FTD MERCURY X2
IMPLEMENTATION GUIDE
FOR PA-DSS

FTD Mercury X2 Implementation Guide for PA-DSS

Last Updated: March 1, 2010
Last Reviewed: February 11, 2010

The purpose of this implementation guide is to explain how to implement FTD Mercury Point of Sale version X2 (10.2) in a PCI-DSS compliant fashion, which is one step for florists who are interested in achieving PCI compliance for their shop.

The implementation in this guide is only for a new FTD Mercury server; to implement FTD Mercury X2 in a PCI-DSS compliant manner, you must use a new server provided by FTD. (After you have transferred your database to the new server, you should destroy your original hard drive in a PCI-compliant manner.)

Any self-provided FTD Mercury client systems need to have antivirus software installed on them and maintained per PCI compliance guidelines. Computers provided by FTD include antivirus software.

CONFIGURING YOUR NETWORK

Your network must be behind a hardware firewall or a router with NAT translation (which acts as a hardware firewall). You also must change the default firewall or router password. Be sure to use a strong password (as detailed in PCI-DSS 8.5.10 and 8.5.11). Consult your firewall or router documentation to ensure you configure settings as appropriate in a PCI-DSS-compliant manner.

FTD Mercury does not require a wireless network to work. If you implement a wireless network, ensure it is implemented in a PCI-compliant manner. Best practices include:

- Changing the SSID of the wireless network to something other than the default and disable broadcast of the SSID.
- Changing the default channel for the network.
- Install and enable software firewalls on all computers accessing the wireless network.
- Use WPA (or better) encryption.
- Verify NAT translation is active on the wireless gateway.
- Verify SPI is enabled on the firewall.
- Ensure only necessary ports are enabled.

CONFIGURING WINDOWS ON THE FTD MERCURY SERVER

CONFIGURING PASSWORD POLICIES FOR THE SERVER

You must configure the local password policies for the server to ensure passwords meet PCI requirements described in the PCI-DSS. The following password policies must be met:

- Passwords must change every 90 days.
- Passwords require a minimum of seven characters and must contain both numeric and alphabetic characters.
- New passwords cannot be the same as any of the last four passwords used.
- Accounts must lock out after a maximum of 6 failed logon attempts. The lockout duration must be at least 30 minutes or until the account is manually reset.
- If the computer has been idle for more than 15 minutes, the screen must lock and require the user’s password to unlock the computer.

To configure password policies:

1. Click the **Windows Start** button, point to **Control Panel**, then to **Administrative Tools**, and then click **Local Security Policy**. The **Local Security Settings** window opens.
2. Double-click the **Security Settings** icon on the tree in the left pane.
3. Double-click the **Account Policies** folder.
4. Double-click the **Password Policy** folder.
5. Double click the **Enforce password history** policy. The **Enforce password history Properties** window opens.
6. Change the number of passwords remembered to **4** (or greater).
7. Click **OK**.
8. Double-click the **Maximum password age** policy. The **Maximum password age Properties** window opens.
9. Change the number of days for password expiration to **90 days** (or less).
10. Click **OK**.
11. Double-click the **Minimum password length** policy. The **Minimum password length Properties** window opens.
12. Change the minimum characters to **7** (or greater).
13. Click **OK**.
14. Double-click the **Password must meet complexity requirements** policy. The **Password must meet complexity requirements Properties** window opens.
15. Change the setting to **Enabled**. Note that the following complexity requirements will be in place:
    - The password cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters
    - The password must be at least six characters in length
    - The password must contain characters from three of the following four categories:
        - English uppercase characters (A through Z)
        - English lowercase characters (a through z)
        - Base 10 digits (0 through 9)
        - Non-alphanumeric characters (for example, !, $, #, %)
16. Click **OK**.
17. Double-click the **Account Lockout Policy** icon in the left pane.
18. Double-click the **Account lockout threshold** policy. The **Account lockout threshold Properties** window opens.
19. Change the number of invalid logon attempts to **6** (or less).
20. Click **OK**.
21. When the **Suggested Value Changes** window appears, click **OK**.
22. Verify that both the **Account lockout duration** policy and the **Reset account lockout counter after** policy now have security settings of **30 minutes**.
23. Close the **Local Security Settings** window.
24. Click the **Windows Start** button, point to **Control Panel**, and then click **Display**. The **Display Properties** window opens.
25. Click the **Screen Saver** tab.
26. In the **Screen saver** area, change the **Wait time** to **15 minutes** (or less).
27. Ensure the **On resume, password protect** check box is selected.
28. Click **OK**.
29.

