



Automated Auditing, Alerting and Reporting of Active Directory, Group Policy, File System, File Security, and Logon Activities for Windows® environments.

Your 24x7x365 solution that provides compliance and control.

Administrator's Guide

Visual Click Software, Inc.

Copyrights

This manual contains proprietary information that is protected by copyright. The information in this manual is subject to change without notice. No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose other than the licensee's personal use without prior written permission of Visual Click Software. The software described in this manual is furnished under a license granted by Visual Click Software to the licensee. This software may be used or copied only in accordance with the terms of the license agreement.

© 2013 Visual Click Software, Inc. **All rights reserved.**

Trademarks

CPTRAX®, DSMETER®, DSRAZOR®, and Visual Click® are registered trademarks of Visual Click Software, Inc. Microsoft® and Windows® are registered trademarks of the Microsoft Corporation in the United States and other countries. Active Directory is a trademark of the Microsoft Corporation. Other marks cited in this document are the property of their respective owners.

Patents

U.S. Patent No. 6,438,742
Issue Date: August 20, 2002

Documentation Conventions

Special information in this manual is presented using the following conventions:

- **Bold** text indicates commands, command-line options, and interface controls, such as the names of icons, menus, menu items, buttons, checkboxes, and tabs.
- *Quotes* "" surrounding text indicate button and other labels shown in screenshots.
- *Italic* text indicates variables that must be replaced with a value. It also indicates book titles and emphasized terms.
- `Monospace` text indicates data to enter, filenames, and code examples.

Contact Us

Thanks for using CPTRAX for Windows. Visual Click Software, Inc. is committed to the ongoing support of its products. For information and the latest download of the CPTRAX product, visit the web site at <http://www.visualclick.com>. For information, help, and to report problems associated with this product, or if needing features or functionality that are not currently offered by Visual Click Software, contact our customer support team at supportw@visualclick.com. To purchase additional licenses, contact the sales team at sales@visualclick.com.

You can also contact us at the following mailing address and phone numbers:

Visual Click Software, Inc.
P.O. Box 161657
Austin, TX 78716

(512) 330 0542
(877) 902 5425

Pubrev 021213

CPTRAX for Windows End User License Agreement

Visual Click Software, Inc. End User License Agreement

THIS SOFTWARE IS LICENSED, NOT SOLD, AND AVAILABLE FOR USE ONLY UNDER THE TERMS OF THIS LICENSE AGREEMENT. PLEASE READ THIS LEGAL AGREEMENT CAREFULLY. VISUAL CLICK WILL ONLY LICENSE THE SOFTWARE PROVIDED WITH THIS AGREEMENT TO YOU IF YOU FIRST ACCEPT THE TERMS OF THIS AGREEMENT. REGARDLESS OF HOW YOU ACQUIRE THE SOFTWARE (ELECTRONICALLY, PRELOADED, ON MEDIA, OR OTHERWISE), USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THESE TERMS.

Visual Click Software, Inc. (“Visual Click”) grants you a nonexclusive license under the terms states below to the Software in the country in which you acquire it.

1 License Grant. This license agreement is your proof of license to use the Software and must be retained by you. Under this license, Visual Click grants to you (either as an individual or entity) a personal, non-exclusive object code only license to use the copy of the object code version of the Visual Click software accompanying this license (the “Software”) by (i) installing the Software on one server, (ii) running the install program to create the number of remote user copies and associated user IDs for which you have a paid-up license, (iii) loading such remote user copies and user IDs on remote personal computers, and (iv) making backup or archival copies. You agree you will not copy the Software except as permitted under the terms of this license. You agree that you will not copy the written materials accompanying the Software.

This agreement is effective for the duration of Visual Click’s copyright in the Software unless earlier terminated by Visual Click for breach of this license by you. You may not rent or lease the Software, but you may assign your rights under this agreement on a permanent basis to another person who agrees in writing prior to the assignment to be bound by this agreement and to re-register the Software in their name and provided that you transfer all copies of the Software and related documentation to the other person or destroy any copies not transferred. Except as set forth above, you may not assign your rights under this agreement. The Software is owned by Visual Click and/or its suppliers, and is copyrighted and licensed, not sold. You agree to reproduce the copyright notice and any other legend of ownership on each copy, or partial copy, of the Software.

