Facet***Win***®
Security Pack

Encrypted Terminal Emulator
for use with the Facet***Win***
Windows to UNIX Connectivity Package

Facet***Corp***

Trademarks and Copyright

Facet***Win*** Security Pack

February 2001

Facet***Corp*** 1820 Preston Park Blvd., Suite 1000 Plano, TX 75093 USA
Telephone: 1-877-322-3846 (1-877-FacetGo) or 1-972-985-9901
FAX: 1-800-982-9901 or 1-972-612-2035

License Agreement / Warranty

This Software is the property of Facet***Corp***, and is protected by both United States Copyright Law and International Treaty provisions. You are granted a license to use this Software under the terms stated in this Agreement. You may move the Software from one computer to another, but at no time may a single copy of the Software be installed on more than one computer. Facet***Corp*** authorizes You to make archival copies of the Software for the sole purpose of backing up Your Software and protecting Your investment from loss. Any other use or transfer of the Software without written permission is in violation of Facet***Corp***'s Copyright. You may not sub-license, reverse engineer, decompile, or disassemble the Software.

Title/Ownership

Facet***Corp*** retains title, copyrights, intellectual property rights, and ownership in the Software. This is not a sale of the Software. You are purchasing only the physical media upon which the Software is recorded.

Limited Warranty

With respect to the physical diskette or tape and physical documentation enclosed with the Licensed Product, Facet***Corp*** warrants the same to be free of defects in materials and workmanship for a period of thirty (30) days from the date of purchase by the end-user customer. Licensee may return any defective media to their supplier during the warranty period for a replacement free of charge. The remedy for breach of this warranty shall be limited to replacement and shall not encompass any other damages, including but not limited to loss of profits, special, incidental, consequential, or other similar claims.

The Software and any accompanying written materials are provided "as is" without warranty of any kind. Facet***Corp*** does not guarantee or make any representations regarding Your use of this Software. The entire risk as to the quality, performance and results of this Software is with You. Should the Software be defective in any way, You (and not Facet***Corp*** or their distributors or dealers) assume the entire cost of all necessary servicing, repair or correction.

Facet***Corp*** SPECIFICALLY DISCLAIMS ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL Facet***Corp*** BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGE, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

The Software and documentation are provided with “RESTRICTED RIGHTS.” Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013. Rights for non-DOD U.S. Government Departments and Agencies are set forth in FAR 52.227-19 (c) (1,2).

Facet***Corp*** reserves the right to conduct or have conducted audits to verify Your compliance with this Agreement.

This Agreement shall be governed by the laws of the State of Texas.

Termination

This license is in effect until terminated. You may terminate it at any time by destroying all copies of the Software in Your possession and providing written notice certifying this termination and destruction of Software copies. Your Software license granted under this Agreement will automatically and immediately terminate if You violate any of the terms and conditions of this Agreement without notice.

Acknowledgment

You acknowledge that You have read this license Agreement and limited warranty and agree to be bound by its terms and conditions. You agree that this Agreement supersedes any and all prior oral and written communications relating to the subject matter hereof.

Contents

General

The FacetWin Security Pack uses 56 bit DES encryption to protect the privacy of a FacetWin Terminal emulation session.

The session key used for the encryption is based on a 8 to 64 character passphrase that is entered on both the UNIX server and the PC. Each user is still required to have a valid UNIX user name and password, in addition to knowing the passphrase.

The UNIX administrator controls whether or not an encrypted form of the passphrase can be stored on the PC or must be entered each time by the user. The encrypted form of the passphrase on the UNIX system is accessible only by root and is not usable on the PC. The passphrase can optionally be dependent on the IP address of the PC.

