

**ppnPRO Operating Manual**  
Latest update: July 18, 2004

**Table of Contents**

**1.0 Introduction**

**2.0 Purpose**

The Purpose of ppnPRO  
The Purpose of ppnVault

**3.0 Operational Features**

**4.0 Operational Characteristic**

Cryptographic System  
Authentication Mechanisms  
Operational Limitations  
Operational Interfaces  
Operating Environments

**5.0 Operating Procedures**

Setting Up for a new ppnPRO Account  
User Name and User Password Rules  
Setting Up for a new ppnPRO Group  
Group Name and Group Password Rules  
Setting up a ppnVault account  
Basic Password Security Rules  
Operating ppnPRO  
ppnPRO Window Set-up  
Function of ppnPRO Operational Buttons

**6.0 Trouble Shooting a Problem**

>>>><<<<<

**1.0 Introduction**

This ppnPRO Operational Manual is intended to be a reference source which provides information on the operational procedures; features; limits and characteristic of ppnPRO and ppnVault programs and

services. As these various items evolve and new features are added this manual will be revised.

Although this Manual is copy written material your are granted the license rights to make a limited number of copies for your use in operating the ppnPRO and ppnVault software and services.

## **2.0 Purpose**

### **The Purpose of ppnPRO**

**Purpose:** The purpose of **ppnPRO** is to provide the public, particularly the professional, and all private industry and public entities with a secure means of transferring data between one or more parties, quickly and simply.

**Objective:** The objective is to provide this capability at a level of security which is higher (stronger) than is common in the community. Currently the common standard (or community standard) for data file transfer is SSL (secure socket level).

We provide this capability in a unique format, which is easier to use, very mobile and fully compatible with existing computer operations. **ppnPRO** is an outstanding secure data file transfer service which fully meets these important objectives. In reviewing the features of our products and services it is abundantly clear that **ppnPRO's** security is higher level than SSL and other currently commercially available security systems, and, of course, much, much better than no security.

**ppnPRO** accomplishes these objectives using the patent-pending ppn technology. This technology utilizes government approved 256-bit encryption, a special secure pipeline network, a set of proprietary encryption management algorithm, and other great security features. The security design and operation of **ppnPRO** is significantly enhanced by the fact that it does NOT use any internet browsers, the world wide web, email or FTP services, all of which are very vulnerable to penetration and other types of cyber-attacks.

For those parties who claim that no security can stop every serious cyber-attack, the answer is **ppnPRO** is as close as you can get to full security. It is much more secure than SSL and VPNs and at a much more affordable price.

If SSL is equivalent to transporting your valuables to your bank in your briefcase; then **ppnPRO** is equivalent to transporting your valuables to the bank in an Armored Truck with arm guards and a police escort.

Which way would you prefer to transfer your valuables? **ppnPRO** is the safe and secure answer to the transfer of all type of electronic valuables.

### **The Purpose of ppnVault**

**Purpose:** The purpose of **ppnVault** is to provide the public, particularly the professional, and all private industry and public entities with a secure storage facility for data which can be accessed by authorized parties, quickly and simply.

**Objective:** The objective is to provide this capability at a level of security which is higher (stronger) than is common in the community and at an affordable price. It is also our objective to provide this capability in a format, which is easy to use, very mobile and fully compatible with existing computer operations. **ppnVault** is an outstanding secure data file storage service which fully meets these important objectives. In reviewing the features of our products and services it is abundantly clear that **ppnVault's** higher level of security is more secure than is currently available secure storage systems.

Whether your need a secure off-site storage facility for backup of critical data files or a location to securely deposit private or confidential data files for either an extended period of time or just temporarily ppnVault is available. It is not only a secure data file storage facility, but with ppnPRO as the secure pipeline into and out of the Vault, the data is secure from your computer to the Vault and back to your computer.

### **3.0 Operational Features**

Both ppnPRO and ppnVault provides the highest level of security for those data transfer applications for which the protection of information is critical. It is the preferred data transfer medium for those individuals and organizations that want privacy and security and/or that are required to comply with Federal, or state, or local laws and regulations that address the protection of an individual's privacy and/or the maintaining of the confidentiality of electronic data.

