-U assumes that all connections not explicitly allowed should be denied. This is also known as "an implicit 'Deny All' rule". With this in mind, make sure you add a 'wildcard allow' rule (such as `Allow *.*.*.*`) at the end of your IP Access rule list.

Matching All Addresses

Use a mask of `*.*.*.*` to match any IPv4 address. Use a mask of `*:*` to match any IPv6 address. Remember to add Allow ranges for both IPv4 and IPv6 addresses if you use both IPv4 and IPv6 listeners.

DNS Lookup

If a dynamic DNS service is used, then a domain name can be specified in place of an IP address to allow access to clients that travel and do not have a static IP address. Reverse DNS names are also acceptable. If a domain name or reverse DNS rule is created, Serv-U must perform either a reverse DNS look-up or DNS resolution in order to apply these rules. This can cause a slight delay during login depending on the speed of the system's DNS server.

Rule Use During Connection

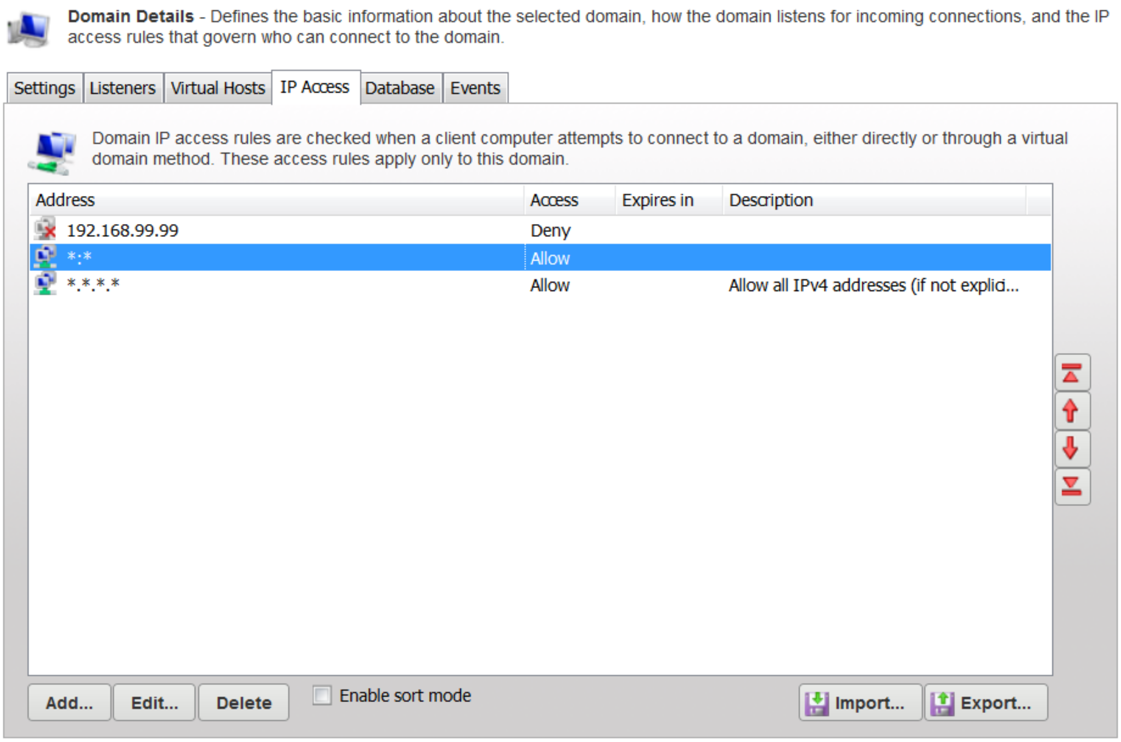
The level at which an IP access rule is specified also defines how far a connection is allowed before being rejected. Server and domain level IP access rules are applied before the Welcome message is sent. Domain level IP access rules are also applied when responding to the HOST command to connect to a virtual domain. Group and user level IP access rules are applied in response to a USER command when the client identifies itself to the server.

Anti-Hammering

Serv-U allows administrators to set up an "anti-hammering policy" that blocks clients who connect and fail to authenticate more than a certain number of times within a certain period of time. These policies can be configured server-wide in **Server Limits and Settings > Server Settings** and domain-wide in **Domain Limits and Settings > Domain Settings**.

IP addresses blocked by anti-hammering rules will appear in your Domain IP Access rules with a value in the **Expires in** column. If you have multiple domains with different listeners, blocked IPs will appear in the domain that contains the listener. (Blocked IP addresses will never appear in the Server IP Access list, even if anti-hammering was set up at the server level.)

The **Expires in** value of the blocked IP will tick down second by second until the entry disappears. You can unblock any blocked IP early by deleting its entry from the list.



Domain Details - Defines the basic information about the selected domain, how the domain listens for incoming connections, and the IP access rules that govern who can connect to the domain.

Domain IP access rules are checked when a client computer attempts to connect to a domain, either directly or through a virtual domain method. These access rules apply only to this domain.

