teleflora®

Teleflora Point of Sales

Eagle 8

PA-DSS Implementation Guide

Version:	1.6
Version Date:	July 27, 2011

REVISIONS

Document Version	Date	Description
1.6	July 27, 2011	Corrected “How to Enable the Customer Service Access using GoToAssist” and “Data backup” sections
1.5	May 30, 2011	PA-DSS review for 2011, change eCare to GoToAssist, update backup procedures
1.4	Mar 2010	Updated Card Holder Data Retention and step 7 of How to Update your Eagle Software, to cover .bin file removal and disable system restore. Updated Collecting Sensitive Data for Debugging, logging.
1.3	Jan 2010	Updated *Customer Remote Access* section, added *How To Setup Goto My PC* section and added *How To Update Your Eagle Software* section.
1.2	Jan 2010	Updated based on changes to installation process, review comments, and PCI/PA-DSS 1.2 changes
1.1	Sept 2009	Updated per review comments
1.0	Jan 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 mandated from the PCI SSC (Payment Card Industry Security Standards Council. This council is comprised of represenatives from each of the major credit card companies. (Visa, Mastercard, American Express, JCB, Discover).

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 an Eagle point of sale software environment.

Scope and Definitions

In order to reduce retail credit card fraud, PCI SSC has mandated the use of a PA-DSS (Payment Application – Data Security Standards) certified applications to merchants. 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 Eagle 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 "Eagle specific" applications to the various PCI's PA-DSS requirements. Please refer to PCI's Data Security Standards 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
PCI-SSC	Payment Card Industry – Security Standards Council
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 an Eagle workstation, or Eagle server with "Administrative' windows privileges. Or, any person who has administrative privileges to the Eagle database.
"Data Security Standard"	A document, published by PCI, 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.

Note: At the time of this writing, the following document versions were used:

- PCI
    - Payment Card Industry (PCI) Data Security Standard – Requirements and Security Assessment Procedures Version 1.2.1 (July 2009)
        - https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
    - Payment Card Industry (PCI) Data Security Standard Self-Assessment Questionnaire – Instructions and Guidelines Version 1.2 (October 2008)
        - https://www.pcisecuritystandards.org/saq/index.shtml
    - Payment Card Industry (PCI) Data Security Self-Assessment Questionnaire and Attestation of Compliance Version 1.2 (October 2008)
        - https://www.pcisecuritystandards.org/saq/index.shtml
- PA-DSS
    - Payment Card Industry (PCI) Payment Application Data Security Standard – Requirements and Security Assessment Procedures Version 1.2.1 (July 2009)
        - https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml

Dissemination of This Document

<u>Addresses:</u>
PA-DSS 14.1

A copy of this document should be freely available to all persons who administer your Eagle 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 Eagle 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.

Eagle Customer Service Contact Information:

Phone: 800-237-7673

Postal Mail:
Attn: Eagle Support
Teleflora LLC
3737 NW 34th St.
Oklahoma City, OK. 73112

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 Eagle, it is important to realize that your legacy POS may still contain sensitive information 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 "Eraser" 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 Eagle 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 (Eagle 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 Eagle 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 Eagle 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 Eagle 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 Eagle 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.

Logs:
Though Eagle will never intentionally log non-PCI compliant data, it is still important that you are aware that your Eagle system can log details of some actions and transactions.

Please note, modifying or completely disabling logging on your Eagle system may render your system out of PCI compliance; do not modify or disable Eagle logging Capabilities. If you believe any logging settings have been changed, please call Teleflora Customer Support to correct these settings.

Cardholder Data Retention

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

Eagle retains the following Cardholder data in its database: Encrypted Credit Card number and Encrypted Expiration Date.

Eagle contains a tool to purge data from its 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 Eagle Policies document. Teleflora has also provided a tool to purge cardholder data from the Eagle database.

The Purge function in Eagle will remove cardholder data from your system based on your data retention limits. 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. The Eagle Encryption Key Rotation Utility also creates a backup copy of your database prior to rotating the encryption keys. Upgrading you Eagle software also creates a backup copy of your database prior to upgrade.

Teleflora recommends that, after you have verified the purging of the cardholder data, encryption key rotation, or upgrade of the software is complete, you use the Eraser tool to securely delete the backup copy of your database(EagleFMS.mdb) and encryption key(EagleFMS.bin). See appendix “Using the Eraser Tool”.

By default your Eagle system will come with Windows System Restore turned off. Teleflora recommends that you leave System Restore off. If you believe System Restore has been turned on, please call Teleflora Customer Support to change these settings.

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 Eagle environment is ensuring that users are properly authenticated for the task to be performed. The Eagle application does not require users to have administrative privileges in order to run. Note that, for the purpose of Eagle, 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 Eagle 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 Eagle 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 Eagle 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 network will have an Adminsitrative account with the username Administrator. The owner and manager are responsible to maintain the passwords for these accounts as Teleflora will not manage the password rotations. It is important that as the passwords are changed the shops owners or managers keep track of the passowords. If a shop becomes locked out of a windows computer Teleflora does have a recovery process but this process will take several hours to complete.

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 ninety days. Please see the appendix for specific instructions on adding and removing non-administrative users from your Eagle 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 Eagle system(s), even if the account is not used often.

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 1.3.9
PCI DSS 2.1.1
PCI DSS 4.1.1

Teleflora does not recommend, sell, nor support, the use of wireless networks within the Eagle 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 Eagle Server:
PA-DSS 9.1.b
The Eagle “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 Eagle server and the internet which restricts connections established from the internet, to your Eagle server.

Protecting Eagle Workstations
PA-DSS 10.1
The Eagle 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 Eagle 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 Eagle server, may compromise your system’s security, and your PCI compliance. If you are considering adding any additional machines to your Eagle network, you must ensure that the new computer(s) do not expose any network services to the public internet (for example, game related servers, file sharing programs).

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 Eagle network.

Using a Remote Eagle System

Addresses:
PA-DSS 11.2
PCI DSS 8.3

In the event that you wish to use your Eagle 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).

Remote Administration of a Eagle 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.
- If a request for GoToAssist is ever sent via email from a Teleflora support tech to a customer the shop will be on the phone with the tech to confirm before clicking a link. This would typically occur in an after hours situation.
- 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 Eagle 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 – Unless you have a defined business need, Teleflora does not recommend providing Remote access into your Eagle system. Teleflora customer service does employ the use of “GoToAssist”, a web based, remote desktop utility, for assisting customers. In the event that you have a business need for Remote access into your Eagle system, you must use a remote access solution which meets or exceeds PCI-DSS standards related to remote access. Teleflora currently provides you the option of using the “Goto My PC Corporate” service which has been configured to meet guidelines as defined in the PCI-DSS. Please see the section below in regards to proper setup of the “Goto My PC Corporate” software onto your PC.
In any case in which you wish to remotely access your Eagle system, your remote access solution must comply with PCI-DSS standards. Below are some of the applicable requirements, as found within the PCI-DSS document:

PCI-DSS
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”.

Eagle Transactions with Public Networks:

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

In order to perform functions such as authorizations, settlement, and Dove, your Eagle system does transmit cardholder information across the public internet. To protect this transmission, Eagle 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 Eagle software.

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 Eagle 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

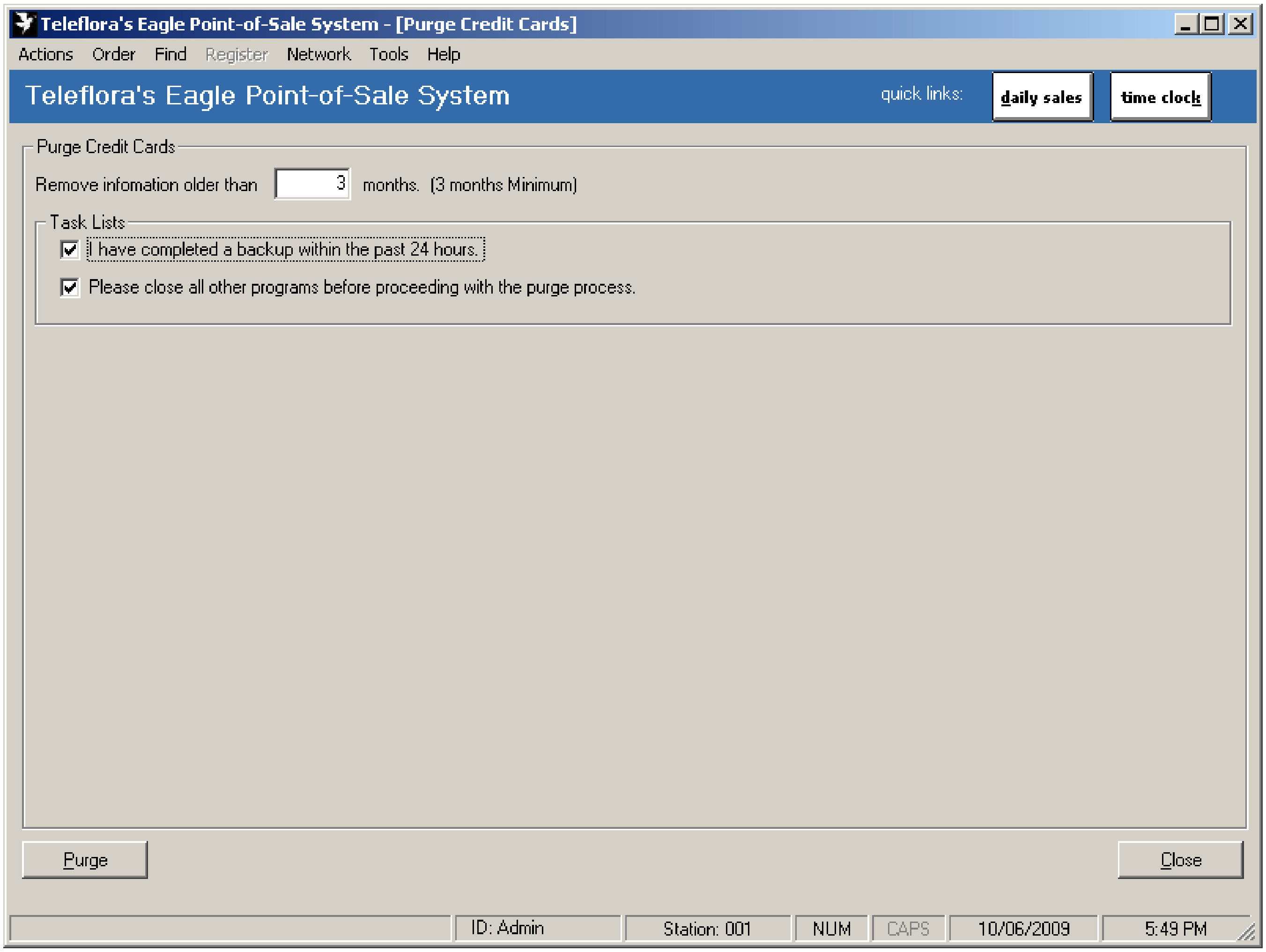
PA-DSS 2.1.a

Use Purge Credit Cards to remove old information from your system. Only data **3 months** or older can be purged. We recommend contacting Teleflora Technical Support before purging records.

To purge records, follow these steps:

From the Eagle **Welcome** window:

1. Select the **Shop Management** button.
2. Select the **Setup & Utilities** button.
3. Select the **Purge** button.
4. In the **Purge** section, select the **Purge Credit Cards** button.


Teleflora's Eagle Point-of-Sale System - [Purge Credit Cards]
Actions Order Find Register Network Tools Help
Teleflora's Eagle Point-of-Sale System
quick links:
daily sales
time clock
Purge Credit Cards
Task Lists
Purge
Close
ID: Admin
Station: 001
NUM
CAPS
10/06/2009
5:49 PM

Remove infomation older than 3 months. (3 months Minimum)

☑ I have completed a backup within the past 24 hours.

☑ Please close all other programs before proceeding with the purge process.

5. In the **Remove Information older than** field,enter age of data to be removed.
6. Select **Purge** to permanently delete this information from Eagle.

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

All remote administration of the Eagle application will occur via the “Administrator” user.

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

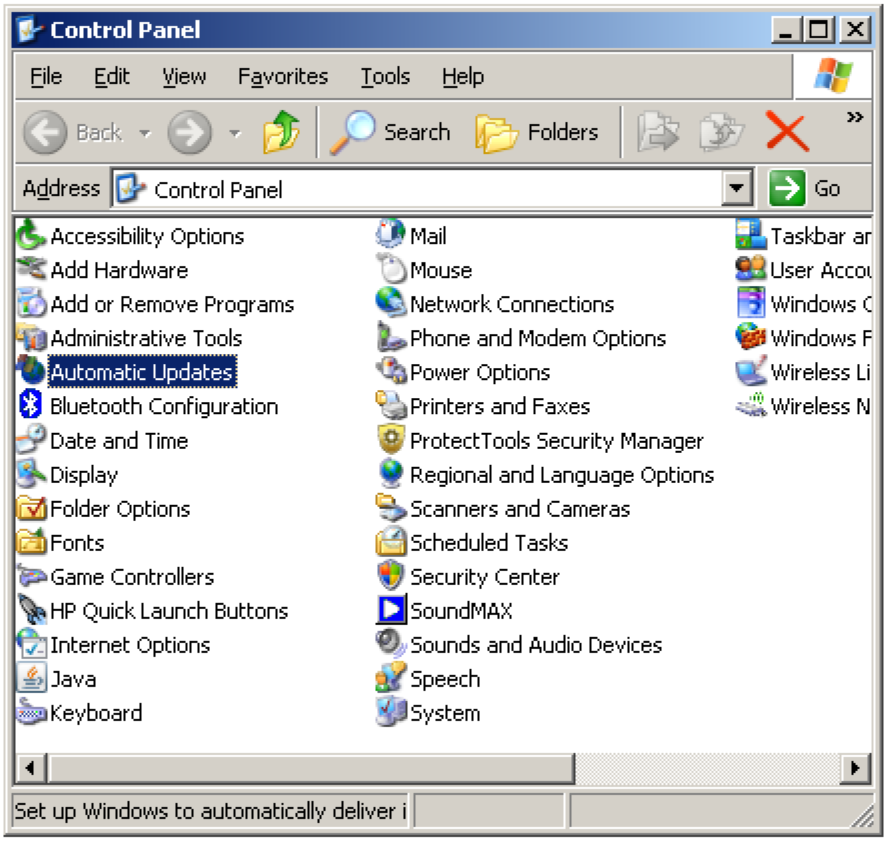
The Eagle application server requires outbound internet connections to the following destination IP Ports:
TCP Port 443 (SSL / HTTPS)

How to update your Eagle Server's Operating System

PA-DSS 10.1
PCI 6.1

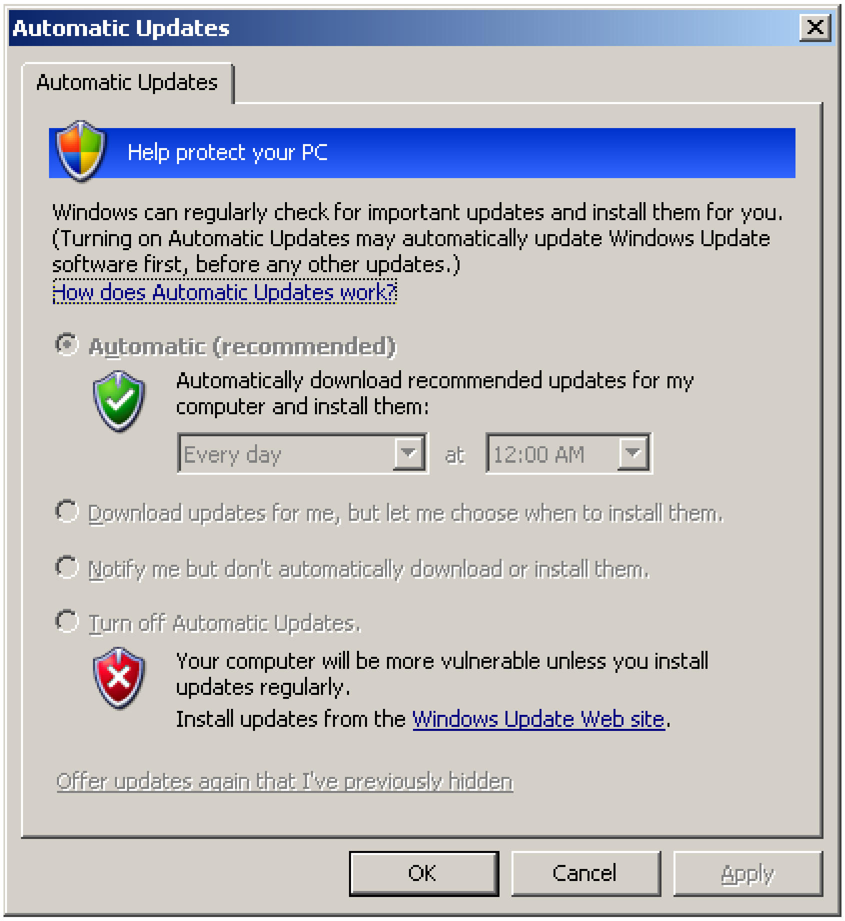
Your Eagle server must be up-to-date with security bulletins. Following are instructions for performing a manual OS update.

Windows XP
Log in as Administrator.



Set up Windows to automatically deliver i

Start | Settings | Control Panel | Automatic Updates



Windows can regularly check for important updates and install them for you. (Turning on Automatic Updates may automatically update Windows Update software first, before any other updates.)
How does Automatic Updates work?

● Automatic (recommended)
Automatically download recommended updates for my computer and install them:
Every day at 12:00 AM

○ Download updates for me, but let me choose when to install them.

○ Notify me but don't automatically download or install them.

○ Turn off Automatic Updates.
Your computer will be more vulnerable unless you install updates regularly.
Install updates from the Windows Update Web site.

Offer updates again that I've previously hidden

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 Eagle Software (Install Media)

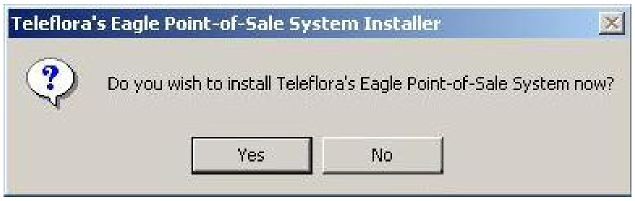
PA-DSS 10.1

This section of the document outlines the Server Upgrade process of Eagle 8. The Eagle Server Install/Upgrade still has the same layout and appearance as the previous 6.0 release version.

The following instructions are for installing Eagle 8 as a Server Upgrade installation.

1. Insert the Eagle 8 Installation CD into the CD/DVD-ROM Drive.

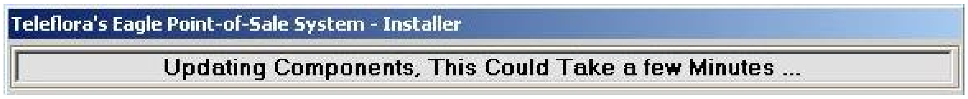
   Note: *The CD should Autorun. If it does not, instruct the user to do the following: Click Start > Run. Click Browse. Select the CD-ROM Drive from the Look in box. Click on Setup.exe to select it. Click OK. Click OK Again on the Run box.*



Teleflora's Eagle Point-of-Sale System Installer

Do you wish to install Teleflora's Eagle Point-of-Sale System now?

2. Click Yes

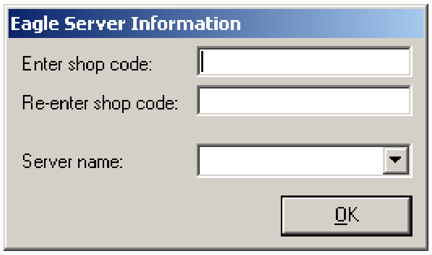


Teleflora's Eagle Point-of-Sale System - Installer

Updating Components, This Could Take a few Minutes ...

Note: *During this step of the installation process, a 3rd party updater is used to ensure that MDAC (Microsoft Data Access Controls), DAO (Data Access Object), and Microsoft Jet (Joint Engine Technology) Engine Drivers are up to date. Any needed or out of date components are installed. If any components are already installed that are the same or a newer version of the component, those components are skipped.*

3. Enter the correct shop code and select the correct server on the Eagle Server Information dialog.

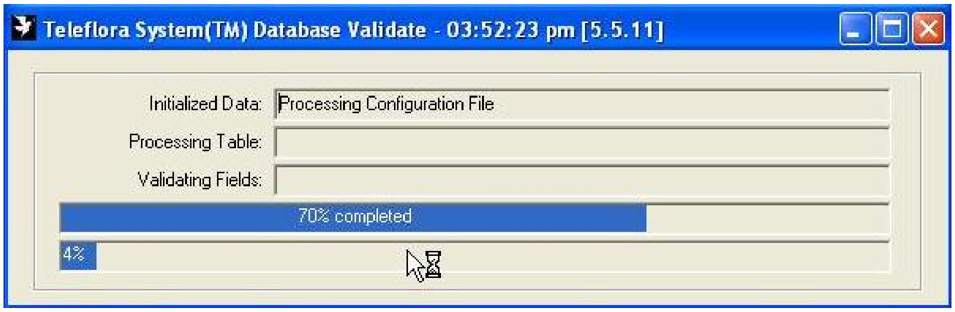


Eagle Server Information

Enter shop code:

Re-enter shop code:

Server name:



Teleflora System(TM) Database Validate - 03:52:23 pm [5.5.11]

Initialized Data: Processing Configuration File

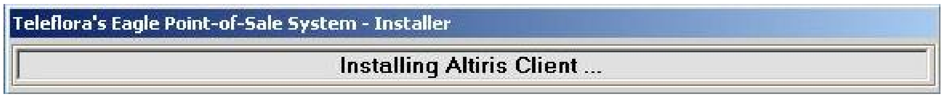
Processing Table:

Validating Fields:

70% completed

4%

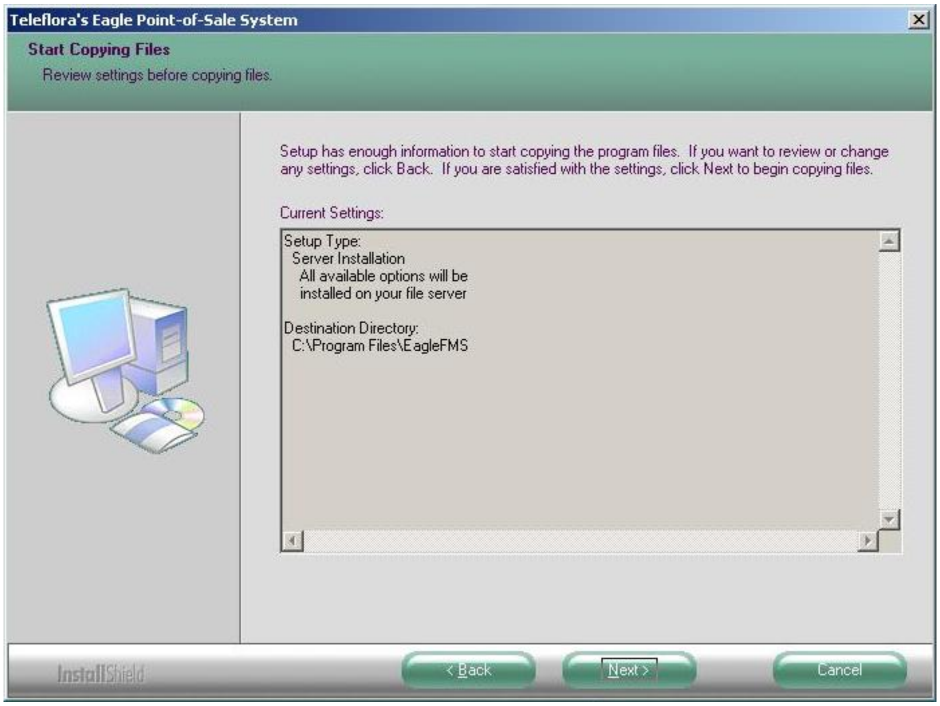
Note: *During this step of the installation process, the existing EagleFMS.MDB database table structure and data are validated for consistency. If any errors are found during this process, the installation process will halt. If any inconsistencies in the database are encountered, obtain the ValidateFMS.log file that exists in the Eagle installation directory. Contact the Eagle Support Lead or QA for assistance if support is not available before continuing any further!*



Teleflora's Eagle Point-of-Sale System - Installer

Installing Altiris Client ...

Note: *During this step of the installation process, an Altiris Agent Service is installed to all versions of Windows supported with Eagle.*



Teleflora's Eagle Point-of-Sale System

Start Copying Files

Review settings before copying files.

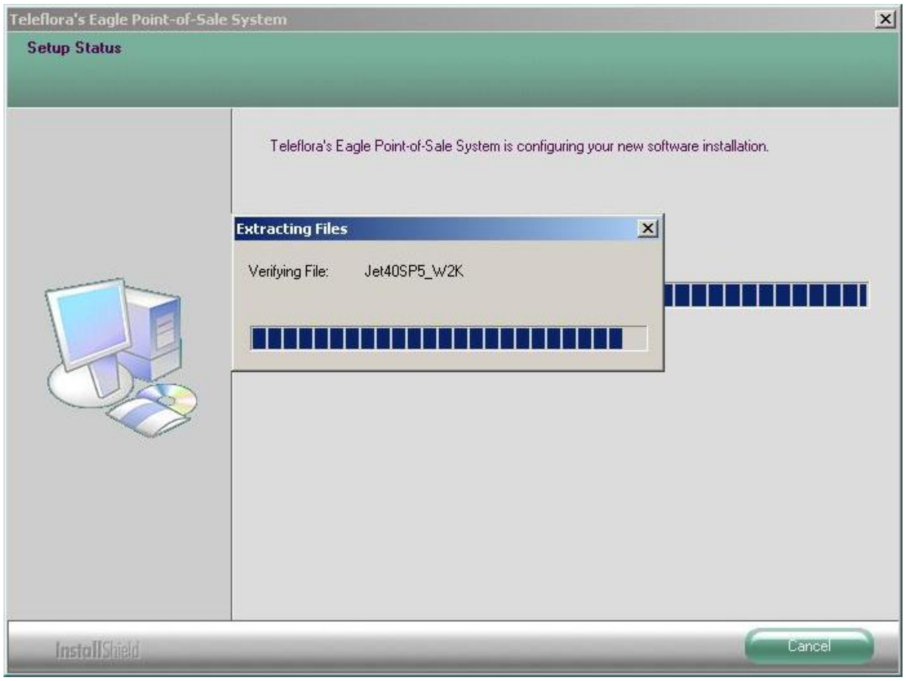
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

Setup Type:
  Server Installation
    All available options will be
    installed on your file server

Destination Directory:
  C:\Program Files\EagleFMS

4. Verify that the Setup Type and Destination Directory are correct. Click Next.



Teleflora's Eagle Point-of-Sale System

Setup Status

Teleflora's Eagle Point-of-Sale System is configuring your new software installation.

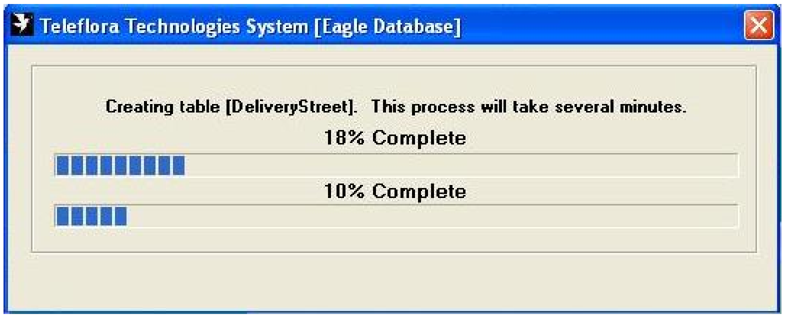
Extracting Files

Verifying File: Jet40SP5_W2K

Note: *In this step of the installation process, the install shield wizard executes a windows update file to upgrade Microsoft Jet Engine Drivers to 4.0 SP8. Different update files will be executed from the CD based on the user's operating system.*

Note: *During this step of the installation procedure, the QBFC 5.0 (QuickBooks File Control) Utility is installed. This is a 3*rd *party utility provided by Intuit. QBFC 5.0 has it's own entry in the Add/Remove Programs Menu and it is not removed if you uninstall Eagle.*

5. Click Finish.



Teleflora Technologies System [Eagle Database]

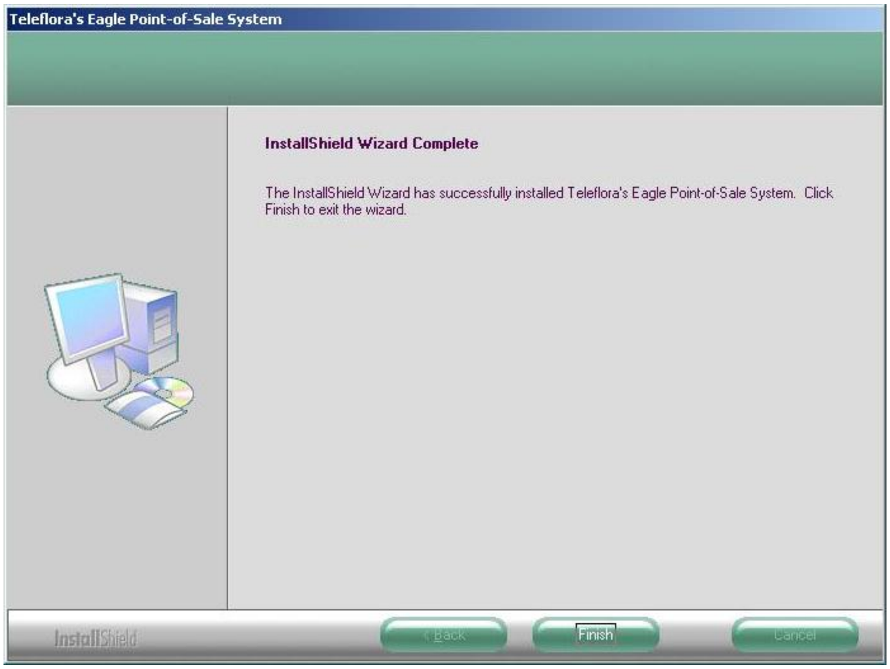
Creating table [DeliveryStreet]. This process will take several minutes.

18% Complete

10% Complete

Note: *During this step of the installation procedure, EagleFMS.MDB, EagleWD.MDB, and Statements.MDB are imported into new 6.0 structured databases. The databases will be upgraded one at a time. A separate progress bar window will be displayed for each database. Other data modifications may be performed at this time depending on what version of Eagle the user is upgrading from. The upgrade process may take some time at some points during this process. If the customer has a fairly large customer and order count, minimum hardware requirements, or a combination of both, give this process extra time to continue before considering that the application is frozen.*

Note: *During this step of the installation procedure, the installation will launch a minimized window that will update filesystem permissions needed to properly run Eagle.*



Teleflora's Eagle Point-of-Sale System

InstallShield Wizard Complete

The InstallShield Wizard has successfully installed Teleflora's Eagle Point-of-Sale System. Click Finish to exit the wizard.

6. Click Finish

7. After completing the upgrade on the server, perform a search for the following files:

   ..\EagleFMS\Data\EagleDHF.Bin
   ..\EagleFMS\DTTier30.dll
   ..\EagleFMS\DTTier40.dll
   ..\EagleFMS\DTTier50.dll
   ..\EagleFMS\DTTier55.dll
   ..\EagleFMS\DTTier60.dll

Note: *The version of the DTTier file will depend on what version the user is upgrading from. If the user is upgrading from 5.x version of Eagle, the DTTier will be named DTTier50.dll, etc.*

   If any of these files are found, right click on them and select Erase on the menu then select Yes on the verification prompt. This will securely delete these files using the Eraser Utility, per PA-DSS compliance.

8. Proceed to upgrade any Workstations that meet minimum hardware and operating system requirements.

How to Enable the Customer Service Access using GoToAssist

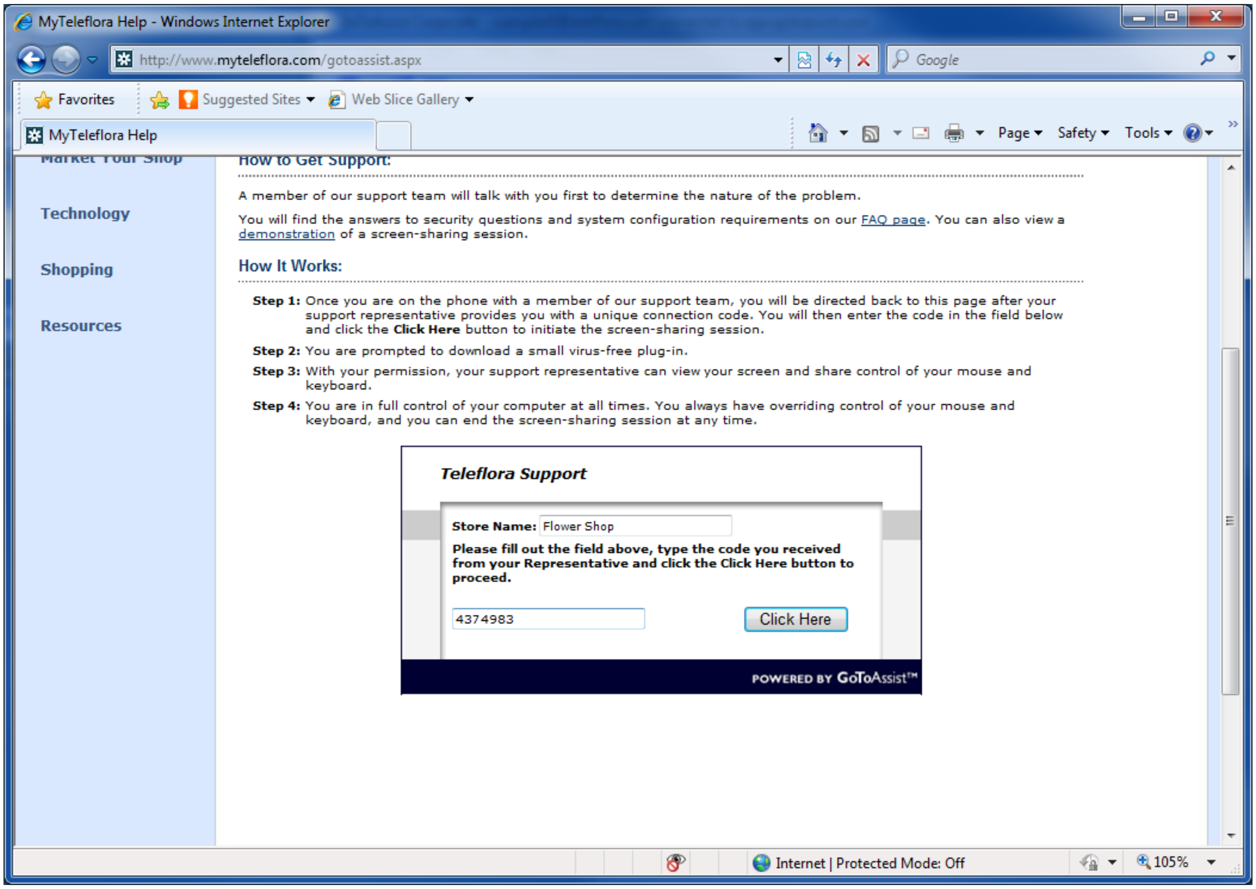
PA-DSS 10.1
PA-DSS 11.3.b

Eagle 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.



How to Get Support:

A member of our support team will talk with you first to determine the nature of the problem.

You will find the answers to security questions and system configuration requirements on our FAQ page. You can also view a demonstration of a screen-sharing session.

How It Works:

Step 1: Once you are on the phone with a member of our support team, you will be directed back to this page after your support representative provides you with a unique connection code. You will then enter the code in the field below and click the **Click Here** button to initiate the screen-sharing session.

Step 2: You are prompted to download a small virus-free plug-in.

Step 3: With your permission, your support representative can view your screen and share control of your mouse and keyboard.

Step 4: You are in full control of your computer at all times. You always have overriding control of your mouse and keyboard, and you can end the screen-sharing session at any time.

