solarwinds

SolarWinds

Serv-U File Server

Adminstration Guide

Version: 15.1.5

Last updated: 2/13/2017

Table of Contents

Tips and tricks

- To confirm that a file transfer has been completed, configure a Serv-U event to receive notifications about successful file transfers. For information about configuring events, see Domain events.
- Use $ macros for events and in system messages (such as login messages or customized FTP responses) and % macros for configuration values. For more information about macros, see System variables and Directory access rules.
- To automatically add new users to a group, use a user template in which a default group is specified. For information about setting up user templates, see User accounts.
- Organize user accounts into collections to make account management more logical and organized. For information about creating user collections, see User accounts.
- To limit user access to client views, modify the system settings that control client view accessibility. For more information about configuring limits and settings, see Server limits and settings.
- To send emails to multiple recipients and to groups when an event (such as a file transfer) occurs, configure email actions. For more information, see Domain events.
- To back up your Serv-U configuration, save the following files and folders:
  - `serv-u.archive` file
  - `Users` folder
  - `serv-uid.txt` file
- To identify the user's home directory, use the `%DOMAIN_HOME%` macro. For example, to place a user's home directory into a common location, use `%DOMAIN_HOME%\%USER%`. For more information, see User information.
- 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. For more information about setting encryption levels, see Configure server encryption.
- To control access to virtual paths, configure virtual paths for individual users or groups. For more information, see Virtual paths.

- To override default system limits when configuring the file server, create a new limit. The value of the new limit takes precedence over the default value. For more information, see Server limits and settings.

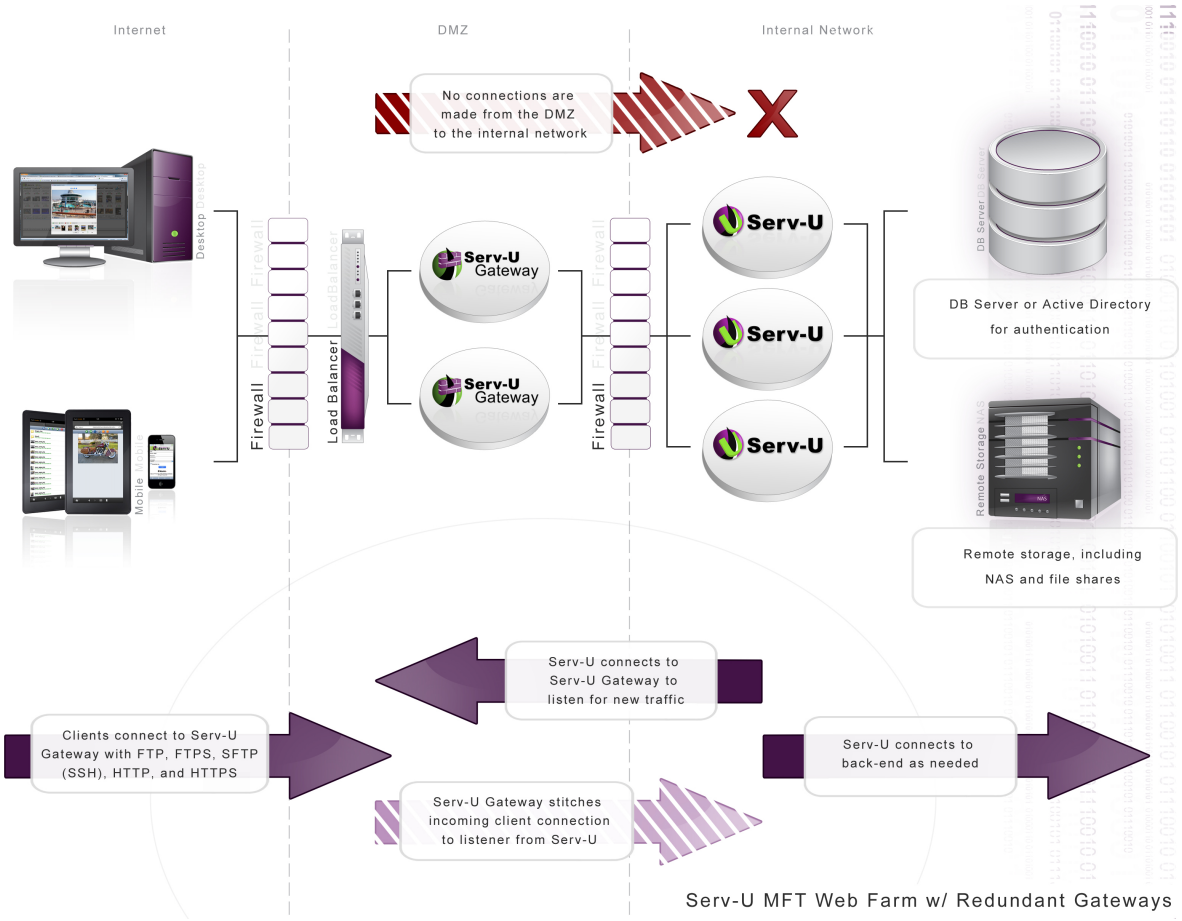
Serv-U File Server

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

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

In addition to Serv-U's support for a large collection of 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. Server administrators looking to provide a full-featured FTP client to users who may not have an FTP client license of their own can even license FTP Voyager JV. FTP Voyager JV is a Java-enabled FTP client delivered to the user after logging in to their Serv-U account.

The following graphic shows a high level overview of a Serv-U deployment.



Using the 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 Serv-U MFT Server 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.

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

Serv-U editions

Serv-U is available in two editions:

Serv-U 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.

Serv-U MFT Server

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

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.

Purchase options

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

You can purchase a license online at the Serv-U website. Choose which edition of the Serv-U File Server is required and the quantity to purchase. Discount pricing applies for bulk purchasing. You must purchase a 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 Serv-U Sales web 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

solarwinds

System requirements

Hardware requirements

The hardware requirements are modest, but Serv-U can take advantage of multi-core processors and multiple processor architectures.

HARDWARE	MINIMUM REQUIREMENT
CPU	1 GHz+
RAM	256 MB+
Network	10/100 Mbps NIC
Hard drive space	30 MB
Video	128 MB Video RAM

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

HARDWARE	MINIMUM REQUIREMENT FOR MODEST TRAFFIC
CPU	2 GHz+ multi-core
RAM	2 GB+
Network	10/100/1000 Mbps NIC
Hard drive space	120 GB
Video	128 MB Video RAM

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

HARDWARE	MINIMUM REQUIREMENT FOR HIGH TRAFFIC
CPU	Multiple 3.2 GHz+ multi-core

Hardware	Minimum requirement for high traffic
RAM	4 GB+
Network	10/100/1000 Mbps NIC
Hard drive space	120 GB
Video	128 MB Video RAM

Operating system and software requirements

Operating system or software	Requirement
Microsoft Windows	• Windows Server 2012 • Windows Server 2012 RC2 • Windows Server 2008, 2008 SP2, 2008 R2, and 2008 R2 SP1 - 64 bit versions only
Linux	• Red Hat Enterprise Linux (RHEL) v.7.2 (Recommended) • Fedora 24 • Ubuntu 16.04 • CentOS 7.2 • OpenSUSE 42.1
Database server (optional)	• MS SQL 2014 • MS SQL 2012, 2012 SP1 • MySQL 5.7 • PostgreSQL: 9.5
LDAP server (optional)	• Active Directory - same as Windows Server support • Open Directory 4 • OpenLDAP 2.4

Client requirements

The default web browser on many mobile devices can be used to transfer files, work with files and folders, or run the web-based Management Console of Serv-U.

DEVICE	SUPPORTED FUNCTIONALITY
Apple iPhone 5+	Download, manage, and preview files.
Apple iPad 2	Download, manage, preview files, and run the Management Console.
Google Android 4.0 (Ice Cream Sandwich)	Upload, download, manage, and preview files.

The following major browsers are supported with the basic web client, for file management and for web administration purposes:

- Microsoft Internet Explorer 11
- Mozilla Firefox: latest version
- Safari 6+
- Google Chrome: latest version

Java Runtime Environment (JRE) 7 and 8 are supported for Web Client Pro and FTP Voyager JV.

Notes:

- To be able to use Web Client Pro and FTP Voyager JV, Java must be installed and enabled in the browser.
- Web Client Pro does not work on Linux in Google Chrome version later than 35 due to an incompatibility between Chrome and the Java browser plug-in.
- Apple users must have at least Mac OS X 10.6 installed.

Server concepts

Serv-U File Server makes use of several concepts that help you understand how to configure and administer your file server as a single, hierarchical unit. Serv-U File Server contains four related levels of configuration: the server, the domain, the group, and the user. Only the group level is optional. The other levels are mandatory parts of the file server.

Server

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

Domain

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

Group

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

User

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

User collection

Contrary to groups, a user collection does not offer any level of configuration to the user accounts they contain. Instead, a user collection offers a way to organize users into containers for easy viewing and administration. For example, collections can be created to organize user accounts based on group membership. User collections must be maintained manually when user accounts change group membership.

Glossary

Listener

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

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.

Event

A Serv-U 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 events are used to automate behavior and to provide greater visibility of important file transfer processes.

Anti-hammering

A Serv-U 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.

IP access rules

IP access rules are used in Serv-U 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. Rules set up at the group and user levels define who can connect using a given user account.

Directory access

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.

Quick start guide

Install Serv-U File Server

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 on the License Management tab. Refer to Serv-U licenses now available in Customer Portal for steps to access this information.

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

Upgrade Serv-U

Before upgrading, create a backup of the original installation folder, your database, and your configuration data.

OPERATING SYSTEM	LOCATION OF CONFIGURATION FILES
Windows Vista Windows 7 Windows 8 Windows Server 2008 Windows Server 2012	`C:\ProgramData\RhinoSoft\Serv-U` The location is hidden by default.
Windows XP Windows Server 2003	`C:\Program Files\RhinoSoft\Serv-U`
Linux	`/usr/local/Serv-U`

If you experience issues with the Serv-U Management Console after upgrading, clear your browser cache.

Create domains

When the Serv-U Management Console finishes loading, you are prompted to create a new domain if no domains exist.

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

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

Click Yes to start the domain creation wizard. You can run this wizard any time by clicking + (New Domain) at the top of the Serv-U Management Console.

1. Click + (New Domain).
2. Type a unique name and an optional description for the new domain.

   The domain name is not visible to any of its users, and it does not affect the way the domain is accessed. The name makes the identification and management of the domain easier for administrators. The name must be unique.

3. To make the domain temporarily unavailable to users while you are configuring it, clear the Enable domain check box, and click Next.

4. Select File Transfer Domain, File Sharing Domain, or both, and click Next.
   - If you are setting up a File Transfer Domain only, perform the following steps:
     a. On the Protocols page, select the protocols and port numbers the domain should use to provide access to its users, and click Next.

        The standard file sharing protocol is FTP, which operates on the default port 21. However, you can change any of the available ports to a custom value. To run the server on a non-default port, SolarWinds recommends you use a port above 1024.

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

        If you do not specify an address, Serv-U uses any available IP address on the computer.

     c. On the Encryption page, select the encryption mode to use when storing passwords on the domain.
     d. To enable users to recover their passwords, select the appropriate option.
     e. Click Finish to create the domain.

- If you are setting up a File Sharing Domain only, perform the following steps:
    a. On the File Sharing page, specify the domain URL, the file sharing repository, and whether to use a secure URL.
    b. Click Configure SMTP to set up an SMTP server, which is necessary for sending email notifications and for events that use email actions.
    c. Click Next.
    d. On the IP Listeners page, specify the IP address that is used to connect to this domain.

    > If you do not specify an address, Serv-U uses any available IP address on the computer.

    e. Click Finish to create the domain.

- If you are setting up a File Transer and File Sharing Domain, perform the following steps:
    a. On the File Sharing page, specify the domain URL, the file sharing repository, and whether you want to use a secure URL.
    b. Click Configure SMTP to set up an SMTP server, which is necessary for sending email notifications and for events that use email actions.
    c. Click Next.
    d. On the Protocols page, select the protocols and port numbers the domain should use to provide access to its users, and click Next.

    > The standard file sharing protocol is FTP, which operates on the default port 21. However, you can change any of the available ports to a custom value. To run the server on a non-default port, SolarWinds recommends you use a port above 1024.

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

    > If you do not specify an address, Serv-U uses any available IP address on the computer.

    f. On the Encryption screen, select the encryption mode to use when storing passwords on the domain.
    g. To enable users to recover their passwords, select the appropriate option.
    h. Click Finish to create the domain.

Create user accounts

After your first domain is created, you are taken to the user's page of the Serv-U Management Console. Click Yes to start the User Wizard and create a new user account.

You can run this wizard at any time by navigating to the Users menu under Global or Domain, and then clicking Wizard on the Users page.

First, provide a login ID for the account. The login ID must be unique for the domain. Other domains on your server can have an account with the same login ID.


To create an anonymous account, specify `anonymous` or `ftp` as the login ID.

You can also specify a name and email address for the user account. The email address is used by Serv-U to send email notifications and recovered passwords to the user account. Click Next to continue.

After specifying a unique login ID, you must also specify a password for the account. You can leave this field blank, but that allows anyone who knows the login ID to access your domain. Click Next to continue.

The third step is to specify a home directory for the account. The home directory is the location on the hard drive of the server, or on an accessible network resource that the user account is placed in after a successful login. It is the location you want the user account to use when sending and receiving files on the server. Type the location or click Browse to select a location on the hard drive. If users are locked in their home directory, they cannot access files or folders above the directory structure of their home directory. Additionally, the actual location of their home directory is masked and displayed as "/". Click Next to proceed to the last step.

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

After selecting the directory access rights, click Finish to create the user account.

Serv-U File Server is now accessible and ready for sharing. You can create more accounts just like this one to share with friends, family, or colleagues. Each user can have a different home directory. This way you can share different files with different people.

The Serv-U Management Console is designed to provide quick and easy access to the configuration options of the file server in a familiar way. When viewing a

configuration page, you can return to the main Management Console page at any time by clicking the Serv-U File Server logo in the top-left corner.

Management Console layout

The Management Console is presented with an accordion list on the left and the global dashboard on the right. The accordion menu contains the name of the server on top, and then the list of configured domains. The global dashboard contains the session statistics, the server log, information about the active sessions, and it also provides direct access to the thwack community.

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

Domain administrators only have access to configuring settings and options for their particular domain, and do not have access to the server-level categories that are displayed to system administrators.

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

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

Launch the Web Client

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

To use FTP Voyager JV, you must install the Java Runtime Environment.

User interface conventions

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.

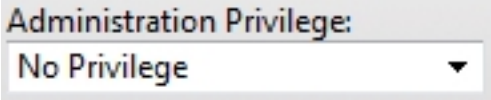
When an option inherits its value from a parent, the text of the option is displayed in

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.

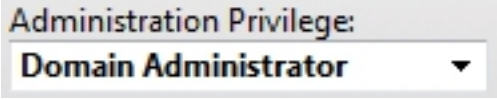
However, if the value is overriding the default, the text of the value is displayed in **bold**. The value that is currently displayed is always the value of that option, regardless of changes to its parent.

Example use case

Example Technology is a computer repair company that maintains a 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.



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.



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.

Server

If you configure a setting at the server level, the setting applies to all users, groups, and domains on the server unless it is 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.

Server details

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

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

Specifying IP access masks

IP access rules use masks to authorize IP addresses and domain names. The masks can contain specific values, ranges, and wildcards made up of the following elements.

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

VALUE OR WILDCARD	EXPLANATION
	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`.

Caveats

Specific IP addresses listed in Allow rules will not be blocked by anti-hammering. These IP addresses are white-listed. However, addresses matched by a wildcard or a range are subject to anti-hammering prevention.

Implicit deny all

Until you add the first IP access rule, connections from any IP address are accepted. After you add the first 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.

Matching all addresses

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.

DNS lookup

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 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.

Rule use during connection

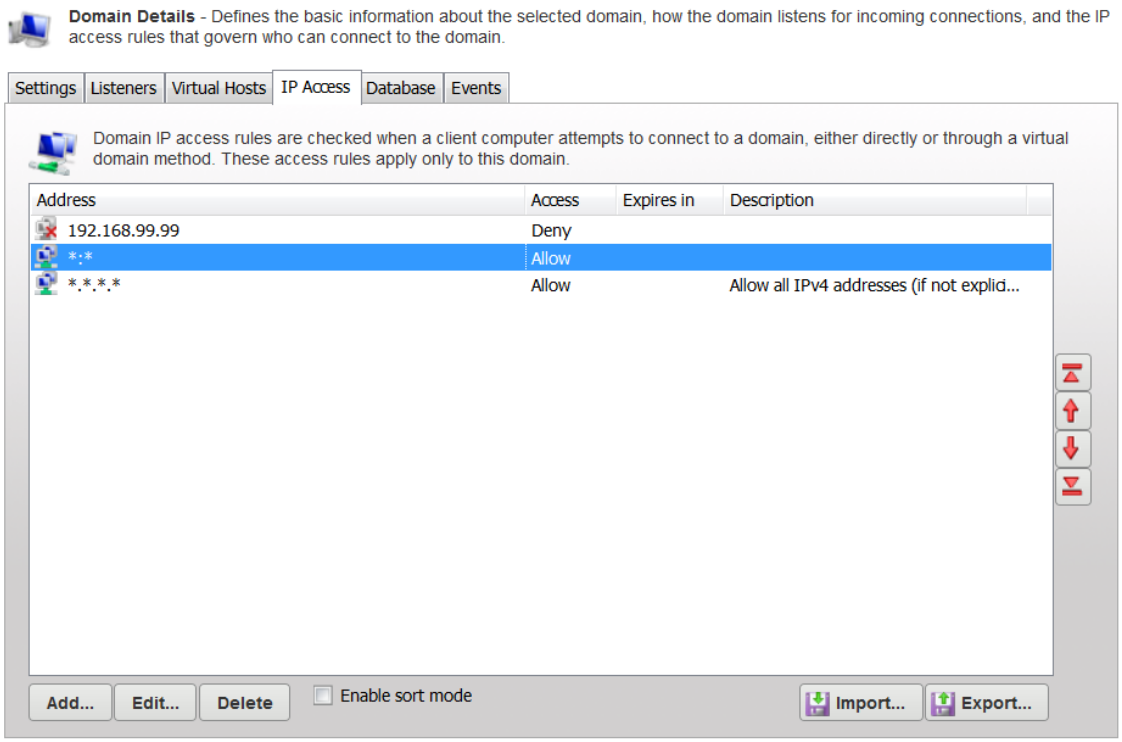
The level at which you specify an IP access rule also defines how far a connection is allowed before it is rejected. Server and domain level IP access rules are applied before the welcome message is sent. Domain level IP access rules are also applied when responding to the `HOST` command to connect to 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.

Anti-hammering

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. You can configure an anti-hammering policy server-wide in Server Limits and Settings > Settings and domain-wide in Domain Limits and Settings > Settings.

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.

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



IP access list controls

The following options are available on the IP Access page.

Using the sort mode

You can 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.

Importing and exporting IP access rules

You can export and import Serv-U IP access rules from users, groups, domains, and the server by using a text-based `.csv` file. To export IP access rules, view the list of rules to export, click Export, and specify the path and file name you want to save the list to. To import IP access rules, click Import and select the file that contains the rules you want to import. The `.csv` file must contain the

following fields, including the headers:

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

Examples of IP address rules

Office-only access

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 access rule 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 provides an implicit Deny All rule at the end of the list.

Prohibited computers

Users should normally be able to access Serv-U 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 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.

DNS-based access control

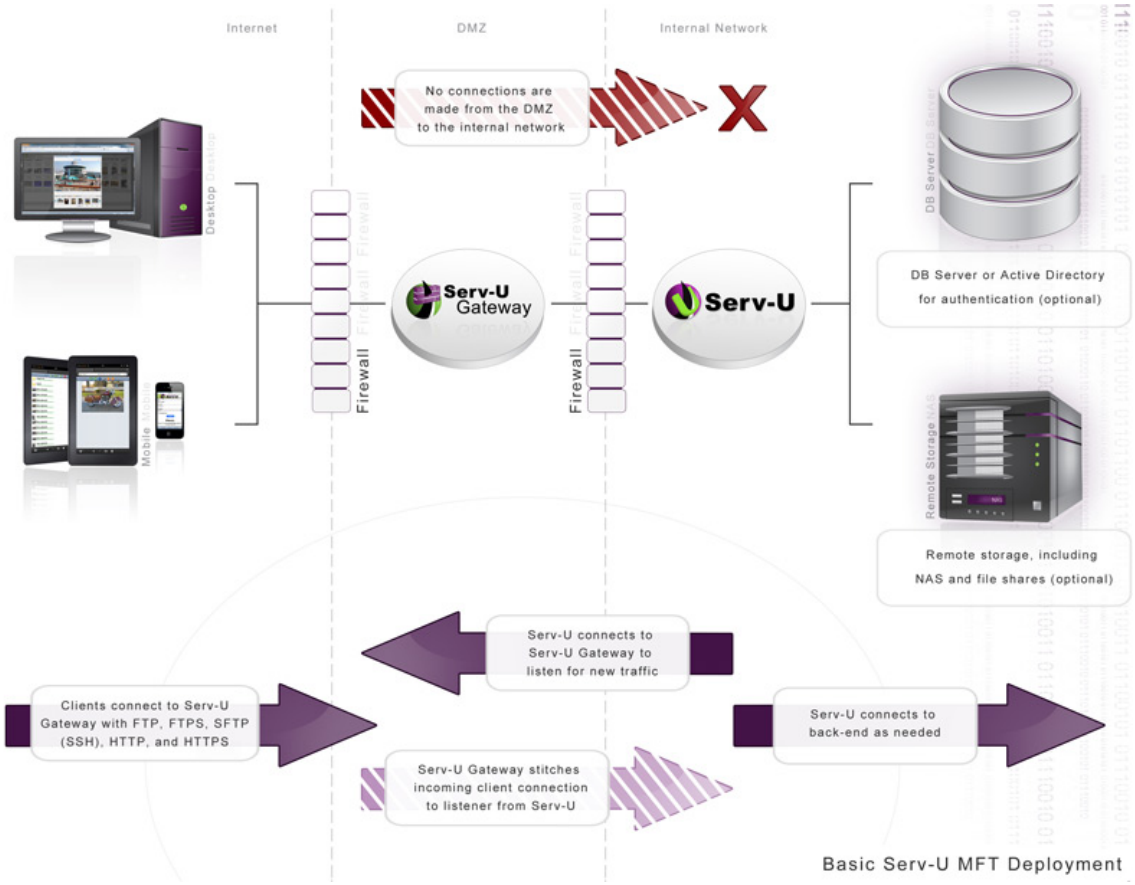
The only users allowed to access a Serv-U domain connect from `*.example.com` or `*.example1.com`. The related Serv-U access rules should be `Allow *.example.com` and `Allow *.example1.com` in any order, and these rules should be added to the domain IP access rules. No deny rule is required because Serv-U provides an implicit Deny All rule at the end of the list.

Serv-U Gateway

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

It acts as a reverse proxy in demilitarized zone (DMZ) segments and prevents your Serv-U deployments from storing data in the DMZ, or opening connections from the DMZ to the internal network.

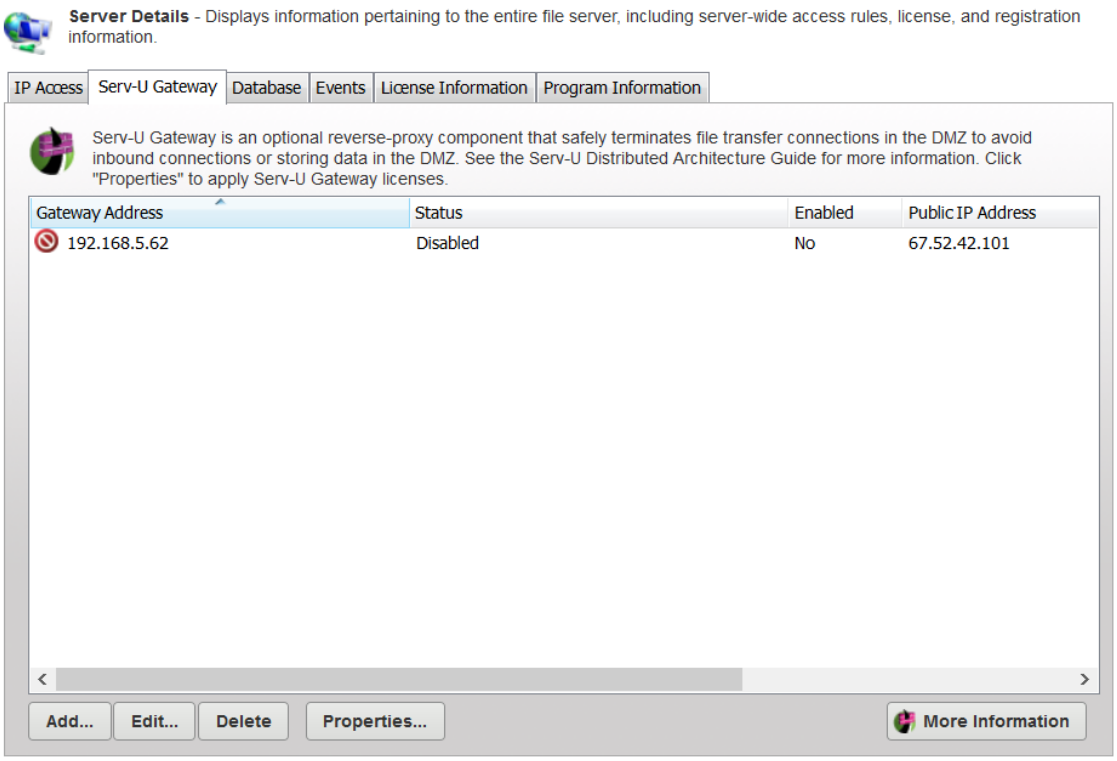
This type of architecture is essential to meet Payment Card Industry Data Security Standard (PCI DSS), managed file transfer, and other high-security requirements.