The ppnPRO is a personal private network (ppn) which is "personal" to a specific subscriber. The services and features are attached to a ppnPRO User Name and User Password and can be accessed and used by that User Name and User Password from and computing device which can access the Internet from any location in the world. To obtain service the computing device must have installed ppnPRO and JAVA (j2re-1\_4\_2\_05 or higher) installed which can always be downloaded and installed on any computer. Both are available for download from the ACAP website at: [www.acapsecurity.com](http://www.acapsecurity.com).

These two components are needed to open the ppnPRO operating window. Upon opening the ppnPRO window, enter the Host name; ["acapsecurity.com"]; the Port number ["7123"]; your ppnPRO User Name [your ppnPRO User Name]; the name of the Group which you desire to participate [Group Name]; your ppnPRO User Password [your ppnPRO User Password]; and then click on "Connect." If everything is correct and you are an active ppnPRO subscriber, you will be connected.

You may open multiple ppnPRO windows at the same time. You can be on-line and active with more than one Group at a time. You may be a member of as many Groups as is desired.

If you are connected to a Group and you are not active for a period of 30 minutes you will be notified of your inactivity, and if you continue to be inactive you will be disconnected. You may re-join the Group by clicking on "Connect."

ppnVault is the secure storage media used by ppnPRO to facilitate the secure transfer of communications and data between members of a Group. ppnVault operates with two distinct types of secure storage service. One is temporary secure storage which is used to facilitate the secure storage of data during the depository transfer of information between Group members. The other type is permanent secure storage which is used by a Group to provide long term secure storage of data files.

Secure temporary storage is provided as part of each subscriber's ppnPRO service. The permanent secure storage is leased as an add-on to ppnPRO services. Access to permanent storage is open to all members of a Group therefore if a ppnPRO subscriber desires to be the only party with access right to secure area of ppnVault the User needs only to set up a Group and the User is the only member of the Group.

For a discussion of the transfer and data file size limitations for both temporary and permanent secure storage see Section 4- Operational Characteristics.

For a discussion of the specific features of ppnPRO see Section 5.0 – Operating Procedures. Also see the demonstration movies provided on the ACAP website at: [www.acapsecurity.com](http://www.acapsecurity.com).

## **4.0 Operational Characteristics**

This section of the Manual provides information on the features and characteristics of the Cryptographic System; the Authentication Mechanisms; the Operational Limitations; the Operational Interfaces; and the Operating Environments.

For security reasons some unique cryptographic information and encryption process management features are not discussed.

### **Cryptographic System**

- U.S. Government Approved and Authorized encryption algorithm
- No "Backdoor" access to the encryption algorithm
- Communications encryption with AES with 256-bit encryption keys
- Complies with FIPS 197, Advanced Encryption Standard (AES), November 2001
- Encrypted data files and messages stored in encrypted form in ppnVault
- Separate AES key for each ppnPRO user
- Electronic AES key generation
- Automatic AES re-keying
- Manual initiation of AES re-keying upon demand
- Password access encrypted using SHA encryption
- Complies with FIPS 180-2, Secure Hash Standard (SHS)
- Biometrics access mapping data stored in encrypted form in ppnVault
- Finger print biometrics as optional password access (under development)
- No use of any Internet Browser in any secure ppnPRO operations
- No use of the world wide web (www) in any secure ppnPRO operations
- No use of ftp services in any secure ppnPRO operations
- No use of any e-mail services in any secure ppnPRO operations

### **Authentication Mechanisms**

Group Participation Access:

User Name and User Password combined with Group Name  
User Password can be provide by biometric finger print (option under development)

Group Management Access:

User Name and User Password combined with Group Name and Group Password  
User Password can be provide by biometric finger print (option under development)

Account Management Access:

User Name and User Password  
User Password can be provide by biometric finger print (option under development)

Access to Group Data Files (Temporary Storage) at ppnVault:

User Name and User Password combined with Group Name  
User Password can be provide by biometric finger print (option under development)

Access to Group Data Files (Permanent Storage) at ppnVault:

User Name and User Password combined with Group Name and Group Password  
User Password can be provide by biometric finger print (option under development)

**Operational Limitations**

Group Usage of Temporary Storage at ppnVault

Single data file transfer size- 5.0 MB  
Maximum available secure temporary data file storage per Group- **50 MB**  
Automatic secure destruction of temporary data files storage-  
Secure destruction occurs without notice  
120 hours after time of deposit into ppnVault

Group Activities

Created Group name and Group automatically cancelled if not utilized  
by at least one Group member within 90 days of creation  
Active Group member is automatically disconnect after 30 minutes of non-use  
Newly created Group is automatically cancelled if Group is not actively utilized within 48 hours of creation of the Group  
Established Group is automatically cancelled and all data files

securely destroyed if Group creator is deleted from Group

#### Group Usage of Permanent Storage at ppnVault

Single data file transfer size- 50 MB

Maximum available secure permanent data file storage per Group

Set by the ppnVault subscription option – see your Account

Typical storage options are 50 MB; 100 MB; 300 MB;  
500 MB; 1 G; 3 G and 5 G.

### **Operational Interfaces**

Both ppnPRO and ppnVault support operations interfaces with:

#### All Internet Dial-up and DSL services

AOL

EarthLink

Net Zero

Juno

Highstream

SBC

Qwest

Version

AT&T

All Internet Access Providers

All ISPs (Internet Service Providers)

#### All Internet Cable Modem services

Comcast

Time-Warner/Roadrunner

Cox

Adelphi

Charter

All Cable Modem ISPs

#### All Internet Satellite services

Direct TV

Dish Network

All Satellite Based ISPs

### **Operating Environments**

Both ppnPRO and ppnVault will support operations with:

Notebooks/Laptops

Tablet PCs  
Desktops  
Midsize systems/workstations  
Large Mainframes/workstations  
Microsoft Windows 98/Me/NT/2000/XP/others  
Sun Solaris  
IBM AIX  
HP UX  
Linux  
Lindows  
Apple System 10  
All Unix based operating systems

## **5.0 Operational Procedures**

This section addresses the procedures and rules of operation of ppnPRO and the temporary storage area of ppnVault. Specific operational procedures associated with the permanent storage area of ppnVault will be provided in an update to this Manual.

### **Setting Up for a new ppnPRO Account**

ppnPRO and ppnVault are products and services which are attached to a specific User Name and User Password. The service is computer or workstation independent in that anyone with a ppnPRO user Name and User password can access the ppnPRO services from any computer anywhere in the world as long as they can gain Internet access.

Due to this User independence and mobility the security of your User Name and User Password is very important to maintaining of security of your Groups and the security of the Groups to which you are a member. If you detect, or suspect, a compromise of your ppnPRO User Password you should immediately go to your ppnPRO Account and change your password or on your ppnPRO operations window select the "Misc." button and the "Change Password" button and change your current password.

Similarly, if you suspect that your Group has been compromised, or that your Group Password has been comprised, remove all of the Group's data files stored in temporary storage in the ppnVault and delete the Group. Thereafter you can create a new Group to replace the deleted Group. To delete a Group, visit the ppnPRO operating window and select "Admin" and thereafter select "Delete Group."

To set up a ppnPRO account you must select one of the many options available to obtain a ppnPRO subscription and complete the request for information.

Following your creation of a ppnPRO User name and User Password you will be provide access to your personal Account page.

Your Account allows you determine the number of days remaining on your ppnPRO subscription and to initiate the procedure to add days to your open account.

It also provides you with the ability: to complete an install of ppnPRO on your computer system; to create a new ppnPRO Group; to add new and additional members (ppnPRO subscribers) to any Group which you have created; and to change your password.

