Teleflora Point of Sales

Dove POS 5

PA-DSS Implementation Guide

Version: 1.3
Version Date: July 7, 2011

REVISIONS

Document Version	Date	Description
1.3	July 7, 2011	Reviewed for PA-DSS 2011, Elavon and GoToAssist changes
1.2	June 23, 2009	Renamed DovePOS version to 5
1.0	June 2009	Initial document creation

Table of Contents

Purpose of this Document

If you are a merchant who accepts credit card payments for Visa and other major banks, you are responsible for ensuring that your business is in compliance with PCI DSS regulations. These requirements have not been created by Teleflora, but instead, they were authored by the majority of major credit card banks.

This document is intended to supplement PCI Payment Applications Data Security Standards guidelines, as well as the PCI Data Security Standard. In short, this document is intended to give "POS Specific" interpretation to some guidelines which otherwise, would seem ambiguous. The intended audience of this document is the owner and administrator of a Dove POS software environment.

Scope and Definitions

In order to reduce retail credit card fraud, Visa and other credit card companies have introduced a new program called "PA-DSS", Payment Application – Data Security Standards. This new program specifies a number of policies and guidelines needed to maintain a "secure" Point of Sale environment. Teleflora has made a number of application and procedural changes in order to ensure that your Dove POS system is compliant with these new PA-DSS requirements. However, to remain compliant, you will be responsible for maintaining some procedures as well.

This document serves to provide a number of "Dove POS Specific" applications to the various Visa PA-DSS requirements. Please refer to Visa's "Payment Applications Best Practices" document, as well as the associated "Payment Card Industry Data Security Standard" document for full details on compliance regulations.

Following are definitions for some terms used throughout this document.

Term	Definition
PA-DSS	Payment Applications Data Security Standards
Cardholder Information	Minimally, a full credit card number. Could also be a credit card magnetic stripe data, CVV value and/or Debit card "pin" value or Debit card "pin block".
Sensitive Data	Either Cardholder information or username/password information.
Administrative user	Any person capable of logging into a Dove POS workstation, or Dove POS server with "Administrative' windows privileges. Or, any person who has administrative privileges to the Dove POS database.
"Data Security Standard"	A document, published by Visa, which specifies all polices and requirements fundamental to PA-DSS compliance.

For more information about PCI's PA-DSS requirements and process, please visit:

http://www.pcisecuritystandards.org

In particular, you should obtain and read the following documents:
PCI DSS Version 1.1 Requirements
(https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm)
Payment Application Data Security Standard (PA-DSS)
(https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml)
PCI DSS Self-Assessment Questionnaire
(https://www.pcisecuritystandards.org/pdfs/pci_saq_v1-0.pdf)

Do note that at the time of this writing, we are using the PCI - Payment Application Data Security Standard - Security Audit Procedures, version 1.1 (April 2008) and PCI DSS Revision 1.1 documents.

Dissemination of This Document

Addresses:
PA-DSS 14.1

A copy of this document should be freely available to all persons who use or administer your Dove POS system. This includes not only Teleflora staff (Customer Service, software developers, trainers) , but all staff in your shop who use, or are responsible for administering, or otherwise maintaining Dove POS computers and their associated networks.

This document is date stamped. If you received this document over one year ago, it is highly likely that updates have been made. Please contact Customer service to ensure that you have the latest version of this document.

Dove POS Customer Service Contact Information:

Phone: 866-444-3683

Postal Mail:
Dove POS Support
3737 NW 34th St.
Oklahoma City, OK. 73112

Default System Configurations

The computers that you have purchased for use with your Teleflora POS system have been designed, configured and approved to meet the PCI -DSS guidelines. There are certain areas that should never be changed on the system to ensure compliance with the PCI (Payment Card Industry) guidelines and for general security of your system. Areas that should never be changed or modified without assistance from Teleflora are.

1. System Restore Points.
2. Logging
3. Database Access
4. Encryption Utilities
5. Firewall or Virus Settings

Areas or tasks that can be added or changed without contacting Teleflora include

1. Creating new users
2. User access controls

Legacy Data Removal

Addresses:
PA-DSS 1.4.a
PA-DSS 1.5.c
PCI DSS 3.2
PCI DSS 3.5.1
PCI DSS 3.5.2
PCI DSS 3.6
PCI DSS 3.6.1
PCI DSS 3.6.4

Upgrading Software
When upgrading from a legacy POS, to Dove POS, it is important to realize that your legacy POS may still contain sensitive information (credit cards, pin blocks, magnetic stripe data, encryption keys, etc.) stored in an unsafe manner. To be PCI compliant, you must ensure that any sensitive data from your previous POS be securely removed. This is best achieved by using a secure "wipe" tool.

In the event that your upgrade involved new hardware, understand that your older hardware may contain sensitive information stored in a non-compliant manner, and you are responsible for removing such.

NOTE: Please consult with your legacy POS provider for guidance on removing sensitive data.

Encryption Key Management

Addresses:
PA-DSS 2.5
PA-DSS 2.6
PA-DSS 2.7
PCI DSS 3.5

Your Dove POS system encrypts the cardholder information being retained on disk. An "encryption key", comprising of special files is ultimately used to protect the data. In order to retain a level of security, you must follow some key management procedures as per PCI DSS 3.

Directives you must follow are summarized as follows:

- Restrict access to the decryption key material (Dove POS files) to the fewest number of people possible. (PCI 3.5.1)
- Store the cryptographic files in the fewest possible locations and formats. Do not make multiple "copies" of your Dove POS files in unprotected or insecure storage locations. (PCI 3.5.2)
- Store the cryptographic files in a secure location and form. (PCI 3.6.3)
- In the event of software or system changes, ensure that older encryption keys are securely deleted (See appendix on using secure delete utility). (PCI 3.6.5, PCI 3.6.8)
- Change the encryption key (DeK), at least annually. See appendix on How to Change your Dove POS Data Encryption Key (PCI 3.6.4)
- Do not retain old cryptographic files; destroy them once you are done with them. (PCI 3.6.5)
- Prevent the possibility of unauthorized substitution of cryptographic material. For example, do not tamper with the file permissions structure of your Dove POS system (PCI 3.6.7)
- If you know, or even suspect, that your data encryption key(s) have been taken, stolen, or otherwise compromised, you should take action to rotate the encryption keys immediately (See appendix on How to Change your Dove POS Data Encryption Key)(PCI 3.6.8)

Collecting Sensitive Data for Debugging

Addresses:
PA-DSS 1.1.6
PA-DSS 4.2.b
PCI DSS 3.2

In rare cases, Teleflora customer service may need to work with you to troubleshoot a credit card issue specific to your shop. In such a case, customer service is required to collect only a limited amount of cardholder information, and store this data in a secure location. Furthermore, any sensitive data must be stored in an encrypted format, and must be securely removed once no longer needed.

Log Debug Settings:

Though Dove POS will never intentionally log non-PCI compliant data (even in full debug mode), it is still important that you are aware that your Dove POS system can log details of some actions and transactions. Furthermore, many of these logs have a "full debug" mode which stores more verbose data. Please see the appendix on "How to Disable Debug Logging" for instructions on enabling and disabling these logs debug settings.

Cardholder Data Retention

Addresses:
PA-DSS 2.1.a
PA-DSS 2.7.b
PA-DSS 3.1

Dove POS retains the following Cardholder data in its database: Encrypted Credit Card number, Encrypted Expiration Date, and Hashed Number.

Teleflora has provided a tool to Purge cardholder data from the Dove POS database, please see the appendix "How to Purge Cardholder Data" for details on this tool.

According to PCI DSS requirement 3.1, merchants need to create a data retention business policy. Teleflora provides a template to help merchants develop this policy in the POS Template Policies document. Teleflora has also provided a tool to purge cardholder data from the Dove POS database. Using the Tools>Support Tools>Purge Cardholder Data menu in DovePOS will purge cardholder data from your system based on your data retention limit. Please see the appendix "How to Purge Cardholder Data" for more details on this tool. Cardholder data exceeding your defined retention period needs to be purged to be compliant with PCI DSS.

The Purge Cardholder Data tool creates a backup copy of your database prior to executing the cardholder data purge. Teleflora recommends that, after you have verified the purging of the cardholder data is complete, you use the Eraser tool to securely delete this backup copy of your database. See appendix "Using the Eraser Tool".

User Identification and Authentication

Addresses:
PA-DSS 3.1.c
PA-DSS 3.2
PCI DSS 6.5.8
PCI DSS 8.1
PCI DSS 8.2
PCI DSS 8.3
PCI DSS 8.4
PCI DSS 8.5

A key component to securing your Dove POS environment is ensuring that users are properly authenticated for the task to be performed. The Dove POS application does not require users to have administrative privileges in order to run. Note that, for the purpose of Dove POS, any user who is a member of the "Administrators" windows group is considered an "Administrative user". In order to prevent impersonation and unauthorized access to your Dove POS system, the following guidelines should be followed. This is not an exhaustive list. You are responsible for reading, and following all guidelines under PCI DSS 8.5:

- PCI DSS 8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects
- PCI DSS 8.5.2 Verify user identity before performing password resets
- PCI DSS 8.5.3 Set first-time passwords to a unique value for each user and change immediately after the first use
- PCI DSS 8.5.4 Immediately revoke access for any terminated users
- PCI DSS 8.5.5 Remove inactive user accounts at least every 90 days
- PCI DSS 8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed
- PCI DSS 8.5.7 Communicate password procedures and policies to all users who have access to cardholder data
- PCI DSS 8.5.8 Do not use group, shared, or generic accounts and passwords
- PCI DSS 8.5.9 Change user passwords at least every 90 days
- PCI DSS 8.5.10 Require a minimum password length of at least seven characters
- PCI DSS 8.5.11 Use passwords containing both numeric and alphabetic characters
- PCI DSS 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
- PCI DSS 8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts
- PCI DSS 8.5.14 Set the lockout duration to thirty minutes or until administrator enables the user ID
- PCI DSS 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
- PCI DSS 8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users

Administrative Users
Teleflora does not recommend you login to your Dove POS workstations as an Administrative user, unless you have a specific administrative task which needs to be accomplished. As a normal matter of practice, you and your employees should use the Dove POS workstations as a non-administrative user. In order to be PCI compliant, you must ensure that all Administrative accounts be assigned a complex password

Administrator Account:
Every windows computer on your Dove POS network will have an administrative user account with the user name "Administrator". For each of these computers which Teleflora Customer support manages, Teleflora retains and maintains the password for this account. Furthermore, Teleflora may use this account for remotely managing your system.

Non-administrative Usernames:
Teleflora strongly advises that, for all non-administrative access, a username and a strong password be used for each end user. Teleflora recommends you rotate passwords every forty-five days. Please see the appendix for specific instructions on adding and removing non-administrative users from your Dove POS systems.

Password Complexity:
PCI DSS specifies a number of requirements defining a "strong" password. These may be found in PCI DSS section 8.5. Teleflora has provided a password generation tool which you can use to create PCI compliant passwords, please see the appendix "How to create a PCI compliant password" for details on this tool. You are advised to assign a strong password to any account created on your Dove POS system(s), even if the account is not used often.

Default system logging should never be disabled, if you believe that system level access has changed please contact the support desk to have them verify the logging is correct.

NOTE: Making any changes to the "Out of the Box" installation settings for unique usernames and secure authentication may result in non compliance with PCI DSS.

Wireless Networks

Addresses:
PA-DSS 6.1.b
PCI DSS v1.1 Section 1.3.9
PCI DSS v1.1 Section 2.1.1
PCI DSS v1.1 Section 4.1.1

Teleflora does not recommend, sell, nor support, the use of wireless networks within the Dove POS environment.

Protection from External Access

Addresses:
PA-DSS 9.1.b
PA-DSS 10.1
PCI DSS 1.3
PCI DSS 1.3.4
PCI DSS 1.3.10
PCI DSS 1.3.9
PCI DSS 12.3.9

Protecting the Dove POS Server:
PA-DSS 9.1.b
The Dove POS "Server" computer contains cardholder data stored to disk. Because of such, it is critically important to never have this computer directly accessible from the internet. It is therefore, required that you employ a "firewall" device between the Dove POS server and the internet which restricts connections established from the internet, to your Dove POS server.

Protecting Dove POS Workstations
PA-DSS 10.1
The Dove POS Workstation software does not store cardholder information to disk. However, because these computers do receive payment information (both in the form of "keyed" transactions, as well as magnetic stripe data), it is important that these computers be protected from unauthorized administrative access. In particular, the use of a hardware firewall, and, in the case of multiple locations, use of a PCI compliant "VPN" to network these workstations to the server, is required.

Protecting other Computers on your Dove POS Network
PA-DSS 9.1.a
PA-DSS 9.1.b
It is important to understand that adding computers on the same network as your Dove POS server, may compromise your system's security, and your PCI compliance. If you are considering adding any additional machines to your Dove POS network, you must ensure that the new computer(s) do not expose any network services to the public internet (for example, game related servers).

Firewall Configurations:
For more information on PCI compliant firewall settings, please see PCI section 1.3. The appendix of this document also details how to securely configure a wired network router.
How to Securely Configure a Wired Network Router

Protecting Mobile Computers (Laptops):
PA-DSS 10.1
Teleflora does not recommend nor support the use of mobile computing devices (most notably, laptops) connecting to your Dove POS network.

Using a Remote Dove POS System

Addresses:
PA-DSS 11.2
PCI DSS 8.3

In the event that you wish to use your Dove POS system across the internet, PCI requires that some form of “two factor authentication” be used to authentication your internet connections. The most common form of two factor authentication is to use a “token based” VPN which also employs a password. Note that “factors” include:

- Something you "Know"
  For example, a username and password.

- Something you "Are"
  For example, fingerprints scanners, retinal scanners, or other forms of “biometrics”.

- Something you "Have"
  For example, a “smart card”, and encryption “token”.

It is important to clarify that two factor authentication requires two of the above three genres of authentication. Thus, for example, needing to pass through two separate (and different) username/passwords does not count as “two factor”, as, only one “factor” is being used (something you know).

Teleflora only supports Goto My PC Corporate for remotely accessing your Dove POS System.

Remote Administration of a Dove POS System

Addresses:
PA-DSS 11.3.b
PA-DSS 13.1
PCI DSS 8.1
PCI DSS 8.2
PCI DSS 8.3
PCI DSS 8.4
PCI DSS 8.5

Teleflora "GoToAssist" Remote Assistance:
In the event that you need remote assistance, Teleflora Customer Service will use the "GoToAssist" system to access your computer. You will find instructions for using "GoToAssist" in the appendix of this document. Be aware of the following requirements and points of note for GoToAssist:

- Teleflora's GoToAssist system will always be accessed using the URL: http://www.myteleflora.com/gotoassist.aspx. Never use a different or unknown URL in order to access the GoToAssist home page.
- Teleflora will never solicit remote access requests via email.
- Your GoToAssist sessions will be encrypted using a 128 bit SSL connection. Never attempt to disable, or otherwise override this encryption.
- Do not use the GoToAssist system if your browser indicates the GoToAssist SSL certificate is not trustworthy.
- Never leave an GoToAssist session "open" for Customer service to login at an arbitrary time. Limit the duration on which your machine may be accessed.
- Be aware that Teleflora will be recording what happens during GoToAssist sessions.
- Teleflora Customer Service cannot access your computer until you explicitly allow such access through the GoToAssist system.
- The Teleflora customer service representative only has the security privileges of the user you are currently logged in as. Thus, if you are logged-in as a non-administrative user, customer service will not have administrative privileges.

For more information on GoToAssist, and how it works, please visit:
https://www.gotoassist.com/en_US/corpHIW.tmpl

Other Remote Administration:
In the event that you choose to allow a third party to remotely administrate your Dove POS server and/or network, be aware that, to remain PCI compliant, these third parties must use PCI compliant practices. Encryption technology, such as SSL, SSH, TLS or VPNs must be employed for any remote administration tasks.

Console access: Non Console access using technologies such as RDP cannot be used on the local network unless the connections are encrypted. Telnet is never allowed.

See PA-DSS 11.3 and PA-DSS 13.1 for more information regarding remote administrant requirements.

Customer Remote Access

11.3 Remote access – Teleflora does not recommend the use of any type of remote access into the shop except the usage of GoToAssist. If a shop installs remote access then the florist must use a technology that meets PCI-DSS sections relating to connectivity including :

PCI-DSS V1.1
8.3 Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.
8.4 Encrypt all passwords during transmission and storage on all system components.
8.5 Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:
8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects
8.5.2 Verify user identity before performing password resets
8.5.3 Set first-time passwords to a unique value for each user and change immediately after the first use
8.5.4 Immediately revoke access for any terminated users
8.5.5 Remove inactive user accounts at least every 90 days
8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed
8.5.7 Communicate password procedures and policies to all users who have access to cardholder data
8.5.8 Do not use group, shared, or generic accounts and passwords
8.5.9 Change user passwords at least every 90 days
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
8.5.14 Set the lockout duration to thirty minutes or until administrator enables the user ID
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
8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.

Encrypting over Public Networks

Addresses:
PA-DSS 12.1.b
PCI DSS 4.1

"Public Networks" Defined:
Note that, you should consider the following networks as being "public":

- The Internet
- Any Wireless (Wi-Fi) network.
- Cellular telephone networks, such as "GSM" or "GPRS".
- In the event that you are using a network whose security you are unsure of, you should assume that network to be "public".

Dove POS Transactions with Public Networks:
In order to perform functions such as authorizations, settlement, and Dove, your Dove POS system does transmit cardholder information across the public internet. To protect this transmission, Dove POS uses the "https" (HTTP over SSL) protocol. To protect cardholder information, it is important that you not intentionally take measures to disable, or otherwise hinder, encryption in the Dove POS software.

Multi-Site Connectivity:
Some florists may have multiple, physical locations which all communicate to a single, Dove POS server. In such a case, it is critically important that hardware firewall devices be used at each site, and all network traffic between sites, be transmitted through a secure mechanism, such as an IPSEC VPN, or SSL sockets.

3rd Party Software:
In the event that you use any 3rd party software which sends or receives cardholder information, to remain PCI compliant, you are responsible for ensuring that your third party software properly encrypts its cardholder traffic, again, by use of technologies such as SSL sockets or a VPN.

End-User Messaging Technologies

Addresses:
PA-DSS 12.2.b
PCI DSS 4.2

Your Dove POS system does not send cardholder information via any type of End User Messaging. End User Messaging may include but is not limited to email, instant messaging and text messaging. Teleflora does not recommend ever sending cardholder information over the public internet via End User Messaging. In the event that you choose to use any of these messaging types to transact credit card information, PCI 4.2 requires that you encrypt the sensitive data with some form of strong encryption.

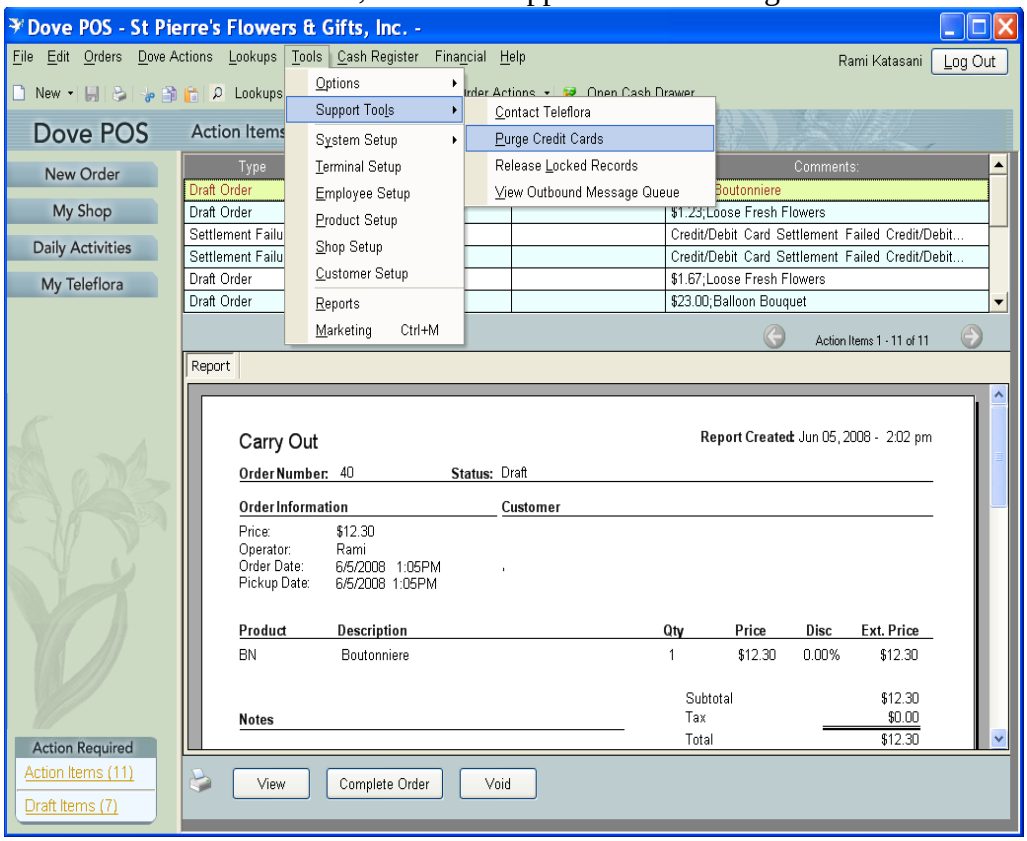
Appendix

How to Purge Cardholder Data

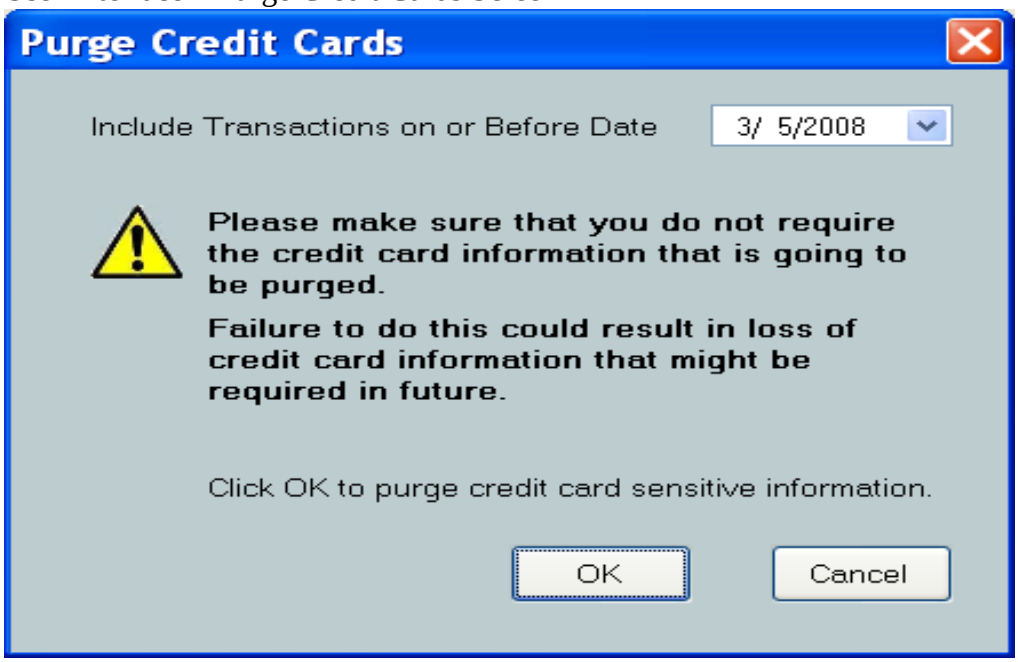
PA-DSS 2.1.a

The process of implementation for purging credit cards sensitive information includes the following.
A Menu Item, Tools -> Support Tools -> Purge Credit Cards, is created to access the screen. Refer to the screen shot below.
Employees with Manager/Owner rights (role) only have access to the Menu Item, Tools -> Support Tools -> Purge Credit Cards.
A form is developed to allow the user to specify the criteria date; all credit card sensitive information older than this date will be purged. Refer to the screen shot below.
The form also includes label that warns the user about losing the data permanently, if he proceeds with purging process. Refer to the screen shot below.
If user selects a criteria date which is less than 90 days in the past, a warning message is shown saying that the minimum criteria date should be at least 90 days in the past. Refer to the screen shot below.
Once user clicks OK button, a warning message is displayed to make sure that the user wants to proceed with the purging process. Refer to the screen shot below.
Once the user proceeds with the purging data, all the eligible credit cards sensitive information which is older than the specified date is purged.
An activity history item mentioning the purge process success is added to the system. Refer to the screen shot below.

User Interface – Menu Item, Tools -> Support Tools -> Purge Credit Cards



User Interface – Purge Credit Cards Screen



Dove POS Connectivity Specifications

PA-DSS Executive Summary - Network Diagram

This information is made available for you to confirm incoming connections. Or, in the event that you are providing your own network security configurations, to apply appropriate firewall and modem blocking rules.

The Dove POS firewall device may use the following, modem dial-out capabilities:
PPP Connection to Teleflora dial-backup network.

All remote administration of the Dove POS application will occur via the "Administrator" user.

Your firewall device should be configured to deny all "inbound" internet traffic.

The Dove POS application uses a service located on the server to handle workstation communications using WSE 2.0. The server listens on the following inbound "IP ports" for "Local Area Network" (LAN) traffic.
Ports:
TCP Port 5050 (Server Service)
TCP Port 8514 (CMC)
TCP Port 1433 (SQL Server)
TCP Port 1434 (SQL Browser Service)

The Dove POS application server requires outbound internet connections to the following destination IP Ports:
TCP Port 80 (HTTP)
TCP Port 443 (SSL / HTTPS)

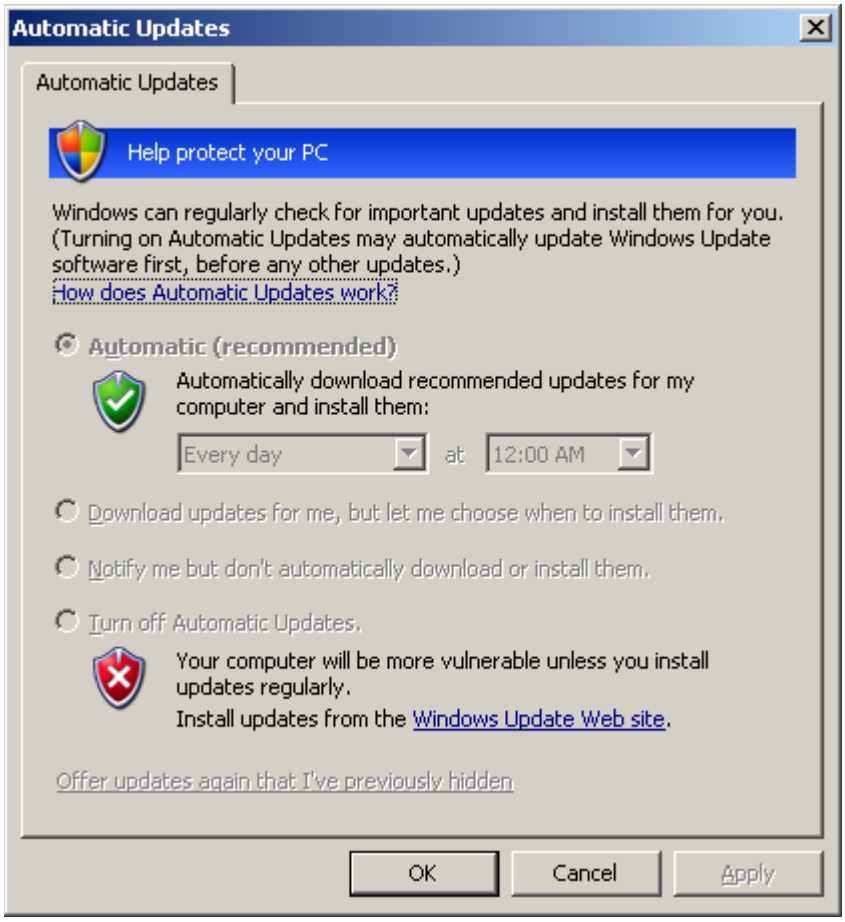
How to update your Dove POS Server's Operating System

PA-DSS 10.1
PCI 6.1

Your Dove POS server must be up-to-date with security bulletins. Following are instructions for performing a manual OS update.

Windows XP
Log in as Administrator.

Start | Settings | Control Panel | Automatic Updates



Select “Automatic”
Update “Every day”, and choose a time during which you know the computer will usually be turned on (e.g. 2:00 pm)
Click “OK”.

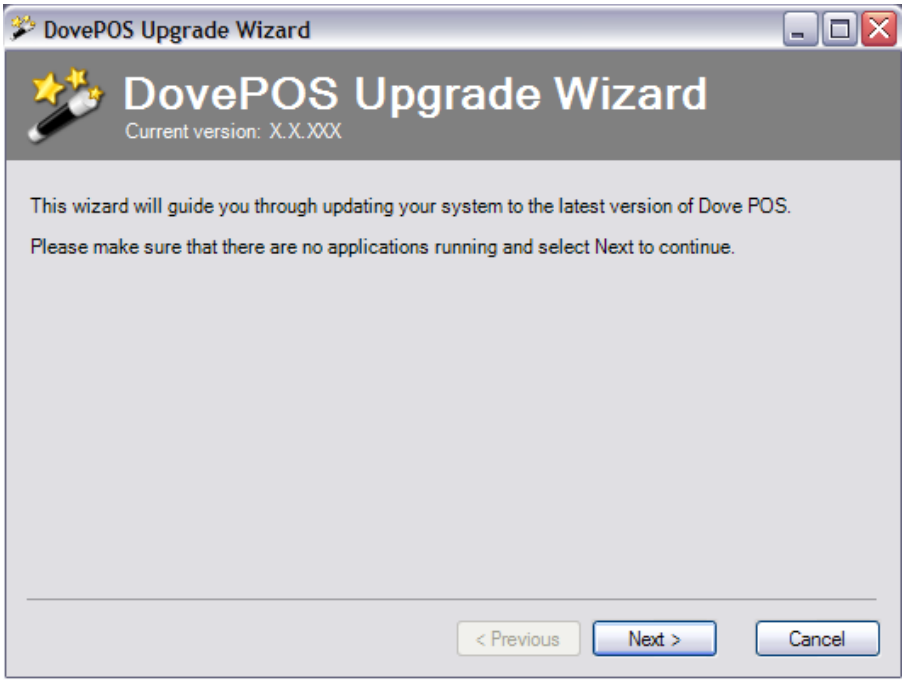
How to Update your Dove POS Software (Install Media)

PA-DSS 10.1

Complete this upgrade on the Server before upgrading the workstations. Make sure all the workstations are shut down while upgrading the Server.

NOTE: Make sure there are no other programs running while completing the upgrade. Make sure that this procedure is completed using Administrator access to the computer.
You should be able to simply insert the disk and start the upgrade. But the patch installation will require you to stop the services so please read the Patch Instructions carefully.

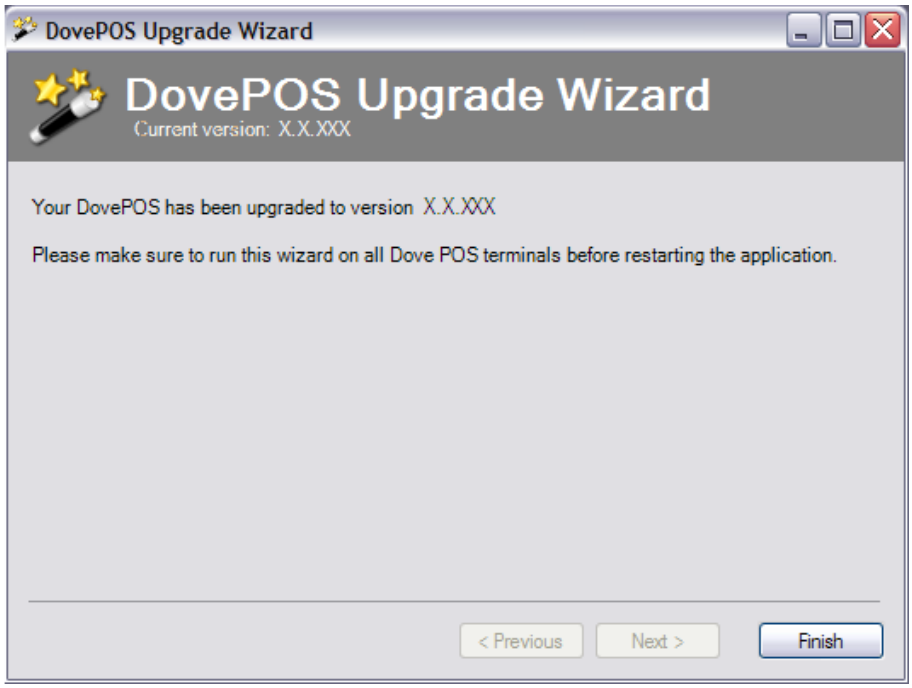
Insert the Dove POS Install/Upgrade DVD into the CD/DVD-ROM drive of the computer you are upgrading. If the disk does not auto run, right-click the My Computer icon on the desktop, select Explore and double-click the CD/DVD-ROM icon. The DovePOS Upgrade Wizard will automatically start.