Serv-U Gateway deployment documentation

- Serv-U distributed architecture guide
- Serv-U Gateway installation instructions
  - For Windows
  - For Linux
- Plan your Serv-U Gateway deployment

Serv-U Gateway tab



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

Gateway Address column

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

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.

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

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.

Public IP Address column

The Public IP Address column shows the IP address file transfer clients should connect to.

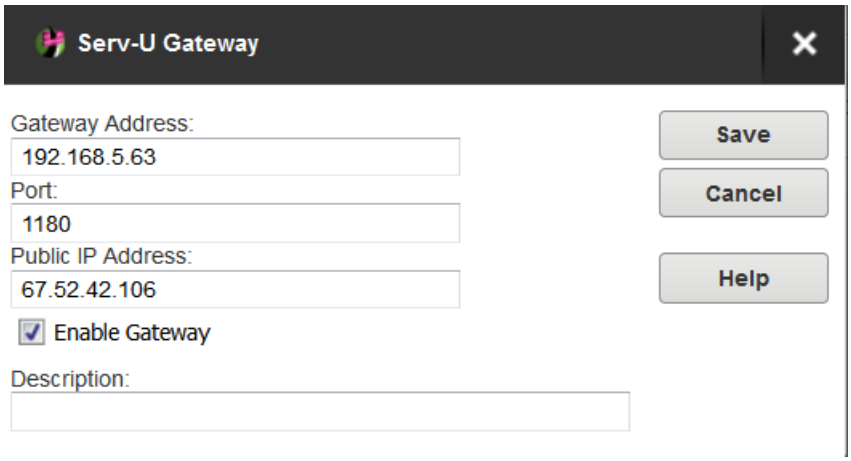
A private IP address is displayed in the Public IP Address column if a private IP address was explicitly configured in the gateway. This occurs if the gateway has no public IP addresses, which is common during trials and situations in which the gateway is placed behind network address translation (NAT).

Description column

The Description column displays any note that is added to the gateway configuration. It does not affect behavior.

Manage gateways

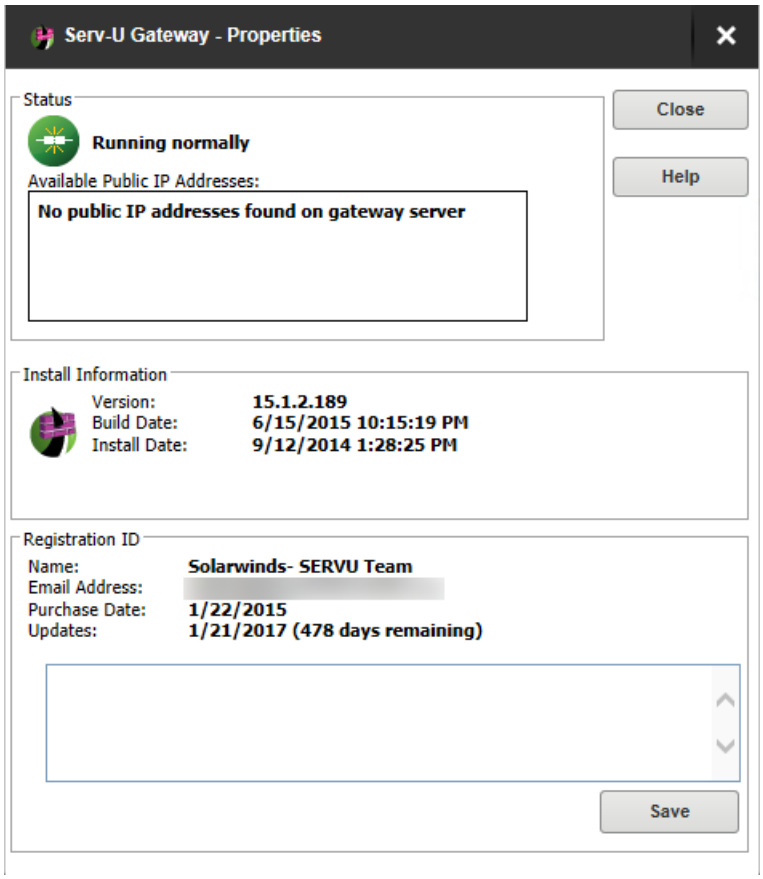
Click Add, Edit, or Delete to manage gateway configurations.



- Gateway Address is the IP address on the Serv-U Gateway that Serv-U uses to communicate with Serv-U Gateway. This should almost always be a private IP address.
- Port is the TCP port on the Serv-U Gateway that Serv-U uses to communicate with Serv-U Gateway. The default is TCP port 1180.
- Public IP Address should contain 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).
- The Enable Gateway option is used to turn the gateway on and off. The default is selected.
- Description is an optional note about the gateway. It has no effect on the behavior.

Serv-U 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 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.

The Available Public IP Addresses field contains a list of all the public IP addresses automatically detected on Serv-U Gateway. If a private address 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 Serv-U Gateway software running on the gateway, the date Serv-U Gateway was installed or last updated, and, if applicable, the number of days left in the evaluation period.

Registration ID

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

If you have lost your registration ID, visit the Online Customer Service Center to retrieve it.

Database access

Serv-U enables the use of an Open Database Connectivity (ODBC) database to store and maintain group and user accounts at the domain and server levels. You can configure the ODBC connections in two locations:

- Domain > Domain Details > Database
- Server > Server Details > Database.

Serv-U can automatically create all of the tables and columns necessary to begin storing users and groups in the database. Because Serv-U uses one set of table names to store its information, individual ODBC connections must be configured for each item which stores details in the database. In other words, the server and each domain must have a unique ODBC connection to ensure they are stored separately.

Configure a database

1. Create an ODBC connection for Serv-U to use. SolarWinds recommends MySQL, but you can use any database that has an ODBC driver available. Use a System data source name (DSN) if Serv-U is operating as a system service, or a User DSN if Serv-U is operating as a regular application.
2. Open the Serv-U Management Console and browse to the appropriate domain or server database settings. Enter the required information, and click Save.

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

SQL templates

Serv-U uses multiple queries to maintain the databases that contain user and group

information. These queries conform to the Structured Query Language (SQL) standards. However, if your database has problems working with Serv-U, you may need to alter these queries. In the SQL Templates window, you can modify each query used by Serv-U to conform to the standards supported by your database.

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

User and group table mappings

By default, Serv-U 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 to an existing database that contains this information, you must customize the table and column names to conform to the existing database structure. Click User Table Mappings or Group Table Mappings to get started.

Serv-U stores information for a user or group in 10 separate tables. Only the User/Group Info Table and User/Group Dir Access Table are required. 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.

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 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 Serv-U Management Console through scripted database operations which can be built into many existing account provisioning systems. A DSN must first be created in Control Panel > Administrative Tools > ODBC Data Sources. Use a System DSN if Serv-U is running as a service or a User DSN if Serv-U is running as an application. After you create the appropriate DSN, enter the required information and click Save. Serv-U creates the tables and columns. You can manage database users and groups in the Database Users and Database Groups pages of Serv-U, located near the normal Users and Groups pages.

Data source name creation in Linux

Database access in Serv-U on Linux follows the same method as Serv-U 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
- postgressql-odbc
- unixodbc

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

```
[MySQL-test]
Description = MySQL test database
Trace = Off
TraceFile = stderr
Driver = MySQL
SERVER = YOURIPADDRESS
USER = USERNAME
```

```
PASSWORD = PASSWORD
PORT = 3306
DATABASE = YOURDATABASE

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

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.

Domain events

You can automatically create a list of the most common events. You can choose to create these common events using email or balloon tip actions. Click Create Common Event on the Events page. Select the Send Email or Show balloon tip option for the action you want to perform on the common events. If you choose to send email, enter an email address.

> The Write to Windows Event Log and Write to Microsoft Message Queue (MSMQ) options are available for Windows only.

Event actions

You can select from the following actions that are executed when an event is triggered:

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

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

Email actions

You can configure email actions to send emails to multiple recipients and to Serv-U groups when an event is triggered.

To add an email address, enter it in the To or Bcc fields. To send emails to a Serv-U group, use the Group icon to add or remove Serv-U groups from the distribution list. Separate email addresses by commas or semicolons. Email actions contain a To, Subject and Message parameter. You can use special variables to send specific data pertaining to the event. For more information about the variables, see System variables.

To use email actions, you must first SMTP configuration.

Balloon tip actions

You can configure a balloon tip to show in the system tray when an event is triggered. Balloon tip actions contain a Balloon Title and a Balloon Message parameter. You can use special variables to send specific data pertaining to the event. For more information about the variables, see System variables.

Execute command actions

You can configure execute command actions to execute a command on 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 for no waiting.

Time spent waiting delays any processing that Serv-U can perform.

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

Windows Event Log

By writing event messages to a local Windows Event Log, you can monitor and record Serv-U activity by using third-party network management software. All messages appear in the Windows Application Log from a source of Serv-U.

This event has only one field:

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

Microsoft Message Queuing (MSMQ)

Microsoft Message Queuing (MSMQ) is an enterprise technology that provides a method for independent applications to communicate quickly and reliably. Serv-U 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.

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 attempts to create it. This normally only works on public queues on the local machine. You can also use Serv-U 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 system variables can also be used in this field. This field may be left blank, but usually is not.

Microsoft message queues created in Windows do not grant access to SYSTEM by default, preventing Serv-U 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 runs) has permission to the queue.

Event filters

Use event filters to control when a Serv-U event is triggered. By default, events trigger each time the event occurs. The event filter allows events to be triggered only if certain conditions are met. For example, a standard 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. For example, you can configure a File Uploaded event to only send an email when the file name contains the string `important`, so an email would be sent when the file `Important Tax Forms.pdf` is uploaded but not when other files are uploaded to the server. Additionally, you can 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.

Event filter fields

Each event filter has the following critical values that must be set:

- Name: This is the name of the filter, used to identify the filter for the event.
- Description (Optional): This is the description of the event, which may be included for reference.
- Logic: This determines how the filter interacts with other filters for an event. In most cases, AND 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).
- Filter Comparison: This is the most critical portion of the filter. The Filter Comparison contains the evaluation that must occur for the event to trigger. For example, a filter can be configured so that only the user *admin* triggers the event. In this case, the comparison is `If $Name = (is equal to) admin`, and the data type is `string`. For bandwidth, either an unsigned integer or double precision floating point value is used.

Event filters also support wildcards when evaluating text strings. The supported wildcards include:

- `*` - 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`.

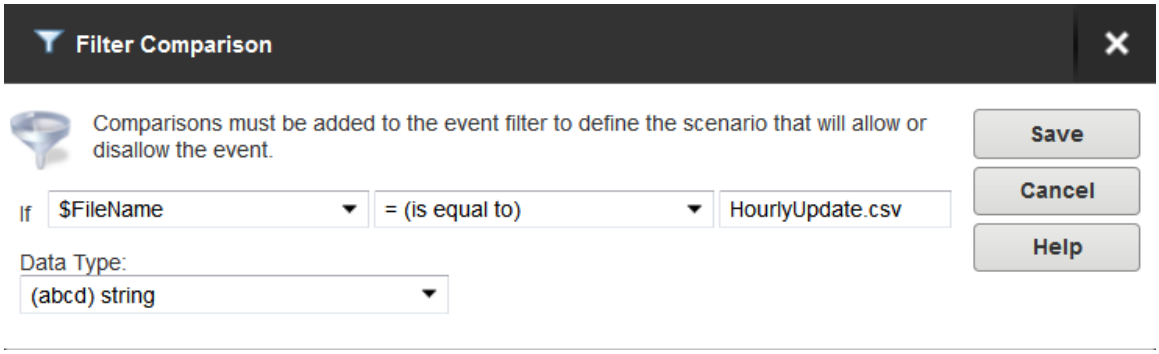
- `[]` - The bracket wildcard matches a character against the set of characters inside the brackets. For example:
  - An event filter that compares the `$FileName` variable to the string `data[687].txt` matches files named `data6.txt`, `data7.txt` and `data8.txt` but not `data5.txt`.
  - An event filter that compares the `$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.

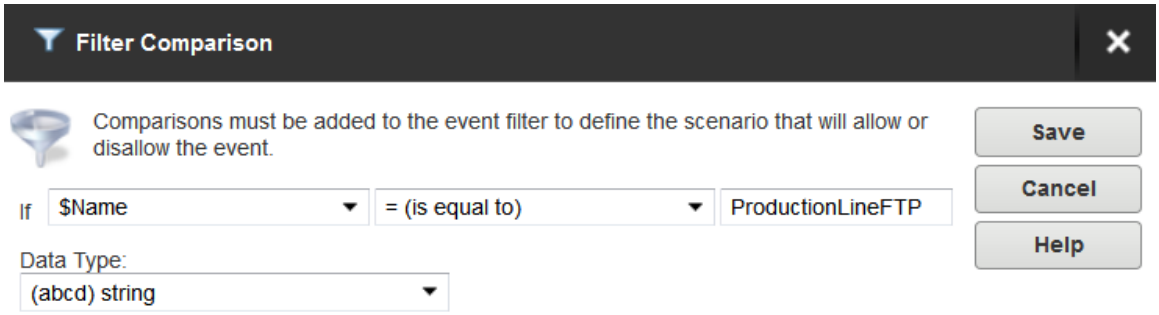
Event filters

Event filters are used by comparing fields to expected values in the Event Filter menu. The best example is raising an event only when a certain user triggers the action, or when a certain file is uploaded. For example, 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:

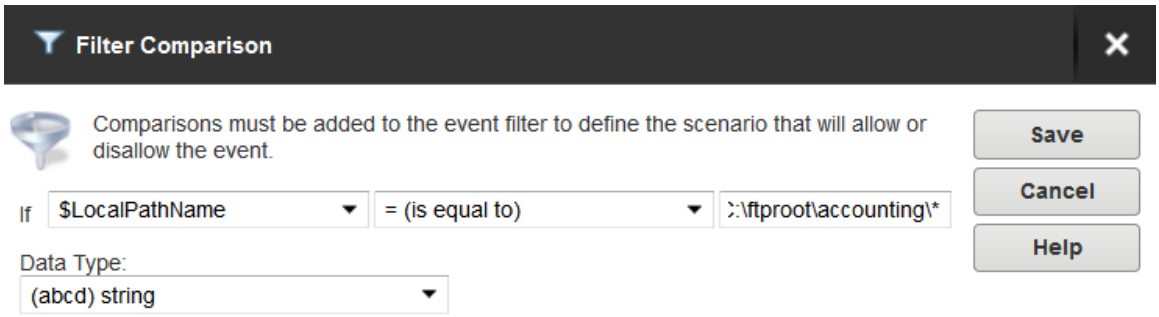


As another example, it may be necessary to know when a file transfer fails for a specific user account. To perform this task, create a new File Upload Failed event, and add a new filter.

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



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\`.



License information

The License Information tab displays the information contained in the current registration ID in use by 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 edition	The Serv-U edition that is enabled by the current license. For more information, see Serv-U editions.
Copies	The number of concurrent installations allowed by the current license.
Purchase date	The date the current license was purchased.
Updates	The date through which the current license allows free updates to the latest version. If Serv-U is running as a trial version, the number of trial days remaining is displayed.
Additional products	Additional add-ons for Serv-U, and whether they are enabled.
Edition information	The enabled functionality and limitations of the licensed Serv-U edition.

Serv-U registration

To register Serv-U File Server, click Enter License ID on the bottom toolbar, and enter your alphanumeric registration ID. If you lost your ID, click Lost ID to retrieve it. If you want to purchase an ID, click Purchase to visit the Serv-U website. To upgrade, click Upgrade License.

Program Information

The Program Information page displays information about the current version of Serv-U installed on the server.

SMTP configuration

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 in the Events tab on the Domain Details and Server Details pages.

Click Configure SMTP to launch the dialog.

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 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.

ERROR MESSAGE	EXPLANATION
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.
Timeout while contacting SMTP server. Please check that the SMTP server address is correct.	The connection to the SMTP server timed out.

Directory access rules

Directory access rules define the areas of the system which are accessible to user accounts. While traditionally restricted to the user and group levels, in Serv-U, the usage of directory access rules is extended to both the domain and the server levels through the creation of global directory access rules. Directory access rules specified at the server level are inherited by all users of the file server. 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 they are listed. The first rule in the list that matches the path of a client's request is the one that is applied for that rule. In other words, if a rule exists that denies access to a particular subdirectory but is listed below the rule that grants access to the parent directory, then a user still has access to the 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 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.

File permissions

PERMISSION	DESCRIPTION
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	DESCRIPTION
	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 permissions

PERMISSION	DESCRIPTION
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 permissions

PERMISSION	DESCRIPTION
Inherit	Allows all subdirectories to inherit the same permissions as the parent

PERMISSION	DESCRIPTION
	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.

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, you can configure the Serv-U File Server service to run under a network account. The alternative, preferred when many servers exist, or if the Serv-U File Server service 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.

> 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.

Quota permissions

Maximum size of directory contents

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

changes made to the directory contents outside of a user's file server activity.

Mandatory access control

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.

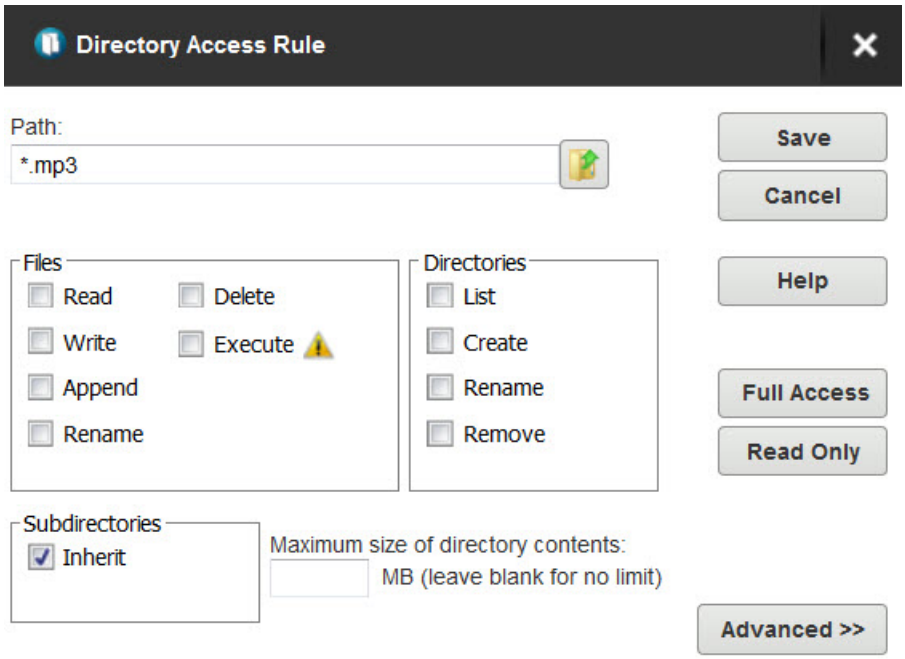
In the following example, the rule applies to `C:\ftproot\`.

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 Serv-U File Server.

Restrict file types

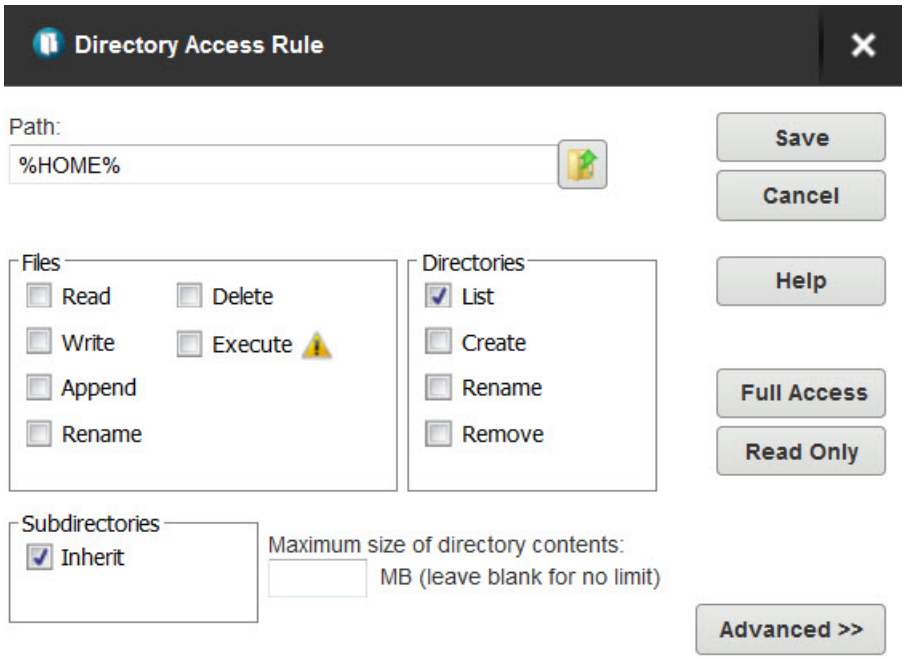
If users are using storage space on the Serv-U File Server to store non-work-related files, such as .mp3 files, you can prevent this by configuring a directory access rule placed above the main directory access rule to prevent .mp3 files from being transferred as shown below.

In the text entry for the rule, type `*.mp3`, and use the permissions shown beolw:



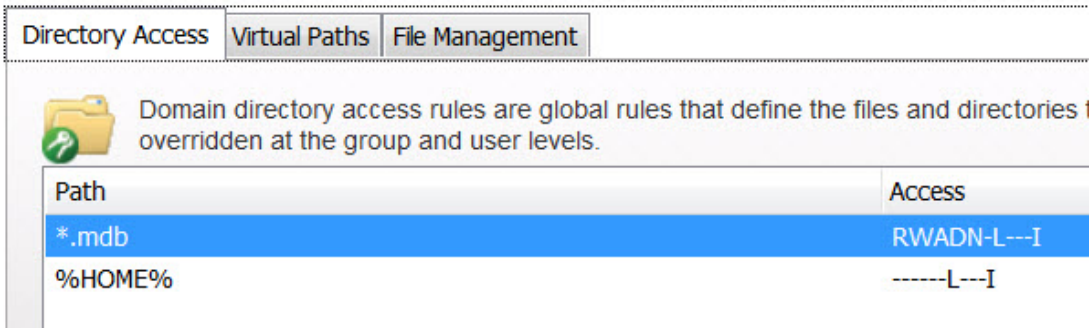
The rule denies permission to any transfer of files with the `.mp3` extension and can be modified to reflect any file extension. Similarly, if accounting employees only need to transfer files with the `.mdb` extension, configure a pair of rules that grants permissions for `.mdb` files but denies access 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.



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

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.



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. When virtual paths are created at the domain level, they are only accessible by users belonging to that domain.

You can also create virtual paths specifically for individual users or groups.

Physical path

The physical path is the actual location on the system, or network, that is to be placed in a virtual location accessible by a user. If the physical path is located on the same computer, 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 that the physical path should appear in for the user. The `%HOME%` macro is commonly used in the virtual path to place the specified

physical path in the home directory of the user. When specifying the virtual path, the last specified directory is used as the name displayed in directory listings to the user. For example, a virtual path of `%HOME%/public` places the specified physical path in a folder named `public` within the user's home directory. 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.

Virtual paths example

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 example

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.

Automated file management

Using file management rules, you can automatically remove or archive files from the file server. You can configure automated 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 uses the creation or change date of files to determine the expiration date. On Windows, the creation date of the file is used to determine when a file expires. On 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. This way you can manage files that are transferred by clients, or that are copied to the folder outside of Serv-U.

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 deletes or moves an expired file.

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

Define a new file management rule

1. Navigate to Directories > File Management, and click Add.
2. Type the path to the file or folder in the Directory Path field, or click Browse to navigate to the file or folder.

3. Select the action you want to perform on the file:
    a. If you want to delete the file after it expires, select Delete file(s) after specified time.
    b. If you want to move the file after it expires, select Move file(s) after specified time, and then 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 regularly checks each file in the directory for its age, and performs the specified action on the files that meet the age criteria you specify.

Server limits and settings

Serv-U contains options which you can use to customize how Serv-U can be used, and which also provide ways to apply limits and custom settings to users, groups, domains, and the server in its entirety. The limits stack intelligently, with user settings overriding group settings, group settings overriding domain settings, and domain settings overriding server settings. In addition, you can configure limits so that they are only applied during certain days of the week or times of the day. You can also grant exceptions to administrators and restrict specific users more than others, providing total control over the server. The limits and settings in Serv-U consist of the following categories:

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

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

1. In the Serv-U Management Console, click Limits & Settings.
2. From the Limit Type list, select the Directory Listing.
3. Click Add.
4. From the Limit list, select Lock users in home directory.
5. Deselect the option.
6. Click Save.

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

You can delete limits by selecting them and clicking Delete. To edit an overridden value, select the limit, and then click Edit.

Default rules cannot be edited or deleted. Create a new limit to override a default limit.

To create a limit that is restricted to a specific time of day, or specific days of the week, click Advanced in the New Limit or Edit Limit window. Select Apply limit only at this time of day to specify a start and stop time for the new limit. To restrict the limit to certain days of the week, deselect the days for which you do not want the limit applied. When a limit is restricted in this way, default values (or the value of other limit overrides) are applied when the time of day or day of the week restrictions are not met for this limit.

Server settings

On the Server Limits & Settings > Settings pages, you can configure basic server settings that affect performance, security, and network connectivity. To configure a setting, type the value you want in the appropriate area, and then click Save. This

topic contains detailed information about the settings that 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 IP addresses for the specified number of minutes 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 given to the client.

Default Web Client

Specifies whether the Web Client, Web Client Pro, or FTP Voyager JV 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.

Network settings

Auto-configure firewall through UPnP (Windows Only)

When enabled, Serv-U automatically configures the necessary port forwards in your UPnP-enabled network device (usually a router) so that the file server is accessible from outside your network. This is particularly useful in enabling

PASV mode FTP data transfers.

Packet time-out

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

PASV Port Range

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

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

Other settings

Ratio Free Files

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

Change Admin Password

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

FTP settings

In the Serv-U File Server, you can customize the FTP commands that Serv-U accepts, and you can also customize the responses of Serv-U to the FTP commands it receives.

If you configure these options at the server level, all domains inherit the customizations. 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 have the domain revert back to the default settings of the server.

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

Global properties

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

FTP Responses

Global FTP responses are responses shared amongst most FTP commands, such as the error message sent when a file is not found. Customizing a global FTP response ensures that the response is used by all other FTP commands rather than having to customize it for each individual FTP command. FTP command responses can contain special macros that allow real-time data to be inserted in to the response. For more information, see System variables.

Message File

The server welcome message is sent in addition to the standard "220 Welcome Message" that identifies the server to clients when they first connect. If the Include response code in text of message file option is selected, 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

Block "FTP_bounce" attacks and FXP (server-to-server transfers): Select this option to block all server-to-server file transfers involving this Serv-U File Server by only allowing file transfers to the IP address in use by the command channel. For more information about FTP_bounce attacks, see CERT advisory CA-97.27.

Include response code on all lines of multi-line responses: The FTP protocol defines two ways in which a multi-line response can be issued by an FTP server. Some older FTP clients have trouble parsing multi-line responses that do not contain the 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.

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.

Edit FTP commands and responses

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

Information

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

FTP Responses

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

Message Files

Certain FTP commands allow a message file to be associated with them. The contents of a message file are sent along with the standard FTP response. In addition, a secondary message file path is available as a default option. This

allows for message files to be specified using a path relative to the 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.

The following FTP commands can be used for specifying a message file:

- CDUP
- CWD
- QUIT

Managing Recursive Listings

Serv-U supports recursive listings by default, allowing FTP clients to obtain large directory listings with a single command. In some cases, clients may request excessively large directory listings using the -R parameter to the LIST and NLST commands. If performance in Serv-U is 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

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

- LIST
- MDTM
- NLST

Case file: Custom FTP command response

Users connecting to the server need to know how much quota space is available in a given folder when they have completed a transfer. To do this, edit the response to the **STOR** command to include a report 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 `DELE` command, so that every time a user deletes a file, their updated quota value, showing an increase in available space, is displayed. This can be done for any FTP command response.

Configure 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 method 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 to the server.

When creating SSL/TLS, SSH, and HTTPS encrypted domains within Serv-U, it is important to know that encrypted domains cannot share listeners. Because SSL/TLS and SSH encryption is based on encrypting traffic sent between IP addresses, each domain must have unique listeners in order to operate properly. In the case that multiple encrypted domains are created that share listeners, the domain 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

To use an existing certificate:

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

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

To create a new certificate:

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

9. Specify the common name of the certificate. The IP address or the Fully Qualified Domain Name (FQDN) that users use to connect must be listed here.

   > If the Common Name is not the IP address or FQDN used by clients to connect, clients may be prompted that the certificate does not match the domain name they are connecting to.

10. Specify the business unit the server is located in.
11. Specify the key length in bits.
12. Click Create to complete the certificate creation.

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

Viewing 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 TLSv1.1 and TLSv1.2, and 15 new 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 among the advanced SSL options:

- Enable low-security SSL ciphers: Select this option to enable low-security SSL ciphers to be used. Some older or international clients may not support today's best SSL ciphers. Because these ciphers are considered insecure by today's

computing standards, Serv-U does not accept these ciphers by default.

- Disable SSLv2 or SSLv3 support: Serv-U supports several different versions of SSL. SSLv2 and SSLv3 have documented security weaknesses that make 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.
- SSLv2 cipher suites: Cipher suites used only by SSLv2. If you disabled SSLv2, changing a setting here has no effect.
- Low security cipher suites: Cipher suites that are considered to be insecure for modern cryptographic use, but may be required for legacy applications. If you disabled low security ciphers, changing a setting here has no effect.

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)

To use an existing private key:

1. Obtain a private key file.
2. Place the private key file in a secured directory in the server. Use Browse in Serv-U to select the file.
3. Enter the password for the private key file.
4. Click Save. After clicking Save, Serv-U displays the SSH key fingerprint associated with the private key.

To create a private key:

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

SSH ciphers and MACs

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

Configure custom HTML for the Serv-U login pages

You can use custom HTML for the HTTP and HTTPS login pages of Serv-U. 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. Basic branding (custom logo and limited text changes) is also available. For more information, see Domain 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 file and footer file. The custom HTML interface also uses a CSS file which defines the style used in the login form. This CSS file can also be used to define custom CSS styles, containers, and other CSS 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. Serv-U Custom HTML and CSS has step-by-step instructions to explore 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 that is inserted before the login form.
- Footer File: This .HTM file contains the content for the HTML footer that is inserted after the login form.

- Enable Custom HTML: The custom HTML 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:

```
<img src="/%CUSTOM_HTML_DIR%/images/image.png" alt="My Image">
```

Configure file sharing

By using the file sharing feature, domain users can send or receive files from guests.

> 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.

For more information about file sharing, see the Serv-U Web Client and File Sharing User Guide.

To enable file sharing:

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

8. If it is not configured yet, configure your SMTP to be able to send and receive notification emails. For more information about configuring an SMTP server, see SMTP configuration.
9. Click Save.

Server activity

The Server Activity > Sessions and Domain Activity > Sessions pages display the current file server session activity.

When you view the Sessions page from the server, all connected sessions from all domains 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, 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.

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.

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.

Cancel 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.

Server and domain statistics

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

Session statistics

DATA	DESCRIPTION
Current Sessions	The number of sessions currently connected.
Total Sessions	The total number of sessions that have connected since being placed online.
24 hrs. Sessions	The number of sessions that have connected in the past 24 hours.
Highest Num. Sessions	The highest number of concurrent sessions that has been recorded since being placed online.
Average Session Length	The average length of time a session has remained connected.
Longest Session	The longest recorded time for a session.

Login statistics

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

connecting and disconnecting.

DATA	DESCRIPTION
Logins	The total number of successful logins.
Average Duration Logged In	The average login time for all sessions.
Last Login Time	The last recorded valid login time. This is not the last time a connection was made.
Last Logout Time	The last recorded valid logout time.
Most Logged In	The highest number of users logged in concurrently.
Currently Logged In	The number of sessions currently logged in.

Transfer statistics

DATA	DESCRIPTION
Download Speed	The cumulative download bandwidth currently being used.
Upload Speed	The cumulative upload bandwidth currently being used.
Downloaded	The total amount of data, and number of files, downloaded since being placed online.
Uploaded	The total amount of data, and number of files, uploaded since being placed online.
Average Download Speed	The average download bandwidth used since being placed online.
Average Upload Speed	The average upload bandwidth used since being placed online.

User 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

DATA	DESCRIPTION
	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.

Server and domain log

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

The server log shows file server startup, configuration, and shutdown information. It does not show domain activity information. 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.

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 so you can copy it 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.

Download Log

To download the full log file from Serv-U, click Download Log. If you have permission to download the file, your web browser prompts you to choose a location to save the file, or it begins to download the file automatically.

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

When you run a new installation of the Serv-U File Server for the first time, you are prompted to create your first domain using the New Domain Wizard. Follow the instructions on each page of the wizard to create your first domain. For more information about creating domains, see the Quick start guide.

Manage domains

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

If it is supported by your license, you can create new domains at any time by clicking + (New Domain) in the Management Console. After you change the active domain, the current page is automatically reloaded to reflect the settings of the new active domain.

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

 This action cannot be undone.

Domain details

Domain name and description

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

In addition, you can associate additional descriptive information to each domain through the description. Like the domain name, the description text is also only available to users with administrative access. This field is useful for describing the purpose of the domain or summarizing the resources made available by the existence of the domain on the file server.

You can temporarily disable a domain by clearing the Enable domain option. While disabled, the domain is inaccessible to all users. The domain still exists on the file server, all settings are preserved, and you can still administer it while it is disabled. To make the domain accessible to users again, select Enable domain.

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

Domain home directory

You can limit the disk space available to a domain by configuring a home directory for the domain and specifying a maximum size. The home directory of the domain does not affect user directory access rules, and it does not restrict the paths that are available to a user in any way. However, in order to calculate the amount of disk space in use by a domain, you must specify the root directory under which Serv-U expects all domain files to be stored.

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

Click Save to apply the changes.

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

Domain listeners

The Serv-U File Server offers a highly configurable interface for enabling the different file sharing protocols on a domain. You can add, edit, and delete listeners. Each domain can listen on multiple ports and IP addresses by adding a listener bound to the IP address and port you want. In addition to selecting these connection attributes for a listener, 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 both for an IPv4 address and an IPv6 address.

The following section contains the list and short description of the file sharing protocols supported by the Serv-U File Server.

FTP - File Transfer Protocol

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

FTPS - File Transfer Protocol using SSL

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

SFTP - Secure File Transfer Using SSH2

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

HTTP - Hypertext Transfer Protocol

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

HTTPS - Hypertext Transfer Protocol using SSL

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

Add a listener

After clicking Add, the listener configuration window is displayed. After configuring each of the listener options, click Save to add the listener to the domain.

The following section contains the list and short description of the options you can configure for a listener.

Type

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

IP Address

You can bound a listener to a single IP address by entering the IP address here. Serv-U supports both IPv4 and IPv6 addresses. If the file server does not have an external IP address (for example, it is behind a router), you can leave this

field blank. 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 you are running a purely IPv6 network, it is recommended to use IPv4 addresses and add IPv6 listeners as needed.

PASV IP Address or Domain Name (FTP ONLY)

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

Use only with SSL connections

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

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 you use a non-standard port, it is recommended that you use a value above 1024 to prevent potential conflicts.

Enable listener

You can temporarily disable a listener by deselecting this option. When they are disabled, listeners are displayed with a different icon in the list.

Pure virtual domains

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

This method of "piggybacking" only works with the FTP and HTTP protocols 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.

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. By using virtual hosts, you can host multiple domains on a system that only has one unique IP address without having to use non-standard port numbers. The domains can share the same listeners by proper implementation of virtual hosts. This feature is only available when the current license supports hosting multiple domains.

To configure virtual hosts for a domain, click Add under Domain Details > Virtual Hosts, and then type the virtual host name for the domain. The virtual host name is usually the fully qualified domain name used to connect to the domain, such as `ftp.Serv-U.com`.

The method used by a client to connect to a specific virtual host depends on the protocol 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: `virtual_host_name|login ID`. The virtual host name is entered first, followed by the vertical bar character ('|'), then the login ID.

SFTP

SFTP users who want to connect to a specific virtual host must use the specially crafted login ID format as described 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, configure virtual hosts on each domain so that Serv-U can distinguish between requests for the two domains. After setting up the same listener properties on each domain, open the Virtual Hosts page, click Add, and then type the FQDN that clients should use to connect to the domain (such as `ftp.Serv-U.com`).

After connecting to the server with FTP, users can send a `HOST ftp.Serv-U.com` command to connect to the appropriate domain on the File Server. FTP and SFTP users can also identify the virtual host through their login ID of `ftp.Serv-U.com|login ID`. If connecting through HTTP, users can connect to this domain by visiting `http://ftp.Serv-U.com`.

Server details

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

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

Specifying IP access masks

IP access rules use masks to authorize IP addresses and domain names. The masks can contain specific values, ranges, and wildcards made up of the following elements.

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`.

Caveats

Specific IP addresses listed in Allow rules will not be blocked by anti-hammering. These IP addresses are white-listed. However, addresses matched by a wildcard or a range are subject to anti-hammering prevention.

Implicit deny all

Until you add the first IP access rule, connections from any IP address are accepted. After you add the first 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.

Matching all addresses

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.

DNS lookup

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 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.

Rule use during connection

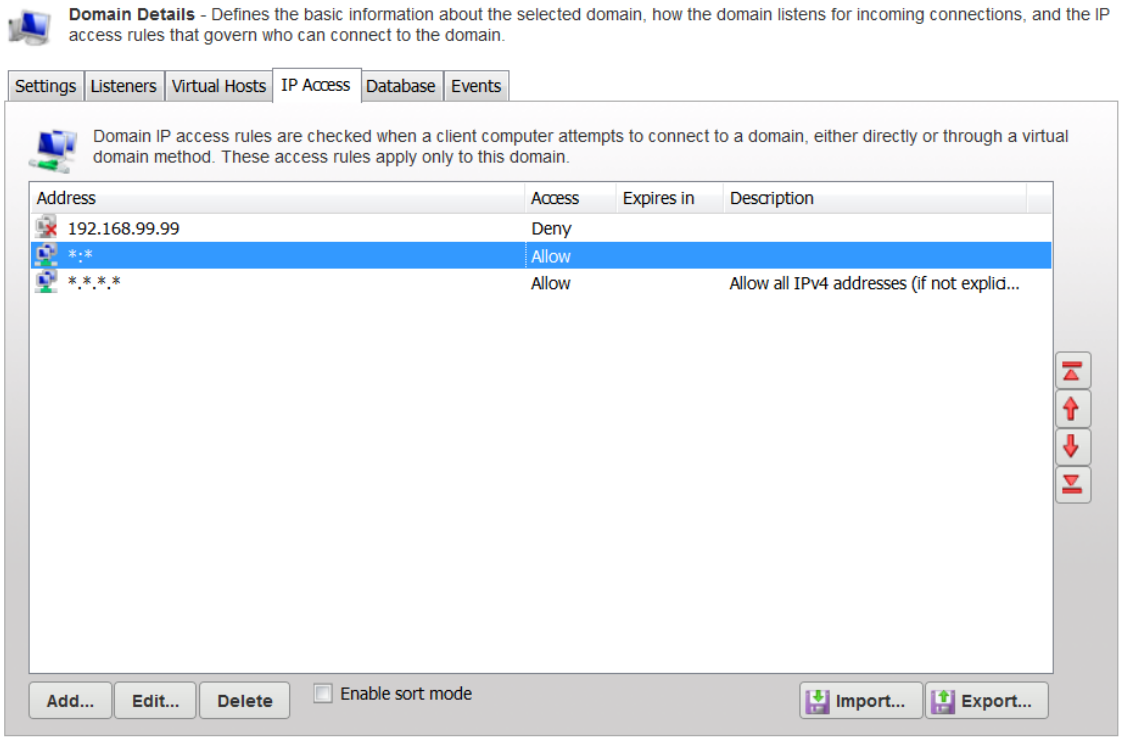
The level at which you specify an IP access rule also defines how far a connection is allowed before it is rejected. Server and domain level IP access rules are applied before the welcome message is sent. Domain level IP access rules are also applied when responding to the `HOST` command to connect to 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.

Anti-hammering

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. You can configure an anti-hammering policy server-wide in Server Limits and Settings > Settings and domain-wide in Domain Limits and Settings > Settings.

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.

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



IP access list controls

The following options are available on the IP Access page.

Using the sort mode

You can 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.

Importing and exporting IP access rules

You can export and import Serv-U IP access rules from users, groups, domains, and the server by using a text-based `.csv` file. To export IP access rules, view the list of rules to export, click Export, and specify the path and file name you want to save the list to. To import IP access rules, click Import and select the file that contains the rules you want to import. The `.csv` file must contain the following fields, including the headers:

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

Examples of IP address rules

Office-only access

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 access rule 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 provides an implicit Deny All rule at the end of the list.

Prohibited computers

Users should normally be able to access Serv-U 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 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.

DNS-based access control

The only users allowed to access a Serv-U domain connect from `*.example.com` or `*.example1.com`. The related Serv-U 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 provides an implicit Deny All rule at the end of the list.

Database access

Serv-U enables the use of an Open Database Connectivity (ODBC) database to store and maintain group and user accounts at the domain and server levels. You can configure the ODBC connections in two locations:

- Domain > Domain Details > Database
- Server > Server Details > Database.

Serv-U can automatically create all of the tables and columns necessary to begin storing users and groups in the database. Because Serv-U uses one set of table names to store its information, individual ODBC connections must be configured for each item which stores details in the database. In other words, the server and each domain must have a unique ODBC connection to ensure they are stored separately.

Configure a database

1. Create an ODBC connection for Serv-U to use. SolarWinds recommends MySQL, but you can use any database that has an ODBC driver available. Use a System data source name (DSN) if Serv-U is operating as a system service, or a User DSN if Serv-U is operating as a regular application.
2. Open the Serv-U Management Console and browse to the appropriate domain or server database settings. Enter the required information, and click Save.

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

SQL templates

Serv-U uses multiple queries to maintain the databases that contain user and group information. These queries conform to the Structured Query Language (SQL) standards. However, if your database has problems working with Serv-U, you may need to alter these queries. In the SQL Templates window, you can modify each query used by Serv-U to conform to the standards supported by your database.

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

User and group table mappings

By default, Serv-U 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 to an existing database that contains this information, you must customize the table and column names to conform to the existing database structure. Click User Table Mappings or Group Table Mappings to get started.

Serv-U stores information for a user or group in 10 separate tables. Only the User/Group Info Table and User/Group Dir Access Table are required. 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.

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 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 Serv-U Management Console through scripted database operations which can be built into many existing account provisioning systems. A DSN must first be created in Control Panel > Administrative Tools > ODBC Data Sources. Use a System DSN if Serv-U is running as a service or a User DSN if Serv-U is running as an application. After you create the appropriate DSN, enter the required information and click Save. Serv-U creates the tables and columns. You can manage database users and groups in the Database Users and Database Groups pages of Serv-U, located near the normal Users and Groups pages.

Data source name creation in Linux

Database access in Serv-U on Linux follows the same method as Serv-U 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
- postgressql-odbc
- unixodbc

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

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

[PostgreSQL-test]
```

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

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.

Domain events

You can automatically create a list of the most common events. You can choose to create these common events using email or balloon tip actions. Click Create Common Event on the Events page. Select the Send Email or Show balloon tip option for the action you want to perform on the common events. If you choose to send email, enter an email address.

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

Event actions

You can select from the following actions that are executed when an event is triggered:

- Send Email
- Show Balloon Tip*
- Execute Command*

- Write to Windows Event Log (Windows only)*
- Write to Microsoft Message Queue (MSMQ) (Windows only)*

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

Email actions

You can configure email actions to send emails to multiple recipients and to Serv-U groups when an event is triggered.

To add an email address, enter it in the To or Bcc fields. To send emails to a Serv-U group, use the Group icon to add or remove Serv-U groups from the distribution list. Separate email addresses by commas or semicolons. Email actions contain a To, Subject and Message parameter. You can use special variables to send specific data pertaining to the event. For more information about the variables, see System variables.

To use email actions, you must first SMTP configuration.

Balloon tip actions

You can configure a balloon tip to show in the system tray when an event is triggered. Balloon tip actions contain a Balloon Title and a Balloon Message parameter. You can use special variables to send specific data pertaining to the event. For more information about the variables, see System variables.

Execute command actions

You can configure execute command actions to execute a command on 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 for no waiting.

> Time spent waiting delays any processing that Serv-U can perform.

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

Windows Event Log

By writing event messages to a local Windows Event Log, you can monitor and record Serv-U activity by using third-party network management software. All messages appear in the Windows Application Log from a source of Serv-U.

This event has only one field:

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

Microsoft Message Queuing (MSMQ)

Microsoft Message Queuing (MSMQ) is an enterprise technology that provides a method for independent applications to communicate quickly and reliably. Serv-U 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.

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 attempts to create it. This normally only works on public queues on the local machine. You can also use Serv-U 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 system variables can also be used in this field. This field may be left blank, but usually is not.

Microsoft message queues created in Windows do not grant access to SYSTEM by default, preventing Serv-U 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 runs) has permission to the queue.

Event filters

Use event filters to control when a Serv-U event is triggered. By default, events trigger each time the event occurs. The event filter allows events to be triggered only if certain conditions are met. For example, a standard 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. For example, you can configure a File Uploaded event to only send an email when the file name contains the string `important`, so an email would be sent when the file `Important Tax Forms.pdf` is uploaded but not when other files are uploaded to the server. Additionally, you can 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.

Event filter fields

Each event filter has the following critical values that must be set:

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

- Logic: This determines how the filter interacts with other filters for an event. In most cases, AND 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).
- Filter Comparison: This is the most critical portion of the filter. The Filter Comparison contains the evaluation that must occur for the event to trigger. For example, a filter can be configured so that only the user *admin* triggers the event. In this case, the comparison is `If $Name = (is equal to) admin`, and the data type is `string`. For bandwidth, either an unsigned integer or double precision floating point value is used.

Event filters also support wildcards when evaluating text strings. The supported wildcards include:

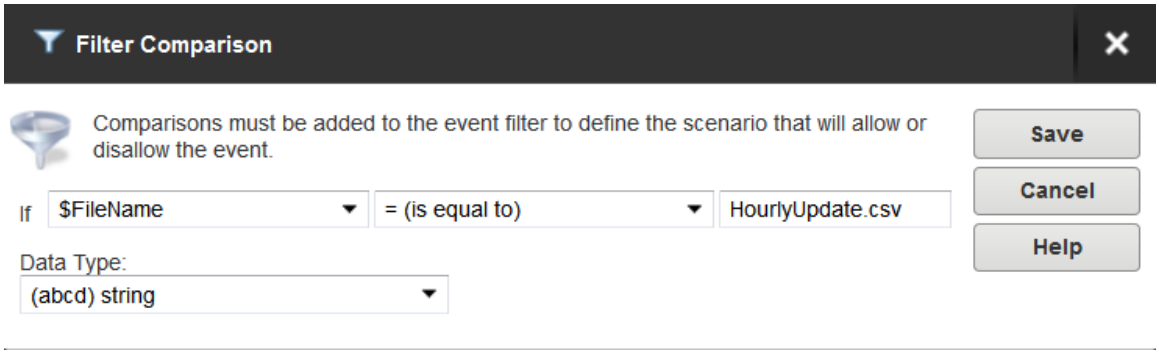
- `*` - The asterisk wildcard matches any text string of any length. For example:
  - An event filter that compares the `$FileName` variable to the string `data*` matches files named `data`, `data7`, `data77`, `data.txt`, `data7.txt`, and `data77.txt`.
- `?` - The question mark wildcard matches any one character, but only one character. For example:
  - An event filter that compares the `$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.

