



Teleflora Point of Sales

Daisy Version 8.0

PA-DSS Implementation Guide

Version: 1.7
Version Date: May, 2010

REVISIONS

Document Version	Date	Description
1.7	May 28,2010	Updated section "Daisy Connectivity Specifications". Removed outbound internet connections not used by Daisy. Updated section "Collecting Sensitive Data for Debugging" - Added information for log settings. Updated document to make text more user friendly and steps easier for shop owners/managers to follow. Updated firewall requirements, removed old firewall information and Netgear information.
1.6	May 7, 2010	Updated sections "Storage of cardholder information", "How to permanently remove credit card information"
1.5	Apr 6, 2010	Added CC purge steps
1.4	Sep 22, 2009	Updated document per Chris Campbell's comments
1.3	Mar 1, 2009	Updated document per Doug King's comments
1.2	Feb 27, 2009	Recreated document using Dove POS and updated RTI PADSS Implementation guides
1.1	Feb 26, 2009	Updated document per Doug King's comments
1.0	Feb 26, 2009	Initial Document Creation

Table of Contents

Purpose of this Document.....	1
Scope and Definitions	2
To Learn More	3
Dissemination of the PA-DSS Implementation Guide.....	4
Storing Cardholder Information	5
3 rd Party Application Integration	7
Encryption Key Management	8
Collecting Sensitive Data for Debugging	10
User Identification and Authentication	11
Wireless Networks	13
Protection from External Access	14
Using a Remote Daisy System.....	16
Remote Administration of a Daisy System	17
Customer Remote Access	19
Local Administration.....	20
Encrypting over Public Networks.....	21
End-User Messaging Technologies.....	22
Accessing the Daisy Application	23
<u>Appendix.....</u>	24
Daisy Connectivity Specifications.....	24
Firewall Requirements	25
How to Update your Daisy Server's Operating System	26
How to Update your Daisy Software (Altiris).....	28
How to Remove Previous Builds of Daisy from Your System	29
How to Enable the Customer Service Access using eCare	30
How to Enable/Disable the Teleflora Customer Service User Account	36
How to Add a Daisy User Account	37
How to Remove a Daisy User Account	51
How to Securely "Wipe" a Hard Drive.....	53
How to Change/Rotate your Daisy Data Encryption Key	55
How to Permanently Remove Credit Card Information.....	56
How to Create a "Strong" Password in Linux.....	60
How to Verify Password Policies in Windows XP / Vista	62
How to set a Screensaver Lock in Windows XP	64
How to Set a Screensaver Lock in Windows Vista	65
How to Configure your SSH Daemon.....	67
Using the "Shred" Secure Wipe Tool.....	71
Daisy Application Summary	74
Typical Daisy Network Topology	75

Purpose of this Document

If you are a merchant who accepts credit card payments for Visa, American Express, Discover, MasterCard or JCB, you are responsible for making sure your business is in compliance with PCI DSS regulations. These requirements were not created by Teleflora, but were created by the Payment Card Industry Security Standards Council (PCI SSC).

This document is a supplement to the PCI Data Security Standard. It is intended to give “POS Specific” interpretation to guidelines which otherwise, would seem ambiguous. The intended audience of this document is the owner and administrator of a Daisy point-of- sale software system.

Scope and Definitions

In order to reduce retail credit card fraud, Visa and other credit card companies have introduced a new program, Payment Applications Data Security Standards or PA-DSS. 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 Daisy POS system is compliant with these new PA-DSS requirements. However, to remain compliant, you will be responsible for maintaining some procedures as well.

This document provides a number of “Daisy Specific” applications to the various PA-DSS requirements. Please refer to the “Payment Card Industry Data Security Standard” document for full details on compliance regulations.

Following are definitions for some terms used throughout this document.

Term	Definition
PA-DSS	Payment Application Data Security Standard
PABP	Payment Applications Best Practices
PCI	Payment Card Industry (Data Security Standards)
PCI DSS	
Cardholder Information	Minimally, a full credit card number. Could also be a credit card swipe, CVV value and/or Debit card “pin” value or Debit card “pin block”.
Sensitive Data	Either Cardholder information or username/password information.
Daisy Application Server	Physical server (and all software installed by Teleflora) which hosts the Daisy application and its associated data files.
Administrative user	Any Unix user account capable of obtaining a Unix shell on the Daisy Application server.
Data Security Standard	A document, published by Visa, which specifies all policies and requirements fundamental to PABP compliance.

To Learn More

PA-DSS 14.2

The best starting point for PA-DSS information is the PCI Security Council website.

<http://www.pcisecuritystandards.org>

Two specific documents should be considered “must have” supplements to the PA-DSS Implementation Guide:

- 1) PCI DSS Version 1.2 Requirements

https://www.pcisecuritystandards.org/security_standards/supporting_documents_home.shtml

- 2) PCI DSS Self-Assessment Questionnaire

https://www.pcisecuritystandards.org/pdfs/pci_saq_v1-0.pdf

At the time of this writing of this guide (May 2010), we are using the PA-DSS specifications version 1.2 and PCI DSS Revision 1.2 documents.

Dissemination of the PA-DSS Implementation Guide

Addresses:

PA-DSS 14.1

A copy of the PA-DSS Implementation Guide should be available to all who use or administer your Daisy system. This includes not only Teleflora staff (Customer Service, software developers, trainers) , but staff in your shop who use, or are responsible for administering, or otherwise maintaining the Daisy application server and its associated network of workstations.

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 Daisy Customer Service to ensure that you have the latest version of this document.

Daisy Customer Service Contact Information:

Phone: 888-324-7963

Email: daisysupport@teleflora.com

Postal Mail:

Daisy Customer Service
3309 E. Kings Highway
Paragould, AR 72450

Storing Cardholder Information

Addresses:

PA-DSS 1.1

PCI DSS 3.2

It is critically important to protect Credit Card numbers, Credit Card “CVV” (sometimes called “CVC”) numbers, Credit Card “Track” Data (Track1, Track2), and Debit card “pin blocks”.

Your Daisy system has been created to never require storage of CVV and “Swipe” data., As of Daisy version 8.0, Daisy does not yet support “Debit Card” transactions (transactions which require customer entry of a ‘pin’); sensitive “pin block” information is never obtained or captured.

Credit card numbers can be retained if a business need requires retention. However, it is recommended that credit card numbers/information NOT be retained. To locate all credit card information, you should look in non-obvious places/locations. For instance, phone order paper logs and old credit card settlement reports may contain one, or a number of Credit Card Numbers. Older POS servers, or backup media, could also contain unprotected cardholder information. It is essential that you destroy this data, unless you have significant business reasons to retain the information. In the case that cardholder information must be retained, it is then your responsibility to properly protect this data as per PCI DSS specifications.

How-to remove data from older servers (PA-DSS 1.1.4):

If you have old computers that contain a legacy POS system and its data, you must securely remove all Swipe and CVV data from that POS system computer. Removal of this data is absolutely necessary for PCI DSS compliance. Because it is often impossible to know, for sure, *if* such data exists, and, if so, *where* the data would reside, your safest route to data removal is to use a secure “wipe” tool which both erases and low-level formats all hard drives. Teleflora suggests using a “disk wipe” utility, such as “DBAN” (<http://dban.sourceforge.net>) for securely wiping hard drives. DBAN is a free download. Please see the appendix of this document for the step-by-step procedure for securely wiping the hard disk of a computer.

Updating Daisy Versions:

If you are updating from one “build” of Daisy to the next, your “old” version of Daisy is renamed to /d/daisy-YYYYMMDDHHMMSS, where “YYYYMMDDHHMMSS” represents the date and time on which the install occurred. By recursively removing these “archive” directories, with the ‘shred’ command, you will have safely removed any CVV or Swipe data these legacy POS environments may have stored.

Please see the appendix for step-by-step directions on how to remove any and all previous versions of Daisy from your Daisy system.

Destroying Legacy Paper Artifacts:

Many older POS Systems printed full credit card numbers on paper items such as receipts and reports. It is your responsibility to locate and destroy any of these items which are no longer needed for relevant business purposes. Teleflora recommends you purchase a cross-cut shredder for such purposes. Any documents which remain intact should be protected under lock and key as per PCI DSS section 9.

Protecting Legacy Data Backups:

Legacy data backups should also be protected, as, many of these could contain sensitive data in an unencrypted format. If you believe it is unlikely that you will use these backups, it is best to physically destroy the backup media. Any media which remain intact should be protected under lock and key as per PCI DSS section 9.

3rd Party Application Integration

Addresses:

PA-DSS 1.1.1

PA-DSS 1.1.2

PA-DSS 1.1.3

Your Daisy Application server has been configured to ensure PA-DSS compliance. To maintain this level of secure integrity, Teleflora recommends against the modification of system configurations or the installation of additional software on the Daisy application server.

In the event third party applications are added or modifications made to the Daisy application server, the additional application(s) must not negatively impact the integrity of PA-DSS compliance. In keeping with PA-DSS standards, the following rules also apply.

- Any 3rd party applications installed must NOT retain Credit Card “CVV”, “CVV2”, Swipe or Debit Pin information subsequent to (following) card authorization. (1.1.1/1.1.2/1.1.3)
- In order to maintain security integrity, Teleflora does not recommend installation of any additional applications onto the Daisy Application server. In the event that third party applications are added to the Daisy application server which are capable of accessing Daisy application data files, these applications must also conform to the PCI Data Security Standards. (3.x.y)
- If any 3rd party applications produces log files containing cardholder information, these log files must be removed immediately upon being used. The customer should, by default, disable logging of full cardholder information.
- Any 3rd party applications must encrypt any and all network communications. 128 bit SSL (or greater) encryption must be used. (5.1.3 / 12.1)

Once you have completed any system modifications, or software additions, Teleflora recommends you perform a re-evaluation of PA-DSS system compliance. The re-evaluation procedure is located in the Visa CISP “Payment Applications Best Practices” document.

Encryption Key Management

Addresses:

PA-DSS 1.1.4
PA-DSS 2.7
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

Your Daisy system uses AES-128 bit encryption technology in order to encrypt any cardholder information being retained on disk. AES-128 is the Advanced Encryption Standard selected by the National Institute of Standards and Technology. This encryption process is incredibly secure. The NSA uses this same standard for Top Secret data. An “encryption key”, comprised of special files on disk, is used to protect data.

In order to retain the proper level of security, you must follow some key management procedures as per PCI DSS 3. Directives you must follow are summarized as follows:

- 1) Restrict access to the decryption key material (Daisy files) to the fewest number of people possible. (PCI 3.5.1)
- 2) Store the cryptographic files in the fewest possible locations and formats. Do not make multiple “copies” of your Daisy files in unprotected or insecure storage locations. (PCI 3.5.2)
- 3) Store the cryptographic files in a secure location and form. (PCI 3.6.3)
- 4) In the event of software or system changes, ensure that older encryption keys are securely deleted (See appendix on using a secure delete utility). (PCI 3.6.5, PCI 3.6.8)
- 5) Change the encryption password (DeK), at least annually. (PCI 3.6.4)
- 6) Do not retain old cryptographic files; destroy them once you are finished using them. (PCI 3.6.5)
- 7) Prevent the unauthorized substitution of cryptographic material. For example, do not tamper with the file permissions structure of your Daisy system (PCI 3.6.7)
- 8) If you know, or even suspect, that your data encryption key(s) have been taken, stolen, or in any way compromised, you should rotate the encryption keys immediately (PCI 3.6.8)

Upgrading Software

In the event that you are updating from a previous version of Daisy, or even a different point-of-sale platform, cryptographic material (encryption/decryption keys) must be securely deleted from your Daisy system. This secure deletion is required for PCI DSS compliance. (PCI 3.6.5)

If you are installing Daisy on a computer which was formerly used for another purpose, you must, prior to installing the Daisy point-of-sale, “wipe” the hard disk with a utility such as “DBAN” (<http://dban.sourceforge.net>); then, a “clean” Operating System image can be installed. Please work with Teleflora Customer Service to create a PCI DSS compliant deployment strategy which is least intrusive to your business.

Each time you update your Daisy software, a complete copy of your previous Daisy system (software, data and configurations) is encrypted and saved in a file called /d/daisy-YYYYMMDDHHMMSS.

Though this data is encrypted, it is still important to save this file off to external media (DVD, rev disk, etc.) then securely remove the file from your hard disk. The external media should be stored in a safe physically locked location.

If you are updating from one “build” of Daisy to the next, your “old” version of Daisy is automatically renamed to /d/daisy-YYYYMMDDHHMMSS, where “YYYYMMDDHHMMSS” represents the date and time when the install occurred. As part of the upgrade process, this older directory should be securely removed, however, in the rare instance that the upgrade process is abruptly halted; your “old” directory may still be present on disk. By recursively removing these “archive” directories, you will have safely removed all decryption keys contained within the previous version of Daisy software. PCI requires that you securely remove any and all old keys from your Daisy system (PCI 3.6.5)

Please read “How to remove past builds of Daisy” in the appendix of this document for detailed instructions of removing older cryptographic materials from disk.

Data Encryption Keys:

Your Daisy system never stores credit card “swipe” information or “CVV” to disk, subsequent to authentication. However, your system may store Credit Card numbers to disk in an encrypted form using AES, 128 bit (or greater) encryption. The password used to encrypt your data is part of what is called the “Data Encryption Key” (DEK). The data encryption key is contained as one of the data files on your Daisy system (in the “daisy” directory) and is encrypted with a “Key encrypting Key”, as well as being accessible only in a programmatic fashion to users of the Daisy system. You may choose to “rotate” the password used to encrypt your cardholder data at any time you like. **Note:** PCI requires rotating encryption keys at least once per year (PCI 3.6.4). It is recommended that you rotate encryption keys any time an employee with administrative privileges leaves your employ. (PCI 3.6.8).

Please read “How to Change your Daisy Data Encryption Key” process in the appendix for detailed instructions on changing your Daisy Data Encryption Key.

Key Encryption Keys:

Your Daisy Data Encryption Key (DeK) is encrypted with a “Key Encryption Key” (KeK). The value of this second key is stored within a separate data file in your /d/daisy directory. Because the KeK is stored within your file system, it is important not to compromise the security settings (chmod, chown, chgrp) of your “daisy” directory, doing so could result in unauthorized substitution of your encryption keys. (PCI 3.6.7) Note your KeK is managed by the Daisy system and is periodically changed as your Daisy system is upgraded. If you think your KeK has been compromised, contact Daisy Customer Support.

Collecting Sensitive Data for Debugging

Addresses:

PA-DSS 1.1.5

PCI DSS 3.2

To assist with troubleshooting, the Daisy application creates a defined set of log files for some applications. These unencrypted log files do not contain sensitive cardholder information, even when the highest level of debug is enabled. Log files are retained only for a month, and then they are overwritten.

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

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

If you purchased your Daisy system through a reseller, or installed Daisy through a third party integrator, your employees, resellers and integrators must comply with the following requirements:

- Resellers/integrators must collect sensitive authentication data only when needed to solve a specific problem.
- Resellers / Integrators must store sensitive data only in specific, known locations with limited access.
- Resellers / Integrators must collect only the limited amount of data needed to solve a specific problem.
- Resellers / Integrators must encrypt sensitive authentication while it is being stored.
- Resellers / Integrators must securely delete sensitive data immediately after use.

User Identification and Authentication

Addresses:

PA-DSS 3.1.c
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

If a data breach occurs, you need to be able to effectively identify who had access to compromised cardholder data. Your Daisy system relies on the Linux “PAM shadow” authentication mechanism which employs MD5 hashing, to provide unique and secure sessions. In order to prevent impersonation and unauthorized access to your Daisy system, the following guidelines should be followed. Note that 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

Limited Access Users:

PA-DSS section 3.1 specifically notes that PCI 8.5 does not need to apply to employees who have access to only one credit card number at any time. This means that employees who do not have “manager” privileges, and who can only use the Daisy application, and do not have the ability to obtain a Unix “shell”, do not need to comply with PCI DSS section 8.5. However, Teleflora recommends you follow section PCI DSS for all of your employees, regardless of their level of access to the Daisy system.

Teleflora Remote Administration Account:

Daisy Customer Service uses the “tfsupport” user account in order to remotely administer your Daisy system. Unless debugging a specific, user related problem, customer service should not login to your system as any other, already existing user account. As with your local user accounts, the “tfsupport” account is also required to use a PCI DSS authentication rules as per 8.5.1 – 8.5.16.

Wireless Networks

Addresses:

PA-DSS 6.1.b

PCI DSS v1.1 Section 1.3.9

PCI DSS v1.1 Section 2.1.1

PCI DSS v1.1 Section 4.1.1

Teleflora DOES NOT recommend, sell or support the use of wireless networks within the Daisy POS environment.

Protection from External Access

Addresses:

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

Protecting the Daisy Server:

PA-DSS 9.1.b

The Daisy server contains cardholder data stored to disk. It is critically important that your Daisy server IS NOT directly accessible from the internet. It is required that you use a “firewall” device between the Daisy server and the internet to restrict connections established from the internet to your Daisy server.

Protecting Daisy Workstations:

PA-DSS 10.1

The Daisy Workstation does not store cardholder information to disk. However, workstations 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. It is required that each workstation use a hardware firewall, and, in the case of multiple locations, use a PCI compliant “VPN” to network these workstations to the server.

Protecting other Computers on your Daisy Network:

PA-DSS 9.1.a

PA-DSS 9.1.b

Adding computers on the same network as your Daisy server may compromise your system’s security, and your PCI compliance. If you are considering adding any additional machines to your Daisy network, you must ensure that the new computer(s) do not expose any network services to the public internet (for example, game related servers).

Firewall Configurations:

For more information on PCI compliant firewall settings, please see PCI section 1.3. See: How to Securely Configure a Wired Network Router in the appendix.

Protecting Mobile Computers (Laptops):

PA-DSS 10.1

Teleflora DOES NOT recommend or support the use of mobile computing devices (most notably, laptops) connecting to your Daisy network.

Protecting Modems:

PCI 12.3.9

You must protect any dialup modem access to your Daisy server. If you still use a “customer service modem”, be sure to leave the modem device powered off until the time it is needed. Once Customer Service has completed their maintenance of your system, you should turn the modem off again and leave it in the “off” position.

Daisy Software Updates:

Occasionally, Teleflora will need to update your Daisy system with critical security updates. Critical updates may be securely installed on your machine in either an automated or manual fashion. In an automated update, the “Altiris” software will use a secure SSL connection to update your Daisy system. In a manual update, you will be notified by Teleflora customer service of an upcoming update to your system. Teleflora Customer service will then remotely update your system at either a specified time, or a time you have coordinated with customer service. If you refuse, or otherwise prevent these Daisy software updates, the security and PCI compliance of your system will be at risk.

Other Servers:

PA-DSS 9.1.a

PA-DSS 9.1.b

If you choose to host an internet accessible server (such as a web server), PA-DSS compliance requires that your internet accessible server CANNOT be used to store cardholder data. Your internet accessible server must be a different server and be located on a network which is DMZ'ed from any server (e.g. your Daisy server) which stores cardholder data. A DMZ network is a separate and unfiltered connection that effectively isolates your internet accessible server from the secure network where your Daisy server resides. Any internet accessible server you create CANNOT store cardholder data. Teleflora does not recommend running a Web Server on the same network as your Daisy server. Your Daisy system does not contain a web server.

Using a Remote Daisy System

Addresses:

PA-DSS 11.2

PCI DSS 8.3

Any time you use the internet to connect from a workstation to your Daisy server, you are remotely accessing your Daisy server. A good example of remote access would be if you had multiple locations, but only one location houses your Daisy server. The other locations would be remotely accessing the Daisy server. When you remotely access your Daisy server, PCI DSS 8.3 requires “two factor” authentication to be used to authorize the remote connections. Teleflora recommends the use of an IPSEC based VPN which employs both “certificate” based authentication, as well as “username/password” based authentication.

Remote Administration of a Daisy System

Addresses:

PA-DSS 11.3
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 eCare Remote Assistance:

When you need remote assistance, Teleflora Customer Service will use the eCare system to access your computer. You will find instructions for using eCare in the appendix of this document. Be aware of the following requirements and points of note for eCare:

- Teleflora's eCare system will always be accessed using the URL: <http://help.myteleflora.com>. Never use a different or unknown URL in order to access the eCare home page.
- Teleflora will never solicit remote access requests via email.
- Your eCare sessions will be encrypted using a 128 bit SSL connection. DO NOT attempt to disable, or otherwise override this encryption.
- Do not use the eCare system if your browser indicates the eCare SSL certificate is not trustworthy.
- Never leave an eCare 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 eCare sessions.
- Teleflora Customer Service cannot access your computer until you explicitly allow such access through the eCare system.