NOTE: In the above (and following) graphic, "X.X.XXX" represents the build number for the current installed version.

Press Next to continue. Next you will see the license agreement.

Select the "I agree to the terms above" option and press Next. Progress screens will appear while the upgrade is being completed. NOTE: Do NOT attempt to stop this process.



NOTE: In the above graphic, "X.X.XXX" represents the build number for this upgrade.

Press Finish to complete the upgrade.
NOTE: This upgrade must be completed on all terminals before the application is restarted.

How to Enable the Customer Service Access using GoToAssist

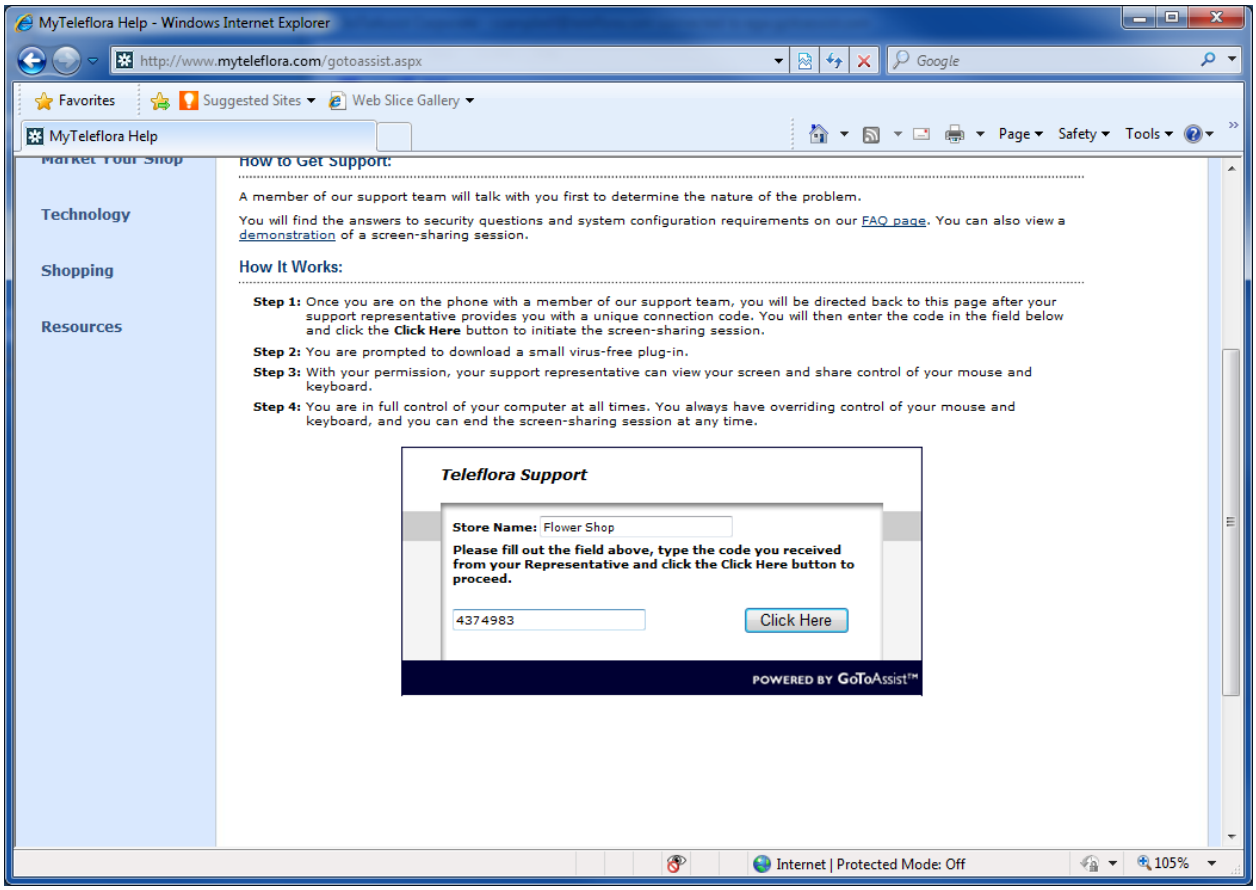
PA-DSS 10.1
PA-DSS 11.3.b

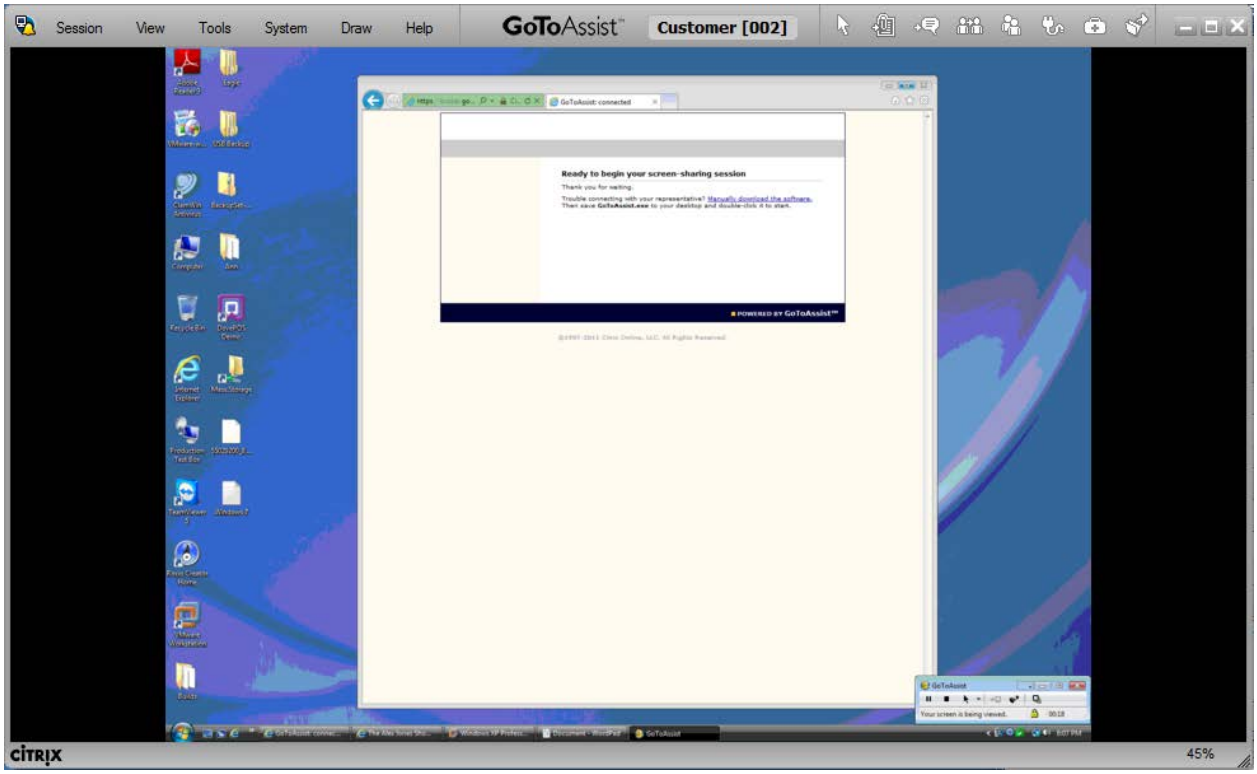
Dove POS Customer Support is only able to assist you if you enable access via the "GoToAssist" system. By default, GoToAssist access is not available to support representatives. Following are detailed instructions for allowing Teleflora Customer Support to assist you via the GoToAssist system.

Below are instructions for using GoToAssist.

Open your browser, and go to http://www.myteleflora.com/gotoassist.aspx

Enter their Store Name and the Code you receive from the support technican and click Click Here.





To close the remote control session, simply close the GoToAssist window and click Yes to confirm exit.

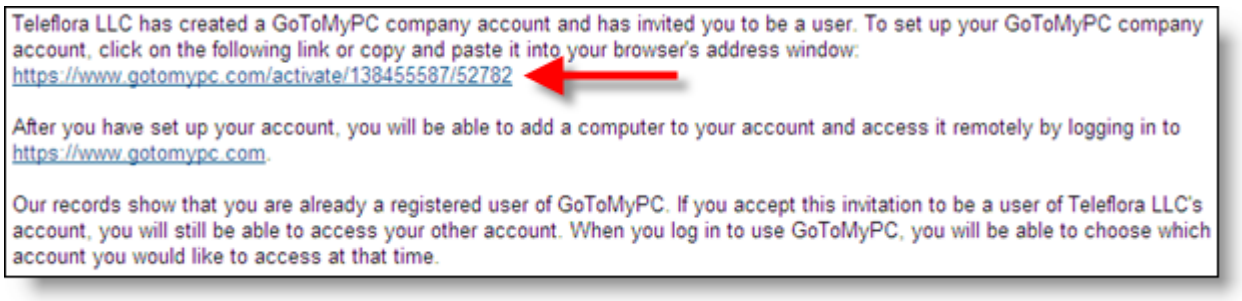
How to Setup Teleflora's "Goto My PC Corporate" On Your Dove POS System

When Managed Services is notified that you have purchased remote access, a Managed Services technician will perform initial customer setup in the GoToMyPC portal. An email will then be sent to the your email address.

Follow the steps below to configure the Host machine for remote access.

Setting up the Host

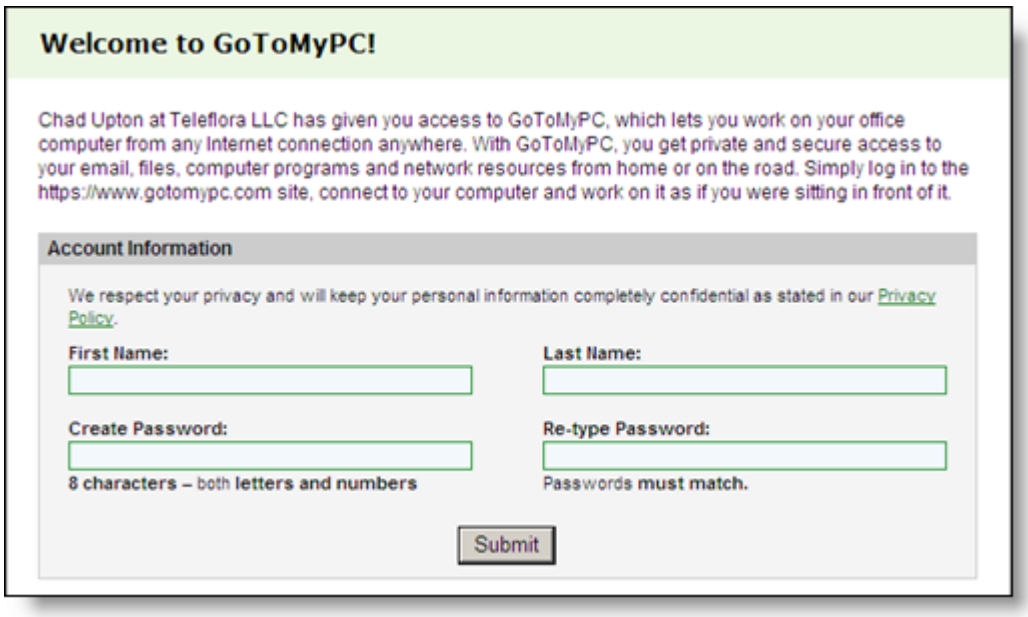
1. The customer will need to access their email account ***from the PC they wish to control*** and look for the email sent from GoToMyPC.
2. Login to PC as "Owner" account.
3. Inside, it will have the activation link they will need to click.


Teleflora LLC has created a GoToMyPC company account and has invited you to be a user. To set up your GoToMyPC company account, click on the following link or copy and paste it into your browser's address window:
https://www.gotomypc.com/activate/138455587/52782

After you have set up your account, you will be able to add a computer to your account and access it remotely by logging in to https://www.gotomypc.com.

Our records show that you are already a registered user of GoToMyPC. If you accept this invitation to be a user of Teleflora LLC's account, you will still be able to access your other account. When you log in to use GoToMyPC, you will be able to choose which account you would like to access at that time.

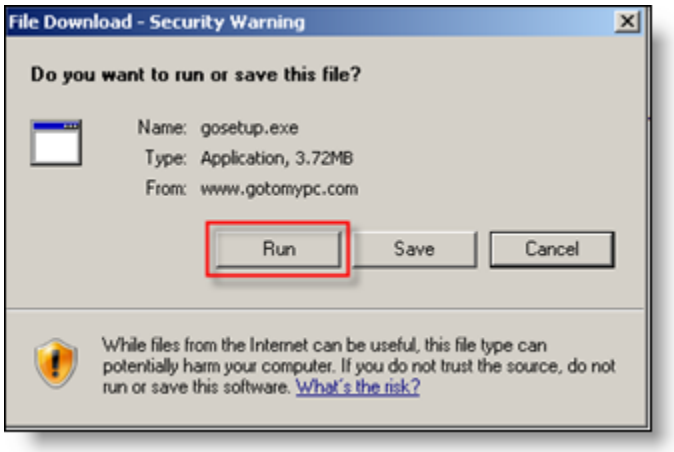
4. The customer will need to fill out the information and set their password.
    a. Note: Password MUST be 8 characters or more and contain both letters and numbers.



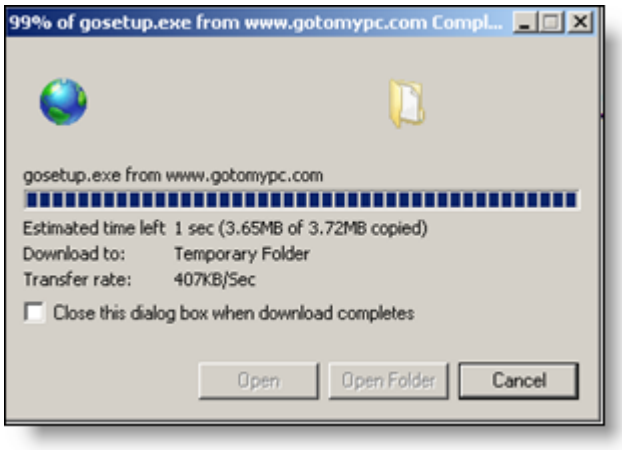
5. Install the GoToMyPC client.

6. Click Download

7. Click Run on the download dialog box.



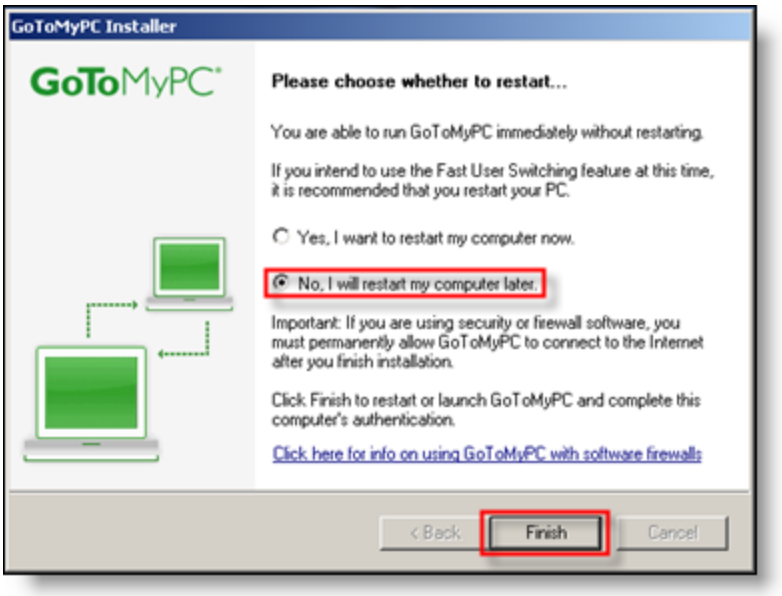
8. Wait for the progress bar to finish.



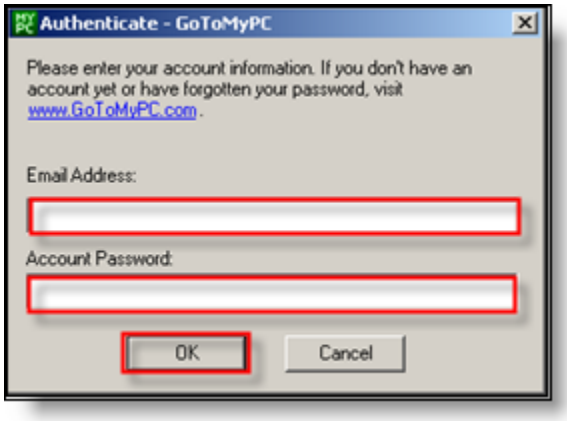
9. Click Run on the Installation box.

10. Click Next on the GoToMyPC Installer.

11. Choose No or leave as default when asked to choose to restart.
    a. Click Finish.



12. Authenticate on the machine to be “remote controlled”.
    a. Enter the email address the account was setup with.
    b. Enter the password the customer setup previously.



13. Computer setup
    a. Enter a Nickname for the computer. This should describe "where or what" this computer is so it can be easily identifiable in the future.
    b. Enter an Access Code. This code should be different from the password setup previously and only known to the customer. Teleflora will not ever ask you for this password.
    c. Click OK.

14. Click Next.
15. A dialog box with 2 pieces of information will open. This information needs to be given to the MSG team to complete setup.
    a. MAC Address: Ex: 00-0C-29-EE-7C-C9
    b. C: Drive Serial Number: Ex: ECBA-9670

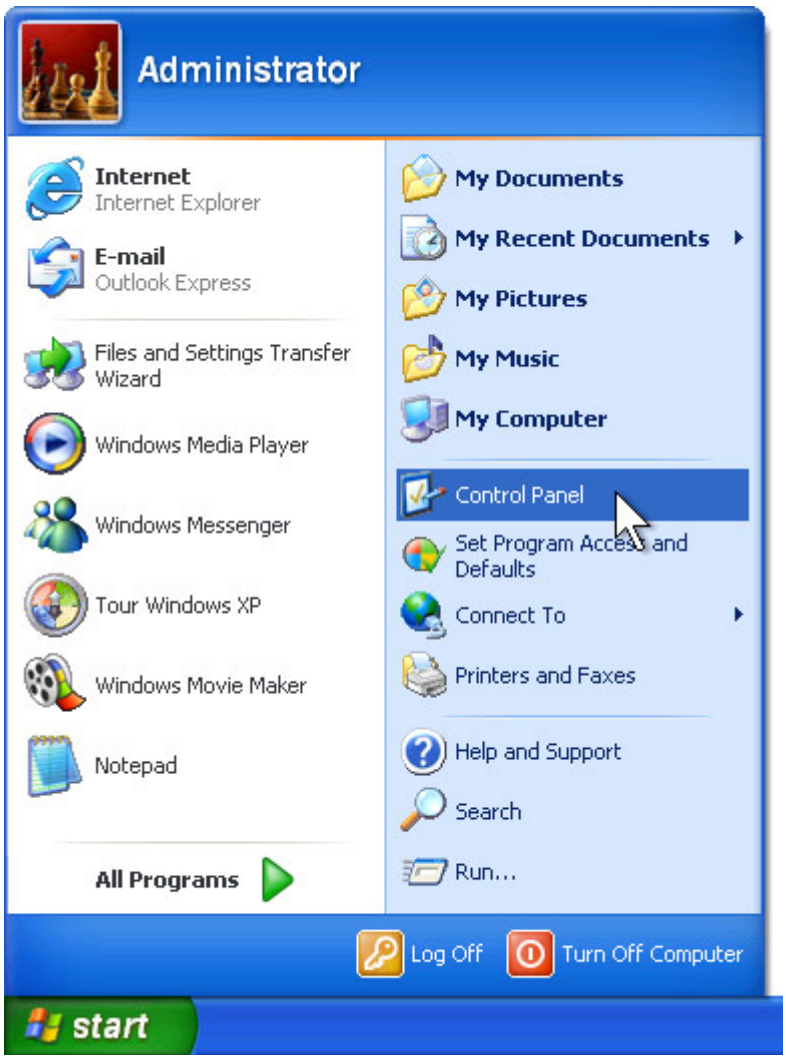
16. Send an email with the following information to Managed Services at msg@teleflora.com:
    a. Shop code
    b. Customers email address
    c. MAC address and C: drive serial number from step 15.

17. Once the requested information has been received by the MSG team, we will activate the host machine. An email will then be sent to the customer's email address with instructions on how to setup the client machine that they wish to use for accessing the host machine.

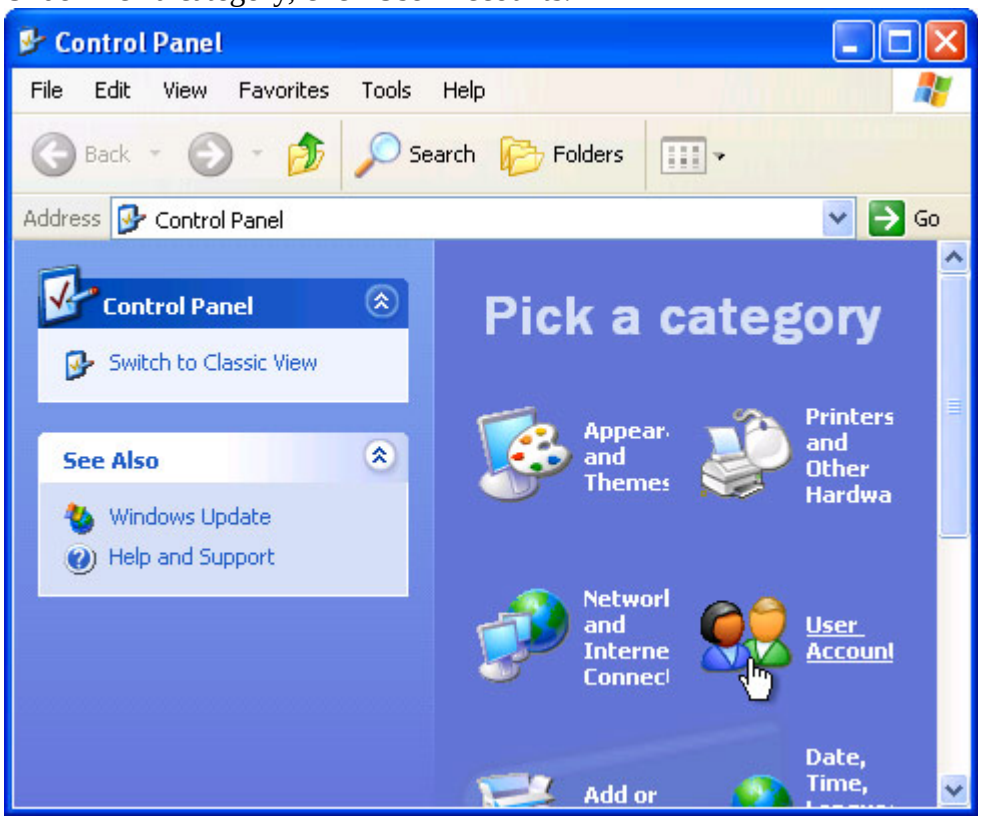
How to Add a Non-Administrative Windows User Account

PA-DSS 3.1

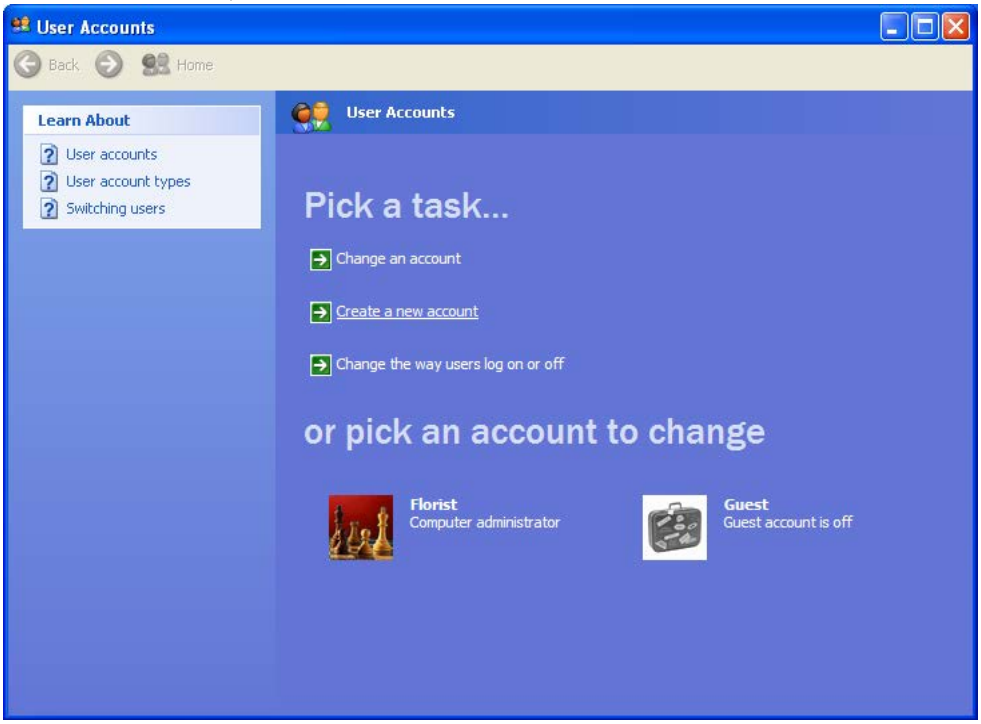
1. Log on to your computer as “Florist” (Florist has administrative privileges). Click Start, and then click Control Panel.



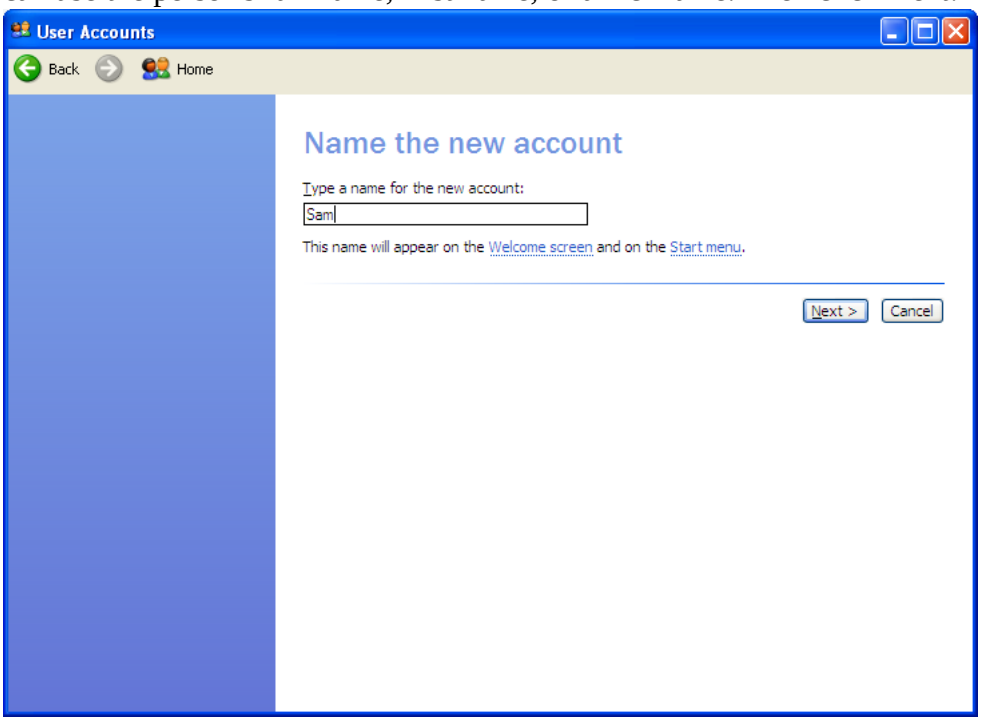
2. Under Pick a category, click User Accounts.



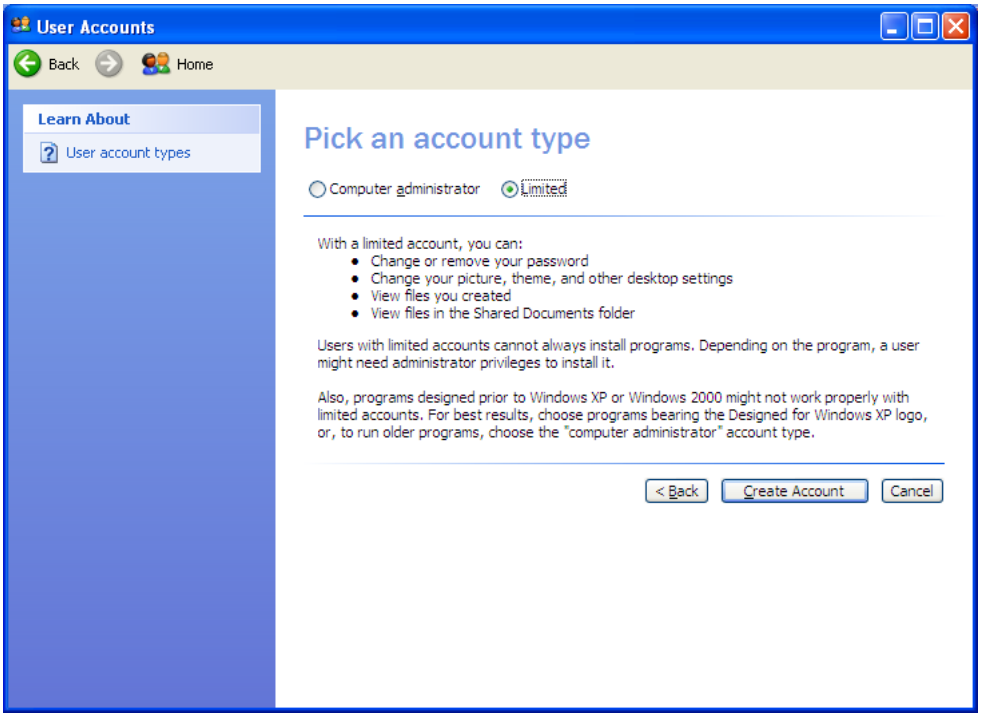
3. Under Pick a task, click Create a new account.



4. In the User Accounts wizard, on the Name the new account page, type the name for the user. You can use the person's full name, first name, or a nickname. Then click Next.