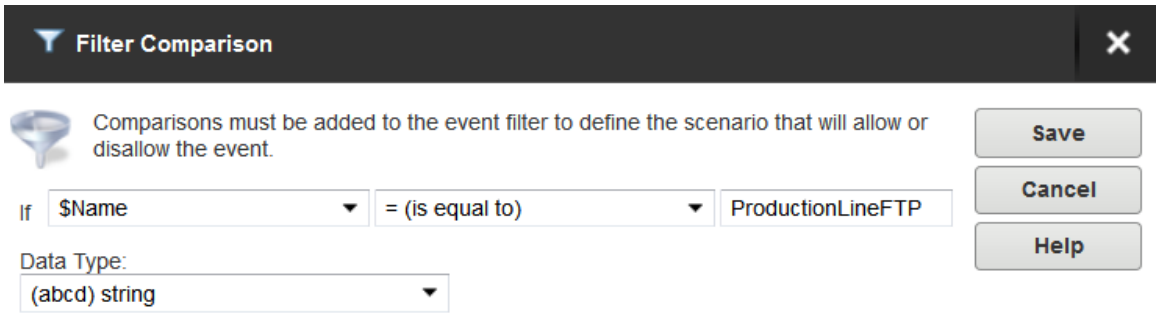
Event filters

Event filters are used by comparing fields to expected values in the Event Filter menu. The best example is raising an event only when a certain user triggers the action, or when a certain file is uploaded. For example, 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:

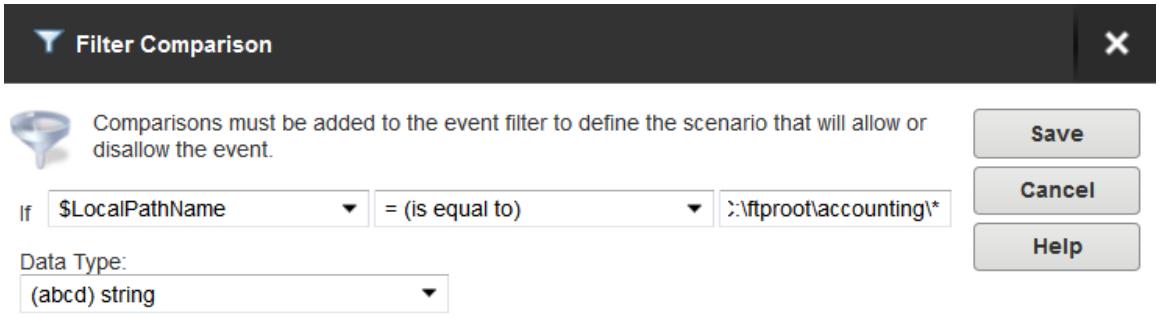


As another example, it may be necessary to know when a file transfer fails for a specific user account. To perform this task, create a new File Upload Failed event, and add a new filter.

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



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\`.



SMTP configuration

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 in the Events tab on the Domain Details and Server Details pages.

Click Configure SMTP to launch the dialog.

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 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	An unspecified error occurred. Check your

ERROR MESSAGE	EXPLANATION
that SMTP server settings are correct, and that the SMTP server is up and running.	SMTP connection details, and try the test again.
Timeout while contacting SMTP server. Please check that the SMTP server address is correct.	The connection to the SMTP server timed out.

Directory access rules

Directory access rules define the areas of the system which are accessible to user accounts. While traditionally restricted to the user and group levels, in Serv-U, the usage of directory access rules is extended to both the domain and the server levels through the creation of global directory access rules. Directory access rules specified at the server level are inherited by all users of the file server. 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 they are listed. The first rule in the list that matches the path of a client's request is the one that is applied for that rule. In other words, if a rule exists that denies access to a particular subdirectory but is listed below the rule that grants access to the parent directory, then a user still has access to the 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 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.

File permissions

PERMISSION	DESCRIPTION
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 permissions

PERMISSION	DESCRIPTION
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 permissions

PERMISSION	DESCRIPTION
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.

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, you can configure the Serv-U File Server service to run under a network account. The alternative, preferred when many servers exist, or if the Serv-U File Server service 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.

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.

Quota permissions

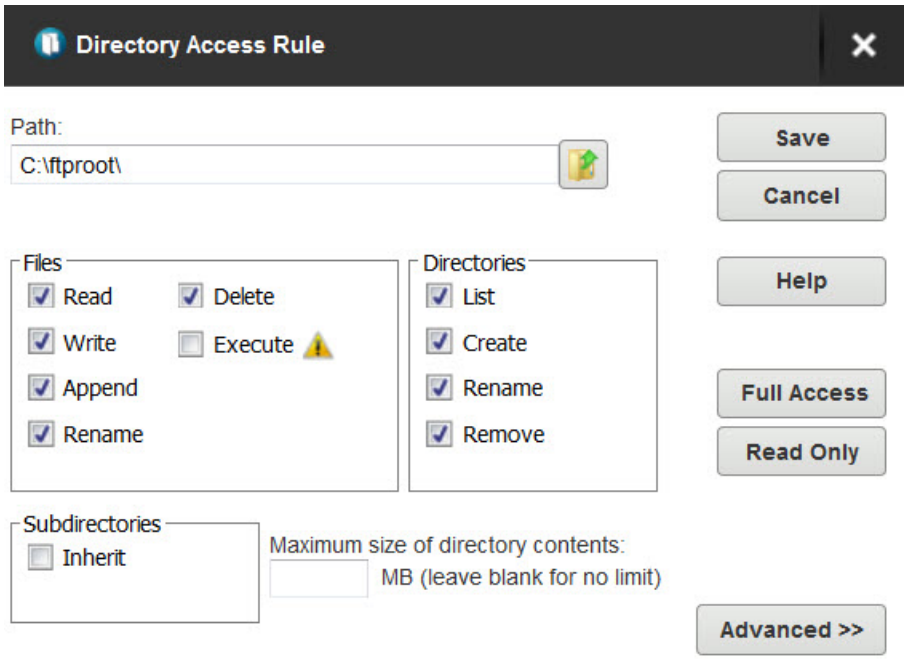
Maximum size of directory contents

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

Mandatory access control

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\`.

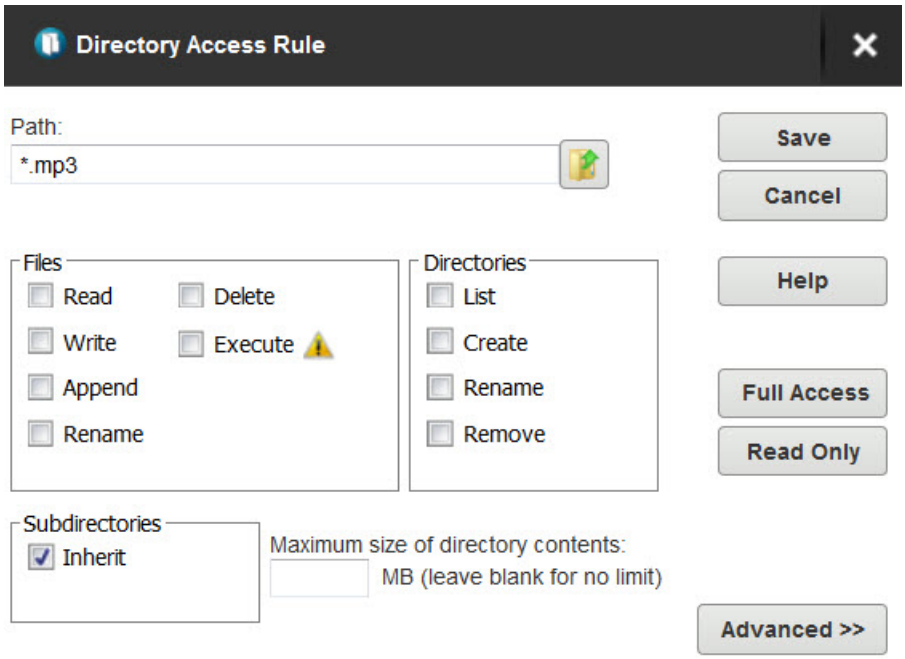


Now, the user has access to the `ftproot` folder but to no folders below it. Permissions must individually be granted to subfolders that the user needs access to, providing the security of mandatory access control in Serv-U File Server.

Restrict file types

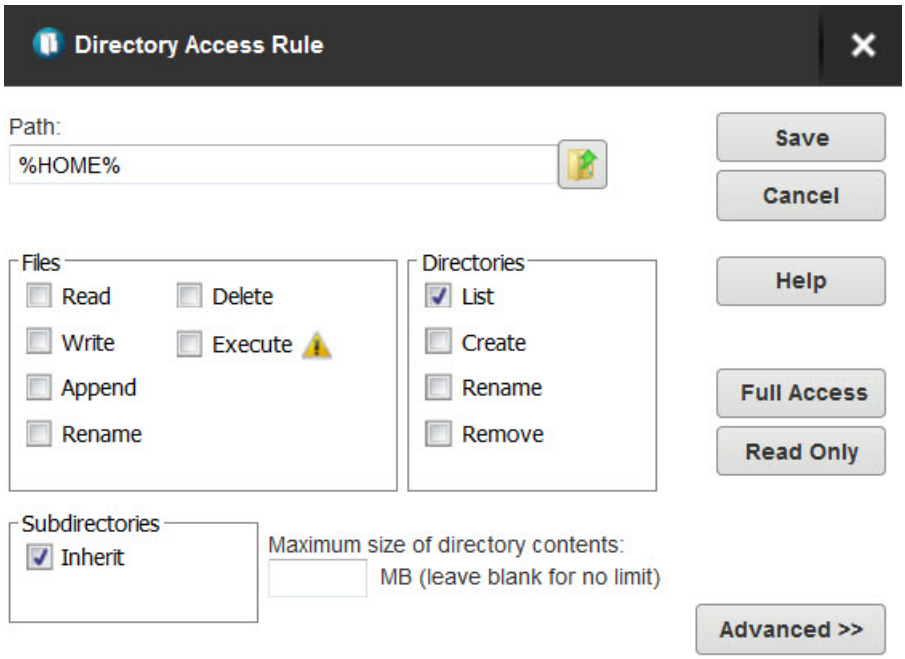
If users are using storage space on the Serv-U File Server to store non-work-related files, such as .mp3 files, you can prevent this by configuring a directory access rule placed above the main directory access rule to prevent .mp3 files from being transferred as shown below.

In the text entry for the rule, type `*.mp3`, and use the permissions shown beolw:



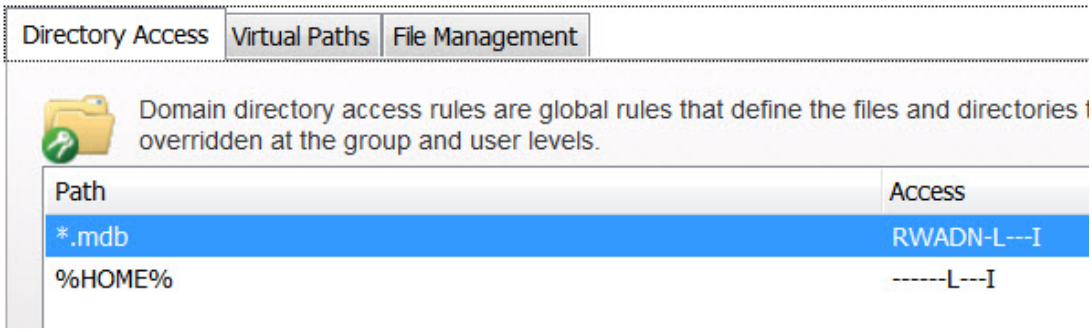
The rule denies permission to any transfer of files with the `.mp3` extension and can be modified to reflect any file extension. Similarly, if accounting employees only need to transfer files with the `.mdb` extension, configure a pair of rules that grants permissions for `.mdb` files but denies access 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.



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

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.



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. When virtual paths are created at the domain level, they are only accessible by users belonging to that domain.

You can also create virtual paths specifically for individual users or groups.

Physical path

The physical path is the actual location on the system, or network, that is to be placed in a virtual location accessible by a user. If the physical path is located on the same computer, 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 that the physical path should appear in for the user. The `%HOME%` macro is commonly used in the virtual path to place the specified

physical path in the home directory of the user. When specifying the virtual path, the last specified directory is used as the name displayed in directory listings to the user. For example, a virtual path of `%HOME%/public` places the specified physical path in a folder named `public` within the user's home directory. 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.

Virtual paths example

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 example

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.

Automated file management

Using file management rules, you can automatically remove or archive files from the file server. You can configure automated 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 uses the creation or change date of files to determine the expiration date. On Windows, the creation date of the file is used to determine when a file expires. On 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. This way you can manage files that are transferred by clients, or that are copied to the folder outside of Serv-U.

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 deletes or moves an expired file.

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

Define a new file management rule

1. Navigate to Directories > File Management, and click Add.
2. Type the path to the file or folder in the Directory Path field, or click Browse to navigate to the file or folder.

3. Select the action you want to perform on the file:
    a. If you want to delete the file after it expires, select Delete file(s) after specified time.
    b. If you want to move the file after it expires, select Move file(s) after specified time, and then 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 regularly checks each file in the directory for its age, and performs the specified action on the files that meet the age criteria you specify.

Domain limits and settings

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

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

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

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

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

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

To create a limit that is restricted to a specific time of day or days of the week, click Advanced in the New Limit or Edit Limit window. Select Apply limit only at this time of day to specify a start and stop time for the new limit. To restrict the limit to certain days of the week, deselect the days for which you do not want to apply the limit. When a limit is restricted in this way, default values (or the value of other limit overrides) are applied when the time of day or day of the week restrictions are not met for this limit.

Domain settings

On the Domain Limits and Settings > Settings pages, you can configure basic domain settings that affect performance, security, and network connectivity. To configure a setting, type the value you want in the appropriate area, and then click Save. This topic contains detailed information about the settings that 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 IP addresses for the specified number of minutes 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 given to the client.

Default Web Client

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

Custom HTTP settings

Basic branding (custom logo and limited text changes) can be implemented using the Custom HTTP Settings. Advanced branding is also available. For more information, see Configure custom HTML for the Serv-U login pages.

Specify a custom logo to be displayed on the login and Web Client pages

Custom logos must have a width of 400 pixels and a height of 100 pixels. If a

logo does not meet this criteria an error message will appear when you attempt to save the logo.

> JPEG images which use CMYK instead of RGB encoding may not work properly in certain browsers. Test your logo image to make sure it is displayed properly in all browsers.

To add a logo, click Browse next to Custom Logo Path, and then select the path to your logo. Click Save and the logo will appear below the Custom Logo Path field. To delete a custom logo, clear the path in the Custom Logo Path field, and then click Save.

HTTP Login Title Text (no HTML)

Provide text to be used as the title of the HTTP login and Web Client pages.

HTTP Login Page Text

Provide any custom login page text you want in this area. This text can be HTML-formatted, including links, images, and standard formatting like italics, bold, underline, alignment and more.

HTTP Client Interface Background (CSS Only)

Provide a custom CSS background style for the Web Client, File Sharing and FTP Voyager JV landing page. This style follows the CSS background shorthand standard. The "background:" string is assumed so it does not need to be entered here. The format for a CSS background is `color url('/%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 Email Message

Send email messages to users with their login credentials using this customizable password recovery message.

The password recovery email message has a simple default subject and message with the user's login ID and password. This message will be sent if the user has a valid email address recorded in Serv-U. Users can request this message from the Serv-U login page.

Administrators can also send this message to users using the Recover Password button under domain users and global users in the Management Console.

Integration DLL / Shared Library

For information about writing an Integration DLL or Shared Library, see the Serv-U Integration Sample DLL installed with Serv-U in the `Serv-U Integration Sample DLL` sub-directory. The Integration API is documented in this sample.

Other settings

Ratio Free Files

Files listed by clicking Ratio Free Files are exempt from transfer ratio limitations on file transfers. Ratio free files specified at the server or domain level are inherited by all their users accounts. For more information about ratio free files, see Transfer ratios and quotas.

FTP settings

In the Serv-U File Server, you can customize the FTP commands that Serv-U accepts, and you can also customize the responses of Serv-U to the FTP commands it receives. If you configure these options at the server level, all domains inherit the customizations. 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 have the domain revert back to the default settings of the server.

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

Global properties

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

FTP Responses

Global FTP responses are responses shared amongst most FTP commands, such as the error message sent when a file is not found. Customizing a global FTP response ensures that the response is used by all other FTP commands rather than having to customize it for each individual FTP command. FTP command responses can contain special macros that allow real-time data to be inserted in to the response. For more information, see System variables.

Message File

The server welcome message is sent in addition to the standard "220 Welcome Message" that identifies the server to clients when they first connect. If the Include response code in text of message file option is selected, 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

Block "FTP_bounce" attacks and FXP (server-to-server transfers): Select this option to block all server-to-server file transfers involving this Serv-U File Server by only allowing file transfers to the IP address in use by the command channel. For more information about FTP_bounce attacks, see CERT advisory CA-97.27.

Include response code on all lines of multi-line responses: The FTP protocol defines two ways in which a multi-line response can be issued by an FTP server. Some older FTP clients have trouble parsing multi-line responses that do not contain the 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.

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.

Edit FTP commands and responses

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

Information

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

FTP Responses

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

Message Files

Certain FTP commands allow a message file to be associated with them. The contents of a message file are sent along with the standard FTP response. In addition, a secondary message file path is available as a default option. This

allows for message files to be specified using a path relative to the 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.

The following FTP commands can be used for specifying a message file:

- `CDUP`
- `CWD`
- `QUIT`

Managing Recursive Listings

Serv-U supports recursive listings by default, allowing FTP clients to obtain large directory listings with a single command. In some cases, clients may request excessively large directory listings using the -R parameter to the `LIST` and `NLST` commands. If performance in Serv-U is 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

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

- `LIST`
- `MDTM`
- `NLST`

Case file: Custom FTP command response

Users connecting to the server need to know how much quota space is available in a given folder when they have completed a transfer. To do this, edit the response to the **`STOR`** command to include a report 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 `DELE` command, so that every time a user deletes a file, their updated quota value, showing an increase in available space, is displayed. This can be done for any FTP command response.

Configure 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 method 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 options specified at the domain level automatically overrides the corresponding server-level option. Certain configuration options are only available to the server.

When creating SSL/TLS, SSH, and HTTPS encrypted domains within Serv-U, it is important to know that encrypted domains cannot share listeners. Because SSL/TLS and SSH encryption is based on encrypting traffic sent between IP addresses, each domain must have unique listeners in order to operate properly. In the case that multiple encrypted domains are created that share listeners, the domain 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

To use an existing certificate:

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

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

To create a new certificate:

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

9. Specify the common name of the certificate. The IP address or the Fully Qualified Domain Name (FQDN) that users use to connect must be listed here.

   > If the Common Name is not the IP address or FQDN used by clients to connect, clients may be prompted that the certificate does not match the domain name they are connecting to.

10. Specify the business unit the server is located in.
11. Specify the key length in bits.
12. Click Create to complete the certificate creation.

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

View the certificate

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

SFTP (Secure File Transfer over SSH2)

To use an existing private key:

1. Obtain a private key file.
2. Place the private key file in a secured directory in the server. Use Browse in Serv-U to select the file.
3. Enter the password for the private key file.
4. Click Save. After clicking Save, Serv-U displays the SSH key fingerprint associated with the private key.

To create a private key:

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

SSH ciphers and MACs

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

Configure custom HTML for the Serv-U login pages

You can use custom HTML for the HTTP and HTTPS login pages of Serv-U. 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. Basic branding (custom logo and limited text changes) is also available. For more information, see Domain 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 file and footer file. The custom HTML interface also uses a CSS file which defines the style used in the login form. This CSS file can also be used to define custom CSS styles, containers, and other CSS 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. Serv-U Custom HTML and CSS has step-by-step instructions to explore 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 that is inserted before the login form.
- Footer File: This .HTM file contains the content for the HTML footer that is inserted after the login form.
- Enable Custom HTML: The custom HTML 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:

```
<img src="/%CUSTOM_HTML_DIR%/images/image.png" alt="My Image">
```

Configure file sharing

By using the file sharing feature, domain users can send or receive files from guests.

> 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.

For more information about file sharing, see the Serv-U Web Client and File Sharing User Guide.

To enable file sharing:

1. Navigate to Server Limits and Settings > File Sharing.
2. Type the address for the domain URL.
3. Type the location of the file sharing repository.
4. Select the number of days until the shares expire.
5. Select whether you want to use the inherited default email invitation subject, or customize your own. If the option is deselected, you can type in a custom email invitation subject.
6. Select whether you want to use the inherited default email notification message, or customize your own. If the option is deselected, you can type in a custom message.
7. Select Enable File Sharing.
8. If it is not configured yet, configure your SMTP to be able to send and receive notification emails. For more information about configuring an SMTP server, see SMTP configuration.
9. Click Save.

Server activity

The Server Activity > Sessions and Domain Activity > Sessions pages display the current file server session activity.

When you view the Sessions page from the server, all connected sessions from all domains 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, 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.

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.

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.

Cancel 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.

Server and domain statistics

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

Session statistics

DATA	DESCRIPTION
Current Sessions	The number of sessions currently connected.

Data	Description
Total Sessions	The total number of sessions that have connected since being placed online.
24 hrs. Sessions	The number of sessions that have connected in the past 24 hours.
Highest Num. Sessions	The highest number of concurrent sessions that has been recorded since being placed online.
Average Session Length	The average length of time a session has remained connected.
Longest Session	The longest recorded time for a session.

Login statistics

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

Data	Description
Logins	The total number of successful logins.
Average Duration Logged In	The average login time for all sessions.
Last Login Time	The last recorded valid login time. This is not the last time a connection was made.
Last Logout Time	The last recorded valid logout time.
Most Logged In	The highest number of users logged in concurrently.
Currently Logged In	The number of sessions currently logged in.

Transfer statistics

DATA	DESCRIPTION
Download Speed	The cumulative download bandwidth currently being used.
Upload Speed	The cumulative upload bandwidth currently being used.
Downloaded	The total amount of data, and number of files, downloaded since being placed online.
Uploaded	The total amount of data, and number of files, uploaded since being placed online.
Average Download Speed	The average download bandwidth used since being placed online.
Average Upload Speed	The average upload bandwidth used since being placed online.

User 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	The average length of time a session has remained connected.

DATA	DESCRIPTION
Length	
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.

Server and domain log

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

The server log shows file server startup, configuration, and shutdown information. It does not show domain activity information. 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.

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 so you can copy it 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.

Download Log

To download the full log file from Serv-U, click Download Log. If you have permission to download the file, your web browser prompts you to choose a location to save the file, or it begins to download the file automatically.

Configure domain logs

In the Serv-U File Server, you can customize the logging of domain events and activity to a great extent. Logging consists of two sections: File and Screen. To enable a logging option, select the appropriate option in the File or Screen column. When an option is selected from the File column, the appropriate logging information is saved to the specified log file if Enable logging to file is selected. When an option is selected from the Screen column, the event is displayed in the log when viewed from the Serv-U Management Console. 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.

Log to file settings

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.

You can use the following wildcard characters.

WILDCARD	DESCRIPTION
%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, 2015).
%X	The 2-digit value of the current year (for example, 15 for 2015).

WILDCARD	DESCRIPTION
%S	The name of the domain whose activity is being logged.

Enable logging to file

Select this option to enable Serv-U to begin saving log information to the file specified in the Log file path. If this option is not selected, Serv-U does not log any information to the file, regardless of the individual options selected in the File column.

Rotate the log file automatically

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.

Purge old 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`

The following wildcards can be used for log variables:

%D --> ??
%N --> ??
%M --> *
%Y --> ????
%X --> ??
%S --> *

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.

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.

Users

User accounts

A user account is required in order to provide access to the file server. At its most basic level, a user account defines login credentials (that is, login ID and password), a home directory, and a set of directory access rules that define the areas of the system that are 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 that identifies the client to the administrator.

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

Domain users

Defined at the domain level, domain users can only log in to the domain under which they are created.

Global users

Defined at the server level, global users can log in to any domain on the file server.

Database users

Available at both the server and domain level, database users are stored in an external database accessible through ODBC and supplement the local account database.

Windows users

Defined at the domain level, Windows users use the credentials and often, the home directories, of Windows accounts from the local machine or Windows domain controller (including Active Directory). Windows users only work on Windows, and require a Serv-U MFT Server license.

LDAP users

Defined at the domain level, LDAP users use the credentials and often, the email and other attributes, of LDAP accounts from a remote LDAP server. Unlike Windows users, LDAP users work on both Windows and Linux, and may access LDAP servers, including Active Directory and OpenLDAP, in any accessible domain. LDAP users require a Serv-U MFT Server license.

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.

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.

Warning: 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.

New User Wizard

Click Wizard on the Users page to open the New User Wizard. The New User Wizard walks you through the four steps required to create a user account with the minimum number of required attributes. After it is created, you can edit the user account to configure more advanced settings, such as group membership or additional directory access rules. For more information about using the New User Wizard, see the Quick start guide.

User Template

While the New User Wizard 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.