Address	Access	Expires in	Description
192.168.99.99	Deny		
:	Allow		
..*.*	Allow		Allow all IPv4 addresses (if not explici...

IP Access List Controls

Enable Sort Mode

This option allows the IP Access list to be sorted numerically rather than in the processing order. Displaying the IP Access list in sort mode will not change the order in which rules are processed. To view rule precedence disable this option. Viewing the IP Access list in numerical order can be a valuable tool when reviewing long lists of access rules to determine if an entry already exists.

Importing/Exporting IP Access Rules

Serv-U IP Access rules can be imported and exported from users, groups, domains, and the server using a standard text-based comma separated values (CSV) file. To export IP Access rules, view the list of rules to export, and then click **Export**, specifying the path and the file name to save the list to. To import IP Access rules, click **Import** and select the file with the rules

to be imported. The CSV file must contain the following fields, headers included:

-IP - The IP address, IP range, CIDR block, or domain name for which the rule will apply

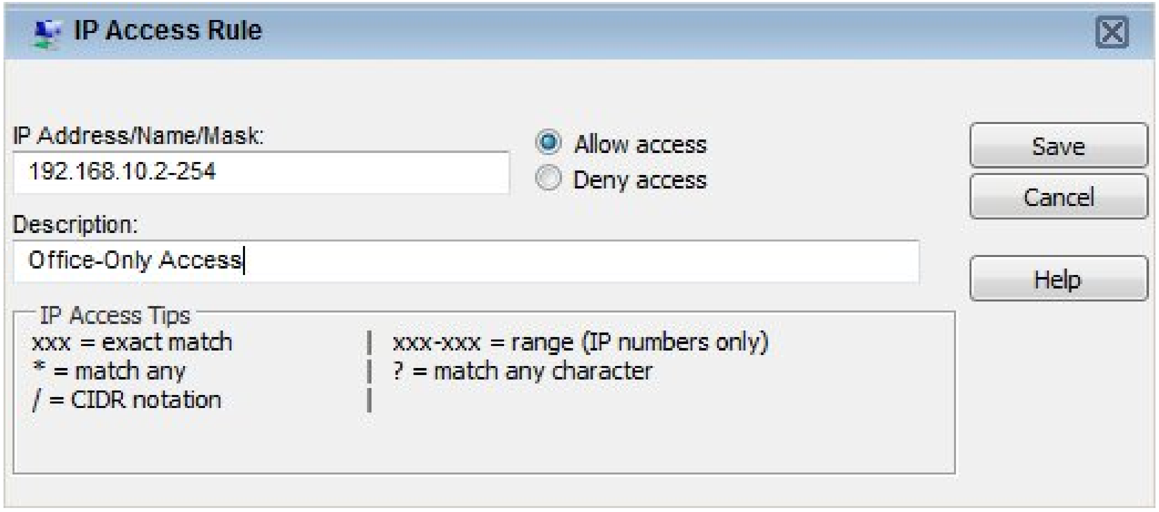
-Allow - Set this value to 0 for Deny, or to 1 for Allow

-Description - A text description of the rule for reference purposes

Examples

Case File - Office-Only Access

A contractor has been hired to work in the office, and only in the office. Office workstations have IP addresses from 192.168.10.2 to 192.168.10.254. The related Serv-U access rule should therefore be `Allow 192.168.10.2-254` (see below), and it should be added to either the contractor's user account or a 'Contractors' group that will contain multiple contractors. (Note that no "Deny" rule is required here because Serv-U provides an implicit 'deny all' at the end of the list.)



IP Address/Name/Mask: 192.168.10.2-254

● Allow access
○ Deny access

Description: Office-Only Access

IP Access Tips
xxx = exact match | xxx-xxx = range (IP numbers only)
* = match any | ? = match any character
/ = CIDR notation |

Case File - Prohibited Machines

Users should normally be able to access Serv-U from anywhere, except from a bank of special internal machines in the IP address range of 192.168.15.100 -

192.168.15.110. The related Serv-U access rules should therefore be `Deny 192.168.15.100-110`, followed by `Allow *.*.*.*`, and these should both be added to either the domain or the server IP Access rules.

Case File - DNS-based Access Control

The only users allowed to access a Serv-U Domain will be connecting from `*.internal.com` or `*.trustedpartner.com`. The related Serv-U access rules should therefore be `Allow *.internal.com` and `Allow *.trustedpartner.com` (in any order) and these should both be added to the domain IP Access rules. (Note that no "Deny" rule is required here because Serv-U provides an implicit 'deny all' at the end of the list.)

Limits and Settings

Serv-U offers advanced options which can be used to customize how it may be used as well as ways to apply limits and custom settings to Users, Groups, Domains, and the Server in its entirety. The limits stack intelligently, with user settings overriding group settings, group settings overriding domain settings, and domain settings overriding server settings. In addition, limits can be applied only during certain days of the week or times of the day. It is possible to grant exceptions to administrators and restrict specific users more than others, providing total control over the server. The Limits and Settings in Serv-U are split into the following categories:

- Connection
- Password
- Directory Listing
- Data Transfer
- HTTP
- Email

- File Sharing
- Advanced

To apply a limit, select the appropriate category, click **Add**, select the limit, and then select or enter the value. For example, to disable the **Lock users in home directory** option for a Domain, follow these steps:

- Select **Domain > Domain Limits & Settings** from the Serv-U Management Console.
- Select **Directory Listing** from the **Limit Type** list.
- Click **Add**.
- Select **Lock users in home directory** from the **Limit** list.
- Deselect the option.
- Click **Save**.

