Teleflora Point of Sales

RTI Version 15

PA-DSS Implementation Guide

Version: 1.0
Version Date: June 2013

REVISIONS

Document Version	Date	Description
1.0	June 2013	Initial document creation for RTI version 15 PA-DSS 2.0 standard

Table of Contents

Purpose of this Document

Every merchant who accepts and stores credit (and debit) card payment data from national card providers (ex. Visa, Mastercard, American Express, Discover, JCB) through a Point of Sale (POS) computer system must ensure that their computers systems adhere to the guidelines of the Payment Card Industry (PCI) Security Standards Council.

The 2.0 standards are freely available under "PCI Documents and Standards" at the Security Standards Council webpage:

https://www.pcisecuritystandards.org/

Two related Security Council documents at this site specifically frame our obligations to cardholder security:

1. PCI Data Security Standards (PCI DSS) Requirements and Security Assessment Procedures Version 2.0 (October 2010)
2. PCI **Payment Application** Data Security Standards (PCI **PA-**DSS) Requirements and Security Assessment Procedures Version 2.0 (October 2010)

Teleflora is a partner in your compliance with these standards. We have submitted your Point of Sale (POS) software application, and supporting security documentation, to an auditor who are independently trained to verify our adherence to the PCI standards documents. In the context of the standards, these auditors test and verify the security risks in our software design practices, as well as operating system and hardware configurations.

Additionally, the PCI Security Council mandates (PA-DSS requirement 13) thtat we publish this *Implementation Guide* document. In short, this document gives you, and anyone involved in administration of your POS Computer System, "Teleflora and RTI POS-Specific" interpretation to PCI-mandated guidelines which might otherwise seem ambiguous.

Scope and Definitions

In order to reduce retail credit card fraud, the Payment Card Industry has set forth a number of policies and guidelines needed to maintain a “secure” Point of Sale environment. These guidelines are defined in the Payment Application Data Security Standards (PA-DSS). Teleflora has made a number of application and procedural changes in order to ensure that your RTI POS system is compliant with the 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 “RTI Specific” applications to the various PA-DSS requirements. Please refer to the associated “Payment Card Industry Data Security Standard” document for full details on compliance regulations.

Following are definitions for some terms used throughout this document.

Term	Definition
PA-DSS	Payment 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.
RTI Application Server	Physical server (and all software installed by Teleflora) which hosts the RTI application and its associated data files.
Administrative user	Any Unix user account capable of obtaining a Unix shell on the RTI Application server.
“Data Security Standard”	A document, published by Visa, which specifies all polices and requirements fundamental to PABP compliance.

Learning More

PA-DSS 13.2.1

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

http://www.pcisecuritystandards.org

Teleflora also provides information and guidance as to becoming, and remaining PCI compliant. You will find a "PCI" related section in the RTI User Group forum at:
http://rti.myteleflora.com/

These particular documents should be considered "must have" supplemental to this document:

1) PCI DSS Version 2.0 Requirements
   https://www.pcisecuritystandards.org/security_standards/supporting_documents_home.shtml

2) PCI DSS Self-Assessment Questionnaire
   https://www.pcisecuritystandards.org/security_standards/documents.php?category=saqs

Do note that at the time of this writing, we are using the PA-DSS specifications version 2.0 and PCI DSS Revision 2.0 documents.

Dissemination of This Document

Addresses:
PA-DSS 13.1
PA-DSS 13.2

A copy of this document should be freely available to all persons who use or administer your RTI 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 the RTI 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 RTI Customer service to ensure that you have the latest version of this document.

RTI Customer Service Contact Information:

Phone: 800-621-8324
Email: rtisupport@teleflora.com

Postal Mail:
RTI Customer Service
3309 E. Kings Highway
Paragould, AR 72450

Storage of Cardholder Information

PA-DSS 1.1.4
PA-DSS 1.1.5

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”.

Previous versions of RTI have never stored magnetic stripe data, card validation values or codes, PINs, or encrypted PIN block data.

Your RTI system has been written to never require storage of CVV and “Swipe” data. Furthermore, RTI does not support “Debit Card” transactions (transactions which require customer entry of a ‘pin’), and hence, sensitive “pin block” information is never obtained or captured.

Credit card “Numbers” may be retained if a business need requires. It is important to look in non-obvious places for these values. 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.

Destroying Legacy Paper Artifacts:
Bear in mind that many older POS’s 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 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.

Deletion of previous RTI builds/data:
The RTI system is automatically updated when a new build is released. The process does not retain copies of the previous software versions nor copies of any sensitive data. However, check with your system administrator to ensure copies or backups have not been made on the server itself. Following is an example of properly removing older RTI files from disk.

IMPORTANT NOTE!

On most RTI systems, “/usr2/bbx” contains your current RTI system, removing this directory will render your RTI application unusable and permanently destroy data. Please double check your typing in the below process.

WARNING:

This process permanently removes files, there is no “undelete”. Since these files are in close proximity to your “live” RTI system, typing the wrong command could entail your “live” RTI system being permanently deleted. 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:

Locate the files you wish to delete.

1) Login as root
2) `Sudo shred –uv {filename}`
3) `sudo rm –rf {filename}`
4) `logout`

Deletion of sensitive authentication data gathered as a result of troubleshooting the application:
Your RTI system logs various communications level information pertaining to Credit Card transactions. It is possible for these logs to be made on an “informational” and then “verbose” level. RTI does NOT log sensitive cardholder information into these logs. In order to change the logging level or to turn off logging, please see the section titled “Credit Card Debug Logging”.

Cardholder Data Retention

PA-DSS 2.1
PA-DSS 2.7

RTI retains the following Cardholder data in its database: Encrypted Credit Card number and Encrypted Expiration Date. This data is contained in the BBj Database 'RTI' in the table CCXF01.

Teleflora has provided a tool to Purge cardholder data from the RTI database, please see the section "Purge Cardholder Data" for details on this tool.

According to PCI DSS requirement 3.1, merchants need to create a data retention business policy. Teleflora provides a template to help merchants develop this policy in the POS Template Policies document. Cardholder data exceeding your defined retention period needs to be purged to be compliant with PCI DSS.

Purge Cardholder Data

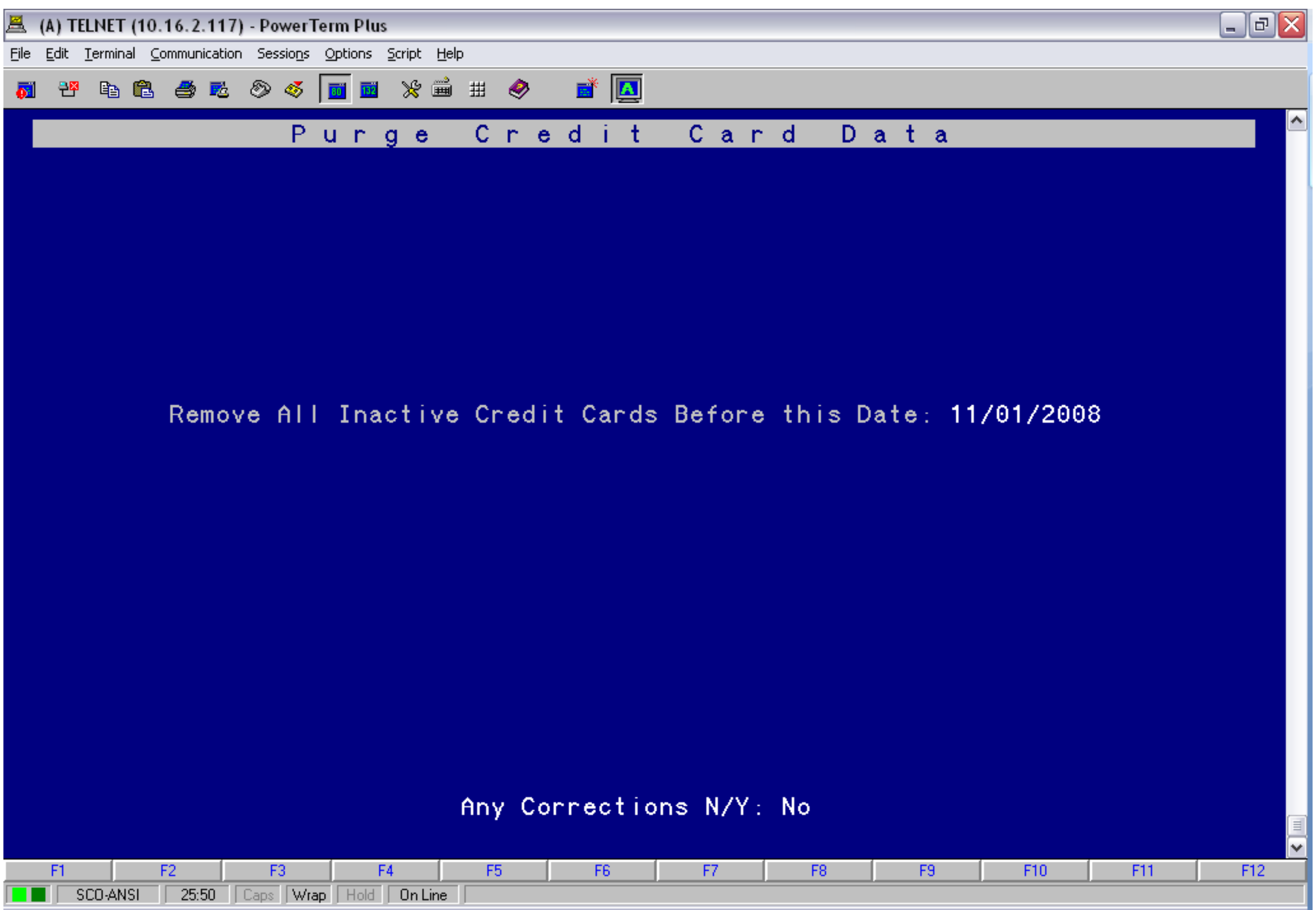
PA-DSS 2.1

Your RTI system is capable of removing cardholder information based on a specified time frame (retention period). The process will securely delete all inactive credit cards within the specified range.

Teleflora recommends that cardholder data be stored on the RTI server for a minimum of 3 months and no longer than 9 months, yet cardholder data that is 3 months or older can be purged as needed by utilizing the Purge Credit Card Data program.

Process:

1) Login as an administrative user
2) From the 4-Box Menu go to
    a. 1F (File Maintenance)
    b. 11 (Purge Files Menu)
    c. 11 (Purge Credit Cards)



Encryption Key Management

PA-DSS 2.5
PA-DSS 2.6
PA-DSS 2.7

Your RTI system uses AES-128 bit encryption technology in order to encrypt any cardholder information being retained on disk. An "encryption key", comprising of special files on disk are ultimately used to protect data.
In order to retain a level of security, you must follow some key management procedures as per PCI DSS. Directives you must follow are summarized as follows:

1) Restrict access to the decryption key material (RTI 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 RTI 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 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 done with them. (PCI 3.6.5)
7) Prevent the possibility of unauthorized substitution of cryptographic material. For example, do not tamper with the file permissions structure of your RTI system (PCI 3.6.7)
8) 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 (PCI 3.6.8)

Data Encryption Keys:
Your RTI 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 many data files on your RTI system (in the 'bbxd' directory), and is, itself encrypted with a "Key encrypting Key", as well as being accessible only in a programmatic fashion to users of the RTI system.
You may, at any point in time, choose to "rotate" the password used to encrypt your cardholder data. PCI requires rotating encryption keys at least once per year (PCI 3.6.4). However, key rotation should also occur any time an employee with administrative privileges leaves (PCI 3.6.8). Please read "How to Change your RTI Data Encryption Key" process in the appendix for detailed instructions on changing your RTI Data Encryption Key.