DISABLING REMOTE DESKTOP

You must ensure the remote desktop functionality in Windows is disabled.

To disable remote desktop:

1. Log in to Windows using an account with administrative privileges.
2. Right-click on **My Computer** and select **Properties**. The **System Properties** window opens.
3. Click the **Remote** tab.
4. Ensure **Enable Remote Desktop on this Computer** is unchecked.
5. Click **Apply**.
6. Click **OK**.

CREATING A NEW ADMINISTRATOR ACCOUNT ON THE FTD MERCURY SERVER

You must create a new administrator account on the FTD Mercury server. This account should only be used for tasks that require administrator access on the server, and not for day-to-day operations.

To create an administrator account on the server:

1. Right-click on **My Computer** and select **Manage**. The **Computer Management** window opens.
2. On the **Action** menu, select **New User**.
3. Enter information about the user, including name, login name, and password. Be sure to use a strong password (as detailed in PCI-DSS 8.5.10 and 8.5.11).
4. Select the **User must change password at next login** option.
5. Click **Create**.
6. Double-click on the user you created.
7. Click the **Member Of** tab.
8. Click **Add**.
9. In the **Enter** the object names to select field, type **administrators**.
10. Click **OK**.
11. Click **OK** again.

This password is necessary for future upgrades to FTD Mercury. If you lose this password, FTD cannot recover it and there is a potential for data loss. You should limit access to the administrator account to as few people as possible.

ADDING USER ACCOUNTS ON THE FTD MERCURY SERVER

To add an account on the server:

1. Right-click on **My Computer** and select **Manage**. The **Computer Management** window opens.
2. On the **Action** menu, select **New User**.
3. Enter information about the user, including name, login name, and password. Be sure to use a strong password (as detailed in PCI-DSS 8.5.10 and 8.5.11).
4. Select the User must change password at next login at next login option.
5. Click Create.
6. Double-click on the user you created.
7. Click the **Member Of** tab.
8. Click **Add**.
9. In the **Enter** the object names to select field, type **users**.
10. Click **OK**.
11. Click **OK** again.

You must repeat this procedure for each person who will be using the FTD Mercury Server. If you fail to create unique logins for each user, you will be in violation of PCI-DSS requirements.

After you have created and configured all users for the FTD Mercury server, reboot log out of the system and log in using a login name and password you created.

IMPORTANT: Restrict access to the system as much as possible. Only provide user accounts to those who need them for their jobs, and only for as long as necessary. All user IDs, passwords, and authentication to the system should be done in a PCI-DSS compliant manner.

DISABLING DEFAULT ACCOUNTS ON THE FTD MERCURY SERVER

Once you have added and configured the new user accounts on the server, you need to change the passwords for the Admin, Administrator, and Florist users and then disable the accounts.

To change the passwords for the existing accounts and then disable the accounts:

1. Right-click on **My Computer** and select **Manage**. The **Computer Management** window opens.
2. Click **Local Users and Groups** to expand it, and then click **Users**.
3. Right-click on the **Admin** user and select **Properties**.
4. Change the password on the account. Be sure to use a strong password (as detailed in PCI-DSS 8.5.10 and 8.5.11).
5. Ensure the **Account is disabled** check box is selected.
6. Click **OK**.

Repeat this procedure for both the Administrator and Florist users.

RUNNING THE SETUP WIZARD

The FTD Mercury Setup Wizard allows you to configure some initial settings in FTD Mercury (enough to get you up and running so you can perform other FTD Mercury configurations).

