CPTRAX TECHNICAL BRIEF

Why choose CPTRAX for Logon and Logout Auditing?

Does not use Windows Event Logs
Does not use Polling
Low Overhead – No Windows configuration changes needed or required
Real-Time Reporting and Alerting

You have several choices when selecting a logon / logout auditing solution for your Windows® network. We created CPTRAX to give you a *better* choice. This document has been prepared to provide a technical review of logon / logout auditing methods and how CPTRAX for Windows is a better choice.

CPTRAX *versus:* Windows Event Log Readers

Most logon auditing products available rely upon Windows Event Logs to provide input for their reporting. To begin, a local or domain policy must be set to enable auditing of logons, logouts and, separately, failed logon attempts.

In the event logs there are essentially two different types of logon events, local and network / remote. The monikers "local" and "network / remote" are event designations from the perspective of the machine that was logged onto.

Local logon events are when the logon results in at least one process being created on the local machine that is owned by the account that logged on. When viewing processes in "task manager" there is column that indicates username, it is this column that identifies the owner of the selected process. For instance, a local logon occurs when using the selected machine's keyboard, Remote Desktop Protocol (RDP), Remote Web Workplace (RWW) and Independent Computing Architecture (ICA) to logon.

Network logon events occur when a successful logon does not result in a process being created that is owned by the account that logged on. For instance, a network logon occurs when a drive is mapped to a server from a different node on a network.

For local logon and logout events, including terminal server sessions, the event logs do accurately reflect logon and logout/logoff times.

For network (remote) logon and logout events, the event logs are not always accurate. To explain, network logon connections are auto-disconnected after a preset 'watchdog' timer elapses without

© 2010 Visual Click Software, Inc. All Rights Reserved.

any activity occurring on the connection. This timer generally defaults to 15 minutes. No error or message is generated when this timeout occurs, just an entry in the event log indicating a logout has occurred. However, from the user's perspective they believe they are still logged on as the user did not initiate a logout. In fact, the next time the user begins using that connection they are auto-reconnected with no logon prompt – this auto-logon event is recorded as an Account Logon (DC) and regular logon (DC or server). Thus it is very possible for a user to have multiple logons and logouts recorded during what is actually a single actual logon session.

Depending on your needs the multiple logons and logouts for what is a single logon session (with a single logout – from the user's perspective) can interfere with determining when the user actually logged on and when they actually logged off.

When a *failed logon* event occurs an accurate entry is recorded in the event log.

Choice: CPTRAX for Windows

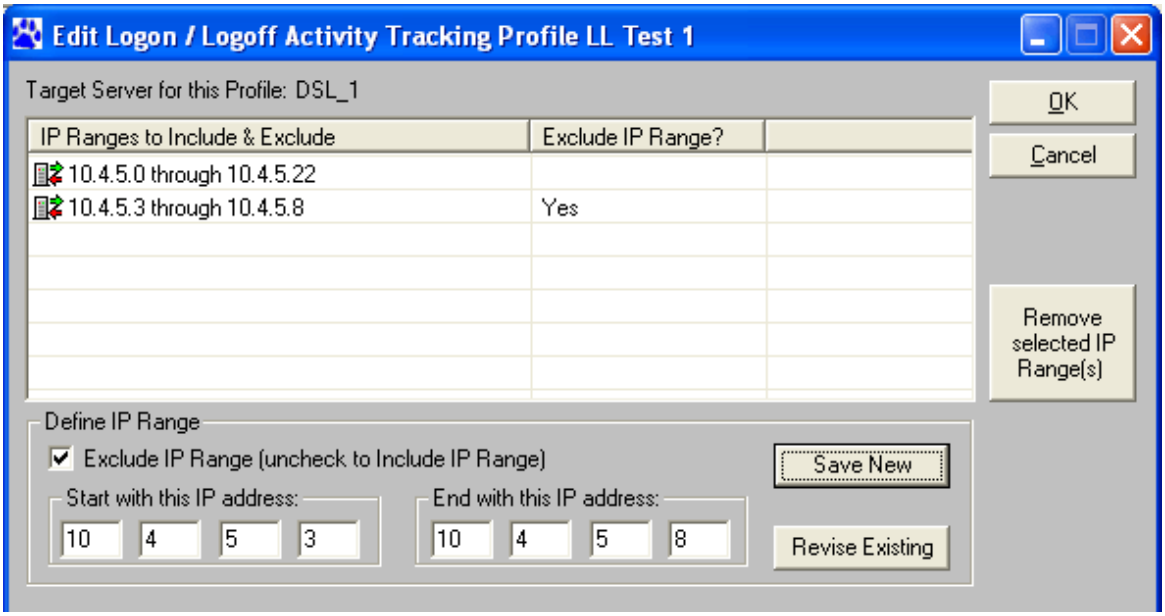
CPTRAX integrates with the Windows operating system to provide a better choice when you need to accurately report when a user logged on and when they actually logged out. Unlike the Windows Event Logs, CPTRAX records a single logon and single logout for network/remote connections. Including recording of logouts when the user's workstation crashes or otherwise is disconnected without an actual user logout request. And CPTRAX will record logons and logouts on any server where it is installed; this means its abilities are *not limited* to domain controllers only.

All tracking performed by CPTRAX is completely independent of Windows Event Logs, therefore there is no requirement to enable auditing polices or worry about event logs filling up and losing data as log files 'rollover'.

Additionally, CPTRAX provides the ability to set up selective alerting and reporting based upon the IP Address of where the logon originated (including the originating IP address used for terminal service logons). CPTRAX will also track failed logon attempts and the reason why the logon attempt failed (bad password, disabled account, and so on).

© 2010 Visual Click Software, Inc. All Rights Reserved.

CPTRAX TECHNICAL BRIEF



Benefited by kernel-level development design experience stretching back to the late 1980's and all versions of Windows since, CPTRAX offers a better choice for Windows Logon, Logout and Failed Logon Auditing and Alerting.

Contact us today to schedule your customized free online demonstration of CPTRAX.

sales@visualclick.com

Toll-free: (877) 902-5425
Direct dial: (512) 330-0542

http://www.visualclick.com/content/cptraxw.htm

© 2010 Visual Click Software, Inc. All Rights Reserved.