Setting Up PCI Compliance

The responsibility to delete any sensitive authentication data kept by the system lies with both the merchant and the reseller. Removal of this prohibited historical data is necessary for PCI compliance. Collecting sensitive authentication data should be done only when it is essential to solving a specific problem.

Objectives

- PCI Flag Server Setup
- Credit Card Encryption
- Activating PCI Flags

PCI Flag Server Setup

To guarantee the secure use, storage, and transmission of cardholder data, follow these steps for best industry practice. The first step is to ensure you have role-based security set up.

Performing the PCI Flag Server setup procedure requires role-based security and checking if the Admin and System roles have high-security bits *14, 91, 506, 689,691, and 757* turned on. *For more information on assigning Role-Based Security, refer to the Role-Based Security for PCI course in Epicor Learning.*

Verify the *Secure Shell (SSH)* plug is installed and turned on in the RF guns. If not, you must download, install, and configure TelnetCE to use *Secure Shell (SSH).* Refer to the document attached to this course for more information on how to configure TelnetCE. You do not need to install *Secure Shell (SSH)* if using Eagle Mobile on your RF Gun.

Now, check if any Price Checkers are using RF. If yes, ensure your price checkers are capable of *Secure Shell (SSH).*
Otherwise, replace the price checkers.

Next, set the server's IP address and ensure that the server is running on *Secure Access* rather than *Network Access.* From the *Home* page, select *Network Access.*

Select *Options* and then choose *Network.* In the *Host 1* field, enter the IP address of the Eagle server. If you do not know your Eagle Server's IP address, check *Internet Security Services (ISS).*

Check these three boxes. In the Login ID box, enter M. Leave the password field blank. Finally, click Ok. Once you enable the PCI flag, *Secure Access* will open automatically in place of *Network Access*. You must switch all PCs using *Network Access* to *Secure Access*.

Credit Card Encryption

Credit card encryption is a set of security measures that, when implemented, significantly lowers the likelihood that hackers can steal sensitive and priceless card information. It is best practice to set the option for keeping credit card data in *QuickRecall* to 180 days or less. Assigning this time period will purge any *Credit Card* information older than the date.

To set this option, enter *OPT* in the *Launch* bar. Select *ID* and enter *311* in the *Option ID* field. Click *OK.* Make sure the current value is *180.* To save the changes, select *Change.*

You must next truncate the credit card number or encrypt it in *Quick Recall.* If you truncate the number, the system removes the middle eight digits of the credit card number, and you cannot see the whole number. To encrypt the number, from the *Home* page, select *Network Access.* Now, log in with *Osprey.*

In the *Osprey main menu*, enter *QRCCC.* In the action prompt, enter *E* or *T* and then *E*
Note: You can still see the number if you have the decryption key.

Now, let us set *Option ID 8965* to *D.* This ensures the system does not write trace logs to the PC.
Enter *OPT* in the Launch bar from the *Home* page. Select *ID.*

In the *Option ID,* enter *8965* and click *OK.* Select the *Option D.* For *Option ID 561*, change the number in the Current Value column to 900. This activates the time-out timer.

Now, you need to set *Modify Terminal Record (MTR)* to ask for the username and password for each terminal. Also ensure the default user is not assigned high-security bits. In *Option Configuration,* select *ID.*

In the *Option ID* field, enter *520.* Click OK. Change the *Current value* of Option ID 520 to *S.*

Set the *Current value* of Option ID 1098 and 1099 to Yes. Finally, select Change to save all the updates.

Activating PCI Flags

After setting up the PCI flag server and credit card encryption, let's look at how to enable the PCI flag. To indicate that your system is *Payment Application Data Security Standard* (PA-DSS) compliant, you must set option ID *1061* to Yes. This option is password controlled.

In the *Option Configuration* page, Select *ID.* In the *Option ID* field, enter *1061* and click OK. Select *MISC.*

Choose *Restore Highlighted Option to Factory Default.* Click *Change* to save. It is best practice to perform these steps before opening or after closing so that you can reboot the server immediately.

