



ADMINISTRATOR GUIDE

# Serv-U File Server

Version 15.2

© 2020 SolarWinds Worldwide, LLC. All rights reserved.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of SolarWinds. All right, title, and interest in and to the software, services, and documentation are and shall remain the exclusive property of SolarWinds, its affiliates, and/or its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SolarWinds, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.

# Table of Contents

<b>Introduction to the SolarWinds Serv-U File Server</b>	<b>7</b>
<b>Serv-U glossary</b>	<b>10</b>
<b>Serv-U Editions</b>	<b>13</b>
<b>Serv-U Purchase options</b>	<b>14</b>
<b>The Serv-U Management Console</b>	<b>15</b>
Serv-U user interface conventions	16
<b>Create a Serv-U domain</b>	<b>17</b>
<b>Add a Serv-U user</b>	<b>19</b>
View and add users at the global level	19
Add a user using the wizard	20
Add a User manually	22
Advanced settings	27
The User Template	28
Edit a User	28
Copy a User	28
User collections (MFT only)	28
Recovering passwords	29
<b>Add a Serv-U group</b>	<b>30</b>
Add a Group	30
Advanced settings	35
Edit a Group	36
The Group Template	36
<b>Serv-U settings</b>	<b>37</b>
<b>Serv-U global level settings</b>	<b>38</b>
The Serv-U global dashboard	39

Serv-U server details .....	42
Serv-U global users .....	62
Serv-U groups .....	73
Serv-U global directories .....	80
Serv-U server limits and settings .....	89
Serv-U server activity .....	105
<b>Serv-U domain level settings .....</b>	<b>112</b>
Serv-U domain details .....	112
Serv-U domain users .....	133
Serv-U groups .....	146
Domain Directories .....	155
Domain Limits & Settings .....	164
Domain activity .....	179
<b>Group properties .....</b>	<b>186</b>
Group Properties: Group Information .....	187
Group Properties: Directory Access .....	191
Group Properties: Virtual Paths .....	197
Group Properties: Logging .....	198
Group Properties: Members .....	200
Group Properties: Events .....	200
Group Properties: IP Access .....	210
Serv-U group properties: limits & settings .....	213
<b>User properties .....</b>	<b>215</b>
User Properties: User Information .....	216
User Properties: Directory Access .....	222
User Properties: Virtual Paths .....	227
User Properties: Logging .....	229

Serv-U User Properties: Groups .....	231
User Properties: Events .....	232
User Properties: IP Access .....	242
Serv-U user properties: limits & settings .....	245
<b>Common topics .....</b>	<b>247</b>
Access rule examples and caveats .....	247
SMTP configuration for the Serv-U File Server .....	248
New SSH Key Pair creation .....	250
Transfer Ratio, Quota Management, and Ratio free files .....	254
<b>Compare Windows Active Directory and LDAP authentication .....</b>	<b>258</b>
Differences between Windows Active Directory and LDAP authentication .....	258
Configure Windows and LDAP authentication .....	258
Configure Windows and LDAP authentication .....	259
Keep Serv-U updated .....	259
Windows Authentication (MFT only) .....	259
LDAP authentication (MFT only) .....	260
Domain User and Group Statistics .....	273
<b>Serv-U File Sharing .....</b>	<b>275</b>
The Serv-U File Sharing console .....	275
Serv-U file sharing: View All .....	276
Serv-U file sharing: the Send Files wizard .....	277
Serv-U file sharing: the Request Files wizard .....	280
Serv-U file sharing: Share details .....	282
<b>The Serv-U Web Client .....</b>	<b>283</b>
Web Client layout .....	284
Manage directories .....	286
Manage files .....	287

Thumbnails, slideshows, and the media player .....	289
Web Client Pro .....	290
<b>Serv-U FTP Voyager JV (MFT only) .....</b>	<b>296</b>
FTP Voyager help .....	297
<b>The Serv-U Gateway .....</b>	<b>298</b>
Gateway deployment documentation .....	299
The Gateway tab in Serv-U .....	299
Manage Gateways .....	300
Gateway properties dialog .....	300
<b>System variables .....</b>	<b>301</b>
Server information .....	302
Server statistics .....	304
Domain statistics .....	305
User statistics .....	305
Last transfer statistics .....	306
Date/Time .....	307
Server settings .....	308
Session information .....	308
File information .....	311
Current activity .....	311
FileShare .....	312

# Introduction to the SolarWinds Serv-U File Server

The SolarWinds Serv-U File Server (Serv-U) is a multi-protocol file server capable of sending and receiving files from other networked computers through various means. Serv-U comes in two editions: Serv-U FTP and Serv-U MFT, as described [here](#).

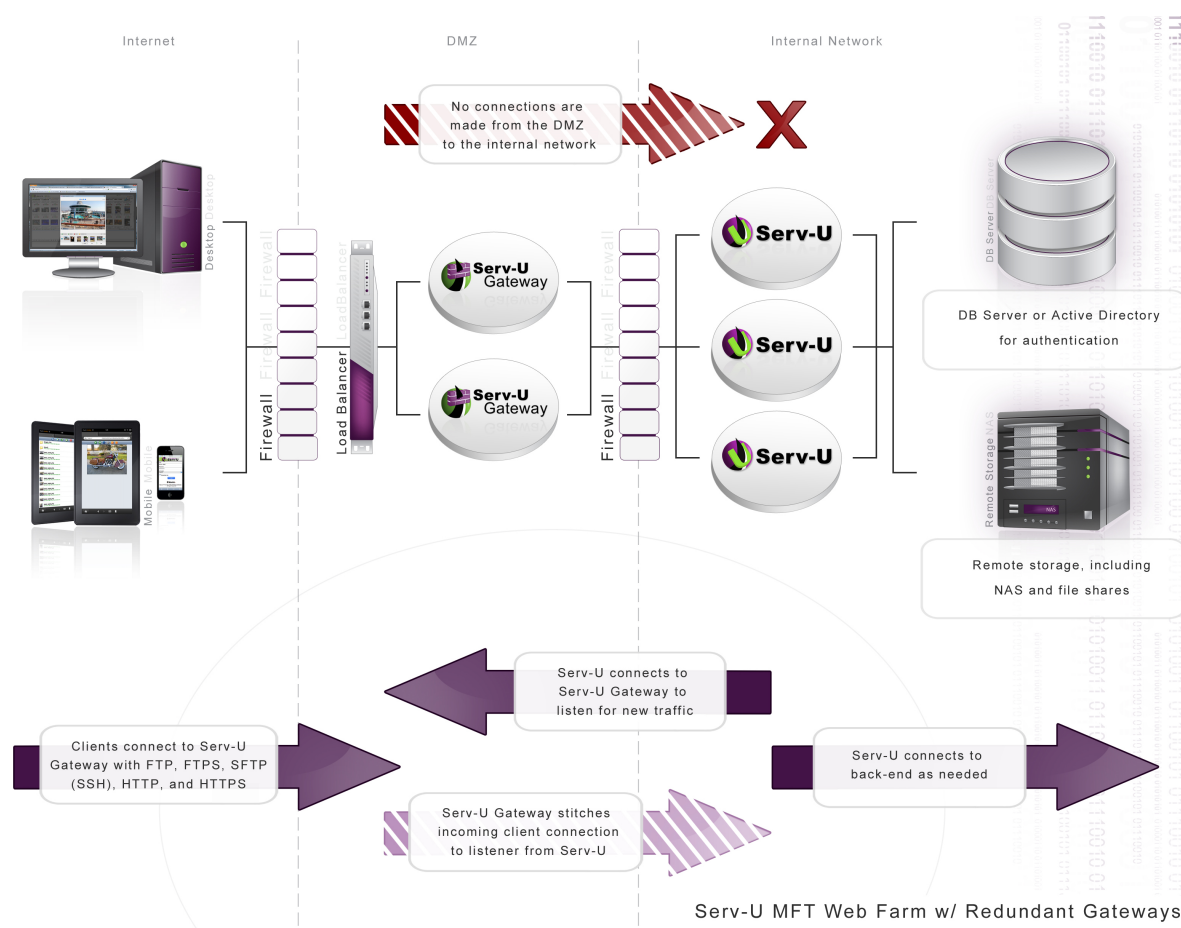
Administrators create accounts for users allowing access to specific files and folders on the server or any other available network resource. Access permissions define where, when, and how users can access the available resources. Serv-U File Server's multi-protocol support means users can employ whatever access method is available to them when connecting to your server. Serv-U File Server supports both IPv4 and IPv6 for next-generation networks. SolarWinds 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)\*

\* These protocols are only available with the Managed File Transfer (MFT) Server edition.

In addition to Serv-U File Server's support for the most popular FTP clients, you can use your favorite web browser or SSH client to connect and transfer files to and from Serv-U File Server. With the Managed File Transfer (MFT) Server edition, administrators wanting to provide a full-featured FTP client can enable FTP Voyager JV, a Java-enabled FTP client delivered to the user when they log in to their Serv-U File Server account.

The following graphic shows a high level overview of a Serv-U File Server deployment (including the optional [Serv-U Gateway](#) module).



Using the SolarWinds Serv-U File Server, you can perform the following actions:

- Access files from anywhere.
- Share files with friends, family, and clients.
- Provide employees in the field with a central location to send and receive data files.
- Use 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 a granular level to control resource usage on the server.
- Connect securely using SSL/TLS or SSH2.
- Use third party digital certificates to guarantee the identity of the server to clients.
- Host multiple domains on the same IP address and port.
- Use multiple sources of authentication on the same domain (local user database, NT/SAM, ODBC).
- Automatically build the tables necessary for ODBC authentication.

You can test both editions in a non-production environment for a limited period of time. After the



evaluation period expires, a commercial license or maintenance renewal provides you with free software updates and technical support through email, phone, or both, depending on your edition, for the duration of the associated maintenance plan.

## Serv-U glossary

**Administration privilege** Serv-U provides four levels of administration privilege:

- **No Privilege:** 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.
- **Group Administrator:** can perform administrative duties relating to the primary group to which they belong. They can add, edit, and delete users which are members of their primary group, and they can also assign permissions at or below the level of the Group Administrator. The primary group is that listed first in their Groups memberships list.
- **Domain Administrator:** can perform administrative duties for the domain to which their account belongs, except configuring their domain listeners, configuring or administering LDAP groups, and configuring ODBC database access for the domain.
- **Service Administrator:** can perform any file server administration activity including creating and deleting domains, user accounts, or even updating the license of the file server. A user account with System Administrator privileges that is logged in through HTTP remote administration can administer the server as if they had physical access to the server.

You can also create read-only group, domain and system administrator accounts which can allow administrators to log in and view configuration options. 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.

<b>Anti-hammering</b>	A Serv-U File Server feature that 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.
-----------------------	--

<b>Bounce attack</b>	A method of exploiting the FTP where an FTP client instructs the FTP server to make an outbound data connection to a different IP address, rather than the client's IP address.
----------------------	---

<b>Directory access rules</b>	Directory access encompasses all of the permissions applied to a server, domain, group, and user that grant and deny access to files and folders. Directory access rules are the foundation of file access rights, because they determine what a user can or cannot access, and how they can access it.
-------------------------------	---

Event	A Serv-U File Server event primarily consists of an event type (for example, User Login or File Upload Failed), and an action type (for example, Show Balloon Tip or Send Email). Serv-U File Server events are used to automate behavior and to provide greater visibility of important file transfer processes.
FTP	The standard network protocol used for transferring computer files between a client and server over the internet.
FTPS	This is a more secure extension to the commonly used File Transfer Protocol that adds encryption using the Transport Layer Security (TLS).
Gateway	The optional Serv-U Gateway allows you to safely accept incoming connections in the DMZ, and provides deeper protection for file transfers on secure networks. It safely handles traffic that should not be directly passed from the Internet to secure internal systems.
Group	A collection of user accounts that share certain attributes. A user can be a member of multiple groups.
Home directory	The home directory for a Serv-U user account is where the user is placed immediately after logging in to the file server. Home directories must be specified using a full path including the drive letter or the UNC share name.
HTTP	The Hypertext Transfer Protocol (HTTP) is a request–response protocol in the client–server computing model.
HTTPS	This is a more secure extension to the HTTP that adds encryption using the Transport Layer Security (TLS).
IP access rules	IP access rules are used in Serv-U File Server to determine who can 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 File Server. Rules set up at the group and user levels define who can connect using a given user account.
Limit	A configuration option that 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.
Listener	A listening service in Serv-U File Server that is configured in a domain to accept incoming FTP, FTPS, SFTP, HTTP or HTTPS connections.
PASV	This is the command that the FTP client uses to tell to the server it's in passive mode. Passive FTP is a preferred FTP mode for FTP clients behind a firewall.
SSH	Secure Shell (SSH) is a cryptographic protocol for operating securely over an unsecured network. It provides a secure channel connecting an SSH client application with an SSH server.

SSH keys	SSH keys are an access credential used in the SSH protocol. SSH keys always come in pairs, made up of a private key and a public key.
TLS	Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications security to FTP and HTTP.
Virtual Hosts	Virtual hosts are used to access a specific domain when listeners are shared by multiple domains.
Virtual Paths	Virtual paths are used to link a physical path outside a user's home directory into the directory listings received by that user.

## Serv-U Editions

Serv-U File Server is available in two editions:

File Transfer Protocol (FTP) Server	This edition is designed for small businesses and project teams requiring FTPS to secure FTP, scripted transfers, and a smaller number of users and domains supported on a single server.
Managed File Transfer (MFT) Server	<p>This edition is designed for businesses of all sizes that need to secure data in transit through SFTP, FTPS or HTTPS in addition to FTP. It adds remote administration through web browsers and iPad, authentication through Active Directory or a database, clustering and event-driven automation, and branding.</p> <p>MFT includes:</p> <ul style="list-style-type: none"><li>• Events</li><li>• File Sharing</li><li>• Additions protocols</li><li>• Web Client Customization</li><li>• LDAP and Window Authorization</li><li>• The FTP Voyager JV module</li></ul>

Both editions support FTP, web transfer, and mobile devices. Both editions also support the optional [Serv-U Gateway](#) module, which is a reverse proxy component that prevents data at rest in a DMZ segment.

For a feature-by-feature comparison of the versions, see the [Serv-U FTP Server Editions Information](#).

## Serv-U Purchase options

Serv-U File Server is available as a fully functional MFT Server trial for 14 days after the date of initial installation. To continue using Serv-U File Server with its full set of features, you must purchase a Serv-U File Server license.

You can purchase a license online at the [Serv-U website](#). Choose which edition of the SolarWinds Serv-U File Server is required and the quantity to purchase. Discount pricing applies for bulk purchasing. You must purchase a SolarWinds Serv-U File Server license before adding an FTP Voyager JV license to your shopping cart.

You can find pricing information at the [Serv-U FTP Server pricing web page](#).

Serv-U licenses are now available in the [Customer Portal](#). Any license purchased or renewed after July 27, 2016 will be available in the Customer Portal Management tab. Refer to [Serv-U licenses now available in Customer Portal](#) for steps to access this information.

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

You can send a purchase order to SolarWinds in one of the following ways:

1. Send an email purchase order, preferably in a PDF, JPG, or GIF format, to a marketing representative at the [SolarWinds sales](#) page.
2. Send a fax purchase order to +1 512 682 9301.
3. Send a mail directly to SolarWinds to the following address:

SolarWinds  
7171 Southwest Parkway  
Bldg 400  
Austin, TX 78735  
USA

# The Serv-U Management Console

When you launch Serv-U, the Management Console is displayed. This is where you access the settings for all areas of Serv-U.

The Navigation column provides access to the Global or Server level settings, and the settings for the domains you have created. Through these menus you can create and access groups and users created at the global or domain level.

To [create domains](#), click the plus icon at the top.

Statistics and logs for the entire server are displayed by default when you access this page.

Use the Serv-U Products menu to access the [Serv-U Web Client](#) or [FTP Voyager JV](#).

The screenshot displays the Serv-U Management Console interface. The left sidebar contains a navigation menu with options: Global, Dashboard, Server Details, Users, Groups, Directories, Limits & Settings, and Server Activity. Below this is a 'DOMAINS (3)' section with a '+ New Domain' button and three domains: domain01, domain02, and FTP Domain. The main content area shows the 'Global > Dashboard' view. At the top, there's a 'New Features in Serv-U File Server 15.2' section with a list of improvements and a 'View Release Notes' button. Below this is the 'Session Statistics' section, which provides a summary of server activity across all domains. It includes a table with columns for Statistics Start Time, Session Statistics, Login Statistics, and Transfer Statistics. The 'SERVER LOG' section is also visible, showing a list of system events and messages. At the bottom, there's a status bar with information about server uptime, sessions, and domains.

**Serv-U Management Console - Home**

(Local Admin) ?

**Global > Dashboard**

**New Features in Serv-U File Server 15.2**

- Improved user interface
- Security improvements
- Performance and stability improvements
- Chinese and Korean characters support in file transfer on Linux
- Increased password security
- Internet explorer compatibility improvements

[View Release Notes](#)

**Session Statistics**

View statistics about the entire file server across all domains, including session information, transfer stats, and current activity totals.

Statistics Start Time	Session Statistics	Login Statistics	Transfer Statistics
Date: <b>May 15, 2020</b>	Current Sessions: <b>0</b>	Logins: <b>0</b>	Download Speed: <b>0 KB/sec</b>
Time: <b>10:12:48 AM</b>	Total Sessions: <b>0</b>	Average Duration Logged In: <b>0</b>	Upload Speed: <b>0 KB/sec</b>
Server has been active for: <b>0 days, 00:00:57</b>	24 hrs. Sessions: <b>0</b>	Last Login Time: <b>0</b>	Downloaded: <b>0 KB (0 files)</b>
	Highest Num. Sessions: <b>0</b>	Last Logout Time: <b>0</b>	Uploaded: <b>0 KB (0 files)</b>
	Avg. Session Length: <b>00:00:00</b>	Most Logged In: <b>0</b>	Avg. DL Speed: <b>0 KB/sec</b>
	Longest Session: <b>00:00:00</b>	Currently Logged In: <b>0</b>	Avg. UL Speed: <b>0 KB/sec</b>

**SERVER LOG** ACTIVE SESSIONS THWACK COMMUNITY

The server log is displayed below with real-time updates. The server log contains start-up information, global messages, and errors.

```
[01] Fri 15May20 10:12:48 - Serv-U File Server (64-bit) - Version 15.2 (15.2.0.428) - (C) 2020 SolarWinds Worldwide, LLC. All rights reserved.
[01] Fri 15May20 10:12:48 - Build Date: Friday, May 15, 2020 12:13 PM
[01] Fri 15May20 10:12:48 - Operating System: Windows 8 64-bit; Version: 6.2.9200
[01] Fri 15May20 10:12:48 - Loaded graphics library.
[01] Fri 15May20 10:12:48 - Loaded ODBC database library.
[01] Fri 15May20 10:12:48 - Loaded SSL/TLS libraries.
[01] Fri 15May20 10:12:48 - Loaded SQLite library.
[01] Fri 15May20 10:12:48 - FIPS 140-2 mode is ON. Serv-U uses an embedded FIPS 140-2 validated cryptographic module (Certificate #1051) per FIPS 140-2 Implementation Guidance.
[01] Fri 15May20 10:12:48 - Valid registration key found.
[01] Fri 15May20 10:12:48 - WinSock Version 2.2 Initialized.
[01] Fri 15May20 10:12:48 - HTTP server listening on port number 43958, IP 127.0.0.1
[01] Fri 15May20 10:12:48 - HTTP server listening on port number 43958, IP ::1
[01] Fri 15May20 10:12:48 - FTP server listening on port number 21, IP 0.0.0.0 (10.110.229.158, 192.168.0.15, 127.0.0.1)
[01] Fri 15May20 10:12:48 - FTPS server listening on port number 990, IP 0.0.0.0 (10.110.229.158, 192.168.0.15, 127.0.0.1)
[01] Fri 15May20 10:12:48 - SFTP (SSH) server listening on port number 22, IP 0.0.0.0 (10.110.229.158, 192.168.0.15, 127.0.0.1)
[01] Fri 15May20 10:12:48 - HTTP SERVER IS NOT LISTENING ON IP 0.0.0.0 (10.110.229.158, 192.168.0.15, 127.0.0.1): Port number 80
[01] Fri 15May20 10:12:48 - HTTPS SERVER IS NOT LISTENING ON IP 0.0.0.0 (10.110.229.158, 192.168.0.15, 127.0.0.1): Port number 443 is already in use
[01] Fri 15May20 10:12:48 - FTP server listening on port number 21, IP :: (fe80::ec0b:31a8:1a8a:9367%12, ::c592:4ad:f53d:9085, ::45dd:d561:c74c:e93d, fe80::c592:4ad:f53d:9085%10, ::1)
[01] Fri 15May20 10:12:48 - FTPS server listening on port number 990, IP :: (fe80::ec0b:31a8:1a8a:9367%12, ::c592:4ad:f53d:9085, ::45dd:d561:c74c:e93d, fe80::c592:4ad:f53d:9085%10, [01] Fri 15May20 10:12:48 - SFTP (SSH) server listening on port number 22, IP :: (fe80::ec0b:31a8:1a8a:9367%12, ::c592:4ad:f53d:9085, ::45dd:d561:c74c:e93d, fe80::c592:4ad:f53d:9085%10, ::1)
```

☐ Freeze Log [Select All](#) [Copy to Clipboard](#) [Clear Log](#) [Filter Log...](#)

Serv-U 15.2.0.428 © 1995 - 2020 SolarWinds Worldwide, LLC. All rights reserved.

Serv Up Time: 0 day(s), 00:40:00 Sessions: 0 current; 0 past 24 hrs; 0 total Up: 0 Bytes; Down: 0 Bytes Domains: 3 of 3 online

## Serv-U user interface conventions

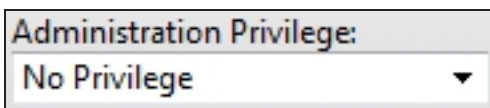
SolarWinds Serv-U File Server uses a consistent method of representing configuration options in a manner that conveys the current value of the option, and also indicates whether that value is the default or the inherited value.

When an option inherits 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.

### Example use case

X-Ample Technology is a computer repair company that maintains a SolarWinds Serv-U File Server, which provides 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 makes each user account a member of the "Technician" group. The Administration Privilege level of this group is set to No Privilege because none of the technicians have any file server administration duties.



Administration Privilege:  
No Privilege ▼

A technician receives a promotion. In addition to his current 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 technician's Administration Privilege level 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 of the "Technician" group.



Administration Privilege:  
**Domain Administrator** ▼

At a later date, the Administration Privilege can be reverted to the default value which is inherited from the "Technician" group by selecting Inherit Default Value from the Administration Privilege list.



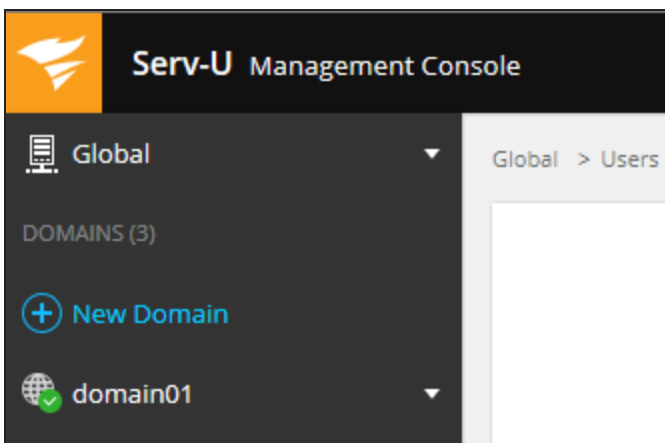
## Create a Serv-U domain

At the core of the Serv-U File Server is the Serv-U domain. At the most basic level, a Serv-U domain is a 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. With careful advanced planning, you can specify an acceptable level of default options at the server level to minimize the amount of configuration required for a domain.

Serv-U FTP Server supports up to three domains. Serv-U MFT Server can support an unlimited number of domains. Domains can share listeners, or they can each be hosted on a unique IP address if the system has multiple IP addresses.

To set up a domain, click the New Domain icon in the Domains section.



The domain wizard is automatically launched when you first run Serv-U.

1. Enter a unique name and optional description for the domain, and click Next.

The default is to enable the domain immediately, but if you do not want it enabled uncheck the Enable domain box.

2. If you have the MFT edition of Serv-U, you can use this domain for both file transfer and file sharing. Uncheck either of these if you specifically do not want to use this domain for both purposes, and click Next.

For the standard edition only file transfer is allowed.

3. If you have enable File Sharing:
  - a. enter the domain URL to be used.
  - b. Select or create the File Sharing repository.
  - c. Check Use Secure URL to use HTTPS.
  - d. Click [Configure SMTP](#) if you want to configure Serv-U to send email for email notifications and events that use email actions.
  - e. Click Next.
4. If you have enabled File Transfer, enter the protocol to be used and the associated ports.

For the standard edition of Serv-U you can use:

  - FTP and explicit SSL, TLS
  - Implicit FTPS (SSL, TLS)
  - HTTP

For the MFT edition of Serv-U you can also use:

  - SFTP using SSH
  - HTTPS (SSL encrypted HTTP)
5. Select or enter the IP addresses this domain should listen on for incoming connections. By default it will listen on all available IPv4 and IPv6 addresses, but you can specify addresses or range of addresses using wild cards. To create a more detailed list of listeners, use the [Listeners](#) tab in Domain Details.
6. If you have enabled File Transfer, select the password encryption mode. The default is to use server settings, but you can change it to:
  - One-way encryption
  - Simple two-way encryption
  - No encryption
7. Check Allow users to recover passwords if you want to enable self-service password recovery via the HTTP login page.
8. To change the server-level settings, click Change Server Settings.
9. Click Finish.
10. When you finish creating a domain, you are asked if you want to [create a user account](#) for this domain.

Once a domain has been created, you can configure further [domain details](#).

# Add a Serv-U user

- [Add a User using the Wizard](#)
- [Add a User manually](#)
- [The User Template](#)
- [Edit a User](#)
- [Copy a User](#)
- [User collections \(MFT only\)](#)
- [Recovering passwords](#)
- [Advanced settings](#)

You can add users at the global or domain level.


- Global users are defined at the server level and have access to all domains.
- Domain users are defined for the specific domain, and only have access to that domain.

For information on Domain users, see the [Domain Users](#) topic.


You can create users quickly using the wizard, or manually enter user properties for more precise set-up.

## View and add users at the global level

1. Click Global in the navigation column.
2. Click Users.




 **Users** - Create, modify, and delete global user accounts for all domains on the file server.

Global Users Database Users

 This list shows the global user accounts that are allowed to connect to any domain on the file server. Global accounts can be overridden by creating the account on individual domains.


Select user collection  
General


Filter Users

Login ID	Full Name	Description	Last Login Time	Home Directory
 chris1969	Christopher Cooper	Austin		%DOMAIN_HOM...
 gill1988	Gillian Gill	Dublin		%DOMAIN_HOM...
 helen1990	Helen Helvetica			%DOMAIN_HOM...

## Add a user using the wizard

1. Click the Wizard button. The User Wizard is displayed.

 **User Wizard - Step 1 of 4**

 Welcome to the Serv-U user account wizard. This wizard helps you quickly create new users to access your file server.


The login ID is provided by the client to identify their account when attempting to login to the file server.

Login ID:

Full Name:  (optional)

Email Address:  (optional)

2. Enter a unique login ID for the user.

 Login IDs cannot contain any of the following special characters:

\ / < > | : . ? \*

Two special login IDs exist: Anonymous and FTP. These are synonymous with one another, and can be used for guests. They do not require a password, so the Password field should be left blank. Serv-U requires users who log on with one of these accounts to provide their email address to complete the login process.

3. Optionally, enter a name and email address for this user.
4. Click Next.
5. Enter a password for this user, or accept the suggested eight character, complex password.

You can leave the password blank, which will enable anyone knowing the login ID to access this account.

You can place restrictions on the length and complexity of passwords, and disable the automatic password generator if required.

6. Check the box if you want the user to create their own password when they first login.
7. Enter or navigate to the home directory for this user. This is where the user is placed immediately after logging in to the file server. This must be specified using a full path including the drive letter or the UNC share name.

When you specify the home directory, you can use the %USER% macro 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 it is combined with a directory access rule for %HOME%, a new user can be configured with a unique home directory and the appropriate access rights to that location with a minimal amount of effort.

You can also use the %DOMAIN\_HOME% macro 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.

Check the Lock user in home directory box if you want this user's access to be restricted to this directory.

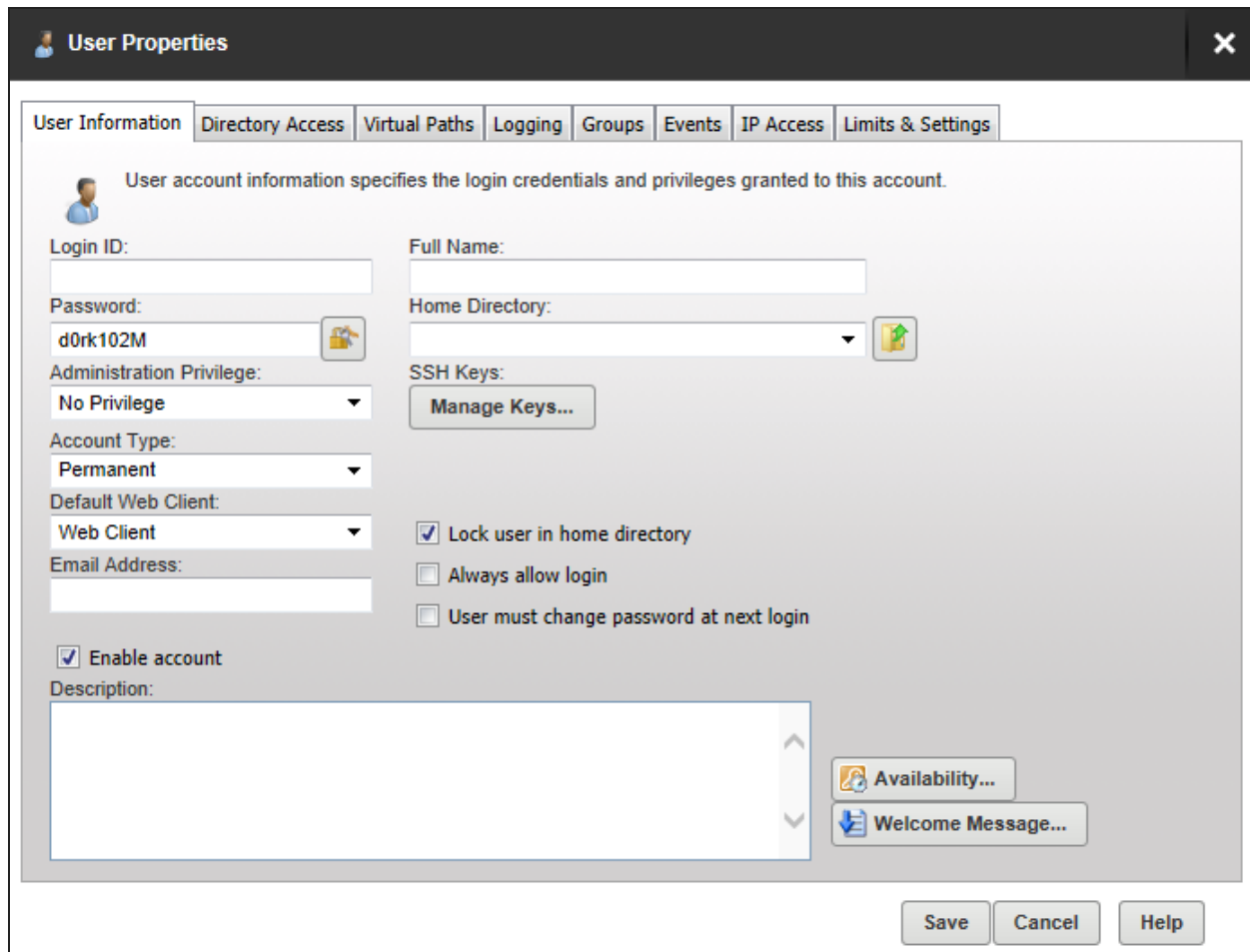
8. Click Next.

9. Select Read Only Access if you want this user to only be able to browse and download files or Full Access if you want to grant the user full control of files and directories in their home directory.
10. Click Finish.
11. The user is added to the list of users. You can edit this user if you want to apply more advanced settings.

## Add a User manually

1. Click the Add button.

The User Properties window is displayed.




The User Properties window is displayed, showing the User Information tab. The window title is "User Properties" with a close button (X) in the top right corner. The tabs are: User Information, Directory Access, Virtual Paths, Logging, Groups, Events, IP Access, and Limits & Settings. The main content area contains the following fields and options:

- User account information specifies the login credentials and privileges granted to this account.**
- Login ID:** Text field with value "d0rk102M".
- Password:** Text field with value "d0rk102M" and a password icon.
- Administration Privilege:** Dropdown menu with value "No Privilege".
- Account Type:** Dropdown menu with value "Permanent".
- Default Web Client:** Dropdown menu with value "Web Client".
- Email Address:** Text field.
- Full Name:** Text field.
- Home Directory:** Text field with a dropdown arrow and a folder icon.
- SSH Keys:** Text field with a "Manage Keys..." button.
- ☒ Lock user in home directory
- ☐ Always allow login
- ☐ User must change password at next login
- ☒ Enable account
- Description:** Text area.
- Availability...** button.
- Welcome Message...** button.

At the bottom right, there are three buttons: Save, Cancel, and Help.

2. Enter a unique login ID for the user.

 Login IDs cannot contain any of the following special characters:

\ / < > | : . ? \*

Two special login IDs exist: Anonymous and FTP. These are synonymous with one another, and can be used for guests. They do not require a password, so the Password field should be left blank. Serv-U requires users who log on with one of these accounts to provide their email address to complete the login process.

3. Enter a name for this user.

4. Enter a password for this user, or click the lock button to create an eight character, complex password.

You can leave the password blank, which will enable anyone knowing the login ID to access this account.

You can place restrictions on the length and complexity of passwords through User limits. For more information about password limits, see [User Limits and Settings - Passwords](#).

5. Enter or navigate to the home directory for this user. This is where the user is placed immediately after logging in to the file server. This must be specified using a full path including the drive letter or the UNC share name.

When you specify the home directory, you can use the %USER% macro 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 it is combined with a directory access rule for %HOME%, a new user can be configured with a unique home directory and the appropriate access rights to that location with a minimal amount of effort.

You can also use the %DOMAIN\_HOME% macro 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.

6. Select the Administration Privilege for this user. This can be:

No Privilege	A regular user account that can only transfer files to and from the File Server. The Serv-U Management Console is not available.
--------------	--

Group Administrator	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, and they can also assign permissions at or below the level of the Group Administrator. They may not make any other changes.
Domain Administrator	<p>A Domain Administrator can only perform administrative duties for the domain to which their account belong, and 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 are:</p> <ul style="list-style-type: none"><li>• configuring their domain listeners</li><li>• configuring or administering LDAP groups</li><li>• configuring ODBC database access for the domain</li></ul>
System Administrator	A System Administrator can perform any file server administration activity including creating and deleting domains, user accounts, and even updating the license of the file server. A user account with System Administrator privileges logged in through HTTP remote administration can administer the server as if they had physical access to the server.
Read-only Group/Domain/Server Administrator	Read-only administrator accounts can allow administrators to log in and view configuration options at the group, 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, and cannot create, delete or edit user accounts.

7. If you have the MFT edition of Serv-U, you can specify a SSH public key to be used to authenticate a user when logging in to 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 of the domain, set in Domain Details > Settings, used if the keys are in a central folder relative to the domain home directory.

Examples:



`%HOME%\SSHpublic.pub`

`%HOME%\%USER%.pub`

`%DOMAIN_HOME%\SSHKeys\%USER%.pub`

For information on SSH public key authentication, adding a SSH key pair, and creating an key pair for testing, see [New SSH Key Pair Creation](#).


8. Select the account type. By default, all accounts are permanent and exist on the file server until they are manually deleted or disabled. You can configure an account 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 is displayed. Click the calendar or expiration date to select when the account should be disabled or deleted.

The account is accessible until the beginning of the day on which it is set to be disabled. For example, if an account is set to be disabled on 15 July 2015, the user can log in until 14 July 2015, 23:59.

9. Select the default web client to be displayed when a user logs in.

If you have the MFT edit, 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, you can also specify a default client. If you change this option, 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.

10. Enter an Email address for this user. Type an email address here to allow password recovery for the user account.

 For the MFT edition, this email address can also be used for event notifications.

## 11. Check or uncheck the following checkboxes:


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.
Lock user in home directory	Users 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 because Serv-U always reports it as "/" (root). The value of this attribute can be inherited through group membership.
Always allow login	<p>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. 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.</p> <p>Enabling the Always Allow Login option does not override <a href="#">IP access rules</a>. If both options are defined, the IP access rules prevail.</p>
User must change password at next login	<p>If enabled, the user will be prompted to change their password when they next log in.</p> <p>This option takes priority to the "Allow user to change password" setting on the Limits &amp; Setting tab. This means even if that setting is set to No, checking this box still will require the user to change their password.</p>

## 12. Enter an optional description of this user account.

## 13. Click Availability if you want to place limits on when this user can log in.

- Check Apply limit and select the start and end time to specify the period this user may log in.
- Tick the checkboxes for the days of the week on which this user may log in.

## 14. Click Welcome Message if you want to sent a welcome message to this user when they log in. This may also be set at the Group level.

 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 through SFTP over SSH2, because SSH2 does not define a method for sending general text information to users.

- a. Check Include if you want to include the response code in the welcome message test when an FTP connection is made.
- b. Either:
  - Select or navigate to a message file if you have already created a text file containing a welcome message.or:
  - Check the Override box, and enter a message specific to this user in the text box above it.
- c. Click Save.

## Advanced settings

Once you have added the User information you can use the following tabs on this window to complete the user setup.

### [Directory Access](#)

Directory access rules define the files and directories that the user has permission to access. At the user level, these rules are inherited from any groups the user belongs to as well as those rules defined at the domain and server level.

### [Virtual Paths](#)

Virtual paths are used to link a physical path that is outside the directory structure of the user's home directory into the directory listings received by that user.

### [Logging](#)

This tab provides checkboxes to configure what information you want to be logged.

### [Groups](#)

From the User Properties window you can select groups to which you want to add a user. Group membership allows you to assign various basic attributes to users that are members of the group.

### [Events](#)

MFT only: Events let you automatically run programs, send email and show messages when triggered by Serv-U activities.

### [IP Access](#)

Set up and maintain Server IP access rules so that specific IP address can be allowed or denied access to all your file server domains. These are checked when a physical connection is established with the file server, but before a welcome message is sent.

### [Limits & Settings](#)

There are many options that can be applied at the user level. You can specify on which days and at which time these limits apply.

# The User Template

While the New User Wizard provides a way to quickly create a user account with the minimum number of required attributes, most File Server administrators have a collection of settings that 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. You can configure the template user 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.

By using user templates, you can add users to a specific default group. If you set up the user template as a member of the group you want all users to be a member of. This way, when new users are created, they will automatically be added to the particular group which is specified in the user template.

## Edit a User

Select a user and click Edit to open the User Properties window with the selected user's information.

## Copy a User

Select a user and click Copy to open the User Properties window with the selected user's information. You will need to supply at least a new Login ID to save the new user.

## User collections (MFT only)

In Serv-U MFT Server, you can organize user accounts into collections to make account management more logical and organized. This can be useful when you manage all users from a department or physical location. For example, you can place all users in the accounting department in a collection named Accounting, or place all users at an office in Topeka in a collection named Topeka Users.

To create a collection, click Add in the Select user collection area in the users window. In the new window, type the name of your collection, and then click Save. You can add users to this new collection by selecting them and clicking Add below the user list. To move a user from one collection to another, click Move below the user list, and then select the destination collection for the highlighted user accounts. You can also rename or delete collections by using the appropriate button.

When deleting a collection, all user accounts contained in that collection are deleted, too. If you want to keep the user accounts, make sure you move them before deleting the collection.

By default, all users are created in the General user collection.

## Recovering passwords

Serv-U supports password recovery both through the Management Console and through the Web Client. For password recovery to be available, you must configure the SMTP options for the server or domain, and the user account must have an email address listed. To use password recovery from the user page:

1. Select the user's account,
2. 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.

# Add a Serv-U group

- [Add a Group](#)
- [Advanced settings](#)
- [Edit a Group](#)
- [The Group Template](#)

Groups provide a method of sharing common configuration options with multiple user accounts. Configuring a group is similar to configuring a user account. Groups can be created at the server or domain level.

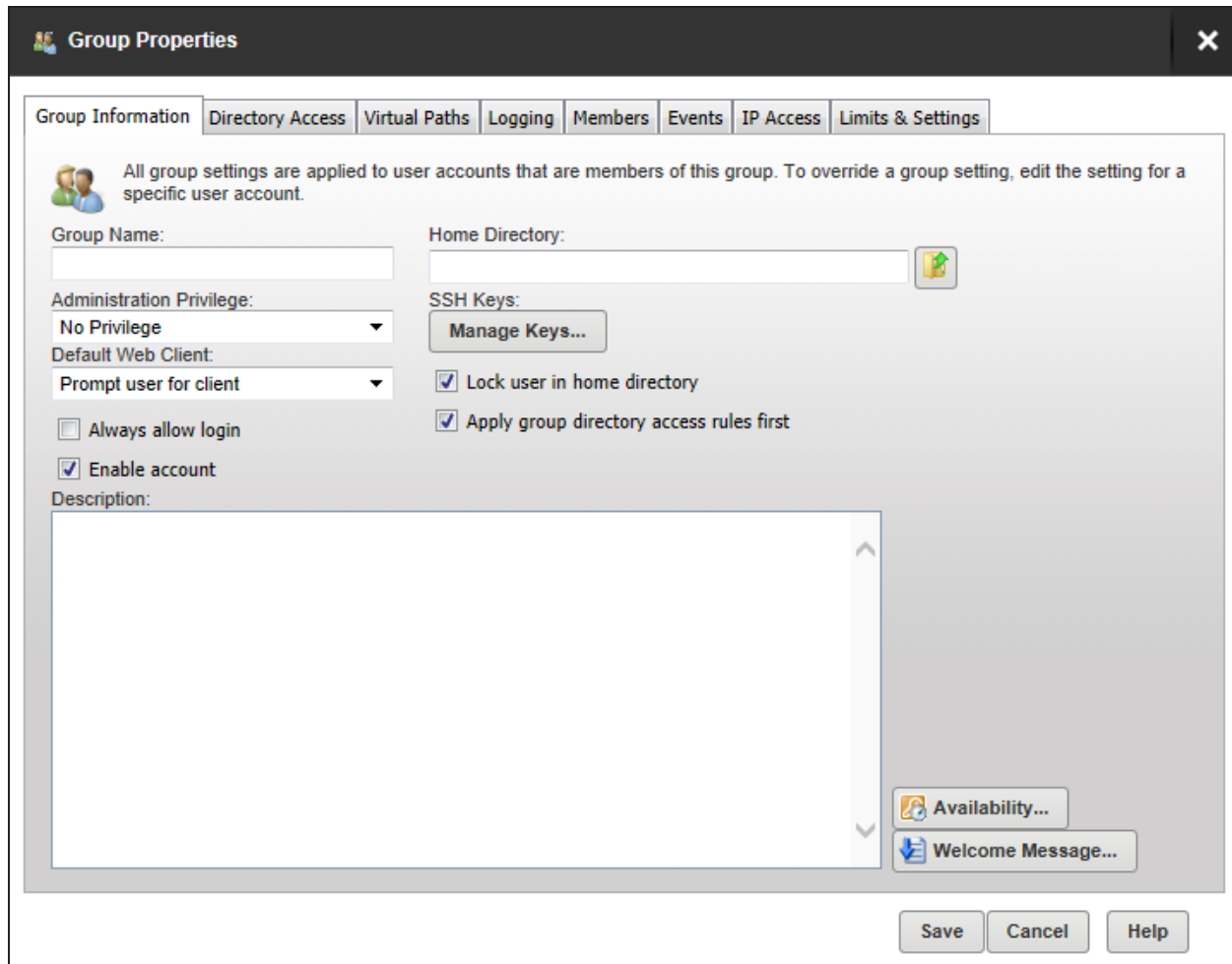
Virtually every configuration option available for a user account can be set at the group level. For a user to inherit a group's settings, it must be a member of the group. Permissions and attributes inherited by a user through group membership can still be overridden at the user level. A user can be a member of multiple groups in order to acquire multiple collections of permissions, such as directory or IP access rules.

However, groups are only available to user accounts that are defined at the same level. In other words, a global user (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.

## Add a Group

1. From the Groups page, click the Add button.

The Group Properties window is displayed.




**Group Properties** [X]

Group Information | Directory Access | Virtual Paths | Logging | Members | Events | IP Access | Limits & Settings

All group settings are applied to user accounts that are members of this group. To override a group setting, edit the setting for a specific user account.

Group Name:

Home Directory:  

Administration Privilege: **No Privilege** ▼

SSH Keys: **Manage Keys...**

Default Web Client: **Prompt user for client** ▼



☐ Always allow login

☒ Lock user in home directory

☒ Enable account

☒ Apply group directory access rules first

Description:

 Availability...  Welcome Message...

**Save** **Cancel** **Help**

2. Enter or navigate to the home directory for users in this group. This is where the users are placed immediately after logging in to the file server. This must be specified using a full path including the drive letter or the UNC share name.

When you specify the home directory, you can use the %USER% macro 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 it is combined with a directory access rule for %HOME%, a new user can be configured with a unique home directory and the appropriate access rights to that location with a minimal amount of effort.

You can also use the %DOMAIN\_HOME% macro 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.

3. Select the Administration Privilege for this users in this group. This can be:

No Privilege	A regular user account that can only transfer files to and from the File Server. The Serv-U Management Console is not available.
Group Administrator	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, and they can also assign permissions at or below the level of the Group Administrator. They may not make any other changes.
Domain Administrator	<p>A Domain Administrator can only perform administrative duties for the domain to which their account belong, and 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 are:</p> <ul style="list-style-type: none"><li>• configuring their domain listeners</li><li>• configuring or administering LDAP groups</li><li>• configuring ODBC database access for the domain</li></ul>
System Administrator	A System Administrator can perform any file server administration activity including creating and deleting domains, user accounts, and even updating the license of the file server. A user account with System Administrator privileges logged in through HTTP remote administration can administer the server as if they had physical access to the server.
Read-only Group/Domain/Server Administrator	Read-only administrator accounts can allow administrators to log in and view configuration options at the group, 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, and cannot create, delete or edit user accounts.

4. If you have the MFT edition of Serv-U, you can specify a SSH public key to be used to authenticate users in this group when logging in to 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 of the domain, set in Domain Details > Settings, used if the keys are in a central folder relative to the domain home directory.

**Examples:**

```
%HOME%\SSHpublic.pub
```

```
%HOME%\%USER%.pub
```

```
%DOMAIN_HOME%\SSHKeys\%USER%.pub
```

For information on SSH public key authentication, adding a SSH key pair, and creating an key pair for testing, see [New SSH Key Pair Creation](#).

5. Select the default web client to be displayed when a user in this group logs in.

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, you can also specify a default client. If you change this option, 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.

6. Check or uncheck the following checkboxes:


Always allow login	<p>Enabling this option means that users in this group are 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. As with any option that allows bypassing access rules, care should be taken in granting this ability.</p> <p>Enabling the Always Allow Login option does not override IP access rules. If both options are defined, the IP access rules prevail.</p>
Enable account	<p>Deselect this option to disable user accounts in this group. Disabled accounts remain on the file server but cannot be used to log in. To re-enable accounts in this group, select the Enable account option again.</p>
Lock user in home directory	<p>Users 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 because Serv-U always reports it as "/" (root).</p>
Apply group directory access rules first	<p>Deselect this option to place the directory access rules of the group below the user access rules.</p> <p>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 directory access rules specified at the user level. However, there are certain instances where you may want the user level rules to take precedence.</p>

7. Enter an optional description for this group account.

8. Click Availability if you want to place limits on when users in this group can log in.

- Check Apply limit and select the start and end time to specify the period users in this group may log in.
- Tick the checkboxes for the days of the week on which users in this group may log in.

9. Click Welcome Message if you want to sent a welcome message to the users in this group when they log in.

 The welcome message is a message traditionally sent to FTP clients 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 through SFTP over SSH2, because SSH2 does not define a method for sending general text information to users.

- a. Check Include if you want to include the response code in the welcome message test when an FTP connection is made.
- b. Either:
  - Select or navigate to a message file if you have already created a text file containing a welcome message.or:
  - Check the Override box, and enter a message specific to this user in the text box above it.
- c. Click Save.

## Advanced settings

Once you have added the Group information you can use the following tabs on this window to complete setup.

<a href="#">Directory Access</a>	Directory access rules define the files and directories that users in this group have permission to access. At the group level, these rules are inherited from the domain and server level.
<a href="#">Virtual Paths</a>	Virtual paths are used to link a physical path that is outside the directory structure of the home directory of users in this group into the directory listings received by that user.
<a href="#">Logging</a>	This tab provides checkboxes to configure what information you want to be logged.
<a href="#">Members</a>	Displays the list of users in this group. This tab is display only - you need to use the <a href="#">Groups</a> tab in the individual User Properties to select the groups to which that user belongs.
<a href="#">Events</a>	MFT only: Events let you automatically run programs, send email and show messages when triggered by Serv-U activities.
<a href="#">IP Access</a>	Set up and maintain Server IP access rules so that specific IP address can be allowed or denied access to all your file server domains for users in this group. These are checked when a physical connection is established with the file server, but before a welcome message is sent.
<a href="#">Limits &amp; Settings</a>	There are various options that can be applied at the group level. You can specify on which days and at which time these limits apply.

## Edit a Group

Select a group and click Edit to open the Group Properties window, allowing you to edit that information for users in this group.

## The Group Template

You can configure a template for creating new groups by clicking Template. The template group can be configured just like any other group, with the exception of giving it a name. After the settings are saved to the template, all new groups are created with their default settings set to those found within this template. This way you can configure the basic settings that you want all of your groups to use by default.

## Serv-U settings

Serv-U settings can be defined at four levels: global, domain, group and user. Although some settings are specific to the level, many can be defined at multiple levels.

<a href="#">Global</a>	Global level settings apply throughout Serv-U unless overridden at a lower level. (Sometimes Global settings are referred to as Server settings.)
<a href="#">Domain</a>	If you configure a setting at the domain level, the setting applies to all users, groups, in that specific domains unless overridden at the group or user level.
<a href="#">Group</a>	Groups are optional in Serv-U, and enable you to apply settings to a group of users. Users can be easily added and removed from groups.
<a href="#">User</a>	User settings are applied at the individual user level and override all other settings.

# Serv-U global level settings

Serv-U settings can be defined at four levels: global, domain, group and user. Although some settings are specific to the level, many can be defined at multiple levels. If you configure a setting at the global level, the setting applies to all users, groups and domains, unless overridden at the domain, group or user level.

Global settings are divided into the following areas, each accessible from the navigation column.

<a href="#">Dashboard</a>	Displays statistics about the entire file server across all domains, including session information, transfer stats, and current activity totals. <ul style="list-style-type: none"><li>• <a href="#">Server Log</a></li><li>• <a href="#">Active Sessions</a></li></ul>
<a href="#">Server Details</a>	Displays information pertaining to the entire file server, including server-wide access rules, license, and registration information. <ul style="list-style-type: none"><li>• <a href="#">IP Access</a></li><li>• <a href="#">Serv-U Gateway</a></li><li>• <a href="#">Database</a></li><li>• <a href="#">Events</a></li><li>• <a href="#">License Information</a></li><li>• <a href="#">Program Information</a></li></ul>
<a href="#">Users</a>	Create, modify, and delete global user accounts for all domains on the file server.
<a href="#">Groups</a>	Create, modify, and delete global groups for use by global accounts on the file server.
<a href="#">Directories</a>	Configure the basic directory structure available to all users of the file server, including default directory access rules and virtual paths.
<a href="#">Limits &amp; Settings</a>	Limits and settings are used to configure the basic settings and behavior for the entire file server, including FTP command processor customization and SSL/SSH encryption and certificate options. Limits and settings configured at this level are inherited by all domains, groups, and users.
<a href="#">Server Activity</a>	Displays information about and allows management of user sessions across all domains on the file server. The log tab displays server-wide messages and information.

