SECURITY OUT OF THE BOX

Cybersecurity today is a critical concern in this work-from-home world, driven by recent worldwide events. Because Cybersecurity is at the root of what we do, TDi is taking a pro-active approach to ensure we deliver the most secure product out of the box.

TDi strongly urges existing ConsoleWorks users to upgrade to the new, recommended security settings, available in ConsoleWorks Version 5.3-1u0, as soon as possible.

TLS VERSIONS DEPRECATED

Transport Layer Security (TLS) 1.0 and 1.1 are disabled. While these protocols will remain available for customers to re-enable as needed, we recommend that all organizations move off TLS 1.0 and TLS 1.1 as soon as is practical. Newer versions of the TLS protocol enable more modern cryptography and are broadly supported across modern browsers

PASSWORD RULES AND INACTIVITY TIMER

Default Password Rules have been updated to be more in line with NIST 800-63b standards. This includes:

- a default minimum password length of 8 characters
- required admin unlock for locked out accounts due to login failures
- a default value of 5 minutes for account lockout if the admin unlock is disabled
- a new option to force a password reset on a user's next log in

Additionally, default values for the Inactivity Timer (15 min) and Inactivity Warning (7 min) were updated to be more in line with NIST recommendations though these values remain configurable.

FORCE SSL, SELF-SIGNED CERTIFICATES, AND LOG FILE SIGNING

The Force SSL setting is enabled by default for new ConsoleWorks installations and to facilitate that setting the install process for all platforms now auto-generates a self-signed certificate if one does not exist.

Lastly, the log file signing feature is enabled by default.

For new ConsoleWorks installations, these settings are configured by default during the product installation.

To minimize disruptions during the upgrade process, these security changes will not affect existing ConsoleWorks installations. TDi strongly recommends the following configuration steps after upgrading to version 5.3-1u0:

Step 1. Upgrade all instances of the ConsoleWorks Windows Event Forwarder running in your environment to the latest version included in the 5.3-1u0 release.
Step 2. Connect to your ConsoleWorks invocation using HTTPS and log in.
Step 3. From the ConsoleWorks Navigation Menu, go to ADMIN > Server Management > Configuration. Select the Force SSL check box, which will force all incoming connections to ConsoleWorks to be secure.
Step 4. Open the TLS Compatibility section and select "Current recommendations" from the TLS Compatibility Mode selection box.
Step 5. Open the Session Timers section and adjust the Inactivity Timer to 15 minutes and the Timeout Warning to 7 minutes (recommended).
Step 6. From the Navigation Menu, go to SECURITY > Password Rules and make the following recommended changes:

- Minimum Length: 8 characters
- Select the Require Admin Unlock check box

Step 7. Enable secure logging for all existing Consoles. This can be done individually or via Mass Change. If you need assistance or do not have a license for Log File Signing, please contact TDi Support.

Please contact Support@TDiTechnologies.com if you have questions during the upgrade process.

To ensure that the environments where ConsoleWorks runs are secure, TDi has consulted with former NSA engineers to develop a set of best practices for securing and hardening the ConsoleWorks host server running on the Linux or Windows platforms. These recommendations are available to TDi customers as a reference to assess the security configuration settings for your environment. Click here for the link to this guide.