Teleflora Support

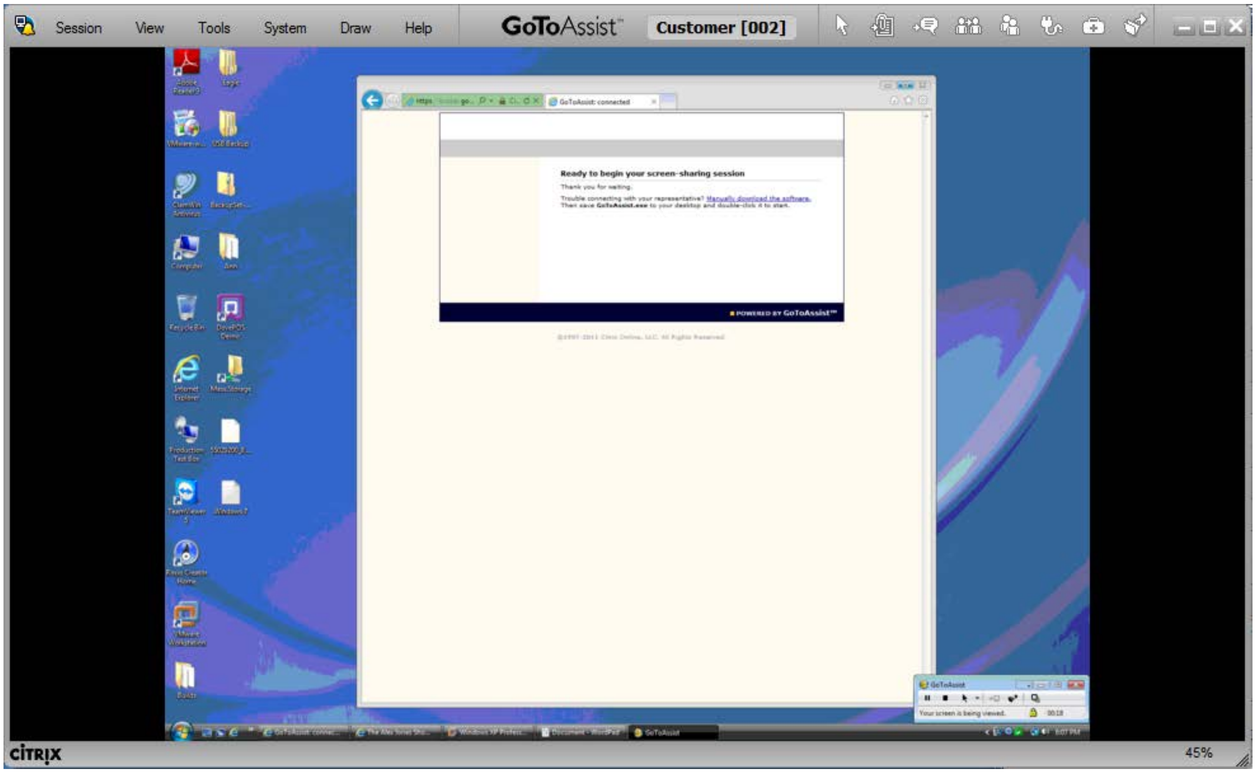
Store Name: Flower Shop

Please fill out the field above, type the code you received from your Representative and click the Click Here button to proceed.

4374983

Click Here

POWERED BY GoToAssist™



Ready to begin your screen-sharing session

Thank you for waiting.

Trouble connecting with your representative? Manually download the software. Then save **GoToAssist.exe** to your desktop and double-click it to start.

POWERED BY GoToAssist™

©1997-2011 Citrix Online, LLC. All Rights Reserved.

Your screen is being viewed.

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

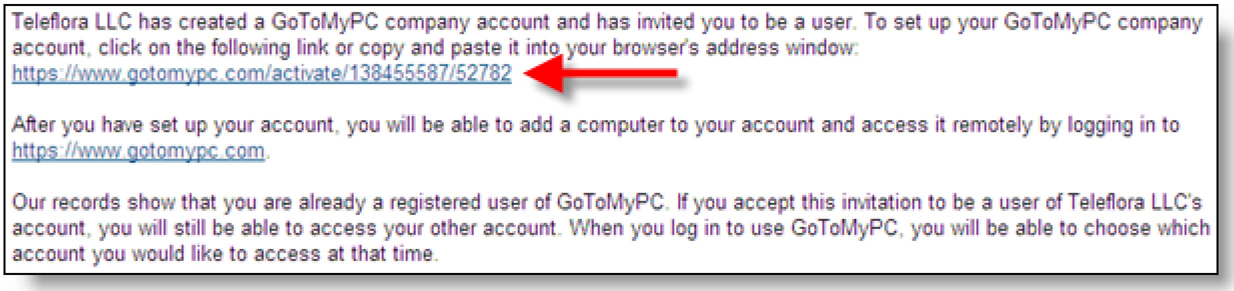
How to Setup Teleflora's "Goto My PC Corporate" On Your Eagle System

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.

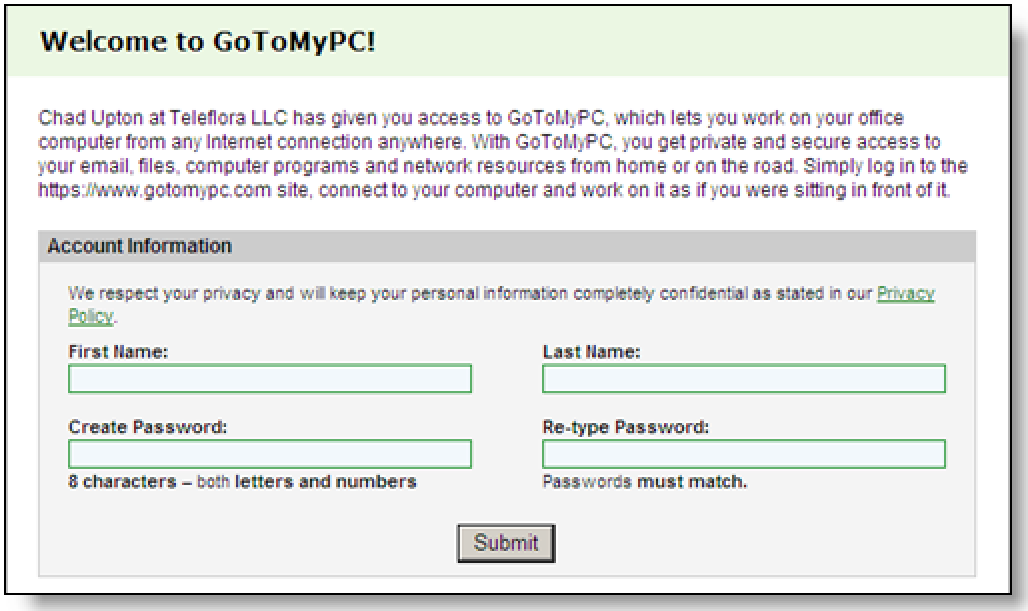


Teleflora LLC has created a GoToMyPC company account and has invited you to be a user. To set up your GoToMyPC company account, click on the following link or copy and paste it into your browser's address window: https://www.gotomypc.com/activate/138455587/52782

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.



Welcome to GoToMyPC!

Chad Upton at Teleflora LLC has given you access to GoToMyPC, which lets you work on your office computer from any Internet connection anywhere. With GoToMyPC, you get private and secure access to your email, files, computer programs and network resources from home or on the road. Simply log in to the https://www.gotomypc.com site, connect to your computer and work on it as if you were sitting in front of it.

Account Information

We respect your privacy and will keep your personal information completely confidential as stated in our Privacy Policy.

First Name:

Last Name:

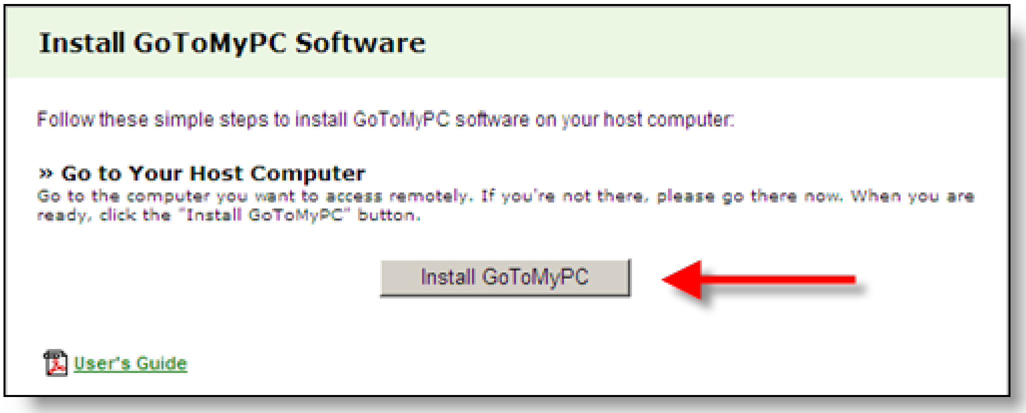
Create Password:

8 characters – both letters and numbers

Re-type Password:

Passwords must match.

5. Install the GoToMyPC client.

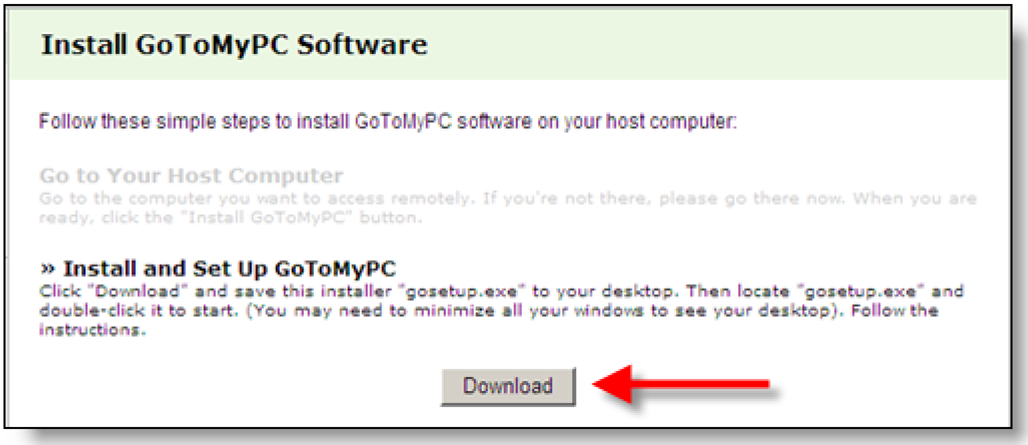


Install GoToMyPC Software

Follow these simple steps to install GoToMyPC software on your host computer:

» Go to Your Host Computer
Go to the computer you want to access remotely. If you're not there, please go there now. When you are ready, click the "Install GoToMyPC" button.

6. Click Download



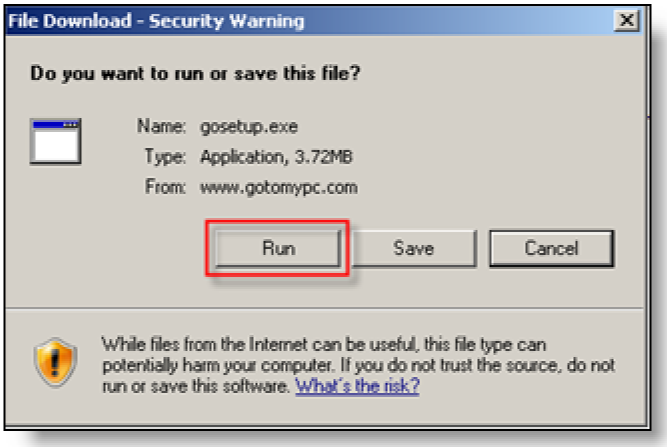
Install GoToMyPC Software

Follow these simple steps to install GoToMyPC software on your host computer:

Go to Your Host Computer
Go to the computer you want to access remotely. If you're not there, please go there now. When you are ready, click the "Install GoToMyPC" button.

» Install and Set Up GoToMyPC
Click "Download" and save this installer "gosetup.exe" to your desktop. Then locate "gosetup.exe" and double-click it to start. (You may need to minimize all your windows to see your desktop). Follow the instructions.

7. Click Run on the download dialog box.



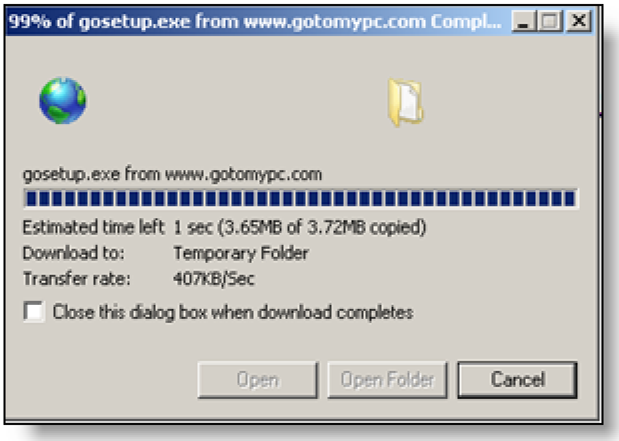
File Download - Security Warning

Do you want to run or save this file?

Name: gosetup.exe
Type: Application, 3.72MB
From: www.gotomypc.com

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

8. Wait for the progress bar to finish.



99% of gosetup.exe from www.gotomypc.com Compl...

gosetup.exe from www.gotomypc.com

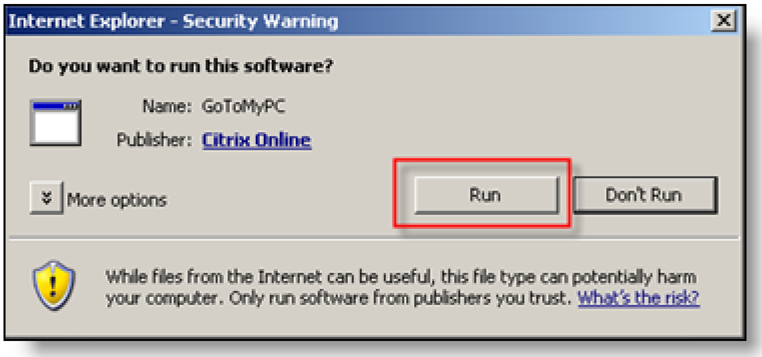
Estimated time left 1 sec (3.65MB of 3.72MB copied)

Download to: Temporary Folder

Transfer rate: 407KB/Sec

□ Close this dialog box when download completes

9. Click Run on the Installation box.



Internet Explorer - Security Warning

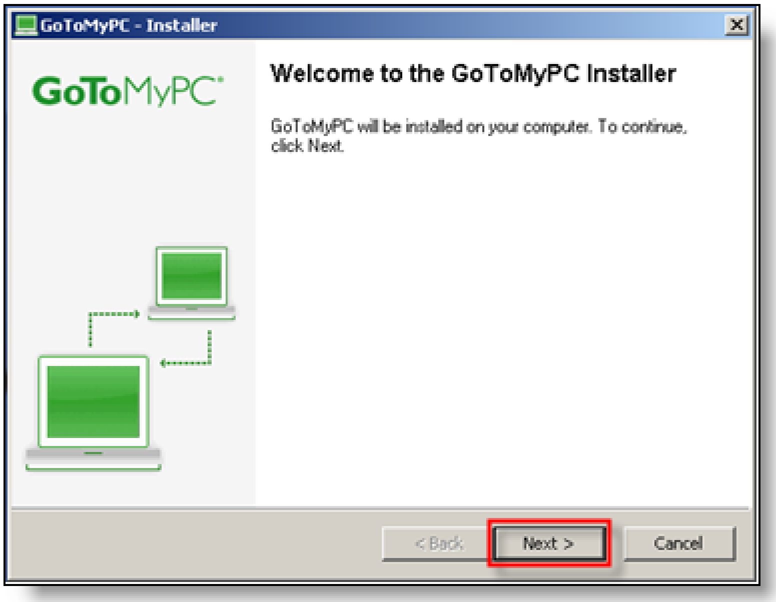
Do you want to run this software?

Name: GoToMyPC

Publisher: Citrix Online

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

10. Click Next on the GoToMyPC Installer.

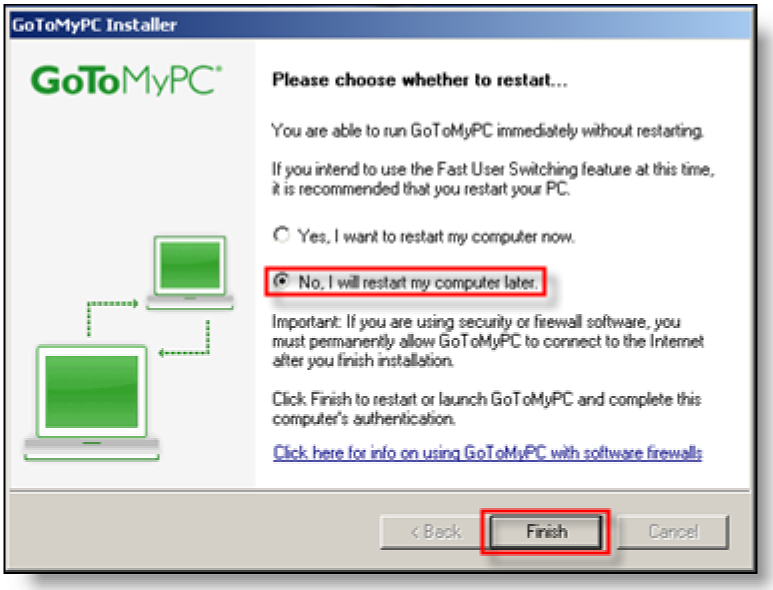


GoToMyPC - Installer

Welcome to the GoToMyPC Installer

GoToMyPC will be installed on your computer. To continue, click Next.

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



GoToMyPC Installer

Please choose whether to restart...

You are able to run GoToMyPC immediately without restarting.

If you intend to use the Fast User Switching feature at this time, it is recommended that you restart your PC.

○ Yes, I want to restart my computer now.

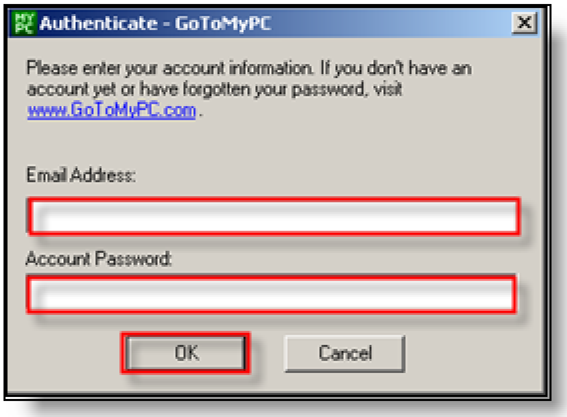
● No, I will restart my computer later.

Important: If you are using security or firewall software, you must permanently allow GoToMyPC to connect to the Internet after you finish installation.

Click Finish to restart or launch GoToMyPC and complete this computer's authentication.

Click here for info on using GoToMyPC with software firewalls

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.



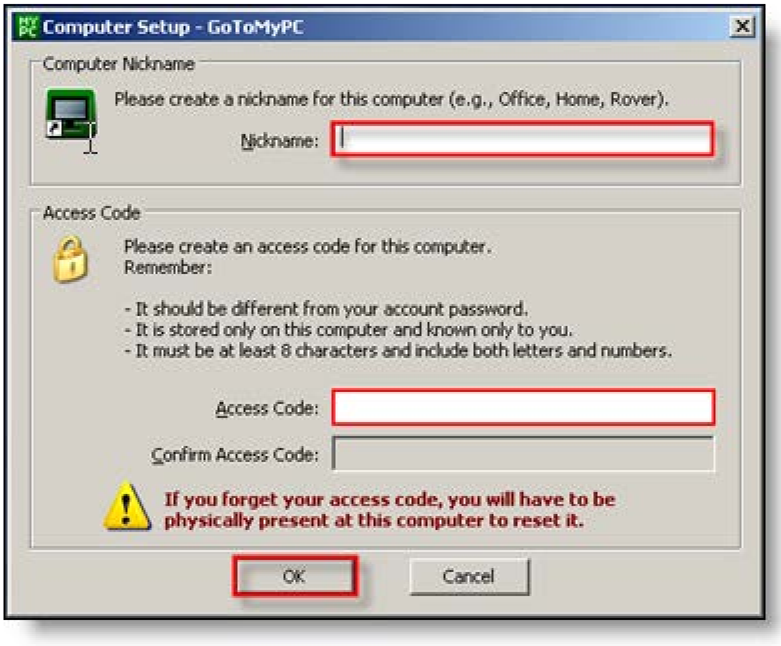
Authenticate - GoToMyPC

Please enter your account information. If you don't have an account yet or have forgotten your password, visit www.GoToMyPC.com.

Email Address:

Account Password:

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.



Computer Setup - GoToMyPC

Computer Nickname

Please create a nickname for this computer (e.g., Office, Home, Rover).

Nickname:

Access Code

Please create an access code for this computer.
Remember:

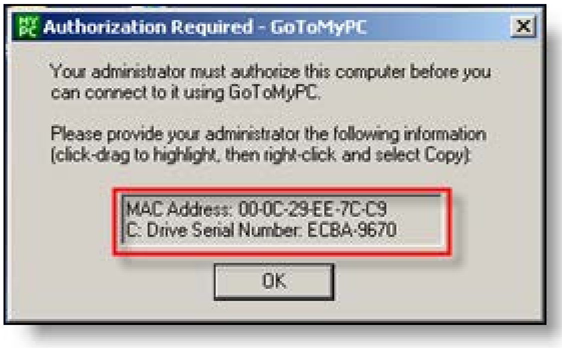
- It should be different from your account password.
- It is stored only on this computer and known only to you.
- It must be at least 8 characters and include both letters and numbers.

Access Code:

Confirm Access Code:

If you forget your access code, you will have to be physically present at this computer to reset it.

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



Authorization Required - GoToMyPC

Your administrator must authorize this computer before you can connect to it using GoToMyPC.

Please provide your administrator the following information (click-drag to highlight, then right-click and select Copy):

MAC Address: 00-0C-29-EE-7C-C9
C: Drive Serial Number: ECBA-9670

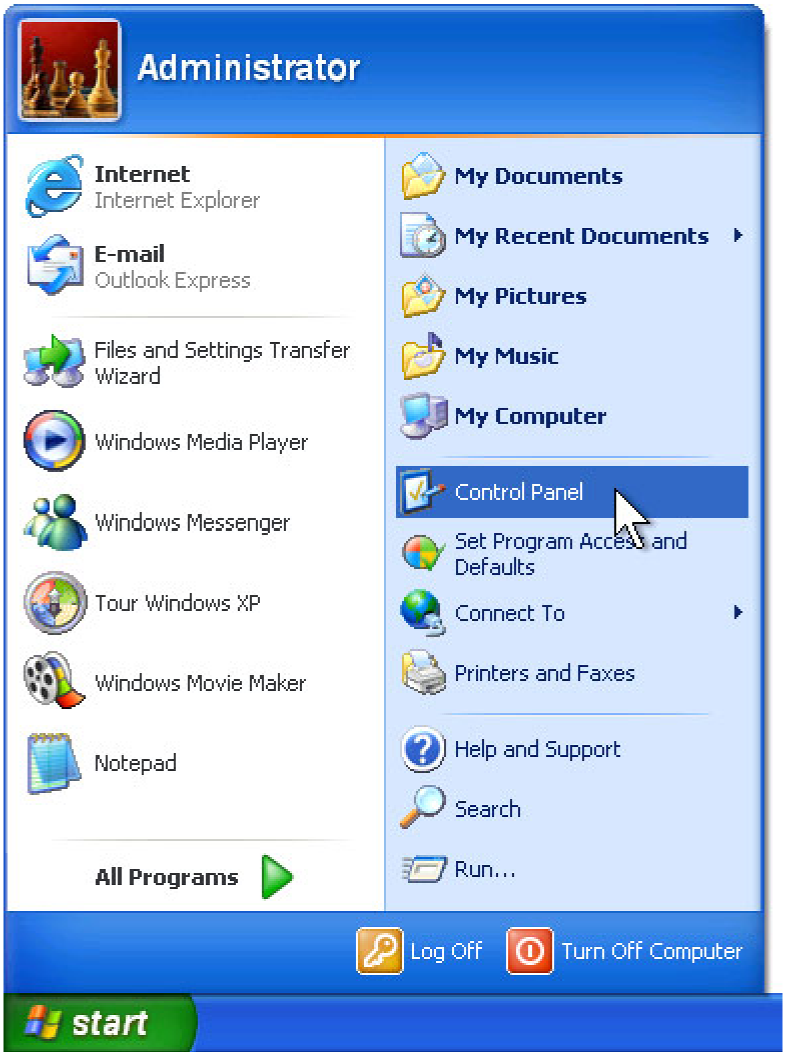
16. Send an email with the following information to Managed Services at msg@teleflora.com:
    a. Shop code
    b. Customers email address
    c. MAC address and C: drive serial number from step 15.

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.

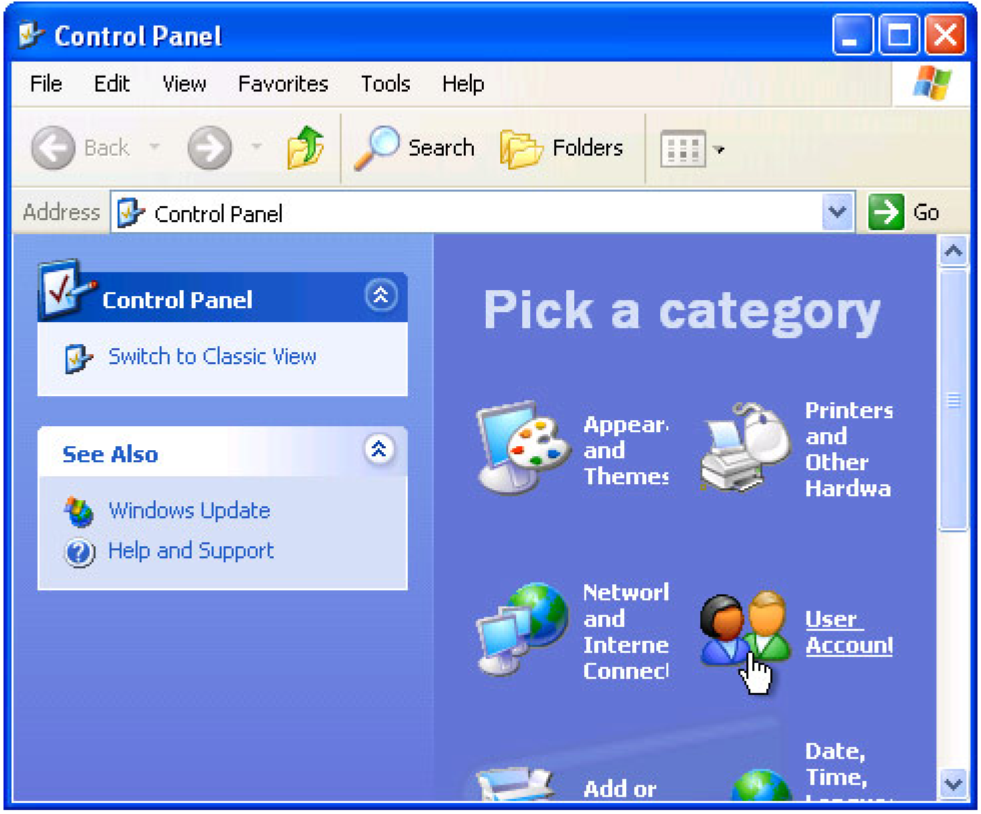
How to Add a Non-Administrative Windows User Account

PA-DSS 3.1

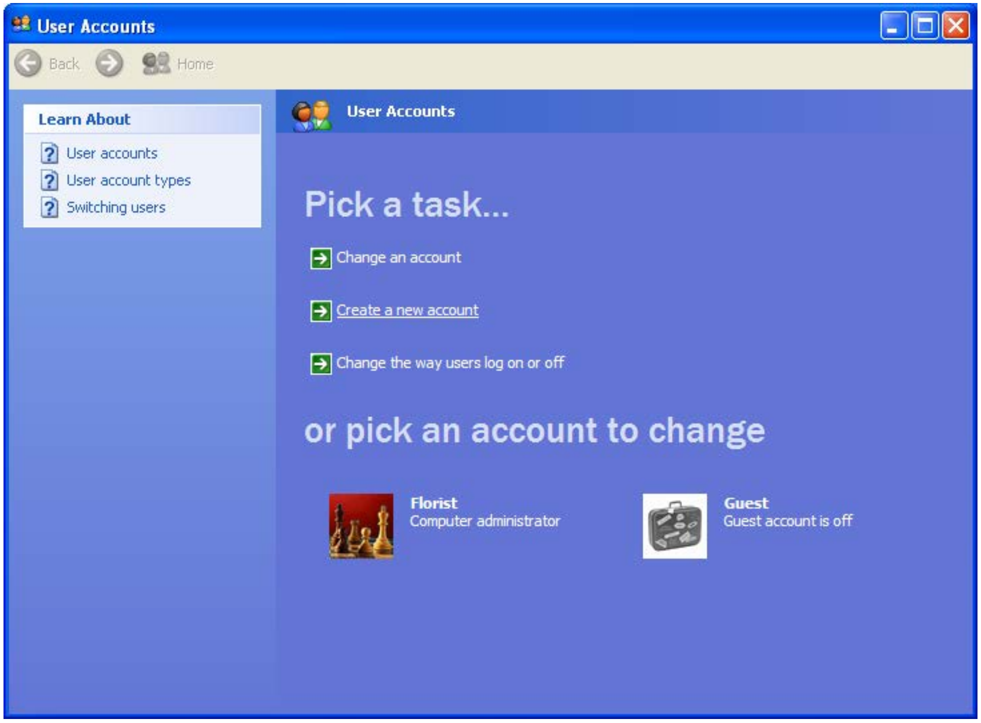
1. Log on to your computer as “Florist” (Florist has administrative privileges). Click Start, and then click Control Panel.



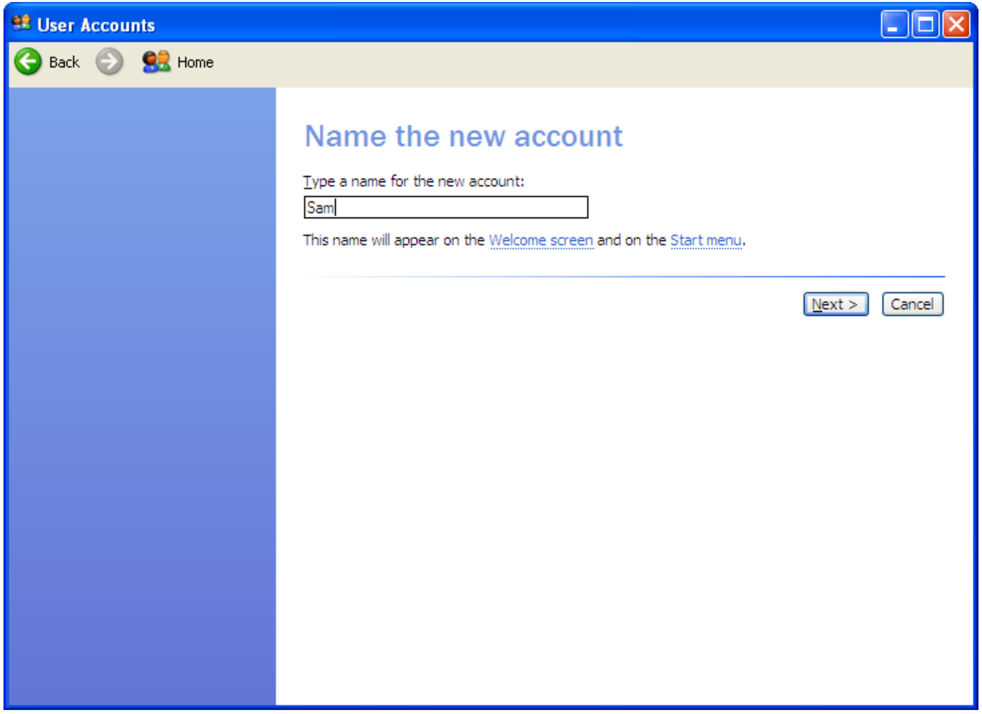
2. Under Pick a category, click User Accounts.



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.



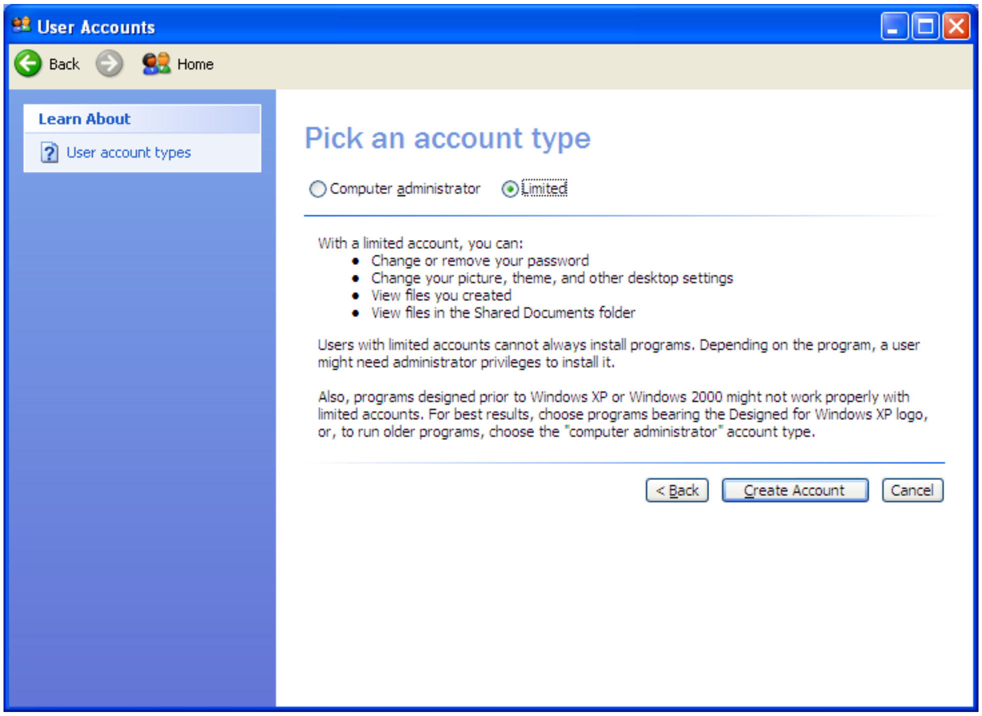
Name the new account

Type a name for the new account:

Sam

This name will appear on the Welcome screen and on the Start menu.

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



Pick an account type

○ Computer administrator ● Limited

With a limited account, you can:

- Change or remove your password
- Change your picture, theme, and other desktop settings
- View files you created
- View files in the Shared Documents folder

Users with limited accounts cannot always install programs. Depending on the program, a user might need administrator privileges to install it.

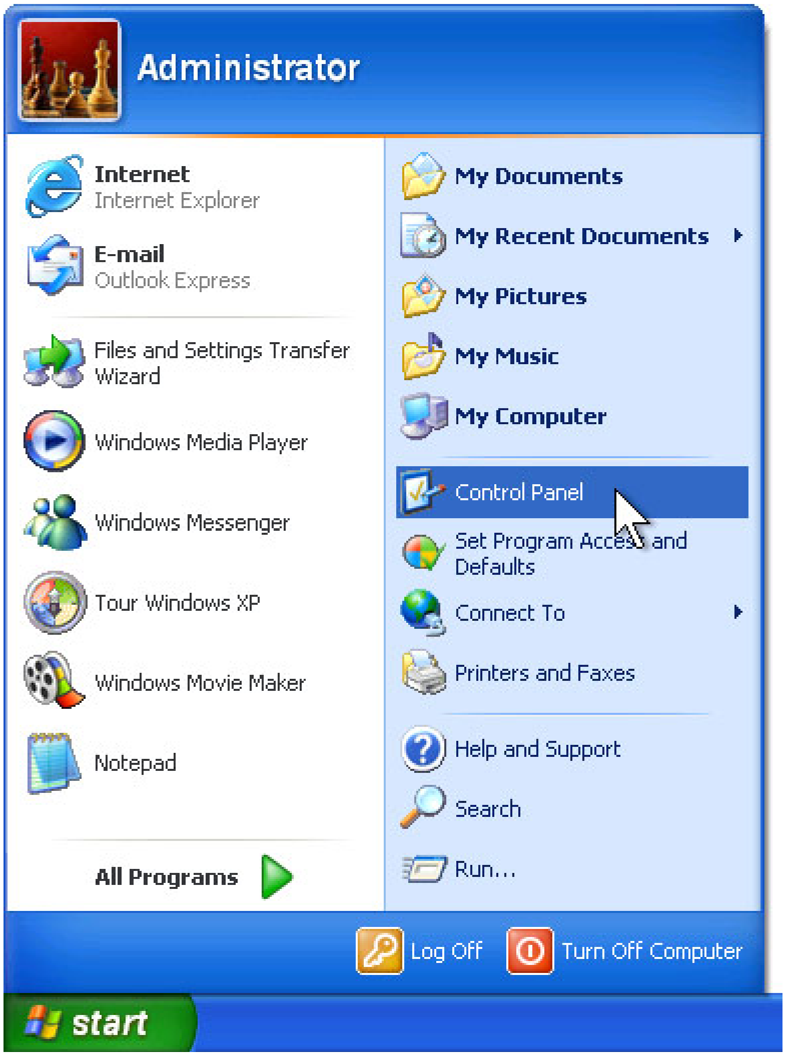
Also, programs designed prior to Windows XP or Windows 2000 might not work properly with limited accounts. For best results, choose programs bearing the Designed for Windows XP logo, or, to run older programs, choose the "computer administrator" account type.