For more information on eCare, and how it works, please visit:

<http://www.netopia.com/software/products/ecare/index.html>

- When remote administrative access is needed on the Daisy application server, Teleflora will use the "tfsupport" Unix User account and possibly, the "root" user account.
- Teleflora recommends that the "root" user account never be directly accessible remotely. Instead, administrators should log in as an account with normal user privileges, and then use the "sudo" utility to execute privileged commands.
- Any account on the Daisy server capable of obtaining a shell should use complex passwords as per PCI 8.5.8 – 8.5.15. (PA-DSS 3.2)
- Unencrypted protocols (such as Telnet, rsh or FTP) must NEVER be used to administer a Daisy application server, or transmit unencrypted sensitive data. Teleflora recommends the use of the "ssh" protocol for any remote administration of the Daisy application server. (PA-DSS 13.1)
- Unencrypted protocols (such as HTTP or Telnet) must NEVER be used to administer the Daisy firewall device. Teleflora recommends the use of either "HTTPS" or "SSH" protocols. (PA-DSS 13.1)
- Automatic security update services (such as 'yum' in Linux, or 'Windows Update' in Windows) should always be enabled. The system should be checked on a regular basis to ensure that patches are available and being applied. (PA-DSS 7.1.a)
- The firewall device firmware or software should be updated in the event that security updates are made available by the vendor. (PA-DSS 7.1.a)

Other Remote Administration:

If you allow a third party to remotely administer your Daisy server and/or network, be aware that these third parties must also use PCI compliant practices so that your system can continue to be PCI compliant. Encryption technology, such as SSL, SSH, TLS or VPNs must be employed for any remote administration tasks.

Customer Remote Access

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

PCI-DSS V1.1

8.3 Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.

8.4 Encrypt all passwords during transmission and storage on all system components.

8.5 Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:

8.5.1 Control addition, deletion, and modification of user IDs, credentials and other identifier objects

8.5.2 Verify user identity before performing password resets.

8.5.3 Set first-time passwords to a unique value for each user and change immediately after the first use.

8.5.4 Immediately revoke access for any terminated users.

8.5.5 Remove inactive user accounts at least every 90 days.

8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed.

8.5.7 Communicate password procedures and policies to all users who have access to cardholder data.

8.5.8 Do not use group, shared, or generic accounts and passwords.

8.5.9 Change user passwords at least every 90 days.

8.5.10 Require a minimum password length of at least seven characters.

8.5.11 Use passwords containing both numeric and alphabetic characters.

8.5.12 A minimum of five (5) unique passwords must be used for each UNIX user. Meaning that the user can not use the same password used in the last 4 password changes. The system will store the last 5 passwords used so after the 5th password has been entered and validated password #1 could be used again.

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.

Local Administration

- The Daisy application does not require “root” privileges to execute. Teleflora strongly recommends against running the Daisy application as the “root” user or any other user with “root” privileges.
- Administrative activities must be associated with an individual. If an administrative activity is needed, Teleflora recommends against logging in as the “root” user. Instead, each administrative user should be assigned a unique, UNIX user account, and then use “sudo” to execute any privileged commands.
- When an administrator-level employee is terminated from your shop, that user’s account should be immediately disabled or removed from the Daisy application server. (PCI 8.5.4)

Encrypting over Public Networks

Addresses:

PA-DSS 12.1

PCI DSS 4.1

Public Networks are:

- The Internet
- Any Wireless (Wi-Fi) network.
- Cellular telephone networks, such as “GSM” or “GPRS”.
- Any network whose security you are unsure of should be considered “public”.

If a device, such as a PC or laptop, is capable of connecting to the Daisy server via a Wireless (Wi-Fi), Internet, GSM or GPRS networks, session encryption must be used. Teleflora recommends the use of the “SSH” protocol in order to meet PCI DSS requirements 4.1 for encryption. To provide connectivity between shops, Teleflora recommends the use of an IPSEC based VPN, or any other VPN which provides AES-128 bit encryption capabilities as well as two factor authentication.

Unlike older versions of Daisy, use of the telnet protocol is absolutely forbidden for PCI compliance.

End-User Messaging Technologies

Addresses:

PA-DSS 12.2

PCI DSS 4.2

Your Daisy system will never send cardholder information via email, instant messaging, or any other end-user messaging technology. Your Daisy server is not capable of receiving cardholder data via email or other end-user messaging technologies. Teleflora strongly advises against the use of email, chat, instant messaging or any other end-user messaging technologies as method for sending cardholder information.

If your business requires the use of email or other end-user messaging technologies for sending cardholder information, PCI DSS section 4.2 requires that any credit card number be sent in an encrypted format using at least 128 bit strong encryption.

Note: Your Daisy system has an internal email system built in for allowing intra-department communications. This email system does not use traditional internet email mechanisms, but instead, uses Daisy database files for storing messages and their status. From a Credit Card compliance perspective, these email boxes are not encrypted. You must NEVER send cardholder information via these internal email systems.

Accessing the Daisy Application

Your Daisy application relies on the underlying authentication mechanism of your Operating System to protect against unknown parties accessing your system. It is important that you and your staff are aware of and adhere to the following guidelines:

PA-DSS 3.1

PCI 8.5.15

On any workstation, a screensaver must be enabled. The screensaver must require a password to unlock access to the workstation. The screen should automatically lock after 15 minutes of inactivity. See the appendix for directions on setting your local screensaver locks.

PA-DSS 3.1

PA-DSS 3.2

PCI 8.5.8

PCI 8.5.15

Each user with administrative (UNIX shell) access to the Daisy server or whose permissions allow viewing more than one credit card at a time must log in with a unique username and complex password in compliance with PCI standards 8.5.8 through 8.5.15.

PA-DSS 3.1

PCI 8.5.13

If a user attempt to log on and fails login authentication six consecutive times, that user account will be automatically locked for at least 30 minutes or until an administrator manually unlocks the account (whichever occurs first).

PA-DSS 3.3

PCI 8.4

An encrypted protocol (Daisy uses SSH) must be used to encrypt all login (authentication) attempts into the Daisy server.

Appendix

Daisy Connectivity Specifications

The Daisy Connectivity Specification section will assist you with confirming incoming connections. If you are providing your own network security configurations, it will allow you to apply appropriate firewall and modem blocking rules.

The Daisy application server supports (but does not require) the following modem dial-in capabilities:

- Dove Network
- Customer Support

The Daisy application server may use the following modem dial-out capabilities:

- Dove Network
- Credit Card Authorizations and Settlements

All Dove Network dial-in calls will originate with the caller ID of 405-440-6408.

All Teleflora Support dial-in (data) connections will originate with a caller ID of 870-236-7731.

All remote administration of the Daisy application will occur through the tfssupport user.

Your firewall device should be configured to deny all “inbound” internet traffic except for the following IP Ports.

The Daisy application server requires outbound internet connections to the following destination IP Ports:

- TCP Port 22 (SSH)
- TCP Port 80 (HTTP)
- TCP Port 443 (SSL / HTTPS)

Firewall Requirements

1. Firewall configuration must restrict connections between un-trusted networks and any system components in the cardholder data environment. *PCI DSS Requirement 1.2*
2. Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment. *PCI DSS Requirement 1.2.1*
3. Ensure router configuration files are secure. *PCI DSS Requirement 1.2.2*
4. Firewall must be installed between any wireless networks and the cardholder data environment and configured to deny or control any traffic (if such traffic is necessary for business purposes) from the wireless environment into the cardholder data environment. *PCI DSS Requirement 1.2.3*
5. Prohibit direct public access between the internet and any system component in the cardholder data environment. *PCI DSS Requirement 1.3*
6. Implement a DMZ (demilitarized zone) to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment. *PCI DSS Requirement 1.3.1*
7. Block all inbound traffic except to addresses within a DMZ (demilitarized zone). *PCI DSS Requirement 1.3.2*
8. Do not allow any direct routes inbound or outbound for traffic between the internet and the cardholder data environment. *PCI DSS Requirement 1.3.3*
9. Do not allow internal addresses to pass from the internet into the DMZ (demilitarized zone). *PCI DSS Requirement 1.3.4*
10. Restrict outbound traffic from the cardholder data environment to the internet such that outbound traffic can only access IP addresses within the DMZ (demilitarized zone). *PCI DSS Requirement 1.3.5*
11. Implement dynamic packet filtering, allowing only “established” connections into the network. *PCI DSS Requirement 1.3.6*
12. Implement IP masquerading to prevent internal addresses from being translated and revealed on the internet. Use NAT (network address translation). *PCI DSS Requirement 1.3.8*
13. Change the default password before installing the firewall on the network. *PCI DSS Requirement 2.1*
14. Incorporate two-factor authentication for remote access (network-level access originating outside of the network) to the network by employees, administrators and third parties. *PCI DSS Requirement 8.3*
15. Set first-time password to a unique value for each user and change immediately after first use. *PCI DSS Requirement 8.5.3*
16. Immediately revoke access for any terminated users. *PCI DSS Requirement 8.5.4*
17. Remove/disable inactive user accounts at least every 90 days. *PCI DSS Requirement 8.5.5*
18. Enable accounts used by vendors for remote maintenance only during the time period needed. *PCI DSS Requirement 8.5.6*
19. Change user passwords at least every 90 days. *PCI DSS Requirement 8.5.9*
20. Require a minimum password length of at least seven characters. *PCI DSS Requirement 8.5.10*
21. Use passwords containing both numeric and alphabetic characters. *PCI DSS Requirement 8.5.11*
22. 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 Requirement 8.5.12*
23. Limit repeated access attempts by locking out the user ID after not more than six attempts. *PCI DSS Requirement 8.5.13*
24. Set the lockout requirement to a minimum of 30 minutes. *PCI DSS Requirement 8.5.14*
25. If a session has been idle for more than 15 minutes, require the user to re-enter the password. *PCI DSS Requirement 8.5.15*

How to Update your Daisy Server's Operating System

PA-DSS 8.1
PA-DSS 10.1
PCI 6.1

Your Daisy Server uses the RedHat Enterprise Linux environment. RedHat Enterprise Linux uses a tool called “up2date” to ensure that security patches are in place. Daisy is written to run reliably when all OS auto-updates are enabled. (PA-DSS 8.1) PCI DSS requires that you install all security patches within one month of their release. (PCI 6.1). It is highly recommended that you enable (and leave enabled) all auto-update functionality of your Linux operating system. If you want to update your RedHat system, go to **Linux -> RedHat Updates**

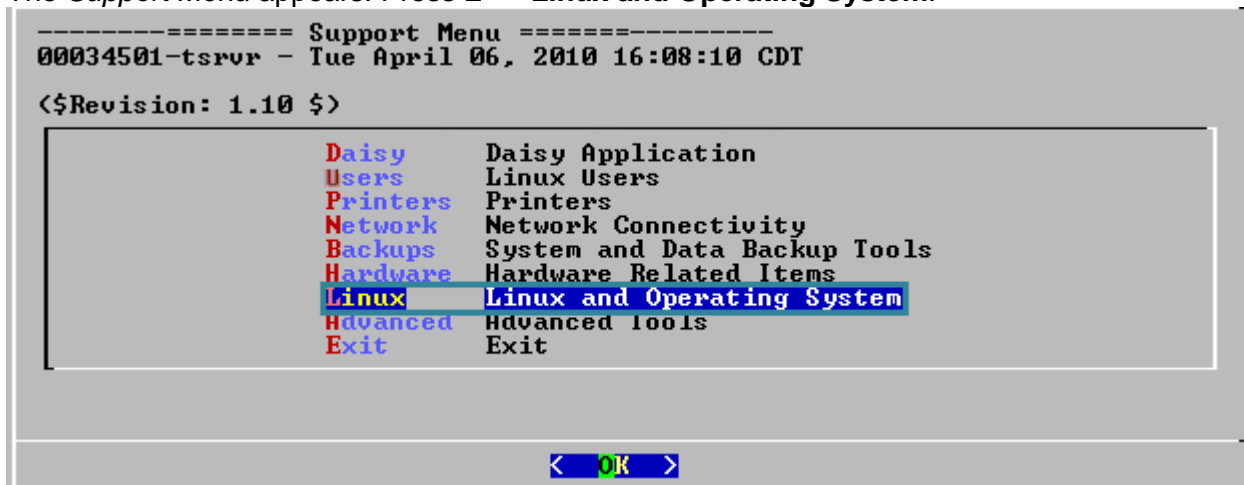
Important:

RedHat Enterprise Linux requires an annual subscription fee to obtain security updates. If your system issues an error, you will need to pay your RedHat entitlement fee. Until you have paid your fees, your system is not receiving security update and cannot be considered PCI compliant. If you are not receiving RedHat OS updates, contact RedHat for more information on purchasing annual entitlements. Also note that, once you stop paying for support for your Daisy system, your Daisy software will no longer receive security updates and your Operating system will no longer receive Daisy updates.

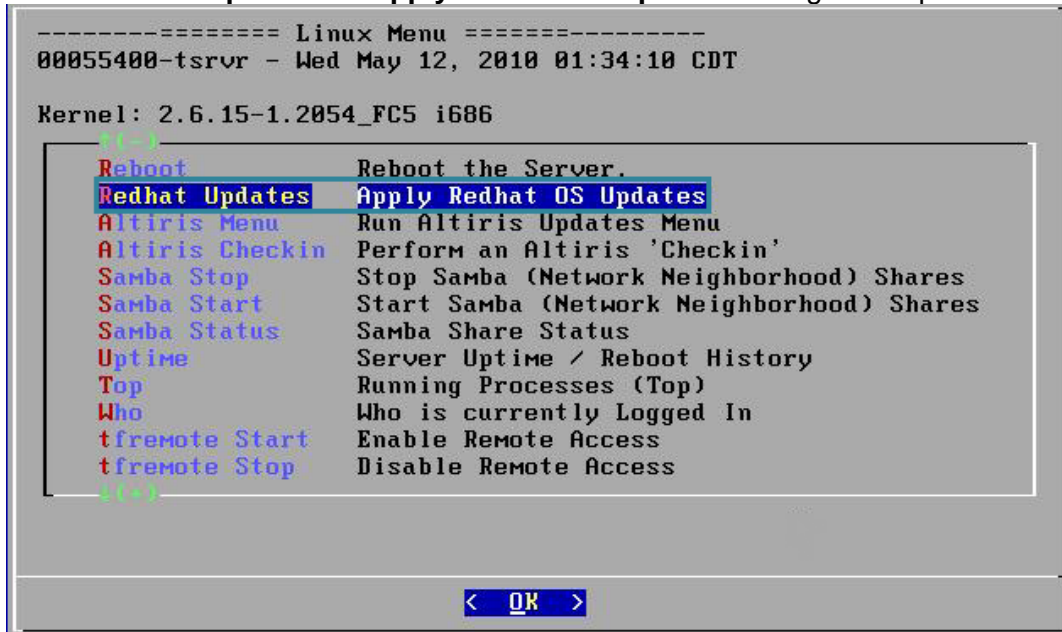
1. Press **Alt-F12**. At the **login as:** prompt, type your *Daisy Admin* login.

login as: █

2. The *Support Menu* appears. Press **L** **Linux and Operating System**.



3. Select RedHat Updates **Apply RedHat OS updates** to begin the update.



4. The *Download and Apply RedHat OS Updates Now?* Screen appears. Select **Yes**.



If your shop is running RedHat 7.2, FC3 or FC5, you should upgrade to the latest version of RedHat. If you are running the latest version of RedHat, it is important that they maintain an up-to-date entitlement with the RedHat updates portal.

How to Update your Daisy Software (Altiris)

PA-DSS 10.1

Your Daisy software is updated via Altiris. Altiris provides a secure mechanism for transferring Daisy updates to your system. It also provides you an easy to use interface for updating your Daisy builds. PCI DSS requires you update your Daisy system with any security patches within one month of their release. (PCI 6.1)

To update your Daisy system using the Altiris:

1. Ensure all users are logged out of the Daisy system.
2. Login to Daisy as an administrative user.
3. `sudo /d/daisy/bin/altiriscontrol.pl -updates`
4. Choose the Build you wish to install.

The Daisy Update will run to completion.

How to Remove Previous Builds of Daisy from Your System

PA-DSS 1.1
PA-DSS 1.1.4
PA-DSS 1.1.5

The Daisy software is released in a build. Each build contains all software needed to run Daisy. The process of updating from one build to another is automated. This update process may leave your old Daisy build, as well as a copy of your Daisy data, on-disk. This data is encrypted but, over time, it can be compromised. You need to ensure these old builds are securely removed from disk.

To remove previous builds of Daisy from your system:

IMPORTANT NOTE!

On most Daisy systems, “/d/daisy” contains your current Daisy system, removing this directory will render your Daisy application unusable and permanently destroy data. Follow the process exactly and enter information very carefully.

WARNING:

This process permanently removes files. It cannot be undone. Since these files are in close proximity to your “live” Daisy system, typing the wrong command could cause your “live” Daisy system to be permanently deleted. Please consult with Teleflora customer service prior to removing files, to ensure you are following proper, up-to-date procedures.

Process:

1. Login as root
2. `find /d/daisy-[0-9]* -type f -exec shred -uv {} \;`
3. `rm -rf /d/daisy-[0-9]*`
4. type exit to logout

How to Enable the Customer Service Access using eCare

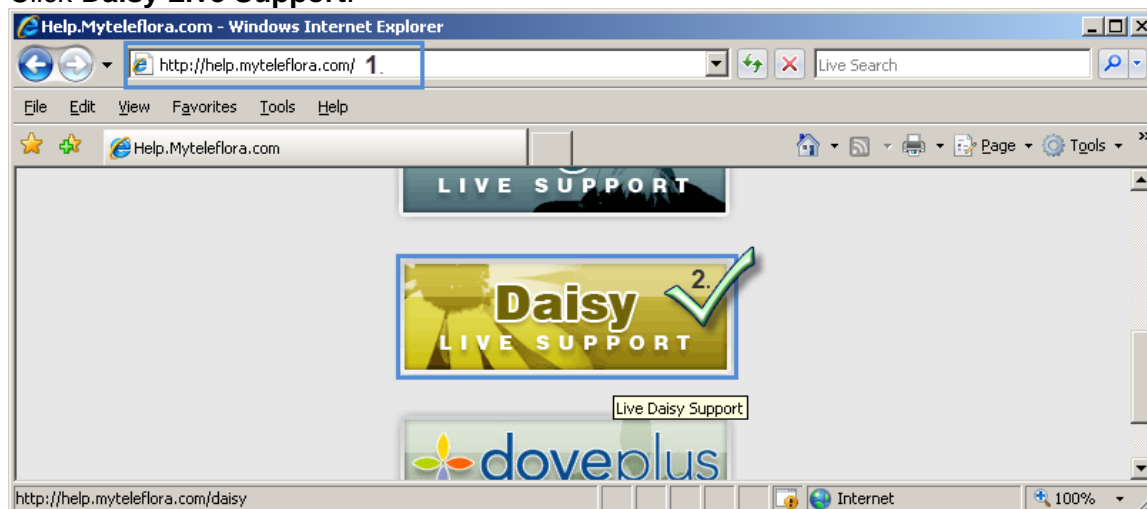
PA-DSS 10.1

PA-DSS 11.3.b

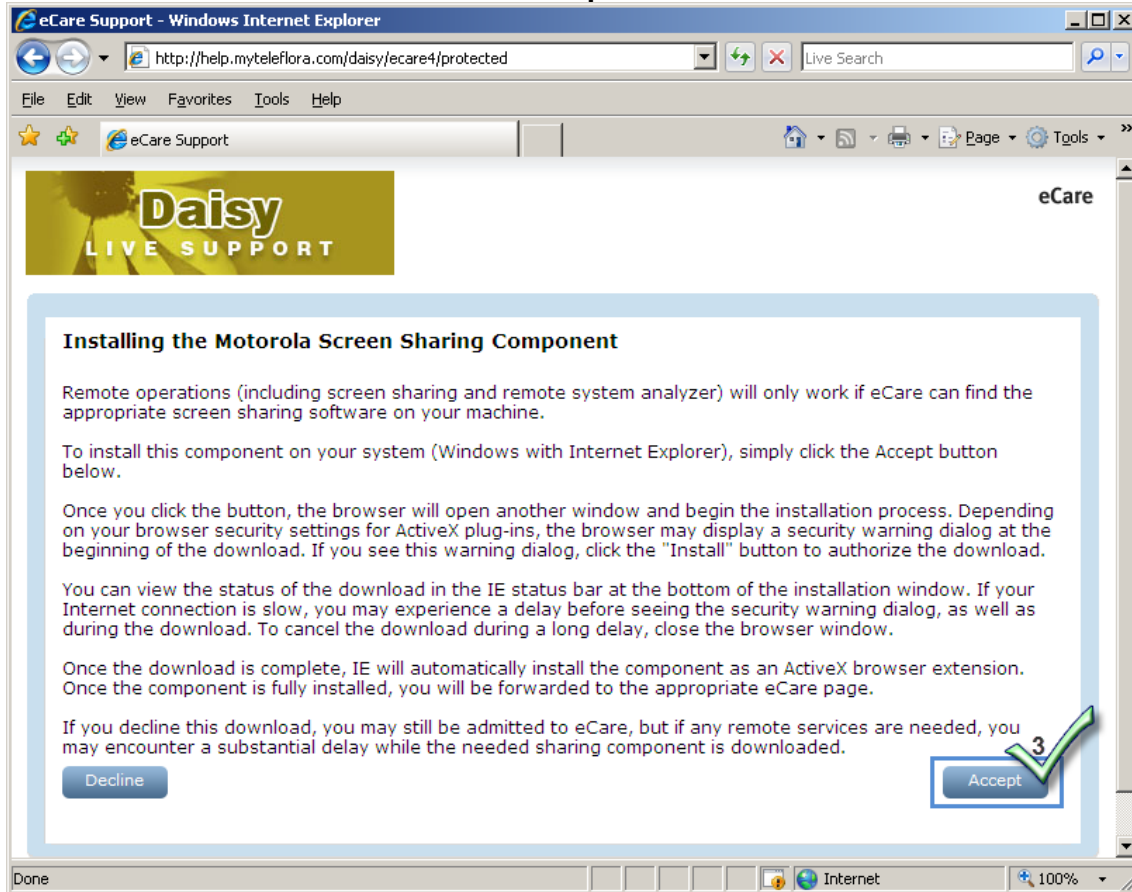
Daisy Customer Support can assist you only if eCare access is enabled. By default, eCare access is not available to support representatives.