The limits list displays the current limits applied to the domain. Limits with a light-blue shade to the background are default values. Limits with a white background are values that override the defaults. After completing the above steps, a new **Lock users in home directory** limit appears in the list that displays "No" for the value. Because of inheritance rules, this option applies to all users in the domain unless overridden at the group or user level. For more information about this method of inheritance, see "User Interface Conventions".

Limits can be deleted by selecting them and clicking **Delete**. To edit an overridden value, select the limit, and then click **Edit**. Default rules cannot be edited or deleted. Create a new limit to override a default one.

To create a limit that is restricted to a specific time of day or days of the week, click **Advanced** from the New / Edit Limit dialog. The additional options allow you to Apply limit only at this time of day at which point a start and stop time for the new limit can be entered. To restrict the limit to certain days of the week, deselect the days for which you do not want to apply the limit. When a limit is restricted in this way, default values (or the value of other limit overrides) are applied when the time of day or day of the week restrictions are not met for this limit.

The following is a reference of all available group limits, organized by category.

Connection

Maximum number of sessions for group

Specifies the maximum number of concurrent sessions that may be allowed for all Users that are a member of the Group.

Maximum sessions per IP address for group

Specifies the maximum number of concurrent sessions that may be opened from a single IP address for all Users of the Group.

Maximum number of sessions per user account

Specifies the maximum number of concurrent sessions that may be opened from a single User account.

Maximum sessions per IP address for user account

Specifies the maximum number of concurrent sessions that a User may open from a single IP address.

Require secure connection before login

Requires that a connection be secure, (for example, FTPS, SFTP, or HTTPS), before it is accepted.

Automatic idle connection timeout

Specifies the number of minutes that must pass after the last client data transfer before a session is disconnected for being idle.

Note: Setting the Packet time-out is a requirement for this limit to work. The value of Packet time-out must be less than the value of the Automatic idle connection timeout for the Automatic idle connection timeout to work properly. For information about setting the packet time-out, see "Server Settings".

Automatic session timeout

Specifies the number of minutes a session is allowed to last before being disconnected by the server.

Block anti-timeout schemes

Blocks the use of commands such as "NOOP", which is commonly used to keep FTP Command Channel connections open during long file transfers or other periods of inactivity where no information is being transferred on the control channel. When these are blocked, Serv-U disconnects the client when the connection has been idle, that is, not transferring data, for a specified period of time.

Block IP address of timed out session

Specifies the number of minutes for which the IP address of a timed out session is blocked.

Allow FTP and FTPS connections

Allows the user to connect using the FTP and FTPS protocols. Deselect **Allow FTP and FTPS connections** to disable the FTP and FTPS protocols.

Allow SFTP connections

Allows the user to connect using the SFTP protocol. Deselect **Allow SFTP connections** to disable the SFTP protocol.

Allow HTTP and HTTPS connections

Allows the user to connect using the HTTP and HTTPS protocols. Deselect **Allow HTTP and HTTPS connections** to disable the HTTP and HTTPS protocols.

Password

Require complex passwords

Specifies that all user account passwords must contain at least one uppercase and one non-alphabetic character to be considered valid.

Minimum password length

Specifies the minimum number of characters required in a user account's password. Specifying 0 characters indicates that there is no minimum requirement.

Automatically expire passwords

Specifies the number of days a password is valid before it must be changed. Specifying 0 days means passwords never expire.

Allow users to change password

Specifies whether or not Users are allowed to change their own passwords.

Mask received passwords in logs

Masks the passwords received from clients from being shown in log files. Disabling this allows passwords to be displayed in log files, which can be useful for debugging connection problems or auditing User account security.

SSH authentication type

Specifies how SSH authentication is to occur. Options include: **Password and Public Key** - requires both a password and a public key (when specified) for login; **Password or Public Key** - requires either a password or public key for login; "Public Key Only" - requires that a public key is provided for successful login, a password is not allowed; **Password Only** - requires that a password is provided for successful login, a public key is not allowed.

Allow users to recover password

If enabled, this limit allows users to recover passwords using the Web Client password recovery utility at the login page.

FTP Password Type

All passwords are stored in an encrypted, irreversible state in Serv-U's configuration files (unless the File Server is configured to not encrypt stored passwords through a password limit). In addition to the **Regular Password** option, two additional types of password storage are available for accounts that use the FTP protocol: **MD4** and **MD5 OTP S/KEY** passwords. This type of password setting allows the user to login via FTP without sending the password to the File Server as plain text. These options only apply to the FTP protocol. Setting this option does not affect a user's ability to login via other protocols.