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

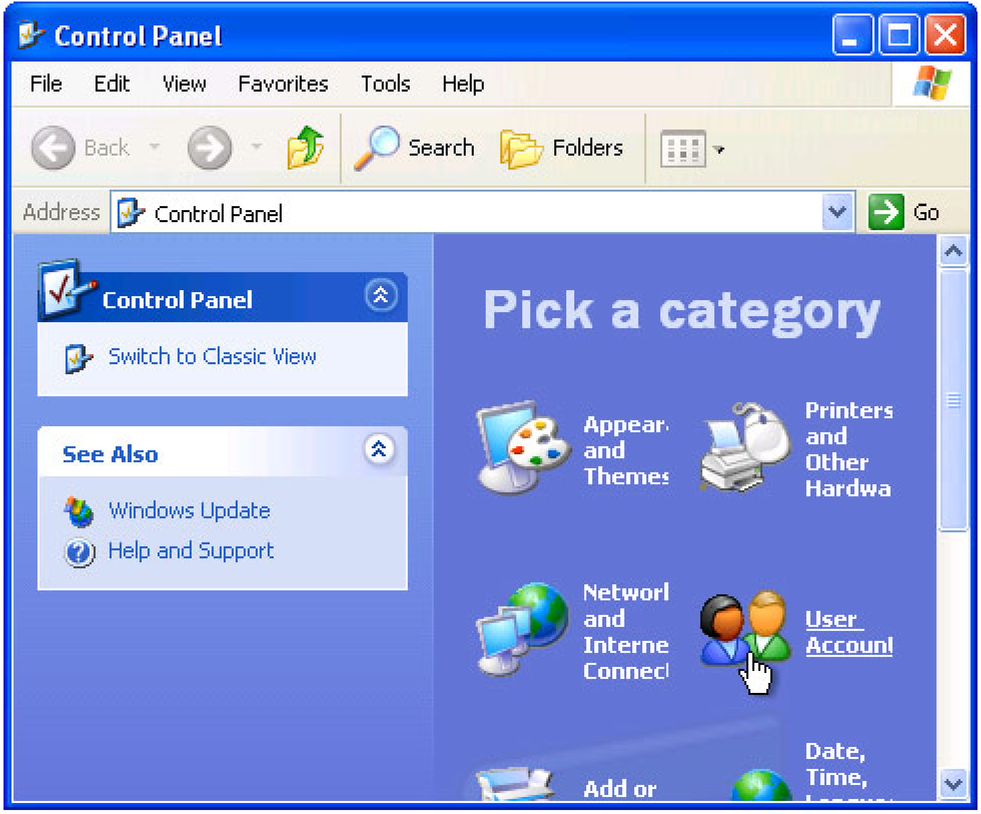
How to Add an Administrative Windows User Account

PA-DSS 3.1

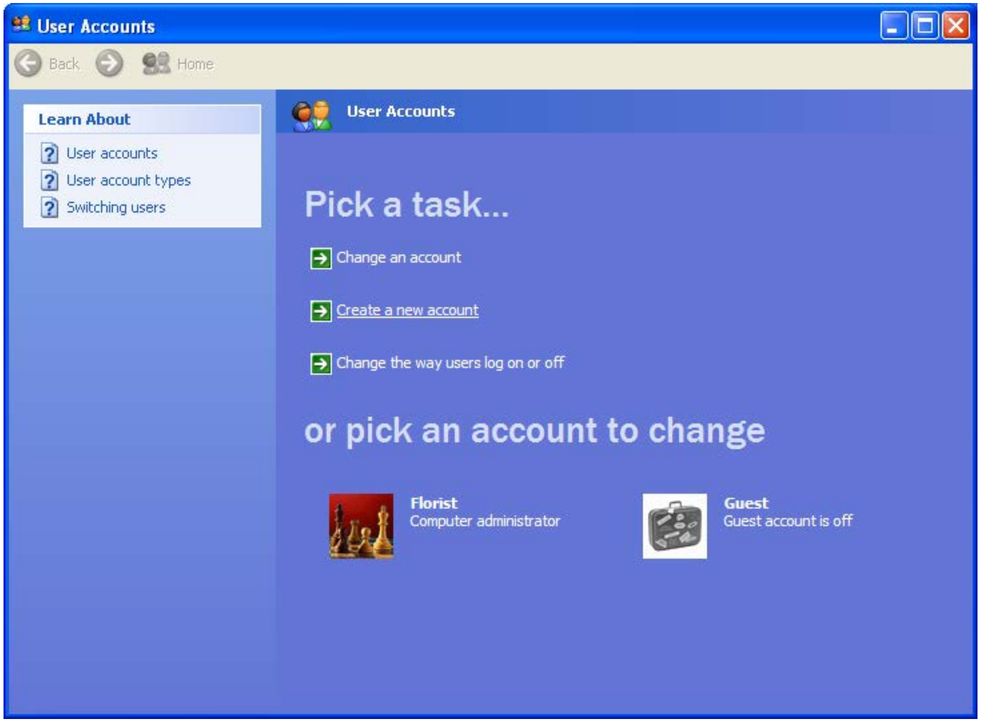
1. Log on to your computer as “Florist” (Florist has administrative privileges). Click Start, and then click Control Panel.



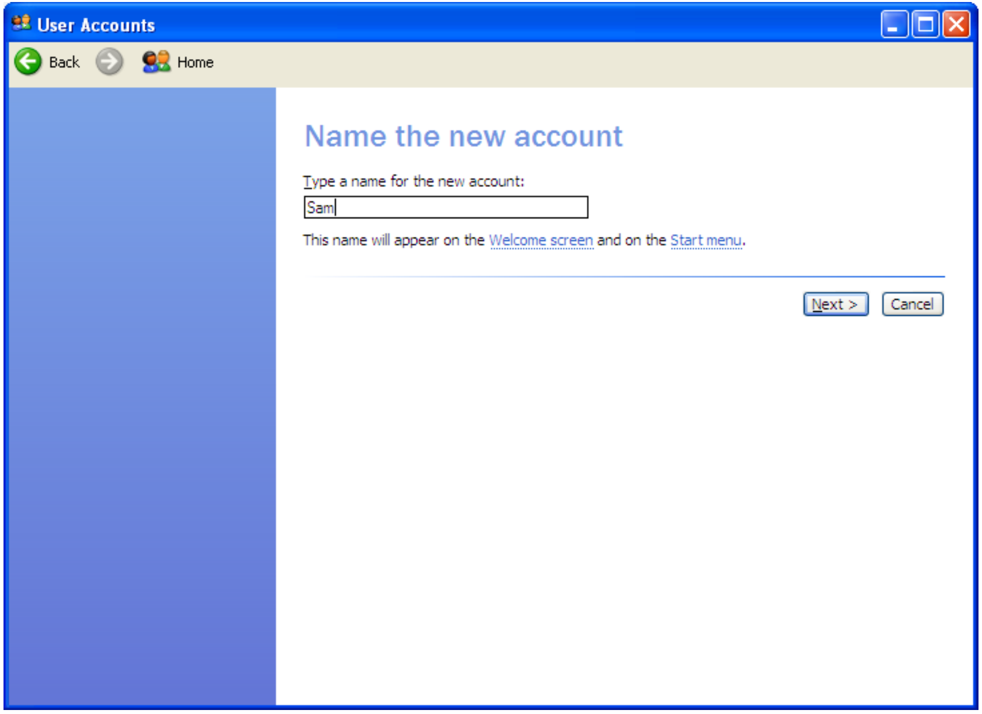
2. Under Pick a category, click User Accounts.



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.



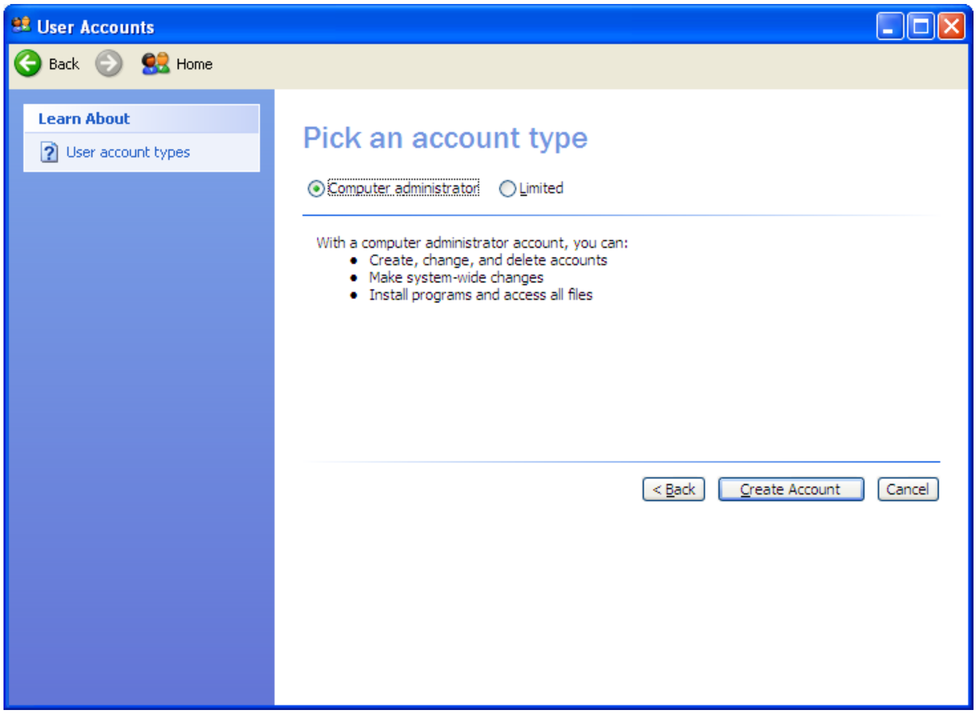
Name the new account

Type a name for the new account:

Sam

This name will appear on the Welcome screen and on the Start menu.

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



Pick an account type

● Computer administrator ○ Limited

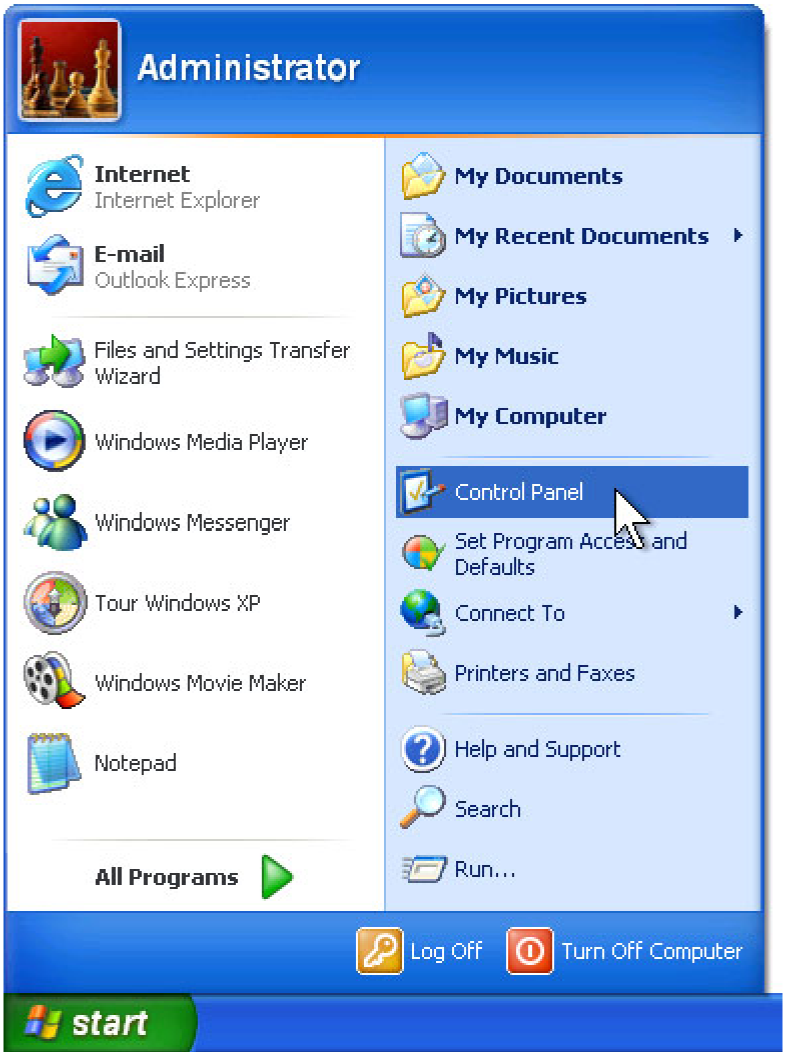
With a computer administrator account, you can:
- Create, change, and delete accounts
- Make system-wide changes
- Install programs and access all files

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

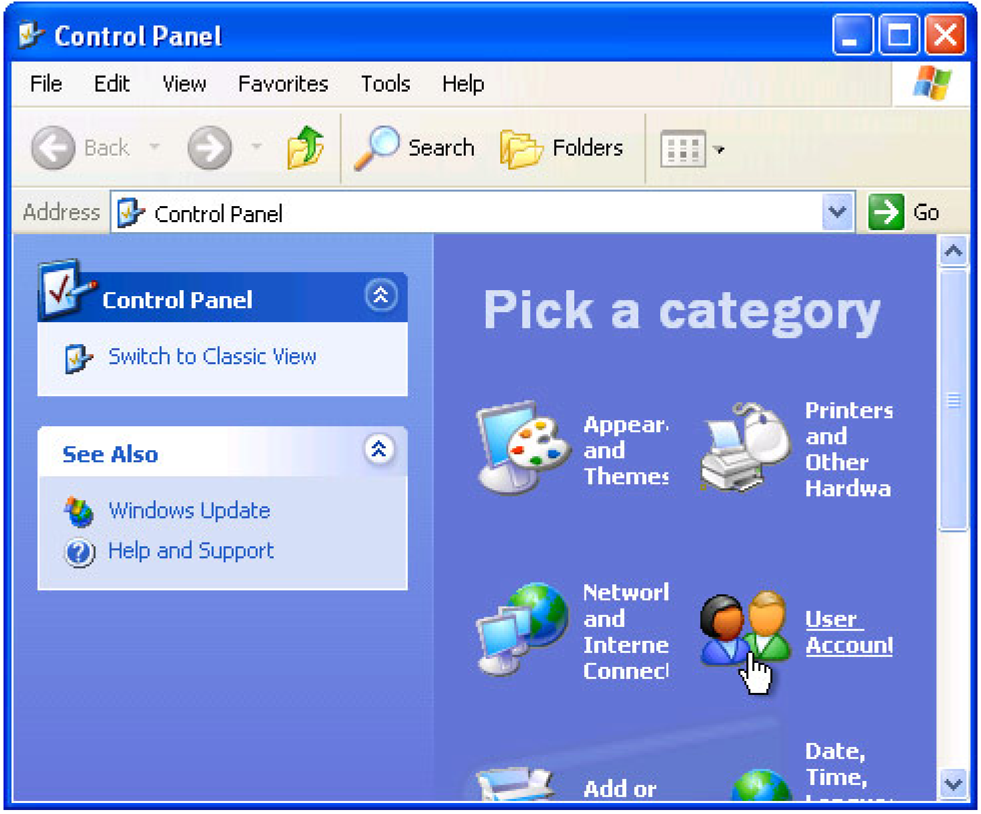
How to Remove a Windows Administrative User Account

PA-DSS 3.1
PCI 8.5.4
PCI 8.5.5

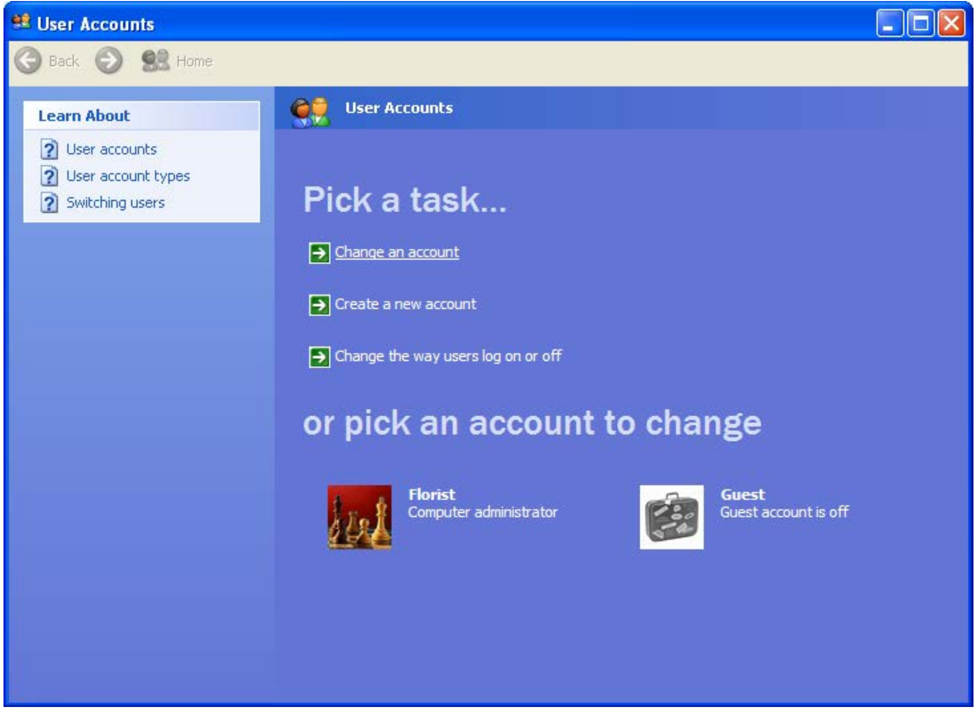
1. Log on to your computer as “Florist” (Florist has administrative privileges). Click Start, and then click Control Panel.



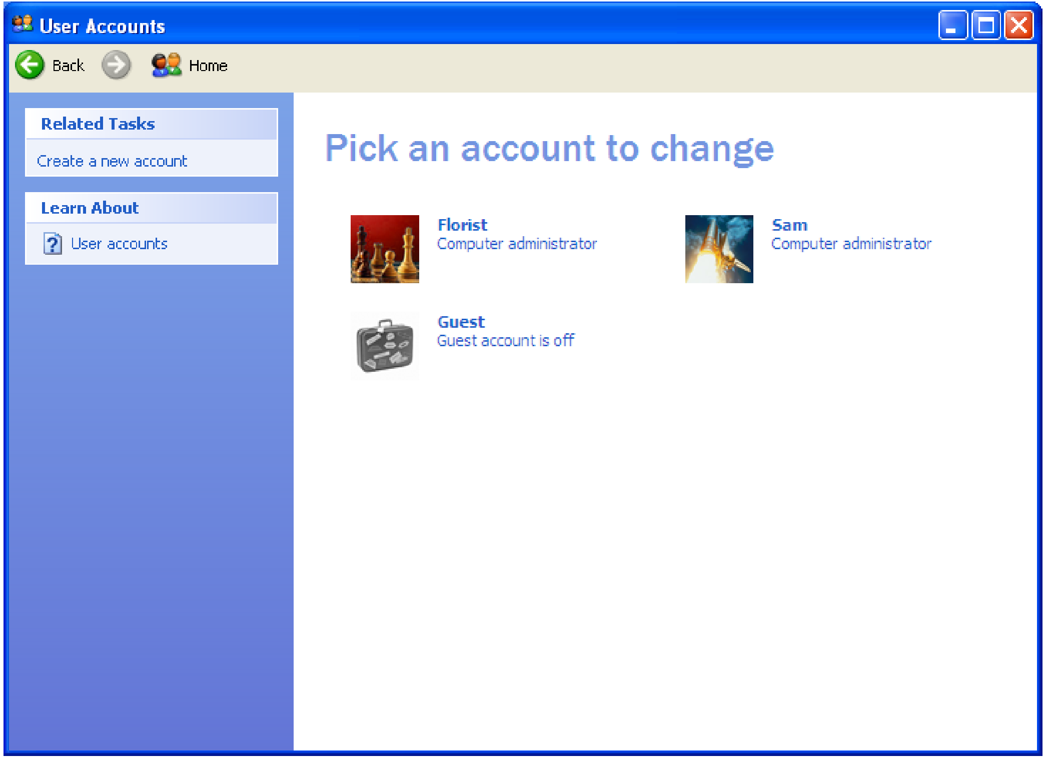
2. Under Pick a category, click User Accounts.



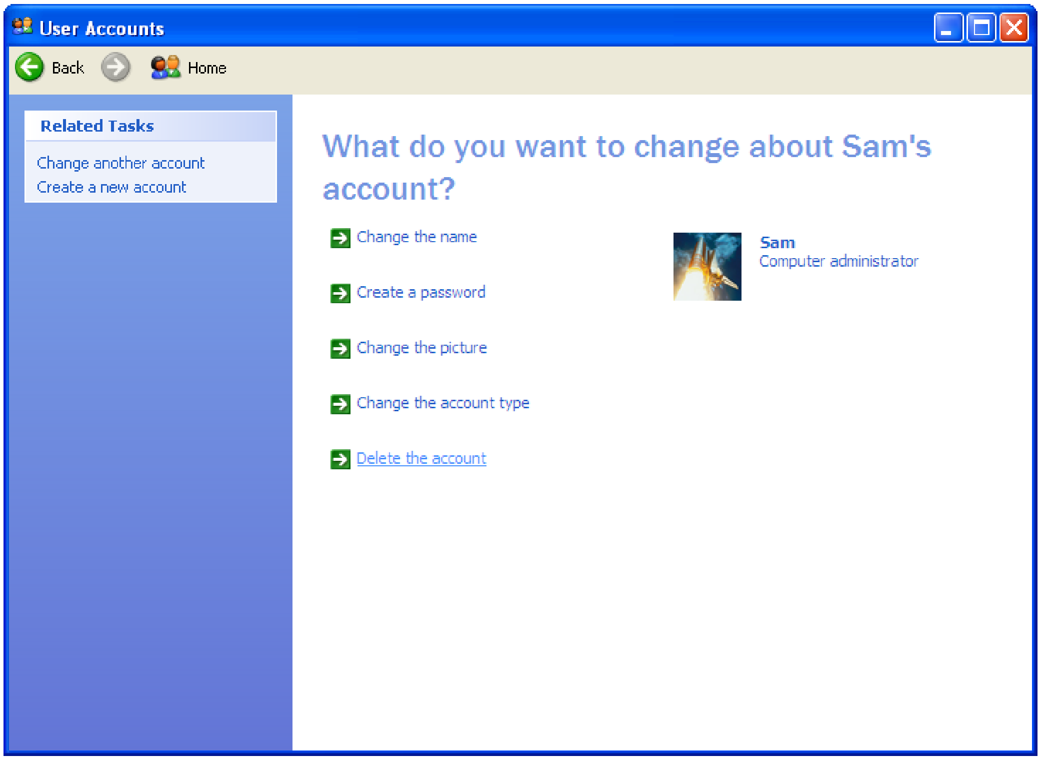
3. Under Pick a task, click Change an account.



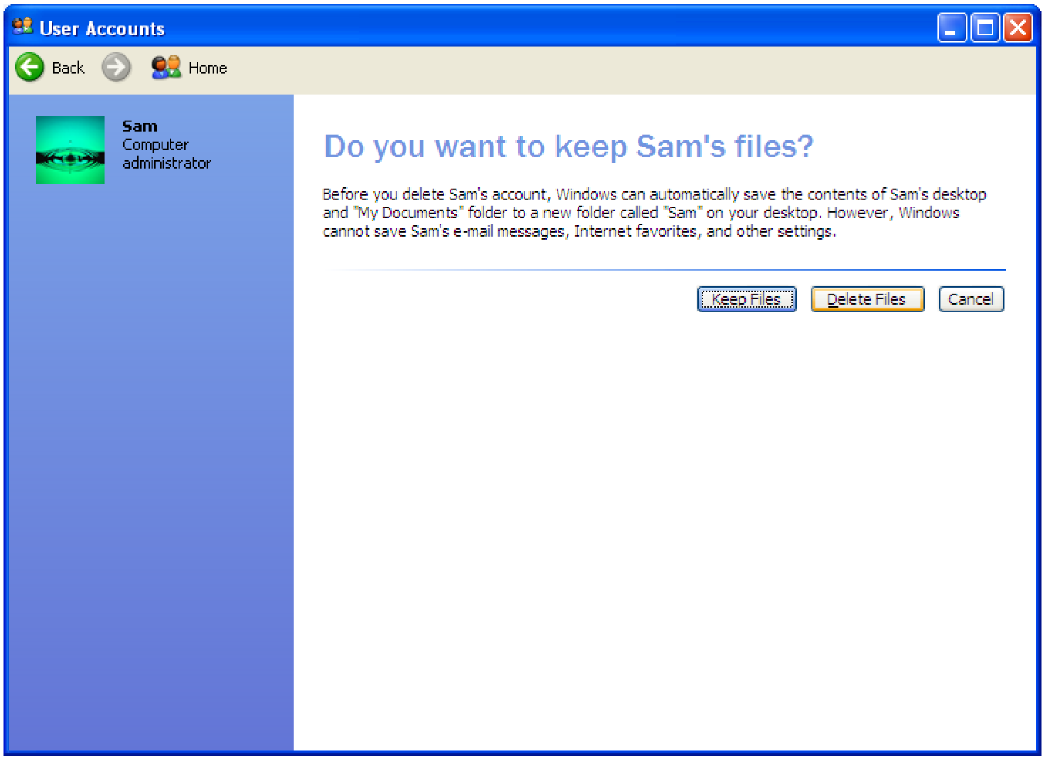
4. Under Pick an account to change, click the name of the account you want to delete.



5. Click on Delete the account.



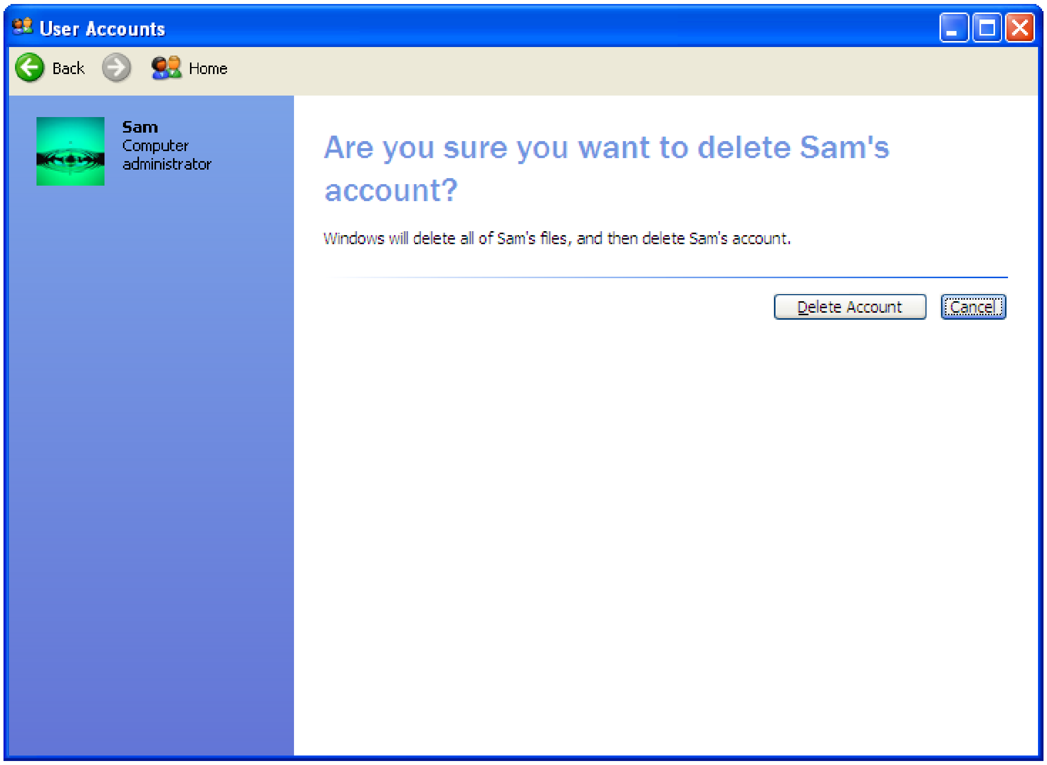
6. Click on the Delete Files button.



Do you want to keep Sam's files?

Before you delete Sam's account, Windows can automatically save the contents of Sam's desktop and "My Documents" folder to a new folder called "Sam" on your desktop. However, Windows cannot save Sam's e-mail messages, Internet favorites, and other settings.

7. Click the Delete Account button.



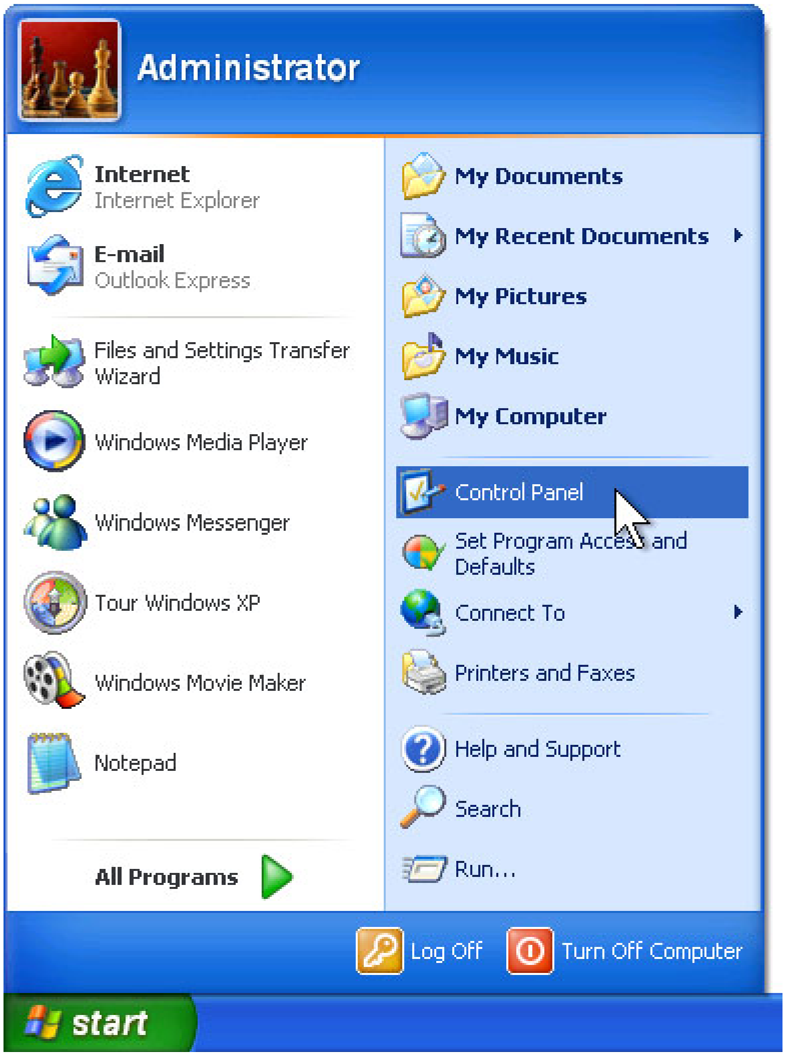
Are you sure you want to delete Sam's account?

Windows will delete all of Sam's files, and then delete Sam's account.

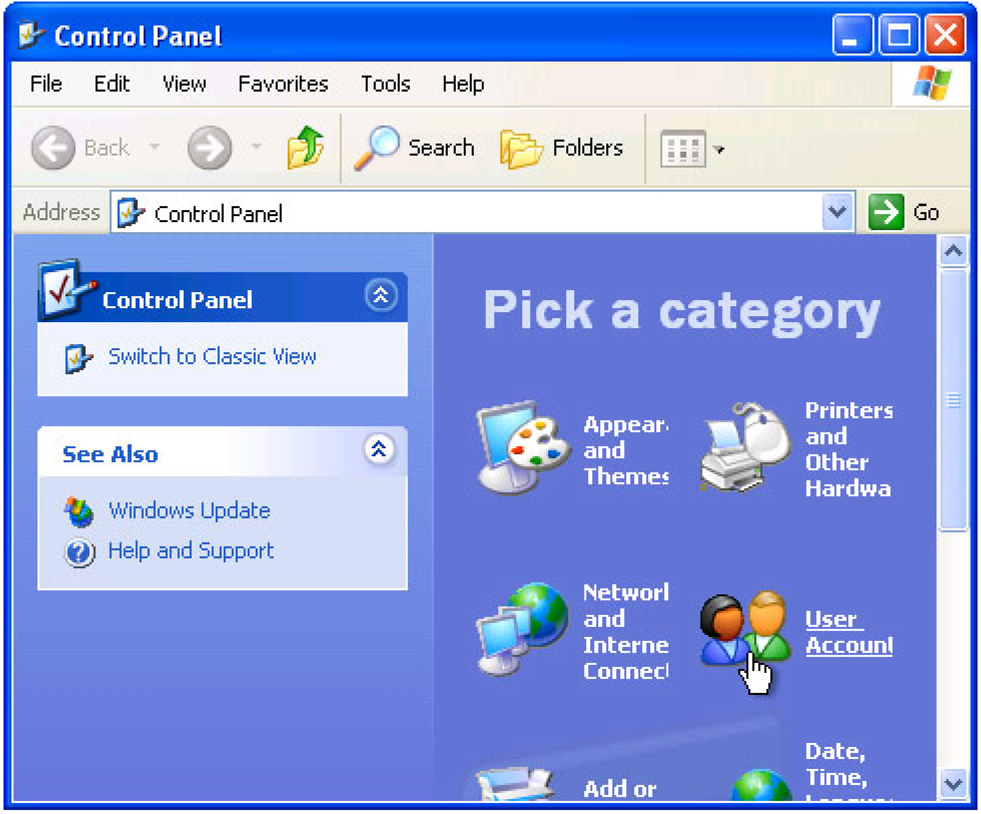
How to Remove a Windows Non-Administrative User Account

PA-DSS 3.1
PCI 8.5.4
PCI 8.5.5

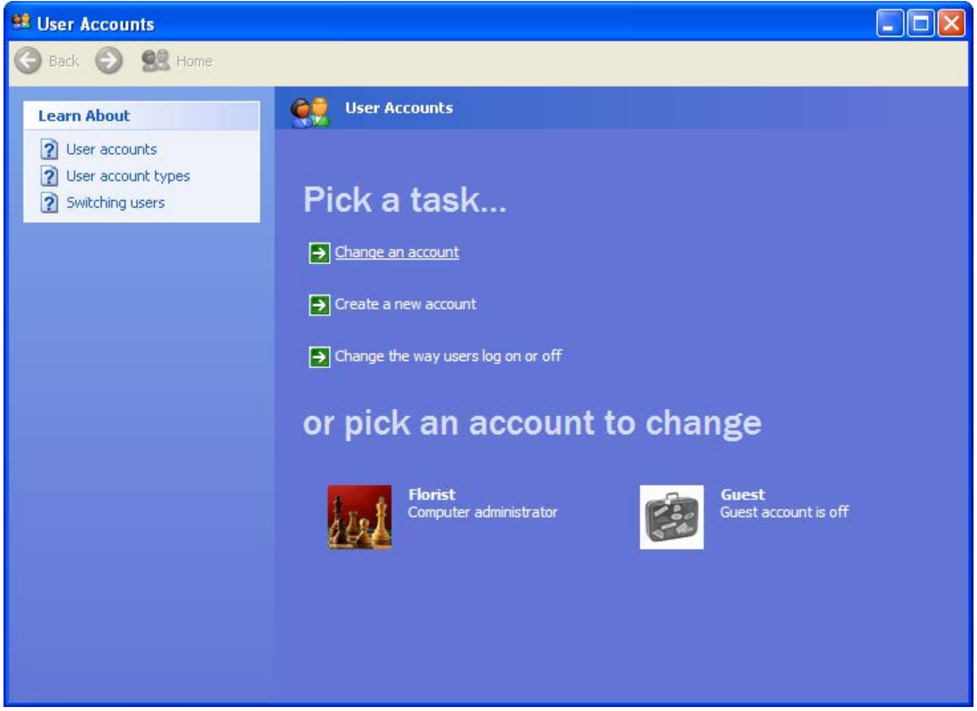
1. Log on to your computer as “Florist” (Florist has administrative privileges). Click Start, and then click Control Panel.