To enable eCare:

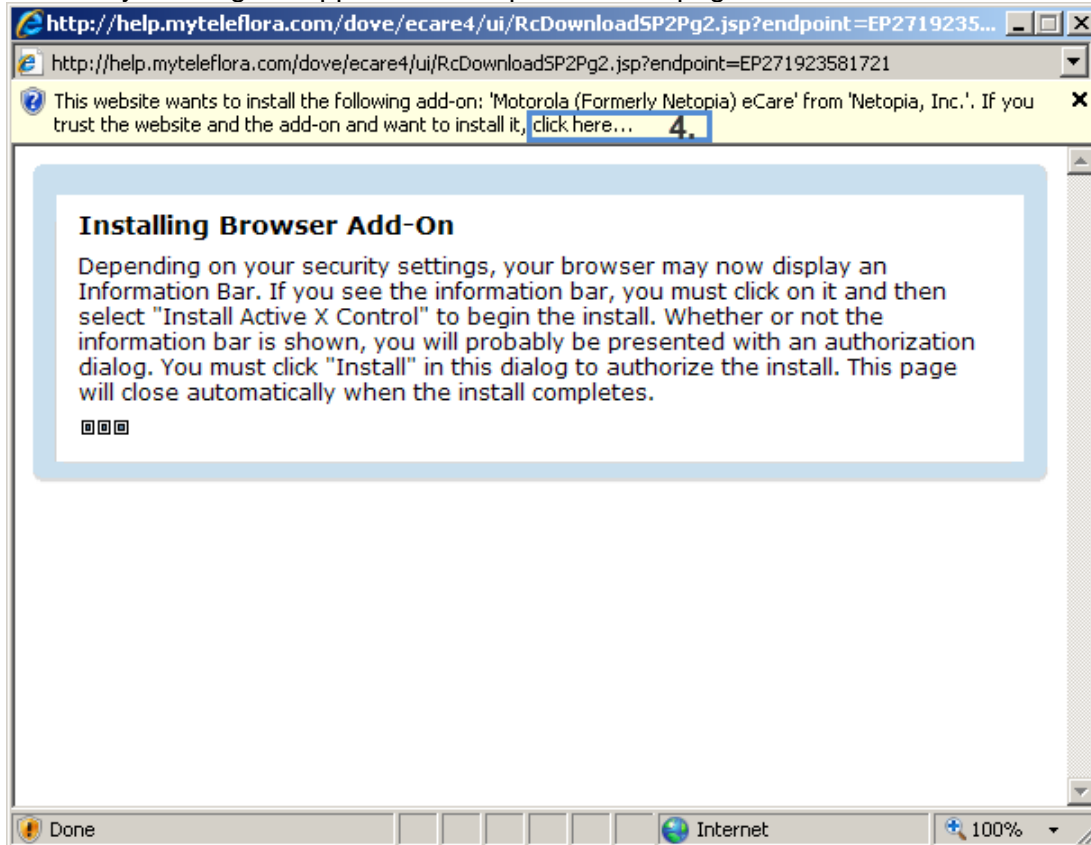
1. Open your browser. Type <http://help.myteleflora.com> in the IP Address bar.
2. Click **Daisy Live Support**.



3. Read the Terms and Conditions. Click **Accept**.

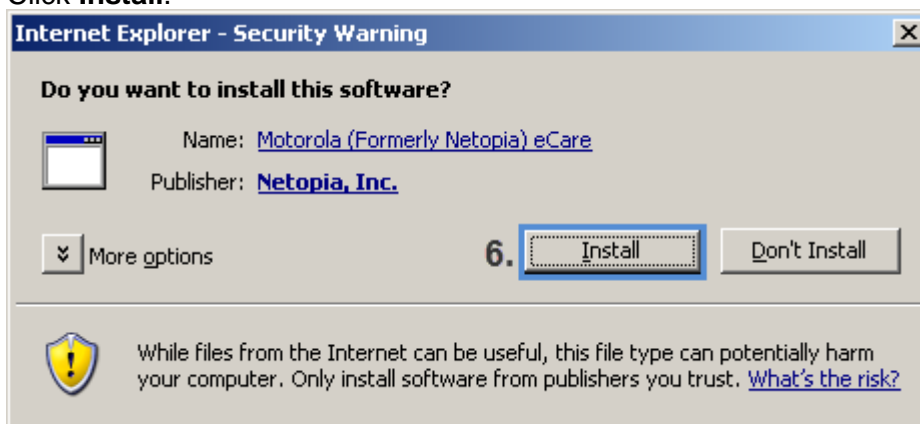


4. A security warning will appear at the top of the web page. Click **here**.

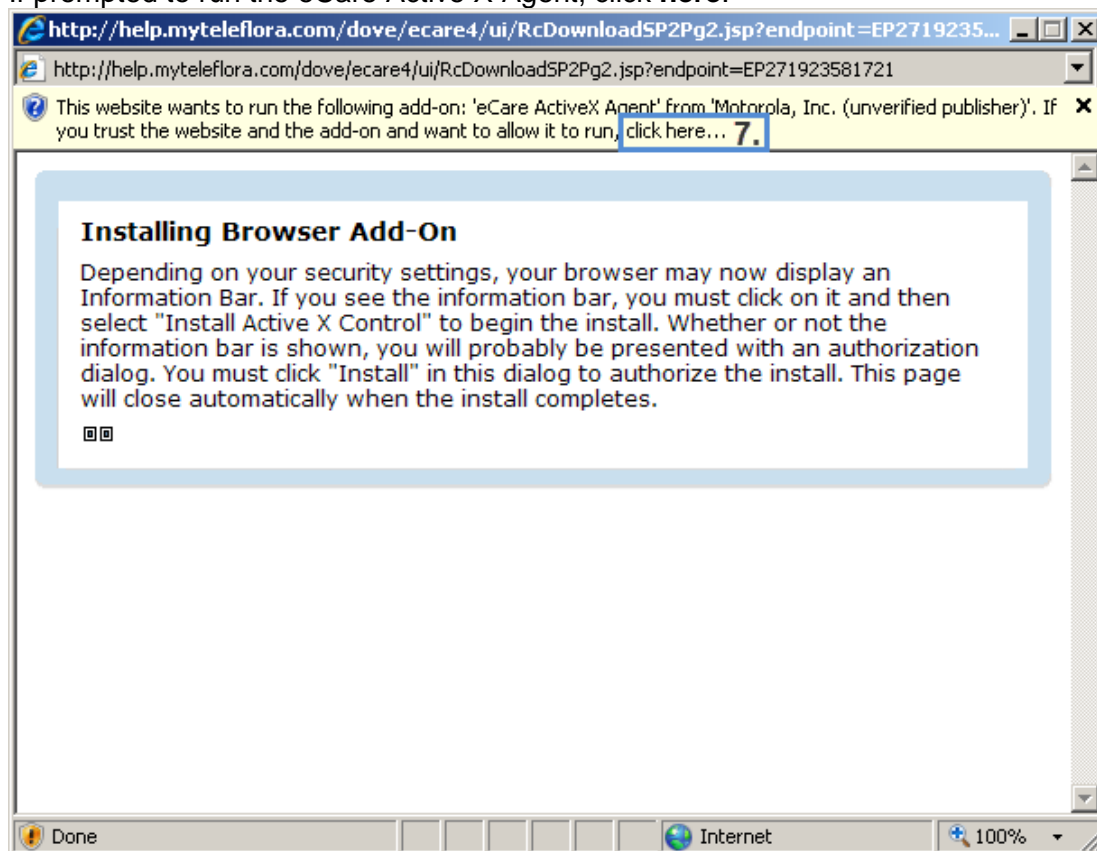


5. Click **Accept**. Make sure the add-on is from Motorola (formerly Netopia).

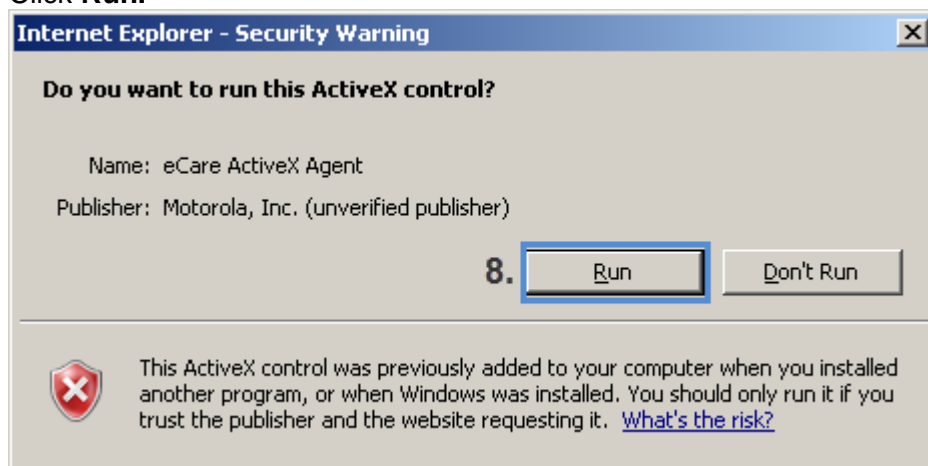
6. Click **Install**.



7. If prompted to run the eCare Active X Agent, click **here**.



8. Click **Run**.



9. Complete the on-screen form then click **Submit**.

eCare Support - Windows Internet Explorer

http://help.myteleflora.com/dove/ecare4/protected

Daisy
LIVE SUPPORT

Welcome To eCare Support

Please complete this form, giving your name, contact information, and a short description of your request.

Shop Code: 12345678

Contact Name: Jane Rose

Phone: 405 440 6000

Email: jane@flowers.com

How may we assist you? (optional)

Question about end of day process

Clear Form Submit

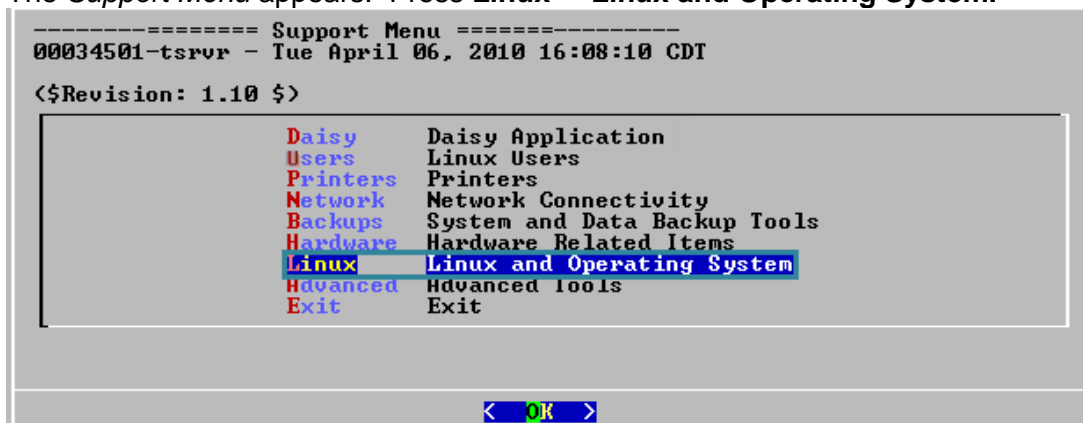
9.

If you can't use eCare, use the direct remote session available via the *Support Menu*.

1. Press **Alt-F12**. At the **login as:** prompt, type your Daisy login information.



2. The *Support Menu* appears. Press **Linux** **Linux and Operating System**.



3. Using the arrow keys select **tfremote Start** to allow remote access. Press **Enter**.

```
----- Linux Menu -----
00055400-tsrr - Wed May 12, 2010 01:34:10 CDT

Kernel: 2.6.15-1.2054_FC5 i686

Reboot          Reboot the Server.
Redhat Updates  Apply Redhat OS Updates
Altiris Menu    Run Altiris Updates Menu
Altiris Checkin Perform an Altiris 'Checkin'
Samba Stop      Stop Samba (Network Neighborhood) Shares
Samba Start     Start Samba (Network Neighborhood) Shares
Samba Status    Samba Share Status
Uptime          Server Uptime / Reboot History
Top             Running Processes (Top)
Who             Who is currently Logged In
tfremote Start  Enable Remote Access
tfremote Stop   Disable Remote Access

< OK >
```

4. Using the arrow keys select **tfremote Stop** to disallow remote access. Press **Enter**.

```
----- Linux Menu -----
00055400-tsrr - Wed May 12, 2010 01:34:10 CDT

Kernel: 2.6.15-1.2054_FC5 i686

Reboot          Reboot the Server.
Redhat Updates  Apply Redhat OS Updates
Altiris Menu    Run Altiris Updates Menu
Altiris Checkin Perform an Altiris 'Checkin'
Samba Stop      Stop Samba (Network Neighborhood) Shares
Samba Start     Start Samba (Network Neighborhood) Shares
Samba Status    Samba Share Status
Uptime          Server Uptime / Reboot History
Top             Running Processes (Top)
Who             Who is currently Logged In
tfremote Start  Enable Remote Access
tfremote Stop   Disable Remote Access

< OK >
```

How to Enable/Disable the Teleflora Customer Service User Account

PA-DSS 10.1

PA-DSS 11.3.b

Warning:

If you disable Daisy customer service access, Daisy customer service will not be able to troubleshoot or provide assistance for any problems you have with your Daisy server until you enable the account again.

Disabling Daisy Customer Service User Account:

1. Login as root
2. At the root prompt, type **passwd -l tfsupport**. Press **Enter**.

Enabling Daisy Customer Service User Account:

1. Login as root
2. At the root prompt, type **passwd -u tfsupport** Press **Enter**.

Identifying a login history for Customer Service:

1. Login as root
2. At the root prompt, type **last tfsupport**.

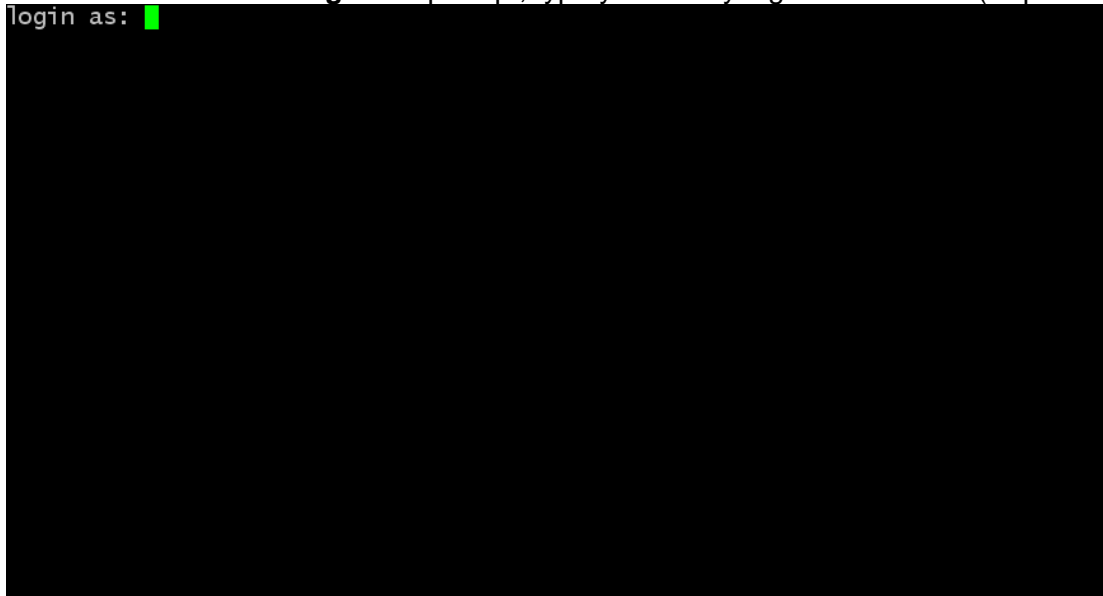
How to Add a Daisy User Account

PA-DSS 3.1

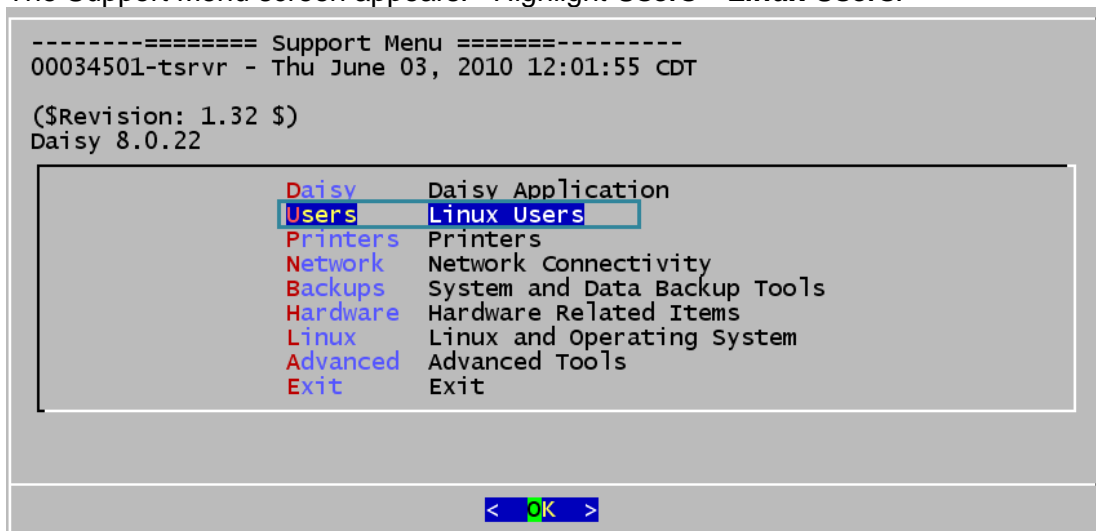
Your Daisy application uses discretionary permissions which only allow members of the rti UNIX group to access Daisy-related files. The *rtiuser.pl* script ensures that users are members of the appropriate UNIX groups. The script also ensures that Daisy users are taken directly into the Daisy application upon login.