- Download and Install ppnPRO on this computer
- Report on My ppnPRO subscription status
- Create a New Group
- Add Members to a Group
- Change My Password

## **User Name and User Password Rules**

### User Name

Purpose and function: a part of your unique personal identifier  
and a segment of the User access authentication process

Maximum number of characters: open

Minimum number of characters: 1

Upper and lower case character rules: case sensitive

Allowable characters: All numbers and alpha characters- can be upper  
and lower

Disallowable characters: No special characters

Other limitations: NO spaces between characters

### User Password

Purpose and function: a part of your unique personal identifier  
and a segment of the User access authentication process

Maximum number of characters: open

Minimum number of characters: at least 8

Upper and lower case (size) character rules: case sensitive

Allowable characters: All numbers and alpha characters- can be upper and lower

Disallowable characters: No special characters

Other limitations: NO spaces between characters

Do not make password same as User Name

### Customized User Names and User Password for a Specific Group

Group member names

No

Group member passwords (

{ they can not change their user name and set one up for a group?})

### Biometrics as User Password access option

ppnPRO and ppnVault will soon be offering finger print biometrics as an access option to ppnPRO and ppnVault services. As that feature becomes available this Manual will be amended to include the operational procedures for biometric access.

## **Setting Up for a new ppnPRO Group**

The creation of all new Groups is performed within your Account Management page at the ACAP website. At the Home page on the top row of buttons select "Account." Complete the information needed to enter your Account.

### Create a New Group and Add Members to a Group

For security reasons, ppnPRO access control software is very strict about User Names, Group Names and all types of passwords. You may use either upper or lower case letters in Group Names, Group passwords, User Names and User Password but what you initially enter must be what you re-entry for access or you will be denied access. The short, ppnPRO is very letter case sensitive.

To create a ppnPRO Group, the Group Name must be at least 8 characters in length; be either letters or numbers, no special characters. The Group Password must be at least 8 characters in length. A ppnPRO Group Password is not a ppnPRO User Password.

Do not use your ppnPRO User Name for a ppnPRO Group Name and do not use your ppnPRO User Password for a ppnPRO Group Password.

Remember the Group Name because it is a required identifier when you use ppnPRO. Also remember and protect the Group Password. The Group Password allows the holder of the password to disable and enable member's access to the Group and provides other control features.

As a ppnPRO subscriber you can be included in one or many Groups created by other ppnPRO subscribers. You can, but you do not have to, create a Group. As a ppnPRO subscriber you may create many Groups and any Group may have many members. If you create a new Group, as the creator, you are immediately a member. You may thereafter add new and additional member as you desire. The input form allows for the entry of up to 5 new members at a time. New members are included by adding the party's ppnPRO User Name. Following the creation of a Group notify the included member of the Group Name. Make sure every Group you create has different Group name and Group Password.

Only ppnPRO subscribers may participate in a Group; therefore if you desire someone to participate, even temporarily, in one or more of your Groups have them subscribe to ppnPRO, either by obtaining a free evaluation copy or by ordering the service. To delete an existing member open the ppnPRO operating window and select the "Admin" pull down; then select "Delete Account." To delete an existing Group select "Delete Group."

When opening your ppnPRO window for use the following is to be entered into the appropriate input slots- Your Host is: "acapsecurity.com" and Your Port is: "7123" these are the only acceptable inputs.

If you know the name of a Group someone else has created for you to be part of, then enter that name next to the Group field of the ppnPRO window.

Note Group Names and Passwords: Group and Group passwords can be any alphanumeric characters, must contain at least 8 characters and begin with a letter.

You may open multiple ppnPRO windows at the same time and you can be on-line and active with more than one group at a time.

You may be a member of as many groups as desire. There is no limit to the number of parties who may be a member of a specific group; however, the number of group members who can simultaneously participate on-line in a group is 128 parties.

If you are connected to a group and you are not active for a period of 30 minutes you will be notified of your inactivity, and if you continue to be inactive you will be disconnected. You may re-join the group by clicking on "Connect."

## **Group Name and Group Password Rules**

### Group Name

Group Name can be any alphanumeric characters, must contain at least 8 characters and begin with a letter.