To run the Setup Wizard and perform initial FTD Mercury configurations (if it is not already running, start at Step 1; otherwise, start at Step 4):

1. On the **Windows Start** menu, point to **All Programs**, then to **Accessories**, and click **Command Prompt**.
2. At the **C:** prompt, type **cd \wings**.
3. At the **C:\Wings** prompt, type **setupwizard /w**. The **FTD Mercury Setup Wizard** opens.
4. On the **Welcome** panel, click **Next**.
5. On the **Software License** panel, read the license agreement. You must scroll to the bottom of it to enable the **I Accept** button.
6. Click the **I Accept** button, and then click the **Next** button.
7. In the **Step 1: Company Information** panel, fill out the company information as instructed for the florist. Click **Next**.
8. In the **Step 2: Dial Prefix** panel, fill out the **Dial Prefix** as necessary. If you need to change the time settings, click the appropriate buttons to do so. Click **Next**.
9. In the **Step 3: Store Information** panel, enter your store information. If you select Canada for the country, select your province, enter your GST ID #, and the U.S. exchange rate.
10. When the **Wire Service Code** window opens, enter the FTD shop code and click **Add**. If there are additional codes to add, enter them and click **Add**. Once you have entered all codes, click **No More Codes**. Repeat for any additional wire services.
11. Click **Next**.
12. On the **License Keys** panel, click **Next**.
13. On the **Tax Rates** panel, enter the label for the tax rate in **Tax 1 Label**. Enter the sales tax for your state in the **State Sales Tax** labels. If this is a Canadian shop, you need to enter both the **Federal Tax** label and the **Provincial Tax** labels, plus the GST/HST tax percentage and PST tax percentage. If you are in a province where there is tax on tax, click the check box.
14. Click **Next**.
15. On the **Internet Settings** panel, in the **Account** tab, enter your account ID, account user ID, and account password in the appropriate fields. Re-enter your password in the **Confirm Password** field.
16. Click the **Host** tab and change settings as necessary.
17. Click the **ISP** tab.
18. In the **Internet Connection Type** are, select **Always Online**.
19. If you use a proxy sever, in the **Permanent** area, click the **Proxy Server Is Used** check box and then enter details about the proxy server.
20. Click **Finish**.

CONFIGURING FTD MERCURY ON THE FTD MERCURY SERVER

CHANGING THE ADMINISTRATOR PASSWORD

To change the administrator password for FTD Mercury:

1. Log into FTD Mercury using your existing FTD Mercury administrator password.
2. On the **FTD Mercury Main Menu**, click the **Tools** menu, and then click **Change Password**.
3. In the **FTD Server Password** window, in the **Login** field, enter admin as the login name.
4. In the **Old Password** field, enter the current password for the admin account.
5. In the **New Password** field, enter the new password for the admin account. Be sure to use a strong password.
6. In the **Confirm Password** field, re-enter the new password.
7. Click **Save**.
8. Close FTD Mercury and restart all instances of Mercury for changes to take effect.

You should change this password in accordance with PCI-DSS standards.

CONFIGURING DATA RETENTION

To configure the data retention period for FTD Mercury:

1. Double-click the **Mercury Administration** icon on the desktop.
2. At the **Login** window, enter your login name and password.
3. Click **OK**.
4. When Mercury Administration opens, double-click the **Store** folder.
5. Double-click the **General** icon. The **General** screen opens.
6. In the **Automatic Data Purge** area, set the number of months you want to retain customer data. (Consult your local taxing authority and/or accountant for guidance on your retention period.)
7. Click **Apply**.
8. Close Mercury Administration.

You will need to restart all instances of FTD Mercury for changes to take effect.

CONFIGURING USERS

CONFIGURING JOB FUNCTIONS

FTD Mercury uses job functions to set default access for new users. When you create a new user, you select a job function, and the user inherits window access based on the window access settings for that job function. You can then override the job function access as necessary for that particular user.

