Ascend Password Protocol Server Software Release Note 2.0Ci1

October 29, 1997

This release note describes corrections and enhancements made to the Ascend Password Protocol Server (App Server) since software release 2.0C.

If you need Technical Assistance, contact Ascend in one of the following ways:

Telephone in the United States	800-ASCEND-4 (800-272-3634)
Telephone outside the United States	510-769-8027 (800-697-4772)
Austria/Germany/Switzerland	(+33) 492 96 5672
Benelux	(+33) 492 96 5674
France	(+33) 492 96 5673
Italy	(+33) 492 96 5676
Japan	(+81) 3 5325 7397
Middle East/Africa	(+33) 492 96 5679
Scandinavia	(+33) 492 96 5677
Spain/Portugal	(+33) 492 96 5675
UK	(+33) 492 96 5671
Email	support@ascend.com
Email (outside US)	EMEAsupport@ascend.com
Facsimile (FAX)	510-814-2312
Customer Support BBS by modem	510-814-2302

The AppSrv-970924.tar.gz (TARed and GZIPed) file will expand to several sub-directories, each housing the set of binaries for each of the 6 different platforms supported (UNIX, DOS, Apple Macintosh, Windows 3.1, Windows 95, and Windows NT). The README files provided in the sub-directories contain installation instructions.

New features in this release

Axent Softkey support for App Server

Ascend units affected: Pipeline models used with Windows 95 and Windows NT

Introduced in: 2.0Ci1

This enhancement simplifies authentication when using the Axent SecureNet Softkey.

Using App Server with Softkey

When using SecureNet, you must install a Softkey on your computer's hard drive, or supply a diskette-based Softkey that needs to be inserted in your computer's floppy drive when logging onto a SecureNet system. If the Softkey is present when App Server is installed, the App Server INI file is automatically modified to work with the Axent SecureNet Softkey. (If the Softkey is installed after App Server, you can manually modify the Path key in the WinSNK section of the INI file, as shown below.)

The App Server functions as usual with Softkey, except that whenever App Server is started it attempts to find the Softkey, and if found, the Axent SecureNet software prompts for a PIN. Once entered, all subsequent transactions between the authentication server and the App Server are transparent, unless an error occurs, or if the Softkey has expired.

Initialization file changes

A new section has been added to AppSrvr.ini called WinSNK. The purpose of this section is to maintain a list of text messages received from the authentication server, which allows you to keep App Server synchronized with any change made by the SecureNet administrator.

Initialization file structure

There are three sections in AppSrvr.ini. The sections are described in the following table:

INI section	Description

`[BANNER]`	Up to 5 line of text, each one must begin with the syntax "line x=", where x is a number from 1 to 5. For example
	[BANNER]
	`line 1="First line of text"`
	`line 2="Second line of text"`
	`...`

INI section	Description
[PROFILE]	Allows for the following two key names: Name = User = Name is the name of the remote Ascend unit. **Note:** This field is ignored when using Axent SecureNet since this information is contained in the Softkey authentication routine.) User is the profile name to use when connection.
[WinSNK]	Consists of 33 lines with the first using the key name, Path, and all remaining lines using a number from 0 to 31. Path is the fully qualified path to the location of the installed Axent SecureNet Softkey. 0-31 contain the text as entered on the authentication server.

Additionally, a section entitled [App Server] is added to WIN.INI when App Server is installed, containing the default socket data (automatically entered by the App Server utility). Even though the data is listed in WIN.INI, the values are actually stored in the Windows Registry.

Two keys are included in the [App Server] section of WIN.INI:

- udp_port
- bcast_udp_port

Sample AppSrvr.ini file

The following is a sample AppSrvr.ini file that illustrates the overall format.

```
[BANNER]
line1="This is a sample for testing"
[PROFILE]
Name=Max4
User=jgray
[WinSNK]
Path=F:\WinSNK
0=Call intercepted by Defender Security Server
1=Unauthorized use of this system is prohibited
3=Enter ID:
4=SNK Challenge: %s ^M^JEnter Response:
5=Invalid Identification.
6=Invalid SNK Response^M^JSNK Challenge: %s ^M^JEnter Response:
7=Access Approved. You are now connected to service.^M^J
8=Access Denied.^M^J
9=All Channels of Security Server are busy.  Try again later ^M^J
10=Unexpected packet from Agent^M^J
11=Cannot start new call on active channel^M^J
12=Cannot start new call on active channel^M^J
13=Unexpected input from user.^M^J
14=Enter Password:
```

```
15=Invalid Identification.^M^JEnter ID:
16=Your password has expired.^M^JEnter New Password:
17=Enter New Password:
18=Enter New Password again:
19=Passwords didn't match.^M^JEnter New Password:
20=Outside your time class.^M^J
21=Outside your date class.^M^J
22=New password must differ from old.^M^JEnter New Password:
23=New password is too short.^M^JEnter New Password:
24=New password must include numeric digit.^M^JEnter New Password:
25=Request noted.^M^JEnter old password
26=Your account is locked due to excess violations.^M^J
27=Your ID is already active on another channel.^M^J
28=Your password has been changed.^M^J
29=Your account is locked due to non-usage.^M^J
30=You are not authorized for that host.^M^J
31=Inactivity Timeout.^M^J
```