5. The User Accounts wizard displays the Pick an account type page. Click Limited, and then click Create Account.

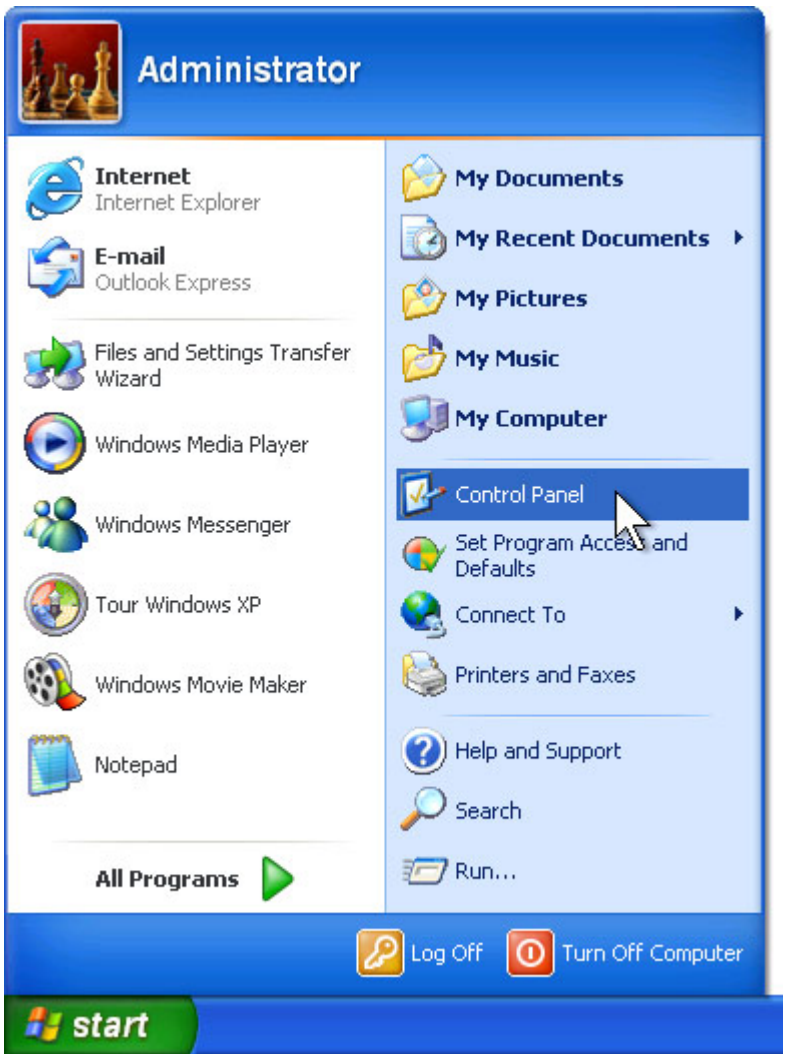


6. To create another account, return to step 3.

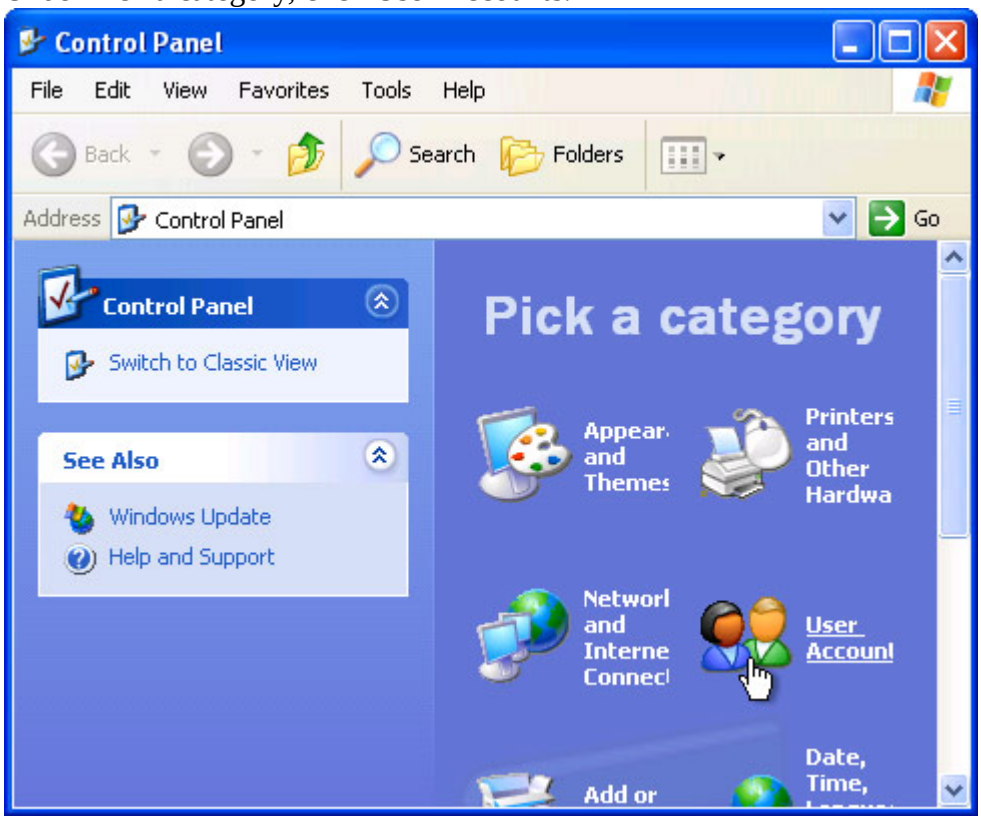
How to Add an Administrative Windows User Account

PA-DSS 3.1

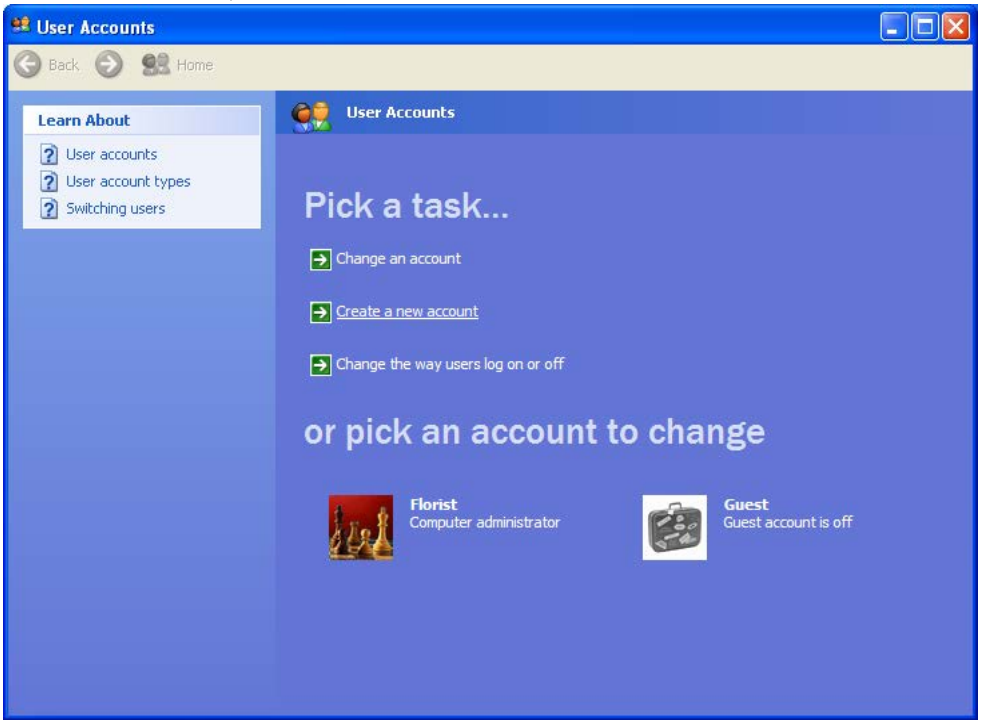
1. Log on to your computer as “Florist” (Florist has administrative privileges). Click Start, and then click Control Panel.



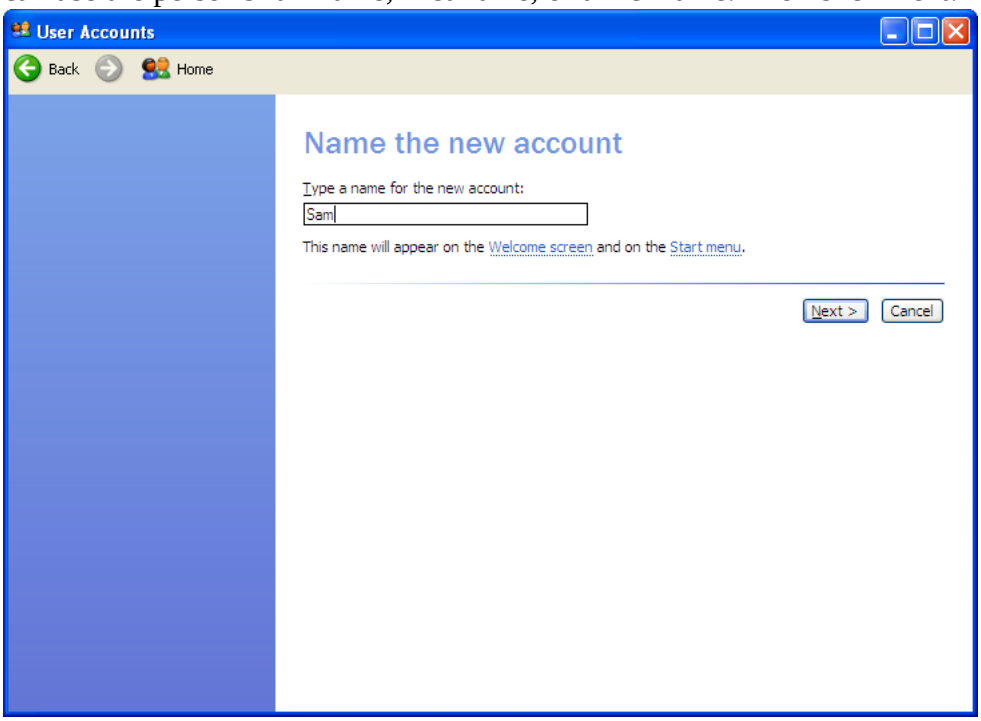
2. Under Pick a category, click User Accounts.



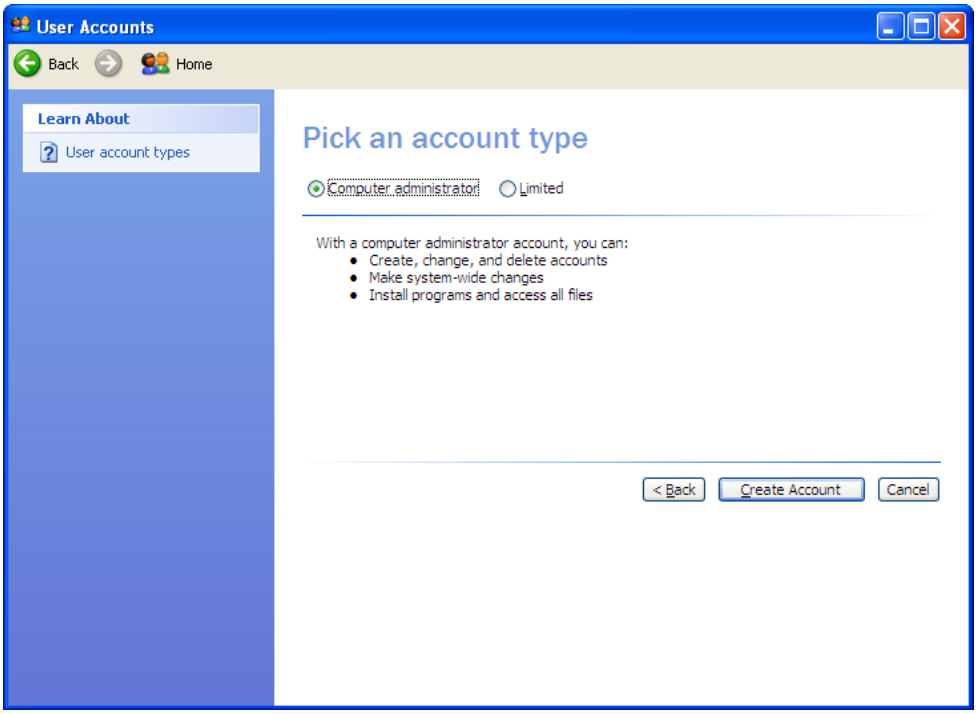
3. Under Pick a task, click Create a new account.



4. In the User Accounts wizard, on the Name the new account page, type the name for the user. You can use the person's full name, first name, or a nickname. Then click Next.



5. The User Accounts wizard displays the Pick an account type page. Click Computer Administrator, and then click Create Account.

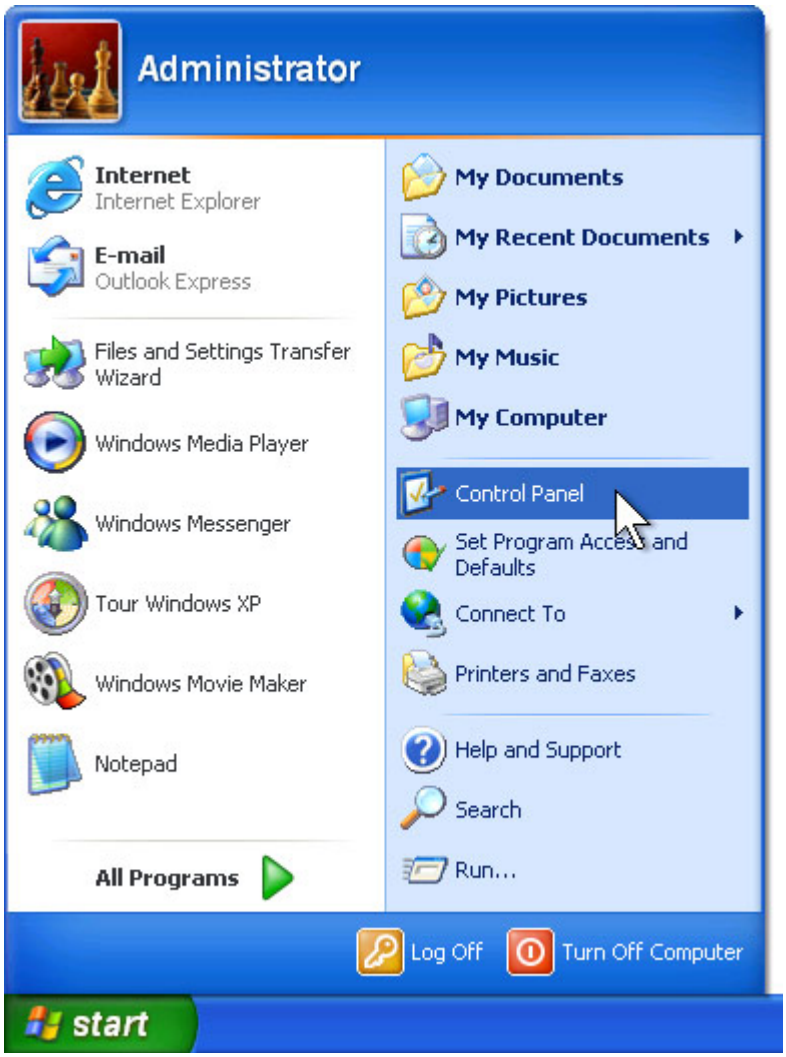


6. To create another account, return to step 3.

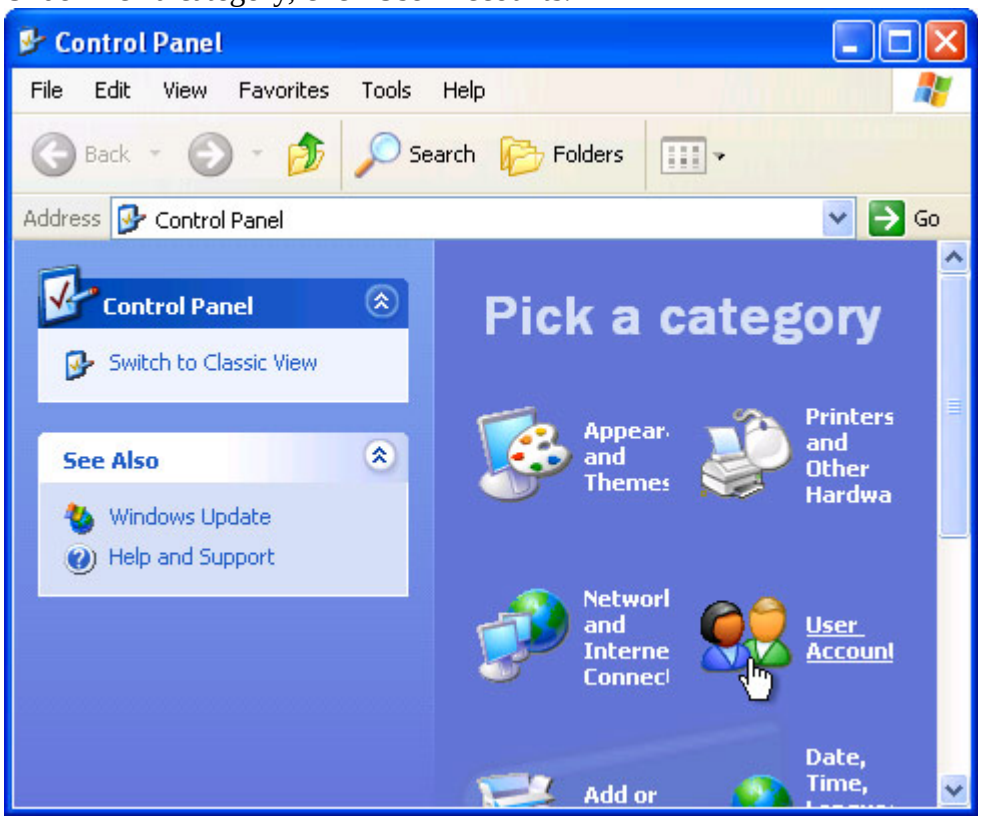
How to Remove a Windows Administrative User Account

PA-DSS 3.1
PCI 8.5.4
PCI 8.5.5

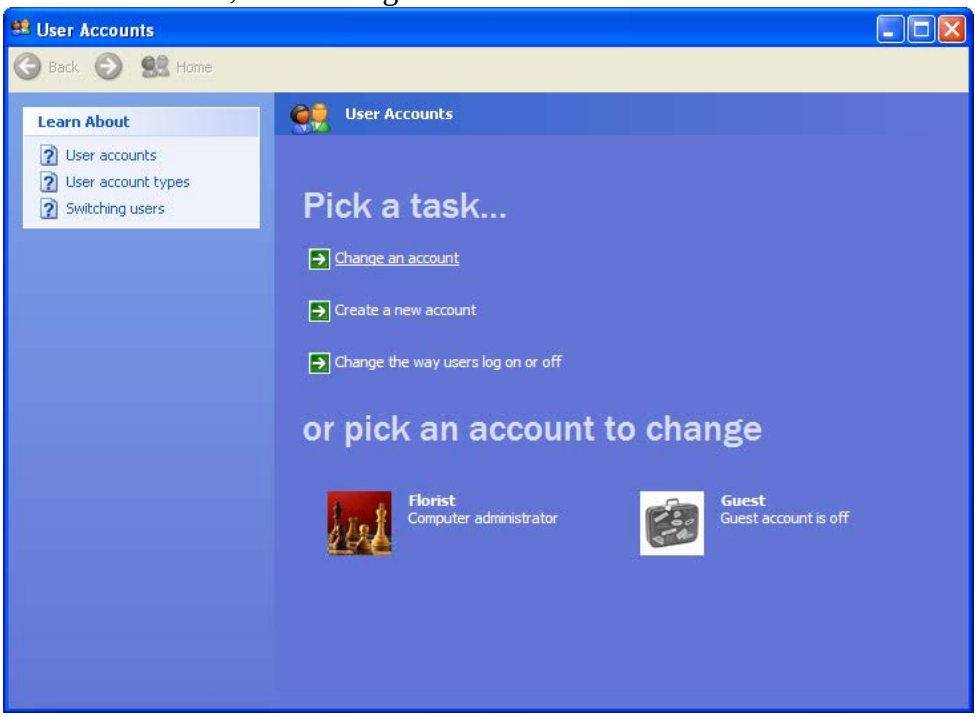
1. Log on to your computer as “Florist” (Florist has administrative privileges). Click Start, and then click Control Panel.



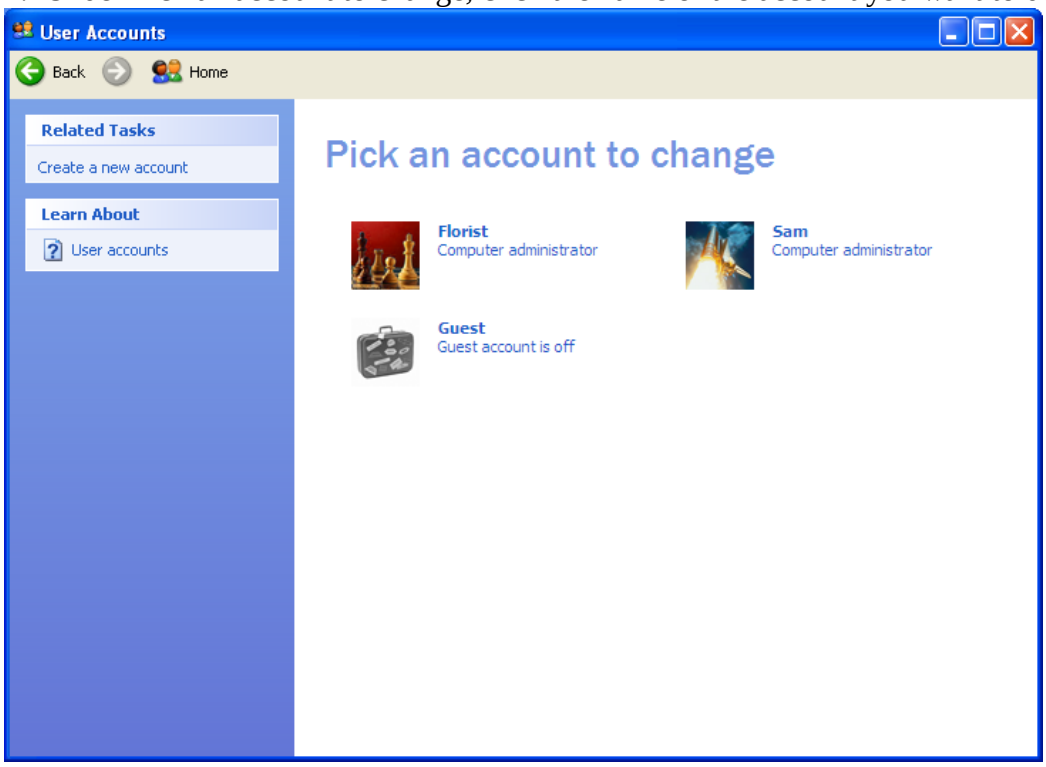
2. Under Pick a category, click User Accounts.



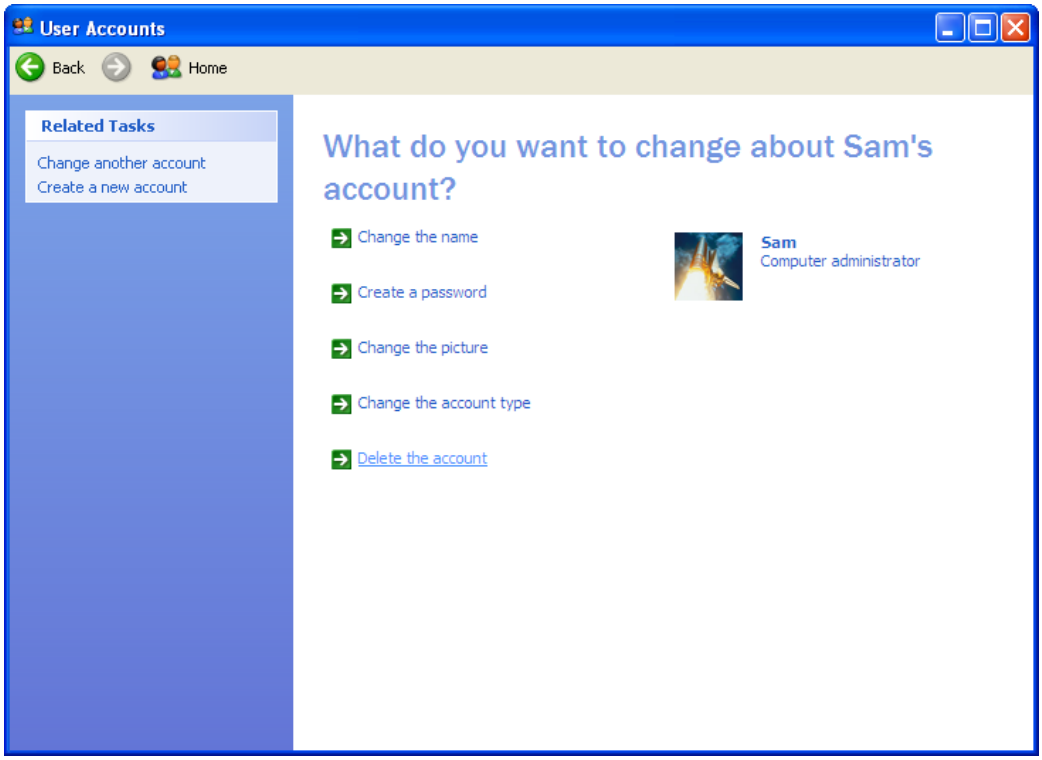
3. Under Pick a task, click Change an account.



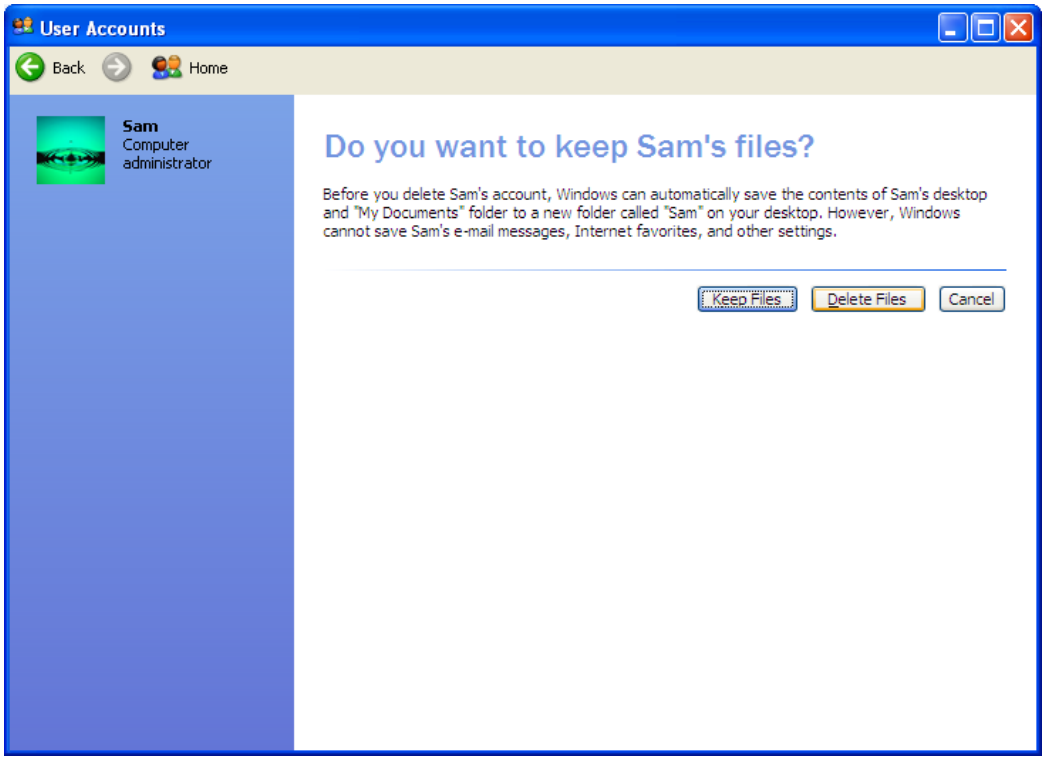
4. Under Pick an account to change, click the name of the account you want to delete.



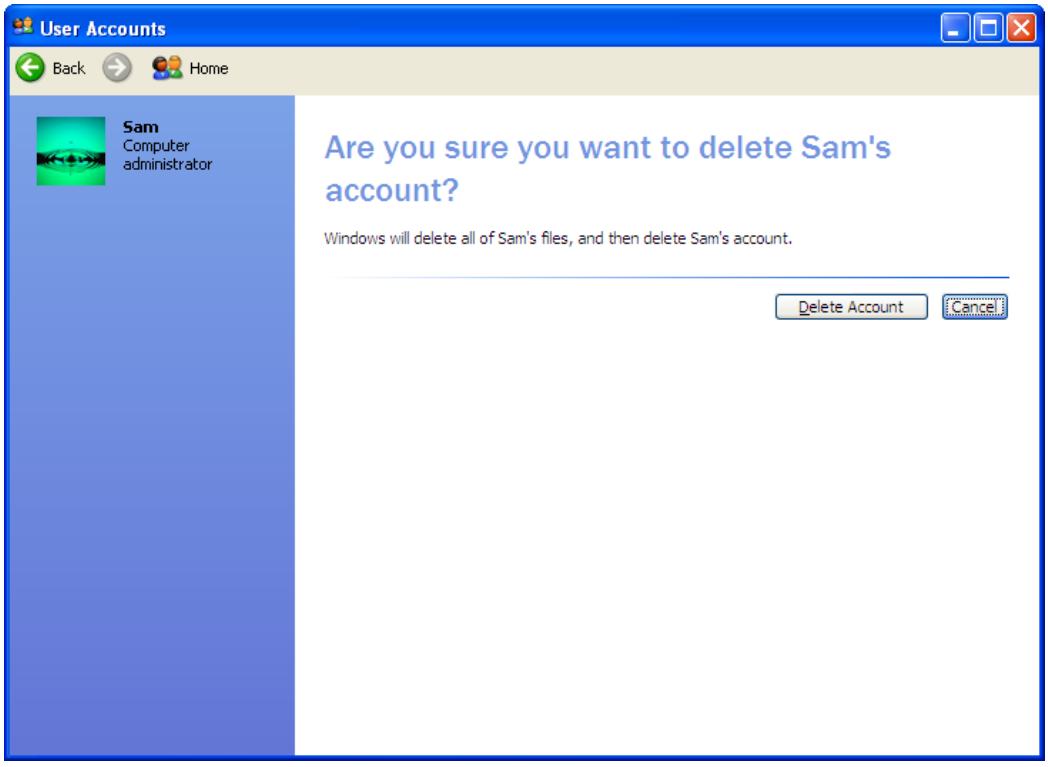
5. Click on Delete the account.



6. Click on the Delete Files button.



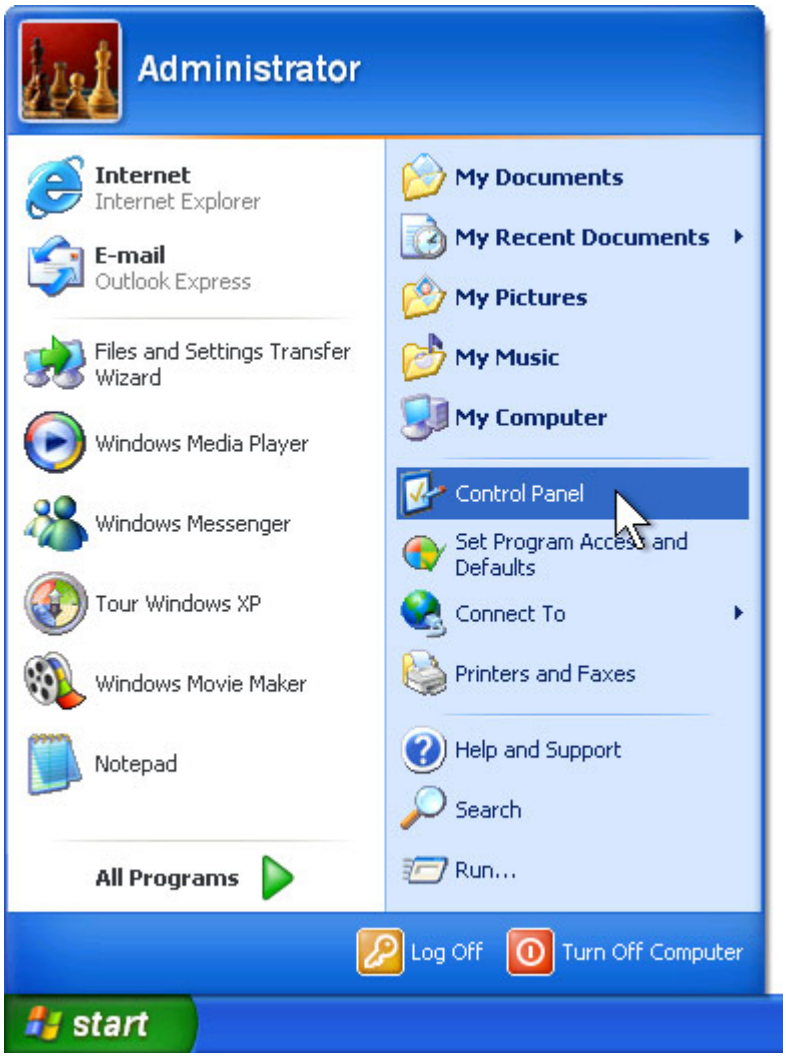
7. Click the Delete Account button.



