

Reviewing System Logs Transcript

In today's course, we will be discussing the importance of reviewing and auditing System Logs. This process is vital when troubleshooting potential system issues along with maintaining data integrity and system security.

We will take a look at the SHOWLOG function and then go over the Boot, Manager's Override, Options Change, and Security Logs.

System Logs are created automatically and can be viewed on screen, printed out or even downloaded to a file.

Some of the Logs generated can even be printed automatically.

You can select to review one on the screen by two different methods.

The first is to type SHOWLOG into the Launch bar of the Eagle Browser and press Enter.

Or, you can open the Utilities menu and select 'Show Application/System Logs'.

The Log Selection Viewer opens.

Simply double click the Log that you wish to view.

Use the 'Next' and 'Previous' buttons to scroll through the pages of the Report Viewer.

You can Print out a copy by pressing the Print button.

If you would like to generate a PDF document, open the Miscellaneous menu and choose option 7.

You can also turn the data into a flat file or copy to your Windows clipboard. This makes it easy to share the information with anyone that needs to review it.

The Boot Log is very beneficial since it compiles details from various functions.

It can identify when Reports were run and include detailed information such as when the report Started, Finished and from which terminal.

You will also be able to review a list of all reports that generated as part of the End of Day process along with backup start and finish times.

The File Update Manager Error Log, included in the Boot Log, can be especially helpful.

If an error occurs when the System tries to finalize data from a Point of Sale transaction to a supporting file, it records here.

For example, an item was sold at Point of Sale and at some point during the day the SKU was accidentally deleted.

The File Update Manager Error Log would report the Transaction or the Files that were affected.

Another log that management should review is the Override Log.

Dependent on how your Security Roles are assigned, your Point of Sale clerks may be required to obtain a Manager's Override to complete certain transactions.

These security bits are identified with an (MO) in their description.

The Manager's Override Log provides a list of each instance that required a user name and password to complete a process.

If you notice system behavior changing or that a process seems to involve different steps to complete, you will want to review the Options Change Log.

This provides a list of all system options that have been altered.

It shows you how the options were set originally and what they were changed to.

It also provides the User and the Terminal where the change was made.

Finally, you will need to check the Security Log when using High Security Passwords on your Eagle System.

This file identifies when employees with high-security passwords are enabled, disabled, or changed.

By accessing and reviewing System Logs you can effectively troubleshoot potential issues, maintain your data integrity and oversee the security of your Eagle System.

Management should spend time each month reviewing the Boot Log, Managers Override Log, Options Change Log, and the Security Log.



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 © 2016 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.



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

Bldv. 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