# The Serv-U global dashboard

The default page shown when you launch Serv-U is the global dashboard. To return to it, if another page is displayed:

1. Click Global > Dashboard in the Navigation column.

**Serv-U Management Console - Home**

Global > Dashboard

**New Features in Serv-U File Server 15.2**

- Improved user interface
- Security improvements
- Performance and stability improvements
- Chinese and Korean characters support in file transfer on Linux
- Increased password security
- Internet explorer compatibility improvements

[View Release Notes](#)

**Session Statistics**

View statistics about the entire file server across all domains, including session information, transfer stats, and current activity totals.

Statistics Start Time	Session Statistics	Login Statistics	Transfer Statistics
Date: <b>May 15, 2020</b>	Current Sessions: <b>0</b>	Logins: <b>0</b>	Download Speed: <b>0 KB/sec</b>
Time: <b>10:12:48 AM</b>	Total Sessions: <b>0</b>	Average Duration Logged In: <b>0</b>	Upload Speed: <b>0 KB/sec</b>
Server has been active for: <b>0 days, 00:00:57</b>	24 hrs. Sessions: <b>0</b>	Last Login Time: <b>0</b>	Downloaded: <b>0 KB (0 files)</b>
	Highest Num. Sessions: <b>0</b>	Last Logout Time: <b>0</b>	Uploaded: <b>0 KB (0 files)</b>
	Avg. Session Length: <b>00:00:00</b>	Most Logged In: <b>0</b>	Avg. DL Speed: <b>0 KB/sec</b>
	Longest Session: <b>00:00:00</b>	Currently Logged In: <b>0</b>	Avg. UL Speed: <b>0 KB/sec</b>

**SERVER LOG** ACTIVE SESSIONS THWACK COMMUNITY

The server log is displayed below with real-time updates. The server log contains start-up information, global messages, and errors.

```
[01] Fri 15May20 10:12:48 - Serv-U File Server (64-bit) - Version 15.2 (15.2.0.428) - (C) 2020 SolarWinds Worldwide, LLC. All rights reserved.
[01] Fri 15May20 10:12:48 - Build Date: Friday, May 15, 2020 12:13 PM
[01] Fri 15May20 10:12:48 - Operating System: Windows 8 64-bit; Version: 6.2.9200
[01] Fri 15May20 10:12:48 - Loaded graphics library.
[01] Fri 15May20 10:12:48 - Loaded ODBC database library.
[01] Fri 15May20 10:12:48 - Loaded SSL/TLS libraries.
[01] Fri 15May20 10:12:48 - Loaded SQLite library.
[01] Fri 15May20 10:12:48 - FIPS 140-2 mode is ON. Serv-U uses an embedded FIPS 140-2 validated cryptographic module (Certificate #1051) per FIPS 140-2 Implementation Guidance
[01] Fri 15May20 10:12:48 - Valid registration key found
[01] Fri 15May20 10:12:48 - WinSock Version 2.2 initialized.
[01] Fri 15May20 10:12:48 - HTTP server listening on port number 43958, IP 127.0.0.1
[01] Fri 15May20 10:12:48 - HTTP server listening on port number 43958, IP ::1
[01] Fri 15May20 10:12:48 - FTP server listening on port number 21, IP 0.0.0.0 (10.110.229.158, 192.168.0.15, 127.0.0.1)
[01] Fri 15May20 10:12:48 - FTPS server listening on port number 990, IP 0.0.0.0 (10.110.229.158, 192.168.0.15, 127.0.0.1)
[01] Fri 15May20 10:12:48 - SFTP (SSH) server listening on port number 22, IP 0.0.0.0 (10.110.229.158, 192.168.0.15, 127.0.0.1)
[01] Fri 15May20 10:12:48 - HTTP SERVER IS NOT LISTENING ON IP 0.0.0.0 (10.110.229.158, 192.168.0.15, 127.0.0.1): Port number 80
[01] Fri 15May20 10:12:48 - HTTPS SERVER IS NOT LISTENING ON IP 0.0.0.0 (10.110.229.158, 192.168.0.15, 127.0.0.1): Port number 443 is already in use
[01] Fri 15May20 10:12:48 - FTP server listening on port number 21, IP :: (fe80::ec0b:31a8:1a8a:9367%12, ::c592:4ad:f53d:9085, ::45dd:d561:c74c:e93d, fe80::c592:4ad:f53d:9085%10, ::1)
[01] Fri 15May20 10:12:48 - FTPS server listening on port number 990, IP :: (fe80::ec0b:31a8:1a8a:9367%12, ::c592:4ad:f53d:9085, ::45dd:d561:c74c:e93d, fe80::c592:4ad:f53d:9085%10, ::1)
[01] Fri 15May20 10:12:48 - SFTP (SSH) server listening on port number 22, IP :: (fe80::ec0b:31a8:1a8a:9367%12, ::c592:4ad:f53d:9085, ::45dd:d561:c74c:e93d, fe80::c592:4ad:f53d:9085%10, ::1)
```

☐ Freeze Log [Select All](#) [Copy to Clipboard](#) [Clear Log](#) [Filter Log...](#)

Serv-U 15.2.0.428 © 1995 - 2020 SolarWinds Worldwide, LLC. All rights reserved.

Server Up Time: 0 day(s), 00:40:00 Sessions: 0 current; 0 past 24 hrs; 0 total Up: 0 Bytes; Down: 0 Bytes Domains: 3 of 3 online

When first launched, a pane showing information about the current release is displayed. This can be closed to avoid future display.

The top section of the page shows the current session statistics across all domains. To display statistics for each domain, see [Domain Activity](#).

The rest of the page can display the [Server Log](#), [Active Sessions](#) or the [Thwack page for Serv-U](#).

## The Serv-U server log

To display the server log:

1. Navigate to Global > Dashboard and click on the Server Log tab.

The server log displays start-up information, listening protocols, global messages, and errors in real time. It also shows the version and build of Serv-U.

You can copy the contents of the log to your clipboard, clear the log or filter the log to display entries showing a specific string.

## Serv-U sessions activity

To display the active sessions for the server:


1. Navigate to Global > Dashboard and click on Active Sessions.

On this page you can see an overall picture of the current activity on the file server. In addition, you can view individual sessions, including their current status, connection state, and transfer information.

To view detailed information about 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 an accurate and up-to-date snapshot of the activities of the session.

The following options are available for sessions:



Button	Description						
Disconnect	<p>Select a session and click to bring up a window with the following options:</p> <table> <tr> <td>Disconnect</td><td>Immediately disconnects the session. Another session can be immediately established by the disconnected client. This is also known as "kicking" the user.</td></tr> <tr> <td>Disconnect and ban IP for x</td><td>Immediately disconnects the session and bans its IP address for the specified number of minutes, preventing the client from immediately reconnecting.</td></tr> <tr> <td>Disconnect and block IP permanently</td><td>Immediately disconnects the session and adds a deny IP access rule for the IP address, preventing the client from ever reconnecting from the same IP address.</td></tr> </table> <p>The last two methods can be applied for the entire server or only the domain currently in use.</p> <p>In addition to disconnecting the session, you can also disable the user account in use by the session by selecting Disable user account.</p> <p>If the current session is using the FTP protocol, you can send a message to the user before disconnecting them by typing it in the Message to user field.</p> <div>  MFT Users: This option is not available for HTTP or SFTP sessions because neither protocol defines a method for chatting with users. </div>	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 x	Immediately disconnects the session and bans its IP address for the specified number of minutes, preventing the client from immediately reconnecting.	Disconnect and block IP permanently	Immediately disconnects the session and adds a deny IP access rule for the IP address, preventing the client from ever reconnecting from the same IP address.
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 x	Immediately disconnects the session and bans its IP address for the specified number of minutes, preventing the client from immediately reconnecting.						
Disconnect and block IP permanently	Immediately disconnects the session and adds a deny IP access rule for the IP address, preventing the client from ever reconnecting from the same IP address.						
Abort	Select a session and click to cancel the file transfer without disconnecting the session. After confirming the command, the current file transfer for that session is terminated by the server. Some clients, especially FTP and SFTP clients, may automatically restart the canceled transfer, making it appear that the cancellation failed. If this is the case, try disconnecting the session instead.						
Broadcast	Broadcast is the same as Chat as described below, except instead of selecting a single session and chatting with a single FTP user, you can broadcast a message to all current users.						

Button	Description
Spy & Chat	<p>Select a session and click. This displays all the detailed information normally visible by highlighting the session, and also includes a complete copy of the session log since it first connected to the file server. This way you can browse the log and view all actions taken by the user of the session.</p> <p>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.</p> <p>To send a message to the session, type the message text in the Message Content field, and then click Send.</p> <p>When a message is received from the session, it is automatically displayed here.</p> <p>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 discarding them.</p>

## Serv-U server details

If you configure details at the server level, the settings apply to all users, groups, and domains on the server unless overridden at a lower level. Settings you can configure at the server level include directory access rules, IP access rules, bandwidth limitations, global user accounts, and more. The following sections contain detailed information about each setting and how it can be configured.

Tab	Description
<a href="#">IP Access</a>	Set up and maintain Server IP access rules so that specific IP address can be allowed or denied access to all your file server domains. These rules are checked when a physical connection is established with the file server, and before a welcome message is sent.
<a href="#">Serv-U Gateway</a>	The optional Serv-U Gateway module is an optional reverse-proxy component that will safely terminate file transfer connections in the DMZ to avoid inbound connections or storing data in the DMZ. See <a href="#">The Serv-U Gateway</a> for more information about this product.
<a href="#">Database</a>	If you have an external database you can load users and groups from it. The database must have an ODBC driver installed and must exist as an ODBC data source on the system. Users and groups loaded in this manner that conflict with locally created users and groups are overridden.

Tab	Description
<a href="#">Events</a>	MFT only: Events let you automatically run programs, send email and show messages when triggered by Serv-U activities.
<a href="#">License Information</a>	Displays information about your Serv-U license, including restrictions, limitations, and upgrade information.  This tab is also where you enter or upgrade your Serv-U license.
<a href="#">Program Information</a>	Displays information pertaining to the entire file server.

## Serv-U Server Details: IP Access

The IP Access tab shows the IP access rules set up for the server, domain, group or individual user, and allows you to add, import, edit, export and delete these rules.

Rules set at the server level are inherited by all domains, groups and user unless overridden.

IP access rules enable you to specify IP addresses, or ranges of IP addresses to which access is allowed or denied. These rules are applied as soon as a physical connection is established. Rules are applied in the order 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. Use the arrows on the right side of the list to change the position of an individual rule in the list.

### Display the IP access list

1. Navigate to Global > Server Details.
2. Click the IP Access tab.

The list of IP addresses set up at this level is displayed.

Use the arrows on the right side of the list to change the position of an individual rule in the list.

Check the Enable sort mode box to sort the IP access list numerically rather than in the processing order. Displaying the IP access list in sort mode does 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 useful when you review long lists of access rules to determine if an entry already exists.

## Add an IP access rule

- From the IP tab, click Add.  
The IP Access Rule window is displayed.

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

- Enter the IP Address, name or mask using the following conventions.

Value or wildcard	Explanation
xxx	Stands for an exact match, such as 192.0.2.0 (IPv4), fe80:0:0:0:a450:9a2e:ff9d:a915 (IPv6, long form) or fe80::a450:9a2e:ff9d:a915 (IPv6, shorthand).
xxx-xxx	Stands for a range of IP addresses, such as 192.0.2.0-19 (IPv4), fe80:0:0:0:a450:9a2e:ff9d:a915-a9aa (IPv6, long form), or fe80::a450:9a2e:ff9d:a915-a9aa (IPv6, shorthand).
*	Stands for any valid IP address value, such as 192.0.2.*, which is analogous to 192.0.2.0-255, or fe80::a450:9a2e:ff9d:*, which is analogous to fe80::a450:9a2e:ff9d:0-ffff.
?	Stands for any valid character when specifying a reverse DNS name, such as server?.example.com.
/	Specifies 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.

- Enter a description.
- Select Allow or Deny access.
- Click Save.

## Edit an IP access rule

1. From the IP tab, click Edit.
2. Amend the rule information as required..
3. Click Save.

## Delete an IP access rule

1. From the IP tab, select the IP rule or rules to delete.
2. Click Delete and confirm.

## Import and export global IP address rules

You can speed up the creation of IP address rules by creating a text file of addresses, descriptions and access permissions.

1. Create a text file using Notepad or similar text editor.
2. On the first line enter "IP","Description","Allow".
3. Enter the details of each IP access rule:

IP	The IP address, IP range, CIDR block, or domain name for which the rule applies.
Description	A text description of the rule for reference purposes.
Allow	Set this value to 0 for Deny, or 1 for Allow.

For example:

```
"IP", "Description", "Allow"
"172.16.0.1", "Flange Software", "1"
"172.16.0.*", "Do not allow", "0"
"2001:db8::/32", "New test site", "1"
```

4. From the IP tab, click Import.
5. Navigate to the file you created, and click Select.


Similarly, the list of existing IP address rules can be exported to a text file by clicking Export.

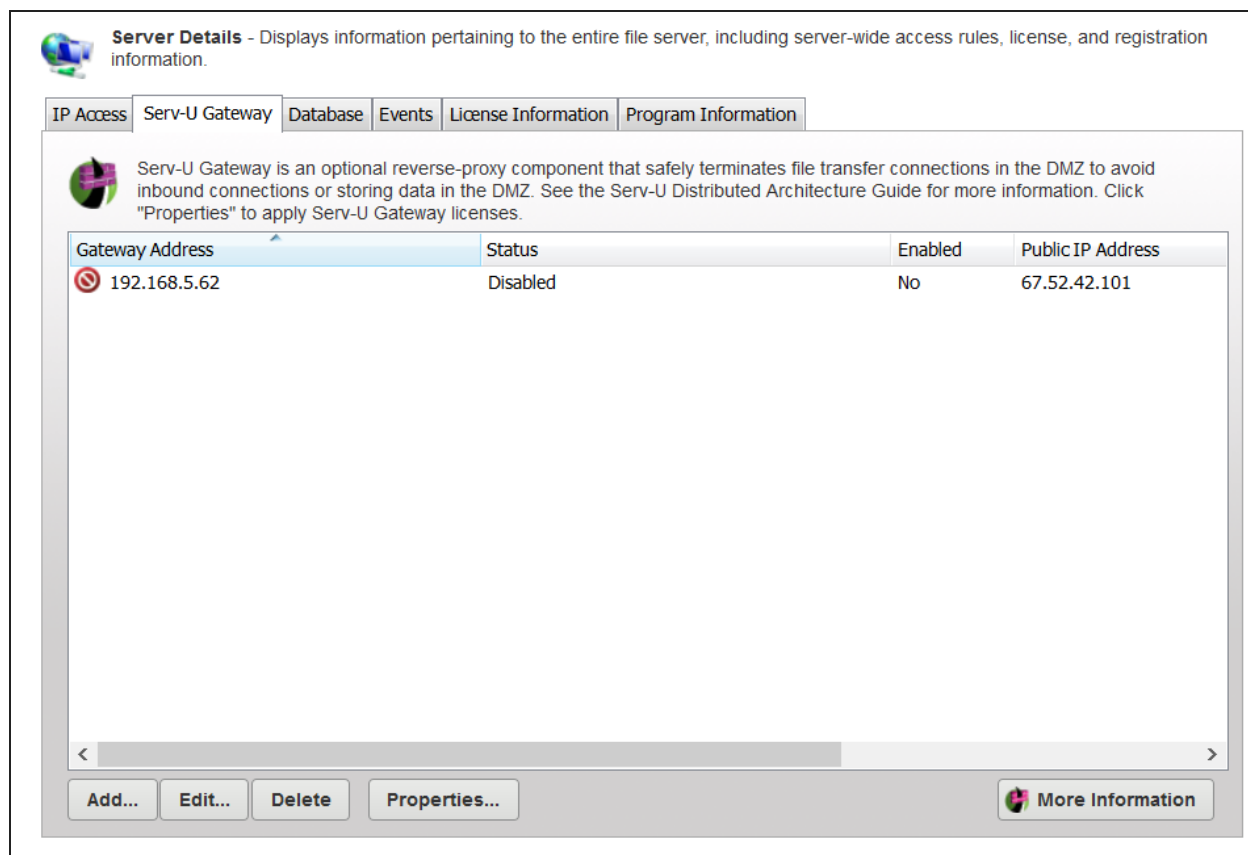
For examples of IP address rules and IP address caveats see [Examples of IP address rules and caveats](#).

## Serv-U Server Details: The Serv-U Gateway

The Serv-U Gateway provides defense in depth to Serv-U File Server deployments. It acts as a reverse proxy in demilitarized zone (DMZ) segments and prevents your Serv-U File Server deployments from storing data in the DMZ, or opening connections from the DMZ to the internal network. This type of architecture is essential to meet Payment Card Industry Data Security Standard (PCI DSS), managed file transfer, and other high-security requirements.

The Gateway tab in Server Details displays all configured gateways known to the Serv-U File Server deployment. Serv-U File Server periodically checks every configured gateway and displays a status message here.


 If you do not have Serv-U Gateway, you can download a free, 14-day trial copy by clicking [More information](#).




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

IP Access | **Serv-U Gateway** | Database | Events | License Information | Program 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

< >

Add... Edit... Delete Properties...  More Information





### Add a gateway

1. Navigate to Global > Server Details.
2. Click the Serv-U Gateway tab.  
The list of Gateways is displayed.
3. Click Add.

## 4. Enter the gateway details:

**Gateway Address** The gateway address is the IP address on the Gateway that Serv-U File Server uses to communicate with Gateway. This should almost always be a private IP address.

When listed, a status icon is displayed on the left of the gateway address.

Icon	Description
	The gateway is ready for connections. However, the gateway still needs listeners to receive connections.
	Serv-U is checking the status of the gateway. Another status will appear in a few seconds.
	The gateway is ready but the Serv-U installation is running close to the end of the trial period, or support period.
	An error occurred. For more information about why it is not possible connect to the gateway, select the gateway entry, and select Properties.

The icon in the Gateway Address column changes to reflect the current gateway status.

<b>Port</b>	The TCP port on the Gateway that Serv-U File Server uses to communicate with Gateway. The default is TCP port 1180.
<b>Status</b>	This displays a brief message that indicates the current status of the gateway.
<b>Public IP Address</b>	The Public IP Address column shows the IP address file transfer clients should connect to. A private IP address is displayed in the Public IP Address column if a private IP address was explicitly configured in the gateway. This occurs if the gateway has no public IP addresses, which is common during trials and situations in which the gateway is placed behind network address translation (NAT).
<b>Enable Gateway</b>	This option is used to turn the gateway on and off. The default is selected.
<b>Description</b>	An optional note about the gateway. It has no effect on the behavior.

## 5. Click Save.

The Gateway is added to the list.

## Edit a Gateway

1. Navigate to Global > Server Details

2. Click the Serv-U Gateway tab.

The list of Gateways currently installed is displayed.

3. Select a Gateway and click Edit.

4. Amend the gateway details as required.

5. Click Save.

## Display the Gateway properties

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

Status	<p>The large icon in the Status area and a status message indicate if the gateway is running, and whether or not it is running with a trial or commercial license.</p> <p>The Available Public IP Addresses field contains a list of all the public IP addresses automatically detected on Gateway. If a private address is configured in the Public IP Address field of the gateway, this field displays a message indicating that no public IP addresses are found on the gateway server. This is expected behavior.</p>
Install Information	<p>The Install Information area shows the version and build date of the Gateway software running on the gateway, the date Gateway was installed or last updated, and, if applicable, the number of days left in the evaluation period.</p>
Registration ID	<p>Copy and paste your Gateway Registration ID (not your Serv-U File Server Registration ID) into this field, and click Save to apply a commercial license to your Gateway software.</p> <p>If you have lost your registration ID, visit the Online Customer Service Center to retrieve it.</p>

For further information, see:

- [Introduction to the Serv-U Gateway](#)
- [Serv-U distributed architecture guide](#) (PDF)
- [Plan your Serv-U Gateway deployment](#)
- Gateway installation instructions:
  - [For Windows](#)
  - [For Linux](#)



## Serv-U Server details: Database

Serv-U File Server enables the use of an Open Database Connectivity (ODBC) database to store and maintain group and user accounts at both the server and domain levels.

Serv-U File Server can automatically create all the tables and columns necessary to store users and groups in the database. Because Serv-U File Server 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 and each domain must have unique ODBC connections to ensure they are stored separately.

### Configure a database


Create an ODBC connection for Serv-U File Server to use. SolarWinds recommends MySQL, but you can use any database that has an ODBC driver available.

1. Enter a Data source Name (DSN) if the Serv-U File Server is operating as a system service, or a User DSN if Serv-U File Server is operating as a regular application.
2. Open the Management Console and browse to the appropriate domain or server database settings. Enter the required information, and click Save.
3. If configuring the database connection for the first time, leave the "Automatically create" options selected. With these options selected, the SolarWinds Serv-U File Server builds the database tables and columns automatically.

### SQL templates

Serv-U File Server uses multiple queries to maintain the databases containing user and group information. These queries conform to the Structured Query Language (SQL) standards. However, if your database has problems working with Serv-U File Server, you may need to alter these queries.

1. Click SQL Templates.
2. In the SQL Templates window, modify each query used by Serv-U File Server to conform to the standards supported by your database, and click Close.

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

### User and group table mappings

By default, Serv-U File Server creates and maintains the tables and columns necessary to store user and group information in a database. However, if you want to connect Serv-U File Server to an existing database that contains this information, you must customize the table and column names to conform to the existing database structure.

1. Click User Table Mappings or Group Table Mappings to get started.
2. Select the Object Table.

Serv-U File Server 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. You can change the current table in 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 displays the table name and you can change the name.

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

3. Select an attribute and 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 can be disabled to reduce the number of ODBC (database) calls. For example, if you do not use [ratios and quotas](#), you can disable the User Ratio-Free Files, Per User Files Ratio, Per User Bytes Ratio, Per Session Files Ratio, and Per Session Bytes Ratio tables to prevent unnecessary ODBC calls. Use caution when you disable tables, because although the fields appear in dialogs, they will not be saved or loaded.

The User Info and Group Info tables cannot be disabled.

## Case file: ODBC authentication

Authentication in the SolarWinds Serv-U File Server can be handled through an ODBC database, allowing for scripted account management and maintenance. To use ODBC functionality, migrate to ODBC authentication through a database. By storing credentials in settings in a database, accounts can be managed from outside the 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 File Server is running as a service or a User DSN if Serv-U File Server is running as an application. After you create the appropriate DSN, enter the required information and click Save. Serv-U File Server creates the tables and columns. You can manage database users and groups in the Database Users and Database Groups pages of Serv-U File Server, located near the normal Users and Groups pages.

## Data source name creation in Linux

Database access in Serv-U File Server on Linux follows the same method as Serv-U File Server on Windows, with the one change to how data source names are created. On Linux, you can create a DSN after installing the following packages:

- `mysql-connector-odbc`
- `postgresql-odbc`
- `unixodbc`

Only the ODBC driver corresponding to the database needs to be installed. If Serv-U File Server 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 File Server 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 =
```

Adjust the names in brackets to the DSN name string you want. Finally, test the DSN with the `isql %DSN% -c -v` command.

For further customization options, see the [Serv-U Database Integration Guide](#).

## Serv-U Global Properties: Events (MFT only)

With the MFT edition of the Serv-U File Server, you can automatically associate file server events with email notifications, balloon tip alerts or posts to the Windows Event Log or Microsoft Message

Queue (MSMQ). For example, you might want to be notified in the event of a listener failure or whenever a new file is uploaded.

To access the Events tab for the entire server, navigate to Global > Server Details.

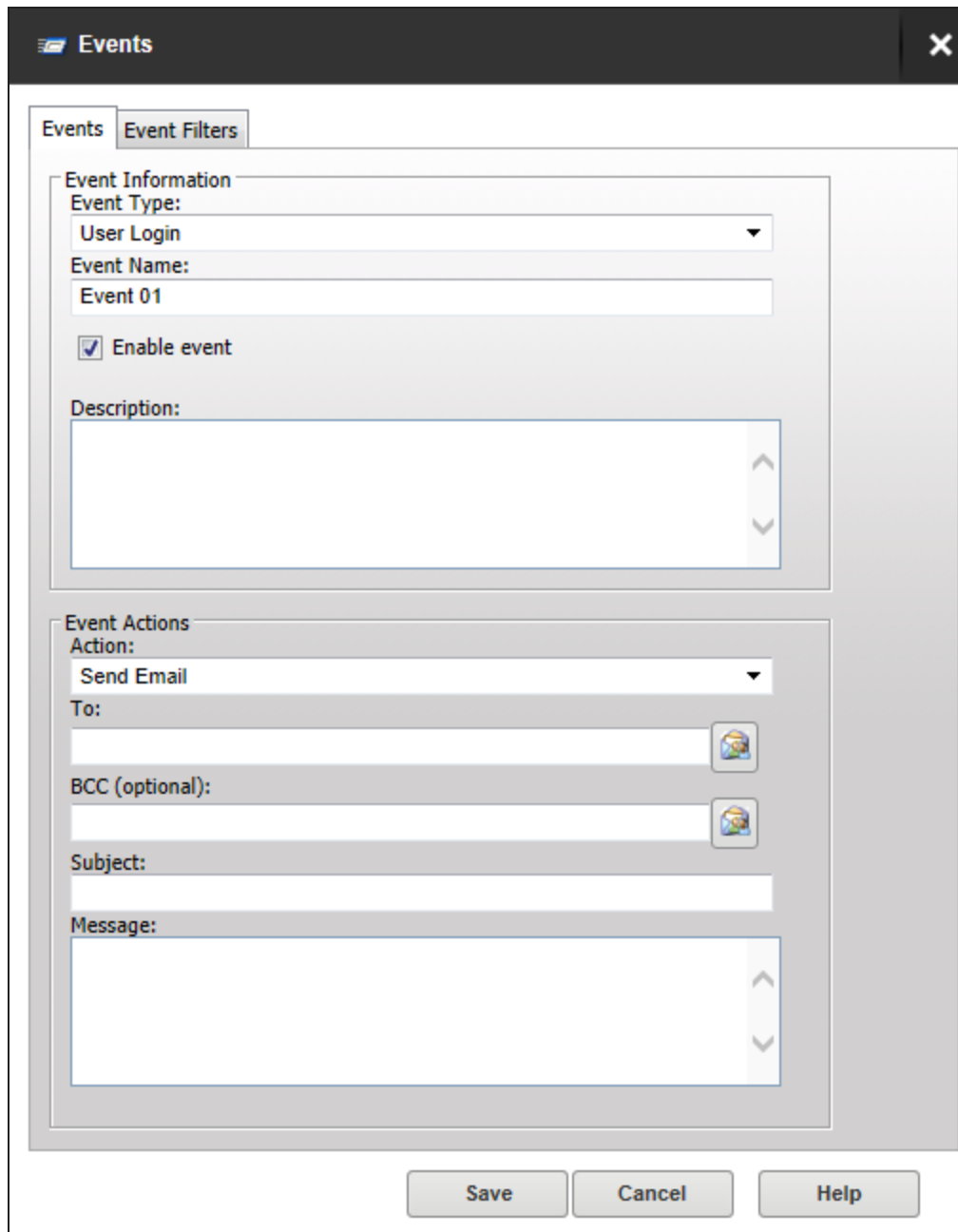
## Create Common Events

To instantly populate the events list with the most commonly used file server events:

1. Click Create Common Events.
2. Select the event action to apply to all common events.
3. Enter the email address to receive all notifications if you selected Send Email.
4. Enter the Message Queue Path if you selected Write to Microsoft Message Queue.
5. Click OK.
6. The 13 most common file server events are created. These can be customized by selecting an event and clicking Edit.

## Add an event

1. Click Add.



**Events** [X]

Events | Event Filters

**Event Information**

Event Type:  
User Login ▼


Event Name:  
Event 01


☒ Enable event

Description:

**Event Actions**

Action:  
Send Email ▼

To:  



BCC (optional):  


Subject:

Message:


Save Cancel Help

2. Select the Event Type.
3. Enter a name and description for this event.


 If you want to create but not immediately enable an event, uncheck the Enable event box.

4. Select the action to be triggered by this event, and complete the associated fields.


The actions that can be triggered are:

Event Action	Description
Send Email	<p>You can configure email actions to send emails to multiple recipients and to Serv-U File Server groups when an event is triggered.</p> <p>Enter the recipients in the To and BCC fields. Separate email addresses by commas or semicolons.</p> <p>To send emails to Serv-U groups, click the Group icon and drag the required groups from the Available Groups column to the Group Email List column.</p> <p>Enter the subject and message. You can use <a href="#">system variables</a> to include data specific to the event.</p>
Show Balloon Tip	<p>Balloon Tips are displayed in the system tray when an event is triggered. Balloon tip actions require a Balloon Title and Balloon Message. You can use <a href="#">system variables</a> to include data specific to the event.</p>
Execute Command (not available for Common Events)	<p>You can configure the execute of a file when an event is triggered. Execute command actions contain an Executable Path, Command Line Parameters, and a 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 zero to execute immediately.</p> <div> Time spent waiting delays any processing that Serv-U File Server can perform.</div> <p>A wait value should only be used to give an external program enough time to perform an operation, such as move a log file before it is deleted (for example, <code>\$LogFilePath</code> for the Log File Deleted event). You can use <a href="#">system variables</a> to use data specific to the event.</p>

Event Action	Description
Write to Windows Event Log (Windows only)	<p>By writing event messages to a local Windows Event Log, you can monitor and record Serv-U File Server activity using third-party network management software.</p> <p>The message entered into the Log Information field is 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. <a href="#">System variables</a> are supported for this field. This field can be left blank, but usually is not.</p>

Event Action	Description
Write to Microsoft Message Queue (MSMQ) (Windows only)	<p data-bbox="774 226 1511 590">Microsoft Message Queuing (MSMQ) is an enterprise technology that provides a method for independent applications to communicate quickly and reliably. Serv-U File Server can send messages to new or existing MSMQ queues whenever an event is triggered. 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 occurred.</p> <div data-bbox="786 625 1468 999"><p> Microsoft message queues created in Windows do not grant access to SYSTEM by default, preventing Serv-U File Server from writing events to the queue. 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 File Server runs) has permission to the queue.</p></div> <p data-bbox="774 1041 1382 1075">These events have the following two fields:</p> <p data-bbox="774 1106 1511 1598"><b>Message Queue Path:</b> The MSMQ path that addresses the queue. Remote queues can be addressed when a full path (for example, <code>MessageServer\Serv-U Message Queue</code>) is specified. Public queues on the local machine can be addressed when a full path is not specified (for example, <code>.\Serv-U Message Queue</code> or <code>Serv-U Message Queue</code>). If the specified queue does not exist, Serv-U File Server attempts to create it. This normally only works on public queues on the local machine. You can also use Serv-U File Server system variables in this field.</p> <p data-bbox="774 1629 1511 1871"><b>Message Body:</b> 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 File Server system variables can also be used in this field. This field may be left blank, but usually is not.</p>



 Only the email action is available to users other than Serv-U File Server server administrators.

## Edit an Event

1. Select the event you want to edit and click Edit.
2. Edit the event details and the event filters as required.
3. Click Save.

## Add an Event filter

Event filters allow you to control when a Serv-U File Server event action is triggered. By default, event actions are triggered each time the event occurs. Event filters allow events to be triggered only if certain conditions are met.

For example, a standard event may trigger an email each time a file is uploaded to the server. However, by using an event filter, events can be triggered on a more targeted basis, such as configuring a File Uploaded event to send an email only if the file name contains the string `important`. Thus an email would be sent when the file `Important Tax Forms.pdf` is uploaded but not for other files.

Additionally, you could configure a File Upload Failed event to run only when the FTP protocol is used, not triggering for failed HTTP or SFTP uploads. You can do this by controlling the variables and values related to the event and by evaluating their results when the event is triggered.

To add an event filter to an event:

1. Click the Events Filters tab.
2. Click Add.

**Event Filter**

Filters may have a unique name and description to identify them from other filters. Enable or disable the filter, select the appropriate filter logic and add filter comparisons using the tools below.

**Filter Information**

Name:

Description:

Logic

☒ AND ☐ OR

☒ Filter Enabled

Variable	Comparison	Constant	Data Type

Add... Edit... Delete...

3. Enter the following filter information:

Name	The name of the filter, used to identify the filter for the event.
------	--

Description (Optional)	The description of the event, which may be included for reference.
---------------------------	--

Logic	This determines how the filter interacts with any other filter set up for an event. In most cases, AND is used, and 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).
-------	--

4. Click Add to open the File Comparison window.
5. Select the [System Variable](#) to be used in the comparison.
6. Select the comparison method.

## 7. Enter the value the system variable is to be compared to. The following wild cards can be used.

- \* The asterisk wildcard matches any text string of any length. For example:
  - An event filter that compares the `$FileName` variable to the string `data*` matches files named `data`, `data7`, `data77`, `data.txt`, `data7.txt`, and `data77.txt`.
- ? The question mark wildcard matches any one character, but only one character. For example:
  - An event filter that compares the `$FileName` variable to the string `data?` matches a file named `data7` but not `data`, `data77`, `data.txt`, `data7.txt`, or `data77.txt`.
  - An event filter that compares the `$FileName` variable to the string `data?.*` matches files named `data7` and `data7.txt` but not `data`, `data77`, `data.txt`, or `data77.txt`.
  - An event filter that compares the `$Name` variable to the string `A????` matches any five-character user name that starts with `A`.
- [ ] The bracket wildcard matches a character against the set of characters inside the brackets. For example:
  - An event filter that compares the `$FileName` variable to the string `data[687].txt` matches files named `data6.txt`, `data7.txt` and `data8.txt` but not `data5.txt`.
  - An event filter that compares the `$LocalPathName` variable to the string `[CD]:\*` matches any file or folder on the `C:` or `D:` drives.

You can use multiple wildcards in each filter. For example:


- An event filter that compares the `$FileName` variable to the string `[cC]:\*.???` matches any file on the `C:` drive that ends in a three letter file extension.
- An event filter that compares the `$FileName` variable to the string `?:\*Red[678]\?????.*` matches 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.


## 8. Select the data type.

## 9. And another filter for this event or click Save to close.

### Filter examples

**Example 1.** An administrator may want to raise an email event when the file `HourlyUpdate.csv` is uploaded to the server, but not when other files are uploaded. To do this, create a new event 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 below:


**Filter Comparison**
✕


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

Save

Cancel


Help


If  = (is equal to)

Data Type:

**Example 2.** It may be necessary to know when a file transfer fails for a specific user account. To perform this task, create a new File Upload Failed event, and add a new filter.

The filter comparison is the \$Name variable, and the value to compare is the user name, such as ProductionLineFTP:


**Filter Comparison**
✕


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

Save


Cancel


Help

If  = (is equal to)

Data Type:

**Example 3, using wildcards.** You can also filter for events based on specific folders using wildcards. 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, create a new File Uploaded event in the Domain Details > Events menu, and set it to Send Email. Enter the email recipients, subject line, and message content, and then open the Event Filters page. 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\.


**Filter Comparison**
✕


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

Save

Cancel

Help

If  = (is equal to)

Data Type:

## Serv-U license information

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

Field	Description
Name	The name associated with the current license.
Email address	The email address associated with the current license.
Serv-U File Server edition	The Serv-U File Server edition that is enabled by the current license. For more information, see <a href="#">Serv-U File Server editions</a> .
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 Serv-U File Server is running as a trial version, the number of trial days remaining is displayed.
Additional products	Additional add-ons for Serv-U File Server, and whether they are enabled.
Edition information	The enabled functionality and limitations of the licensed Serv-U File Server edition.

### Registering Serv-U File Server

1. Navigate to Global > Server Details
2. Click the License Information tab.
3. Click Enter License ID at the bottom of the page.
4. Enter your alphanumeric registration ID.



- If you have lost your ID, click Lost ID to retrieve it.
- To purchase an ID, click Purchase to visit the Serv-U website.
- To upgrade, click Upgrade License.

## Serv-U program information

The Program Information tab displays Serv-U version, build and install date, operating system and legal information.

1. Navigate to Global > Server Details
2. Click the Program Information tab.


## Serv-U global users

A user account is required to access the file server. At its most basic level, a user account defines login credentials (that is, the login ID and password), a home directory, a set of directory access rules that define areas of the system accessible to this user, and the actions the user can perform in those locations. Each active session on the file server has a user account associated with it identifying the client to the administrator.

<a href="#">Global users</a>	Defined at the server level, global users can log in to any domain on the file server.
------------------------------	--


<a href="#">Database users</a>	Database users are stored in an external database accessible through ODBC and supplement the local account database.
--------------------------------	--

Because user accounts can be assigned at various levels with the same login ID, a hierarchy is used by Serv-U to determine which account takes precedence.

 Where user accounts can be specified at both the domain and server levels, the domain level account always takes precedence over the server account.

When you create users, consider what kind of access they will need, and select the appropriate location for the user account accordingly. You can save time and effort by entering such settings at the server level to remove the need for multiple user accounts at the domain level.

## User collections

 With Serv-U MFT Server, you can organize user accounts into collections to make account management more logical and organized. This can be useful when you manage all users from a department or physical location. For example, you can place all users in the accounting department in a collection named Accounting, or place all users at an office in Topeka in a collection named Topeka Users.

## Serv-U global users

- [Add a User using the Wizard](#)
- [Add a User manually](#)
- [The User Template](#)
- [Edit a User](#)
- [Copy a User](#)
- [User collections \(MFT only\)](#)
- [Recovering passwords](#)
- [Advanced settings](#)

You can add users at the global or domain level.

- Global users are defined at the server level and have access to all domains.
- Domain users are defined for the specific domain, and only have access to that domain.

For information on Domain users, see the [Domain Users](#) topic.

You can create users quickly using the wizard, or manually enter user properties for more precise set-up.

### View and add users at the global level

1. Click Global in the navigation column.
2. Click Users.



Users - Create, modify, and delete global user accounts for all domains on the file server.

Global Users
Database Users

This list shows the global user accounts that are allowed to connect to any domain on the file server. Global accounts can be overridden by creating the account on individual domains.

Select user collection  
General
Add...
Import...
Export...

Filter Users  

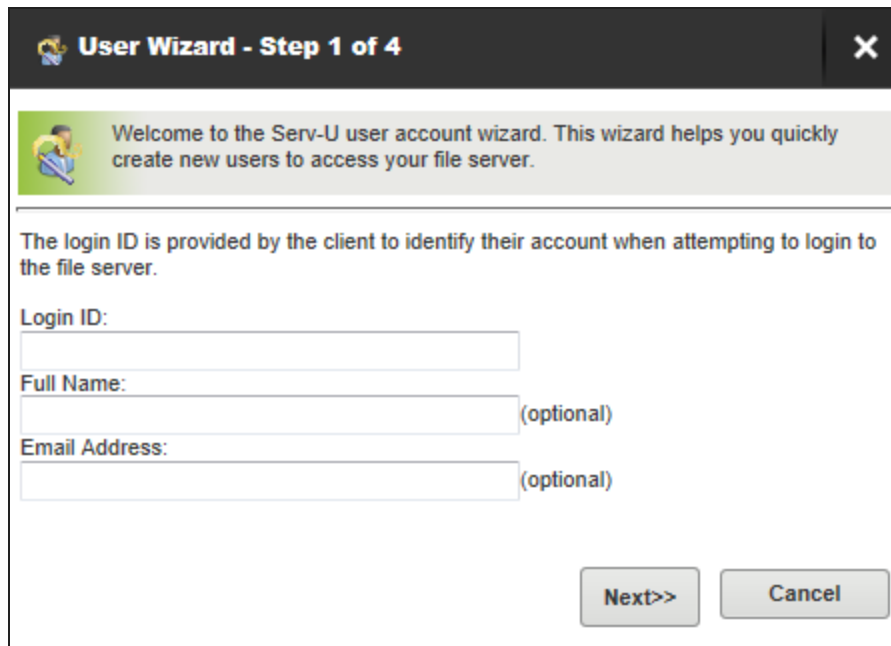
Clear Filter

Login ID	Full Name	Description	Last Login Time	Home Directory
chris1969	Christopher Cooper	Austin		%DOMAIN_HOM...
gill1988	Gillian Gill	Dublin		%DOMAIN_HOM...
helen1990	Helen Helvetica			%DOMAIN_HOM...

Add...
Edit...
Delete
Copy...
Move...
Wizard...
Template...
Recover Password


## Add a user using the wizard

1. Click the Wizard button. The User Wizard is displayed.



The dialog box is titled "User Wizard - Step 1 of 4" with a close button (X) in the top right corner. It features a green header bar with a wizard icon and the text: "Welcome to the Serv-U user account wizard. This wizard helps you quickly create new users to access your file server." Below this, a message states: "The login ID is provided by the client to identify their account when attempting to login to the file server." There are three input fields: "Login ID:" (required), "Full Name:" (optional), and "Email Address:" (optional). At the bottom right are "Next>>" and "Cancel" buttons.

2. Enter a unique login ID for the user.

 Login IDs cannot contain any of the following special characters:

\ / < > | : . ? \*

Two special login IDs exist: Anonymous and FTP. These are synonymous with one another, and can be used for guests. They do not require a password, so the Password field should be left blank. Serv-U requires users who log on with one of these accounts to provide their email address to complete the login process.

3. Optionally, enter a name and email address for this user.
4. Click Next.
5. Enter a password for this user, or accept the suggested eight character, complex password.

You can leave the password blank, which will enable anyone knowing the login ID to access this account.

You can place restrictions on the length and complexity of passwords, and disable the automatic password generator if required.

6. Check the box if you want the user to create their own password when they first login.



7. Enter or navigate to the home directory for this user. This is where the user is placed immediately after logging in to the file server. This must be specified using a full path including the drive letter or the UNC share name.

When you specify the home directory, you can use the %USER% macro 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 it is combined with a directory access rule for %HOME%, a new user can be configured with a unique home directory and the appropriate access rights to that location with a minimal amount of effort.

You can also use the %DOMAIN\_HOME% macro 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.

Check the Lock user in home directory box if you want this user's access to be restricted to this directory.

8. Click Next.
9. Select Read Only Access if you want this user to only be able to browse and download files or Full Access if you want to grant the user full control of files and directories in their home directory.
10. Click Finish.
11. The user is added to the list of users. You can edit this user if you want to apply more advanced settings.

## Add a User manually

1. Click the Add button.

The User Properties window is displayed.

**User Properties**

User account information specifies the login credentials and privileges granted to this account.

Login ID:   
 Password:    
 Administration Privilege:   
 Account Type:   
 Default Web Client:   
 Email Address:   
☒ Enable account

Full Name:   
 Home Directory:    
 SSH Keys:

☒ Lock user in home directory  
☐ Always allow login  
☐ User must change password at next login

Description:

2. Enter a unique login ID for the user.

Login IDs cannot contain any of the following special characters:

\ / < > | : . ? \*

Two special login IDs exist: Anonymous and FTP. These are synonymous with one another, and can be used for guests. They do not require a password, so the Password field should be left blank. Serv-U requires users who log on with one of these accounts to provide their email address to complete the login process.

3. Enter a name for this user.
4. Enter a password for this user, or click the lock button to create an eight character, complex password.

You can leave the password blank, which will enable anyone knowing the login ID to access this account.

You can place restrictions on the length and complexity of passwords through User limits. For more information about password limits, see [User Limits and Settings - Passwords](#).

5. Enter or navigate to the home directory for this user. This is where the user is placed immediately after logging in to the file server. This must be specified using a full path including the drive letter or the UNC share name.

When you specify the home directory, you can use the %USER% macro 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 it is combined with a directory access rule for %HOME%, a new user can be configured with a unique home directory and the appropriate access rights to that location with a minimal amount of effort.

You can also use the %DOMAIN\_HOME% macro 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.

6. Select the Administration Privilege for this user. This can be:

No Privilege	A regular user account that can only transfer files to and from the File Server. The Serv-U Management Console is not available.
Group Administrator	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, and they can also assign permissions at or below the level of the Group Administrator. They may not make any other changes.
Domain Administrator	<p>A Domain Administrator can only perform administrative duties for the domain to which their account belong, and 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 are:</p> <ul style="list-style-type: none"> <li>• configuring their domain listeners</li> <li>• configuring or administering LDAP groups</li> <li>• configuring ODBC database access for the domain</li> </ul>

System Administrator	A System Administrator can perform any file server administration activity including creating and deleting domains, user accounts, and even updating the license of the file server. A user account with System Administrator privileges logged in through HTTP remote administration can administer the server as if they had physical access to the server.
Read-only Group/Domain/Server Administrator	Read-only administrator accounts can allow administrators to log in and view configuration options at the group, 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, and cannot create, delete or edit user accounts.

7. If you have the MFT edition of Serv-U, you can specify a SSH public key to be used to authenticate a user when logging in to 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 of the domain, set in Domain Details > Settings, used if the keys are in a central folder relative to the domain home directory.

#### Examples:

`%HOME%\SSHpublic.pub`

`%HOME%\%USER%.pub`

`%DOMAIN_HOME%\SSHKeys\%USER%.pub`

For information on SSH public key authentication, adding a SSH key pair, and creating an key pair for testing, see [New SSH Key Pair Creation](#).


8. Select the account type. By default, all accounts are permanent and exist on the file server until they are manually deleted or disabled. You can configure an account 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 is displayed. Click the calendar or expiration date to select when the account should be disabled or deleted.

The account is accessible until the beginning of the day on which it is set to be disabled. For example, if an account is set to be disabled on 15 July 2015, the user can log in until 14 July 2015, 23:59.

9. Select the default web client to be displayed when a user logs in.

If you have the MFT edit, 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, you can also specify a default client. If you change this option, 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.


10. Enter an Email address for this user. Type an email address here to allow password recovery for the user account.

 For the MFT edition, this email address can also be used for event notifications.

11. Check or uncheck the following checkboxes:

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.
Lock user in home directory	Users 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 because Serv-U always reports it as "/" (root). The value of this attribute can be inherited through group membership.
Always allow login	<p>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. 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.</p> <p>Enabling the Always Allow Login option does not override <a href="#">IP access rules</a>. If both options are defined, the IP access rules prevail.</p>
User must change password at next login	<p>If enabled, the user will be prompted to change their password when they next log in.</p> <p>This option takes priority to the "Allow user to change password" setting on the Limits &amp; Setting tab. This means even if that setting is set to No, checking this box still will require the user to change their password.</p>

12. Enter an optional description of this user account.
13. Click Availability if you want to place limits on when this user can log in.
  - a. Check Apply limit and select the start and end time to specify the period this user may log in.
  - b. Tick the checkboxes for the days of the week on which this user may log in.
14. Click Welcome Message if you want to sent a welcome message to this user when they log in. This may also be set at the Group level.

 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 through SFTP over SSH2, because SSH2 does not define a method for sending general text information to users.

- a. Check Include if you want to include the response code in the welcome message test when an FTP connection is made.
- b. Either:
  - Select or navigate to a message file if you have already created a text file containing a welcome message.or:
  - Check the Override box, and enter a message specific to this user in the text box above it.
- c. Click Save.

## Advanced settings

Once you have added the User information you can use the following tabs on this window to complete the user setup.

### [Directory Access](#)

Directory access rules define the files and directories that the user has permission to access. At the user level, these rules are inherited from any groups the user belongs to as well as those rules defined at the domain and server level.

### [Virtual Paths](#)

Virtual paths are used to link a physical path that is outside the directory structure of the user's home directory into the directory listings received by that user.

### [Logging](#)

This tab provides checkboxes to configure what information you want to be logged.

<a href="#">Groups</a>	From the User Properties window you can select groups to which you want to add a user. Group membership allows you to assign various basic attributes to users that are members of the group.
<a href="#">Events</a>	MFT only: Events let you automatically run programs, send email and show messages when triggered by Serv-U activities.
<a href="#">IP Access</a>	Set up and maintain Server IP access rules so that specific IP address can be allowed or denied access to all your file server domains. These are checked when a physical connection is established with the file server, but before a welcome message is sent.
<a href="#">Limits &amp; Settings</a>	There are many options that can be applied at the user level. You can specify on which days and at which time these limits apply.

## The User Template

While the New User Wizard provides a way to quickly create a user account with the minimum number of required attributes, most File Server administrators have a collection of settings that 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. You can configure the template user 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.

By using user templates, you can add users to a specific default group. If you set up the user template as a member of the group you want all users to be a member of. This way, when new users are created, they will automatically be added to the particular group which is specified in the user template.

### Edit a User

Select a user and click Edit to open the User Properties window with the selected user's information.

### Copy a User

Select a user and click Copy to open the User Properties window with the selected user's information. You will need to supply at least a new Login ID to save the new user.

## User collections (MFT only)

In Serv-U MFT Server, you can organize user accounts into collections to make account management more logical and organized. This can be useful when you manage all users from a department or physical location. For example, you can place all users in the accounting department in a collection named Accounting, or place all users at an office in Topeka in a collection named Topeka Users.

To create a collection, click Add in the Select user collection area in the users window. In the new window, type the name of your collection, and then click Save. You can add users to this new collection by selecting them and clicking Add below the user list. To move a user from one collection to another, click Move below the user list, and then select the destination collection for the highlighted user accounts. You can also rename or delete collections by using the appropriate button.

When deleting a collection, all user accounts contained in that collection are deleted, too. If you want to keep the user accounts, make sure you move them before deleting the collection.

By default, all users are created in the General user collection.

## Recovering passwords

Serv-U supports password recovery both through the Management Console and through the Web Client. For password recovery to be available, you must configure the SMTP options for the server or domain, and the user account must have an email address listed. To use password recovery from the user page:

1. Select the user's account,
2. 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.



## Serv-U database users

You can connect the Serv-U File Server to an external database to load users and groups. Users and groups are loaded from the specified ODBC data source. These supplement the local user account database, and are displayed on the Database Users and Database Groups tabs in Server Details and Domain details. You can use different data sources at the global and each domain level. Changes to user and groups accounts stored in this manner can be made through this interface or one supported by the database.

## Serv-U groups

Groups provide a method of sharing common configuration options with multiple user accounts. Configuring a group is similar to configuring a user account. Groups can be created at the server or domain level.

Virtually every configuration option available for a user account can be set at the group level. 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.

At the server level, the following options are available:

<a href="#">Global Groups</a>	Add or edit groups available to global user accounts on the file server.
<a href="#">Database Groups</a>	Database groups are loaded from the specified ODBC data source and supplement the local group database.

At the domain level, the additional options are available:

<a href="#">Windows Groups</a>	Create and maintain groups representing settings for your Windows Organization (OU).
<a href="#">LDAP Groups</a>	Create and maintain groups representing settings for your LDAP groups.

## Global groups

- [Add a Group](#)
- [Advanced settings](#)
- [Edit a Group](#)
- [The Group Template](#)

Groups provide a method of sharing common configuration options with multiple user accounts. Configuring a group is similar to configuring a user account. Groups can be created at the server or domain level.

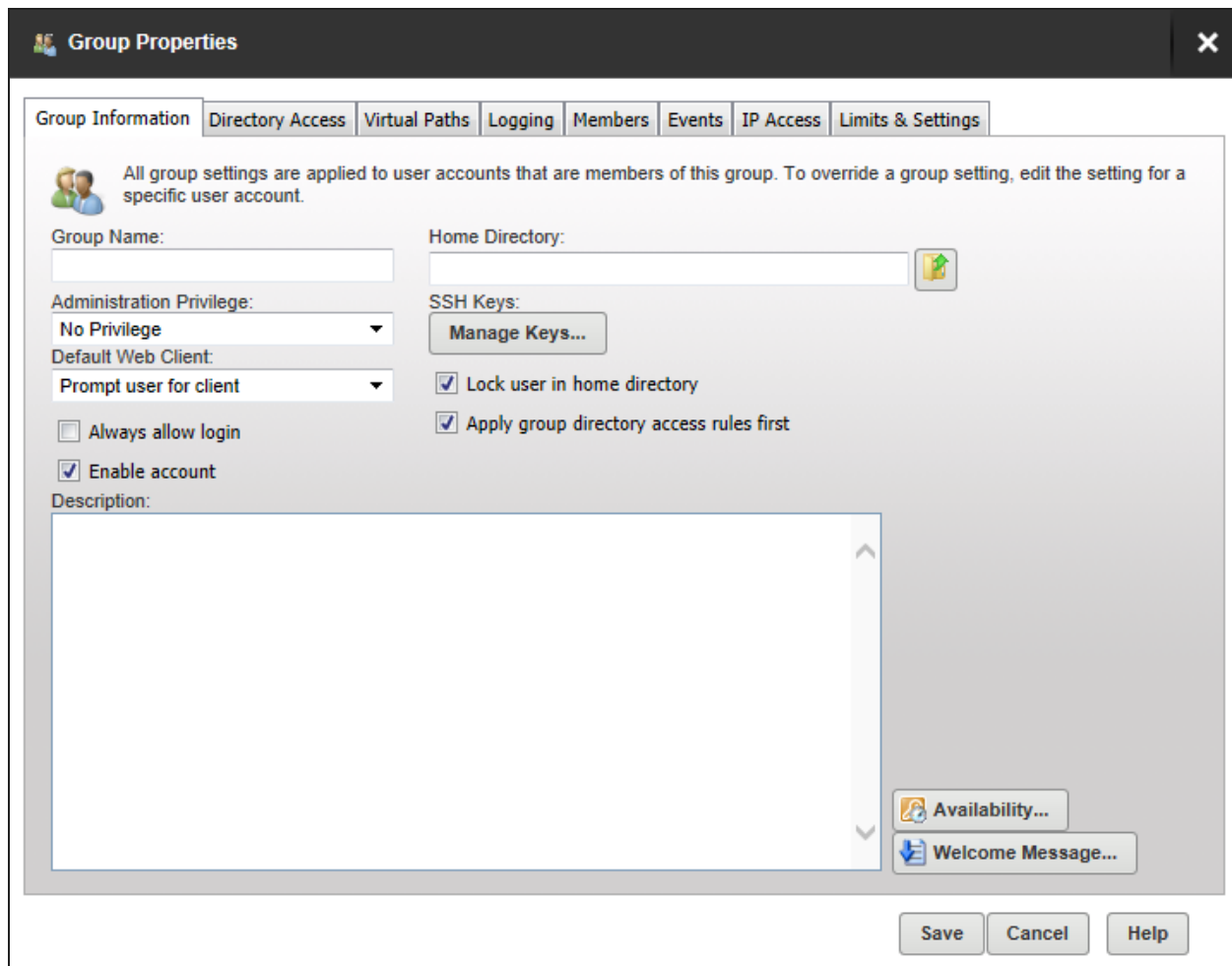
Virtually every configuration option available for a user account can be set at the group level. For a user to inherit a group's settings, it must be a member of the group. Permissions and attributes inherited by a user through group membership can still be overridden at the user level. A user can be a member of multiple groups in order to acquire multiple collections of permissions, such as directory or IP access rules.

However, groups are only available to user accounts that are defined at the same level. In other words, a global user (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.

## Add a Group

1. From the Groups page, click the Add button.

The Group Properties window is displayed.




**Group Properties**

Group Information | Directory Access | Virtual Paths | Logging | Members | Events | IP Access | Limits & Settings

All group settings are applied to user accounts that are members of this group. To override a group setting, edit the setting for a specific user account.

Group Name:

Home Directory:  

Administration Privilege: **No Privilege**

Default Web Client: **Prompt user for client**

☐ Always allow login

☒ Enable account

SSH Keys:

☒ Lock user in home directory

☒ Apply group directory access rules first

Description:

2. Enter or navigate to the home directory for users in this group. This is where the users are placed immediately after logging in to the file server. This must be specified using a full path including the drive letter or the UNC share name.

When you specify the home directory, you can use the %USER% macro 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 it is combined with a directory access rule for %HOME%, a new user can be configured with a unique home directory and the appropriate access rights to that location with a minimal amount of effort.

You can also use the %DOMAIN\_HOME% macro 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.

3. Select the Administration Privilege for this users in this group. This can be:

No Privilege	A regular user account that can only transfer files to and from the File Server. The Serv-U Management Console is not available.
Group Administrator	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, and they can also assign permissions at or below the level of the Group Administrator. They may not make any other changes.
Domain Administrator	<p>A Domain Administrator can only perform administrative duties for the domain to which their account belong, and 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 are:</p> <ul style="list-style-type: none"><li>• configuring their domain listeners</li><li>• configuring or administering LDAP groups</li><li>• configuring ODBC database access for the domain</li></ul>
System Administrator	A System Administrator can perform any file server administration activity including creating and deleting domains, user accounts, and even updating the license of the file server. A user account with System Administrator privileges logged in through HTTP remote administration can administer the server as if they had physical access to the server.
Read-only Group/Domain/Server Administrator	Read-only administrator accounts can allow administrators to log in and view configuration options at the group, 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, and cannot create, delete or edit user accounts.

4. If you have the MFT edition of Serv-U, you can specify a SSH public key to be used to authenticate users in this group when logging in to 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 of the domain, set in Domain Details > Settings, used if the keys are in a central folder relative to the domain home directory.

**Examples:**