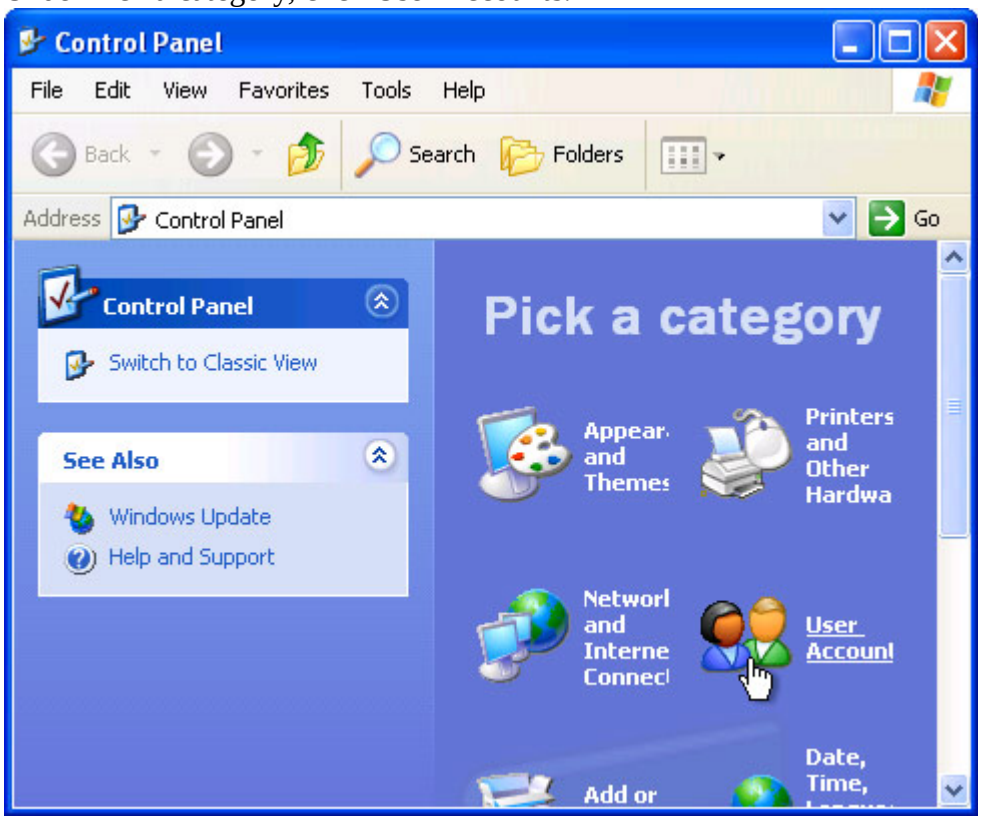
How to Remove a Windows Non-Administrative User Account

PA-DSS 3.1
PCI 8.5.4
PCI 8.5.5

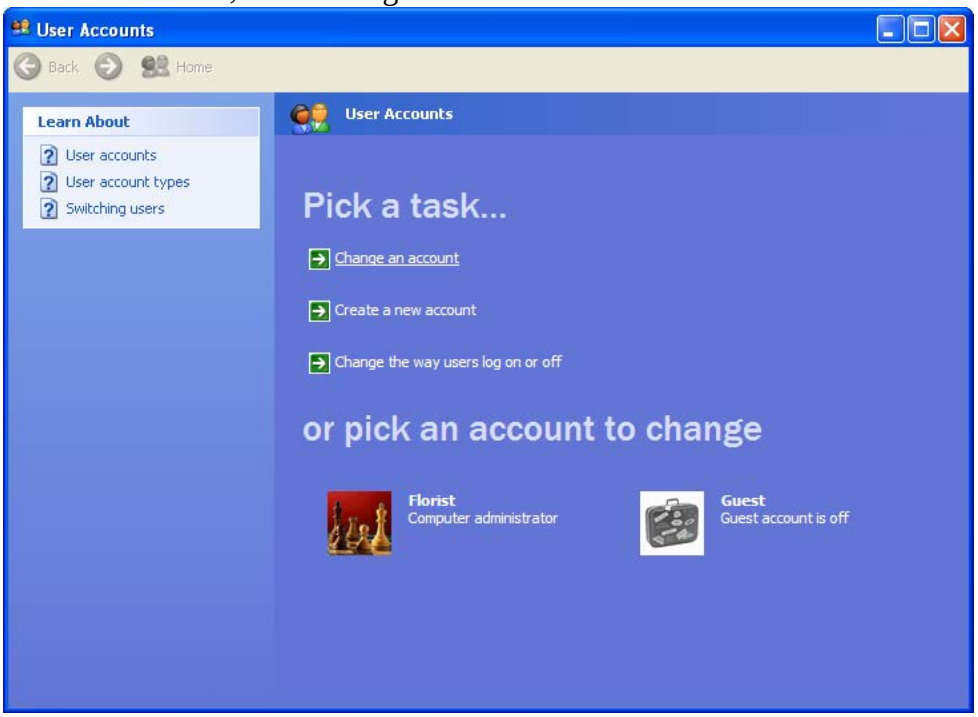
1. Log on to your computer as “Florist” (Florist has administrative privileges). Click Start, and then click Control Panel.



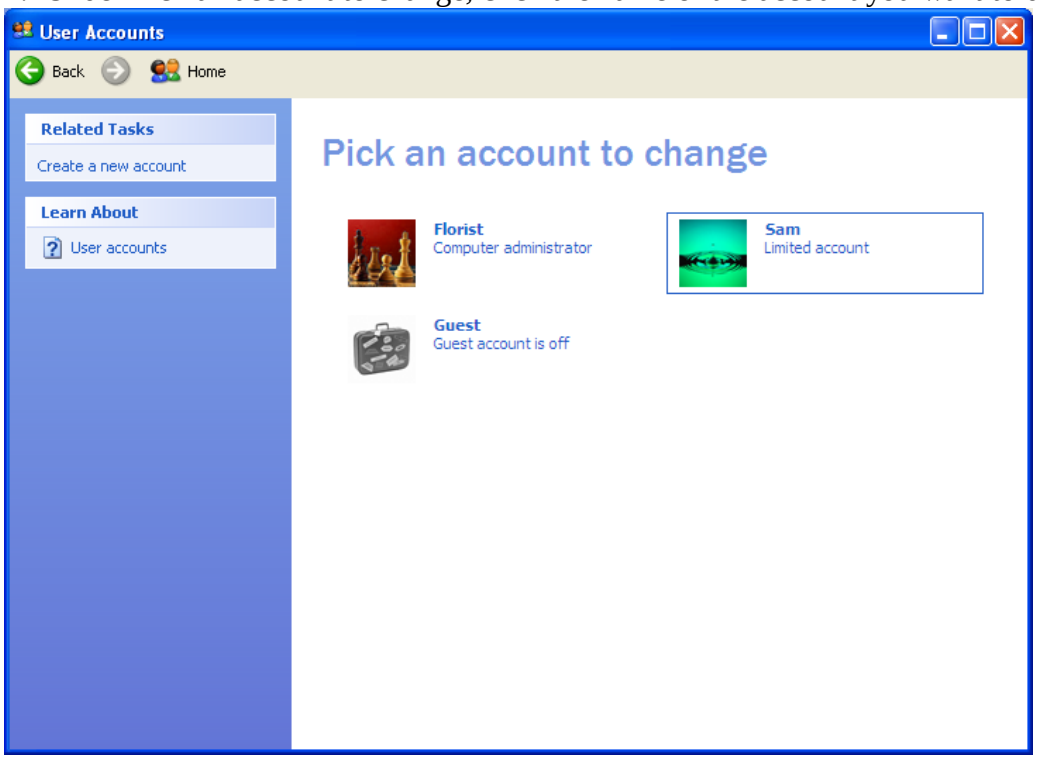
2. Under Pick a category, click User Accounts.



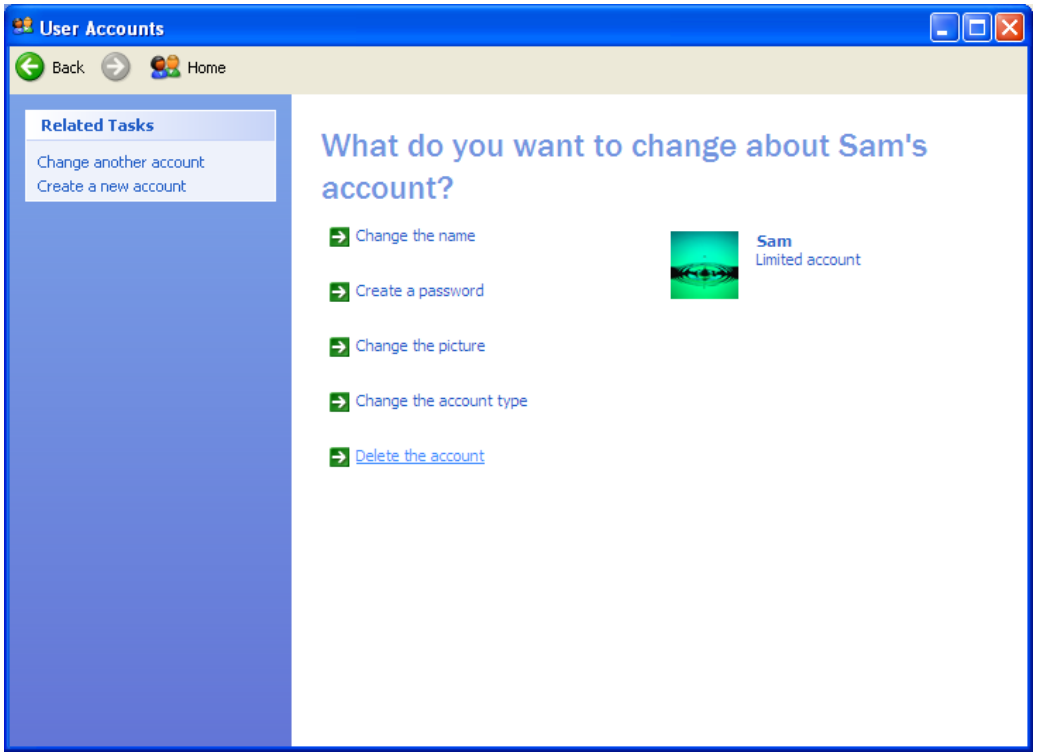
3. Under Pick a task, click Change an account.



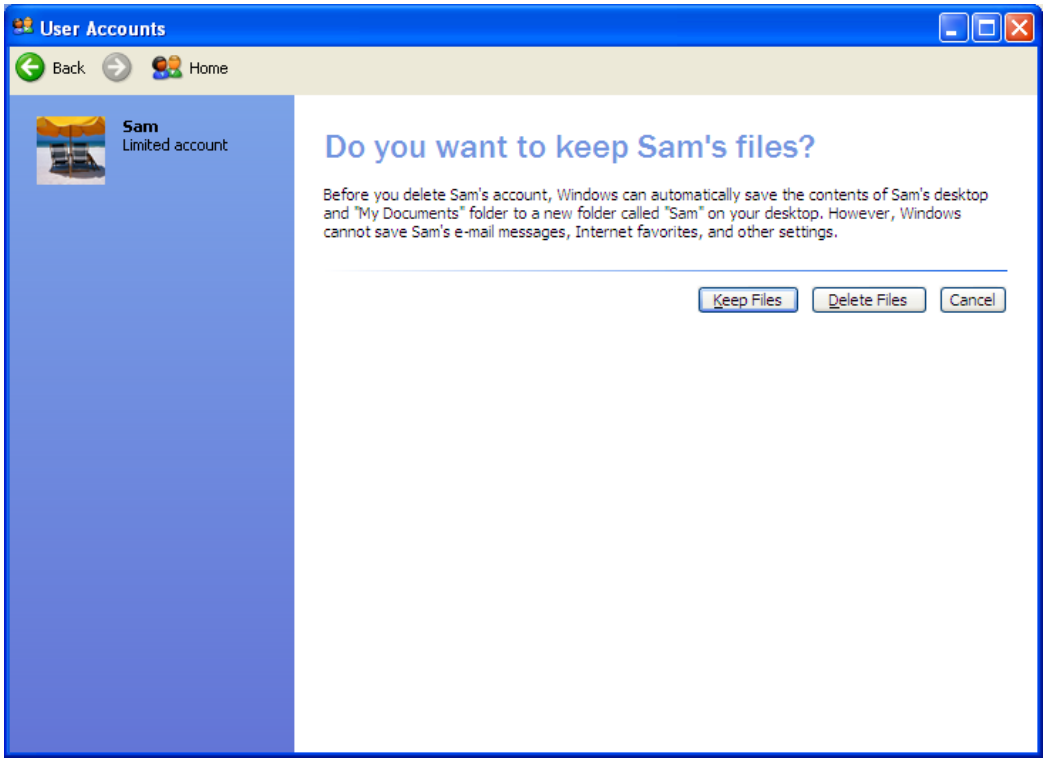
4. Under Pick an account to change, click the name of the account you want to delete.



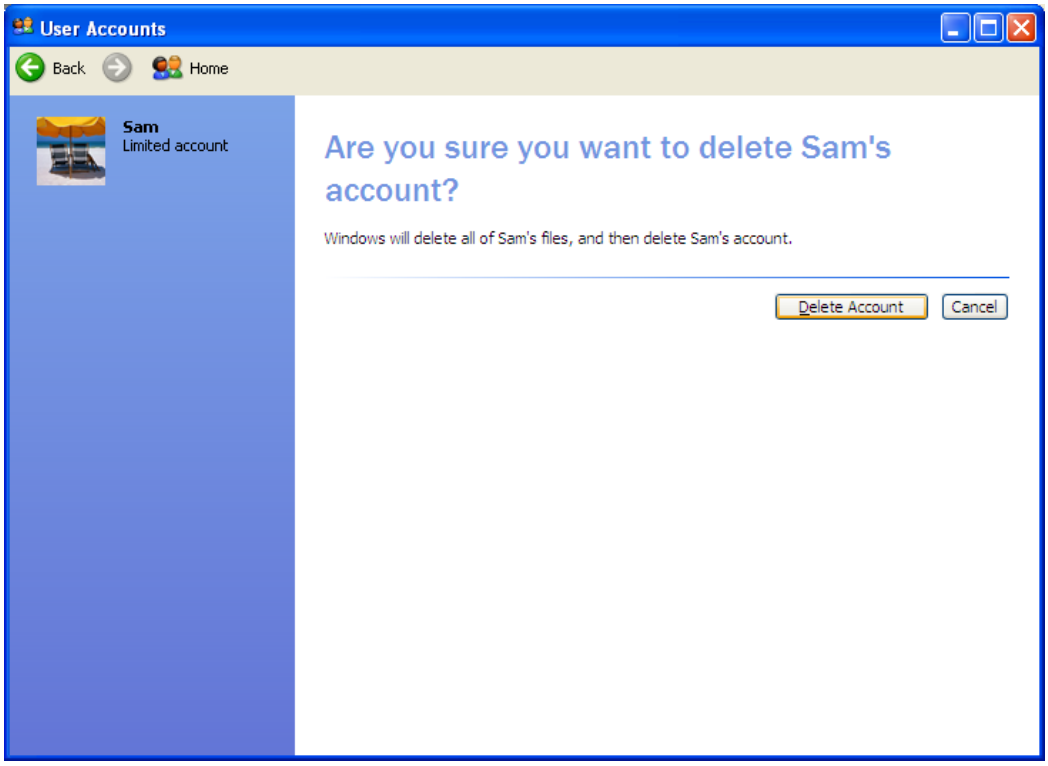
5. Click on Delete the account.



6. Click on the Delete Files button.



7. Click the Delete Account button.



How to Add/Remove a Dove POS User Account

PA-DSS 3.1
PCI 8.5.4
PCI 8.5.5

To add an Employee:

1. Access the screen
    a. Select My Shop from the left-hand navigation menu. The My Shop screen appears.

b. Select Employee Setup. The Employee Setup screen appears. This screen lists any employees you have already setup in your system.

c. Click the Add New button at the bottom of the Employee Setup Screen.

Or

Select Tools > Employee Setup from the Menu at the top of the screen.

The Add/Modify Employee screen appears.

2. Enter Employee Information.

3. Set up Employee Security:

Dove POS contains 4 security groups. Each group is setup with pre-defined security roles. The level of access a user has in the system is determined by the user group they are associated with.

To set a user's security level, select a checkbox in the Employee Security section. Options are:

Manager/Owner - This is the highest security level and allows access to all areas of the system.
Bookkeeper - This setting is similar to Manager/Owner, except the bookkeeper does not have access to all the System Maintenance screens.
Sales Clerk - This setting has limited or no access to the System Maintenance screens.
Restricted Sales Clerk - This setting has access to the order-related screens only.

4. Complete the Process:

You have several options when you have completed entering information on the screen. You can:

Save the Profile and Open a New Screen - To save the new employee profile and open a blank Add/Modify Employee screen, click the Save and New button.

Save the Profile and Close the Screen - To save the new employee profile and close the Add/Modify Employee screen, click the Save and Close button.

Close the Screen without Saving - To close the screen without saving your changes, click the Close button.

How to Securely "Wipe" a Hard Drive

PA-DSS 1.4.a
PA-DSS 1.5.c

This document specifies how to securely wipe a hard disk. You would need to do this in a number of events:

- You are retiring a computer which, at some point in time, contained, or otherwise processed, sensitive cardholder data.
- You are installing the Dove POS on a computer which, in the past, was used for other purposes.
- Your Dove POS Server or workstation has experienced a security compromise.

WARNING:
This process permanently formats your hard disk, there is no "undelete". It is advised that you consult with Teleflora customer service, prior to removing files, to ensure you are following proper, up-to-date procedures.

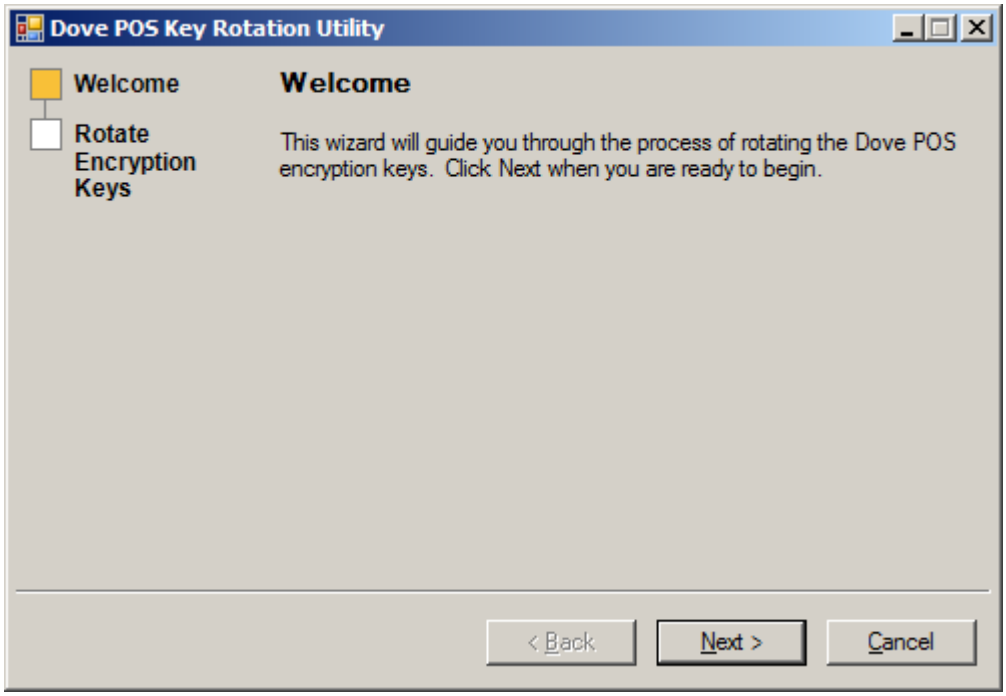
See:
Appendix: Using the Eraser Tool.

How to Change your Dove POS Data Encryption Key

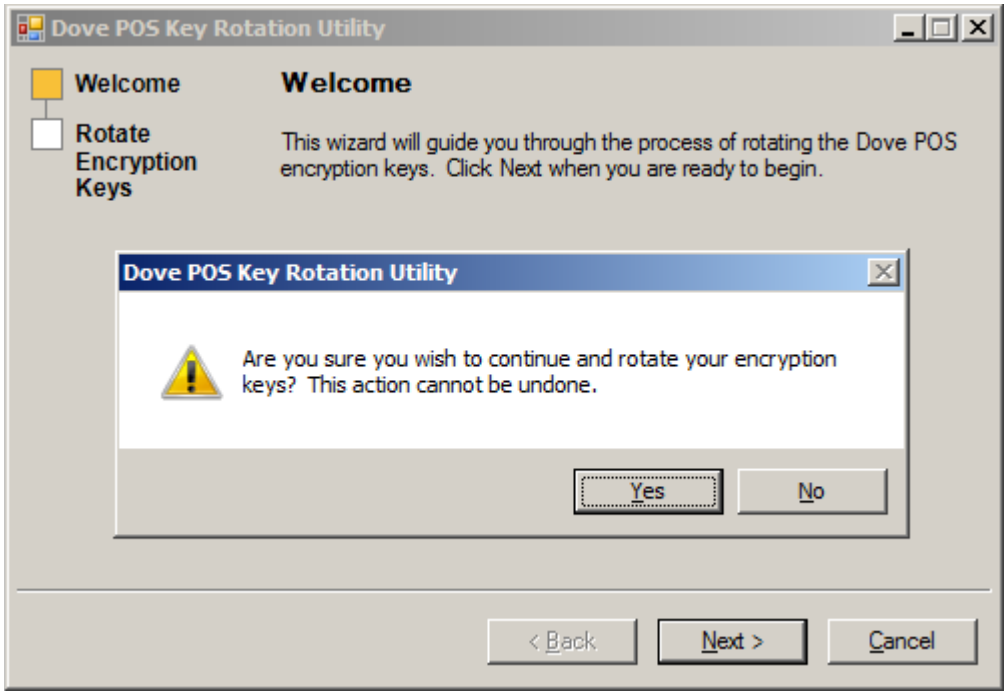
PA-DSS 1.5
PCI DSS 3.6
PCI DSS 8.5

The DovePOS Key Rotation Utility is an application provided by Teleflora to rotate the data encryption keys for you. The DovePOS Key Rotation Utility is located in the Dove POS Server directory.

This Utility can only be executed by a Windows Administrator. Widows will display an error if you are not logged in as an administrator.



1. Launch DovePOS Key Rotation Utility and click on Next.



2. Click Yes to continue with the key rotation.

3. Click Finish to close the application.

How to Create a "Strong" Password

PCI 8.5

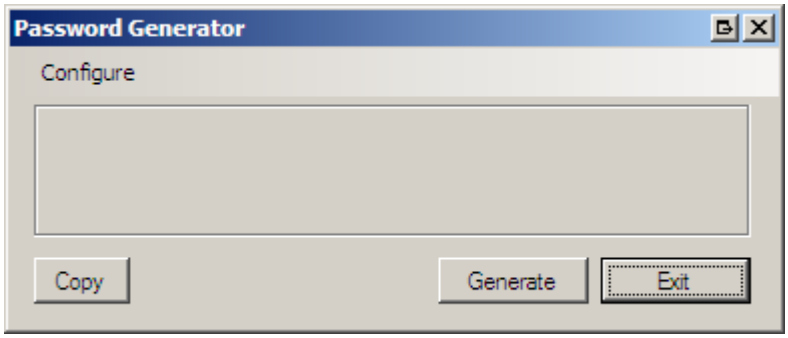
PCI DSS gives specifications as to password strengths required. Following are relevant PCI DSS specifications, as well as some techniques you may use to help generate random passwords.

A PA-DSS compliant password must meet all of the following requirements. Note that you are responsible for ensuring that you use a compliant password:

Minimum of 7 characters long (PCI 8.5.10)
Contains both least numeric and alphabetic characters (PCI 8.5.11)
Different from one of the last four passwords you have used in the past. (PCI 8.5.12)

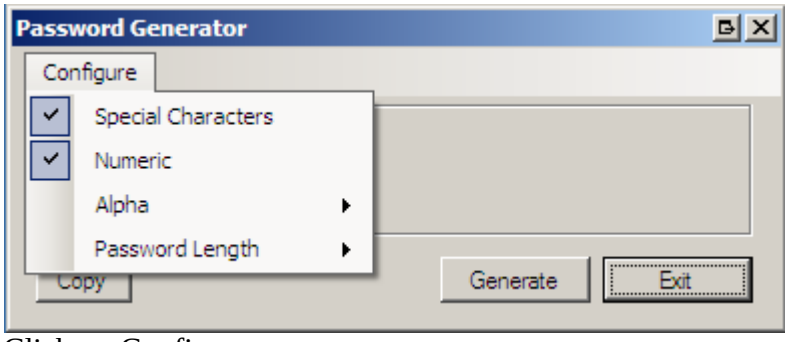
Password Generator

Password Generator is an application provided with DovePOS to assist you in generating secure passwords. Password Generator is located in the Dove POS Terminal directory.



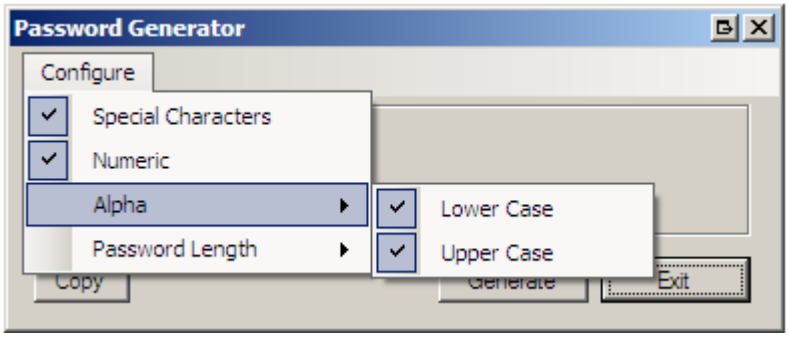
By default Special Characters, Numeric, and Alpha upper and lower case settings are enabled. And, the password length is set to seven characters long.

To modify the complexity settings of the password:



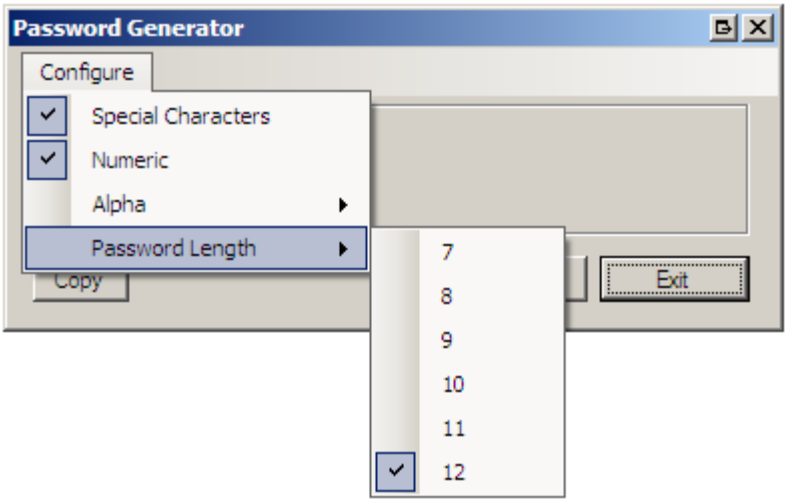
Click on Configure.

Select or deselect Special Characters and/or Numeric.



Click on Alpha

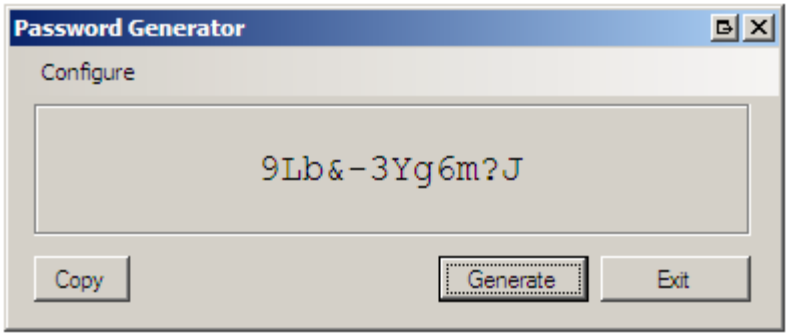
Select or deselect Lower and/or Upper Case characters.



Click on Password length.

Select the desired password length.

To create password:



Click Generate.

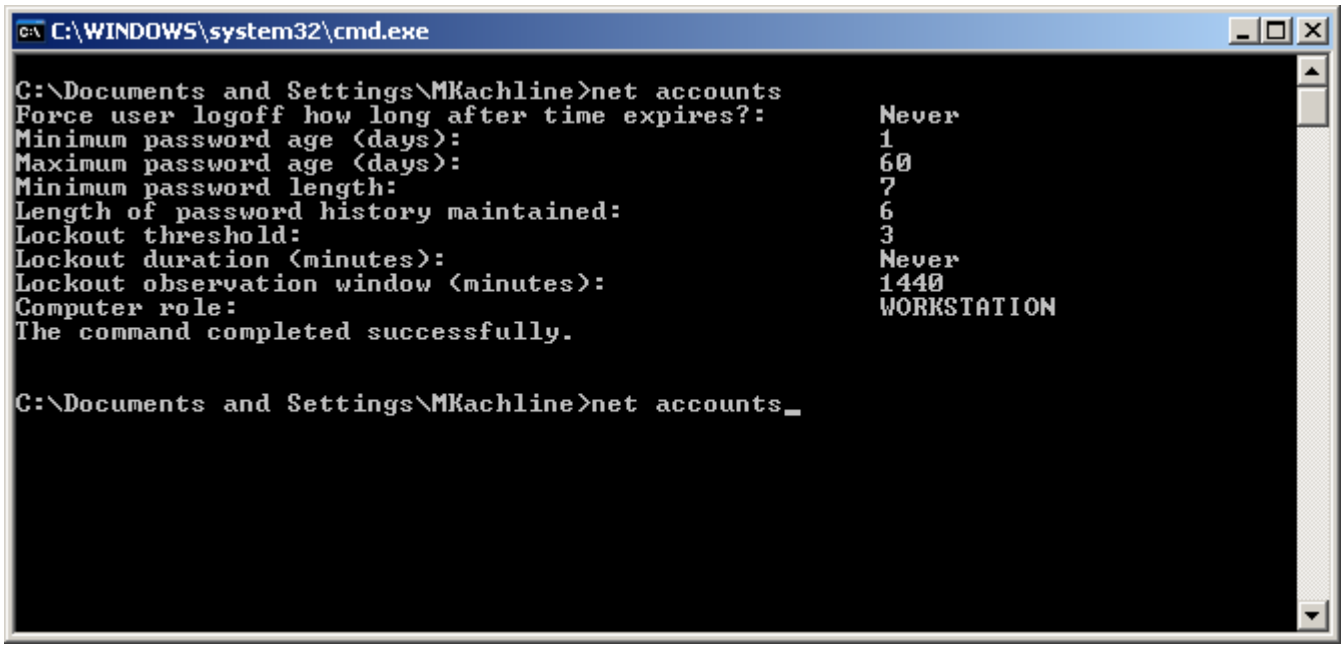
To select a different password click generate again.

Clicking the Copy button puts the password on the clipboard.

How to Verify Password Policies in Windows XP

PCI 8.5

PCI 8.5.x specify a number of password complexity rules which must be in place. Following is how to verify those settings are in place on your windows computer(s).

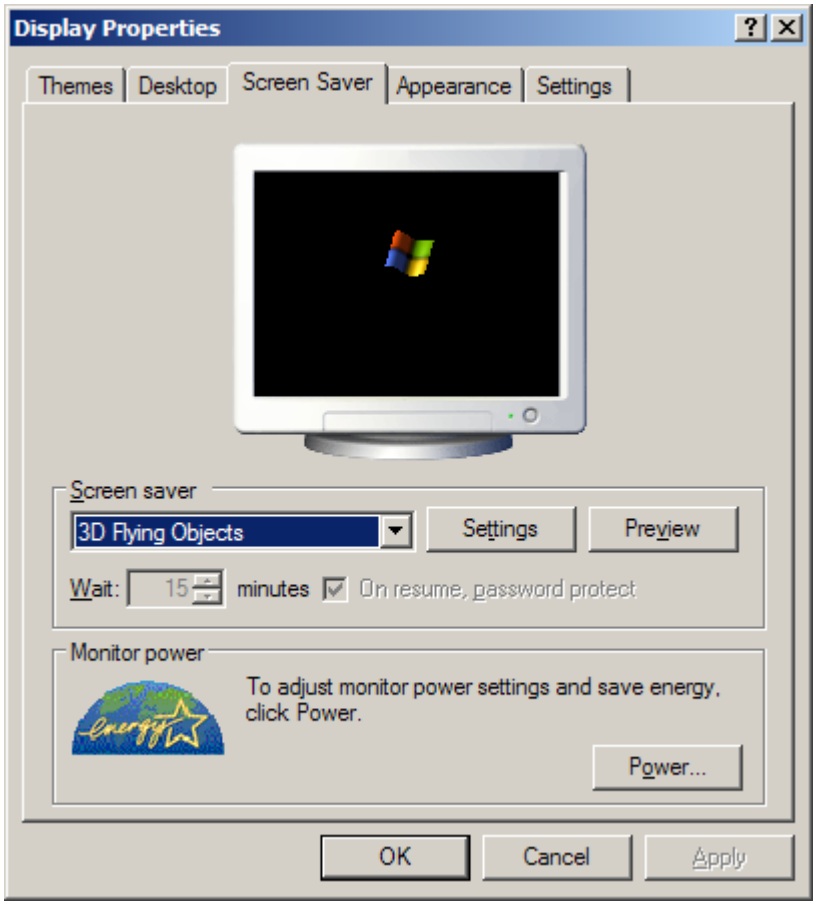


Start | Run |cmd.exe"
From the "C:" prompt:
Net accounts

Look for:

- "Maximum Password Age" of 90 days or less
- "Minimum Password Length" of 7 or greater
- "Length of Password History" of 4 or greater.

How to set a Screensaver Lock in Windows XP



PA-DSS 3.1
PCI 8.5.15

In order to be compliant with PA-DSS requirements, each workstation with access to the Dove POS server must have a “locking” screensaver set. The Screensaver must “lock” (thus, require a password to unlock) after fifteen minutes of inactivity.

To ensure that a Screensaver lock is established, do as follows:

1. Log into Windows computer.
2. Right-click the desktop
3. Select the “Screen Saver” tab
4. Put “15” (or less that 15) in the “Wait xx minutes” box.
5. Check the “On resume, password protect” box.
6. Click “OK” button.