You agree that you will not attempt, and if you are a corporation, you will use your best efforts to prevent your employees and contractors from attempting, to reverse compile, modify, translate, or disassemble the Software in whole or in part. You also agree that you will not (i) use or copy the Software except as provided in this Agreement; (ii) modify or merge the Software; (iii) sublicense the license for or rent the Software; or (iv) distribute the Software to any third party.

2 Limited Warranty. Visual Click warrants that for a period of ninety (90) days from the date of purchase, the Software, when executing on compatible computers and operating systems designated by Visual Click, will perform substantially in accordance with the accompanying documentation, and that the documentation and media are free from any physical defects (“Limited Warranty”). VISUAL CLICK AND ITS SUPPLIERS DO NOT WARRANT THAT

THE SOFTWARE OR DOCUMENTATION WILL SATISFY YOUR REQUIREMENTS, THAT THE SOFTWARE AND DOCUMENTATION ARE WITHOUT DEFECT OR ERROR OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED. BECAUSE IT IS IMPOSSIBLE FOR VISUAL CLICK TO KNOW THE PURPOSES FOR WHICH YOU ACQUIRED THIS SOFTWARE OR THE USES TO WHICH YOU WILL PUT THIS SOFTWARE, YOU ASSUME FULL RESPONSIBILITY FOR THE SELECTION OF THE SOFTWARE, AND FOR ITS INSTALLATION AND USE, AND THE RESULTS OF THAT USE.

3 Disclaimer of Warranties. EXCEPT FOR THE LIMITED WARRANTY DESCRIBED IN PARAGRAPH 2 (“Limited Warranty”), VISUAL CLICK MAKES NO OTHER EXPRESS OR IMPLIED WARRANTIES TO THE EXTENT PERMITTED BY LAW AND SPECIFICALLY DISCLAIMS THE WARRANTIES OF NON-INFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IF SUCH DISCLAIMER IS NOT PERMITTED BY LAW, THE DURATION OF ANY SUCH IMPLIED WARRANTIES IS LIMITED TO NINETY (90) DAYS FROM THE DATE OF DELIVERY. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY MAY LAST, OR THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO SUCH LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION.

4 Customer Remedies. Visual Click’s entire liability and your sole and exclusive remedy for a breach of the Limited Warranty for the Software shall be, at Visual Click’s option, for Visual Click to (a) correct the error, (b) help you work around or avoid the error, or (c) authorize a refund. In the case of defective media or documentation, Visual Click’s entire liability and your sole and exclusive remedy will be to replace the defective media or documentation at no charge. To obtain the benefits of this Limited Warranty, you must return the Software, documentation and media to Visual Click during the Limited Warranty period with a copy of your receipt. This Limited Warranty is void if failure of the Software has resulted from accident, abuse, or misapplication. Any replacement Software, documentation or media will be warranted for the remainder of the original warranty period.

5 Limitation on Liability. In no event will Visual Click’s liability for any claim, whether in contract, tort or any other theory of liability, exceed the license fee paid by you. This limitation is cumulative, with all payments to you for claims or damages being aggregated to determine satisfaction of the limit. Visual Click’s pricing reflects the allocation of risk and limitations on liability contained in this agreement.

6 No Liability for Consequential Damages. IN NO EVENT SHALL VISUAL CLICK BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, SPECIAL, INCIDENTAL OR INDIRECT DAMAGES OF ANY KIND ARISING OUT OF THE USE OF THE VISUAL CLICK SOFTWARE, INCLUDING LOST PROFITS, LOSSES ASSOCIATED WITH BUSINESS INTERRUPTION, LOSS OF USE OF THE SOFTWARE, LOSS OF DATA OR COSTS OF RE-CREATING LOST DATA, EVEN IF VISUAL CLICK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7 Force Majeure. Neither you nor Visual Click is responsible for failure to fulfill any obligations due to causes beyond its control.