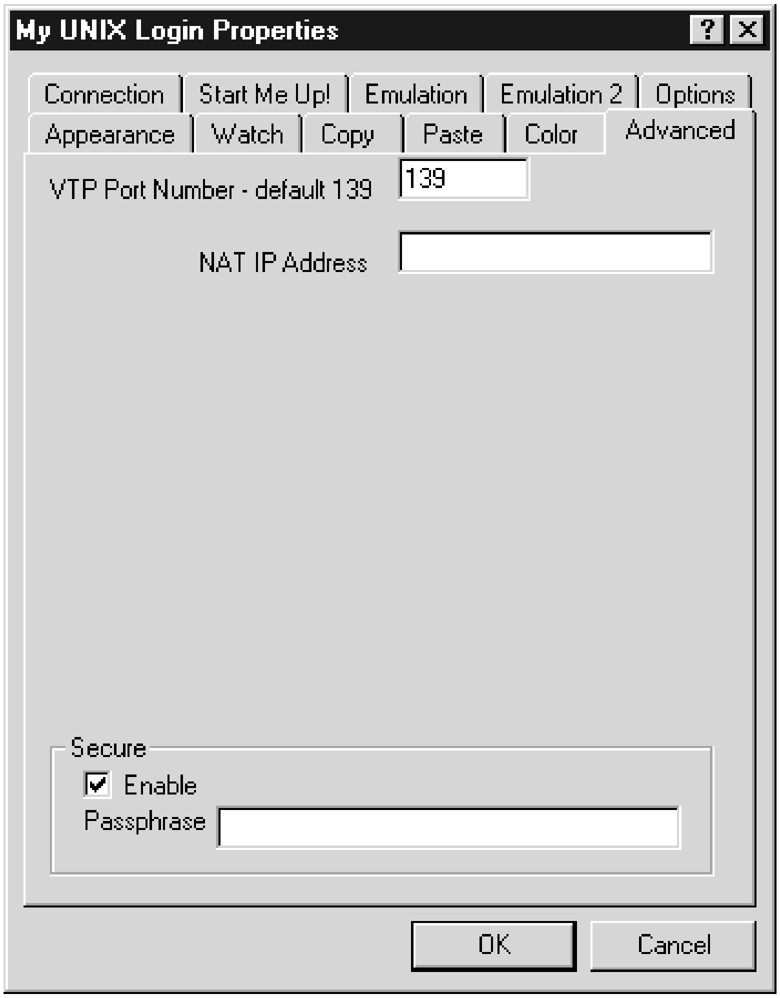
The Security Pack session can be conducted on TCP/IP port 139 normally used by the FacetWin Terminal emulator. It also can be moved to another port selected by the system administrator. This would normally be done when connecting across the internet. See "Configuring Security Pack for a Different TCP Port" for this procedure.

PC Setup

Install the Security Pack emulator on the PC by double clicking the setup.exe on either the CD or diskette 1. When installing from diskette, insert diskette 2 when prompted.

The security Pack emulator will replace your normal FacetWin Terminal emulator. The Security Pack emulator can be used for both normal or encrypted sessions.

After installing the Security Pack emulator, you will see two additional fields on the "Advanced" page of the "Properties". In a box labeled "Secure" at the bottom of the page, there is a check box labeled "Enable" and an edit box labeled "Passphrase":



My UNIX Login Properties

VTP Port Number - default 139: 139

NAT IP Address:

Secure

☑ Enable

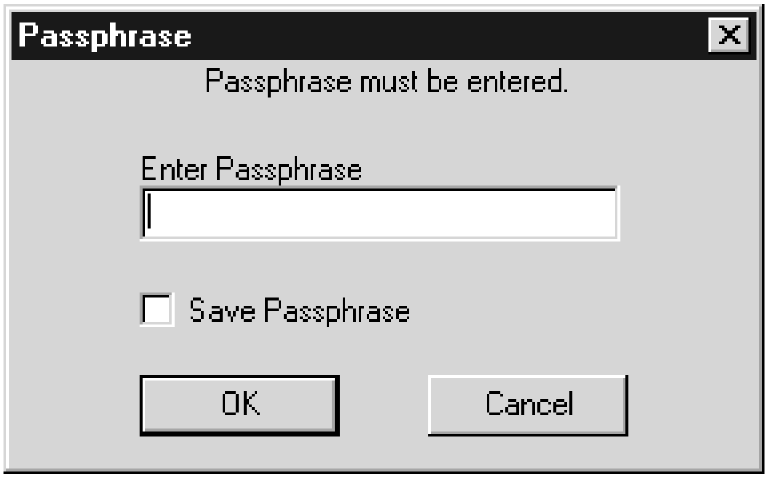
Passphrase:

To conduct a privacy enhanced session, check the "Enable" box and enter the passphrase provided to you by the system administrator in the "Passphrase" box.