How to Disable Debug Logging

Addresses:
PA-DSS 4.2.b

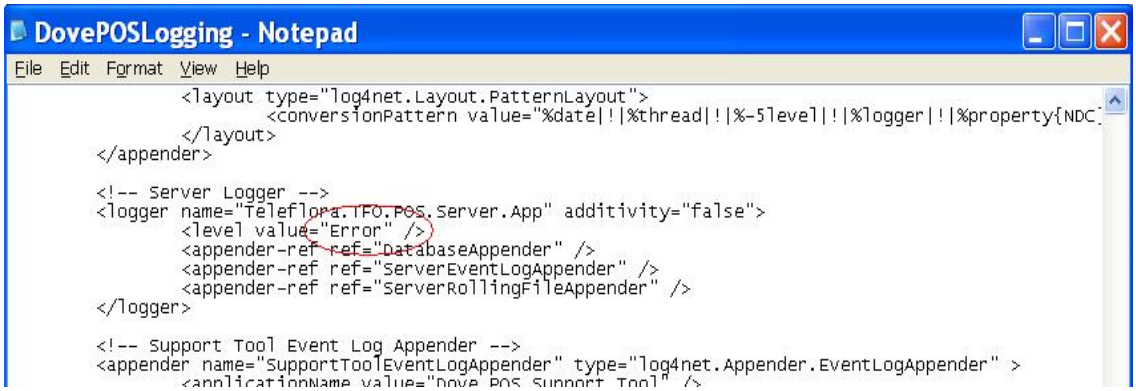
Your Dove POS system logs various communications information pertaining to credit card transactions at configured or above log level in the hierarchy. The various log levels, in the increasing order of hierarchy, are “Debug”, “Info”, “Warn” and “Error”. It is possible to change the log level through configuration file so that the system logs information at that or above level. Please note, completely disabling logging on your Dove POS may render your system out of PCI compliance; do not disable Dove POS logging Capabilities.

Following is the procedure you may follow to turn off debug/info logging.

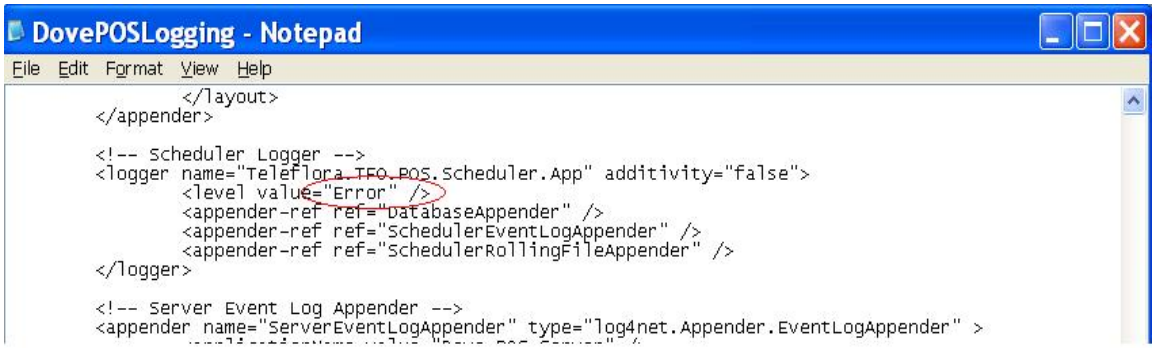
WARNING:
You must take great care while editing configuration files manually. If an error is caused in the configuration file, Dove POS system may not function properly.

For Dove POS Terminal application,
Using Notepad, open logger configuration file located at;
C:\Program Files\Teleflora\Terminal\DovePOSLogging.config
Locate the logger section with the name as “DovePOS”.
To disable debug/info logging, change the “level” element “value” to either “Warn” or “Error” (refer to the figure below).
Save and close the file.

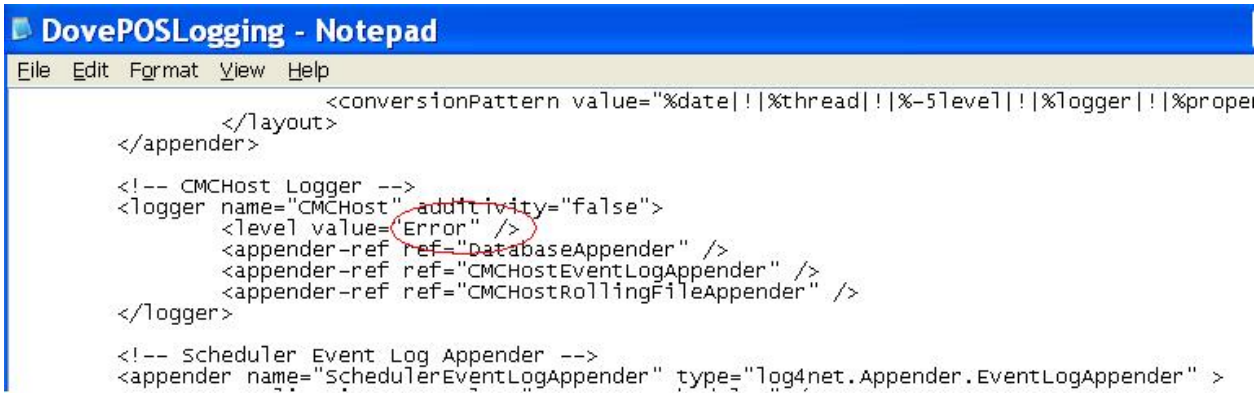
For Dove POS Server application,
Using Notepad, open logger configuration file located at:
C:\Program Files\Teleflora\Server\DovePOSLogging.config
Locate the logger section with the name as “Teleflora.TFO.POS.Server.App”.
To disable debug/info logging, change the “level” element “value” to either “Warn” or “Error” (refer to the figure below).
Save and close the file.



For Dove POS Scheduler application,
Using Notepad, open logger configuration file located at:
C:\Program Files\Teleflora\Server\DovePOSLogging.config
Locate the logger section with the name as “Teleflora.TFO.POS.Scheduler.App”.
To disable debug/info logging, change the “level” element “value” to either “Warn” or “Error” (refer to the figure below).
Save and close the file.



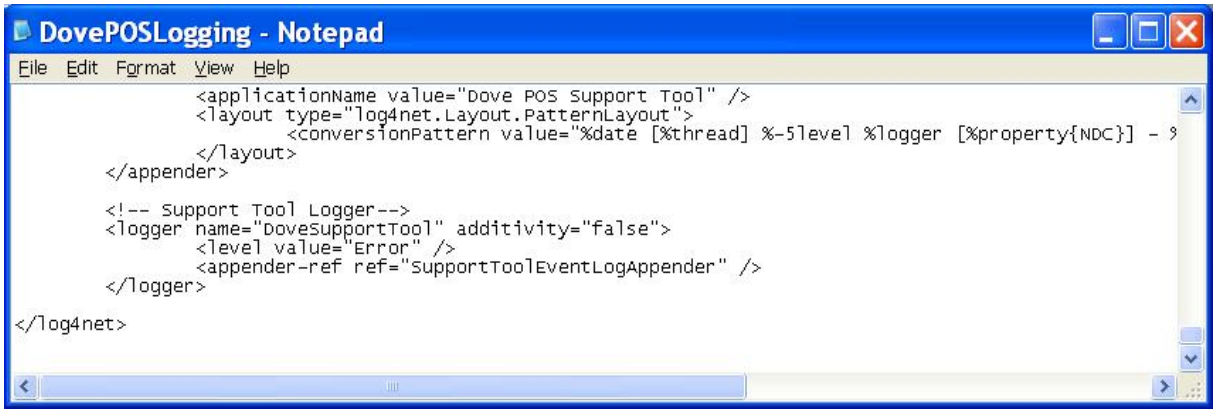
For Dove POS CMC Host application,
Using Notepad, open logger configuration file located at:
C:\Program Files\Teleflora\Server\DovePOSLogging.config
Locate the logger section with the name as “CMCHost”.
To disable debug/info logging, change the “level” element “value” to either “Warn” or “Error” (refer to the picture below).
Save and close the file.



For Dove POS Support Tool application,
Using Notepad, open logger configuration file located at;

C:\Program Files\Teleflora\Server\DovePOSLogging.config

Locate the logger section with the name as “DoveSupportTool”.
To disable debug/info logging, change the “level” element “value” to either “Warn” or “Error” (refer to the picture below).
Save and close the file.



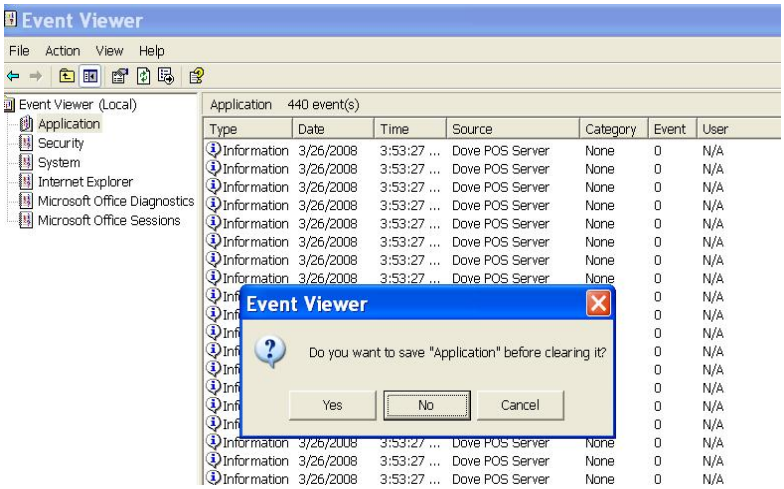
How to Remove Log Files

Addresses:
PA-DSS 1.1.6

Dove POS system uses database and Windows application event log to log events. The database table used to record log events is TU_ActivityLog. Typically, the Windows application event log file is located at C:\Windows\system32\config\AppEvent.Evt.
The information written to the Windows event log and database is valuable in troubleshooting many issues which you may experience in your use of the application. Though Dove POS has been carefully written to never log accountholder's sensitive data in these logged information, in the event of either unforeseen bugs or the need for "special case" logging, accountholder's sensitive data could be contained within these logged information.
Remove Dove POS Logging – Windows Event Log
Following is the process you may follow to clear-off (securely over-write) all log events in Windows application event log.

WARNING:
You cannot retrieve records from a cleared event log using an undelete tool.
For details, refer to the information at the following link.
http://www.microsoft.com/technet/scriptcenter/guide/sas_log_pcna.mspx?mfr=true

Process:
Log in to your Dove POS Terminal/Server as an administrative account.
Click the Start button.
Click Control Panel.
Click Administrative Tools.
Double-click Event Viewer.
Right click on the Application in the left pane of the Event Viewer.
Click on Clear all Events. You will be asked "Do you want to save "Application" before clearing it?"



Click "No" to clear-off all the events, without saving.

Setup / Configure the Netgear FVS338 Firewall

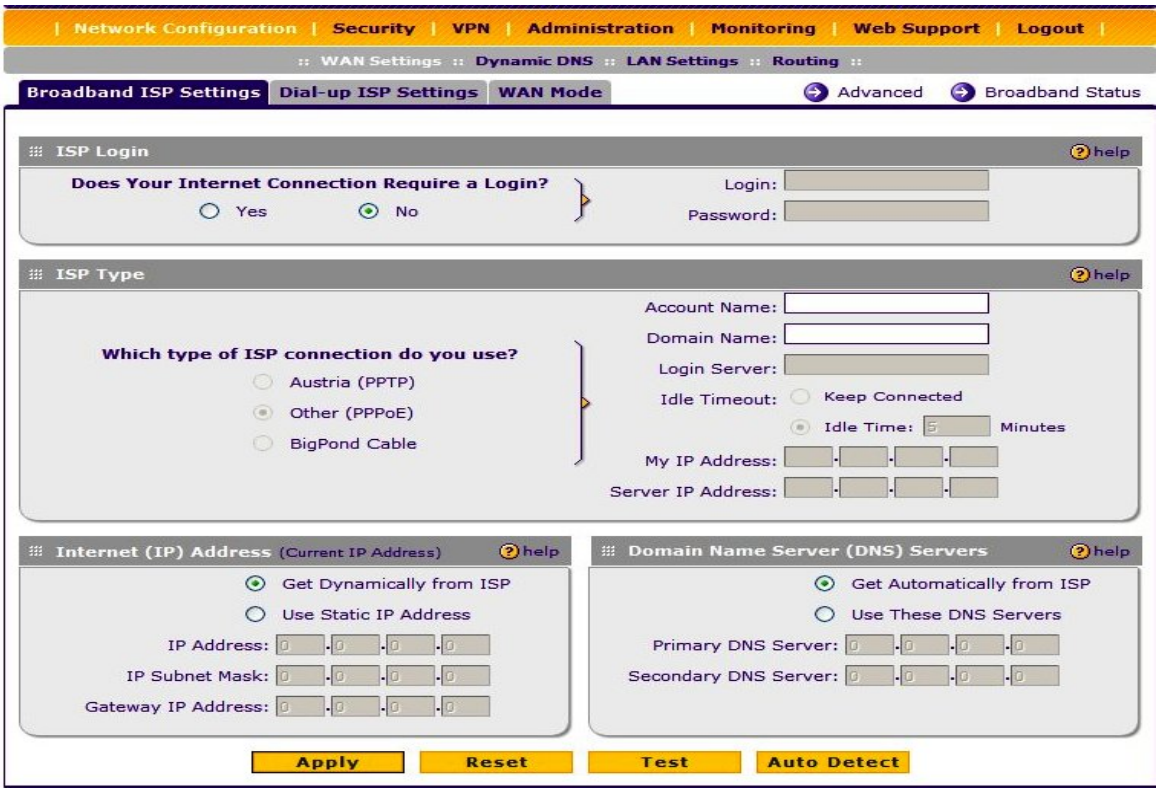
To access the router control panel:

1. Open Internet Explorer

2. Enter 192.168.1.1 in for the address. The router login page should display.

3. Enter the admin user name and password. The default user name/password is:
   User Name: admin
   Password: password

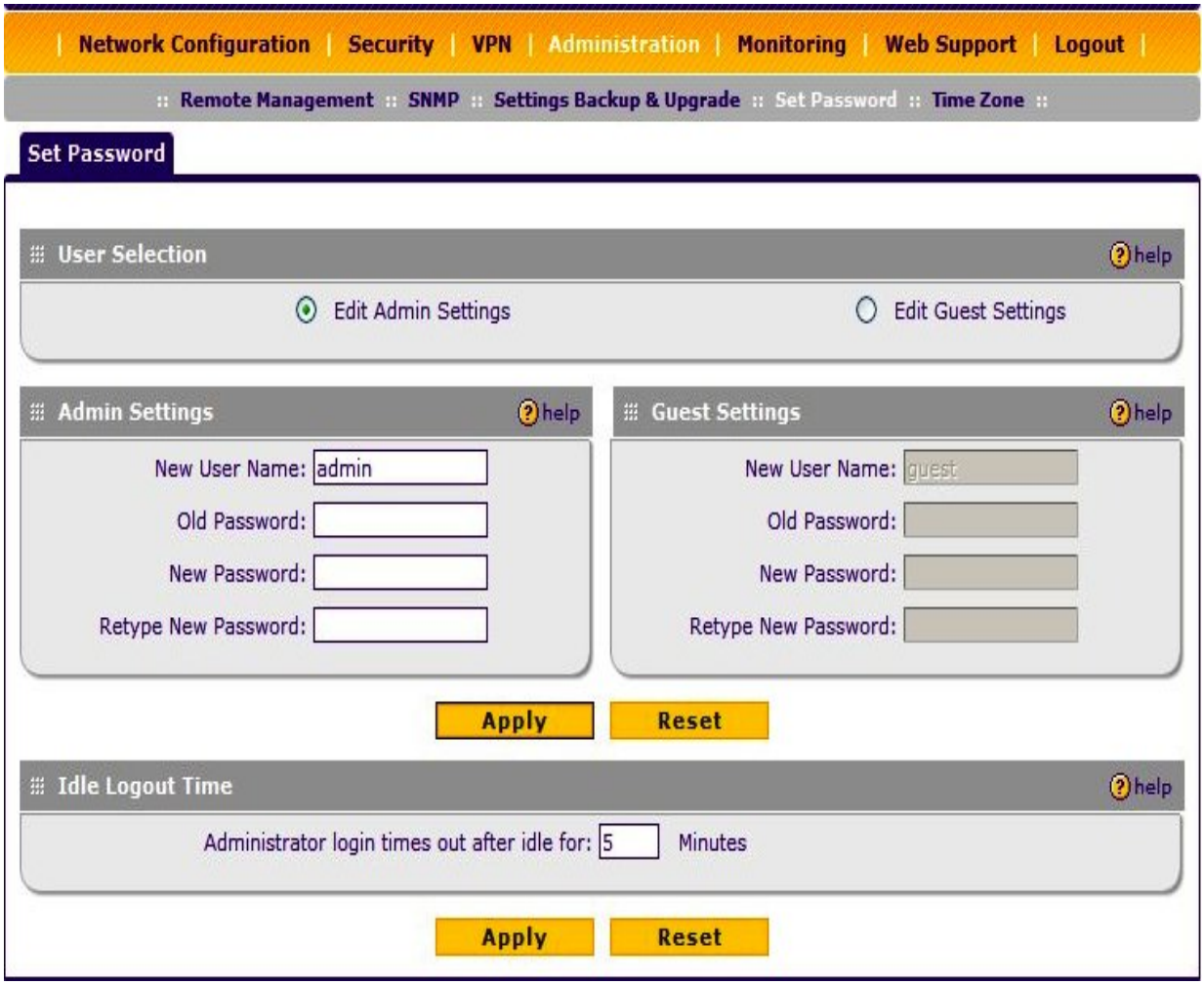
Step 1: Configure the Broadband ISP



1. Does the internet connection require a login?
   (a.) If you selected "No" then scroll down and set the IP addresses if necessary; if not, then press "Apply" and proceed to next step.

   (b.) If you selected "Yes" then fill in the ISP information as appropriate. If no "Account Name" was specified by the ISP, then use the same information in this blank as the "Login" blank (copy & paste works well). Next, scroll down and set the IP address.

Step 3: Set the Password



1. In the top menu bar, click "Administration"

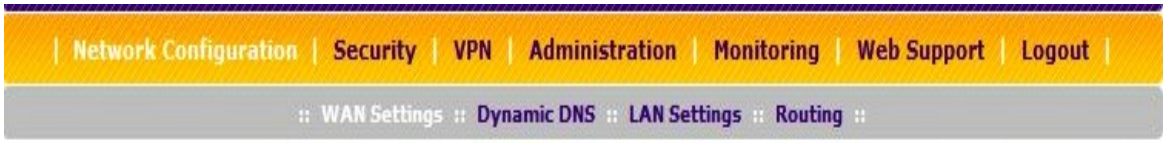
2. In the sub menu bar, click "Set Password"

3. The default Old Full Access password is "password". The New Full Access Password must be generated using alphanumeric codes with substitution. The password must be ALL CAPITAL LETTERS Use the first 4 letters of the state followed by the last 5 of the shop code to generate the base password, then use the substitution chart to change the letters and numbers to the final password.

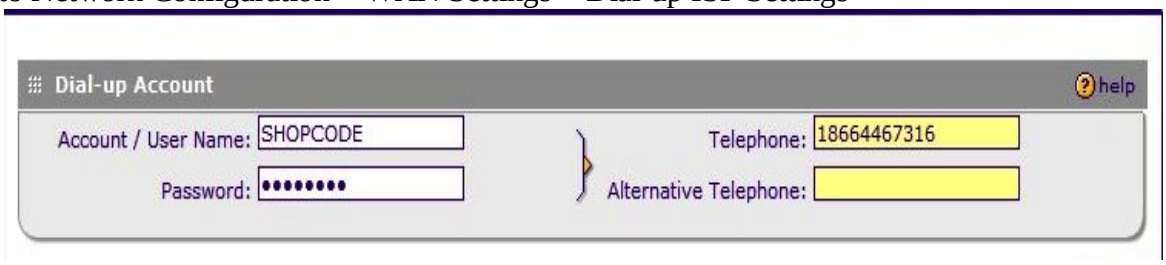
4. Change the guest password from "password" to "T3l3fl0r4".

5. Click “Apply” to complete the change

Step 4: The Dialup Connection



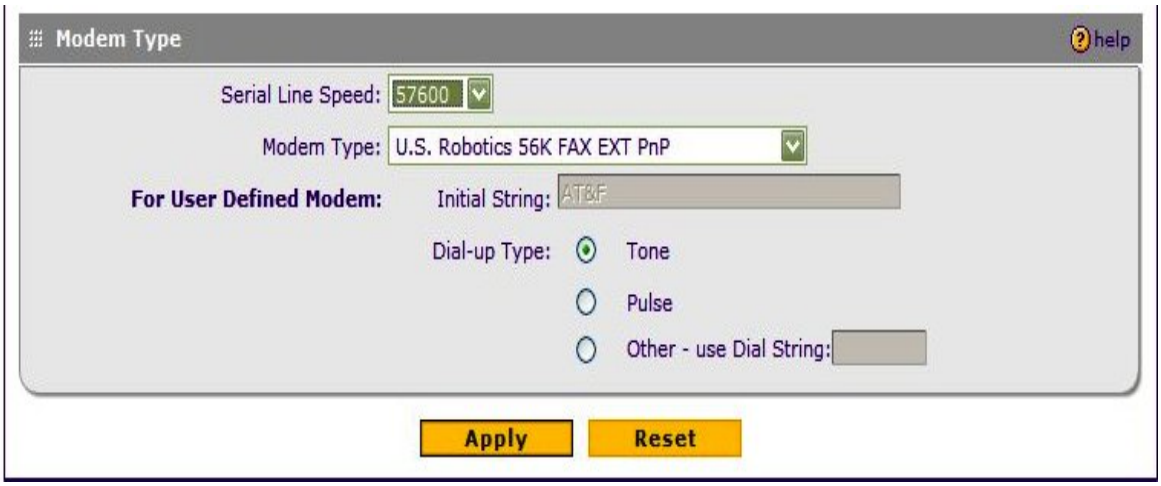
1. Go to Network Configuration > WAN Settings > Dial-up ISP Settings



A. Account / User Name: SHOPCODE ex: 00070750

B. Password: TWS Password (Same one you use in DovePOS setup)

C. Telephone: 1.800-443-3597 (Remember to input 9 if you need to get an outside line)



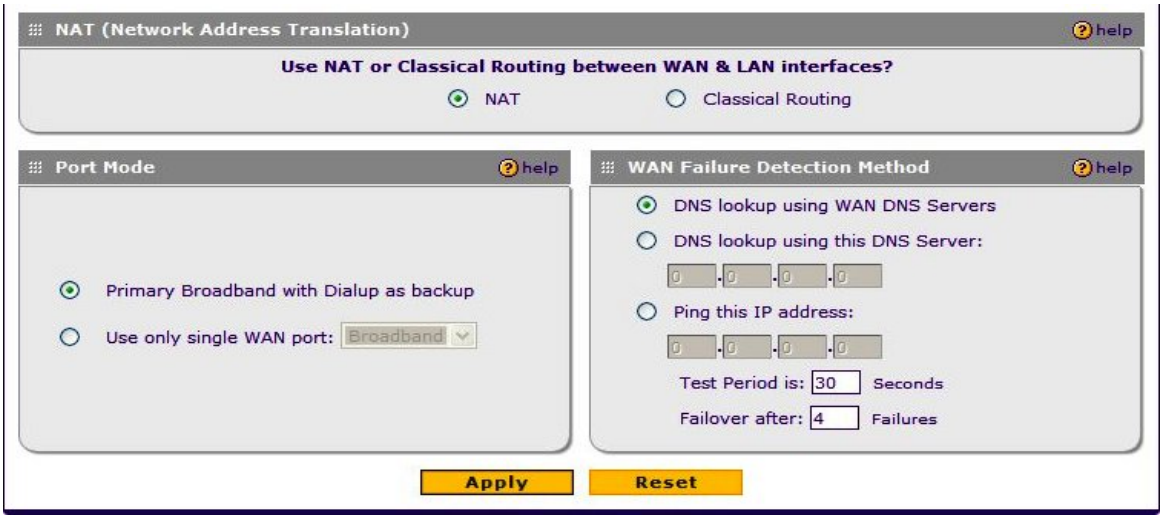
D. Set the Serial Line Speed to 57600.

E. Select U.S. Robotics FAX PnP, from the Modem Type Dropdown box.

F. Leave everything else as defaults, click Apply.

Step 5: WAN Mode

Click Network configuration > Wan Settings

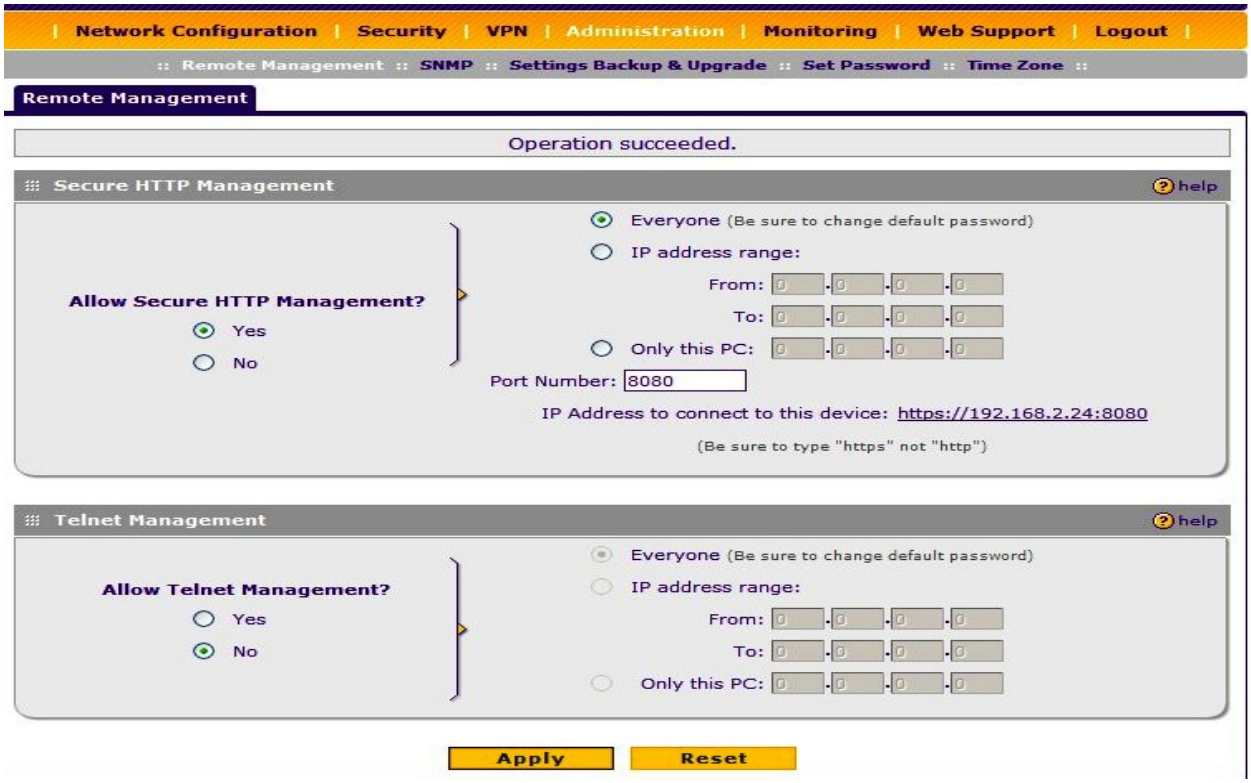


A. Port Mode: Primary Broadband with Dial up as Backup

B. WAN Failure Detection Method: Failover after 4 failures (Default is 2 change it)

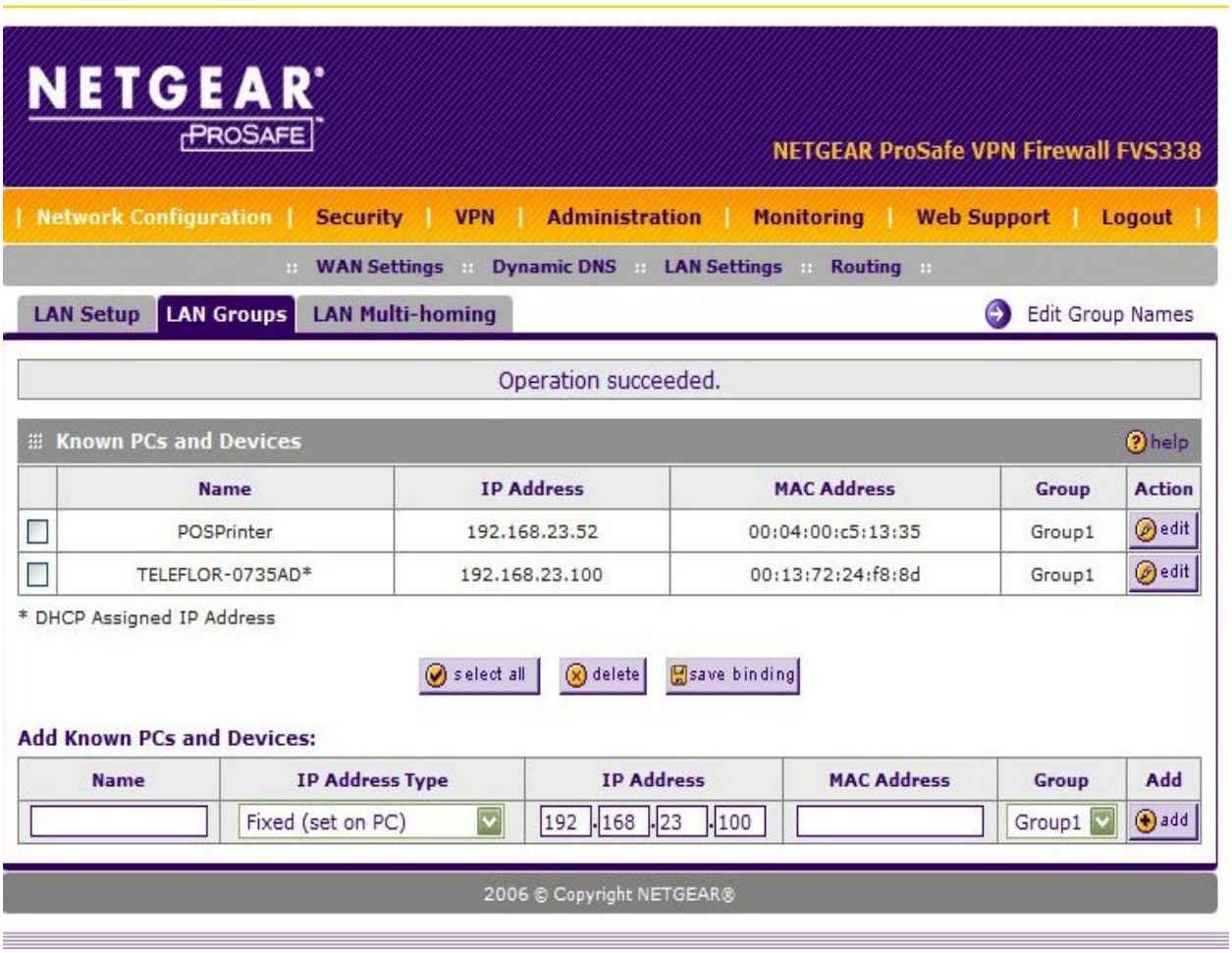
C: Click Apply

Step 6: Remote Management



1. In the top menu bar, click "Administration".
2. In the sub menu bar, click "Remote Management".
3. Check the "Yes" button under "Allow Remote Management".
4. Click "Apply" to complete the change.

Step 7: Groups and Hosts



Note: In this section, it is necessary to configure the FVS338 based on how the NICS have been configured. All network cards connected to the FVS338 should be auto-detected on this screen. If not, press “Refresh”. If all adapters still do not show, check the NIC's for functionality.

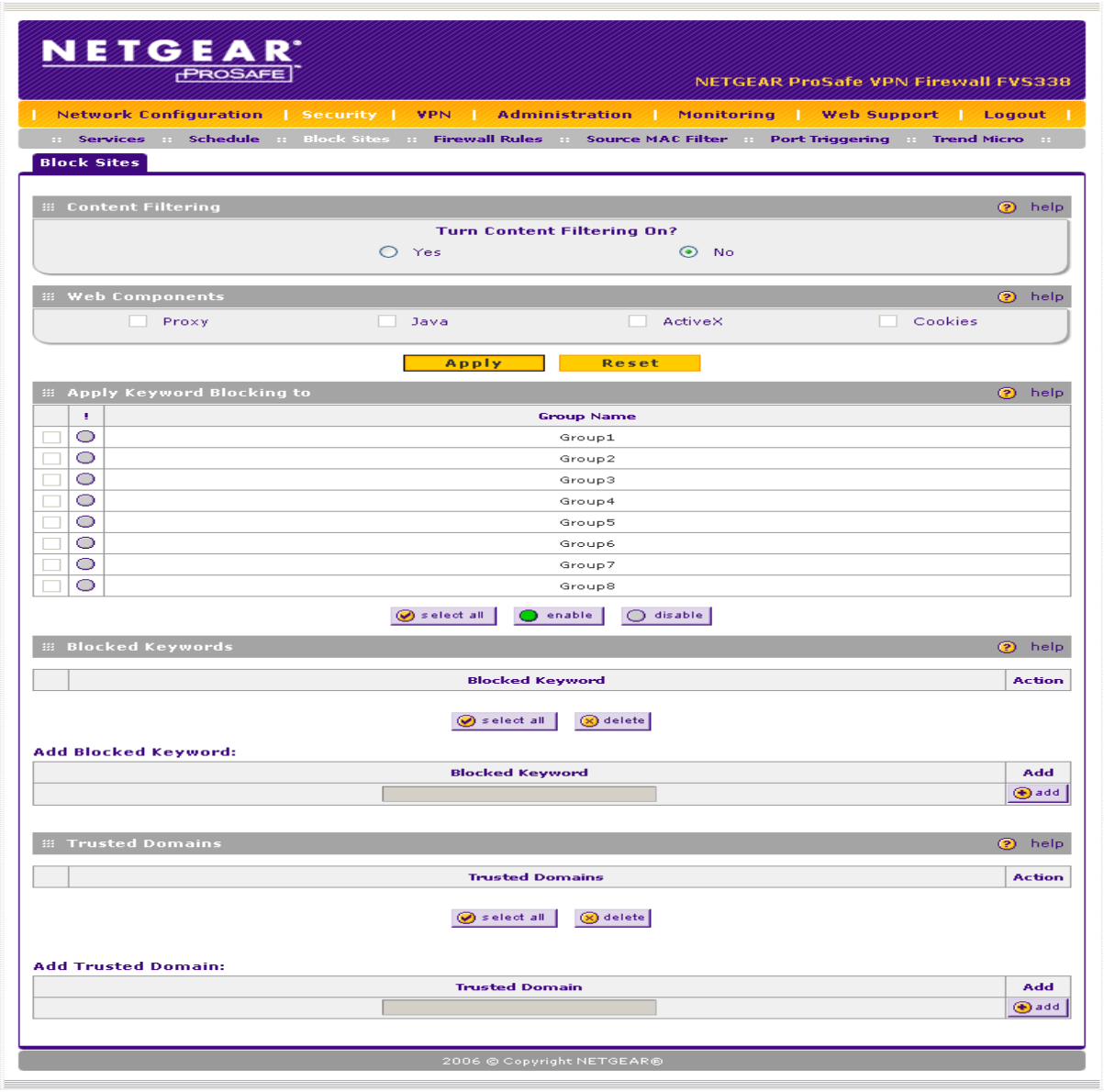
1. In the top menu bar, select "Network Configuration".