8 Export. You agree that you will not export or re-export the Software without the appropriate United States or foreign government licenses.

9 Tax Liability. You are responsible for paying any sales or use tax imposed at any time whatsoever on this transaction.

10 Governing Law. The Software is protected by United States copyright laws and international treaty provisions. The United Nations Convention on Contracts for the International Sale of Goods is specifically disclaimed. This agreement will be governed by the laws of the country in which you acquired the Software, except (i) in Australia, the laws of the State or Territory in which the transaction is performed govern this agreement; (ii) in Albania, Armenia, Belarus, Bosnia/Herzegovina, Bulgaria, Croatia, Czech Republic, Federal Republic of Yugoslavia, Georgia, Hungary, Kazakhstan, Kirghizia, Former Yugoslav Republic of Macedonia (FYROM), Moldova, Poland, Romania, Russia, Slovak Republic, Slovenia, and Ukraine, the laws of Austria govern this agreement; (iii) in the United Kingdom, all disputes relating to this agreement will be governed by English Law and will be submitted to the exclusive jurisdiction of the English courts; (iv) in Canada, the laws in the Province of Ontario govern this Agreement; and (v) in the United States and Puerto Rico, and People's Republic of China, the laws of the State of Texas as they are applied to agreements between Texas residents entered into and to be performed entirely within Texas govern this agreement.

11 Severability. In the event of invalidity of any provision of this agreement, the parties agree that such invalidity shall not affect the validity of the remaining portions of this agreement.

12 Entire Agreement. This is the entire agreement between you and Visual Click which supersedes any prior agreement, whether written or oral, relating to the subject matter of this agreement and may be amended only by a writing signed by both parties. No vendor, reseller or other person is authorized to modify this agreement or to make any warranty, representation or promise that is different than, or in addition to, the warranties provided in this license agreement.

U.S. GOVERNMENT RESTRICTED RIGHTS

If this product is acquired under the terms of a: DoD contract: Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of 252.227-7013 and restrictions set forth in the accompanying end user agreement. Civilian agency contract: Use, reproduction or disclosure is subject to 52.227-19 and restrictions set forth in the accompanying end user agreement. Unpublished: Rights reserved under the copyright laws of the United States. Visual Click Software, Inc., P.O. Box 161657, Austin, Texas 78716-1657.

Should you have any questions concerning this agreement, or if you desire to contact Visual Click for any reason, please write: Visual Click Software, Inc., P.O. Box 161657, Austin, Texas 78716-1657.

Table of Contents

Administrator's Guide.....	1
Trademarks	2
Patents	2
Documentation Conventions	2
Contact Us	2
CPTRAX for Windows End User License Agreement	3
<i>Before you begin using CPTRAX for Windows</i>	9
Welcome	9
Why use CPTRAX - Comparative Review of Features.....	9
Minimum System Requirements and Recommendations	11
Minimum Permissions for Installation and Configuration	11
Operational Overview Summary	12
Actions on the Server.....	12
Actions on your workstation	13
Departments and Enterprise Hosts.....	14
Defining a Department.....	14
Defining an Enterprise Host.....	15
Combining Enterprise Hosts	18
FAQ: Department and Enterprise Hosts	18
Chapter 2 – CPTRAX Installation	20
<i>Installing the CPTRAX Download Package</i>	20
CPTRAX Basic Installation	24
Setting up your first server.....	24
Continuing CPTRAX Installation after Server and Share selection	25
CPTRAX Configuring Profiles	29
File System Activity Profile: Add New	30
File System Activity Profile: Add Tracking / Blocking Item	31
File System Activity Profile: Add Users to Exclude	33
File System Activity Profile: Alerts.....	35
File System Activity Profile: Done.....	35
Logon / Logoff Activity Profile: Add New	36
Logon / Logoff Activity Profile: Add IP Range	38
Logon / Logoff Activity Profile: Alerts	39
Logon / Logoff Activity Profile: Done	40
Failed Logon Activity Profile: Add New.....	40
Failed Logon Activity Profile: Add IP Range	42
Failed Logon Activity Profile: Alerts	43
Failed Logon Activity Profile: Done	44
Active Directory Activity Profile: Add New	44
Active Directory Activity Profile: Add Object Class to Track.....	46
Active Directory Activity Profile: Add Attribute to Track.....	48
Active Directory Activity Profile: Add Directory Objects to Track.....	49
Active Directory Activity Profile: Alerts.....	50
Active Directory Activity Profile: Done.....	50
GPO Change Activity Profile: Add New.....	50
GPO Change Activity Profile: Add GPO to Track.....	52
GPO Change Activity Profile: Active Directory Tracking Options	53