Key Encryption Keys:

Your RTI Data Encryption Key (DeK) is, itself, encrypted with a “Key Encryption Key” (KeK). The value of this second key is stored within a separate data file in your bbxd directory. As this KeK is stored within your filesystem, it is important not to compromise the security settings (chmod, chown, chgrp) of your “bbxp” directory, doing so could result in unauthorized substitution of your encryption keys. (PCI 3.6.7) Note your KeK is managed by the RTI system and, in as such, is periodically changed as your RTI system is upgraded. In the event that you believe your KeK has been compromised, it is important to take action to rotate the encryption keys immediately.

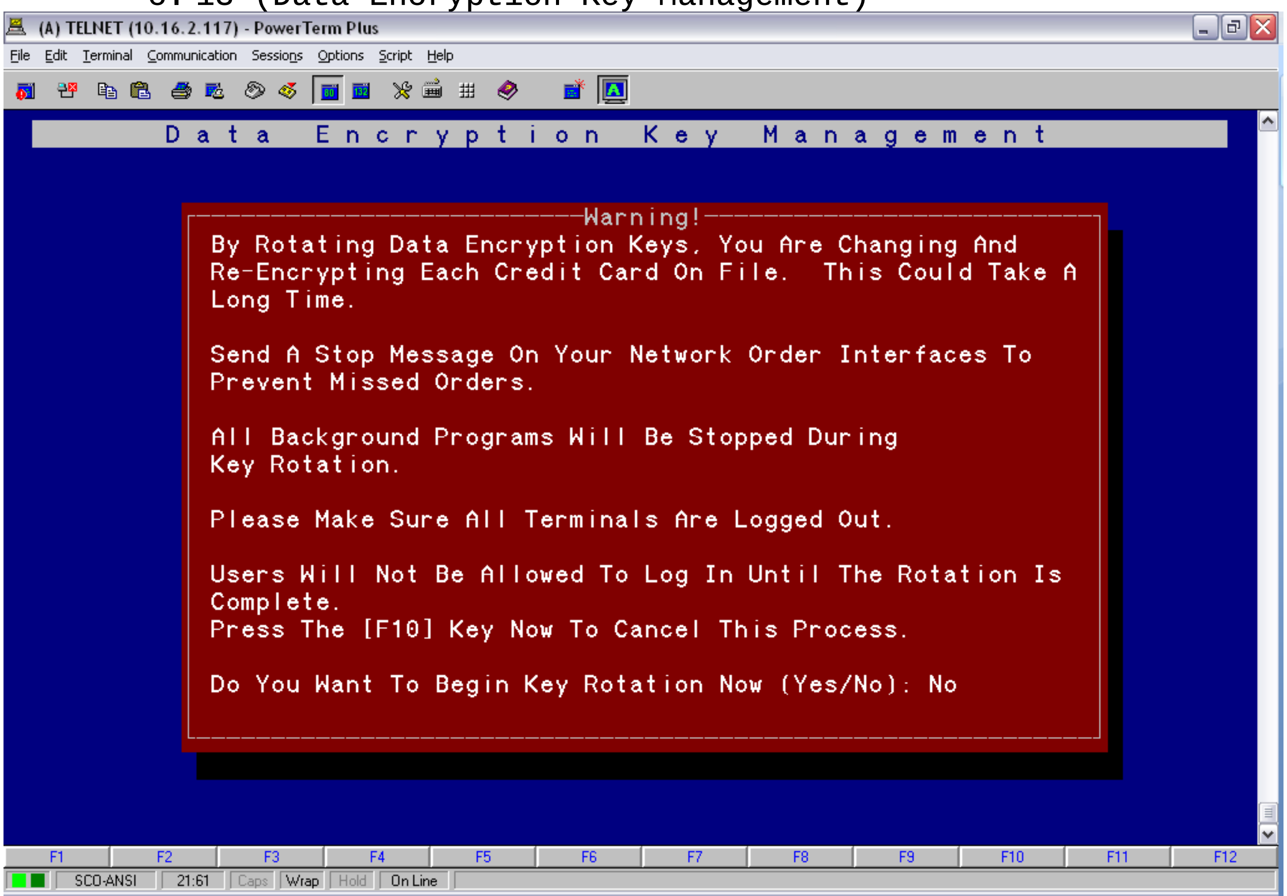
How to Change your RTI Data Encryption Key

PA-DSS 2.6

Your RTI 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. Following is the process you should follow in order to change your encryption key.

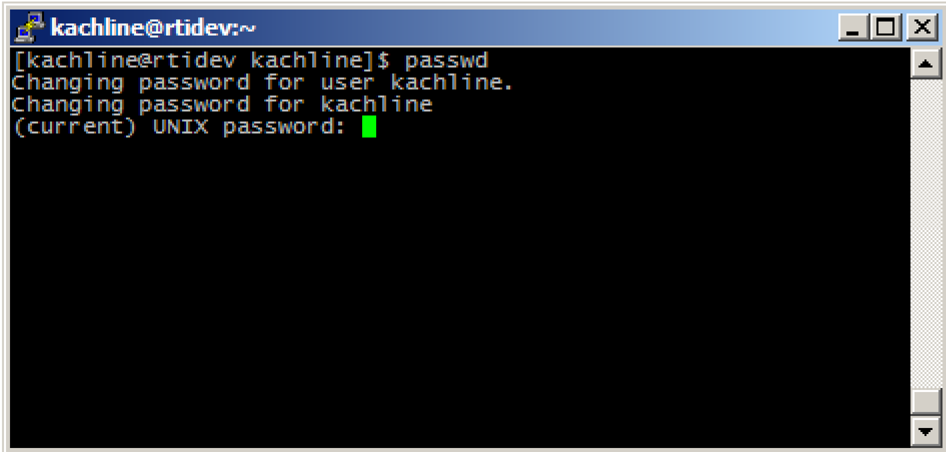
<u>Process:</u>

1) Login as root
2) Ensure that all users are logged off of your RTI system.
3) `killem`
4) `sshbbx`
5) From the 4-Box Menu go to
    a. 1F (File Maintenance)
    b. 13 (File Maintenance Continued)
    c. 13 (Data Encryption Key Management)



User accepts that they wish to rotate encryption keys.
System creates a new DeK and then executes the process of rotating keys while the user waits. Periodically, a "status" is given to indicate signs of life.
When process is complete, end user is notified.
The user will then need to restart the programs using the "startbbx" process.

User Identification and Authentication



PA-DSS 3.1
PA-DSS 3.2

If a data breach were to occur, it is important to be able to effectively identify who may have had access to compromised cardholder data. Your RTI 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 RTI 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 need not apply to employees who have access to only one credit card number at any time. In the context of your RTI system, this means that employees who do not have "administrative" privileges, and who can only use the RTI application, and do not have the ability to obtain a Unix "shell", need not comply with PCI DSS section 8.5. Regardless, Teleflora recommends you follow section PCI DSS for all of your employees, regardless of their level of access to the RTI system.

Teleflora Remote Administration Account:

RTI Customer Service uses the "tfsupport" user account in order to remotely administer your RTI system. Unless debugging a specific, user related problem, customer service should not need to login to your system as any other, already existing user account.
Just 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.

How to Add an RTI User Account

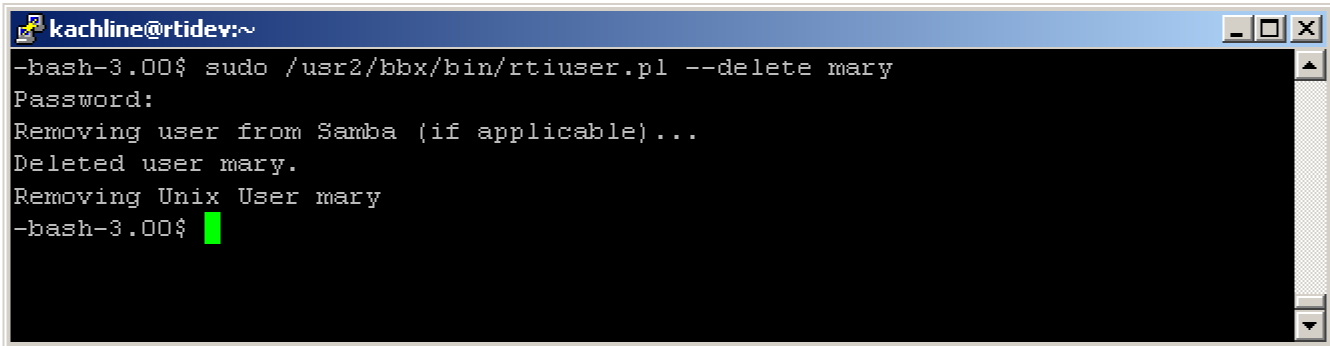
```
kachline@rtidev:~
-bash-3.00$ sudo /usr2/bbx/bin/rtiuser.pl --add mary
Creating User mary
chcon: .profile: No such file or directory
chcon: /home/mary/.bash_profile: No such file or directory
Disabling mary User Account.
Failed to find entry for user mary.
Failed to modify password entry for user mary
Locking password for user mary.
passwd: Success
-bash-3.00$ mkpasswd -l 8
O(v4hWZp
-bash-3.00$ sudo /usr2/bbx/bin/rtiuser.pl --setpw mary
Changing password for user mary.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
-bash-3.00$
```

PA-DSS 3.1

Following are steps needed to add an RTI user account. Note that the RTI application uses discretionary permissions which only allow members of the “rti” Unix group to access RTI related files. The “rtiuser.pl” script ensures that users are members of the appropriate Unix groups, as well as ensuring that RTI users are taken directly into the RTI application upon login.

Process:
1) `sudo /usr2/bbx/bin/rtiuser.pl --add newuser`
2) `mkpasswd –l 8 # Make sure to verify the password meets password complexity requirements as per PCI 8.5`
3) `sudo /usr2/bbx/bin/rtiuser.pl --setpw newuser`
4) `Type in a strong password`
5) `Have the user login and change their password to a new, PCI compliant password.`

How to Remove an RTI User Account



PA-DSS 3.1

The following process completely removes a user account from your RTI server. This must be done immediately upon termination of an employee, or after 90 days of inactivity of any employee.

Process:

1) `sudo /usr2/bbx/bin/rtiuser.pl --delete newuser`

RTI Operating System Logging

PA-DSS 4.2
PA-DSS 4.3

Operating System Logging:
Your RTI system logs various security information that is critical to being compliant with PA-DSS and PCI-DSS. Any action that results in the system logs being disabled will result in non-compliance with PCI-DSS. Please contact RTI Support with any concerns regarding your system logging.

Your RTI system utilizes the linux operating systems syslog feature to log all security related actions taken at the RTI server's operating system level. The following is the default syslog.conf setup for the RTI server. This setup will ensure compliance with PA-DSS 4.2 and 4.3.

```
# Log all kernel messages to the console.
#kern.*                                   /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none      /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                /var/log/secure

# Log all the mail messages in one place.
mail.*                                    -/var/log/maillog

# Log cron stuff
cron.*                                    /var/log/cron

# Everybody gets emergency messages
*.emerg                                   *

# Save news errors of level crit and higher in a special file.
uucp,news.crit                            /var/log/spooler

# Save boot messages also to boot.log
local7.*                                  /var/log/boot.log
kern.debug                /var/log/secure
```

AIDE & Audit Logging

The RTI server utilizes the linux AIDE and Audit modules to manage system level object integrity. These two modules are preconfigured on the RTI server. Disabling may result in non-compliancy with PCI regulations.

Audit manual:

http://linux.die.net/man/8/auditd

AIDE manual:

http://linux.die.net/man/1/aide

The directories noted below contain system level objects in which the aide and audit modules continually monitor.