To add a Daisy Admin user account:

1. Press **Alt-F12**. At the **login as:** prompt, type your Daisy login information. (requires Admin login)



2. The Support Menu screen appears. Highlight **Users** **Linux Users**.



3. Highlight **Add User**, then press **Enter**

```
-----===== User Menu -----  
00034501-tsrvr - Thu June 03, 2010 12:03:24 CDT
```

Add User	Add User
Enable Admin	Set User as Administrator
Disable Admin	Remove Administrative Privileges
Remove	Remove User
Info	Get User Info
List	List all users.
ResetPW	Reset Password
Password Generator	Suggest New Passwords
Login	Login as a different user.
Close	Close This Menu

< OK >

4. Type your *Username*, then press **Enter**.

```
Choose a Username to Add
```

DaisyUser █

< OK >

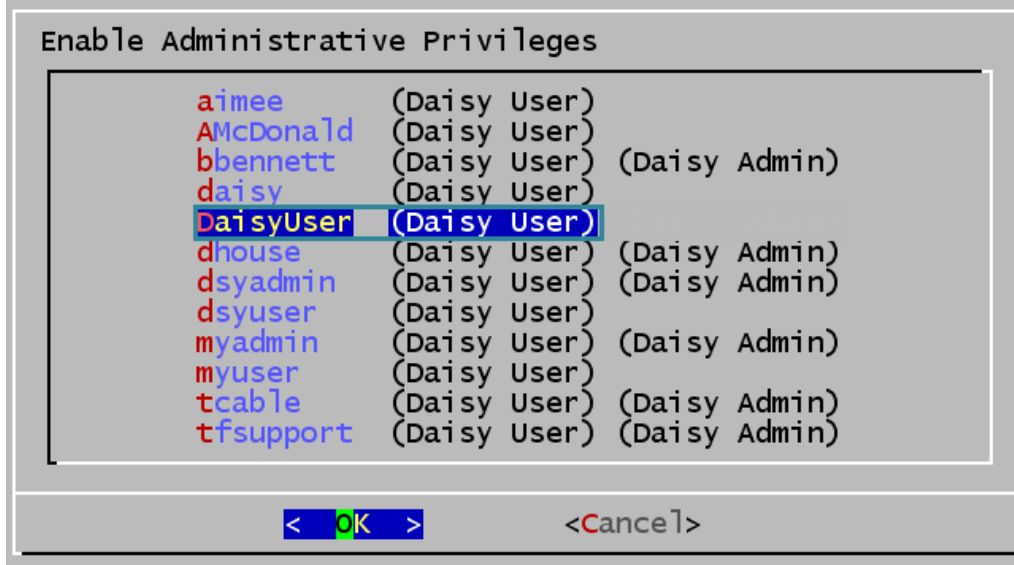
5. Select **Enable Admin**.

```
-----===== User Menu -----  
00034501-tsrvr - Thu June 03, 2010 12:04:43 CDT
```

Add User	Add User
Enable Admin	Set User as Administrator
Disable Admin	Remove Administrative Privileges
Remove	Remove User
Info	Get User Info
List	List all users.
ResetPW	Reset Password
Password Generator	Suggest New Passwords
Login	Login as a different user.
Close	Close This Menu

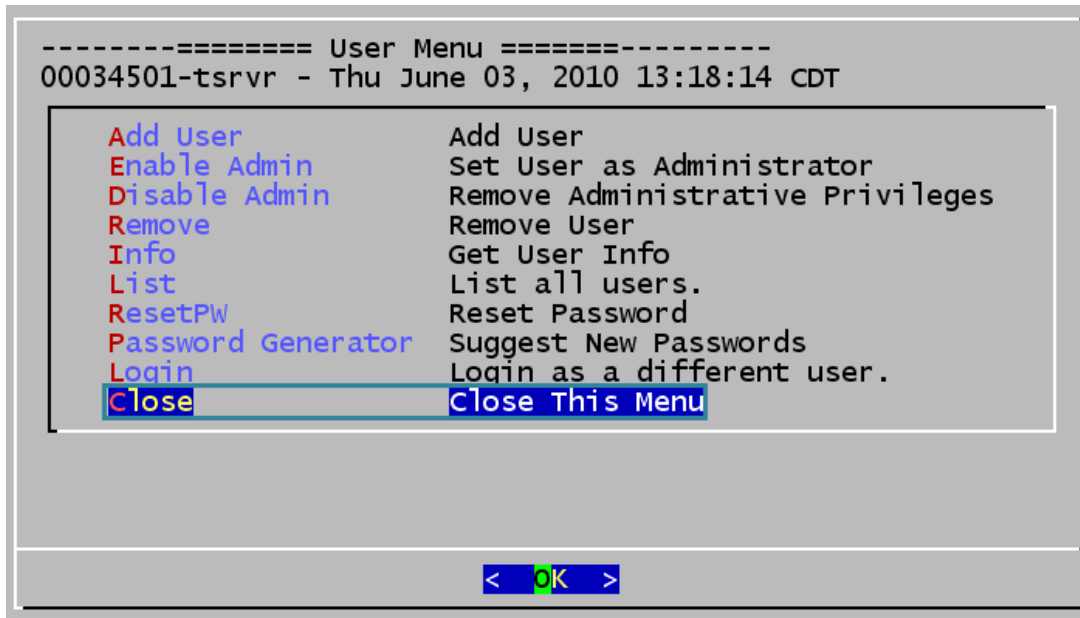
< OK >

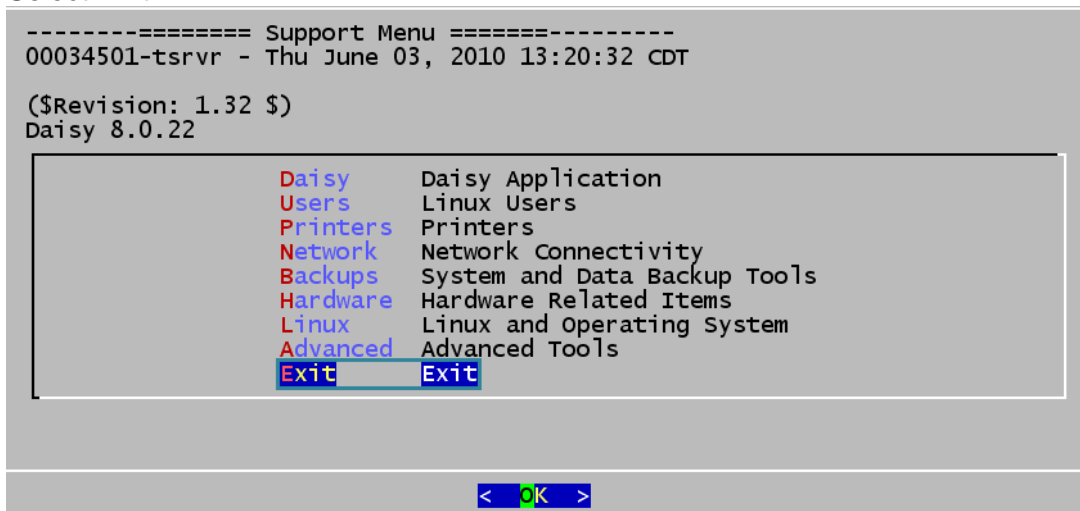
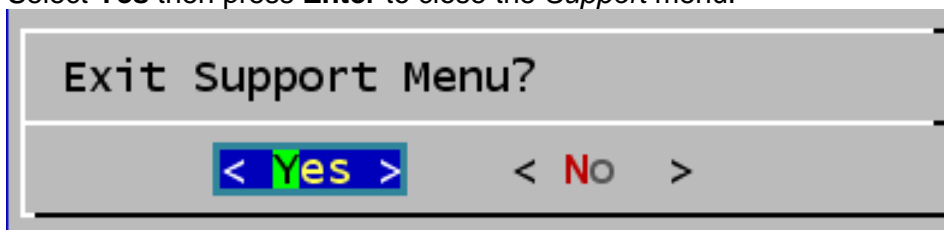
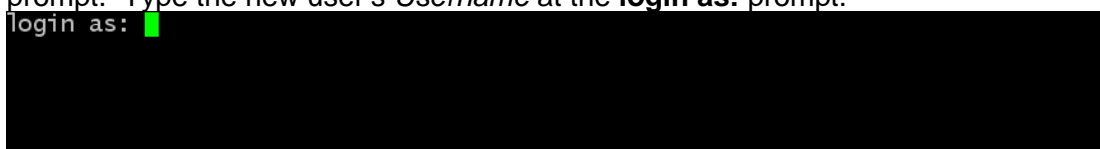
6. Select the username of the employee that will have admin privileges.



7. Assign a password. Note: The one time temporary password will allow a dictionary word.

8. Select **Close**.



9. Select **Exit**.10. Select **Yes** then press **Enter** to close the *Support* menu.11. The newly created user will need to reset the temporary password. Return to the **Alt-F12 login as:** prompt. Type the new user's *Username* at the **login as:** prompt.

12. You will see a large amount of text on the screen. This information reminds you of the importance of changing your password. To reset your password, type your temporary one-time password at the **(current) UNIX password** prompt.

```
of monitoring individuals improperly using this system, or in the
course of system maintenance, the activities of authorized users
may also be monitored by properly authorized personnel. Anyone using
this system expressly consents to such monitoring and is advised that
if such monitoring reveals possible evidence of criminal activity,
system personnel may provide the evidence of such monitoring to law
enforcement officials.
tfssupport@192.168.1.21's password:
You are required to change your password immediately (root enforced)
This system is for the use of authorized users only. Individuals using
this computer system without authority, or in excess of their authority,
are subject to having all of their activities on this system monitored
and recorded by properly authorized system personnel. In the course
of monitoring individuals improperly using this system, or in the
course of system maintenance, the activities of authorized users
may also be monitored by properly authorized personnel. Anyone using
this system expressly consents to such monitoring and is advised that
if such monitoring reveals possible evidence of criminal activity,
system personnel may provide the evidence of such monitoring to law
enforcement officials.
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user tfssupport.
Changing password for tfssupport
(current) UNIX password: [REDACTED]
```

13. Now you need to create a new complex password. Complex passwords must be at least 7 characters in length and include at least one of ALL of the following:

- Uppercase letter
- Lowercase letter
- Number
- Special Characters (@, #,). Special characters can include a space.

Some examples of complex passwords:

J58ate83

I like D3isy.

Cr@bsliveb3ach

The br@wn fox runs f3st!

Type the new password at the **New UNIX password** prompt.

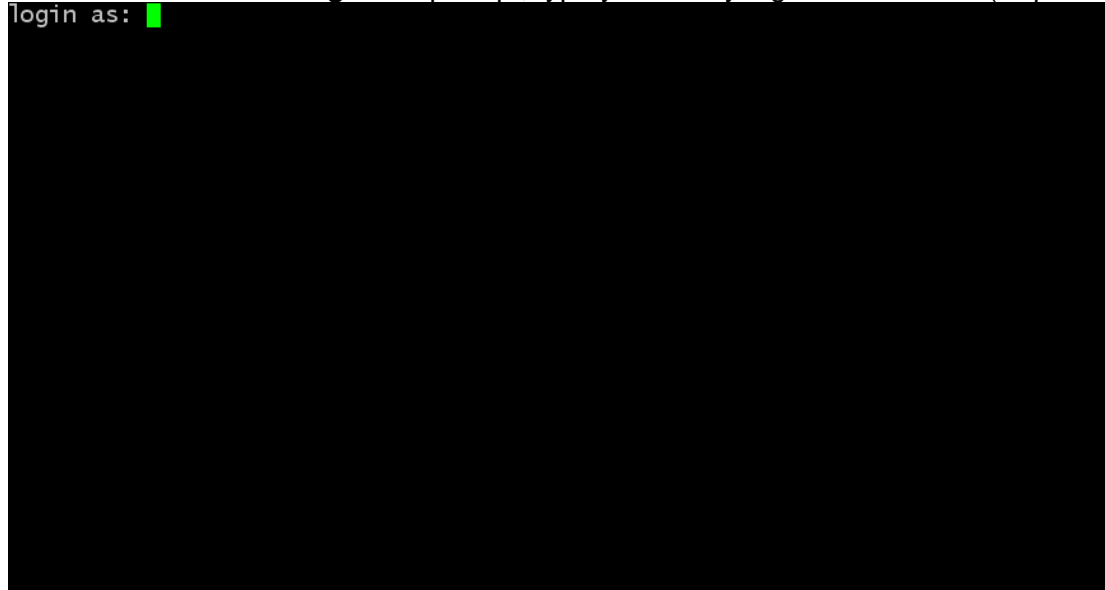
```
may also be monitored by properly authorized personnel. Anyone using
this system expressly consents to such monitoring and is advised that
if such monitoring reveals possible evidence of criminal activity,
system personnel may provide the evidence of such monitoring to law
enforcement officials.
tfssupport@192.168.1.21's password:
You are required to change your password immediately (root enforced)
This system is for the use of authorized users only. Individuals using
this computer system without authority, or in excess of their authority,
are subject to having all of their activities on this system monitored
and recorded by properly authorized system personnel. In the course
of monitoring individuals improperly using this system, or in the
course of system maintenance, the activities of authorized users
may also be monitored by properly authorized personnel. Anyone using
this system expressly consents to such monitoring and is advised that
if such monitoring reveals possible evidence of criminal activity,
system personnel may provide the evidence of such monitoring to law
enforcement officials.
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user tfssupport.
Changing password for tfssupport
(current) UNIX password:
New UNIX password: 
```

14. Retype the new password at the **Retype new UNIX password** prompt.

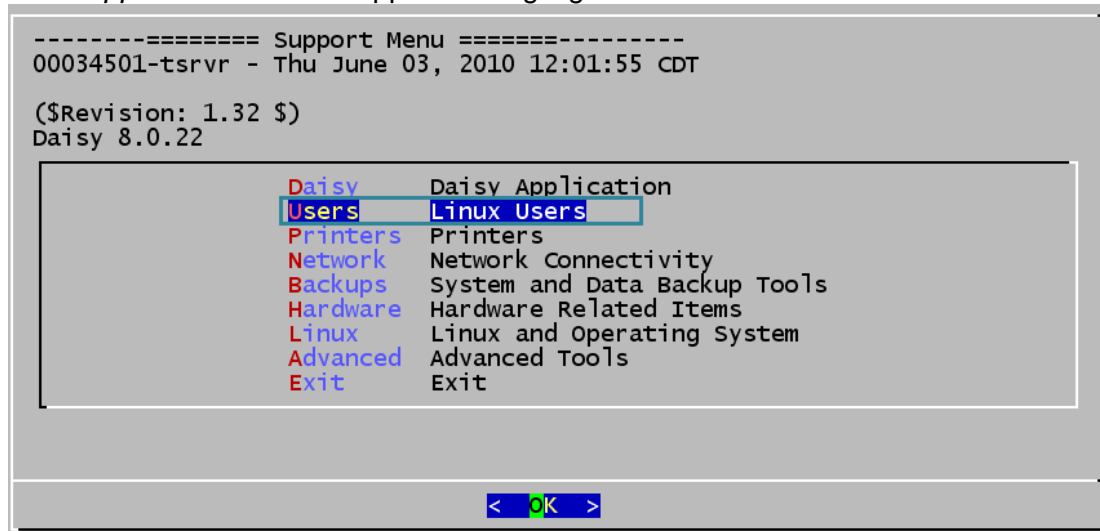
```
may also be monitored by properly authorized personnel. Anyone using
this system expressly consents to such monitoring and is advised that
if such monitoring reveals possible evidence of criminal activity,
system personnel may provide the evidence of such monitoring to law
enforcement officials.
tfssupport@192.168.1.21's password:
You are required to change your password immediately (root enforced)
This system is for the use of authorized users only. Individuals using
this computer system without authority, or in excess of their authority,
are subject to having all of their activities on this system monitored
and recorded by properly authorized system personnel. In the course
of monitoring individuals improperly using this system, or in the
course of system maintenance, the activities of authorized users
may also be monitored by properly authorized personnel. Anyone using
this system expressly consents to such monitoring and is advised that
if such monitoring reveals possible evidence of criminal activity,
system personnel may provide the evidence of such monitoring to law
enforcement officials.
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user tfssupport.
Changing password for tfssupport
(current) UNIX password:
New UNIX password:
Retype new UNIX password: █
```

To add a Daisy non-admin user account:

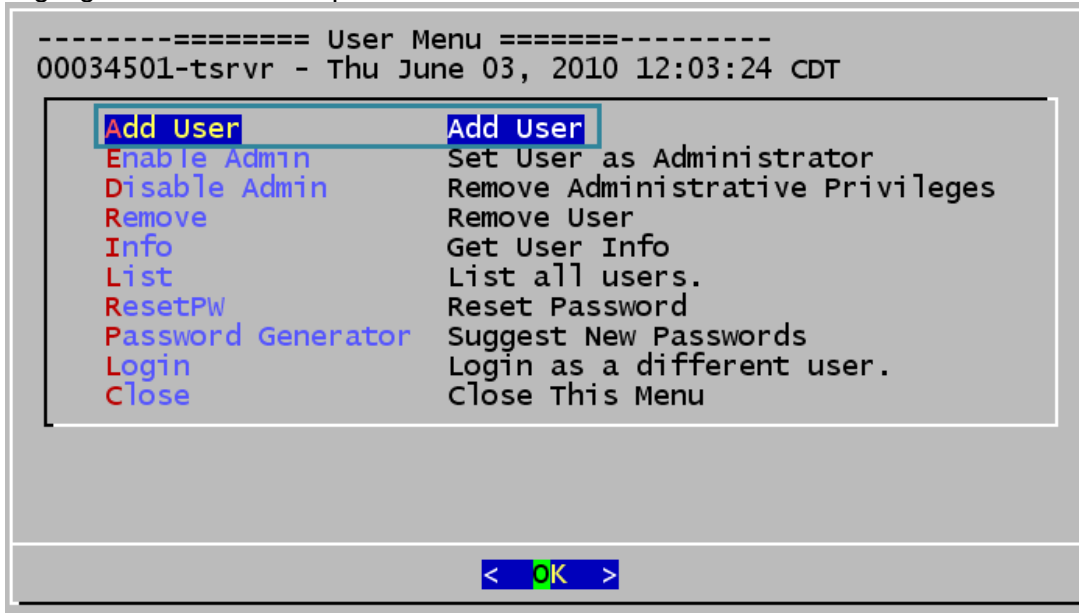
1. Press **Alt-F12**. At the **login as:** prompt, type your Daisy login information. (requires Admin login)



2. The *Support Menu* screen appears. Highlight **Users Linux Users**.



3. Highlight **Add User** then press **Enter**.

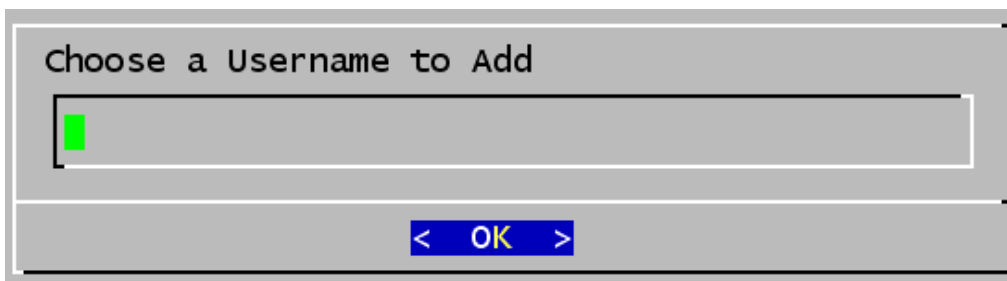


4. The **Choose a Username to Add** screen will appear. The *Username* is the same thing as a *Login*. You will now need to create login and password to allow your employees to access your Daisy system. The Login can be the employee name, first initial and last name. Some examples of Logins:

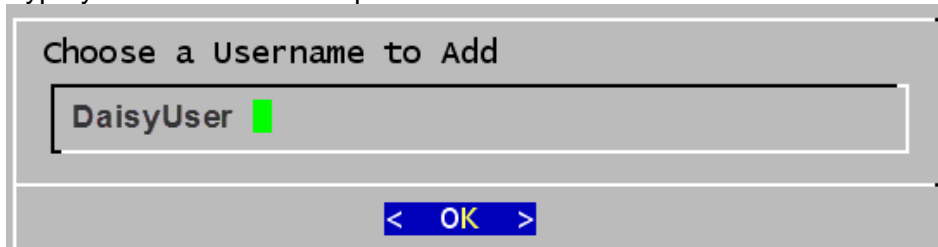
ksamson

TonyE

katherine



5. Type your Username then press **Enter**.

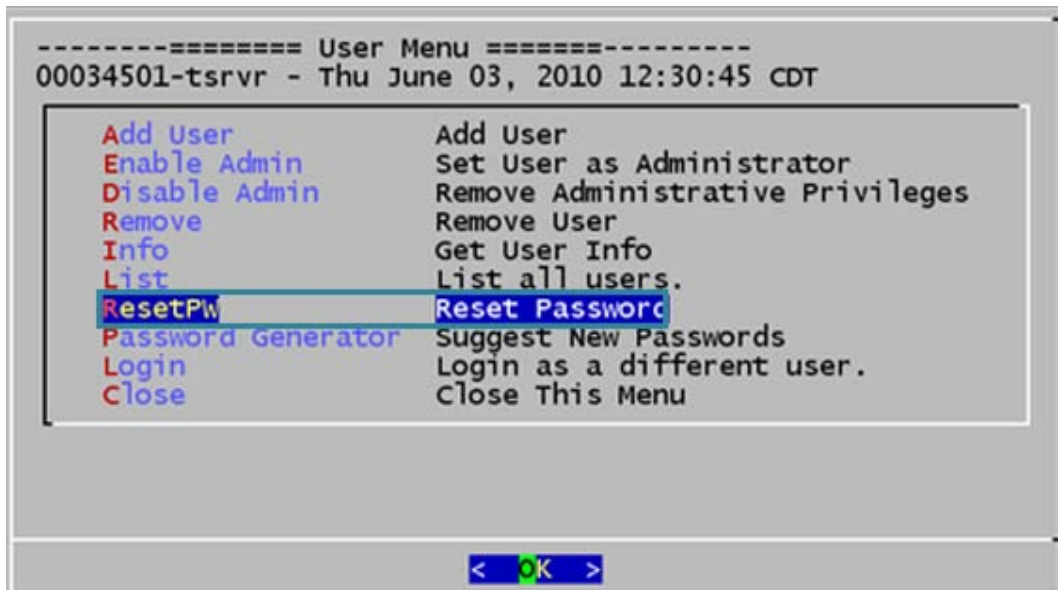


Choose a Username to Add

DaisyUser █

< OK >

6. Select **ResetPW**.

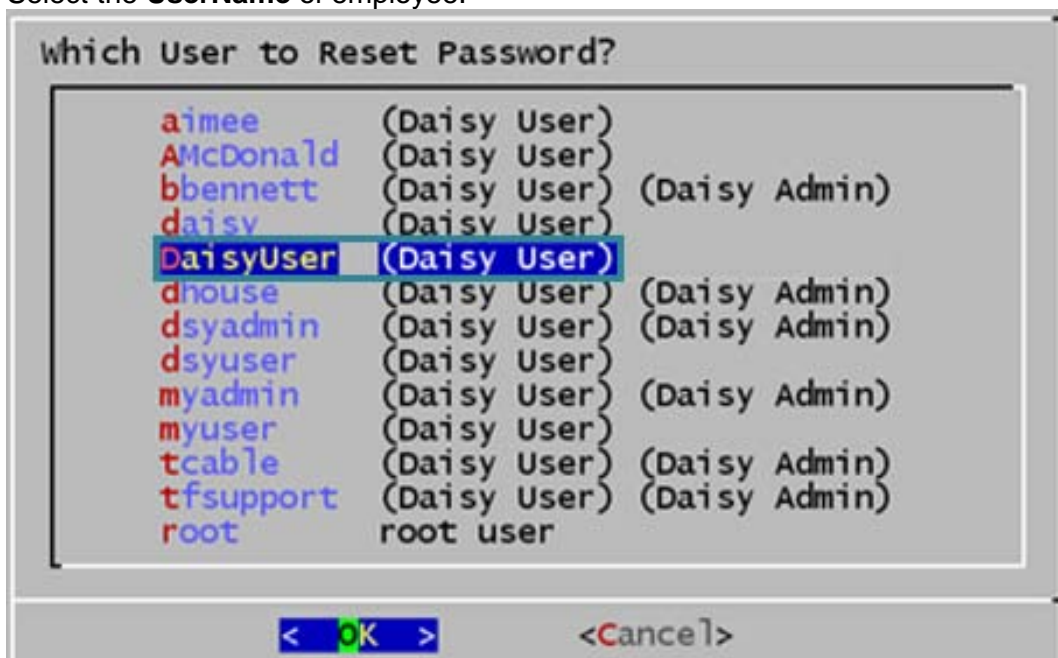


----- User Menu -----
00034501-tnr - Thu June 03, 2010 12:30:45 CDT

Add User	Add User
Enable Admin	Set User as Administrator
Disable Admin	Remove Administrative Privileges
Remove	Remove User
Info	Get User Info
List	List all users.
ResetPW	Reset Password
Password Generator	Suggest New Passwords
Login	Login as a different user.
Close	Close This Menu