To modify default job function access:

1. Double-click the **Mercury Administration** icon on the desktop.
2. At the **Login** window, enter your login name and password.
3. Click **OK**.
4. When Mercury Administration opens, double-click the **Security** folder.
5. Double-click **Window Access**.
6. Select the job function you want to modify from the **Job Functions** list.
7. Select the window function you want to modify, and then select the individual windows to allow access (checking the **Access** check box provides access to that window for that job function). Repeat for all windows.
8. Click **Apply** to save your changes.

Repeat for any additional job functions.

If you need to create a new job function and set default window access for the new job function, you can also do so.

To create a new job function and configure window access for it:

1. Double-click the **Mercury Administration** icon on the desktop.
2. At the **Login** window, enter your login name and password.
3. Click **OK**.
4. When Mercury Administration opens, double-click the **Employee** folder.
5. Double-click **Job Functions**.
6. Right-click and select **New Job Function**.
7. Configure the job function access as necessary.
8. Click **Apply**.

Repeat for any additional job functions.

CREATING NEW USERS

Each user in FTD Mercury needs to have a unique user account. If you use shared accounts, you will be in violation of PCI-DSS guidelines.

To create a new user for FTD Mercury:

1. Double-click the **Mercury Administration** icon on the desktop.
2. At the **Login** window, enter your login name and password.
3. Click **OK**.
4. When Mercury Administration opens, double-click the **Employee** folder.
5. Double-click **Employees**.
6. Right-click in the screen, click **New** and select **Employee**.
7. When prompted “Do you want to add a new Employee?”, click Yes.
8. Double-click **New Employee**.
9. In the **Employee** screen, enter information about the new employee:
    a. In the **Name** field, enter the employee’s name.
    b. In the **Login Name** field, enter the employee’s login name.
    c. In the **Password** field, enter employee’s password. Be sure to use a strong password.
    d. In the **Confirm** field, re-enter the employee’s password.
    e. Ensure the **Active Status** box is checked.
    f. From the **Job Function** list, select the employee’s job function.
    g. The employee’s window access is inherited from the employee’s job function. If you want to give more or less access, change the access from the **Window Access** area.
10. Click **Apply**.
11. Close Mercury Administration.

You will need to restart all instances of FTD Mercury for changes to take effect.
Ensure passwords are changed in accordance with PCI-DSS 8.5.

SETTING AUDIT TRAIL SETTINGS

To set the audit trail settings for FTD Mercury:

1. Double-click the **Mercury Administration** icon on the desktop.
2. At the **Login** window, enter your login name and password.
3. Click **OK**.
4. When Mercury Administration opens, double-click the **Security** folder.
5. Click **Audit Trail**. The **Audit Trail** screen opens.
6. Ensure all boxes are checked for both customers and orders.
7. Click **Apply**.
8. Close Mercury Administration.

You will need to restart all instances of FTD Mercury for changes to take effect.

CONFIGURING WINDOWS ON FTD MERCURY CLIENTS

You must perform each of these procedures on every FTD Mercury client.

CONFIGURING PASSWORD POLICIES FOR THE SERVER

You must configure the local password policies for the server to ensure passwords meet PCI requirements described in the PCI-DSS. The following password policies must be met:

- Passwords must change every 90 days.
- Passwords require a minimum of seven characters and must contain both numeric and alphabetic characters.
- New passwords cannot be the same as any of the last four passwords used.
- Accounts must lock out after a maximum of 6 failed logon attempts. The lockout duration must be at least 30 minutes or until the account is manually reset.
- If the computer has been idle for more than 15 minutes, the screen must lock and require the user's password to unlock the computer.

