Table of Contents

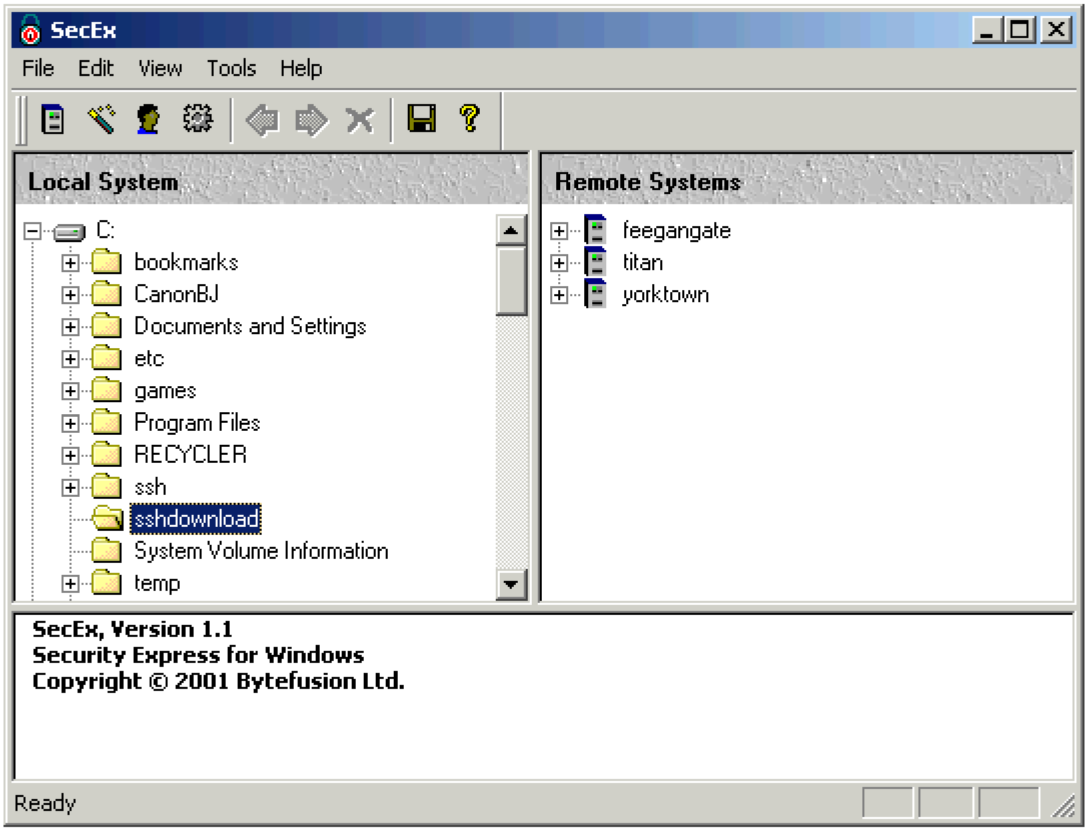
1 SecEx Overview

1.1 What is SecEx ?

SecEx is a network file manager and secure terminal emulator that allows encrypted file transfer between your PC and network servers running Secure Shell. SecEx seamlessly interoperates with either SSH1 or SSH2 servers on both Unix and Windows operating systems. You can transfer files to and from remote servers, view remote files, and execute remote files on your local PC - using strong, industry standard encryption. If you are a travelling executive who wants to access files on a corporate server or a system administrator maintaining a remote site, SecEx is your complete remote file management solution.

SecEx automatically detects available carrier protocols available on server systems. Newer SSH servers tend to make SFTP (Secure FTP) available while older secure shell implementations feature SCP (Secure Copy Program).

SecEx also shields against IP and DNS spoofing by recording a server's public host key. During subsequent connection attempts, the known host key is compared to the host key offered by the server. See IP/DNS spoofing for details. See Quick Start if you just want to get "on the road".



SecEx, Version 1.1
Security Express for Windows
Copyright © 2001 Bytefusion Ltd.

Ready

Secure Terminal Emulator :

SecEx supports a "Secure Command Prompt" facility for remote systems which is equivalent to a Windows (TM) command prompt. "Secure Command Prompt" supports fully interactive programs or facilities normally offered by a VT100+ terminal emulators.

Secure Shell Introduction :

SSH Secure Shell is a replacement for the telnet command and supports encrypted client / server connections. Secure file transfer is achieved via two secure shell supplements : SCP and SFTP. SCP (secure copy program) accompanies most SSH version 1 servers. SFTP (Secure FTP) accompanies most SSH version 2 servers. Secure Shell was conceived as an academic project at the University of Finland in 1995. Open Source initiatives have since emerged from the publicly available source code as well as commercial versions of Secure Shell. The lettering "ssh" in its lowercase rendition is a trademark owned by SSH Communications Security.

Session Profiles :

A session profile holds all information necessary to connect to a Secure Shell server.

Server Login :

To log into a remote server, simply double-click the associated session profile.

File Transfer :

After successfully logging into a SSH server, you may browse the remote file system and copy files to and from the server. Simply, select the files you wish to copy and drag them to a directory on your local system.

Quick View :

To view the contents of a file on the remote server, right-click the file with your mouse and select "Quick View" from the pop-up menu.

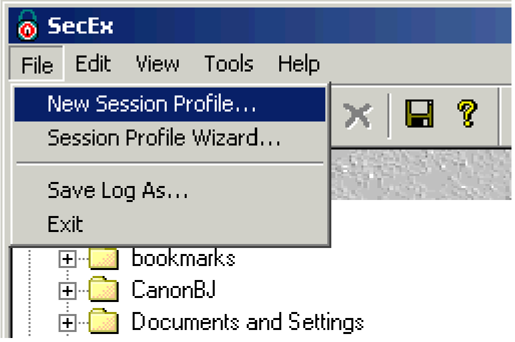
Technical Data :

SecEx is compatible with Secure SSH servers. The default mode of communication is SSH protocol version 2 with automatic fall-back to SSH protocol version 1. Secure file transfer to and from SSH servers is achieved via SFTP (Secure FTP) where available, with automatic fall-back to SCP (Secure Copy Program). Host authentication is via 1024 bit DSS / RSA keys. Supported encryption modes are 3DES, Blowfish and AES. 3DES is the default mode of encryption depending on server-side availability.

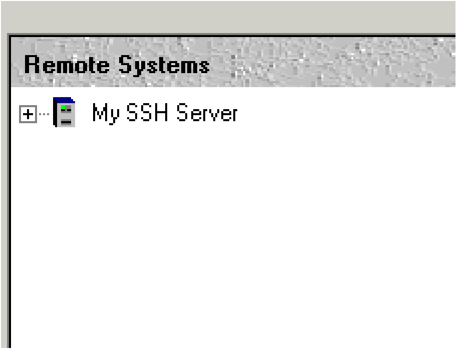
1.2 Quick start

You just want to connect to Secure Shell server and start transferring files ?

To connect to a Secure Shell server you will need to tell SecEx about the server's IP address or DNS name and provide your login information. This information is called a session profile. You can add a session profile via the wizard or the New Session Profile Dialog from the "File" menu as shown below.



Once you have entered your session profile, SecEx will make a corresponding entry for your SSH server in the remote systems pane. Simply click this entry to connect to the server.



2 Configuring SecEx

2.1 Session Profiles

A session profile holds all information necessary to connect to a Secure Shell server. To create a new session profile, select "New Session Profile" from the "File" menu. The following items are required:

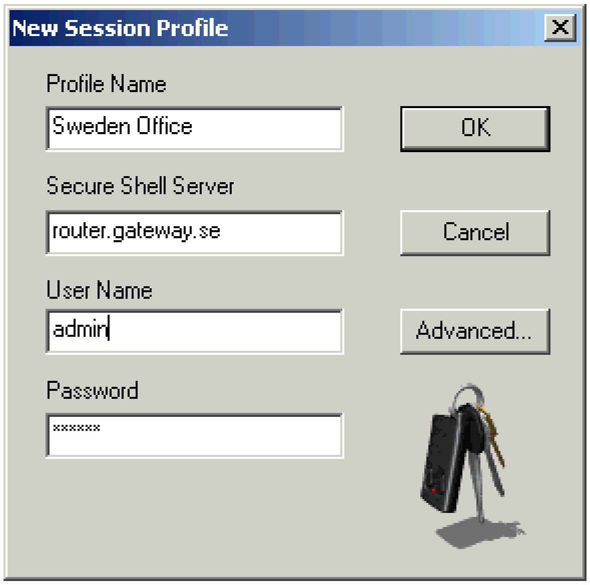
- **Session Profile Name**
A descriptive name. This name will appear in the remote systems pane on the right.

- **Secure Shell Server**
IP address or DNS name of the remote system

- **User Name**
Your login name on the remote system

- **Password**
Your password on the remote system

Click the Advanced... button to access the Advanced Session Properties dialog.



New Session Profile

Profile Name: Sweden Office

Secure Shell Server: router.gateway.se

User Name: admin

Password: ******

2.2 Advanced Session Properties

Advanced Session Properties lets you fine tune a session profile. To access the Advanced Session Properties dialog, click the ***Advanced...*** button in Session Profiles. The following items can be configured:

- **Initial Remote Directory**

On UNIX systems this will be your home directory, usually "/home/<your name>".
For UNIX root users this will typically be "/root". Please note that the file system root "/" is made available by default in addition to your home directory.
On Windows systems the initial directory is auto detected and this parameter is ignored.

- **Preferred Cipher**

The preferred cipher parameter determines the encryption algorithm SecEx attempts to negotiate with the server for data transfer. What algorithm is selected also depends on what ciphers are made available by the server. Possible values are :

1. auto-detect	->	Let SecEx chose
2. 3des	->	Use Triple DES encryption
3. blowfish	->	Use Blowfish encryption
4. aes	->	Use Advanced Encryption Standard (SSH2 servers only)

- **Server Port**

The port number of the Secure Shell server on the remote system. It is safe to leave this value unchanged.