< OK >

7. Select the **UserName** of employee.

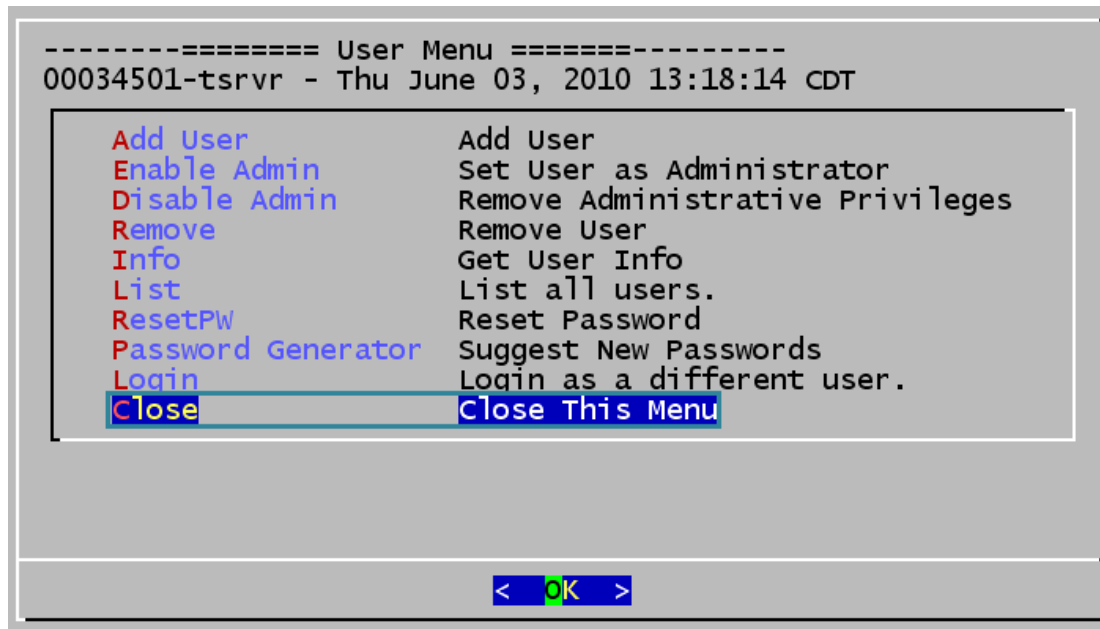


which User to Reset Password?

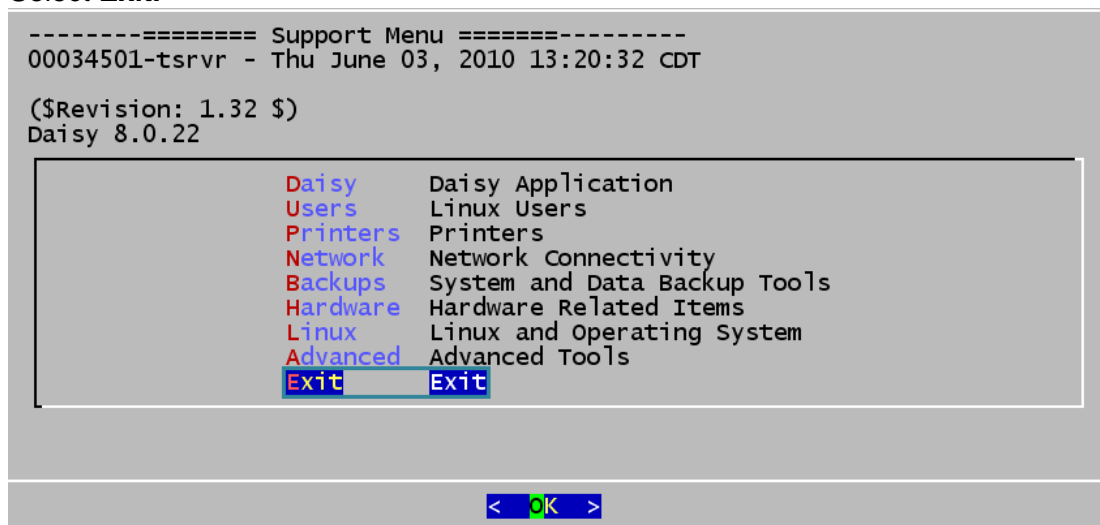
aimee	(Daisy User)	
AMcDonald	(Daisy User)	
bbennett	(Daisy User)	(Daisy Admin)
daisy	(Daisy User)	
DaisyUser	(Daisy User)	
dhouse	(Daisy User)	(Daisy Admin)
dsyadmin	(Daisy User)	(Daisy Admin)
dsyuser	(Daisy User)	
myadmin	(Daisy User)	(Daisy Admin)
myuser	(Daisy User)	
tcable	(Daisy User)	(Daisy Admin)
tfsupport	(Daisy User)	(Daisy Admin)
root	root user	

< OK > <Cancel>

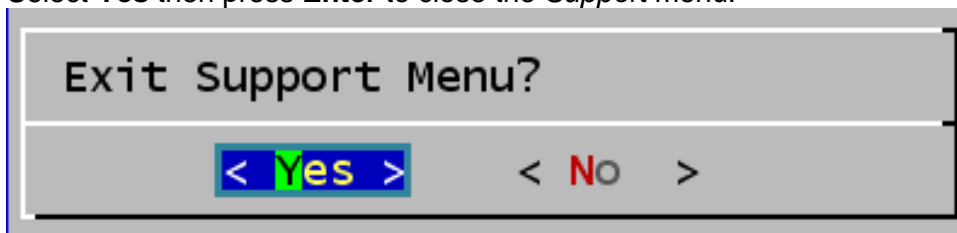
8. Assign a password. Note: The one time temporary password will allow a dictionary word.
9. Select **Close**.



10. Select **Exit**.



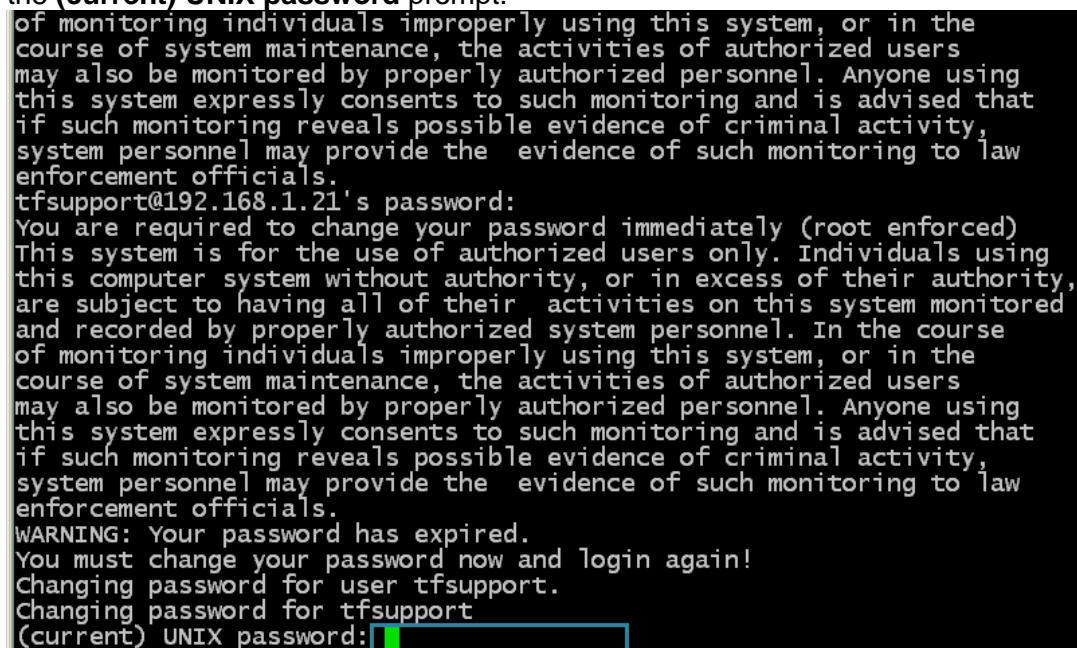
11. Select **Yes** then press **Enter** to close the *Support* menu.



12. The newly created user will need to reset the temporary password. Return to the *Alt-F12 login* prompt. Type the new users Username at the **login as:** prompt.



13. You will see a large amount of text on the screen. This information reminds you of the importance of changing your password. To reset your password, type your temporary one-time password at the **(current) UNIX password** prompt.



14. Now you need to create a new complex password. Complex passwords must be at least 7 characters in length and include at least one of ALL of the following:

- Uppercase letter
- Lowercase letter
- Number
- Special Characters (@, #,). Special characters can include a space.

Some examples of complex passwords:

J58ate83

I like D3isy.

Cr@bsliveb3ach

The br@wn fox runs f3st!

Type the new password at the **New UNIX password** prompt.

```
may also be monitored by properly authorized personnel. Anyone using
this system expressly consents to such monitoring and is advised that
if such monitoring reveals possible evidence of criminal activity,
system personnel may provide the evidence of such monitoring to law
enforcement officials.
tfsupport@192.168.1.21's password:
You are required to change your password immediately (root enforced)
This system is for the use of authorized users only. Individuals using
this computer system without authority, or in excess of their authority,
are subject to having all of their activities on this system monitored
and recorded by properly authorized system personnel. In the course
of monitoring individuals improperly using this system, or in the
course of system maintenance, the activities of authorized users
may also be monitored by properly authorized personnel. Anyone using
this system expressly consents to such monitoring and is advised that
if such monitoring reveals possible evidence of criminal activity,
system personnel may provide the evidence of such monitoring to law
enforcement officials.
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user tfsupport.
Changing password for tfsupport
(current) UNIX password:
New UNIX password: 
```

15. Retype the new password at the **Retype new UNIX password** prompt.

```
may also be monitored by properly authorized personnel. Anyone using
this system expressly consents to such monitoring and is advised that
if such monitoring reveals possible evidence of criminal activity,
system personnel may provide the evidence of such monitoring to law
enforcement officials.
tfssupport@192.168.1.21's password:
You are required to change your password immediately (root enforced)
This system is for the use of authorized users only. Individuals using
this computer system without authority, or in excess of their authority,
are subject to having all of their activities on this system monitored
and recorded by properly authorized system personnel. In the course
of monitoring individuals improperly using this system, or in the
course of system maintenance, the activities of authorized users
may also be monitored by properly authorized personnel. Anyone using
this system expressly consents to such monitoring and is advised that
if such monitoring reveals possible evidence of criminal activity,
system personnel may provide the evidence of such monitoring to law
enforcement officials.
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user tfssupport.
Changing password for tfssupport
(current) UNIX password:
New UNIX password:
Retype new UNIX password: 
```

After logging into the Daisy system, an Admin user will see the *Support Menu* displayed on the screen. The non-Admin user will see the *POS Menu* at login.

How to Remove a Daisy User Account

PA-DSS 3.1

PCI 8.5.4

PCI 8.5.5

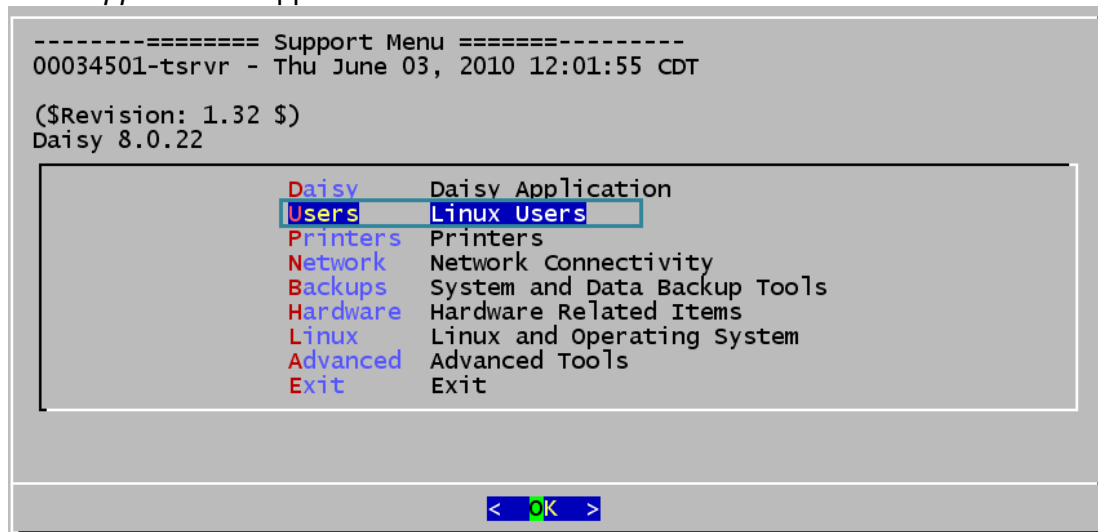
You must remove an employee user account immediately upon termination of an employee or after 90 days of inactivity of any employee.

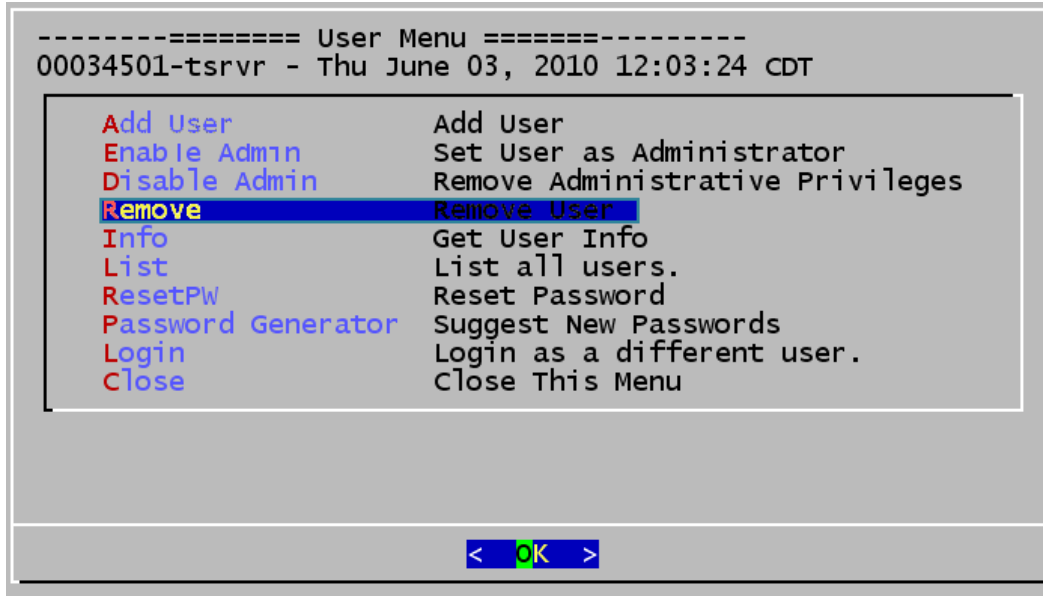
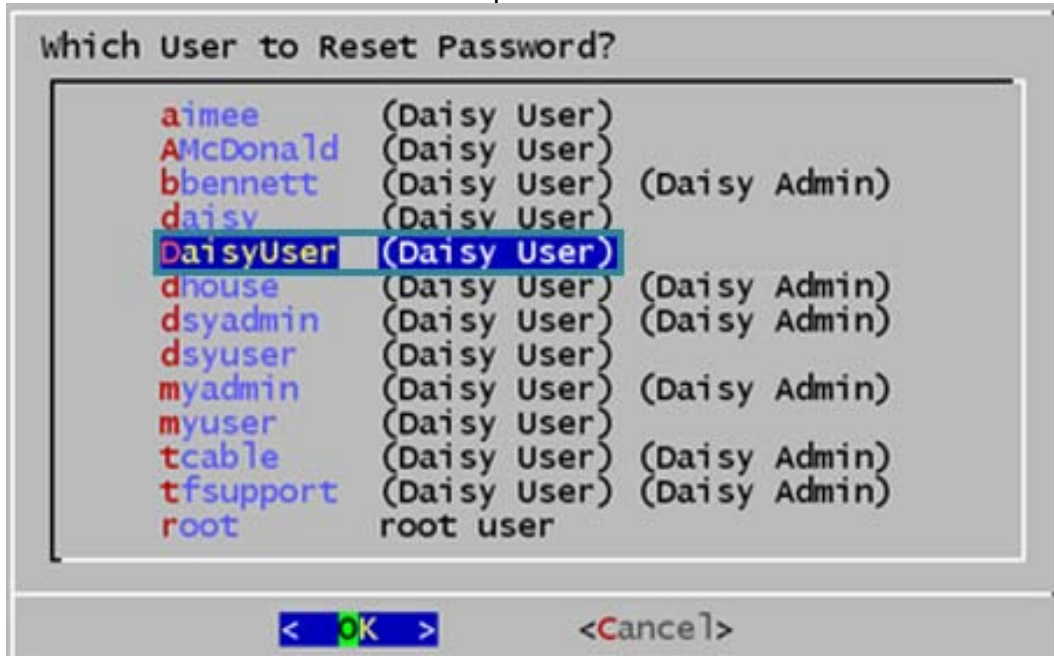
To remove a Daisy User Account:

1. Press **Alt-F12**. At the **login as:** prompt, log in as a *Daisy Admin* user.



2. The *Support Menu* appears. Select **Users** for Linux Users.



3. Select Remove **User**.4. Select a user name from the list then press **enter**.5. Select **Yes** you want to remove the user then press **ENTER**.