To configure password policies:

1. Click the **Windows Start** button, point to **Control Panel**, then to **Administrative Tools**, and then click **Local Security Policy**. The **Local Security Settings** window opens.
2. Double-click the **Security Settings** icon on the tree in the left pane.
3. Double-click the **Account Policies** folder.
4. Double-click the **Password Policy** folder.
5. Double click the **Enforce password history** policy. The **Enforce password history Properties** window opens.
6. Change the number of passwords remembered to **4** (or greater).
7. Click **OK**.
8. Double-click the **Maximum password age** policy. The **Maximum password age Properties** window opens.
9. Change the number of days for password expiration to **90 days** (or less).
10. Click **OK**.
11. Double-click the **Minimum password length** policy. The **Minimum password length Properties** window opens.
12. Change the minimum characters to **7** (or greater).
13. Click **OK**.
14. Double-click the **Password must meet complexity requirements** policy. The **Password must meet complexity requirements Properties** window opens.
15. Change the setting to **Enabled**. Note that the following complexity requirements will be in place:
    - The password cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters
    - The password must be at least six characters in length
    - The password must contain characters from three of the following four categories:
        - English uppercase characters (A through Z)
        - English lowercase characters (a through z)
        - Base 10 digits (0 through 9)
        - Non-alphanumeric characters (for example, !, $, #, %)
16. Click **OK**.
17. Double-click the **Account Lockout Policy** icon in the left pane.
18. Double-click the **Account lockout threshold** policy. The **Account lockout threshold Properties** window opens.
19. Change the number of invalid logon attempts to **6** (or less).
20. Click **OK**.
21. When the **Suggested Value Changes** window appears, click **OK**.
22. Verify that both the **Account lockout duration** policy and the **Reset account lockout counter after** policy now have security settings of **30 minutes**.
23. Close the **Local Security Settings** window.
24. Click the **Windows Start** button, point to **Control Panel**, and then click **Display**. The **Display Properties** window opens.
25. Click the **Screen Saver** tab.
26. In the **Screen saver** area, change the **Wait time** to **15 minutes** (or less).
27. Ensure the **On resume, password protect** check box is selected.
28. Click **OK**.

DISABLING REMOTE DESKTOP

You must ensure the remote desktop functionality in Windows is disabled.

To disable remote desktop:

1. Log in to Windows using an account with administrative privileges.
2. Right-click on **My Computer** and select **Properties**. The **System Properties** window opens.
3. Click the **Remote** tab.
4. Ensure **Enable Remote Desktop on this Computer** is unchecked.
5. Click **Apply**.
6. Click **OK**.

ADDING USER ACCOUNTS ON A FTD MERCURY CLIENT

To add an account on a client:

1. Right-click on **My Computer** and select **Manage**. The **Computer Management** window opens.
2. On the **Action** menu, select **New User**.
3. Enter information about the user, including name, login name, and password. Be sure to use a strong password (as detailed in PCI-DSS 8.5.10 and 8.5.11).
4. Select the **User must change password at next login** option.
5. Click **Create**.
6. Double-click on the user you created.
7. Click the **Member Of** tab.
8. Click **Add**.
9. In the **Enter the object names to select** field, type **users**.
10. Click **OK**.
11. Click **OK** again.

You must repeat this procedure for each person who will be using the FTD Mercury client. If you fail to create unique logins for each user, you will be in violation of PCI-DSS requirements.

For full audit traceability and PCI compliance, users should not share accounts on the computer.

After you have created and configured all users for the FTD Mercury client, log out of the system and log in using a login name and password you created.

DISABLING DEFAULT ACCOUNTS ON A FTD MERCURY CLIENT

Once you have added and configured the new user accounts on the client, you need to change the passwords for the Admin, Administrator, and Florist users and then disable the accounts.

To change the passwords for the existing accounts and then disable the accounts:

1. Right-click on **My Computer** and select **Manage**. The **Computer Management** window opens.
2. Click **Local Users and Groups** to expand it, and then click **Users**.
3. Right-click on the **Admin** user and select **Properties**.
4. Change the password on the account. Be sure to use a strong password (as detailed in PCI-DSS 8.5.10 and 8.5.11).
5. Ensure the **Account is disabled** check box is selected.
6. Click **OK**.

Repeat this procedure for both the Administrator and Florist users.

