Pragma SecureShell

Pragma Systems' SecureShell brings the world's first Secure Shell Server with SSH1 and SSH2 capability to Windows XP, Windows 2000 and Windows NT. Secure Shell (SSH) is a de-facto industry standard for remote access of systems over a secure connection using strong cryptography. A serious problem with current popular tools like telnet and FTP is that they transfer password and data in clear text on the net thus compromising security. Use of SecureShell virtually eliminates the risk of remote management as all session data are encrypted using strong ciphers with keys exchanged dynamically using RSA/DSA public key algorithms.

The Pragma SecureShell package contains a full-featured Secure Shell Server (sshd) & Secure File Transfer Server (sftp-server) for Windows XP/2000/NT. Full-featured Secure Shell client, Secure File Transfer Client and SCP (Secure Copy Program) are included, which can run in any 32-bit Windows environment. Pragma's SecureShell server supports both the industry standards ssh1 and ssh2 protocols, so it can be accessed from any vendor's ssh1 or ssh2 level client running in any operating system.

Pragma SecureShell provides:

- Secure Remote Access
- Secure File Transfer
- Software VPN (Port Forwarding/Tunneling)
- Encryption and Compression
- Key Management

Primary Programs Included

Sshd.exe	SecureShell server for XP/2000/NT
Sftp-server.exe	Secure File Transfer protocol server for XP/2000/NT
Ssh.exe	Secure Shell Client supporting VT and WYSE emulations.
Sftp.exe	Secure File Transfer protocol client for XP/2000/NT/95/98/Me
Inetdsrv.exe	The Inetd Service for XP/2000/NT
Sshkeygen.exe	SSH RSA key generator for XP/2000/NT/95/98/Me
scp.exe	Secure copy program to transfer files.
imgr.exe	User Management and server con figuration graphical programs

Why is SecureShell Important?

Remote access of systems is one of the most common tasks performed by most professionals and IT staff. Since the days of the internet, it is very rare for one to work with one local computer alone. Quite frequently, one has to access another machine to transfer data, start some task or monitor the progress of some tasks started earlier.

The Internet and TCP/IP standards for remote access are telnet, rsh, rexec or rlogin. But the flaws in them are that they are not secure as the password is sent in clear text and data is not encrypted. A hacker can simply sniff the data exchanges and pick the password up or look at data that may be sensitive. Secure shell puts an end to all of these security flaws. It introduces a single client (ssh) and a single server (sshd), which can authenticate users based on any of the means used in telnet (password), rsh, rexec (password) and rlogin. It does this securely by establishing a secure channel using public key cryptography and strong encryption. Once a secure channel is established, credentials like password and data can be sent without worry as they are all encrypted.

Further, with the port forwarding feature of Secure Shell, a software VPN tunnel is established between the ssh client and sshd server node over which non-secured TCP/IP applications like SMTP, POP, Telnet, FTP, X-windows, etc. can be run making them run securely without any change. All these capabilities make the users' task easy and secured when SecureShell is introduced in an organization.

Pragma SecureShell

SecureShell Features

- **Multiple Protocol Support**
  Pragma SecureShell supports both SSH1 and SSH2 dynamically. The server will respond to the client requested protocol. Either protocol can be blocked to prevent access by an unwanted client.

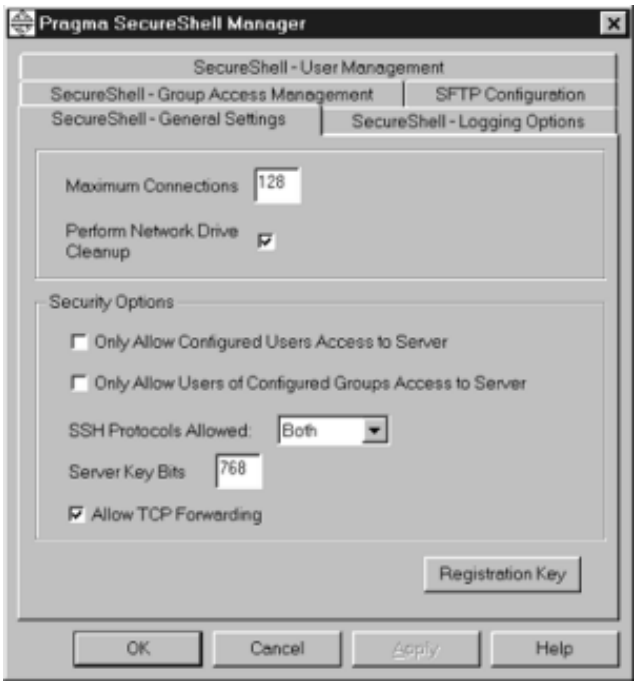
- **Multiple Encryption Ciphers**
  DES, 3DES, Blowfish, CAST-128, Arcfour and new AES (Rijndael) encryption is supported.