How to Securely “Wipe” a Hard Drive

PA-DSS 1.1.4

PA-DSS 2.7

You will need to securely wipe your hard drive if:

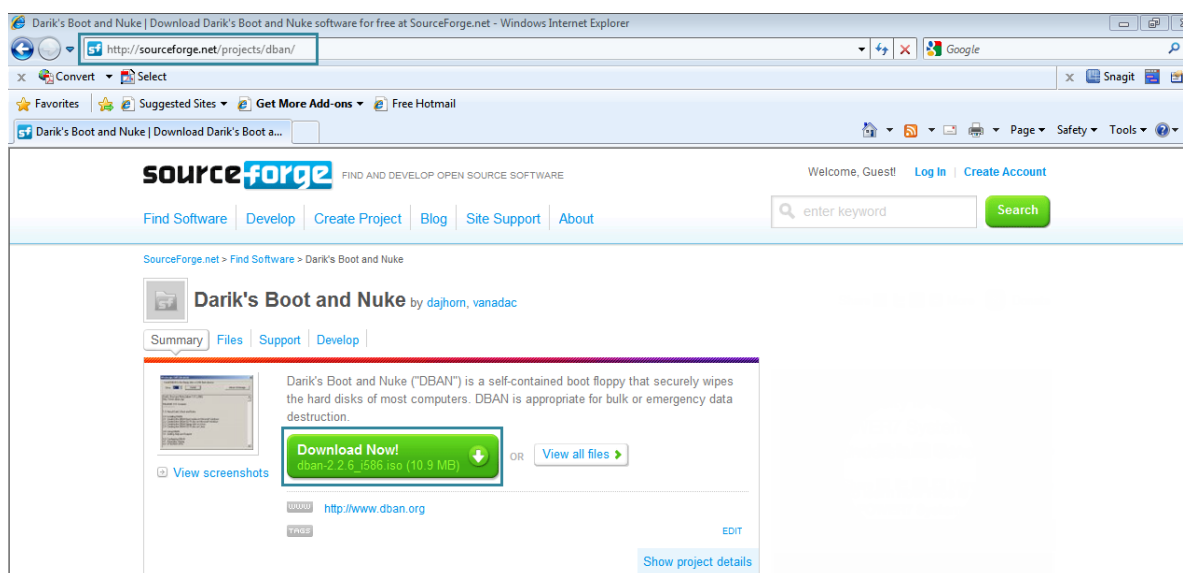
- You are retiring a computer which contained or processed sensitive cardholder data.
- You are installing the Daisy POS on a computer which was used for other purposes.
- Your Daisy POS has experienced a security compromise.

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.

Process:

1. Download the “DBAN” utility. Go to <http://sourceforge.net/projects/dban/>



2. Read the DBAN Documentation. Click **Documentation**.
The DBAN Documentation screen appears. Begin reading the Quick Start section, then FAQ.
Make sure you are speaking with Daisy support when attempting to wipe a hard drive.

Darik's Boot And Nuke

[Download](#) | [Help](#) | [News](#) | [Contact](#) | [About DBAN](#)

[SourceForge Project Page](#) | [Development Status](#) | [Documentation](#)

[Home](#)

DBAN Documentation

- [Quick Start](#)
- [Frequently Asked Questions \(FAQ\)](#)
- [Screen Shots](#)
- [Errata](#)
- [Defects](#)

Boot And Nuke is a registered trademark of GEEP EDS LLC.

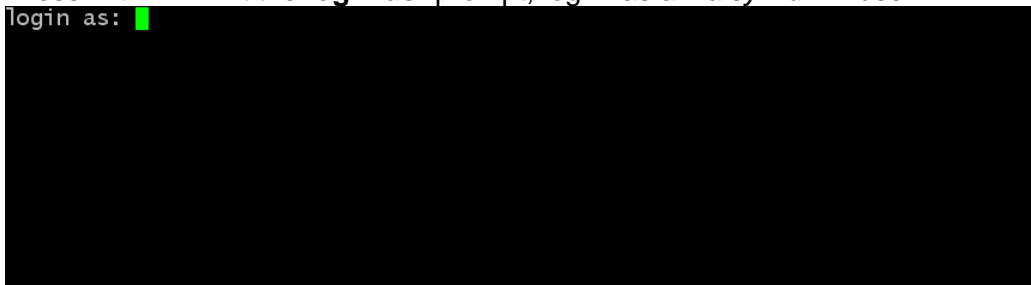
All other marks are the property of their owners and used without permission.

How to Change/Rotate your Daisy Data Encryption Key

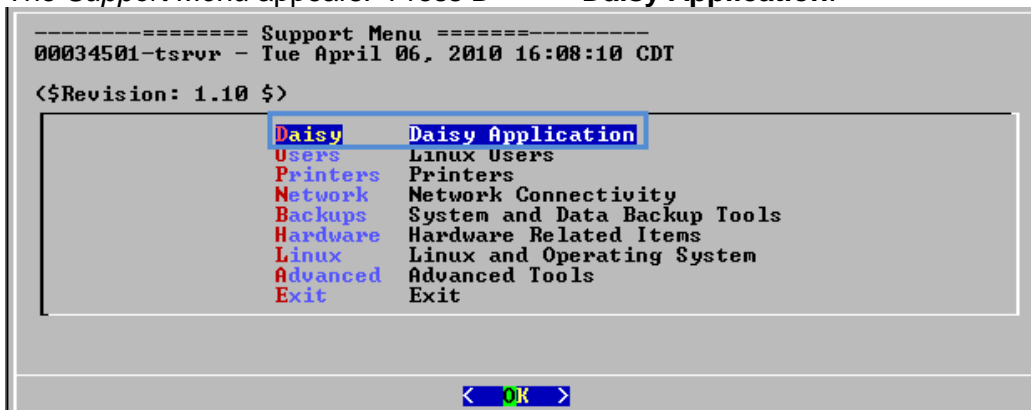
PA-DSS 1.5
PCI DSS 3.6
PCI DSS 8.5

Your Daisy system is capable of retaining cardholder information. This data is stored to disk, encrypted with an encryption key. PCI DSS Section 3.6 mandates changing your data encryption key at least once every year.

1. Press **Alt-F12**. At the **login as:** prompt, log in as a *Daisy Admin* user.



2. The *Support Menu* appears. Press **D** **Daisy Application.**



3. Select **Rotate Keys**
4. Type **Rotate** at the prompt (or type **Cancel** to cancel the screen and return to the menu)
5. After successfully rotating the keys press enter to return to the menu

How to Permanently Remove Credit Card Information

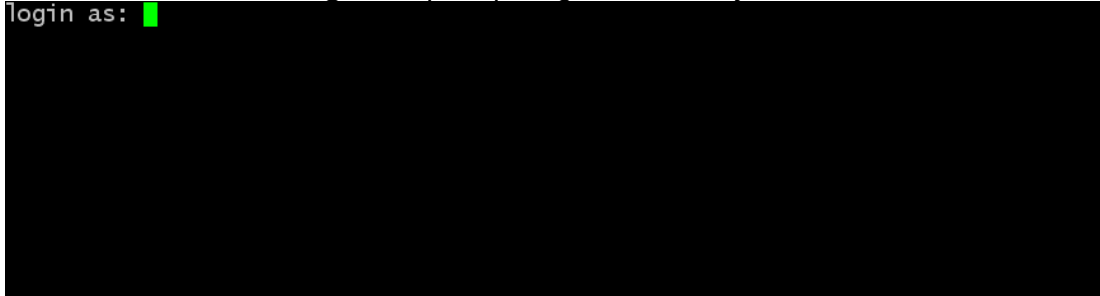
PA-DSS 2.1
PCI DSS 3.1

Your Daisy system can purge cardholder information based on a specified time frame (retention period). The process will securely delete all inactive credit cards within the specified range. According to PCI DSS Requirement 3.1, merchants need to create a data retention business policy. Teleflora provides a template to help merchants develop this policy in the POS Template Policies document. Cardholder data exceeding your defined retention period needs to be purged to be compliant with PCI DSS.

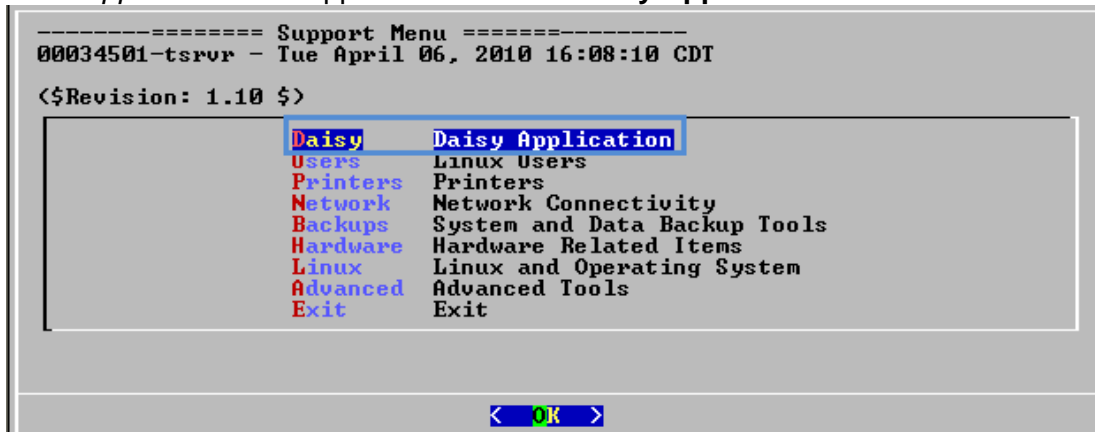
To purge credit cards:

1. Press **Alt-F12**. At the **login as:** prompt, log in as a *Daisy Admin* user

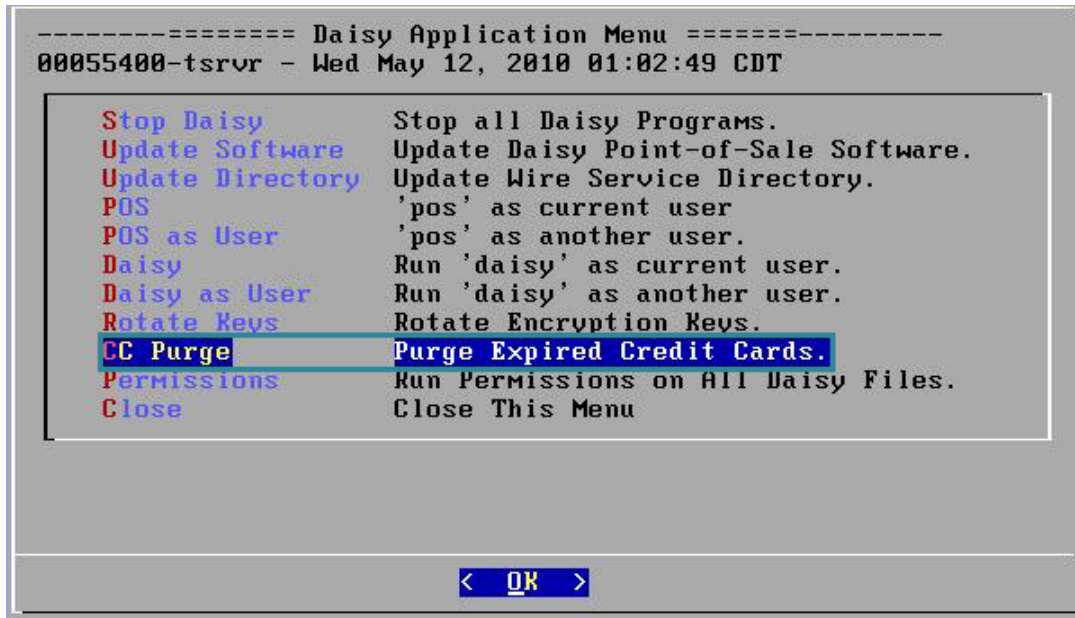
login as: █



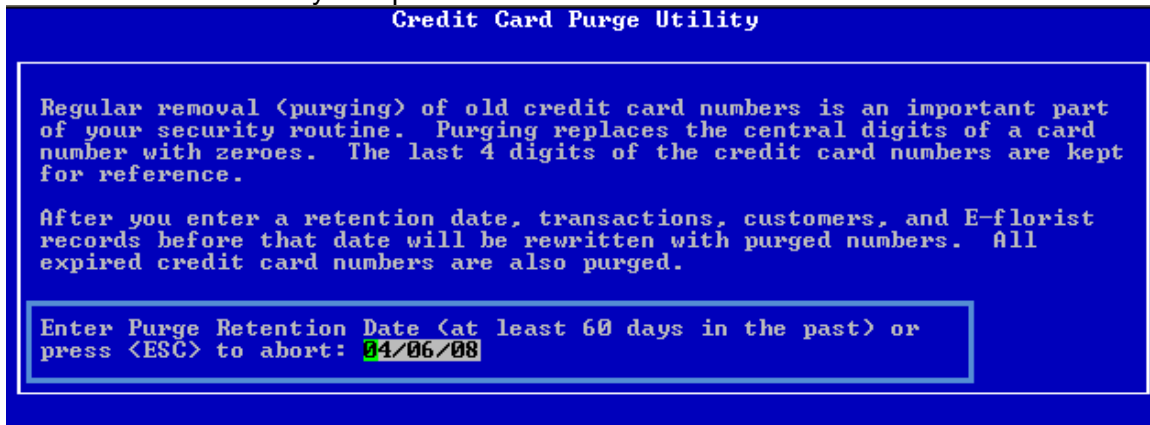
2. The *Support Menu* will appear. Press **D** **Daisy Application** then **Enter**.



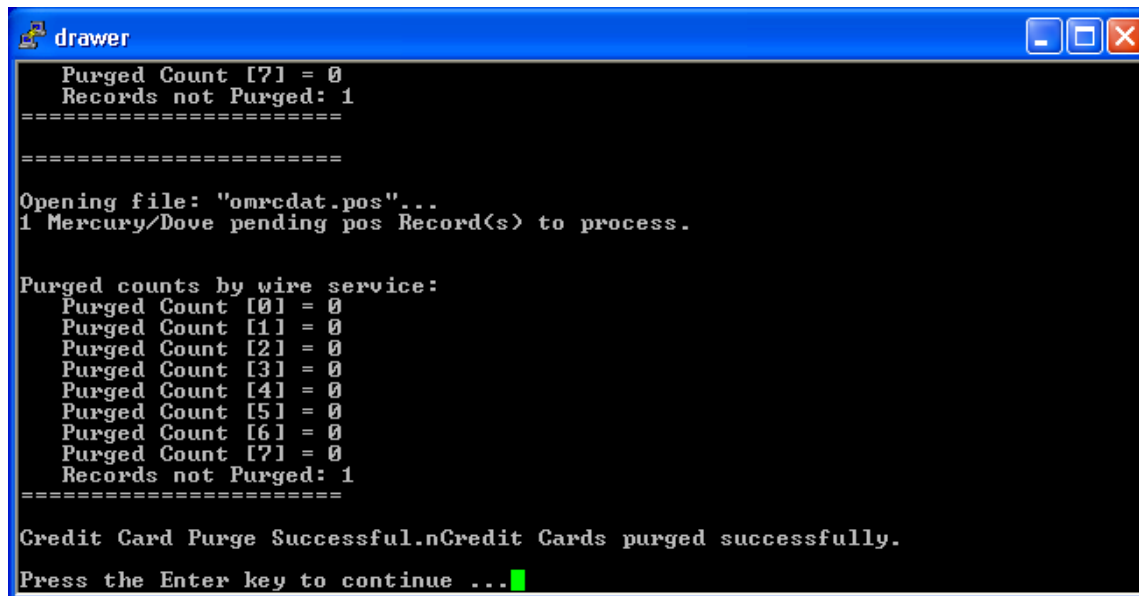
3. Press **C** **CC Purge**, then press **Enter** to run the **CCPurge Purge Expired Credit Cards** tool.



4. Enter a date at least 60 days in the past or press **Esc** to exit the Credit Card Purge Utility. The default date will be two years previous to the current date.



5. A confirmation box will appear prompting you to type **Purge** to confirm the date entered or press **Esc** to abort. Type **Purge**.
6. The system will scan the database purging sensitive card data. When finished the screen should display **Credit Card Purge Successful. # Credit Cards Purged successfully**. Press **Enter** to continue.



```

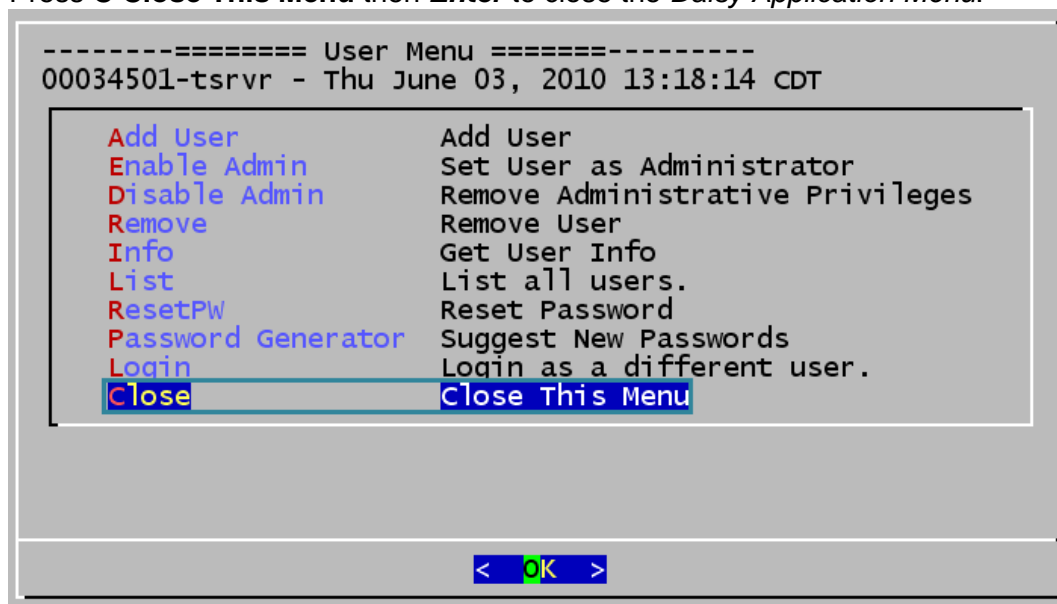
drawer
Purged Count [7] = 0
Records not Purged: 1
=====

Opening file: "omrcdat.pos"...
1 Mercury/Dove pending pos Record(s) to process.

Purged counts by wire service:
Purged Count [0] = 0
Purged Count [1] = 0
Purged Count [2] = 0
Purged Count [3] = 0
Purged Count [4] = 0
Purged Count [5] = 0
Purged Count [6] = 0
Purged Count [7] = 0
Records not Purged: 1
=====

Credit Card Purge Successful.nCredit Cards purged successfully.
Press the Enter key to continue ...
  
```

7. Press **C Close This Menu** then **Enter** to close the *Daisy Application Menu*.



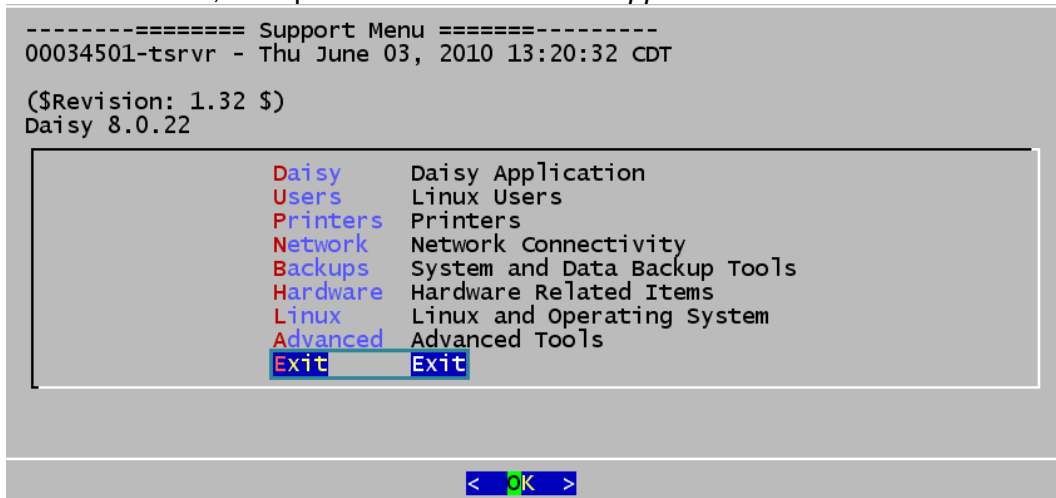
```

----- User Menu -----
00034501-tsrr - Thu June 03, 2010 13:18:14 CDT

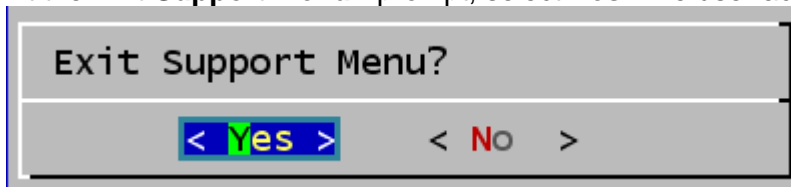
Add User          Add User
Enable Admin      Set User as Administrator
Disable Admin     Remove Administrative Privileges
Remove           Remove User
Info             Get User Info
List            List all users.
ResetPW         Reset Password
Password Generator Suggest New Passwords
Login          Login as a different user.
Close          Close This Menu

< OK >
  
```

8. Press **E** **Exit**, then press **Enter** to exit the *Support Menu*.



9. At the **Exit Support Menu?** prompt, select **Yes**. The user account is logged out.



How to Create a “Strong” Password in Linux

PCI DSS 8.5

PCI DSS gives specifications as to password strengths required. 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. Complex passwords must be at least 7 characters in length (PCI 8.5.10) and include at least one of ALL of the following:

- Uppercase letter (PCI 8.5.11)
- Lowercase letter (PCI 8.5.11)
- Number (PCI 8.5.11)
- Special Characters (@, #,). Special characters can include a space.
- Different from one of the last four passwords you have used in the past. (PCI 8.5.12)

Some examples of complex passwords:

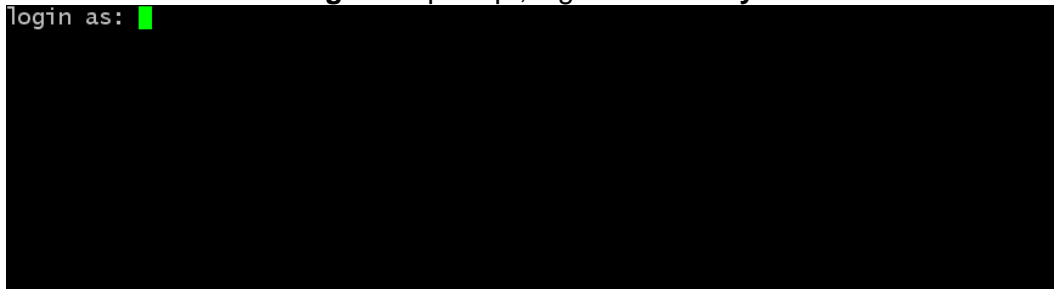
J58ate83

I like D3isy.