ADDING SITES TO YOUR WHITE LIST

In accordance with PCI requirements, you will need to add the following URLs to your white list of sites that your computers can access:

- ftd.com
- ftdi.com
- ftdflorists.com
- ftdfloristsonline.com
- ftdflowerexchange.com
- floristwiki.ftdi.com
- mercurynetwork.com
- folmail.com
- ftdimarketplace.com
- ftdflorist.com
- myfolsite.com
- myftdsite.com
- symantecliveupdate.com
- s3.amazonaws.com
- constantcontact.com
- verisign.com

PA-DSS & UPDATE CDS/DVDS

When you receive an update CD or DVD from FTD, including but not limited to product updates, the FTD Florist Directory, or Centrus Address Verification updates, you must authenticate the CD or DVD as coming from FTD. This is done via the Automatic Software Updates feature, which is included with FTD Mercury X2.

IMPORTANT: Each CD or DVD from FTD must be authenticated to maintain compliance with PCI guidelines. If you receive more than one copy of a CD (for example, if you receive extra program CDs to facilitate installing upgrades on multiple clients more quickly), you need to authenticate each physical CD.

To check for authenticity of an upgrade CD or DVD you receive:

1. Put the CD or DVD into your drive.
2. Cancel out of any installation that may start automatically.
3. Double-click the Automatic Software Update icon in the system tray.
4. Click the Verify FTD Media button.

If Automatic Software Updates determines the CD or DVD is valid, you will be prompted to continue with the installation. If validation of the CD or DVD fails, the program will inform you the update is not authentic and you should contact Mercury Technology Support and then destroy the CD or DVD.

SPECIFIC PA-DSS REQUIREMENTS

PA-DSS REQUIREMENT 1

Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2), or PIN block data.

FTD Mercury does not store sensitive authentication data (including track 1 and 2 information). FTD Mercury neither uses nor stores CVV information. All PIN data for debit transactions (only provided for Canadian systems) are handled by the debit pin pad (VeriFone SC 500 Series PINpad).

FTD Mercury log files are only stored for 7 days, and do not include any sensitive data. You should retain log files per your PCI retention policy; you need to copy and save the following log files each week to ensure you have at least a year's worth of log files (to conform with PCI DSS requirements).

The following log files are located in the C:\Wings folder:

- MercuryAdminMonday.log
- MercuryAdminTuesday.log
- MercuryAdminWednesday.log
- MercuryAdminThursday.log
- MercuryAdminFriday.log
- MercuryAdminSaturday.log
- MercuryAdminSunday.log

The Mercury log files are located in the C:\Wings\Database folder. Seven of them are retained (one for each day of the week). On the eighth day, the first log is removed. The log files are named using the following format:

Mercury_Log_db_yyyyMMddhhmm.bak (yyyy is year, MM is month, dd is date, hh is hour, and mm is minute).

If required, you can enable and disable verbose logging in FTD Mercury. Keep in mind that this significantly increases the size of the log files. You turn on this expanded logging in three files: Client.ini, Server.ini, and Mercury.xml (all located in the C:\Wings folder).

To enable logging in Client.ini:

1. Open **Client.ini** using a text editor.
2. In the **[Preferences]** section, ensure **Log Networking=YES**.
3. Save the file.

To enable logging in Server.ini:

1. Open **Server.ini** in a text editor.
2. In the **[Logging]** section, ensure **Debug=YES**.
3. Save the file.

To enable logging in Mercury.xml:

1. Open **Mercury.xml** in a text editor.
2. Uncomment the line that currently reads **<!-- <level value="ALL" /> -->**. You can do this by removing the **<!--** and **-->** from the beginning and end of the line.
3. Save the file.

You may also need to retain Windows user logs and SQL server logs for your backups. Consult Microsoft documentation for instructions on accessing and saving these logs. See http://technet.microsoft.com/en-us/library/bb418937.aspx for details on SQL server logs; see http://technet.microsoft.com/en-us/library/dd349798%28WS.10%29.aspx and http://support.microsoft.com/kb/308427 for details on Windows user logs and Event Viewer.

IMPORTANT: Restrict access to the system as much as possible. Only provide user accounts to those who need them for their jobs, and only for as long as necessary. All user IDs, passwords, and authentication to the system should be done in a PCI-DSS compliant manner.