Copy user accounts

User templates offer a way for large numbers of users to be created with the same settings. In cases where only the settings of a single user must be duplicated or there is a need for multiple user templates, use Copy to create a copy of a user account that only lacks the user name and the password. To copy a user, select the user account, and then choose Copy.

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 Management Console, select a user account, and then click Recover Password. If the password is stored using one-way encryption, the password will be reset and the new password will be sent to the user's email address. If the password is stored using two-way encryption or no encryption, the original password will be sent by email.

Password Recovery from the Web Client requires that the Allow users to recover password limit be enabled for the user account. Once this option is enabled, users can use the Recover Password option in the Web Client. Password Recovery from the Web Client otherwise works the same as from the Management Console.

Importing and exporting user accounts

User accounts can be imported and exported using the Import and Export options. Click Export to export all users in either the current domain or server, or the current Collection to a comma-separated values file (CSV file), which can be viewed in Excel and analyzed by database engines, among other things. Additionally, by creating a CSV file using the same format as the export it is possible to import lists of users from CSV files into Serv-U.

Filtering user and group ID lists

In larger deployments of Serv-U, the user list can grow very large. In order to easily find a specific user account, you can filter user and group lists by login ID using input from the administrator. The following wildcards are also supported:

- Use the "*" parameter to filter for Users or Group login IDs when the whole ID is unknown (for example, `*Department`, `*Admin*`, `Tech*`).
- Use the "?" parameter when a specific character is unknown (for example, `????Lastname, Firstname???`).
- Use the "[]" parameter when a specific character is unknown but should contain one of the specified characters in the brackets (for example, `[utr]sername, User[fmn]ame`).

User information

A user account consists of several attributes and settings. The User Information page contains general information about the user account including login credentials, the home directory, and the type of account. This topic provides detailed information

about each attribute.

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.

Full name

The full name of the account is available to specify additional identifying information about the account. It is not used by clients when they log in.

Password

The password is the second item 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 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

A user account can be granted one of the following types of administrative privileges:

- No Privilege
- Group Administrator
- Domain Administrator
- System Administrator

The value of this attribute can be inherited through group membership. A user account with No Privilege is a regular user account that can only log in to transfer files to and from the File Server. The Serv-U Management Console is not available to these user accounts.

A Group Administrator can only perform administrative duties relating to their primary group (the group that is listed first in their Groups memberships list). They can add, edit, and delete users which are members of their primary group, and they can also assign permissions at or below the level of the Group Administrator. They may not make any other changes.

A Domain Administrator can only perform administrative duties for the domain to which their account belongs. A Domain Administrator is also restricted from performing domain-related activities that may affect other domains.

The domain-related activities that may *not* be performed by Domain Administrators consist of:

- configuring their domain listeners
- configuring or administering LDAP groups
- configuring ODBC database access for the domain

A System Administrator can perform any file server administration activity including creating and deleting domains, user accounts, or even updating the 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 administrator accounts which can allow administrators to log in and view configuration options at the domain or server level, greatly aiding remote problem diagnosis when working with outside parties. Read-only administrator privileges are identical to their full-access equivalents, except that they cannot change any settings, and cannot create, delete or edit user accounts.

When you configure a user account with administrative privileges, take care in

specifying their home directory. An administrator with a home directory other than "\" (root) that is locked in their home directory may not use absolute file paths outside of their home directory when configuring the file server. Instead, relative paths must be used.

Additionally, such a user account can also use setting files located outside the home directory, however, these files must also be specified by using relative paths, for example, `../../exampleFile.txt`.

Home directory

The home directory for a user account is where the user is placed immediately after logging in to the file server. Each user must have a home directory assigned to it, although it can be specified at the group level if the user is a member of a group. Home directories must be specified using a full path including the drive letter or the UNC share name. If the home directory is not found, you can configure Serv-U to create it.

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.

SSH public key path

The SSH public key can 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 about creating an SSH key pair, see SFTP for users and groups.

Account type

By default, all accounts are permanent and exist on the file server until they are manually deleted or disabled. 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.

Default Web Client

If your Serv-U license enables the use of FTP Voyager JV, then users connecting to the file server through HTTP can choose which client they want to use after logging in. Instead of asking users which client they want to use, 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.

Email address

Serv-U events can use the Email Address field when sending email notifications to groups, and password recovery using the Web Client requires an email address to send a recovered password to a user. Type an email address here to allow email notifications or password recovery for the user account.

Lock user in home directory

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.

Enable account

Deselect this option to disable the current account. Disabled accounts remain on the file server but cannot be used to log in. To re-enable the account, select the Enable account option again.

Always allow login

Enabling this option means that the user account is always permitted to log in, regardless of restrictions placed upon the file server, such as maximum number of sessions. It is useful as a fail-safe in order to ensure that critical system administrator accounts can always remotely access the file server. 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.

Enabling the Always Allow Login option does not override IP access rules. If both options are defined, the IP access rules prevail.

Description

The description allows for the entry of additional notes that are only visible to administrators.

Availability

This feature limits when users can connect to this server. You can place limitations

on the time of day, and also on the day of the week. When users attempt to log in outside the specified available times, they are presented with a message that their user account is currently unavailable.

Welcome message

The welcome message is a message that is traditionally sent to the FTP client during a successful user login. Serv-U extends this ability to HTTP so that users accessing the file server through the Web Client or FTP Voyager JV also receive the welcome message. This feature is not available to users logging in through SFTP over SSH2, because SSH2 does not define a method for sending general text information to users.

The welcome message can contain general information about the status of the server, a special message for the user, disclaimers, or other legal notices. You can configure a welcome message in one of two ways. The first method involves specifying the path to a file containing the welcome message in the Message File Path field. Use Browse to select an existing file on the system.

As an alternative, the text of the welcome message can be explicitly provided to Serv-U in the appropriate text field. In order to override an explicit welcome message at the user level, select the Override inherited group welcome message option first. The provided text is then sent to the user instead of the contents of the file specified in the Message File Path field.

These values can be inherited by the user through group membership.

You can also use system variables in the welcome message. For a comprehensive list of system variables, see System variables.

Directory access rules

Directory access rules define the areas of the system which are accessible to user accounts. While traditionally restricted to the user and group levels, in Serv-U, the usage of directory access rules is extended to both the domain and the server levels through the creation of global directory access rules. Directory access rules specified at the server level are inherited by all users of the file server. 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 they are listed. The first rule in the list that matches the path of a client's request is the one that is applied for that rule. In other words, if a rule exists that denies access to a particular subdirectory but is listed below the rule that grants access to the parent directory, then a user still has access to the 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 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.

File permissions

PERMISSION	DESCRIPTION
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.

PERMISSION	DESCRIPTION
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 permissions

PERMISSION	DESCRIPTION
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 permissions

PERMISSION	DESCRIPTION
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.

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, you can configure the Serv-U File Server service to run under a network account. The alternative, preferred when many servers exist, or if the Serv-U File Server service 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.

> 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.

Quota permissions

Maximum size of directory contents

Setting the maximum size actively restricts the size of the directory contents to the specified value. Any attempted file transfers that cause the directory contents to exceed this value are rejected. This feature serves as an alternative

to the traditional quota feature that relies upon tracking all file transfers (uploads and deletions) to calculate directory sizes and is not able to consider changes made to the directory contents outside of a user's file server activity.

Mandatory access control

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.

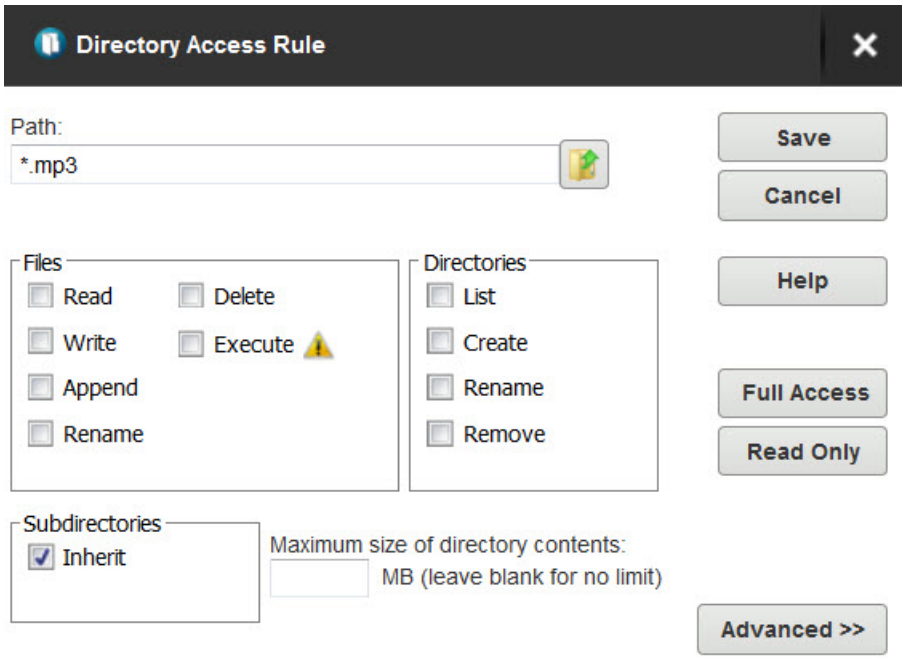
In the following example, the rule applies to `C:\ftproot\`.

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 Serv-U File Server.

Restrict file types

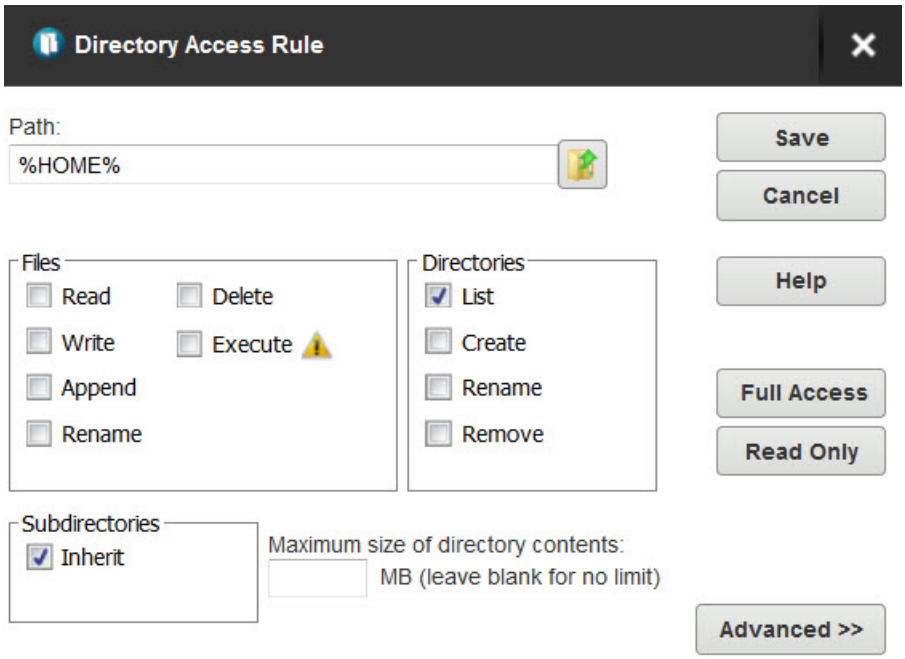
If users are using storage space on the Serv-U File Server to store non-work-related files, such as .mp3 files, you can prevent this by configuring a directory access rule placed above the main directory access rule to prevent .mp3 files from being transferred as shown below.

In the text entry for the rule, type `*.mp3`, and use the permissions shown beolw:



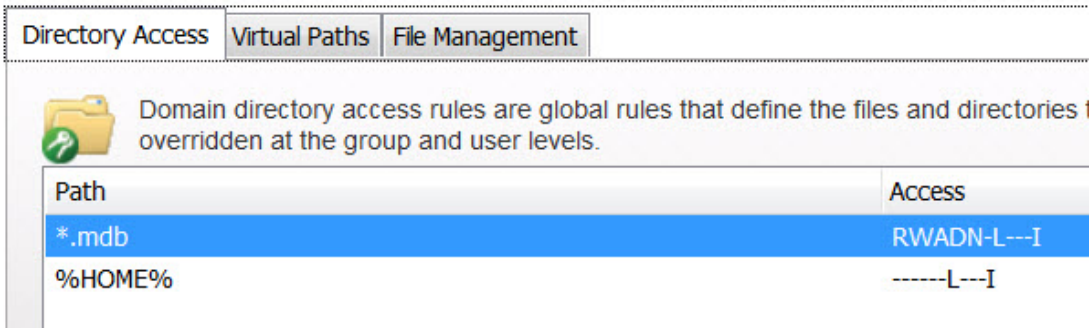
The rule denies permission to any transfer of files with the `.mp3` extension and can be modified to reflect any file extension. Similarly, if accounting employees only need to transfer files with the `.mdb` extension, configure a pair of rules that grants permissions for `.mdb` files but denies access 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.



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

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.



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. When virtual paths are created at the domain level, they are only accessible by users belonging to that domain.

You can also create virtual paths specifically for individual users or groups.

Physical path

The physical path is the actual location on the system, or network, that is to be placed in a virtual location accessible by a user. If the physical path is located on the same computer, 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 that the physical path should appear in for the user. The `%HOME%` macro is commonly used in the virtual path to place the specified physical path in the home directory of the user. When specifying the virtual path, the

last specified directory is used as the name displayed in directory listings to the user. For example, a virtual path of `%HOME%/public` places the specified physical path in a folder named `public` within the user's home directory. 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.

Virtual paths example

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 example

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 and group logs

In the Serv-U File Server, you can customize the logging of user and group events and

activity to a great extent. To enable a logging option, select the appropriate option in the Log Message Options grouping. When an option is selected, the appropriate logging information is saved to the specified log file if the Enable logging to file option is selected. 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.

Log to File settings

You must specify the name of the log file before information can be saved to a file. Click Browse to select an existing file or directory location for the log file. The log file path supports certain wildcard characters. 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. The following list contains the wildcard characters that you can use.

WILDCARD	DESCRIPTION
%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, 2015).
%X	The 2-digit value of the current year (for example, 15 for 2015).
%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.

Rotate the log file automatically

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.

Purge old 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`

The following wildcards can be used for log variables:

%H --> ??
%D --> ??
%N --> ??
%M --> *
%Y --> ????
%X --> ??
%S --> *
%G --> *
%L --> *
%U --> *

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.

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. 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 then add IP addresses as appropriate.

Group memberships

A user can be a member of any number of groups. Groups provide a convenient way of applying a base set of user attributes and settings to multiple users. For more information about configuring groups, see User groups.

Because a user can be a member of multiple groups, the order in which group memberships are presented is important. The first group membership for a user encountered by Serv-U that provides a value for an attribute is the value that is used. Use the arrows on the right side of the group membership list to arrange the order of group memberships.

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.

Domain events

You can automatically create a list of the most common events. You can choose to

create these common events using email or balloon tip actions. Click Create Common Event on the Events page. Select the Send Email or Show balloon tip option for the action you want to perform on the common events. If you choose to send email, enter an email address.

> The Write to Windows Event Log and Write to Microsoft Message Queue (MSMQ) options are available for Windows only.

Event actions

You can select from the following actions that are executed when an event is triggered:

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

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

Email actions

You can configure email actions to send emails to multiple recipients and to Serv-U groups when an event is triggered.

To add an email address, enter it in the To or Bcc fields. To send emails to a Serv-U group, use the Group icon to add or remove Serv-U groups from the distribution list. Separate email addresses by commas or semicolons. Email actions contain a To, Subject and Message parameter. You can use special variables to send specific data pertaining to the event. For more information about the variables, see System variables.

To use email actions, you must first SMTP configuration.

Balloon tip actions

You can configure a balloon tip to show in the system tray when an event is triggered. Balloon tip actions contain a Balloon Title and a Balloon Message

parameter. You can use special variables to send specific data pertaining to the event. For more information about the variables, see System variables.

Execute command actions

You can configure execute command actions to execute a command on 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 for no waiting.

> Time spent waiting delays any processing that Serv-U can perform.

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

Windows Event Log

By writing event messages to a local Windows Event Log, you can monitor and record Serv-U activity by using third-party network management software. All messages appear in the Windows Application Log from a source of Serv-U.

This event has only one field:

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

Microsoft Message Queuing (MSMQ)

Microsoft Message Queuing (MSMQ) is an enterprise technology that provides a method for independent applications to communicate quickly and reliably. Serv-U 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.

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 attempts to create it. This normally only works on public queues on the local machine. You can also use Serv-U 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 system variables can also be used in this field. This field may be left blank, but usually is not.

Microsoft message queues created in Windows do not grant access to SYSTEM by default, preventing Serv-U 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 runs) has permission to the queue.

Event filters

Use event filters to control when a Serv-U event is triggered. By default, events trigger each time the event occurs. The event filter allows events to be triggered only if certain conditions are met. For example, a standard 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. For example, you can configure a File Uploaded event to only send an email when the file name contains the string `important`, so an email would be sent when the file `Important Tax Forms.pdf` is uploaded but not when other files are uploaded to the server. Additionally, you can 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.

Event filter fields

Each event filter has the following critical values that must be set:

- Name: This is the name of the filter, used to identify the filter for the event.
- Description (Optional): This is the description of the event, which may be included for reference.
- Logic: This determines how the filter interacts with other filters for an event. In most cases, AND 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).
- Filter Comparison: This is the most critical portion of the filter. The Filter Comparison contains the evaluation that must occur for the event to trigger. For example, a filter can be configured so that only the user *admin* triggers the event. In this case, the comparison is `If $Name = (is equal to) admin`, and the data type is `string`. For bandwidth, either an unsigned integer or double precision floating point value is used.

Event filters also support wildcards when evaluating text strings. The supported wildcards include:

- `*` - 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`.

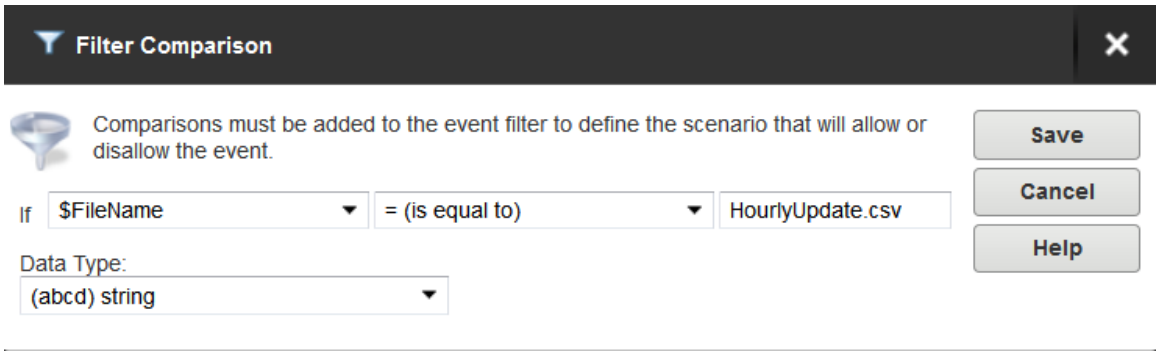
- `[]` - The bracket wildcard matches a character against the set of characters inside the brackets. For example:
  - An event filter that compares the `$FileName` variable to the string `data[687].txt` matches files named `data6.txt`, `data7.txt` and `data8.txt` but not `data5.txt`.
  - An event filter that compares the `$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.

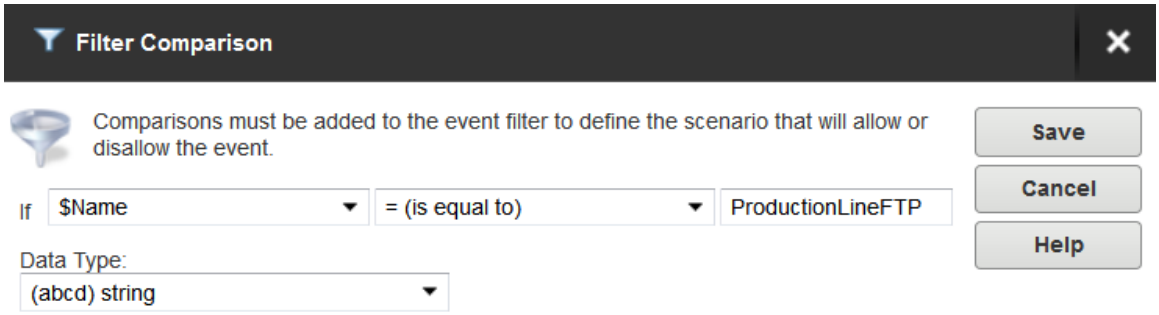
Event filters

Event filters are used by comparing fields to expected values in the Event Filter menu. The best example is raising an event only when a certain user triggers the action, or when a certain file is uploaded. For example, 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:

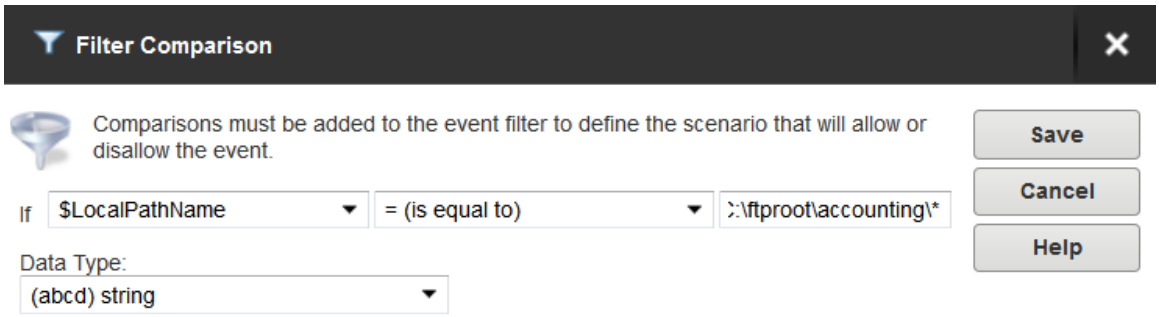


As another example, it may be necessary to know when a file transfer fails for a specific user account. To perform this task, create a new File Upload Failed event, and add a new filter.

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



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\`.



Server details

IP access rules restrict login access to specific IP addresses, ranges of IP addresses, or

a domain name. IP access rules can be configured at the server, domain, group, and user levels.

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

Specifying IP access masks

IP access rules use masks to authorize IP addresses and domain names. The masks can contain specific values, ranges, and wildcards made up of the following elements.

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`.

Caveats

Specific IP addresses listed in Allow rules will not be blocked by anti-hammering. These IP addresses are white-listed. However, addresses matched by a wildcard or a

range are subject to anti-hammering prevention.

Implicit deny all

Until you add the first IP access rule, connections from any IP address are accepted. After you add the first 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.

Matching all addresses

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.

DNS lookup

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 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.

Rule use during connection

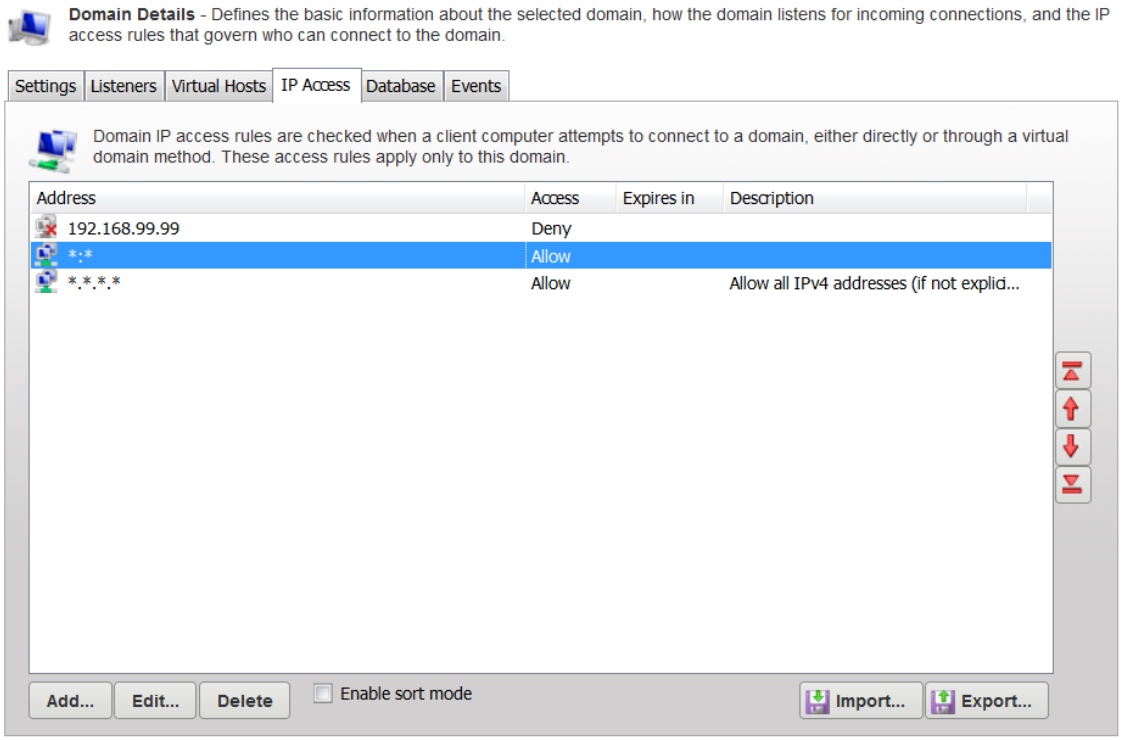
The level at which you specify an IP access rule also defines how far a connection is allowed before it is rejected. Server and domain level IP access rules are applied before the welcome message is sent. Domain level IP access rules are also applied when responding to the `HOST` command to connect to 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.