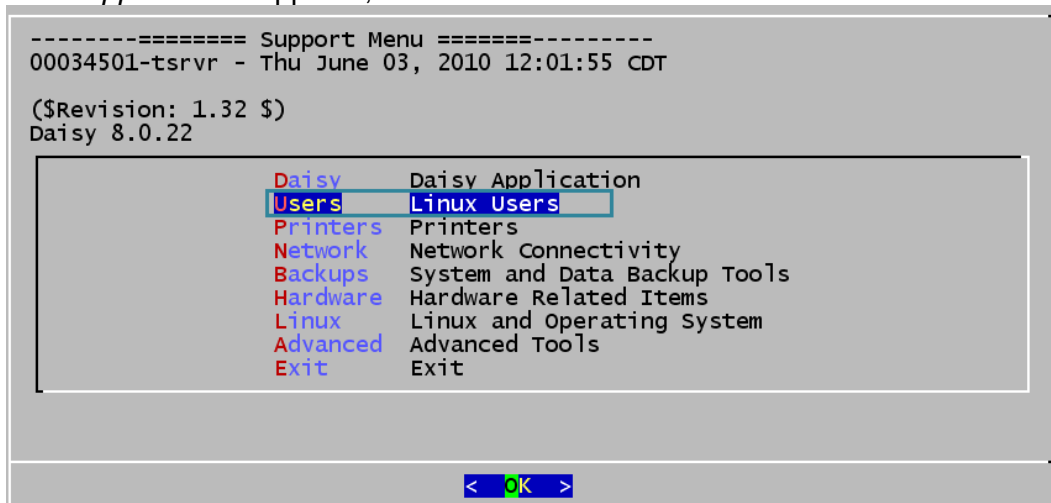
Cr@bsliveb3ach

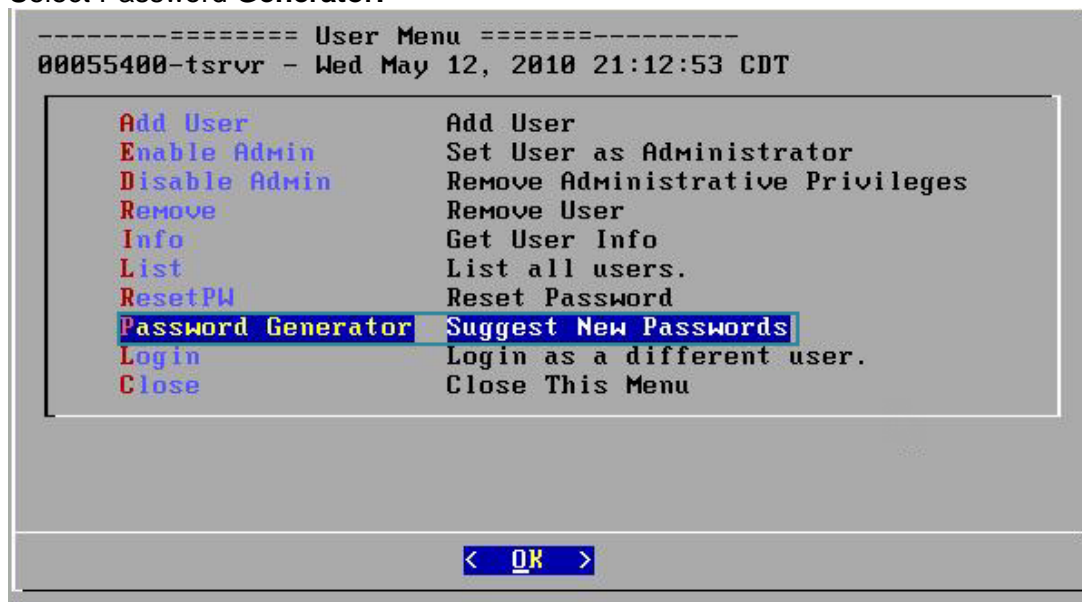
The br@wn fox runs f3st!

1. Press **Alt-F12**. At the **login as:** prompt, log in as a **Daisy Admin** user.

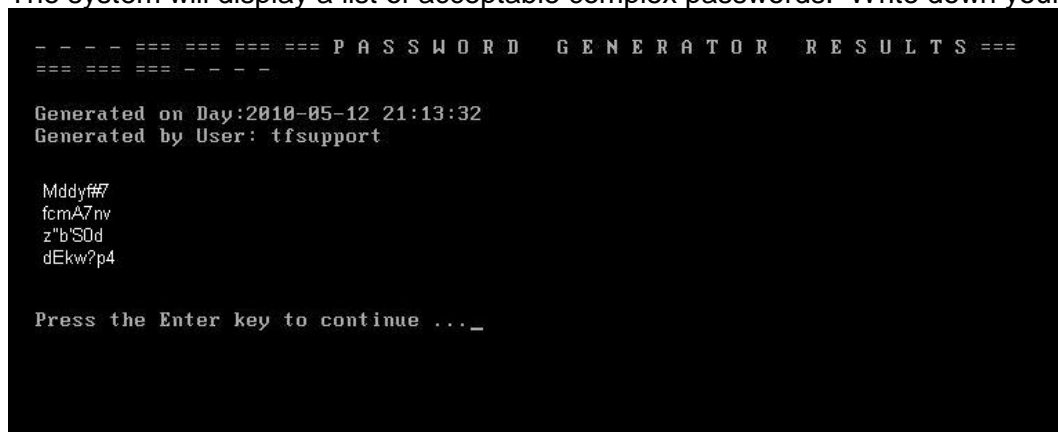


2. The *Support Menu* appears, select **Users Linux Users**.



3. Select Password **Generator**.

4. The system will display a list of acceptable complex passwords. Write down your desired choice.

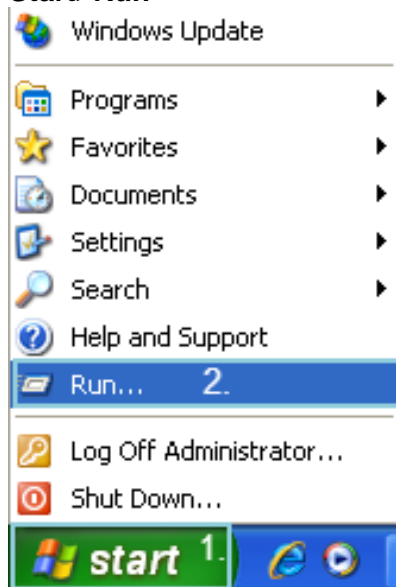
5. Press **Enter** to return to the *User Menu*

How to Verify Password Policies in Windows XP / Vista

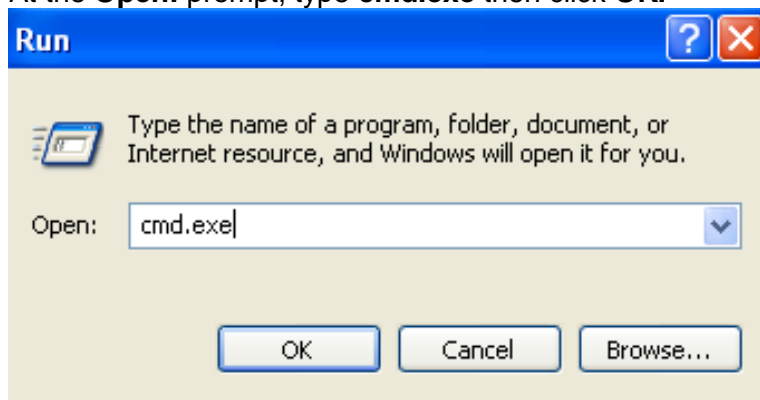
PCI 8.5

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

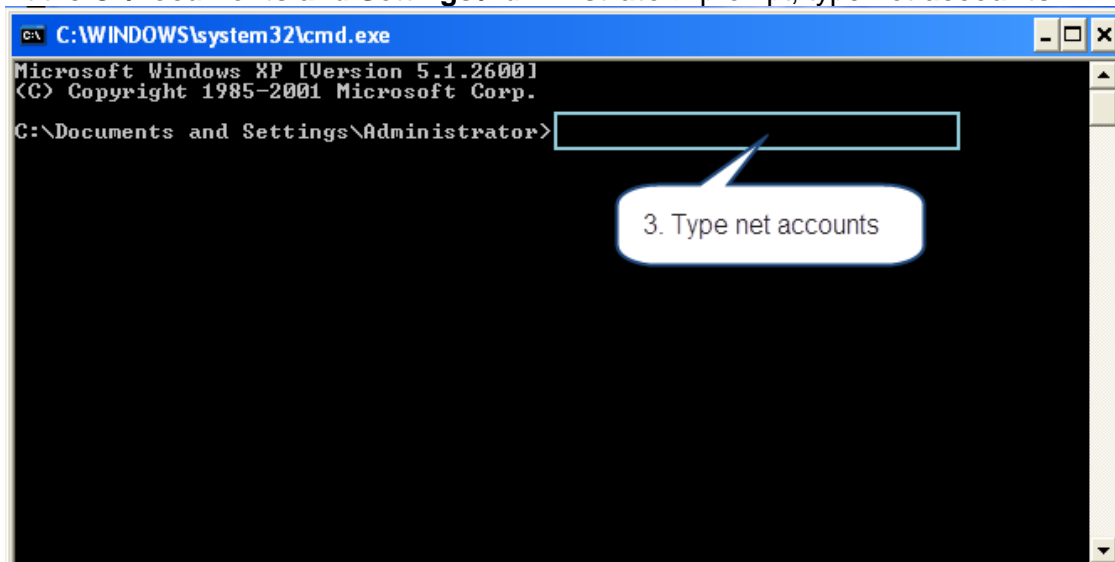
1. Start>Run



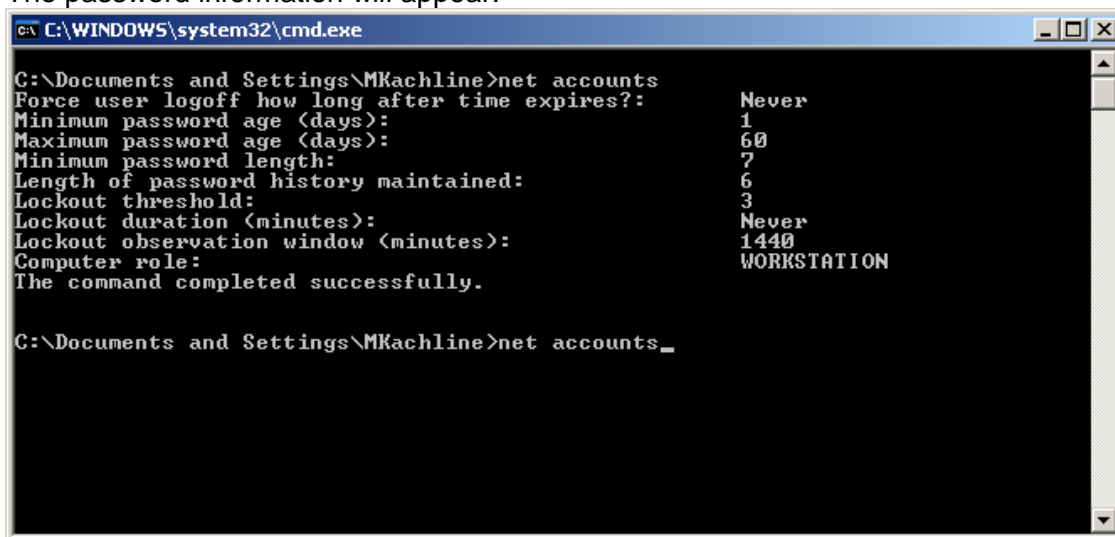
2. At the **Open:** prompt, type **cmd.exe** then click **OK**.



3. At the **C:\Documents and Settings\Administrator>** prompt, type **net accounts**.



4. The password information will appear.



Look for:

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

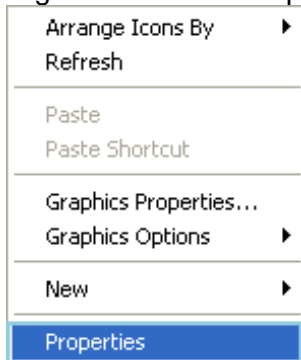
How to set a Screensaver Lock in Windows XP

PA-DSS 3.1
PCI 8.5.15

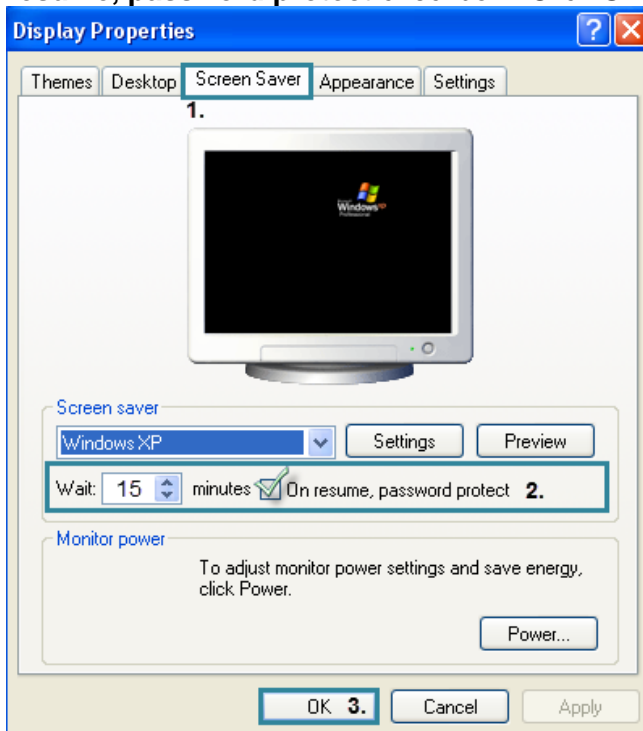
To be compliant with PA-DSS requirements, each workstation with access to the Daisy application must have a locking screensaver. The Screensaver must lock, requiring a password to access the workstation after 15 minutes of inactivity.

To set up Screensaver Lock in Windows XP:

1. Log into Windows computer.
2. Right-click the desktop. Click **Properties**.



3. Click the **Screen Saver** tab. Type **15** (or less than 15) in the **Wait xx minutes** box. Check **On resume, password protect** checkbox. Click **OK**.



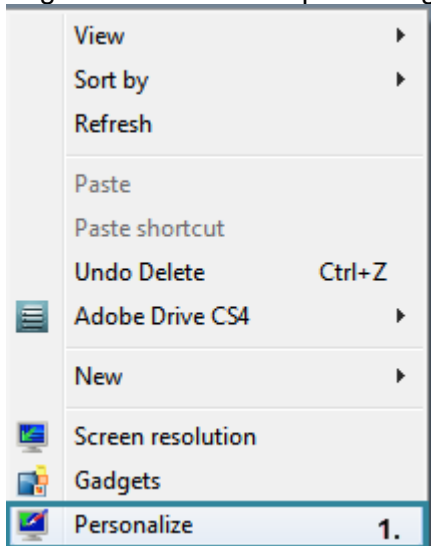
How to Set a Screensaver Lock in Windows Vista

PA-DSS 3.1
PCI 8.5.15

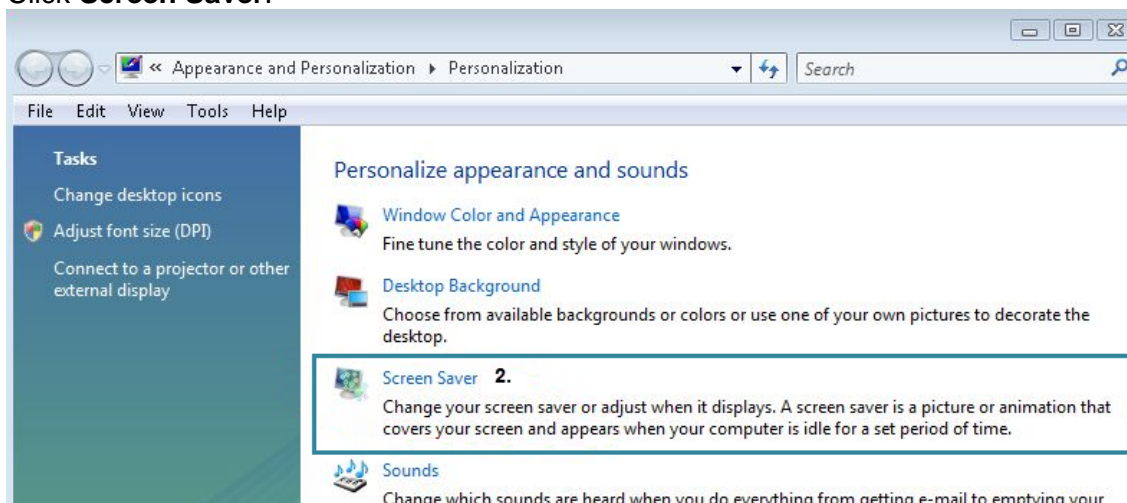
To be compliant with PA-DSS requirements, each workstation with access to the Daisy application must have a locking screensaver. The Screensaver must lock, requiring a password to access the workstation after 15 minutes of inactivity.

To set up Screensaver Lock in Windows Vista:

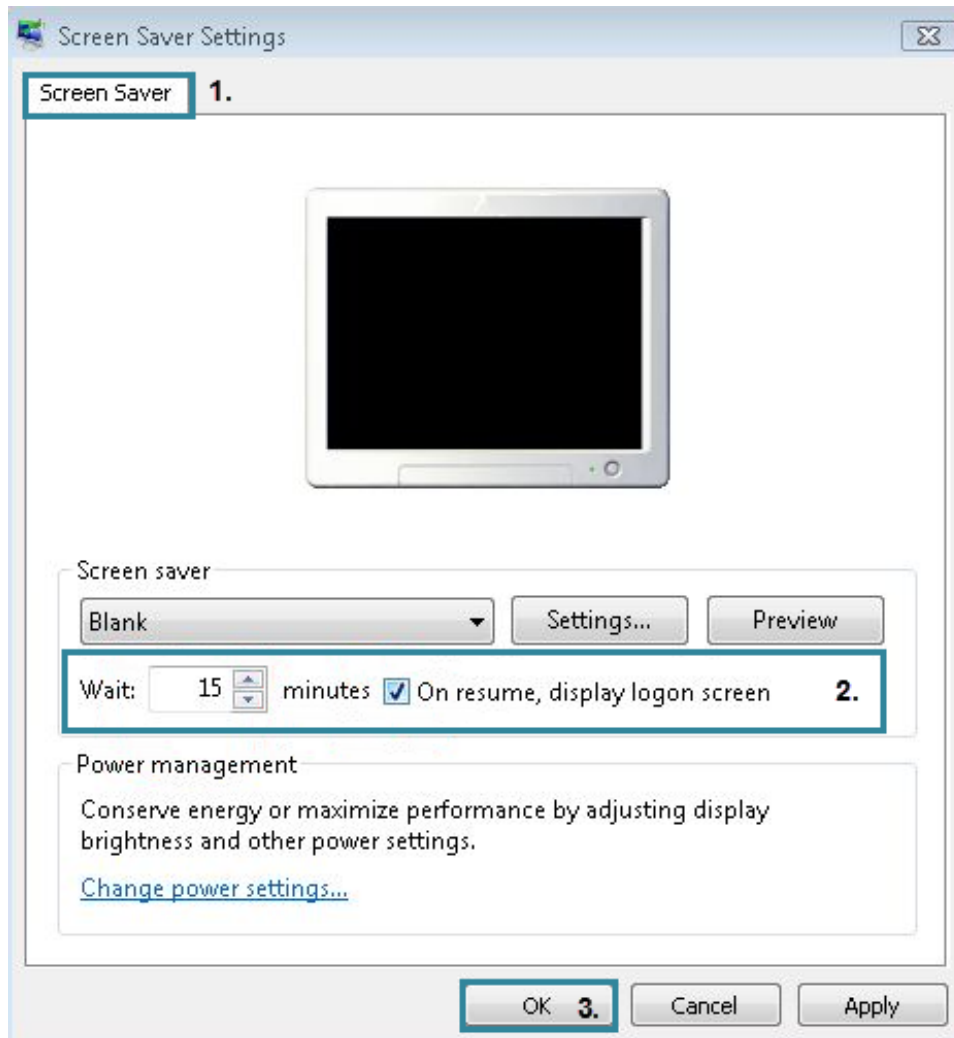
1. Log into Windows computer. Right-click the desktop. Click **Personalize**.



