BIG HAIRY DOG
Feature of the Month

Setting up Retail Pro Passwords to be PCI Compliant as of Oct 2010

This is meant to guide you through setting up the employee passwords to be PCI compliant in Retail Pro. It is not a guide to be completely PCI Compliant.

A few important Points from the pci_dss_saq_navigating_dss.pdf

2.1 *Always change vendor-supplied defaults* ***before*** *installing a system on the network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).*
So the default Sysadmin Password must be changed! Do not lose the Sysadmin password. If the Sysadmin password is lost, security will have to be re-setup in V8 to get security updates to retail pro. The V9 Sysadmin password can only be rest through the developer, Retail Pro (during regular business hours).

8.5.1 *Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.*
So, only a select few should be allowed to add new users to Retail Pro or change rights to user accounts

8.5.3 *Set first-time passwords to a unique value for each user and change immediately after the first use.*
This prevents employees (or former employees) from hacking in and gaining access to information

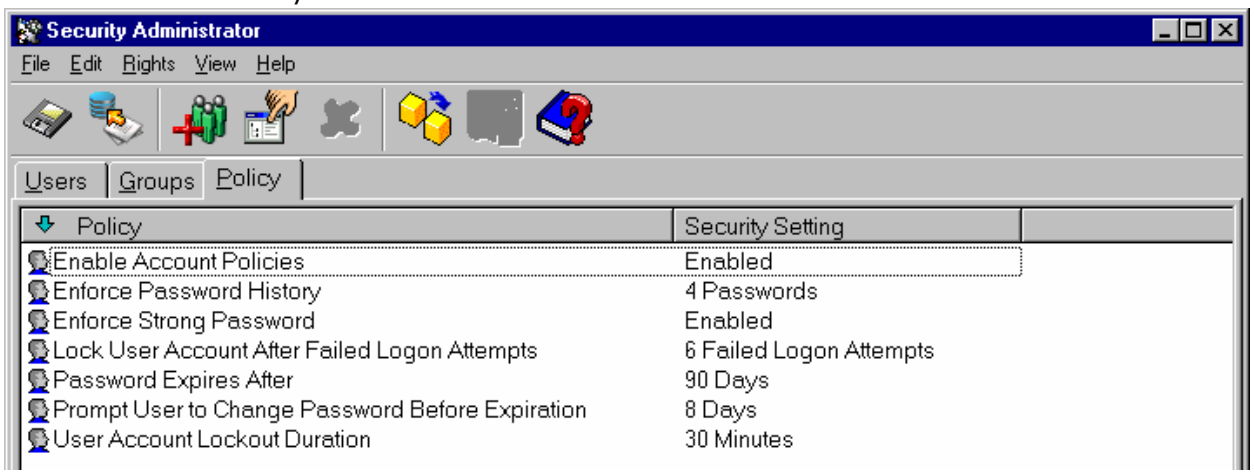
8.5.4 *Immediately revoke access for any terminated users.*
This is always a wise choice. Anyone who is terminated should be removed from the system.

8.5.7 *Communicate password procedures and policies to all users who have access to cardholder data.*
Communicating password procedures to all users helps those users understand and abide by the policies, and to be alert for any malicious users who may attempt to exploit their passwords to gain access to cardholder data (for example, by calling an employee and asking for their password so the caller can “troubleshoot a problem”).

8.5.8 *Do not use group, shared, or generic accounts and passwords.*
If multiple users share the same account and password, it becomes impossible to assign accountability for, or to have effective logging of, an individual’s actions, since a given action could have been performed by anyone in the group that shares the account and password.

Setting up Security

In Retail Pro Version 8 select Tools > Sec Admin > Policies:
Note: If Policies is not a tab on the screen, then update your retail Pro to the latest version.
Double click each Polcy to set the value. The screen below is set to the Minimum standard.



A screen shot from "pci_dss_saq_navigating_dss.pdf":

Requirement		Guidance
8.5.8	Do not use group, shared, or generic accounts and passwords.	If multiple users share the same account and password, it becomes impossible to assign accountability for, or to have effective logging of, an individual's actions, since a given action could have been performed by anyone in the group that shares the account and password.
8.5.9	Change user passwords at least every 90 days.	Strong passwords are the first line of defense into a network since a malicious individual will often first try to find accounts with weak or non-existent passwords. There is more time for a malicious individual to find these weak accounts, and compromise a network under the guise of a valid user ID, if passwords are short, simple to guess, or valid for a long time without a change. Strong passwords can be enforced and maintained per these requirements by enabling the password and account security features that come with your operating system (for example, Windows), networks, databases and other platforms.
8.5.10	Require a minimum password length of at least seven characters.	
8.5.11	Use passwords containing both numeric and alphabetic characters.	
8.5.12	Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	
8.5.13	Limit repeated access attempts by locking out the user ID after not more than six attempts.	Without account-lockout mechanisms in place, an attacker can continually attempt to guess a password through manual or automated tools (for example, password cracking), until they achieve success and gain access to a user's account.
8.5.14	Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.	If an account is locked out due to someone continually trying to guess a password, controls to delay reactivation of these locked accounts stops the malicious individual from continually guessing the password (they will have to stop for a minimum of 30 minutes until the account is reactivated). Additionally, if reactivation must be requested, the admin or help desk can validate that the account owner is the cause (from typing errors) of the lockout.
8.5.15	If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.	When users walk away from an open machine with access to critical network or cardholder data, that machine may be used by others in the user's absence, resulting in unauthorized account access and/or account misuse.