/usr2/bbx/bbxp/
/usr2/bbx/bin/
/usr2/bbx/log/
/usr2/basis/bin/
/usr2/basis/log/
/usr2/basis/lib/

Example audit log using ausearch:

bash-4.1$ **sudo ausearch -f tcc_a_new_copy**
time->Tue Aug 6 15:00:21 2013
type=PATH msg=audit(1375819221.746:2676749): item=1 name="tcc_a_new_copy" inode=21104201 dev=08:03 mode=0100555 ouid=0 ogid=500 rdev=00:00 obj=unconfined_u:object_r:usr_t:s0
type=PATH msg=audit(1375819221.746:2676749): item=0 name="/usr2/bbx/bin" inode=21102792 dev=08:03 mode=040555 ouid=500 ogid=501 rdev=00:00 obj=system_u:object_r:usr_t:s0
type=SYSCALL msg=audit(1375819221.746:2676749): arch=c000003e syscall=2 success=yes exit=4 a0=7fff3517295a a1=c1 a2=16d a3=2 items=2 ppid=4897 pid=4898 auid=504 uid=0 gid=500 euid=0 suid=0 fsuid=0 egid=500 sgid=500 fsgid=500 tty=pts7 ses=404506 comm="cp" exe="/bin/cp" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="ROOT_ACTION"

bash-4.1$ **sudo rm -r tcc_a_new_copy**
bash-4.1$ **sudo ausearch -f tcc_a_new_copy**
----
time->Tue Aug 6 15:00:21 2013
type=PATH msg=audit(1375819221.746:2676749): item=1 name="tcc_a_new_copy" inode=21104201 dev=08:03 mode=0100555 ouid=0 ogid=500 rdev=00:00 obj=unconfined_u:object_r:usr_t:s0
type=PATH msg=audit(1375819221.746:2676749): item=0 name="/usr2/bbx/bin" inode=21102792 dev=08:03 mode=040555 ouid=500 ogid=501 rdev=00:00 obj=system_u:object_r:usr_t:s0
type=SYSCALL msg=audit(1375819221.746:2676749): arch=c000003e syscall=2 success=yes exit=4 a0=7fff3517295a a1=c1 a2=16d a3=2 items=2 ppid=4897 pid=4898 auid=504 uid=0 gid=500 euid=0 suid=0 fsuid=0 egid=500 sgid=500 fsgid=500 tty=pts7 ses=404506 comm="cp" exe="/bin/cp" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="ROOT_ACTION"
----
time->Tue Aug 6 15:01:08 2013
type=PATH msg=audit(1375819268.389:2677113): item=1 name="tcc_a_new_copy" inode=21104201 dev=08:03 mode=0100555 ouid=0 ogid=500 rdev=00:00 obj=unconfined_u:object_r:usr_t:s0
type=PATH msg=audit(1375819268.389:2677113): item=0 name="/usr2/bbx/bin" inode=21102792 dev=08:03 mode=040555 ouid=500 ogid=501 rdev=00:00 obj=system_u:object_r:usr_t:s0
type=SYSCALL msg=audit(1375819268.389:2677113): arch=c000003e syscall=263 success=yes exit=0 a0=ffffffffffffff9c a1=229c0c0 a2=0 a3=20 items=2 ppid=5566 pid=5567 auid=504 uid=0 gid=500 euid=0 suid=0 fsuid=0 egid=500 sgid=500 fsgid=500 tty=pts7 ses=404506 comm="rm" exe="/bin/rm" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="ROOT_ACTION"

Example aureport:
bash-4.1$ **sudo aureport**

Summary Report
======================
Range of time in logs: 08/06/2013 13:33:19.141 - 08/06/2013 15:03:47.950
Selected time for report: 08/06/2013 13:33:19 - 08/06/2013 15:03:47.950
Number of changes in configuration: 1
Number of changes to accounts, groups, or roles: 0
Number of logins: 7
Number of failed logins: 0
Number of authentications: 16
Number of failed authentications: 4
Number of users: 9
Number of terminals: 16
Number of host names: 12
Number of executables: 39
Number of files: 1162
Number of AVC's: 0
Number of MAC events: 7
Number of failed syscalls: 1087
Number of anomaly events: 0
Number of responses to anomaly events: 0
Number of crypto events: 75
Number of keys: 1
Number of process IDs: 2460
Number of events: 45487

Application Logging

PA-DSS 4.2
PA-DSS 4.3

Your RTI system logs various security information that is critical to being compliant with PA-DSS and PCI-DSS.

Credit Card Logging

Your RTI system logs various communications information pertaining to Credit Card transactions in the /usr2/bbx/log directory. RTI does **not** log sensitive cardholder information into these logs. These logs cannot be disabled. Any modification to disable the logging will result in non-compliance with PCI-DSS.

Example logging entry (/usr2/bbx/log/tcc-Day_##.log)

```
2013-07-15 09:19:57 (tcc) <I>  linux Log File Opened:Mon, 15 Jul 2013 09:19:57 -0500
tcc:TCCConfiguration parsed from XML:
  tcc:AdvantageSSLCertificate   "/usr2/bbx/bin/CERT1.pem"
  tcc:Logfile                   "/usr2/bbx/log/tcc.log"
  tcc:PrimaryAdvantageHost      "https://webgate.viaconex.com"
  tcc:PrimaryDialupPhone        "18009999999"
  tcc:PrimaryModem              "/dev/ttyUSB0"
  tcc:PrimaryModemInitString    "USR"
  tcc:PrimaryModemType          ""
  tcc:ProxyServer               ""
  tcc:SecondaryAdvantageHost    "https://webgate.viaconex.com"
  tcc:XSLTDirectory             "/usr2/bbx/bin/"

tcc:BatchAddRequest record# 1 parsed from XML:
  tcc:BillingAddress            "25 MAIN DR"
  tcc:BillingZip                "72450"
  tcc:CCExpiration              has length: 4
  tcc:CCNumber                  "4444********1092"
  tcc:CCSwipe                   ""
  tcc:CVV                       has length: 3
  tcc:ClerkInitials             "0026"
  tcc:DeliveryPennies           "0"
  tcc:IssuingBank               "Visa"
  tcc:KeySerialNumber           ""
  tcc:OrderID                   "00271179"
  tcc:OrderType                 "CustomerPhoneIn"
  tcc:PinBlock                  ""
  tcc:ProcessorResponseData     ""
  tcc:PurchaseOrderNumber       "JAMIE"
```

tcc:TCCId "00271179"
tcc:TaxPennies "736"
tcc:TotalPennies "8095"
tcc:TransactionGuid "00000000-0000-0000-0000-000000000000"
tcc:TransactionType "Purchase"

2013-07-15 09:19:57 (Elavon) <I> Opening Primary Connection to Elavon Host: https://webgate.viaconex.com
2013-07-15 09:19:57 (Elavon) <I> Uploading 1 Requests to Elavon
2013-07-15 09:19:58 (Elavon) <I> Success: APPROVAL TCCId="00271179" Authcode="015903" Pennies="8095" AvsResponse="Y" CvvResponse="M" IsSwiped="0"
2013-07-15 09:19:58 (Elavon) <I> Log File Closed.

Dove Network Logging

Your RTI system logs various communications information pertaining to Dove Network transactions in the /usr2/bbx/log directory. RTI does **not** log sensitive cardholder information into these logs. These logs cannot be disabled. Any modification to disable the logging will result in non-compliance with PCI-DSS.

Log entries for the dove network can be found in:

/usr2/bbx/log/tcc.log
/usr2/bbx/log/callout-Day_##.log
/usr2/bbx/log/doveserver-Day_##.log
/usr2/bbx/log/tws-Day_##.log
/usr2/bbx/log/Delta_Update-Day_##.log
/usr2/bbx/log/Delta_Update.log
/usr2/bbx/log/off-cycle.log

Fax Logging

Your RTI system logs various communications information pertaining to faxed transactions from the application. Fax transactions are logged in the /usr2/bbx/log directory. RTI does **not** log sensitive cardholder information into these logs. These logs cannot be disabled. Any modification to disable the logging will result in non-compliance with PCI-DSS.

Log entries for Dove transactions can be found in:

/usr2/bbx/log/rti-sendfax-Day_##.log

Kiosk Interface Logging
Your RTI system logs various communications information pertaining to the kiosk interface. Kiosk transactions are logged in the /usr2/bbx/log directory. RTI does **not** log sensitive cardholder information into these logs. These logs cannot be disabled. Any modification to disable the logging will result in non-compliance with PCI-DSS.

Log entry for faxing can be found in:

/usr2/bbx/log/kioskserver-Day_##.log

Backup Logging
Your RTI system logs various communications information pertaining to data backup process. Nightly data backups are logged in the /usr2/bbx/log directory. RTI does **not** log sensitive cardholder information into these logs. These logs cannot be disabled. Any modification to disable the logging will result in non-compliance with PCI-DSS.

Log entry for backups can be found in:

/usr2/bbx/log/rtibackup-Day_##.log

Weather Interface Logging
Your RTI system logs various communications information pertaining to weather updates. Weather updates are logged in the /usr2/bbx/log directory. RTI does **not** log sensitive cardholder information into these logs. These logs cannot be disabled. Any modification to disable the logging will result in non-compliance with PCI-DSS.

Log entry for faxing can be found in:

/usr2/bbx/log/weather_check.log

Application Build/Patch installation logging
Your RTI system logs various information pertaining to build and patch updates to the application. Updates are logged in the /usr2/bbx/log directory. RTI does **not** log sensitive cardholder information into these logs. These logs cannot be disabled. Any modification to disable the logging will result in non-compliance with PCI-DSS.

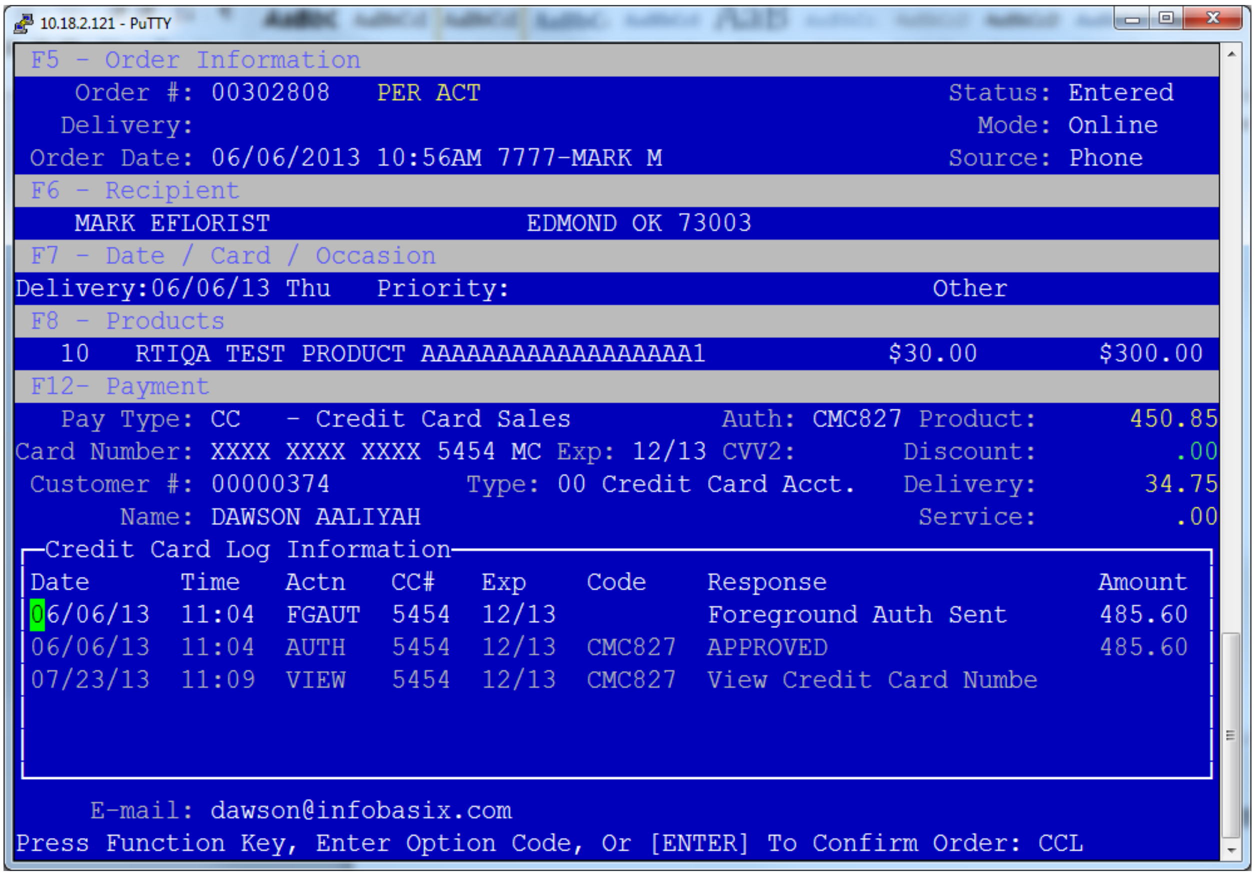
Log entry for faxing can be found in:

/usr2/bbx/log/rti_install-YYYY-DD-MM.log
/usr2/bbx/log/RTI-Patches.log

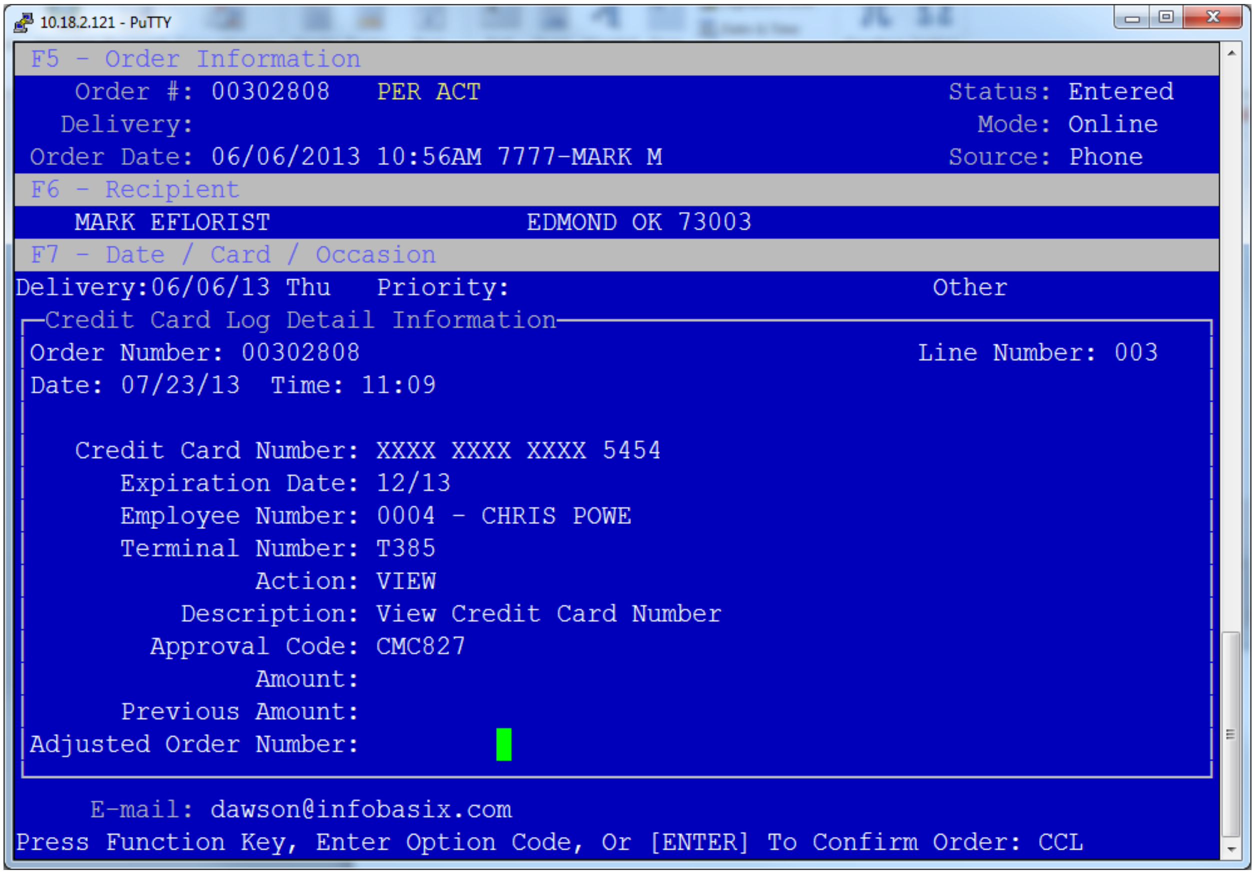
Application Credit Card access logging

The RTI Application only allows administrative users to view a credit card number. Only one credit card number at a time can be viewed. Non-administrative access does not have access to view credit numbers. Viewing a credit card number can only occur during the Order Entry process. If a credit card number is viewed by an administrative user, a log entry is created in the applications Order Entry CCL log (Credit Card Log).

To access the CCL a user must navigate to the Order Entry screen, pull up an existing order paid for by a credit card, and type “CCL” at the bottom of the order.



Arrowing down to the appropriate "View Credit Card Number" line and pressing the F1 function key will display further data.



Centralized Logging

PA-DSS 4.4

Operating System Level Logging

Your RTI system utilizes the linux operating system's syslog feature to log all security related operating system actions taken on the RTI server. The syslog service can be configured to direct all syslog entries to a centralized server.

In order to configure the RTI server to utilize a centralized remote logging server, the rsyslog process must be configured. Redhat © recommends these websites as information on setting up the rsyslog process.

http://www.rsyslog.com/
http://wiki.rsyslog.com/index.php/Main_Page

Application Level Logging

The RTI application incorporates internal logging specific to the application. An automatic nightly backup of the RTI database to removable media is preconfigured, however, to facilitate centralized logging, a daily copy of the database should be made to a centralized logging server. The RTI database tables are stored in /usr2/bbx/bbxd/ on the RTI server.

RTI does NOT log sensitive cardholder information into any application log.

Tables related specifically to security and credit card access:

/usr2/bbx/bbxd/ONCC01 – credit card authorization detail log
/usr2/bbx/bbxd/ONCC02 – credit card order activity log
/usr2/bbx/bbxd/ONCC03 – credit card account activity log
/usr2/bbx/bbxd/ONLG01 – order entry access log
/usr2/bbx/bbxd/ONLG02 – order entry access log detail
/usr2/bbx/bbxd/DCLG01 – credit card settlement log
/usr2/bbx/bbxd/DCLG02 – credit card settlement log detail
/usr2/bbx/bbxd/CSDO01 – Cash register access log

How to Remove RTI Log Files

PA-DSS 1.1.5

Your RTI system uses log files at the operating system level to record specific communication events to disk, always within the "/usr2/bbx/log" directory. These files are valuable in troubleshooting many issues which you may experience in your use of the application. Though RTI has been carefully written to never log sensitive data in these log files, in the event of either unforeseen bugs or the need for "special case" logging, sensitive data could be contained within these log files.
Following is the process you may follow to securely remove all RTI log files.

WARNING:

This process removes files permanently, 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) Login to your RTI server as an administrative account (tfsupport, etc.)
2) cd /usr2/bbx/log
3) shred –u *
4) logout

Directives for (Re)Sellers and Support Personnel:

- You should collect sensitive data only when needed to solve a specific problem.
- Collected data must be stored in specific, known locations with limited access by other persons or users.
- Collect only the limited amount of data needed in order to solve a specific problem.
- You must encrypt sensitive data while it is being stored.

You must securely delete sensitive data immediately after use

RTI Connectivity Specifications

PA-DSS 5.4

This information is made available for you to confirm the use of only necessary and secure services, protocols, components, and dependent software and hardware, including those progived by third parties. Or, in the event that you are providing your own network security configurations, to apply appropriate firewall and modem blocking rules.

- The RTI application server may use the following, modem dial-out capabilities:
    - Dove Network
    - Credit Card Authorizations and Settlements
    - Faxmodem dial out

- All remote administration into the RTI application server which occurs via the internet will come in via the "Secure Shell" (SSH) service, which uses TCP/IP port 22 or TCP/IP port 15022 (tfremote).

- All remote administration into the RTI application server which occurs via the internet will originate from one of the following public IP addresses.
    - 70.128.30.254
    - 65.245.5.209
    - 65.198.163.148
    - 65.245.5.36

- All remote administration of the RTI application will occur through the "tfsupport" user.

- Your firewall device should be configured to deny all "inbound" internet traffic except for the following IP Ports, and only from the Teleflora IP addresses listed above.
    - TCP Port 22 (SSH)
    - TCP Port 15022 (SSH – tfremote)
    - TCP Port 2525 (MyAccount Online)

- The RTI application server may additionally listen on the following inbound "IP ports" for "Local Area Network" (LAN) traffic.
    - UDP Port 137 (Samba)
    - UDP Port 138 (Samba)
    - TCP Port 139 (Samba)
    - TCP Port 445 (Samba)
    - TCP Port 1100 (Pro5 ODBC Server)

- TCP Port 4000 (Artisoft Telephone Integration)
- TCP Port 2301 (Basis Secure Thin Client)

- The RTI application server requires outbound internet connections to the following destination IP Ports:
  - TCP Port 25 (SMTP)
  - TCP Port 22 (SSH)
  - TCP Port 80 (HTTP)
  - TCP Port 443 (SSL / HTTPS)

Wireless Networks

Addresses:
PA-DSS 6.1
PA-DSS 6.2

To best protect your cardholder data, Teleflora does not recommend you use wireless networking for any device which is capable of communicating with your RTI server. In the case that Wireless network is required, however, the guidelines found in PCI DSS sections 1.3.9, 2.1.1 and 4.1.1 must be adhered to. Some suggested guidelines are as follows:

- PCI 1.2.3 An active firewall must be placed between the wireless router, and the network on which the RTI Application server resides. Teleflora recommends placing any wireless router(s) on an Internet DMZ.
- PCI 1.3.9 For mobile computers, it is required to ensure that firewall software is installed and enabled on the computer.
- PCI 2.1.1 - Modify vendor default settings for all wireless devices, and implement strong encryption.
- PCI 2.1.1 - Change default encryption keys for wireless devices. Also change encryption keys after anyone with knowledge of the keys leaves the company or changes positions.
- PCI 2.1.1 - Change default SNMP community strings, and default passwords/passphrases.
- PCI 2.1.1 - Update firmware on wireless devices to support strong encryption (WPA, WPA2) for authentication and transmission.
- PCI 2.1.1 - Modify other security related default settings.
- PCI 4.1.1 - Ensure wireless networks that transmit cardholder data use strong encryption for authentication and transmission
- PCI 4.1.1 - For new wireless implementations, it is prohibited to implement WEP. This went into effect on March 31, 2009.
- PCI 4.1.1 - Existing wireless networks connected to a payment card environment must not use WEP after June 30, 2010.
- PCI 9.1.3 – Physically secure wireless devices
- PCI 10.5.4 – Log wireless activity to a secure central system
- PCI 11.4 – Monitor ofr wireless intrusion attempts and alert personel to potential compomises
- PCI 12.3 – Develop usage policies for wireless access.

Protection from External Access

Addresses:
PA-DSS 9.1
PA-DSS 10.1

Though the internet is an integral part to your RTI system, it is important to ensure that access, from the internet, into your RTI system is restricted. Furthermore, it is your responsibility to ensure that any other computers on your network, which either hold cardholder information, or process cardholder information (for instance, have a swiper device attached), are themselves, protected from direct connections from the internet. These requirements are specified in PCI DSS 1.3 and PA-DSS 9.1.b.

Hardware Firewalls:
PA-DSS 9.1
It is essential that you employ the use of a dedicated hardware "firewall" device to protect all RTI machines from the internet. This firewall device must block all, non-essential traffic from the internet to your internal network. Furthermore, it is highly recommended that the firewall device also block all network traffic, from your network, to the internet. You will find a list of all, RTI required network ports later in this document.