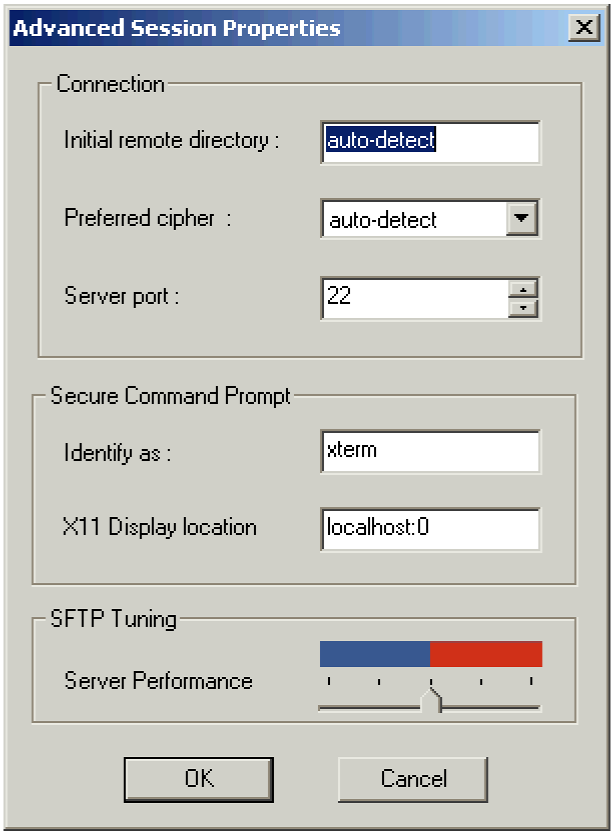
- **Identify As**

This parameter determines the terminal type of the Secure Command Prompt. Common values for this parameter are "xterm" and "linux". If you are unsure what terminal type your server requires, please consult your system administrator.

- **Display Location**

Were your X11 server is located. It is safe to leave this parameter unchanged if are unsure or you do not have an X11 server installed on your system.

- **Server Performance**
This parameter regulates the transfer speed for SFTP data transfer. Some servers may not handle speeds in the area marked red. Speeds marked a blue should be safe with all server implementations.



Initial remote directory : auto-detect

Preferred cipher : auto-detect

Server port : 22

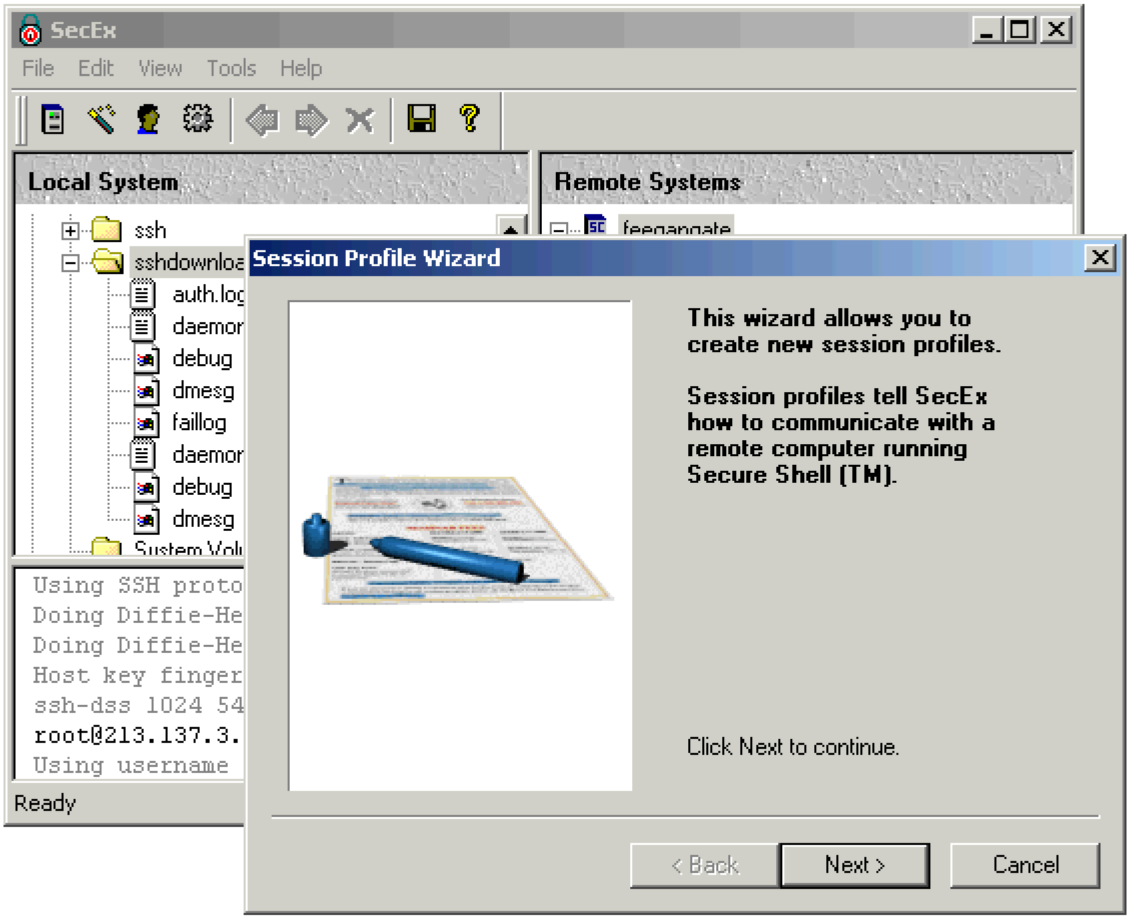
Identify as : xterm

X11 Display location localhost:0

Server Performance

2.3 Session profile wizard

The session profile wizard guides you through the process of entering a new session profile. See New Session Profile for a description of the items contained in a session profile.



```
Using SSH proto
Doing Diffie-He
Doing Diffie-He
Host key finger
ssh-dss 1024 54
root@213.137.3.
Using username
```

This wizard allows you to create new session profiles.

Session profiles tell SecEx how to communicate with a remote computer running Secure Shell (TM).

Click Next to continue.

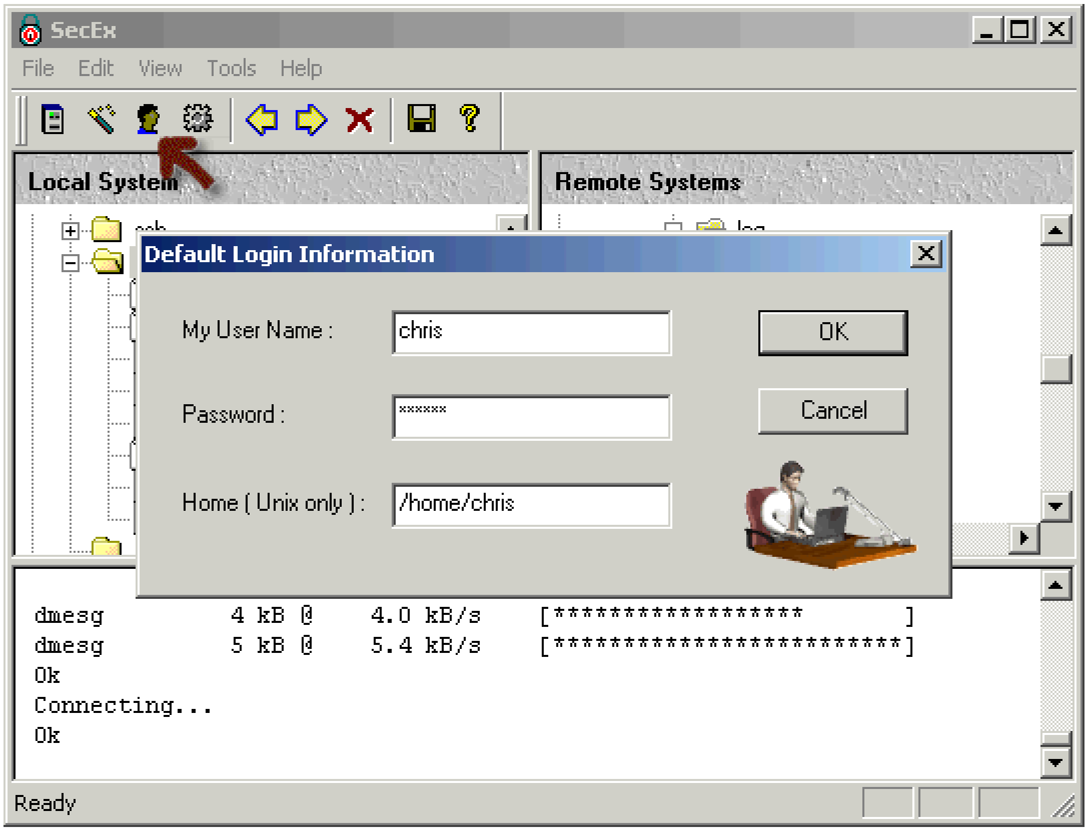
2.4 User settings

You can define user settings to be used as default login information on all new session profiles. The values you provide here will not alter user information in existing session profiles.

- **My User Name**
Your login name on the remote system

- **Password**
Your password on the remote system

- **Home (Unix only)**
On UNIX systems this will be your home directory, usually "/home/<your name>".
On Windows systems the initial directory is auto detected.



My User Name : chris

Password : ******

Home (Unix only) : /home/chris

```
dmesg           4 kB @    4.0 kB/s    [********************       ]
dmesg           5 kB @    5.4 kB/s    [***************************]
Ok
Connecting...
Ok
```