The passphrase is stored in an encrypted format by servername, exactly as it is spelled in the "Server:" field on the "Connection" property sheet. Other connections to the same host using the same name will use the same passphrase.

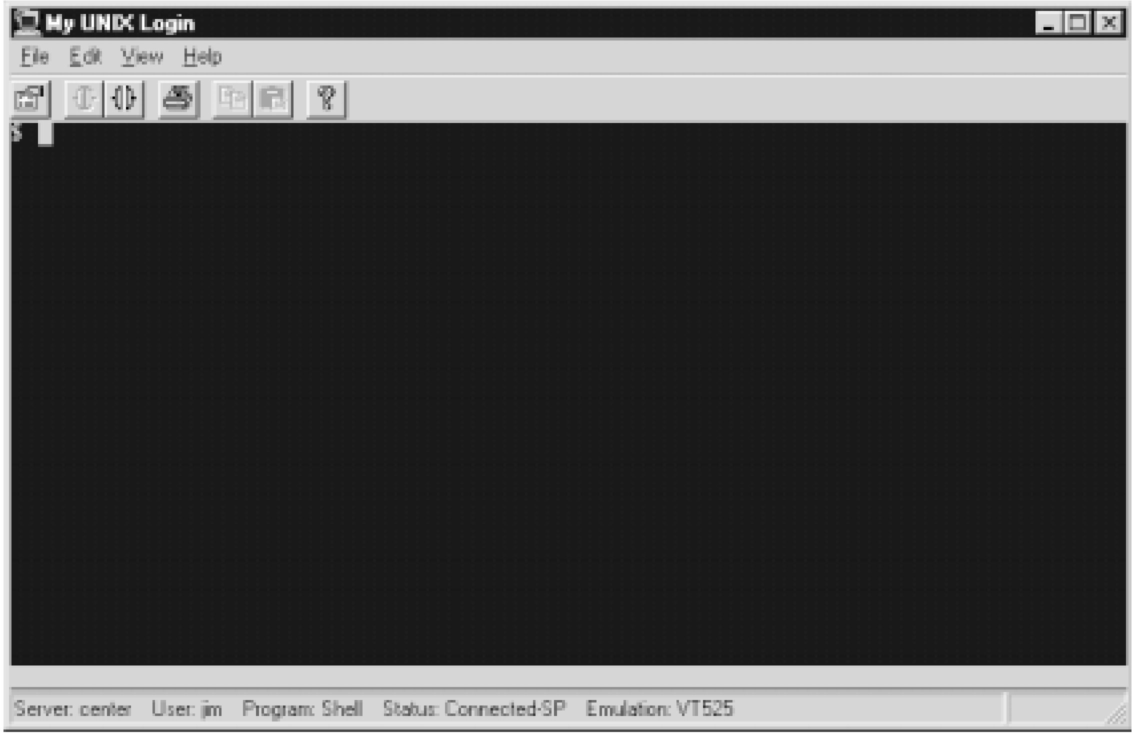
If the system administrator has told you that FacetWin Security Pack sessions are to be run on an alternative TCP/IP port, enter the port number in the "VTP Port Number" box at the top of the property sheet.

If you connect without having stored the passphrase, or if the system administrator has decided not to allow passphrases to be stored on the PC, you will see a dialog box prompting you to enter the passphrase:



Passphrase must be entered.

When the connection is made to the UNIX server, the Status Bar will indicate the Security Pack connection with "-SP" in the "Status:" field:



```
$ 
```

Server: center User: jim Program: Shell Status: Connected-SP Emulation: VT525

UNIX Setup

In the following, /usr/facetwin is the default FacetWin installation directory and should be replaced with the actual directory in which the system administrator installed FacetWin.

Log in as root.

If the passphrase will not be dependent on the IP address of the PC, enter the command:

```
fct_encrypt -e
```

If the passphrase will be dependent on the IP address of the PC, enter the command:

```
fct_encrypt -E 192.168.1.1
```

where 192.168.1.1 is replaced by the IP address of the PC for which you are setting the passphrase.