Group Policy Activity Profile: Alerts	56
Group Policy Activity Profile: Done	56
CPTRAX Additional Installation Options.....	57
Configuring Email Addresses for Alerting	57
Using the Alert Console – Configuring the CPTRAX Server Agent	58
Using the Alert Console – Configuring the workstation Alert Agent	58
Using SQL Transfer – Configuring the CPTRAX Server Agent for SQL Server.....	60
SQL Server Table Column (Field) Definitions.....	63
Viewing SQL Server Statistics	76
Chapter 3 – CPTRAX Quick Reports.....	77
<i>About Quick Reports.....</i>	<i>77</i>
Quick Report Console.....	77
Custom Reporting	78
Manage Log Files	78
Chapter 4 – CPTRAX Administration Console	80
<i>Servers Managed.....</i>	<i>81</i>
Servers Managed.....	81
Start CPTRAX Server Agent	83
Stop CPTRAX Server Agent	83
Manage IP Address used by Server Agent	83
“Agent Running?” responses	84
Agent Version, Driver Version	85
Start Time and IP Address	86
Settings Tab: Overview.....	87
Settings Tab: SQL Transfer Option	87
Settings Tab: Email Server Configuration.....	87
Settings Tab: Update CPTRAX Server Agent.....	87
Uninstall CPTRAX Server Agent.....	88
About Profile Management Access	98
Add New Profile to selected Server.....	98
Rename Profile on selected Server	98
Delete Profile on selected Server.....	98
Disable / Enable Profiles on selected Server	99
Copy Profiles to other Servers	99
Chapter 5 – CPTRAX Custom Reports	101
Custom Reports Creation.....	101
Creating a new Custom Report	103
Viewing list of Custom Reports.....	124
Editing an existing Custom Report	125
Running a Custom Report.....	125
Custom Report Scheduling	125
Creating a Scheduled Activity	126
Viewing current Scheduled Activities	129
Copying Scheduled Activities.....	130
Appendix A – CPTRAX File Extensions	131
Appendix B – All Custom Report Data Services	133

Appendix C – Creating Shared Folder for CPTRAX reporting	135
Appendix D – Setting SYSTEM Account File Permissions	141
Confirming permissions on the <i>drivers</i> folder	141
Confirming permissions on the Share for Activity Log Files	143
Appendix E - Granting non-admin users access for generating CPTRAX reports	146
Appendix F – CPTRAX to SQL Configuration	148
Comprehensive installation details	148
Configuring Protocols for SQL Server (performed at SQL Server Host)	148
Configuring CPTRAX for SQL Server	150
Verifying CPTRAX for SQL Server installation	154
Appendix G – Features FAQ	156
Selected Q & A	156
Troubleshooting Index	158

Before you begin using CPTRAX for Windows

Welcome

Welcome to CPTRAX for Windows your real-time solution for Automated Auditing, Alerting and Reporting of Active Directory, Group Policy, File System, File Security and Logon Activities for Windows environments. Additionally providing regulatory compliance reporting to assist with your compliance activities relevant to:

- Sarbanes-Oxley (SOX)
- Payment Card Industry (PCI) compliance
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Financial Services Authority (FSA)

This guide has been designed to provide you with a thorough review of the installation design, product installation, profile configuration and reporting options of CPTRAX for Windows.