2. Using the drop down menu under "IP Address Type", select "Reserved".
   a. Reserved – The NIC will be given the same IP via DHCP with each renewal, based on its MAC Address

   b. Fixed – You have set the address statically for the NIC. (This removes that address from the DHCP scope, avoiding potential IP address conflicts.)

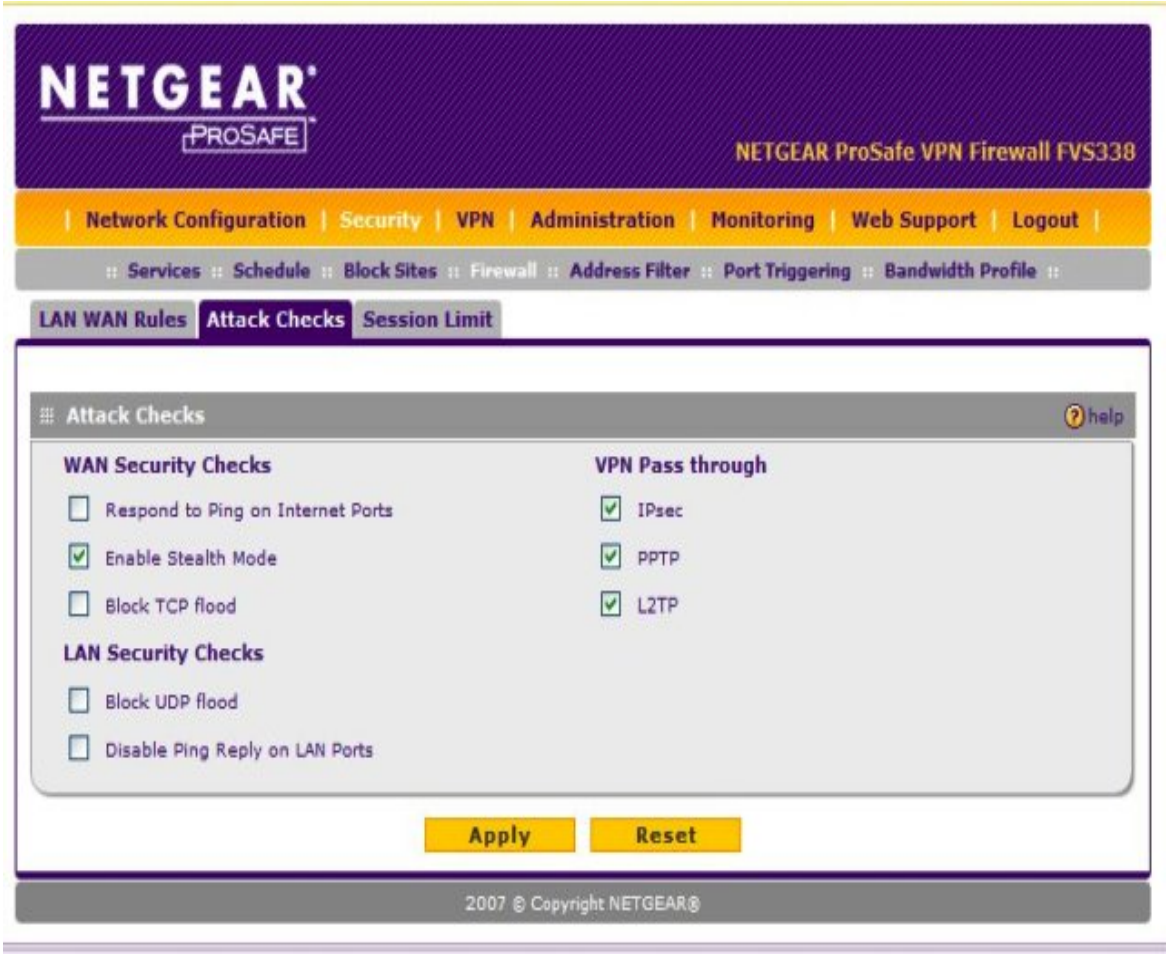
3. Select "Reserved".

Step 8: Block Sites



1. In the top menu bar, select "Security".
2. In the sub menu bar, select "Blocked Sites".
3. Leave all settings at default.

Step 9: Rules



1. In the top menu bar, select "Security".

2. In the sub menu bar, select "Firewall Rules".

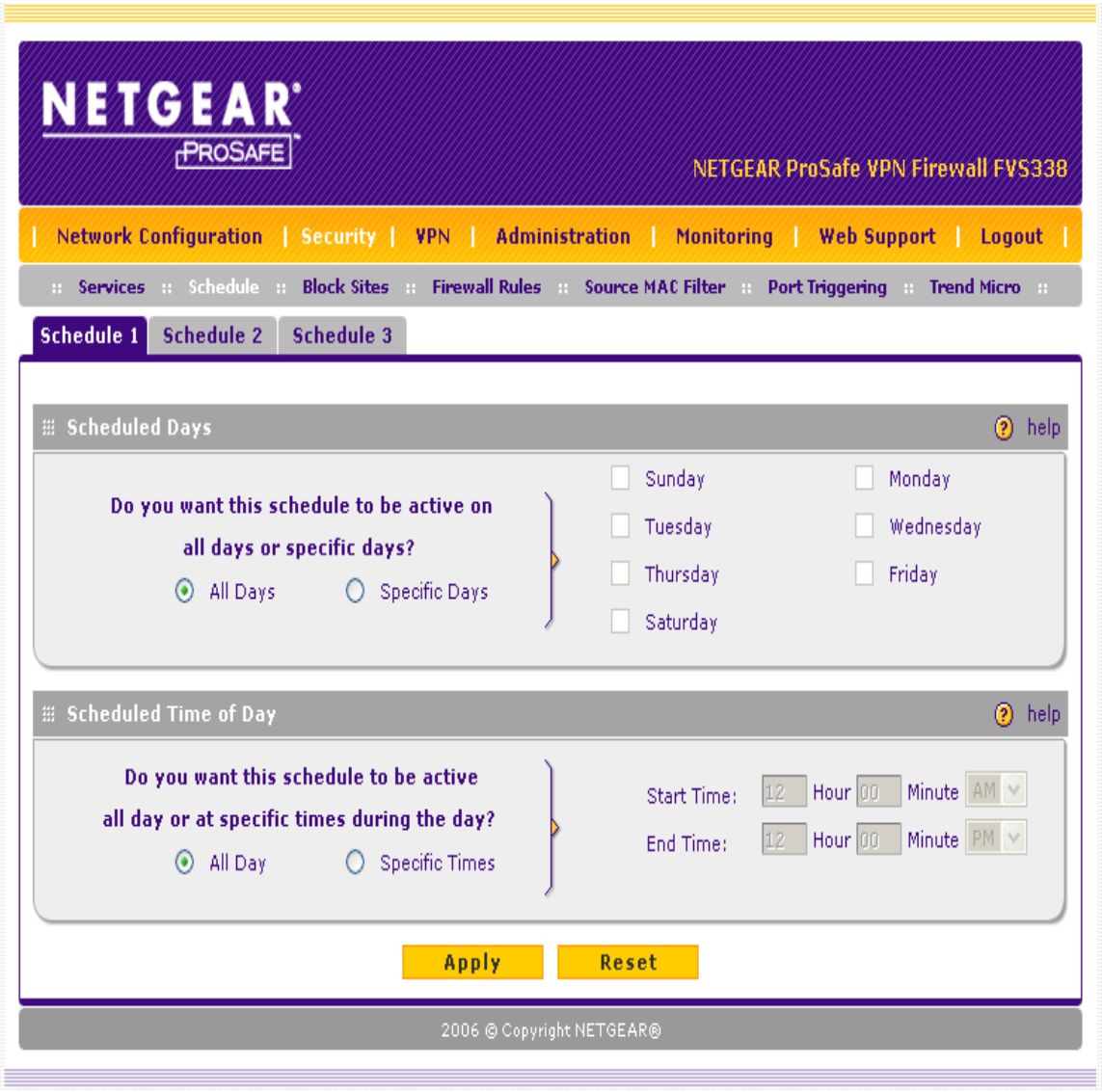
3. Click the tab labeled "Attack Checks".

4. Under the "WAN Security Checks" column, uncheck all rules but “Enable Stealth Mode”. This reduces unfortunate instances where the FVS338 thinks it is being hacked due to high traffic volume (ex: DovePOS on Mother’s Day) and shuts down the WAN connection

5. Under the VPN Pass through column, enable all three options (IPsec, PPTP, and L2PT).

6. Click on Apply.

Step 10: Schedule



1. In the top menu bar, select "Security".

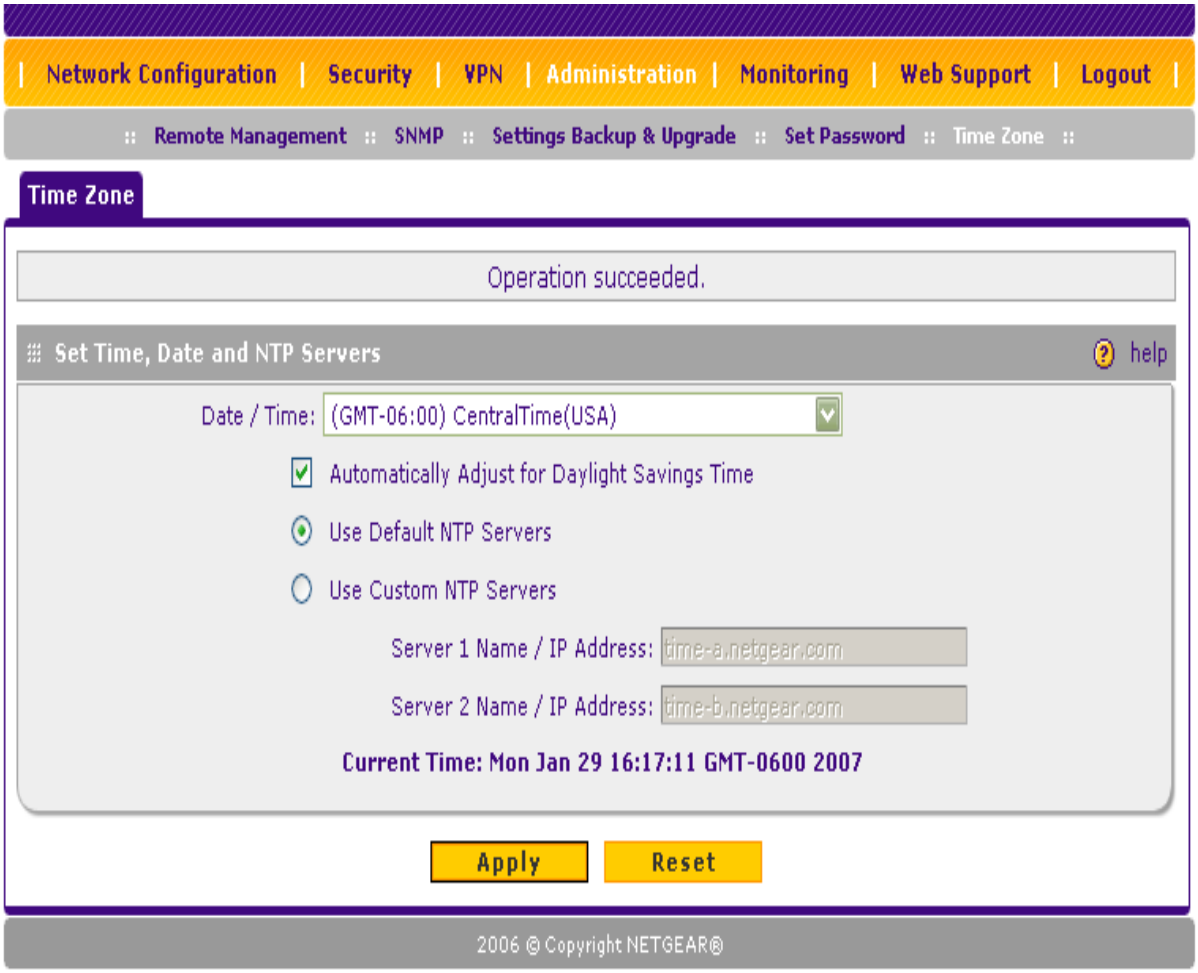
2. In the sub menu bar, select "Schedule".

3. Ensure that 'All Days" is selected unless the shop owner specifies a schedule for workstation internet access.

4. Click "Apply" when finished.

Note: These settings are important for instances where logs must be examined. Time is always a factor.

Step 11: Time Zone



1. In the "Date/Time" Box, select the correct time zone.

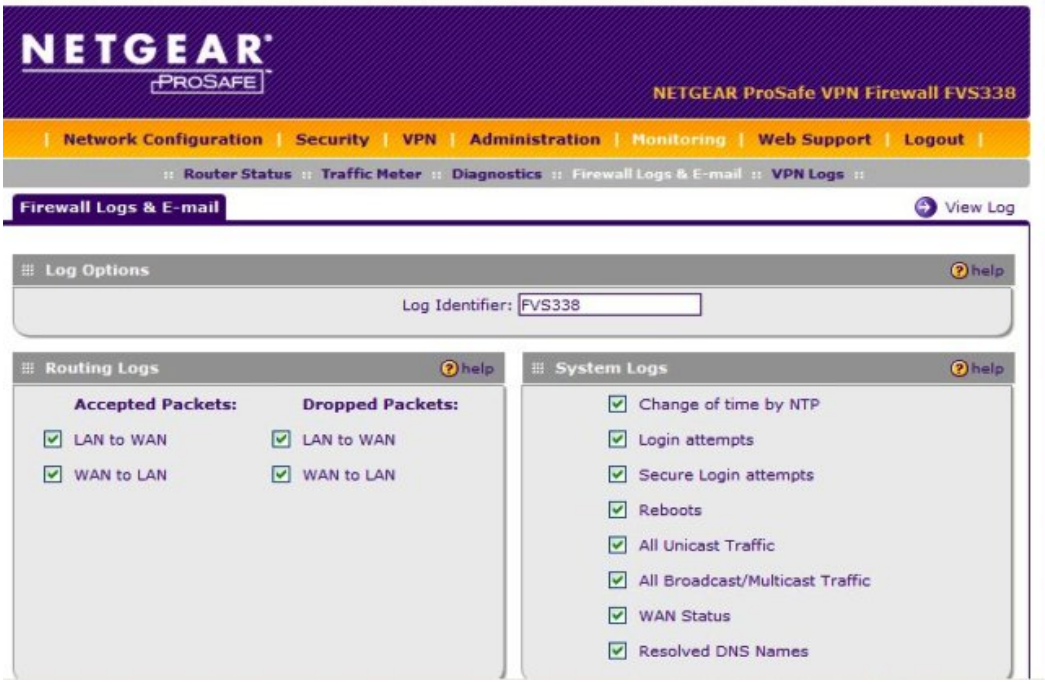
2. Check "Automatically Adjust for Daylight Savings", (unless you happen to be in one of the two areas of the USA that doesn't follow Daylight Savings Time).

3. Ensure that "Use Default NTP Servers" is selected.

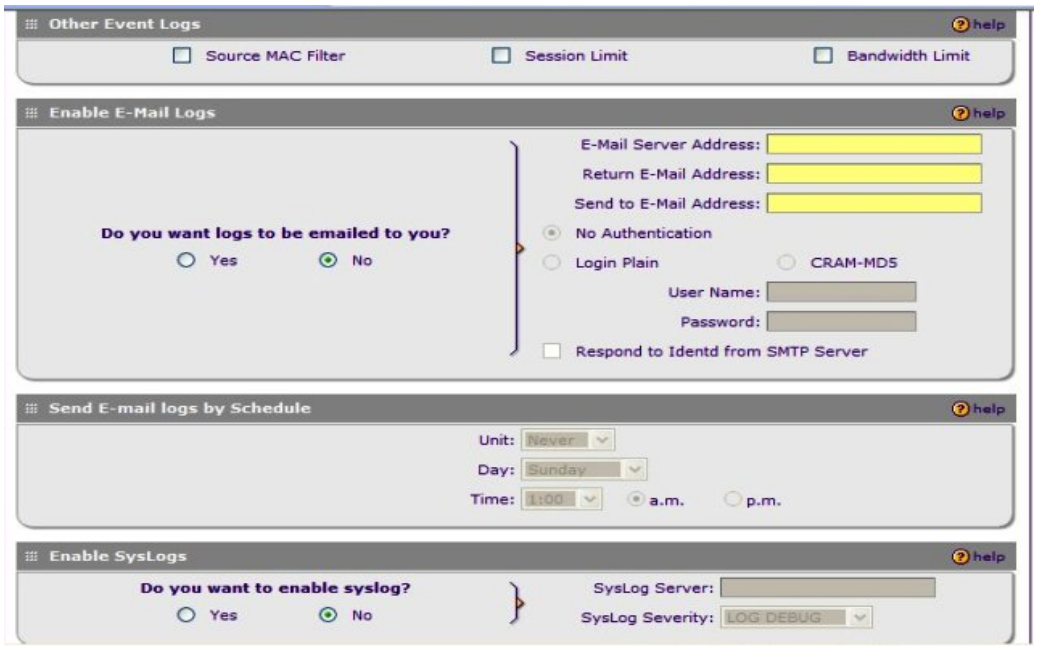
4. Click "Apply" when finished.

Note: These settings are important for instances where the logs must be examined.

Step 12: Logs & Email



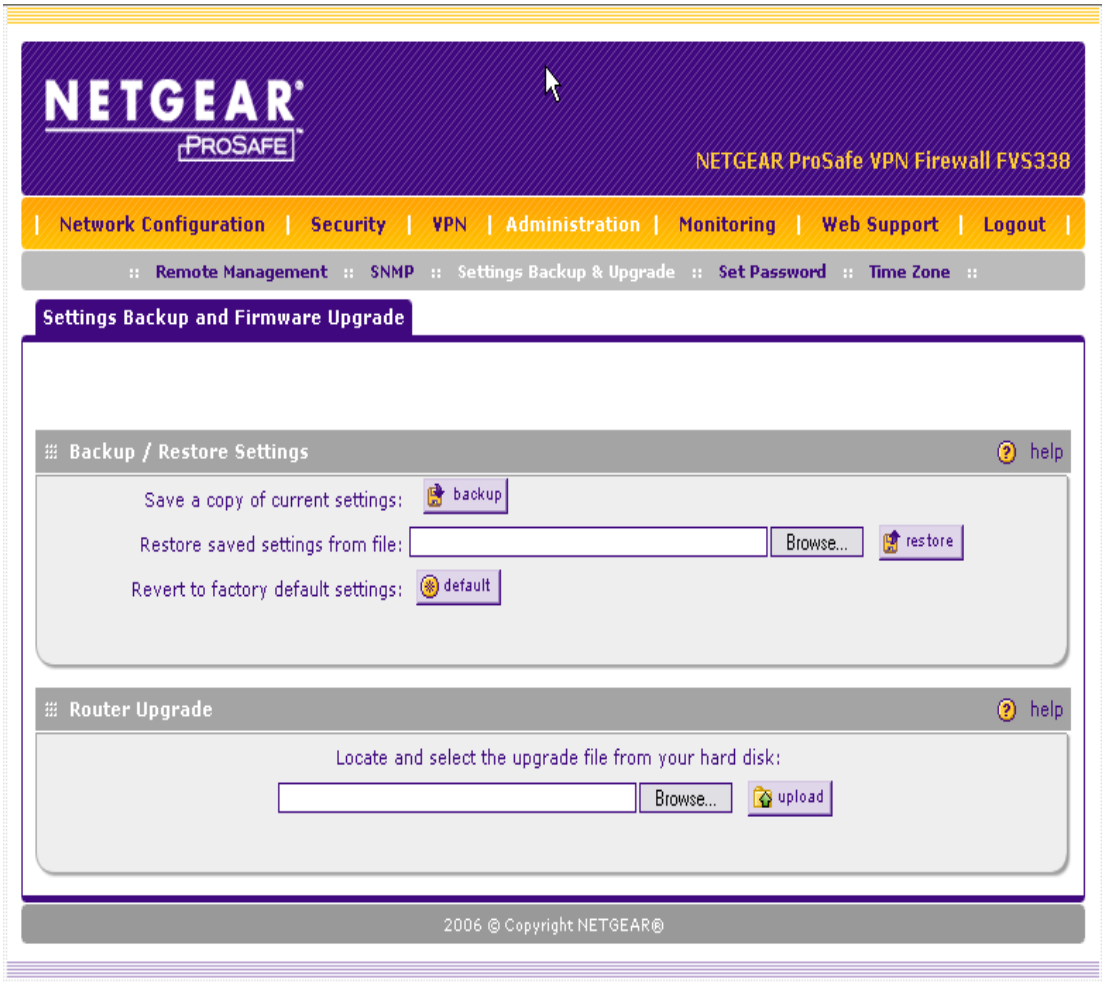
1. In the top menu bar, select "Monitoring".
2. In the sub menu bar, select "Firewall Logs & E-mail".



3. Enable all logging inclusions, except “Allow Policies”. This is helpful in getting the right information into the logs so technicians can better assist the florist should problems arise.

3. Click "Apply" when finished.

Step 13: Settings Backup



Saving the Netgear FVS338 Router Configuration

1. In the top menu bar, select "Administration".
2. In the sub menu bar, select "Settings Backup & Upgrade".
3. Click the "Backup" button.
4. Save the file to the "E:\Hardware\NetGear" folder.

Step 14: Online Port Test

1. Go to https://www.grc.com/x/ne.dll?bh0bkyd2

2. Click on the "Proceed" button, at the bottom of the screen.

3. Click the button labeled "All Service Ports" this will run a test to determine which ports are open to the Internet.

4. All ports should show up green.

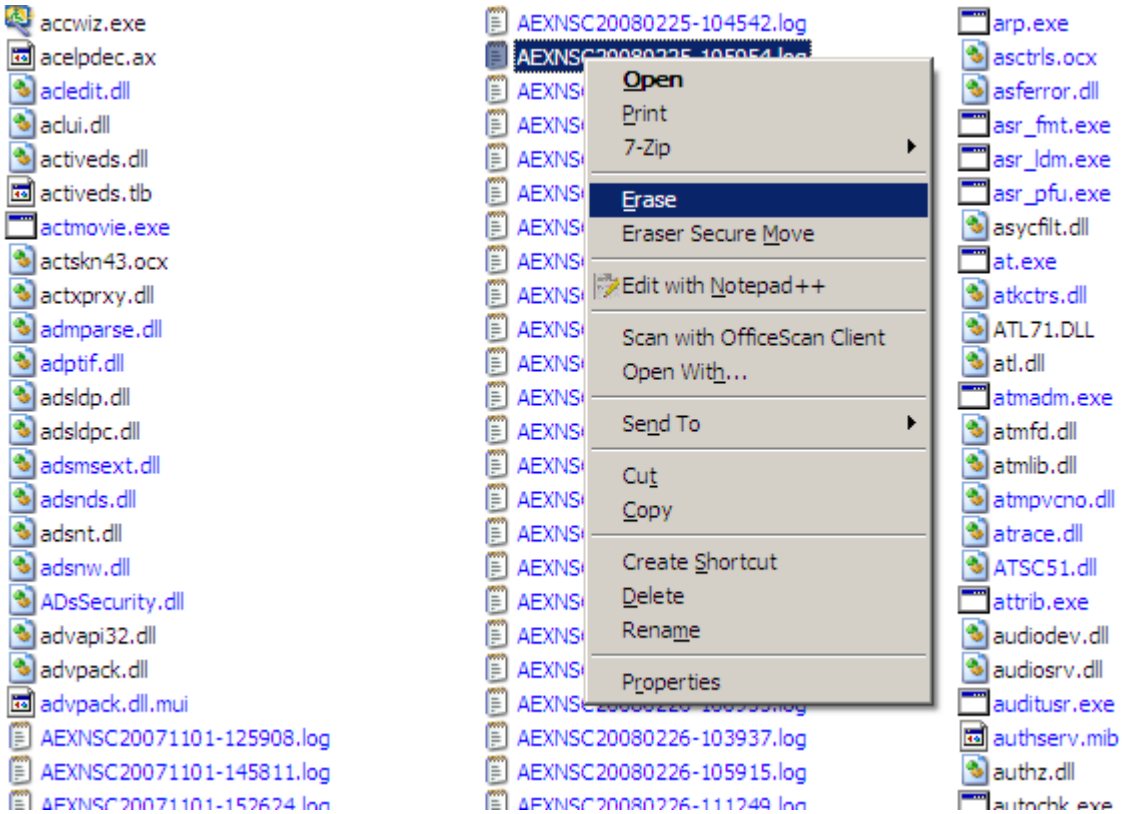
Using the Eraser Tool

PA-DSS 1.4.a
PA-DSS 1.5.c

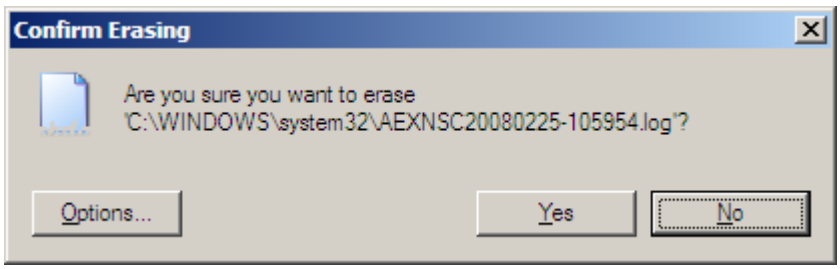
There are multiple ways to use the Erase application to securely delete your files. For advanced options or detailed instruction on how to completely wipe a hard drive refer to the Erase application's help file.

Below is the most basic instruction on how to delete files using this tool.

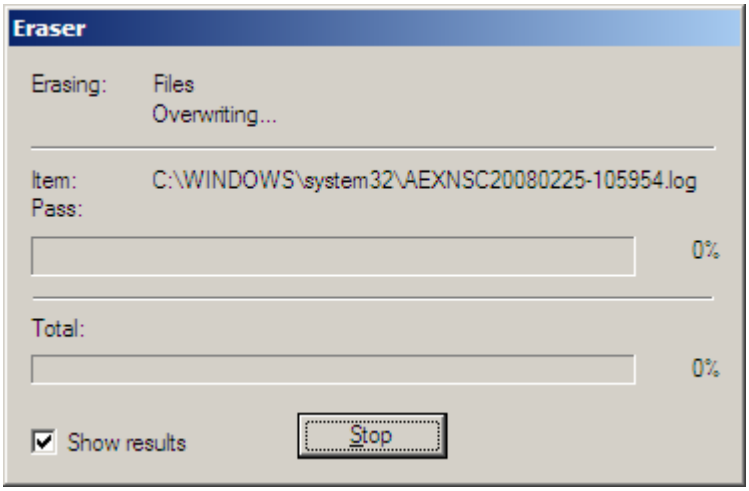
1. Using Windows Explorer navigate to the file(s) you wish to erase.



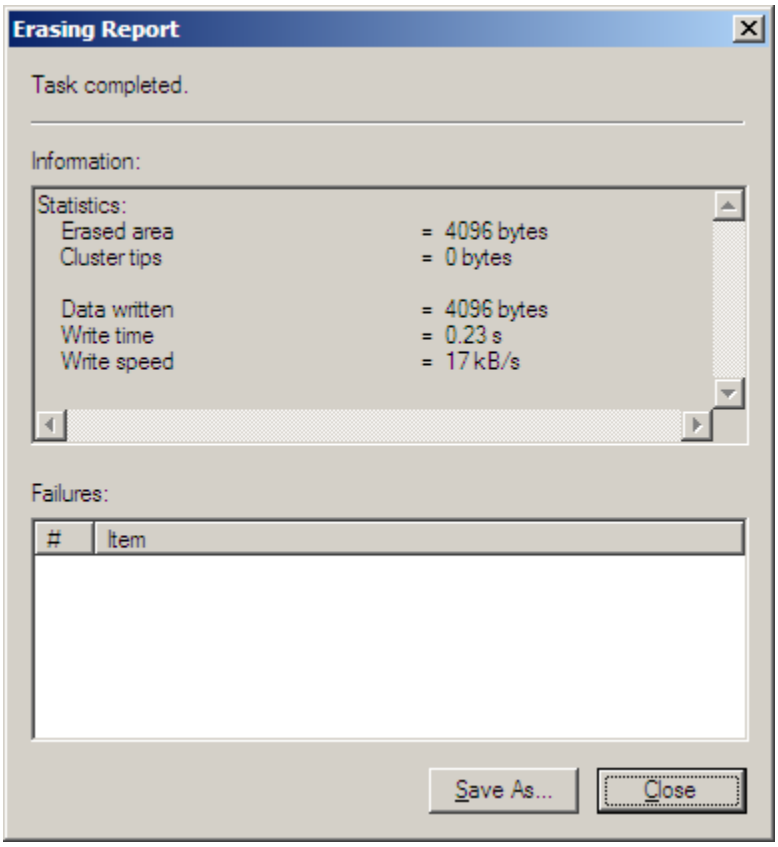
2. Right Click on the file; on the pop-up menu select Erase.



3. Click on Yes to delete the file; click no to cancel.



4. Once the erase process begins you have one last opportunity to cancel the deletion of the file by clicking the Stop button in the progress screen.



5. When the deletion is complete you are given the opportunity to save the deletion report. Click on Save as to save the report. Click Close to exit the application.

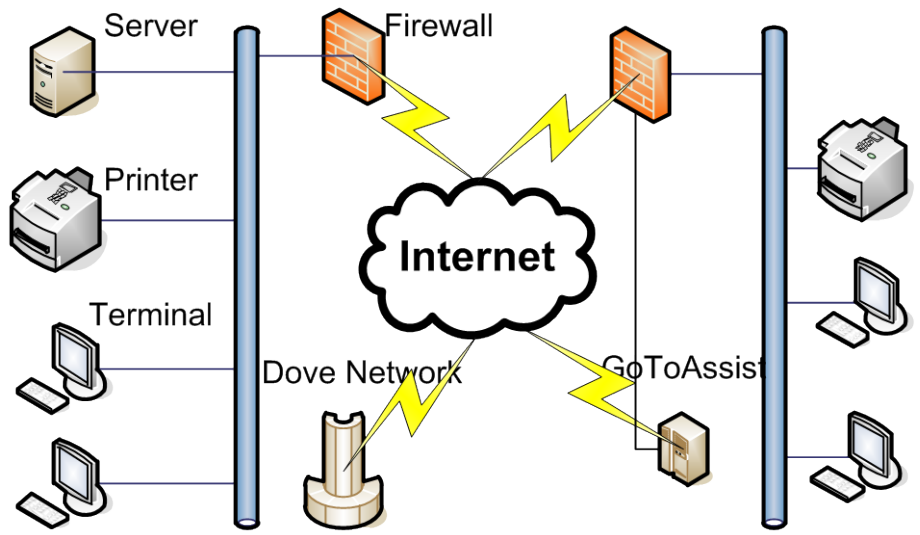
Dove POS Application Summary

PA-DSS Executive Summary

Software Vendor	Teleflora
Teleflora Contact Information:	
Teleflora Mailing Address	
Product Name	Dove POS
Product Version	5
Recommended OS:	Windows XP Professional
Traditional Marketplace:	Retail Florist

Typical Dove POS Network Topology

PA-DSS Executive Summary



A typical Dove POS shop consists of one store with two or three "terminals", a network printer, a Dove POS "server", and a Firewall to the internet.
Larger implementations may have multiple, physical locations, all interconnected via a VPN. In all cases, Dove POS "Terminals" are used to take purchases, and there is only a single Dove POS "Server" computer.