- **TCP/IP Port Forwarding**
  Run protocols like SMTP, POP, TELNET, etc. to run over a secure ssh session.

- **RSA/DSA Cryptography**
  Uses proven reliable RSA\DSA cryptography. User can generate keys independent of client/server connection.

- **Data Compression**
  User can choose between nine levels of data compression.

- **RF Device Special Features**
  data packet size option for slow network links and small screen sizes.



- **Interoperates** with any vendor's ssh1/ssh2 clients & servers like OpenSSH and SSH Communications.

- **Color & PC Keyboard Support** supporting full ANSI color and PC keyboard and character sets support.

- **Supports Multiple Terminal Emulation** like ANSI, Digital VT100, VT220, VT320, VT420, and WYSE terminal emulation support .

- **Windows User Authentication** integrates with Windows XP/2000/NT native security to allow user logon authentication via Windows user account database.

- **Any size screen** access of XP/2000/NT console are supported.

- **Customizable login-shell** allowing UNIX-like shell or custom applications to be run when a ssh clients logs on. Initial directory set to the user's home directory (if specified).

- **User Defined Login Script** and/or shell initializing can be run to setup the user's environment.

- **Console Application Support** allows you to run any console mode or text-mode program that can be run on Windows, including 16-bit DOS applications like: EDIT, VI, EMACS, DEBUG, TREE, DIR, NETSTAT, NET, COMPILER, LINKER, FTP, and LYNX.

- **Multiple users** can log in simultaneously.

- **Dynamic Character Mapping** supports user defined character maps. This will improve the look of any session from any terminal, by assigning a new value to a character that is represented undesirably.

- **Session Logging** logs user sessions to a file. A text or HTML format file can be saved, to be viewed at another time. This will track user logon, logoff and all typing done by remote user.

- **Slow Connection Option** for slow clients, like hand held clients, or slow connections will reduce redraw problems due to information being lost by slow clients.

- **NET USE Cleanup** will automatically disconnect any network drives that were connected during the session.

- **Multiple User Configuration:** Most of the session configurations can be specified on a per-user basis.

- **Group Access Management** specifies that only users of specific Windows groups be allowed access.

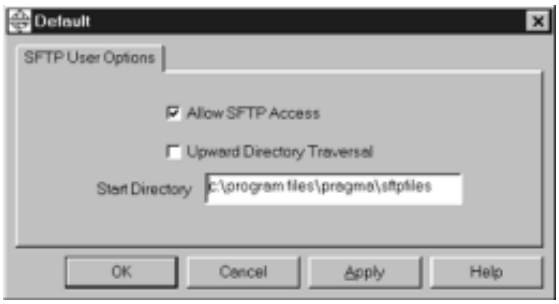
- **IP Address Filtering** will deny or grant access to any configured InetD service by the client IP Address.

- **Graceful Termination of Applications** specifies how open processes started by the session should be handled when the session is dropped.
- **Pragma Manager** is a fully graphical management program to configure and manage.

Software VPN (port forwarding)

Port forwarding feature of ssh and sshd allows any TCP or UDP application be made secure by passing their data over the secure ssh-sshd session without any changes to the application. This creates a software VPN (Virtual Private Network) environment just by using ssh technology. Users can now redirect their email, FTP, telnet, etc. through SecureShell and all of their data and passwords will be encrypted with tight cryptography and security.

Pragma SFTP & SCP



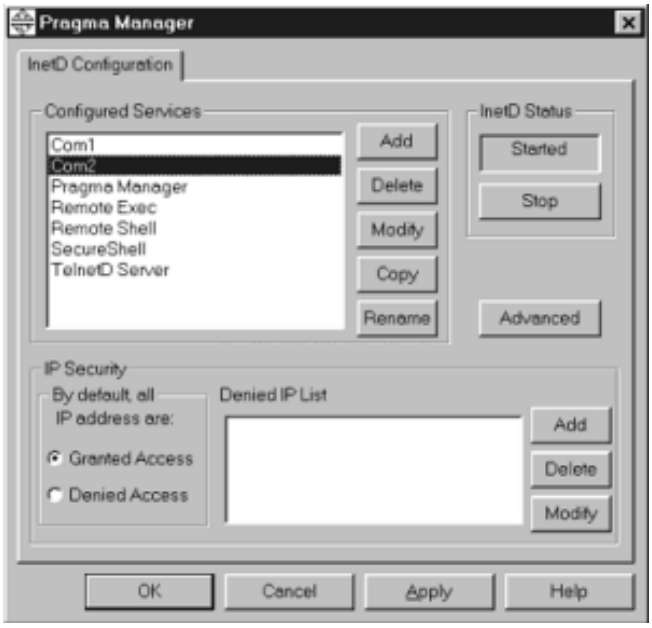
SecureShell environment includes secure file transfer capabilities. In SSH2, a new subsystem sftp-server and a new protocol **SFTP** (like the internet FTP, but not compatible) have been defined and integrated with SSH2 server to make file copying and management easier. An sftp client program works similar to ftp client user interface and uploads or downloads files and directories from an sftp-server. SFTP also uses under the hood ssh client on the client side and sshd server on the server side to create the secure tunnel over which all data transfers and commands travel. Standard FTP can be piped through a SSH tunnel using the port forwarding feature.