```
%HOME%\SSHpublic.pub
```

```
%HOME%\%USER%.pub
```

```
%DOMAIN_HOME%\SSHKeys\%USER%.pub
```

For information on SSH public key authentication, adding a SSH key pair, and creating an key pair for testing, see [New SSH Key Pair Creation](#).

5. Select the default web client to be displayed when a user in this group logs in.

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, you can also specify a default client. If you change this option, 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.

6. Check or uncheck the following checkboxes:


Always allow login	<p>Enabling this option means that users in this group are 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. As with any option that allows bypassing access rules, care should be taken in granting this ability.</p> <p>Enabling the Always Allow Login option does not override IP access rules. If both options are defined, the IP access rules prevail.</p>
Enable account	<p>Deselect this option to disable user accounts in this group. Disabled accounts remain on the file server but cannot be used to log in. To re-enable accounts in this group, select the Enable account option again.</p>
Lock user in home directory	<p>Users 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 because Serv-U always reports it as "/" (root).</p>
Apply group directory access rules first	<p>Deselect this option to place the directory access rules of the group below the user access rules.</p> <p>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 directory access rules specified at the user level. However, there are certain instances where you may want the user level rules to take precedence.</p>

7. Enter an optional description for this group account.

8. Click Availability if you want to place limits on when users in this group can log in.

- Check Apply limit and select the start and end time to specify the period users in this group may log in.
- Tick the checkboxes for the days of the week on which users in this group may log in.

9. Click Welcome Message if you want to sent a welcome message to the users in this group when they log in.

 The welcome message is a message traditionally sent to FTP clients 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 through SFTP over SSH2, because SSH2 does not define a method for sending general text information to users.

- a. Check Include if you want to include the response code in the welcome message test when an FTP connection is made.
- b. Either:
  - Select or navigate to a message file if you have already created a text file containing a welcome message.
 or:
  - Check the Override box, and enter a message specific to this user in the text box above it.
- c. Click Save.

## Advanced settings

Once you have added the Group information you can use the following tabs on this window to complete setup.

<a href="#">Directory Access</a>	Directory access rules define the files and directories that users in this group have permission to access. At the group level, these rules are inherited from the domain and server level.
<a href="#">Virtual Paths</a>	Virtual paths are used to link a physical path that is outside the directory structure of the home directory of users in this group into the directory listings received by that user.
<a href="#">Logging</a>	This tab provides checkboxes to configure what information you want to be logged.
<a href="#">Members</a>	Displays the list of users in this group. This tab is display only - you need to use the <a href="#">Groups</a> tab in the individual User Properties to select the groups to which that user belongs.
<a href="#">Events</a>	MFT only: Events let you automatically run programs, send email and show messages when triggered by Serv-U activities.
<a href="#">IP Access</a>	Set up and maintain Server IP access rules so that specific IP address can be allowed or denied access to all your file server domains for users in this group. These are checked when a physical connection is established with the file server, but before a welcome message is sent.
<a href="#">Limits &amp; Settings</a>	There are various options that can be applied at the group level. You can specify on which days and at which time these limits apply.

## Edit a Group

Select a group and click Edit to open the Group Properties window, allowing you to edit that information for users in this group.

## The Group Template

You can configure a template for creating new groups by clicking Template. The template group can be configured just like any other group, with the exception of giving it a name. After the settings are saved to the template, all new groups are created with their default settings set to those found within this template. This way you can configure the basic settings that you want all of your groups to use by default.

## Serv-U database groups

Database groups are loaded from the specified ODBC data source. They supplement the local group database. Changes to groups stored in this manner can be done through this interface or one supported by the database.

## Serv-U global directories

This tab enables you to configure the basic directory structure available to all users of the file server, including default directory access rules, virtual paths and file management rules.

Default directory access rules, virtual paths and file management rules can also be defined at the [domain](#), [groups](#) and [user](#) level.

---

### [Directory Access](#)

Server directory access rules are global rules defining the files and directories to which all users on this server have access.

### [Virtual Paths](#)

Virtual paths are used to link a physical path outside of the directory structure of the user's home directory into the directory listings received by that user.

### [File Management](#)

File Management Rules allow Serv-U to automatically remove or archive files from your File Server.

---



## Serv-U directory access rules

Directory access rules define which areas of the system are accessible to user accounts. Directory access rules specified at the server level are inherited by all users of the file server. If they are specified at the domain level, they are only inherited by users who belong to the particular domain. The traditional rules of inheritance apply where rules specified at a lower level (for example, the user level) override conflicting or duplicate rules specified at a higher level (for example, the server level).

When you set the directory access path, you can use the `%USER%`, `%HOME%`, `%USER_FULL_NAME%`, and `%DOMAIN_HOME%` variables to simplify the process.

**i** For example, use `%HOME%/ftproot/` to create a directory access rule that specifies the `ftproot` folder in the home directory of the user.

Directory access rules specified in this manner are portable if the actual home directory changes while maintaining the same subdirectory structure. This leads to less maintenance for the file server administrator. If you specify the `%USER%` variable 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. You can use the `%USER_FULL_NAME%` variable 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\%USER_FULL_NAME%` for `D:\ftproot\Tom Smith`. You can also use the `%DOMAIN_HOME%` macro 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 listed. The first rule in the list that matches the path of a client's request is the one 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 particular subdirectory. Use the arrows on the right of the directory access list to rearrange the order in which the rules are applied.

**i** Serv-U File Server allows to list and open the parent directory of the directory the user is granted access to, even if no explicit access rules are defined for the parent directory. However, the parent directory accessed this way will only display the content to which the user has access.

## Permissions

### File Permission

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

## File Permission

Append	Allows users to append data to existing files. This permission is typically used to enable users to resume transferring partially uploaded files.
Rename	Allows users to rename files.
Delete	Allows users to delete files.
Execute	Allows users to remotely execute files. The execute access is meant for remotely starting programs and usually applies to specific files. This is a powerful permission and great care should be used in granting it to users. Users with Write and Execute permissions can install any program on the system.

## Directory Permission

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.
Create	Allows users to create new directories within the directory.
Rename	Allows users to rename directories within the directory.
Remove	Allows users to delete existing directories within the directory.  If the directory contains files, the user also must have the Delete files permission to remove the directory.

## Subdirectory Permission

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 (for example, when implementing mandatory access control), clear the Inherit check box and grant permissions specifically by folder.
---------	--


## 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 would result in the directory content 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.

### Advanced: Access as Windows user (Windows only)

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 File Server, you can configure the SolarWinds Serv-U File Server service to run under a network account. The alternative, preferred where many servers exist, or if the SolarWinds Serv-U File Server service has to run under Local System for security reasons, is to configure a directory access rule to use a specific Windows user for file access. Click Advanced to specify a specific Windows user for each directory access rule. As in Windows authentication, directory access is subject to NTFS permissions, and in this case also to the configured permissions in Serv-U File Server.

 When you use Windows authentication, the NTFS permissions of the Windows user take priority over the directory access rules. This means that when a Windows user tries to access a folder, the security permissions of the user are applied instead of the credentials specified in the directory access rule.

## Examples

### Mandatory access control

You can use mandatory access control (MAC) 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.

In the following example, the rule applies to `C:\ftproot\`.

**Directory Access Rule** [X]

Path: C:\ftproot\ [Folder Icon]

[Save] [Cancel] [Help] [Full Access] [Read Only] [Advanced >>]

**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 SolarWinds Serv-U File Server.

#### Restrict file types

If users are using storage space on the SolarWinds Serv-U File Server to store non-work-related files, such as .mp3 files, you can prevent this by configuring a directory access rule placed above the main directory access rule 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:



**Directory Access Rule**

Path: \*.mp3

**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)

Buttons: Save, Cancel, Help, Full Access, Read Only, Advanced >>

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 the directory to which they need access.



**Directory Access Rule**

Path: %HOME%

**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)

Buttons: Save, Cancel, Help, Full Access, Read Only, Advanced >>

In the second rule, enter the extension of the file that should be accessed, such as \*.mdb.

**Directory Access Rule**

Path: \*.mdb

**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)

Buttons: Save, Cancel, Help, Full Access, Read Only, Advanced >>

These rules only allow users to access .mdb files within the specified directories. You can adapt these rules to any file extension or set of file extensions.

Directory Access		Virtual Paths	File Management
Domain directory access rules are global rules that define the files and directories overridden at the group and user levels.			
Path	Access		
*.mdb	RWADN-L---I		
%HOME%	-----L---I		

## Serv-U virtual paths

If virtual paths are specified, users can 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 access 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 all users of the file server.

## 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, use a full path, such as `D:\inetpub\ftp\public`. You can also use a UNC path, such as `\\Server\share\public`. To make a virtual path visible to users, users must have a directory access rule specified for the physical path.

## Virtual path

The virtual path is the location 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. You can also use a full path without any macros.

Include virtual paths in Maximum Directory Size calculations

When this option is selected, the virtual path is included in Maximum Directory Size calculations. The Maximum Directory Size limits the size of directories affecting how much data can be uploaded.

## Examples

### Virtual paths

A group of web developers have been granted access to the directory `D:\ftproot\example.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 group of web developers, add a virtual path to bring the directory to the users by specifying `D:\corpimages\` as the physical path and `D:\ftproot\example.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.

### Relative virtual paths

Continuing with the previous example, if the home directory of the group of web developers is relocated to another drive, both the home directory and the virtual path must be updated to reflect this change. You can avoid this 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\example.com\corpimages` as the virtual path, use `%HOME%\corpimages`. This way the `corpimages` virtual path is placed within the home directory of the group, regardless of what the home directory is. If the home directory changes at a later date, the virtual path still appears there.

## Serv-U file management

File management rules enable you to automatically remove or archive files from the file server. You can configure file management rules at the server and domain level.

- If they are specified at the server level, the file management rules are accessible to all users of the file server.
- If they are specified at the domain level, they are only accessible to users belonging to that domain.


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

 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 File Server. This way you can manage files that are transferred by clients, or that are copied to the folder outside of Serv-U File Server.

The folder structure is not affected by the file management rules. When expired files are deleted or moved, the folders themselves remain intact.

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


 If you have the MFT edition of Serv-U File Server, you can monitor the status of the file management rules by configuring File Management Rule Success and File Management Rule Error events under Server Details or Domain Details > Events. The file management rules continue to run even if deleting or moving a single file fails. For more information, see [Events](#).

### Define a new file management rule

1. Navigate to Directories > File Management, and click Add.
2. Enter 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 in the Destination Directory Path field, specify the folder where you want to move the file.
4. Specify the number of days after the file creation date when the action should be executed.
5. Click Save.

 Serv-U File Server regularly checks each file in the directory for its age, and performs the specified action on the files that meet the age criteria specified.

## Serv-U server limits and settings

Limits and settings are used to configure the basic settings and behavior for the entire file server, including FTP command processor customization and SSL/SSH encryption and certificate options. Limits and settings configured at the server level are inherited by all domains, groups, and users.

### Limits

Limits are grouped based upon the area of the server they are responsible for configuring. Limits allow specifying multiple values for the same option that are applied based upon the time of day and the day of the week. Server level limits can be overridden at the domain, group, and user level.

### Settings

Server level settings configure the global behavior of the file server. Some settings are used by the domains, user accounts, and groups as default values when not overridden.

### FTP Settings

The server FTP command processor configures advanced behavior such as the text responses to FTP commands, FTP command settings, or disabling the use of an FTP command by clients.

### Encryption

Encryption options specified at the server level are used by default unless overridden at the domain level with different information. The advanced SSL and SSH encryption options can only be configured at the server level.

### Custom HTML

The Custom HTML feature is used to customize the look of your Serv-U File Server login page.

### File Sharing (MFT only)

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


## Serv-U server limits

There are many options to customize how Serv-U can be used, and these can be set at the user, group, domain, and server level.

- For the Domain Limits page, click [here](#).
- For the User Properties: Limits page, click [here](#).
- For the Group Properties: Limits page, click [here](#).

The limits stack intelligently, so user settings override group settings, group settings override domain settings, and domain settings override server settings. In addition, you can configure limits so they only apply during certain days of the week, and certain times of the day.

Select Limits and Settings from the Global menu. The Limits tab is displayed by default.

 Most limits and settings on this tab are self-explanatory. However, the "Allow users to change password" setting in the Password limit types is overridden by the "User must change password at next login" option if set to No.

Default limits are displayed against a blue background. These cannot be edited or deleted, but can be overridden by adding a new limit.


### Override a default limit

1. Select the Limit Type containing the limit to override.
2. Click Add.
3. Select the limit to add.
4. Enter the value for the limit.
5. Click Advanced to specify a day and time to which this limit applies.
6. Check the Apply limit only at this time of day if you want to specify a time period for which this limit is in force, and select the Start and End Times.
7. Select the Days of the Week for which this limit applies.
8. Click Save.

The new limit is displayed in the list. (The default is still displayed, even though it is overridden.)

## Edit a limit

1. Select a non-default limit, and click Edit.

 If you try to edit a default limit a message is displayed informing you that default limits cannot be edited and asking if you want to create a new limit to override it.

2. Amend the value as required.
3. If you want to change the day and time to which this limit applies, click Advanced.
4. Click Save.

## Serv-U server settings

On the Server Limits & Settings > Settings pages, you can configure basic settings that affect performance, security, logo-in display, and network connectivity for the entire file server . 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 you can configure.

### 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 for legitimate users to correct an incorrect password before they are blocked.

When enabled, this option temporarily blocks (for the specified number of minutes) IP addresses that fail to successfully login (after the specified number of attempts within the specified number of seconds). IP addresses blocked in this way can be viewed in the appropriate IP access rules tab. A successful login resets the counter that is tracking login attempts.

**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 provided to the client.

**Default Web Client** For the MFT Server, this enables you to specify whether the Web Client, Web Client Pro, FTP Voyager JV or File Sharing should be used by all HTTP clients by default. The third, default option is to prompt the users for the client they want to use instead. This option is also available at the group and user level.

## Custom HTTP Logo, Login Page Text & Title Settings

HTTP Login Title Text (no HTML)	Enter a text-only title to appear when a HTTP client logs into the file server.
Custom Logo Path	<p>To use your own custom logo, create a 400 x 100 pixel graphic and enter or navigate to its location. An error message will be displayed if this criteria is not met.</p> <p>To reset to original Serv-U log, select &lt;&lt;Inherit default value&gt;&gt; from the drop-down menu.</p>
HTTP Login Page Text	<p>Enter the text to be displayed on the HTTP login page.</p> <p>This text can be HTML-formatted, including links, images, and standard formatting like italics, bold, underline, alignment and more.</p>
HTTP Client Interface Background (CSS Only)	<p>MFT only. Enter a CSS background style for the Web Client, File Sharing and FTP Voyager JV landing page. The format is:</p> <pre>color url('/%CUSTOM_HTML_DIR%/images/yourimage.png') repeat-type horizontal-alignment vertical-alignment.</pre> <p>The %CUSTOM_HTML_DIR% must be used in conjunction with the Custom HTML settings. Custom HTML must be enabled and a Custom HTML Container Directory must be specified.</p> <p>The following examples provide a reference:</p> <ul style="list-style-type: none"><li>• #0b16f8 url('/%CUSTOM_HTML_DIR%/images/Header01.png') no-repeat right top</li><li>• #FFFFFF url('/%CUSTOM_HTML_DIR%/images/MyLogoTile.png') repeat-x left top</li><li>• red (this example uses no image)</li><li>• url('/%CUSTOM_HTML_DIR%/images/MyHeader.png') no-repeat center top (this example uses no custom color)</li></ul>

## 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	<p>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 the PASV port range of Serv-U to a known range. A range of 10 ports is sufficient for the busiest of file servers.</p> <p>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.</p>
Require matching peer IP address for control and data connections	To avoid the risk of FTP bounce attacks, check this box to ensure the peer address of the control connection matches that of the data connection. If they do not match, the transfer will be disallowed. If you are making server-to-server transfers you will need to leave this box unchecked.

## Password Recovery Message

Subject	The subject line for the password recovery message.
---------	---


## Password Recovery Message

Message	Unless using the inherited or default message, enter the message for the password recovery message to be sent to the client.  \$Name will display the user name.  \$Password will display the user password.
Configure SMTP	Click to <a href="#">configure SMTP</a> for the server.

## Other settings


Integration Library	For information about writing an Integration DLL or Shared Library, see the Serv-U Integration Sample DLL in the Serv-U Integration Sample DLL sub-directory. The Integration API is documented in this sample.
<a href="#">Ratio Free Files</a>	Files listed by clicking the Ratio Free Files button are exempt from <a href="#">transfer ratio</a> limitations on file transfers. Ratio Free Files specified at the server or domain level are inherited by all their user and group accounts.
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.

## Serv-U server FTP settings

 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.

### Edit FTP commands and responses

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

 Only the Information and FTP Responses tabs are displayed for all commands. Other tabs are displayed depending on the command type.

Information	On the Information page, basic information about the command is shown along with a link to more information on the Serv-U website. The command can also be disabled by selecting the Disable command option here. Disabled commands are treated as unrecognized commands when received from a client.
-------------	---

FTP Responses	All possible FTP responses to the command as issued by the server are displayed on this tab, and can be modified by clicking Edit for each response. Not all commands have FTP responses. FTP command responses can contain special macros that allow real-time data to be inserted in to the response. For more information, see <a href="#">System variables</a> .
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 home directory of the user for the Message File. If the first message file is not found, 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.
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 impacted by users requesting excessively large listings, recursive listings can be disabled by using the Allow client to specify recursive directory listings with -R parameter option.
Advanced Options	<p>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. The following FTP commands contain advanced configuration options:</p> <ul style="list-style-type: none"><li>• LIST</li><li>• MDTM</li><li>• NLST</li></ul>

## Global Properties

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 <a href="#">System variables</a> .
---------------	--

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, 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 the 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	<p>The following options apply to the FTP protocol in general:</p> <p>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.</p> <p>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 three-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.</p> <p>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.</p>

## 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 about 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 DELETE 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.

## Serv-U Server 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.

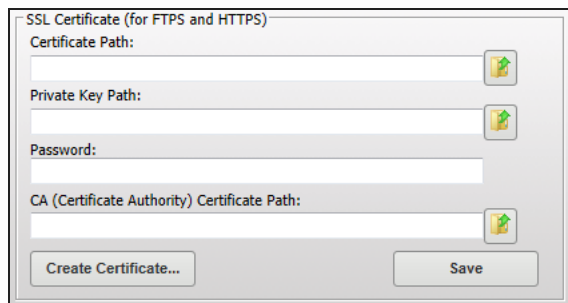
In order for each of these methods of encryption to work, a certificate, a private key, or both must be supplied. SSL requires the presence of both, while SSH2 only requires a private key. If you do not have either of these required files, you can create them in Serv-U.


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

### Configure SSL for FTPS and HTTPS

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 on the server.
3. In Serv-U, go to Global > Limits & Settings > Encryption.

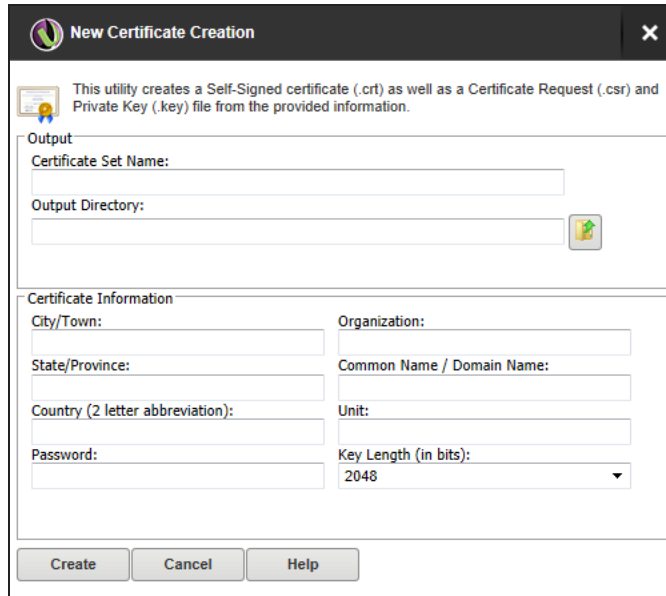


4. Use the appropriate Browse buttons  to select both the certificate and private key files.
5. Enter the password used to encrypt the private key file.
6. If a CA (Certificate Authority) PEM file has been issued, enter or browse to the file.
7. Click Save.

If the provided file paths and password are all correct, Serv-U will start 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.

## Create a new certificate

1. In Serv-U, go to Global > Limits & Settings > Encryption.
2. Click Create Certificate.  
The New Certificate Creation window is displayed.



The dialog box is titled "New Certificate Creation" and contains the following sections:


- Output:** Fields for "Certificate Set Name:" and "Output Directory:" with a folder icon button next to the latter.
- Certificate Information:** Fields for "City/Town:", "State/Province:", "Country (2 letter abbreviation):", "Password:", "Organization:", "Common Name / Domain Name:", "Unit:", and "Key Length (in bits):" (set to 2048).
- Buttons at the bottom: "Create", "Cancel", and "Help".

3. Specify the Certificate Set Name to name each of the files Serv-U creates. For example entering "myName" would result in the creation of:

myName.crt	The self-signed certificate file. This can be used immediately on the server but is not authenticated by any known certificate authority.
myName.csr	The certificate request file. This can be provided to a certificate authority for authentication.
myName.key	The private key file. This is used to secure both certificate files. It is extremely important that you keep the private key in a safe and secure location. If your private key is compromised, your certificate can be used by malicious individuals.

4. Specify the output path where these files are to be placed. In most cases, the installation directory is a safe location. For example: `C:\ProgramData\SolarWinds\Serv-U\`.
5. Enter the city, state (if applicable), two-digit country code, organization, and unit where file server or corporation is located.

6. Specify a password for create the private key.
7. Specify the common name/domain name for the certificate. The IP address or the Fully Qualified Domain Name (FQDN) that users use to connect should be used here.

 If you do not supply the IP address or FQDN used by clients to connect, clients may be prompted that the certificate does not match the domain name to which they are connecting.

8. Select the required key length. 1024 bits provides best performance, 2048 bits is a good median, and 4096 bits provides best security.
9. Click Create.  
The three files are now be created in the specified directory.

## View the certificate

To view the SSL certificate when 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 window.

## 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.

Serv-U now supports SSLv3, TLSv1.0, TLSv1.1 and TLSv1.2 and 21 cipher suites, including Camellia, SEED, higher levels of SHA, and GCM cipher suites where encryption and authentication are native rather than two discrete operations. Serv-U also supports other cipher suites which enable perfect forward secrecy (PFS).

You can configure the following in the advanced SSL options:

Disable SSLv3 support	Serv-U supports several different versions of SSL. SSLv2 and SSLv3 have documented security weaknesses making it less secure than TLS. However, it may be necessary to support SSLv2 or SSLv3 for compatibility with exported clients or old client software. Select the relevant option to disable support for the SSLv2 or SSLv3 protocols.
Disable TLSv1.0, TLSv1.1 or TLSv1.2 support	For compatibility reasons, it may be necessary to disable certain versions of TLS. Select the relevant option to disable support for TLSv1.0, TLSv1.1 or TLSv1.2.

To enable or disable specific cipher suites, click Configure Cipher Suites.

You can configure the following cipher suites:

TLSv1.2 only cipher suites	Cipher suites used only by TLSv1.2. If TLSv1.2 is disabled, changing a setting here has no effect.
TLSv1.x and SSLv3 cipher suites	Cipher suites used by SSLv3 and all versions of TLSv1.

## 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.

By enabling FIPS mode, the OpenSSL library of Serv-U will run in FIPS compliant mode.

When FIPS 140-2 mode is enabled, ciphers which are not FIPS compliant are not accepted, and applications which are not FIPS compliant cannot connect to Serv-U.

In practice it means that older hardware and legacy applications which have embedded support for, for example, SSH, may stop working correctly when FIPS mode is enabled. Additionally, non-compliant SSH keys and certificates stop working after enabling FIPS mode.

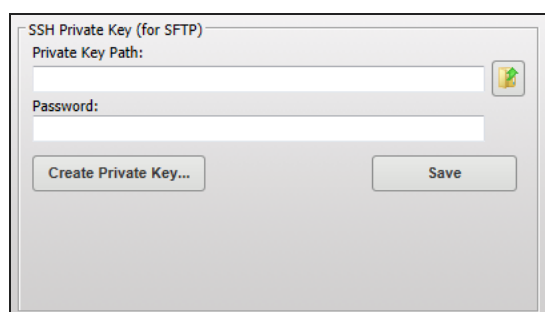
To avoid these issues, the recommended workflow is to first enable FIPS mode, and then configure your security certificates and SSH private keys to make sure they are FIPS compliant.


For the list of encryption algorithms and ciphers compliant with FIPS, see the [NIST website](#).

## SFTP (Secure File Transfer over SSH2)

Use an existing private key

1. Obtain a private key file.
2. Place the private key file in a secured directory in the server.
3. In Serv-U, go to Global > Limits & Settings > Encryption.

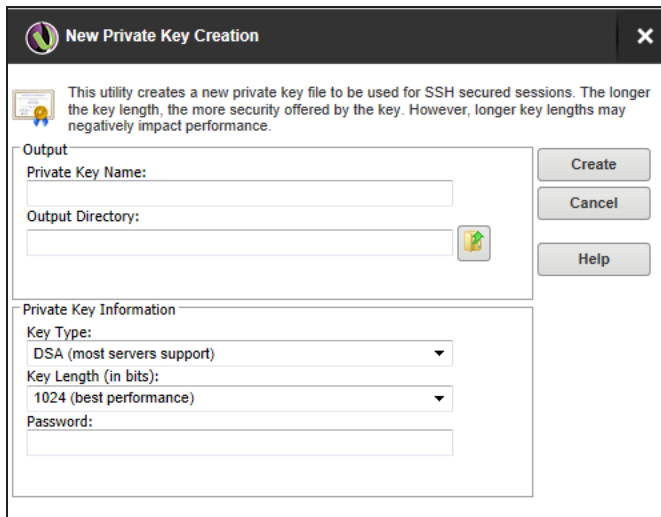


4. Use Browse  to select the file.
5. Enter the password for the private key file.
6. Click Save.

After clicking Save, Serv-U will display the SSH key fingerprint associated with the private key.

#### Create a private key

1. In Serv-U, go to Global > Limits & Settings > Encryption.
2. Click Create Private Key.



The dialog box titled "New Private Key Creation" contains the following elements:

- Header:** A title bar with a close button (X).
- Introductory Text:** "This utility creates a new private key file to be used for SSH secured sessions. The longer the key length, the more security offered by the key. However, longer key lengths may negatively impact performance."
- Output Section:**
  - Private Key Name:** A text input field.
  - Output Directory:** A text input field with a "Browse" button (folder icon) to its right.
- Private Key Information Section:**
  - Key Type:** A dropdown menu with "DSA (most servers support)" selected.
  - Key Length (in bits):** A dropdown menu with "1024 (best performance)" selected.
  - Password:** A text input field.
- Buttons:** "Create", "Cancel", and "Help" buttons are located on the right side of the dialog.

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


After you create a new key, Serv-U displays the SSH key fingerprint associated with the new private key.

## SSH ciphers, MACs and Key Exchange Algorithms

SSH ciphers CAST-128-cbc, Blowfish-cbc and Triple DES-cbc are disabled by default for security reasons. If your specific security needs dictate that only certain ciphers or MACs can be used, you can individually enable (disable) individually ciphers and MACs by selecting (deselecting) the appropriate ciphers or MACs.

## Serv-U custom HTML

If you have the MFT edition of Serv-U File Server, you can use custom HTML to enhance the HTTP and HTTPS login pages of Serv-U at the server and domain levels. By using this feature, web developers can design their login experience to show off their exclusive brand and design the page to match existing business themes.

 Users of the basic Serv-U File Server, can customize the logo, login page text and title at the server and domain levels. For more information on this, see [Settings](#).

By using the custom HTML feature, you can provide a custom header and custom footer for the HTTP and HTTPS login page. The main login form is automatically inserted between the content defined in the header and footer files. The custom HTML interface also uses a CSS file to define the style used in the login form. This CSS file can also be used to define custom styles, containers, and other formatting as needed.

Several branding samples are automatically unpacked to your installation folder (for example, C:\Program Files\SolarWinds\Serv-U\Custom HTML Samples) when Serv-U is installed. The [Serv-U Custom HTML and CSS](#) article has step-by-step instructions for exploring the current set of samples and build your own branding.

The following fields are used by the Custom HTML feature:

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 is used throughout the header file and footer file, and also the styles that will be used by the login form.
Header File	This .HTM file contains the content for the HTML header inserted before the login form.
Footer File	This .HTM file contains the content for the HTML footer inserted after the login form.
Enable Custom HTML	The custom HTML defined on this page is not used by Serv-U until this option is enabled.


Most custom HTML interfaces include custom images. To use custom images, the storage location of the images must be specified. To universalize the storage location, use the `%CUSTOM_HTML_DIR%` tag in paths that refer to 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 in the following way:

```

```

## Serv-U file sharing (MFT only)

The MFT edition of Serv-U File Server enables file sharing, which allows server users to send or receive files from guests. For information, see [File Sharing](#).

 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.

To enable file sharing for the server:

# 1. Navigate to Server Limits and Settings > File Sharing.

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"):

File Sharing Repository:

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

☒ Use inherited default message

☐ Use Secure URL (HTTPS)

☐ Enable File Sharing

Configure SMTP... **Save**

Additional file sharing settings are available under the "Limits" tab.  
In order for Serv-U to automatically send file sharing invitation emails, you must configure your [SMTP settings](#).

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 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 not configured yet, configure SMTP to be able to send and receive notification emails.  
For more information about configuring an SMTP server, see [SMTP configuration](#).
9. Click Save.

## Serv-U server activity

This page displays information about and allows management of user sessions across all domains on the file server. The log tab displays server-wide messages and information.

<a href="#">Sessions</a>	This tab displays information about currently active sessions. From this tab you can view session information, and chat with, or ban, users.
<a href="#">Statistics</a>	This tab displays statistics about the entire file server across all domains, including session information, transfer statistics, and current activity totals.
<a href="#">User &amp; Group Statistics</a>	This tab displays statistics about users and groups, including session information, transfer statistics, and activity totals.
<a href="#">Log</a>	This tab displays the server log with real-time updates. This includes start-up information, global messages, and errors.

## Serv-U sessions

When you view the Sessions page from the Server Activity tab, all connected sessions from the entire file server are displayed. From this page, you can see an overall picture of the current activity on the file server. In addition, you can view individual sessions, including their current status, connection state, and transfer information.

To view detailed information about 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 an accurate and up-to-date snapshot of the activities of the session.

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

## Disconnect sessions

You can disconnect any type of session at any time by clicking Disconnect. Click this button to bring up another window 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 x	Immediately disconnects the session and bans its IP address for the specified number of minutes (x), preventing the client from immediately reconnecting.
Disconnect and block IP permanently	Immediately disconnects the session and adds a deny IP access rule for the IP address, preventing the client from ever reconnecting from the same IP address.

When disconnecting a session from the Server Session view, you can also use the Apply IP rule to option. By using this option, you can select where you want the temporary or permanent IP ban to be applied: for the entire server, or only the domain the session is connected to.

In addition to disconnecting the session, you can also disable the user account in use by the session by selecting Disable user account.

If the current session is using the FTP protocol, you can send a message 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 because neither protocol defines a method for chatting with users.

## Abort sessions

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

## Broadcast messages

You can send a message to all currently connected FTP sessions by clicking Broadcast. Sending a message through broadcast is equivalent to opening the Spy & Chat window to each individual FTP session and sending it a chat message.

## Spy & Chat

You can spy on any type of session by clicking Spy & Chat or by double-clicking a session in the list. Spying on a user displays all the detailed information normally visible by highlighting the session, and also includes a complete copy of the session log since it first connected to the file server. This way you can browse the log and view all actions taken by the user of the session.

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.

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 discarding them.

## Serv-U server activity: user & group statistics

The User and 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 details.

### Session statistics

Data	Description
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 disconnecting.

Data	Description
Logins	The total number of successful logins.
Last Login Time	The last recorded valid login time (not the last time a connection was made).

Data	Description
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

Data	Description
Download Speed	The cumulative download bandwidth currently being used.
Upload Speed	The 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. 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 at the bottom of the page.

## Serv-U user and group statistics

The User and 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 details.

## Session statistics

Data	Description
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 disconnecting.

Data	Description
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

Data	Description
Download Speed	The cumulative download bandwidth currently being used.
Upload Speed	The 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. 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 at the bottom of the page.

## The Serv-U server log

The Server Activity > Log pages show logged activity for the server.

The server log shows file server start-up, configuration, and shutdown information. It does not show domain activity information. For activity logs, view the log of the appropriate domain instead. In addition to status information about libraries, licensing, and the current build that is logged when the file server 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.

You can highlight information contained in the log by clicking and dragging the mouse cursor over the appropriate portion of the log. When it is highlighted, you can copy the selected portion to the clipboard.

Freeze Log	Select this option to temporarily pause the refreshing of the log. This is useful on busy systems so you can highlight and copy a particular section of the log before it scrolls out of view. When you have 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.
Copy to Clipboard	Click this button to automatically freeze the log and copy all information 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 you can use it for reference while you browse the log.
Filter Log	To quickly find and read through specific sections of the log, you can filter it based on a search string. Click this button to bring up the Filter Log window. 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 window, and then click Reset.

## Serv-U domain level settings

Serv-U settings can be defined at four levels: global, domain, group and user. Although some settings are specific to the level, many can be defined at multiple levels. If you configure a setting at the domain level, the setting applies to all users and groups, in that specific domain unless overridden at the group or user level.

The domain settings are divided into the following areas, each accessible from the navigation column.

<a href="#">Domain Details</a>	Displays information pertaining to this domain, including access rules, license, and registration information. <ul style="list-style-type: none"><li>• <a href="#">Settings</a></li><li>• <a href="#">Listeners</a></li><li>• <a href="#">Virtual Hosts</a></li><li>• <a href="#">IP Access</a></li><li>• <a href="#">Database</a></li><li>• <a href="#">Events</a></li></ul>
<a href="#">Users</a>	Create, modify, and delete domain user accounts for all domains on the file server.
<a href="#">Groups</a>	Create, modify, and delete domain groups for use by global accounts on the file server.
<a href="#">Directories</a>	Configure the basic directory structure available to all users on this domain, including default directory access rules and virtual paths.
<a href="#">Limits &amp; Settings</a>	Limits and settings are used to configure the basic settings and behavior for the domain, including FTP command processor customization and SSL/SSH encryption and certificate options. Limits and settings configured at this level are inherited by all groups and users.
<a href="#">Domain Activity</a>	Displays information about and allows management of user sessions across this domain. The log tab displays domain-wide messages and information.

## Serv-U domain details

If you configure details at the domain level, the setting applies to all users, and groups in this domain unless overridden at the group or user level. The following sections contain detailed information about each setting and how it can be configured.



Tab	Description
<a href="#">Settings</a>	Make changes to the domain name and description, and domain home directory.
<a href="#">Listeners</a>	A listener defines how a domain accepts incoming connections.
<a href="#">Virtual Hosts</a>	Virtual hosts are used to access a specific domain when listeners are being shared by multiple domains.
<a href="#">IP Access</a>	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.
<a href="#">Database</a>	Serv-U can use an external database to load additional users and groups. The database must have an ODBC driver installed and must exist as an ODBC data source on the system. Users and groups loaded in this manner that conflict with locally created users and groups are overridden.
<a href="#">Events</a>	Events are used to automatically run programs, send email and show tray icon messages when triggered.

## Serv-U domain details: settings

The Domain Details Settings tab is where you can amend the domain name and description, set up a domain home directory, and enter a maximum size for the directory.

This is also where you can disable or delete the domain, if required.

### Domain information

Name	Each Serv-U domain must be uniquely named. This domain name is used for administrative purposes and not visible or accessible to users.
Description	An optional description can be provided. This is only available to users with administrative access. This field is useful for describing the purpose of the domain or summarizing the resources it provides.
Enable domain	<p>You can temporarily disable a domain by clearing this checkbox. While disabled, all settings are preserved, and it can still be administered, but the domain is inaccessible to users.</p> <p>To make a disabled domain accessible, check this box.</p>

After making changes to any of the previous domain settings, click the associated Save button to apply the changes.

## Domain home directory

Domain Home Directory	<p>The home directory for the domain does not affect user directory access rules, and does not restrict the paths available to a user in any way. However, in order to calculate the amount of disk space in use by a domain, you must specify the root directory under which Serv-U expects all domain files to be stored.</p> <p>Enter the path here, or click Browse. When you create a domain administrator account for this domain, it is suggested you make the home directory the same, ensuring all users of the domain are placed in a subdirectory of the domain home directory.</p>
Maximum Size	<p>Enter the amount of disk space, in megabytes (MB), available to the domain. 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.</p> <p>Calculating the amount of disk space in use by a domain can be a time consuming operation depending on the directory structure.</p>

Click Save to apply the changes.

## Serv-U domain details: listeners

The Domain Details: Listeners tab shows whether the listener is enabled, the IP address(es), port, and file sharing protocol.

Listeners defines how a domain accepts incoming connections. A domain can listen on multiple ports and IP addresses by adding listeners bound to the IP addresses and ports you want. In addition to selecting these connection attributes for a listener, you must also select a file sharing protocol. Serv-U supports IPv4 and IPv6 simultaneously. To offer services to both IPv4 and IPv6 users, create a listener for each.

The following file sharing protocols are supported by the Serv-U File Server:

Protocol	Description	Default Port
FTP and explicit SSL/TLS	FTP is the traditional protocol for transferring files over the Internet. Traditionally, FTP is handled in plain-text. However, SSL connections are explicitly supported through the use of the AUTH command.	21

Protocol	Description	Default Port
Implicit FTPS (SSL/TLS)	FTPS is identical to FTP, although connecting to a listener configured for FTPS means an SSL connection is required before any protocol communication is performed. This is commonly referred to as Implicit FTPS.	990
SFTP 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.	22
HTTP	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.	80
HTTPS (SSL encrypted HTTP)	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.	443


## Add a listener

1. Click Add.

The Listener window is displayed.

2. Select the protocol type (see the table above).
3. The subsequent fields displayed depend on the protocol selected.

**IP Address** Bind a listener to a single IP address by entering the IP address here. Serv-U supports both IPv4 and IPv6 addresses. If you do not specify an IP address, you must select the option to either listen on all available IPv4 addresses or all IPv6 addresses.

 Unless running a purely IPv6 network, it is recommended to use IPv4 addresses and add IPv6 listeners as needed.

If the file server does not have an external IP address (for example, it is behind a router), you can leave this field blank.

Port	The default port for the selected protocol is automatically provided. However, you can use any port between 1 and 65535. When using a non-standard port, clients must know the proper port in advance when they attempt to connect to the domain. If using a non-standard port, it is recommended you use a value above 1024 to prevent potential conflicts.
PASV IP Address or Domain Name	<p>If the listener supports the FTP or FTPS protocol, you can specify a separate IP address here to use for PASV (passive) mode data transfers. This ensures PASV mode works properly on both unsecured and secured connections.</p> <p>If the file server does not have an external IP address, try using a dynamic DNS service and entering your DNS domain name here. Serv-U resolves the DNS domain name to ensure it always has the proper external IP address for PASV command responses.</p>
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 necessary to provide the PASV IP address to connecting clients. When enabled, the IP address specified for PASV mode will not be provided to clients connecting through 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.

## Pure virtual domains

Serv-U allows multiple domains to "share" the same listeners. This means one domain can possess the necessary listener configurations while another domain "piggybacks" on it. 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 FTP and HTTP protocols because 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 that is used to establish the HTTP connection.

## Serv-U domain details: 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. But you can use virtual hosts to host multiple domains on a system with just 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:

1. Click Add under Domain Details > Virtual Hosts.
2. Enter 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.servu_example.com`.

The method used by a client to connect to a specific virtual host depends on the protocol that is used to connect to Serv-U.

---

FTP	FTP users can use one of two methods to connect to a specific virtual host. If it is 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: <code>virtual_host_name login ID</code> . 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 in the FTP section.
------	---

HTTP	For HTTP users, the browser automatically provides Serv-U with the host name that is used to reach the site, allowing Serv-U to identify the virtual host from the fully qualified domain name entered into the navigation bar of the browser.
------	--

---

## Case file: using 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, you must configure virtual hosts on each domain so Serv-U can distinguish between requests for the two domains. After setting up the same listener properties on each domain, open the Virtual Hosts page, click Add, and enter the FQDN that clients should use to connect to the domain (such as `ftp.servu_example.com`).

After connecting to the server with FTP, users can send a HOST `ftp.servu_example.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.servu_example.com|login ID`. If connecting through HTTP, users can connect to this domain by visiting `ftp.servu_example.com`.

## Serv-U domain details: IP access

The IP Access tab shows the IP access rules set up for the server, domain, group or individual user, and allows you to add, import, edit, export and delete these rules.

Rules set at the domain level are inherited by all groups and user within the domain unless overridden.

IP access rules enable you to specify IP addresses, or ranges of IP addresses to which access is allowed or denied. These rules are applied as soon as a physical connection is established. Rules are applied in the order 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. Use the arrows on the right side of the list to change the position of an individual rule in the list.

### Display the IP access list

1. Navigate to the required domain > Domain Details.
2. Click the IP Access tab.

The list of IP addresses set up at this level is displayed.

Use the arrows on the right side of the list to change the position of an individual rule in the list.

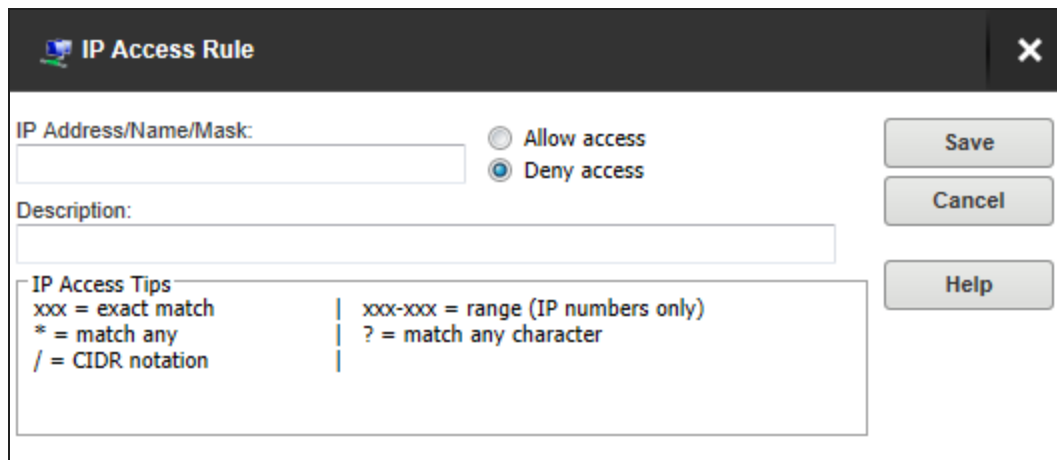
Check the Enable sort mode box to sort the IP access list numerically rather than in the processing order. Displaying the IP access list in sort mode does not change the order in which rules are processed. To view rule precedence, disable this option.



Viewing the IP access list in numerical order can be useful when you review long lists of access rules to determine if an entry already exists.

### Add an IP access rule

1. From the IP tab, click Add.  
The IP Access Rule window is displayed.



The dialog box is titled "IP Access Rule" and has a close button (X) in the top right corner. It contains the following elements:

- IP Address/Name/Mask:** A text input field.
- Access Control:** Two radio buttons: "Allow access" (unselected) and "Deny access" (selected).
- Description:** A text input field.
- Buttons:** "Save", "Cancel", and "Help" buttons are located on the right side.
- IP Access Tips:** A section with a minus sign icon containing the following text:
 

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

- Enter the IP Address, name or mask using the following conventions.

Value or wildcard	Explanation
xxx	Stands for an exact match, such as 192.0.2.0 (IPv4), fe80:0:0:0:a450:9a2e:ff9d:a915 (IPv6, long form) or fe80::a450:9a2e:ff9d:a915 (IPv6, shorthand).
xxx-xxx	Stands for a range of IP addresses, such as 192.0.2.0-19 (IPv4), fe80:0:0:0:a450:9a2e:ff9d:a915-a9aa (IPv6, long form), or fe80::a450:9a2e:ff9d:a915-a9aa (IPv6, shorthand).
*	Stands for any valid IP address value, such as 192.0.2.*, which is analogous to 192.0.2.0-255, or fe80::a450:9a2e:ff9d:*, which is analogous to fe80::a450:9a2e:ff9d:0-ffff.
?	Stands for any valid character when specifying a reverse DNS name, such as server?.example.com.
/	Specifies 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.

- Enter a description.
- Select Allow or Deny access.
- Click Save.

## Edit an IP access rule

1. From the IP tab, click Edit.
2. Amend the rule information as required..
3. Click Save.

## Delete an IP access rule

1. From the IP tab, select the IP rule or rules to delete.
2. Click Delete and confirm.

## Import and export global IP address rules

You can speed up the creation of IP address rules by creating a text file of addresses, descriptions and access permissions.

1. Create a text file using Notepad or similar text editor.
2. On the first line enter "IP","Description","Allow".
3. Enter the details of each IP access rule:

IP	The IP address, IP range, CIDR block, or domain name for which the rule applies.
Description	A text description of the rule for reference purposes.
Allow	Set this value to 0 for Deny, or 1 for Allow.

For example:

```
"IP", "Description", "Allow"
"172.16.0.1", "Flange Software", "1"
"172.16.0.*", "Do not allow", "0"
"2001:db8::/32", "New test site", "1"
```

4. From the IP tab, click Import.
5. Navigate to the file you created, and click Select.

Similarly, the list of existing IP address rules can be exported to a text file by clicking Export.

For examples of IP address rules and IP address caveats see [Examples of IP address rules and caveats](#).

## Serv-U domain details: database

Serv-U File Server enables the use of an Open Database Connectivity (ODBC) database to store and maintain group and user accounts at both the server and domain levels.



Serv-U File Server can automatically create all the tables and columns necessary to store users and groups in the database. Because Serv-U File Server 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 and each domain must have unique ODBC connections to ensure they are stored separately.

## Configure a database


Create an ODBC connection for Serv-U File Server to use. SolarWinds recommends MySQL, but you can use any database that has an ODBC driver available.

1. Enter a Data source Name (DSN) if the Serv-U File Server is operating as a system service, or a User DSN if Serv-U File Server is operating as a regular application.
2. Open the Management Console and browse to the appropriate domain or server database settings. Enter the required information, and click Save.
3. If configuring the database connection for the first time, leave the "Automatically create" options selected. With these options selected, the SolarWinds Serv-U File Server builds the database tables and columns automatically.

## SQL templates

Serv-U File Server uses multiple queries to maintain the databases containing user and group information. These queries conform to the Structured Query Language (SQL) standards. However, if your database has problems working with Serv-U File Server, you may need to alter these queries.

1. Click SQL Templates.
2. In the SQL Templates window, modify each query used by Serv-U File Server to conform to the standards supported by your database, and click Close.

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

## User and group table mappings

By default, Serv-U File Server creates and maintains the tables and columns necessary to store user and group information in a database. However, if you want to connect Serv-U File Server to an existing database that contains this information, you must customize the table and column names to conform to the existing database structure.

1. Click User Table Mappings or Group Table Mappings to get started.
2. Select the Object Table.

Serv-U File Server 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. You can change the current table in 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 displays the table name and you can change the name.

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

3. Select an attribute and 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 can be disabled to reduce the number of ODBC (database) calls. For example, if you do not use [ratios and quotas](#), you can disable the User Ratio-Free Files, Per User Files Ratio, Per User Bytes Ratio, Per Session Files Ratio, and Per Session Bytes Ratio tables to prevent unnecessary ODBC calls. Use caution when you disable tables, because although the fields appear in dialogs, they will not be saved or loaded.

The User Info and Group Info tables cannot be disabled.

## Case file: ODBC authentication

Authentication in the SolarWinds Serv-U File Server can be handled through an ODBC database, allowing for scripted account management and maintenance. To use ODBC functionality, migrate to ODBC authentication through a database. By storing credentials in settings in a database, accounts can be managed from outside the 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 File Server is running as a service or a User DSN if Serv-U File Server is running as an application. After you create the appropriate DSN, enter the required information and click Save. Serv-U File Server creates the tables and columns. You can manage database users and groups in the Database Users and Database Groups pages of Serv-U File Server, located near the normal Users and Groups pages.

## Data source name creation in Linux

Database access in Serv-U File Server on Linux follows the same method as Serv-U File Server on Windows, with the one change to how data source names are created. On Linux, you can create a DSN after installing the following packages:

- `mysql-connector-odbc`
- `postgresql-odbc`
- `unixodbc`

Only the ODBC driver corresponding to the database needs to be installed. If Serv-U File Server 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 File Server 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 =
```

Adjust the names in brackets to the DSN name string you want. Finally, test the DSN with the `isql %DSN% -c -v` command.