Days before considering password to be stale

The number of days prior to expiration that a password is to be considered "stale". A stale password is a password that is about to expire. An event can be configured to identify when a password is about to expire. This value is the lead-time, in days, before password expiration.

Directory Listing

Hide files marked as hidden from listings

Hides files and folders from directory listings that have the Windows "hidden" system attribute set on them.

Use lowercase for file names and directories

Forces Serv-U to display all file names and directories using lowercase characters, regardless of the actual letter case in use by the file or directory.

Interpret Windows shortcuts as links

Instructs Serv-U to treat all valid .lnk files as the actual destination object. In other words, if a .lnk file points to another file, the destination file is shown in the directory listing instead of the .lnk file itself.

Treat Windows shortcuts as target in links

Instructs Serv-U to treat all valid .lnk (shortcut) files as a UNIX symbolic link.

Allow root ("/") to list drives for unlocked users (Windows Only)

Allows Users to change directory to the root ("/") of the system and display all drives on the computer. This option only works when the User is not locked in their home directory.

Hide the compressed state of files and directories

Hides the compressed state of all compressed files and directories being viewed by the user.

Hide the encrypted state of files and directories

Hides the encrypted state of all encrypted files and directories being viewed by the user.

Data Transfer

Maximum upload speed for all group members

Limits the maximum total bandwidth that can be used by all members of the group for all uploads. Setting a limit of 0 KB/s means unlimited bandwidth.

Maximum download speed for all group members

Limits the maximum total bandwidth that can be used by all members of the group for all downloads. Setting a limit of 0 KB/s means unlimited bandwidth.

Maximum upload speed per session

Limits the maximum upload bandwidth for each individual session. Setting a limit of 0 KB/s means unlimited bandwidth.

Maximum download speed per session

Limits the maximum download bandwidth for each individual session. Setting a limit of 0 KB/s means unlimited bandwidth.

Maximum upload speed for user accounts

Limits the maximum upload bandwidth shared between all sessions associated with an individual user account. Setting a limit of 0 KB/s means unlimited bandwidth.

Maximum upload file size

Restricts the maximum single file size a user can upload to Serv-U. File size measured in kilobytes.

Maximum download speed for user accounts

Limits the maximum download bandwidth shared between all sessions associated with an individual user account. Setting a limit of 0 KB/s means unlimited bandwidth.

Delete partially uploaded files

Instructs Serv-U to delete incomplete file uploads. If this option is enabled, users are not able to restart interrupted uploads using the REST (Restart) FTP command.

Interpret line feed byte as a new line when in ASCII mode (Windows Only)

When uploading and downloading files using ASCII mode, Serv-U will assume <LF> characters are the same as <CR><LF> end-of-line markers. Most Windows applications expect <CR><LF> to represent a new-line, as does the FTP protocol. However, since the definition of a new-line sequence is not fully defined in Windows, this option allows Serv-U to assume <LF> is the same as <CR><LF>. When uploading in ASCII mode stand-alone <LF> characters are changed to <CR><LF> prior to writing to the file. When downloading in ASCII mode, stand-alone <LF> characters are changed to <CR><LF> prior to sending to the client.

HTTP

Allow HTTP media playback

The Serv-U Web Client supports fully interactive media playback of audio and video files. This function can be disabled as desired during specific business hours or altogether based on business needs.

Allow users to use Web Client

Serv-U Web Client is enabled by default. Administrators may disallow the use of Serv-U Web Client by disabling this limit.

Allow users to use Web Client Pro

Serv-U Web Client Pro is enabled by default. Administrators may disallow the use of Serv-U Web Client Pro by disabling this limit.

Allow users to use FTP Voyager JV

FTP Voyager JV is enabled by default. Administrators may disallow the use of FTP Voyager JV by disabling this limit.

Default language for Web Client

When the end-user connects with an unsupported language, the HTTP Login Page is displayed in English. The default language can be set to any desired language. When connecting to Serv-U using a supported localization of Windows, the native language of Windows is used.

Allow browsers to remember login information

The HTTP login page supports a "Remember me" option (not enabled by default) that allows usernames to be remembered by the login page. This feature can be disabled for security reasons.

Allow users to change languages

The Serv-U Web Client is supported in many languages, but if users should not be able to select their native language this can be disabled.

Maintain file dates and times after uploading (FTP Voyager JV and Web Client Pro only)

When enabled, Serv-U can maintain the last modification date and time of the file when end-users are using FTP Voyager JV or Web Client Pro. When disabled, Serv-U will not set the file's last modification date and time, it will remain the date and time the file was uploaded.

Allow HTTP sessions to change IP address (disabling may cause mobile devices to fail)

The Serv-U Web Client supports the transfer of HTTP sessions if the IP address changes. This option can be disabled but it may cause mobile devices to be disconnected due to frequent IP address changes by these devices.

File Sharing

Require a password for guest access

Specifies whether it is possible to set up a file share where the guest is required to provide a password. When this limit is set to Always or Never, the creator of the file share will not be able to specify this optional setting.

When this limit is set to Optional, the user can individually specify in each file share whether or not the guest must provide a password.