Personal Firewalls:
PA-DSS 10.1
Mobile computers, such as laptops, should additionally employ "personal firewall" software (such as McAfee) to provide protection in times when the laptop is not behind the RTI firewall device. Please see the "RTI Connectivity Information" section, later in this chapter, for a list of IP "ports" which the RTI application uses. Your use of a personal firewall should not prohibit the use of the RTI application.

Protecting Modems:
PCI 12.3
It is also important to protect any dialup modem access to your RTI server. If you still employ the use of 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.

RTI Software Updates:
Occasionally, Teleflora will need to update your RTI system with critical security updates. Critical updates may be securely installed on your machine in either an automated or manual fashion. In the case of automated update, the "altiris" software will use a secure SSL connection to update your RTI system.
In the case of manual updates, 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.

It is important to note that, in the event that you refuse, or otherwise prevent these RTI software updates, the security, and hence, PCI compliance of your system could be at risk.

Other Servers:
PA-DSS 9.1
In the event that you choose to host an internet accessible server (such as a web server), PA-DSS compliance requires that your internet accessible server never be used to store cardholder data and be located on a network which is DMZ'ed from any server (e.g. your RTI server) which houses cardholder data. Furthermore, for any internet accessible server you create, you must never store cardholder data directly on these systems.

3rd Party Application Integration

Addresses:
PA-DSS 1.1.1
PA-DSS 1.1.2
PA-DSS 1.1.3

Your RTI Application server has been configured in a way to best ensure PA-DSS compliance. In order to maintain this level of secure integrity, Teleflora recommends against the modification of system configurations, or the installation of additional software on the RTI application server.

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

- Any 3rd party applications installed must never 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 RTI Application server. In the event that third party applications are added to the RTI application server which are capable of accessing RTI application data files, these applications must additionally conform to the PCI Data Security Standards. (3.x.y)

- In the event that any 3rd party applications produce 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.

Using a Remote RTI System

Addresses:
PA-DSS 10.1
PA-DSS 10.2
PA-DSS 10.3

PA-DSS 10.2 Remote access – Teleflora does not recommend the use of any type of remote access into the shop except the usage of GoToAssist. If a shop installs remote access then the florist must use a technology that meets PCI-DSS sections relating to connectivity including:

PCI-DSS v2.0

8.2 In addition to assigning a unique ID**,** employ at least one of the following methods to authenticate all users:
_ Something you know, such as a password or passphrase
_ Something you have, such as a token device or smart card
_ Something you are, such as a biometric

8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dialin service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.)
Note: *Two-factor authentication requires that two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one*

Remote Administration of an RTI System

Addresses:
PA-DSS 7.1
PA-DSS 11.3
PA-DSS 13.1

RTI Customer Service is capable of remotely administering your RTI server. Because of the security implications of remote administration, the following guidelines, as established in PCI DSS 8.1, 8.2, 8.3, 8.4 and 8.5 must be followed:

- Change any sensitive default settings (e.g. default usernames and passwords) for remote access devices such as firewalls. (PA-DSS 11.3.b)
- Only allow incoming internet connections from known hosts. (PA-DSS 11.3.b)
- Use token based authentication, and/or complex passwords for login authorization. (PA-DSS 11.3.b)
- Encrypt all data connections using SSH, VPN or SSL/TLS types of connections. (PA-DSS 13.1)
- Enable the automatic lockout of administrative accounts after a certain number of failed login attempts. (PA-DSS 11.3.b)
- The firewall device must have logging capabilities enabled. (PA-DSS 11.3.b)

(Note: For tips on router configuration, see "How to securely configure a wired router" in the appendix below.)

- Teleflora recommends remotely accessing the RTI Application server via a VPN (Virtual Private Network). In the event that a VPN is utilized to access the RTI application server, a unique, "per client" encryption certificate should be used, coupled with a strong password in order to access the VPN. Only VPNs using IPSEC, PPTP or 128 bit (or greater) SSL technologies may be used. (PA-DSS 11.3.b)

- Any dial-in modem(s) which provide the capability of remote administrative support must be turned off, or otherwise disabled, when not in use. (PA-DSS 10.1)

- The "tfsupport" Unix user account should be disabled during times when not in use. (PA-DSS 10.1)

- At any time, the 'tfsupport' Unix user account should be assigned a complex password as per PCI standard 8.5.8 – 8.5.15. (PA-DSS 11.3.b)

- "Two Factor Authentication" is required for any remote administrative access. (PA-DSS 11.2)

    - For RTI Application server support, Teleflora recommends the use of frequently rotated, password-protected, “ssh key pair” for any external administrative access into the RTI application server.
    - For remote administration of firewall devices, Teleflora recommends accessing the router device through a VPN which has been established with a “per-person” certificate and strong password.

- Any administrative user account must comply with PCI-DSS/PA-DSS Standards as dictated in section 8. Some (but not all) of those requirements are as follows:
    - Passwords must be at least 7 characters long, utilizing at least numbers and letters. (PCI 8.5.10)
    - All passwords must be changed every 90 days. (PCI 8.5.9)
    - A minimum of five (5) unique passwords must be used for each Unix user. (PCI 8.5.12)
    - After six (6) failed login attempts, the user account should be disabled for a minimum of thirty (30) minutes. (PCI 8.5.13)

- In the event that Teleflora administrative access is needed on the RTI Application server, Teleflora will use the “tfsupport” Unix User account and possibly thereafter, the “root” user account.

- Teleflora recommends that the “root” user account never be directly accessible remotely. Administrators should instead, log in as an account with “normal” user privileges, and then use the “sudo” utility to execute privileged commands.

- Any account on the RTI 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 an RTI application server, or transmit unencrypted sensitive data. Teleflora recommends the use of the “ssh” protocol for any remote administration of the RTI application server. (PA-DSS 13.1)

- Unencrypted protocols (such as HTTP or Telnet) must never be used to administer the RTI 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 periodically be checked 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)

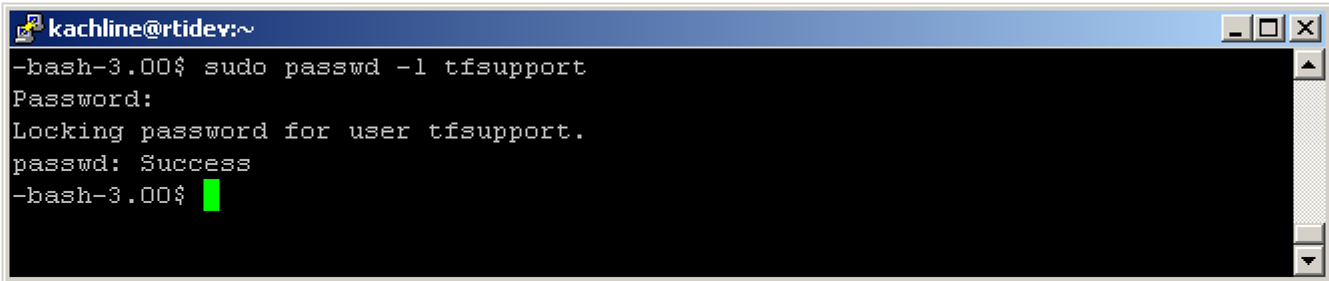
<u>Local Administration:</u>

- The RTI Application does not require “root” privileges to execute. Teleflora strongly recommends against running the RTI application as the “root” user, or any other user with “root” privileges.

- Administrative activities must be associated with individual persons. In the event that 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.

- In the event of termination, any administrator’s user account should be immediately disabled or removed from the RTI Application server. (PCI 8.5.4)

How to Enable/Disable the Teleflora Customer Service User Account



PA-DSS 10.1
PA-DSS 10.2
PA-DSS 10.3
RTI Customer service is capable of remotely administering your computer. Inbound connections occur via the secure “ssh” protocol, and are restricted only from the RTI customer service server. Logins are logged in /var/log/secure, but, the “last” command may also be used to obtain a history of logins.

Warning:

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

Disabling RTI Customer Service User Account:

1) Login as root
2) `sudo passwd –l tfsupport`

Enabling RTI Customer Service User Account:

1) Login as root
2) `sudo passwd –u tfsupport`

Identifying a login history for Customer Service:

1) `last tfsupport`

Updating your RTI Server

Operating System
PA-DSS 8
PA-DSS 10.3.1

Your RTI Server uses the Redhat Enterprise Linux environment. Redhat Enterprise Linux uses a tool called “up2date” to ensure that security patches are in place. RTI 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). With this, it is highly recommended that you enable (and leave enabled) all “auto-update” functionality of your Linux operating system.

To enable auto-updates of your Redhat Linux Operating System:
1) `sudo /sbin/chkconfig --level 3 rhnsd on`
2) `sudo /sbin/chkconfig --level 5 rhnsd on`
3) `sudo up2date`

Important:

It is important to note that Redhat Enterprise Linux requires an annual subscription fee in order to continue obtaining security updates. Until you have paid such fees (included if you have a current RTI Maintenance Plan), your system is not receiving security updates, and is cannot be considered PCI compliant.

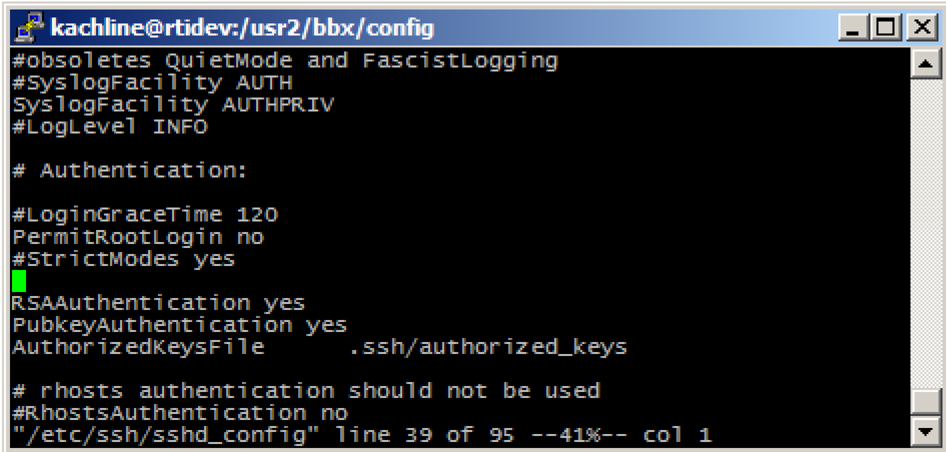
Application
PA-DSS 8
PA-DSS 10.3.1

The RTI application is automatically updated by Teleflora on an ongoing basis. (See Administrator’s Guide, Kaseya Software section)
If, for some reason, it is determined necessary to upgrade an RTI system “manually” (versus using the Kaseya tool), please contact Teleflora RTI Customer Support.

Process:
1) `Login to customer server`
2) `cd /tmp`
3) `sftp rtidev@sftp.teleflora.com`
    a. cd builds
    b. get RTI-x.y.z.iso.gz
    c. bye
4) `gunzip RTI-x.y.z.iso.gz`
5) `sudo mount –o loop RTI-x.y.z.iso /mnt/cdrom`
6) `cd /mnt/cdrom`

7) sudo ./install_rti.pl /usr2/bbx
    a. Wait for update to finish.
8) sudo umount /mnt/cdrom
9) sudo rm –f /tmp/RTI-x.y.z.iso

How to Configure your SSH Daemon



PA-DSS 11.1
Your RTI 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.