SCP is a secure copy of files using the ssh server as a tunnel to encrypt the files. The files are copied through a SecureShell session launched by the scp client. The scp client launches a ssh session to the server, which launches the scp server. A machine must have the scp client, plus the ssh client to initiate a secure copy. The remote machine must have a scp client, plus a ssh daemon to respond to a scp request. The destination file will retain the file attributes of the source file. The copy can be configured to retain the source file date or use the copy timestamp.

InetD Features

InetD server is the communication hub of Pragma's servers. InetD works like the InetD in UNIX.

- Listens on TCP/IP ports and starts any Windows program when a client connects to a given TCP or UDP socket.
- Reduces system load by only starting programs when they are needed.
- Inetd runs as a background process requiring no user to be logged on.
- Inetd is used to start Pragma's secure shell, telnetd, rshd, rexecd and management services. It can be easily extended to start other user programs.
- IP filtering allows for limiting connections by IP address for added security.



pragmasys.com
PRAGMA SYSTEMS

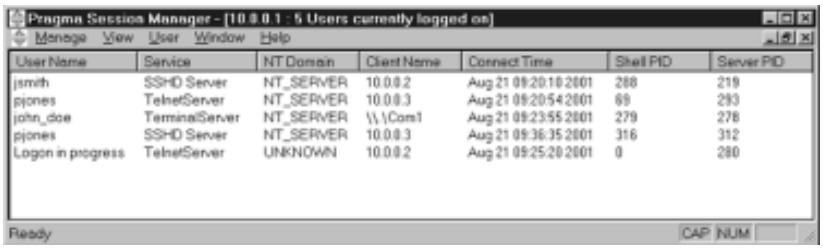
Pragma SecureShell

Key Management

Every Secure Shell node, client or server, needs to have a RSA or DSA key. This key, which is actually a pair of keys: one public and one private, is generated by the sshkeygen.exe program, which is included in our install package. The public part of the key can be distributed widely so that other machines can talk to this machine. The private part of the key must be stored in a secured way. Our ssh key implementation is file based. Public part of the key is one file and private part of the key is another file. Typically these files are named in pairs.

Pragma Manager

Use Pragma Session Manager to monitor ssh, telnet, and terminal connections to a server, local or remote. The manager displays current users and provides a method to remove a single user or all current users. Most Pragma Server settings can be configured with the Pragma Manager executable, using a command line switch. Pragma Manager uses the InetD service to communicate user information between the telmsrvc (or tmsrvc95) and imgr executables. All information communicated between the Pragma Manager and the server is encrypted.



Supported Encryption

ssh1	ssh2
DES	AES128
3DES	AES192
Blowfish	AES256
CAST128	Blowfish
Arcfour	3DES
	Arcfour
	CAST128

Specifications

- SecureShell server (sshd) runs in Windows NT 4.0 Server or Workstation, Windows 2000 Professional, Windows 2000 Server, Windows XP, Windows 2000 Advanced Server, Windows 2000 Data Center Server, Windows Embedded.
- SecureShell client (ssh) runs in Windows 95, Windows 98, Windows ME, Windows NT 4.0 Server or Workstation, Windows 2000 Professional, Windows 2000 Server, Windows XP, Windows 2000 Advanced Server, Windows 2000 Data Center Server, Windows Embedded.
- Intel x86, Pentium and AMD processors are supported
- 10 MB of available hard disk space.
- 2MB of memory is recommended per remote session.
- SecureShell level 1 (ssh1) and level 2 (ssh2) protocol standards are supported.
- SecureShell interoperates with all vendors ssh clients.

About Pragma

Pragma Systems, Inc. was founded March 1990 in Austin, Texas. Pragma is a leading provider of Windows servers for Microsoft Windows NT/2000/XP operating systems. We focus on bringing high-performance, reliable and enterprise class servers for Windows similar to what one would find in UNIX environments. Our software is deployed in the majority of Fortune 500 companies and over 1500 companies worldwide in 60 countries with about one half million nodes deployed.

pragmasys.com
PRAGMA SYSTEMS

Pragma Systems, Inc.
13706 Research Blvd., Suite 301
Austin, TX 78750
USA

Tel: 1-512-219-7270 Fax: 1-512-219-7110

Email: pragma@pragmasys.com
Web Page: http://www.pragmasys.com

Designed for Microsoft® Windows® XP Windows® 2000 Windows NT®

Microsoft CERTIFIED Partner