LOCKING DOWN YOUR PC-DUO RAS SERVER

The PC-Duo RAS Edition allows customers to independently operate and manage their own remote desktop support portal in-house. We thought it would be best to publish some guidelines and recommendations in and around securing an installation of the PC-Duo RAS server. The web site that we've been using as the arbiter of "best practices" is the Qualys SSL Labs site. This site will contact any publicly addressable site/application on port 443 (only) and evaluate the SSL configuration found there. By exposing either IIS or the RAS server on a public port 443, tests can be run against our software.

In Windows, SSL support is handled in a module called "SChannel". This module and its configuration are *global* on the machine, and therefore changing the configuration to secure Web Console changes the configuration for all applications on the machine. As a result, we don't think it's appropriate that the PC-DUO installers change this global machine configuration, but it is our responsibility to call the administrator's attention to the issue and provide guidance on how to establish a good configuration.

Microsoft's guidance on configuring Windows is in their Support Knowledge Base article # 245030. Unfortunately, this does not provide guidance on what configuration should be used and instead documents many registry keys that can be modified to change the configuration. As is, the information within the article wasn't directly helpful. During our exploration of this, we identified a software consulting company called Nartac Software had this same issue and has developed a utility program called IIS Crypto to address it. It's available for free at here.

PC-DUO RAS CUSTOMERS SHOULD FOLLOW THESE STEPS

1. On the server machine to be configured, log into Windows as an administrative user of the machine.
2. Download the tool from https://www.nartac.com/Products/IISCrypto/(or access an already downloaded copy from somewhere).
3. Run the tool, and click the "Best Practices" button.
4. In the "Hashes Enabled" list, uncheck MD5 if it remained checked. This a recent change to "best practices" guidance.
5. Optionally, in the "Ciphers Enabled" list, uncheck "Triple DES 168/168" if it remained checked. This disables the shortest key length (112 bits) and ensures AES either 128 or 256 bit is used.
6. Click Apply.
7. Click the Close box in the upper-left hand corner of the window to close the utility.
8. Restart the machine. This is very important – the utility doesn't force or prompt for a restart, but the configuration changes will not take effect until after the machine is restarted.

THAT'S IT! This is a one-time machine configuration change, at least until SSL best practices change again. Note well that this configures the SERVER side of SSL configurations only, so there's only value in doing this on machines that have SSL-based servers that use the Microsoft SChannel implementation. This specifically includes Internet Information Services (IIS) hosting Web Console, but excludes the Gateway Server, which uses OpenSSL for its SSL support.