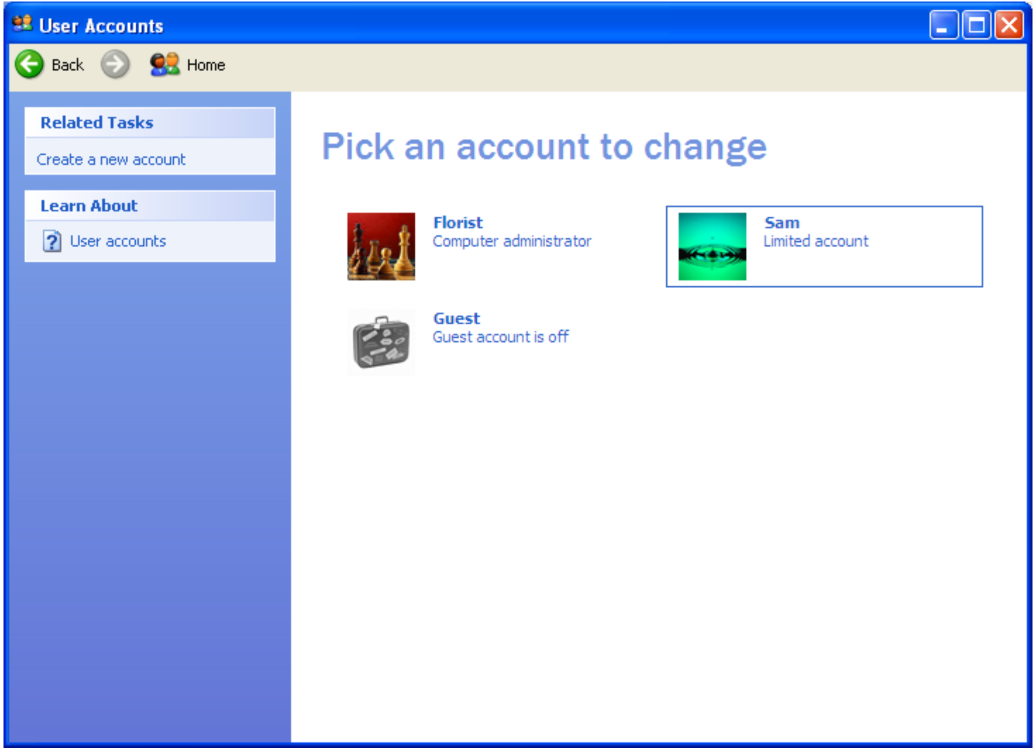
2. Under Pick a category, click User Accounts.



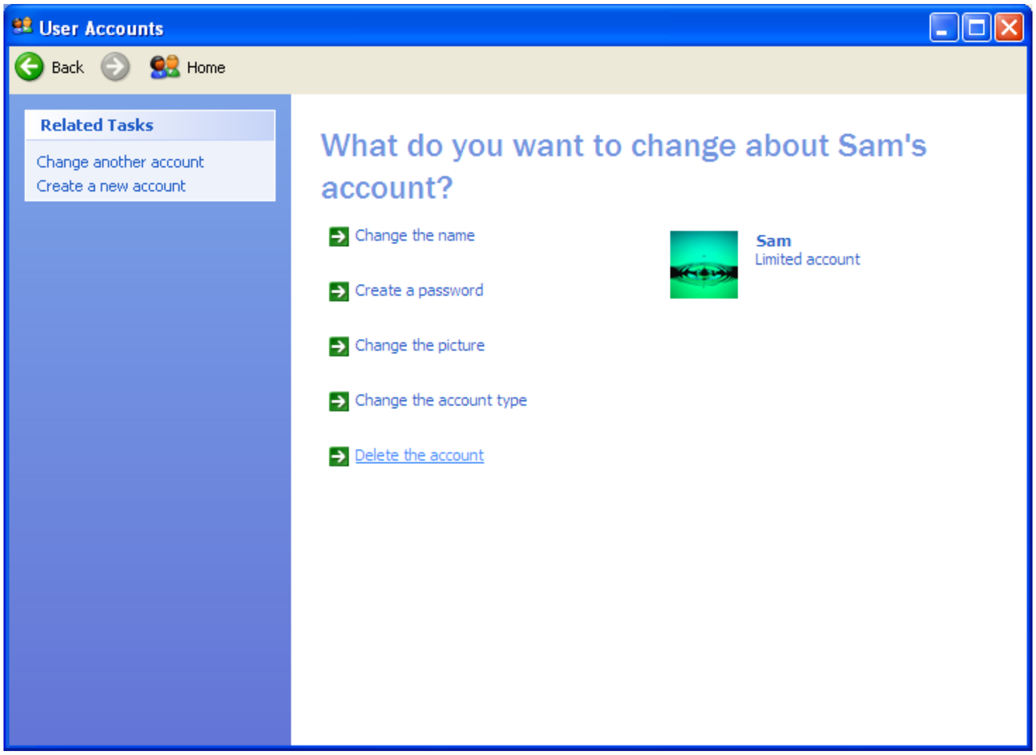
3. Under Pick a task, click Change an account.



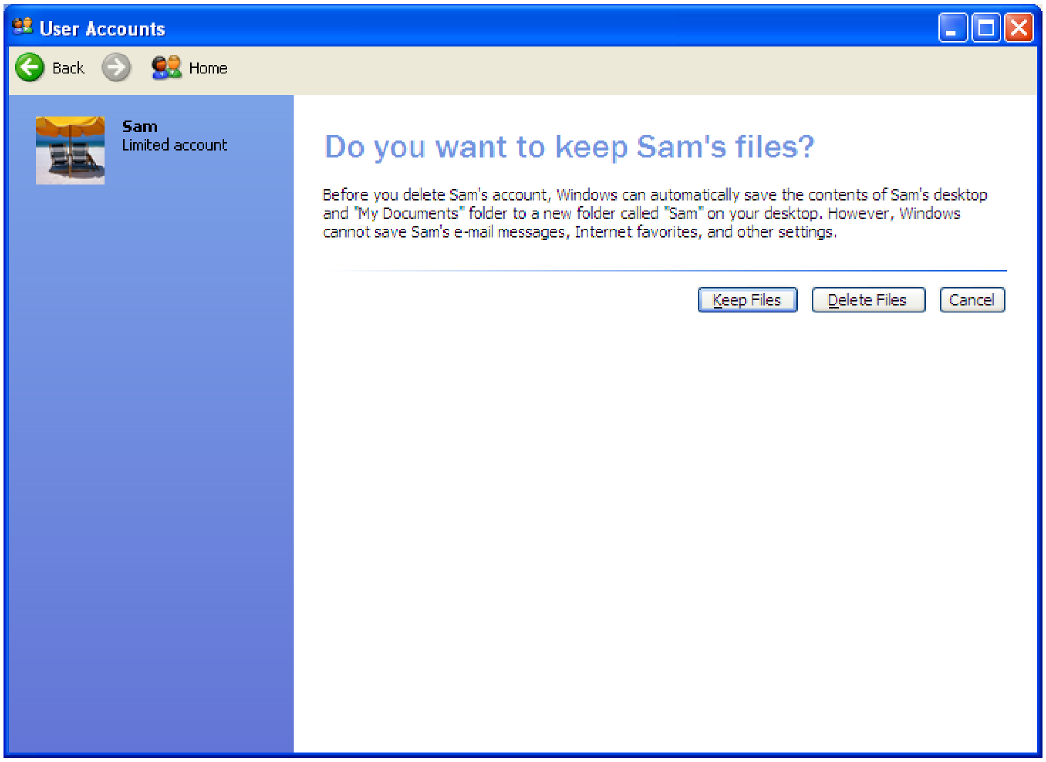
4. Under Pick an account to change, click the name of the account you want to delete.



5. Click on Delete the account.



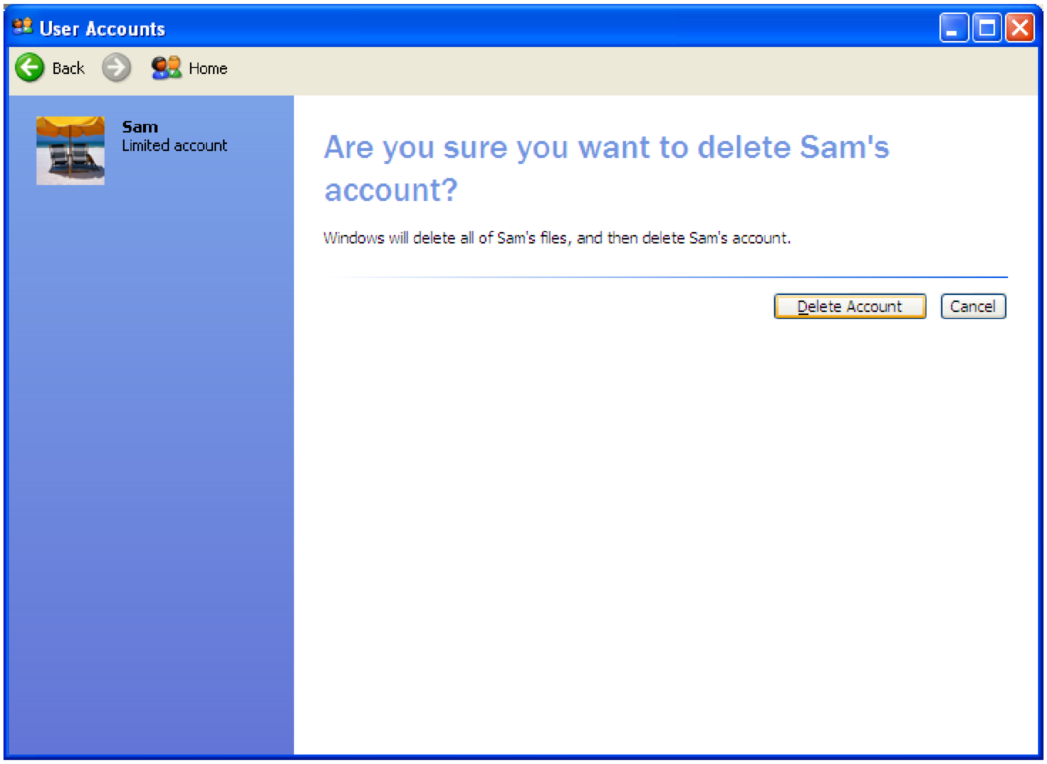
6. Click on the Delete Files button.



Do you want to keep Sam's files?

Before you delete Sam's account, Windows can automatically save the contents of Sam's desktop and "My Documents" folder to a new folder called "Sam" on your desktop. However, Windows cannot save Sam's e-mail messages, Internet favorites, and other settings.

7. Click the Delete Account button.



Are you sure you want to delete Sam's account?

Windows will delete all of Sam's files, and then delete Sam's account.

How to Add/Remove a Eagle User Account

PA-DSS 3.1
PCI 8.5.4
PCI 8.5.5

Eagle provides a robust Employee Maintenance module which allows shop owners and managers to add, update, and delete employees as needed.

Add New Employees:

From the Eagle **Welcome** window:

1. Select the **Shop Management** button.
2. Select the **Employees** button, located in the Manage section along the left side of the page.
3. Select the **Employee Maintenance** button.
4. Select the **New** button.
5. Enter an **Employee ID**, up to 10 characters. This will be the employee's login ID, as well as the ID used to track employee time and other functions.
6. In the **Name**, **Address 1**, **Address 2**, **City**, **State**, **ZIP Code**, and **Phone** fields, insert the necessary employee information. The City and State fields default to your company's city and state.
7. For **Home Store** and **Department**, select from those available by clicking the drop-down arrow in each field.
8. The **Date of Birth** and **Hire Date** fields are optional. Fill these in only if you prefer to have this information.

   [**Note**: When an employee leaves, you can enter his/her **Separation Date**.]
9. The driver's **License** and **SSN** (Social Security Number) fields are optional. Fill these in only if you prefer to have this information.
10. The **Payroll Type** and **Payroll Number** fields are optional. Fill these in only if you prefer to have this information.
11. The **Time Clock Type** field defaults to **Hourly**. If needed, click the drop-down arrow to change this to **Salaried**.
12. Click the **User Group** drop-down arrow to select the user group to which the employee belongs. The three user group options are **Administrator**, **Manager** and **Staff**.

    [**Note:** Employees assigned to the same **Department** do not have to be assigned to the same user group.]
13. Enter a **Password** for the employee's login ID.
14. Re-enter the employee's password in the **Verify Password** field.
15. If desired, you can enter additional information about this employee in the **Notes** section.
16. Select the **Save** button.

Update Employee Information

From the Eagle **Welcome** window:

1. Select the **Shop Management** button.
2. Select the **Employees** button, located in the Manage section along the left side of the page.
3. Select the **Employee Maintenance** button.
4. Double-click the Employee's **Name**.
5. Make changes as needed, using the previous **Add a New Employee** steps as a guide.
6. Click **Save**.

Put an Employee on Inactive Status

Setting an employee as inactive prevents the employee from logging onto Eagle. You should assign inactive status to employees who have taken a leave or absence or who have left the company.

From the Eagle **Welcome** window:

1. Select the **Shop Management** button.
2. Select the **Employees** button, located in the Manage section along the left side of the page.
3. Select the **Employee Maintenance** button.
4. Double-click the Employee's **Name**.
5. De-select the **Active Employee** check box or enter a **Separation Date** that is earlier than the current date.
6. Click **Save**.

Delete an Employee from the System

When an employee leaves the company, you have the option of completely deleting the employee from the system.

[**Note:** The employee administrator cannot be deleted, nor can employees who are currently logged in to the system. You also cannot delete an employee who has entered orders or who has been recorded as the designer of an order.]

From the Eagle **Welcome** window:

1. Select the **Shop Management** button.
2. Select the **Employees** button, located in the Manage section along the left side of the page.
3. Select the **Employee Maintenance** button.
4. Double-click the Employee's **Name**.
5. Select the **Delete** button.
6. Select the **Save** 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 Eagle on a computer which, in the past, was used for other purposes.
- Your Eagle 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.

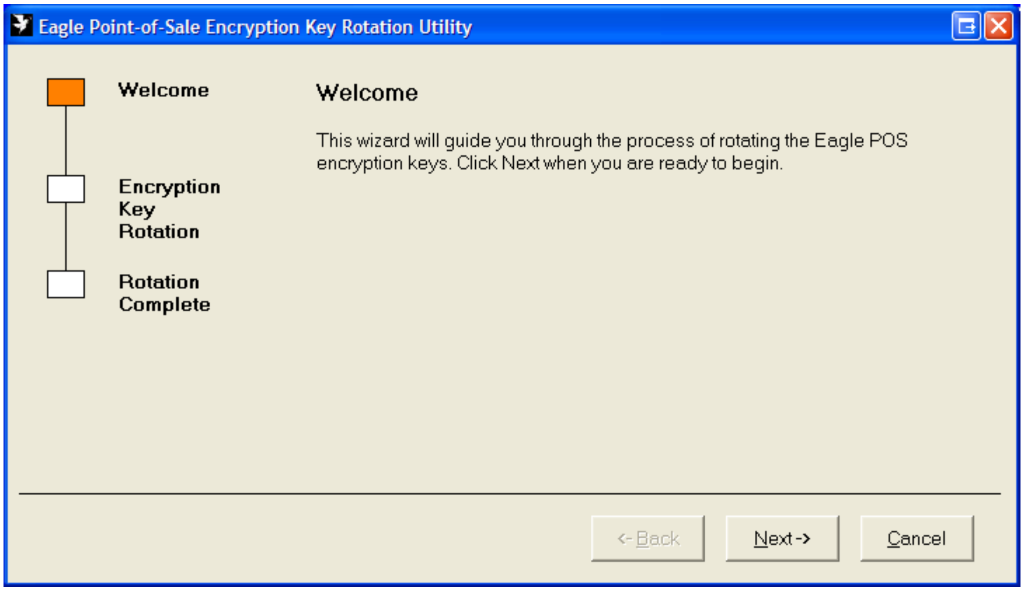
See:
Appendix: Using the Eraser Tool.

How to Change your Eagle Data Encryption Key

PA-DSS 1.5
PCI DSS 3.6
PCI DSS 8.5

The Eagle Encryption Key Rotation Utility is an application provided by Teleflora to rotate the data encryption keys for you. The Eagle Encryption Key Rotation Utility is located in the Eagle FMS directory under Program Files.

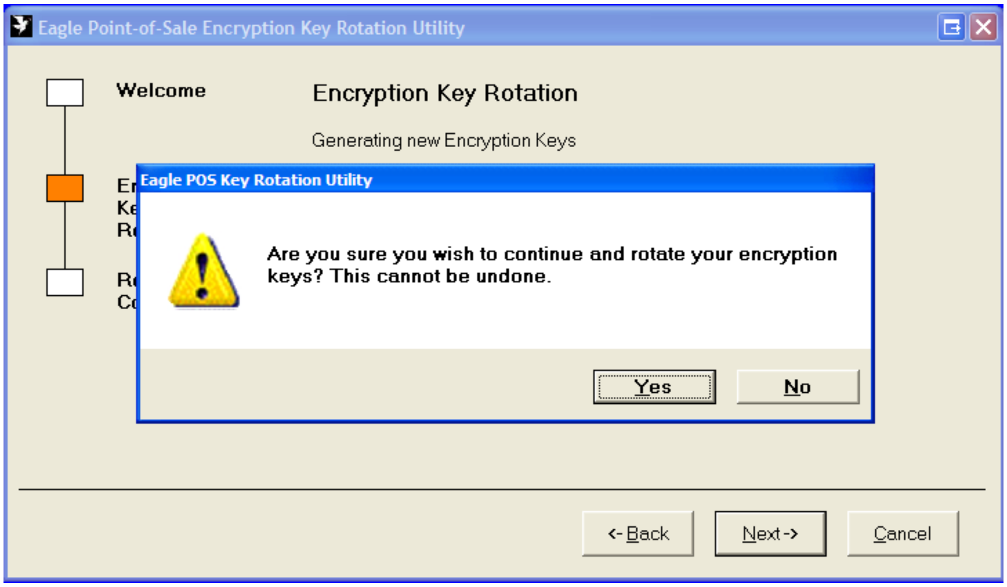
This Utility can only be executed by a Windows Administrator. Widows will display an error if you are not logged in as an administrator.



Welcome

This wizard will guide you through the process of rotating the Eagle POS encryption keys. Click Next when you are ready to begin.

1. Launch Eagle Encryption Key Rotation Utility and click on Next.



Eagle Point-of-Sale Encryption Key Rotation Utility

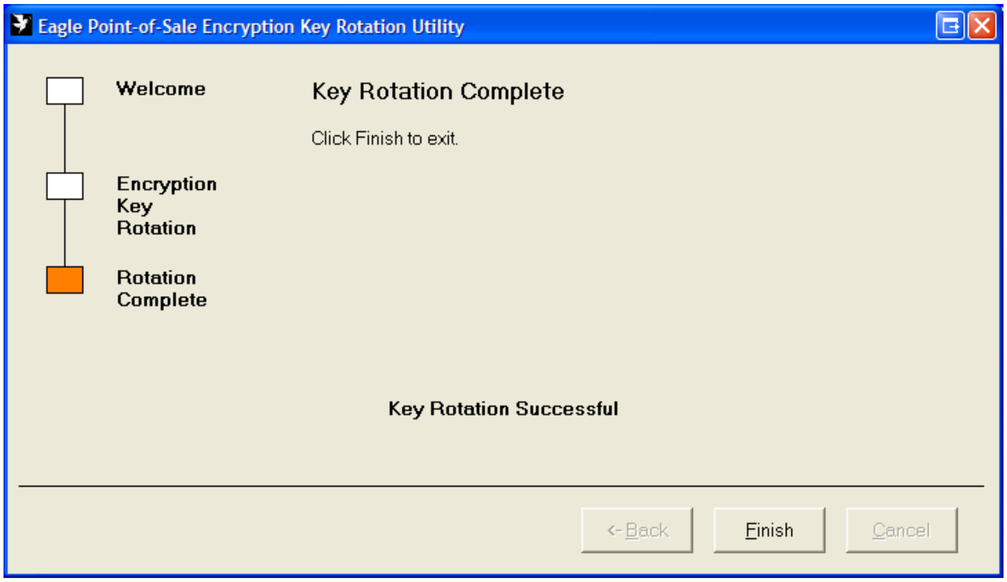
Encryption Key Rotation

Generating new Encryption Keys

Eagle POS Key Rotation Utility

Are you sure you wish to continue and rotate your encryption keys? This cannot be undone.

2. Click Yes to continue with the key rotation.



Eagle Point-of-Sale Encryption Key Rotation Utility

Key Rotation Complete

Click Finish to exit.

Key Rotation Successful

3. Click Finish to close the application.

How to Create a "Strong" Password

PCI 8.5

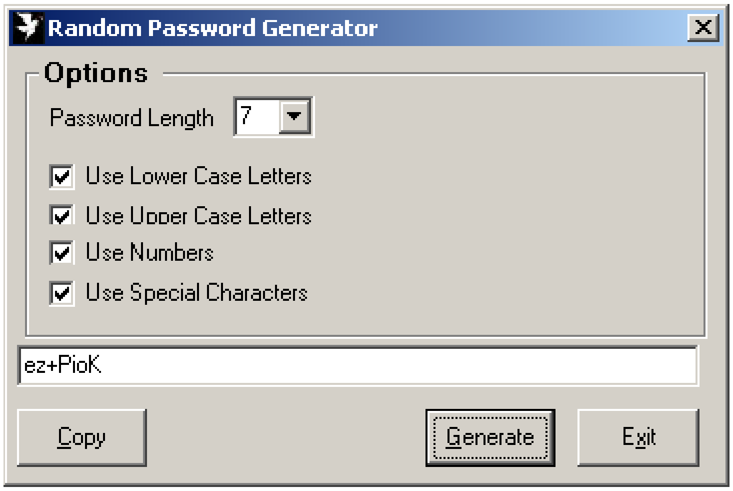
PCI DSS gives specifications as to password strengths required. Following are relevant PCI DSS specifications, as well as some techniques you may use to help generate random passwords.

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 Eagle to assist you in generating secure passwords. Password Generator is located at C:\Program Files\EagleFMS\RandomPassword.exe



Random Password Generator

Options

Password Length 7

☑ Use Lower Case Letters
☑ Use Upper Case Letters
☑ Use Numbers
☑ Use Special Characters

ez+PioK

By default Special Characters, Numbers, 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 Select or deselect Use Special Charaters, Use Numbers, Use Upper Case Letters, or Use Lower Case Letters. To modify the Password Length select the desired length from the available list.

To create password, Click Generate.

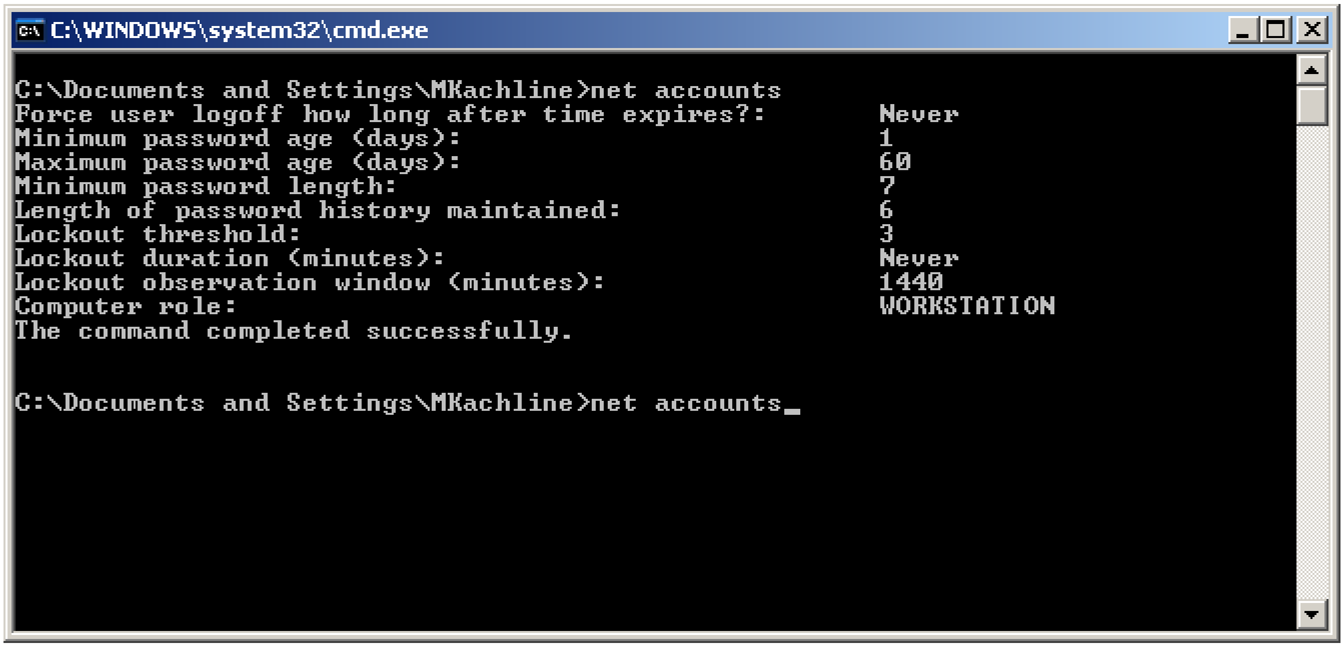
To select a different password click generate again.

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).



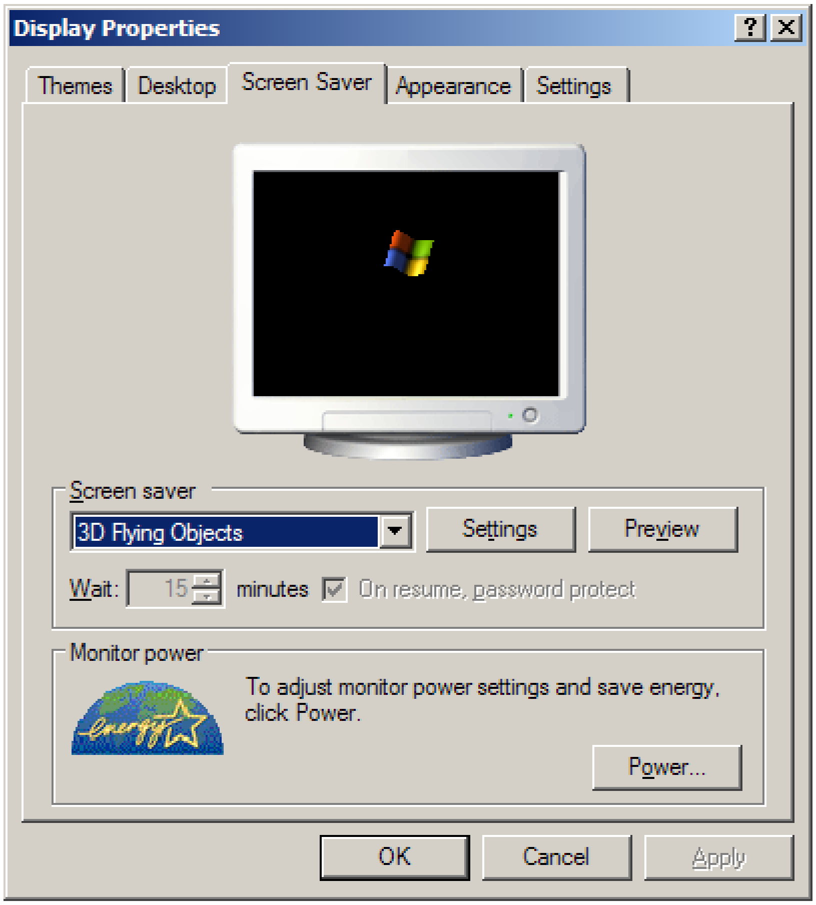
```
C:\Documents and Settings\MKachline>net accounts
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          1
Maximum password age (days):                          60
Minimum password length:                              7
Length of password history maintained:                6
Lockout threshold:                                    3
Lockout duration (minutes):                           Never
Lockout observation window (minutes):                 1440
Computer role:                                        WORKSTATION
The command completed successfully.


C:\Documents and Settings\MKachline>net accounts_
```

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



Screen saver: 3D Flying Objects

Wait: 15 minutes ☑ On resume, password protect

To adjust monitor power settings and save energy, click Power.

PA-DSS 3.1
PCI 8.5.15

In order to be compliant with PA-DSS requirements, each workstation with access to the Eagle 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.

Setup / Configure the Netgear FVS338 Firewall

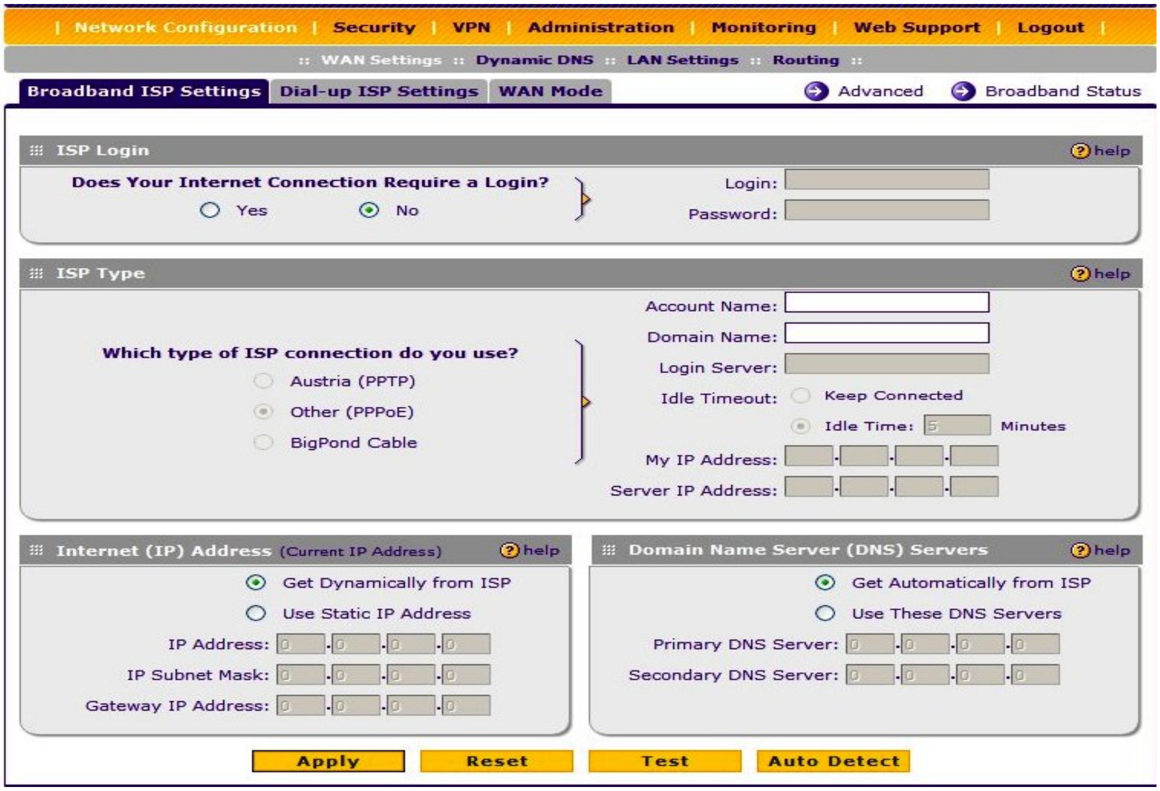
To access the router control panel:

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


| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Dynamic DNS :: LAN Settings :: Routing ::
Broadband ISP Settings
Dial-up ISP Settings
WAN Mode
Advanced
Broadband Status
ISP Login
help
ISP Type
help
Internet (IP) Address (Current IP Address)
help
Domain Name Server (DNS) Servers
help
Apply
Reset
Test
Auto Detect

Does Your Internet Connection Require a Login?
○ Yes ● No
Login:
Password:

Which type of ISP connection do you use?
○ Austria (PPTP)
● Other (PPPoE)
○ BigPond Cable

Account Name:
Domain Name:
Login Server:
Idle Timeout: ○ Keep Connected
● Idle Time: 5 Minutes
My IP Address: . . .
Server IP Address: . . .

● Get Dynamically from ISP
○ Use Static IP Address
IP Address: 0.0.0.0
IP Subnet Mask: 0.0.0.0
Gateway IP Address: 0.0.0.0

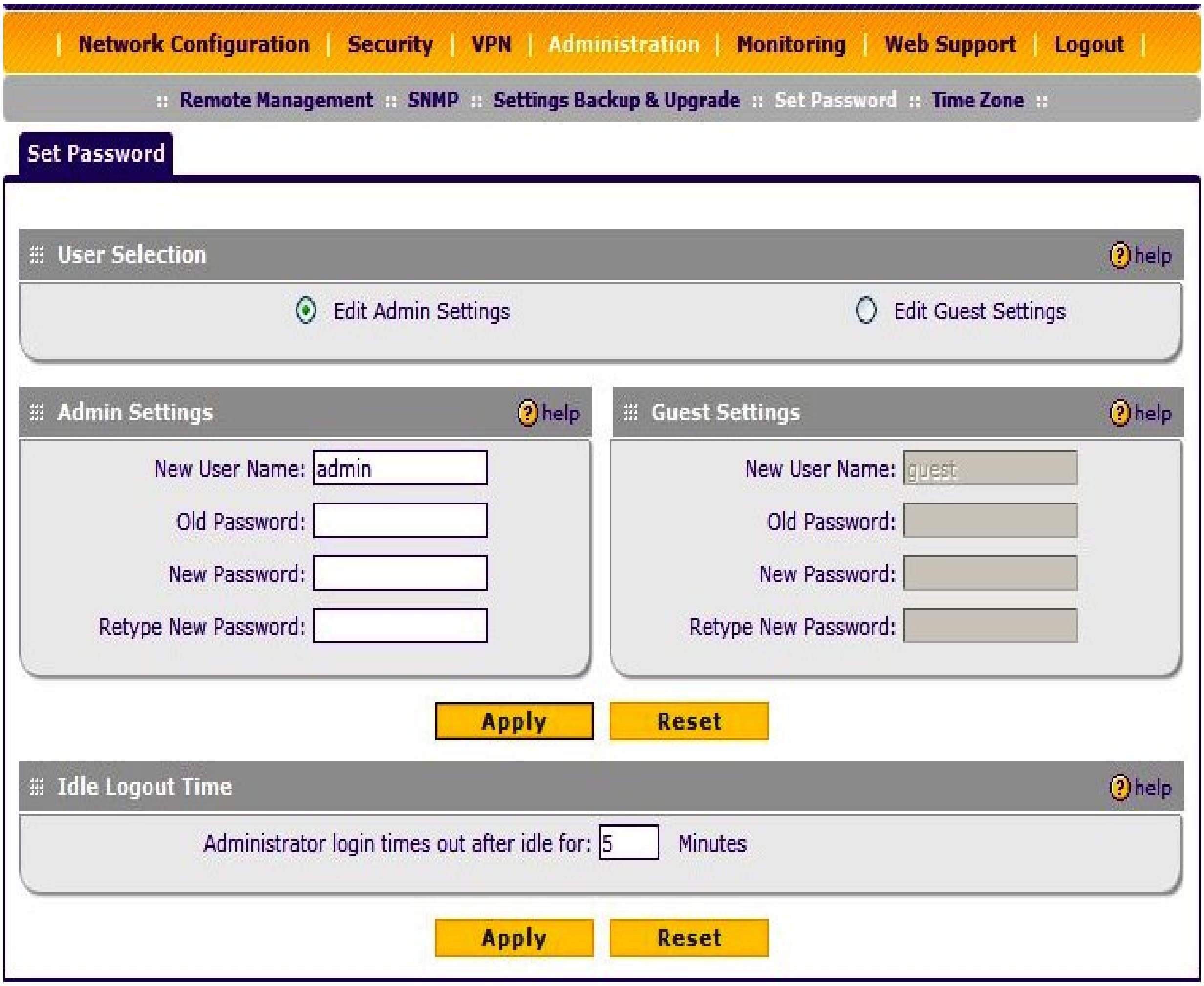
● Get Automatically from ISP
○ Use These DNS Servers
Primary DNS Server: 0.0.0.0
Secondary DNS Server: 0.0.0.0

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


| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Set Password :: Time Zone ::
Set Password
User Selection
help
Admin Settings
help
Guest Settings
help
Apply
Reset
Idle Logout Time
help
Apply
Reset

● Edit Admin Settings ○ Edit Guest Settings

Admin Settings

New User Name: admin
Old Password:
New Password:
Retype New Password:

Guest Settings

New User Name: guest
Old Password:
New Password:
Retype New Password:

Administrator login times out after idle for: 5 Minutes

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

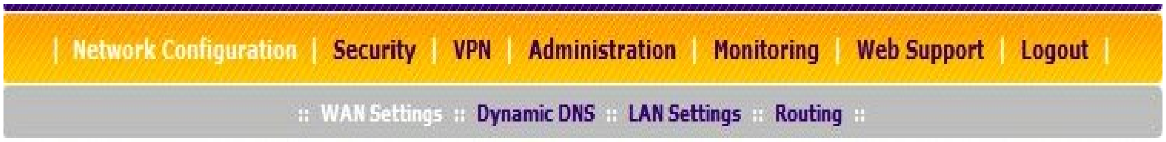
2. In the sub menu bar, click "Set Password"

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.

