

# Managing Risks of Non-scheduled Reboots following Security Patch Installation

## Introduction

As attacks on computer systems by viruses and hackers increase, the frequency at which Microsoft® releases security updates and patches has also increased. Some of our customers have asked us if installing these critical updates will adversely impact our TotalChrom® software. The answer is the risk is very low and **not** installing the Microsoft updates certainly increases the risk of attacks and software-related problems.

## Keeping networks secure

While every effort is being made to evaluate patches and hot fixes as they become available, the reality is we cannot assume responsibility for any adverse impact these patches may have on our application software. In this rapidly changing environment, we believe the end user has to assume some responsibility for keeping their own networks secure and the associated risk (although minimal) for installing patches as their Information Technology group sees fit.

Ideally, we recommend testing critical updates on a non-production TCCS test system for evaluation. Customers in regulated environments should have a test

system in which application and operating system patches or maintenance releases can be installed and tested to evaluate compatibility, functionality, and reliability issues that may impact your application's usability or your existing validation protocol.

## PerkinElmer support

We realize in the case of security patches, some of these updates are urgent and may require immediate installation per your company's policy. This leaves little to no time to evaluate risks to your chromatography data system even if a test system is in place. Any problems that do surface will be uncovered and posted to our staff and user-base as quickly as possible. In the unlikely event a Microsoft patch does cause a problem with PerkinElmer® application software, our global support organization is here to provide the necessary assistance to help investigate and resolve the problem.

## Installing a Microsoft critical update

We also realize that in many sites, security patches may be installed to all systems within the site during off hours for the lab,

without knowledge of people in the lab or the system manager of the data system. After installing a Microsoft Critical Update, the computers within the network usually need to be rebooted. If your lab is not "prepared" for this, the "non-scheduled" server reboots can occur while your TCCS system is up and running. Users may be logged into the TotalChrom system, all of whom will lose connection with the License Manager. This can prevent users from logging into TCCS the following day when they return to the lab. In other cases when users are acquiring data during a server reboot, the data can end up in the wrong folder making the user think they have lost their data. Depending on how the clients are set up will determine the course of action to take.

Rebooting servers during a non-scheduled server reboot while your TCCS system is up and running can be managed in a manner that will have minimal impact to your TCCS system. This is especially true if users are acquiring data.

Below are some tips to help TCCS system managers make it through non-scheduled server reboots.

## Non-scheduled server reboot tips

If you have a TotalChrom CS System with a:

### Single Server

The Single Server includes the License Manager, Acquisition Server and Analysis Server. It is also acting as the File Server. The system manager really has no choice but to reboot the server. Any users that are logged into TCCS will lose contact with the license manager. Any raw files that are being acquired will be buffered in the interface. When the TCCS server comes back live, the raw file that was being acquired during the server reboot will have header information only. A raw file with the same name with a date-time stamp on it will be intact and written to the TCCS server from the interface. Any other raw files that were buffered in the interface will be written to the TCCS server as well.

### Single Server AND separate File Server

The system manager should stop the PENLCD service on the TCCS server. Any raw files that are being acquired will be buffered in the interface. Reboot the File Server and then reboot the TCCS server. This will ensure that the TCCS files will be available for the TCCS server. Any users that are logged into TCCS will lose contact with the License Manager. When the TCCS server comes back live, the raw file that was being acquired during the server reboots will have header information only. A raw file with the same name with a date-time stamp on it will be intact and written to the File Server from the interface. Any other raw files that were buffered in the interface will be written to the File Server as well.

### License Manager AND separate Acquisition/Analysis Servers

The system manager should stop the PENLCD service on the Acquisition Server. Any raw files that are being acquired will be buffered in the interface. Reboot the License Manager. If the Analysis Server is separate from the Acquisition Server, reboot the Analysis Server. Reboot the Acquisition Server. Any users that are logged into TCCS will lose contact with the License Manager. When the Acquisition Server comes back live, the raw file that was being acquired during the server reboots will have header information only. A raw file with the same name with a date-time stamp on it will be intact and written to the Analysis Server from the interface. Any other raw files that were buffered in the interface will be written to the Analysis Server as well.

### License Manager with separate Acquisition/Analysis Servers AND a separate File Server

The system manager should stop the PENLCD service on the Acquisition Server. Any raw files that are being acquired will be buffered in the interface. Reboot the File Server first. This will ensure that the TCCS files will be available for the TCCS servers. Reboot the License Manager. If the Analysis Server is separate from the Acquisition Server, reboot the Analysis Server. Reboot the Acquisition Server. Any users that are logged into TCCS will lose contact with the License Manager. When the TCCS servers come back live, the raw file that was being acquired during the server reboots will have header information only. A raw file with the same name with a date-time stamp on it will be intact and written to the File Server from the interface. Any other

raw files that were buffered in the interface will be written to the File Server as well.

### Citrix server

Citrix servers are full clients in a TCCS system and should be rebooted after all the TCCS servers come back live. If the Citrix servers are rebooted before the TCCS servers, then the PENLCD service needs to be restarted on the Citrix servers after the TCCS servers come back live.

## What should users do when the servers are rebooted?

**Full client:** A user running full client with the PENLCD service running on their PC needs to restart the PENLCD service regardless of whether or not they were logged into TCCS. If the user does not have the privilege to restart services on the PC, they can either reboot the PC or have someone with privileges restart services on the PC. If the full client is running Interactive LCD Control, then all they have to do is log out of TCCS and log back in.

**Small client:** A user running small client needs to log out of TCCS and log back in.

**Citrix client:** A user running a Citrix client needs to log out of TCCS. They need to wait until the Citrix servers came back live after being rebooted and then they can log back into TCCS.

## Summary

We hope this review has been helpful. Please keep it in a handy location. Make certain the people responsible for your information technology security stay in close communication with your lab's data system manager so server re-boots, patch installations, and security changes to your system are done efficiently and safely with your complete knowledge.

**PerkinElmer Life and  
Analytical Sciences**  
710 Bridgeport Avenue  
Shelton, CT 06484-4794 USA  
Phone: (800) 762-4000 or  
(+1) 203-925-4602  
[www.perkinelmer.com](http://www.perkinelmer.com)



---

For a complete listing of our global offices, visit [www.perkinelmer.com/lasoffices](http://www.perkinelmer.com/lasoffices)

©2004 PerkinElmer, Inc. All rights reserved. The PerkinElmer logo and design are registered trademarks of PerkinElmer, Inc. PerkinElmer and TotalChrom are registered trademarks of PerkinElmer, Inc. or its subsidiaries, in the United States and other countries. All other trademarks not owned by PerkinElmer, Inc. or its subsidiaries that are depicted herein are the property of their respective owners. PerkinElmer reserves the right to change this document at any time without notice and disclaims liability for editorial, pictorial or typographical errors.