Pronounced as ‘C’ ‘P’ ‘TRAX’, it is an abbreviation for “Compliance Tracking”.

Why use CPTRAX - Comparative Review of Features

CPTRAX for Windows includes many features, some unique compared to similar real-time products by others.

Many products that include Active Directory and Group Policy auditing/tracking rely upon the native Windows Event Logs. CPTRAX for Windows incorporates a customized system interface that directly interacts with Active Directory to collect auditing and tracking data. Because of this, CPTRAX *does not* require Windows event logs to be enabled nor does it require enabling of any other Windows feature to function.

Whereas most products that compete with CPTRAX for Windows employ a “file system driver” to monitor and capture file system events, CPTRAX utilizes a three point strategy of a packet driver, file system driver and terminal server monitoring to provide comprehensive details of all captured file system and connection activities.

To further elaborate, the “file system driver” (FSD) *only* approach is limited in what it can capture. For instance, when utilizing only a **FSD** the manner in which file system action originated the following is ***not available for remote activity***:

- Name of Share used where remote file system activity originated
- Workstation Name
- IP Address of the Workstation

- User Name (FSD only approach does provide User name for local or terminal service generated activity)

CPTRAX for Windows ***captures all these values*** and more including the SAM/Domain name, FQDN and SID. SAM is short for “security accounts manager” database.

CPTRAX for Windows enables you to answer the questions:

Did the user delete a file while they were logged on to their workstation or via terminal services or from some unknown IP address? Based upon the answer you can further infer if it was in fact that user or someone who potentially compromised that account.

Was access to the file granted through a private share such as C\$ or via another share?

Who was using a particular IP address on a specified date/time?

As included by competitors, CPTRAX for Windows provides centralized reporting. However, CPTRAX goes a step further and also provides decentralized “centralized” reporting via its concepts of [Departments and Enterprise Hosts](#).

Also included are real-time alerts via [email](#) and the [CPTRAX desktop alert viewer](#).

All CPTRAX for Windows activity logs are encrypted to protect the integrity of the data captured. However, unlike our competition, no backend SQL or other database is required. [There is a SQL Option available](#). CPTRAX for Windows maintains its own unique report file structure based on the server where collected, profile name and date of activity. This makes reports simple, quick and highly portable.

Also unique to CPTRAX for Windows is its Auditor License that enables your staff members responsible for auditing to directly receive log files on their desktop. When using an Auditor License, CPTRAX will only receive log files from other servers, it will not generate its own. The Auditor License makes it quick and easy for them to generate the reports they need on demand with no overhead by your technical staff or on your servers.

Other features of CPTRAX for Windows include:

- Interoperability across unrelated Domains, Active Directory Forests and stand-alone servers/workstations
- Scalable Administration interface that enables functionality on a small network to one with thousands of servers
- Unattended and Scheduled Reporting
- Automatic purging of old activity logs
- Active Directory auditing, included is the ability to define the object classes and attributes to track, will also track Active Directory Schema changes
- Blocking File Creates, Deletes, Modifications and Renames
- Blocking of Folder Creates, Deletes and Renames
- Logon and Logoff Tracking for NTLM, NTLMSSP and Kerberos connections

- Logon and Logoff Tracking for Local and Terminal Service Sessions
- Logon and Logoff Tracking for FTP Sessions
- Failed Logon Tracking for NTLM, NTLMSSP and Kerberos connections

Minimum System Requirements and Recommendations

Prior to installation, please ensure you have received a valid CPTRAX Token. The CPTRAX Token is a small file containing clear-text and encrypted- text. The token enables the CPTRAX Server Agent to function. If you do not have a valid CPTRAX Token, please contact sales@visualclick.com and request an evaluation token.