Anti-hammering

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. You can configure an anti-hammering policy server-wide in Server Limits and Settings > Settings and domain-wide in Domain Limits and Settings > Settings.

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.

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



IP access list controls

The following options are available on the IP Access page.

Using the sort mode

You can 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.

Importing and exporting IP access rules

You can export and import Serv-U IP access rules from users, groups, domains, and the server by using a text-based `.csv` file. To export IP access rules, view the list of rules to export, click Export, and specify the path and file name you want to save the list to. To import IP access rules, click Import and select the file that contains the rules you want to import. The `.csv` file must contain the following fields, including the headers:

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

Examples of IP address rules

Office-only access

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 access rule 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 provides an implicit Deny All rule at the end of the list.

Prohibited computers

Users should normally be able to access Serv-U 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 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.

DNS-based access control

The only users allowed to access a Serv-U domain connect from `*.example.com` or `*.example1.com`. The related Serv-U 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 provides an implicit Deny All rule at the end of the list.

Limits and settings

Serv-U contains options which you can use to customize how Serv-U can be used, and which also provide ways to apply limits and custom settings to users, groups, domains, and the server in its entirety. The limits stack intelligently, with user settings overriding group settings, group settings overriding domain settings, and domain settings overriding server settings. In addition, you can configure limits so that they are only applied during certain days of the week, or certain times of the day. You can also grant exceptions to administrators and restrict specific users more than others, providing total control over the server.

The limits and settings in Serv-U are divided into the following categories:

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

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

- In the Serv-U Management Console, click Domain > Domain Limits & Settings.
- From the Limit Type list, select Directory Listing.
- Click Add.
- From the Limit list, select Lock users in home directory.
- Deselect the option.
- Click Save.

The limits list displays the current limits applied to the domain. Limits with a light-

blue background are default values. Limits with a white background are values that override the default values. After you complete the previous steps, a new Lock users in home directory limit appears in the list that displays "No" as the value. Because of inheritance rules, this option applies to all users in the domain unless it is overridden at the group or user level. For more information about this method of inheritance, see User interface conventions.

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

To create a limit that is restricted to a specific time of day or days of the week, click Advanced in the New Limit or Edit Limit window. Select Apply limit only at this time of day to specify a start and stop time for the new limit. To restrict the limit to certain days of the week, deselect the days for which you do not want to apply the limit. When a limit is restricted in this way, default values (or the value of other limit overrides) are applied when the time of day or day of the week restrictions are not met for this limit.

Transfer ratios and quotas

Transfer ratios and quotas are just one of the many ways in which file transfers are managed on the Serv-U File Server. The following sections provide information about their usage.

Transfer ratios

Transfer ratios are a convenient way of encouraging file sharing on your file server. By specifying an appropriate transfer ratio setting, you can grant credits to the user for transferring a specified number of bytes or complete files. This is commonly used to grant a user the ability to download 'x' megabytes of data or files for every 'y' megabytes of data or files that they upload.

To enable transfer ratios for the current user account, click Ratios & Quotas on the User Information page of the User Properties window, and then select Enable transfer ratio. Select the appropriate type of ratio to impose on the user account. Ratios can be tracked in terms of megabytes or complete files. They can also be tracked per session established or for all sessions established by the user account.

The ratio itself is configured by assigning a numeric value to both the uploads and downloads side of the ratio. For example, a 3:1 ratio that is counting files over all sessions means that the user account must upload 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.

Quotas

Quotas are another way to limit the amount of data that is transferred by a user account. When a Maximum quota value is assigned to the user, they are not able to use more disk space than that value. The Current field shows how much disk space is currently being used by the user account. When initially configuring a quota, both fields must be filled in. From that point on, Serv-U tracks the file uploads and deletions made by the user and updates the current value as appropriate.

> 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 a user must upload files in order to earn credits towards downloading a file, a file that matches an entry in this list can always be downloaded by users, even if they have no current credits. This is commonly used to make special files, such as a readme or a directory information file, always accessible to users.

You can use the `*` and `?` wildcard characters when you specify a ratio free file. Using `*` specifies a wildcard of any kind of character and any length. For example, entering `*.txt` makes any file with a `.txt` extension free for download, regardless of the actual filename. You can use a `?` to represent a single character within the file name or directory. You can also specify full paths by using standard directory paths such as `C:\ftproot\common\` (on Windows) or `/var/ftpfiles/shared/` (on Linux).

In addition, you can use full or relative paths when you are specifying an entry. If you use a full path when you specify a file name, only that specific file is exempt from transfer ratios. If you use a relative path, such as when you enter just `readme.txt`, the provided file is exempt from transfer ratios regardless of the directory it is located in.

Compare Windows and LDAP authentication

Both LDAP and Active Directory are 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 users and LDAP users

Windows and LDAP Users are similar in many ways but there are a number of important differences that can help you decide which type of user is right for your environment.

Use Windows users if the following conditions apply:

- You only want to access one Windows machine or domain (per Serv-U domain).
- You want each end user to see that user's home folders and enjoy that user's NTFS permissions. Serv-U uses impersonation so that it respects the Windows directory access rules. The Windows directory access rules can be supplemented with directory access rules defined in Serv-U. For more information, see Directory access rules.

Use LDAP users if the following conditions apply:

- You want to deploy Serv-U on Linux.
- You want to be able to access more than one Windows domain.
- You want to be able to access different Windows domains.
- You do not care about natively incorporating NTFS permissions. It is not possible to pull directory access rules from LDAP directly, but you can define Serv-U directory access rules for LDAP users. For more information, 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
- Integrate Serv-U with Windows accounts
- Windows Groups and Organizational Units in Serv-U
- Enable Windows User NT-SAM - Active Directory Support in Serv-U

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.

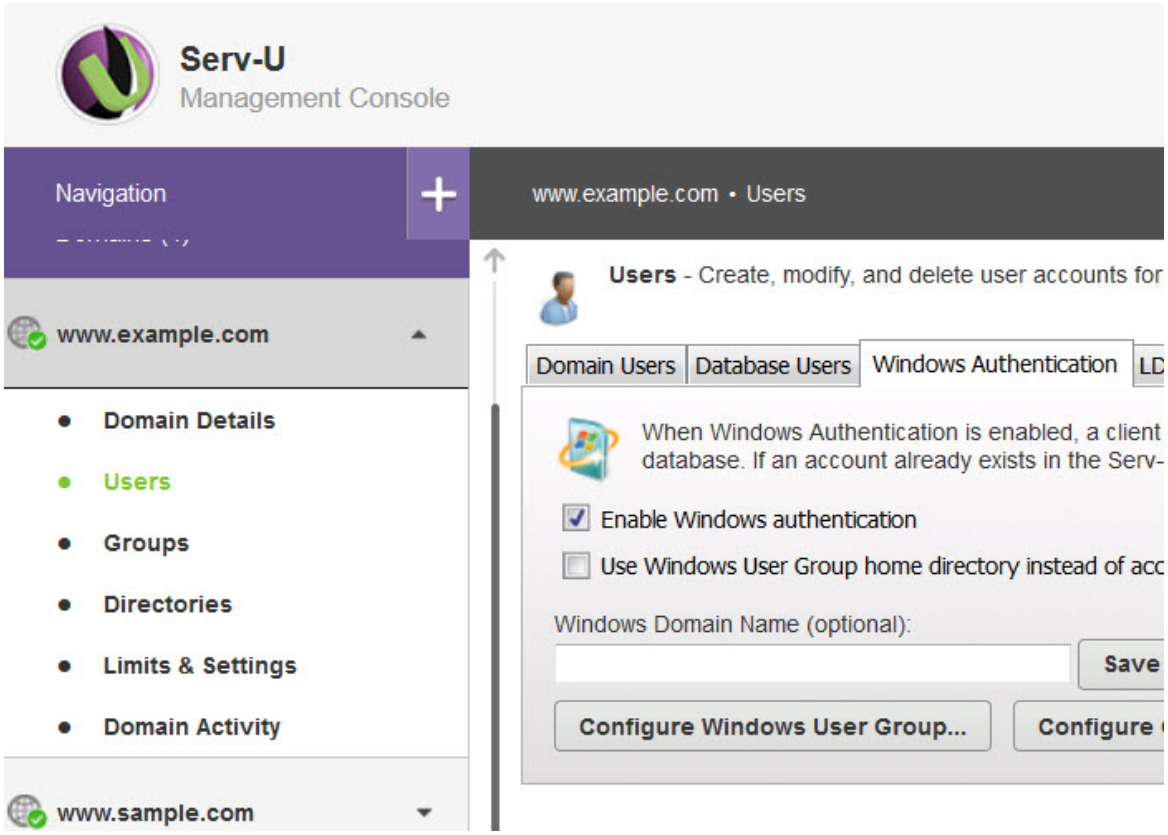
For upgrade, backup, and migration information, refer to the following resources:

- Upgrade to the Latest Version of Serv-U
- Back up or move Serv-U settings

Windows authentication

By enabling Windows authentication, users can log in to Serv-U using their Windows login credentials as provided by the local Windows account database or a specific Windows domain server (Active Directory). When logging in using their Windows account, users are placed in the home directory for their Windows account eliminating the need to manually specify a home directory.

To enable Windows authentication, select Enable Windows authentication.



To authenticate to Active Directory or a Windows domain server, enter a specific domain name in this field and ensure your Serv-U computer is a member of that domain. If the system is a member of a Windows domain, the domain name can be entered in this field to have user logins authorized by the domain server. After changing this field, click Save to apply the changes.

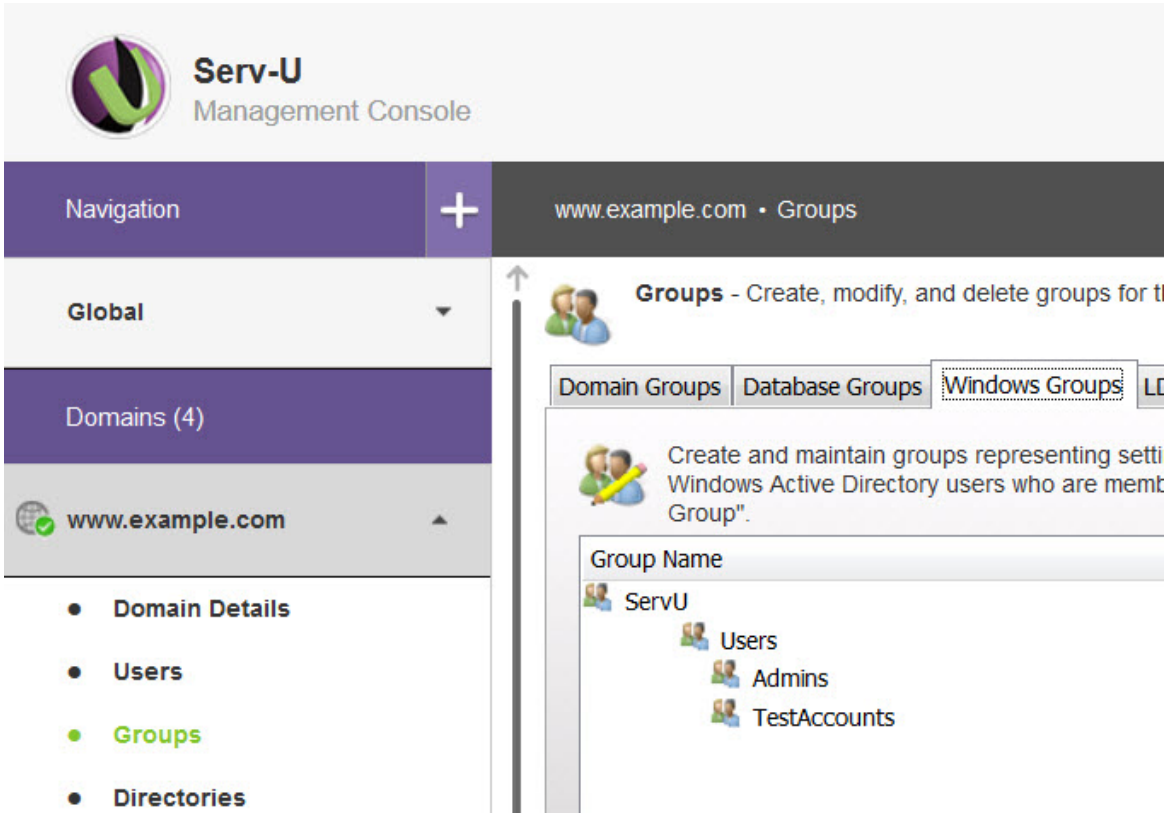
Use a Windows user group home directory instead of the account home directory

By default, Serv-U uses the Windows account's home directory when a client logs in using a Windows user account. Enabling this option causes Serv-U to use the home directory specified in the Windows user group instead. If no home directory is specified at the group level, then the Windows user account's home directory is still used.

Windows user groups

Windows user accounts are not visible, and they cannot be configured on an

individual basis in Serv-U. To aid in configuring the many advanced options of a local user account, all Windows user accounts are a member of a special Windows user group. Click Configure Windows User Group to configure this group just like a normal group.



All settings configured in this group are inherited by Windows user accounts. This feature can be used to add IP access rules, specify bandwidth limitations, or add additional directory access rules.

For more information, see User groups.

Windows user permissions

By default, Windows and Active Directory user accounts do not require any directory access rules to be configured because Serv-U automatically applies their NTFS permissions to their login sessions. This way, administrators do not need to configure specific permissions beyond those already defined on the network, saving time and documentation.

In some cases Windows may cache directory access rules for a short period of time. If an important NTFS permissions change is made that requires immediate application, restarting the Serv-U service can force Windows to provide the updated permissions to the Serv-U File Server.

LDAP authentication

If LDAP authentication is enabled, users can log in to Serv-U using login credentials as provided by a remote LDAP server, such as Active Directory or OpenLDAP. LDAP users can use a home directory from their LDAP account, eliminating the need to manually specify a home directory.

Before you begin

Before you begin the configuration of LDAP authentication, consider the following steps:

- 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.

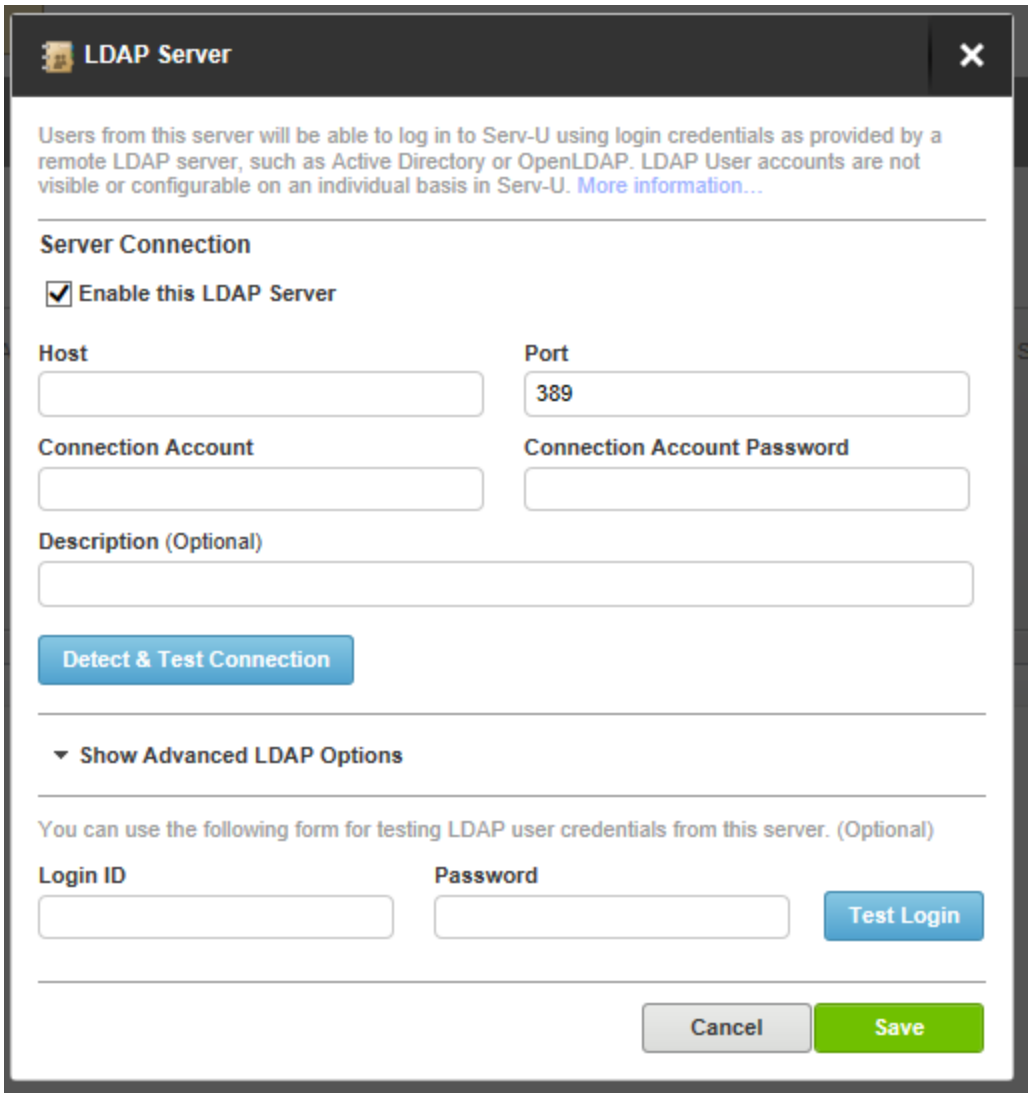
To decide between LDAP authentication and Windows user authentication, see Compare Windows and LDAP authentication.

The examples and illustrations in this topic show a Serv-U instance configured to use authentication through Active Directory.

To start configuring LDAP authentication, navigate to Users > LDAP Authentication in the Serv-U Management Console.

Configure the LDAP server

The LDAP Server configuration dialog is displayed when you click Add, Edit, or Copy on the LDAP Servers list.



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.
- 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 often be 389.

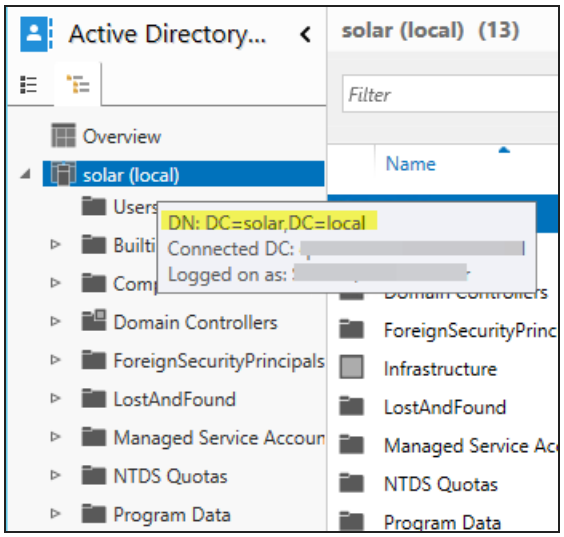
- Connection Account: The user name of the account that is used to connect to the LDAP server and execute queries against it. Provide the account name complete with the UPN suffix. Serv-U does not automatically apply the UPN suffix for the name you provide here.
- Connection Account Password: The password belonging to the account that is used to connect to the LDAP server and execute queries against the LDAP server.

  > If the Connection Account credentials are not supplied, then the credentials that are being authenticated are used.

- Description: An optional field in which you can write more notes about your LDAP server.
- Show Advanced LDAP Options: Select to access the Base DN option.

  Base DN: 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`.

  To determine the correct Base DN, hover over the main node of the LDAP server, and look for the highlighted information.



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, Softerra 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.

The configuration of the following values in the Attribute Mapping grouping is optional.

- 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`.
- 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`.
- 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.
- Group Membership: This field uses all the values found in the named LDAP attribute as additional LDAP Group membership assigments. For example, if this is configured as `grp` and an LDAP user record has both `grp=Green` and `grp=Red` attributes, Serv-U associates that LDAP User with both the "Red" and "Green" LDAP Groups. A typical value on Active Directory is `memberOf`.

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 Groups > LDAP Groups page. If this option is selected, and LDAP Users cannot be matched up to at least one LDAP Group, they will not be allowed to sign on. In this case it is possible that Serv-U successfully authenticates to the LDAP server, and then rejects the user login because the user is not a member of any group.

For more information about group permissions and settings, see User 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.

To configure LDAP groups in Serv-U:

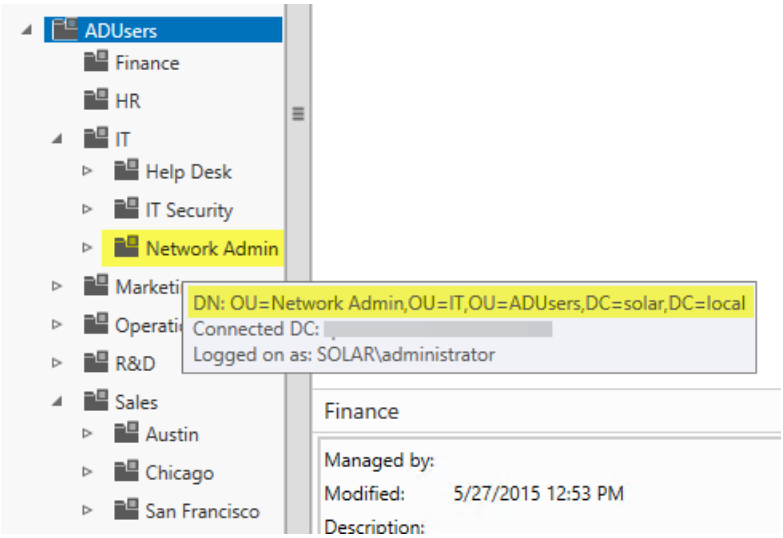
1. Navigate to Users > LDAP Authentication.
2. Click Configure LDAP Groups.

LDAP groups have the same configuration options as other Serv-U groups. For information about the configuration options available at the group level, see LDAP user groups.

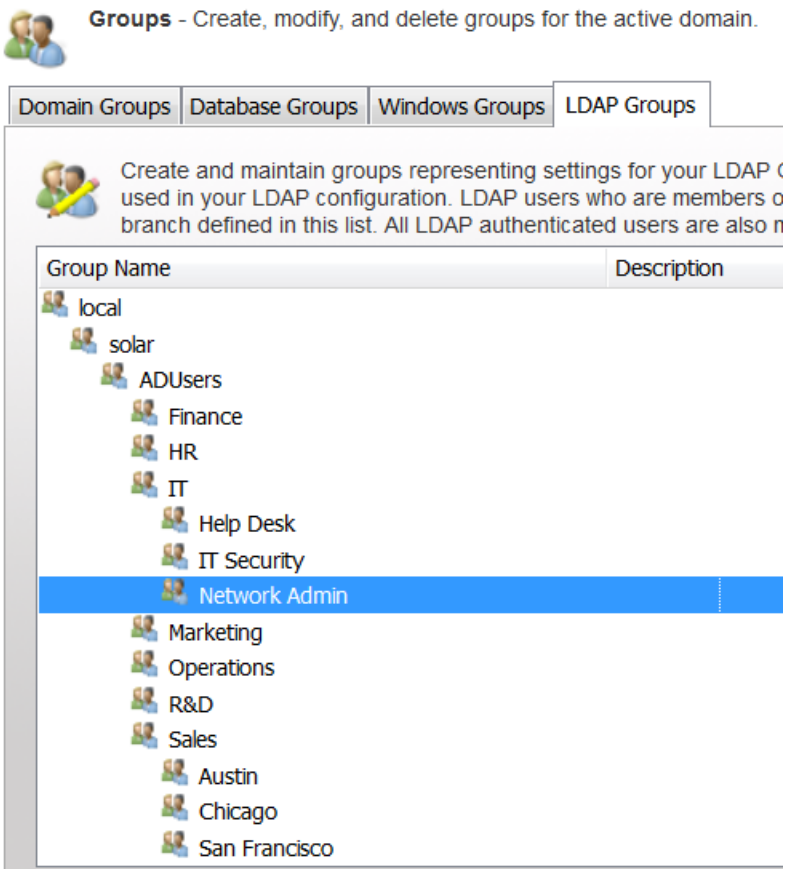
When you configure LDAP groups, recreate the same structure as the group structure in Active Directory, and use the same names as the group names in Active Directory.