Insert passwords within invitation emails

Specifies whether it is possible to set up a file share where the password for the share is included in the invitation email. When this limit is set to Always or Never, the creator of the file share will not be able to specify this optional setting. When this limit is set to Optional, the **Include the password in the email** option can be selected individually in each file share.

Maximum file size guests can upload (per file)

Specifies the file size constraints imposed upon the guest user. If set to 0, there is no file size constraint. In this case, the creator of the file share request can specify the maximum file size in each file share request without an upper limit.

Allow user-defined guest link expiration

When enabled, users will be able to specify link expiration dates individually on the Request Files and Send Files wizards. When disabled, the file share links will expire after the number of days specified in the **Duration before guest link expires** limit.

Duration before guest link expires

Limits the number of days after which a file share link expires if the Allow user-defined guest link expiration limit is disabled.

Notify user after a file is downloaded

Specifies whether the **Notify me when the file(s) have been downloaded** option can be used on the Send Files wizard. When this limit is set to Always or Never, the creator of the file share will not be able to specify this optional setting. When this limit is set to Optional, the user can individually specify in each file share whether to receive notification of the file download.

Notify user after a file is uploaded

Specifies whether the **Notify me when the file(s) have been uploaded** option can be used on the Request Files wizard. When this limit is set to

Always or Never, the creator of the file share request will not be able to specify this optional setting. When this limit is set to Optional, the user can individually specify in each file share request whether to receive notification of the file upload.

Send the guest access link to the recipients

Specifies whether the **Automatically send the download/upload link to the guest user(s) in email** option can be used on the Send Files and Request Files wizard. When this limit is set to Always or Never, the user will not be able to specify this optional setting. When this limit is set to Optional, the user can individually specify in each file share or file share request whether to send the access link automatically.

Send the guest access link to the sender

Specifies whether the **Send me an email copy with the download/upload link** option can be used on the Send Files and Request Files wizard. When this limit is set to Always or Never, the user will not be able to specify this optional setting. When this limit is set to Optional, the user can individually specify in each file share or file share request whether to receive an email copy with the download/upload link.

Allow file sharing

Specifies whether the user is allowed to use file sharing.

Allow user-defined contact information

When enabled, users will be able to edit their name and email address on the Request Files and Send Files wizards. When disabled, users are not allowed to edit their contact information on the Request Files and Send Files wizards.

Maximum number of files for "Sent" shares

Specifies the maximum number of files users can include in a single file share. If set to 0, the default limit of 20 is used.

Maximum number of files for "Requested" shares

Specifies the maximum number of files users can upload after receiving a file share request. If set to 0, the default limit of 20 is used.

Advanced

Convert URL characters in commands to ASCII

Instructs Serv-U to convert special characters contained in command parameters to plain ASCII text. Certain Web browsers can encode special characters contained in file names and directories when using the FTP protocol. This attribute allows Serv-U to decode these special characters.

Maximum Supported SFTP Version

Specifies the maximum verison of SFTP permittted for SFTP connnections. Serv-U supports SFTP versions 3-6.

Automatically check directory sizes during upload

Instructs Serv-U to occasionally check the size of directories in which a maximum directory size has been specified. This attribute ensures that Serv-U always has updated directory sizes available instead of having to calculate them at transfer time, which can be a time consuming operation.

Allow Rename Overwrite

When enabled (default) Serv-U allows files to be renamed to files where the destination already exists. When disabled users are not allowed to rename a file or directory to a path name that already exists.

Apply server and domain directory access rules before user and group

The order in which Directory Access Rules are listed has significance in determining the resources that are available to a User or Group account. By default, Directory Access Rules specified at the Group or User level take precedence over ones specified at the Domain and Server level. However, there are certain instances where you may want the Domain and Server level rules to take precedence. Setting this value to "Yes" places the Group's and User's Directory Access Rules *below* the Server and Domain.

Please also reference the "Apply group directory access rules first" setting which is outlined on Group Information.

Days before automatically disabling account to trigger the pre-disable event

The number of days prior to automatically disabling the user account that the pre-disable event should be triggered.

Days before automatically deleting account to trigger the pre-delete event

The number of days prior to automatically deleting the user account that the pre-delete event should be triggered.

Reset user stats after restart

When this limit is enable the user stats are reset after a server restart.

Reset group stats after restart

When this limit is enable the group stats are reset after a server restart.

Owner ID (user name) for created files and directories (Linux Only)

The user name given to set as owner of a created file or directory.

Group ID (group name) for created files and directories (Linux Only)

The group name given to set as owner of a created file or directory.

Ratio Free Files

Files listed in the ratio free file list are exempt from any imposed transfer ratios. In other words, if a user must upload files in order to earn credits towards downloading a file, a file that matches an entry in this list can always be downloaded by users, even if they have no current credits. This is commonly used to make special files, such as a "read me" or a directory information file, always accessible by users.