On a server where CPTRAX will be used to collect and control activity:

- Windows 2000, Windows 2003 (32bit and [64bit](#)¹), Windows 2008/R2 (32bit and 64bit), Windows 2012
- Up to 32 CPUs (32bit systems) and up to 256 CPUs (64bit systems)
- Virtual Servers (Hyper-V, VMware, etc.)
- 100MB of RAM
- 100MB of Disk Space (may need considerably more depending on volume of activity tracked and where activity logs are stored)
- File Compression is recommended on the folder used for storing activity logs

On a server or workstation where CPTRAX will be used in [Auditor mode](#):

- Windows 2000, Windows 2003, Windows 2008/R2, Windows 2012, Windows XP, Windows Vista or Win7 (can be 32bit or 64bit for any of these)
- 50MB of RAM
- 1GB of Disk Space (may need considerably more depending on volume of activity tracked)
- File Compression is recommended on the folder used for storing activity logs

Because of its lightweight construction, CPTRAX for Windows has no minimum CPU speed requirements and works on machines with up to 32 CPUs (32bit systems) and 256 CPUs (64bit systems).

There are no minimum requirements for use of Domains, Activity Directory, or stand-alone configurations.

Minimum Permissions for Installation and Configuration

Installation and configuration of CPTRAX for Windows requires Administrator level privileges. These privileges are required for installing the CPTRAX Server Agent service, copying of kernel driver files, updating the server's Registry and potentially creating a Reporting Share (an existing public share can be used).

¹ Installation of CPTRAX on Windows 2003 x64 requires the hotfix detailed in Microsoft's KB 942589

Operational Overview Summary

This section provides a technical overview of CPTRAX for Windows and presumes the reader has familiarity with the Microsoft® Windows Server Operating Systems.

Actions on the Server

CPTRAX for Windows includes a server agent that provides real-time file activity and connection tracking, alerting and control. The server agent is composed of two files, CPTRAXW.EXE and CPTW_K32.SYS or CPTW_K64.SYS (CPTWK646.SYS on systems with forced NDIS6 requirement). These files act together to provide full coverage for file system and connection tracking regardless if the activity is generated locally on the server or across the network from other machines to the server or via terminal service sessions hosted by the server.

The CPTRAX for Windows server agent does not depend on Microsoft System Logs or any other optional Microsoft service. Nor does CPTRAX require any configuration changes to your server's operating system installation. For minimum system requirements, see [Chapter 1, Minimum System Requirements](#).

Internally CPTRAX for Windows is set to monitor up to 1500 remote connections per server. Remote connections largely consist of those that map a drive to the server. Connections using Terminal Services have no internal connection limit. If your server will host more than 1500 remote connections, please email us at supportw@visualclick.com and we can provide an updated server agent to meet your needs. There is no upward boundary on the total number of simultaneous connections, just the one preset limit (which was done to conserve kernel memory).

When initially installed CPTRAX for Windows will create a folder named “cptrax” in the \SystemRoot\System32\Drivers folder {32bit systems} or \SystemRoot\SysWow64\Drivers {64bit systems}. And within the “cptrax” folder, another folder named “Q” will be created. The Q directory (folder) is used to stage activity records the agent is gathering and has not yet finalized processing. These activity log files are processed on an ongoing basis and are removed when processing is complete. See [Appendix A](#) for a complete listing of file types used.

The “cptrax” directory (folder) is used for further processing and staging of Q files for transmission. Also, the “cptrax” directory is used to store archived images of the CPTRAX registry key (found under HKEY_LOCAL_MACHINE\Software\Visual Click Software, Inc.) The most recent registry image is always stored in the file named:

CPTRAXW_00000000.savekey

You can use the Administration Console (cptrax_console.exe) to restore these archived registry keys. The CPTRAX agent automatically purges archived registry key images after 7 days. The archived image CPTRAXW_00000000.savekey is never purged, it always holds the most recent CPTRAX registry image.