Upper and lower case character rules: case sensitive

Allowable characters: All numbers and alpha characters- can be upper and lower

Disallowable characters: No special characters

Other limitations: NO spaces between characters

### Group Password

passwords can be any alphanumeric characters, must contain at least 8 characters and begin with a letter.

Upper and lower case character rules: case sensitive

Allowable characters: All numbers and alpha characters- can be upper and lower

Disallowable characters: No special characters

Other limitations: NO spaces between characters

It is suggested you do not make password same as Group Name

## **Setting up a ppnVault account**

### Temporary Secure Storage

Once a Group is created ppnVault automatically establishes a secure storage area for the Group. That secure storage area is maintained for the Group for as long as the Group exists. Upon termination of the Group, the Groups' allocated storage area is securely cleaned and withdrawn.

All of a Group's temporary storage area is limited as to total storage space (size) and data file transfer size. There are also limitations on the time that is available to store the secure data files and messages. For a definition of these limitations see Section 4 – Operating Characteristics.

### Permanent Secure Storage

The operating rules and procedures for access and deposit of data files into the long term secure facilities of the ppnVault are currently being established. Upon completion of these procedures a revision to this Manual will be issued.

### **Basic Password Security Rules**

Your User Password and Group Password are both accesses keys to your secure ppnPRO network and ppnVault depository. It is the access power to your sensitive, confidential and protected information.

As such password are much sought-after by unauthorized parties and cyber-criminals. A weak and ineffective password may give an unauthorized party or cyber-criminal access not only to ppnPRO service, but also to the ppnPRO Groups to which you are a member. Therefore, treat your User Passwords and Group Passwords like they were the key to your safe deposit box and in that box are all of your valuables.

Too many passwords are easily guessed. It's not unusual for many parties to use as their password simple to guess words such as: "password" or "pass" or "secret" or "enter." Other commonly used passwords are the computer user's first, last or child's name, names their favorite sports team and repeated characters such as AAAAAA or bbbbbb.

Your password is the foundation of your ppnPRO security, and it needs to stand up against the tools that hackers utilize to crack passwords. There are 308 million possible letter combinations for a six-letter password using all upper case or all lower case letters. Analysis has shown that a readily available password cracker can check all of them in only 2 minutes 40 seconds.

## Simple Guidelines to Effective Passwords

Each password should contain at least eight (8) characters.

Each password should contain a mix of four different types of characters. The mix should include: upper case letters, lower case letters, numbers, and special characters. Special characters include the top row of your keyboard and others, such as: >?!@#\$\$%^&\*+={}'"<. Do not use a special character for either the first or the last character of your password. Be aware that some limitations exist and various systems may not accept certain or any special characters within a password.

Each password should never be a name, a slang word, or any word in the dictionary.

Each password should never include any part of your name, former name or your current or former e-mail address.

You should be able to type your password quickly, so that someone looking over your shoulder cannot readily see what you have typed.

Each password should be changed at least every 90 days to keep undetected intruders and cyber-criminals from continuing to use it.

### Password Facts

A six-letter password using all upper case letters or all lower case letters has 308 million possible letter combinations. This is easily broken within three (3) minutes by an automated password-cracking program that any cyber-criminal or hacker can easily download from many websites on the Internet.

With some combination of both upper and lower case letters, a six-letter password has 19 billion possible combinations. If you increase the password to eight letters and use both upper and lower case letters, there are 53 trillion possible combinations. Substitute a number for one of the letters, and there are 218 trillion possible combinations. By using at least eight characters, including at least one upper case letter, one lower case letter, one number, and one special character or punctuation there are approximately 6,095 trillion possible combinations.

## Recommended Password Structure

For ppnPRO User Passwords and Group Passwords you are required to begin with a letter use at least eight alphanumeric characters, including at least one upper case letter, one lower case letter, and one number. The recommended password structure can still be cracked, but the process requires a more sophisticated processing algorithm and very long time.

The password used for logging on to your computer should be different from your User password and each Group Password should also be different.