For further customization options, see the [Serv-U Database Integration Guide](#).

## Serv-U domain details: events (MFT edition only)

With the MFT edition of the Serv-U File Server, you can automatically associate file server events with email notifications, balloon tip alerts or posts to the Windows Event Log or Microsoft Message

Queue (MSMQ). For example, you might want to be notified in the event of a listener failure or whenever a new file is uploaded.

To access the Events tab for the entire server, navigate to Global > Server Details.

To access the Events tab for a single domain, navigate to Domains > The Domain Name > Domain Details.

To access the events tab for a group, select Groups from the Global or Domain menu, click Edit, and select the Events tab from the Group Properties window.

To access events for an individual user, select Users from the Global or Domain menu, click Edit, and select the Events tab from the User Properties window.

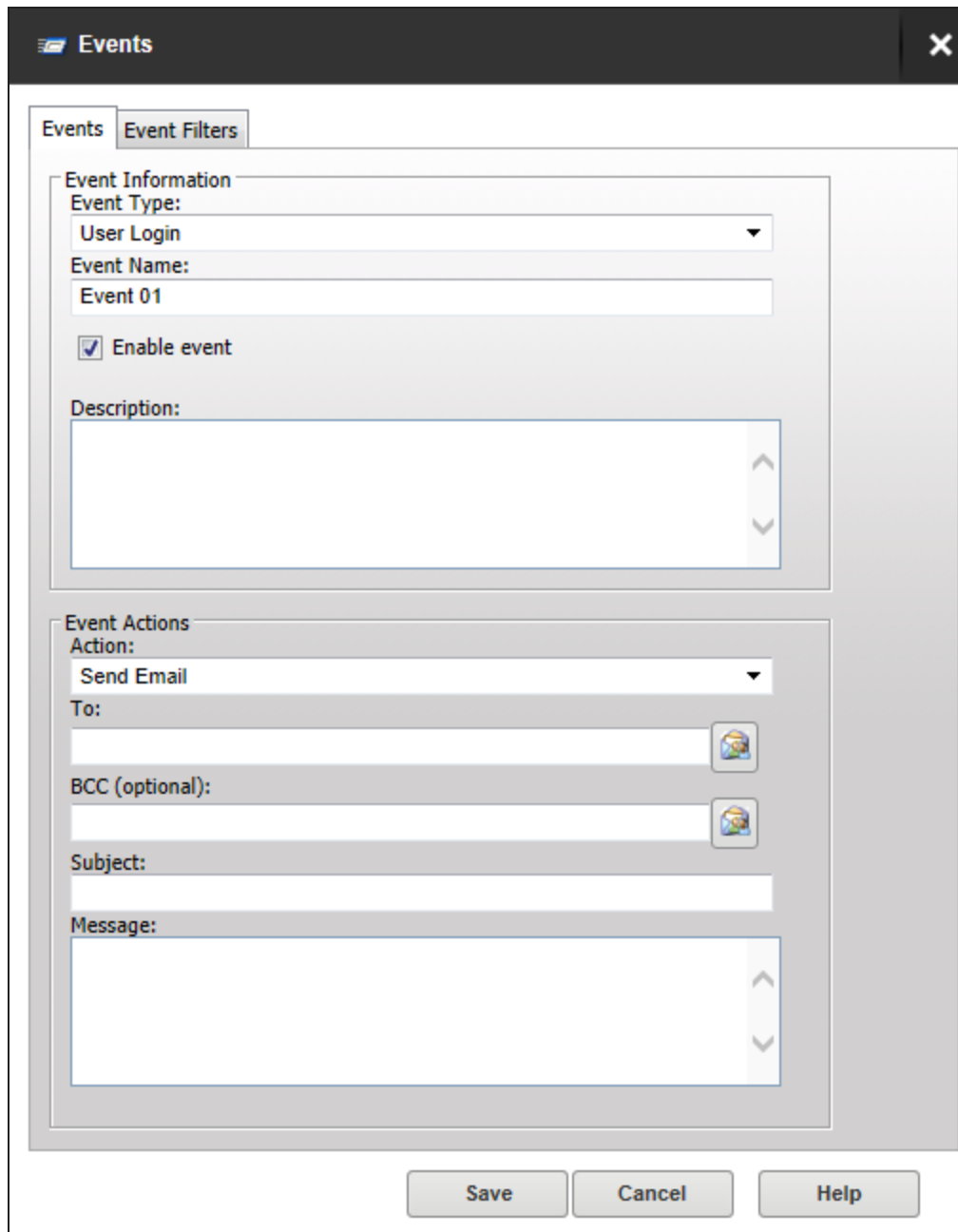
## Create Common Events

To instantly populate the events list with the most commonly used file server events:

1. Click Create Common Events.
2. Select the event action to apply to all common events.
3. Enter the email address to receive all notifications if you selected Send Email.
4. Enter the Message Queue Path if you selected Write to Microsoft Message Queue.
5. Click OK.
6. The 13 most common file server events are created. These can be customized by selecting an event and clicking Edit.

## Add an event

1. Click Add.



**Events**

Events Event Filters

**Event Information**

Event Type:  
User Login

Event Name:  
Event 01

☒ Enable event

Description:

**Event Actions**

Action:  
Send Email

To:


BCC (optional):

Subject:

Message:


Save Cancel Help

2. Select the Event Type.
3. Enter a name and description for this event.


 If you want to create but not immediately enable an event, uncheck the Enable event box.

4. Select the action to be triggered by this event, and complete the associated fields.


The actions that can be triggered are:

Event Action	Description
Send Email	<p>You can configure email actions to send emails to multiple recipients and to Serv-U File Server groups when an event is triggered.</p> <p>Enter the recipients in the To and BCC fields. Separate email addresses by commas or semicolons.</p> <p>To send emails to Serv-U groups, click the Group icon and drag the required groups from the Available Groups column to the Group Email List column.</p> <p>Enter the subject and message. You can use <a href="#">system variables</a> to include data specific to the event.</p>
Show Balloon Tip	<p>Balloon Tips are displayed in the system tray when an event is triggered. Balloon tip actions require a Balloon Title and Balloon Message. You can use <a href="#">system variables</a> to include data specific to the event.</p>
Execute Command (not available for Common Events)	<p>You can configure the execute of a file when an event is triggered. Execute command actions contain an Executable Path, Command Line Parameters, and a 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 zero to execute immediately.</p> <div><p> Time spent waiting delays any processing that Serv-U File Server can perform.</p><p>A wait value should only be used to give an external program enough time to perform an operation, such as move a log file before it is deleted (for example, <code>\$LogFilePath</code> for the Log File Deleted event). You can use <a href="#">system variables</a> to use data specific to the event.</p></div>

Event Action	Description
Write to Windows Event Log (Windows only)	<p>By writing event messages to a local Windows Event Log, you can monitor and record Serv-U File Server activity using third-party network management software.</p> <p>The message entered into the Log Information field is 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. <a href="#">System variables</a> are supported for this field. This field can be left blank, but usually is not.</p>

Event Action	Description
Write to Microsoft Message Queue (MSMQ) (Windows only)	<p>Microsoft Message Queuing (MSMQ) is an enterprise technology that provides a method for independent applications to communicate quickly and reliably. Serv-U File Server can send messages to new or existing MSMQ queues whenever an event is triggered. 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 occurred.</p> <div><p> Microsoft message queues created in Windows do not grant access to SYSTEM by default, preventing Serv-U File Server from writing events to the queue. 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 File Server runs) has permission to the queue.</p></div> <p>These events have the following two fields:</p> <p><b>Message Queue Path:</b> The MSMQ path that addresses the queue. Remote queues can be addressed when a full path (for example, <code>MessageServer\Serv-U Message Queue</code>) is specified. Public queues on the local machine can be addressed when a full path is not specified (for example, <code>.\Serv-U Message Queue</code> or <code>Serv-U Message Queue</code>). If the specified queue does not exist, Serv-U File Server attempts to create it. This normally only works on public queues on the local machine. You can also use Serv-U File Server system variables in this field.</p> <p><b>Message Body:</b> 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 File Server system variables can also be used in this field. This field may be left blank, but usually is not.</p>



 Only the email action is available to users other than Serv-U File Server server administrators.

## Edit an Event

1. Select the event you want to edit and click Edit.
2. Edit the event details and the event filters as required.
3. Click Save.

## Add an Event filter

Event filters allow you to control when a Serv-U File Server event action is triggered. By default, event actions are triggered each time the event occurs. Event filters allow events to be triggered only if certain conditions are met.

For example, a standard event may trigger an email each time a file is uploaded to the server. However, by using an event filter, events can be triggered on a more targeted basis, such as configuring a File Uploaded event to send an email only if the file name contains the string `important`. Thus an email would be sent when the file `Important Tax Forms.pdf` is uploaded but not for other files.

Additionally, you could configure a File Upload Failed event to run only when the FTP protocol is used, not triggering for failed HTTP or SFTP uploads. You can do this by controlling the variables and values related to the event and by evaluating their results when the event is triggered.

To add an event filter to an event:

1. Click the Events Filters tab.
2. Click Add.

**Event Filter**

Filters may have a unique name and description to identify them from other filters. Enable or disable the filter, select the appropriate filter logic and add filter comparisons using the tools below.

**Filter Information**

Name:

Description:

Logic

☒ AND ☐ OR

☒ Filter Enabled

Variable	Comparison	Constant	Data Type

Add... Edit... Delete...

3. Enter the following filter information:

Name	The name of the filter, used to identify the filter for the event.
------	--

Description (Optional)	The description of the event, which may be included for reference.
---------------------------	--

Logic	This determines how the filter interacts with any other filter set up for an event. In most cases, AND is used, and 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).
-------	--

4. Click Add to open the File Comparison window.
5. Select the [System Variable](#) to be used in the comparison.
6. Select the comparison method.

7. Enter the value the system variable is to be compared to. The following wild cards can be used.

- \* The asterisk wildcard matches any text string of any length. For example:
  - An event filter that compares the `$FileName` variable to the string `data*` matches files named `data`, `data7`, `data77`, `data.txt`, `data7.txt`, and `data77.txt`.
- ? The question mark wildcard matches any one character, but only one character. For example:
  - An event filter that compares the `$FileName` variable to the string `data?` matches a file named `data7` but not `data`, `data77`, `data.txt`, `data7.txt`, or `data77.txt`.
  - An event filter that compares the `$FileName` variable to the string `data?.*` matches files named `data7` and `data7.txt` but not `data`, `data77`, `data.txt`, or `data77.txt`.
  - An event filter that compares the `$Name` variable to the string `A????` matches any five-character user name that starts with `A`.
- [ ] The bracket wildcard matches a character against the set of characters inside the brackets. For example:
  - An event filter that compares the `$FileName` variable to the string `data[687].txt` matches files named `data6.txt`, `data7.txt` and `data8.txt` but not `data5.txt`.
  - An event filter that compares the `$LocalPathName` variable to the string `[CD]:\*` matches any file or folder on the `C:` or `D:` drives.

You can use multiple wildcards in each filter. For example:


- An event filter that compares the `$FileName` variable to the string `[cC]:\*.???` matches any file on the `C:` drive that ends in a three letter file extension.
- An event filter that compares the `$FileName` variable to the string `?:\*Red[678]\?????.*` matches 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.


8. Select the data type.

9. And another filter for this event or click Save to close.

#### Filter examples

**Example 1.** An administrator may want to raise an email event when the file `HourlyUpdate.csv` is uploaded to the server, but not when other files are uploaded. To do this, create a new event 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 below:


**Filter Comparison**
×


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

Save

Cancel


Help


If  = (is equal to)

Data Type:

**Example 2.** It may be necessary to know when a file transfer fails for a specific user account. To perform this task, create a new File Upload Failed event, and add a new filter.

The filter comparison is the \$Name variable, and the value to compare is the user name, such as ProductionLineFTP:


**Filter Comparison**
×


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

Save


Cancel


Help

If  = (is equal to)

Data Type:

**Example 3, using wildcards.** You can also filter for events based on specific folders using wildcards. 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, create a new File Uploaded event in the Domain Details > Events menu, and set it to Send Email. Enter the email recipients, subject line, and message content, and then open the Event Filters page. 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\.


**Filter Comparison**
×


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

Save

Cancel

Help

If  = (is equal to)

Data Type:

## Serv-U domain users


A user account is required to access the file server. At its most basic level, a user account defines login credentials (that is, login ID and password), a home directory, a set of directory access rules defining areas of the system accessible to the user, and the actions the user can perform in those locations. Each active session on the file server has a user account associated with it identifying the client to the administrator.

User accounts can be defined in various ways on the Serv-U File Server, including the following:

<a href="#">Domain users</a>	Domain users can only log in to the domain under which they are created.
<a href="#">Database users</a>	Database users are stored in an external database accessible through ODBC and supplement the local account database.
<a href="#">Windows authentication</a> (Windows only, MFT only)	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).
<a href="#">LDAP authentication</a> (MFT only)	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.

Because 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 previously 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 you create users, consider what kind of access they need, and select the appropriate location for the user account accordingly. You can save time and effort by entering such settings at the server level to remove the need for multiple user accounts at the domain level.

 With Serv-U MFT Server, you can also organize user accounts into collections to make account management more logical and organized. This can be useful when you manage all users from a department or physical location. For example, you can place all users in the accounting department in a collection named Accounting, or place all users at an office in Topeka in a collection named Topeka Users.

## Serv-U domain users

- [Add a User using the Wizard](#)
- [Add a User manually](#)
- [The User Template](#)
- [Edit a User](#)
- [Copy a User](#)
- [User collections \(MFT only\)](#)
- [Recovering passwords](#)
- [Advanced settings](#)

You can add users at the global or domain level.

- Global users are defined at the server level and have access to all domains.
- Domain users are defined for the specific domain, and only have access to that domain.

For information on Global users, see the [Global Users](#) topic.

You can create users quickly using the wizard, or manually enter user properties for more precise set-up.

### View and add users for an individual domain

1. Select the domain in the navigation column.
2. Click Users.

The Domain window has additional tabs for [Window Authentication](#) and [LDAP Authentication](#) if you have the MFT edition of the Serv-U File Server.

**Users** - Create, modify, and delete user accounts for this domain.

Domain Users | Database Users | Windows Authentication | LDAP Authentication

This list shows the user accounts that are allowed to connect to the active domain. Use this list, and the list buttons, to maintain this domain's users.

Select user collection: General Add... Import... Export...

Filter Users:  Clear Filter

Login ID	Full Name	Description	Last Login Time	Home Directory
bob2000	Robert Helvetica			%DOMAIN_HOM...
fred1967	Fredrick Franklin			%DOMAIN_HOM...
jasmine1980	Jasmine X. Trebuchet			%DOMAIN_HOM...
uma1959	Uma Umlaut			%DOMAIN_HOM...

Add... Edit... Delete Copy... Move... Wizard... Template... Recover Password

## Add a user using the wizard

1. Click the Wizard button. The User Wizard is displayed.

**User Wizard - Step 1 of 4** ✕

Welcome to the Serv-U user account wizard. This wizard helps you quickly create new users to access your file server.

The login ID is provided by the client to identify their account when attempting to login to the file server.


Login ID:

Full Name:  (optional)

Email Address:  (optional)

Next>> Cancel

2. Enter a unique login ID for the user.

 Login IDs cannot contain any of the following special characters:

\ / < > | : . ? \*

Two special login IDs exist: Anonymous and FTP. These are synonymous with one another, and can be used for guests. They do not require a password, so the Password field should be left blank. Serv-U requires users who log on with one of these accounts to provide their email address to complete the login process.

3. Optionally, enter a name and email address for this user.
4. Click Next.
5. Enter a password for this user, or accept the suggested eight character, complex password.  
  
You can leave the password blank, which will enable anyone knowing the login ID to access this account.  
  
You can place restrictions on the length and complexity of passwords, and disable the automatic password generator if required.
6. Check the box if you want the user to create their own password when they first login.
7. Enter or navigate to the home directory for this user. This is where the user is placed immediately after logging in to the file server. This must be specified using a full path including the drive letter or the UNC share name.

When you specify the home directory, you can use the %USER% macro 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 it is combined with a directory access rule for %HOME%, a new user can be configured with a unique home directory and the appropriate access rights to that location with a minimal amount of effort.

You can also use the %DOMAIN\_HOME% macro 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.

Check the Lock user in home directory box if you want this user's access to be restricted to this directory.

8. Click Next.

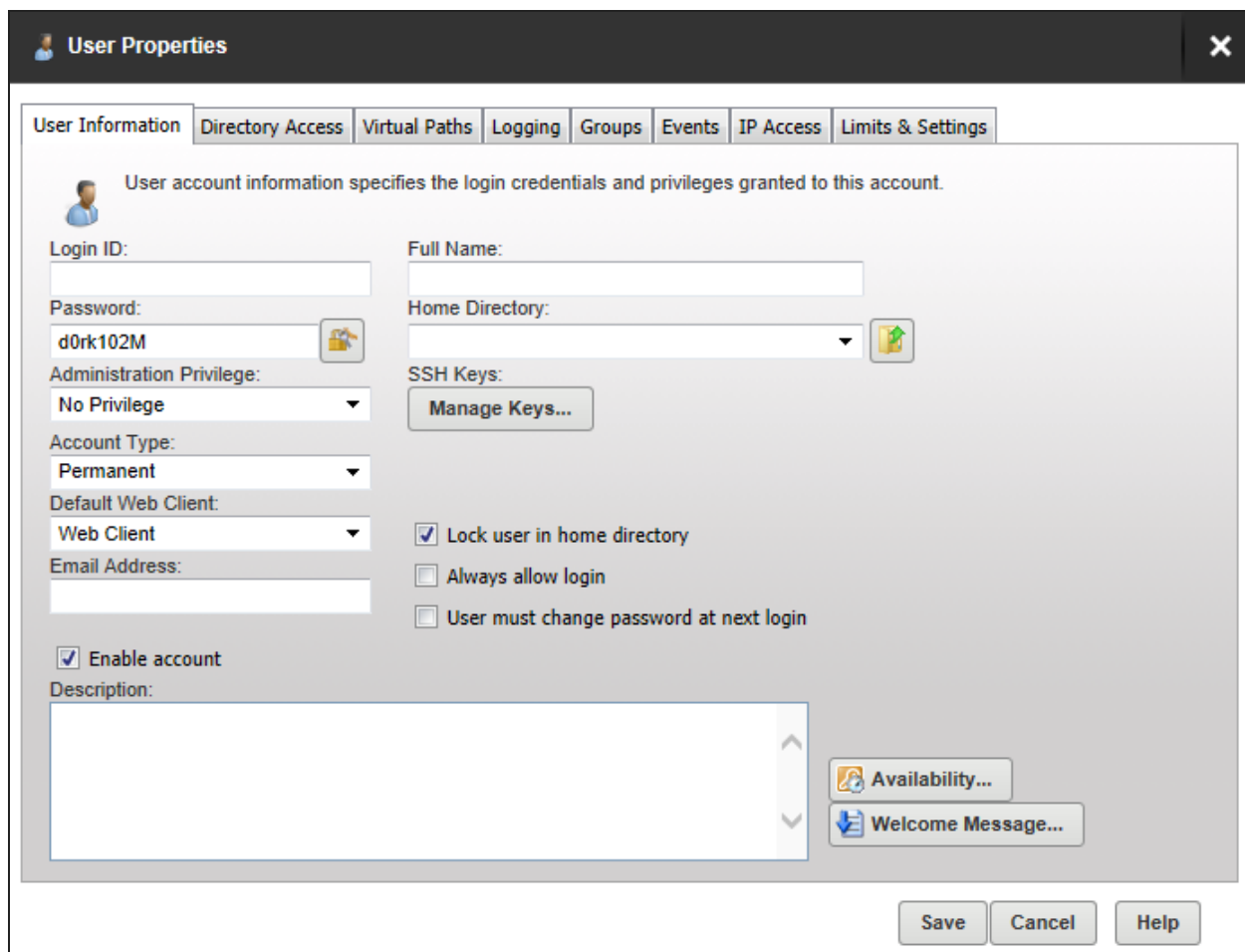


9. Select Read Only Access if you want this user to only be able to browse and download files or Full Access if you want to grant the user full control of files and directories in their home directory.
10. Click Finish.
11. The user is added to the list of users. You can edit this user if you want to apply more advanced settings.

## Add a User manually

1. Click the Add button.

The User Properties window is displayed.




The User Properties window is displayed, showing the User Information tab. The window title is "User Properties" with a close button (X) in the top right corner. The tab bar includes: User Information, Directory Access, Virtual Paths, Logging, Groups, Events, IP Access, and Limits & Settings. The main content area has a header: "User account information specifies the login credentials and privileges granted to this account." Below this, the fields are organized as follows:

- Login ID:** Text field containing "d0rk102M".
- Password:** Text field containing "d0rk102M" with a password icon.
- Administration Privilege:** Dropdown menu set to "No Privilege".
- Account Type:** Dropdown menu set to "Permanent".
- Default Web Client:** Dropdown menu set to "Web Client".
- Email Address:** Text field.
- Full Name:** Text field.
- Home Directory:** Text field with a dropdown arrow and a folder icon.
- SSH Keys:** Section with a "Manage Keys..." button.
- Lock user in home directory:** Checked checkbox.
- Always allow login:** Unchecked checkbox.
- User must change password at next login:** Unchecked checkbox.
- Enable account:** Checked checkbox.
- Description:** Large text area.
- Availability...** Button with a calendar icon.
- Welcome Message...** Button with a document icon.

At the bottom right, there are three buttons: "Save", "Cancel", and "Help".

2. Enter a unique login ID for the user.

 Login IDs cannot contain any of the following special characters:

\ / < > | : . ? \*

Two special login IDs exist: Anonymous and FTP. These are synonymous with one another, and can be used for guests. They do not require a password, so the Password field should be left blank. Serv-U requires users who log on with one of these accounts to provide their email address to complete the login process.

3. Enter a name for this user.

4. Enter a password for this user, or click the lock button to create an eight character, complex password.

You can leave the password blank, which will enable anyone knowing the login ID to access this account.

You can place restrictions on the length and complexity of passwords through User limits. For more information about password limits, see [User Limits and Settings - Passwords](#).

5. Enter or navigate to the home directory for this user. This is where the user is placed immediately after logging in to the file server. This must be specified using a full path including the drive letter or the UNC share name.

When you specify the home directory, you can use the %USER% macro 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 it is combined with a directory access rule for %HOME%, a new user can be configured with a unique home directory and the appropriate access rights to that location with a minimal amount of effort.

You can also use the %DOMAIN\_HOME% macro 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.

6. Select the Administration Privilege for this user. This can be:

---

No Privilege

A regular user account that can only transfer files to and from the File Server. The Serv-U Management Console is not available.

---

Group Administrator	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, and they can also assign permissions at or below the level of the Group Administrator. They may not make any other changes.
Domain Administrator	<p>A Domain Administrator can only perform administrative duties for the domain to which their account belong, and 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 are:</p> <ul style="list-style-type: none"> <li>• configuring their domain listeners</li> <li>• configuring or administering LDAP groups</li> <li>• configuring ODBC database access for the domain</li> </ul>
System Administrator	A System Administrator can perform any file server administration activity including creating and deleting domains, user accounts, and even updating the license of the file server. A user account with System Administrator privileges logged in through HTTP remote administration can administer the server as if they had physical access to the server.
Read-only Group/Domain/Server Administrator	Read-only administrator accounts can allow administrators to log in and view configuration options at the group, 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, and cannot create, delete or edit user accounts.

7. If you have the MFT edition of Serv-U, you can specify a SSH public key to be used to authenticate a user when logging in to 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 of the domain, set in Domain Details > Settings, used if the keys are in a central folder relative to the domain home directory.

Examples:

%HOME%\SSHpublic.pub

%HOME%\%USER%.pub

%DOMAIN\_HOME%\SSHKeys\%USER%.pub

For information on SSH public key authentication, adding a SSH key pair, and creating an key pair for testing, see [New SSH Key Pair Creation](#).


8. Select the account type. By default, all accounts are permanent and exist on the file server until they are manually deleted or disabled. You can configure an account 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 is displayed. Click the calendar or expiration date to select when the account should be disabled or deleted.

The account is accessible until the beginning of the day on which it is set to be disabled. For example, if an account is set to be disabled on 15 July 2015, the user can log in until 14 July 2015, 23:59.

9. Select the default web client to be displayed when a user logs in.

If you have the MFT edit, 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, you can also specify a default client. If you change this option, 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.

10. Enter an Email address for this user. Type an email address here to allow password recovery for the user account.

 For the MFT edition, this email address can also be used for event notifications.

## 11. Check or uncheck the following checkboxes:


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.
Lock user in home directory	Users 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 because Serv-U always reports it as "/" (root). The value of this attribute can be inherited through group membership.
Always allow login	<p>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. 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.</p> <p>Enabling the Always Allow Login option does not override <a href="#">IP access rules</a> . If both options are defined, the IP access rules prevail.</p>
User must change password at next login	<p>If enabled, the user will be prompted to change their password when they next log in.</p> <p>This option takes priority to the "Allow user to change password" setting on the Limits &amp; Setting tab. This means even if that setting is set to No, checking this box still will require the user to change their password.</p>

## 12. Enter an optional description of this user account.

## 13. Click Availability if you want to place limits on when this user can log in.

- Check Apply limit and select the start and end time to specify the period this user may log in.
- Tick the checkboxes for the days of the week on which this user may log in.

## 14. Click Welcome Message if you want to sent a welcome message to this user when they log in. This may also be set at the Group level.

 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 through SFTP over SSH2, because SSH2 does not define a method for sending general text information to users.

- a. Check Include if you want to include the response code in the welcome message test when an FTP connection is made.
- b. Either:
  - Select or navigate to a message file if you have already created a text file containing a welcome message.or:
  - Check the Override box, and enter a message specific to this user in the text box above it.
- c. Click Save.

## Advanced settings

Once you have added the User information you can use the following tabs on this window to complete the user setup.

<a href="#">Directory Access</a>	Directory access rules define the files and directories that the user has permission to access. At the user level, these rules are inherited from any groups the user belongs to as well as those rules defined at the domain and server level.
<a href="#">Virtual Paths</a>	Virtual paths are used to link a physical path that is outside the directory structure of the user's home directory into the directory listings received by that user.
<a href="#">Logging</a>	This tab provides checkboxes to configure what information you want to be logged.
<a href="#">Groups</a>	From the User Properties window you can select groups to which you want to add a user. Group membership allows you to assign various basic attributes to users that are members of the group.
<a href="#">Events</a>	MFT only: Events let you automatically run programs, send email and show messages when triggered by Serv-U activities.
<a href="#">IP Access</a>	Set up and maintain Server IP access rules so that specific IP address can be allowed or denied access to all your file server domains. These are checked when a physical connection is established with the file server, but before a welcome message is sent.
<a href="#">Limits &amp; Settings</a>	There are many options that can be applied at the user level. You can specify on which days and at which time these limits apply.

## The User Template

While the New User Wizard provides a way to quickly create a user account with the minimum number of required attributes, most File Server administrators have a collection of settings that 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. You can configure the template user 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.

By using user templates, you can add users to a specific default group. If you set up the user template as a member of the group you want all users to be a member of. This way, when new users are created, they will automatically be added to the particular group which is specified in the user template.

### Edit a User

Select a user and click Edit to open the User Properties window with the selected user's information.

### Copy a User

Select a user and click Copy to open the User Properties window with the selected user's information. You will need to supply at least a new Login ID to save the new user.

### User collections (MFT only)

In Serv-U MFT Server, you can organize user accounts into collections to make account management more logical and organized. This can be useful when you manage all users from a department or physical location. For example, you can place all users in the accounting department in a collection named Accounting, or place all users at an office in Topeka in a collection named Topeka Users.

To create a collection, click Add in the Select user collection area in the users window. In the new window, type the name of your collection, and then click Save. You can add users to this new collection by selecting them and clicking Add below the user list. To move a user from one collection to another, click Move below the user list, and then select the destination collection for the highlighted user accounts. You can also rename or delete collections by using the appropriate button.

When deleting a collection, all user accounts contained in that collection are deleted, too. If you want to keep the user accounts, make sure you move them before deleting the collection.

By default, all users are created in the General user collection.

## Recovering passwords

Serv-U supports password recovery both through the Management Console and through the Web Client. For password recovery to be available, you must configure the SMTP options for the server or domain, and the user account must have an email address listed. To use password recovery from the user page:

1. Select the user's account,
2. 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.

## Serv-U database users

You can connect the Serv-U File Server to an external database to load users and groups. Users and groups are loaded from the specified ODBC data source. These supplement the local user account database, and are displayed on the Database Users and Database Groups tabs in Server Details and Domain details. You can use different data sources at the global and each domain level. Changes to user and groups accounts stored in this manner can be made through this interface or one supported by the database.

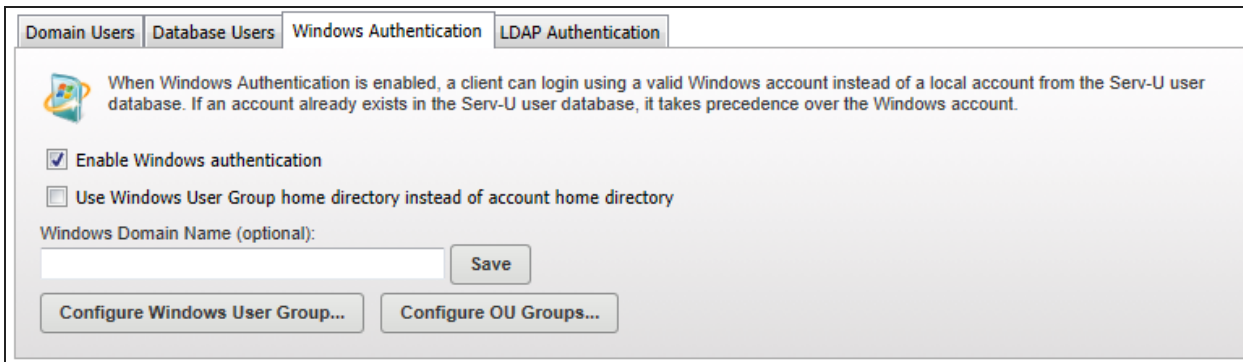
## Serv-U Windows authentication (MFT only)

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:

1. Navigate to the required domain menu > Users.
2. Select the Windows Authentication tab.
3. Check the Enable Windows authentication checkbox.





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.

By default, Serv-U uses the Windows account's home directory when a client logs in using a Windows user account. Enabling the Use a Windows user group home directory instead of the account home directory 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.

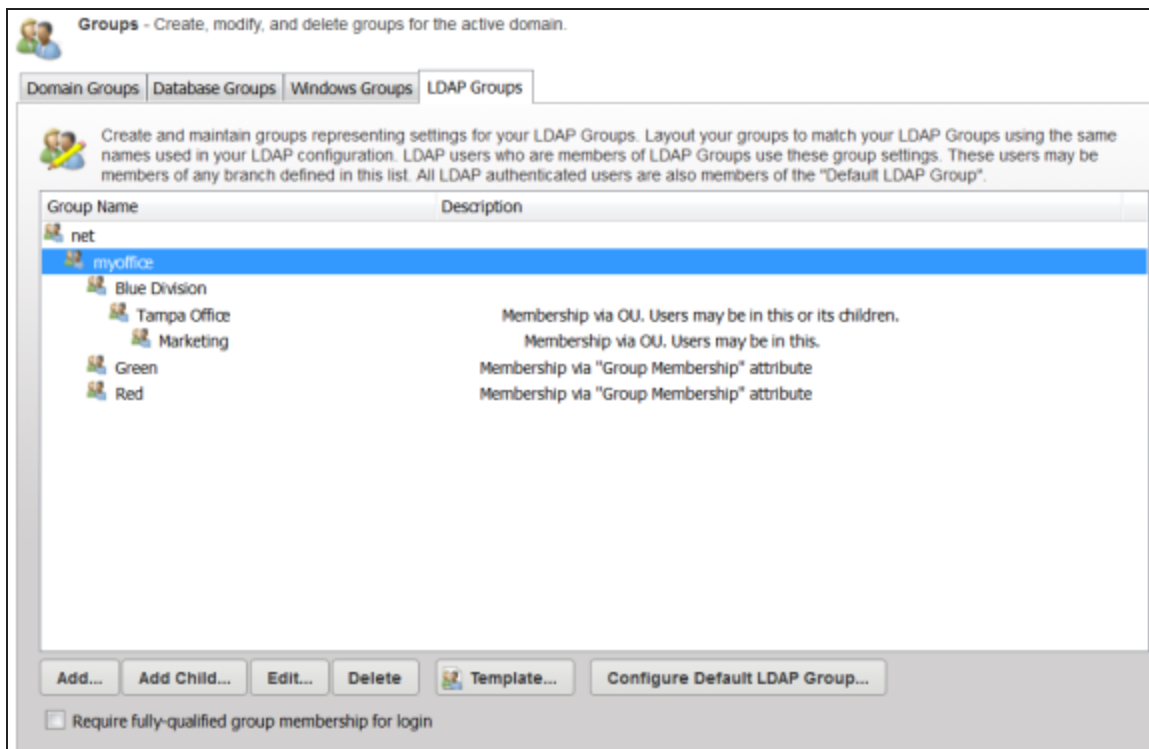
## LDAP authentication

### 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 in Users > LDAP Authentication or in 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 in Users > LDAP Authentication to configure these groups just like normal Serv-U groups.



## 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.

## Serv-U groups

Groups provide a method of sharing common configuration options with multiple user accounts. Configuring a group is similar to configuring a user account. Groups can be created at the server or domain level.

Virtually every configuration option available for a user account can be set at the group level. 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.

At the server level, the following options are available:

<a href="#">Global Groups</a>	Add or edit groups available to global user accounts on the file server.
-------------------------------	--

<a href="#">Database Groups</a>	Database groups are loaded from the specified ODBC data source and supplement the local group database.
---------------------------------	---

At the domain level, the additional options are available:

<a href="#">Windows Groups</a>	Create and maintain groups representing settings for your Windows Organization (OU).
--------------------------------	--

<a href="#">LDAP Groups</a>	Create and maintain groups representing settings for your LDAP groups.
-----------------------------	--

## Serv-U domain groups

- [Add a Group](#)
- [Advanced settings](#)
- [Edit a Group](#)
- [The Group Template](#)

Groups provide a method of sharing common configuration options with multiple user accounts. Configuring a group is similar to configuring a user account. Groups can be created at the server or domain level.

Virtually every configuration option available for a user account can be set at the group level. 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.

However, groups are only available to user accounts that are defined at the same level. In other words, a global user (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.

## Add a Group

1. From the Groups page, click the Add button.

The Group Properties window is displayed.

2. Enter or navigate to the home directory for users in this group. This is where the users are placed immediately after logging in to the file server. This must be specified using a full path including the drive letter or the UNC share name.

When you specify the home directory, you can use the %USER% macro 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 it is combined with a directory access rule for %HOME%, a new user can be configured with a unique home directory and the appropriate access rights to that location with a minimal amount of effort.

You can also use the %DOMAIN\_HOME% macro 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.

3. Select the Administration Privilege for this users in this group. This can be:

No Privilege	A regular user account that can only transfer files to and from the File Server. The Serv-U Management Console is not available.
Group Administrator	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, and they can also assign permissions at or below the level of the Group Administrator. They may not make any other changes.
Domain Administrator	<p>A Domain Administrator can only perform administrative duties for the domain to which their account belong, and 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 are:</p> <ul style="list-style-type: none"> <li>• configuring their domain listeners</li> <li>• configuring or administering LDAP groups</li> <li>• configuring ODBC database access for the domain</li> </ul>
System Administrator	A System Administrator can perform any file server administration activity including creating and deleting domains, user accounts, and even updating the license of the file server. A user account with System Administrator privileges logged in through HTTP remote administration can administer the server as if they had physical access to the server.
Read-only Group/Domain/Server Administrator	Read-only administrator accounts can allow administrators to log in and view configuration options at the group, 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, and cannot create, delete or edit user accounts.

4. If you have the MFT edition of Serv-U, you can specify a SSH public key to be used to authenticate users in this group when logging in to 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 of the domain, set in Domain Details > Settings, used if the keys are in a central folder relative to the domain home directory.

#### Examples:

```
%HOME%\SSHpublic.pub
```

```
%HOME%\%USER%.pub
```

```
%DOMAIN_HOME%\SSHKeys\%USER%.pub
```

For information on SSH public key authentication, adding a SSH key pair, and creating an key pair for testing, see [New SSH Key Pair Creation](#).

5. Select the default web client to be displayed when a user in this group logs in.

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, you can also specify a default client. If you change this option, 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.

## 6. Check or uncheck the following checkboxes:


Always allow login	<p>Enabling this option means that users in this group are 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. As with any option that allows bypassing access rules, care should be taken in granting this ability.</p> <p>Enabling the Always Allow Login option does not override IP access rules. If both options are defined, the IP access rules prevail.</p>
Enable account	Deselect this option to disable user accounts in this group. Disabled accounts remain on the file server but cannot be used to log in. To re-enable accounts in this group, select the Enable account option again.
Lock user in home directory	Users 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 because Serv-U always reports it as "/" (root).
Apply group directory access rules first	<p>Deselect this option to place the directory access rules of the group below the user access rules.</p> <p>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 directory access rules specified at the user level. However, there are certain instances where you may want the user level rules to take precedence.</p>

## 7. Enter an optional description for this group account.

## 8. Click Availability if you want to place limits on when users in this group can log in.

- Check Apply limit and select the start and end time to specify the period users in this group may log in.
- Tick the checkboxes for the days of the week on which users in this group may log in.

## 9. Click Welcome Message if you want to sent a welcome message to the users in this group when they log in.

 The welcome message is a message traditionally sent to FTP clients 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 through SFTP over SSH2, because SSH2 does not define a method for sending general text information to users.

- a. Check Include if you want to include the response code in the welcome message test when an FTP connection is made.
- b. Either:
  - Select or navigate to a message file if you have already created a text file containing a welcome message.or:
  - Check the Override box, and enter a message specific to this user in the text box above it.
- c. Click Save.

## Advanced settings

Once you have added the Group information you can use the following tabs on this window to complete setup.

<a href="#">Directory Access</a>	Directory access rules define the files and directories that users in this group have permission to access. At the group level, these rules are inherited from the domain and server level.
<a href="#">Virtual Paths</a>	Virtual paths are used to link a physical path that is outside the directory structure of the home directory of users in this group into the directory listings received by that user.
<a href="#">Logging</a>	This tab provides checkboxes to configure what information you want to be logged.
<a href="#">Members</a>	Displays the list of users in this group. This tab is display only - you need to use the <a href="#">Groups</a> tab in the individual User Properties to select the groups to which that user belongs.
<a href="#">Events</a>	MFT only: Events let you automatically run programs, send email and show messages when triggered by Serv-U activities.
<a href="#">IP Access</a>	Set up and maintain Server IP access rules so that specific IP address can be allowed or denied access to all your file server domains for users in this group. These are checked when a physical connection is established with the file server, but before a welcome message is sent.
<a href="#">Limits &amp; Settings</a>	There are various options that can be applied at the group level. You can specify on which days and at which time these limits apply.



## Edit a Group

Select a group and click Edit to open the Group Properties window, allowing you to edit that information for users in this group.

## The Group Template

You can configure a template for creating new groups by clicking Template. The template group can be configured just like any other group, with the exception of giving it a name. After the settings are saved to the template, all new groups are created with their default settings set to those found within this template. This way you can configure the basic settings that you want all of your groups to use by default.

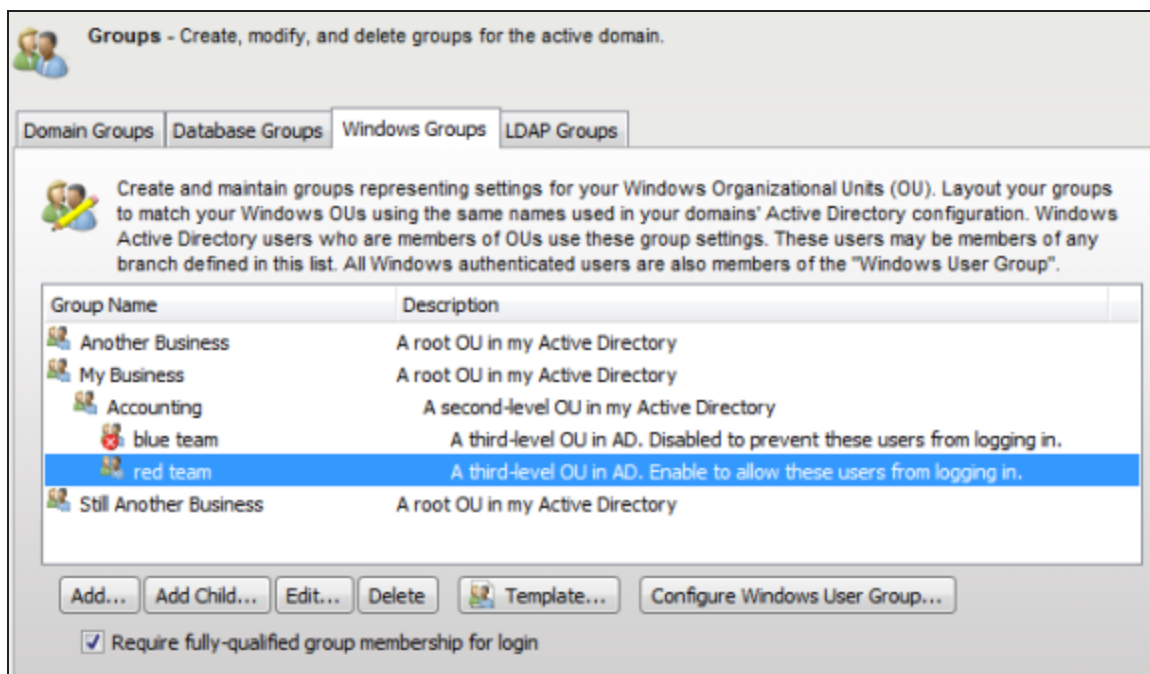
## Domain Groups: Database groups

Database groups are loaded from the specified ODBC data source. They supplement the local group database. Changes to groups stored in this manner can be done through this interface or one supported by the database.

## Domain Groups: Windows Groups

You can use Window groups 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. You can create additional Windows groups to assign different permissions and settings to different groups of Windows users.



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.

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 are not be allowed to log in.

#### Configure a Windows user group

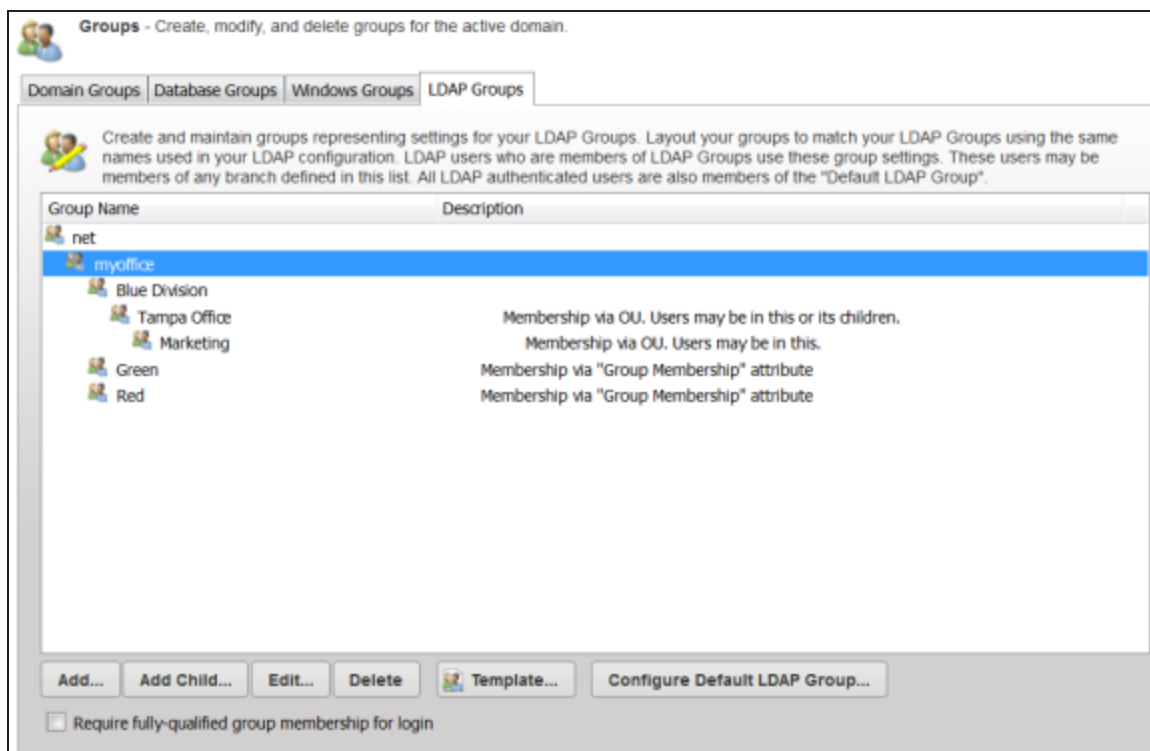
Administrators can allow clients to log in to the file server using the local Windows user database or one that is made accessible through a domain server. These user accounts do not exist in the local Serv-U user database and cannot be configured on an individual basis. To aid in configuring these accounts, 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.

## Domain Groups: LDAP 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 in Users > LDAP Authentication or in 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 in Users > LDAP Authentication to configure these groups just like normal Serv-U groups.



## 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.

## Domain Directories

This tab enables you to configure the basic directory structure available to all users of the file server, including default directory access rules, virtual paths and file management rules.

### [Directory Access](#)

Server directory access rules are global rules defining the files and directories all users on this server have access to.

### Virtual Paths

Virtual paths are used to link a physical path that is outside the directory structure of the user's home directory into the directory listings received by that user.


### File Management

File Management Rules allow Serv-U to automatically remove or archive files from your File Server.

## Domain Directories: Directory Access


Directory access rules define which areas of the system are accessible to user accounts. Directory access rules specified at the server level are inherited by all users of the file server. If they are specified at the domain level, they are only inherited by users who belong to the particular domain. The traditional rules of inheritance apply where rules specified at a lower level (for example, the user level) override conflicting or duplicate rules specified at a higher level (for example, the server level).

When you set the directory access path, you can use the `%USER%`, `%HOME%`, `%USER_FULL_NAME%`, and `%DOMAIN_HOME%` variables to simplify the process.

 For example, use `%HOME%/ftproot/` to create a directory access rule that specifies the `ftproot` folder in the home directory of the user.

Directory access rules specified in this manner are portable if the actual home directory changes while maintaining the same subdirectory structure. This leads to less maintenance for the file server administrator. If you specify the `%USER%` variable 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. You can use the `%USER_FULL_NAME%` variable 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\%USER_FULL_NAME%` for `D:\ftproot\Tom Smith`. You can also use the `%DOMAIN_HOME%` macro 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 listed. The first rule in the list that matches the path of a client's request is the one 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 particular subdirectory. Use the arrows on the right of the directory access list to rearrange the order in which the rules are applied.

 Serv-U File Server allows to list and open the parent directory of the directory the user is granted access to, even if no explicit access rules are defined for the parent directory. However, the parent directory accessed this way will only display the content to which the user has access.

## Permissions

### File Permission

Read	Allows users to read (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 (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 typically used to enable users to resume transferring partially uploaded files.
Rename	Allows users to rename files.
Delete	Allows users to delete files.
Execute	Allows users to remotely execute files. The execute access is meant for remotely starting programs and usually applies to specific files. This is a powerful permission and great care should be used in granting it to users. Users with Write and Execute permissions can install any program on the system.

### Directory Permission

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.
Create	Allows users to create new directories within the directory.
Rename	Allows users to rename directories within the directory.
Remove	Allows users to delete existing directories within the directory.  If the directory contains files, the user also must have the Delete files permission to remove the directory.

### Subdirectory Permission

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 (for example, when implementing mandatory access control), clear the Inherit check box and grant permissions specifically by folder.
---------	--


## 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 would result in the directory content 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.

## Advanced: Access as Windows user (Windows only)

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 File Server, you can configure the SolarWinds Serv-U File Server service to run under a network account. The alternative, preferred where many servers exist, or if the SolarWinds Serv-U File Server service has to run under Local System for security reasons, is to configure a directory access rule to use a specific Windows user for file access. Click Advanced to specify a specific Windows user for each directory access rule. As in Windows authentication, directory access is subject to NTFS permissions, and in this case also to the configured permissions in Serv-U File Server.

 When you use Windows authentication, the NTFS permissions of the Windows user take priority over the directory access rules. This means that when a Windows user tries to access a folder, the security permissions of the user are applied instead of the credentials specified in the directory access rule.

## Examples

### Mandatory access control

You can use mandatory access control (MAC) 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.

In the following example, the rule applies to `C:\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)

**Buttons:** Save, Cancel, Help, Full Access, Read Only, Advanced >>

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 SolarWinds Serv-U File Server.

#### Restrict file types

If users are using storage space on the SolarWinds Serv-U File Server to store non-work-related files, such as `.mp3` files, you can prevent this by configuring a directory access rule placed above the main directory access rule 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:

**Directory Access Rule**

Path: \*.mp3

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)

Buttons: Save, Cancel, Help, Full Access, Read Only, Advanced >>

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 the directory to which they need access.

**Directory Access Rule**

Path: %HOME%

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)

Buttons: Save, Cancel, Help, Full Access, Read Only, Advanced >>

In the second rule, enter the extension of the file that should be accessed, such as \*.mdb.



**Directory Access Rule**

Path: \*.mdb

**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)

Buttons: Save, Cancel, Help, Full Access, Read Only, Advanced >>

These rules only allow users to access .mdb files within the specified directories. You can adapt these rules to any file extension or set of file extensions.

Directory Access		Virtual Paths	File Management
Domain directory access rules are global rules that define the files and directories overridden at the group and user levels.			
Path	Access		
*.mdb	RWADN-L---I		
%HOME%	-----L---I		

## Domain Directories: Virtual paths

If virtual paths are specified, users can 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 access 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 domain level are only accessible by users belonging to that domain.

## 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, use a full path, such as `D:\inetpub\ftp\public`. You can also use a UNC path, such as `\\Server\share\public`. To make a virtual path visible to users, users must have a directory access rule specified for the physical path.

## Virtual path

The virtual path is the location 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. You can also use a full path without any macros.

Include virtual paths in Maximum Directory Size calculations

When this option is selected, the virtual path is included in Maximum Directory Size calculations. The Maximum Directory Size limits the size of directories affecting how much data can be uploaded.