Ready

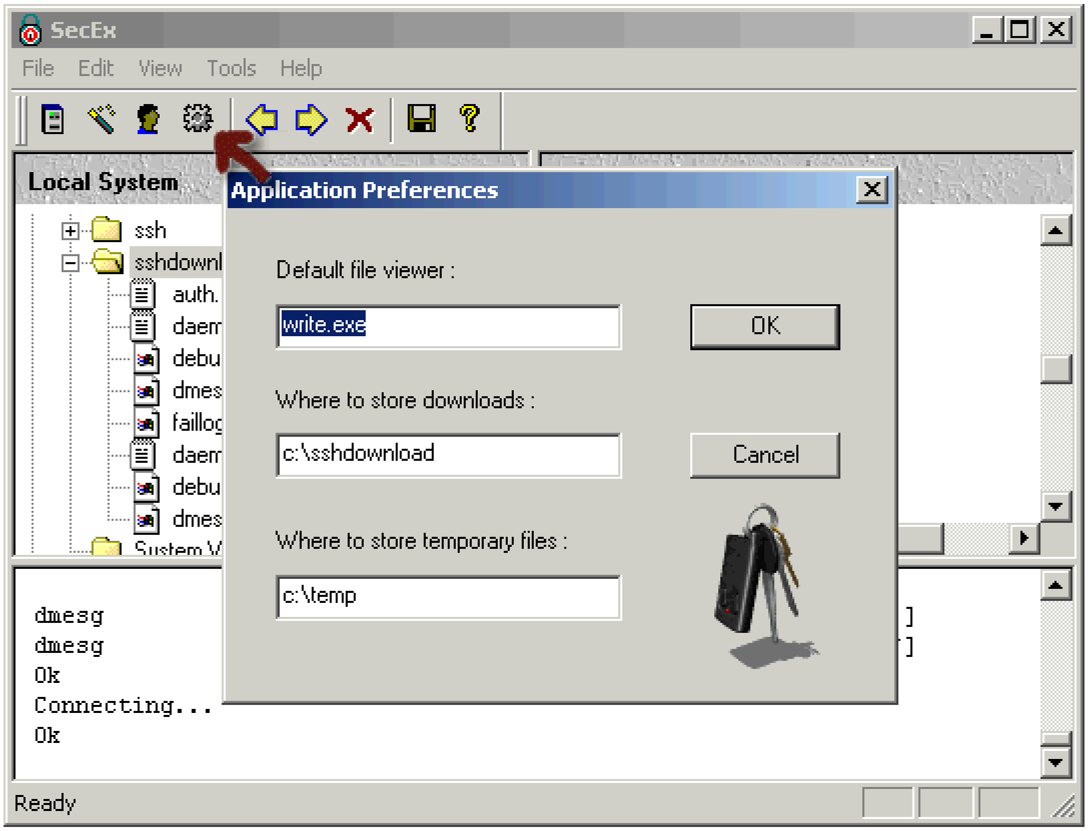
2.5 Application preferences

Use the application preferences dialog to customize the behavior of SecEx.

- **Default file viewer**
  Application to use for "quick view".

- **Where to store downloads**
  Default download directory for data transferred from remote systems. Other download directories may be selected at runtime.

- **Where to store temporary files**
  Remote files downloaded for "quick view" or execution on the local system are stored in the }temporary working folder specified here.



Default file viewer : write.exe

Where to store downloads : c:\sshdownload

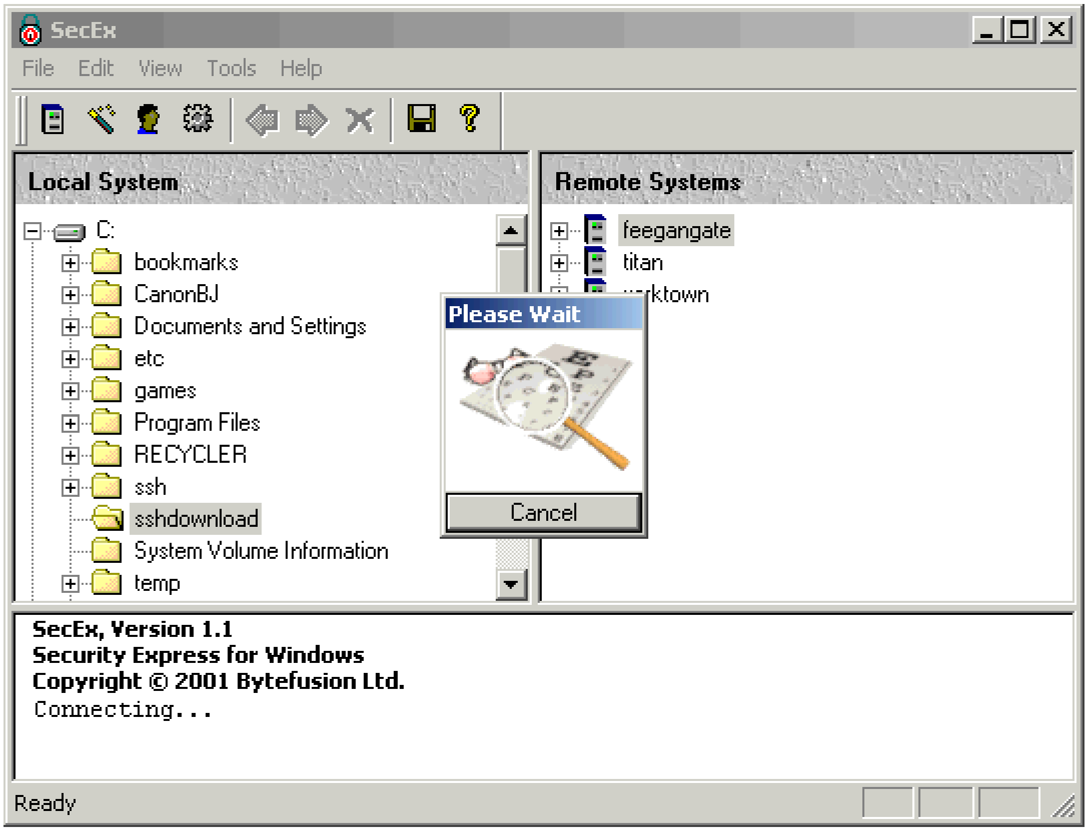
Where to store temporary files : c:\temp

```
dmesg
dmesg
Ok
Connecting...
Ok
```

3 Working with SecEx

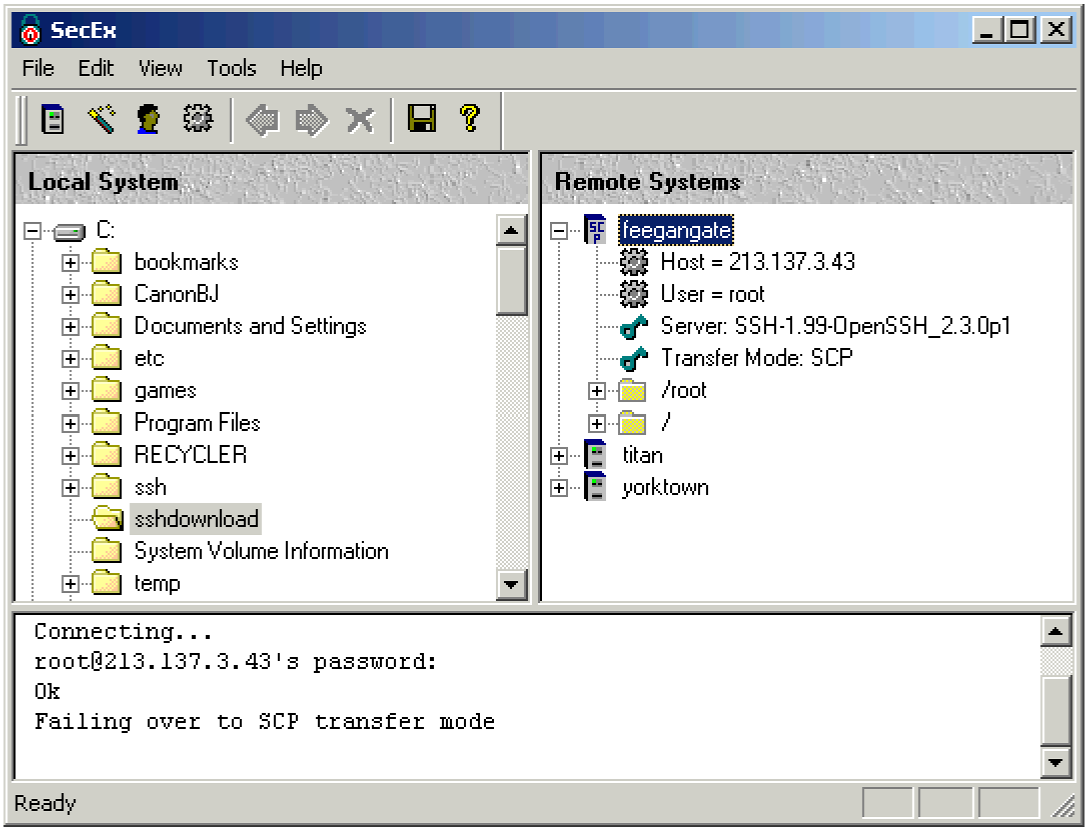
3.1 Server Login

To log into a remote server, simply double-click the associated session profile icon in the "Remote Systems" pane on the right. Secex will contact the server and submit your user name and password for authentication.



```
SecEx, Version 1.1
Security Express for Windows
Copyright © 2001 Bytefusion Ltd.
Connecting...
```

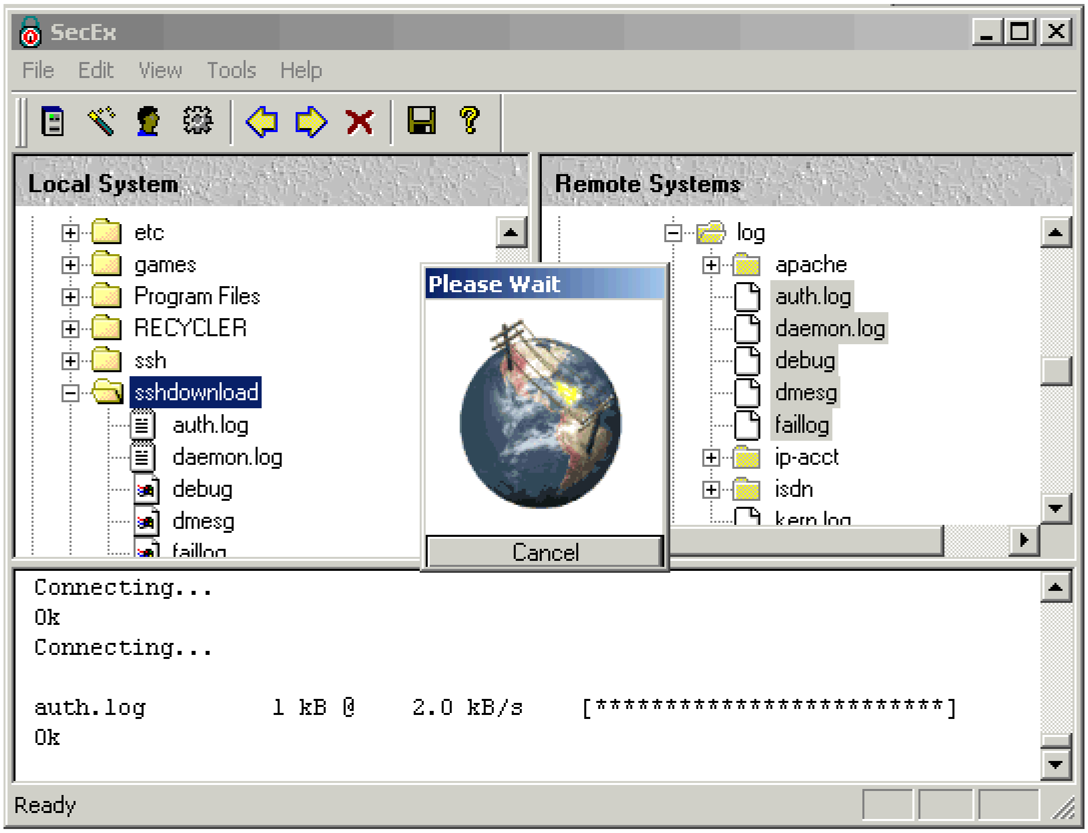
Upon successful login, SecEx will display your home directory, the system root directory, and any relevant server information such as SSH version number and file transfer mode.



```
Connecting...
root@213.137.3.43's password:
Ok
Failing over to SCP transfer mode
```