Dove POS Server
A Dell server running windows. Houses core database of the application. The central point for communications between Terminals and external entities (such as the Dove Network and Elavon). There is only ever one of these servers in a Dove POS "environment".

Dove POS Terminal
Windows PC running Dove POS software in "Client" mode. "Client" software offers minimal data storage, and connects to the Dove POS "Server" for all data communications and data storage. The Dove POS terminal is where a "sale" is taken at. Thus, magnetic stripe data, PANs, CVV and pin blocks almost always originate from these computers.
In the case of small shops, both the "Dove POS Server" and "Dove POS Terminal" will reside on the same computer.

Printer
Small business class network printer, usually one per location.

Firewall
Firewall with built-in VPN and LAN (switch) capabilities. Used to block traffic into and out of each shop, as well as establish VPN connections. One firewall per location. This firewall resides between the Dove POS LAN and either a “DSL Modem” or “Cable Modem”.

GoToAssist Third party website which Teleflora Customer Service (and the customer) use to establish a remote support session. Customer must initiate these encrypted / password protected sessions. File transfers are possible between Customer network and Teleflora Customer Support.

Dove Network
Teleflora’s set of web services. CC magnetic stripe data, PANs, CVV, and Debit pin blocks all may be transmitted from the Dove POS Server, to the Dove Network via an authenticated, SSL encrypted link. Only PANs may be transmitted from the Dove Network back to the Dove POS Server. Only Dove POS Servers communicate with the Dove Network.

Elavon
Elavon “SSL @dvantage” network interface. CC Swipes, PANs, CVV and Debit pin blocks all are transmitted from the Dove POS Server, via an SSL encrypted connection. No CC information is transmitted from Elavon, to the Dove POS server.

Data Backup

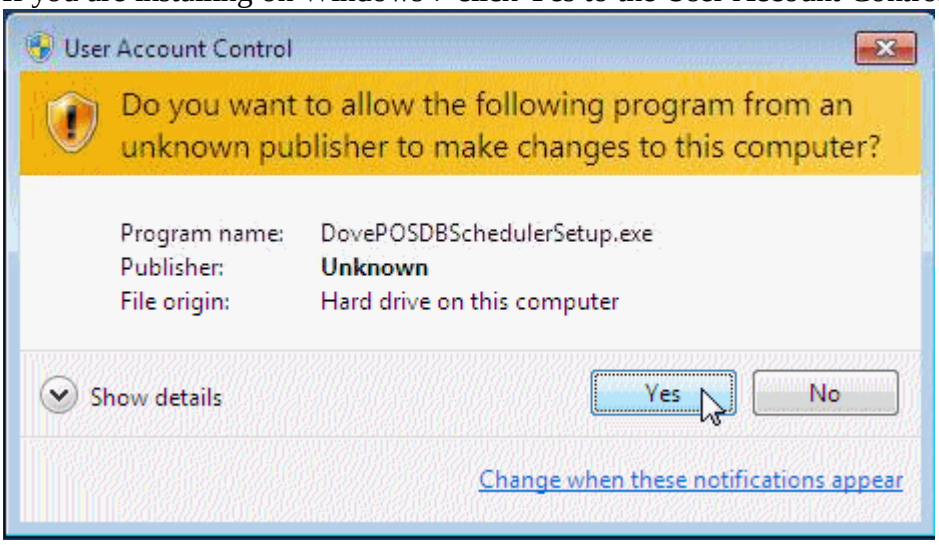
DovePOS Database Scheduler 1.0.0

Installing the DovePOS Database Scheduler

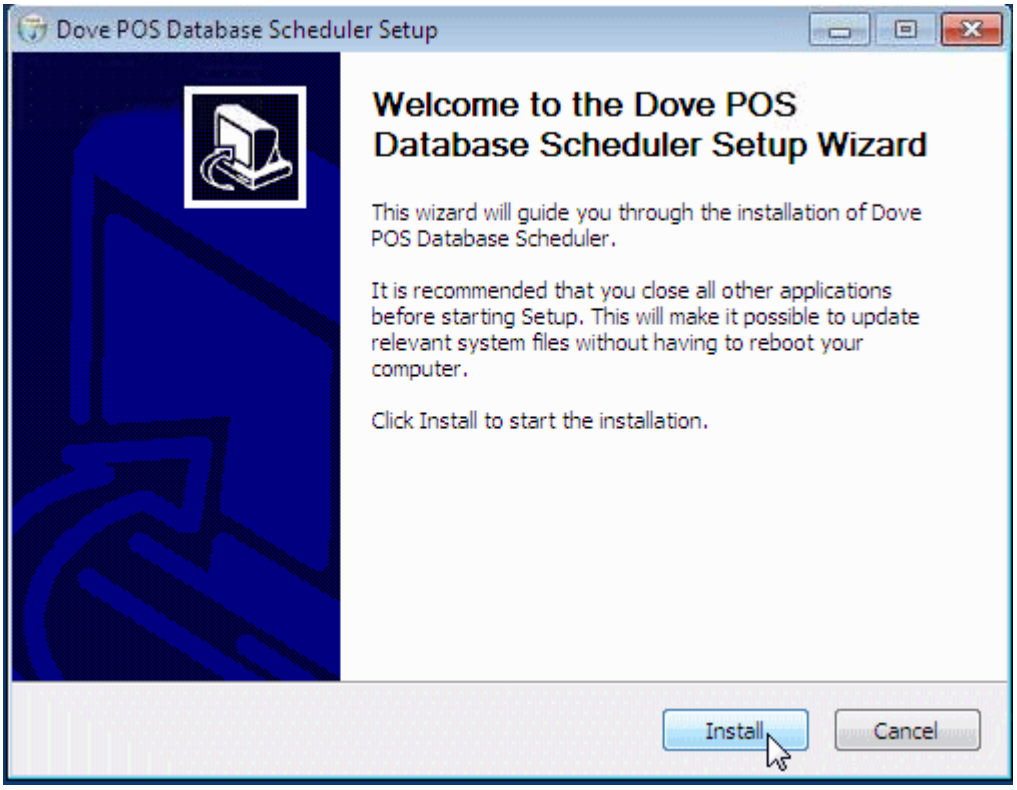
Note: The scheduler automatically installs with DovePOS versions 5.1 and above.

1. Double Click the DovePOSDBSchedulerSetup.exe file.

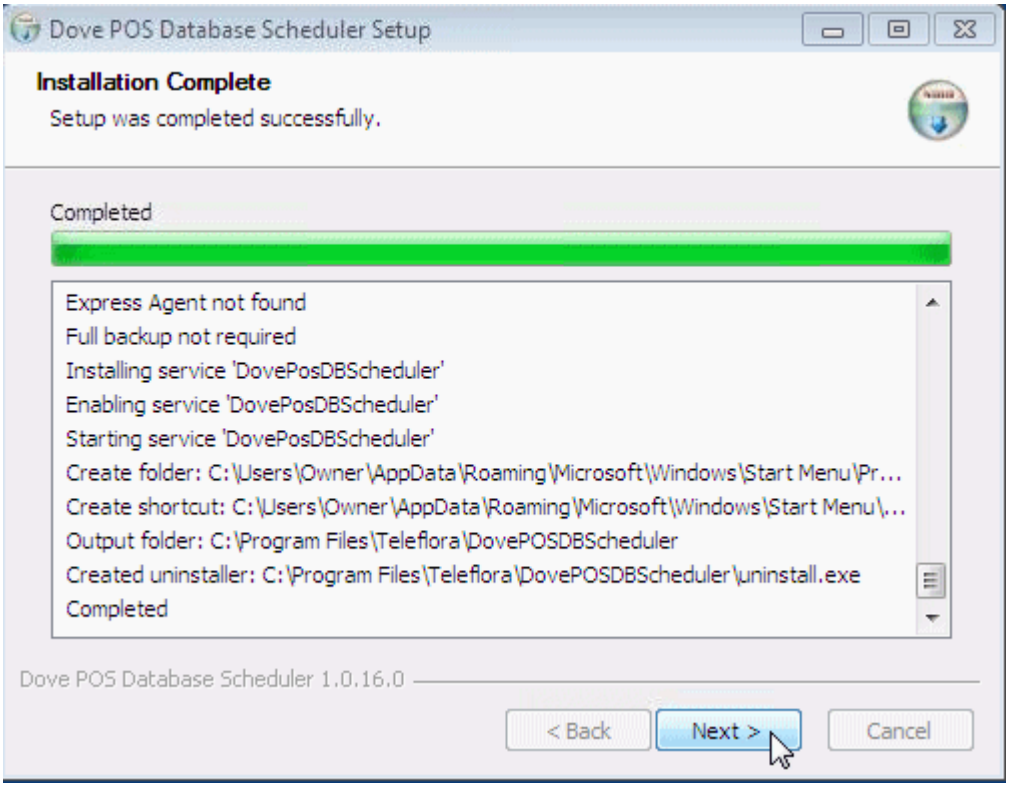
2. If you are installing on Windows 7 click Yes to the User Account Control prompt.



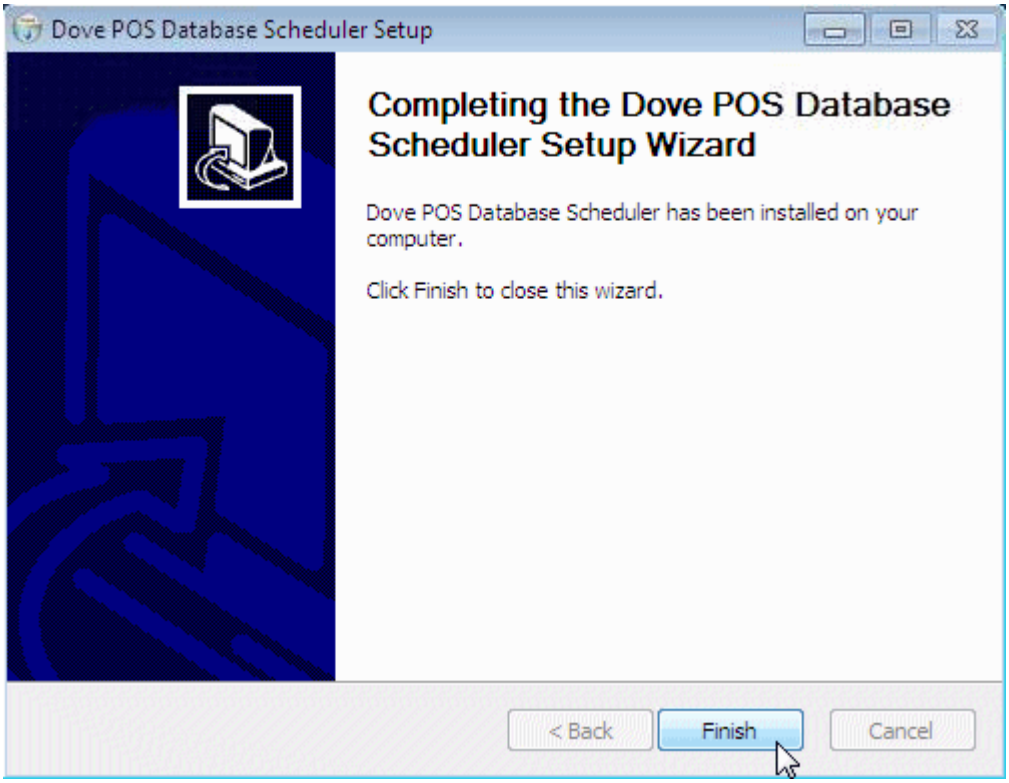
3. Click Install.



4. Once the installation is finished click Next.



5. Click Finish.

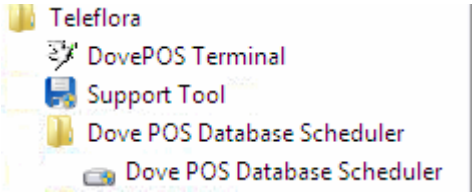


6. Remove any backup software previously used. This can include Automatic Backup Pro, Retrospect, or the backup utility created by Teleflora for the image discs (known as Chad's Backup).

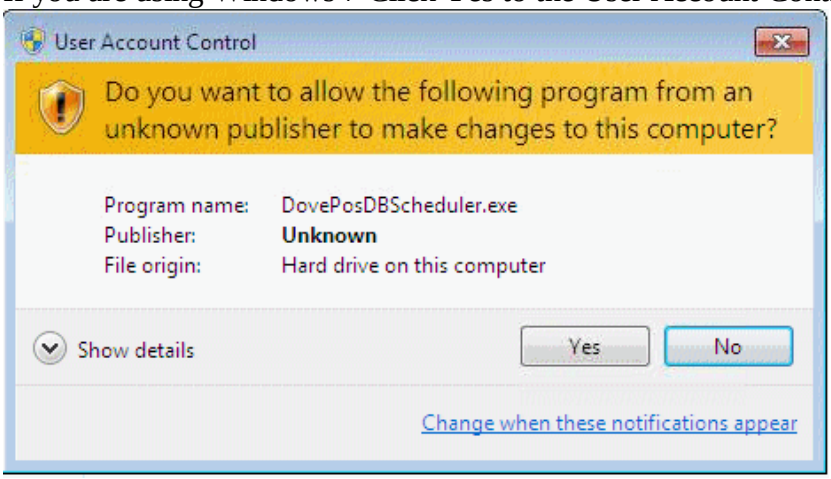
   Note: All drive's must be formatted as NTFS to work correctly with the DovePOSDBScheduler!

Configuring the DovePOS Database Scheduler

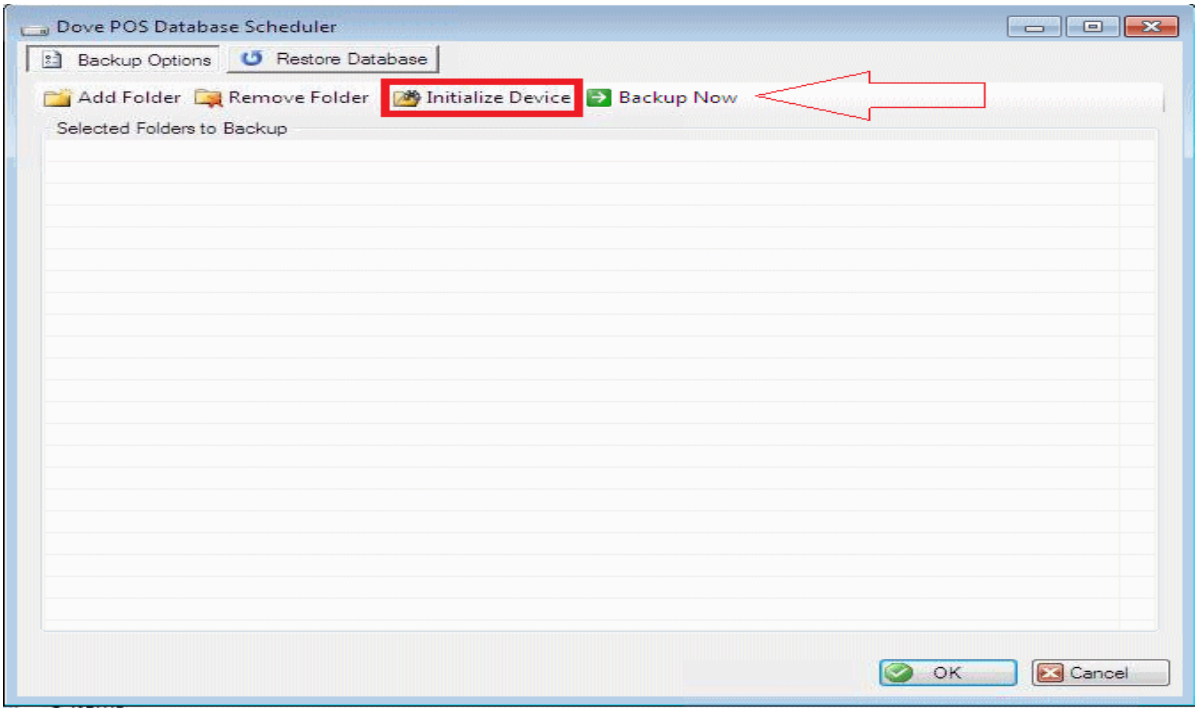
1. Click Start > Programs or All Programs > Teleflora > Dove POS Database Scheduler > Dove POS Database Scheduler



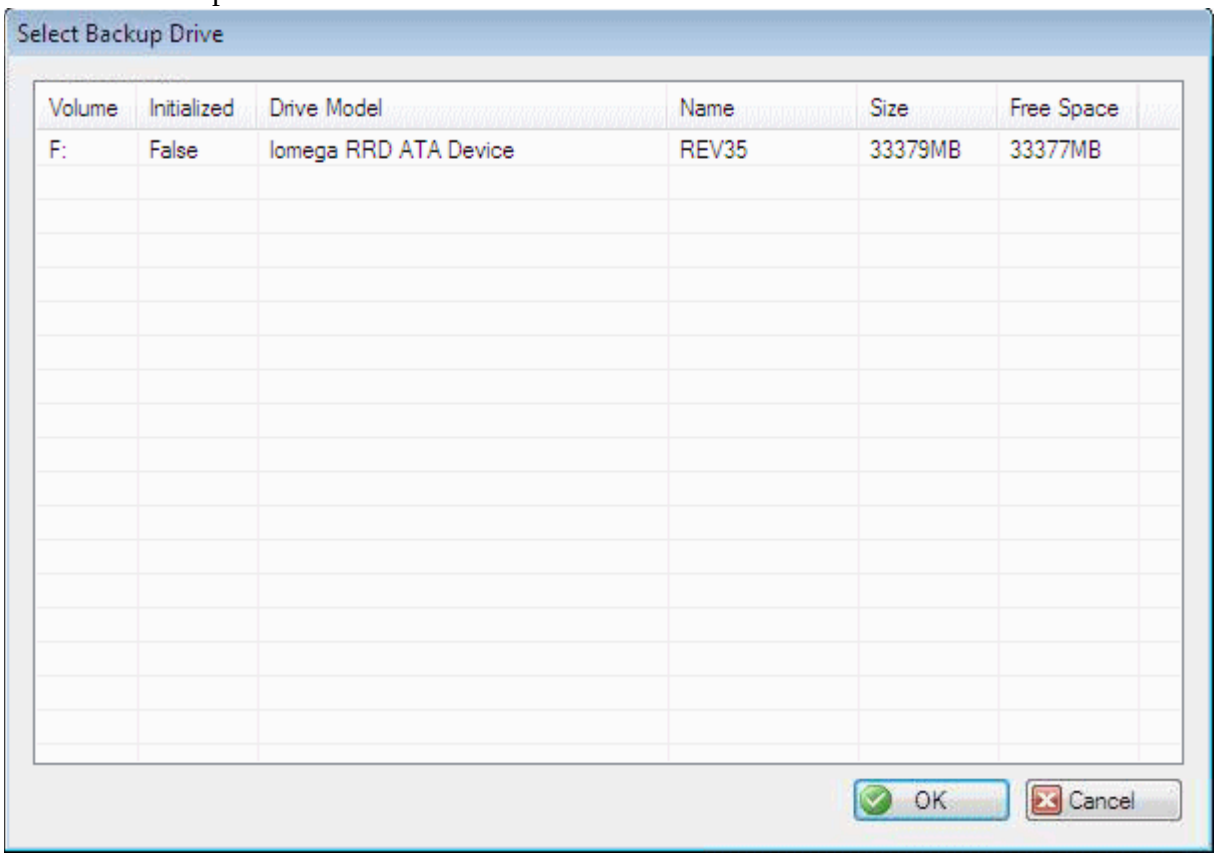
2. If you are using Windows 7 Click Yes to the User Account Control prompt.



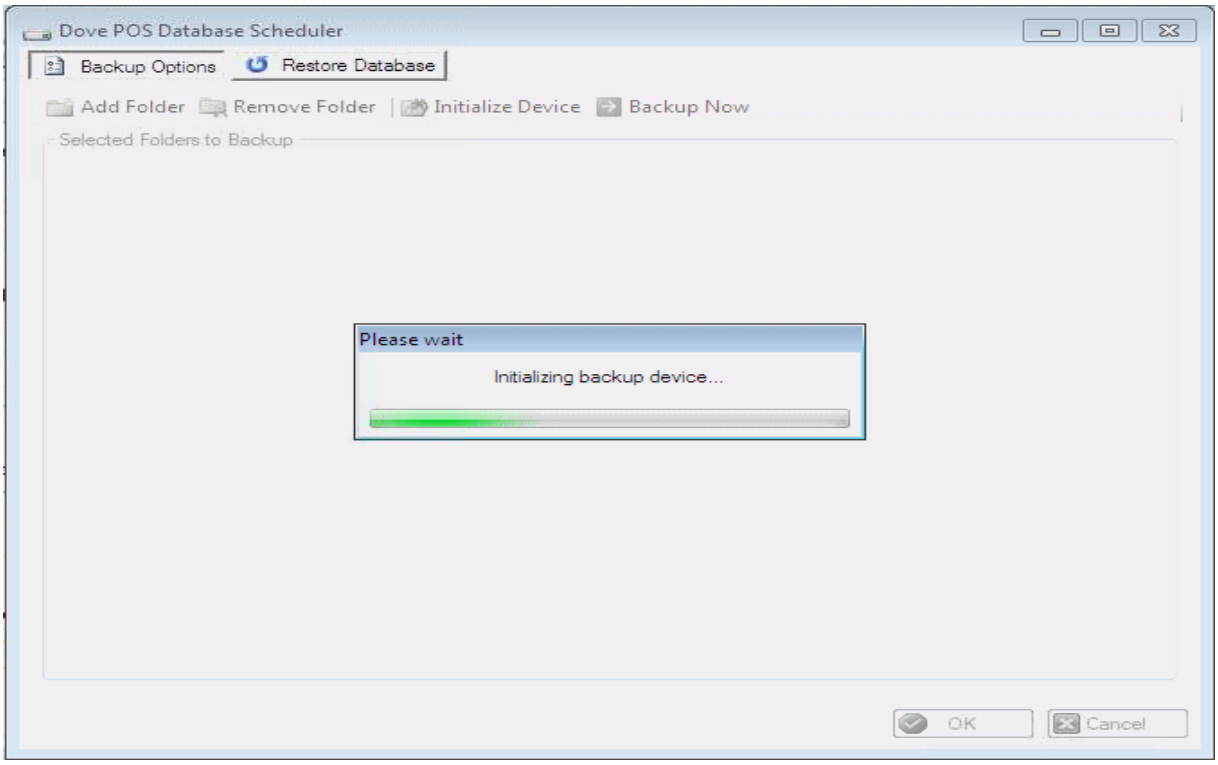
3. After the main window loads click on Initialize Device



4. Select the backup drive to be used and then click OK.

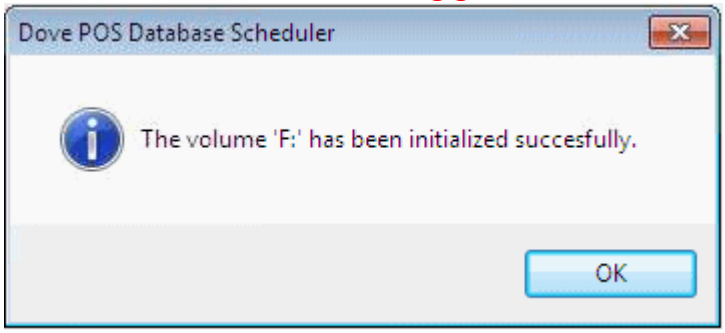


5. Wait for the device to be initialized.

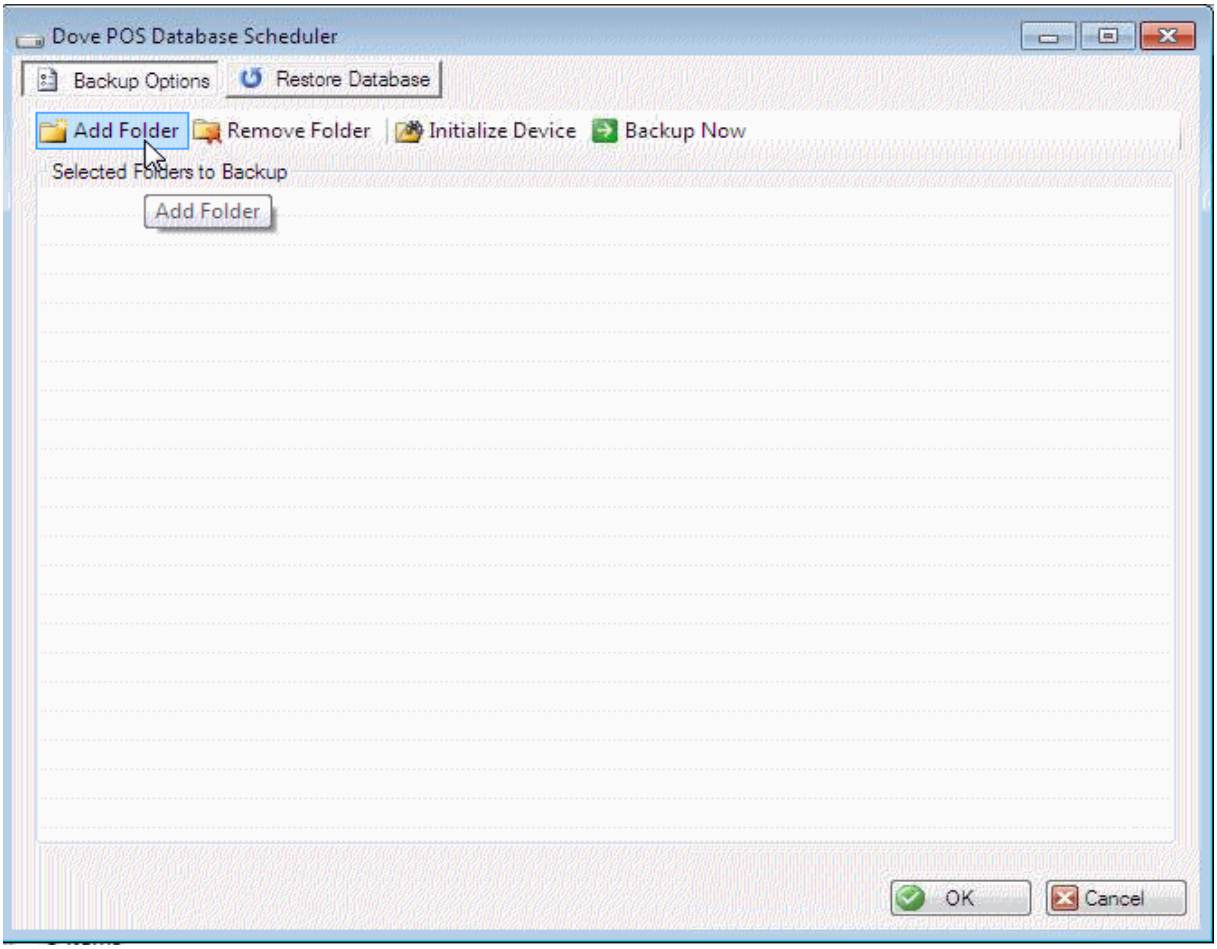


Note: All drive's must be formatted as NTFS to work correctly with the DovePOSDBScheduler!

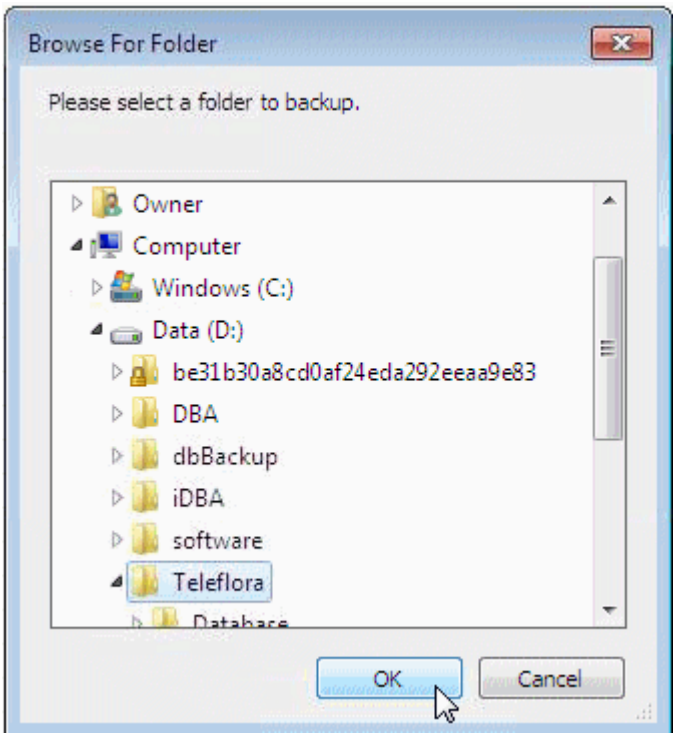
6. Click OK to the successfully initialized device.
   Note: This action will create a 26gig file on the device, this file must not be deleted.



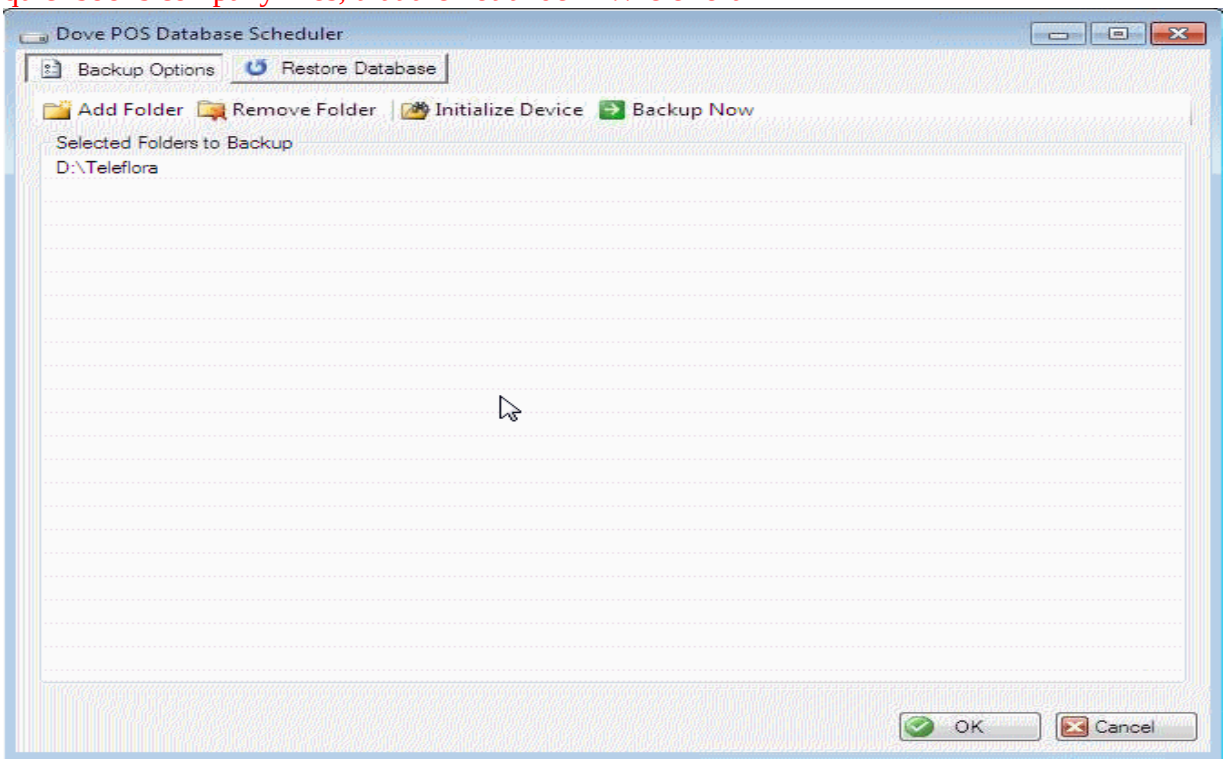
7. Click Add Folder



8. Browse to D:\Teleflora and click OK



9. Verify the D:\Teleflora is a listed folder and click OK the scheduler is now configured for backups. Note: Make sure to add any other folders that need to be backed up, such as quickbooks company files, that are not under D:\Teleflora

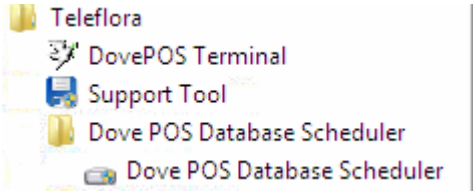


10. Repeat steps 1 – 9 under Configuring the DovePOS Database Scheduler for all backup media.

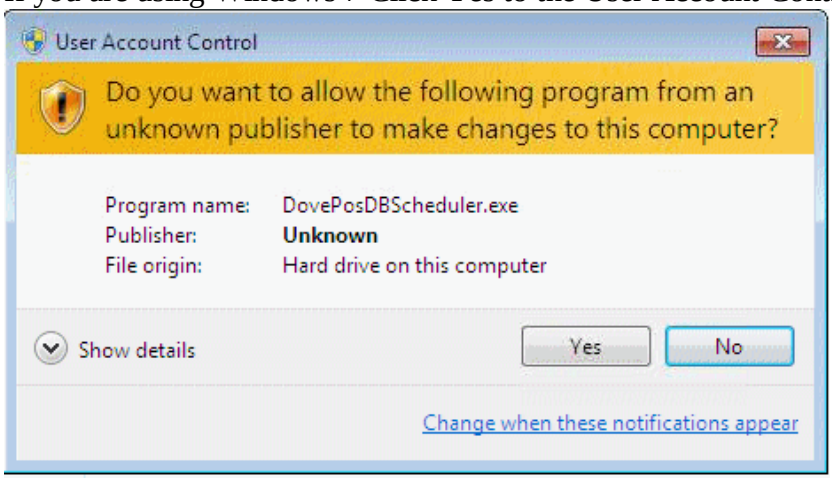
Note: Once complete one of the backup's media must remain plugged into the computer or in the tape drive.