## Examples

### Virtual paths

A group of web developers have been granted access to the directory `D:\ftproot\example.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 group of web developers, add a virtual path to bring the directory to the users by specifying `D:\corpimages\` as the physical path and `D:\ftproot\example.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.

### Relative virtual paths

Continuing with the previous example, if the home directory of the group of web developers is relocated to another drive, both the home directory and the virtual path must be updated to reflect this change. You can avoid this 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\example.com\corpimages` as the virtual path, use `%HOME%\corpimages`. This way the corpimages virtual path is placed within the home directory of the group, regardless of what the home directory is. If the home directory changes at a later date, the virtual path still appears there.

## Domain Directories: File management

File management rules enable you to automatically remove or archive files from the file server. You can configure file management rules at the server and domain level.

- If they are specified at the server level, the file management rules are accessible to all users of the file server.
- If they are specified at the domain level, they are only accessible to users belonging to that domain.


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

 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 File Server. This way you can manage files that are transferred by clients, or that are copied to the folder outside of Serv-U File Server.

The folder structure is not affected by the file management rules. When expired files are deleted or moved, the folders themselves remain intact.


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

 If you have the MFT edition of Serv-U File Server, you can monitor the status of the file management rules by configuring File Management Rule Success and File Management Rule Error events under Server Details or Domain Details > Events. The file management rules continue to run even if deleting or moving a single file fails. For more information, see [Events](#).

### Define a new file management rule

1. Navigate to Directories > File Management, and click Add.
2. Enter 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 in the Destination Directory Path field, specify the folder where you want to move the file.
4. Specify the number of days after the file creation date when the action should be executed.
5. Click Save.

 Serv-U File Server regularly checks each file in the directory for its age, and performs the specified action on the files that meet the age criteria specified.

## Domain Limits & Settings

Limits and settings are used to configure the basic settings and behavior for the selected domain, including FTP command processor customization and SSL/SSH encryption and certificate options. Limits and settings configured at the server level are inherited by all domains, groups, and users. Limits and settings configured at the domain level are inherited by all groups, and users within the domain.

### Limits

Limits are grouped based upon the area of the domain they are responsible for configuring. Limits allow specifying multiple values for the same option that are applied based upon the time of day and the day of the week. Domain level limits can be overridden at the group, and user level.

### Settings

Domain level settings override those specified by the server. They are also used by the domain's user accounts and groups as default values when not overridden. See the help documentation for detailed information on each setting.

### FTP Settings

The domain FTP command processor overrides the settings specified at the server level. It configures advanced behavior such as text responses to FTP commands, individual FTP command settings, and disabling the use of an FTP command by clients.

### Encryption

The encryption options for this domain overrides server-level settings. Encryption options are available for both SSL- and SSH-based connections.

### Custom HTML

The Custom HTML feature is used to customize the look of your Serv-U File Server login page for this domain.

### File Sharing (MFT only)

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


## Serv-U domain limits

There are many options to customize how Serv-U can be used, and these can be set at the user, group, domain, and server level.

- For the Server Limits page, click [here](#).
- For the User Properties: Limits page, click [here](#).
- For the Group Properties: Limits page, click [here](#).

The limits stack intelligently, so user settings override group settings, group settings override domain settings, and domain settings override server settings. In addition, you can configure limits so they only apply during certain days of the week, and certain times of the day.

Select Limits and Settings from the Domain menu. The Limits tab is displayed by default.

 Most limits and settings on this tab are self-explanatory. However, the "Allow users to change password" setting in the Password limit types is overridden by the "User must change password at next login" option if set to No.

Default limits are displayed against a blue background. These cannot be edited or deleted, but can be overridden by adding a new limit.


### Override a default limit

1. Select the Limit Type containing the limit to override.
2. Click Add.
3. Select the limit to add.
4. Enter the value for the limit.
5. Click Advanced to specify a day and time to which this limit applies.
6. Check the Apply limit only at this time of day if you want to specify a time period for which this limit is in force, and select the Start and End Times.
7. Select the Days of the Week for which this limit applies.
8. Click Save.

The new limit is displayed in the list. (The default is still displayed, even though it is overridden.)

## Edit a limit

1. Select a non-default limit, and click Edit.

 If you try to edit a default limit a message is displayed informing you that default limits cannot be edited and asking if you want to create a new limit to override it.

2. Amend the value as required.
3. If you want to change the day and time to which this limit applies, click Advanced.
4. Click Save.

## Domain settings

On the Domain Limits & Settings > Settings pages, you can configure basic settings that affect performance, security, logo-in display, and network connectivity for the domain. 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 you can configure.

### 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 for legitimate users to correct an incorrect password before they are blocked.

When enabled, this option temporarily blocks (for the specified number of minutes) IP addresses that fail to successfully login (after the specified number of attempts within the specified number of seconds). IP addresses blocked in this way can be viewed in the appropriate IP access rules tab. A successful login resets the counter that is tracking login attempts.

**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 provided to the client.

**Default Web Client** For the MFT Server, this enables you to specify whether the Web Client, Web Client Pro, FTP Voyager JV or File Sharing should be used by all HTTP clients by default. The third, default option is to prompt the users for the client they want to use instead. This option is also available at the group and user level.

**Custom HTTP Logo, Login Page Text & Title Settings**

HTTP Login Title Text (no HTML)	Enter a text-only title to appear when a HTTP client logs into the file server.
Custom Logo Path	<p>To use your own custom logo, create a 400 x 100 pixel graphic and enter or navigate to its location. An error message will be displayed if this criteria is not met.</p> <p>To use the logo selected for the server level, select &lt;&lt;Inherit default value&gt;&gt; from the drop-down menu.</p>
Use inherited default message	Select to use the sever level message.
HTTP Login Page Text	<p>Enter the text to be displayed on the HTTP login page.</p> <p>This text can be HTML-formatted, including links, images, and standard formatting like italics, bold, underline, alignment and more.</p>

## Custom HTTP Logo, Login Page Text & Title Settings

HTTP Client Interface Background (CSS Only)

MFT only. Enter a CSS background style for the Web Client, File Sharing and FTP Voyager JV landing page. The format is:

```
color url('/%CUSTOM_HTML_DIR%/images/yourimage.png') repeat-type horizontal-alignment vertical-alignment.
```

The %CUSTOM\_HTML\_DIR% 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('/%CUSTOM\_HTML\_DIR%/images/Header01.png') no-repeat right top
- #FFFFFF url('/%CUSTOM\_HTML\_DIR%/images/MyLogoTile.png') repeat-x left top
- red (this example uses no image)
- url('/%CUSTOM\_HTML\_DIR%/images/MyHeader.png') no-repeat center top (this example uses no custom color)

## Password Recovery Message

Subject	The subject line for the password recovery message.
Use inherited default value	Check this box to use the server level message. .
Message	Unless using the inherited or default message, enter the message for the password recovery message to be sent to the client.  \$Name will display the user name.  \$Password will display the user password.



**Password Recovery Message**

Configure SMTP Click to [configure SMTP](#) for the domain .


**Other settings**

Integration Library For information about writing an Integration DLL or Shared Library, see the Serv-U Integration Sample DLL in the Serv-U Integration Sample DLL sub-directory. The Integration API is documented in this sample.

[Ratio Free Files](#) Files listed by clicking 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 user and group accounts.


## Domain FTP settings

You can customize the FTP commands that Serv-U accepts, and also customize the responses of Serv-U to the FTP commands it receives. If configured at the domain level, these settings only apply to this domain. To customize the FTP behavior for a specific domain, select the appropriate domain, open the FTP Settings page for the domain, and then click Use Custom Settings. At any time, you can click Use Default Settings to revert back to the default settings of the server.

 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.

### Edit FTP commands and responses

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

 Only the Information and FTP Responses tabs are displayed for all commands. Other tabs are displayed depending on the command type.

Information On the Information page, basic information about the command is shown along with a link to more information on the Serv-U website. The command can also be disabled by selecting the Disable command option here. Disabled commands are treated as unrecognized commands when received from a client.

FTP Responses	All possible FTP responses to the command as issued by the server are displayed on this tab, and can be modified by clicking Edit for each response. Not all commands have FTP responses. FTP command responses can contain special macros that allow real-time data to be inserted in to the response. For more information, see <a href="#">System variables</a> .
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 home directory of the user for the Message File. If the first message file is not found, 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.
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 impacted by users requesting excessively large listings, recursive listings can be disabled by using the Allow client to specify recursive directory listings with -R parameter option.
Advanced Options	<p>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. The following FTP commands contain advanced configuration options:</p> <ul style="list-style-type: none"><li>• LIST</li><li>• MDTM</li><li>• NLST</li></ul>

## Global Properties

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 <a href="#">System variables</a> .
---------------	--

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, 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 the 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	<p>The following options apply to the FTP protocol in general:</p> <p>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.</p> <p>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 three-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.</p> <p>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.</p>

## 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 about 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 DELETE 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.

## Domain 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 of these methods of encryption to work, a certificate, a private key, or both must be supplied. SSL requires the presence of both, while SSH2 only requires a private key. If you do not have either of these required files, you can create them in Serv-U.

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

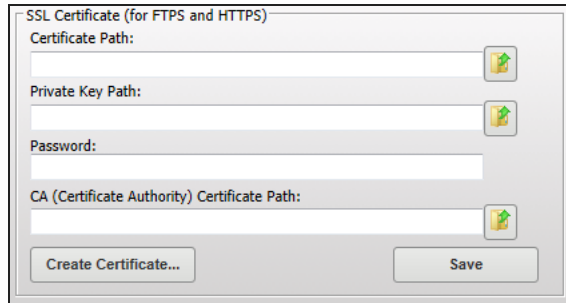
When creating SSL/TLS, SSH, and HTTPS encrypted domains within Serv-U, it is important to know that encrypted domains cannot share listeners. Because SSL/TLS and SSH encryption is based on encrypting traffic sent between IP addresses, each domain must have unique listeners in order to operate properly.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

## Configure SSL for FTPS and HTTPS


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 on the server.

3. In Serv-U, go to select the domain and go to Limits & Settings > Encryption.




SSL Certificate (for FTPS and HTTPS)


Certificate Path:  

Private Key Path:  

Password:

CA (Certificate Authority) Certificate Path:  

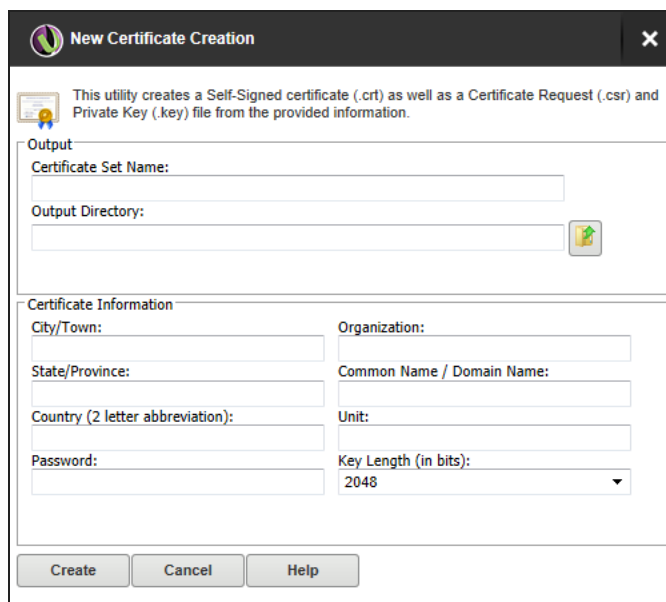
Create Certificate... Save


4. Use the appropriate Browse buttons  to select both the certificate and private key files.
5. Enter the password used to encrypt the private key file.
6. If a CA (Certificate Authority) PEM file has been issued, enter or browse to the file.
7. Click Save.


If the provided file paths and password are all correct, Serv-U will start 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.

## Create a new certificate

1. In Serv-U, select the domain and go to Limits & Settings > Encryption.
2. Click Create Certificate.  
The New Certificate Creation window is displayed.




**New Certificate Creation** 

 This utility creates a Self-Signed certificate (.crt) as well as a Certificate Request (.csr) and Private Key (.key) file from the provided information.

**Output**

Certificate Set Name:

Output Directory:  

**Certificate Information**


City/Town: <input type="text"/>	Organization: <input type="text"/>
State/Province: <input type="text"/>	Common Name / Domain Name: <input type="text"/>
Country (2 letter abbreviation): <input type="text"/>	Unit: <input type="text"/>
Password: <input type="password"/>	Key Length (in bits): <input type="text" value="2048"/>

Create Cancel Help

3. Specify the Certificate Set Name to name each of the files Serv-U creates. For example entering "myName" would result in the creation of:

myName.crt	The self-signed certificate file. This can be used immediately on the server but is not authenticated by any known certificate authority.
myName.csr	The certificate request file. This can be provided to a certificate authority for authentication.
myName.key	The private key file. This is used to secure both certificate files. It is extremely important that you keep the private key in a safe and secure location. If your private key is compromised, your certificate can be used by malicious individuals.

4. Specify the output path where these files are to be placed. In most cases, the installation directory is a safe location. For example: `C:\ProgramData\SolarWinds\Serv-U\`.
5. Enter the city, state (if applicable), two-digit country code, organization, and unit where file server or corporation is located.
6. Specify a password for create the private key.
7. Specify the common name/domain name for the certificate. The IP address or the Fully Qualified Domain Name (FQDN) that users use to connect should be used here.

 If you do not supply the IP address or FQDN used by clients to connect, clients may be prompted that the certificate does not match the domain name to which they are connecting.

8. Select the required key length. 1024 bits provides best performance, 2048 bits is a good median, and 4096 bits provides best security.
9. Click Create.  
The three files are now be created in the specified directory.

## View the certificate

To view the SSL certificate when 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 window.

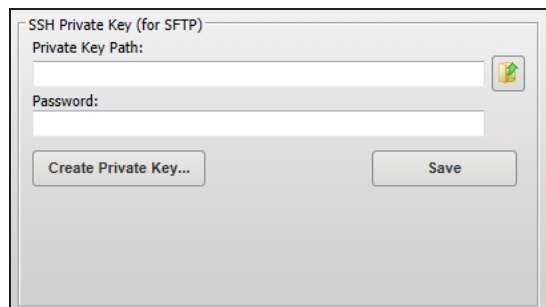
## Advanced SSL options


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

## SFTP (Secure File Transfer over SSH2)

Use an existing private key

1. Obtain a private key file.
2. Place the private key file in a secured directory in the server.
3. In Serv-U, select the domain and go to Limits & Settings > Encryption.

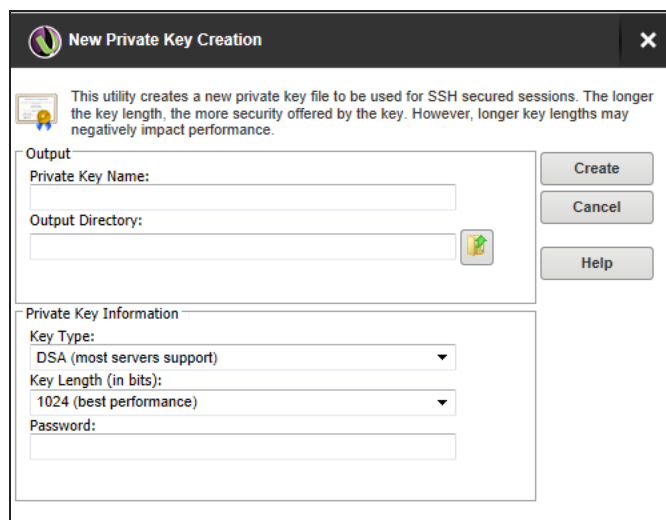


4. Use Browse  to select the file.
5. Enter the password for the private key file.
6. Click Save.

After clicking Save, Serv-U will display the SSH key fingerprint associated with the private key.

Create a private key

1. In Serv-U, select the domain and go to Limits & Settings > Encryption.
2. Click Create Private Key.



3. Enter a name for the private key (for example, MyDomainKey), which is also used to name the storage file.

4. Enter the output path of the certificate. For example,  
`C:\ProgramData\SolarWinds\Serv-U\`
5. Select the Key Type. The default of DSA is preferred, but RSA is available.
6. Select the Key Length. 1024 bits provides best performance, 2048 bits is a good median, and 4096 bits provides best security.
7. Enter the password to use for securing the private key file.
8. Click Create.


After you create a new key, Serv-U displays the SSH key fingerprint associated with the new private key.

## SSH ciphers, MACs and Key Exchange Algorithms

SSH ciphers CAST-128-cbc, Blowfish-cbc and Triple DES-cbc are disabled by default for security reasons. If your specific security needs dictate that only certain ciphers or MACs can be used, you can individually enable (disable) individually ciphers and MACs by selecting (deselecting) the appropriate ciphers or MACs.

## Custom HTML

If you have the MFT edition of Serv-U File Server, you can use custom HTML to enhance the HTTP and HTTPS login pages of Serv-U at the server and domain levels. By using this feature, web developers can design their login experience to show off their exclusive brand and design the page to match existing business themes.

 Users of the basic Serv-U File Server, can customize the logo, login page text and title at the server and domain levels. For more information on this, see [Settings](#).

By using the custom HTML feature, you can provide a custom header and custom footer for the HTTP and HTTPS login page. The main login form is automatically inserted between the content defined in the header and footer files. The custom HTML interface also uses a CSS file to define the style used in the login form. This CSS file can also be used to define custom styles, containers, and other formatting as needed.

Several branding samples are automatically unpacked to your installation folder (for example, `C:\Program Files\SolarWinds\Serv-U\Custom HTML Samples`) when Serv-U is installed. The [Serv-U Custom HTML and CSS](#) article has step-by-step instructions for exploring the current set of samples and build your own branding.

The following fields are used by the Custom HTML feature:



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 is used throughout the header file and footer file, and also the styles that will be used by the login form.
Header File	This .HTM file contains the content for the HTML header inserted before the login form.
Footer File	This .HTM file contains the content for the HTML footer inserted after the login form.
Enable Custom HTML	The custom HTML defined on this page is not used by Serv-U until this option is enabled.


Most custom HTML interfaces include custom images. To use custom images, the storage location of the images must be specified. To universalize the storage location, use the `%CUSTOM_HTML_DIR%` tag in paths that refer to 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 in the following way:

```

```

## File sharing

The MFT edition of Serv-U File Server enables file sharing, which allows domain users to send or receive files from guests. For information, see [File Sharing](#).

 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.

To enable file sharing for the domain:

# 1. Navigate to Domain Limits and Settings > File Sharing.

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"):

File Sharing Repository:

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

☒ Use inherited default message

☐ Use Secure URL (HTTPS)

☐ Enable File Sharing

Configure SMTP... **Save**

Additional file sharing settings are available under the "Limits" tab.  
In order for Serv-U to automatically send file sharing invitation emails, you must configure your [SMTP settings](#).

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 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 not configured yet, configure SMTP to be able to send and receive notification emails.  
For more information about configuring an SMTP server, see [SMTP configuration](#).
9. Click Save.

## Domain activity

This page displays information about and allows management of user sessions across a single domain. The log tab displays server-wide messages and information.

<a href="#">Sessions</a>	This tab displays information about currently active sessions. From this tab, you can view session information, chat with, or ban users.
<a href="#">Statistics</a>	This tab displays statistics about the entire file server across all domains, including session information, transfer stats, and current activity totals.
<a href="#">User &amp; Group Statistics</a>	This tab displays statistics about users and groups, including session information, transfer stats, and activity totals.
<a href="#">Log</a>	This tab displays the server log with real-time updates. This includes start-up information, global messages, and errors.
<a href="#">Settings</a>	This tab provides settings to configure the logging of domain events and activities.

## Domain Sessions

When you view the Sessions page from the Domain Activity tab, all connected sessions from the domain are displayed. When you view the Sessions page while you are administering a domain, only the current sessions of the particular domain are displayed. From this page, you can see an overall picture of the current activity on the file server. In addition, you can view individual sessions, including their current status, connection state, and transfer information.

To view detailed information about 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 an accurate and up-to-date snapshot of the activities of the session.

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

## Disconnect sessions

You can disconnect any type of session at any time by clicking Disconnect. Click this button to bring up another window 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 x	Immediately disconnects the session and bans its IP address for the specified number of minutes (x), preventing the client from immediately reconnecting.
Disconnect and block IP permanently	Immediately disconnects the session and adds a deny IP access rule for the IP address, preventing the client from ever reconnecting from the same IP address.

When disconnecting a session from the Server Session view, you can also use the Apply IP rule to option. By using this option, you can select where you want the temporary or permanent IP ban to be applied: for the entire server, or only the domain the session is connected to.

In addition to disconnecting the session, you can also disable the user account in use by the session by selecting Disable user account.

If the current session is using the FTP protocol, you can send a message 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 because neither protocol defines a method for chatting with users.

## Abort sessions

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

## Broadcast messages

You can send a message to all currently connected FTP sessions by clicking Broadcast. Sending a message through broadcast is equivalent to opening the Spy & Chat window to each individual FTP session and sending it a chat message.

## Spy & Chat

You can spy on any type of session by clicking Spy & Chat or by double-clicking a session in the list. Spying on a user displays all the detailed information normally visible by highlighting the session, and also includes a complete copy of the session log since it first connected to the file server. This way you can browse the log and view all actions taken by the user of the session.

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.

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 discarding them.

## Domain Activity: User & Group Statistics

The User and 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 details.

### Session statistics

Data	Description
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 disconnecting.

Data	Description
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

Data	Description
Download Speed	The cumulative download bandwidth currently being used.
Upload Speed	The 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. 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 at the bottom of the page.

## Domain Log

The Domain Activity > Log pages show logged activity for the domain.

The domain log contains information about and activity pertaining to the currently administered domain only. This includes the status of the listeners of the domain, and any configured activity log information. For more information about the types of activity information that can be placed in the domain log, see [Configure domain logs](#).

You can highlight information contained in the log by clicking and dragging the mouse cursor over the appropriate portion of the log. When it is highlighted, you can copy the selected portion to the clipboard.

Freeze Log	Select this option to temporarily pause the refreshing of the log. This is useful on busy systems so you can highlight and copy a particular section of the log before it scrolls out of view. When you have 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.
Copy to Clipboard	Click this button to automatically freeze the log and copy all information 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 you can use it for reference while you browse the log.
Filter Log	To quickly find and read through specific sections of the log, you can filter it based on a search string. Click this button to bring up the Filter Log window. 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 window, and then click Reset.

## Domain Activity Settings

In the Serv-U File Server, you can customize how domain events and activity are logged. Logging consists of two sections, File and Screen:

**File** 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.

**Screen** When an option is selected from the Screen column, the event is displayed in the log when viewed from the Serv-U Management Console.

To enable a logging option, select the appropriate option in the File or Screen column. You can configure the log to show as much or as little information as you want. After configuring the logging options you want, click Save to save the changes.

**Logfile path name** Before information can be saved to a file, you must specify the name of the log file. Click Browse to select an existing file or directory location for the log file. The log file path supports certain wildcard characters. Wildcard characters which refer to 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 domain activity for audits.

%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, 2019).	????
----	--	------

%X	The 2-digit value of the current year (for example, 15 for 2019).	??
----	---	----

%S	The name of the domain whose activity is being logged.	*
----	--	---

Log files are purged based only on the current log file path name, and they 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

Anything matching the path name you used wildcards for can be purged. Use caution: it is best practice to place log files into a single directory to avoid unexpected file deletion.



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, you can 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.
Keep up to N log files.	You can automatically purge old log files by setting a maximum number of files to keep, a maximum size limit in megabytes, or both. Setting these options to "0" means that the setting is unlimited, and the limit is not applied.
Keep up to N Mb of log files	
Specify IP addresses as exempt from logging	You can 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 significant amount of logging information that can obfuscate domain activity from regular users. It can also be used to save log space and reduce overhead. Click Do Not Log IPs, and then add IP addresses as appropriate.

# Group properties

Group properties can be created at the server or domain level. Settings at the group level are overridden at the user level.

<a href="#"><u>Group Information</u></a>	Basic information required for identifying and using this group.
<a href="#"><u>Directory Access</u></a>	Create rules set up to determine which directories users in this group have access to.
<a href="#"><u>Virtual Paths</u></a>	Link physical paths outside the directory structure of a user's home directory into the directory listings received by that user.
<a href="#"><u>Logging</u></a>	Configure the messages to be logged, the log file path and other logging parameters.
<a href="#"><u>Members</u></a>	The list of members in this group.
<a href="#"><u>Events (MFT only)</u></a>	Create actions such as emails and tray icon messages to be automatically triggered by events specific to this group.
<a href="#"><u>IP Access</u></a>	Create IP access rules for users in this group.
<a href="#"><u>Limited &amp; Settings</u></a>	Configure limits and settings for users in this group. These can apply at specific time on specific days.

## Group Properties: Group Information


The screenshot shows the 'Group Properties' dialog box with the 'Group Information' tab selected. The dialog has a title bar with a close button. Below the title bar is a tabbed interface with tabs for 'Group Information', 'Directory Access', 'Virtual Paths', 'Logging', 'Members', 'Events', 'IP Access', and 'Limits & Settings'. The 'Group Information' tab contains a message: 'All group settings are applied to user accounts that are members of this group. To override a group setting, edit the setting for a specific user account.' Below this message are several settings: 'Group Name' (text field), 'Home Directory' (text field with a browse button), 'Administration Privilege' (dropdown menu set to 'No Privilege'), 'Default Web Client' (dropdown menu set to 'Prompt user for client'), 'Always allow login' (checkbox, unchecked), 'Enable account' (checkbox, checked), 'SSH Keys' (button 'Manage Keys...'), 'Lock user in home directory' (checkbox, checked), and 'Apply group directory access rules first' (checkbox, checked). At the bottom of the tab is a large 'Description' text area. On the right side of the dialog, there are buttons for 'Availability...' and 'Welcome Message...'. At the bottom of the dialog are 'Save', 'Cancel', and 'Help' buttons.

**Group Properties**

Group Information | Directory Access | Virtual Paths | Logging | Members | Events | IP Access | Limits & Settings

All group settings are applied to user accounts that are members of this group. To override a group setting, edit the setting for a specific user account.

Group Name:

Home Directory:  

Administration Privilege: **No Privilege**

Default Web Client: **Prompt user for client**

☐ Always allow login


☒ Enable account


Description:

SSH Keys: **Manage Keys...**

☒ Lock user in home directory

☒ Apply group directory access rules first

 Availability...

 Welcome Message...

**Save** **Cancel** **Help**

Group Name

A unique name for this group.

## Administration Privilege

Select the level of privilege to be applied to users in this group.

**No Privilege.** A regular user account that can only transfer files to and from the File Server. The Serv-U Management Console is not available.

**Group Administrator.** A Group Administrator can only perform administrative duties relating to their primary group - the group listed first in their Groups memberships list. They can add, edit, and delete users which are members of their primary group. They can also assign permissions at or below the level of the Group Administrator. They may not make any other changes.

**Domain Administrator.** A Domain Administrator can only perform administrative duties for the domain to which their account belong, and 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 are:

- configuring their domain listeners
- configuring or administering LDAP groups
- configuring ODBC database access for the domain

**System Administrator.** A System Administrator can perform any file server administration activity including creating and deleting domains, user accounts, and even updating the license of the file server. A user account with System Administrator privileges logged in through HTTP remote administration can administer the server as if they had physical access to the server.

**Read-only Group/Domain/Server Administrator.** Read-only administrator accounts can allow administrators to log in and view configuration options at the group, 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, and cannot create, delete or edit user accounts.

Default Web Client	<p>If your Serv-U license enables the use of FTP Voyager JV, then users in this group connecting to the file server through HTTP can choose which client they want to use after logging in. Instead of asking users in this group which client they want to use, you can also specify a default client. If you change this option, it overrides the option specified at the server or domain level.</p>
Always Allow Login	<p>Enabling this option means that user accounts in this group are 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. 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.</p> <p>Enabling the Always Allow Login option does not override <a href="#">IP access rules</a>. If both options are defined, the IP access rules prevail.</p>
Enable Account	<p>Deselect this option to disable the user accounts in this group. Disabled accounts remain on the file server but cannot be used to log in. To re-enable accounts in this group, select the Enable account option again.</p>
Description	<p>Enter an optional description for this group. This description is only visible to administrators.</p>


Home Directory	<p>Enter or navigate to the home directory for users in this group. This is where the user is placed immediately after logging in to the file server. This must be specified using a full path including the drive letter or the UNC share name.</p> <p>When you specify the home directory, you can use the %USER% macro 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 it is combined with a directory access rule for %HOME%, a new user can be configured with a unique home directory and the appropriate access rights to that location with a minimal amount of effort.</p> <p>You can also use the %DOMAIN_HOME% macro to identify the users in this group's home directory. For example, to place a user's home directory into a common location, use %DOMAIN_HOME%\%USER%.</p> <p>The home directory can be specified as "/" (root) in order to grant system-level access to user in this group, allowing them to access all system drives. In order for this to work properly, users in this group must not be locked in their home directory.</p>
SSH Keys	<p>If you have MFT edition of Serv-U, you can specify a SSH public key to be used to authenticate a user in this group when logging in to the the Serv-U File Server.</p> <p>For information on SSH public key authentication, adding a SSH key pair, and creating an key pair for testing, see <a href="#">New SSH Key Pair Creation</a>.</p>
Lock user in home directory	<p>Users 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 because Serv-U always reports it as "/" (root).</p>
Apply group directory access rules first	<p>The order in which directory access rules are listed has significance in determining the resources that are available to a user account in this group. By default, directory access rules specified at the group level take precedence over directory access rules 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 directory access rules of the group below the user's.</p>

Availability	Click to open the Availability Settings window where you can configure the time of day and/or days of the week when users in this group can log in.
Welcome Message	<p>Click Welcome Message if you want to sent a welcome message to users in this group when they log in. The welcome message is a message traditionally sent to the FTP client during a successful user login. Serv-U extends this ability to HTTP so that users in this group 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 through SFTP over SSH2, because SSH2 does not define a method for sending general text information to users.</p> <p>Check Include if you want to include the response code in the welcome message test when an FTP connection is made.</p> <p>Either select or navigate to a message file if you have already created a text file containing a welcome message or check the Override box, and enter a message specific to the user in this group in the text box above it.</p>

## Group Properties: Directory Access


Directory access rules define which areas of the system are accessible to user accounts. Directory access rules specified at the server level are inherited by all users of the file server. If they are specified at the domain level, they are only inherited by users who belong to the particular domain. The traditional rules of inheritance apply where rules specified at a lower level (for example, the user level) override conflicting or duplicate rules specified at a higher level (for example, the server level).

When you set the directory access path, you can use the `%USER%`, `%HOME%`, `%USER_FULL_NAME%`, and `%DOMAIN_HOME%` variables to simplify the process.

 For example, use `%HOME%/ftproot/` to create a directory access rule that specifies the `ftproot` folder in the home directory of the user.

Directory access rules specified in this manner are portable if the actual home directory changes while maintaining the same subdirectory structure. This leads to less maintenance for the file server administrator. If you specify the %USER% variable 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. You can use the %USER\_FULL\_NAME% variable 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\%USER\_FULL\_NAME% for D:\ftproot\Tom Smith. You can also use the %DOMAIN\_HOME% macro 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 listed. The first rule in the list that matches the path of a client's request is the one 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 particular subdirectory. Use the arrows on the right of the directory access list to rearrange the order in which the rules are applied.

 Serv-U File Server allows to list and open the parent directory of the directory the user is granted access to, even if no explicit access rules are defined for the parent directory. However, the parent directory accessed this way will only display the content to which the user has access.

## Permissions

### File Permission

Read	Allows users to read (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 (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 typically used to enable users to resume transferring partially uploaded files.
Rename	Allows users to rename files.
Delete	Allows users to delete files.
Execute	Allows users to remotely execute files. The execute access is meant for remotely starting programs and usually applies to specific files. This is a powerful permission and great care should be used in granting it to users. Users with Write and Execute permissions can install any program on the system.



## Directory Permission

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.
Create	Allows users to create new directories within the directory.
Rename	Allows users to rename directories within the directory.
Remove	Allows users to delete existing directories within the directory.  If the directory contains files, the user also must have the Delete files permission to remove the directory.

## Subdirectory Permission

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 (for example, when implementing mandatory access control), clear the Inherit check box and grant permissions specifically by folder.
---------	--


## 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 would result in the directory content 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.

## Advanced: Access as Windows user (Windows only)

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 File Server, you can configure the SolarWinds Serv-U File Server service to run under a network account. The alternative, preferred where many servers exist, or if the SolarWinds Serv-U File Server service has to run under Local System for security reasons, is to configure a directory access rule to use a specific Windows user for file access. Click Advanced to specify a specific Windows user for each directory access rule. As in Windows authentication, directory access is subject to NTFS permissions, and in this case also to the configured permissions in Serv-U File Server.

 When you use Windows authentication, the NTFS permissions of the Windows user take priority over the directory access rules. This means that when a Windows user tries to access a folder, the security permissions of the user are applied instead of the credentials specified in the directory access rule.

## Examples

### Mandatory access control

You can use mandatory access control (MAC) 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.

In the following example, the rule applies to `C:\ftproot\`.



The screenshot shows the "Directory Access Rule" dialog box. The "Path" field is set to "C:\ftproot\". The "Files" section has checkboxes for Read, Write, Append, Rename, Delete, and Execute (which is disabled with a warning icon). The "Directories" section has checkboxes for List, Create, Rename, and Remove. The "Subdirectories" section has an "Inherit" checkbox that is unchecked. The "Maximum size of directory contents" field is empty, with the text "MB (leave blank for no limit)". On the right side, there are buttons for "Save", "Cancel", "Help", "Full Access", "Read Only", and "Advanced >>".

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 SolarWinds Serv-U File Server.

## Restrict file types

If users are using storage space on the SolarWinds Serv-U File Server to store non-work-related files, such as .mp3 files, you can prevent this by configuring a directory access rule placed above the main directory access rule 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:



**Directory Access Rule**

Path:

**Files**

<input type="checkbox"/> Read	<input type="checkbox"/> Delete
<input type="checkbox"/> Write	<input type="checkbox"/> Execute 
<input type="checkbox"/> Append	
<input type="checkbox"/> Rename	

**Directories**

<input type="checkbox"/> List
<input type="checkbox"/> Create
<input type="checkbox"/> Rename
<input type="checkbox"/> Remove

**Subdirectories**

☒ Inherit

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

**Buttons:** Save, Cancel, Help, Full Access, Read Only, Advanced >>

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 the directory to which they need access.

**Directory Access Rule**

Path: %HOME%

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)

Buttons: Save, Cancel, Help, Full Access, Read Only, Advanced >>

In the second rule, enter the extension of the file that should be accessed, such as \*.mdb.

**Directory Access Rule**

Path: \*.mdb

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)

Buttons: Save, Cancel, Help, Full Access, Read Only, Advanced >>

These rules only allow users to access .mdb files within the specified directories. You can adapt these rules to any file extension or set of file extensions.

Directory Access		Virtual Paths	File Management
		Domain directory access rules are global rules that define the files and directories overridden at the group and user levels.	
Path		Access	
*.mdb		RWADN-L---I	
%HOME%		-----L---I	

## Group Properties: Virtual Paths

If virtual paths are specified, users can 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 access 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 all users of the file server. Virtual paths created at the domain level are only accessible by users belonging to that domain.

### 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, use a full path, such as `D:\inetpub\ftp\public`. You can also use a UNC path, such as `\\Server\share\public`. To make a virtual path visible to users, users must have a directory access rule specified for the physical path.

### Virtual path

The virtual path is the location 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. You can also use a full path without any macros.

### Include virtual paths in Maximum Directory Size calculations

When this option is selected, the virtual path is included in Maximum Directory Size calculations. The Maximum Directory Size limits the size of directories affecting how much data can be uploaded.

## Examples

### Virtual paths

A group of web developers have been granted access to the directory `D:\ftproot\example.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 group of web developers, add a virtual path to bring the directory to the users by specifying `D:\corpimages\` as the physical path and `D:\ftproot\example.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.

### Relative virtual paths

Continuing with the previous example, if the home directory of the group of web developers is relocated to another drive, both the home directory and the virtual path must be updated to reflect this change. You can avoid this 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\example.com\corpimages` as the virtual path, use `%HOME%\corpimages`. This way the corpimages virtual path is placed within the home directory of the group, regardless of what the home directory is. If the home directory changes at a later date, the virtual path still appears there.

## Group Properties: Logging

In the Serv-U File Server, you can customize the logging of user and group events and activity to a great extent.

### Log Message Options

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 in the Logging to File Settings section is selected. You can configure the log 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 name** Specify the name of the log file for information to 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. Wildcard characters which refer to 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.

%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, 2019).

%X The 2-digit value of the current year (for example, 15 for 2019).

%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 that you 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 area.

**Automatically rotate log file** To ensure that log files remain a manageable size and can be easily referenced during auditing, you can automatically rotate the log file on a regular basis. By specifying a Log file path containing wildcards that reference the current date, Serv-U can rotate the log file and create a unique file name every hour, day, week, month, or year.

Keep up to 'n' log files  
Keep up to MB of log files

You can automatically purge old log files by setting a maximum number of files to keep, a maximum size limit in megabytes, or both. Setting these options to "0" means that 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 they 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
```

Do Not Log IPs

You can 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 log space and reduce overhead. Click Do Not Log IPs, and add IP addresses as appropriate.

Download Log

Click to download the log file.

## Group Properties: Members

The user accounts that are members of the currently selected group are displayed on this page. It can be used to get a quick overview of what users are currently inheriting the settings of the group at this time. 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 Properties: Groups window.

## Group Properties: Events

With the MFT edition of the Serv-U File Server, you can automatically associate file server events with



email notifications, balloon tip alerts or posts to the Windows Event Log or Microsoft Message Queue (MSMQ). For example, you might want to be notified in the event of a listener failure or whenever a new file is uploaded.

To access the events tab for a group, select Groups from the Global or Domain menu, click Edit, and select the Events tab from the Group Properties window.

To access events for an individual user, select Users from the Global or Domain menu, click Edit, and select the Events tab from the User Properties window.

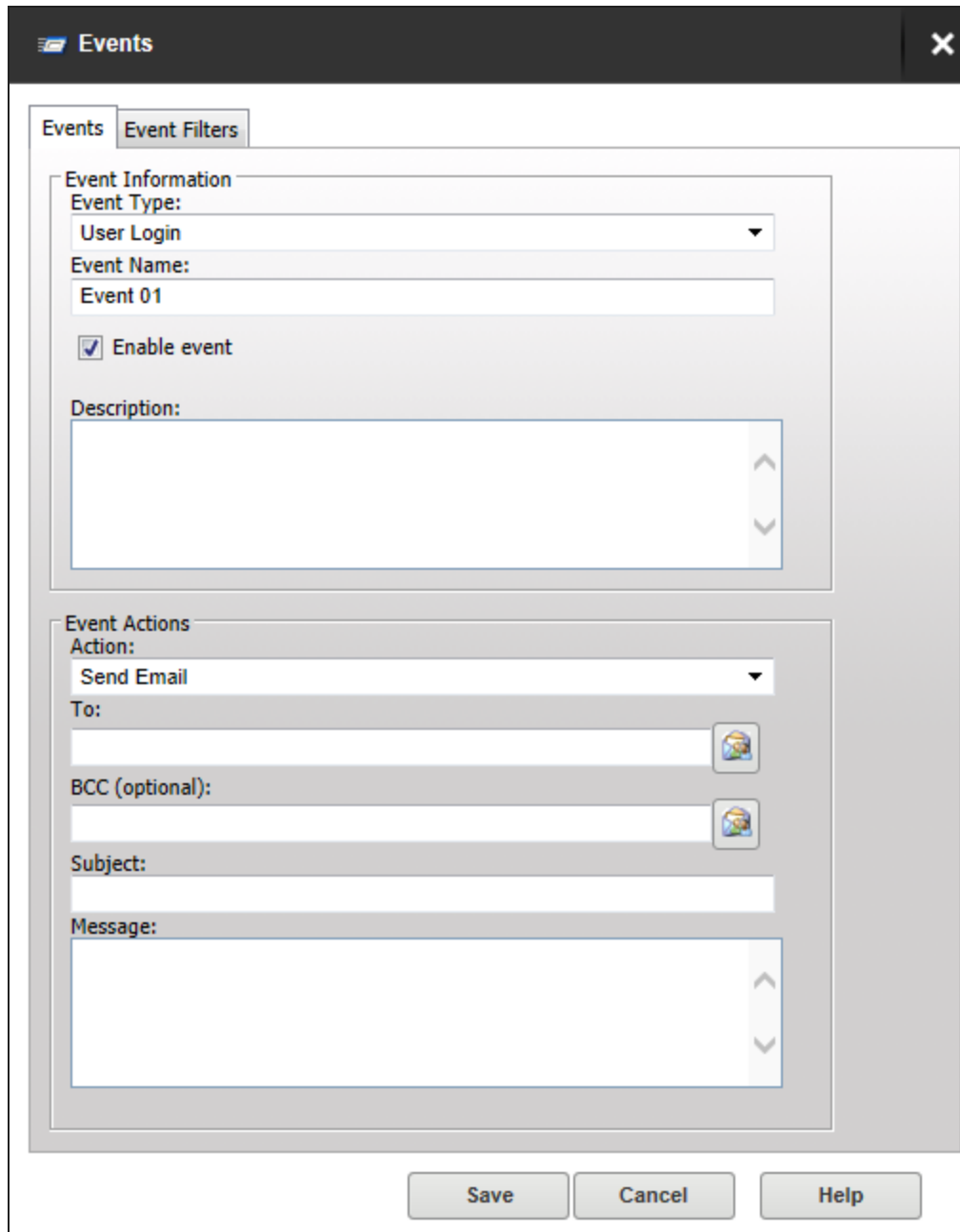
## Create Common Events

To instantly populate the events list with the most commonly used file server events:

1. Click Create Common Events.
2. Select the event action to apply to all common events.
3. Enter the email address to receive all notifications if you selected Send Email.
4. Enter the Message Queue Path if you selected Write to Microsoft Message Queue.
5. Click OK.
6. The 13 most common file server events are created. These can be customized by selecting an event and clicking Edit.

## Add an event

1. Click Add.



**Events** [X]

Events | Event Filters

**Event Information**

Event Type:  
User Login ▼

Event Name:  
Event 01

☒ Enable event

Description:  
[Empty text area]

**Event Actions**

Action:  
Send Email ▼

To:  
[Empty text field] [User icon]


BCC (optional):  
[Empty text field] [User icon]

Subject:  
[Empty text field]

Message:  
[Empty text area]


Save Cancel Help

2. Select the Event Type.
3. Enter a name and description for this event.


 If you want to create but not immediately enable an event, uncheck the Enable event box.


4. Select the action to be triggered by this event, and complete the associated fields.

The actions that can be triggered are:

Event Action	Description
Send Email	<p>You can configure email actions to send emails to multiple recipients and to Serv-U File Server groups when an event is triggered.</p> <p>Enter the recipients in the To and BCC fields. Separate email addresses by commas or semicolons.</p> <p>To send emails to Serv-U groups, click the Group icon and drag the required groups from the Available Groups column to the Group Email List column.</p> <p>Enter the subject and message. You can use <a href="#">system variables</a> to include data specific to the event.</p>
Show Balloon Tip	<p>Balloon Tips are displayed in the system tray when an event is triggered. Balloon tip actions require a Balloon Title and Balloon Message. You can use <a href="#">system variables</a> to include data specific to the event.</p>
Execute Command (not available for Common Events)	<p>You can configure the execute of a file when an event is triggered. Execute command actions contain an Executable Path, Command Line Parameters, and a 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 zero to execute immediately.</p> <div>  Time spent waiting delays any processing that Serv-U File Server can perform.         </div> <p>A wait value should only be used to give an external program enough time to perform an operation, such as move a log file before it is deleted (for example, <code>\$LogFilePath</code> for the Log File Deleted event). You can use <a href="#">system variables</a> to use data specific to the event.</p>

Event Action	Description
Write to Windows Event Log (Windows only)	<p>By writing event messages to a local Windows Event Log, you can monitor and record Serv-U File Server activity using third-party network management software.</p> <p>The message entered into the Log Information field is 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. <a href="#">System variables</a> are supported for this field. This field can be left blank, but usually is not.</p>

Event Action	Description
Write to Microsoft Message Queue (MSMQ) (Windows only)	<p data-bbox="773 226 1511 590">Microsoft Message Queuing (MSMQ) is an enterprise technology that provides a method for independent applications to communicate quickly and reliably. Serv-U File Server can send messages to new or existing MSMQ queues whenever an event is triggered. 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 occurred.</p> <div data-bbox="786 632 1463 999"> <p> Microsoft message queues created in Windows do not grant access to SYSTEM by default, preventing Serv-U File Server from writing events to the queue. 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 File Server runs) has permission to the queue.</p> </div> <p data-bbox="773 1041 1382 1073">These events have the following two fields:</p> <p data-bbox="773 1104 1511 1598"><b>Message Queue Path:</b> 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. Public queues on the local machine can be addressed when a full path is not specified (for example, .\Serv-U Message Queue or Serv-U Message Queue). If the specified queue does not exist, Serv-U File Server attempts to create it. This normally only works on public queues on the local machine. You can also use Serv-U File Server system variables in this field.</p> <p data-bbox="773 1629 1511 1871"><b>Message Body:</b> 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 File Server system variables can also be used in this field. This field may be left blank, but usually is not.</p>

 Only the email action is available to users other than Serv-U File Server server administrators.

## Edit an Event

1. Select the event you want to edit and click Edit.
2. Edit the event details and the event filters as required.
3. Click Save.

## Add an Event filter

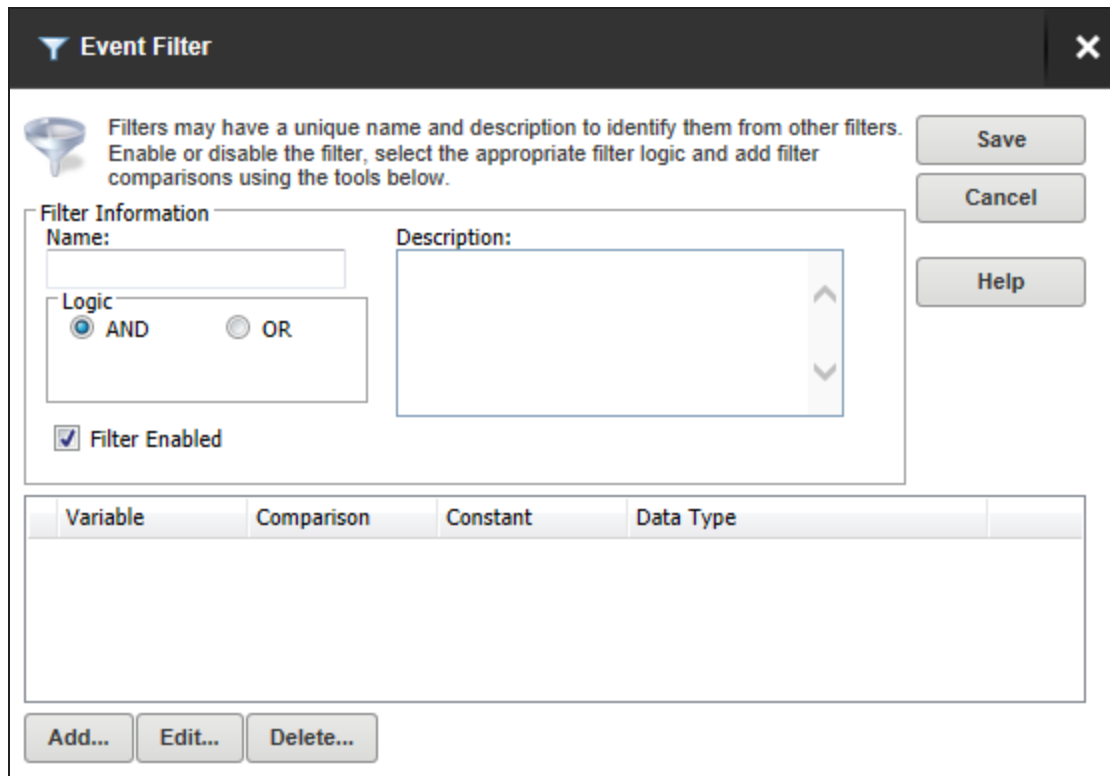
Event filters allow you to control when a Serv-U File Server event action is triggered. By default, event actions are triggered each time the event occurs. Event filters allow events to be triggered only if certain conditions are met.

For example, a standard event may trigger an email each time a file is uploaded to the server. However, by using an event filter, events can be triggered on a more targeted basis, such as configuring a File Uploaded event to send an email only if the file name contains the string `important`. Thus an email would be sent when the file `Important Tax Forms.pdf` is uploaded but not for other files.

Additionally, you could configure a File Upload Failed event to run only when the FTP protocol is used, not triggering for failed HTTP or SFTP uploads. You can do this by controlling the variables and values related to the event and by evaluating their results when the event is triggered.

To add an event filter to an event:

1. Click the Events Filters tab.
2. Click Add.



**Event Filter**

Filters may have a unique name and description to identify them from other filters. Enable or disable the filter, select the appropriate filter logic and add filter comparisons using the tools below.

**Filter Information**

Name:

Description:

Logic

☒ AND ☐ OR

☒ Filter Enabled

Save Cancel Help

Variable	Comparison	Constant	Data Type

Add... Edit... Delete...

3. Enter the following filter information:

Name	The name of the filter, used to identify the filter for the event.
------	--

Description (Optional)	The description of the event, which may be included for reference.
---------------------------	--

Logic	This determines how the filter interacts with any other filter set up for an event. In most cases, AND is used, and 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).
-------	--

4. Click Add to open the File Comparison window.
5. Select the [System Variable](#) to be used in the comparison.
6. Select the comparison method.

7. Enter the value the system variable is to be compared to. The following wild cards can be used.

- \* The asterisk wildcard matches any text string of any length. For example:
  - An event filter that compares the `$FileName` variable to the string `data*` matches files named `data`, `data7`, `data77`, `data.txt`, `data7.txt`, and `data77.txt`.
- ? The question mark wildcard matches any one character, but only one character. For example:
  - An event filter that compares the `$FileName` variable to the string `data?` matches a file named `data7` but not `data`, `data77`, `data.txt`, `data7.txt`, or `data77.txt`.
  - An event filter that compares the `$FileName` variable to the string `data?.*` matches files named `data7` and `data7.txt` but not `data`, `data77`, `data.txt`, or `data77.txt`.
  - An event filter that compares the `$Name` variable to the string `A????` matches any five-character user name that starts with `A`.
- [ ] The bracket wildcard matches a character against the set of characters inside the brackets. For example:
  - An event filter that compares the `$FileName` variable to the string `data[687].txt` matches files named `data6.txt`, `data7.txt` and `data8.txt` but not `data5.txt`.
  - An event filter that compares the `$LocalPathName` variable to the string `[CD]:\*` matches any file or folder on the `C:` or `D:` drives.

You can use multiple wildcards in each filter. For example:

- An event filter that compares the `$FileName` variable to the string `[cC]:\*.???` matches any file on the `C:` drive that ends in a three letter file extension.
- An event filter that compares the `$FileName` variable to the string `?:\*Red[678]\?????.*` matches 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.


8. Select the data type.


9. And another filter for this event or click Save to close.

## Filter examples

**Example 1.** An administrator may want to raise an email event when the file `HourlyUpdate.csv` is uploaded to the server, but not when other files are uploaded. To do this, create a new event 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 below:



 **Filter Comparison** ✕

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

If  = (is equal to)

Data Type:


Save


Cancel

Help

**Example 2.** It may be necessary to know when a file transfer fails for a specific user account. To perform this task, create a new File Upload Failed event, and add a new filter.

The filter comparison is the `$Name` variable, and the value to compare is the user name, such as `ProductionLineFTP`:

 **Filter Comparison** ✕

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

If  = (is equal to)


Data Type:


Save

Cancel

Help

**Example 3, using wildcards.** You can also filter for events based on specific folders using wildcards. 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, create a new File Uploaded event in the Domain Details > Events menu, and set it to Send Email. Enter the email recipients, subject line, and message content, and then open the Event Filters page. 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\`.

 **Filter Comparison** ✕

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

If  = (is equal to)

Data Type:

Save

Cancel

Help

## Group Properties: IP Access

The IP Access tab shows the IP access rules set up for the server, domain, group or individual user, and allows you to add, import, edit, export and delete these rules.

Rules set at the group level are inherited by all users that are member of the group unless overridden.

IP access rules enable you to specify IP addresses, or ranges of IP addresses to which access is allowed or denied. These rules are applied as soon as a physical connection is established. Rules are applied in the order 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. Use the arrows on the right side of the list to change the position of an individual rule in the list.

### Display the IP access list

1. Navigate to Global or select the appropriate domain, click Groups, select the group, and click Edit.
2. Click the IP Access tab.

The list of IP addresses set up at this level is displayed.

Use the arrows on the right side of the list to change the position of an individual rule in the list.

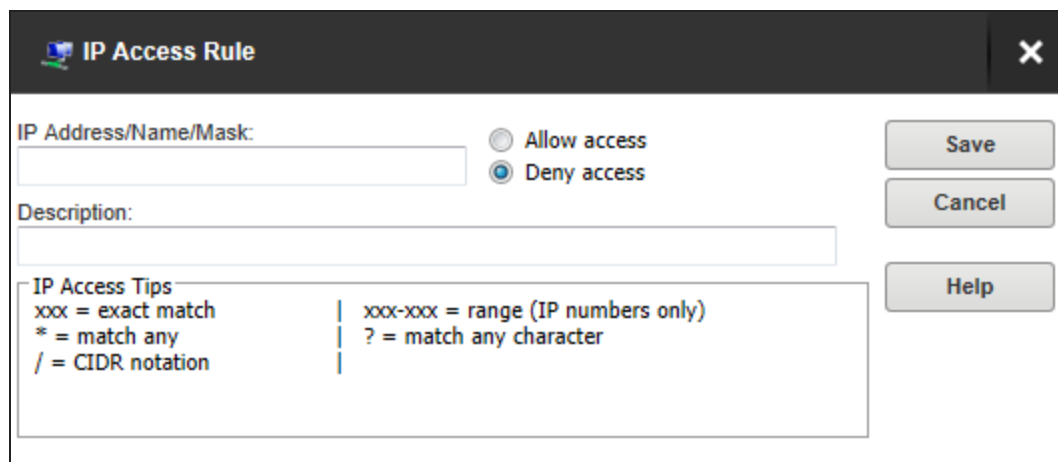
Check the Enable sort mode box to sort the IP access list numerically rather than in the processing order. Displaying the IP access list in sort mode does not change the order in which rules are processed. To view rule precedence, disable this option.



Viewing the IP access list in numerical order can be useful when you review long lists of access rules to determine if an entry already exists.

### Add an IP access rule

1. From the IP tab, click Add.  
The IP Access Rule window is displayed.



**IP Access Rule**

IP Address/Name/Mask:

☐ Allow access  
☒ Deny access

Description:

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

Save Cancel Help

- Enter the IP Address, name or mask using the following conventions.

Value or wildcard	Explanation
xxx	Stands for an exact match, such as 192.0.2.0 (IPv4), fe80:0:0:0:a450:9a2e:ff9d:a915 (IPv6, long form) or fe80::a450:9a2e:ff9d:a915 (IPv6, shorthand).
xxx-xxx	Stands for a range of IP addresses, such as 192.0.2.0-19 (IPv4), fe80:0:0:0:a450:9a2e:ff9d:a915-a9aa (IPv6, long form), or fe80::a450:9a2e:ff9d:a915-a9aa (IPv6, shorthand).
*	Stands for any valid IP address value, such as 192.0.2.*, which is analogous to 192.0.2.0-255, or fe80::a450:9a2e:ff9d:*, which is analogous to fe80::a450:9a2e:ff9d:0-ffff.
?	Stands for any valid character when specifying a reverse DNS name, such as server?.example.com.
/	Specifies 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.

- Enter a description.
- Select Allow or Deny access.
- Click Save.

## Edit an IP access rule

1. From the IP tab, click Edit.
2. Amend the rule information as required..
3. Click Save.

## Delete an IP access rule

1. From the IP tab, select the IP rule or rules to delete.
2. Click Delete and confirm.

## Import and export global IP address rules

You can speed up the creation of IP address rules by creating a text file of addresses, descriptions and access permissions.

1. Create a text file using Notepad or similar text editor.
2. On the first line enter "IP","Description","Allow".
3. Enter the details of each IP access rule:

IP	The IP address, IP range, CIDR block, or domain name for which the rule applies.
Description	A text description of the rule for reference purposes.
Allow	Set this value to 0 for Deny, or 1 for Allow.

For example:

```
"IP", "Description", "Allow"
"172.16.0.1", "Flange Software", "1"
"172.16.0.*", "Do not allow", "0"
"2001:db8::/32", "New test site", "1"
```

4. From the IP tab, click Import.
5. Navigate to the file you created, and click Select.

Similarly, the list of existing IP address rules can be exported to a text file by clicking Export.

For examples of IP address rules and IP address caveats see [Examples of IP address rules and caveats](#).


## Serv-U group properties: limits & settings

There are many options to customize how Serv-U can be used, and these can be set at the user, group, domain, and server level.

- For the Server Limits page, click [here](#).
- For the Domain Limits page, click [here](#).
- For the User Properties: Limits page, click [here](#).

The limits stack intelligently, so user settings override group settings, group settings override domain settings, and domain settings override server settings. In addition, you can configure limits so they only apply during certain days of the week, and certain times of the day.

Select the Limits & Settings tab from the Group Properties window.

 Most limits and settings on this tab are self-explanatory. However, the "Allow users to change password" setting in the Password limit types is overridden by the "User must change password at next login" option if set to No.

Default limits are displayed against a blue background. These cannot be edited or deleted, but can be overridden by adding a new limit.


### Override a default limit

1. Select the Limit Type containing the limit to override.
2. Click Add.
3. Select the limit to add.
4. Enter the value for the limit.
5. Click Advanced to specify a day and time to which this limit applies.
6. Check the Apply limit only at this time of day if you want to specify a time period for which this limit is in force, and select the Start and End Times.
7. Select the Days of the Week for which this limit applies.
8. Click Save.

The new limit is displayed in the list. (The default is still displayed, even though it is overridden.)

## Edit a limit

1. Select a non-default limit, and click Edit.

 If you try to edit a default limit a message is displayed informing you that default limits cannot be edited and asking if you want to create a new limit to override it.

2. Amend the value as required.
3. If you want to change the day and time to which this limit applies, click Advanced.
4. Click Save.

## Ratios Free Files

The Group Limits and Settings page enables you to set up "free" files for each individual user.

- [Ratio Free Files](#)

# User properties

User properties can be created at the server or domain level. Settings at the user level override all others.

<a href="#">User Information</a>	Basic information required for this user.
<a href="#">Directory Access</a>	Create rules set up to determine which directories this user has access to.
<a href="#">Virtual Paths</a>	Link physical paths outside the directory structure of a user's home directory into the directory listings received by that user.
<a href="#">Logging</a>	Configure the messages to be logged, the log file path and other logging parameters.
<a href="#">Groups</a>	The groups to which this user belongs.
<a href="#">Events (MFT only)</a>	Create actions such as emails and tray icon messages to be automatically triggered by events specific to this group.
<a href="#">IP Access</a>	Create IP access rules for users in this group.
<a href="#">Limited and Settings</a>	Configure limits and settings specific to this users. These can apply at specific time on specific days.

# User Properties: User Information

**User Properties** [X]

User Information | Directory Access | Virtual Paths | Logging | Groups | Events | IP Access | Limits & Settings

User account information specifies the login credentials and privileges granted to this account.

Login ID:   
 Password:    
 Administration Privilege: **No Privilege** ▼  
 Account Type: **Permanent** ▼  
 Default Web Client: **Web Client** ▼  
 Email Address:   
☒ Enable account  
 Description:   
 Full Name:   
 Home Directory:    
 SSH Keys:   
☒ Lock user in home directory  
☐ Always allow login  
☐ User must change password at next login

## 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 the particular level. Login IDs cannot contain any of the following special characters:

`\ / < > | : . ? *`

Two special login IDs exist: Anonymous and FTP. These login IDs are synonymous with one another, and they 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.



## Password

The password is the second item that is required so that a session can 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 six characters including a mix of upper and lowercase letters and at least one number. You can place restrictions on the length and complexity of passwords through limits. For more information about password limits, see [User limits and settings](#).

You can also 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 eight 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

Select the level of privilege to be applied to users in this group.

**No Privilege.** A regular user account that can only transfer files to and from the File Server. The Serv-U Management Console is not available.

**Group Administrator.** A Group Administrator can only perform administrative duties relating to their primary group - the group listed first in their Groups memberships list. They can add, edit, and delete users which are members of their primary group. They can also assign permissions at or below the level of the Group Administrator. They may not make any other changes.


**Domain Administrator.** A Domain Administrator can only perform administrative duties for the domain to which their account belong, and 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 are:

- configuring their domain listeners
- configuring or administering LDAP groups
- configuring ODBC database access for the domain

**System Administrator.** A System Administrator can perform any file server administration activity including creating and deleting domains, user accounts, and even updating the license of the file server. A user account with System Administrator privileges logged in through HTTP remote administration can administer the server as if they had physical access to the server.

**Read-only Group/Domain/Server Administrator.** Read-only administrator accounts can allow administrators to log in and view configuration options at the group, 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, and cannot create, delete or edit user accounts.

---

Account Type	<p>By default, all accounts are permanent and exist on the file server until manually deleted or disabled. You can configure an account to be automatically disabled or deleted on a specified date by configuring the account type. After selecting the appropriate type, the Account Expiration Date control is displayed. Click the calendar or expiration date to select when the account should be disabled or deleted.</p> <div> The account is accessible until the beginning of the day on which it is set to be disabled. For example, if an account is set to be disabled on 25 December 2019, the user can log in until 24 December 2019, 23:59.</div>
Default Web Client	<p>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, you can also specify a default client. If you change this option, 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.</p>
Email Address	<p>The Email Address is used when Web Client password recovery requires an email address to send a recovered password to a user. If you have the MFT edition of Serv-U, this is also used by Events.</p>
Enable Account	<p>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.</p>
Description	<p>Enter an optional description for this user. This description is only visible to administrators.</p>
Full Name	<p>The full name of the account user. It is not used by clients when they log in.</p>

## Home Directory

Enter or navigate to the home directory for this user. This is where the user is placed immediately after logging in to the file server. This must be specified using a full path including the drive letter or the UNC share name.

When you specify the home directory, you can use the %USER% macro 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 it is combined with a directory access rule for %HOME%, a new user can be configured with a unique home directory and the appropriate access rights to that location with a minimal amount of effort.

You can also use the %DOMAIN\_HOME% macro 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 to access all system drives. In order for this to work properly, the user must not be locked in their home directory.

## SSH Keys

If you have the MFT edition of Serv-U, you can specify a SSH public key to be used to authenticate a user when logging in to the Serv-U File Server.

For information on SSH public key authentication, adding a SSH key pair, and creating an key pair for testing, see [New SSH Key Pair Creation](#).

## Lock user in home directory

Users 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 because Serv-U always reports it as "/" (root). The value of this attribute can be inherited through group membership.

Always Allow Login	<p>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. 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.</p> <p>Enabling the Always Allow Login option does not override <a href="#">IP access rules</a>. If both options are defined, the IP access rules prevail.</p>
User must change password at next login	<p>If you want the user to create their own password when they next log in, check this box.</p>
Availability	<p>Click Availability if you want to place limits on when this user can log in.</p> <p>Check Apply limit and select the start and end time to specify the period this user may log in.</p> <p>Tick the checkboxes for the days of the week on which this user may log in.</p>
Welcome Message	<p>Click Welcome Message if you want to send a welcome message to this user when they log in. 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 through SFTP over SSH2, because SSH2 does not define a method for sending general text information to users.</p> <p>Check Include if you want to include the response code in the welcome message test when an FTP connection is made.</p> <p>Either select or navigate to a message file if you have already created a text file containing a welcome message or check the Override box, and enter a message specific to this user in the text box above it.</p>

## User Properties: Directory Access

Directory access rules define which areas of the system are accessible to user accounts. Directory access rules specified at the server level are inherited by all users of the file server. If they are specified at the domain level, they are only inherited by users who belong to the particular domain. The traditional rules of inheritance apply where rules specified at a lower level (for example, the user level) override conflicting or duplicate rules specified at a higher level (for example, the server level).

When you set the directory access path, you can use the `%USER%`, `%HOME%`, `%USER_FULL_NAME%`, and `%DOMAIN_HOME%` variables to simplify the process.

**i** For example, use `%HOME%/ftpboot/` to create a directory access rule that specifies the `ftpboot` folder in the home directory of the user.

Directory access rules specified in this manner are portable if the actual home directory changes while maintaining the same subdirectory structure. This leads to less maintenance for the file server administrator. If you specify the `%USER%` variable 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. You can use the `%USER_FULL_NAME%` variable 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:\ftpboot\%USER_FULL_NAME%` for `D:\ftpboot\Tom Smith`. You can also use the `%DOMAIN_HOME%` macro 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 listed. The first rule in the list that matches the path of a client's request is the one 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 particular subdirectory. Use the arrows on the right of the directory access list to rearrange the order in which the rules are applied.

**i** Serv-U File Server allows to list and open the parent directory of the directory the user is granted access to, even if no explicit access rules are defined for the parent directory. However, the parent directory accessed this way will only display the content to which the user has access.

## Permissions

### File Permission

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

**File Permission**

Append	Allows users to append data to existing files. This permission is typically used to enable users to resume transferring partially uploaded files.
Rename	Allows users to rename files.
Delete	Allows users to delete files.
Execute	Allows users to remotely execute files. The execute access is meant for remotely starting programs and usually applies to specific files. This is a powerful permission and great care should be used in granting it to users. Users with Write and Execute permissions can install any program on the system.

**Directory Permission**

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.
Create	Allows users to create new directories within the directory.
Rename	Allows users to rename directories within the directory.
Remove	Allows users to delete existing directories within the directory.  If the directory contains files, the user also must have the Delete files permission to remove the directory.

**Subdirectory Permission**

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 (for example, when implementing mandatory access control), clear the Inherit check box and grant permissions specifically by folder.
---------	--


## 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 would result in the directory content 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.

## Advanced: Access as Windows user (Windows only)

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 File Server, you can configure the SolarWinds Serv-U File Server service to run under a network account. The alternative, preferred where many servers exist, or if the SolarWinds Serv-U File Server service has to run under Local System for security reasons, is to configure a directory access rule to use a specific Windows user for file access. Click Advanced to specify a specific Windows user for each directory access rule. As in Windows authentication, directory access is subject to NTFS permissions, and in this case also to the configured permissions in Serv-U File Server.

 When you use Windows authentication, the NTFS permissions of the Windows user take priority over the directory access rules. This means that when a Windows user tries to access a folder, the security permissions of the user are applied instead of the credentials specified in the directory access rule.

## Examples

### Mandatory access control

You can use mandatory access control (MAC) 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.

In the following example, the rule applies to `C:\ftproot\`.





**Directory Access Rule**

Path: C:\ftproot\

Save Cancel Help Full Access Read Only Advanced >>

**Files**

- ☒ Read
- ☒ Write
- ☒ Append
- ☒ Rename
- ☒ Delete
- ☐ Execute 

**Directories**

- ☒ List
- ☒ Create
- ☒ Rename
- ☒ Remove

**Subdirectories**

☐ Inherit

Maximum size of directory contents: 0 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 SolarWinds Serv-U File Server.

## Restrict file types

If users are using storage space on the SolarWinds Serv-U File Server to store non-work-related files, such as .mp3 files, you can prevent this by configuring a directory access rule placed above the main directory access rule 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:

**Directory Access Rule**

Path: \*.mp3

**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)

Buttons: Save, Cancel, Help, Full Access, Read Only, Advanced >>

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 the directory to which they need access.

**Directory Access Rule**

Path: %HOME%

**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)

Buttons: Save, Cancel, Help, Full Access, Read Only, Advanced >>

In the second rule, enter the extension of the file that should be accessed, such as \*.mdb.




**Directory Access Rule**

Path: \*.mdb

**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)

Buttons: Save, Cancel, Help, Full Access, Read Only, Advanced >>

These rules only allow users to access .mdb files within the specified directories. You can adapt these rules to any file extension or set of file extensions.

Directory Access		Virtual Paths	File Management
 Domain directory access rules are global rules that define the files and directories overridden at the group and user levels.			
Path	Access		
*.mdb	RWADN-L---I		
%HOME%	-----L---I		

## User Properties: Virtual Paths

If virtual paths are specified, users can 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 access 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 all users of the file server. Virtual paths created at the domain level are only accessible by users belonging to that domain.

## 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, use a full path, such as `D:\inetpub\ftp\public`. You can also use a UNC path, such as `\\Server\share\public`. To make a virtual path visible to users, users must have a directory access rule specified for the physical path.

## Virtual path

The virtual path is the location 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. You can also use a full path without any macros.

### Include virtual paths in Maximum Directory Size calculations

When this option is selected, the virtual path is included in Maximum Directory Size calculations. The Maximum Directory Size limits the size of directories affecting how much data can be uploaded.

## Examples

### Virtual paths

A group of web developers have been granted access to the directory `D:\ftproot\example.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 group of web developers, add a virtual path to bring the directory to the users by specifying `D:\corpimages\` as the physical path and `D:\ftproot\example.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.

## Relative virtual paths

Continuing with the previous example, if the home directory of the group of web developers is relocated to another drive, both the home directory and the virtual path must be updated to reflect this change. You can avoid this 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\example.com\corpimages` as the virtual path, use `%HOME%\corpimages`. This way the corpimages virtual path is placed within the home directory of the group, regardless of what the home directory is. If the home directory changes at a later date, the virtual path still appears there.

## User Properties: Logging

In the Serv-U File Server, you can customize the logging of user and group events and activity to a great extent.

### Log Message Options

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 in the Logging to File Settings section is selected. You can configure the log 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 name	<p>Specify the name of the log file for information to be saved to a file. Click Browse to select an existing file or directory location for the log file.</p> <p>The log file path supports certain wildcard characters. Wildcard characters which refer to 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.</p> <table><tr><td>%H</td><td>The hour of the day (24-hour clock).</td></tr><tr><td>%D</td><td>The current day of the month.</td></tr><tr><td>%M</td><td>The name of the current month.</td></tr><tr><td>%N</td><td>The numeric value of the current month (1-12).</td></tr><tr><td>%Y</td><td>The 4-digit value of the current year (for example, 2019).</td></tr><tr><td>%X</td><td>The 2-digit value of the current year (for example, 15 for 2019).</td></tr><tr><td>%S</td><td>The name of the domain whose activity is being logged.</td></tr><tr><td>%G</td><td>The name of the group whose activity is being logged.</td></tr><tr><td>%L</td><td>The name of the login ID whose activity is being logged.</td></tr><tr><td>%U</td><td>The full name of the user whose activity is being logged.</td></tr></table>	%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, 2019).	%X	The 2-digit value of the current year (for example, 15 for 2019).	%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.
%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, 2019).																				
%X	The 2-digit value of the current year (for example, 15 for 2019).																				
%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 that you 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 area.																				
Automatically rotate log file	To ensure that log files remain a manageable size and can be easily referenced during auditing, you can automatically rotate the log file on a regular basis. By specifying a Log file path containing wildcards that reference the current date, Serv-U can rotate the log file and create a unique file name every hour, day, week, month, or year.																				

Keep up to 'n' log files  
Keep up to MB of log files

You can automatically purge old log files by setting a maximum number of files to keep, a maximum size limit in megabytes, or both. Setting these options to "0" means that 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 they 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
```

Do Not Log IPs


You can 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 log space and reduce overhead. Click Do Not Log IPs, and add IP addresses as appropriate.

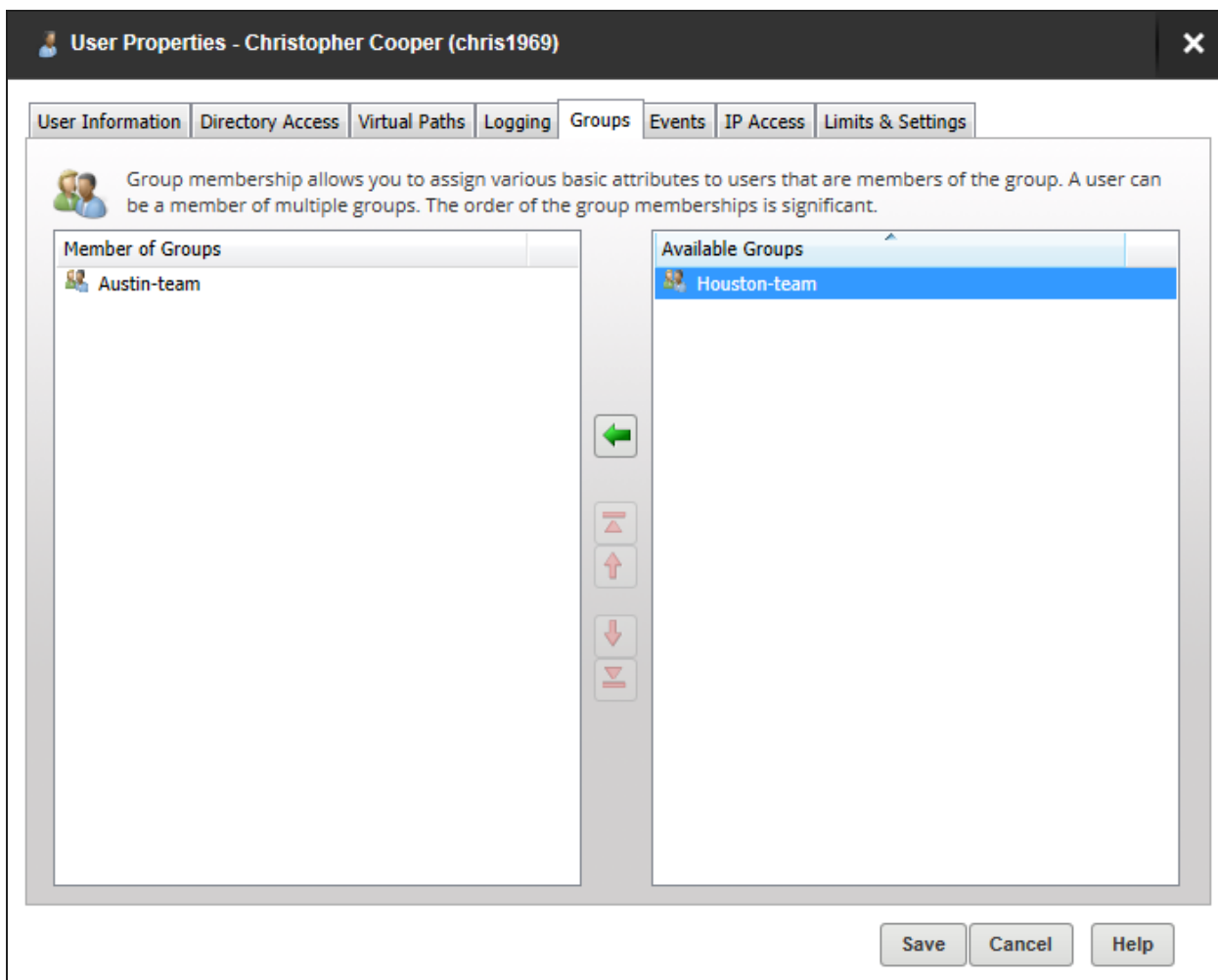
Download Log

Click to download the log file.

## Serv-U User Properties: Groups

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 [Groups](#).

 Because a user can be a member of multiple groups, the order in which group memberships are presented is important. If the highest group in the list does not contain a value for an attribute the value for next highest group is used.



- Use the up and down arrows on the right side of the Member of Groups list to arrange the order of group memberships.
- Use the left arrow buttons to add additional group memberships to the user, or use the right arrow buttons to remove the user from the selected groups.

These arrows are either "grayed out" or not displayed if the associated action is not applicable.

## User Properties: Events

With the MFT edition of the Serv-U File Server, you can automatically associate file server events with email notifications, balloon tip alerts or posts to the Windows Event Log or Microsoft Message Queue (MSMQ). For example, you might want to be notified in the event of a listener failure or whenever a new file is uploaded.

To access events for an individual user, select Users from the Global or Domain menu, click Edit, and select the Events tab from the User Properties window.



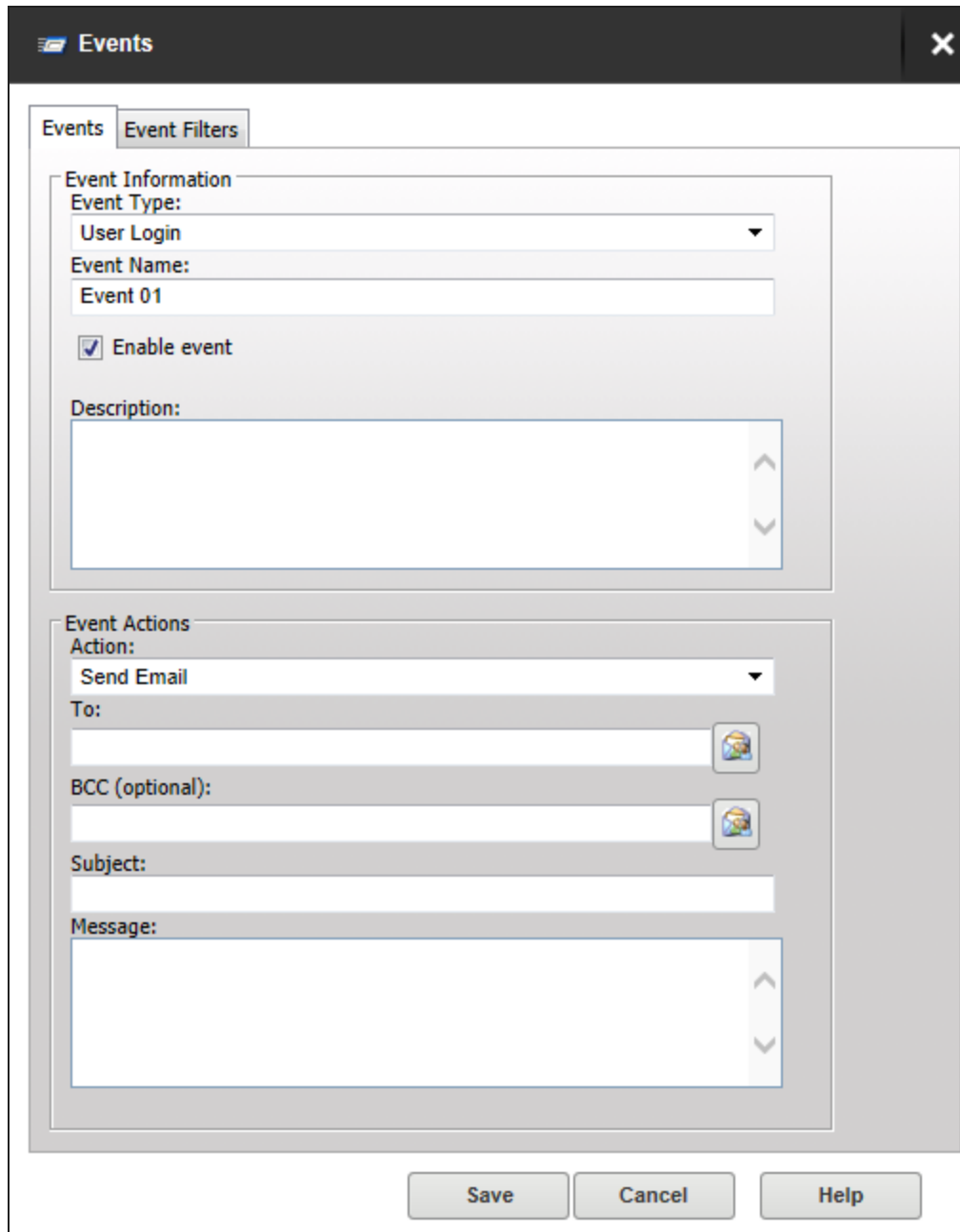
## Create Common Events

To instantly populate the events list with the most commonly used file server events:

1. Click Create Common Events.
2. Select the event action to apply to all common events.
3. Enter the email address to receive all notifications if you selected Send Email.
4. Enter the Message Queue Path if you selected Write to Microsoft Message Queue.
5. Click OK.
6. The 13 most common file server events are created. These can be customized by selecting an event and clicking Edit.

## Add an event

1. Click Add.



**Events** [X]

Events | Event Filters

**Event Information**

Event Type:  
User Login ▼

Event Name:  
Event 01

☒ Enable event

Description:

**Event Actions**

Action:  
Send Email ▼

To:


BCC (optional):

Subject:

Message:


Save Cancel Help

2. Select the Event Type.
3. Enter a name and description for this event.


 If you want to create but not immediately enable an event, uncheck the Enable event box.

4. Select the action to be triggered by this event, and complete the associated fields.

The actions that can be triggered are:

Event Action	Description
Send Email	<p>You can configure email actions to send emails to multiple recipients and to Serv-U File Server groups when an event is triggered.</p> <p>Enter the recipients in the To and BCC fields. Separate email addresses by commas or semicolons.</p> <p>To send emails to Serv-U groups, click the Group icon and drag the required groups from the Available Groups column to the Group Email List column.</p> <p>Enter the subject and message. You can use <a href="#">system variables</a> to include data specific to the event.</p>
Show Balloon Tip	<p>Balloon Tips are displayed in the system tray when an event is triggered. Balloon tip actions require a Balloon Title and Balloon Message. You can use <a href="#">system variables</a> to include data specific to the event.</p>
Execute Command (not available for Common Events)	<p>You can configure the execute of a file when an event is triggered. Execute command actions contain an Executable Path, Command Line Parameters, and a 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 zero to execute immediately.</p> <div>  Time spent waiting delays any processing that Serv-U File Server can perform.         </div> <p>A wait value should only be used to give an external program enough time to perform an operation, such as move a log file before it is deleted (for example, <code>\$LogFilePath</code> for the Log File Deleted event). You can use <a href="#">system variables</a> to use data specific to the event.</p>


Event Action	Description
Write to Windows Event Log (Windows only)	<p>By writing event messages to a local Windows Event Log, you can monitor and record Serv-U File Server activity using third-party network management software.</p> <p>The message entered into the Log Information field is 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. <a href="#">System variables</a> are supported for this field. This field can be left blank, but usually is not.</p>

Event Action	Description
Write to Microsoft Message Queue (MSMQ) (Windows only)	<p>Microsoft Message Queuing (MSMQ) is an enterprise technology that provides a method for independent applications to communicate quickly and reliably. Serv-U File Server can send messages to new or existing MSMQ queues whenever an event is triggered. 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 occurred.</p> <div data-bbox="786 625 1468 999"> <p> Microsoft message queues created in Windows do not grant access to SYSTEM by default, preventing Serv-U File Server from writing events to the queue. 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 File Server runs) has permission to the queue.</p> </div>

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. Public queues on the local machine can be addressed when a full path is not specified (for example, `.\Serv-U Message Queue` or `Serv-U Message Queue`). If the specified queue does not exist, Serv-U File Server attempts to create it. This normally only works on public queues on the local machine. You can also use Serv-U File Server system variables 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 File Server system variables can also be used in this field. This field may be left blank, but usually is not.

 Only the email action is available to users other than Serv-U File Server server administrators.

## Edit an Event

1. Select the event you want to edit and click Edit.
2. Edit the event details and the event filters as required.
3. Click Save.

## Add an Event filter

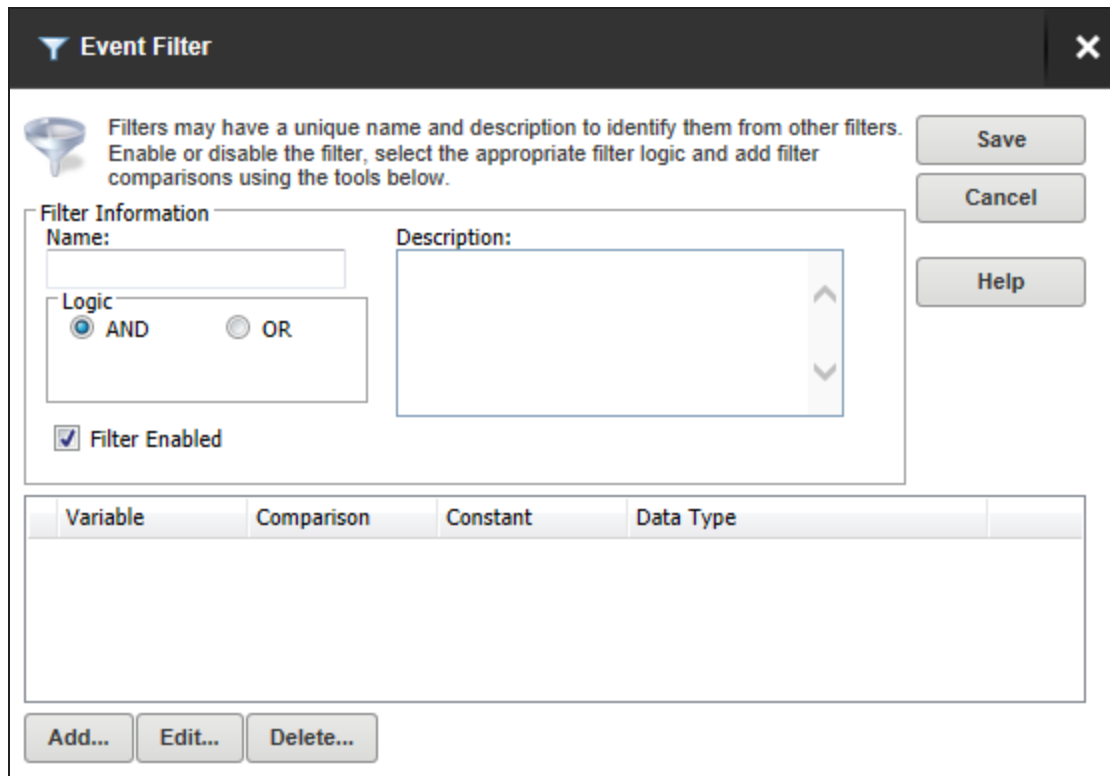
Event filters allow you to control when a Serv-U File Server event action is triggered. By default, event actions are triggered each time the event occurs. Event filters allow events to be triggered only if certain conditions are met.

For example, a standard event may trigger an email each time a file is uploaded to the server. However, by using an event filter, events can be triggered on a more targeted basis, such as configuring a File Uploaded event to send an email only if the file name contains the string `important`. Thus an email would be sent when the file `Important Tax Forms.pdf` is uploaded but not for other files.

Additionally, you could configure a File Upload Failed event to run only when the FTP protocol is used, not triggering for failed HTTP or SFTP uploads. You can do this by controlling the variables and values related to the event and by evaluating their results when the event is triggered.

To add an event filter to an event:

1. Click the Events Filters tab.
2. Click Add.



**Event Filter**

Filters may have a unique name and description to identify them from other filters. Enable or disable the filter, select the appropriate filter logic and add filter comparisons using the tools below.

**Filter Information**

Name:

Description:

Logic

☒ AND ☐ OR

☒ Filter Enabled

Save Cancel Help

Variable	Comparison	Constant	Data Type

Add... Edit... Delete...

3. Enter the following filter information:

Name	The name of the filter, used to identify the filter for the event.
------	--

Description (Optional)	The description of the event, which may be included for reference.
---------------------------	--

Logic	This determines how the filter interacts with any other filter set up for an event. In most cases, AND is used, and 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).
-------	--

4. Click Add to open the File Comparison window.
5. Select the [System Variable](#) to be used in the comparison.
6. Select the comparison method.

7. Enter the value the system variable is to be compared to. The following wild cards can be used.

- \* The asterisk wildcard matches any text string of any length. For example:
  - An event filter that compares the `$FileName` variable to the string `data*` matches files named `data`, `data7`, `data77`, `data.txt`, `data7.txt`, and `data77.txt`.
- ? The question mark wildcard matches any one character, but only one character. For example:
  - An event filter that compares the `$FileName` variable to the string `data?` matches a file named `data7` but not `data`, `data77`, `data.txt`, `data7.txt`, or `data77.txt`.
  - An event filter that compares the `$FileName` variable to the string `data?.*` matches files named `data7` and `data7.txt` but not `data`, `data77`, `data.txt`, or `data77.txt`.
  - An event filter that compares the `$Name` variable to the string `A????` matches any five-character user name that starts with `A`.
- [ ] The bracket wildcard matches a character against the set of characters inside the brackets. For example:
  - An event filter that compares the `$FileName` variable to the string `data[687].txt` matches files named `data6.txt`, `data7.txt` and `data8.txt` but not `data5.txt`.
  - An event filter that compares the `$LocalPathName` variable to the string `[CD]:\*` matches any file or folder on the `C:` or `D:` drives.

You can use multiple wildcards in each filter. For example:

- An event filter that compares the `$FileName` variable to the string `[cC]:\*.???` matches any file on the `C:` drive that ends in a three letter file extension.
- An event filter that compares the `$FileName` variable to the string `?:\*Red[678]\?????.*` matches 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.


8. Select the data type.


9. And another filter for this event or click Save to close.

## Filter examples

**Example 1.** An administrator may want to raise an email event when the file `HourlyUpdate.csv` is uploaded to the server, but not when other files are uploaded. To do this, create a new event 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 below:



 **Filter Comparison** ✕

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

If  = (is equal to)

Data Type:


Save


Cancel

Help

**Example 2.** It may be necessary to know when a file transfer fails for a specific user account. To perform this task, create a new File Upload Failed event, and add a new filter.

The filter comparison is the `$Name` variable, and the value to compare is the user name, such as `ProductionLineFTP`:

 **Filter Comparison** ✕

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

If  = (is equal to)


Data Type:


Save

Cancel

Help

**Example 3, using wildcards.** You can also filter for events based on specific folders using wildcards. 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, create a new File Uploaded event in the Domain Details > Events menu, and set it to Send Email. Enter the email recipients, subject line, and message content, and then open the Event Filters page. 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\`.

 **Filter Comparison** ✕

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

If  = (is equal to)

Data Type:

Save

Cancel

Help

## User Properties: IP Access

The IP Access tab shows the IP access rules set up for the server, domain, group or individual user, and allows you to add, import, edit, export and delete these rules.

Rules set at the user level apply to that user only.

IP access rules enable you to specify IP addresses, or ranges of IP addresses to which access is allowed or denied. These rules are applied as soon as a physical connection is established. Rules are applied in the order 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. Use the arrows on the right side of the list to change the position of an individual rule in the list.

### Display the IP access list

1. Navigate to Global or select the appropriate domain, click Users, select the user, and click Edit.
2. Click the IP Access tab.

The list of IP addresses set up at this level is displayed.

Use the arrows on the right side of the list to change the position of an individual rule in the list.

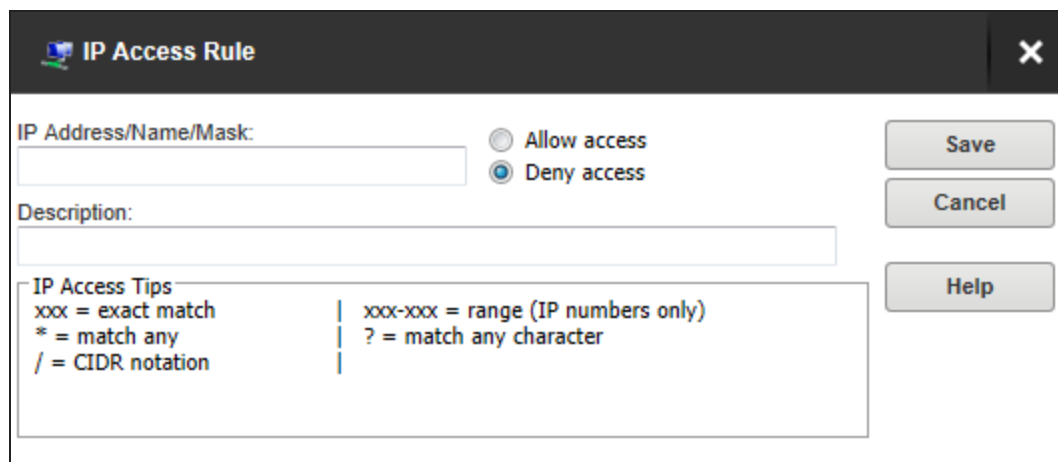
Check the Enable sort mode box to sort the IP access list numerically rather than in the processing order. Displaying the IP access list in sort mode does not change the order in which rules are processed. To view rule precedence, disable this option.



Viewing the IP access list in numerical order can be useful when you review long lists of access rules to determine if an entry already exists.

### Add an IP access rule

1. From the IP tab, click Add.  
The IP Access Rule window is displayed.



**IP Access Rule**

IP Address/Name/Mask:

☐ Allow access  
☒ Deny access

Description:

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

Save Cancel Help

- Enter the IP Address, name or mask using the following conventions.

Value or wildcard	Explanation
xxx	Stands for an exact match, such as 192.0.2.0 (IPv4), fe80:0:0:0:a450:9a2e:ff9d:a915 (IPv6, long form) or fe80::a450:9a2e:ff9d:a915 (IPv6, shorthand).
xxx-xxx	Stands for a range of IP addresses, such as 192.0.2.0-19 (IPv4), fe80:0:0:0:a450:9a2e:ff9d:a915-a9aa (IPv6, long form), or fe80::a450:9a2e:ff9d:a915-a9aa (IPv6, shorthand).
*	Stands for any valid IP address value, such as 192.0.2.*, which is analogous to 192.0.2.0-255, or fe80::a450:9a2e:ff9d:*, which is analogous to fe80::a450:9a2e:ff9d:0-ffff.
?	Stands for any valid character when specifying a reverse DNS name, such as server?.example.com.
/	Specifies 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.

- Enter a description.
- Select Allow or Deny access.
- Click Save.

## Edit an IP access rule

1. From the IP tab, click Edit.
2. Amend the rule information as required..
3. Click Save.

## Delete an IP access rule

1. From the IP tab, select the IP rule or rules to delete.
2. Click Delete and confirm.

## Import and export global IP address rules

You can speed up the creation of IP address rules by creating a text file of addresses, descriptions and access permissions.

1. Create a text file using Notepad or similar text editor.
2. On the first line enter "IP","Description","Allow".
3. Enter the details of each IP access rule:

IP	The IP address, IP range, CIDR block, or domain name for which the rule applies.
Description	A text description of the rule for reference purposes.
Allow	Set this value to 0 for Deny, or 1 for Allow.

For example:

```
"IP", "Description", "Allow"
"172.16.0.1", "Flange Software", "1"
"172.16.0.*", "Do not allow", "0"
"2001:db8::/32", "New test site", "1"
```

4. From the IP tab, click Import.
5. Navigate to the file you created, and click Select.

Similarly, the list of existing IP address rules can be exported to a text file by clicking Export.

For examples of IP address rules and IP address caveats see [Examples of IP address rules and caveats](#).


## Serv-U user properties: limits & settings

There are many options to customize how Serv-U can be used, and these can be set at the user, group, domain, and server level.

- For the Server Limits page, click [here](#).
- For the Domain Limits page, click [here](#).
- For the Group Properties: Limits page, click [here](#).

The limits stack intelligently, so user settings override group settings, group settings override domain settings, and domain settings override server settings. In addition, you can configure limits so they only apply during certain days of the week, and certain times of the day.

Select the Limits & Settings tab from the User Properties window.

 Most limits and settings on this tab are self-explanatory. However, the "Allow users to change password" setting in the Password limit types is overridden by the "User must change password at next login" option if set to No.

Default limits are displayed against a blue background. These cannot be edited or deleted, but can be overridden by adding a new limit.


### Override a default limit

1. Select the Limit Type containing the limit to override.
2. Click Add.
3. Select the limit to add.
4. Enter the value for the limit.
5. Click Advanced to specify a day and time to which this limit applies.
6. Check the Apply limit only at this time of day if you want to specify a time period for which this limit is in force, and select the Start and End Times.
7. Select the Days of the Week for which this limit applies.
8. Click Save.

The new limit is displayed in the list. (The default is still displayed, even though it is overridden.)

## Edit a limit

1. Select a non-default limit, and click Edit.

 If you try to edit a default limit a message is displayed informing you that default limits cannot be edited and asking if you want to create a new limit to override it.

2. Amend the value as required.
3. If you want to change the day and time to which this limit applies, click Advanced.
4. Click Save.

## Ratios & Quotas

The User Limits and Settings page has two additional buttons, enabling you to set up transfer ratios, quotas and "free" files for each individual user.

- [Ratios & Quotas](#)
- [Ratio Free Files](#)

## Common topics

### Access rule examples and caveats

#### Examples of IP address rules

<b>Office-only access</b>	A contractor has been hired to work in the office, and only in the office. Office workstations have IP addresses in the range of 192.0.2.0 - 192.0.2.24. The related Serv-U File Server <a href="#">access rule</a> should be Allow 192.0.2.0-24, and it should be added to either the user account of the contractor or a Contractors group that contains multiple contractors. No deny rule is required because Serv-U File Server provides an implicit Deny All rule at the end of the list.
<b>Prohibited computers</b>	Users should normally be able to access Serv-U File Server from anywhere, except from a bank of special internal computers in the IP address range of 192.0.2.0 - 192.0.2.24. The related Serv-U File Server access rules should be Deny 192.0.2.0-24, followed by Allow *.*.*.*, and these rules should be added to either the domain or the server IP access rules.
<b>DNS-based access control</b>	The only users allowed to access a Serv-U File Server domain connect from *.example.com or *.example1.com. The related Serv-U File Server access rules should be Allow *.example.com and Allow *.example1.com in any order, and these rules should be added to the domain IP access rules. No deny rule is required because Serv-U File Server provides an implicit Deny All rule at the end of the list.

#### Specific IP caveats

<b>Implicit deny all</b>	Until you add the first IP access rule, connections from any IP address are accepted. After you add an IP access rule, all connections that are not explicitly allowed are denied. This is also known as an implicit Deny All rule. Make sure you add a Wildcard Allow rule (such as Allow *.*.*.*) at the end of your IP access rule list.
<b>Matching all addresses</b>	Use the *.*.*.* mask to match any IPv4 address. Use the *.*.* mask to match any IPv6 address. If you use both IPv4 and IPv6 listeners, add Allow ranges for both IPv4 and IPv6 addresses.

## Specific IP caveats

<b>DNS lookup</b>	If you use a dynamic DNS service, you can specify a domain name instead of an IP address to allow access to users who do not have a static IP address. You can also specify reverse DNS names. If you create a rule based on a domain name or reverse DNS, Serv-U File Server performs either a reverse DNS lookup or DNS resolution to apply these rules. This can cause a slight delay during login, depending on the speed of the DNS server of the system.
<b>Rule use during connection</b>	The level at which you specify an IP access rule also defines how far a connection is allowed before it is 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.
<b>Anti-hammering</b>	<p>Specific IP addresses in Allow rules are not blocked by anti-hammering. These IP addresses are white-listed.</p> <p>Addresses matched by a wildcard or a range are subject to anti-hammering prevention.</p> <p>You can set up an anti-hammering policy that blocks clients who connect and fail to authenticate more than a specified number of times within a specified period of time. Anti-hammering policies are set up server-wide in <a href="#">Limits and Settings &gt; Settings</a>.</p> <p>IP addresses blocked by anti-hammering rules appear in the domain IP access rules with a value in the Expires in column. If you have multiple domains with different listeners, blocked IP addresses appear in the domain that contains the listener. Blocked IP addresses do not appear in the server IP access list, even if anti-hammering is configured at the server level.</p>

## SMTP configuration for the Serv-U File Server

Configure an SMTP connection to send email for events which are configured to use email actions.

You can configure SMTP on the server or domain level, or both. SMTP configuration at the domain level can be inherited from the server level.

The SMTP configuration dialog is located on the Events tab on the [Server Details](#) and [Domain Details](#) pages, and also in the [Domain Wizard](#).

1. Click Configure SMTP to launch the dialog.
2. Enter the SMTP server and port.



3. Check the checkbox to use SSL. This will also reveal additional checkboxes if you want to use a SSL Certificate and/or Explicit SSL.
4. Enter the email address and name you want to assign to the emails generated.
5. If your server requires authentication check the checkbox and supply the account name and password.

## Test the SMTP configuration

1. Click Send Test Email.
2. In the Send Test Email window, specify the email address where you want to send the test email to, and click Send. Optionally, you can edit the subject and content of the test message.
3. If the email was sent successfully, click OK on the confirmation window to save your SMTP configuration, or click No to return to the SMTP Configuration window.

If an error occurs at any stage of the configuration test, Serv-U File Server returns one of the following error messages in the SMTP error window:

Error message	Explanation
SMTP connection failed. Please check your SMTP server and port settings.	The most common reason for the SMTP connection to fail is an invalid SMTP server address or port number. Verify that these details are correct.
Unable to send message due to authorization error. Please check user name and password.	The connection to the server is successful, but the provided user name, password, or both is incorrect.  The error can also occur if incorrect server and port settings are specified, but the specified server is listening on the specified port.
Unable to send message due to recipient error. Please check that recipient email address is valid.	The connection to the server is successful, but the email address provided in the To Email Address field of the Send Test Email window is not valid.
Unable to send a message. Please try again later.	The connection to the server is successful, but an unspecified error occurred while sending the test email.
SMTP communication failed. Ensure that SMTP server settings are correct, and that the SMTP server is up and running.	An unspecified error occurred. Check your SMTP connection details, and try the test again.


Error message	Explanation
Timeout while contacting SMTP server.	Please check that the SMTP server address is correct.

## New SSH Key Pair creation

The MFT edition of Serv-U enables you to use SFTP over SSH2. The Secure Shell (SSH) protocol enables secure system administration and file transfers over insecure networks. SSH key pairs enable a client to connect to the server using the SFTP protocol. Two keys are generated by a SSH key generator:

- A private key, `<xxxxxxx>.key`, that is held on the client computer
- A public key `<xxxxxxx>.pub`, that is held on the server

Both keys are required for a connection to be valid.

 SSH key pair generation for users is provided by Serv-U for testing purposes only. Sharing private keys between more than one computer negates the security advantages of SSH Public Key Authentication. The SSH key pair should be generated on the client computer, and then the SSH public key should be sent to the server or server administrator.

## The SSH Public Key Path

The public keys should be located in secured directories on the server. You can then refer to this in Serv-U using the public key path. 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 of the domain, set in Domain Details > Settings, used if the keys are in a central folder relative to the domain home directory.

Examples:


```
%HOME%\SSHpublic.pub
```

```
%HOME%\%USER%.pub
```

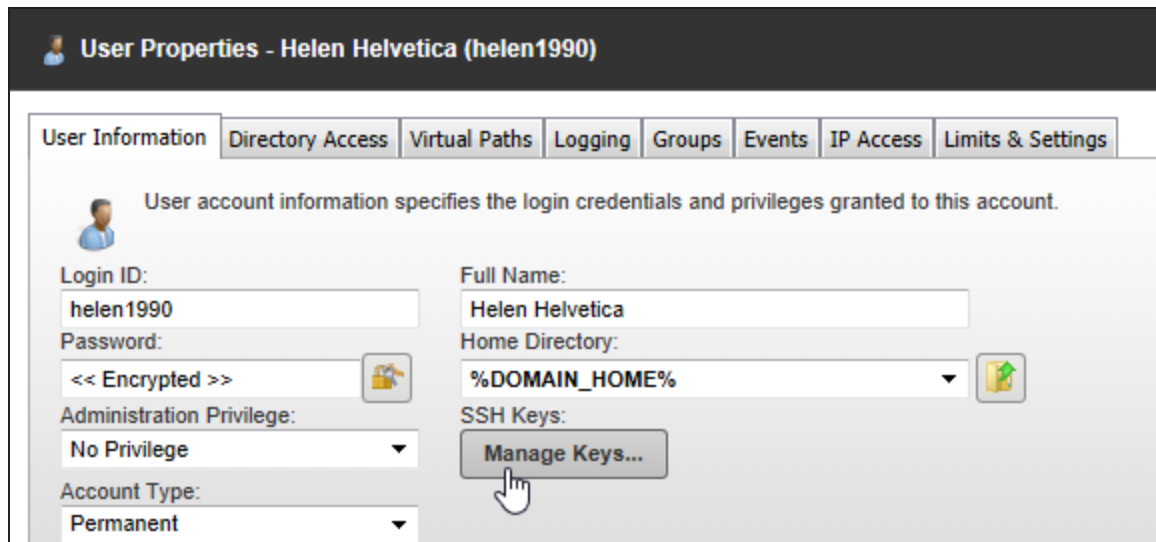
```
%DOMAIN_HOME%\SSHKeys\%USER%.pub
```

## Add a public key for a user or a group

1. A SSH key pair is created on the client computer using a utility such as PUTTYgen or openssh. You can use RSA or DSA keys and a key length of 1024, 2048 or 4096 bits in Serv-U.
2. The public key is sent to the server administrator, the private key retained by the user or group.