Once you have selected an effective password, protect it. Resist the temptation to write your password down. If you do, keep it with you until you remember it, then shred it! NEVER leave a password taped onto a terminal or written on a pin-up board.

Do not disclose your ppnPRO User Password and Group Password to anyone, not even to your systems administrator or maintenance technician. They have no need to know them. They have their own password with system privileges that will allow them to work on your account without the need for you to reveal your passwords. If a system administrator or maintenance technician asks you for any ppnPRO Passwords do not provide them.

Use a password-locked screensaver to make certain no one can perform any activity under your User ID while you are away from your desk. Password-locked screensavers can be set up such that they activate after a computer has been idle for a while.

It takes a little time to perform the tasks of creating and maintaining effective and secure passwords, but the results are well worth the time spent. The benefits include reducing the risk that a cyber-criminal will use your password access to gain entry to your ppnPRO account and the Group accounts to which you are a member.

## **Operating ppnPRO**

### Group Membership Conditions

#### Single Group Size:

Minimum number of members – one.

The group creator is automatically included any created Group  
Maximum number of members in a Group – open

#### Group Setup Limitations:

Minimum number of Groups a ppnPRO user must create – none

Maximum number of Groups a ppnPRO user can create – open

#### Group Participation Limitations:

Minimum number of Groups subscriber can be listed as a member - none

Maximum number of Groups subscriber can be listed as a member - unlimited

## **ppnPRO Window Set-up**

HOST: always "acapsecurity.com"

PORT: always "7123"

USER: your ppnPRO User Name

GROUP: the Group Name of the Group you desire to connect

PASSWORD: your ppnPRO User Password

## **Function of ppnPRO Operational Buttons**

The CONNECT button connects you to the Group you identified in the information provided in the submittal windows. If you are connected to a Group and the DISCONNECT button is clicked you will be disconnected. If you are not connected to the Group and the connect button is clicked you will be connected. In changing connections from one Group to another the historical text in your ppnPRO chat and system windows remains.

The USER buttons provide a listing of the parties currently on-line and active in the Group and also a listing of all of the members of the Group.

The FILES buttons provide many features. The SEND button allows you to copy one or more data files from your computer, or attached digital

devices, and as data files, security send them to the Group's members. This transfer is accomplished by placing the data files on the secure ppnPRO server (the ppnVault) where they can be picked-up by authorized Group members at a later time.

The RECEIVE button allows you to retrieve (copy) one or more data files from the ppnVault and also to receive secure data files that are sent to you. These retrieved secure data files are placed into your computer's ppnDownload file for your use and transfer to a desired folder location.

The LIST REMOTE button allows you to view the secure data files associated with the Group that are currently stored in the ppnVault. Be advised that after 120 hours of residence every secure data file in the ppnVault is subject to secure deletion by ppnPRO. This secure destruction action is automatic.

The DELETE REMOTE button allows you to delete your Group's secure data files that are currently stored in the ppnVault. Be advised that after 120 hours of residence a secure data file is subject to secure deletion by ppnPRO. This secure destruction action is automatic.

The DELETE LOCAL button allows you to delete data files that are currently stored in your computer.

The MISC button also provides a number of control options. The SAVE CHAT WINDOW button saves the text in the chat window providing the ability to archive chat information and also to prove information items were delivered.

Similarly, the SAVE SYS WINDOW button saves the text in the system window providing the ability to archive system information and also to prove data items were delivered and system events occurred.

Every user has a unique AES encryption key that is electronically created. The CHANGE AES KEY button directs ppnPRO to change the user's 256-bit AES encryption key. Note, ppnPRO automatically and frequently changes every 256-bit AES encryption key- this command bottom allows the user to direct ppnPRO to change it again now.

The CHANGE PASSWORD button directs the ppnPRO to change the User's current password to a new password.

The LEAVE MESSAGE button allows a user to leave, for later pick-up, a secure message for any individual who is an authorized participant of the Group.