<u>Configuring SSHd:</u>

1) Login to your RTI server as an administrator.
2) sudo vi /etc/ssh/sshd_config
3) sudo /sbin/service sshd restart
4) logout

<u>Stopping SSHd:</u>

1) Login to your RTI Server as an administrator.
2) sudo /sbin/service sshd stop
3) logout

<u>Starting SSHd (Enabling Encrypted Data Transmission):</u>

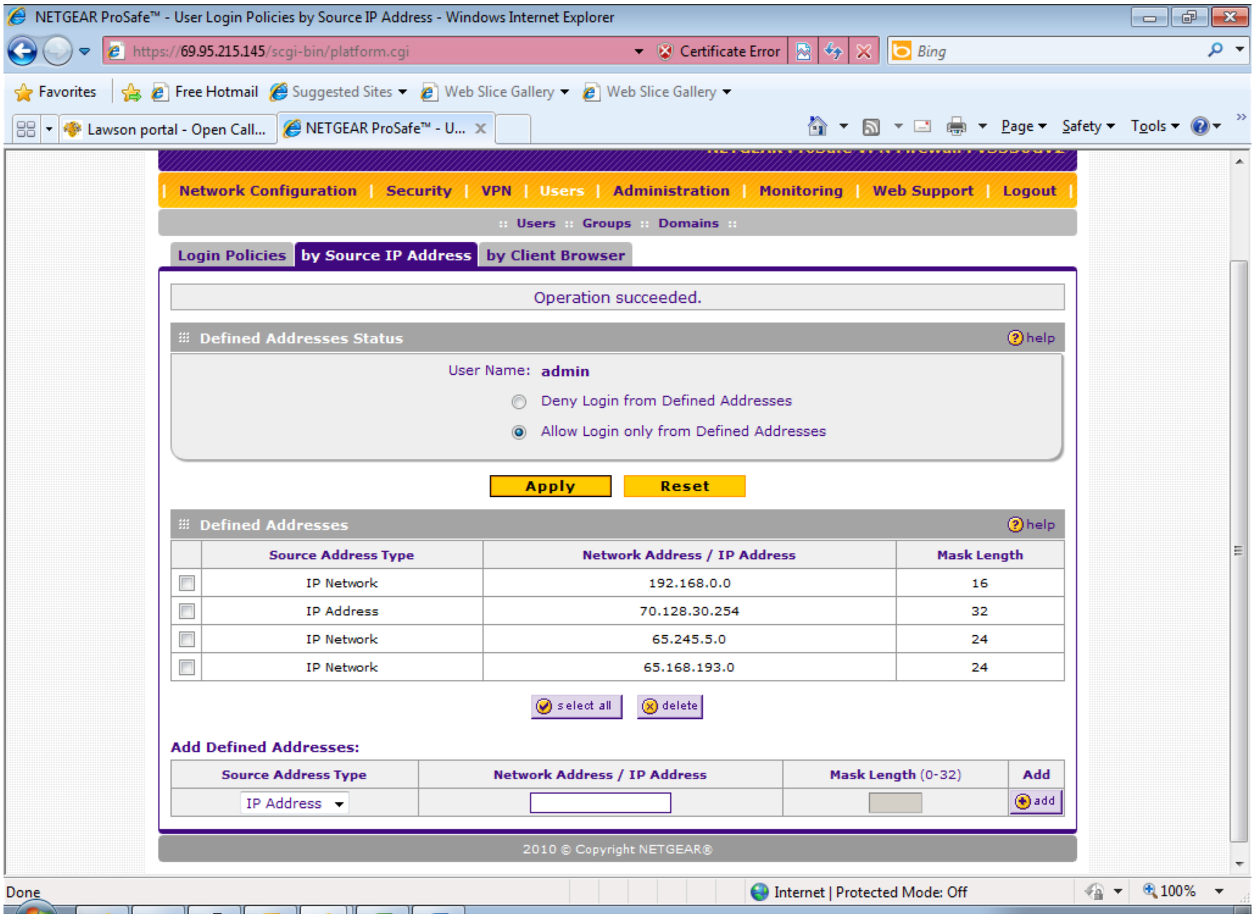
1) Login to your RTI Server as an administrator.
2) sudo /sbin/service sshd start
3) logout

WARNING:

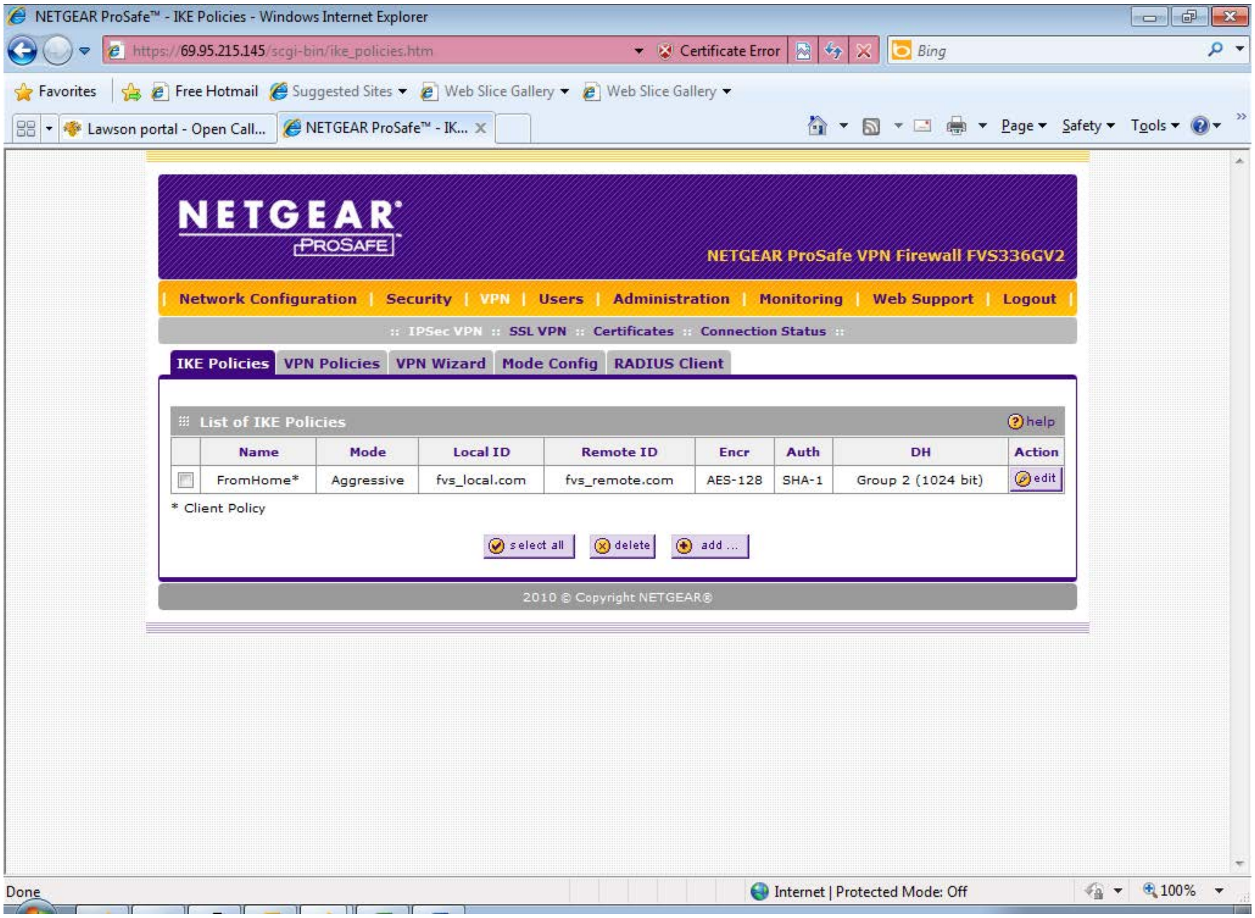
Improper configuration of sshd could enable serious security flaws, or, render your server inaccessible from remote hosts. Before making any changes, make sure you understand what you are changing. Refer to the man page on "sshd".

How to Securely Configure a Wired Network Router

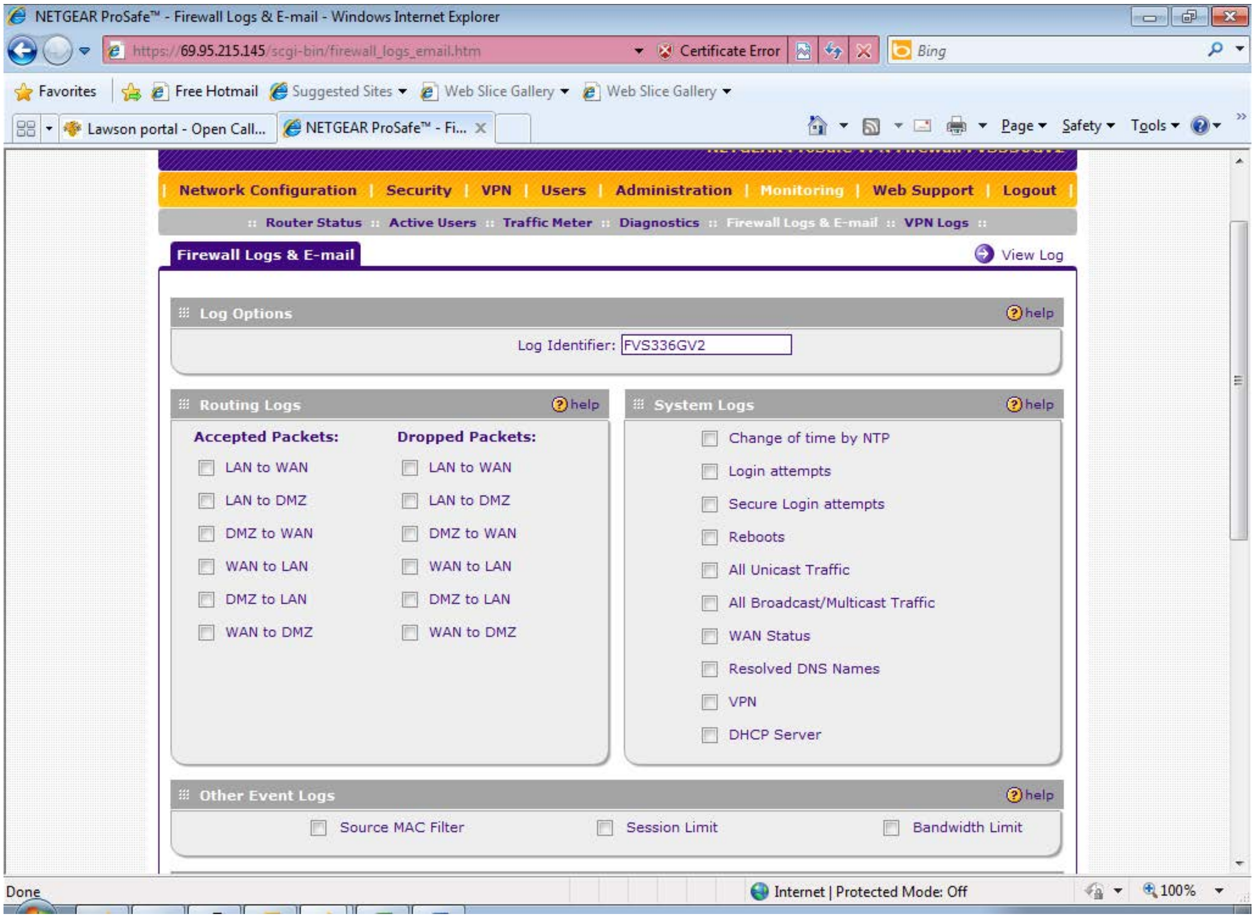
PA-DSS 11.1



- Change any sensitive default settings (e.g. default usernames and passwords) for remote access devices such as firewalls.
- Only allow incoming internet connections from known hosts.
- Enable the automatic lockout of administrative accounts after a certain number of failed login attempts.
- Use token based authentication, or complex passwords for login authorization.



- RTI Customer service must first establish a “VPN” connection before being able to connect to the RTI server.
- Encrypt all data connections.



- The firewall device must have logging capabilities enabled.

Encrypting over Public Networks

Addresses:
PA-DSS 12.1

In the event that a device such as a PC or laptop, are capable of connecting to the RTI 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.
For providing 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 RTI, use of the “telnet” protocol is absolutely not permitted for PCI compliance.