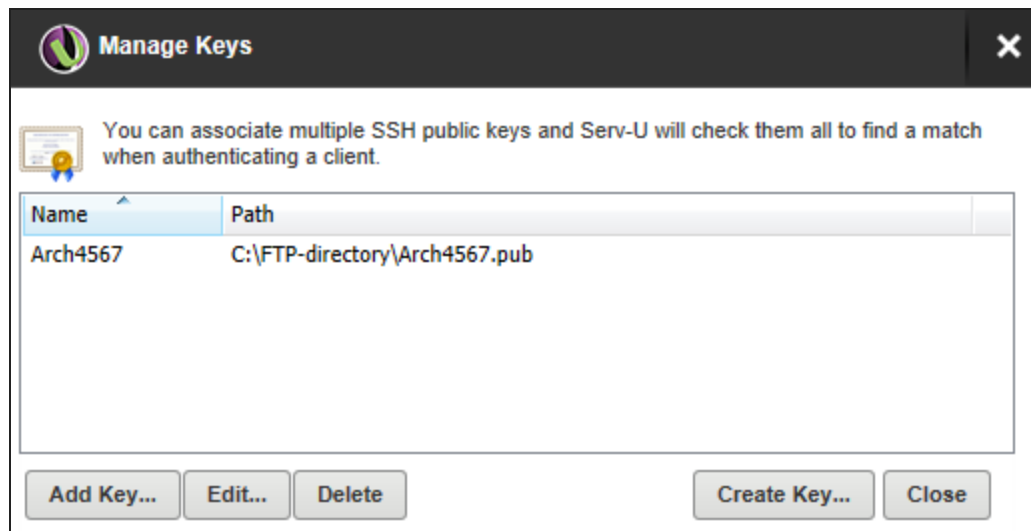
 Refer to the FTP client documentation for instructions on using the private key and SFTP.

3. Copy the public key to the appropriate directory on the server.
4. In Serv-U, navigate to the User Properties page for the client or the Group Properties page for a group.



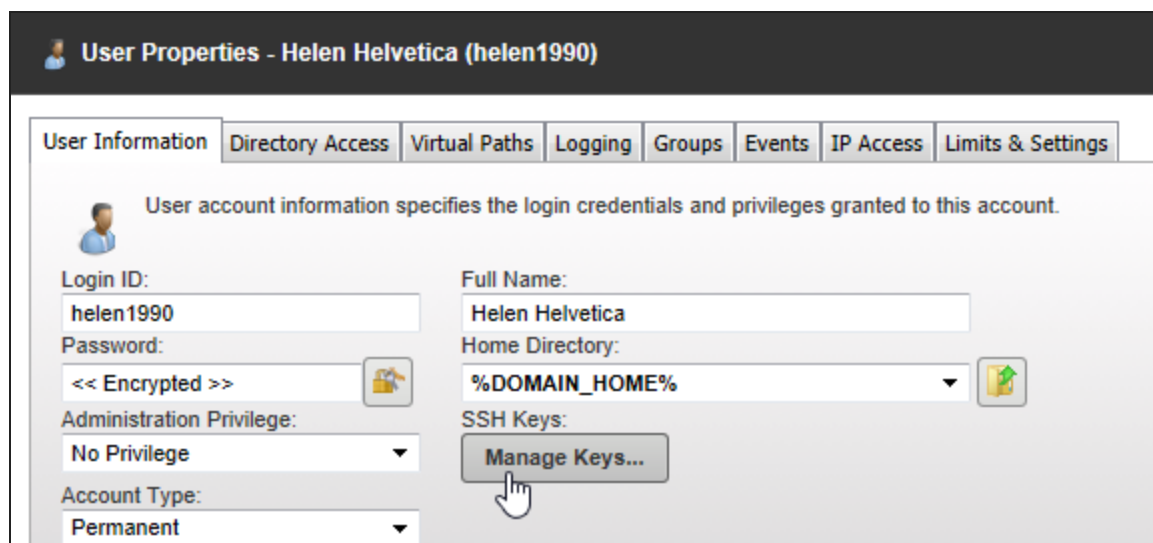
5. Click Manage Keys.
6. Click Add Key.
7. Enter a name to use for this key.
8. Enter or navigate to the directory where the public key is located and select it. See above for the macros that can be used in this path.
9. Click Save.

10. The public key is added for this user or group.



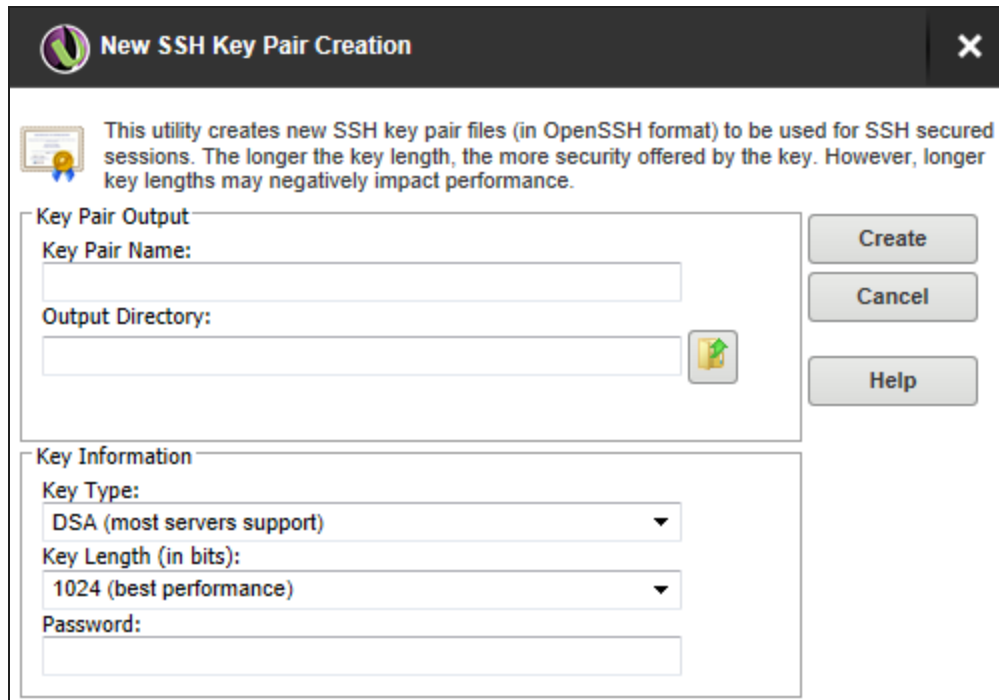
## Create a new SSH key pair for testing

1. In Serv-U, navigate to the User Properties or Group Properties page as appropriate.



2. Click Manage Keys.

3. Click Create Key.



The dialog box is titled "New SSH Key Pair Creation" and features a close button (X) in the top right corner. It contains a descriptive text block at the top, followed by two main sections: "Key Pair Output" and "Key Information". The "Key Pair Output" section includes input fields for "Key Pair Name:" and "Output Directory:", with a folder selection icon to the right of the latter. The "Key Information" section includes dropdown menus for "Key Type:" (set to "DSA (most servers support)") and "Key Length (in bits):" (set to "1024 (best performance)"), along with a "Password:" input field. On the right side of the dialog, there are three buttons: "Create", "Cancel", and "Help".

**New SSH Key Pair Creation**

This utility creates new SSH key pair files (in OpenSSH format) to be used for SSH secured sessions. The longer the key length, the more security offered by the key. However, longer key lengths may negatively impact performance.

**Key Pair Output**

Key Pair Name:

Output Directory:

**Key Information**

Key Type:  
DSA (most servers support)

Key Length (in bits):  
1024 (best performance)

Password:

Create  
Cancel  
Help

4. Type the name of the key pair (for example, MyKey), which is also used to name the storage file.
5. select an output directory of the certificate (for example, C:\ProgramData\SolarWinds\Serv-U\).
6. Select the key type (default of DSA is preferred, but RSA is available).
7. Select the key length (default of 1024 bits provides best performance, 2048 bits is a good median, and 4096 bits provides best security).
8. Enter the password to use for securing the key file.
9. Click Create.


## Create multiple keys

For the purposes of public key authentication, you can associate multiple public keys with a user or group 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 checks all the keys you provide here. If authenticating against one key fails, Serv-U proceeds to check the next key.


 For optimal results, the following best practices are recommended:

- It is recommended that you do not create more than 100 keys per user account.
- If you have a large number of public keys, divide the keys between multiple users, and define the common user properties at group level.
- Avoid storing the public keys in a network path.

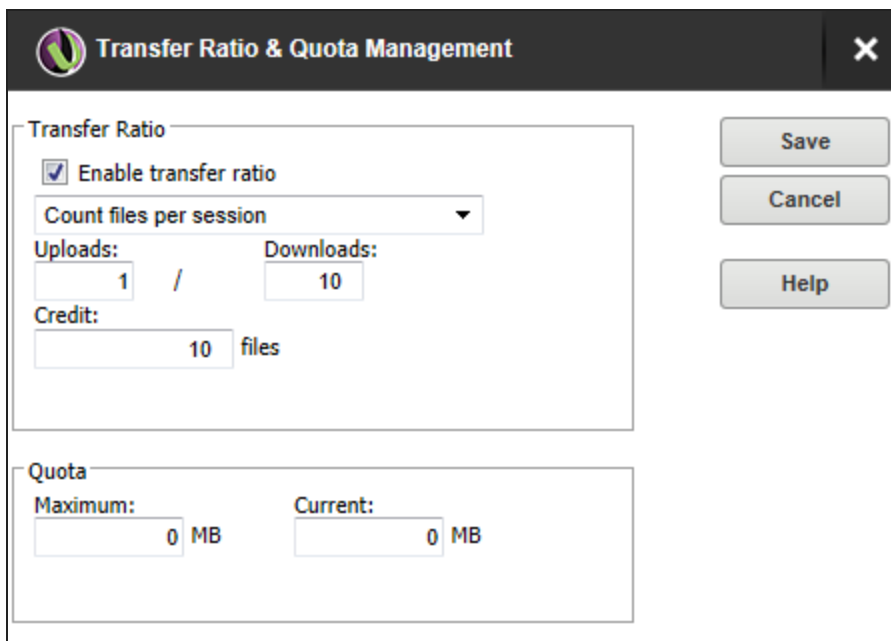
## Transfer Ratio, Quota Management, and Ratio free files

The Limits & Settings tab provides access to three methods for managing the amount of data transferred by your users

- [Transfer Ratio](#)
- [Quota](#)
- [Ratio Free files](#)

 Transfer ratio and quota can only be set for individual users.

### Transfer Ratio



**Transfer Ratio & Quota Management**

☒ Enable transfer ratio

Count files per session

Uploads: 1 / Downloads: 10

Credit: 10 files

Quota

Maximum: 0 MB Current: 0 MB

Save Cancel Help

Transfer ratios are a convenient way of encouraging file sharing by your users.

By specifying an appropriate transfer ratio setting, you can grant credits to a user for uploading 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.


The ratio is configured by assigning a numeric value to both the uploads and downloads. For example, a 3:1 ratio that is counting files over all sessions means that the user account must upload three files in order to have the ability to download one 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.

### To create a ratio

1. On the User Properties - Limits & Settings tab, click Ratios & Quotas.
2. Check the Enable transfer ratio box.
3. Select the method to use. This can be:
  - Files per session
  - Bytes per session
  - Files over all sessions
  - Bytes over all sessions
4. Enter the upload to download ration. The default is 1 / 1.
5. If you want users to start off with a credit for a number of file, enter this value in the Credit field.

## Quotas

Quotas are another way to limit the amount of data transferred by user accounts. When a Maximum quota value is assigned to a user, they are not able to use more disk space than this. The Current field shows how much disk space is currently being used by this user account. When initially configuring a quota, both fields must be filled in. Serv-U tracks the file uploads and deletions made by the user and updates the current value as appropriate.

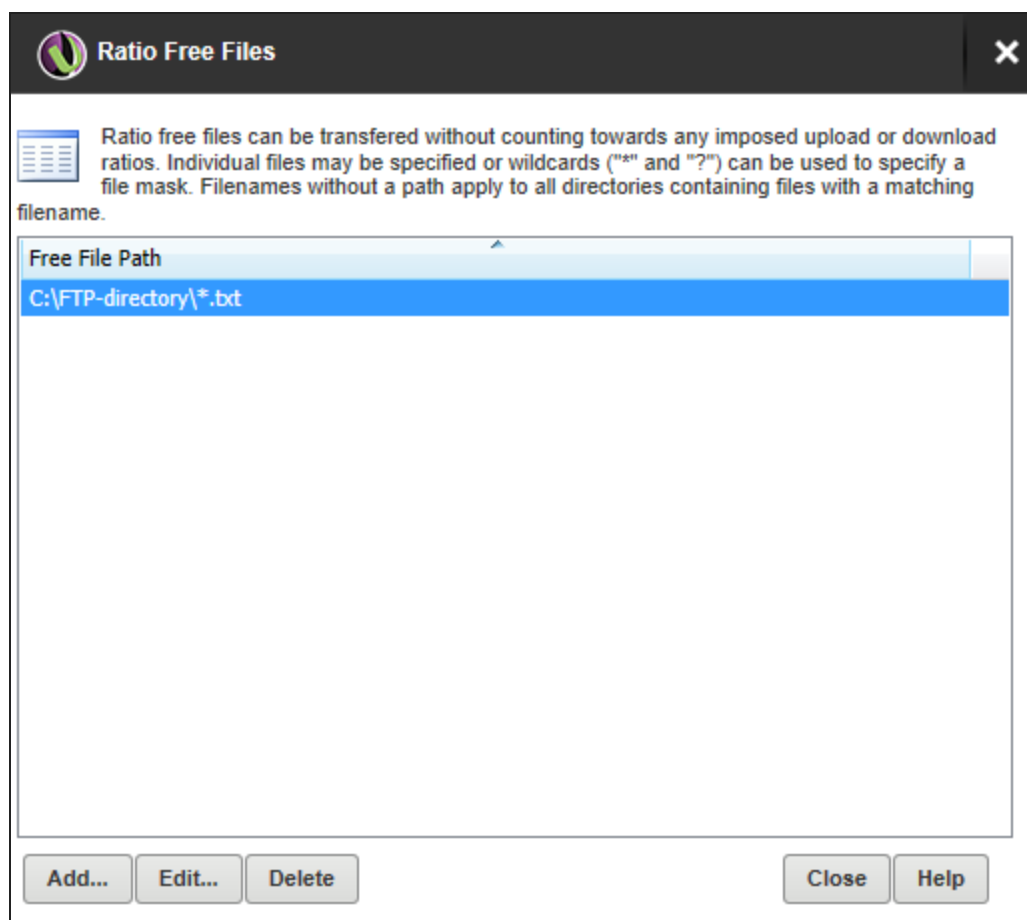
 A considerable drawback to using quotas is that in order for the current value to remain accurate, changes must not be made to the contents of the directories that are accessible by the user account outside of Serv-U. Because these changes take place outside of a file server connection, Serv-U cannot 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 users must upload files in order to earn credits towards downloading files, any file matching an entry in this list can always be downloaded by users, even if they have no current credits. This is commonly used to make files such as readme or directory information files always accessible.

To access the Ratio Free Files list by:

1. Navigate to the required User or Group.
2. Click Limits & Settings.
3. Click Ratio Free Files.



4. Add (or edit) a file by clicking Add (or Edit) and navigating to the appropriate directory.

You can use \* and ? wildcard characters when specifying a ratio free file.

- Use \* to specify any character or characters. For example, \*.txt means any file with a .txt extension is free for download.
- Use ? to represent a single character within the file name or directory. For example readme-?.txt.



You can specify full paths using standard directory paths such as `C:\ftproot\common\` (on Windows) or `/var/ftpfiles/shared/` (on Linux).

You can use full or relative paths when you are specifying an entry:

- If using a full path, only that specific file is exempt from transfer ratios.
- If using a relative path, the file is exempt from transfer ratios regardless of the directory in which it is located.

# Compare Windows Active Directory and LDAP authentication

Both Windows Active Directory and LDAP can be used to allow users to connect to Serv-U by using Active Directory credentials. Additionally, LDAP allows for authentication against other LDAP servers such as Apache Directory Server and OpenLDAP.

## Differences between Windows Active Directory and LDAP authentication

Windows and LDAP authentication are similar in many ways but there some important differences to help you decide which is right for your environment.

Use Windows authentication 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, see [Directory access rules](#).



Users with Serv-U installed on a Windows Server can also connect using Secure LDAP connections.

Use LDAP authentication 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, see [Directory access rules](#).

## Configure Windows and LDAP authentication

For information about configuring Windows authentication in Serv-U, refer to the following resources:

- [Windows authentication](#)
- [User groups](#)

- [Windows Groups and Organizational Units in Serv-U](#)
- [Enable Windows User NT-SAM - Active Directory Support in Serv-U](#)

## Configure Windows and LDAP authentication

For information about configuring LDAP authentication in Serv-U, refer to the following resources:

- [LDAP authentication](#)
- [User groups](#)
- [LDAP Authentication - error: Login was not successful](#)

## Keep Serv-U updated

If you work with LDAP or Windows authentication, it is highly recommended that you make sure your Serv-U installation is up to date. To ensure the best experience, upgrade to the latest version of Serv-U before configuring your advanced user authentication. For more information about the latest version of Serv-U, visit the release notes.

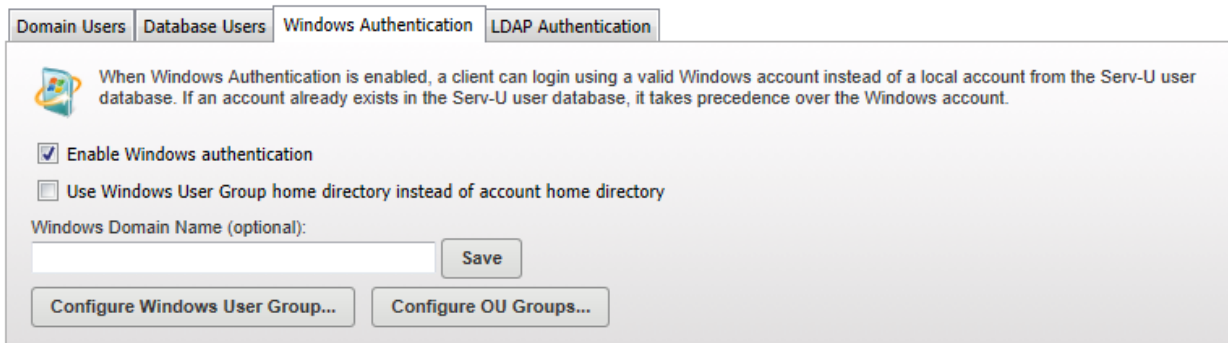
For upgrade, backup, and migration information, refer to the [Serv-U Installation and Upgrade Guide](#).

## Windows Authentication (MFT only)

By enabling Windows authentication, users can log in to Serv-U using their Windows login credentials 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:

1. Navigate to the required domain menu > Users.
2. Select the Windows Authentication tab.
3. Check the Enable Windows authentication checkbox.



To authenticate to Active Directory or to 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.

By default, Serv-U uses the Windows account's home directory when a client logs in using a Windows user account. Enabling the Use a Windows user group home directory instead of the account home directory 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.


## LDAP authentication (MFT only)

If LDAP authentication is enabled, users can log in to Serv-U using credentials 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.

### Before you begin

Before you begin the configuration of LDAP authentication:

- Check the logs of your LDAP server to identify the correct group membership.
- Log in to your LDAP server to verify the correct directory structure.
- Configure the default LDAP group in Serv-U. For information, see [Use LDAP user groups](#).

 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.

To help decide between whether you should use LDAP authentication or Windows authentication, see [Compare Windows and LDAP authentication](#).

The examples and illustrations in this topic show a Serv-U instance configured to use authentication through Active Directory.

To enable LDAP authentication:

1. Navigate to the required domain > Users.
2. Select the LDAP Authentication tab.

The screenshot shows the 'LDAP Authentication' tab in the SolarWinds Serv-U configuration interface. At the top, there are four tabs: 'Domain Users', 'Database Users', 'Windows Authentication', and 'LDAP Authentication'. Below the tabs, a text box explains: '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.' Below this, there are two checkboxes: 'Enable LDAP authentication' (checked) and 'Use LDAP Group home directory instead of the account home directory' (unchecked). A text field for 'LDAP Login ID Suffix:' is followed by a 'Save' button. Below this is a section titled 'LDAP Servers' containing a table with columns 'Host', 'Port', and 'Description'. The table lists one server: 'AUSCDC01.tul.solarwinds.net' on port '389'. To the right of the table are four buttons: 'Add...', 'Edit...', 'Delete', and 'Copy...'. At the bottom of the window are two buttons: 'Configure Default LDAP Group...' and 'Configure LDAP Groups...'.

Host	Port	Description
AUSCDC01.tul.solarwinds.net	389	

The current LDAP servers are listed.

## Configure an LDAP server

The LDAP Server configuration dialog is displayed when you click Add, Edit, or Copy on the LDAP Servers list.

LDAP Server

Users from this server will be able to log in to Serv-U using login credentials as provided by a remote LDAP server, such as Active Directory or OpenLDAP. LDAP User accounts are not visible or configurable on an individual basis in Serv-U. [More information...](#)

---

### Server Connection

☒ Enable this LDAP Server

☒ Use secure LDAP

Host

AUSCDC01.tul.solarwinds.net

Port

636

Connection Account

Connection Account Password

Description (Optional)

Detect & Test Connection

---

▲ Hide Advanced LDAP Options

### Filter Users

Base Distinguished Name (DN)

DC=tul,DC=solarwinds,DC=net

Search Filter

(&(objectclass=user)(userPrincipalName=\$LoginID))

---

### Attribute Mapping

Group Membership

memberOf

Home Directory

homeDirectory

Login ID (Optional)

userPrincipalName

Full Name (Optional)

name

Email Address (Optional)

mail

---

You can use the following form for testing LDAP user credentials from this server. (Optional)

Login ID

Password

Test Login

Cancel

Save

## 1. Provide the following information to configure your LDAP server:

Enable this 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.
Use Secure LDAP	Check to use Secure LDAP (LDAPS).
Host	The host name 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 usually be 389, or 636 for secure LDAPS.
Connection Account	The user name of the account that is used to connect to the LDAP server and execute queries against it. 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	<p>The password belonging to the account that is used to connect to the LDAP server and execute queries against the LDAP server.</p> <p>If the Connection Account credentials are not supplied, then the credentials that are being authenticated are used.</p>
Description	An optional field in which you can write more notes about your LDAP server.

## 2. If you need to configure any of the following settings, click Show Advanced LDAP Options.

Base Distinguished Name (DN)	<p>Use this field to provide the Base DN (or search DN) of the main node in your LDAP server. The Base DN determines the structure in your LDAP server where the search filter will be applied. 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 solar domain, this value can be DC=solar,DC=local.</p> <p>To determine the correct Base DN, hover over the main node of the LDAP server, and look for the highlighted information.</p>
------------------------------	---

## 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. The search filter is used to search in the Users tree of the LDAP server.

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 varies 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. This value is provided by default in Serv-U.

Consult with your local LDAP administrator or use an LDAP client (for example, Softterra LDAP Browser or Apache Directory Studio) to find and test the right value for your LDAP server before deploying into production, and then modify the default search filter according to your specific setup.

For example, if your LDAP server configuration contains subfolders, modify the search filter by adding a wildcard value (\*) to match the whole folder structure. The search filter must be configured in a way that it only returns one user.



To test your search filters against Active Directory, use the Ldp tool. The default location of the tool is C:\Windows\System32\ldp.exe. For more information about the location and usage of the Ldp tool, search for Ldp on the Microsoft Technet or on the Microsoft Support website.

## Group Membership

This field uses all the values found in the named LDAP attribute as additional LDAP Group membership assignments. For example, if this is configured as grp and an LDAP user record has both grp=Green and grp=Red attributes, Serv-U associates that LDAP User with both the "Red" and "Green" LDAP Groups. A typical value on Active Directory is memberOf.



Home Directory	This 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.
Login ID	This 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. In other words, this is your login ID in Serv-U, and it is compared to the userPrincipalName in the search filter.
Full Name	This 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".
Email Address	This 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".

## Specify the LDAP login ID suffix

After configuring the LDAP server, specify the LDAP login ID suffix. The LDAP login ID suffix is necessary to send fully qualified login IDs to the LDAP server. The suffix you specify here is placed at the end of the user name when a user logs in.

A typical value in an Active Directory environment might be @mydomain.com. After changing this field, click Save to apply the change.

## 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 Users > LDAP Authentication 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 [LDAP Groups](#).

## Use 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.

To configure the default LDAP group in Serv-U:

1. Navigate either to Users > LDAP Authentication, or Groups > LDAP Authentication.
2. Click Configure Default LDAP Group.

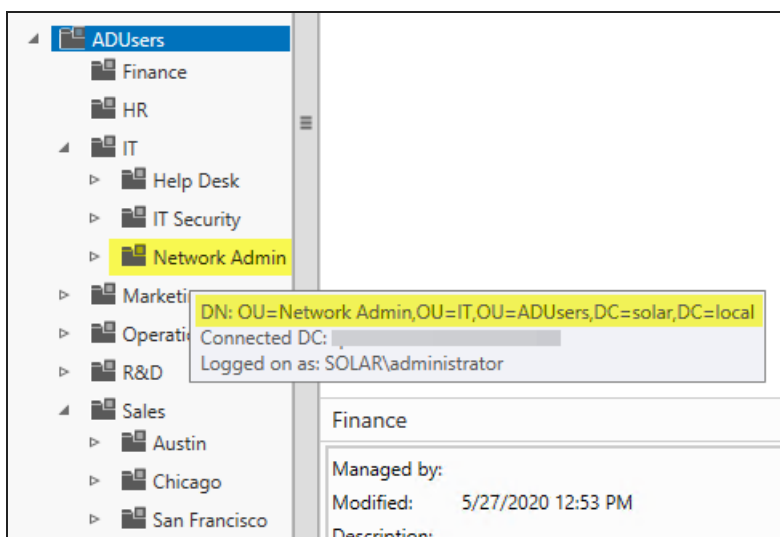
LDAP Users can also be members of individual LDAP Groups.

1. To configure LDAP groups in Serv-U:
2. Navigate to Users > LDAP Authentication.
3. Click Configure LDAP Groups.

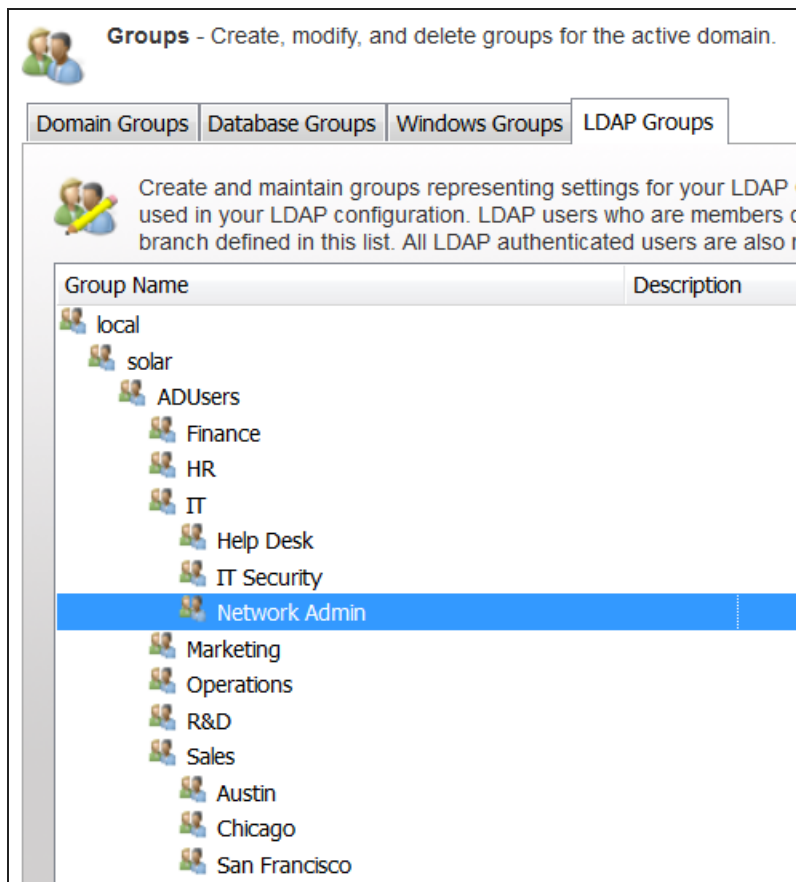
LDAP groups have the same configuration options as other Serv-U groups. For information about the configuration options available at the group level, see Groups.

When you configure LDAP groups, recreate the same structure as the group structure in Active Directory, and use the same names as the group names in Active Directory.

The following image illustrates the group structure in Active Directory. By hovering over a user or group in Active Directory, the group structure is displayed. This information is highlighted in yellow.



The following image illustrates how the group structure of Active Directory is recreated in Serv-U.



## Use a list of LDAP servers

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.


You can define more than one LDAP Server if you want Serv-U to try a backup server in case the primary LDAP server is down, or if you want to try LDAP credentials against different LDAP servers with different sets of users.

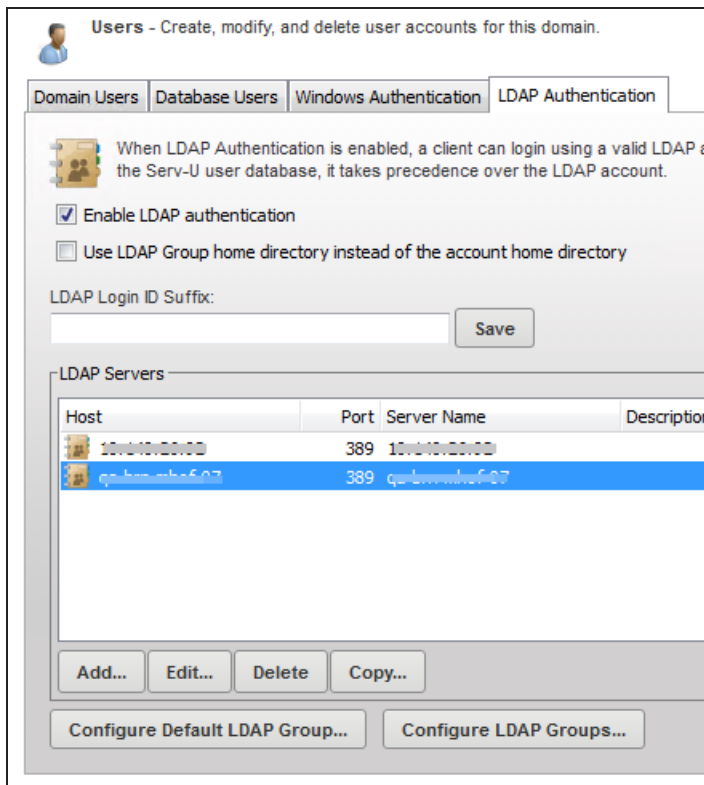
Serv-U attempts authentication against the list of LDAP servers from top to bottom. During login, the first LDAP server that approves a set of credentials will be the server from which the associated LDAP user will draw its full name, email address and other attributes.

After attempting a login against the first LDAP server, Serv-U tries 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, Serv-U makes login attempts on LDAP servers that are lower on the list if the preceding LDAP servers are unresponsive, or if they report that they have no knowledge of the LDAP user.

Serv-U tries each available LDAP server, even if the login credentials fail. The error log provides detailed information of any possible connection failure. For information about the error messages, see [LDAP error messages](#).

 The error log contains information about the last LDAP server Serv-U contacted.



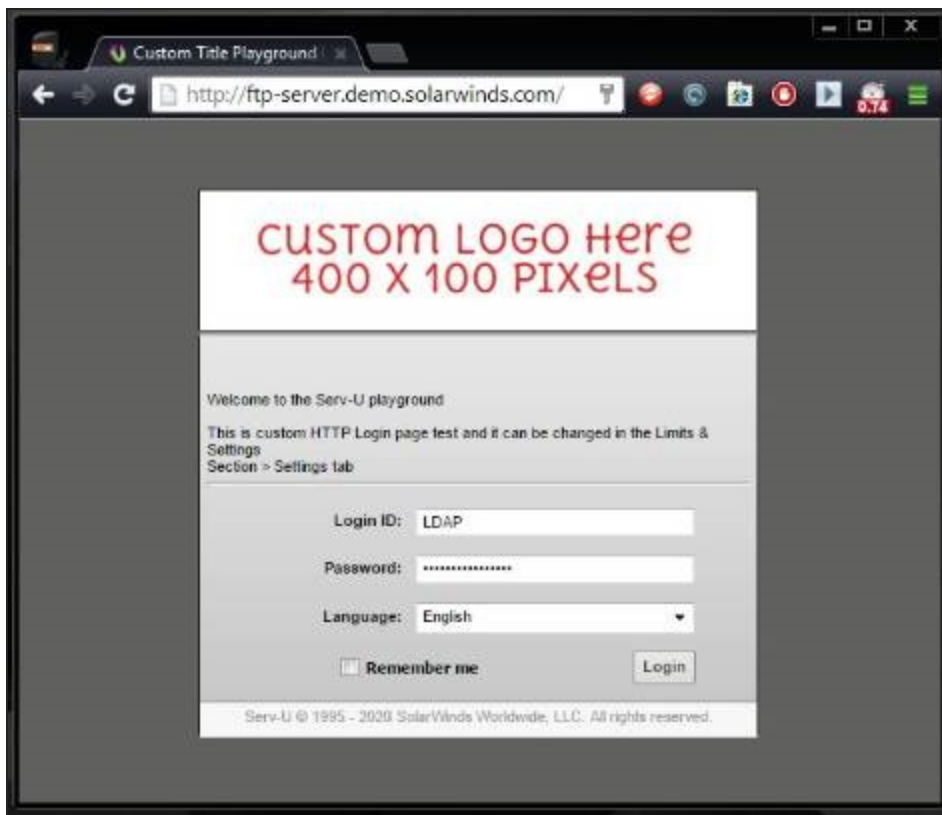
Use the Add, Edit, Delete, and Copy buttons to work with individual LDAP server entries. When there are multiple LDAP server entries in the list, selecting any entry will reveal move up, move down, move to top, and move to bottom ordering arrows on the right of the window.

## Test the connection to the LDAP server

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.

The following images show what a successful HTTP login looks like for the user and for the Serv-U administrator. Note that LDAP and Windows authentication looks identical in the log files.

The following image shows the login page for the user named LDAP.



The log entries for both a successful and a failed login are displayed under Domain > Domain Activity > Log.

The following image shows the log entries for a successful login and logout.

```
[02] Fri 31Oct14 16:03:53 - (000003) Connected to 10.XXX.X.XX (local address 10.XXX.X.XX, port 80)
[40] Fri 31Oct14 16:03:53 - (000003) HTTP_LOGIN: user: LDAP; domain: 10.XXX.X.XX
[02] Fri 31Oct14 16:03:53 - (000003) User "LDAP@lab.aus.example" logged in
[41] Fri 31Oct14 16:03:53 - (000003) HTTP_OKAY (200): SESS_OKAY
[40] Fri 31Oct14 16:03:57 - (000003) HTTP_LIST: path: "~/\"
[41] Fri 31Oct14 16:03:57 - (000003) HTTP_OKAY (200): okay
[40] Fri 31Oct14 16:04:05 - (000003) HTTP_LOGOUT
[41] Fri 31Oct14 16:04:05 - (000003) HTTP_OKAY (200): okay
[02] Fri 31Oct14 16:04:05 - (000003) User "LDAP@lab.aus.example" logged out
[02] Fri 31Oct14 16:04:05 - (000003) Closed session
```

## LDAP error messages

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). The search filter must be configured in a way that it only returns a single user account. For information about configuring the search filter, see <a href="#">above</a> .

#### Other error messages:

- 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".

Additionally, when Serv-U returns unknown LDAP authentication errors, search for the LDAP error codes in the documentation of your LDAP server.

## Enable LDAP authentication

To enable LDAP authentication:

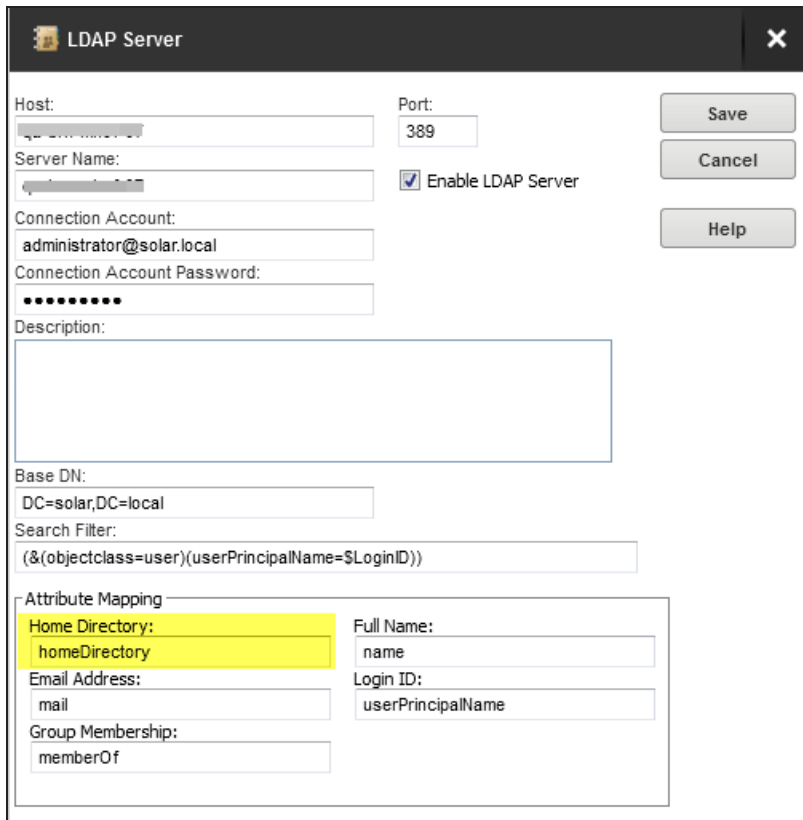
1. In the Serv-U Management Console, navigate to Users > LDAP Authentication.
2. Select Enable LDAP Authentication.

## User home folders

The home folders of LDAP users are pulled from the "Home Directory" LDAP attribute that is 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 the LDAP user group home directory instead of the account home directory

By default, Serv-U uses the LDAP account's home directory when an LDAP user logs in. This is the value of the Home Folder LDAP attribute that is specified in the LDAP server configuration, as highlighted in the following image.



The screenshot shows the 'LDAP Server' configuration window. The 'Home Directory' attribute is highlighted in yellow. The 'Full Name' attribute is set to 'name' and the 'Login ID' attribute is set to 'userPrincipalName'.

Attribute	Value
Home Directory:	homeDirectory
Full Name:	name
Login ID:	userPrincipalName
Email Address:	mail
Group Membership:	memberOf

For information about configuring the LDAP account's home directory, see [Configure the LDAP server](#) above.

If you select the Use LDAP Group home directory instead of account home directory option under Users > LDAP Authentication in the Serv-U Management Console, Serv-U will use the home directory that you specify in the Default LDAP User Group instead of the LDAP account's home directory.

The home directory of the Default LDAP User Group is specified on the Group Properties window of the Default LDAP User Group, as highlighted in the following image.

**Group Properties - Default LDAP User Group**

Group Information | **Directory Access** | Virtual Paths | Logging | Members | Events | IP Access | Limits & Settings

All group settings are applied to user accounts that are members of this group. To override a group setting for a specific user account.

Group Name: Default LDAP User Group

Administration Privilege: No Privilege

Default Web Client: Prompt user for client

Home Directory: /C:/Test Folder

SSH Keys: Manage Keys...

☒ Lock user in home directory

For information about configuring the Default LDAP User Group, see [Use LDAP user groups](#) above.

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.

## The interaction between domain home directories with Default LDAP User Group home directories

If a domain home directory is defined on the Domain Details > Settings page, this directory would be used by Serv-U as the default directory for LDAP authentication, resulting in errors.

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

Settings | Listeners | Virtual Hosts | IP Access | Database | Events

Make changes to the domain name and description, press the Save button to save the changes.

Domain Information

Name: www.example.com

Description: adfadf

☒ Enable domain

Save

Domain Home Directory

Domain Home Directory:

Maximum Size: MB (blank for no limit)

NOTE: Setting a maximum domain home directory size forces Serv-U to check the existing files and sub folders prior to and during uploads. This can be a very lengthy operation depending on the existing directory structure.

Save

To avoid possible issues in this case, make sure that you select the Use LDAP Group home directory instead of the account home directory option under Users > LDAP Authentication, and configure the LDAP group home directory as described in Use LDAP user groups.



## Domain User and Group Statistics

The User and 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 details.

### Session statistics

Data	Description
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 disconnecting.

Data	Description
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.

Data	Description
Shortest Login Duration Seconds	The shortest amount of time a session was logged in.

## Transfer statistics

Data	Description
Download Speed	The cumulative download bandwidth currently being used.
Upload Speed	The 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. 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 at the bottom of the page.

## Serv-U File Sharing

This section contains information about file sharing with the MFT edition of Serv-U. The information is organized into the following topics:

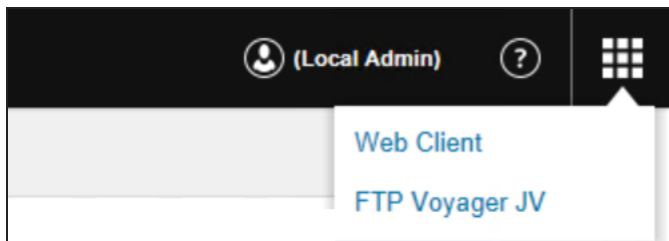
- [The Serv-U File Sharing console](#)
- [View all](#)
- [Share details](#)
- [The Send Files wizard](#)
- [The Request Files wizard](#)

File Sharing is available on MFT edition Serv-U servers where File Sharing has been [enabled](#) at the global or domain level. It can also be specified as the default web client at all levels.

### The Serv-U File Sharing console

Use the file sharing feature to send and receive files from guests.

To access File Sharing, click on File Sharing in the Serv-U tools menu. This option is only available in the MFT edition of Serv-U.



On the File Sharing web console you can search for, view, manage, and edit all incoming and outgoing file sharing requests. This dashboard is where all file sharing requests are initiated.

Common use case scenarios for File Sharing are the following:

- Send a file internally within your organization typically in the same network using a link in an email.
- Send a file outside of your organization and outside of your network using a link in an email.
- Receive a file from someone by sending a link to a page, where the other party can easily upload to it.
- Search for file shares or files among existing sent, requested, or both sent and requested shares using the search field.

Home **Request Files** **Send Files** Daily Activity 3 0 Jump to: **File Sharing**

**Requested Files** (Last 5 File Shares) Updated Friday, April 4, 2014 at 3:41:21 PM

Date Received	Subject	Sender(s)	Status	Size	# of Files	Expires	Download	Delete
Friday, April 4, 2014 3:13:24 PM	Serv-U File Sharing Link [expires Friday, April 11, 2014 12:00:00 AM]	Undisclosed recipients	Pending	0 KB	0	Friday, April 11, 2014		✗
Friday, April 4, 2014 3:12:30 PM	Serv-U File Sharing Link [expires Friday, April 11, 2014 12:00:00 AM]	Undisclosed recipients	Pending	0 KB	0	Friday, April 11, 2014		✗

[View All Requested >>](#) (2 Shares)

**Sent Files** (Last 5 File Shares) Updated Friday, April 4, 2014 at 3:34:30 PM [Refresh](#)

Date Sent	Subject	Recipient(s)	Status	Size	# of Files	Expires	Download	Delete
Tuesday, April 1, 2014 11:52:21 AM	Serv-U File Sharing Link [expires 8. april 2014 0:00:00 GMT+2]	Undisclosed recipients	Downloaded	77.75 KB	2	Tuesday, April 8, 2014	📄	✗

[View All Sent >>](#) (1 Shares)

💡 Refresh the list of all incoming and outgoing files by clicking [View All Requested](#) or [View All Sent](#).

## Serv-U file sharing: View All

Clicking View All Requested or View All Sent displays an overview of files sent or received, dates, recipients and when they expire.

**Requested Files** (Last 5 File Shares) Last updated 7/8/2013

Date Received	Subject
7/8/2013 04:20 PM	Serv-U File Share Link [expires 7/15/2013]

[View All Requested >>](#)

**Sent Files** (Last 5 File Shares) Last updated 7/8/2013 at 04:20 PM

Date Sent	Subject
7/8/2013 04:20 PM	Serv-U File Share Link [expires 7/15/2013]

[View All Sent >>](#)

Click Refresh if you do not see the file you are expecting to see.

To remove a file from the list, click Delete.

 The Expiration dates determine how long until the download link expires.

Deleting the only file in an outgoing share leaves nothing for the guest to download. You may want to delete the entire file share instead.

## Serv-U file sharing: the Send Files wizard

By using the File Share outgoing wizard, you can share files by entering the email addresses of your recipients. You can add a message, set your own expiration date, or type a password for security. Finally, you select the files you want to send and complete the share.

Serv-U saves the files and sends an email with web links to each of your recipients.


When your recipients receive their notifications, they click their links, enter any required passwords, and then download their files.

As each file is downloaded, Serv-U updates the information on your share, and may send you email receipts to tell you that your file was downloaded.



You can also create anonymous shares. In this case, you do not have to specify the recipients of the file share. When creating anonymous shares, only a link is generated, which you can then send out manually.

To send files to a guest user:


# 1. Enter the guest user email address.


**Send Files to Guest User: Add Details**(Step 1 of 2)

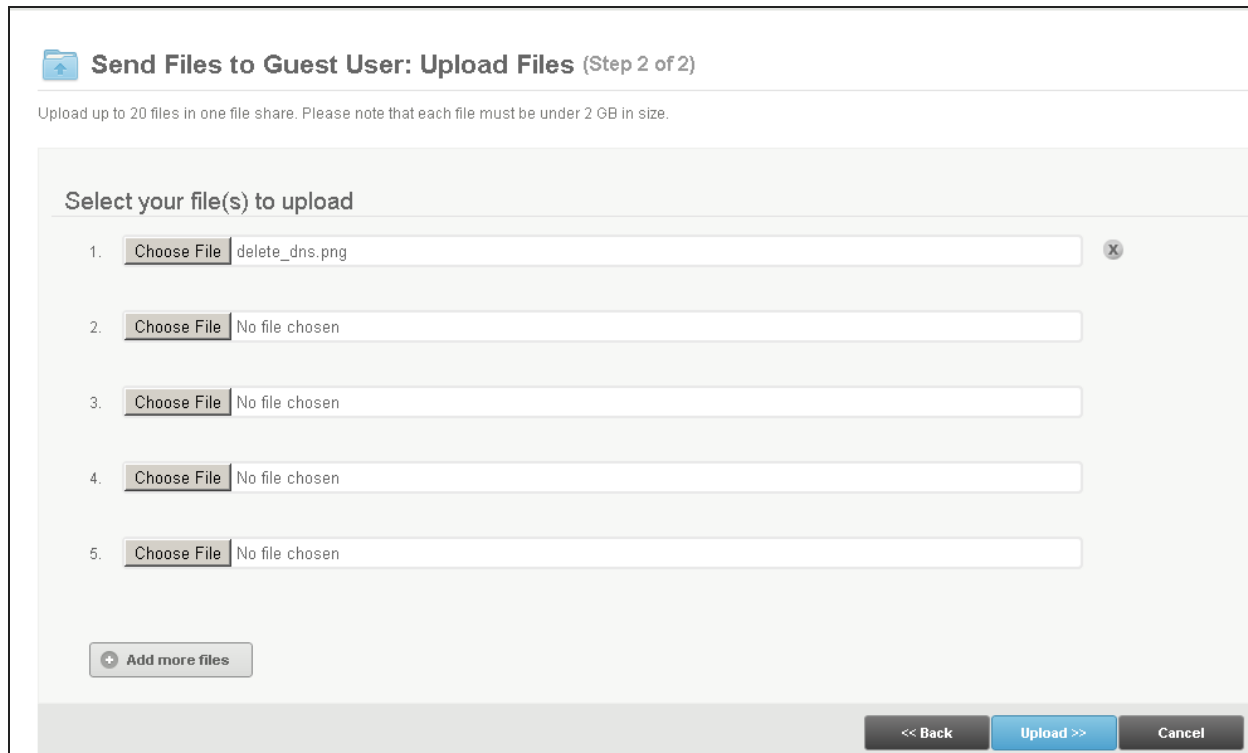
Enter email details and other information to be included with the uploaded file(s). Email will be sent to the guest user(s) with a link that grants them access to the uploaded file(s). For added security, set a custom or a system generated password, and specify a download link expiration time or date.

<b>Email Information</b> <p>Guest Email Address(es)</p> <input type="text"/> <p>Email Subject</p> <input type="text" value="Serv-U File Share Link [expires 02/02/2020 12:00:00 AM]"/> <p>Comments (optional)</p> <div style="border: 1px solid #ccc; height: 100px;"></div>	<b>Serv-U Access Link Expiration</b> <p>The link to download files should expire:</p> <p><input checked="" type="radio"/> on this specific date <input type="text" value="02/02/2020"/> </p> <p><input type="radio"/> in <input type="text" value="24"/> hours</p> <p><input type="radio"/> in <input type="text" value="30"/> days</p> <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> Expiration dates help keep your files more secure by limiting access.</p> </div>
<b>My Contact Information</b> <p>Name</p> <input type="text"/> <p>Email Address</p> <input type="text"/> <p>Confirm Email Address</p> <input type="text"/>	<b>Other Settings (optional)</b> <p><input checked="" type="checkbox"/> Notify me when the file(s) have been downloaded</p> <p><input checked="" type="checkbox"/> Automatically send the download link to the guest user(s) in an email</p> <p><input checked="" type="checkbox"/> Send me an email copy with the download link</p> <p><input type="checkbox"/> Require the guest to enter this password to access Serv-U. (To generate a password, click on the key button)</p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;"> <input type="text"/>  </div> <p><input type="checkbox"/> Include the password in the email (less secure)</p> <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> Your passwords are not recoverable. In the case of a lost password, the file(s) would need to be resent with a new password.</p> </div>

2. Enter an email subject title.
3. Enter any additional comments if required.
4. Enter your name, email address, and confirm email address.
5. Set an expiration date or period for when the link to the download files will expire.
6. To be notified when files have been downloaded, select the Notify me option.
7. To create an anonymous share, deselect Automatically send the download link to the guest user(s) in an email.
8. To require the guest to enter a password before downloading the files, select this option, and enter or generate the password.

 You can include the password with the notification, if appropriate.

## 9. Click Next.



**Send Files to Guest User: Upload Files (Step 2 of 2)**

Upload up to 20 files in one file share. Please note that each file must be under 2 GB in size.

Select your file(s) to upload

1. **Choose File** delete\_dns.png ✕
2. **Choose File** No file chosen
3. **Choose File** No file chosen
4. **Choose File** No file chosen
5. **Choose File** No file chosen

**+ Add more files**

**<< Back** **Upload >>** **Cancel**


## 10. For each file, click Choose File, and select the file.

**i** The files you share this way are virtually linked. If you modify the file, the latest version will be available for guests to download. If you rename or delete the file, it will not be available for guests to download. Guest users are notified when attempting to download or delete a virtually linked file whose name or location changed since the creation of the file share.