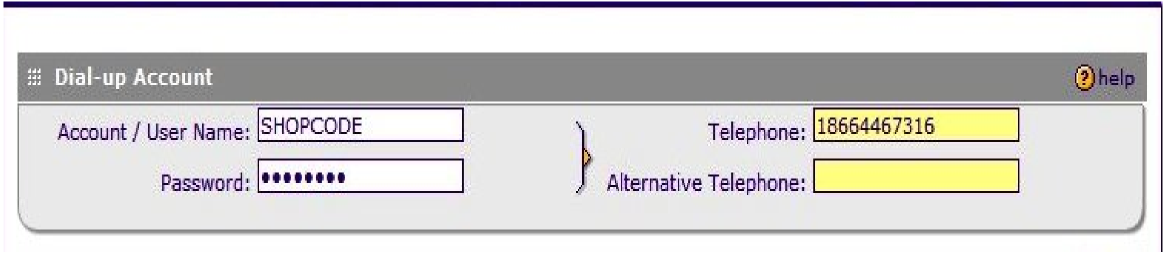
4. Change the guest password from "password" to "T3l3fl0r4".

5. Click "Apply" to complete the change

Step 4: The Dialup Connection


| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Dynamic DNS :: LAN Settings :: Routing ::

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

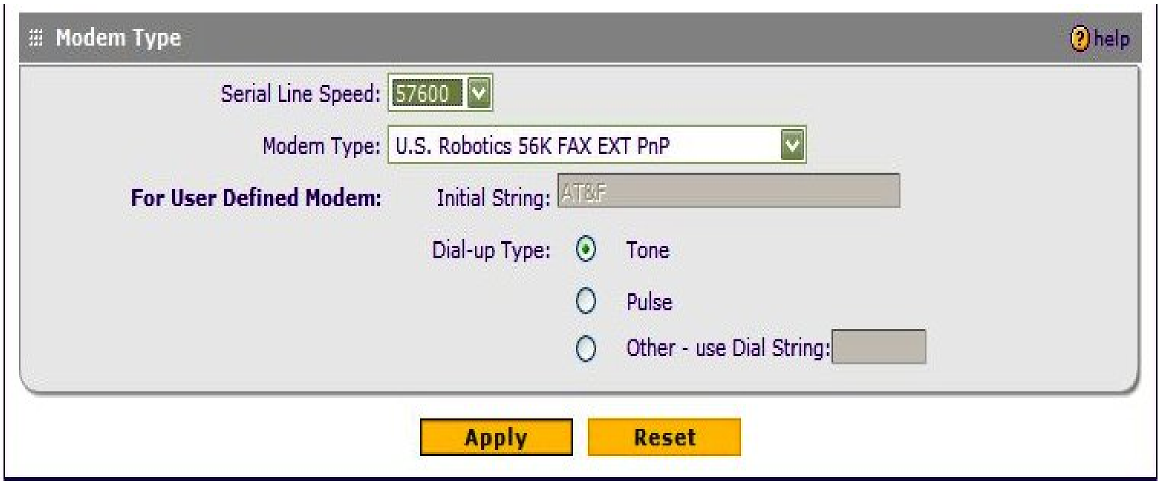


Account / User Name:	SHOPCODE
Password:	••••••••
Telephone:	18664467316
Alternative Telephone:	

A. Account / User Name: SHOPCODE ex: 00070750

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

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



Serial Line Speed: 57600

Modem Type: U.S. Robotics 56K FAX EXT PnP

For User Defined Modem: Initial String: AT&F

Dial-up Type: ● Tone

○ Pulse

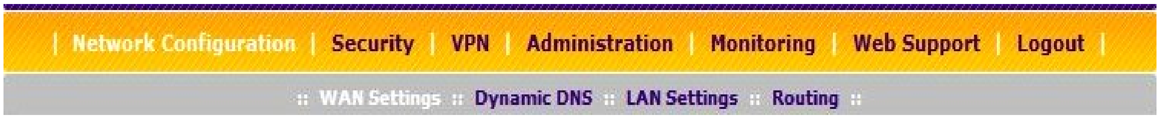
○ Other - use Dial String:

D. Set the Serial Line Speed to 57600.

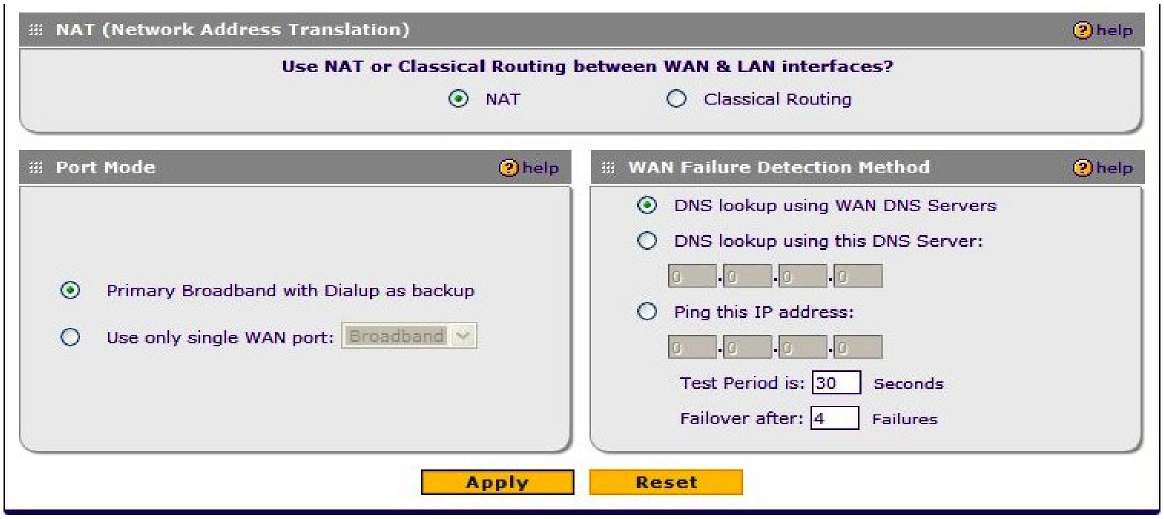
E. Select U.S. Robotics FAX PnP, from the Modem Type Dropdown box.

F. Leave everything else as defaults, click Apply.

Step 5: WAN Mode


| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Dynamic DNS :: LAN Settings :: Routing ::

Click Network configuration > Wan Settings



NAT (Network Address Translation)

Use NAT or Classical Routing between WAN & LAN interfaces?

● NAT ○ Classical Routing

Port Mode

● Primary Broadband with Dialup as backup

○ Use only single WAN port: Broadband

WAN Failure Detection Method

● DNS lookup using WAN DNS Servers

○ DNS lookup using this DNS Server: 0.0.0.0

○ Ping this IP address: 0.0.0.0

Test Period is: 30 Seconds

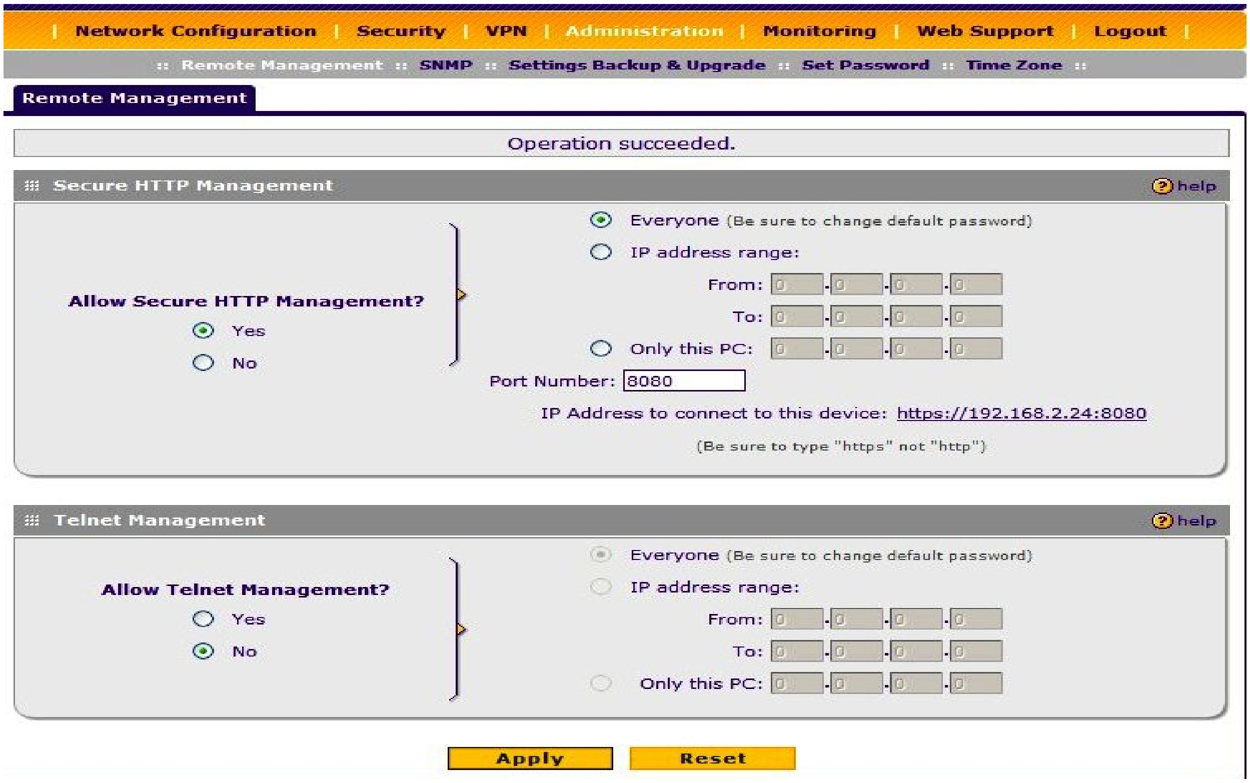
Failover after: 4 Failures

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


| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Set Password :: Time Zone ::
Remote Management
help
help
Apply
Reset

Operation succeeded.

Secure HTTP Management

Allow Secure HTTP Management?

● Yes
○ No

● Everyone (Be sure to change default password)
○ IP address range:
From: 0 . 0 . 0 . 0
To: 0 . 0 . 0 . 0
○ Only this PC: 0 . 0 . 0 . 0

Port Number: 8080

IP Address to connect to this device: https://192.168.2.24:8080

(Be sure to type "https" not "http")

Telnet Management

Allow Telnet Management?

○ Yes
● No

● Everyone (Be sure to change default password)
○ IP address range:
From: 0 . 0 . 0 . 0
To: 0 . 0 . 0 . 0
○ Only this PC: 0 . 0 . 0 . 0

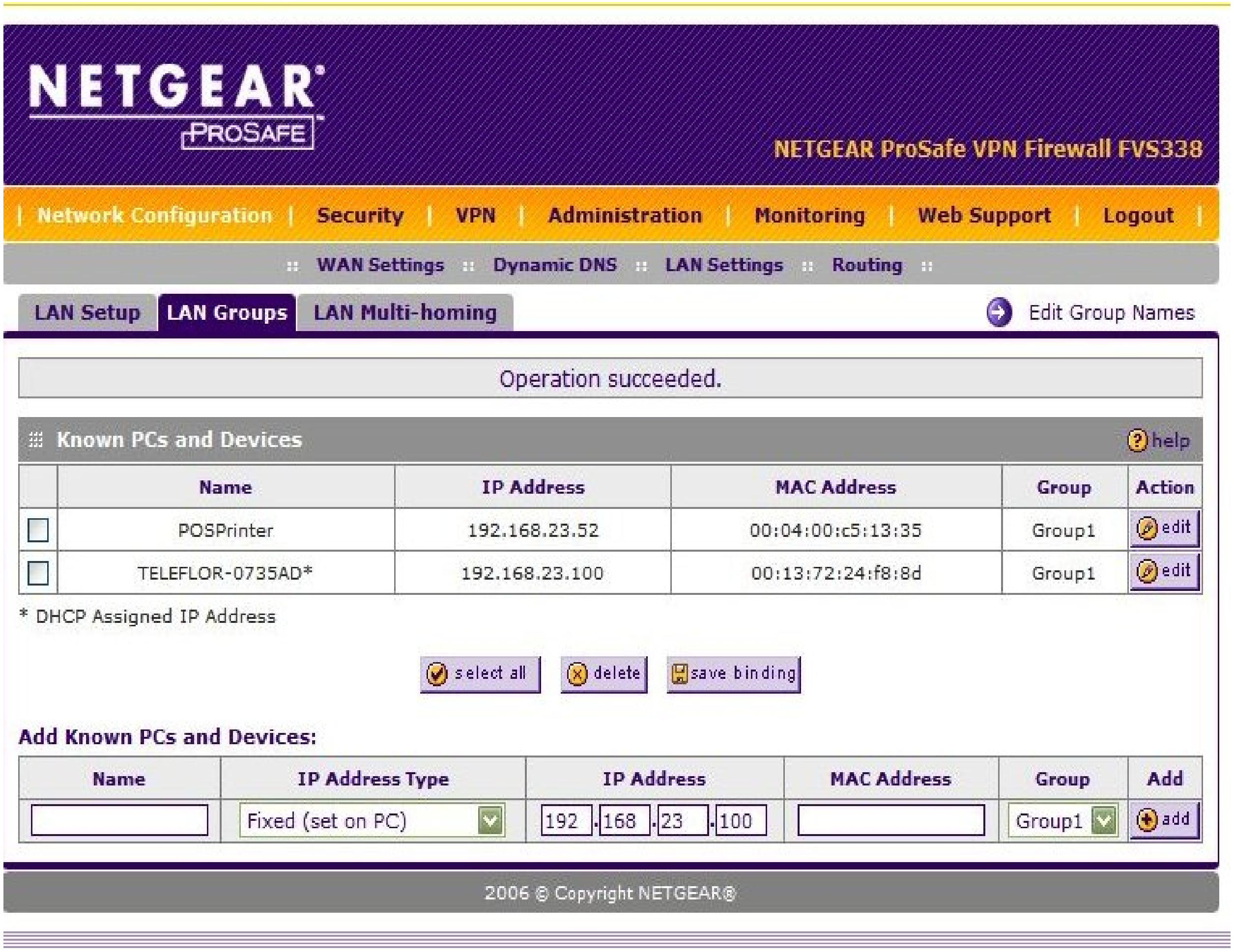
1. In the top menu bar, click "Administration".

2. In the sub menu bar, click "Remote Management".

3. Check the "Yes" button under "Allow Secure HTTP Management".

4. Click "Apply" to complete the change.

Step 7: Groups and Hosts



Operation succeeded.

Known PCs and Devices

	Name	IP Address	MAC Address	Group	Action
□	POSPrinter	192.168.23.52	00:04:00:c5:13:35	Group1	edit
□	TELEFLOR-0735AD*	192.168.23.100	00:13:72:24:f8:8d	Group1	edit

* DHCP Assigned IP Address

Add Known PCs and Devices:

Name	IP Address Type	IP Address	MAC Address	Group	Add
	Fixed (set on PC)	192.168.23.100		Group1	add

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".

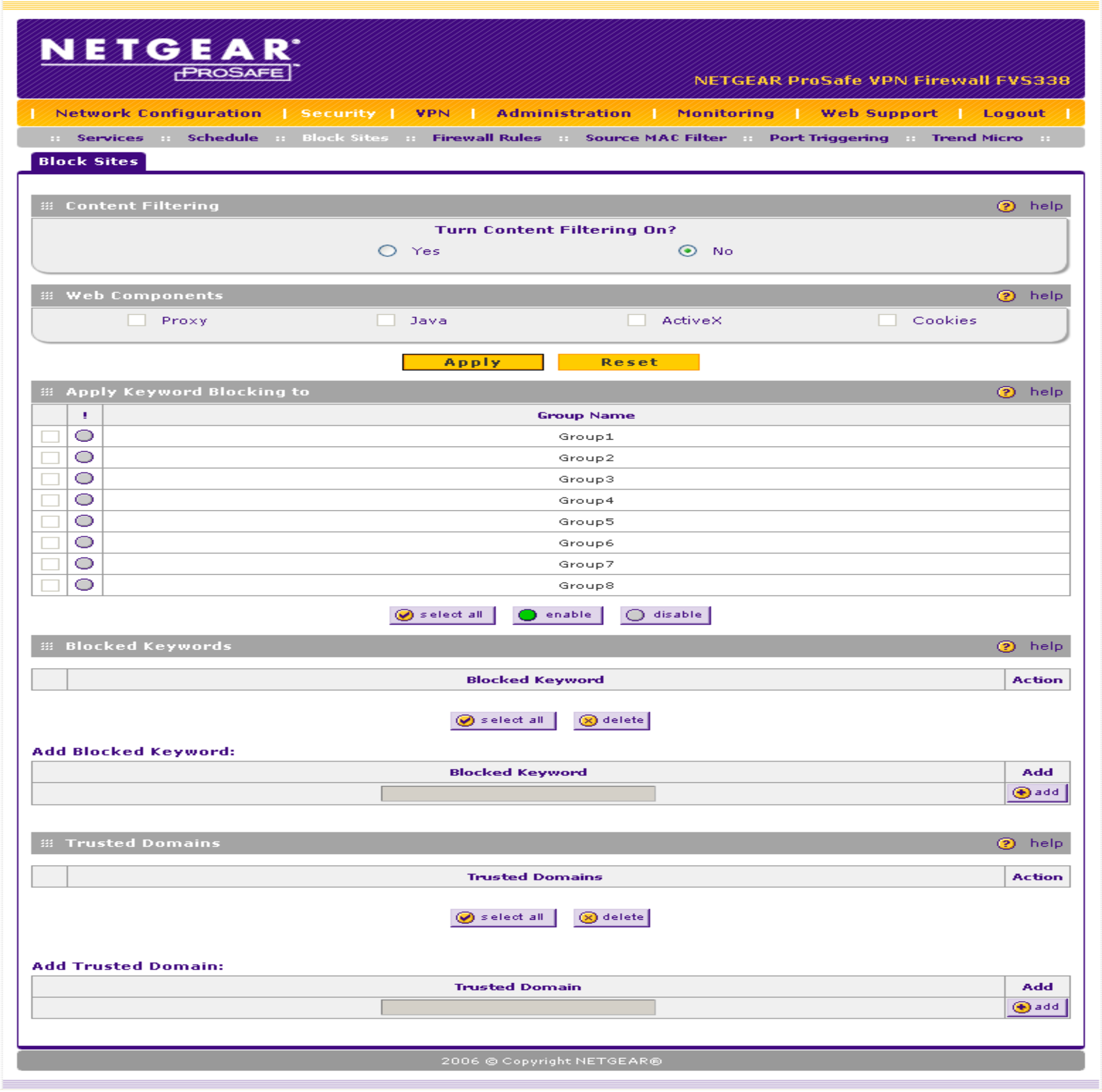
2. Using the drop down menu under "IP Address Type", select "Reserved".

   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


NETGEAR PROSAFE
NETGEAR ProSafe VPN Firewall FVS338
| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Block Sites :: Firewall Rules :: Source MAC Filter :: Port Triggering :: Trend Micro ::
Block Sites
help
Apply
Reset
select all
enable
disable
delete
add
2006 © Copyright NETGEAR®

Content Filtering

Turn Content Filtering On?

○ Yes ● No

Web Components

□ Proxy □ Java □ ActiveX □ Cookies

Apply Keyword Blocking to

	!	Group Name
□	○	Group1
□	○	Group2
□	○	Group3
□	○	Group4
□	○	Group5
□	○	Group6
□	○	Group7
□	○	Group8

Blocked Keywords

	Blocked Keyword	Action

Add Blocked Keyword:

Blocked Keyword	Add
	add

Trusted Domains

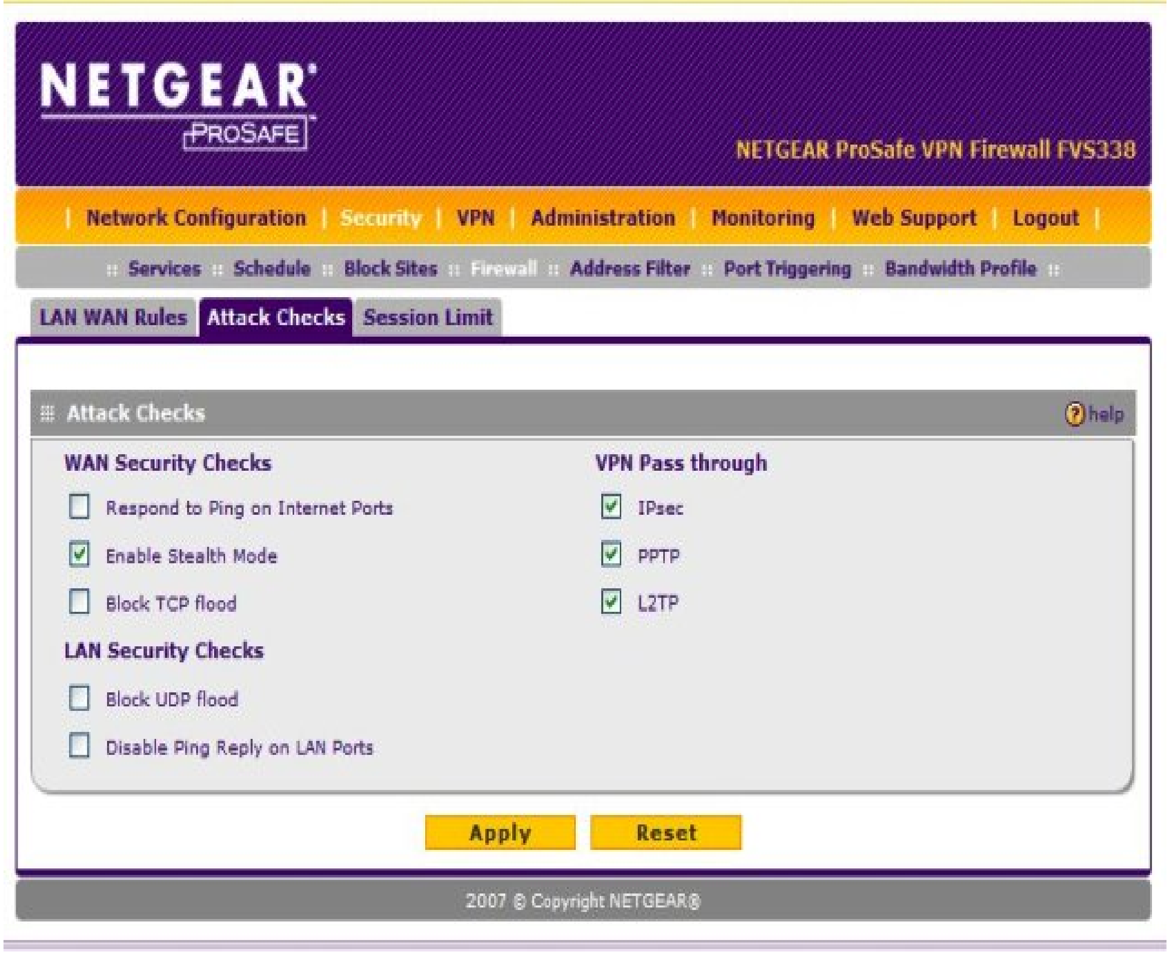
	Trusted Domains	Action

Add Trusted Domain:

Trusted Domain	Add
	add

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


NETGEAR
PROSAFE
NETGEAR ProSafe VPN Firewall FVS338
| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Block Sites :: Firewall :: Address Filter :: Port Triggering :: Bandwidth Profile ::
LAN WAN Rules
Attack Checks
Session Limit
help
Apply
Reset
2007 © Copyright NETGEAR®

Attack Checks

WAN Security Checks

□ Respond to Ping on Internet Ports

☑ Enable Stealth Mode

□ Block TCP flood

LAN Security Checks

□ Block UDP flood

□ Disable Ping Reply on LAN Ports

VPN Pass through

☑ IPsec

☑ PPTP

☑ L2TP

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

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

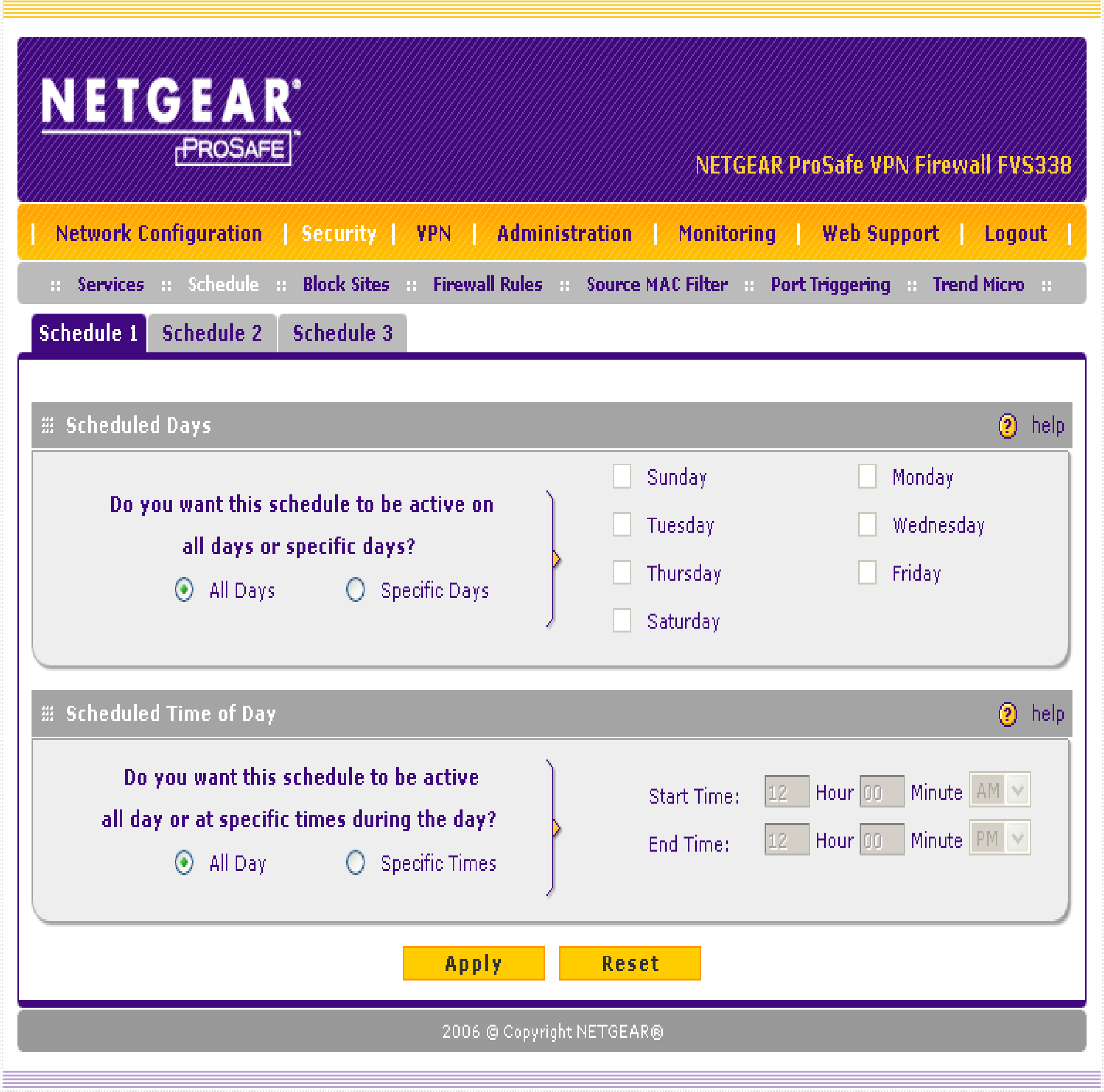
3. Click the tab labeled "Attack Checks".

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: Eagle 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


NETGEAR PROSAFE
NETGEAR ProSafe VPN Firewall FVS338
| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Block Sites :: Firewall Rules :: Source MAC Filter :: Port Triggering :: Trend Micro ::
Schedule 1
Schedule 2
Schedule 3
help
help
Apply
Reset
2006 © Copyright NETGEAR®

Scheduled Days

Do you want this schedule to be active on all days or specific days?

● All Days ○ Specific Days

□ Sunday □ Monday
□ Tuesday □ Wednesday
□ Thursday □ Friday
□ Saturday

Scheduled Time of Day

Do you want this schedule to be active all day or at specific times during the day?

● All Day ○ Specific Times

Start Time: 12 Hour 00 Minute AM

End Time: 12 Hour 00 Minute PM

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

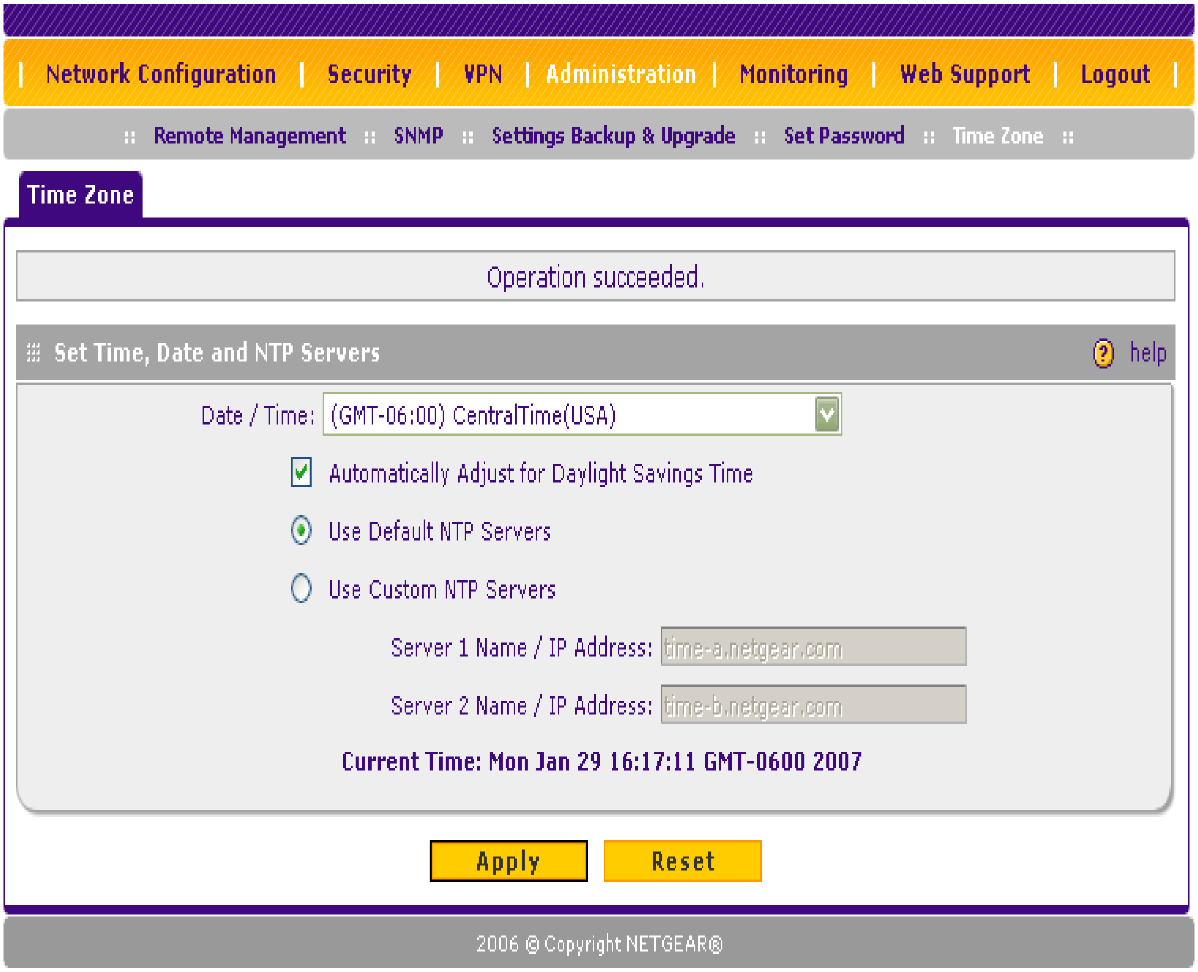
2. In the sub menu bar, select "Schedule".

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


| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Set Password :: Time Zone ::
Time Zone
help
Apply
Reset
2006 © Copyright NETGEAR®

Operation succeeded.

Set Time, Date and NTP Servers

Date / Time: (GMT-06:00) CentralTime(USA)

☑ Automatically Adjust for Daylight Savings Time

● Use Default NTP Servers

○ Use Custom NTP Servers

Server 1 Name / IP Address: time-a.netgear.com

Server 2 Name / IP Address: time-b.netgear.com

Current Time: Mon Jan 29 16:17:11 GMT-0600 2007

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

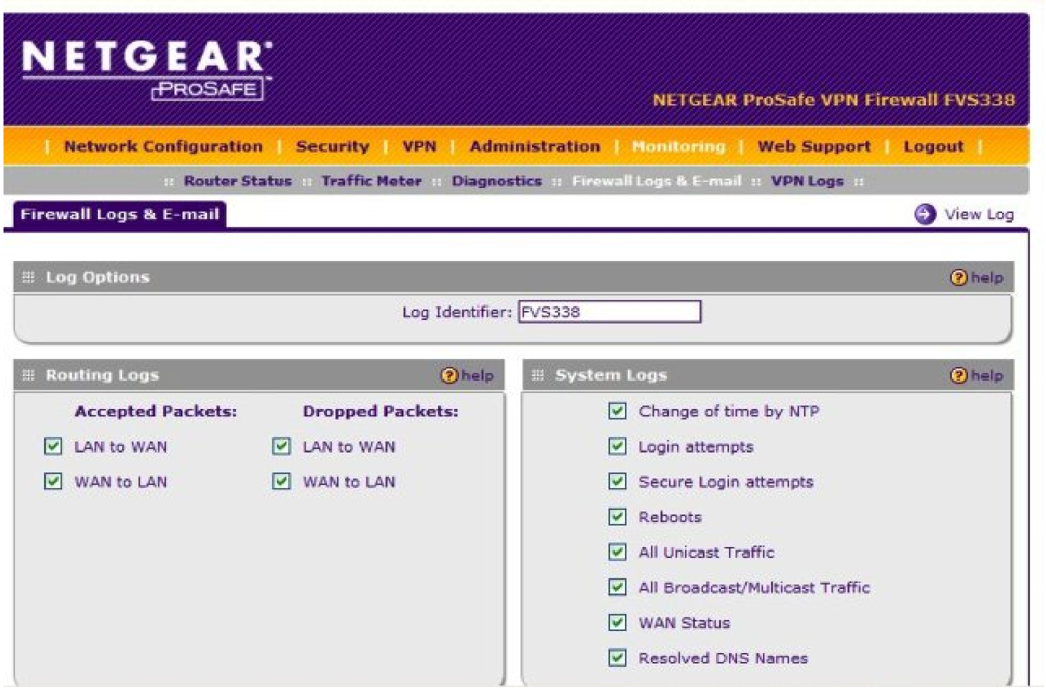
2. Check "Automatically Adjust for Daylight Savings", (unless you happen to be in one of the two areas of the USA that doesn't follow Daylight Savings Time).

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


NETGEAR PROSAFE
NETGEAR ProSafe VPN Firewall FVS338
| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Firewall Logs & E-mail
View Log
help

Log Options

Log Identifier: FVS338

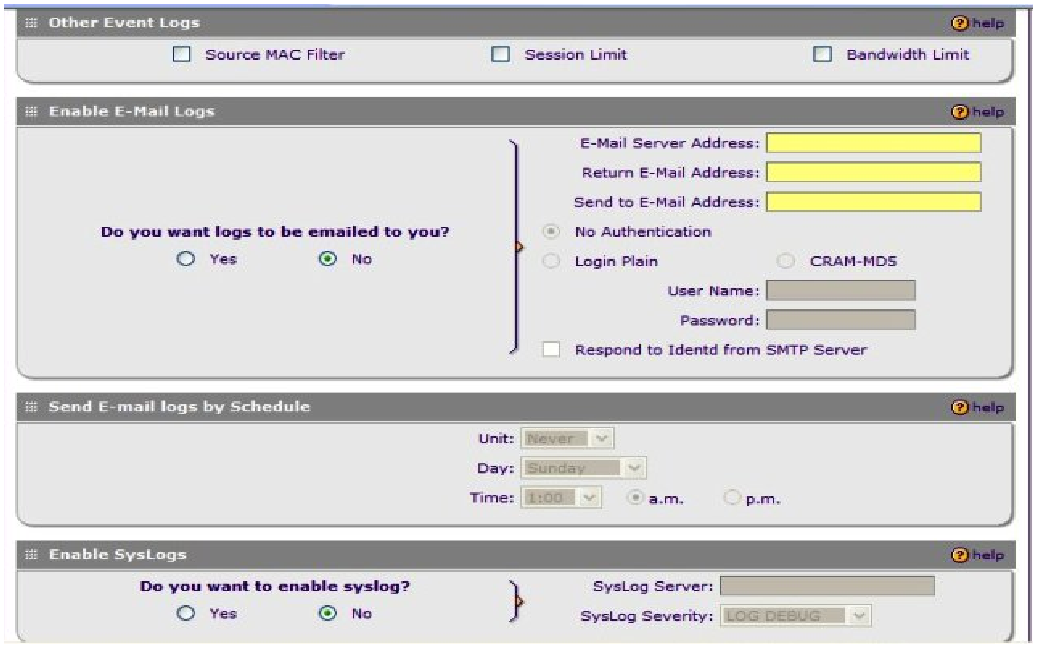
Routing Logs

Accepted Packets:	Dropped Packets:
☑ LAN to WAN	☑ LAN to WAN
☑ WAN to LAN	☑ WAN to LAN

System Logs

☑ Change of time by NTP
☑ Login attempts
☑ Secure Login attempts
☑ Reboots
☑ All Unicast Traffic
☑ All Broadcast/Multicast Traffic
☑ WAN Status
☑ Resolved DNS Names

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



Other Event Logs

□ Source MAC Filter □ Session Limit □ Bandwidth Limit

Enable E-Mail Logs

Do you want logs to be emailed to you?
○ Yes ● No

E-Mail Server Address:
Return E-Mail Address:
Send to E-Mail Address:
● No Authentication
○ Login Plain ○ CRAM-MD5
User Name:
Password:
□ Respond to Identd from SMTP Server

Send E-mail logs by Schedule

Unit: Never
Day: Sunday
Time: 1:00 ● a.m. ○ p.m.

