



Technical Service Bulletin

To: NeXGen Service and Help Desk Personnel

From: Allied Electronics Technical Support

Date: March 15, 2012

Re: ANDI_DGS PCI User Name and Password Management

** For the remainder of this document, the NeXGen controller will be referred to as **NXG**.*

PCI requires that a user name and password file be created and maintained in order to be in compliance. The ANDI_DGS application allows one to create and maintain user names and passwords via the *Users* file.

The PCI standard requires the following password complexity for compliance:

- Passwords must be at least 7 characters
- Passwords must include both numeric and alphabetic characters
- Passwords must be changed at least every 90 days
- New passwords can not be the same as the last 4 passwords

PCI user account requirements beyond uniqueness and password complexity are listed below:

- If an incorrect password is provided 6 times, the account should be locked out
- Account lock out duration should be at least 30 min. (or until an administrator resets it)
- Sessions idle for more than 15 minutes should require re-entry of user name and password to reactivate the session.

There are two types of users that may be added to the *Users* file:

- 1) Normal User
- 2) Administrator

Upon initial startup of a PCI-compliant ANDI or NXG system, an "Administrator" user name and password **MUST** be setup in order to employ **ANY** ANDI_DGS functions (i.e. warm start, cold start, port assignment, port monitoring, etc).

Fueling the Future of Service Station Automation

P.O. Box 624 • 2210 Farragut Avenue • Bristol, PA 19007 • 215.785.6200 • FAX 215.785.0230

www.AlliedElectronics.com • Sales@AlliedElectronics.com

The following is the procedure for setting up an "Administrator" user name and password upon initial startup on a NXG system (the same procedure applies to ANDI PCI systems but we'll use NXG verbiage):

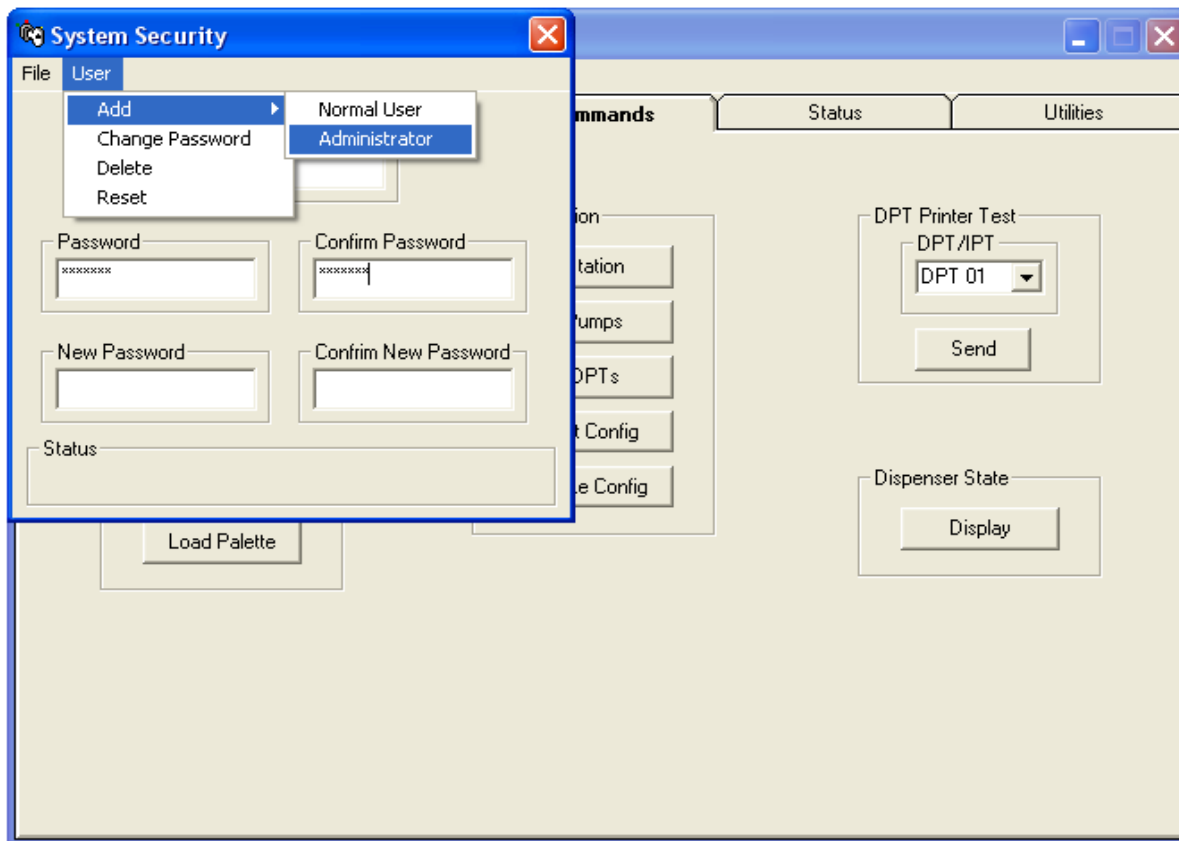
- 1) Launch ANDI_DGS and connect to NXG.
- 2) From the **Commands** tab, click on the "Accounts" button (under Security). A Query box will appear prompting you to sign on as a device providing RFA services. Click "OK."



- 3) A "System Security" box will appear.



- 4) Enter a user name and a password. Remember that the password must be a minimum of 7 characters and alphanumeric. The user name and password are also **CASE SENSITIVE!**



- 5) As seen above, click on the "User" pull-down menu. Click on "Add" and then "Administrator."
You should see "Command Accepted" in the "Status" box.



- 7) A user name and password with "administrator" privileges is now set up.

Contact Allied Electronics Technical Support with any questions or concerns:

800-223-3619

SupportRequest@AlliedElectronics.com