2. Click **Screen Saver**.



3. The *Screen Saver* screen appears. Type **15** (or less than 15) in the **Wait xx minutes** box. Check **On resume, display logon screen** checkbox. Click **OK**.



How to Configure your SSH Daemon

PA-DSS 11.3.b

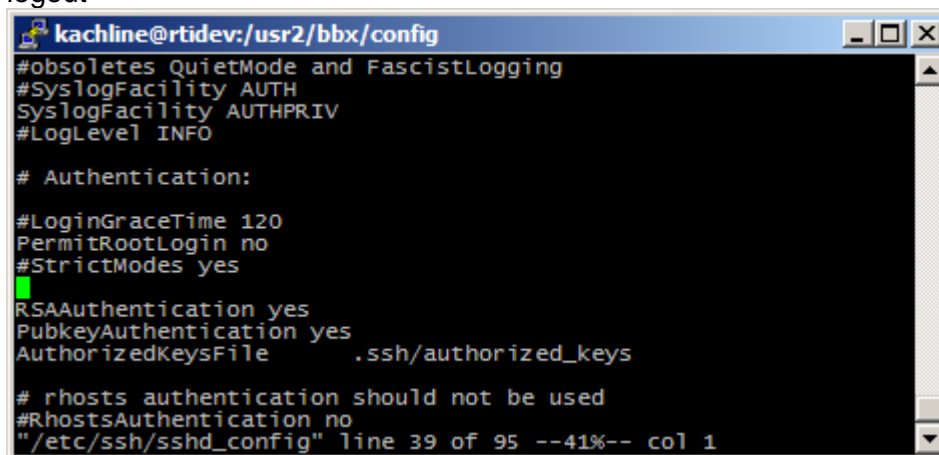
Your Daisy System is accessed primarily through the “SSH” protocol. All SSH connections are established through a background program called “sshd”. Following are instructions for stopping, starting, and configuring your SSH Daemon.

WARNING:

Improper configuration of SSHd could enable serious security flaws, or render your server inaccessible from remote hosts. Before making any changes, make sure you understand what you are changing.

Configuring SSHd:

1. Login to your Daisy server as an administrator.
2. `sudo vi /etc/ssh/sshd_config`
3. Make your changes to the file, write the file, and then quit: `(:wq!)`
4. To quit without saving your changes: `:q!`
5. `sudo /sbin/service sshd restart`
6. `logout`



```
kachline@rtidev:/usr2/bbx/config
#obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

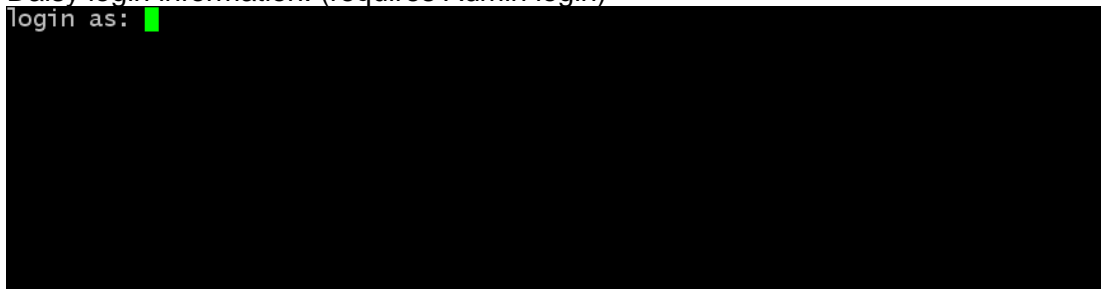
# Authentication:

#LoginGraceTime 120
PermitRootLogin no
#StrictModes yes
RSAAuthentication yes
PubkeyAuthentication yes
AuthorizedKeysFile .ssh/authorized_keys

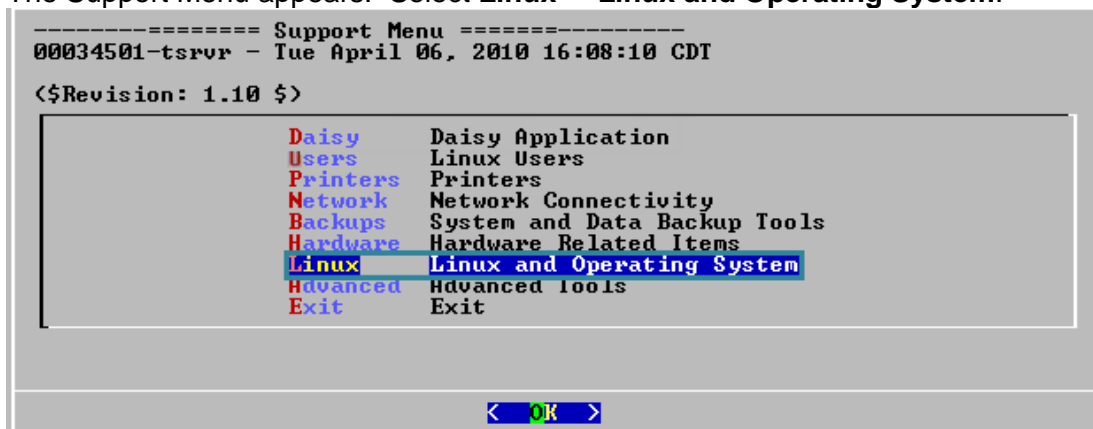
# rhosts authentication should not be used
#RhostsAuthentication no
"/etc/ssh/sshd_config" line 39 of 95 --41%-- col 1
```

Starting SSHd (Enabling Encrypted Data Transmission):

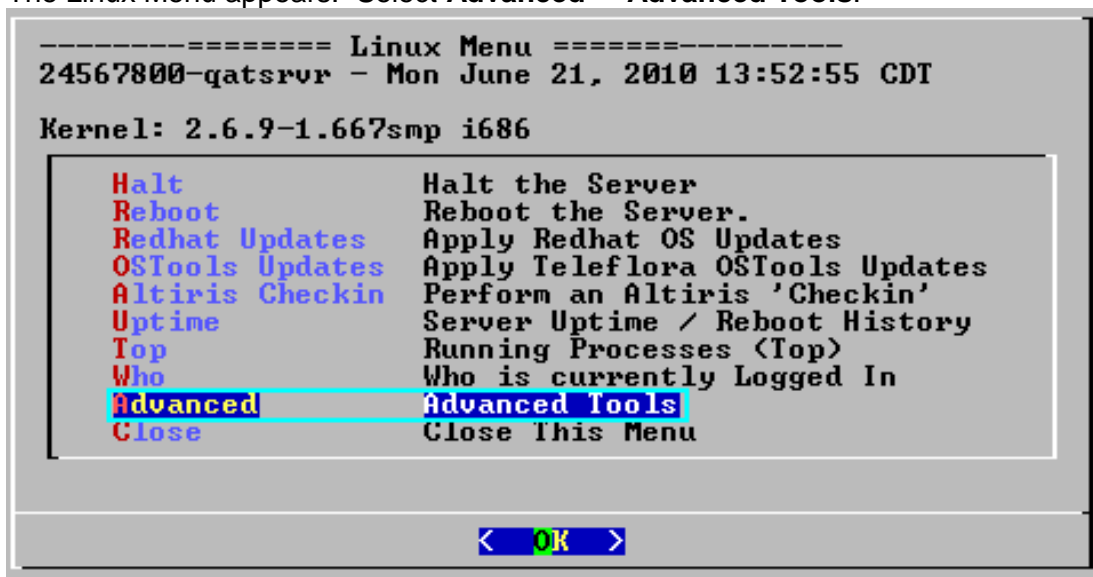
1. Login to your Daisy server as an administrator. Press **Alt-F12**. At the **login as:** prompt, type your Daisy login information. (requires Admin login)



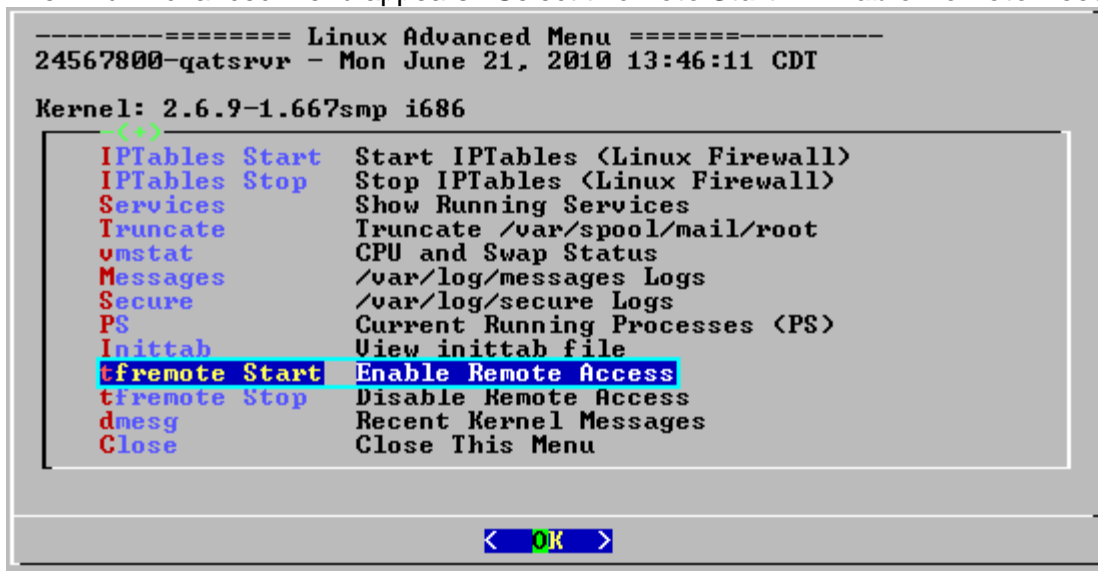
2. The Support Menu appears. Select **Linux** **Linux and Operating System**.



3. The Linux Menu appears. Select **Advanced** **Advanced Tools**.



4. The Linux Advanced Menu appears. Select **tfremote Start** **Enable Remote Access**.

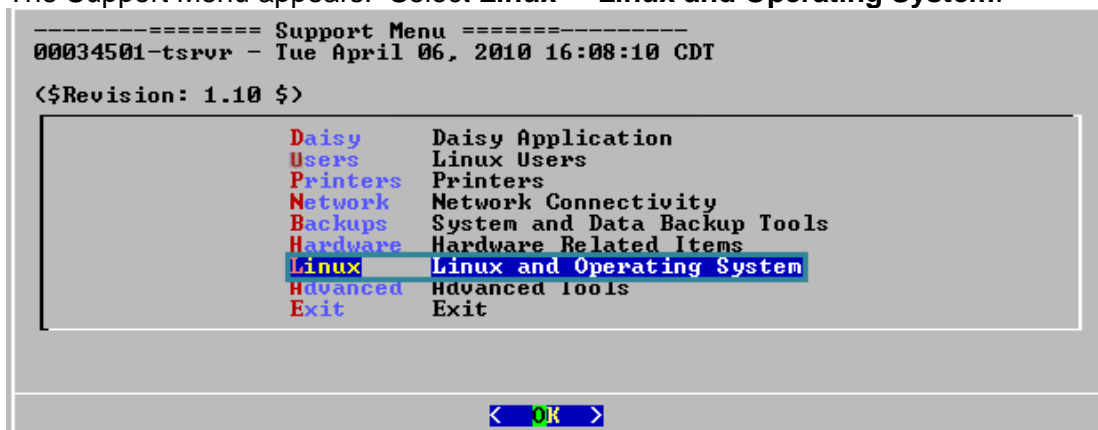


Stopping SSHd:

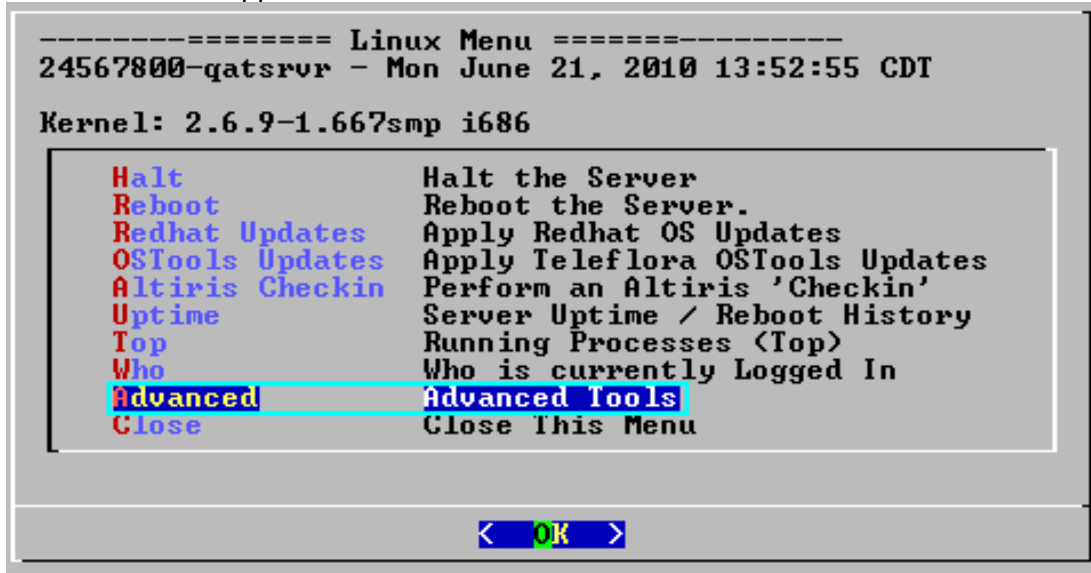
1. Login to your Daisy server as an administrator. Press **Alt-F12**. At the **login as:** prompt, type your Daisy login information. (requires Admin login)



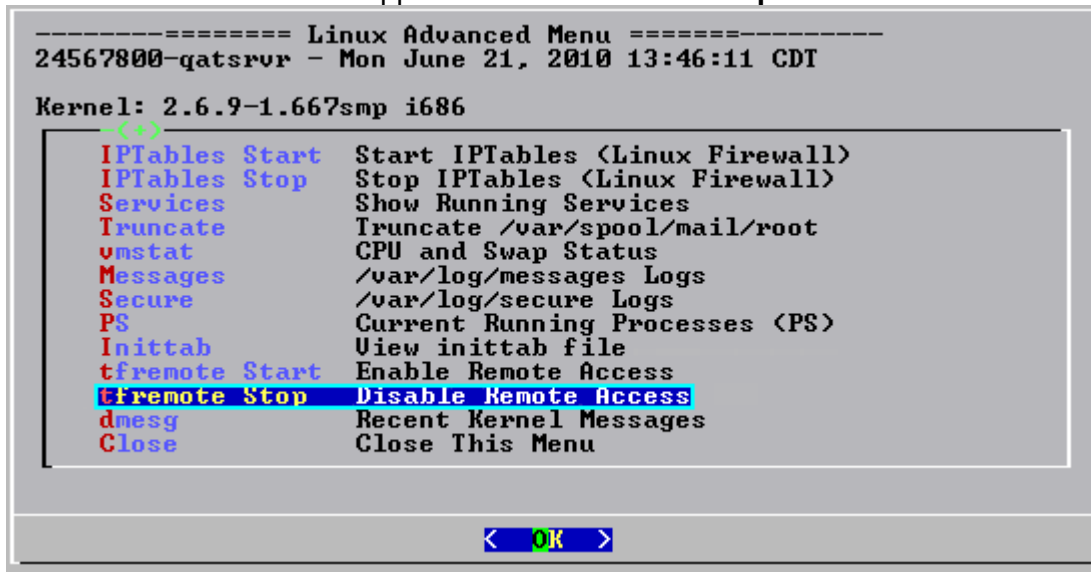
2. The Support Menu appears. Select **Linux** **Linux and Operating System**.



3. The Linux Menu appears. Select **Advanced** **Advanced Tools**.



4. The Linux Advanced Menu appears. Select **tfremote Stop** **Disable Remote Access**.



Using the “Shred” Secure Wipe Tool

PA-DSS 1.1.4

PA-DSS 2.7

Your RedHat Linux system includes Shred, a command line utility. This tool must be used to securely delete any cryptographic key material and/or files containing cardholder data. Following is a summary of how you may use the “shred” utility. Note that you will find the most up-to-date documentation on using ‘shred’ by running:

shred

on the command line.

SHRED(1)

FSF

SHRED(1)

NAME

shred - delete a file securely, first overwriting it to hide its contents

SYNOPSIS

shred [OPTIONS] FILE [...]

DESCRIPTION

Overwrite the specified FILE(s) repeatedly, in order to make it harder for even very expensive hardware probing to recover the data.

Mandatory arguments to long options are mandatory for short options too.

-f, --force
change permissions to allow writing if necessary

-n, --iterations=N
Overwrite N times instead of the default (25)

-s, --size=N
shred this many bytes (suffixes like K, M, G accepted)

-u, --remove
truncate and remove file after overwriting

-v, --verbose
show progress

-x, --exact
do not round file sizes up to the next full block

-z, --zero
add a final overwrite with zeros to hide shredding

- shred standard output
- help display this help and exit
- version
output version information and exit

Delete FILE(s) if --remove (-u) is specified. The default is not to remove the files because it is common to operate on device files like /dev/hda, and those files usually should not be removed. When operating on regular files, most people use the --remove option.

CAUTION: Note that shred relies on a very important assumption: that the filesystem overwrites data in place. This is the traditional way to do things, but many modern filesystem designs do not satisfy this assumption. The following are examples of filesystems on which shred is not effective:

- * log-structured or journaled filesystems, such as those supplied with
AIX and Solaris (and JFS, ReiserFS, XFS, Ext3, etc.)
- * filesystems that write redundant data and carry on even if some writes
fail, such as RAID-based filesystems
- * filesystems that make snapshots, such as Network Appliance's NFS
server
- * filesystems that cache in temporary locations, such as NFS
version 3 clients
- * compressed filesystems

In addition, file system backups and remote mirrors may contain copies of the file that cannot be removed, and that will allow a shredded file to be recovered later.

AUTHOR

Written by Colin Plumb.

REPORTING BUGS

Report bugs to <bug-coreutils@gnu.org>.

COPYRIGHT

Copyright (C) 2002 Free Software Foundation, Inc.
This is free software; see the source for copying conditions. There is
NO warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR
PURPOSE.

SEE ALSO

The full documentation for shred is maintained as a Texinfo manual. If the info and shred programs are properly installed at your site, the command

info shred

should give you access to the complete manual.

shred (coreutils) 4.5.3

August 2003

SHRED(1)

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.

Daisy Application Summary

Software Vendor	Teleflora
Teleflora Contact Information:	
Teleflora Mailing Address	
Product Name	Daisy
Product Version	8.0
Recommended OS:	RedHat Enterprise Linux ES 4.0 i386 RedHat Enterprise Linux ES 5.0 i386
Traditional Marketplace:	Retail Florist

Typical Daisy Network Topology

Overall Description:

The typical Daisy deployment is a classic star topology network, similar to the older dumb terminal era. Because Daisy workstations are essentially dumb terminals, a typical deployment will consist of only a single Daisy server, connected to multiple terminals. If you have multiple physical locations, many terminals are connected to the Daisy server over a VPN connection. Most terminal/server connections occur via the SSH protocol.

Windows PC with Terminal Emulator

PCs running Microsoft Windows is the typical platform for a terminal station. An integrated keyboard swiper or a wedge is used to capture credit card swipes. All communications to the Daisy server is via terminal emulation software such as puTTY. These terminals usually interface to the Application Server via a hard-wired LAN.

Broadband Router

Many shops are connected to the internet via a typical business class broadband connection. In most cases, the Daisy system comes with a business class router/firewall device, used to establish a Daisy LAN, implement firewall rules and establish multi-site VPN connectivity. In most cases, Daisy Customer support has remote administrative access to these routers.

Credit Card Modem

A limited number of shops may use dial-backup modem for dial-out credit card transactions.

Dove Network Modem

A limited number of shops may employ the use of a dial-backup modem for connecting to the Dove Network. This modem would both dial-out to the Dove network, as well as accept inbound calls from the Dove Network.