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.

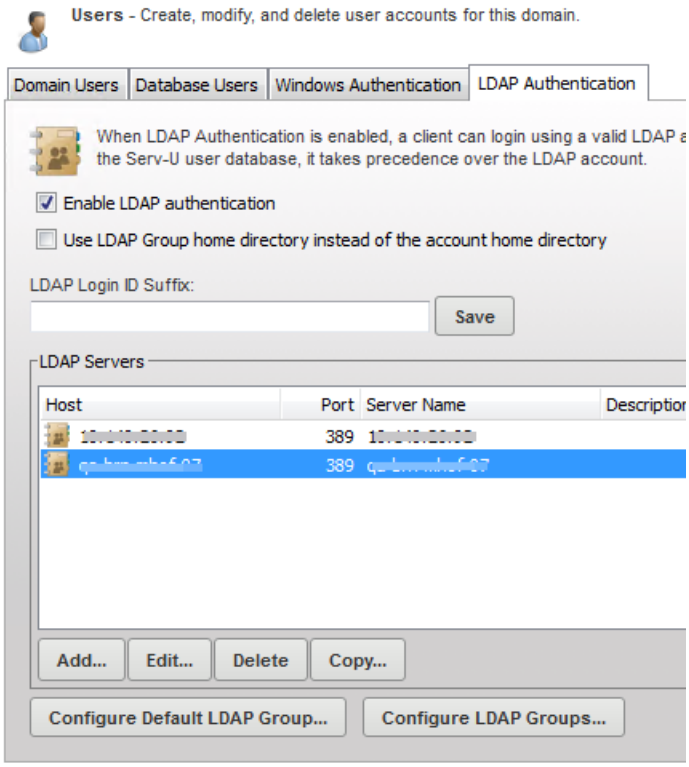
Serv-U attempts authentication against the list of LDAP servers from top to bottom. During login, the first LDAP server that approves a set of credentials will be the server from which the associated LDAP user will draw its full name, email address and other attributes.

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.



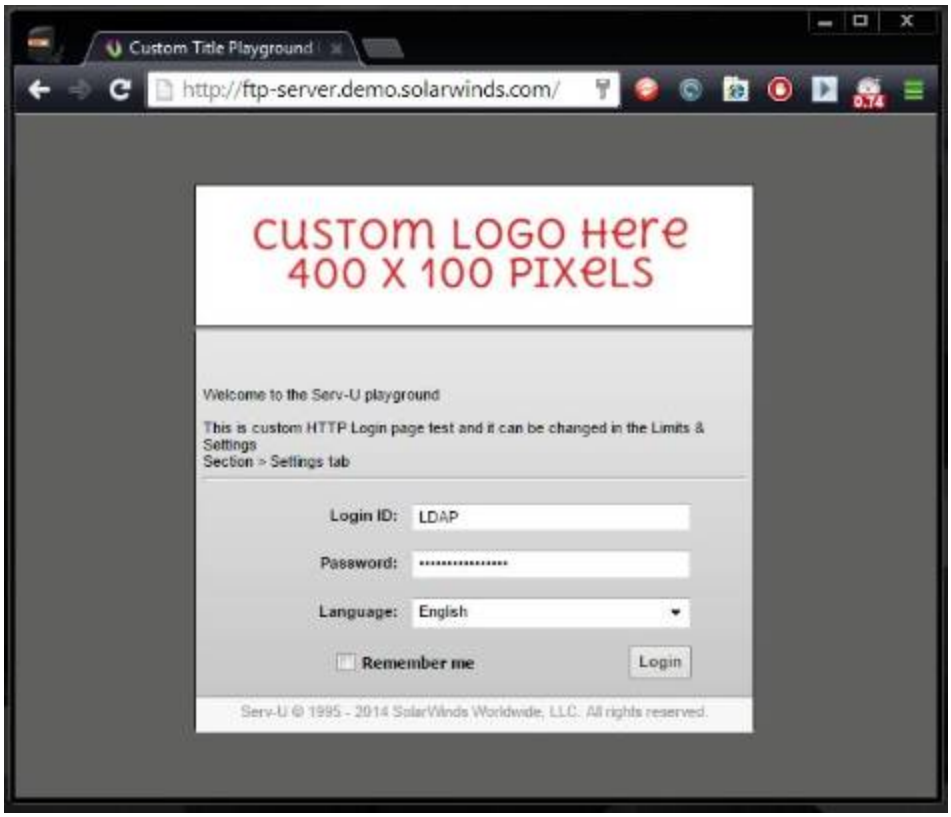
Use the Add, Edit, Delete, and Copy buttons to work with individual LDAP server entries. When there are multiple LDAP server entries in the list, selecting any entry will reveal move up, move down, move to top, and move to bottom ordering arrows on the right of the window.

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 Search Filter.
- 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:

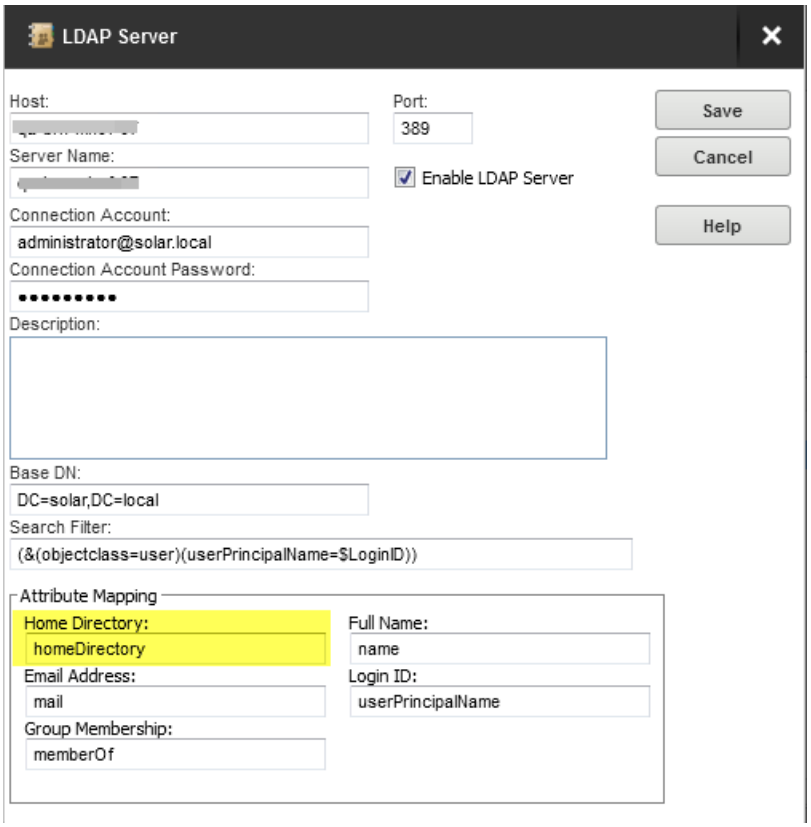
1. In the Serv-U Management Console, navigate to Users > LDAP Authentication.
2. Select Enable LDAP Authentication.

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

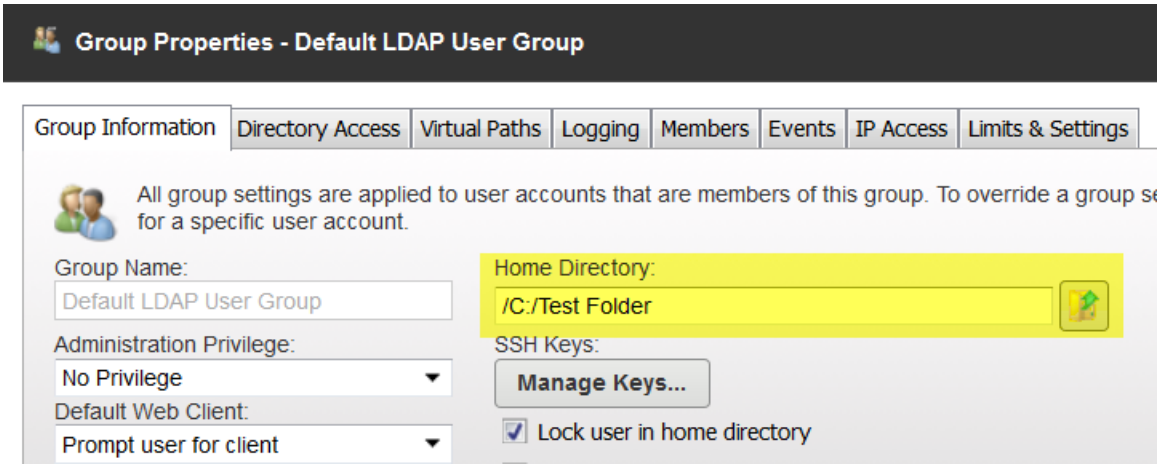
By default, Serv-U uses the LDAP account's home directory when an LDAP user logs in. This is the value of the Home Folder LDAP attribute that is specified in the LDAP server configuration, as highlighted in the following image.



For information about configuring the LDAP account's home directory, see Configure the LDAP server.

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.

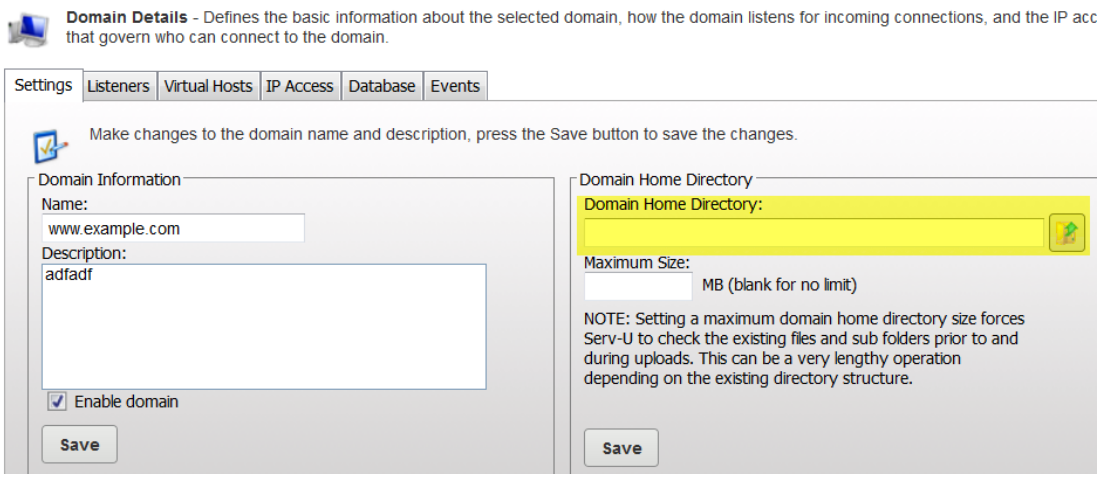


For information about configuring the Default LDAP User Group, see Use LDAP user groups.

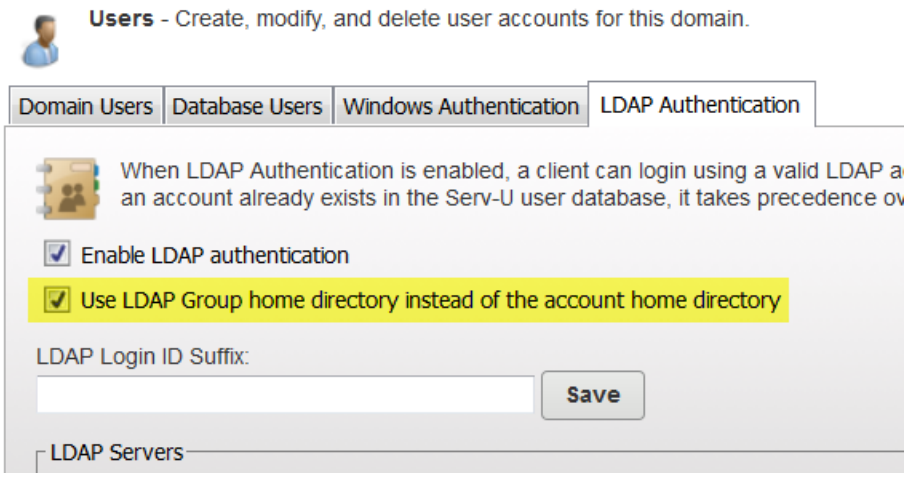
If no home directory is specified at the group level, then the LDAP account's home directory is still used. However, if no home directory is defined at the user, group, domain, or system level, and none is available from the LDAP server, the user will not be allowed to sign on.

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.



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.



SFTP for users and groups

Use an existing public key

1. Obtain a public key file.
2. Place the public key file in a secured directory in the server, and then use Browse in Serv-U to select the file.
3. Click Save.

Create a key pair

1. Click Manage Keys.
2. Click Create Key.
3. Type the name of the key pair (for example, `MyKey`), which is also used to name the storage file.
4. Type the output directory of the certificate (for example, `C:\ProgramData\SolarWinds\Serv-U\`).
5. Select the key type (default of DSA is preferred, but RSA is available).
6. Select the key length (default of 1024 bits provides best performance, 2048 bits is a good median, and 4096 bits provides best security).

7. Enter the password to use for securing the key file.
8. Click Create.

Create multiple keys per user

For the purposes of public key authentication, you can associate multiple public keys with a user account.

To create multiple keys for an account:

1. Click Manage Keys.
2. Click Add Key, and then specify the key name and the key path.

When authenticating a client, Serv-U 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.

Groups

User groups

Groups are a method of sharing common configuration options with multiple user accounts. Configuring a group is similar to configuring a user account. Virtually every configuration option available for a user account can be set at the group level. In order for a user to inherit a group's settings, it must be a member of the group. Permissions and attributes inherited by a user through group membership can still be overridden at the user level. A user can be a member of multiple groups in order to acquire multiple collections of permissions, such as directory or IP access rules.

Like user accounts, groups can be created at multiple different levels, including the following:

- Global Groups
- Domain Groups
- Database Groups (available at both the server and domain levels)
- Windows Groups

However, groups are only available to user accounts that are defined at the same level. In other words, a global user (that is, a user defined at the server level) can only be a member of a global group. Likewise, a user defined for a specific domain can only be a member of a group also created for that domain. This restriction also applies to groups created in a database in that only users created within a database at the same level can be members of those groups.

Use the Add, Edit, and Delete buttons to manage the available groups.

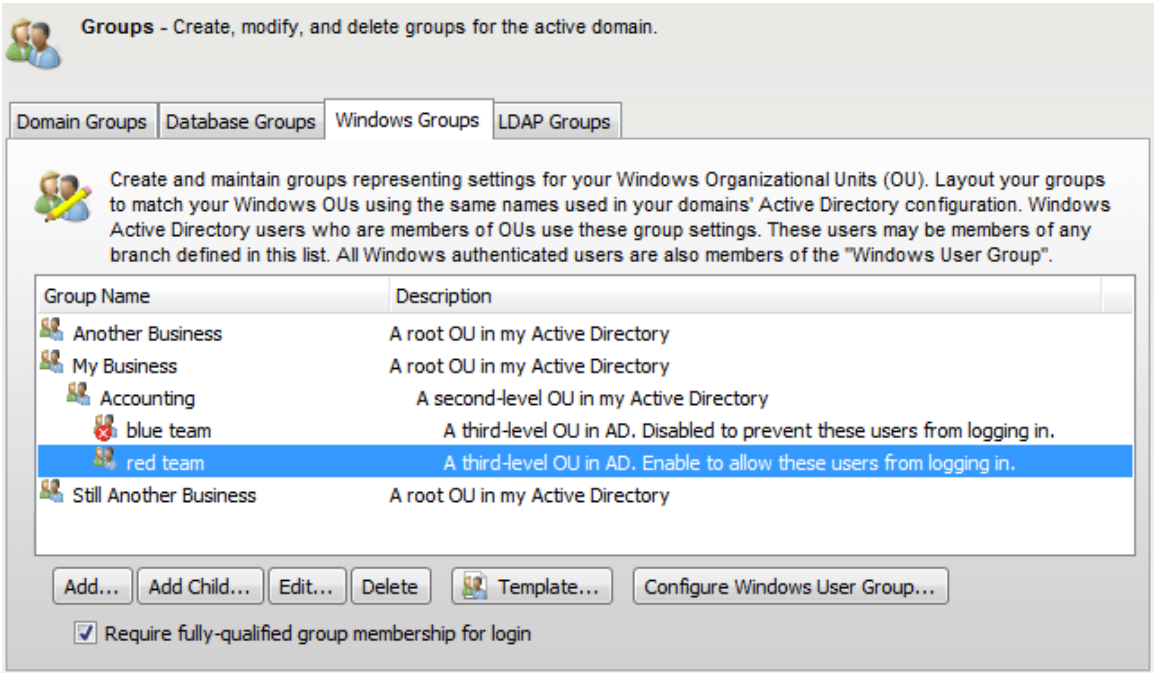
Group templates

You can configure a template for creating new groups by clicking Template. The template group can be configured just like any other group object, 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 the template. This way you can configure some basic settings that you want all of your groups to use by default.

Windows groups (Windows only)

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. (Visually, "My Business" would be the top Windows group, "Accounting" would be an indented child Windows group under that, and "red team" would be an indented child under "Accounting".)

Membership in one or more Windows Groups is required if the Require fully-qualified group membership for login option is selected on the Windows Groups page. If this option is selected and Windows users cannot be matched up to at least one Windows group, they are not be allowed to log in.

Windows groups are only available when the following conditions apply:

- Serv-U is running on Windows.
- Serv-U has an MFT Server license.
- Windows Authentication is enabled under Domain Users > Windows Authentication.

Configure a Windows user group (Windows only)

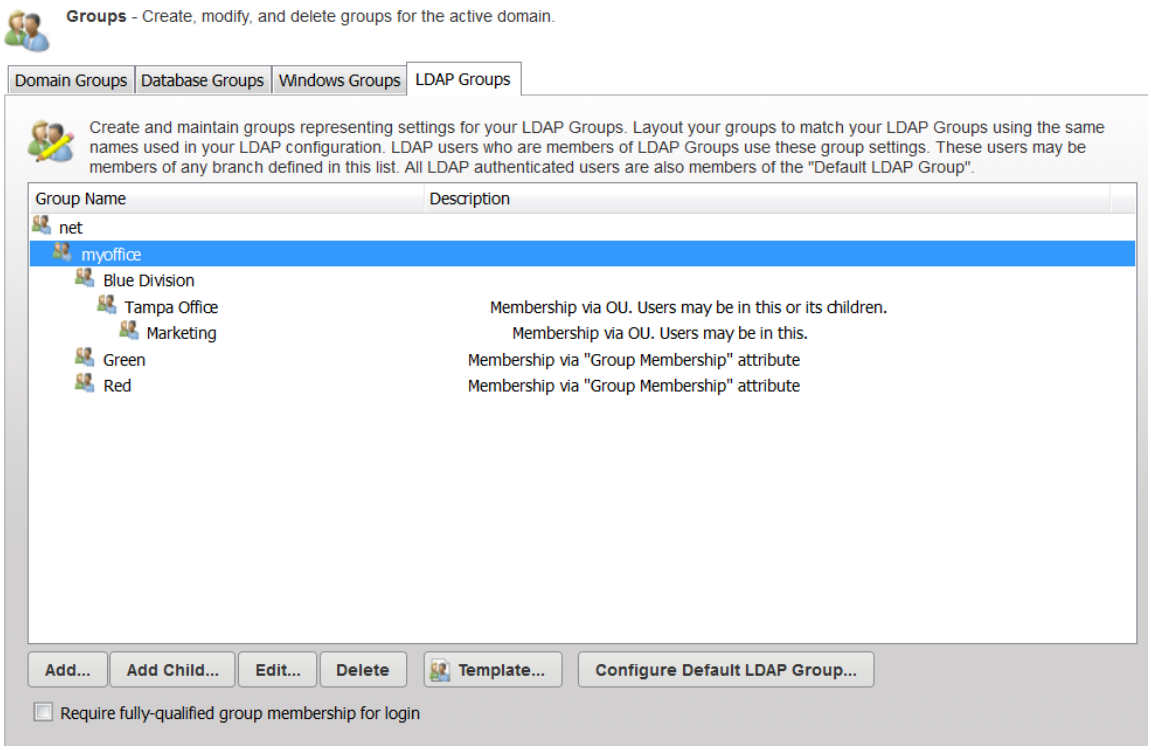
Administrators can allow clients to log in to the file server using the local Windows user database or one that is made accessible through a domain server. These user accounts do not exist in the local Serv-U user database and cannot be configured on an individual basis. To aid in configuring these accounts,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

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.

For more information about LDAP authentication, see LDAP authentication.

Group information

Virtually every attribute available for a user account can be configured at the group level. Group level settings are inherited by the group members and can be overridden at the user level. The Group Information tab contains general information about the group including the name, home directory, and the default administrative privilege for group members. The following sections contain detailed information about each of the available attributes.

Group name

The group name is a unique identifier that must be unique for each group specified at the particular level (server or domain). Group names may not contain any of the following special characters:

```
\ / < > . | : ? *
```

Home directory

The home directory for a user account is where the user is placed immediately after logging in to the file server. Each user must have a home directory assigned to it, although the home directory can be specified at the group level if the user is a member of a group. Home directories must be specified using a full path including the drive letter or the UNC share name. If the home directory is not found, Serv-U can be configured to create it.

When specifying the home directory, you can use the %USER% macro to insert the login ID into the path. This is used mostly to configure a default home directory at the group level or within the new user template to ensure that all new users have a unique home directory. When combined with a directory access rule for %HOME%, a new user can be configured with a unique home directory and the proper access rights to that location with a minimal amount of effort.

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 users, allowing them the ability to access all system drives. In order for this to work properly, the user must not be locked in their home directory.

Administration privilege

A user account can be granted one of the following types of administrative privileges:

- No Privilege
- Group Administrator
- Domain Administrator
- System Administrator

The value of this attribute can be inherited through group membership.

A user account with no privilege is a regular user account that can only log in to transfer files to and from the file server. The Serv-U Management Console is not available to these user accounts.

A group administrator can only perform administrative duties relating to their primary group (the group that is listed first in their group 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.

A domain administrator can only perform administrative duties for the domain to which their account belongs. A domain administrator is also restricted from performing domain-related activities that may affect other domains. The domain-related activities that may *not* be performed by domain administrators consist of configuring their domain listeners or configuring ODBC database access for the domain.

A system administrator can perform any file server administration activity including creating and deleting domains, user accounts, or even updating the license of the file server. A user account with system administrator privileges that is logged in through HTTP remote administration can essentially administer the server as if they had physical access to the system.

Default web client

If your Serv-U license enables the use of FTP Voyager JV, then users connecting to the file server through HTTP can choose which client they want to use after logging in. Instead of asking users which client they want to use, you can also specify a default client. If this option is changed, it overrides the option specified at the server or domain level. It can also be inherited by a user through group membership. Use the Inherit default value option to reset it to the appropriate default value.

Lock user in home directory

Users who are locked in their home directory cannot 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.

Apply group directory access rules first

The order in which directory access rules are listed has significance in determining the resources that are available to a user account. By default, directory access rules specified at the group level take precedence over 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.

Always allow login

Enabling this option means that the user account is always permitted to log in, regardless of restrictions placed upon the file server such as maximum number of sessions. It is useful as a fail-safe in order to ensure that critical system administrator accounts can always remotely access the file server. 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.

Enabling the Always Allow Login option does not override IP access rules. If both options are defined, the IP access rules prevail.

Description

The description allows for the entry of additional notes that are only visible by administrators.

Availability

This feature limits when users can connect to this server. You can place limitations on the time of day and also on the day of the week. When users attempt to log in outside the specified available times, they are presented with a message that their user account is currently unavailable.

Directory access rules

Directory access rules define the areas of the system which are accessible to user accounts. While traditionally restricted to the user and group levels, in Serv-U, the usage of directory access rules is extended to both the domain and the server levels through the creation of global directory access rules. Directory access rules specified at the server level are inherited by all users of the file server. 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 they are listed. The first rule in the list that matches the path of a client's request is the one that is applied for that rule. In other words, if a rule exists that denies access to a particular subdirectory but is listed below the rule that grants access to the parent directory, then a user still has access to the 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 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.

File permissions

PERMISSION	DESCRIPTION
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	DESCRIPTION
	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 permissions

PERMISSION	DESCRIPTION
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 permissions

PERMISSION	DESCRIPTION
Inherit	Allows all subdirectories to inherit the same permissions as the parent

PERMISSION	DESCRIPTION
	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.

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, you can configure the Serv-U File Server service to run under a network account. The alternative, preferred when many servers exist, or if the Serv-U File Server service 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.