Enable SysLogs

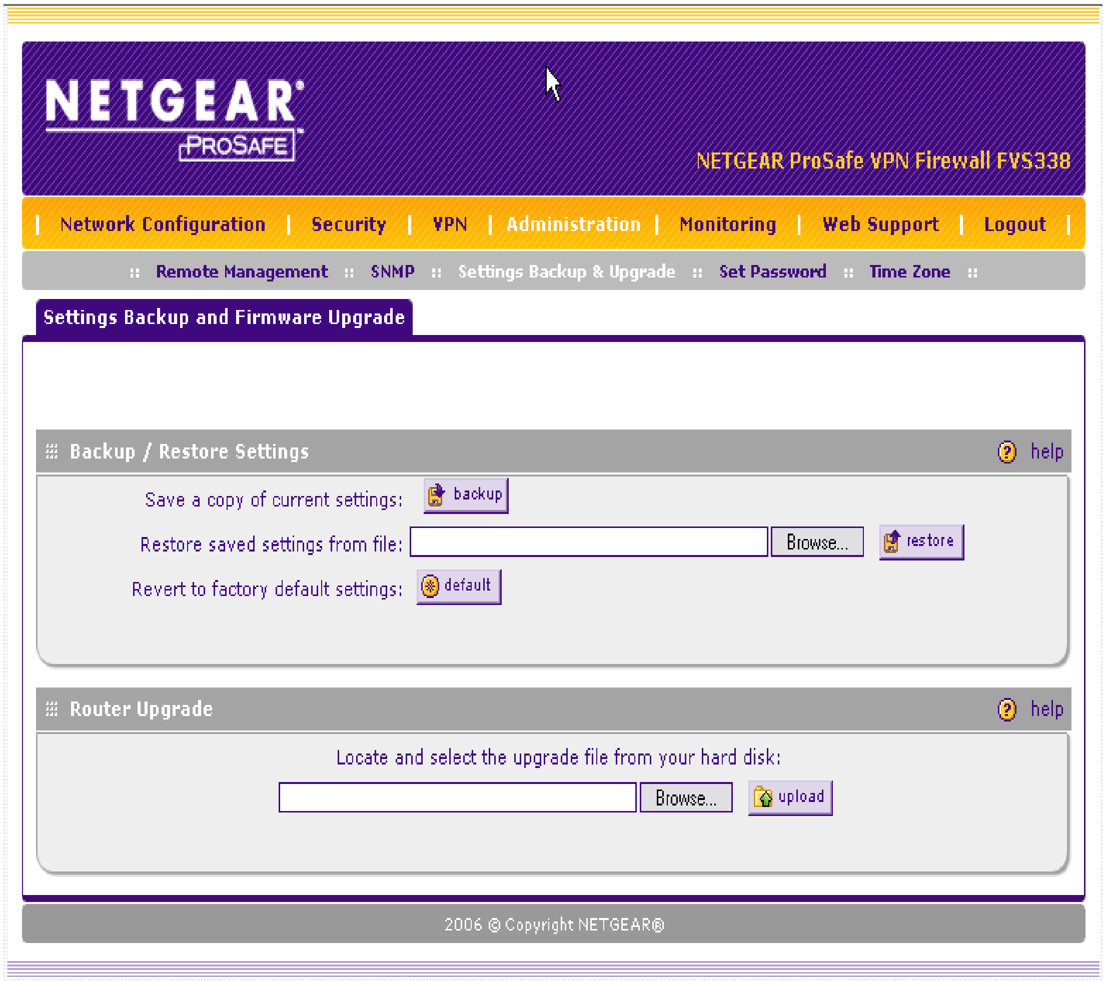
Do you want to enable syslog?
○ Yes ● No

SysLog Server:
SysLog Severity: LOG DEBUG

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


NETGEAR PROSAFE
NETGEAR ProSafe VPN Firewall FVS338
| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Set Password :: Time Zone ::
Settings Backup and Firmware Upgrade
Backup / Restore Settings
help
Save a copy of current settings:
backup
Restore saved settings from file:
Browse...
restore
Revert to factory default settings:
default
Router Upgrade
help
Locate and select the upgrade file from your hard disk:
Browse...
upload
2006 © Copyright NETGEAR®

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.

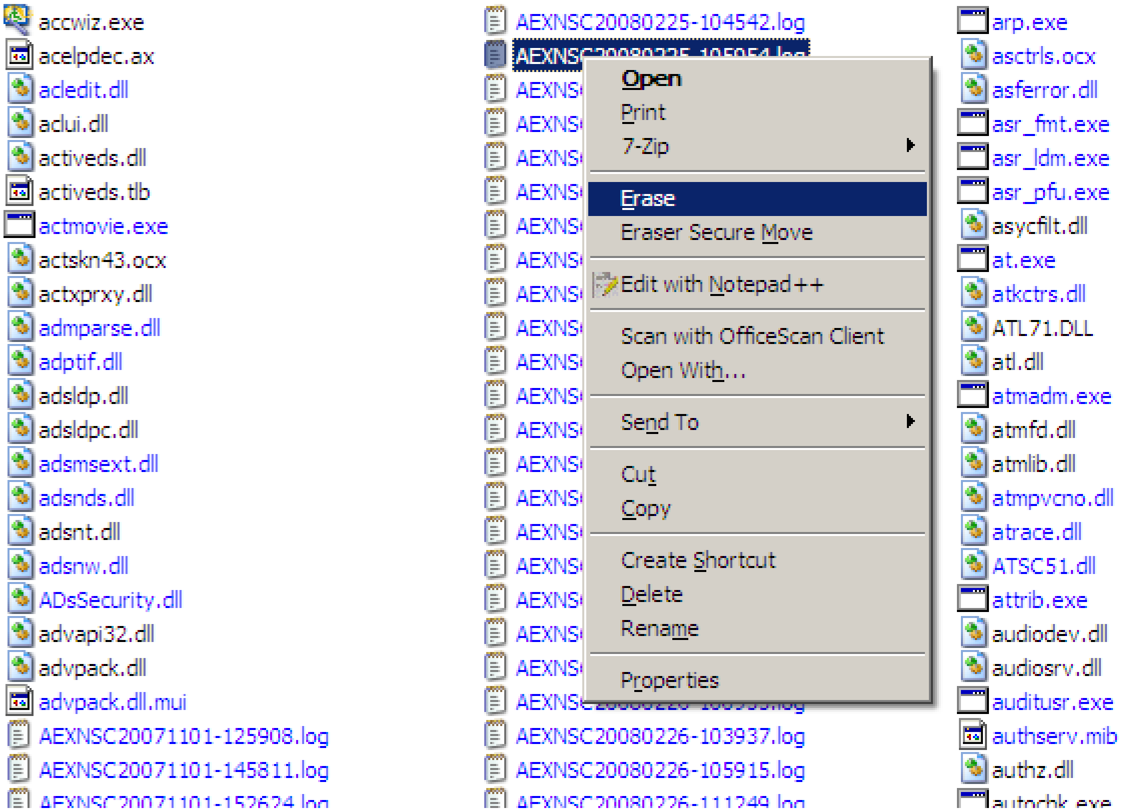
Using the Eraser Tool

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

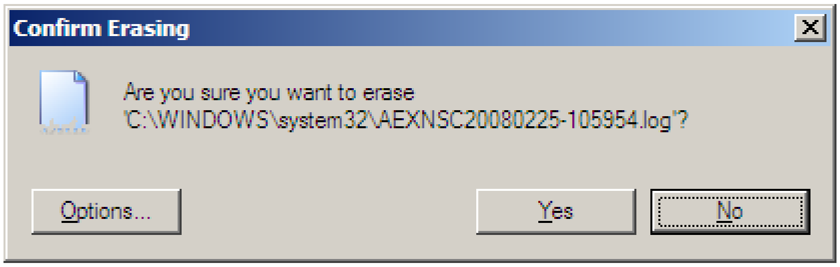
There are multiple ways to use the Erase application to securely delete your files. For advanced options or detailed instruction on how to completely wipe a hard drive refer to the Erase application's help file.

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.

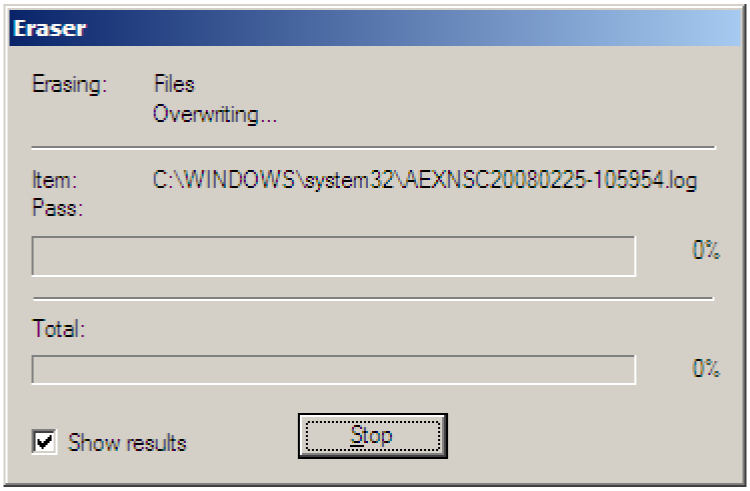


2. Right Click on the file; on the pop-up menu select Erase.


Confirm Erasing

Are you sure you want to erase 'C:\WINDOWS\system32\AEXNSC20080225-105954.log'?

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



Erasing: Files
Overwriting...

Item: C:\WINDOWS\system32\AEXNSC20080225-105954.log
Pass:

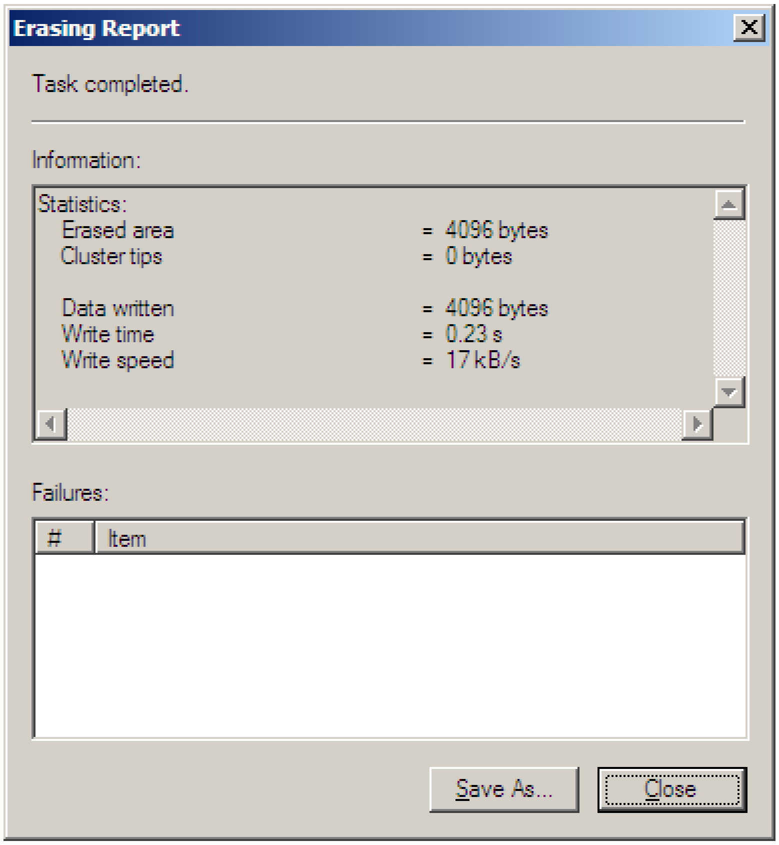
0%

Total:

0%

☑ Show results

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.



Task completed.

Information:

```
Statistics:
    Erased area                    =  4096 bytes
    Cluster tips                   =  0 bytes

    Data written                   =  4096 bytes
    Write time                     =  0.23 s
    Write speed                    =  17 kB/s
```

Failures:

#	Item

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.

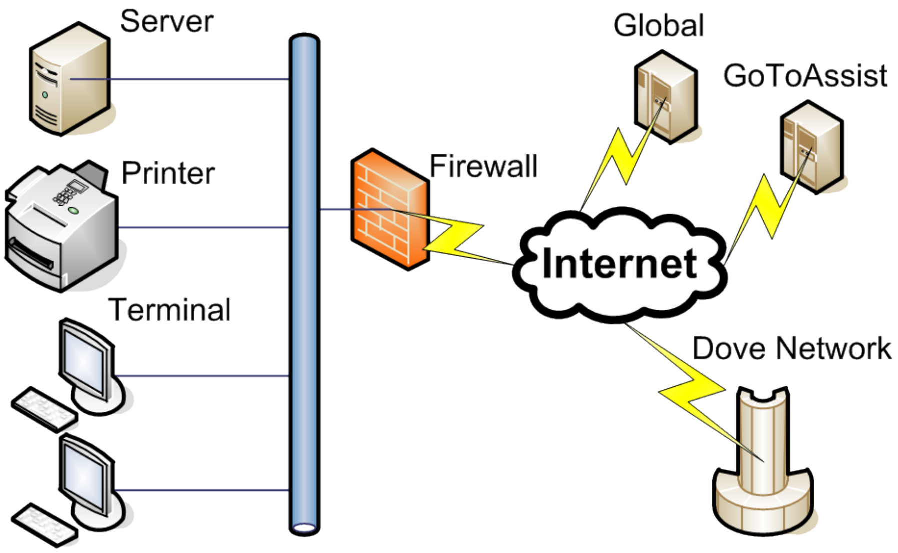
Eagle Application Summary

PA-DSS Executive Summary

Software Vendor	Teleflora
Teleflora Contact Information:	Chris Campbell
Teleflora Mailing Address	3737 NW 34th St
	Oklahoma City, OK 73112
Product Name	Eagle
Product Version	8
Recommended OS:	Windows XP Professional
Traditional Marketplace:	Retail Florist

Typical Eagle Network Topology

PA-DSS Executive Summary



A typical Eagle shop consists of one store with multiple “terminals”, a network printer, an Eagle “server”, and a Firewall to the internet.

Eagle 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). There is only one of these servers in a Eagle “environment”.

Eagle Terminal
Windows PC running Eagle software in “Client” mode. “Client” software offers minimal data storage, and connects to the Eagle “Server” for all data communications and data storage. The Eagle 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 “Eagle Server” and “Eagle 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 Eagle 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 Eagle Server, to the Dove Network via an authenticated, SSL encrypted link. Only PANs may be transmitted from the Dove Network back to the Eagle Server. Only Eagle Servers communicate with the Dove Network.

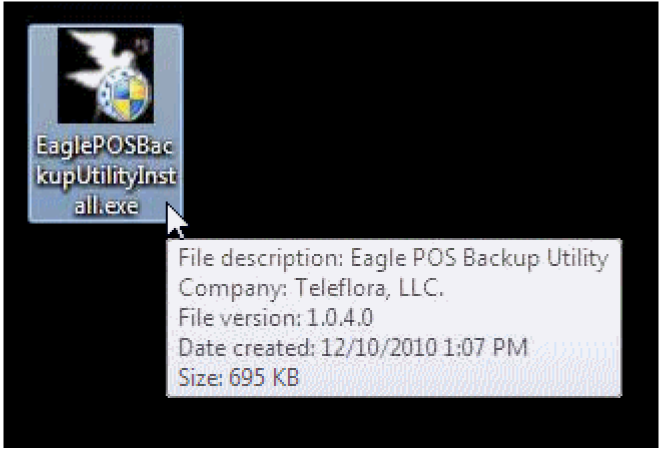
Data Backup

Eagle POS Backup Utility

Installing the Eagle POS Backup Utility

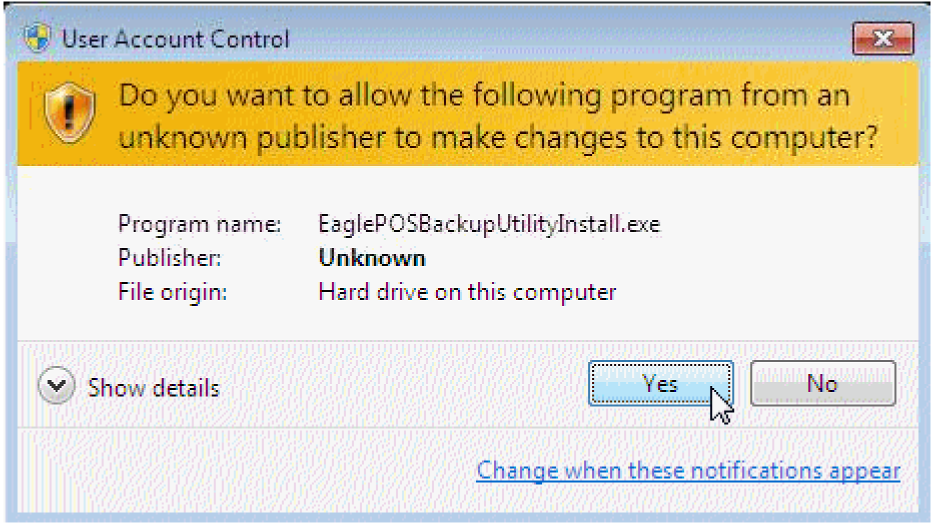
Note: The backup automatically installs with EagleFMS versions 8.0.18 and above.

1. Double Click the EaglePOSBackupUtilityInstall.exe file.



File description: Eagle POS Backup Utility
Company: Teleflora, LLC.
File version: 1.0.4.0
Date created: 12/10/2010 1:07 PM
Size: 695 KB

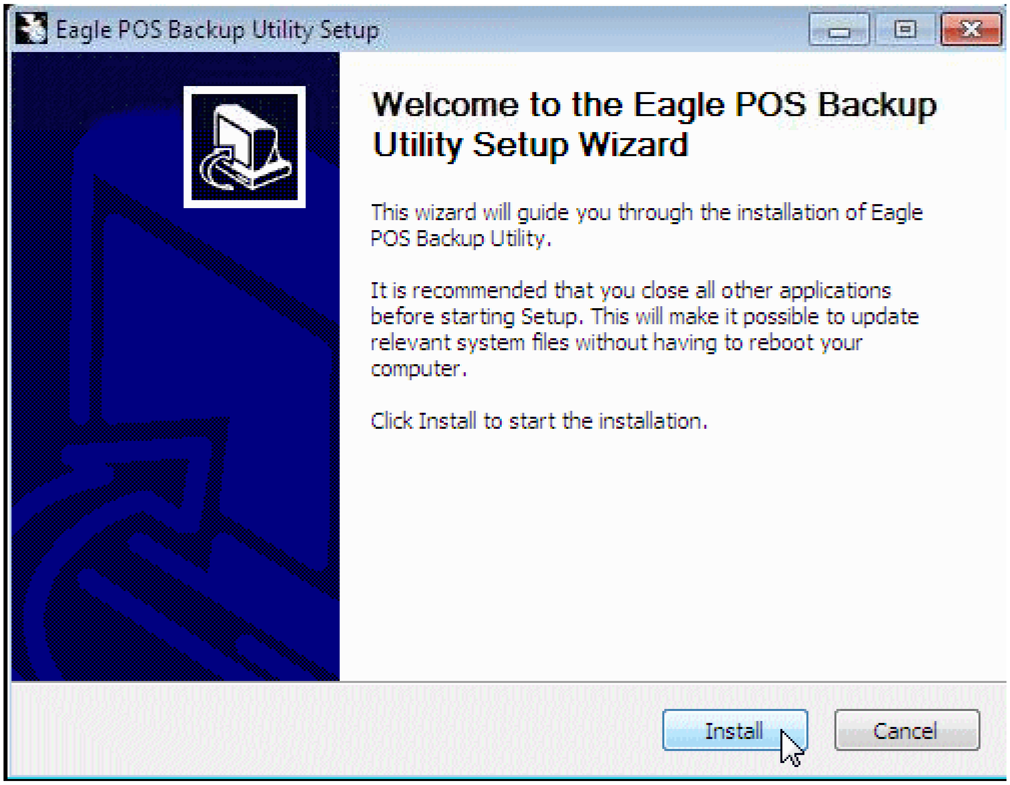
2. If you are installing on Windows 7 click Yes to the User Account Control prompt.



Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name: EaglePOSBackupUtilityInstall.exe
Publisher: **Unknown**
File origin: Hard drive on this computer

3. Click Install.



Eagle POS Backup Utility Setup

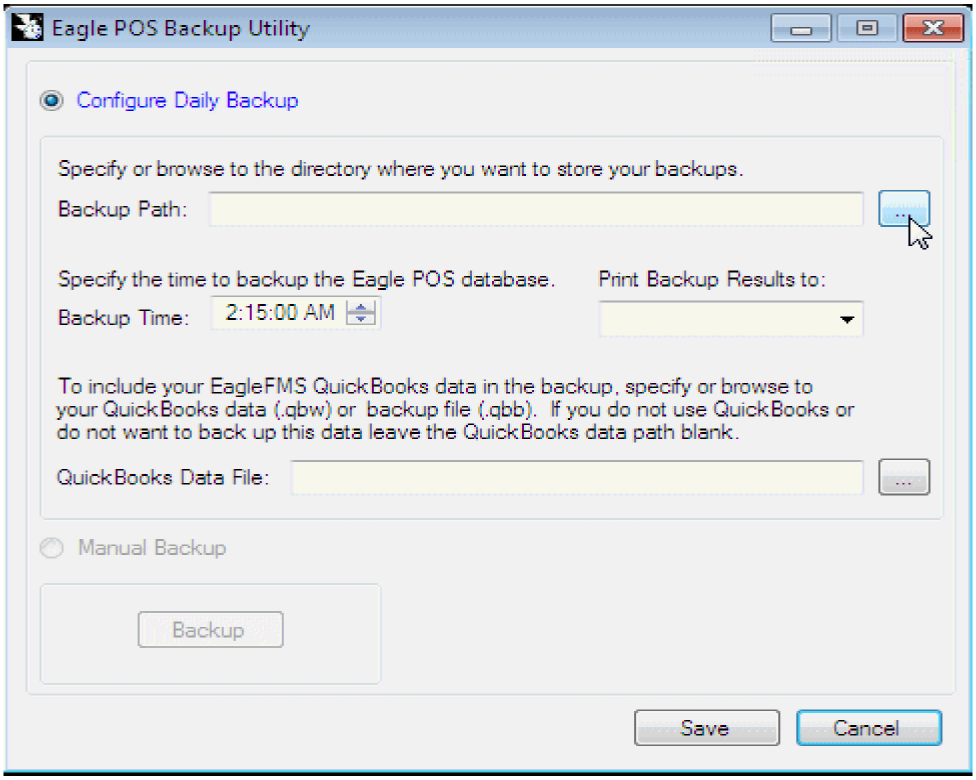
Welcome to the Eagle POS Backup Utility Setup Wizard

This wizard will guide you through the installation of Eagle POS Backup Utility.

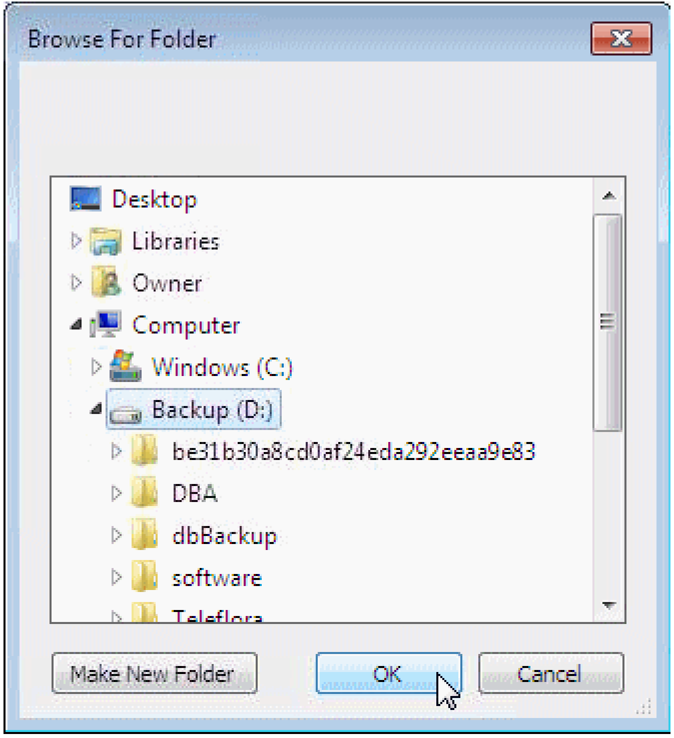
It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Install to start the installation.

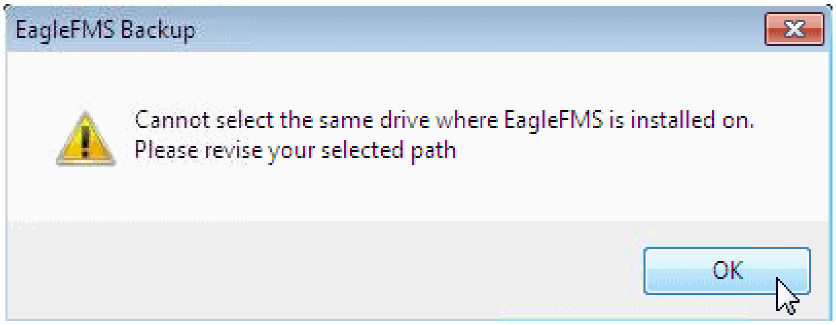
4. The Eagle POS Backup Utility will install and open the configuration screen automatically, click the Ellipsis to setup the Backup Path.
   Note: If Cancel is clicked you can still configure these options by clicking the configuration link in the start menu.


Eagle POS Backup Utility
● Configure Daily Backup
Specify or browse to the directory where you want to store your backups.
Backup Path:
...
Specify the time to backup the Eagle POS database.
Backup Time: 2:15:00 AM
Print Backup Results to:
To include your EagleFMS QuickBooks data in the backup, specify or browse to your QuickBooks data (.qbw) or backup file (.qbb). If you do not use QuickBooks or do not want to back up this data leave the QuickBooks data path blank.
QuickBooks Data File:
...
○ Manual Backup
Backup
Save
Cancel

5. Select the External Drive to store the backups.
Note: Selecting the root of the drive such as D:\ will add EaglePOS_Backups as the path in that drive for the backups.

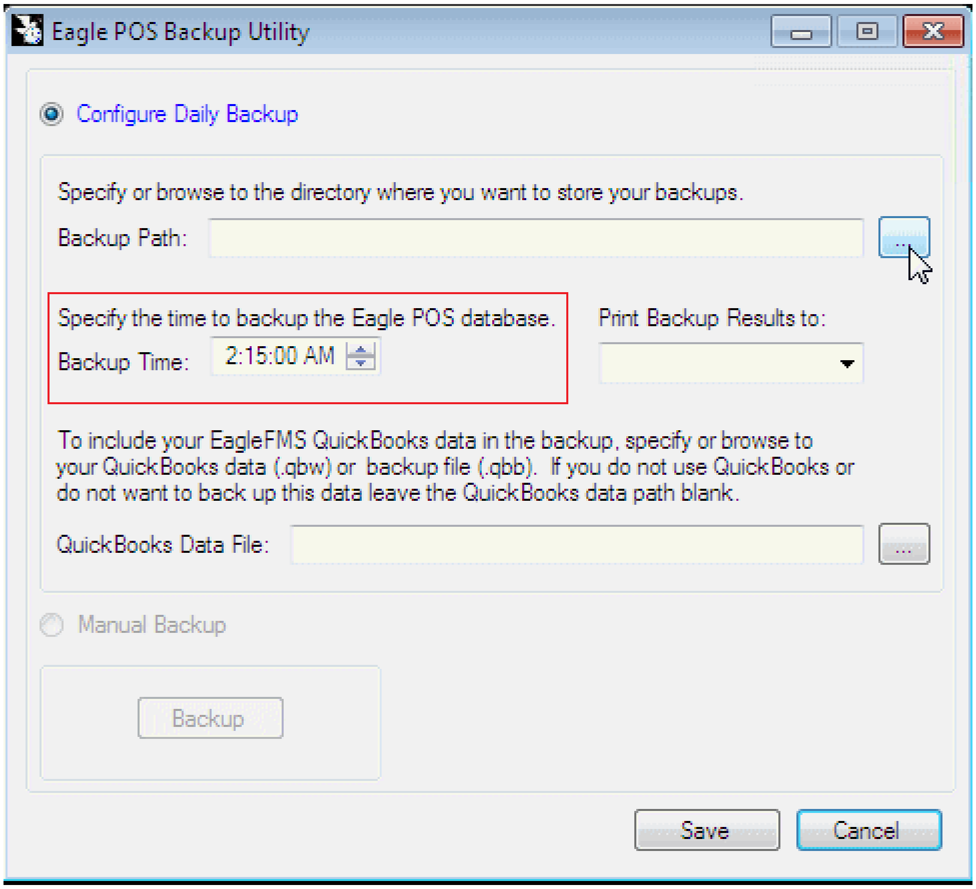


Note: The location cannot be the same drive that has the EagleFMS application installed.



Cannot select the same drive where EagleFMS is installed on.
Please revise your selected path

6. Next set the time for the backup to occur.



Eagle POS Backup Utility

● Configure Daily Backup

Specify or browse to the directory where you want to store your backups.

Backup Path:

Specify the time to backup the Eagle POS database.

Backup Time: 2:15:00 AM

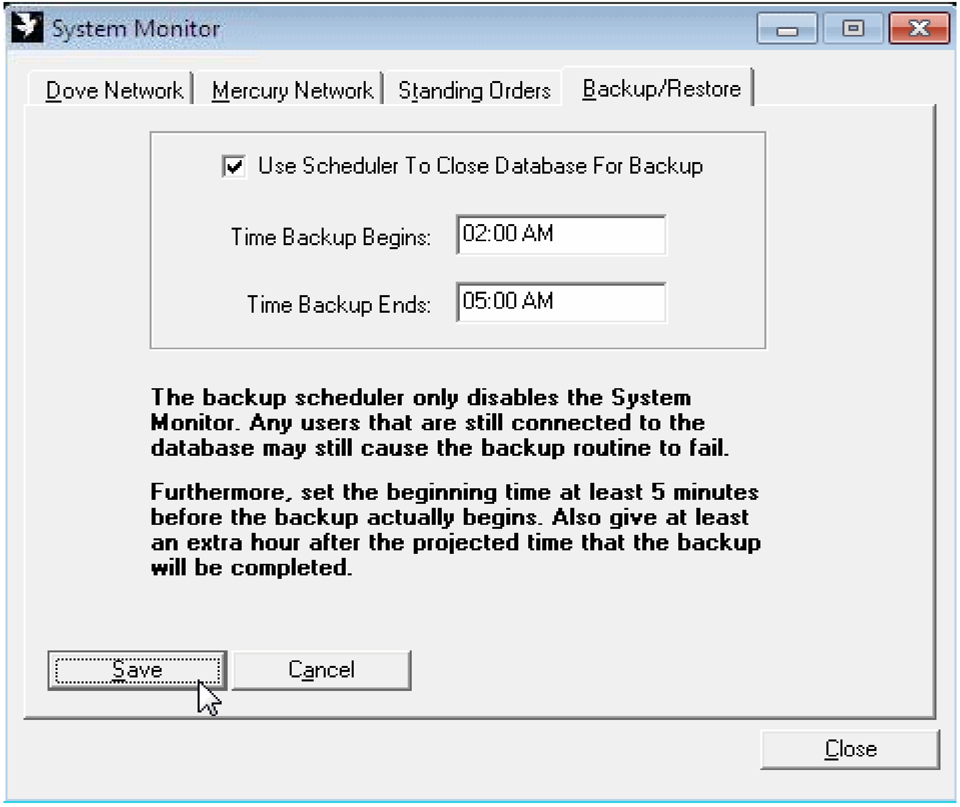
Print Backup Results to:

To include your EagleFMS QuickBooks data in the backup, specify or browse to your QuickBooks data (.qbw) or backup file (.qbb). If you do not use QuickBooks or do not want to back up this data leave the QuickBooks data path blank.

QuickBooks Data File:

○ Manual Backup

Note: Verify the time set in the EaglePOS Backup configuration coincides with System Monitor



System Monitor

☑ Use Scheduler To Close Database For Backup

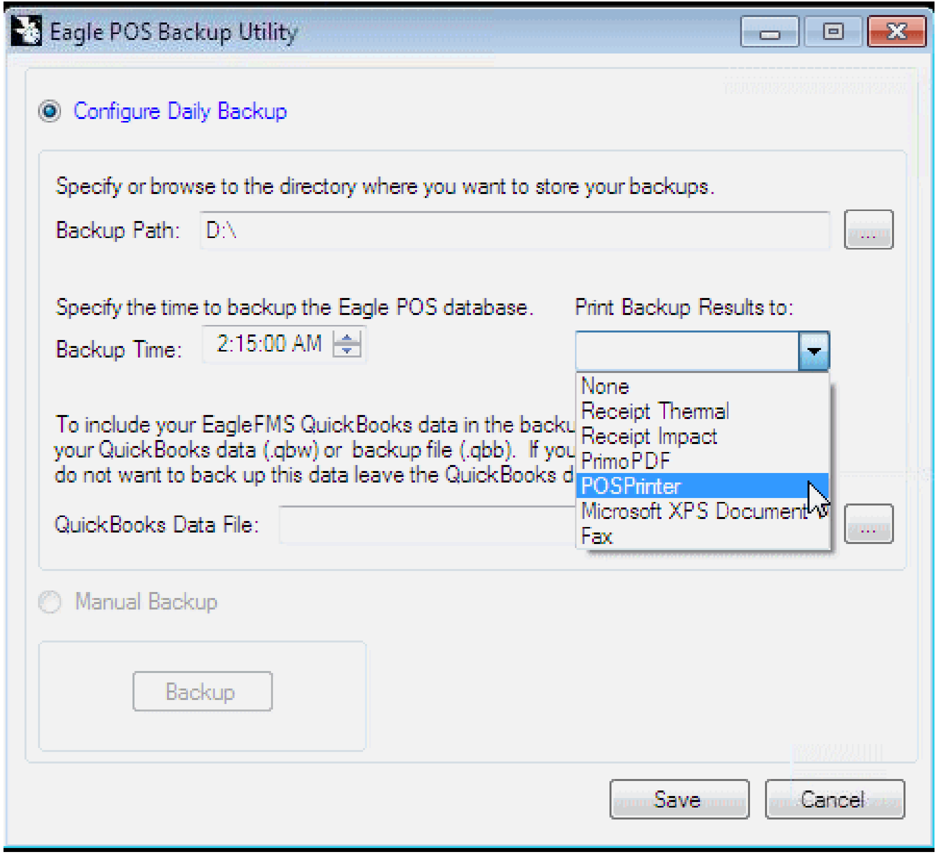
Time Backup Begins: 02:00 AM

Time Backup Ends: 05:00 AM

The backup scheduler only disables the System Monitor. Any users that are still connected to the database may still cause the backup routine to fail.

Furthermore, set the beginning time at least 5 minutes before the backup actually begins. Also give at least an extra hour after the projected time that the backup will be completed.

7. Next select the printer for the backup results.



● Configure Daily Backup

Specify or browse to the directory where you want to store your backups.

Backup Path: D:\

Specify the time to backup the Eagle POS database.