3.2 File transfer

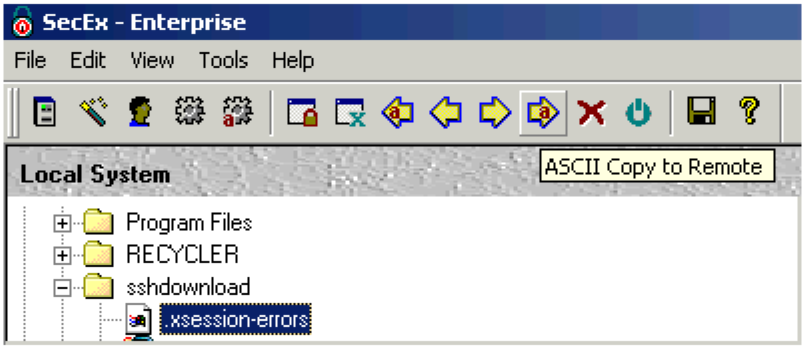
After successfully logging into a SSH server, you may browse the remote file system and copy files to and from the server. Simply, select the files you wish to copy and drag them to a directory on your local system. The session log window at the bottom will indicate the progress. Clicking "Cancel" will terminate the file transfer and log you out of the server.



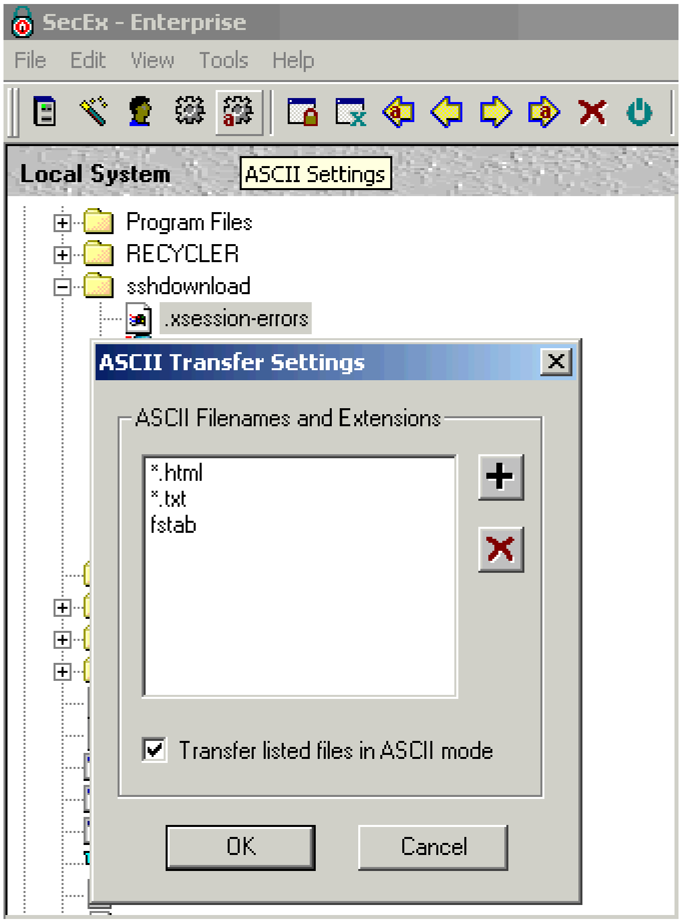
```
Connecting...
Ok
Connecting...

auth.log         1 kB @    2.0 kB/s    [**************************]
Ok
```

3.3 ASCII / Binary Transfer

The default mode of file transfer is binary. Unless otherwise directed, SecEx will transfer all files in binary mode. You can force ASCII transfer of files via the copy buttons on the toolbar marked with an "a" as shown below.



Alternatively, SecEx can automatically transfer files with specific extensions or certain names in ASCII mode. Simply click the "ASCII Settings" button on the toolbar and define extensions and files you wish to transfer in ASCII mode. Extensions are prefixed with "*.". Be sure to enable this feature by selecting "Transfer listed files in ASCII mode".

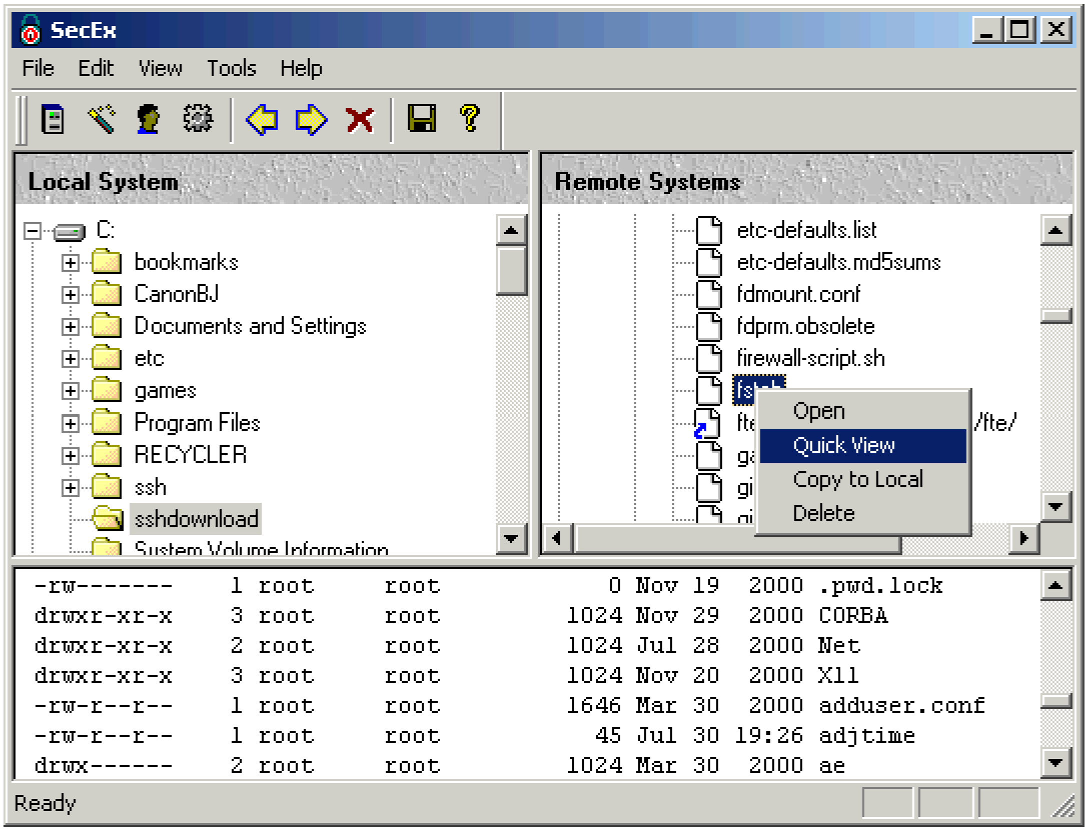


*.html
*.txt
fstab

☑ Transfer listed files in ASCII mode

3.4 Quick view

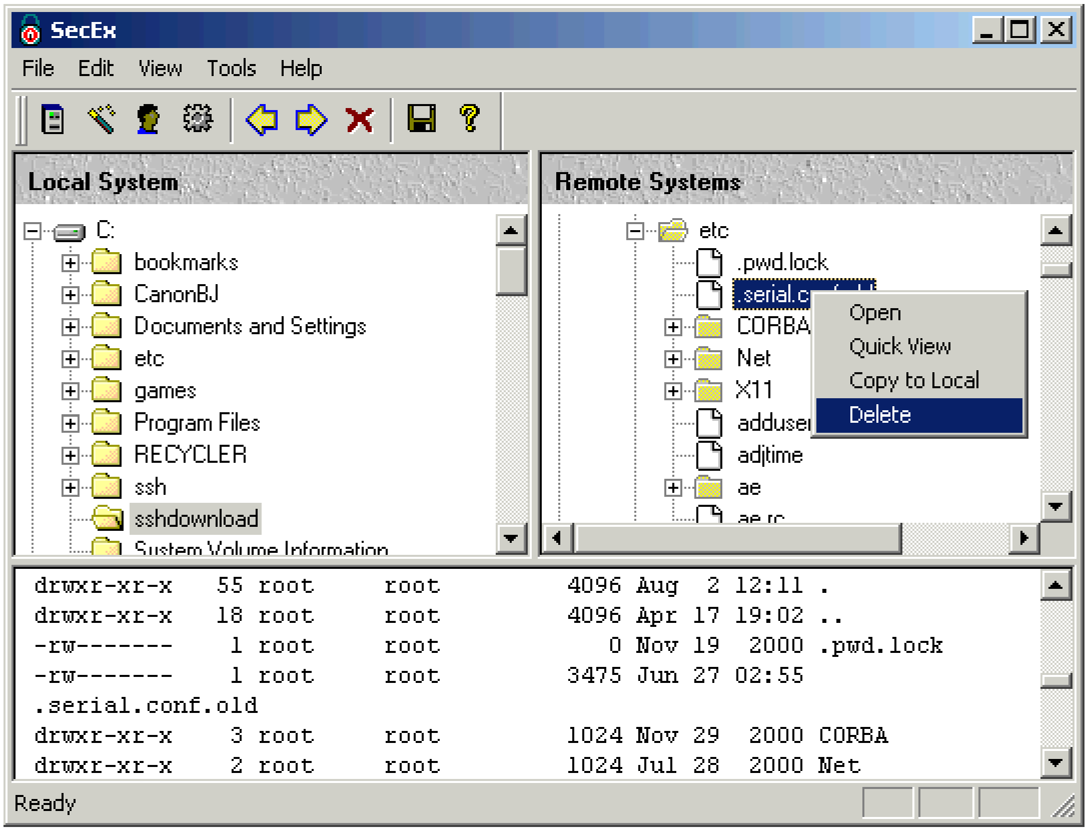
To view the contents of a file on the remote server, right-click the file with your mouse and select "Quick View" from the pop-up menu. The file with be downloaded to the temporary working folder and opened in the default viewer. Both, temporary working folder and default viewer are configured under "Application Preferences".



```
-rw-------    1 root     root          0 Nov 19  2000 .pwd.lock
drwxr-xr-x    3 root     root       1024 Nov 29  2000 CORBA
drwxr-xr-x    2 root     root       1024 Jul 28  2000 Net
drwxr-xr-x    3 root     root       1024 Nov 20  2000 X11
-rw-r--r--    1 root     root       1646 Mar 30  2000 adduser.conf
-rw-r--r--    1 root     root         45 Jul 30 19:26 adjtime
drwx------    2 root     root       1024 Mar 30  2000 ae
```

