File Server Serv-U

Total Security

P.O Box 53, Helenville, WI 53137 U.S.A. ● www.RhinoSoft.com ●

RhinoSoft.com

Internet users demand security for both their personal and corporate files, and Serv-U can guarantee the confidentiality and integrity of your files. With support for FTPS and HTTPS employing high-grade 128-bit SSL encryption as well as full SFTP support, Serv-U provides the **best** security available for both personal and corporate information resources.

Security Features

To protect the confidentiality and integrity of vital information, Serv-U utilizes industry standard SSL encryption for both FTPS and HTTPS communications. For a secure file transfer option that eliminates the challenge of configuring complex networks, use the SFTP functionality in Serv-U Corporate Edition. Whether a client is connected to Serv-U via FTPS, SFTP, or HTTPS, the same settings and features are available to the same collection of user accounts. Users connecting to the File Server through their Web browser via secured connections can rest assured that their login information and data are safe. Whether users are transferring important technical documents to clients or pictures to relatives, **the Serv-U File Server will meet your security needs.**

FIPS 140-2 & HIPAA

To meet the rigorous needs of government agencies and health organizations, Serv-U's FTPS and HTTPS services are both fully HIPAA compliant. Additionally, Serv-U Gold supports **FIPS 140-2** compliant services, meeting even higher security standards mandated for use in government deployments and high-security organizations. The **FIPS 140-2** encryption module in Serv-U is tested regularly by independent security organization to ensure that it meets the exceptional standards of the National Institute of Standards and Technologies.

Administrative Control

Server security depends greatly upon the ability of the administrator to control and manage user access. Serv-U empowers administrators to restrict or configure user access to the server during specific times of the day or certain days of the week. Various limits and settings can be used to enforce password requirements, require certain users to make secure connections, limit upload and download speeds at both the Server and Domain level, and more!

P.O Box 53, Helenville, WI 53137 U.S.A. ● www.RhinoSoft.com ●

User Directory Access

Directory Access rules allow administrators to grant and deny access to folders on a per-folder basis to users, groups, or even whole domains and servers. However, Serv-U goes beyond the standard with the use of Virtual Paths, which allow administrator-created virtual "folders" to reduce the navigation time needed to look for a directory. Administrators can also grant users access to a sub-directory within a parent directory they do not have access to. This is an important tool in maintaining the security of sensitive materials because it prevents unauthorized access to files while allowing users access to necessary resources.

Password Limits and Requirements

Serv-U grants both administrators and users a greater degree of control over password security. By using Limits and Settings, an administrator can require complex passwords or passwords of a minimum length. Additionally, once the account is created the user can be granted the ability to change their password to whatever they desire, providing it meets the requirements set by the administrator. This grants the user the power to secure their account, and therefore increase the security of the server.

Public Key Authentication

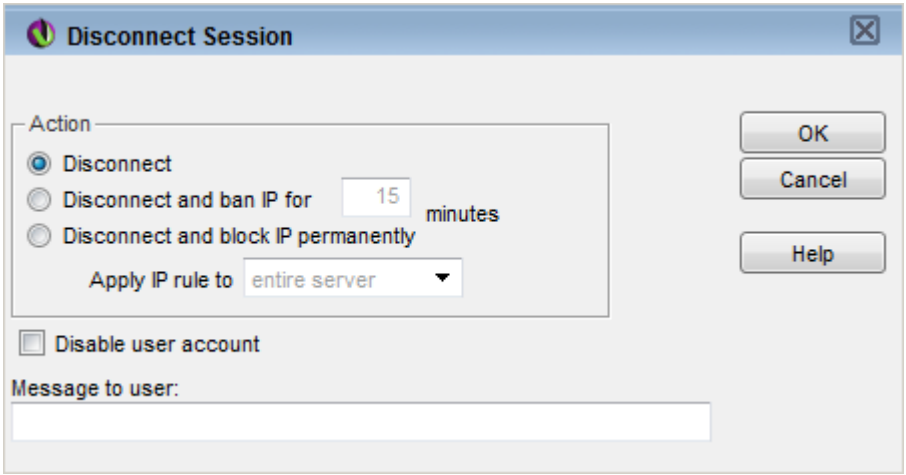
Serv-U features full support for Public Key Authentication, providing password-less authentication to command line clients like those featured on many Linux systems that is just as secure as typical forms of authentication. Providing PKA to clients increases compatibility with scripting engines commonly used by these systems as well as many enterprise backup solutions. It is even possible to require both a password *and* a private key for authentication when extra security is required for user access.

Connection, Directory Listing, and Data Transfer Limits

Administrators can also configure various settings regarding connections, directory listings, and data transfers. Connection limits include how many sessions can run at one time, whether session timeouts should be enforced, and whether to limit idle sessions. Directory Listing limits determine how different objects appear on the server and how a user can interact with them. The Data Transfer limit can restrict the speed of transfers on the server and during what hours the speed is most concentrated, allowing more important transfers to take precedence over less important ones. As with other limits, these limits can be configured to take effect at any time of day, any day of the week.

Session Monitoring

Serv-U also enables administrators to view exactly which users are accessing the server and which resources they are viewing. This security feature allows administrators to manage the server by maintaining a record of all server activity. If a user is unauthorized to access specific files the administrator has the ability to disconnect them for one session, a set amount of time, or block them permanently with a few clicks. The administrator can then edit the user's directory access while their account is disabled and then reinstate the user account with the updated directory access rules in place.



Trusted Certificates

Proving your identity online is an important hurdle in establishing client trust. Serv-U 7 allows administrators to use trusted third party certificates in the industry-standard X509 format to guarantee their identity to clients connecting securely. Using one is simple – simply create an interim self-signed certificate and send the automatically generated Certificate Signing Request to a trusted Certificate Authority for signing. Rest assured that your clients will always know they are connecting to a trusted host.

Dynamic IP Addresses - Reverse DNS

The administrator has the power to specify IP access rules in one of 3 ways: explicit IP addresses, reverse DNS names, or a domain name, giving administrators more ways to grant and deny server access. Giving users these specific means of accessing the server grant them security to utilize a known address without the risk of having their account used without permission.