The CLIENT VERSION button provides notice of the version of ppnPRO which is currently being utilized. It also provides a special notice when a new version or an upgrade is available. If a new version or an upgrade is available and you select to accept the upgrade this button will automatically install the updated version. All upgrades and new versions are included in the ppnPRO subscription.

The SERVER STATUS button provides general and specific information about the Users, the Group and the operations of ppnPRO. The information is displayed in the ppn System Window.

The LICENSE button provides a viewable copy of the ppnPRO user license agreement.

The ADMIN button also provides a number of operational control options. The use of these controls is limited to the party or parties who have access to the Group Password. Therefore, usually these features are limited to usage by the creator of the Group.

The GROUP INFO button provides a status report on the Group. The data includes the number of time a Group member has been active in the Group and whether the member is currently enabled or disabled.

The DISABLE ACCOUNT button allows for the temporary removal of the identified Group member from the Group. If the identified member is disabled when he attempts to join the Group his access request will be denied.

The ENABLE ACCOUNT button allows the re-instatement of the Group access privileges to a Group member whose access has previously been disabled.

The DELETE ACCOUNT button permanently removes the identified Group member from the Group.

The DELETE GROUP button totally and securely deletes the complete Group and all secure data files which may be resident in the Group's section of the ppnVault.

Note that once you are in a communications session and you have provided ppnPRO with the correct Group password, the ADMIN control functions are available for use without re-entering the Group password each time a function is requested.

The HELP button provides information on the General Features; Characteristics; Operating Procedures; and Trouble Shooting.

The CHAT line provides an input window for leaving text information to the on-line and active members of the group. Typed text is sent to the online members upon the author hitting the enter key.

## **6.0 Trouble Shooting a Problem**

### Incorrect User name or User Password

Some of the errors or troubles which could arise in the usage of ppnPRO are related to the entry of an incorrect User password or User name. If you have forgotten your User Name or User Password visit the ACAP Security web site: [www.acapseceutiy.com](http://www.acapseceutiy.com) and complete the form for a lost or forgotten User Name or User Password and if the correct information is provide your request will be provided the requested item by email.

### Incorrect Group Name

If you have forgotten the Group Name, the creator of the Group or any authored member of the Group may be contacted to provide you with the Group Name.

### Incorrect Group Password

As a creator of a Group you are the creator and holder of the Group Password. If you lose or forget your Group Password your Group will continue to operate but you will be unable to add new members or to use the Group's administrative functions provided with ppnPRO. The recommended solution is for you to remove all data files from the ppnVault and create a new Group with a new Group Name and new Group Password and then enter the desired members to the new Group.

### PpnPRO-operating window will not open

Your copy of the ppnPRO config file or the program file may have become corrupted or your version of JAVA could be ineffective. First, close any ppnPRO window that is open, within your ppnPRO folder find all of the ppn.conf files and transfer each to the Recycle Bin. Upon completion of that event, double click on the ppn\_extern file. If that does not solve the problem then again remove all ppn.conf files to the Recycle Bin; then remove all of the ppn\_extern files to the Recycle Bin. Go to the ACAP Security web site at: [www.acapseceutiy.com](http://www.acapseceutiy.com). On the Home page select the Account button and enter your Account and then select the incremental install and download a new copy of ppnPRO.

If that does not solve the problem then again remove all ppn.conf files to the Recycle Bin; then remove all of the ppn\_extern files to the Recycle Bin. Go to the ACAP Security web site at: [www.acapseceutiy.com](http://www.acapseceutiy.com). On the Home page select the Account button and enter your Account and then select the incremental install and (first) download a new copy of JAVA. Then install the new copy of JAVA (it must be the j2re-1\_4\_2\_05 version). During the install process the program will (or may) ask if you want to modify the existing JAVA on your computer. Answer yes, modify. Following the re-installation of JAVE, go to your Account page, select the incremental install and download a new copy of ppnPRO.

Other problem or error: If a problem or error occurs which you can not resolve email a brief description of the problem and the events associated with the problem to: [technicalsupport@acapsecurity.com](mailto:technicalsupport@acapsecurity.com).