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.

Quota permissions

Maximum size of directory contents

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

changes made to the directory contents outside of a user's file server activity.

Mandatory access control

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.

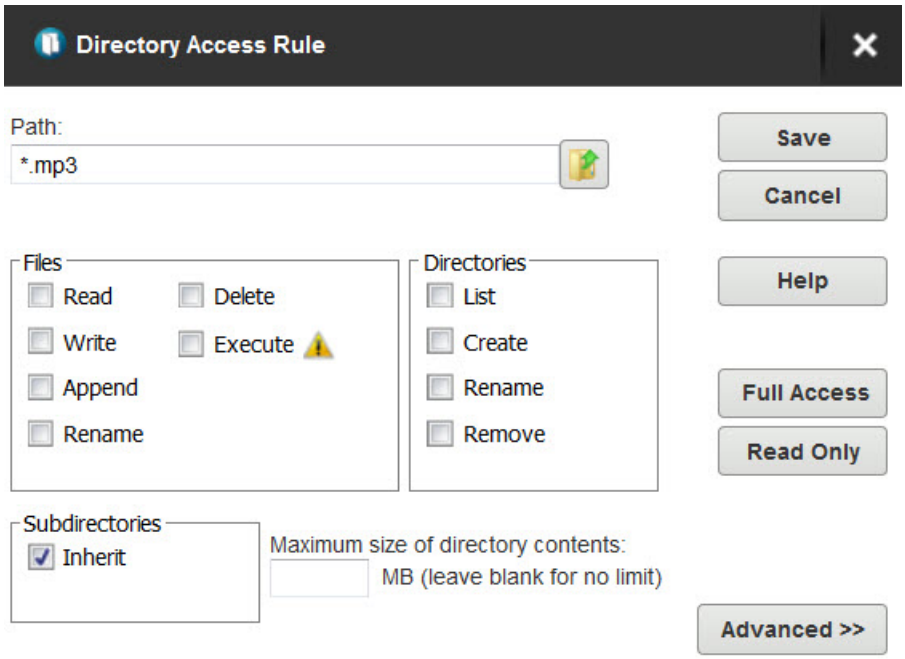
In the following example, the rule applies to `C:\ftproot\`.

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 Serv-U File Server.

Restrict file types

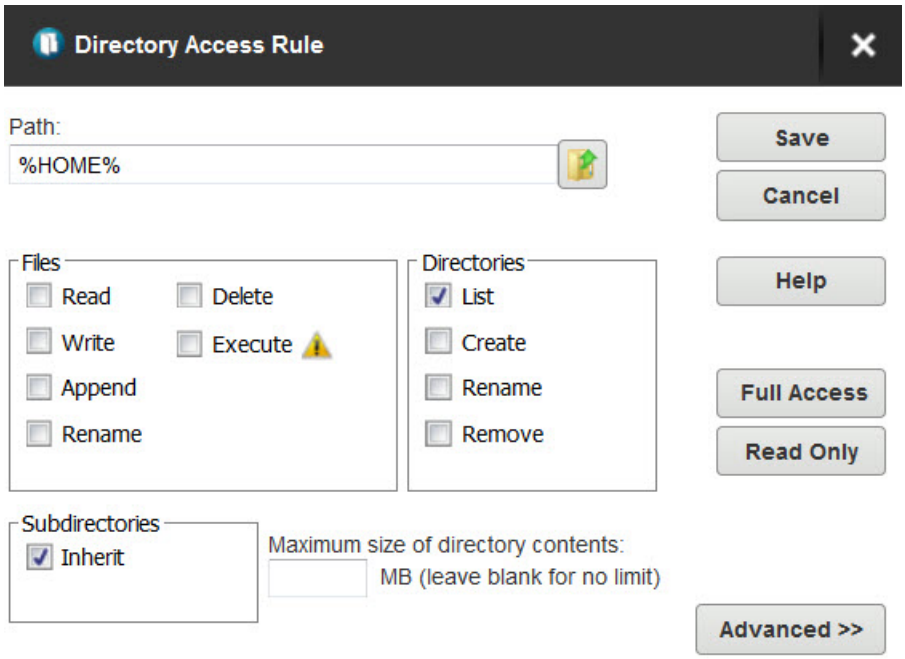
If users are using storage space on the Serv-U File Server to store non-work-related files, such as .mp3 files, you can prevent this by configuring a directory access rule placed above the main directory access rule to prevent .mp3 files from being transferred as shown below.

In the text entry for the rule, type `*.mp3`, and use the permissions shown beolw:



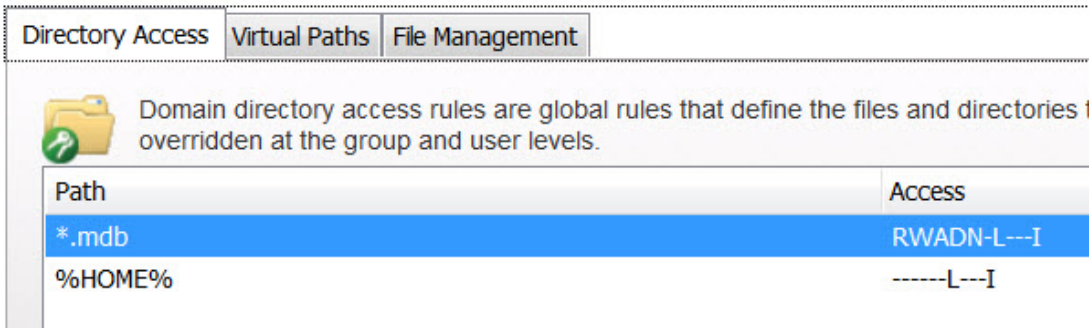
The rule denies permission to any transfer of files with the `.mp3` extension and can be modified to reflect any file extension. Similarly, if accounting employees only need to transfer files with the `.mdb` extension, configure a pair of rules that grants permissions for `.mdb` files but denies access 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.



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

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.



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. When virtual paths are created at the domain level, they are only accessible by users belonging to that domain.

You can also create virtual paths specifically for individual users or groups.

Physical path

The physical path is the actual location on the system, or network, that is to be placed in a virtual location accessible by a user. If the physical path is located on the same computer, 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 that the physical path should appear in for the user. The `%HOME%` macro is commonly used in the virtual path to place the specified physical path in the home directory of the user. When specifying the virtual path, the

last specified directory is used as the name displayed in directory listings to the user. For example, a virtual path of `%HOME%/public` places the specified physical path in a folder named `public` within the user's home directory. 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.

Virtual paths example

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 example

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 and group logs

In the Serv-U File Server, you can customize the logging of user and group events and

activity to a great extent. To enable a logging option, select the appropriate option in the Log Message Options grouping. When an option is selected, the appropriate logging information is saved to the specified log file if the Enable logging to file option is selected. 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.

Log to File settings

You must specify the name of the log file before information can be saved to a file. Click Browse to select an existing file or directory location for the log file. The log file path supports certain wildcard characters. 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. The following list contains the wildcard characters that you can use.

WILDCARD	DESCRIPTION
%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, 2015).
%X	The 2-digit value of the current year (for example, 15 for 2015).
%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.

Rotate the log file automatically

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.

Purge old 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`

The following wildcards can be used for log variables:

%H --> ??
%D --> ??
%N --> ??
%M --> *
%Y --> ????
%X --> ??
%S --> *
%G --> *
%L --> *
%U --> *

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.

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. 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 then add IP addresses as appropriate.

Group 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's account properties window.

A user account can be granted one of four types of administrative privileges:

- No Privilege
- Group Administrator
- Domain Administrator
- System Administrator

The value of this attribute can be inherited through group membership. A user account with no privilege is a regular user account that can only log in to transfer files to and from the file server. The Serv-U Management Console is not available to these user accounts.

A group administrator can only perform administrative duties relating to their primary group (the group that is listed first in their groups memberships list). They can add, edit, and delete users which are members of their primary group, and they can also assign permissions at or below the level of the group administrator. They may not make any other changes.

A domain administrator can only perform administrative duties for the domain to which their account belongs. A domain administrator is also restricted from performing domain-related activities that may affect other domains. The domain-related activities that may not be performed by domain administrators consist of configuring their domain listeners or configuring ODBC database access for the domain.

A system administrator can perform any file server administration activity including creating and deleting domains, user accounts, or even updating the license of the file server. A user account with system administrator privileges that is logged in through HTTP remote administration can essentially administer the server as if they had physical access to the system.

Serv-U also supports read-only administrator accounts which can allow administrators to log in and view configuration options at the domain or server level, greatly aiding remote problem diagnosis when working with outside parties. Read-only administrator privileges are identical to their full-access equivalents, except that they cannot change any settings or create, delete or edit user accounts.

When you configure a user account with administrative privileges, take care in specifying their home directory. An administrator with a home directory other than "\" (root) that is locked in their home directory may not use absolute file paths outside of their home directory when configuring the file server. Instead, relative paths must be used.

Additionally, such a user account can also use setting files located outside the home directory, however, these files must also be specified by using relative paths, for example, `../../exampleFile.txt`.

Domain events

You can automatically create a list of the most common events. You can choose to create these common events using email or balloon tip actions. Click Create Common Event on the Events page. Select the Send Email or Show balloon tip option for the action you want to perform on the common events. If you choose to send email, enter an email address.

> The Write to Windows Event Log and Write to Microsoft Message Queue (MSMQ) options are available for Windows only.

Event actions

You can select from the following actions that are executed when an event is triggered:

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

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

Email actions

You can configure email actions to send emails to multiple recipients and to Serv-U groups when an event is triggered.

To add an email address, enter it in the To or Bcc fields. To send emails to a Serv-U group, use the Group icon to add or remove Serv-U groups from the distribution list. Separate email addresses by commas or semicolons. Email actions contain a To, Subject and Message parameter. You can use special variables to send specific data pertaining to the event. For more information about the variables, see System variables.

To use email actions, you must first SMTP configuration.

Balloon tip actions

You can configure a balloon tip to show in the system tray when an event is triggered. Balloon tip actions contain a Balloon Title and a Balloon Message parameter. You can use special variables to send specific data pertaining to the event. For more information about the variables, see System variables.

Execute command actions

You can configure execute command actions to execute a command on 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 for no waiting.

> Time spent waiting delays any processing that Serv-U can perform.

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

Windows Event Log

By writing event messages to a local Windows Event Log, you can monitor and record Serv-U activity by using third-party network management software. All messages appear in the Windows Application Log from a source of Serv-U.

This event has only one field:

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

Microsoft Message Queuing (MSMQ)

Microsoft Message Queuing (MSMQ) is an enterprise technology that provides a

method for independent applications to communicate quickly and reliably. Serv-U 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.

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 attempts to create it. This normally only works on public queues on the local machine. You can also use Serv-U 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 system variables can also be used in this field. This field may be left blank, but usually is not.

Microsoft message queues created in Windows do not grant access to SYSTEM by default, preventing Serv-U 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 runs) has permission to the queue.

Event filters

Use event filters to control when a Serv-U event is triggered. By default, events trigger each time the event occurs. The event filter allows events to be triggered only if certain conditions are met. For example, a standard 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. For example, you can configure a File Uploaded event to only send an email when the file name contains the string `important`, so an email would be sent when the file `Important Tax Forms.pdf` is uploaded but not when other files are uploaded to the server. Additionally, you can 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.

Event filter fields

Each event filter has the following critical values that must be set:

- Name: This is the name of the filter, used to identify the filter for the event.
- Description (Optional): This is the description of the event, which may be included for reference.
- Logic: This determines how the filter interacts with other filters for an event. In most cases, AND 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).
- Filter Comparison: This is the most critical portion of the filter. The Filter Comparison contains the evaluation that must occur for the event to trigger. For example, a filter can be configured so that only the user *admin* triggers the event. In this case, the comparison is `If $Name = (is equal to) admin`, and the data type is `string`. For bandwidth, either an unsigned integer or double precision floating point value is used.

Event filters also support wildcards when evaluating text strings. The supported wildcards include:

- `*` - 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`.

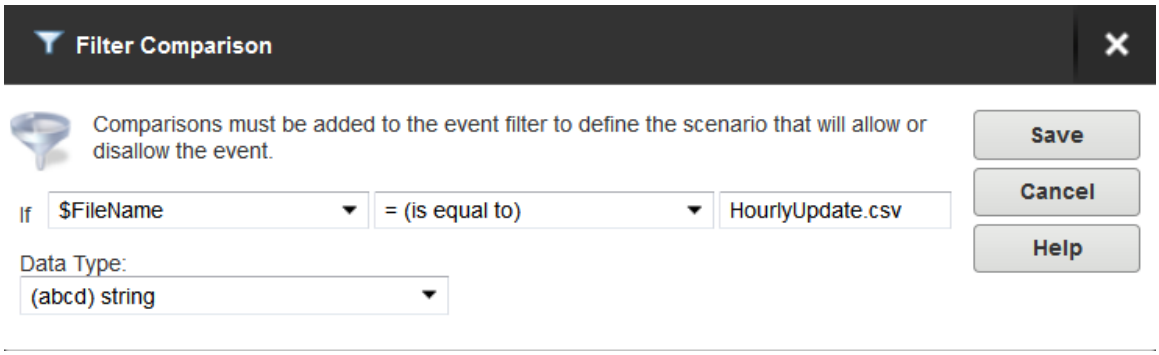
- `?` - The question mark wildcard matches any one character, but only one character. For example:
  - An event filter that compares the `$FileName` variable to the string `data?` matches a file named `data7` but not `data`, `data77`, `data.txt`, `data7.txt`, or `data77.txt`.
  - An event filter that compares the `$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.

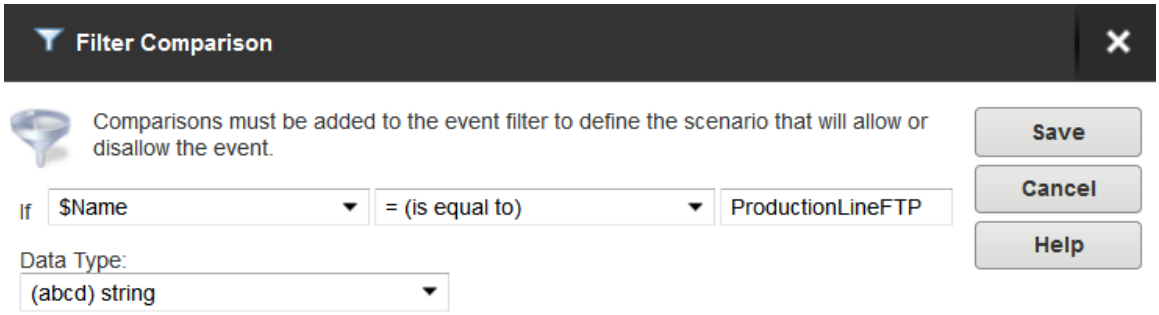
Event filters

Event filters are used by comparing fields to expected values in the Event Filter menu. The best example is raising an event only when a certain user triggers the action, or when a certain file is uploaded. For example, 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:

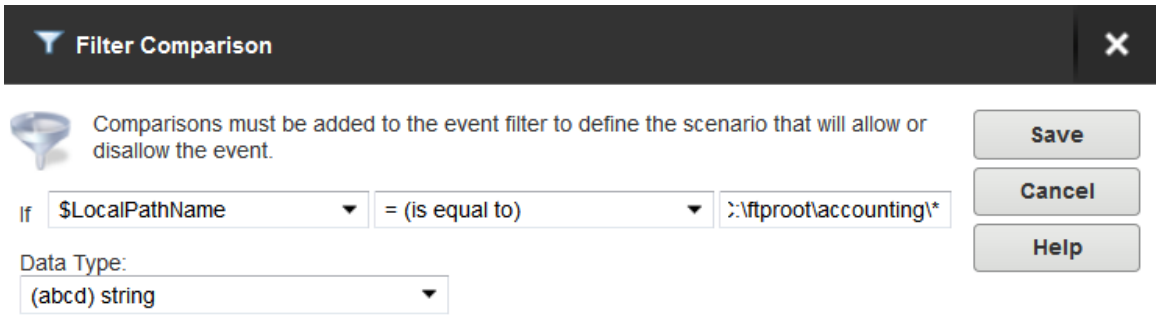


As another example, it may be necessary to know when a file transfer fails for a specific user account. To perform this task, create a new File Upload Failed event, and add a new filter.

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



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\`.



Server details

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

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

Specifying IP access masks

IP access rules use masks to authorize IP addresses and domain names. The masks can contain specific values, ranges, and wildcards made up of the following elements.

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`.

VALUE OR WILDCARD	EXPLANATION
?	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`.

Caveats

Specific IP addresses listed in Allow rules will not be blocked by anti-hammering. These IP addresses are white-listed. However, addresses matched by a wildcard or a range are subject to anti-hammering prevention.

Implicit deny all

Until you add the first IP access rule, connections from any IP address are accepted. After you add the first 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.

Matching all addresses

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.

DNS lookup

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 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.

Rule use during connection

The level at which you specify an IP access rule also defines how far a

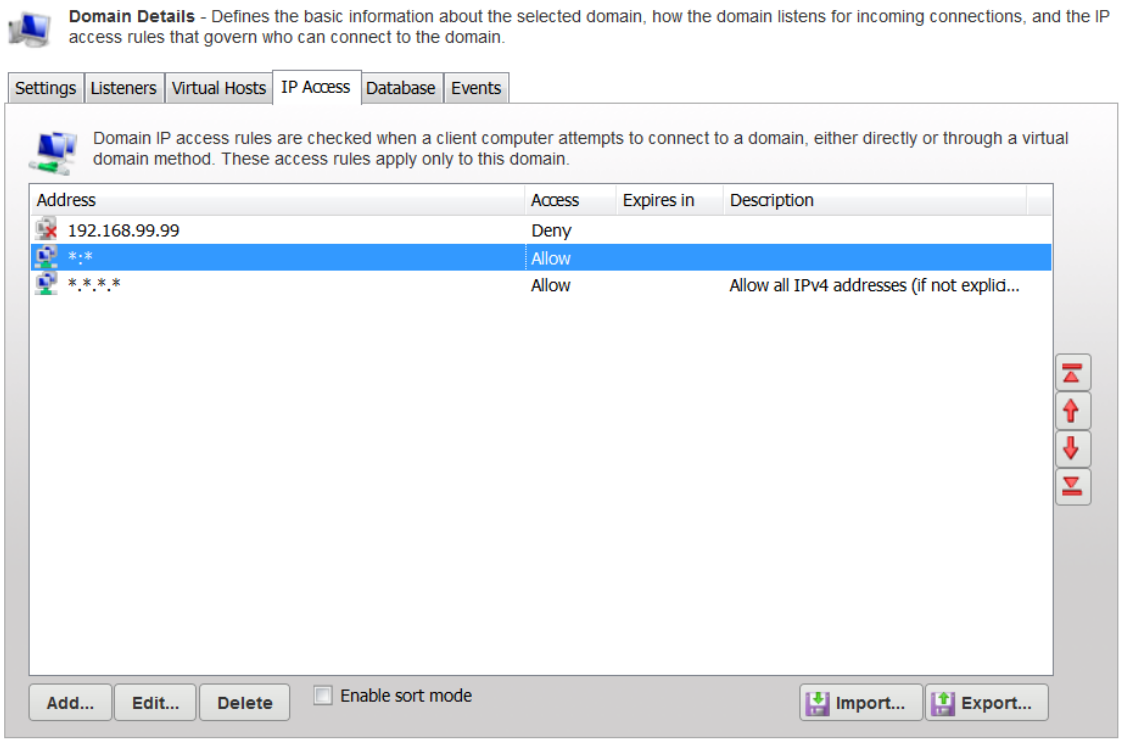
connection is allowed before it is rejected. Server and domain level IP access rules are applied before the welcome message is sent. Domain level IP access rules are also applied when responding to the `HOST` command to connect to a virtual domain. Group and user level IP access rules are applied in response to a `USER` command when the client identifies itself to the server.

Anti-hammering

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. You can configure an anti-hammering policy server-wide in Server Limits and Settings > Settings and domain-wide in Domain Limits and Settings > Settings.

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.

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



IP access list controls

The following options are available on the IP Access page.

Using the sort mode

You can 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.

Importing and exporting IP access rules

You can export and import Serv-U IP access rules from users, groups, domains, and the server by using a text-based `.csv` file. To export IP access rules, view the list of rules to export, click Export, and specify the path and file name you want to save the list to. To import IP access rules, click Import and select the file that contains the rules you want to import. The `.csv` file must contain the

following fields, including the headers:

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

Examples of IP address rules

Office-only access

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 access rule 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 provides an implicit Deny All rule at the end of the list.

Prohibited computers

Users should normally be able to access Serv-U 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 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.

DNS-based access control

The only users allowed to access a Serv-U domain connect from `*.example.com` or `*.example1.com`. The related Serv-U 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 provides an implicit Deny All rule at the end of the list.

Limits and Settings

Serv-U contains options which you can use to customize how Serv-U can be used, and which also provide ways to apply limits and custom settings to users, groups, domains, and the server in its entirety. The limits stack intelligently, with user settings overriding group settings, group settings overriding domain settings, and domain settings overriding server settings. In addition, you can configure limits so that they are only applied during certain days of the week, or certain times of the day. You can also grant exceptions to administrators and restrict specific users more than others, providing total control over the server.

The Limits and Settings in Serv-U are divided into the following categories:

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

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

- Select Domain > Domain Limits & Settings from the Serv-U Management Console.
- Select Directory Listing from the Limit Type list.
- Click Add.
- Select Lock users in home directory from the Limit list.
- Deselect the option.
- Click Save.

The limits list displays the current limits applied to the domain. Limits with a light-blue background are default values. Limits with a white background are values that override the defaults. After you complete the previous steps, a new Lock users in

home directory limit appears in the list that displays "No" as the value. Because of inheritance rules, this option applies to all users in the domain unless it is overridden at the group or user level. For more information about this method of inheritance, see User interface conventions.

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

To create a limit that is restricted to a specific time of day or days of the week, click Advanced in the New Limit or Edit Limit window. Select Apply limit only at this time of day to specify a start and stop time for the new limit. To restrict the limit to certain days of the week, deselect the days for which you do not want to apply the limit. When a limit is restricted in this way, default values (or the value of other limit overrides) are applied when the time of day or day of the week restrictions are not met for this limit.

Ratio free files

Files listed in the ratio free file list are exempt from any imposed transfer ratios. In other words, if a user must upload files in order to earn credits towards downloading a file, a file that matches an entry in this list can always be downloaded by users, even if they have no current credits. This is commonly used to make special files, such as a readme or a directory information file, always accessible to users.

You can use the '*' and '?' wildcard characters when specifying a ratio free file. Using '*' specifies a wildcard of any kind of character and any length. For example, entering `*.txt` makes any file with a .txt extension free for download, regardless of the actual file name. A '?' can be used to represent a single character within the file name or directory. Finally, full paths can be specified by using standard directory paths such as `C:\ftproot\common\` (on Windows) or `/var/ftpfiles/shared/` (on Linux).

In addition, full or relative paths can be used when making an entry. If a full path is used when specifying a file name, only that specific file is exempt from transfer ratios. If a relative path is used, such as entering only `readme.txt`, the provided file is exempt from transfer ratios regardless of the directory it is located in.

SFTP for users and groups

Use an existing public key

1. Obtain a public key file.
2. Place the public key file in a secured directory in the server, and then use Browse in Serv-U to select the file.
3. Click Save.

Create a key pair

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

Create multiple keys per user

For the purposes of public key authentication, you can associate multiple public keys with a user account.

To create multiple keys for an account:

1. Click Manage Keys.
2. Click Add Key, and then specify the key name and the key path.

When authenticating a client, Serv-U 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.

System variables

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 Directory access rules.

> 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).
$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).

VARIABLE	DESCRIPTION
$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

VARIABLE	DESCRIPTION
	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.

VARIABLE	DESCRIPTION
$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.

VARIABLE	DESCRIPTION
$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.
$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.
$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.

VARIABLE	DESCRIPTION
$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.
$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.

VARIABLE	DESCRIPTION
$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.
$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.

VARIABLE	DESCRIPTION
$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.
$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

VARIABLE	DESCRIPTION
	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.

VARIABLE	DESCRIPTION
$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 `C:\Temp\File.fid` instead of `/Temp/file.fid`.
$LocalFileName	Retrieves the name of the file as it is stored on the local computer. See $LocalPathName for details.
$OldLocalPathName	Same as $LocalPathName, but contains the path prior to renaming.
$OldLocalFileName	Same as $LocalFileName, but contains the file name prior to renaming.
$OldPathName	Retrieves the remote path name prior to renaming.
$OldFileName	Retrieves the remote file name prior to renaming.

Current activity

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

VARIABLE	DESCRIPTION
	anonymous user on the Serv-U File Server.
$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.