Emailing Cardholder Information

Addresses:
PA-DSS 11.2

Your RTI system will never send cardholder information via email, instant messaging, or any other “end-user messaging technology”. Furthermore, your RTI 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”, “IM”, or any other end-user messaging technologies as an implement 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 that your RTI system does have an internal “email” system built in for allowing intra-department communications. Despite its name, this “email” system does not use traditional internet “email” mechanisms, but instead, uses RTI database files for storing messages and their status. From a Credit Card compliance perspective, these “Email” boxes are not encrypted, thus, you must never send cardholder information via these internal “email” systems.

Accessing the RTI Application

Your RTI application relies on the underlying authentication mechanism of your Operating System in order to protect against unknown parties from accessing your system. It is therefore, important that you and your staff are aware of, and follow, the following guidelines:

PA-DSS 3.1
PCI 8.5.15

- On any workstation, a screensaver must be enabled which requires a password to unlock. The screen should automatically lock after 15 minutes of inactivity. See Appendix for direction on setting your local screensaver locks.

PA-DSS 3.1
PA-DSS 3.2
PCI 8.5.8
PCI 8.5.15

- Every user with administrative (Unix shell) access to the RTI server, or, any user who has the ability to view 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

- In the event that an RTI server user fails authentication six consecutive times, that user account should be automatically 'locked' for at least a duration of 30 minutes, or until an administrator manually unlocks the account (whichever occurs first)

PA-DSS 3.3
PCI 8.4

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

Kaseya Software

Kaseya is a third party software package which allows us to distribute RTI patches in a secure manner with a known "chain of trust".

Installing Kaseya

In order to provide a secure connection and prevent spoofing, the Kaseya client/server uses an https connection (SSL) to encrypt all traffic across the internet. Furthermore, to provide a level of authentication, Kaseya clients will verify the SSL certificate of the Kaseya server being used. Finally, when a Kaseya client is newly installed, the Kaseya Server administrator (Shannon Jackson in Paragould) must manually add your client to the active account list before the client can receive any transactions from the Teleflora Kaseya server.

To Install Kaseya:

- Obtain a copy of KcsSetup.sh from the sftp server
- Place KcsSetup.sh in /tmp on the clients server
- ./KcsSetup.sh
- Call Kaseya Administrator (Shannon Jackson, Paragould). Request your "Computer ID" be added to the active accounts list.

To Turn Off Kaseya:

- Login to customer's server
- sudo chkconfig kagent-TLFRLC38702197701560 off
- sudo service kagent-TLFRLC38702197701560 stop

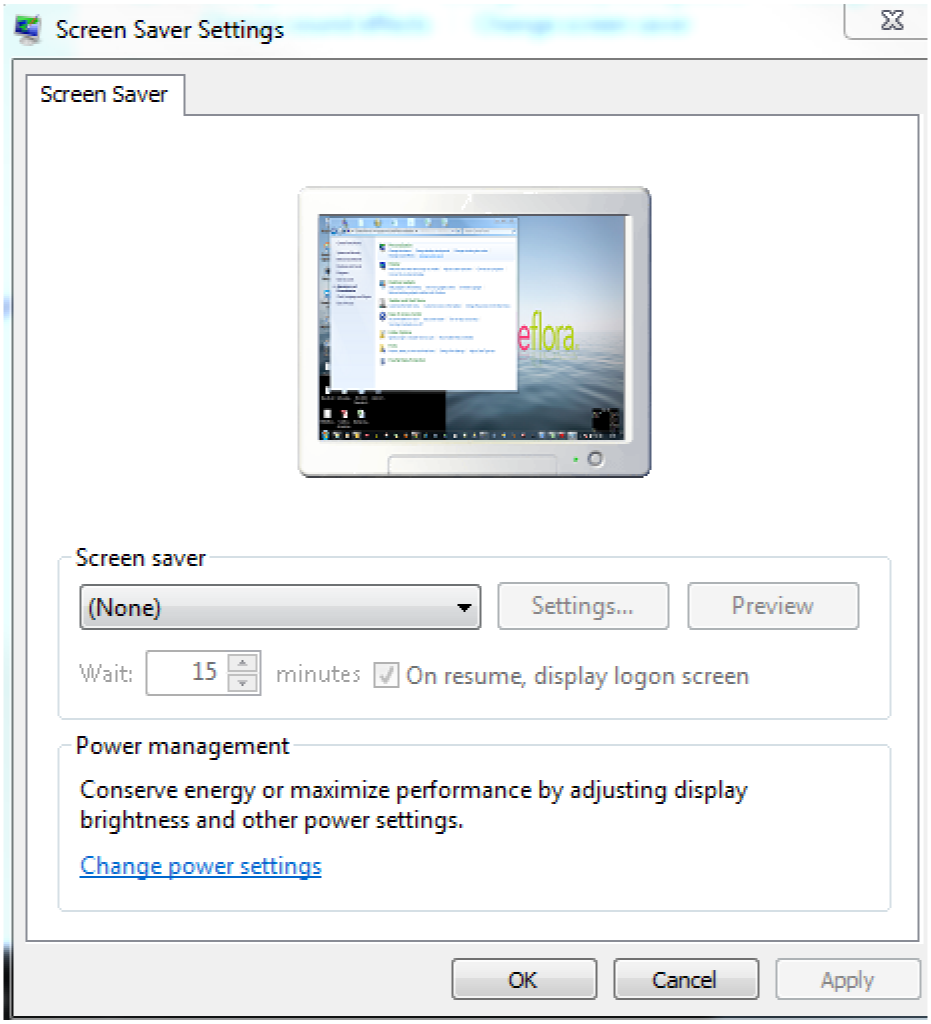
To Turn On Kaseya:

- Login to customer's server
- sudo chkconfig kagent-TLFRLC38702197701560 on
- sudo service kagent-TLFRLC38702197701560 start

WARNING:

The RTI system has the Kaseya client loaded by default. Any modifications or disabling of the service could enable serious security flaws, or, render your server inaccessible. Before making any changes, make sure you understand what you are changing. Please contact Teleflora before making any changes.

How to set a Screensaver Lock in Windows 7



PA-DSS 3.1

In order to be compliant with PA-DSS requirements, each workstation with access to the RTI application, 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) Navigate to Control Panel
3) Select "Appearance and Personalization"
4) Select "Change Screen Saver" under Personalization.
5) Put "15" (or less than 15) in the "Wait xx minutes" box.
6) Check the "On resume, password protect" box.
7) Click "OK" button.

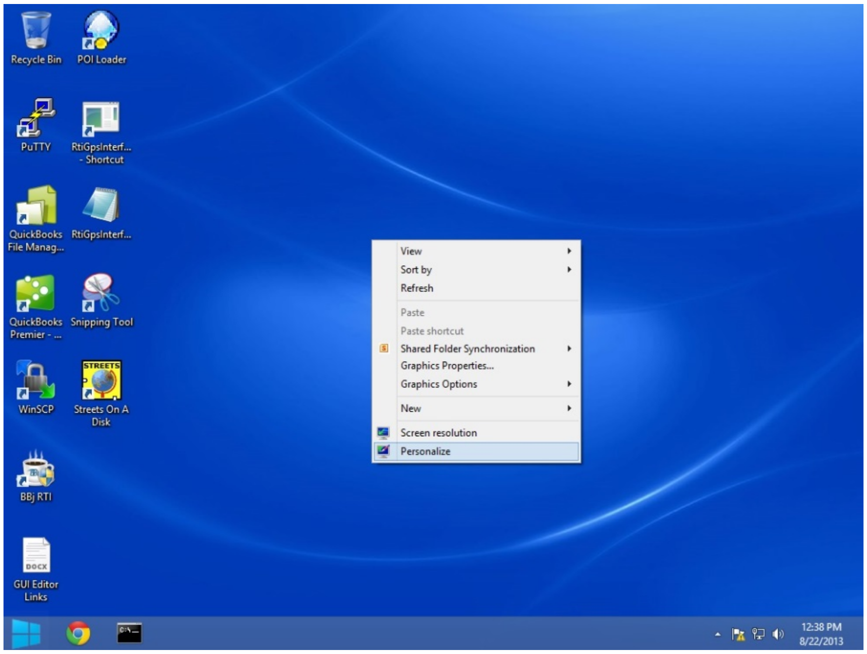
How to set a Screensaver Lock in Windows 8

PA-DSS 3.1
PCI 8.5.15

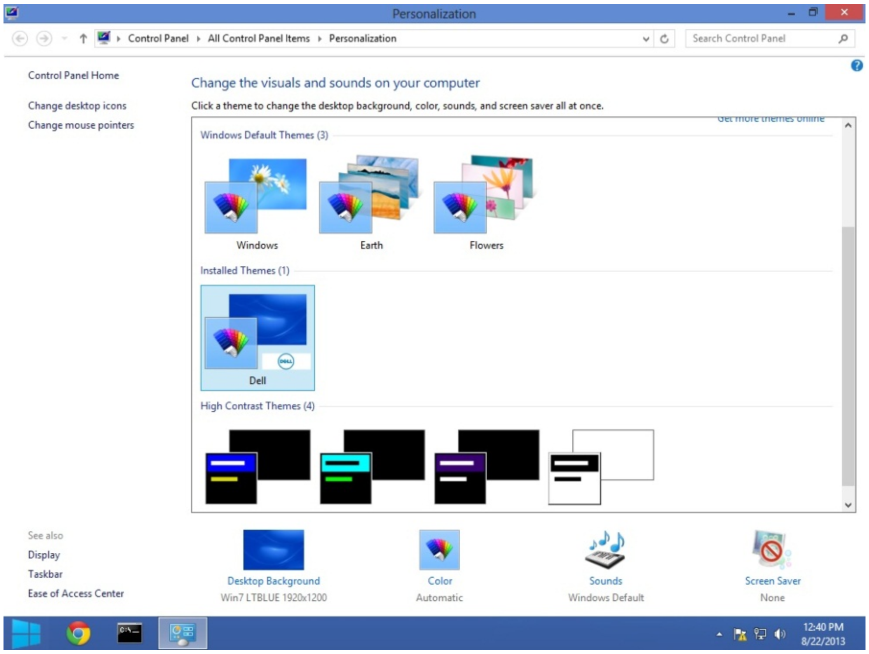
In order to be compliant with PA-DSS requirements, each workstation with access to the RTI application, must have a "locking" screensaver set. The Screensaver must "lock" (thus, require a password to unlock) after fifteen minutes of inactivity.

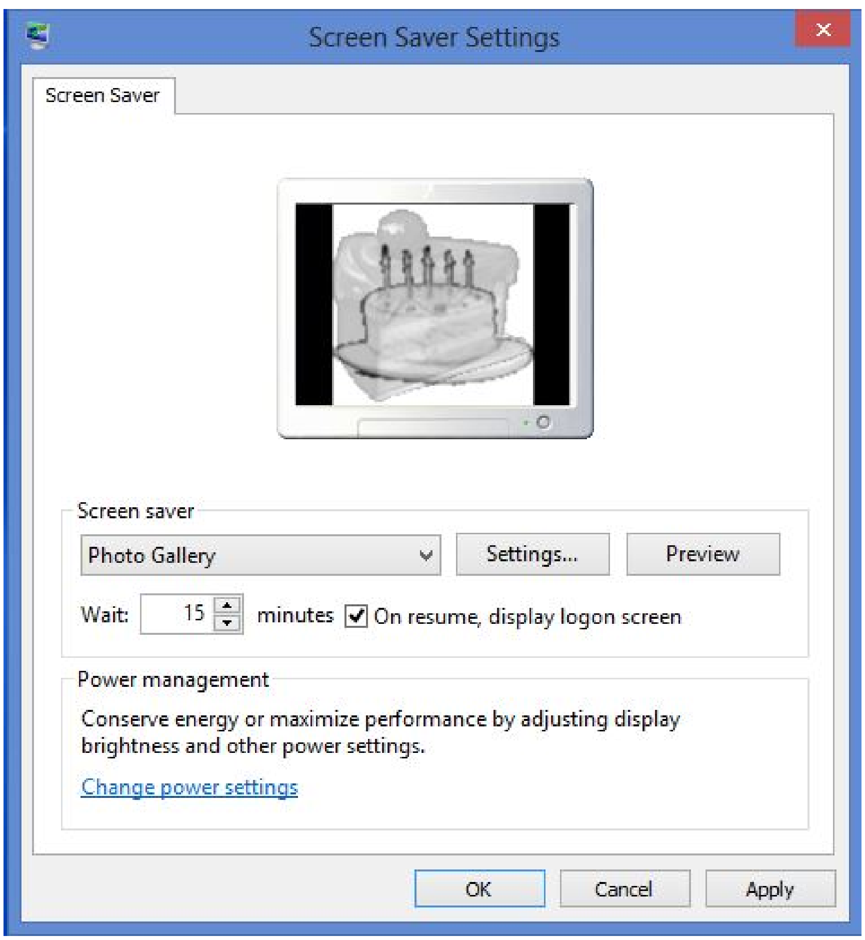
To ensure that a Screensaver lock is established, do as follows:

1) Log into Windows computer.
2) Right-click the desktop
3) Select the "Personalize" tab



4) Click on Screen Saver in the bottom corner.