Now, let's see how to reboot the *Eagle Server.* Confirm that no one else is using the system before rebooting the system. From the *Home* page, select *Network Access.* In the Network Access prompt, enter *OSPREY* in the *eagle login.* In the password field, enter *AVATAR.*

Select *Reboot the system* or in the Selection field, type *REBOOT* and press enter. Enter *E* to reboot the server. Next, it is best practice to restart all PCs to ensure the *Secure File Transfer Protocol (SFTP) and Secure Shell (SSH)* are set correctly.

Now, re-download offline POS.

You must execute Create Offline Refresh (COR) every night to get the most up-to-date information. To manually execute Create Offline Refresh (COR), enter *COR* in the *Launch* bar.

If you have multiple stores, ensure an asterisk (*) is in the *Store* field. Click *Run.*
Note: Create Offline Refresh can take time to complete. It must finish before updating offline files.

You can view Create Offline Refresh progress by entering *QUE* in the *Launch* bar. Click KPad+ until the Create Offline Refresh process completes.

When Create Offline Refresh finishes, select Scheduler at the bottom of the screen. Select the *Full Update* column and click *Run Now*. When the process completes, minimize the Scheduler at the bottom of the screen.
This completes the process for Activating PCI Flags.

Recap

Now that you've made the necessary preparations for the payment card industry, you can delete the sensitive authentication data previously stored in your system.

The contents of this document are for informational purposes only and are subject to change without notice. Epicor Software Corporation makes no guarantee, representations or warranties with regard to the enclosed information and specifically disclaims, to the full extent of the law, any applicable implied warranties, such as fitness for a particular purpose, merchantability, satisfactory quality or reasonable skill and care. This document and its contents, including the viewpoints, dates and functional content expressed herein are believed to be accurate as of its date of publication. The usage of any Epicor software shall be pursuant to the applicable end user license agreement and the performance of any consulting services by Epicor personnel shall be pursuant to applicable standard services terms and conditions. Usage of the solution(s) described in this document with other Epicor software or third party products may require the purchase of licenses for such other products. Epicor, the Epicor logo, and are trademarks of Epicor Software Corporation, registered in the United States and other countries. All other marks are owned by their respective owners. Copyright © 2021 Epicor Software Corporation. All rights reserved.

About Epicor

Epicor Software Corporation drives business growth. We provide flexible, industry-specific software that is designed around the needs of our manufacturing, distribution, retail, and service industry customers. More than 40 years of experience with our customers' unique business processes and operational requirements is built into every solution—in the cloud, hosted, or on premises. With a deep understanding of your industry, Epicor solutions spur growth while managing complexity. The result is powerful solutions that free your resources so you can grow your business. For more information, connect with Epicor or visit www.epicor.com.

epicor

Corporate Office
804 Las Cimas Parkway
Austin, TX 78746
USA
Toll Free: +1.888.448.2636
Direct: +1.512.328.2300
Fax: +1.512.278.5590

Latin America and Caribbean
Blvd. Antonio L. Rodriguez #1882 Int. 104
Plaza Central, Col. Santa Maria
Monterrey, Nuevo Leon, CP 64650
Mexico
Phone: +52.81.1551.7100
Fax: +52.81.1551.7117

Europe, Middle East and Africa
No. 1 The Arena
Downshire Way
Bracknell, Berkshire RG12 1PU
United Kingdom
Phone: +44.1344.468468
Fax: +44.1344.468010

Asia
238A Thomson Road #23-06
Novena Square Tower A
Singapore 307684
Singapore
Phone: +65.6333.8121
Fax: +65.6333.8131

Australia and New Zealand
Suite 2 Level 8,
100 Pacific Highway
North Sydney, NSW 2060
Australia
Phone: +61.2.9927.6200
Fax: +61.2.9927.6298