3.5 Deleting remote files

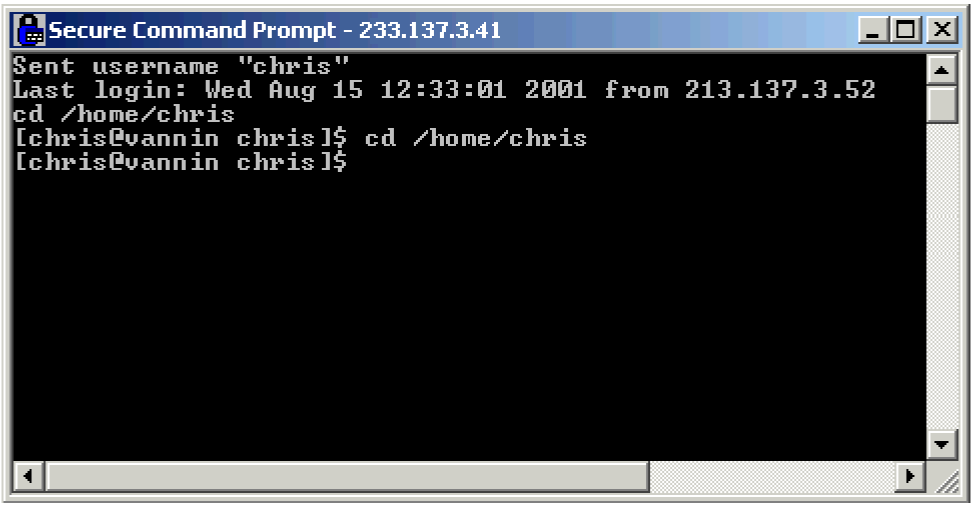
To delete a file on the remote server, right-click the file with your mouse and select "Delete" from the pop-up menu. Note that depending on your access privileges on the remote system, you may not be allowed to delete some files.



```
drwxr-xr-x   55 root     root         4096 Aug  2 12:11 .
drwxr-xr-x   18 root     root         4096 Apr 17 19:02 ..
-rw-------    1 root     root            0 Nov 19  2000 .pwd.lock
-rw-------    1 root     root         3475 Jun 27 02:55
.serial.conf.old
drwxr-xr-x    3 root     root         1024 Nov 29  2000 CORBA
drwxr-xr-x    2 root     root         1024 Jul 28  2000 Net
```

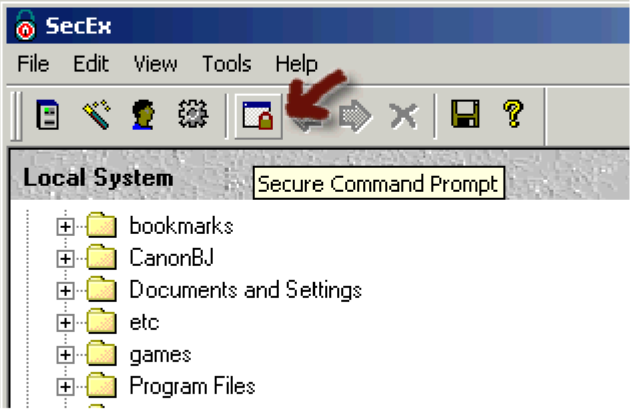
3.6 Secure Command Prompt

How do I get a secure terminal on a Secure Shell Server ?



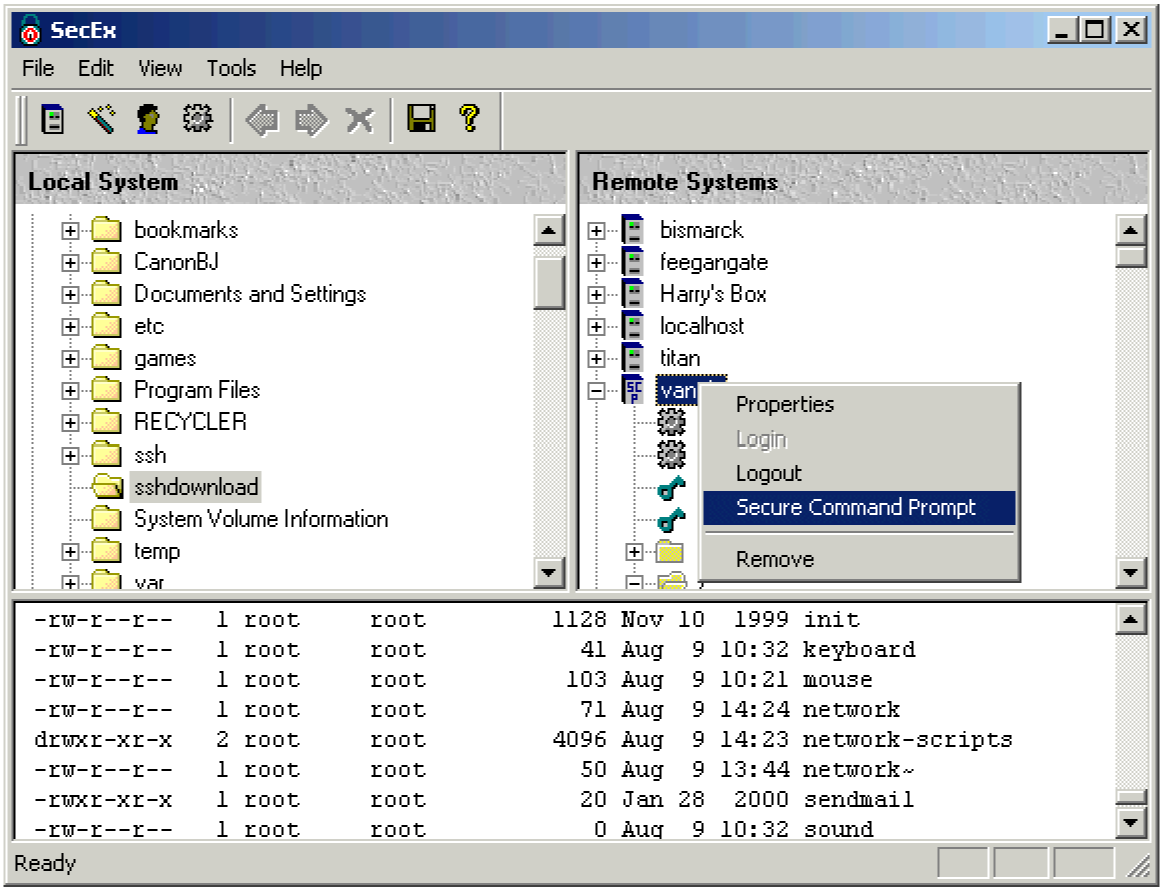
```
Sent username "chris"
Last login: Wed Aug 15 12:33:01 2001 from 213.137.3.52
cd /home/chris
[chris@vannin chris]$ cd /home/chris
[chris@vannin chris]$
```

SecEx supports a "Secure Command Prompt" facility for remote systems which is equivalent to a Windows (TM) command prompt. "Secure Command Prompt" supports fully interactive programs or facilities normally offered by a VT100+ terminal emulators.



When you are logged into a Secure Shell Server, you can click on the toolbar button shown above to activate a Secure Command Prompt on the remote system. Secure Command Prompt will automatically log you into your default shell on the remote SSH server. When logging into a Windows SSH Server you will see the familiar "cmd.exe" on Windows NT/2000 or "command.com" on 95/98 systems. When logging into a SSH server running a UNIX style operating system, you will be presented with the same shell you normally use, Bourne Shell, Z-Shell, etc.

When navigating the remote files system of a SSH Server, you may right-click on any folder and select "Secure Command Prompt Here" to obtain a secure shell prompt in that specific folder.