PA-DSS REQUIREMENT 2

Protect stored cardholder data.

Credit card data is not stored in FTD Mercury X2.

PA-DSS REQUIREMENT 3

Provide secure authentication features.

To protect data, secure authentication tools and practices are necessary.

- Default administrative account passwords must not be used for FTD Mercury.
- To run FTD Mercury, during installation the implementation specialist will configure a non-administrative account with a custom password.
- Although FTD Mercury is configured not to use the administrative account, you should always change the default password for the administrative account.

Any changes to use the administrator account for running FTD Mercury or returning to default passwords for Windows will result in non-compliance with PCI-DSS requirements.

IMPORTANT: Restrict access to the system as much as possible. Only provide user accounts to those who need them for their jobs, and only for as long as necessary. All user IDs, passwords, and authentication to the system should be done in a PCI-DSS compliant manner.

PA-DSS REQUIREMENT 4

Log payment application activity.

Payment activity is logged via the Audit Trail feature in FTD Mercury.

To view activities customer-related activities:

1. On the **FTD Mercury Main Menu**, in the **Search** area, click **Customer**. The **Customer Search** window opens.
2. In the **Customer Search** window, enter criteria to locate the customer and click **Search**.
3. From the results list, double-click the customer. The **Customer Detail Information** window opens.
4. Click the **Life Cycle** tab.

All logged information for the customer is displayed under the Life Cycle tab.

To view order-related activities:

1. On the **FTD Mercury Main Menu**, in the **Search** area, click **Ticket**. The **Ticket Search** window opens.
2. In the **Ticket Search** window, enter criteria to locate the ticket and click **Search**.
3. From the results list, double-click the order. The **Order Entry** window opens for the ticket.
4. Click the **Status** button. The **Ticket Status** window opens.

All logged information for the order is displayed in the Ticket Status window. This information is read-only.

IMPORTANT: If you disable Audit Trail functionality using Mercury Administration, you will no longer be in compliance with PCI DSS requirements.

PA-DSS REQUIREMENT 6

Protect wireless transmissions.

FTD Mercury does not require a wireless network to work. If you implement a wireless network, ensure it is implemented in a PCI-compliant manner. Best practices include:

- Changing the SSID of the wireless network to something other than the default and disable broadcast of the SSID.
- Changing the default channel for the network.
- Install and enable software firewalls on all computers accessing the wireless network.
- Use WPA (or better) encryption.
- Verify NAT translation is active on the wireless gateway.
- Verify SPI is enabled on the firewall.
- Ensure only necessary ports are enabled.

PA-DSS REQUIREMENT 10

Facilitate secure remote software updates.

Software updates for FTD Mercury patches and Centrus Address Verification are accomplished via automatic software updates. Updates are always initiated by FTD Mercury and never by FTD personnel.

Updates on physical media (CDs or DVDs) require the use of a verification feature in Automatic Software Updates to authenticate the media as coming from FTD.

PA-DSS REQUIREMENT 11

Facilitate secure remote access to payment application.

Mercury Technology support personnel use a client-initiated remote connection with commercially available software when it is necessary for FTD support specialists to access a customer’s FTD Mercury system. This software requires a unique PIN that is created only at the time of connection. Further, the connection is always initiated by the customer, and never by FTD support personnel.

If you access your own system remotely, PCI DSS guidelines require two-factor authentication. Typically, two-factor authentication requires two of three ways to prove your identity: something you know, such as a password or PIN, something you have, such as a token or certificate, and something you are (a fingerprint or other biometric-based tool).

PA-DSS REQUIREMENT 12

Encrypt sensitive traffic over public networks.

FTD Mercury transmits data over secure socket layers (SSL).

Customers are strongly discouraged from installing any messaging technology that sends “in the clear” communications (GoogleTalk, AOL Instant Messenger, etc.) on the FTD Mercury server, and customers especially should not send any credit card information using any “in the clear.”

PA-DSS REQUIREMENT 13

Encrypt all non-console administrative access.

FTD Mercury does not provide any non-console administrative access.