The '*' and '?' wildcard characters may be used when specifying a ratio free file. Using '*' specifies a wildcard of any kind of character and any length. For example, entering `*.txt` makes any file with a .txt extension free for download, regardless of the actual filename. A '?' may be used to represent a single character within the filename or directory. Finally, full paths can be specified using standard directory paths like `C:\ftproot\common\` (in Windows) or `/var/ftpfiles/shared/` (in Linux).

In addition, full or relative paths may be used when making an entry. If a full path is used when specifying a filename, then only that specific file is exempt from transfer ratios. If a relative path is used, such as entering just `readme.txt`, then the provided file is exempt from transfer ratios regardless of the directory it is located in.

SFTP (Secure File Transfer over SSH2) for Users and Groups

Using an Existing Public Key

1. Obtain a public key file.
2. Place the public key file in a secured directory in the server, and then use **Browse** in Serv-U to select the file.
3. Click **Save**.

Creating a Key Pair

1. Click **Manage Keys**.
2. Click **Create Key**.
3. Type the name of the key pair (for example, `MyKey`), which is also used to name the storage file.
4. Type the output directory of the certificate (for example, `C:\ProgramData\RhinoSoft\Serv-U\`).
5. Select the Key Type (default of DSA is preferred, but RSA is available).
6. Select the Key Length (default of 1024 bits provides best performance, 2048 bits is a good median, while 4096 bits provides best security).
7. Enter the password to use for securing the key file.
8. Click **Create**.

Creating Multiple Keys Per User

For the purposes of public key authentication, you can associate multiple public keys with a user account.

To create multiple keys for an account:

1. Click **Manage Keys**.
2. Click **Add Key**, and then specify the Key Name and the Key Path.

When authenticating a client, Serv-U will check all the keys you provide here. If authenticating against one key fails, Serv-U proceeds to check the next key.

Chapter 7: System Variables

Certain configurable messages in Serv-U can be customized to include a wide range of variables as outlined in the list below. These variables are replaced at run-time with the appropriate value allowing up-to-date statistics and feedback to be provided to logged in Users. Some of the places where these variables can be used include event messages, customized FTP command responses, or a welcome message.

Furthermore, the `&#37;USER&#37;`, `&#37;HOME&#37;`, `&#37;USER_FULL_NAME&#37;`, and `&#37;DOMAIN_HOME&#37;` variables are also available. For more information about these variables, see "Directory Access Rules".

All variables are case sensitive. Statistical information, unless otherwise specified, is calculated since the Serv-U File Server was last started.

Server Information

- $ServerName - The full name of the server (that is, Serv-U)
- $ServerVersionShort - The first two digits of the current version of the Serv-U File Server (for example, 12.0)
- $ServerVersionLong - The full version number of the Serv-U File Server (for example, 12.0.0.1)
- $OS - The name of the operating system (for example, Windows Server 2008 R2)
- $OSVer - The full version number of the operating system (for example, 6.1.7601)
- $OSAndPlatform - The name of the operating system (for example, Windows Server 2008 R2) and platform (for example, 32-bit or 64-bit)
- $OSCaseSensitive - States if the operating system is case sensitive

- $ComputerName - The name of the computer retrieved from the operating system, normally the same as the UNC name on a Windows network (for example, WEB-SERVER-01)
- $EventName - Contains the configured name of the event
- $EventType - Contains the type of the event that was triggered
- $EventDescription - Contains the configured description of the event
- $LogFilePath - Retrieves the path to the log file (Log File Deleted and Log File Rotated Events only)
- $OldLogFilePath - Retrieves the old path to the log file (Log File Rotated Events only)
- $GatewayIPAddress - Retrieves the Gateway IP address (Gateway Listener Success, Gateway Listener Failure, Permanent Gateway Listener Success, Permanent Gateway Listener Failure Events only)
- $GatewayPort - Retrieves the Gateway port (Gateway Listener Success, Gateway Listener Failure, Permanent Gateway Listener Success, Permanent Gateway Listener Failure Events only)
- $ListenerIPAddress - Retrieves the listener IP address (Listener Success, Listener Failure, Permanent Listener Success, Permanent Listener Failure Events only)
- $ListenerPort - Retrieves the listener port (Listener Success, Listener Failure, Permanent Listener Success, Permanent Listener Failure Events only)
- $ListenerType - Retrieves the listener type (Listener Success, Listener Failure, Permanent Listener Success, Permanent Listener Failure Events only)
- $ListenResult - Retrieves the listener result (Listener Success, Listener Failure, Permanent Listener Success, Permanent Listener Failure Events only)