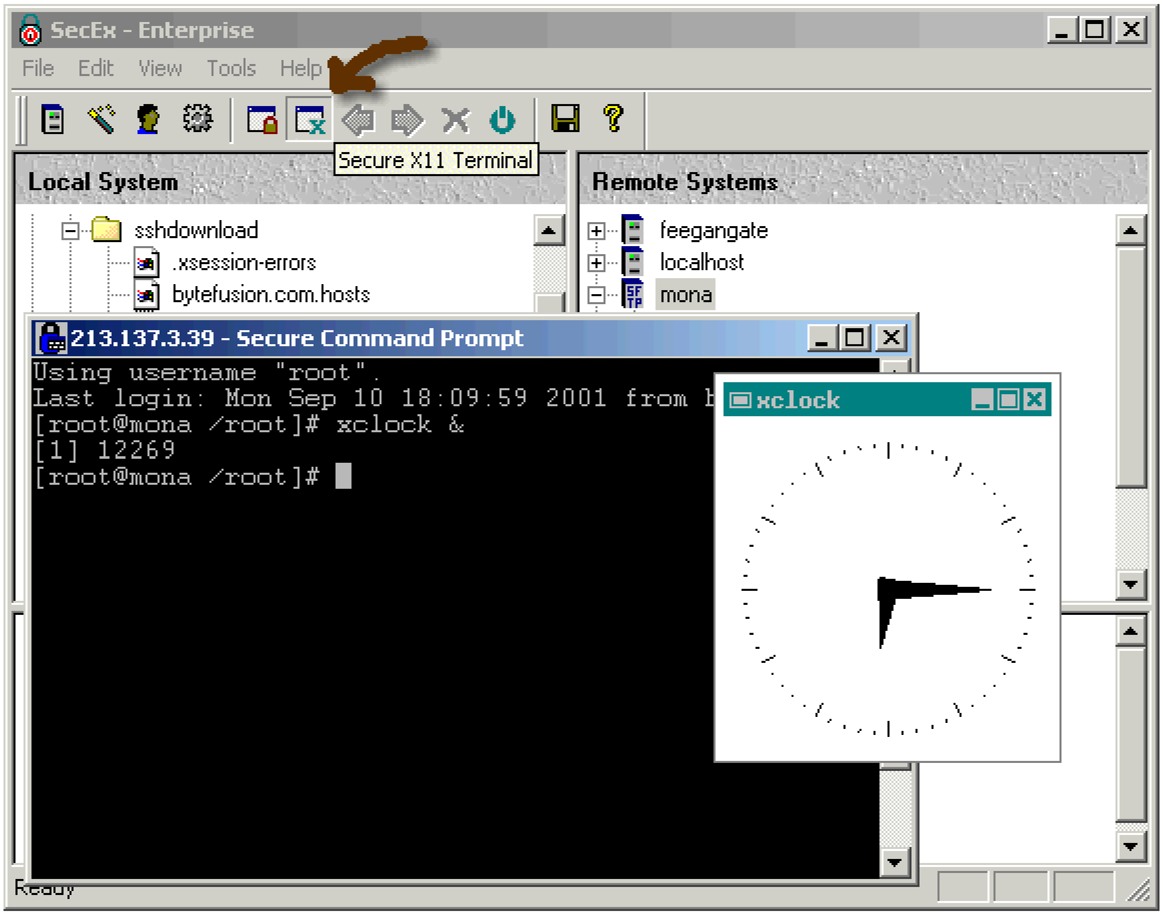
```
-rw-r--r--    1 root     root         1128 Nov 10  1999 init
-rw-r--r--    1 root     root           41 Aug  9 10:32 keyboard
-rw-r--r--    1 root     root          103 Aug  9 10:21 mouse
-rw-r--r--    1 root     root           71 Aug  9 14:24 network
drwxr-xr-x    2 root     root         4096 Aug  9 14:23 network-scripts
-rw-r--r--    1 root     root           50 Aug  9 13:44 network~
-rwxr-xr-x    1 root     root           20 Jan 28  2000 sendmail
-rw-r--r--    1 root     root            0 Aug  9 10:32 sound
```

Windows, Windows NT, and Windows 2000 are trademarks of Microsoft Corporation.

3.7 X11 Forwarding

To securely forward X11 sessions from a SSH server to your PC, simply click the "Secure X11 Terminal" button after logging in to the server. This will create a Secure Command Prompt session which is X11 enabled. All X11 traffic for X based applications launched from this session will be encrypted. Please note that availability of this feature depends both on X11 forwarding support on the Secure Shell server as well as the presence of an X11 display server on your PC.

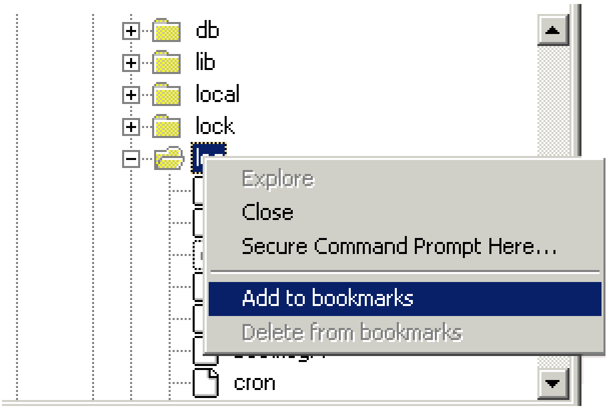
You might also have to adjust the X11 display location parameter under Advanced Session Properties to reflect the settings of your X11 display server.



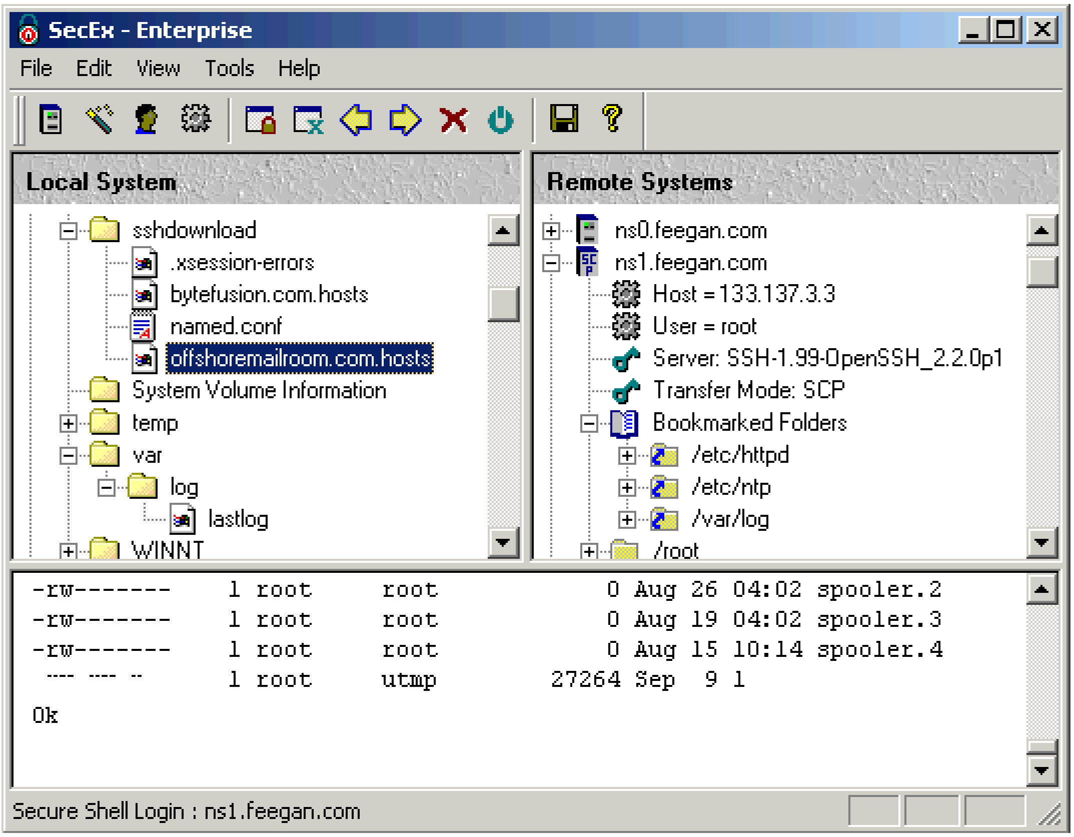
```
Using username "root".
Last login: Mon Sep 10 18:09:59 2001 from l
[root@mona /root]# xclock &
[1] 12269
[root@mona /root]#
```

3.8 Folder Bookmarks

Folder bookmarks are similar to shortcuts on your desktop or bookmarks in your favorite web browser. If you frequently access files in a particular folder on a Secure Shell server, you might wish to bookmark that folder for easy access. To bookmark a folder, simply right-click on the folder with your mouse and select "Add to bookmarks" as shown below.



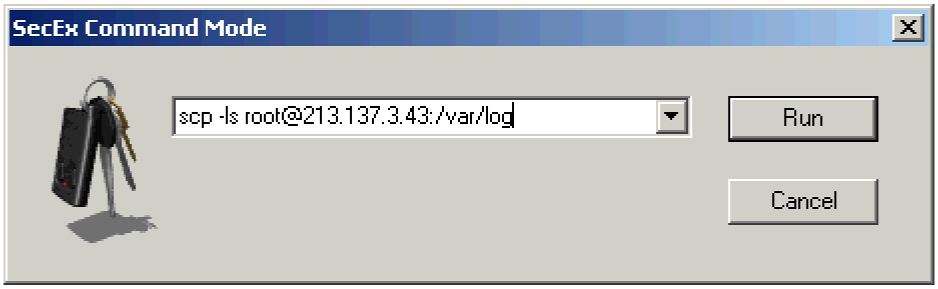
This will add the folder to the bookmarks node for the SSH server you are logged into. You can navigate, copy to, and copy from bookmarked folders in the same manner as when working with ordinary folders.



```
-rw-------     1 root     root          0 Aug 26 04:02 spooler.2
-rw-------     1 root     root          0 Aug 19 04:02 spooler.3
-rw-------     1 root     root          0 Aug 15 10:14 spooler.4
 ---- ---- --  1 root     utmp      27264 Sep  9 1

Ok
```

3.9 Command mode

To enter command mode, select "Command Mode" from the "Tools" menu. This will enable you to execute SCP (Secure Copy Program) and SFTP (Secure FTP) commands directly. Output will be displayed in the session log window at the bottom. You will also be able to interact with the process by typing directly in the session log window, for example if asked to enter your password for the remote system.



```
scp -ls root@213.137.3.43:/var/log
```

The syntax for SecEx SCP client is reproduced below. Please note that SCP is stateless and does not maintain a session on the remote server. Thus one SCP command with server and logon information is required for every SCP operation performed.

```
SecEx SCP Client
Version 1.1
Usage: scp [switches] [user@]host:source target
       scp [switches] source [source...] [user@]host:target
       scp [switches] -ls user@host:directory
       scp [switches] -del user@host:file_to_delete
       scp [switches] -mkdir user@host:new_directory
       scp [switches] -rmdir user@host:directory_to_delete
Switches:
        -r        copy directories recursively
        -v        show verbose messages
        -P port   connect to specified port
        -pw passw login with specified password
```

The syntax for SecEx SFTP client is as follows :

```
SecEx SFTP Client
Version 1.1
Usage : sftp [switches] user@host
Switches :

  -P port   Connect to specified port
  -pw passw Login with specified password
  -v        Display verbose output
```

Upon successful login, SFTP maintains a session on the remote server and SFTP shell until you log out.
The SFTP shell commands available are as follows :