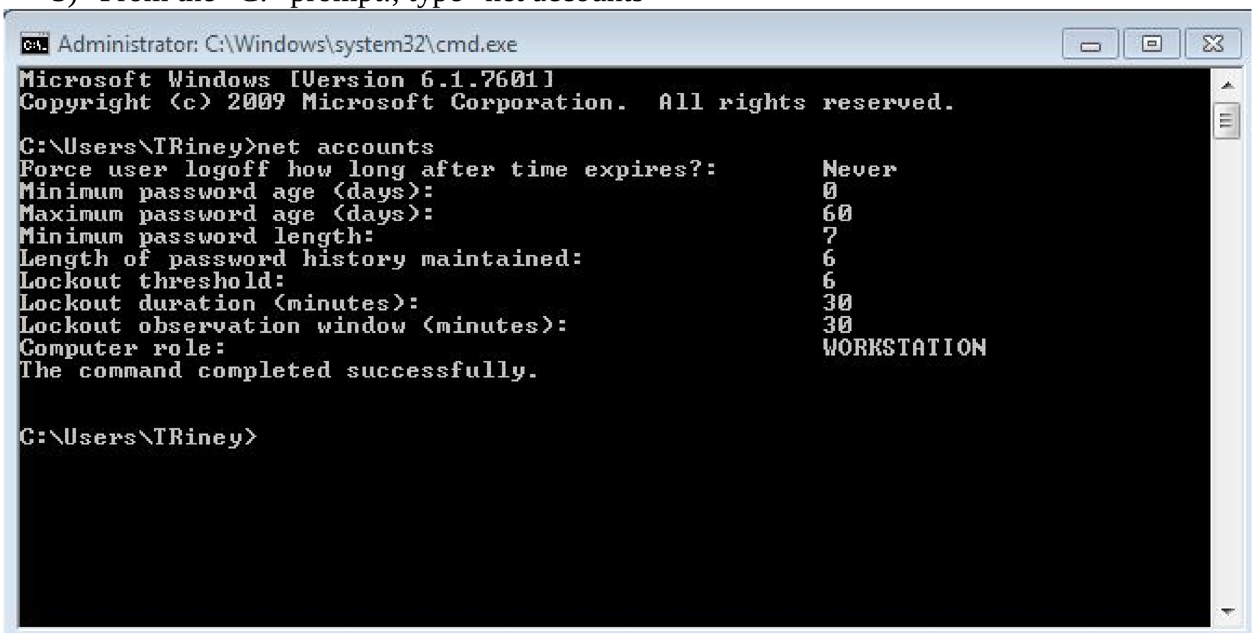
5) Put “15” (or less than 15) in the “Wait xx minutes” box.
6) Check the “On resume, password protect” box.
7) Click “OK” button.

Verifying/Setting Password Policy in Windows 7

PA-DSS 3.1
PA-DSS 3.2

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).

1) Start
2) Type cmd in the “Search programs and files” field and press enter.
3) From the “C:” prompt:, type “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.

To set the password policies:

Login to the Windows computer as an administrator.

PCI 8.5.9
C:> Net accounts /maxpwage:90

PCI 8.5.10
C:> Net accounts /minpwlen:7

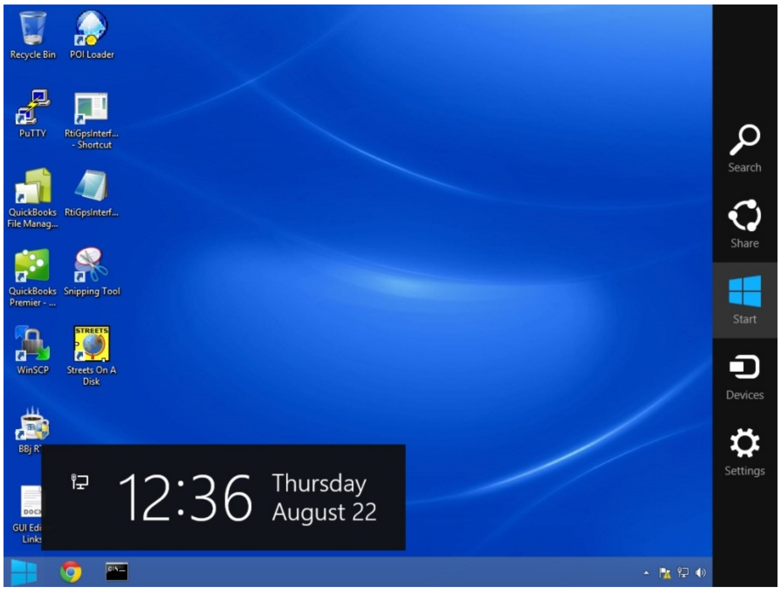
PCI 8.5.12
C:> Net accounts /uniquepw:4

Verifying/Setting Password Policy in Windows 8

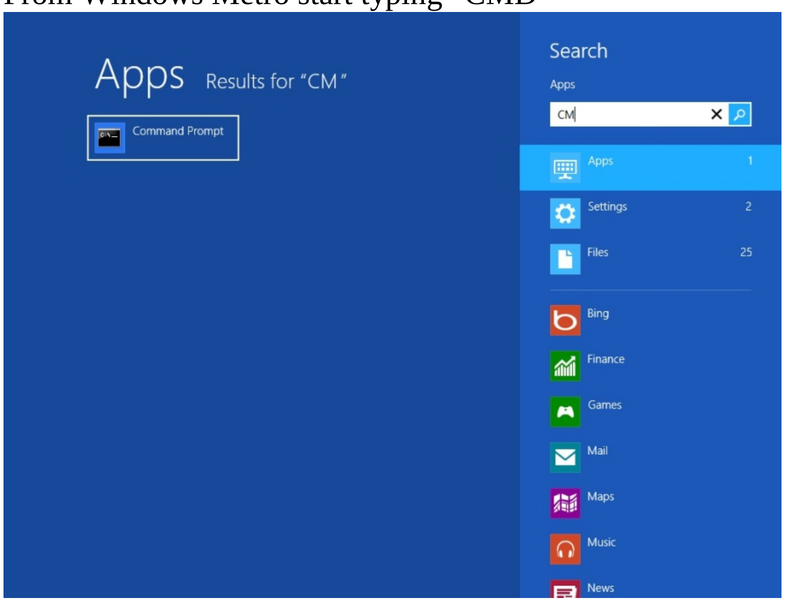
PCI 8.5

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).

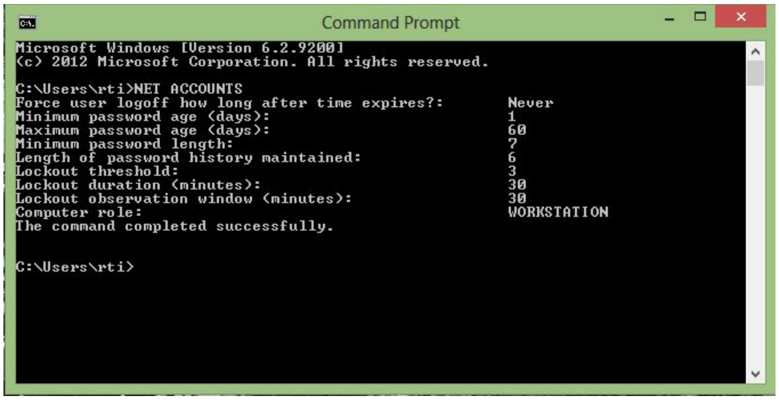
1. Start



2. From Windows Metro start typing "CMD"



3. Click on "Command Prompt"



4. Enter the command “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.

To set the password policies:

Login to the Windows computer as an administrator.

PCI 8.5.9
C:> Net accounts /maxpwage:90

PCI 8.5.10
C:> Net accounts /minpwlen:7

PCI 8.5.12
C:> Net accounts /uniquepw:4

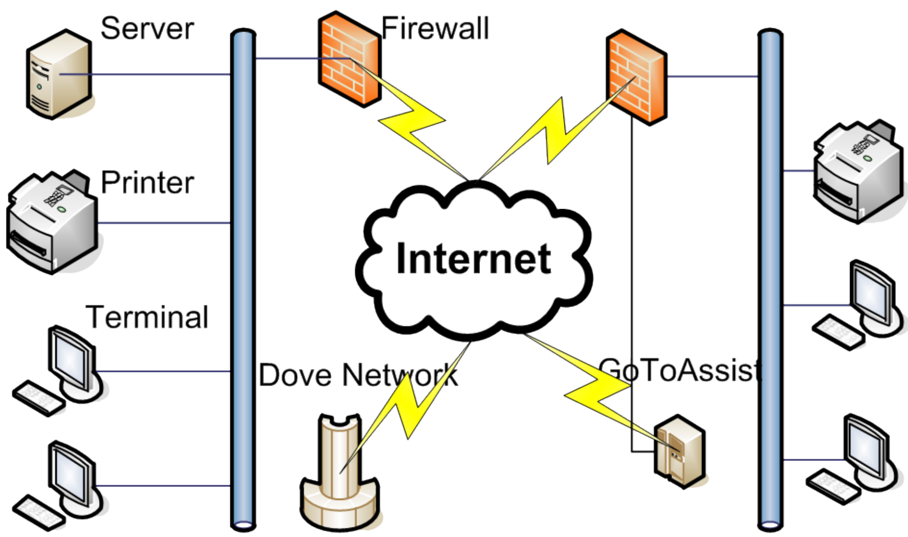
RTI Application Summary

PA-DSS Executive Summary

Software Vendor	Teleflora
Teleflora Contact Information:	RTI Support
Teleflora Mailing Address	3737 NW 34th St
	Oklahoma City, OK 73112
Product Name	RTI
Product Version	15
Recommended OS:	RHEL 6
Traditional Marketplace:	Retail Florist

Typical RTI Network Topology

PA-DSS Executive Summary



A typical RTI shop, on average, consists of one store with an average of twenty “terminals”, multiple network printers, an RTI server”, and a Firewall to the internet.
Larger implementations may have multiple, physical locations, all interconnected via a VPN. In all cases there is only a single RTI “Server” computer.

RTI Server
A Dell server running Redhat Linux. Houses core database of the application. The central point for communications between Terminals and external entities (such as the Dove Network and Elavon). There is only ever one of these servers in an RTI “environment”.

RTI Terminal
Windows PC (Windows recommended but not required) running SSH Terminal Emulation software offering <u>no</u> data storage, and connects to the RTI “Server” for all data communications via a secure SSH connection.

Printer
Small business class network printer, usually two 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 RTI 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.

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

Elavon
Elavon “SSL @dvantage” network interface. CC Swipes, PANs, and CVV are transmitted from the RTI Server, via an SSL encrypted connection. No CC information is transmitted from Elavon, to the RTI Server.