Server Statistics

- $ServerDays - The total number of days the Server has been online continuously
- $ServerHours - The number of hours from 0 to 24 the Server has been online, carries over to $ServerDays
- $ServerMins - The number of minutes from 0 to 60 the Server has been online, carries over to $ServerHours
- $ServerSecs - The number of seconds from 0 to 60 the Server has been online, carries over to $ServerMins
- $ServerKBup - The total number of kilobytes uploaded
- $ServerKBdown - The total number of kilobytes downloaded
- $ServerFilesUp - The total number of files uploaded
- $ServerFilesDown - The total number of files downloaded
- $ServerFilesTot - The total number of files transferred, essentially ($ServerFilesUp + $ServerFilesDown)
- $LoggedInAll - The total number of established sessions
- $ServerUploadAvgKBps - The average upload rate in KB/s
- $ServerDownloadAvgKBps - The average download rate in KB/s
- $ServerAvg - The average data transfer rate (uploads and downloads) in KB/s
- $ServerUploadKBps - The current upload transfer rate in KB/s
- $ServerDownloadKBps - The current download transfer rate in KB/s
- $ServerKBps - The current aggregate data transfer rate in KB/s
- $ServerSessions24HPlusOne - The total number of sessions in the past 24 hours plus one additional session
- $ServerSessions24H - The total number of sessions in the past 24 hours

Domain Statistics

- $DomainKBup - The total number of kilobytes uploaded
- $DomainKBdown - The total number of kilobytes downloaded
- $DomainFilesUp - The total number of files uploaded
- $DomainFilesDown - The total number of files downloaded
- $DomainFilesTot - The total number of files transferred, essentially ($DomainFilesUp + $DomainFilesDown)
- $DomainLoggedIn - The total number of sessions currently connected
- $DomainUploadAvgKBps - The average upload rate in KB/s
- $DomainDownloadAvgKBps - The average download rate in KB/s
- $DomainAvg - The average aggregate data transfer rate (uploads and downloads) in KB/s
- $DomainUploadKBps - The current upload transfer rate in KB/s
- $DomainDownloadKBps - The current download transfer rate in KB/s
- $DomainKBps - The current aggregate data transfer rate in KB/s
- $DomainSessions24HPlusOne - The total number of sessions in the past 24 hours plus one additional session
- $DomainSessions24H - The total number of sessions in the past 24 hours

User Statistics - Applies to all sessions attached to the User account

- $UserKBUp - The total number of kilobytes uploaded
- $UserKBDown - The total number of kilobytes downloaded
- $UserKBTot - The total amount of kilobytes transferred
- $UserLoggedIn - The total number of sessions
- $UserUploadAvgKBps - The average upload rate in KB/s
- $UserDownloadAvgKBps - The average download rate in KB/s

- $UserAvg - The average aggregate data transfer rate (uploads and downloads) in KB/s
- $UserUploadKBps - The current upload transfer rate in KB/s
- $UserDownloadKBps - The current download transfer rate in KB/s
- $UserKBps - The current aggregate data transfer rate in KB/s
- $UserSessions24HPlusOne - The total number of sessions in the past 24 hours plus one additional session
- $UserSessions24H - The total number of sessions in the past 24 hours

Last Transfer Statistics - Applies to the most recently completed successful data transfer

- $TransferBytesPerSecond - The effective (compressed) transfer rate in bytes/s
- $TransferKBPerSecond - The effective (compressed) transfer rate in KB/s
- $TransferBytes - The effective (compressed) number of bytes transferred, formatted for display, for example, 32,164
- $NoFormatTransferBytes - The effective (compressed) number of bytes transferred, unformatted, for example, 32164
- $TransferKB - The effective (compressed) number of kilobytes transferred, formatted for display
- $ActualTransferBytesPerSecond - The actual (uncompressed) transfer rate in bytes/s
- $ActualTransferKBPerSecond - The actual (uncompressed) transfer rate in KB/s
- $ActualTransferBytes - The actual (uncompressed) number of bytes transferred, formatted for display, for example, 32,164
- $NoFormatActualTransferBytes - The actual (uncompressed) number of bytes transferred, unformatted, for example, 32164

- $ActualTransferKB - The actual (uncompressed) number of kilobytes transferred, formatted for display
- $CompressionRatio - The ratio of compression for the transfer expressed as a percentage of the expected amount of data transfered. For example, a value of 100.00 means the data could not be compressed. A value of 200.00 means the data compressed to half its original size.
- $CommandResult - The command result in any command's return response providing information like compression level, and so on. (FTP only)
- $Command - The FTP command name, such as RETR, MODE, or SIZE (FTP only)
- $Parameters - The parameters used for the command, such as "Z" for the MODE command indicating the compression type, a file name for the STOR command, and so on. (FTP only)
- $DataMode - The data transfer mode for an FTP data transfer, which may be either BINARY for binary mode transfers or ASCII for ASCII mode data transfers (FTP only)
- $CurrentCompressedTransferBytes - The current effective (compressed) number of bytes transferred so far, unformatted, e.g., 32164 (FTP only)
- $CurrentUncompressedTransferBytes - The current actual (uncompressed) number of bytes transferred so far, unformatted, for example, 32164 (FTP only)

Date/Time

- $Date - The current date according to the Serv-U File Server, in the system's local date format
- $Time - The current time according to the Serv-U File Server, in the system's local time format
- $Day - Day of the month
- $Month - Two-digit numeric month

- $TextMonth - Text version of the month
- $Year - Four-digit year
- $2DigitYear - Two-digit year
- $Hour - Hour (24-hour clock)
- $Minute - Minute
- $Second - Second