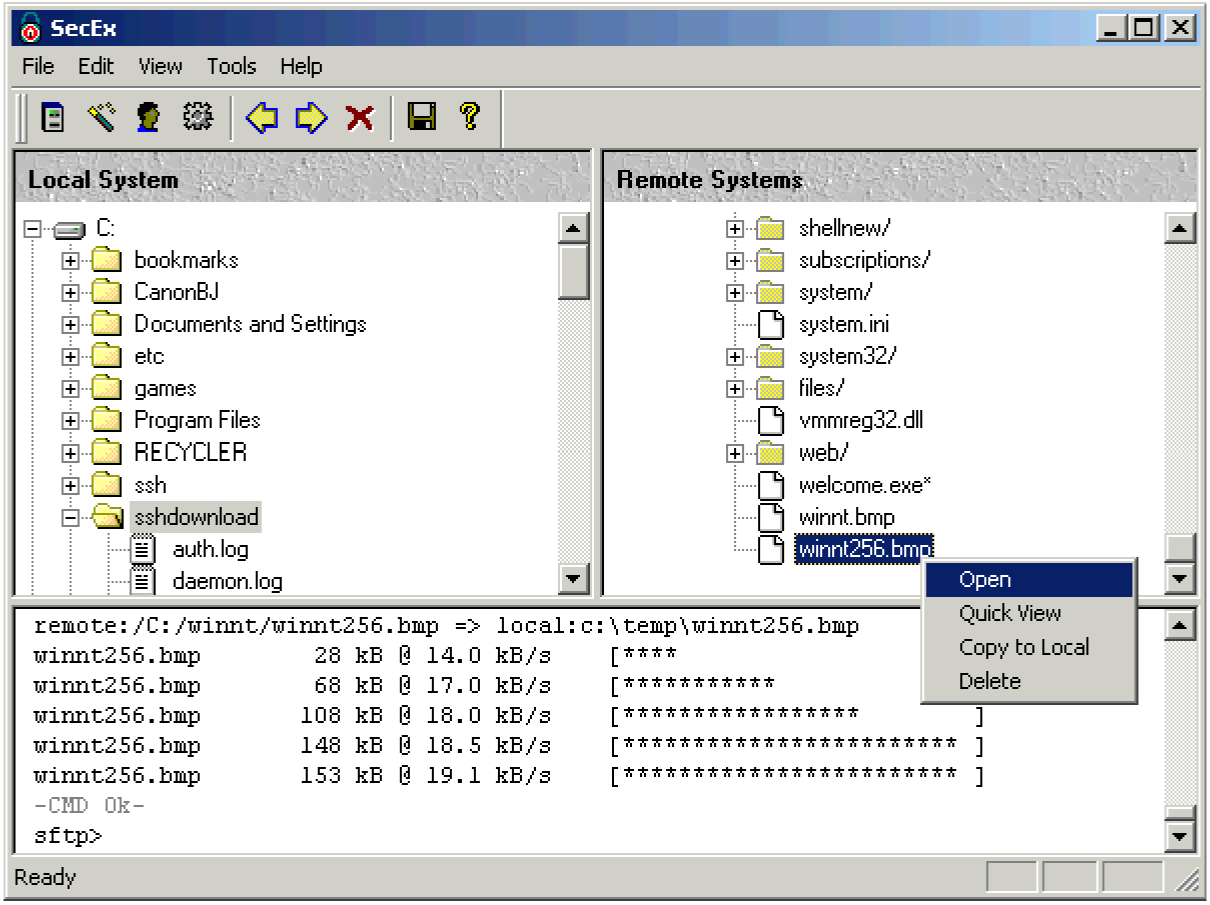
```
SecEx SFTP Client Command Set

ls - display folder information for server working directory
cd <remote path> - change working directory on server
lcd <local path> - change working directory on local system
pwd - display current working directory on server
lpwd - display current working directory on local system
get <remote file> <local file> - fetch file from server
put <local file> <remote file> - copy file to server
mkdir <folder path> - create remote directory
rmdir <folder path> - remove remote directory
rm <file path> - remove file
help - show this help information
```

```
exit - end sftp session
```

3.10 Executing remote files

To execute a file from the remote server on your computer, right-click the file with your mouse and select "Open" from the pop-up menu. Please note that you will not be able to execute Unix binaries on your Windows computer. Certain files, such as ".bmp" image files for example, will have file relevant file associations on both Unix and Windows systems and will therefore be opened with the correct application on your computer.

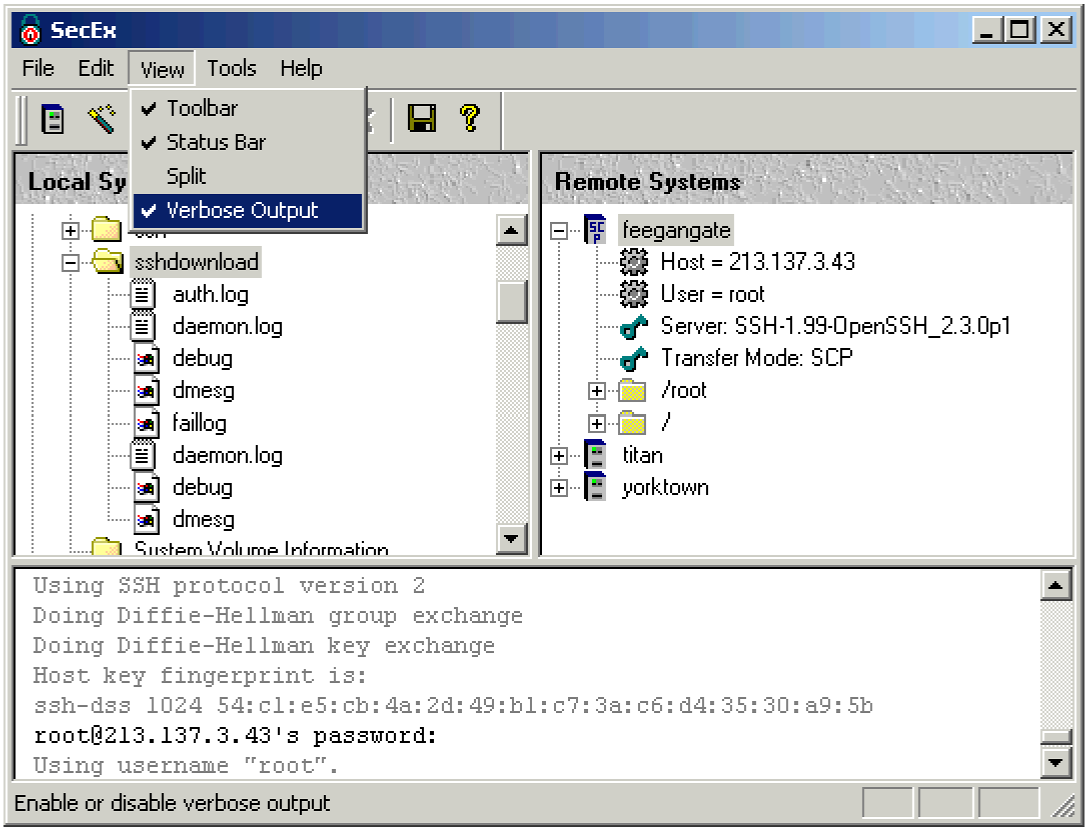
Before being able to execute the file locally, SecEx will download the file from the remote system and store it in the temporary working folder, as configured under Application Preferences.



```
remote:/C:/winnt/winnt256.bmp => local:c:\temp\winnt256.bmp
winnt256.bmp         28 kB @ 14.0 kB/s    [****
winnt256.bmp         68 kB @ 17.0 kB/s    [***********
winnt256.bmp        108 kB @ 18.0 kB/s    [*****************         ]
winnt256.bmp        148 kB @ 18.5 kB/s    [************************  ]
winnt256.bmp        153 kB @ 19.1 kB/s    [************************  ]
-CMD Ok-
sftp>
```

3.11 Verbose output

To display verbose output in the session log window, select "Verbose Output" from the "View" menu. This is useful if you are reporting problems or simply want to take a peek "under the hood". Verbose output is printed in a light grey font and contains details such as SSH protocol version number, host key, as well as file transfer and encryption mode. See also Saving the session log.



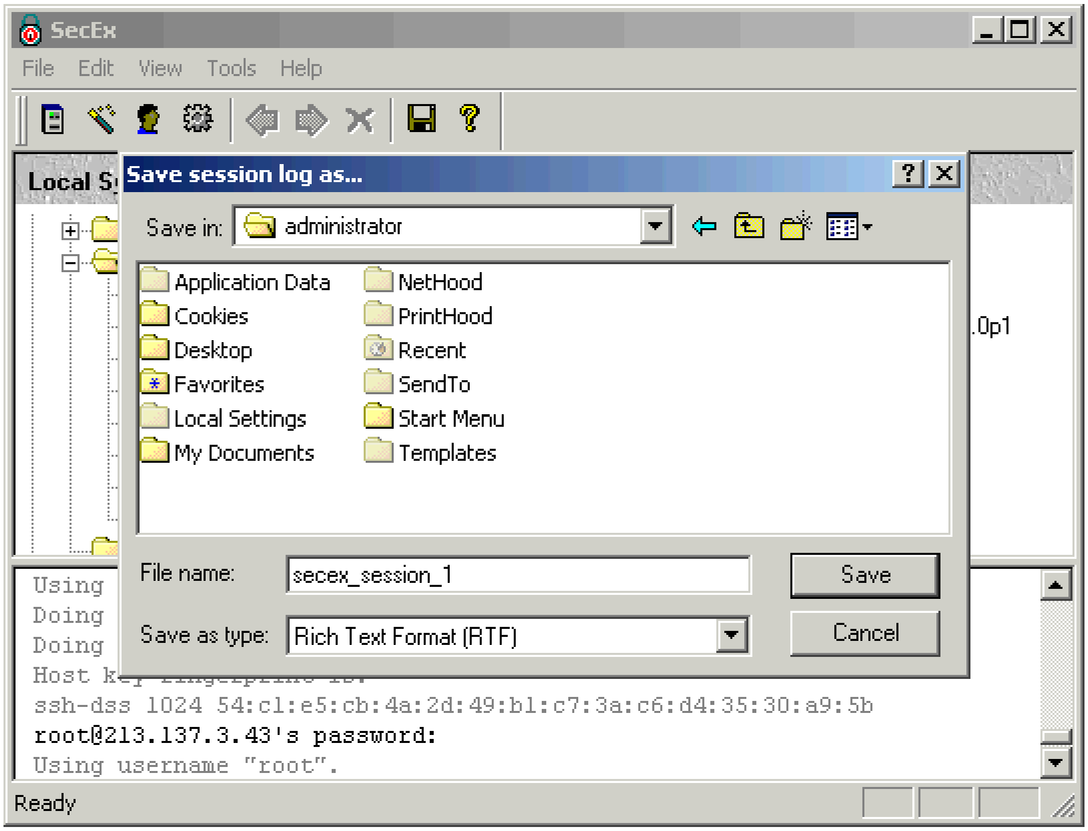
Host = 213.137.3.43
User = root
Server: SSH-1.99-OpenSSH_2.3.0p1
Transfer Mode: SCP

```
Using SSH protocol version 2
Doing Diffie-Hellman group exchange
Doing Diffie-Hellman key exchange
Host key fingerprint is:
ssh-dss 1024 54:c1:e5:cb:4a:2d:49:b1:c7:3a:c6:d4:35:30:a9:5b
root@213.137.3.43's password:
Using username "root".
```

Enable or disable verbose output

3.12 Saving the sessesion log

To save the session log, simple select "Save log as..." from the "File" menu.
If you submit a bug report, please be sure to include a relevant verbose session log.