If you are not root, you will receive the error:

```
ERROR: Must be root.
```

The program will create the directory /usr/facetwin/SECURE. If the directory cannot be created, you will see the message:

```
ERROR: Cannot create directory for Security Pack key
```

At the prompt:

```
Enter passphrase( 8 to 64 characters ):
```

enter the passphrase that you have chosen. See "Creating a good passphrase" for tips on choosing the passphrase. A bad passphrase creates a weak link in the security chain.

A passphrase with an invalid length results in the message:

```
ERROR: Must be 8 to 64 characters
```

At the prompt:

```
Re-enter passphrase:
```

type the passphrase again.

If the two passphrases do not match you will see the message:

```
ERROR: Entries did not match
```

and you will return to the first passphrase prompt. Enter a zero length passphrase to quit without setting a passphrase.

If the two typed passphrases match, they will be added to the passphrase file:

```
/usr/facetwin/SECURE/secure.cfg
```

and you will see the message:

```
Security Pack key successfully updated.
```

If there is any problem updating the Security Pack key file, you will see one of the messages:

```
ERROR: could not create temp file for Security Pack key
ERROR: could not set permissions on temp file for Security Pack key
ERROR: could not read old file for Security Pack key
ERROR: could not write temp file for Security Pack key
ERROR: could not rename temp file for Security Pack key
```

Contact FacetWin support if you encounter one of these errors. Note that it is normal for the key stored in the file to be different, even if the same passphrase is stored again.

Make sure that your installation is secure by checking the permissions on the files and directories:

The file /usr/facetwin/SECURE/secure.cfg should be 0600 and owned by root:

```
# ls -l /usr/facetwin/SECURE
-rw-------  1 root auth   83 Jan 19 10:30 secure.cfg
```

The directory /usr/facetwin/SECURE should be 0700 and owned by root:

```
# ls -ld /usr/facetwin/SECURE
drwx------  2 root auth  512 Jan 22 23:10 /usr/facetwin/SECURE
```

The directory /usr/facetwin should be 0755 and owned by root:

```
# ls -ld /usr/facetwin
drwxr-xr-x  35 root sys 2048 Jan 30 06:40 /usr/facetwin
```

To require PC users to enter the passphrase each time a connection is made, add the line:

```
saved_security_pack_key=NO
```

to the file

```
/usr/facetwin/SECURE/secure.cfg
```

Troubleshooting

If the PC user attempts to connect to a port on which there is no server running, the following message will be displayed:

```
Connection failed.
Winsock connect failed to 192.168.1.1
Connection refused
```

To fix this problem, correct the server on the connection tab, the port number on the advanced tab, or correct the installation of the server.

If the PC user attempts to connect to a server for which the passphrase has not be set on the server, the following message will be displayed:

```
Connection failed
Encryption server refused.
```

To fix this problem, install the passphrase on the server.

To troubleshoot a connection problem, enable your syslog to record debug level messages. When a pc connects you will see the messages:

```
Jan 8 13:08:01 mysystem fct_nbsd[10222]: Connection from (192.168.6.127)
Jan 8 13:08:01 mysystem fct_etpd[10223]: Connection from (192.168.6.127)
Jan 8 13:08:01 mysystem fct_etpd[10223]: fct_etpd -n PCNAME
Jan 8 13:08:01 mysystem fct_etpd[10224]: User user3 (uid=0) logged in.
```

When a PC connects with an incorrect passphrase, you will see:

```
Jan 8 13:29:03 mysystem fct_nbsd[11087]: Connection from (192.168.6.127)
Jan 8 13:29:03 mysystem fct_etpd[11091]: Connection from (192.168.6.127)
Jan 8 13:29:04 mysystem fct_etpd[11091]: fct_etpd -n PCNAME
Jan 8 13:29:04 mysystem fct_etpd[11091]: facetwin vtp exit: Encryption key
   error
```

The PC user will see the message:

```
Connection failed.
Receive error on startup 1.
Protocol error
```

Make sure the passphrase is entered correctly, and try again.

Creating a Good Passphrase

A good passphrase should be easy to type and hard to guess.

