Welch Allyn®
Q-Stress® with Enhanced Security
Quick reference

Information on the hardened Q-Stress System for Department of Defense Customers:

> *For instructions on first time system setup and software activation refer to the Q-Stress System Installation Manual, DIR 9515-205-60.*

The Q-Stress system has been configured to comply with the Department of Defense's Risk Management Framework to mitigate potential security vulnerabilities. The following hardened measures are applied to this system:

1. Default accounts *Guest* and *Administrator* have been renamed.
2. Administrator Account credentials set as:
   - Username: **QStressHRLocalAdmin**
   - Password: **QStressHRlocaladm1n!**
   - Recommended to change password after first login.
   - Recommended to disable account if the system is joined to a network domain.
3. DoD specified and created Group Policy Objects (GPOs) are locally enabled:
   - DoD Internet Explorer 11 Computer v1r18
   - DoD Internet Explorer 11 User v1r18
   - DoD Windows 10 Computer v1r19
   - DoD Windows 10 User v1r19
4. Public Key Infrastructure (PKI) certificates have been installed.
5. BitLocker protection has been enabled on fixed drive present on the system.
6. Windows Data Execution Prevention has been disabled.
7. Windows Speculative Execution has been configurated as per Recommended Settings to mitigate "speculative execution side-channel attacks".

If joining the Q-Stress system to a network domain, note that the locally enabled GPOs on the Q-Stress system may be overwritten by any GPOs applied by the network domain. In order to maintain the level of hardening specified by the DoD for the Q-Stress system, the four GPOs mentioned in #3 above must be applied.

From the Domain Controller, GPOs can be managed and applied to PCs as needed. The required GPOs can be found on the additional provided CD, or can be downloaded as a part of a larger package from the DoD website: https://public.cyber.mil/stigs/gpo/

> ⚠ Caution: If enabling the DoD Windows 10 GPOs the FIPS policy must be disabled for the Q-Stress system to function.

To disable this policy, create a new GPO on the network domain with a higher priority than the DoD Windows 10 GPOs. In the new GPO find the Policy, "System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing," and set it to **Disabled**. The policy can be found under: Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options.

To ensure the policy has been disabled, reboot the system after disabling the policy, then navigate to the specified policy location and ensure the FIPS policy is disabled.

hillrom.com REF 772001, 80026577 Ver A Revision date: 2020-04
Hillrom Technical Support: hillrom.com/en-us/about-us/locations/, 1.888.667.8272