Save in: administrator

File name: secex_session_1

Save as type: Rich Text Format (RTF)

```
Using
Doing
Doing
Host key fingerprint is:
ssh-dss 1024 54:cl:e5:cb:4a:2d:49:bl:c7:3a:c6:d4:35:30:a9:5b
root@213.137.3.43's password:
Using username "root".
```

4 Technical Data

4.1 Technical specifications

SecEx is compatible with Secure SSH servers. The default mode of communication is SSH protocol version 2 with automatic fall-back to SSH protocol version 1.

Secure file transfer to and from SSH servers is achieved via SFTP (Secure FTP) where available, with automatic fall-back to SCP (Secure Copy Program).

Host authentication is via 1024 bit DSS / RSA keys.

Supported encryption modes are 3DES, Blowfish and AES. 3DES is the default mode of encryption depending on server-side availability. The selected encryption mode for each session is indicated in the verbose session log output.

4.2 What is Secure Shell ?

SSH Secure Shell is a replacement for the telnet command and supports encrypted client / server connections. Secure file transfer is achieved via two secure shell supplements : SCP and SFTP.

SCP (secure copy program) accompanies most SSH version 1 servers.
SFTP (Secure FTP) accompanies most SSH version 2 servers.

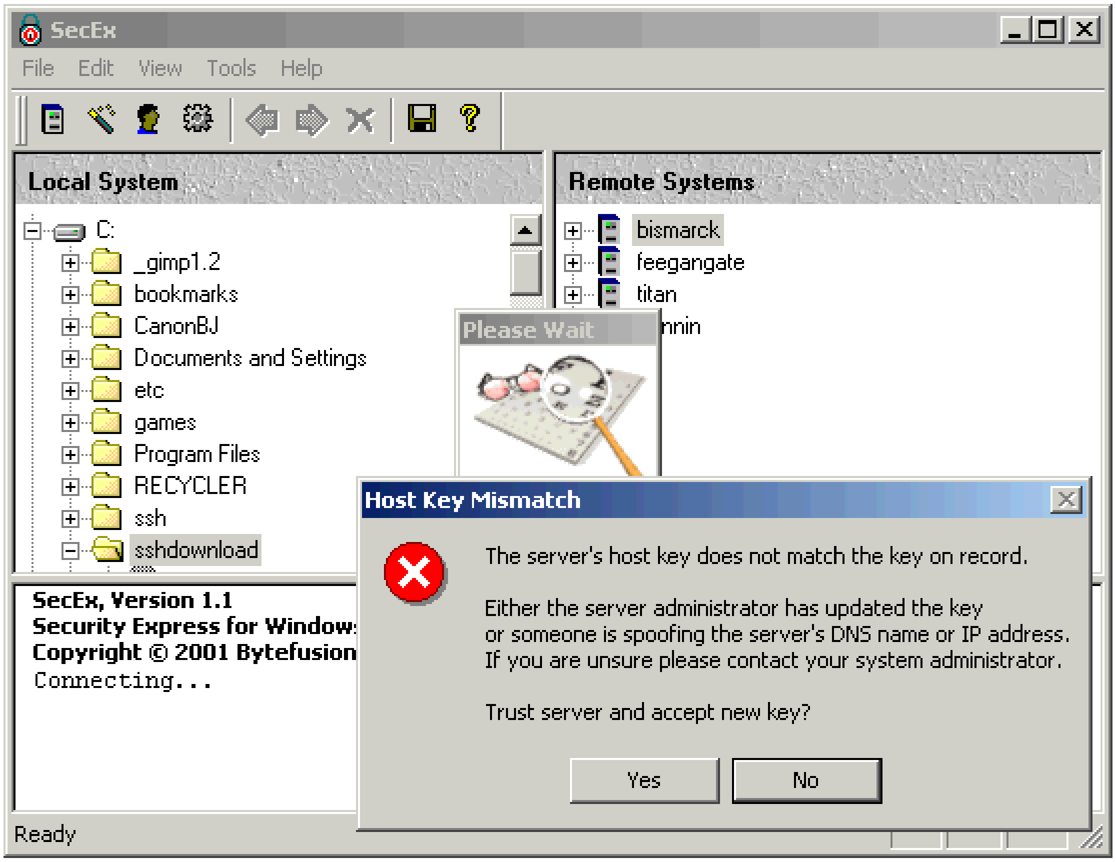
SSH was conceived as an academic project at the University of Finland in 1995. Open Source initiatives have since emerged from the publicly available source code as well as commercial versions of Secure Shell. The lettering "ssh" in its lowercase rendition is a trademark owned by SSH Communications Security.

4.3 DNS/IP Spoofing

IP spoofing is the creation of IP packets using someone else's IP address. DNS spoofing is the substitution of a different IP address for a DNS name. DNS spoofing is commonly achieved by corrupting the DNS database of the DNS server your computer connects to in order to match human readable computer names to physical IP addresses. In both instances, the computer you are connecting to is not the server you expect.

This can be used, for example, to trick you into giving your server user name and password to the computer acting as the impostor. Alternatively, the impostor might simply act as a conduit whilst talking to the real server on your behalf. This is called a "Man-in-the-middle attack" and is commonly used to intercept network traffic without the knowledge of the original participants.

SecEx protects against IP and DNS spoofing by recording each server's public host key. During subsequent connection attempts, the known host key is compared to the host key offered by the server. While an impostor might well offer the same public host key as the server whose identity it is trying to assume, it will fail the subsequent authentication challenge without the corresponding private key owned by the real server.



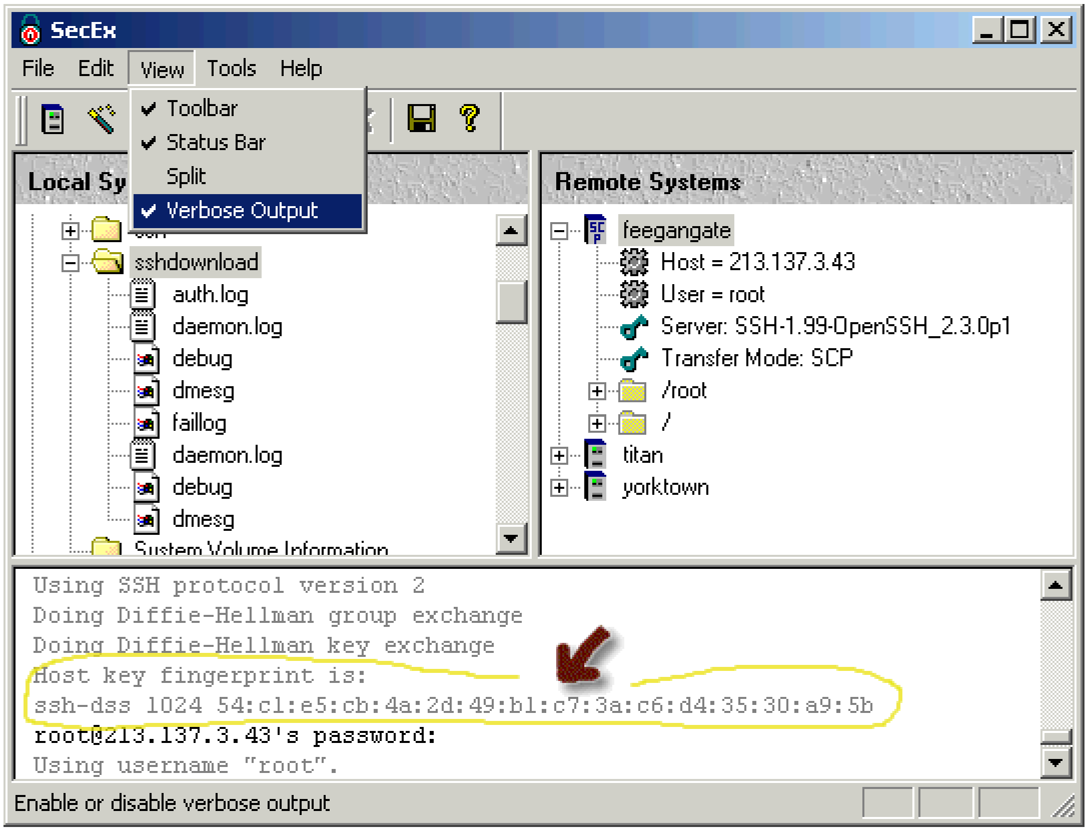
```
SecEx, Version 1.1
Security Express for Window:
Copyright © 2001 Bytefusion
Connecting...
```

The server's host key does not match the key on record.

Either the server administrator has updated the key
or someone is spoofing the server's DNS name or IP address.
If you are unsure please contact your system administrator.

Trust server and accept new key?

When connecting to a server for the first time, there is no reasonable and universal method of ensuring the key's authenticity. They key is therefore accepted by default. If you have any reason to believe that the server you are connecting to has been compromised, you should contact the server's administrator and personally verify the host key fingerprint. The host key fingerprint appears in the log window in verbose mode when logging on to the server.



```
Using SSH protocol version 2
Doing Diffie-Hellman group exchange
Doing Diffie-Hellman key exchange
Host key fingerprint is:
ssh-dss 1024 54:c1:e5:cb:4a:2d:49:b1:c7:3a:c6:d4:35:30:a9:5b
root@213.137.3.43's password:
Using username "root".
```

5 About

5.1 About SecEx

SecEx Security Express
Version 1.5
Copyright © 2001-2002, Bytefusion Ltd.
All Rights Reserved

5.2 About Bytefusion Ltd.

Bytefusion Ltd.
22 Duke Street
Douglas, IOM
IM1 2AY
British Isles

Inquiries: sales@bytefusion.com