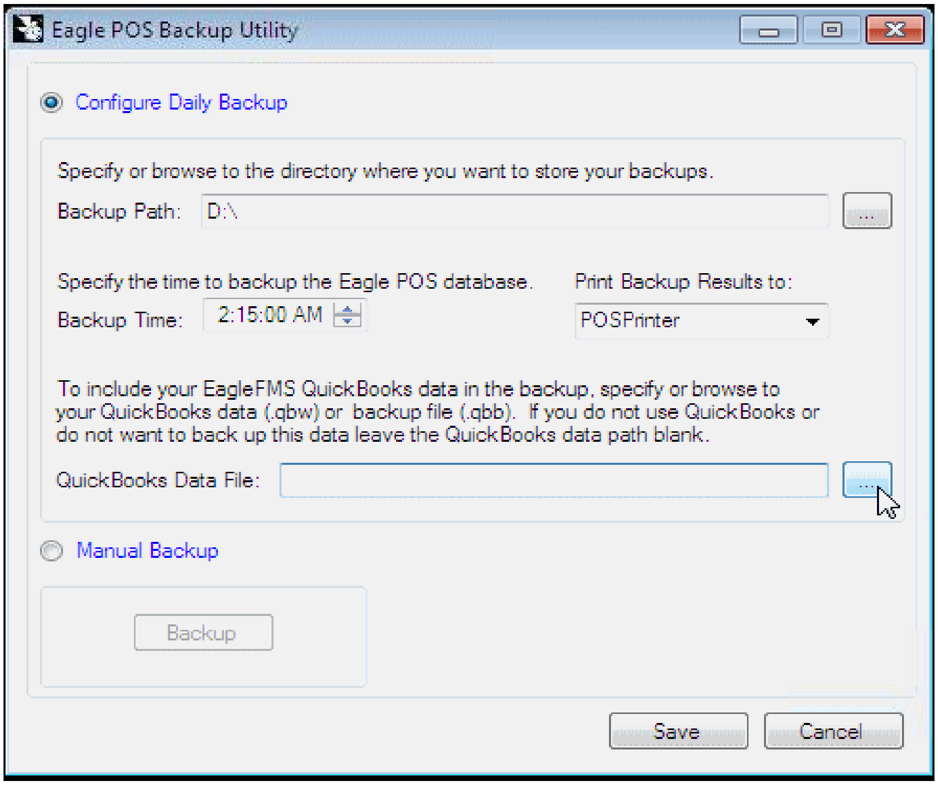
Backup Time: 2:15:00 AM

To include your EagleFMS QuickBooks data in the backu
your QuickBooks data (.qbw) or backup file (.qbb). If you
do not want to back up this data leave the QuickBooks d

QuickBooks Data File:

○ Manual Backup

8. If Quick Books is installed you can also backup the company or backup file. Click the ellipsis to browse for the file.



● Configure Daily Backup

Specify or browse to the directory where you want to store your backups.

Backup Path: D:\

Specify the time to backup the Eagle POS database.

Backup Time: 2:15:00 AM

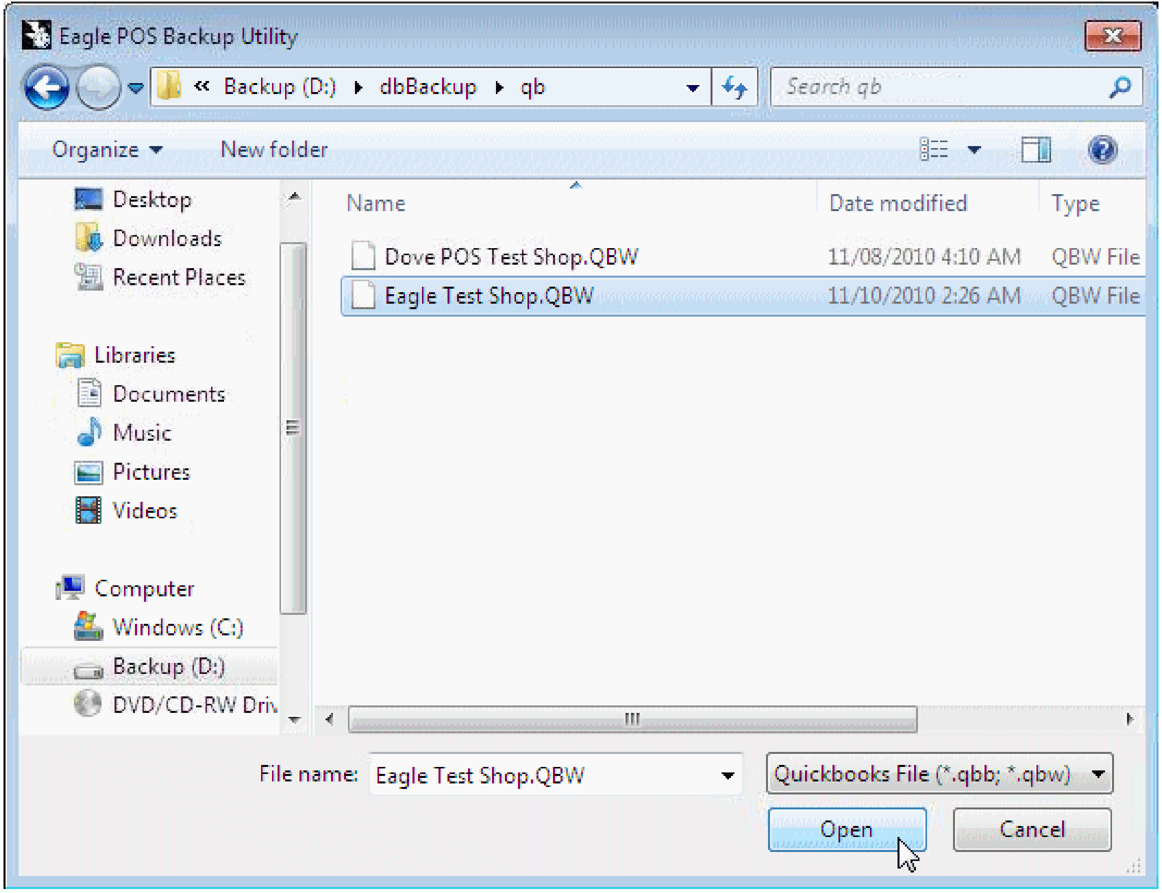
Print Backup Results to: POSPrinter

To include your EagleFMS QuickBooks data in the backup, specify or browse to your QuickBooks data (.qbw) or backup file (.qbb). If you do not use QuickBooks or do not want to back up this data leave the QuickBooks data path blank.

QuickBooks Data File:

○ Manual Backup

9. Locate the *.qbw or *.qbb file, select it, and then click open.

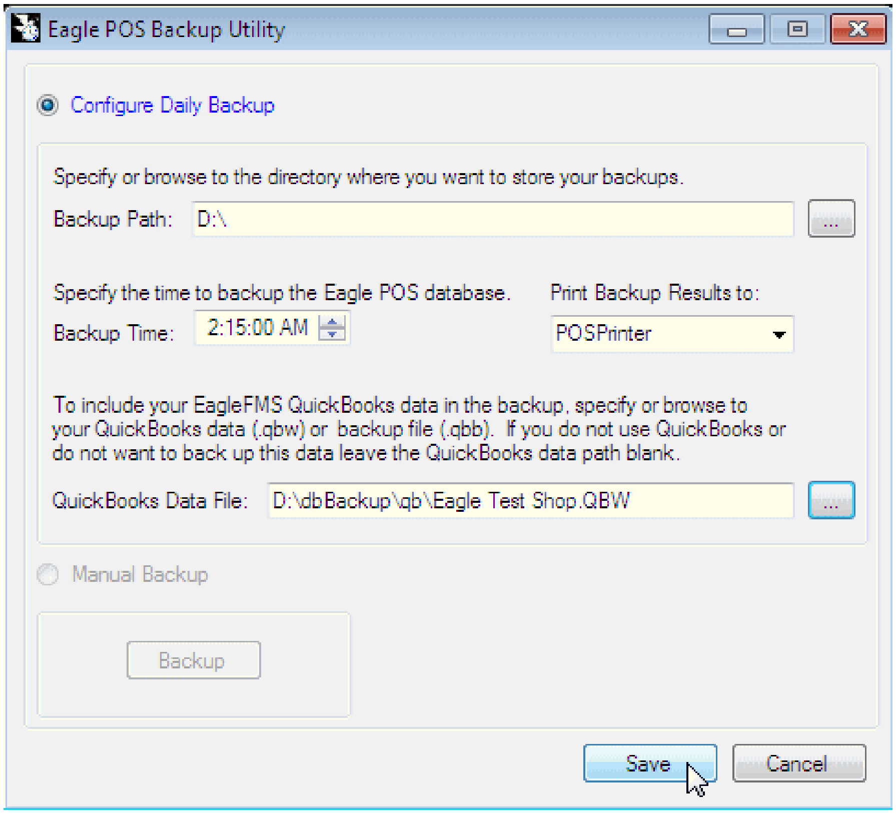


Name	Date modified	Type
Dove POS Test Shop.QBW	11/08/2010 4:10 AM	QBW File
Eagle Test Shop.QBW	11/10/2010 2:26 AM	QBW File

File name: Eagle Test Shop.QBW

Quickbooks File (*.qbb; *.qbw)

10. Click Save.



● Configure Daily Backup

Specify or browse to the directory where you want to store your backups.

Backup Path: D:\

Specify the time to backup the Eagle POS database.

Backup Time: 2:15:00 AM

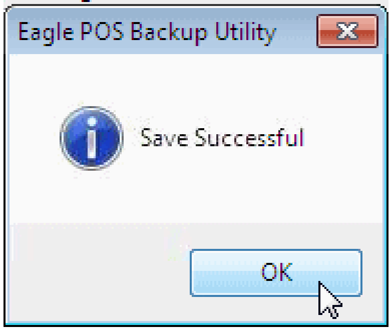
Print Backup Results to: POSPrinter

To include your EagleFMS QuickBooks data in the backup, specify or browse to your QuickBooks data (.qbw) or backup file (.qbb). If you do not use QuickBooks or do not want to back up this data leave the QuickBooks data path blank.

QuickBooks Data File: D:\dbBackup\qb\Eagle Test Shop.QBW

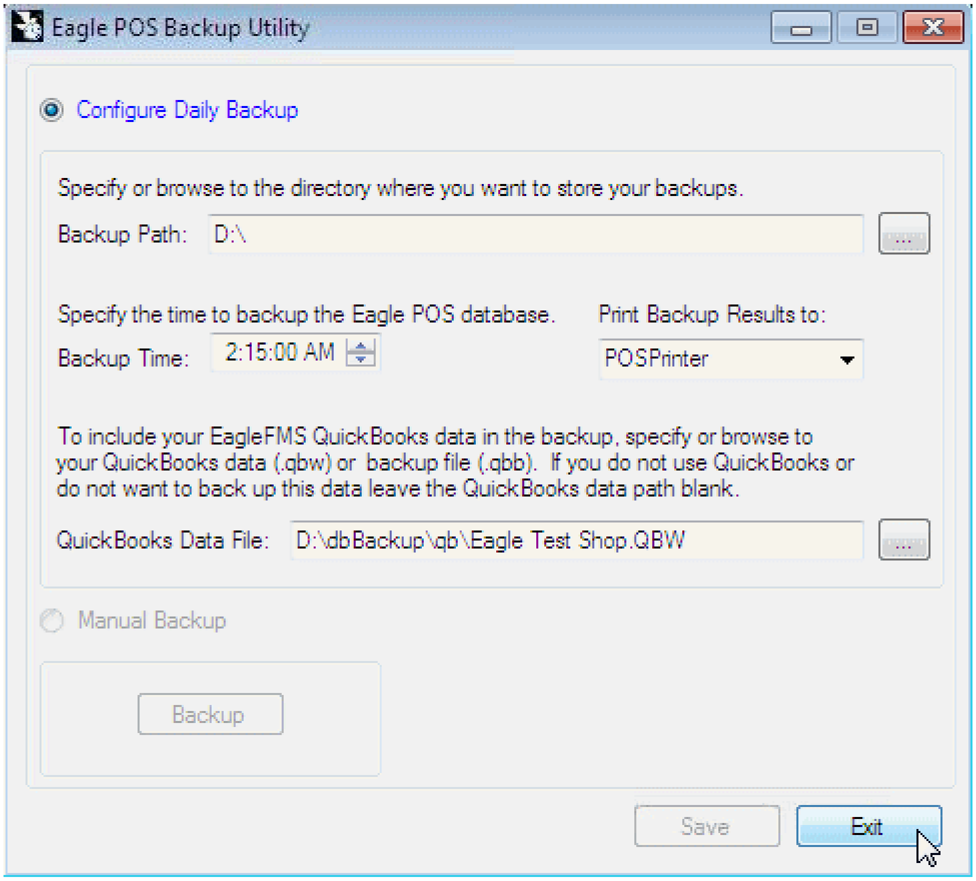
○ Manual Backup

11. Click OK to the save successful prompt.



Save Successful

12. Click Exit to close the configuration tool.



● Configure Daily Backup

Specify or browse to the directory where you want to store your backups.

Backup Path: D:\

Specify the time to backup the Eagle POS database.

Backup Time: 2:15:00 AM

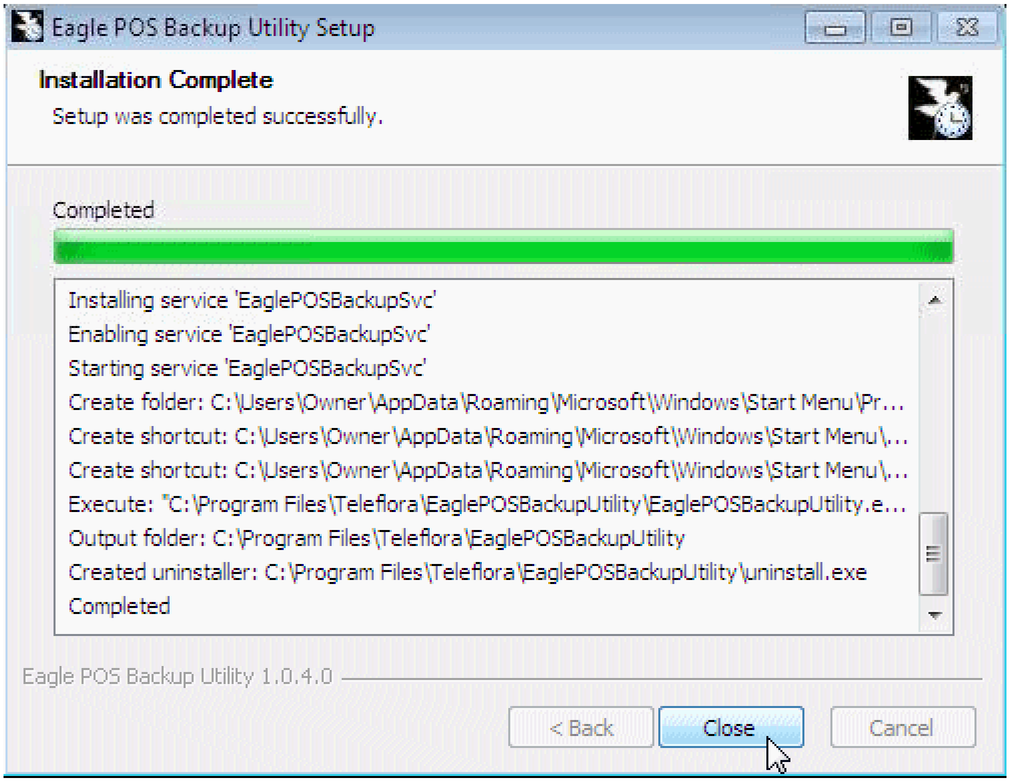
Print Backup Results to: POSPrinter

To include your EagleFMS QuickBooks data in the backup, specify or browse to your QuickBooks data (.qbw) or backup file (.qbb). If you do not use QuickBooks or do not want to back up this data leave the QuickBooks data path blank.

QuickBooks Data File: D:\dbBackup\qb\Eagle Test Shop.QBW

○ Manual Backup

13. Click Close to finish the installation.



Eagle POS Backup Utility Setup

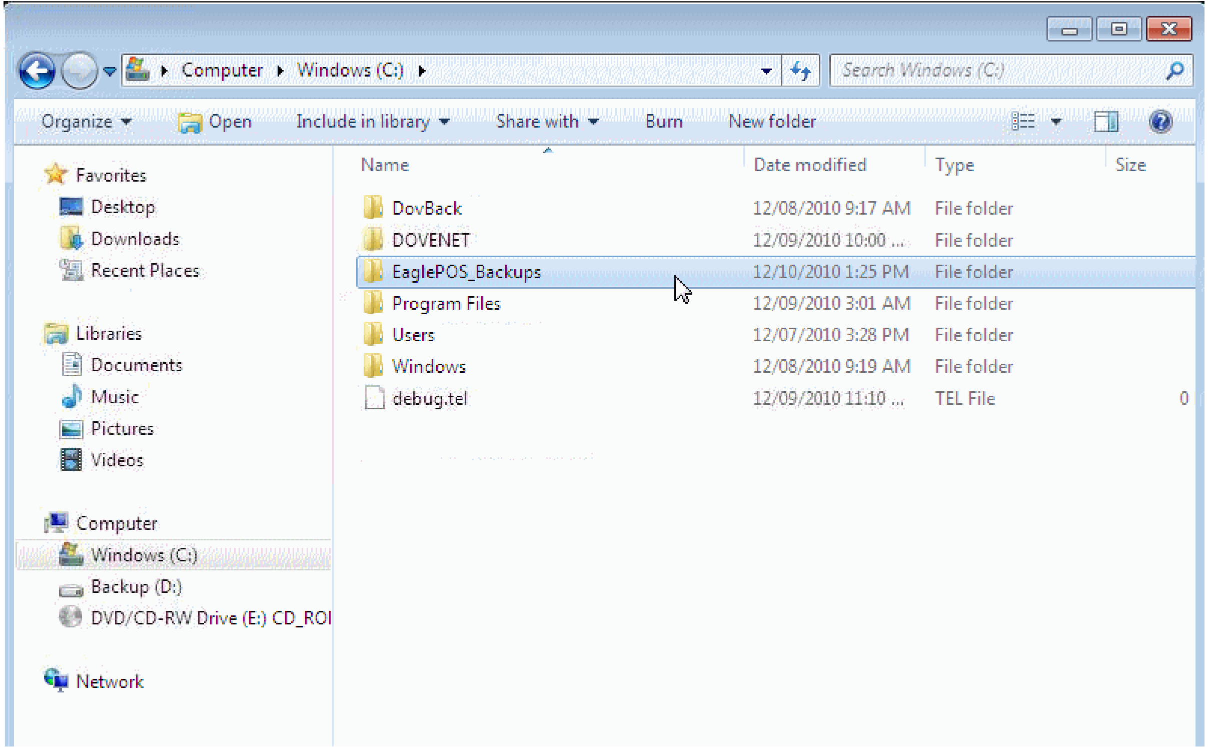
Installation Complete

Setup was completed successfully.

Completed

```
Installing service 'EaglePOSBackupSvc'
Enabling service 'EaglePOSBackupSvc'
Starting service 'EaglePOSBackupSvc'
Create folder: C:\Users\Owner\AppData\Roaming\Microsoft\Windows\Start Menu\Pr...
Create shortcut: C:\Users\Owner\AppData\Roaming\Microsoft\Windows\Start Menu\...
Create shortcut: C:\Users\Owner\AppData\Roaming\Microsoft\Windows\Start Menu\...
Execute: "C:\Program Files\Teleflora\EaglePOSBackupUtility\EaglePOSBackupUtility.e...
Output folder: C:\Program Files\Teleflora\EaglePOSBackupUtility
Created uninstaller: C:\Program Files\Teleflora\EaglePOSBackupUtility\uninstall.exe
Completed
```

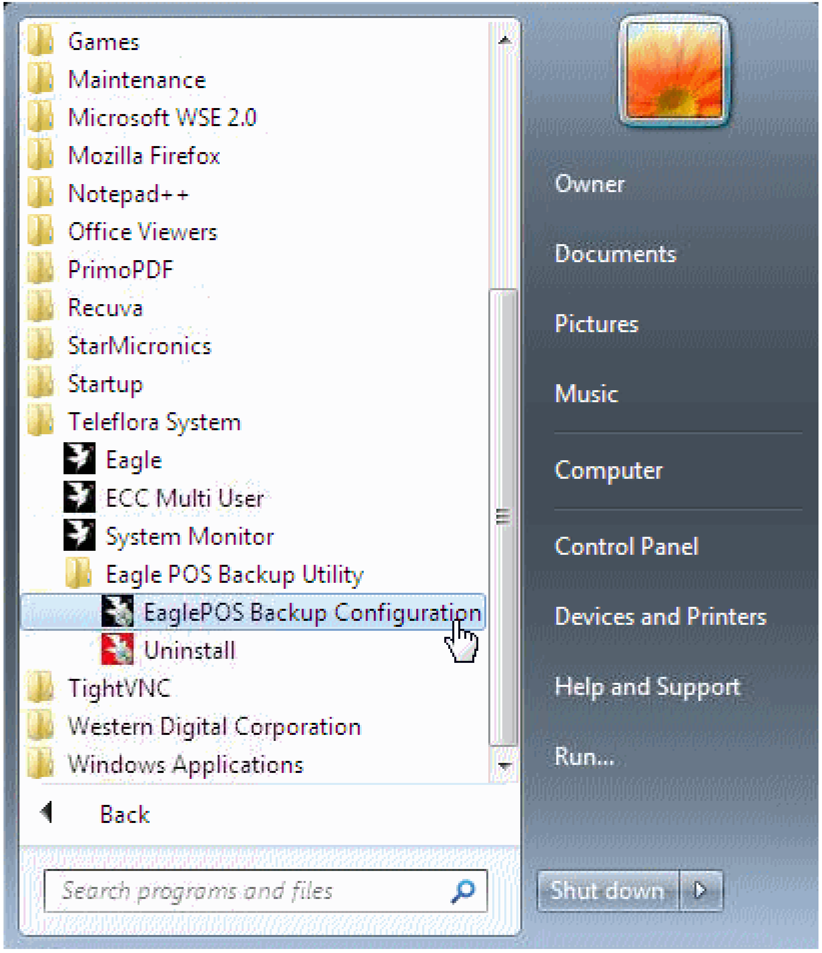
14. The backup utility will perform an automatic backup once the install is finished. It may take several minutes to complete depending on the size of the files. A folder will be created at the root of the drive were EagleFMS is installed named EaglePOS_Backups.



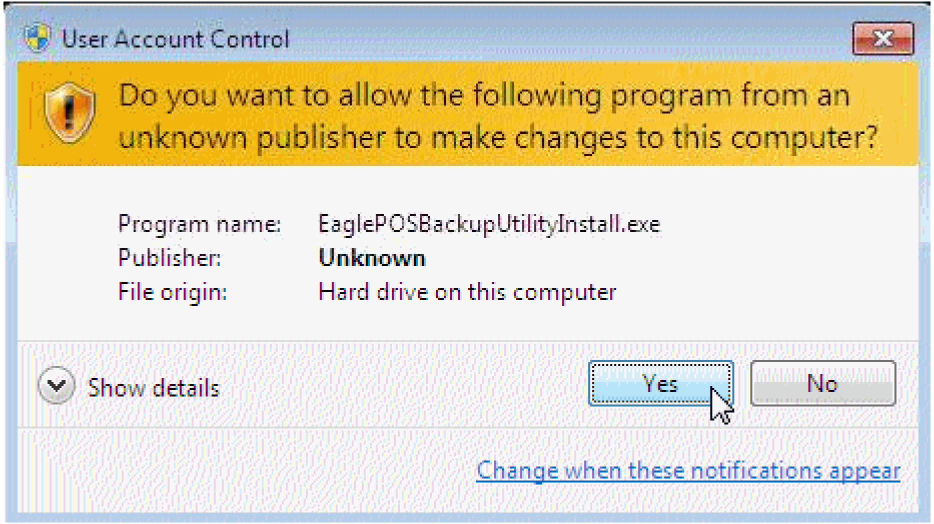
Name	Date modified	Type	Size
DovBack	12/08/2010 9:17 AM	File folder	
DOVENET	12/09/2010 10:00 ...	File folder	
EaglePOS_Backups	12/10/2010 1:25 PM	File folder	
Program Files	12/09/2010 3:01 AM	File folder	
Users	12/07/2010 3:28 PM	File folder	
Windows	12/08/2010 9:19 AM	File folder	
debug.tel	12/09/2010 11:10 ...	TEL File	0

Performing a manual Backup

1. Locate the Backup Configuration in the start menu under Start > Programs > Teleflora System > EaglePOS Backup Utility > EaglePOS Backup Configuration and double click it.



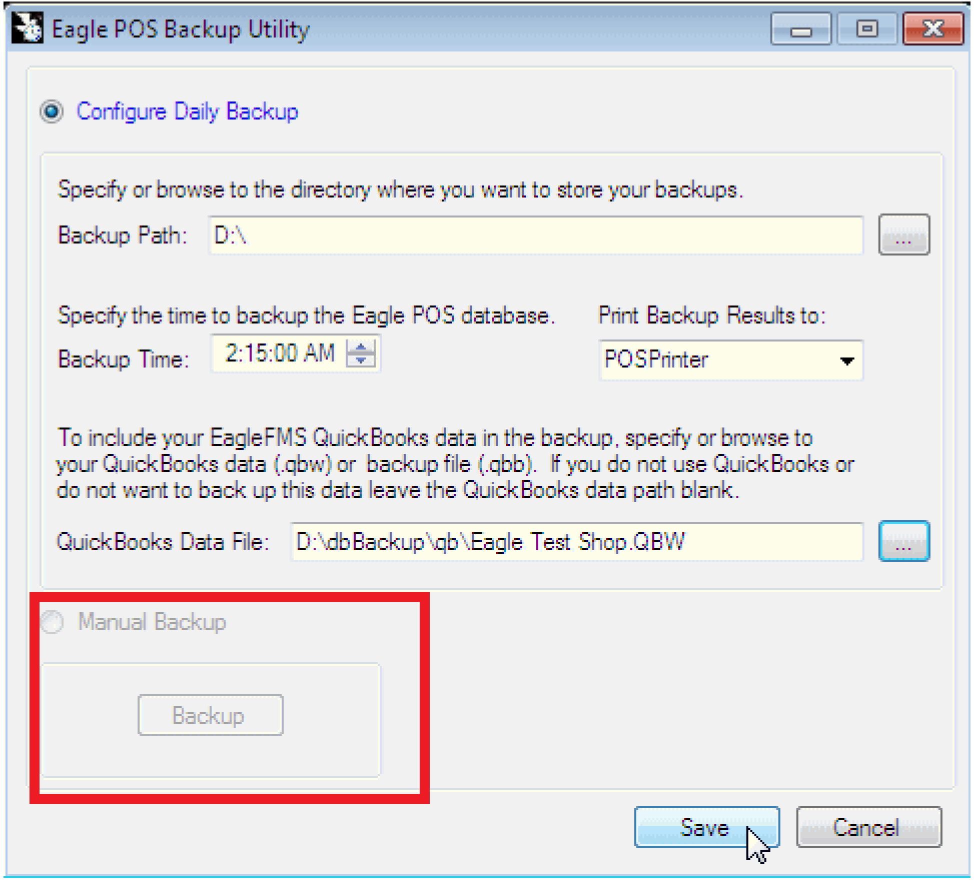
2. If you are using windows 7 click Yes to the user account control prompt.



Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name: EaglePOSBackupUtilityInstall.exe
Publisher: **Unknown**
File origin: Hard drive on this computer

3. Click the Manual Backup radio button to select it.



Eagle POS Backup Utility

● Configure Daily Backup

Specify or browse to the directory where you want to store your backups.

Backup Path: D:\

Specify the time to backup the Eagle POS database.

Backup Time: 2:15:00 AM

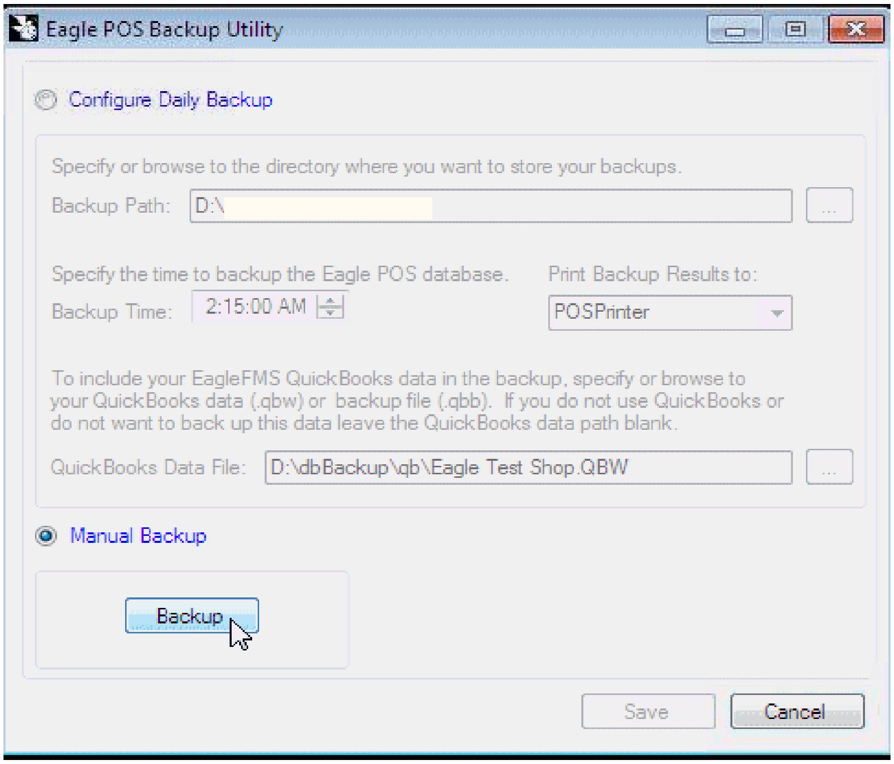
Print Backup Results to: POSPrinter

To include your EagleFMS QuickBooks data in the backup, specify or browse to your QuickBooks data (.qbw) or backup file (.qbb). If you do not use QuickBooks or do not want to back up this data leave the QuickBooks data path blank.

QuickBooks Data File: D:\dbBackup\qb\Eagle Test Shop.QBW

○ Manual Backup

4. Click the Backup button to start the manual backup
   Note: Be sure the backup media is ready for use.



Eagle POS Backup Utility

○ Configure Daily Backup

Specify or browse to the directory where you want to store your backups.

Backup Path: D:\

Specify the time to backup the Eagle POS database.

Backup Time: 2:15:00 AM

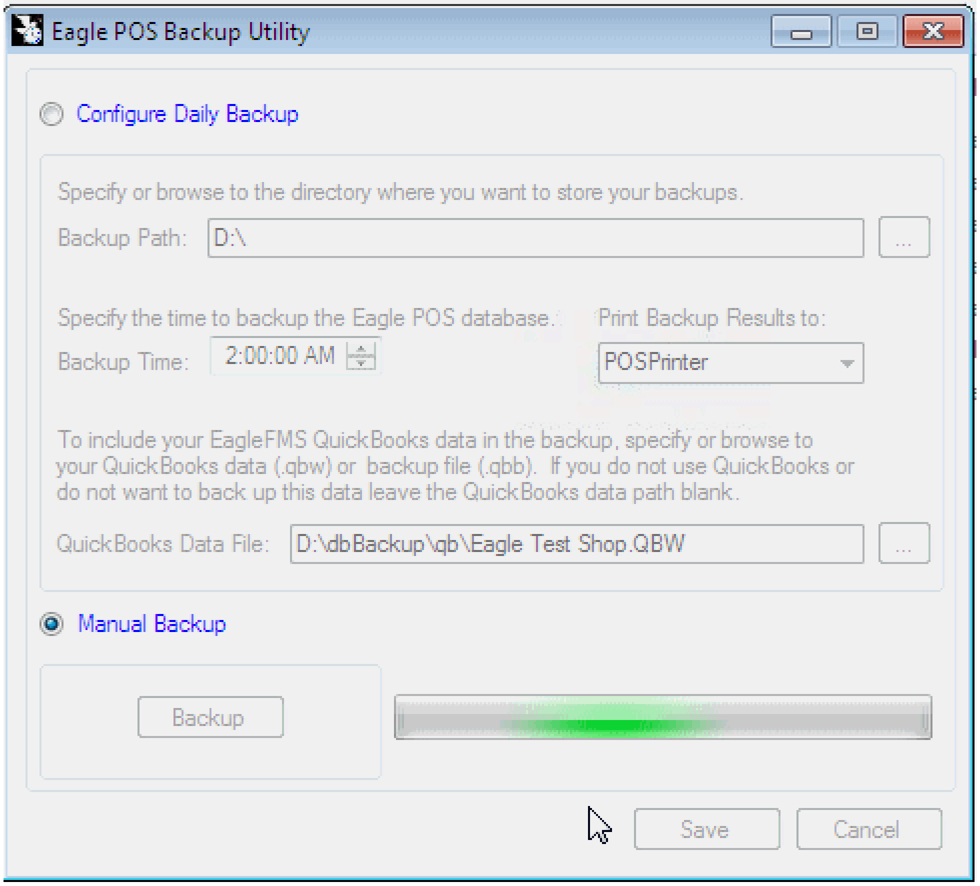
Print Backup Results to: POSPrinter

To include your EagleFMS QuickBooks data in the backup, specify or browse to your QuickBooks data (.qbw) or backup file (.qbb). If you do not use QuickBooks or do not want to back up this data leave the QuickBooks data path blank.

QuickBooks Data File: D:\dbBackup\qb\Eagle Test Shop.QBW

● Manual Backup

5. Wait for the backup to complete.



Eagle POS Backup Utility

○ Configure Daily Backup

Specify or browse to the directory where you want to store your backups.

Backup Path: D:\

Specify the time to backup the Eagle POS database.

Backup Time: 2:00:00 AM

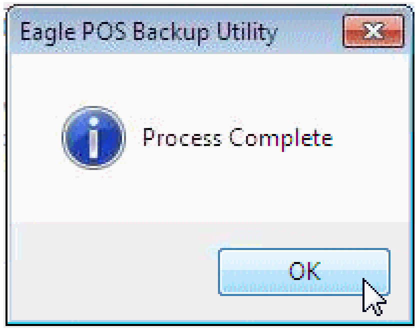
Print Backup Results to: POSPrinter

To include your EagleFMS QuickBooks data in the backup, specify or browse to your QuickBooks data (.qbw) or backup file (.qbb). If you do not use QuickBooks or do not want to back up this data leave the QuickBooks data path blank.

QuickBooks Data File: D:\dbBackup\qb\Eagle Test Shop.QBW

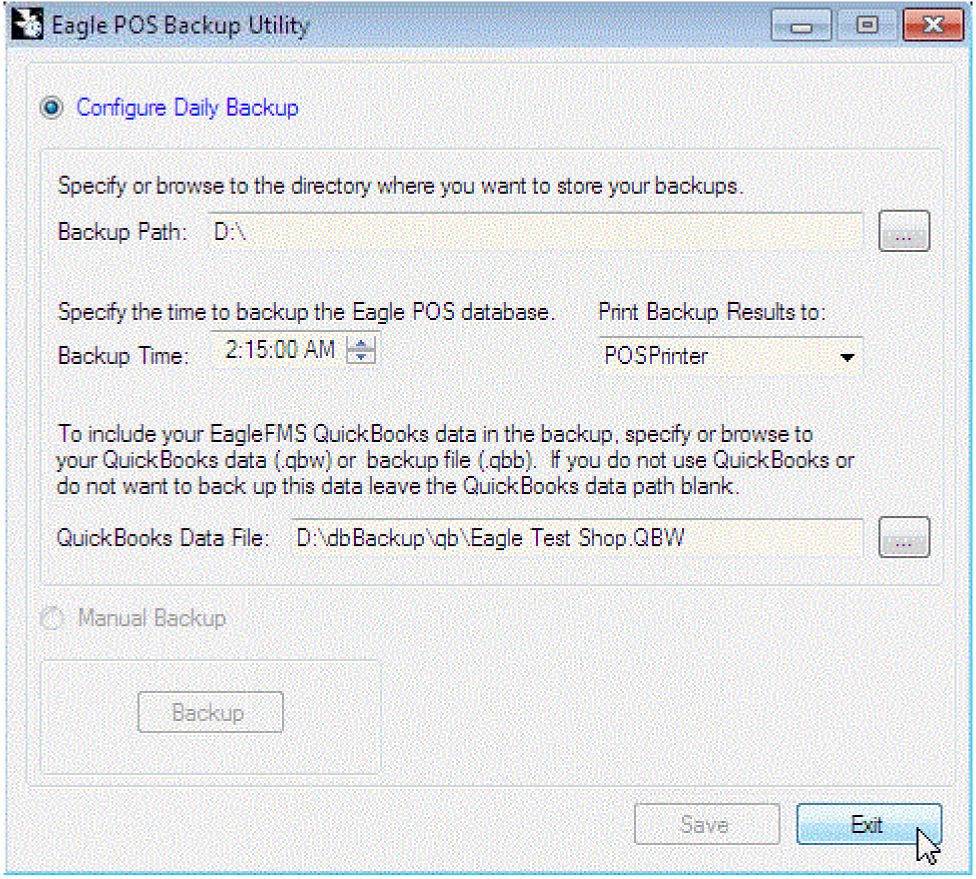
● Manual Backup

6. Click OK to the prompt for the backup completing



Process Complete

7. Click Exit to close the backup configuration screen.



● Configure Daily Backup

Specify or browse to the directory where you want to store your backups.