Server Settings

- $MaxUsers - The maximum number of sessions allowed to log in, which could be limited by the license
- $MaxAnonymous - The maximum number of anonymous users allowed to log in

Session Information - Applies to the current session

- $Name - The login ID of the attached User account
- $LoginID - The session's login ID, operates like $Name. $Name can refer to the login ID for target user accounts but $LoginID refers only to the login ID of the session.
- $IP - The client IP address
- $IPName - The reverse DNS name as obtained by performing a reverse DNS lookup on $IP
- $Dir - The session's current directory
- $Disk - The local drive letter being accessed
- $DFree - The amount of free space on $Disk in MB
- $FUp - The total number of files uploaded
- $FDown - The total number of files downloaded
- $FTot - The total number of files transferred, essentially ($FUp + $FDown)

- $BUp - The total number of kilobytes uploaded
- $Bdown - The total number of kilobytes downloaded
- $BTot - The total number of kilobytes transferred
- $TConM - The total number of minutes the session has been connected
- $TConS - The number of seconds from 0 to 60 that the session has been connected, carries over to $TconM
- $RatioUp - The 'upload' portion of the applied ratio, "N/A" if not in use
- $RatioDown - The 'download' portion of the applied ratio, "N/A" if not in use
- $RatioType - The type of ratio being applied, either per session or per User
- $RatioCreditType - The type of ratio credit granted for transfers, either per bytes or per complete file
- $RatioCredit - The current transfer credit for the applied ratio, either megabytes or complete files
- $QuotaUsed - Displays how much disk quota is currently being used in MB, "Unlimited" if no quota is in use
- $QuotaLeft - Displays how much disk quota is available in MB, "Unlimited" if no quota is in use
- $QuotaMax - Displays the maximum amount of disk space that can be used in MB, "Unlimited" if no quota is in use
- $CurrentDirMaxSize - Displays the maximum size of the current directory in MB. If the directory has no size limit, the variable will return "unlimited". If permission is denied in the directory, or any other error occurs, the value "N/A" will be returned.
- $SessionID - The unique session ID of the current session. Session IDs are counted from 000001, and the counter is reset each time Serv-U is started.
- $Protocol - The current protocol being used (FTP, FTPS, HTTP, HTTPS, or SFTP (SSH2))

- $UserDomainName - Uses either the logged in domain name or the user's parent domain name. A blank name is returned if the user is a global server user that is not logging in
- $DomainName - The current domain that the session is logged into
- $DomainDescription - The description of the current domain that the session is logged into
- $TimeRemaining - The time remaining when blocking an IP address for an amount of time (available only in Event notifications)
- $LocalHomeDirectory - The local home directory. It should only be used for events that need this specific information such as user creation.
- $Password - The password associated with the user account. It is intended only for events. It should NOT be used for welcome messages.
- $UserEmailAddress - The user's email address.
- $FullName - The user's full name as entered into the "Full Name" field for a user account.
- $SpaceFullName - The same as "$FullName" with the addition of a space before the user's full name. Blank (no space or name) when the user's full name is empty.
- $FullNameSpace - The same as "$FullName" with the addition of a space after the user's full name. Blank (no space or name) when the user's full name is empty.
- $Port – The client's port number.
- $ServerIP – The server's IP address.
- $ServerPort – The server's port number.

Note: Using the $IPName variable inside of an event or sign-on message can cause a slight delay while the reverse DNS information for $IP is retrieved.

File Information - Applies to the last remotely accessed file, which is not necessarily the last transferred file

- $PathName - Retrieves the full remote path
- $FileName - Retrieves just the file name from $PathName
- $FileSize - Retrieves the size, in bytes, of the file from $FileName
- $FileSizeFmt - A formatted version of the file size, containing the thousands separator (comma or period depending on the computer's regional settings)
- $FileSizeKB - A formatted floating point value representing the file size in KB
- $LocalPathName - Retrieves the fully qualified local path name for an operation, as it relates to Windows. For example `C:\Temp\File.fid` instead of `/Temp/file.fid`
- $LocalFileName - Retrieves the name of the file as it is stored on the local computer. See $LocalPathName for details
- $OldLocalPathName - Same as $LocalPathName, but contains the path prior to renaming
- $OldLocalFileName - Same as $LocalFileName, but contains the file name prior to renaming
- $OldPathName - Retrieves the remote path name prior to renaming
- $OldFileName - Retrieves the remote file name prior to renaming

Current Activity

- $UNow - The current number of sessions on the Serv-U File Server
- $UAll - The total number of sessions that have connected to the Serv-U File Server since it was last started
- $U24h - The total number of sessions that have connected to the Serv-U File Server in the last 24 hours

- $UAnonAll - The current number of sessions attributed to the anonymous user on the Serv-U File Server
- $UAnonThisDomain - The current number of sessions attributed to the anonymous user on the connected Domain
- $UNonAnonAll - The current number of sessions not attributed to the anonymous user on the Serv-U File Server
- $UNonAnonThisDomain - The current number of sessions not attributed to the anonymous user on the connected Domain
- $UThisName - The current number of sessions attributed to the connected User account