**i** You can upload up to 20 files in one file share. The file size you can upload depends on the browser you use. The size limitations mostly apply to older versions of Internet Explorer.

## 11. Click Upload.

After uploading your files and sending them, you will see the File Upload Confirmation page which summarizes the outgoing file upload.

 **File Upload Confirmation**


---

File uploaded completed on **7/10/2013 05:51 PM**.

If you have selected to automatically send the download link, in the file upload settings, **no further action is required**. Your email will be sent and you can access the files.

**This URL will provide access to download your files:**  
<http://127.0.0.1/?ShareToken=B02B6777B01390A288E6C3914FD76CA43240535C>


The following file was successfully uploaded:

1  ipmon.png

---

Optional Next Steps:	Please note:
<ul style="list-style-type: none"><li>Manually send the URL by <b>copying and pasting the URL</b> into an email to send to your recipient(s)</li><li><b>Generate an email</b> from your email client (<i>opens a new email window in your email application like Microsoft Outlook</i>)</li><li>Select <b>Cancel File Share</b> to delete this file share and return to the Home screen</li></ul>	<ul style="list-style-type: none"><li>The File Share is <b>NO</b></li></ul>

12. Click Done to finish.

 End users may request files from other people by sending email invites (with options for share expiration dates and password protection). Guests automatically receive a notification inviting them to send files, and the end user will get additional notifications as files are sent.

## Serv-U file sharing: the Request Files wizard


By using the Request Files wizard, you can receive a file from someone by sending a link to a page where the other party can upload the file to.

The user receives a link in email that grants them access to upload files. For added security, you can set the page link expiration and add file constraints and restrictions.



To send a file share request:




## 1. Enter the guest user's email address.


**Request Files From Guest User**

Invite a guest user to temporarily access Serv-U File Share to upload files. The user will receive a link, via email, that grants them access to upload files. For added security, there are options to set the page link expiration and add file constraints and restrictions.

Email Information	Serv-U Access Link Expiration
Guest Email Address(es) <input type="text"/>	The link to upload files should expire: <input checked="" type="radio"/> on this specific date <input type="text" value="02/02/2020"/>
Email Subject <input type="text" value="Serv-U File Share Link [expires 02/02/2020]"/>	<input type="radio"/> in <input type="text" value="24"/> hours <input type="radio"/> in <input type="text" value="30"/> days
Comments (optional) <input type="text"/>	<div>  <b>Note:</b> Expiration dates help keep your files more secure by limiting access.           </div>
<b>My Contact Information</b> Name <input type="text"/> Email Address <input type="text"/> Confirm Email Address <input type="text"/>	<b>Other Settings (optional)</b> <input checked="" type="checkbox"/> Notify me when the file(s) have been uploaded <input checked="" type="checkbox"/> Automatically send the upload link to the guest user(s) in an email <input checked="" type="checkbox"/> Send me an email copy with the upload link <input type="checkbox"/> Constrain individual file sizes to: <input type="text" value="10"/> <input type="text" value="MB"/> <input type="checkbox"/> Require the guest to enter this password to access Serv-U. (To generate a password, click on the key button) <input type="text"/> <input type="checkbox"/> Include the password in the email (less secure) <div>  <b>Note:</b> Your passwords are not recoverable. In the case of a lost password, the invitation would need to be resent with a new password.           </div>

2. Enter the email subject title.
3. Enter any additional comments.
4. Enter your name, email address, and confirm the email address.
5. Set an expiration date or period for when the link to upload files will expire.

 90 days is the maximum time for link availability.

6. Select Notify me when the file(s) have been uploaded if you want to receive an email when the guest user(s) have uploaded files.
7. If you want to restrict the size of the uploaded files, check the Constrain individual file, and enter the maximum size.
8. To require the guest to enter a password to access Serv-U, select this option, and enter or generate the password.

## Serv-U file sharing: Share details

The File Share details page provides an overview of all the files sent, and the download history of each file. You can also download the files belonging to a file share on this page, either individually, or in bulk, by clicking Download All. If the file share contains remote files, and the files were renamed, moved, or deleted in the meantime, the corresponding Download and Delete buttons are replaced by exclamation points to indicate that it is not possible to perform these actions on the files. Additionally, if a remote file was renamed, moved or deleted, it will not be included in the download if you click Download All.

After the file share access link has expired, Serv-U automatically deletes the entire file share and there will not be any record of it after this period of time. The setting where you can configure the number of days that elapse after a download is located in the Management Console under Domain Limits & Settings > [File Sharing](#).

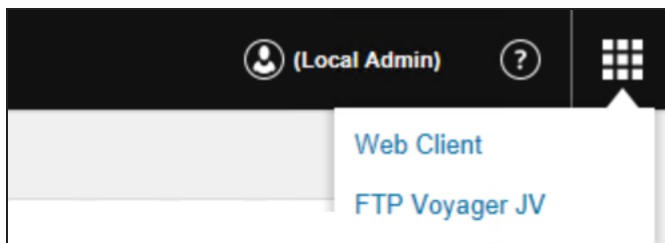
You can delete the file share sooner by clicking Delete File Share Now.


## The Serv-U Web Client

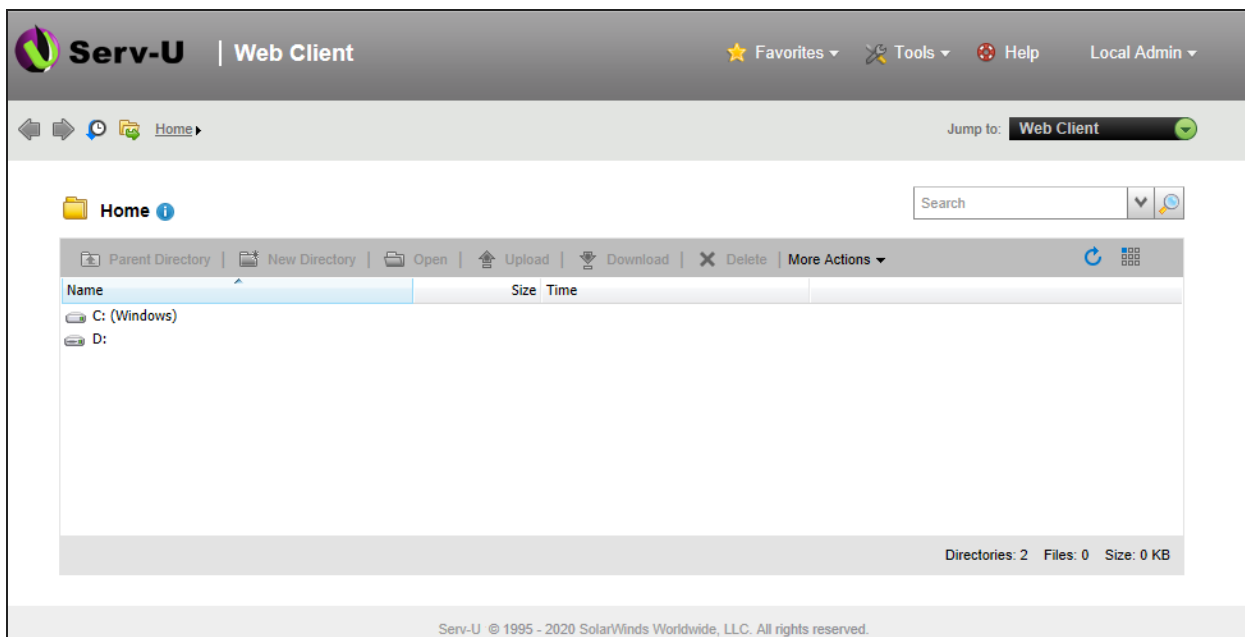
The Serv-U Web client allows users to log into the file server and access all of their files online without needing to use an external FTP client.

The Web Client interface is presented as a standard web page as shown below, containing a list of the files and directories available from the current remote path, and links that perform various file transfer related actions. All functionality of the Web Client is available from this single page to keep interactions quick and easy to perform. The Web Client can be accessed from mobile devices and is optimized for use in a variety of display resolutions.

To access the web client from the Serv-U console, select Web Client from the tools drop-down menu.



 You can specify the web client to be the default FTP client displayed when users log into your file server.



# Web Client layout

The Web Client is presented as a standard web page containing a list of the files and directories available from the current remote path and clickable links that perform various file transfer related actions. All functionality of the Web Client is available from this single page to keep interactions quick and easy to perform.

## User bar

At the top of the page is a header containing options relevant to your Web Client session. These options apply to your Serv-U user account or the session that has been established with Serv-U by your browser.

Favorites	In the Serv-U Web Client, you can save favorite folders, which can be quickly accessed from the User Bar. You can add a folder to the favorites in one of the following two ways: by right-clicking the folder and selecting Add to Favorites, or by selecting the folder, and then clicking Add to Favorites under More Actions.
Tools	Open the Tools menu to enable or disable Web Client Pro. Launching Web Client Pro will give you the added functionality of multiple concurrent uploads and downloads, upload and download of directories, multiple file delete, and additional management over transfers.
Help	The help launches the Serv-U Web Client help documentation. Visit our <a href="#">community forums</a> for more help.


## User menu

In the user menu, which shows your account's full name or login ID, you can perform a variety of actions.

Change Password	If the administrator allows users to change their account's password, this option is available. Click Change Password to bring up a new window that asks for your current password and the new password you want. After entering the appropriate information, click OK to change the account's password. If the new password does not meet the administrator's security settings for passwords, a message is displayed that explains how the new password does not meet these security requirements.
Change Email Address	If the administrator allows users to change their account's email address, this option is available. Click Change Email Address to bring up a new window that lets you update your account email address. You can use your email address to receive or reset your password if this option is enabled by your administrator.
Log out	When you are finished with the Web Client, click Logout to end your session.

## The navigation bar

The Serv-U Web Client features full history navigation including back and forward buttons, a history browser, and an address toolbar.

Back	Navigates the Web Client to the previously listed directory.								
Forward	Navigates the Web Client to the next most recent directory listed.								
History list	Displays the full navigation history since the Web Client was loaded.								
	 Reloading the Web Client clears your navigation history.								
Address toolbar	Lists the current directory with each of the directory segments a clickable link. To navigate directly to a particular directory, click the directory name. Additionally, click the arrow next to a directory segment to display its sub-directories in a pop-up menu. After this menu is displayed, select the sub-directory you want to make your current directory.								
Go to directory	On the right of the navigation bar, the Go To icon displays a dialog that allows you to enter a path. Once entered and submitted, the directory listing is updated for that path. This is the fastest way to navigate directly to a directory when you know the full path. If you visit this directory frequently, consider adding it to your Favorites for faster navigation in the future.								
Jump to	In the Jump To menu you can change which HTTP interface you are using with Serv-U. The following options are available:								
	<table> <tr> <td>Web Client</td><td>The HTTP interface that offers access to Web Client Pro.</td></tr> <tr> <td>Management Console</td><td>If your user account has administrative privileges in Serv-U, this link opens the Management Console.</td></tr> <tr> <td>FTP Voyager JV</td><td>Available with Serv-U MFT Server licenses, this link launches the FTP Voyager JV full-featured transfer client. Java must be installed to use FTP Voyager JV.</td></tr> <tr> <td>File Sharing</td><td>If File Sharing is enabled for your domain, this link opens the File Sharing interface where you can send and receive files from users without a Serv-U account.</td></tr> </table>	Web Client	The HTTP interface that offers access to Web Client Pro.	Management Console	If your user account has administrative privileges in Serv-U, this link opens the Management Console.	FTP Voyager JV	Available with Serv-U MFT Server licenses, this link launches the FTP Voyager JV full-featured transfer client. Java must be installed to use FTP Voyager JV.	File Sharing	If File Sharing is enabled for your domain, this link opens the File Sharing interface where you can send and receive files from users without a Serv-U account.
Web Client	The HTTP interface that offers access to Web Client Pro.								
Management Console	If your user account has administrative privileges in Serv-U, this link opens the Management Console.								
FTP Voyager JV	Available with Serv-U MFT Server licenses, this link launches the FTP Voyager JV full-featured transfer client. Java must be installed to use FTP Voyager JV.								
File Sharing	If File Sharing is enabled for your domain, this link opens the File Sharing interface where you can send and receive files from users without a Serv-U account.								

## Directory listing and actions

Below the navigation bar is the directory listing returned by the server for the current directory. Above the directory listing are the various actions that you can perform to navigate the server, transfer files, or change the layout of the listings. For more information about these actions, see the [Manage directories](#), [Manage files](#), and [Thumbnails, slideshows, and the media player](#) topics.

In the bottom right of the directory listing is a summary of the contents of the current directory. Listed here is the number of directories, the number of files, and the total size of the files contained in the current directory.

## Manage directories


The majority of the view of the Web Client is dedicated towards displaying the contents of the current directory being browsed on the server. This directory listing shows all the files and folders contained in the current directory. Depending on the access rights granted to your user account by the administrator, you can perform various actions on the files and folders in this listing.

To change the current directory:

- Double-click a directory in the listing.
- Right-click a directory, and then click Open.
- Select a directory in the listing, and then click Open in the toolbar above the listing.


### To...

Go to Parent directory	If your user account is locked in your home directory and the current directory is your home directory, this button is not available. Click the button to change the current directory to the parent directory. For example, if your current directory is <code>/public/files</code> , clicking the button changes the current directory to <code>/public</code> .
Create new directory	Click New Directory, and then specify the name of the new directory. If your user account does not have the permission to create directories, or there is a conflict with the new directory name, an error message is displayed.
Delete directory	Select the directory from the listing, and click Delete. This option is also available by right-clicking the directory you want to delete. If your user account does not have the permission to delete directories, an error message is displayed.

 Deleting a directory deletes all files and folders that are contained in the directory. This action cannot be undone on the server.

**To...**

Rename directory	Select the directory to rename in the directory listing, and click Rename in the More Actions drop-down menu. This option is also available by right-clicking the directory you want to rename. The current name is displayed in a new dialog. Change this name to the new name, and click OK. If your user account does not have the permission to rename directories, or there is a conflict with the new directory name, an error message is displayed.
------------------	--

 Refreshing the current directory listing causes the Web Client to retrieve the directory listing again and update the displayed files and folders.

## Thumbnails/Details

Click Thumbnails to change the view from a detailed view to a thumbnails view. While in thumbnails view, the Web Client retrieves and displays small versions of any image files in the current directory. When in thumbnail view, an additional menu is available where you can change the size of thumbnails that are displayed. For more information about thumbnails, see [Thumbnails, slideshows, and the media player](#). Click this button again to return the view to the default Details mode.

## Folder favorites

To add folders to the Favorites list, select a folder in the directory listing, and then click Add to Favorites under More Actions. This option is also available by right-clicking a folder, and then selecting Add to Favorites.

## Manage files

The majority of the view of the Web Client is dedicated towards displaying the contents of the current directory being browsed on the server. This directory listing shows all the files and folders contained in the current directory. Depending on the access rights granted to your user account by the administrator, you can perform various actions on the files and folders in this listing.

**To...****Upload files**

If your user account has permission to upload new files, you can upload a single file at a time to the server using this button. Click Upload to open a new window from which you can browse your system for the file you want to upload. After you have selected the appropriate file, click Upload to begin the transfer.

When the upload has started, a progress dialog is displayed that is regularly updated with live information, including the current transfer rate, how much data has been sent, how much data remains to be sent, and the estimated time until completion of the transfer. While a file is being uploaded, no other action can be taken including changing the current directory or transferring another file. You can terminate the transfer at any time by clicking Cancel. Canceled file transfers cannot be resumed and must be started over.

After the upload has completed, the progress dialog disappears and the directory listing is refreshed to show the new file.

**Download files**

To begin a file download, select the file you want to download, and then click Download. This option is also available by right-clicking the file you want to download. The browser prompts you for a location on your system to save the file. Some browsers may also offer the option to open the file instead of saving it to a permanent location. While a file is being downloaded, the Web Client is free to perform other actions.


**Rename files**

To rename a file, select the file you want to rename in the directory listing, and then click Rename under More Actions. This option is also available by right-clicking the file you want to rename. The current name is displayed in a new dialog. Change this name to the new name, and then click OK

If your user account does not have the permission to rename files or there is a conflict with the new file name, an error message is displayed.

**Delete files**

To delete a file, select the file from the listing, and then click Delete. This option is also available by right-clicking the file you want to delete. If your user account does not have the permission to delete files, an error message is displayed.

 Files are permanently deleted from the server. This action cannot be undone.



# Thumbnails, slideshows, and the media player

The Web Client, combined with advanced features in Serv-U, is a perfect platform for sharing photos with friends, family, or clients. Using advanced on-the-fly compression techniques, the Web Client can request a custom sized thumbnail image for virtually any type of image file. This thumbnail image is generated by the server upon receiving the request and sent back to the client. In this way, you can view a smaller version of an image file in a fraction of the time it would take to download the entire file and open it up locally. This also minimizes the amount of bandwidth used by the server to send these image files.

## View images

The Web Client supports two image viewing modes: thumbnails and slideshows. Slideshows can be viewed when in either the detailed or thumbnail view mode.

To display thumbnails or slideshow, click on a file and select Preview Image or Slide Show from the More Actions drop-down menu.

### Thumbnails

The thumbnail view replaces the detailed directory listing with one that allows a thumbnail image to be displayed for each file. If the file is not of a supported image type, then the appropriate icon for the file type is displayed instead. While in thumbnail view mode, you can use the same toolbar displayed above the directory listing to open folders, transfer files, and rename or delete the currently selected file.

You can customize the size of each image thumbnail by opening the thumbnail size menu next to the Thumbnail View mode button. Three sizes are offered to help you find a balance between the size of the thumbnails and the time it takes to retrieve them. When creating thumbnail images, Serv-U preserves the aspect ratio of the image to avoid distorting the original image.

You can preview images in both the thumbnail and detailed view mode. An image that you preview is displayed in a new dialog as if in a slideshow, however, it is paused on the previewed image. Images are displayed at a maximum width of 600 pixels. If the previewed image is smaller than this size, then the image is shown using its actual dimensions. While previewing an image, you can start a slideshow by clicking Play in the bottom left of the preview dialog.

### Slideshows

Slideshows provide a way to automatically preview the images contained in the current directory. While viewing an image in slideshow mode, you can perform standard actions on that file including downloading, renaming, and deleting, by clicking the appropriate button below the image.

You can control the slideshow manually by using the buttons on either side of the current slideshow image. The current position in the slideshow is displayed at the top of the dialog. A >Play Slide Show or Pause Slide Show link is displayed in the top right corner. Next to this is an options button that displays a slider to control the speed at which images advance in the slideshow. Adjusting the slider to the left increases the time each image is displayed while adjusting it to the right decreases the amount of time for each image. On some servers, a loading image may be displayed when advancing to the next image if the current pace is faster than the server is capable of generating and sending the slideshow image.

Along the bottom of the dialog a strip of the next five images in the slideshow is displayed. The arrows to the left and right of these images can be used to browse all images in the slideshow. To jump to a specific image in the slideshow, click that image in the thumbnail strip.


When you are finished viewing the slideshow, press Escape on your keyboard, or click the 'x' in the top right corner of the dialog.

## Use the media player

In the media player you can play most common media formats instantly using the Media Player window in the Web Client. By using the media player, you can preview audio and video files before downloading, and you can also build playlists to stream audio straight from the Web Client.

Playlists are dynamically generated by Serv-U to play all audio files located in your current directory. If audio files are detected in the current directory, a Play List option is displayed. Click the button to begin successively streaming all audio files in your current directory to the built-in media player.

You can control the media player manually by using the Previous and Next buttons above the player. Next to these controls is a counter showing the position of the current media file along with the total number of media files in the current directory.

 These controls manually change to the previous or next media file in the current directory. After the media file has been played, the media player does not automatically move on to the next media file.

To play multiple audio files in succession, use the Play List option. When you are using this feature, you can use the controls in the appropriate media player plug-in to change the current track. While streaming a playlist from Serv-U, the download, delete, and rename actions are hidden.

## Web Client Pro

This topic provides information about the features and options of Web Client Pro. The information is organized into the following sections:

- [Web Client Pro layout](#)
- [Web Client Pro transfer pane](#)
- [Operation management](#)
- [Preferences](#)
- [About](#)
- [Install Java](#)

## About

In the About dialog, you can get information about the version of Web Client Pro you are using, contact information for SolarWinds and local translator partners, and legal information regarding the Web Client Pro software package.

### Program information

The Program information page includes the following information:

- Web Client Pro Version: The software version of Web Client Pro.
- Build Date: The date that this version was built.
- Contact Information: The contact information for SolarWinds.
- Development: Information about the developers of Web Client Pro.
- Legal: Legal disclaimers regarding the software.

### Computer information

The Computer information page provides a technical readout of the computing environment in use by Web Client Pro. The Copy to clipboard option allows easy copying of this information for use with technical support when needed.

## Preferences

On the preferences page, you can change Web Client Pro settings according to individual needs. The following section contains information about the settings you can change.

### Confirmation options

Disabling any of the following options removes confirmations from the given action. For example, disabling Confirm upload overwrite allows users to overwrite existing files without confirmation, while disabling Confirm file delete allows files to be deleted without confirmation.

- Confirm upload overwrite and 'resume'
- Confirm download overwrite and 'resume'
- Confirm upload folder merge

- Confirm download folder merge
- Confirm file delete
- Confirm folder delete
- Confirm folder relists when restarting transfers

## Transfer pane

Options in the transfer pane menu affect transfer operations and the display options of the transfer pane.

Number of Threads (1-10)	By default, Web Client Pro transfers four files at a time. However, you can decrease this for faster performance on slower systems, or increase on higher-performance systems.
Enable Row Colors	Enabling row colors will alternate coloring of rows in the transfer pane for users who want even and odd rows to be identified. The colors can be selected as well.
Automatically Expand New Transfer Groups	Transfer Groups or Operation Groups are expanded by default to show a list of all files and folders being operated upon. This option can be disabled.
Automatically Start New Transfer Items	By default, new transfers are started immediately. You can disable this setting so that operations can be queued, then started on demand.
Automatically Remove Completed Transfers	The transfer pane does not automatically clear completed items, allowing users to review transferred items before clearing the list. This can be set to automatically clear items that are successfully transferred. Failed transfers, or operations that encountered an error, are left in the list for review.

## Install Java

If Java is not installed on your system, or if you are using a third-party version of Java, you may encounter trouble running Web Client Pro. In order to correct this, follow the directions below to install Java on your operating system.

### Windows

To install Java on Windows:

1. Navigate to <http://java.com/en/download/>.
2. Click Free Java Download to download the Java Runtime Environment.

3. Follow the prompts to complete Java installation.
4. Restart the browser, and then log in to Serv-U to start Web Client Pro.

## Mac OS X

Oracle does not maintain the Java Runtime Environment on the Macintosh operating system. To install the Java Runtime Environment or to update it, use the Apple Menu > System Update menu in the Finder.

## Linux

Installing Java on Linux can be complicated because most distributions ship with a third party JRE called "IcedTea", which functions differently than the Oracle JRE.

To install the official Java Runtime Environment:

1. Navigate to [http://java.com/en/download/linux\\_manual.jsp](http://java.com/en/download/linux_manual.jsp).
2. Download the Linux (Self-Extracting File) for x86-based kernels or Linux x64 for x86\_64 kernels.
3. Create the directory `/usr/java/`, and then move the JRE into the directory.
4. Type `chmod a+x jre%VER%.bin` to change permissions on the JRE file to allow execution.
5. Type `./JRE~.bin` to extract the JRE to the file system.
6. In 64-bit Linux, type `sudo rm /usr/lib64/mozilla/plugins/libjavaplugin.so` to remove the IcedTea Java plugin, which is not supported by Web Client Pro. In 32-bit Linux, type `sudo rm /usr/lib/mozilla/plugins/libjavaplugin.so`.
7. Type `sudo ln -s /usr/java/jre%VER%/lib/amd64/libnpjp2.so /usr/lib64/mozilla/plugins/ (or /usr/lib/ for 32-bit Linux)` to allow the plugin to load in your browsers.

**i** If SELinux is enabled, it must be configured to allow "execstack", required by Oracle Java. To do this, type `sudo setsebool -P allow_execstack 1`.

## Web Client Pro layout

Web Client Pro provides file transfer using a Java applet within the web browser, providing a balance between the ease of use in the Web Client and the advanced file transfer capabilities of FTP Voyager JV. With Web Client Pro, you can upload or download multiple files and folders quickly and easily, with a detailed Transfer Pane for easy review of ongoing transfers.

The Web Client Pro is displayed as an additional area below the normal Web Client toolbar, and is separated into two sections:

- The Transfer Pane, providing a list of pending or ongoing operations.
- The Web Client Pro toolbar, used to manage the transactions and operations.







## Web Client Pro transfer pane





The transfer pane provides a comprehensive view of all active file operations in Web Client Pro, grouped together according to operations that began at the same time. A set of operations is referred to as an operation group, and is named according to the type of action (Download, Upload, Delete) and which order it occurred in. The transfer pane provides the following information about each transfer:

Operation	The status of the operation.
Name	The name of the file being uploaded, downloaded, or deleted.
Status	The current speed of the operation.
Completion	The estimated time until the completion of the operation.
Source path	The full path to the source file. This may be a local path (such as C:\files\myfile.txt), or a remote path (such as /files/myfile.txt).
Destination path	The full path to the destination file. It operates the same way as the source path, showing the destination of the file.

## Operation management

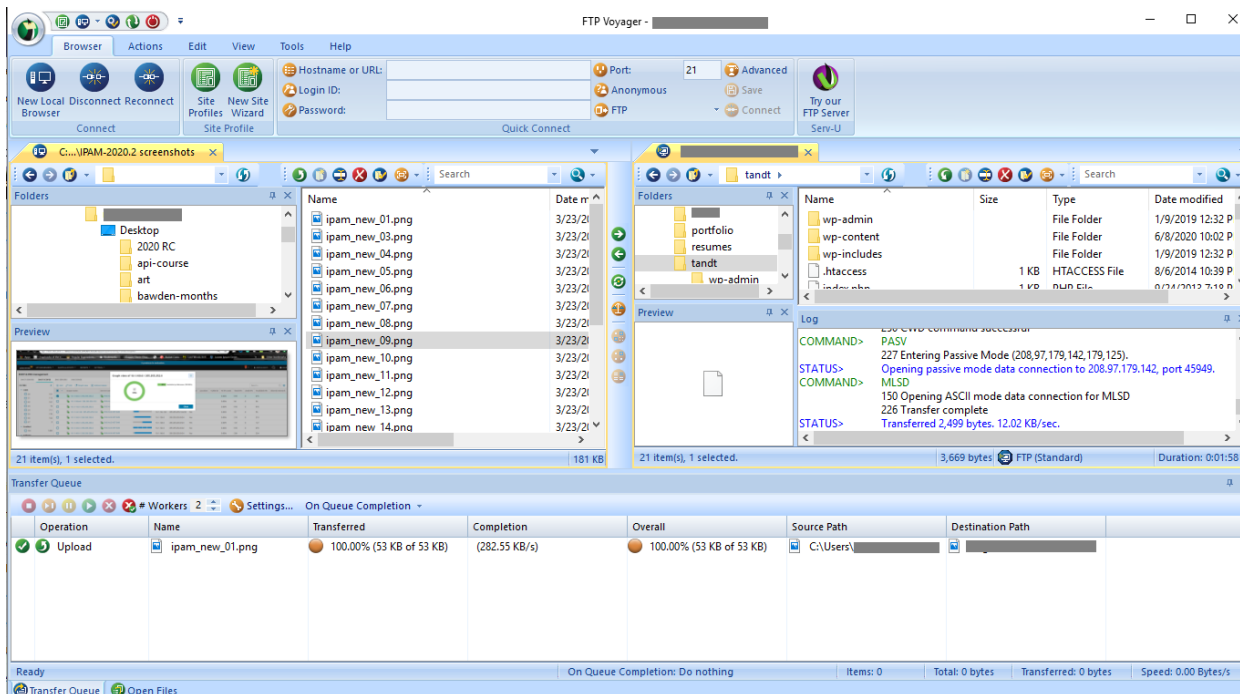
The Web Client Pro toolbar includes all functions needed to manage ongoing operations in the transfer pane. The following section contains the list of these functions.

	Show in Folder	Launches the default file explorer of the operating system and navigates to the download's target directory of the selected row.
	Open File	Launches the operating system's default program for the download's target file of the selected row.
	Stop After File Completes	Waits for the current operation to finish, then stops all upcoming transfers and awaits user input.
	Skip File	Skips the currently uploading or downloading file, and then moves on to the next operation in the queue.
	Pause	Pauses the current operation and the rest of the operation queue.
	Resume	Resumes the current transfer operation and the rest of the operation queue.

	Start	Starts an operation queue that has been stopped completely.
	Restart/Relist	Restarts a failed operation or relists a directory listing operation that has failed.
	Remove	Removes a file or operation group from the transfer pane.
	Remove Completed	Removes completed operations only from the transfer pane.
	Remove Canceled	Removes canceled operations only from the transfer pane.
	Remove Skipped	Removes skipped operations only from the transfer pane.
	Remove Paused	Removes paused operations only from the transfer pane.
	Remove Waiting	Removes waiting operations only from the transfer pane.
	Remove Stopped	Removes stopped operations only from the transfer pane.
	Remove All	Removes all completed, canceled, skipped, paused, waiting, and stopped operations from the transfer pane.
	Settings	Provides access to the configuration options for Web Client Pro.
	About	Displays version and developer information about Web Client Pro.


# Serv-U FTP Voyager JV (MFT only)

The SolarWinds FTP Voyager JV is a fully functional FTP Client which can be loaded on-demand for MFT edition Serv-U servers.



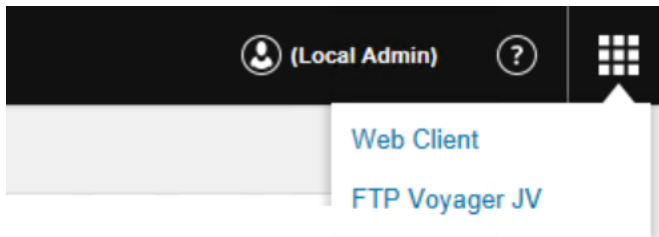
Some important features of FTP Voyager JV include:

- No installation required - FTP Voyager JV only requires the Java Runtime Environment.
- Operates using the HTTP protocol for easy firewall configuration.
- Supports SSL encrypted communications using HTTPS.
- Thumbnail view of remote images that minimizes bandwidth usage.
- Maintains timestamps of transferred files.
- Easy drag and drop file transfers between local and remote panes.
- Multiple concurrent transfers for fast delivery of files.
- Customizable appearance, giving users a sense of familiarity between applications.
- Easily manage transfers through a Transfer Queue.

 You can specify FTP Voyager JV to be the default FTP client displayed when users log into your file server.

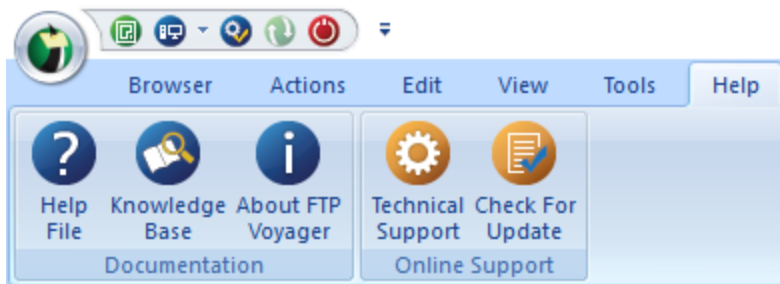


To access FTP Voyager from the Serv-U console, click on the icon in the upper right corner and select FTP Voyager.



## FTP Voyager help

FTP Voyager comes with its own help file and knowledge, which are accessed from the Help tab as shown below.



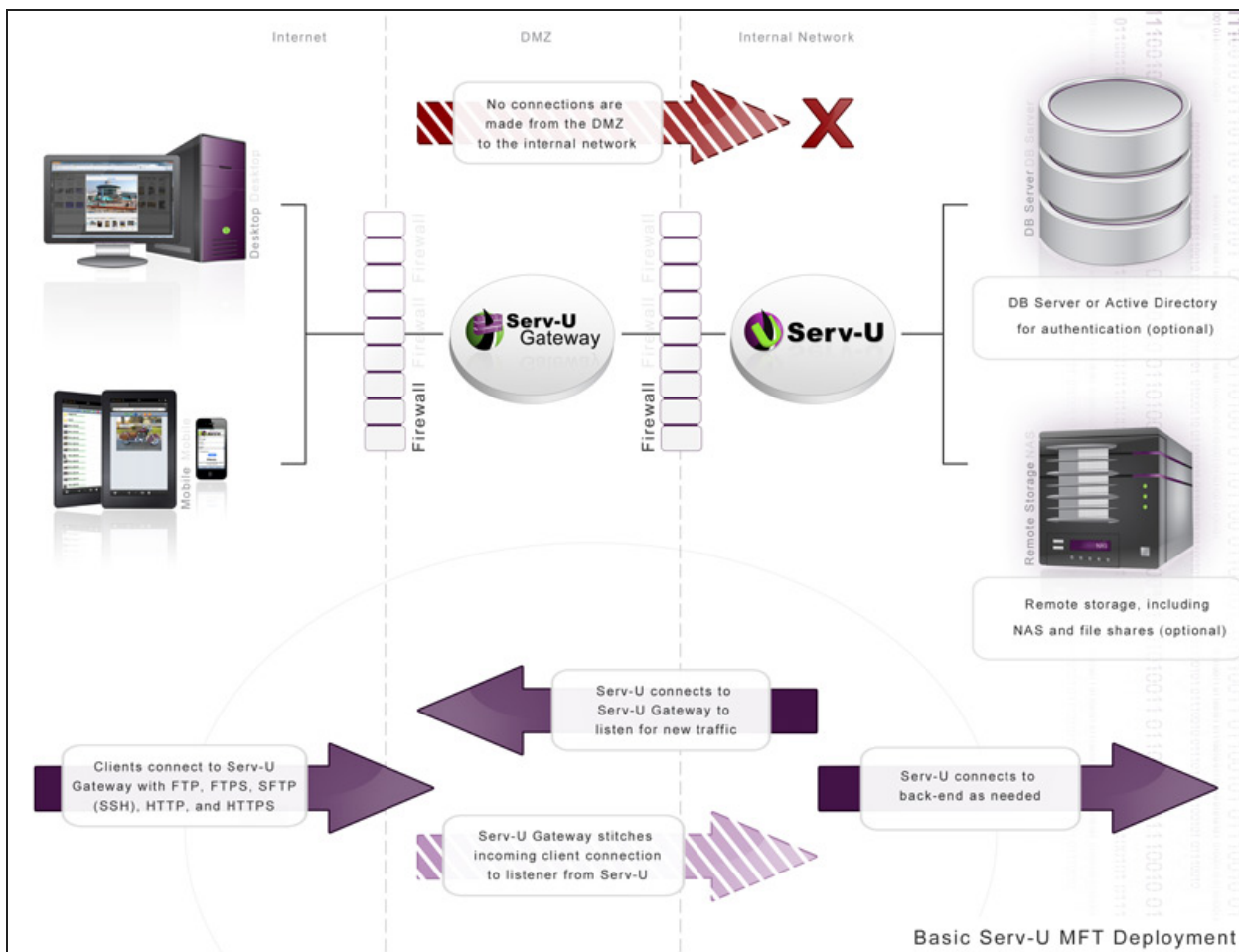
# The Serv-U Gateway

- Gateway deployment documentation
- The Gateway tab
- Manage Gateways

The Serv-U Gateway provides defense in depth to Serv-U File Server deployments.

It acts as a reverse proxy in demilitarized zone (DMZ) segments and prevents your Serv-U File Server deployments from storing data in the DMZ, or opening connections from the DMZ to the internal network.

This type of architecture is essential to meet Payment Card Industry Data Security Standard (PCI DSS), managed file transfer, and other high-security requirements.







# Gateway deployment documentation

- Serv-U distributed architecture guide
- Gateway installation instructions
  - For Windows
  - For Linux
- Plan your Serv-U Gateway deployment

## The Gateway tab in Serv-U

The Gateway page in Server Details displays all configured gateways known to the Serv-U File Server deployment. Serv-U File Server periodically checks every configured gateway and displays a status message here.

Gateway Status	<p>The icon in the Gateway Address column changes to reflect the current gateway status.</p> <div><div></div><div>The gateway is ready for connections. However, the gateway still needs listeners to receive connections.</div></div> <div><div></div><div>Serv-U is checking the status of the gateway. Another status will appear in a few seconds.</div></div> <div><div></div><div>The gateway is ready but the Serv-U installation is running close to the end of the trial period, or support period.</div></div> <div><div></div><div>An error occurred. For more information about why it is not possible connect to the gateway, select the gateway entry, and select Properties.</div></div>
Gateway Address	<p>The gateway address is the IP address on the Gateway that Serv-U File Server uses to communicate with Gateway. This should almost always be a private IP address.</p> <p>A status icon is displayed on the left of the gateway address. The Status column displays a brief message that indicates the current status of the gateway.</p>
Public IP Address	<p>The Public IP Address column shows the IP address file transfer clients should connect to.</p> <p>A private IP address is displayed in the Public IP Address column if a private IP address was explicitly configured in the gateway. This occurs if the gateway has no public IP addresses, which is common during trials and situations in which the gateway is placed behind network address translation (NAT).</p>
Description	<p>The Description column displays any note that is added to the gateway configuration. It does not affect behavior.</p>

# Manage Gateways

Serv-U Gateway

Gateway Address:  
192.168.5.63

Port:  
1180

Public IP Address:  
67.52.42.106

☒ Enable Gateway

Description:

Save

Cancel

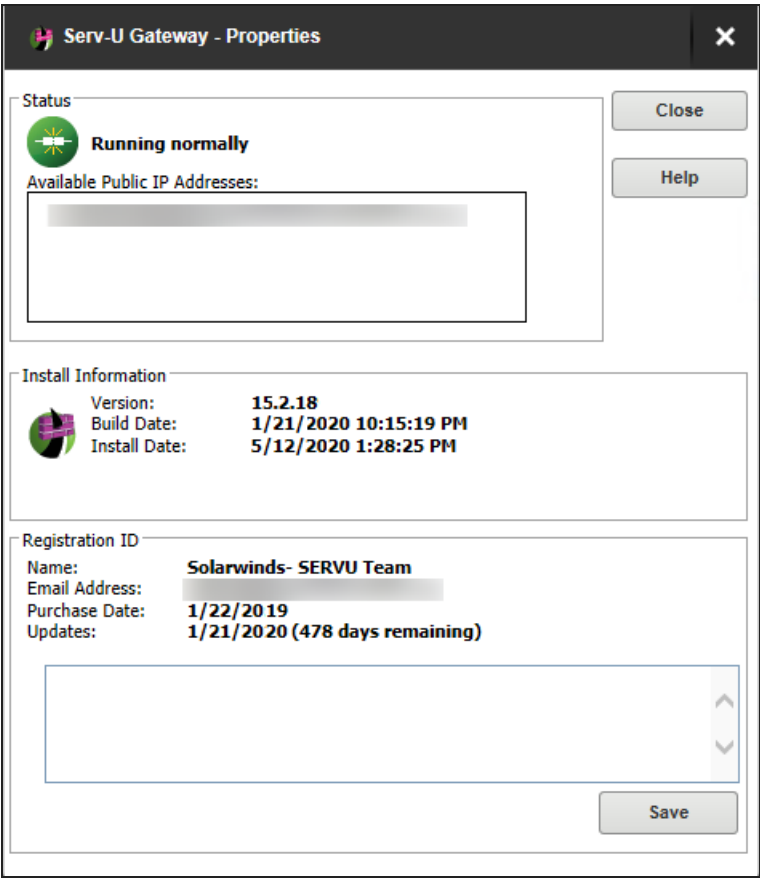
Help

Click Add, Edit, or Delete to manage Gateway configurations.

Gateway Address	The IP address on the Gateway that Serv-U File Server uses to communicate with Gateway. This should almost always be a private IP address.
Port	The TCP port on the Gateway that Serv-U File Server uses to communicate with Gateway. The default is TCP port 1180.
Public IP Address	The IP address file transfer clients should connect to. 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 is behind NAT (network address translation).
Enable Gateway	Use to turn the gateway on and off. The default is on.
Description	An optional note about the gateway. It has no effect on the behavior.

## Gateway properties dialog

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




Status	The large icon in the Status area and a status message indicate if the gateway is running, and whether or not it is running with a trial or commercial license.
Available Public IP Addresses	The field contains a list of all the public IP addresses automatically detected on Gateway. If a private address is configured in the Public IP Address field of the gateway, this field displays a message indicating that no public IP addresses are found on the gateway server. This is expected behavior.
Install Information	The Install Information area shows the version and build date of the Gateway software running on the gateway, the date Gateway was installed or last updated, and, if applicable, the number of days left in the evaluation period.
Registration ID	<p>Copy and paste your Gateway Registration ID (not your Serv-U File Server Registration ID) into this field, and click Save to apply a commercial license to your Gateway software.</p> <p>If you have lost your registration ID, visit the Online Customer Service Center to retrieve it.</p>

# System variables

- [Server information](#)
- [Server statistics](#)
- [Domain statistics](#)
- [User statistics](#)
- [Last transfer statistics](#)
- [Date/Time](#)
- [Server settings](#)
- [Session information](#)
- [File information](#)
- [Current activity](#)
- [FileShare](#)

You can customize certain configurable messages in Serv-U to include a wide range of variables as outlined in the following list. 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 you can use these variables include event messages, customized FTP command responses, or a welcome message.

Furthermore, you can also use the %USER%, %HOME%, %USER\_FULL\_NAME%, and %DOMAIN\_HOME% variables. For more information about these variables, see [Group Properties: Directory Access](#).

 When you use macros, in general, it is best to use \$ macros for events and in system messages (such as login messages or customized FTP responses) and % macros for configuration values. Many of the \$ macros do not have explicit values until a session has been successfully established or a specific action has taken place, whereas the % macros have explicit values at all times.

All variables are case sensitive. Statistical information, unless otherwise specified, is calculated since the Serv-U File Server was last started.

## Server information

Variable	Description
\$ServerName	Displays the full name of the server (that is, Serv-U).
\$ServerVersionShort	Displays the first two digits of the current version of the Serv-U File Server (for example, 15.1).
\$ServerVersionLong	Displays the full version number of the Serv-U File Server (for example, 15.1.0.480).

Variable	Description
\$OS	Displays the name of the operating system (for example, Windows Server 2008 R2).
\$OSVer	Displays the full version number of the operating system (for example, 6.1.7601).
\$OSAndPlatform	Displays 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	Displays 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

Variable	Description
\$ServerDays	Displays the total number of days the server has been online continuously.
\$ServerHours	Displays the number of hours from 0 to 24 the server has been online, carries over to \$ServerDays.
\$ServerMins	Displays the number of minutes from 0 to 60 the server has been online, carries over to \$ServerHours.
\$ServerSecs	Displays the number of seconds from 0 to 60 the server has been online, carries over to \$ServerMins.
\$ServerKBup	Displays the total number of kilobytes uploaded.
\$ServerKBdown	Displays the total number of kilobytes downloaded.
\$ServerFilesUp	Displays the total number of files uploaded.
\$ServerFilesDown	Displays the total number of files downloaded.
\$ServerFilesTot	Displays the total number of files transferred, essentially (\$ServerFilesUp + \$ServerFilesDown).
\$LoggedInAll	Displays the total number of established sessions.
\$ServerUploadAvgKBps	Displays the average upload rate in KB/s.
\$ServerDownloadAvgKBps	Displays the average download rate in KB/s.
\$ServerAvg	Displays the average data transfer rate (uploads and downloads) in KB/s.
\$ServerUploadKBps	Displays the current upload transfer rate in KB/s.
\$ServerDownloadKBps	Displays the current download transfer rate in KB/s.
\$ServerKBps	Displays the current aggregate data transfer rate in KB/s.
\$ServerSessions24HPlusOne	Displays the total number of sessions in the past 24 hours plus one additional session.
\$ServerSessions24H	Displays the total number of sessions in the past 24 hours.



## Domain statistics

Variable	Description
\$DomainKBup	Displays the total number of kilobytes uploaded.
\$DomainKBdown	Displays the total number of kilobytes downloaded.
\$DomainFilesUp	Displays the total number of files uploaded.
\$DomainFilesDown	Displays the total number of files downloaded.
\$DomainFilesTot	Displays the total number of files transferred, essentially (\$DomainFilesUp + \$DomainFilesDown).
\$DomainLoggedIn	Displays the total number of sessions currently connected.
\$DomainUploadAvgKBps	Displays the average upload rate in KB/s.
\$DomainDownloadAvgKBps	Displays the average download rate in KB/s.
\$DomainAvg	Displays the average aggregate data transfer rate (uploads and downloads) in KB/s.
\$DomainUploadKBps	Displays the current upload transfer rate in KB/s.
\$DomainDownloadKBps	Displays the current download transfer rate in KB/s.
\$DomainKBps	Displays the current aggregate data transfer rate in KB/s.
\$DomainSessions24HPlusOne	Displays the total number of sessions in the past 24 hours plus one additional session.
\$DomainSessions24H	Displays the total number of sessions in the past 24 hours.

## User statistics

This data applies to all sessions attached to the user account.

Variable	Description
\$UserKBUp	Displays the total number of kilobytes uploaded.
\$UserKBDown	Displays the total number of kilobytes downloaded.
\$UserKBTot	Displays the total amount of kilobytes transferred.

Variable	Description
\$UserLoggedIn	Displays the total number of sessions.
\$UserUploadAvgKBps	Displays the average upload rate in KB/s.
\$UserDownloadAvgKBps	Displays the average download rate in KB/s.
\$UserAvg	Displays the average aggregate data transfer rate (uploads and downloads) in KB/s.
\$UserUploadKBps	Displays the current upload transfer rate in KB/s.
\$UserDownloadKBps	Displays the current download transfer rate in KB/s.
\$UserKBps	Displays the current aggregate data transfer rate in KB/s.
\$UserSessions24HPlusOne	Displays the total number of sessions in the past 24 hours plus one additional session.
\$UserSessions24H	Displays the total number of sessions in the past 24 hours.

## Last transfer statistics

This data applies to the most recently completed successful data transfer.

Variable	Description
\$TransferBytesPerSecond	Displays the effective (compressed) transfer rate in bytes/s.
\$TransferKBPerSecond	Displays the effective (compressed) transfer rate in KB/s.
\$TransferBytes	Displays the effective (compressed) number of bytes transferred, formatted for display, for example, 32,164.
\$NoFormatTransferBytes	Displays the effective (compressed) number of bytes transferred, unformatted, for example, 32164.
\$TransferKB	Displays the effective (compressed) number of kilobytes transferred, formatted for display.
\$ActualTransferBytesPerSecond	Displays the actual (uncompressed) transfer rate in bytes/s.
\$ActualTransferKBPerSecond	Displays the actual (uncompressed) transfer rate in KB/s.
\$ActualTransferBytes	Displays the actual (uncompressed) number of bytes transferred, formatted for display, for example, 32,164.

Variable	Description
\$NoFormatActualTransferBytes	Displays the actual (uncompressed) number of bytes transferred, unformatted, for example, 32164.
\$ActualTransferKB	Displays the actual (uncompressed) number of kilobytes transferred, formatted for display.
\$CompressionRatio	Displays the ratio of compression for the transfer expressed as a percentage of the expected amount of data transferred. 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	Displays the command result in the return response of any command, providing information such as compression level, and so on. (FTP only)
\$Command	Displays the FTP command name, such as RETR, MODE, or SIZE. (FTP only)
\$Parameters	Displays 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	Displays 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	Displays the current effective (compressed) number of bytes transferred so far, unformatted, for example, 32164. (FTP only)
\$CurrentUncompressedTransferBytes	Displays the current actual (uncompressed) number of bytes transferred so far, unformatted, for example, 32164. (FTP only)

## Date/Time

Variable	Description
\$Date	Displays the current date according to the Serv-U File Server, in the local date format of the system.

Variable	Description
\$Time	Displays the current time according to the Serv-U File Server, in the local time format of the system.
\$Day	Displays the day of the month.
\$Month	Displays the two-digit numeric month.
\$TextMonth	Displays the text version of the month.
\$Year	Displays the four-digit year.
\$2DigitYear	Displays the two-digit year.
\$Hour	Displays the hour (24-hour clock).
\$Minute	Displays the minute.
\$Second	Displays the second.

## Server settings

Variable	Description
\$MaxUsers	Displays the maximum number of sessions allowed to log in, which could be limited by the license.
\$MaxAnonymous	Displays the maximum number of anonymous users allowed to log in.


## Session information

This information applies to the current session.

Variable	Description
\$Name	Displays the login ID of the attached user account.
\$LoginID	Displays 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	Displays the client IP address.
\$IPName	Displays the reverse DNS name as obtained by performing a reverse DNS lookup on \$IP.

Variable	Description
\$Dir	Displays the session's current directory.
\$Disk	The local drive letter being accessed.
\$DFree	Displays the amount of free space on \$Disk in MB.
\$FUp	Displays the total number of files uploaded.
\$FDown	Displays the total number of files downloaded.
\$FTot	Displays the total number of files transferred, essentially (\$FUp + \$FDown).
\$BUp	Displays the total number of kilobytes uploaded.
\$Bdown	Displays the total number of kilobytes downloaded.
\$BTot	Displays the total number of kilobytes transferred.
\$TConM	Displays the total number of minutes the session has been connected.
\$TConS	Displays the number of seconds from 0 to 60 that the session has been connected, carries over to \$TconM.
\$RatioUp	Displays the 'upload' portion of the applied ratio, "N/A" if not in use.
\$RatioDown	Displays the 'download' portion of the applied ratio, "N/A" if not in use.
\$RatioType	Displays the type of ratio being applied, either per session or per user.
\$RatioCreditType	Displays the type of ratio credit granted for transfers, either per bytes or per complete file.
\$RatioCredit	Displays 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.

Variable	Description
\$SessionID	Displays 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	Displays 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	Displays the current domain that the session is logged into.
\$DomainDescription	Displays the description of the current domain that the session is logged into.
\$TimeRemaining	Displays the time remaining when blocking an IP address for an amount of time (available only in Event notifications).
\$LocalHomeDirectory	Displays the local home directory. It should only be used for events that need this specific information such as user creation.
\$Password	Displays the password associated with the user account. It is intended only for events. It should NOT be used for welcome messages.
\$UserEmailAddress	Displays the user's email address.
\$FullName	Displays 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	Displays the port number of the client.
\$ServerIP	Displays the IP address of the server.
\$ServerPort	Displays the port number of the server.

 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

This information applies to the last remotely accessed file, which is not necessarily the last transferred file.

Variable	Description
\$PathName	Retrieves the full remote path.
\$FileName	Retrieves only the file name from \$PathName.
\$FileSize	Retrieves the size, in bytes, of the file from \$FileName.
\$FileSizeFmt	Displays a formatted version of the file size, containing the thousands separator (comma or period depending on the computer's regional settings).
\$FileSizeKB	Displays 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 <code>C:\Temp\File.fid</code> instead of <code>/Temp/file.fid</code> .
\$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

Variable	Description
\$UNow	Displays the current number of sessions on the Serv-U File Server.
\$UAll	Displays the total number of sessions that have connected to the Serv-U File Server since it was last started.
\$U24h	Displays the total number of sessions that have connected to the Serv-U File Server in the last 24 hours.
\$UAnonAll	Displays the current number of sessions attributed to the anonymous user on the Serv-U File Server.

Variable	Description
\$UAnonThisDomain	Displays the current number of sessions attributed to the anonymous user on the connected domain.
\$UNonAnonAll	Displays the current number of sessions not attributed to the anonymous user on the Serv-U File Server.
\$UNonAnonThisDomain	Displays the current number of sessions not attributed to the anonymous user on the connected domain.
\$UThisName	Displays the current number of sessions attributed to the connected user account.

## FileShare

Variable	Description
\$FileShareExpires	Displays the link expiration date.
\$FullName	Displays the Serv-U username of the user who shared the file.
\$FileShareTokenURL	Displays the fileshare URL.
\$FileShareComments	Displays an optional message.