Performing a Manual Backup

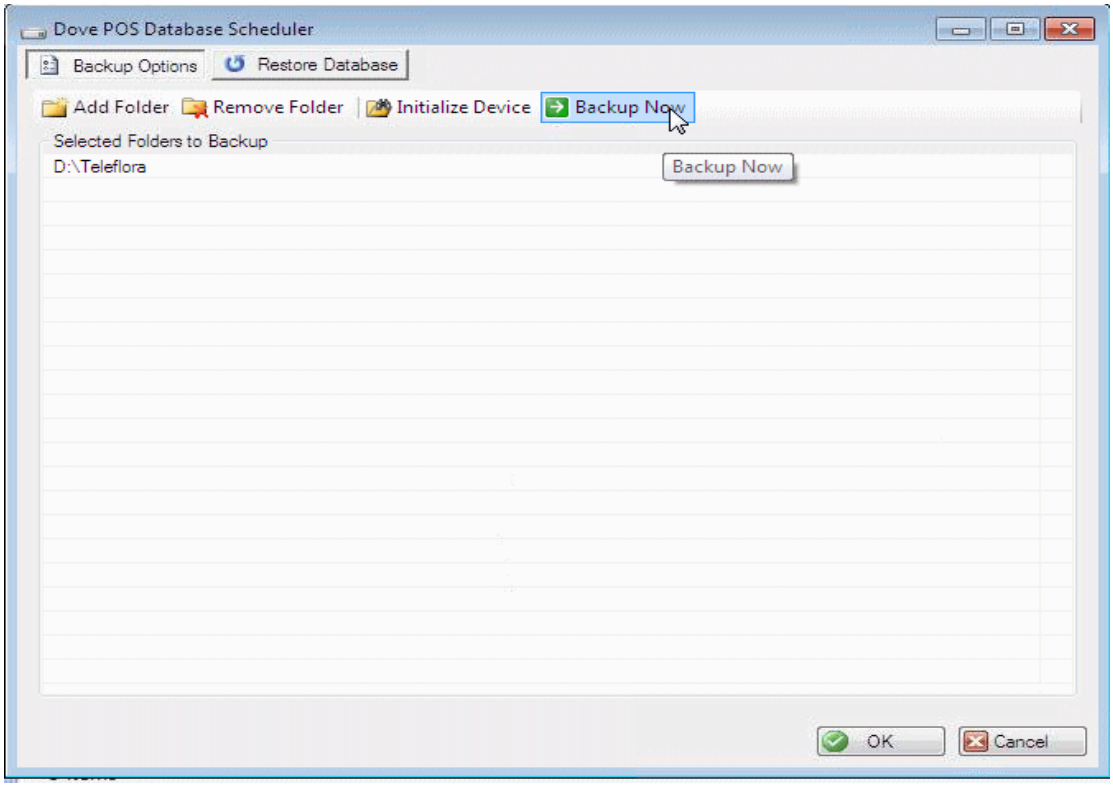
1. Click Start > Programs or All Programs > Teleflora > Dove POS Database Scheduler > Dove POS Database Scheduler



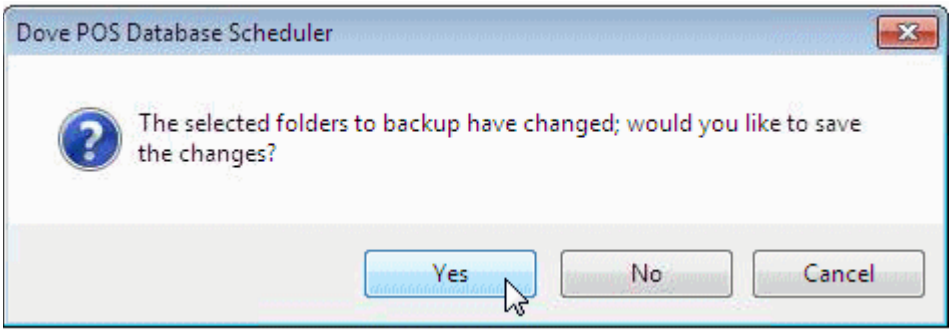
2. If you are using Windows 7 Click Yes to the User Account Control prompt.



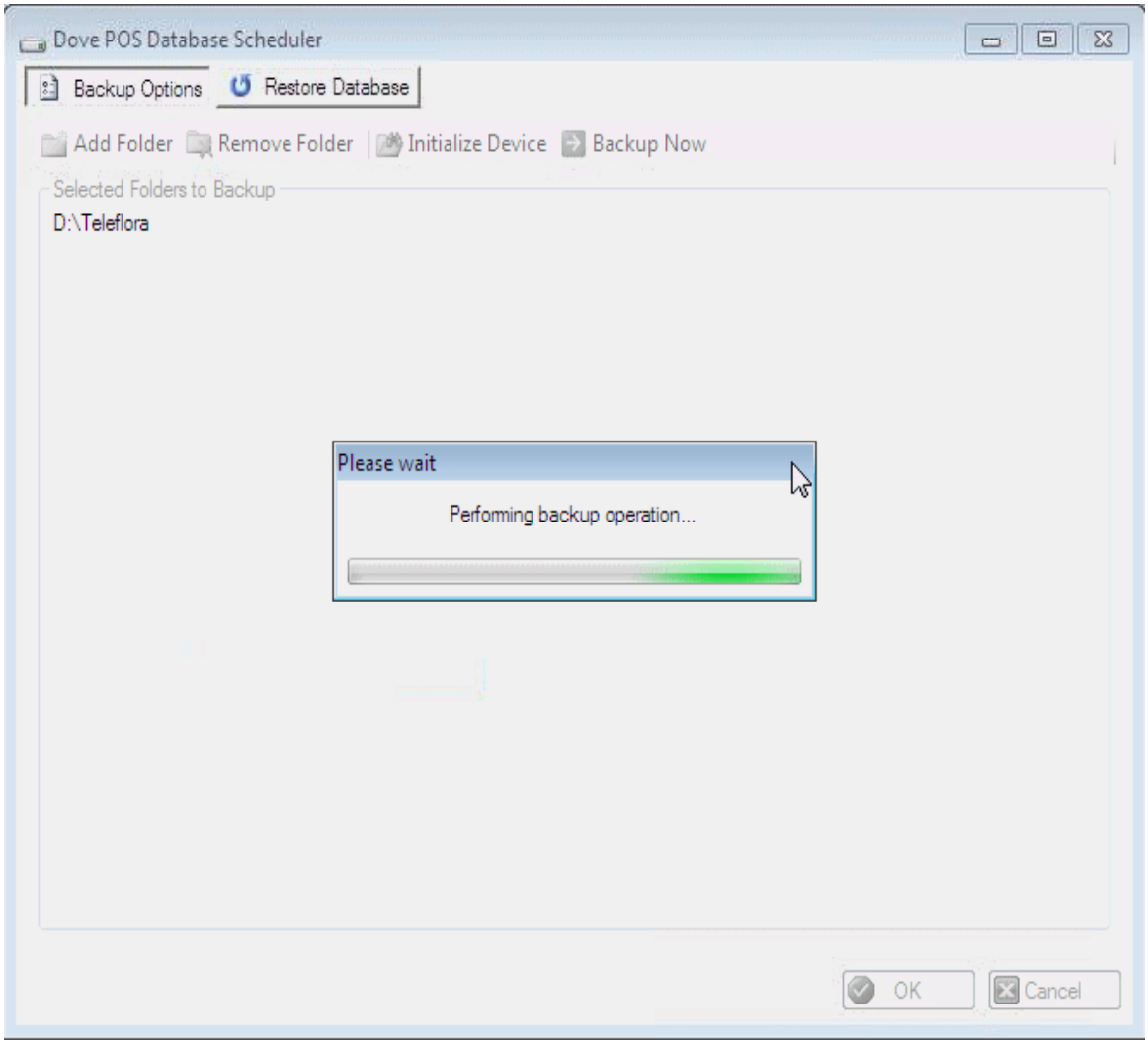
3. Click Backup Now



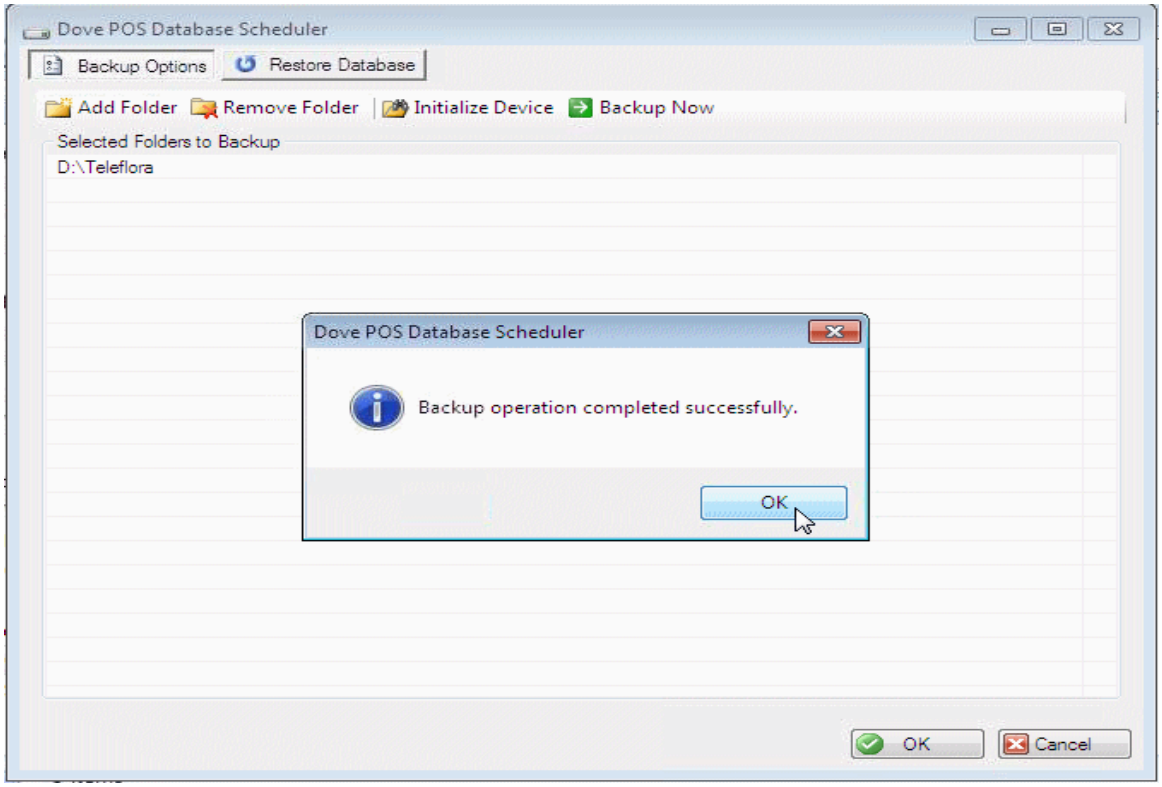
4. If you have made changes to the folders such as adding or removing any, click Yes to the prompt to save changes.



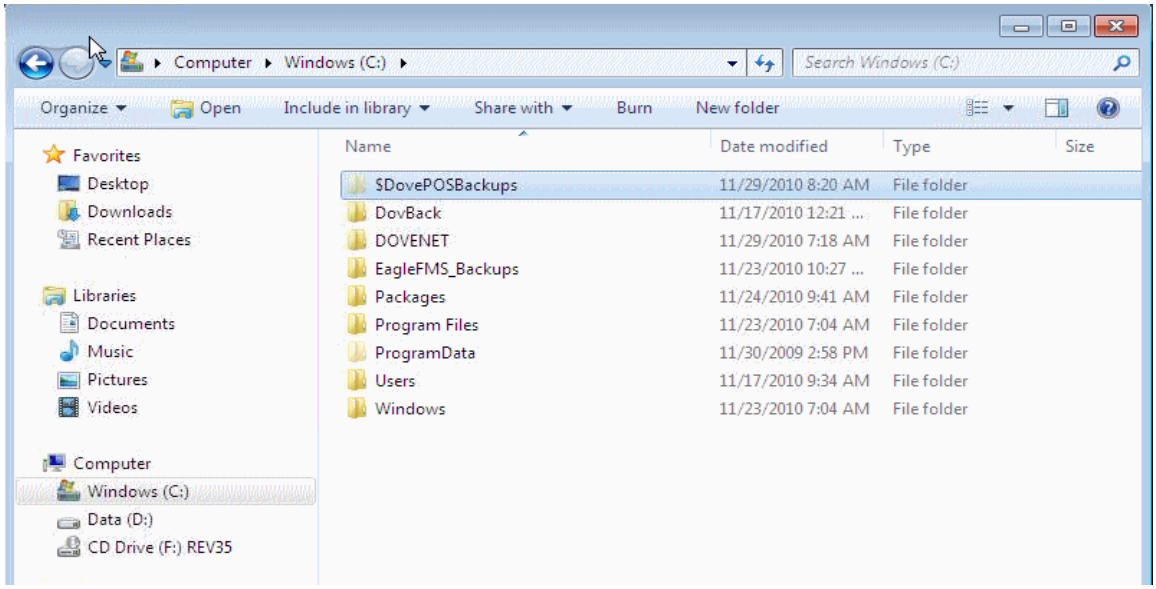
5. Wait for the backup operation to complete.

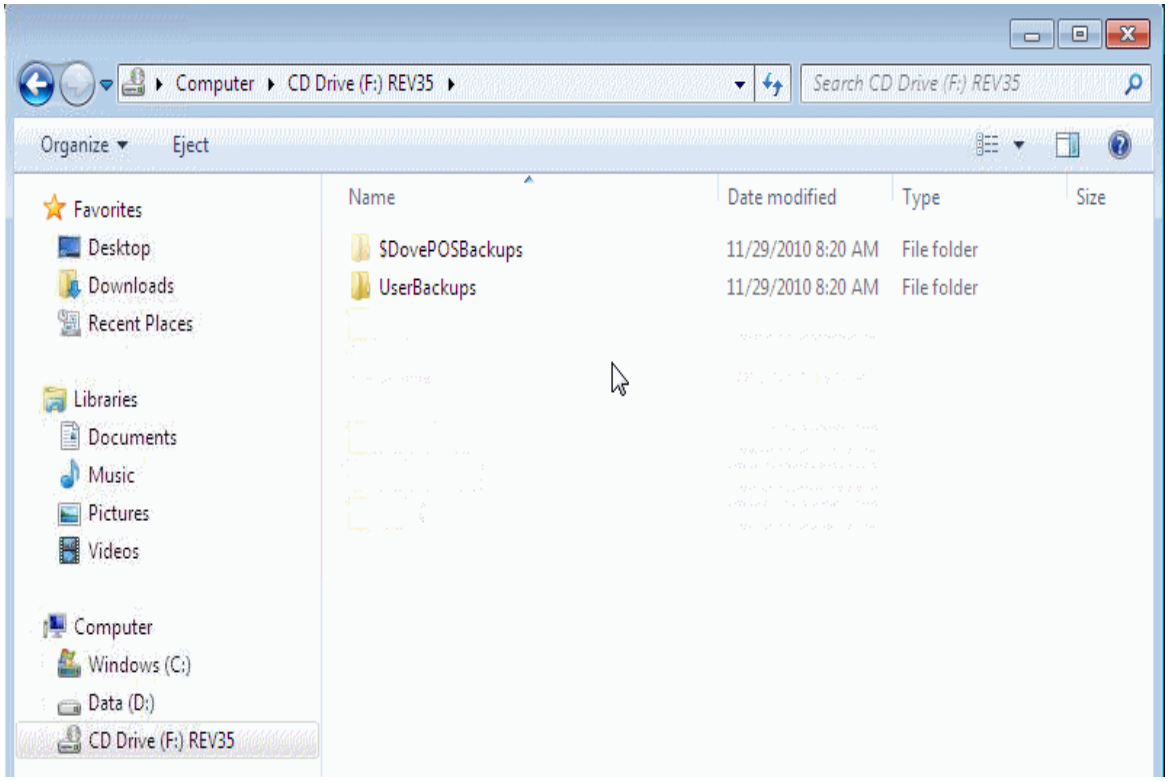


6. Once complete click OK

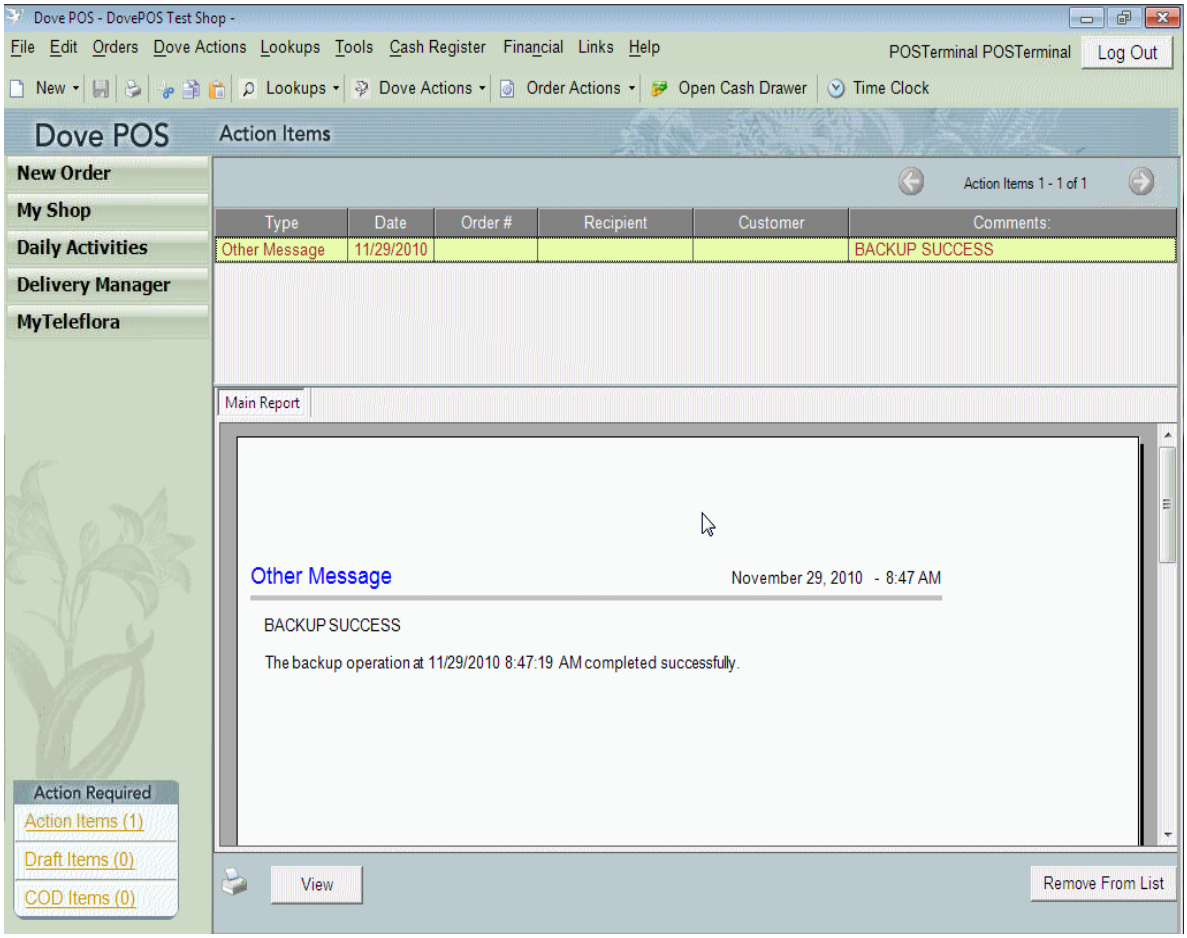


7. There are hidden files under the windows root drive and backup media's root drive you can look for to make sure the backup copied files. Note: These files are hidden and should never be changed or removed manually!





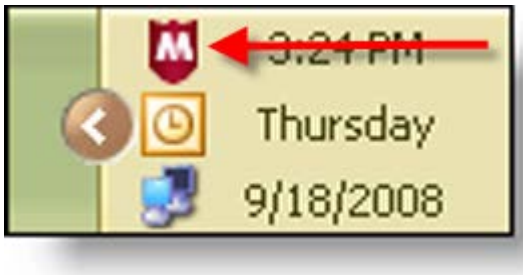
8. Log into Dove POS to see an action item for a successful backup.


Dove POS - DovePOS Test Shop -
File Edit Orders Dove Actions Lookups Tools Cash Register Financial Links Help
POSTerminal POSTerminal
Log Out
New
Lookups
Dove Actions
Order Actions
Open Cash Drawer
Time Clock
Dove POS
Action Items
New Order
My Shop
Daily Activities
Delivery Manager
MyTeleflora
Action Items 1 - 1 of 1
Type
Date
Order #
Recipient
Customer
Comments:
Other Message
11/29/2010
BACKUP SUCCESS
Main Report
Other Message
November 29, 2010 - 8:47 AM
BACKUP SUCCESS
The backup operation at 11/29/2010 8:47:19 AM completed successfully.
Action Required
Action Items (1)
Draft Items (0)
COD Items (0)
View
Remove From List

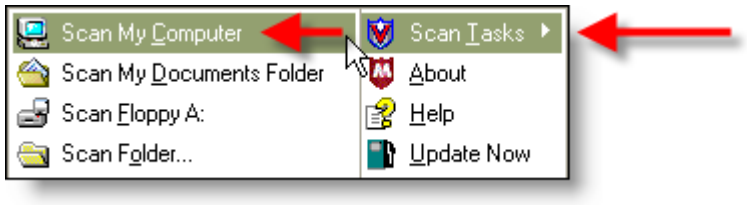
Manually System Virus Scan Using McAfee Total Protection Suite for Small Business

By default, we have the program configured to automatically run this scan silently within the first 15 minutes after the computer is powered up. In some instances it may be necessary to manually initiate the scan. This document will provide you with the necessary steps for manually performing a complete system virus scan.

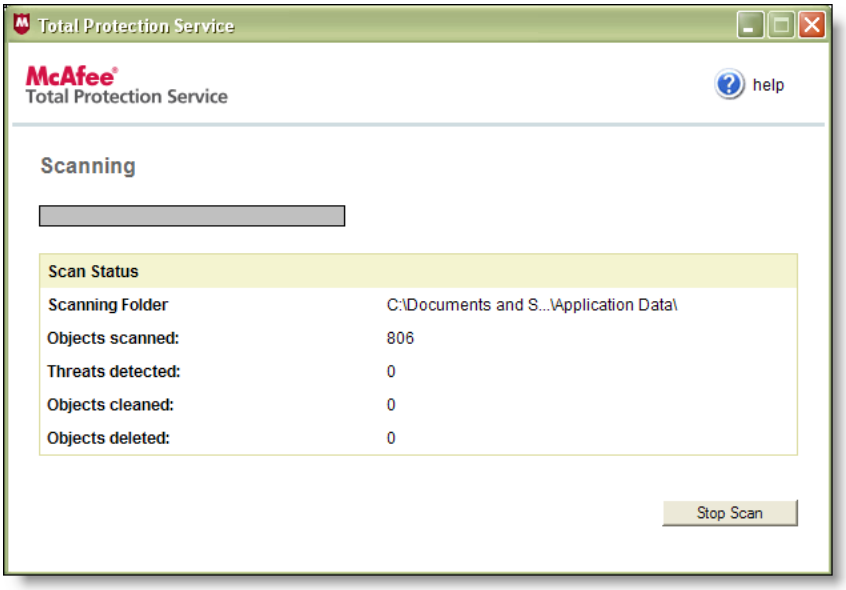
1. Locate the McAfee icon (red shield with a white M in the middle) in the system tray at the bottom right corner of the screen.



2. Right click the McAfee icon and select ‘Scan Tasks’, then select ‘Scan My Computer’.



3. The virus scan will now begin and you will see a screen similar to the one below.



4. The virus scan is now running. The remainder of the process is automated so no further user input is required.

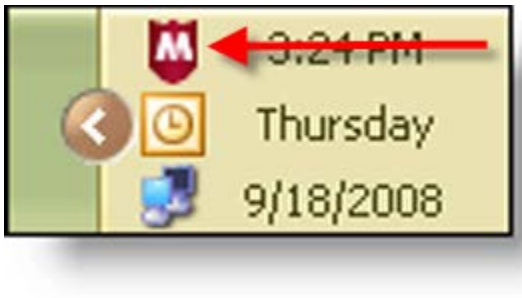
5. Once the scan is complete the results will display on the screen. To view the report details, click the 'Report' button at the bottom of the screen. When finished, click the 'Close' button. The scan is now complete.

Manual Update for McAfee Total Protection Suite for Small Business

This document will provide you with the necessary steps for manually updating the McAfee Virus Definition (DAT) File. McAfee generally releases new DAT files daily and we have configured the program to automatically check for new updates every 4 hours. In the event you find a machine that does not have the most recent update, follow the steps below to install the latest DAT file.

Updating the Virus Definition (DAT) File is a relatively simple process. There are two options available for checking for new updates.

1. Locate the McAfee icon (red shield with a white M in the middle) in the system tray at the bottom right corner of the screen.

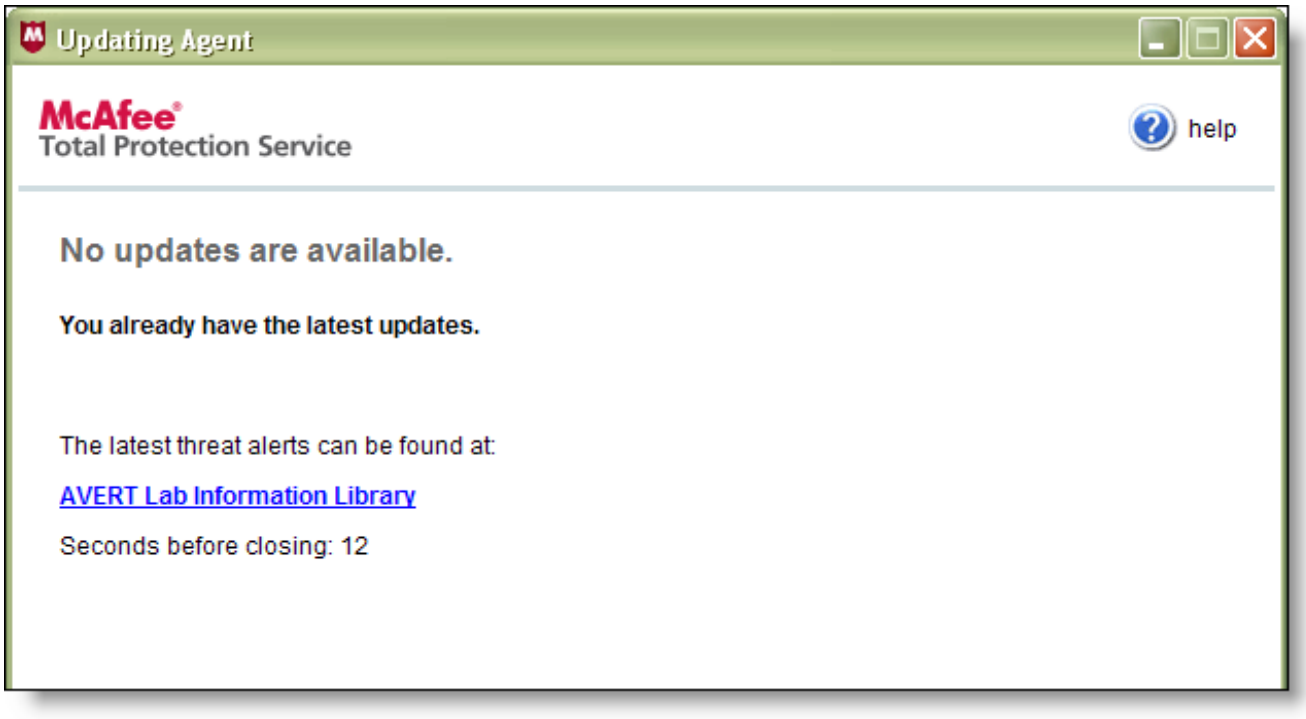


2. At this point you have two options:

    - Option 1: Double click the McAfee icon to initiate the update process.
    - Option 2: Right click on the icon and choose ‘Update Now’.

3. Regardless of which option you choose, you will see the following screen:

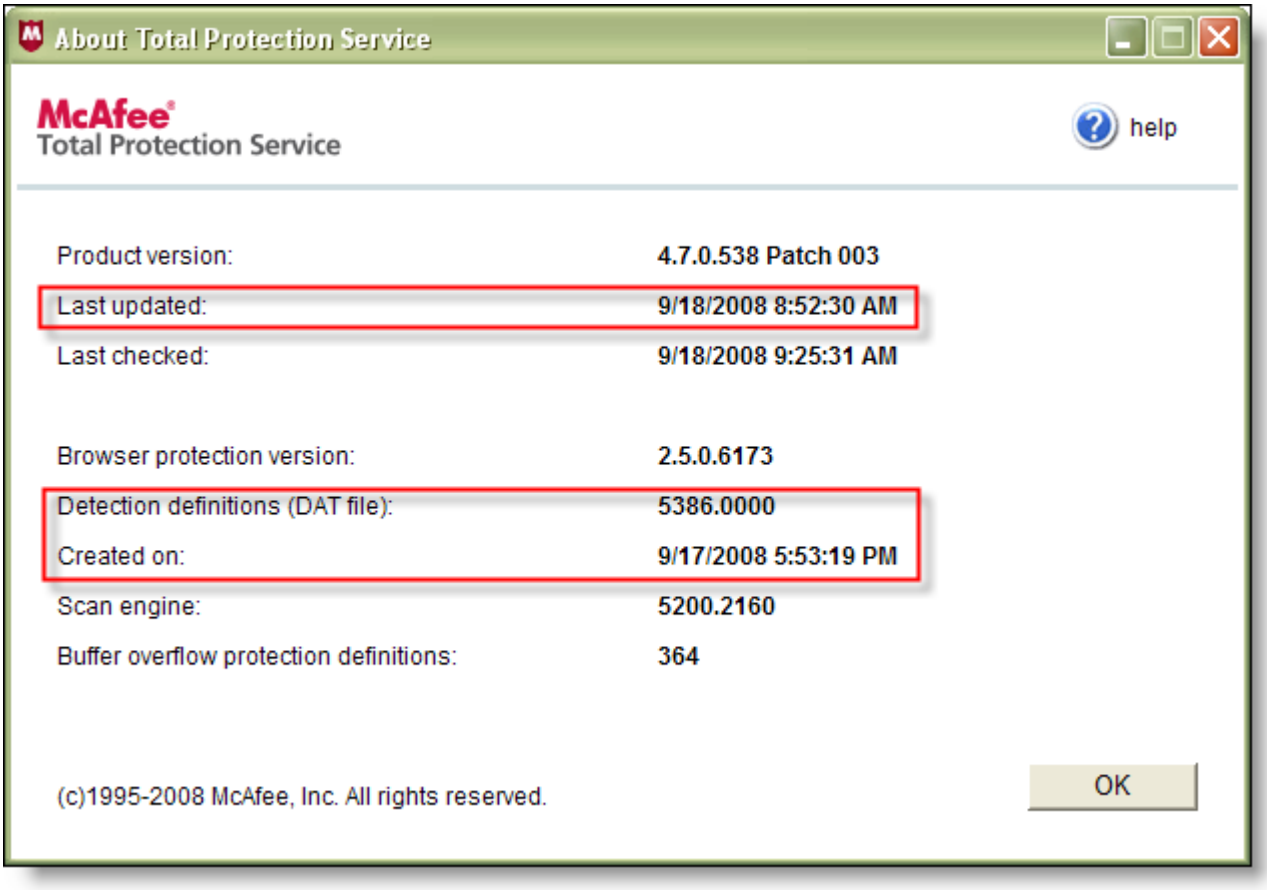
4. If updates are available, they will now download and install. Once the installation is complete, you will receive a message similar to the one below.



5. The final step is to verify that the system does in fact have the latest DAT file installed. To check this, simply right click on the McAfee tray icon and select 'About'. This will open the screen below. Check the following items:

    - 'Last Updated'
    - 'Detection definitions (DAT file)
    - 'Created on'

    Make sure these items reflect the most recent update information.



6. Once the data has been verified, click the 'OK' button to close the window. Updating is now complete.