The hard to guess part says to not make it a single word, name, company name, address etc. It also says not to make it anything you have seen as an example.

The easy to type part rules out a really good passphrase which is a long string of completely random characters.

A reasonable compromise is a phrase of several words with varying case and several symbols and/or numbers scattered through them. Another good method is to take a longer phrase or sentence and use the first letter of each (or second or last), again with some symbols or numbers added.

Configuring Security Pack for a Different TCP Port

Define the alternate port in the "services" file.

Add the following line to the /etc/services file:

```
fwspport 7014/tcp # FacetWin Security Pack Port
```

where "7014" is the unused port number you want to use.

Configure the "inetd" daemon to listen for new service.

FacetWin does not attach to the TCP port and wait for incoming connections. We instruct the inted daemon to do this for us. This can be done by editing the /etc/inetd.conf file. Just copy the "fct_nbsd" line that is already in "inetd.conf", change the port name at the beginning of the line to be your new port name, and change the name of the program at two places at the end of the line to fct_etpd:

```
#### FacetWin ####
nb-ssn   stream tcp nowait NOLUID /usr/facetwin/sys/fct_nbsd fct_nbsd
fwspport stream tcp nowait NOLUID /usr/facetwin/sys/fct_etpd fct_etpd
#### FacetWin ####
```

So, in the above example, the existing line in /etc/inetd.conf beginning with "nb-ssn" is copied and "nb-ssn" is changed to "fwspport", and "fct_nbsd" is changed to "fct_etpd" in two places.

Get the "inetd" daemon to reread its configuration file.

This is done by sending the inetd process a SIGHUP (hangup signal). First use the ps command to locate the inetd process like this:

```
ps -e | grep inetd
```

The process ID (PID) is the very first number on the line that is returned. Now, issue a "kill -1" on that process, like this:

```
kill -1 INETD_PID
```

where "INETD_PID" is the process ID number of "inetd" we obtained from the ps command.

Verify that the UNIX server is listening on the port.

This can be done using a netstat command like this:

```
netstat -na | grep FWSPPORT
```

where FWSPPORT is the port number you used in step 1. This should generate output like this:

```
tcp    0   0  *.7014       *.*             LISTEN
```

Be sure to notify users of the port number that is being used for the Security Pack emulator so that they can specify this port number on the "Advanced" page of the emulator's property sheet as described in the "PC Setup" section above.

Automatic Upgrading of the Security Pack Emulator

Similarly to the way the normal FacetWin Terminal emulator will inform you that a newer version is available on the server, the FacetWin Security Pack emulator will check for a newer version if that feature is enabled. Of course, it checks the version of a different set of files so that it gets the correct emulator.

Note that, just like the normal emulator, the Security Pack emulator loads a new version by running the setup.exe using FacetWin file sharing services. You would normally have file sharing available if you are using the Security Pack on a local LAN. You would not normally have file sharing services when connecting over the internet. In this case, you would upgrade the PC using the CD or diskettes.

To activate the feature, create a new directory:

```
/usr/facetwin/fwt/SECURE
```

It should be owned by root and have the permissions rxwr-xr-x:

```
chown root /usr/facetwin/fwt/SECURE
chmod 755  /usr/facetwin/fwt/SECURE
```

In that directory, copy the setup.exe and version.txt from the CD. (The files on the diskettes are not suitable for this purpose.)

In the configuration file:

```
/usr/facetwin/facetwin.cfg
```

add the following line to enable the server to tell the PC that this version is available:

```
S_PC_upgrade=OK
```

Creating Diskettes

If installing the FacetWin Security Pack emulator on multiple PCs from one CD is a problem, diskettes can be created.

Two diskettes are required. They will be formatted by the script. Label them "FacetWin Security Pack", the build number from the CD, and "disk 1" and "disk 2".

Using the explorer or an MSDOS command prompt, change to the directory on the top level of the CD:

```
    \diskette
```

Double click or run the script:

```
    makedisk.bat
```

At the prompt, enter "B" to make both diskettes, or choose one of the other options to make the first or second diskette only.

The diskettes are installed by running setup.exe from the first diskette and inserting the second diskette when prompted.