Security Audit report states weak ciphers are enabled

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT, v7.x and later

SYMPTOM

Security Audit report states weak ciphers are enabled.

CAUSE

The EFT server administrator has complete control over which ciphers to enable or disable. In this case, weak ciphers are enabled.

In EFT v8.0 and later, TLS v1.2 is set by default.

RESOLUTION/WORKAROUND

To ensure only strong ciphers are being used

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the server node that you want to configure.
3. In the right pane, click the **Security** tab.
4. In the **SSL Compatibility** area, specify the SSL versions/ciphers to use.
5. Select the check box of one or more ciphers/algorithms to use, or manually specify the ciphers. At least one cipher must be specified.
6. Click the arrows to arrange the ciphers in top-down priority. If more than one approved cipher is specified, and the connecting client has in its list one or more ciphers that are also on EFT's approved list, EFT will select and use the cipher based on ordering (priority) shown in the list box.

7. Click **Apply** to save the changes to EFT.

For more information, refer to "Enabling SSL on the Server" in the help for your version of EFT.

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11515/Security-Audit-report-states...