Backup Path: D:\

Specify the time to backup the Eagle POS database.

Backup Time: 2:15:00 AM

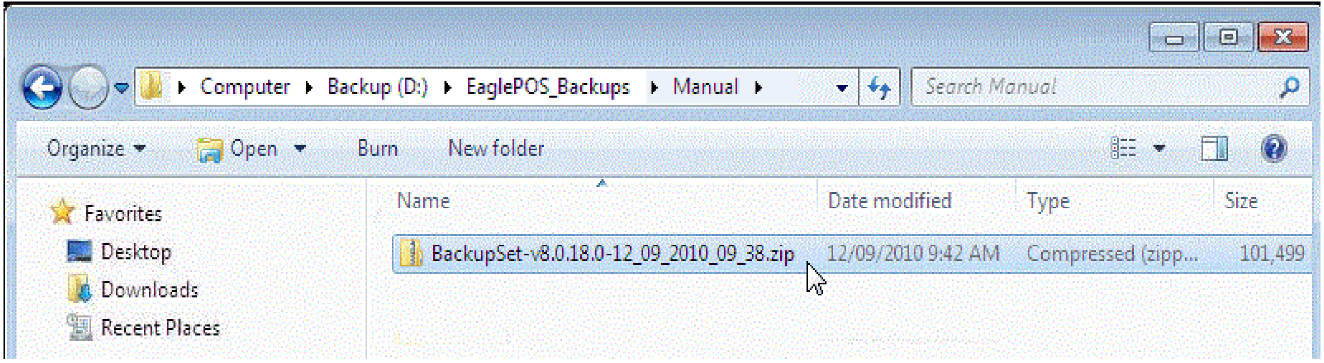
Print Backup Results to: POSPrinter

To include your EagleFMS QuickBooks data in the backup, specify or browse to your QuickBooks data (.qbw) or backup file (.qbb). If you do not use QuickBooks or do not want to back up this data leave the QuickBooks data path blank.

QuickBooks Data File: D:\dbBackup\qb\Eagle Test Shop.QBW

○ Manual Backup

8. Navigate to the backup media and verify the manual backup took place.

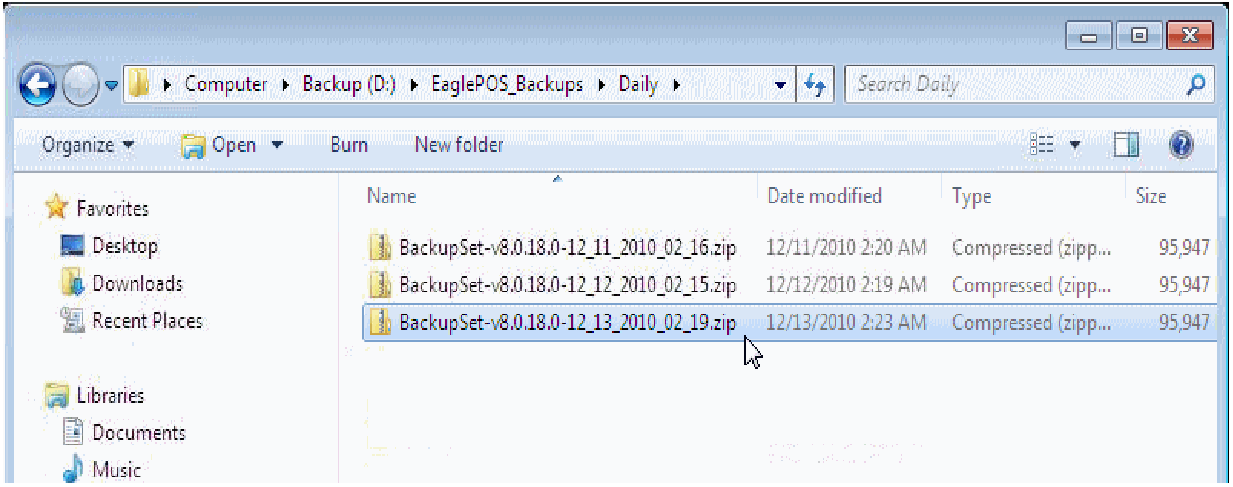


Name	Date modified	Type	Size
BackupSet-v8.0.18.0-12_09_2010_09_38.zip	12/09/2010 9:42 AM	Compressed (zipp...	101,499

Restoring data from the Eagle POS Backup Utility

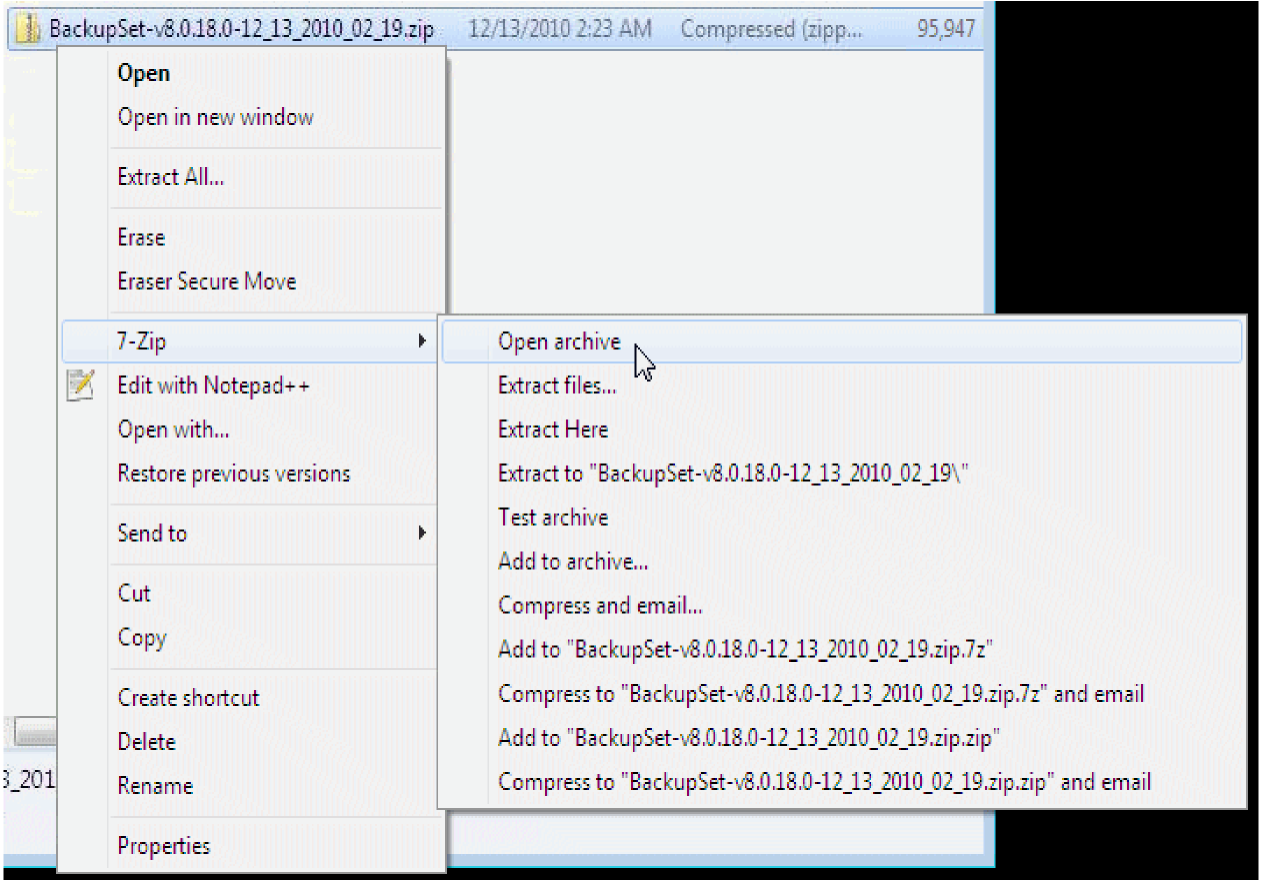
1. If 7-zip is not installed navigate to (http://www.7-zip.org/download.html) and install it.

2. Locate the Backup file that will be used in the restore process on the backup media, it should be located in a folder named EaglePOS_Backups. Depending on which backup was last done look in the Daily or Manual backup folder for the newest backup.



Name	Date modified	Type	Size
BackupSet-v8.0.18.0-12_11_2010_02_16.zip	12/11/2010 2:20 AM	Compressed (zipp...	95,947
BackupSet-v8.0.18.0-12_12_2010_02_15.zip	12/12/2010 2:19 AM	Compressed (zipp...	95,947
BackupSet-v8.0.18.0-12_13_2010_02_19.zip	12/13/2010 2:23 AM	Compressed (zipp...	95,947

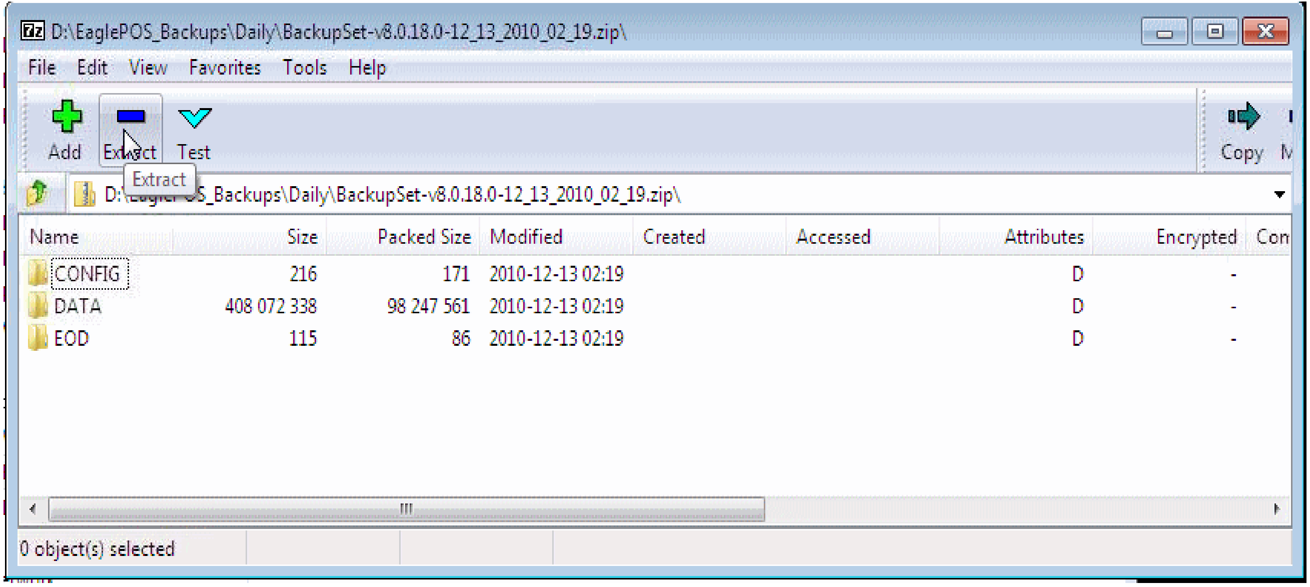
3. Right click the backup file and choose the 7-zip menu option then click on Open archive.



BackupSet-v8.0.18.0-12_13_2010_02_19.zip	12/13/2010 2:23 AM	Compressed (zipp...	95,947

Open
Open in new window
Extract All...
Erase
Eraser Secure Move
7-Zip
Edit with Notepad++
Open with...
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties
Open archive
Extract files...
Extract Here
Extract to "BackupSet-v8.0.18.0-12_13_2010_02_19\"
Test archive
Add to archive...
Compress and email...
Add to "BackupSet-v8.0.18.0-12_13_2010_02_19.zip.7z"
Compress to "BackupSet-v8.0.18.0-12_13_2010_02_19.zip.7z" and email
Add to "BackupSet-v8.0.18.0-12_13_2010_02_19.zip.zip"
Compress to "BackupSet-v8.0.18.0-12_13_2010_02_19.zip.zip" and email
3_201

4. Click on the Extract option on the top menu toolbar.

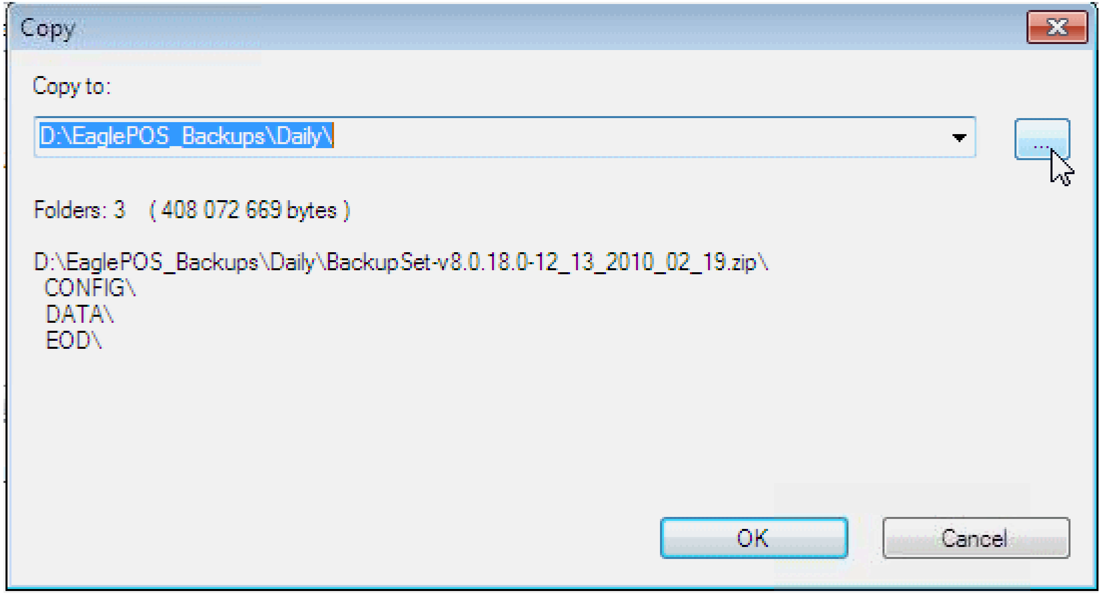


D:\EaglePOS_Backups\Daily\BackupSet-v8.0.18.0-12_13_2010_02_19.zip\

Name	Size	Packed Size	Modified	Created	Accessed	Attributes	Encrypted	Con
CONFIG	216	171	2010-12-13 02:19			D	-	
DATA	408 072 338	98 247 561	2010-12-13 02:19			D	-	
EOD	115	86	2010-12-13 02:19			D	-	

0 object(s) selected

5. Click the ellipsis to configure where the files will be extracted to.



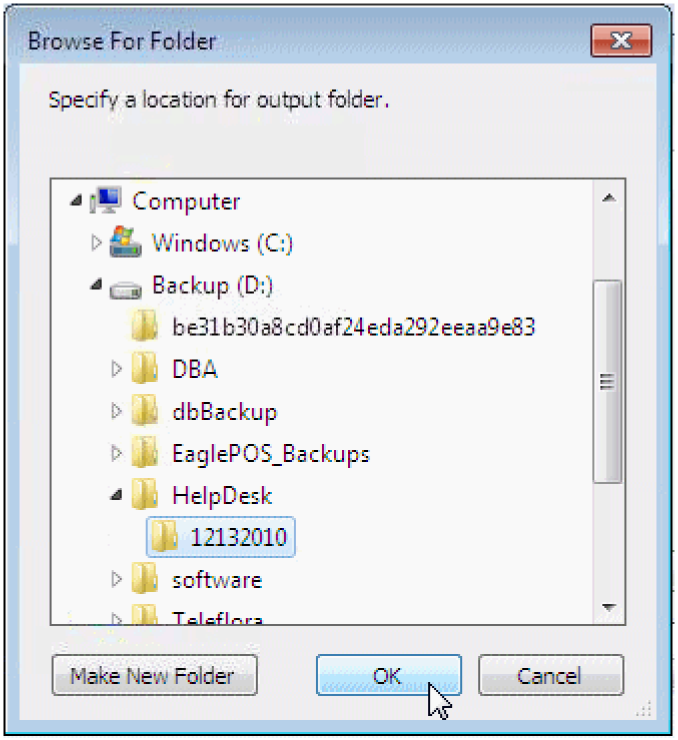
Copy to:

D:\EaglePOS_Backups\Daily\

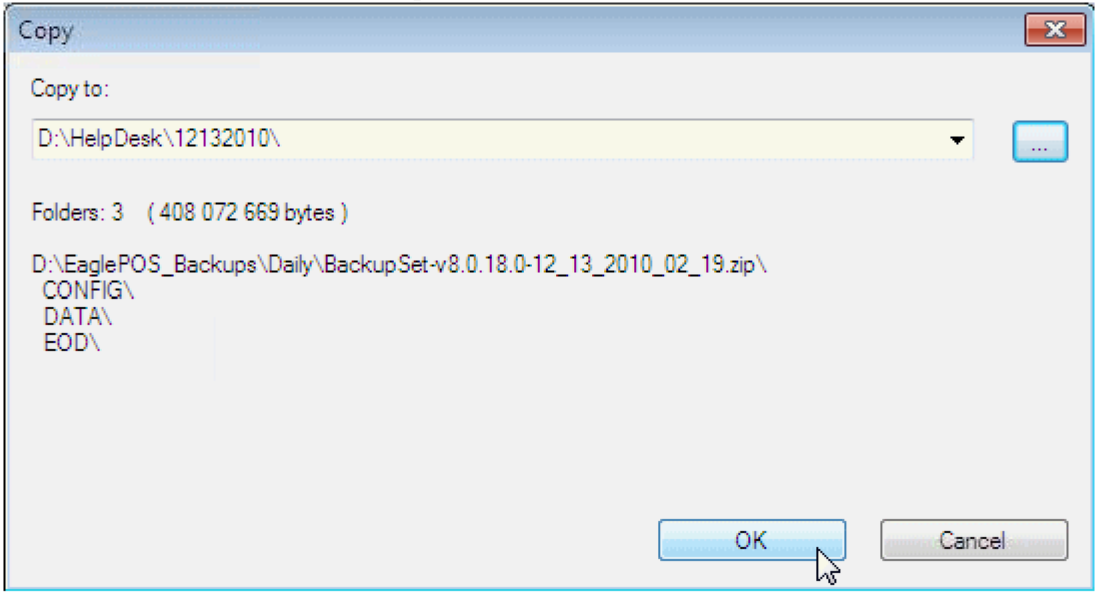
Folders: 3 (408 072 669 bytes)

D:\EaglePOS_Backups\Daily\BackupSet-v8.0.18.0-12_13_2010_02_19.zip\
CONFIG\
DATA\
EOD\

6. In the Browse for Folder window navigate to the Help Desk folder if one does not exist create on. In the Help Desk folder create another folder and give it the days date. In the example provided the date is 12092010 for December 9, 2010.



7. Click OK to start the extraction process.



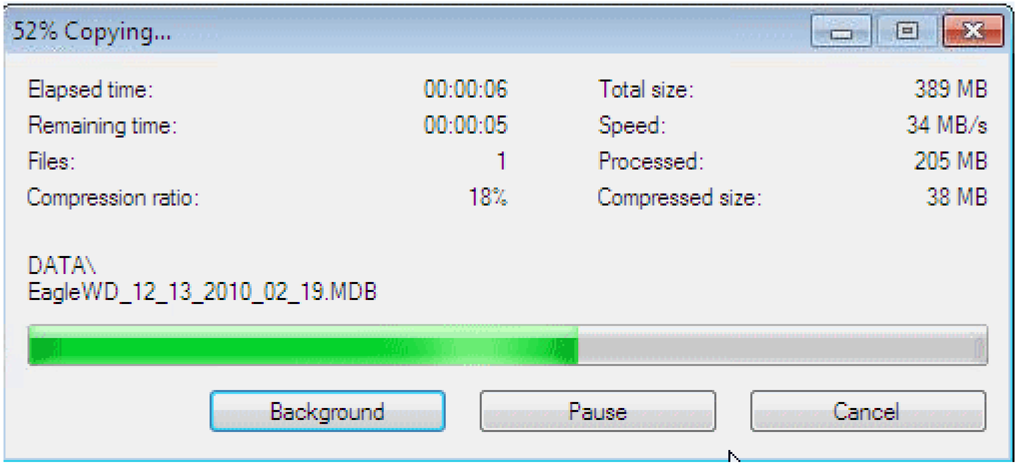
Copy to:

D:\HelpDesk\12132010\

Folders: 3 (408 072 669 bytes)

```
D:\EaglePOS_Backups\Daily\BackupSet-v8.0.18.0-12_13_2010_02_19.zip\
 CONFIG\
 DATA\
 EOD\
```

8. Wait while the files are extracted into the location you specified.

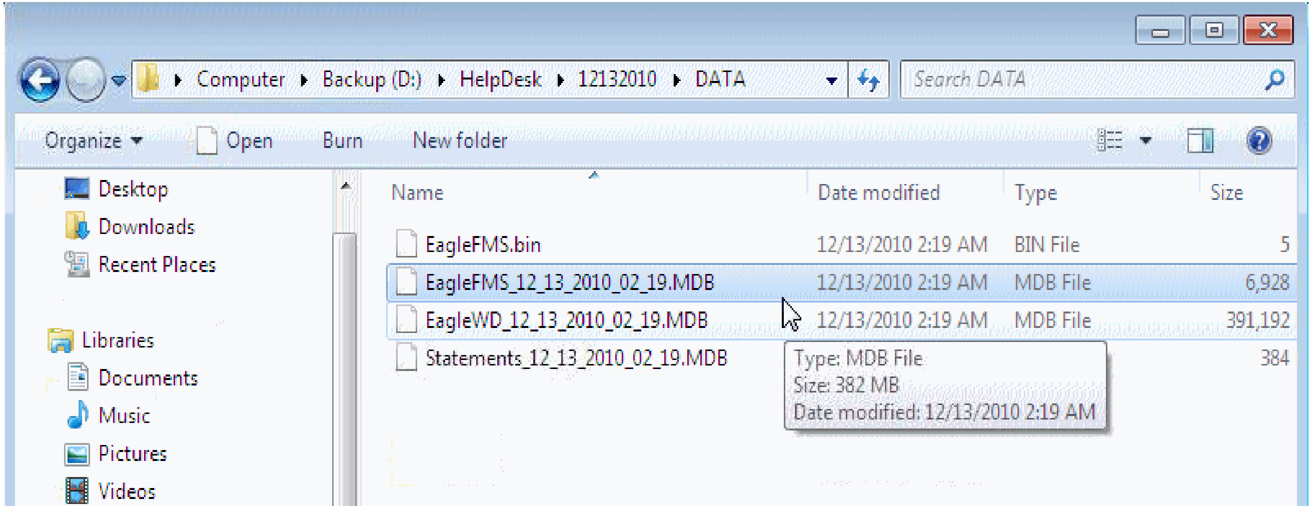


52% Copying...

Elapsed time:	00:00:06	Total size:	389 MB
Remaining time:	00:00:05	Speed:	34 MB/s
Files:	1	Processed:	205 MB
Compression ratio:	18%	Compressed size:	38 MB

DATA\
EagleWD_12_13_2010_02_19.MDB

9. Navigate to the location specified for the extracted files.
Note: The files will have the date/time listed in the file name and will need to be renamed to the correct file format. Example EagleFMS.mdb, EagleWD.mdb, and Statements.mdb



Computer ▸ Backup (D:) ▸ HelpDesk ▸ 12132010 ▸ DATA

Name	Date modified	Type	Size
EagleFMS.bin	12/13/2010 2:19 AM	BIN File	5
EagleFMS_12_13_2010_02_19.MDB	12/13/2010 2:19 AM	MDB File	6,928
EagleWD_12_13_2010_02_19.MDB	12/13/2010 2:19 AM	MDB File	391,192
Statements_12_13_2010_02_19.MDB			384

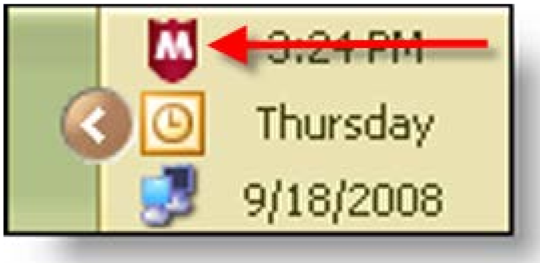
Type: MDB File
Size: 382 MB
Date modified: 12/13/2010 2:19 AM

10. Copy the files into the current EagleFMS data install path.

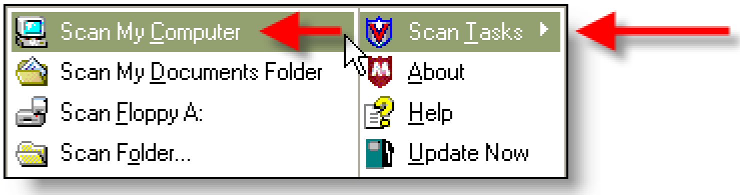
Manually System Virus Scan Using McAfee Total Protection Suite for Small Business

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.

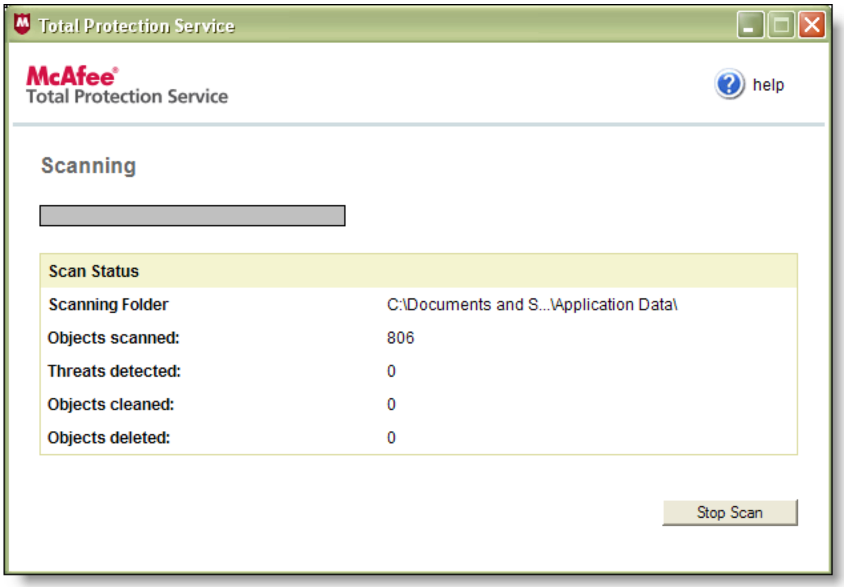
1. Locate the McAfee icon (red shield with a white M in the middle) in the system tray at the bottom right corner of the screen.



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.



Scan Status	
Scanning Folder	C:\Documents and S...\Application Data\
Objects scanned:	806
Threats detected:	0
Objects cleaned:	0
Objects deleted:	0

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

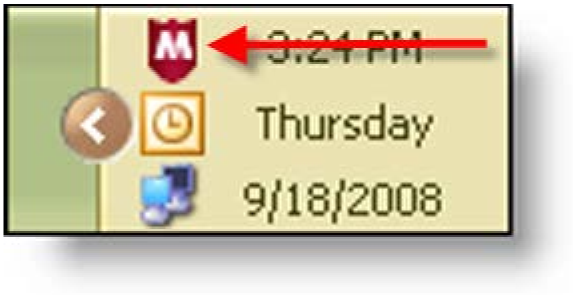
5. Once the scan is complete the results will display on the screen. To view the report details, click the ‘Report’ button at the bottom of the screen. When finished, click the ‘Close’ button. The scan is now complete.

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.

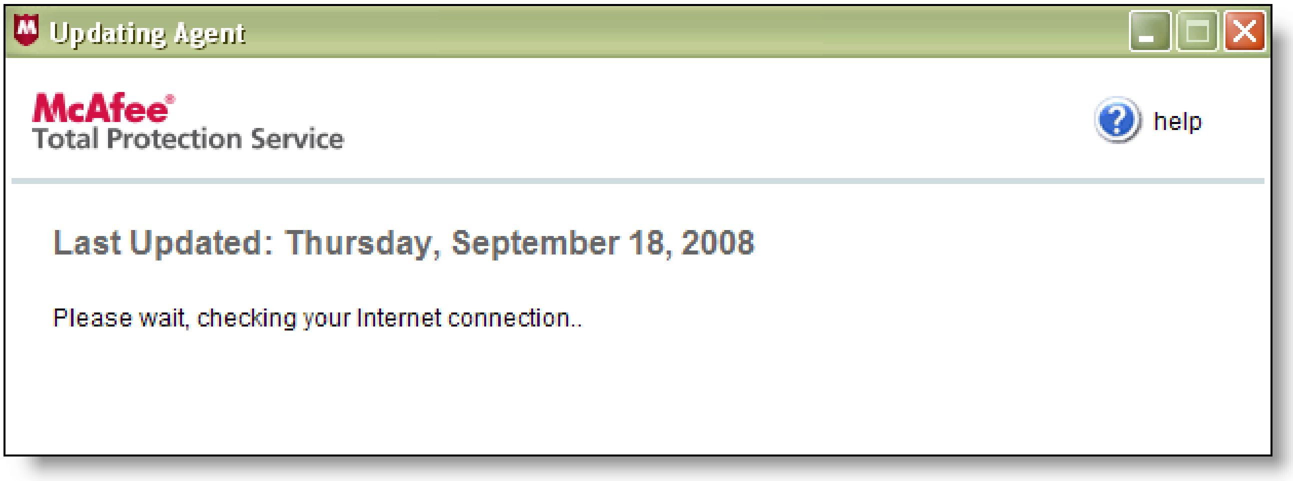
1. Locate the McAfee icon (red shield with a white M in the middle) in the system tray at the bottom right corner of the screen.



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’.

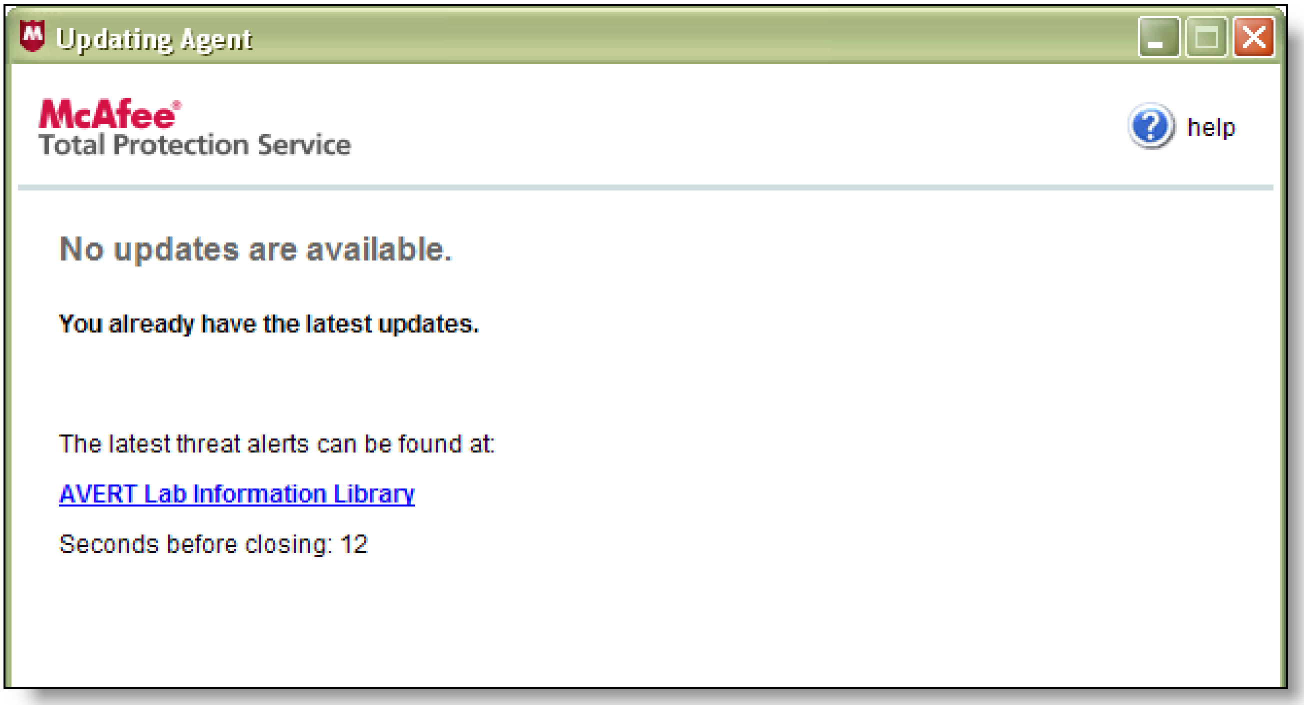
3. Regardless of which option you choose, you will see the following screen:



Last Updated: Thursday, September 18, 2008

Please wait, checking your Internet connection..

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.



No updates are available.

You already have the latest updates.

The latest threat alerts can be found at:

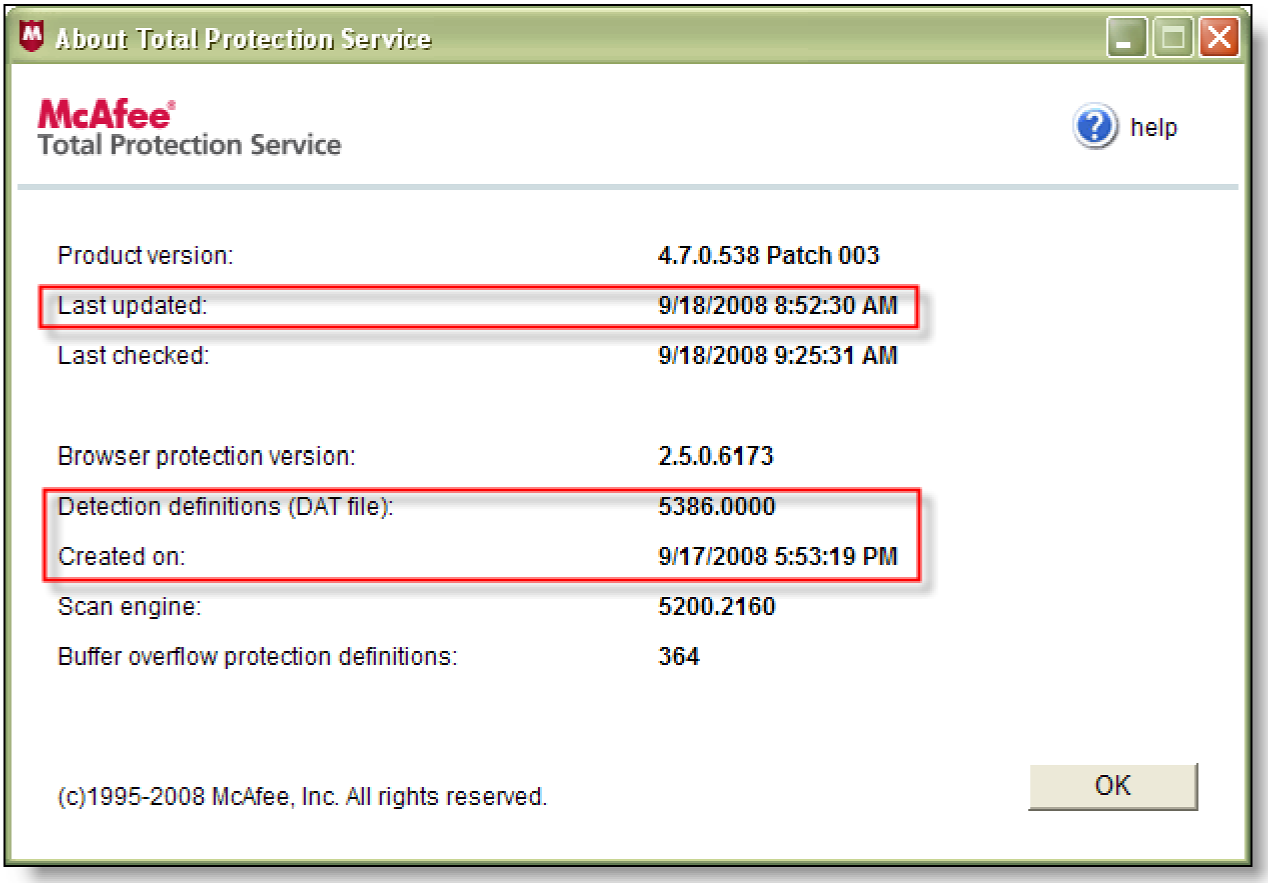
AVERT Lab Information Library

Seconds before closing: 12

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.



Product version: 4.7.0.538 Patch 003
Last updated: 9/18/2008 8:52:30 AM
Last checked: 9/18/2008 9:25:31 AM

Browser protection version: 2.5.0.6173
Detection definitions (DAT file): 5386.0000
Created on: 9/17/2008 5:53:19 PM
Scan engine: 5200.2160
Buffer overflow protection definitions: 364

(c)1995-2008 McAfee, Inc. All rights reserved.

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