The CPTRAX agent archives the registry key 2 minutes after the most recent change. Changes include adding or changing a profile, adding or changing a custom report, defining or modifying

a scheduled activity, installing a token, updating a server agent configuration and so on. Additionally, the CPTRAX agent will save/archive the registry key each time the agent is started – even if there have not been any changes since the last save.

Once installed, CPTRAX will allow functionality as specified by the token(s) you install. And, depending on the token(s) installed, you would define activity profiles to track file system and connection activity with optional control on file system activity. Alerts can be configured and delivered via email and/or the [cptalert.exe desktop alert agent](#) (uses TCP/IP). For the [Auditor token type](#) you would merely configure the Department and Enterprise host settings. More regarding the Auditor token in [Chapter 4](#).

Departments and Enterprise host settings are further elaborated upon later in this section.

For CPTRAX agents hosting a Department or where no Department membership is defined, activity log files are stored in a folder named “cptlogs” created on the reporting share identified during installation or follow-on configuration. These log files are created in response to profiles that define actions to track.

Activity log files are uniquely named for the date of activity, server where collected and profile name. There will be a single file for any specific date for activity from a selected server for a particular profile. As log files are received they are concatenated to ensure the one file for one date/server/profile rule.

Actions on your workstation

On the workstation or server where CPTRAX Administration console (`cptrax_console.exe`) is run upon, a registry key structure will be created under the

`HKEY_CURRENT_USER\Software\Visual Click Software, Inc.`

key. This registry key stores details used by the `cptrax_console.exe` such as servers listed in the CPTRAX Console and Alert Console settings used separately by `cptalert.exe`.

Therefore, if you regularly use a specific workstation with `cptrax_console.exe` and sometimes use a different workstation you will notice different settings (or none at all) for these tabs. To quickly establish your settings on the “sometimes” workstation you can export this registry key with the Windows tool (`regedit.exe`) from your regular workstation and import on your “sometimes” workstation.

The CPTRAX Administration console uses the following communication protocols:

- SMB – each require a sufficiently privileged logon
 - Secure Registry is used when connecting with a selected server; used when working with profiles, custom reports, scheduled activities and server configuration
 - Named Pipes are used when gathering CPTRAX server agent details shown on each server tile
 - File System services are used when managing and reporting from files

- Control Panel services – to install, remove, start and stop the CPTRAX server agent
- TCP/IP – Port 4060 is opened and used by the CPTRAX Server Agent
 - Scanning for current active `cpalert.exe` users

The CPTRAX Alert Agent (`cpalert.exe`) uses TCP/IP to connect with and receive alerts from selected CPTRAX Server Agent(s). The TCP/IP port used by `cpalert.exe` is automatically configured when loaded, it communicates this port to the CPTRAX Server Agent and this port number can be viewed via the “View Active Alert Agent Connection” located at the bottom of the ‘Settings’ tab.

Departments and Enterprise Hosts

In brief, if no Departments or [Enterprise Hosts](#) are defined each server where CPTRAX is installed it will operate in a stand-alone capacity. The main result being report generation of activity recorded will require direct access to each such defined server. You may be wondering how else reporting can be accomplished. The balance of this section will provide further details.

Defining a Department

Because CPTRAX for Windows only expects its server agent at each server to be connected via the same network and is not expecting a common domain or forest membership we developed two conveyances to allow servers hosting CPTRAX to connect and work together. The first is the Department; the second is the Enterprise Host Server (described in next section).

A Department is simply a name you define. The Department name you choose is only shared between CPTRAX server agents. The Department’s focus is to establish where CPTRAX Activity Log files are to be stored. When a CPTRAX server agent records an activity (Active Directory, file system, logon/logoff, GPO change), the activity is queued, finalized and finally transmitted to its destination(s). A server can host *one Department only* (which it is automatically a member of) and/or be a member of one or more Departments.

The *default* is for no Department and for no Department membership to be defined. In this *default* case the completed log files are merely moved from the “cptrax” folder to the “cptlogs” folder in the reporting share path.

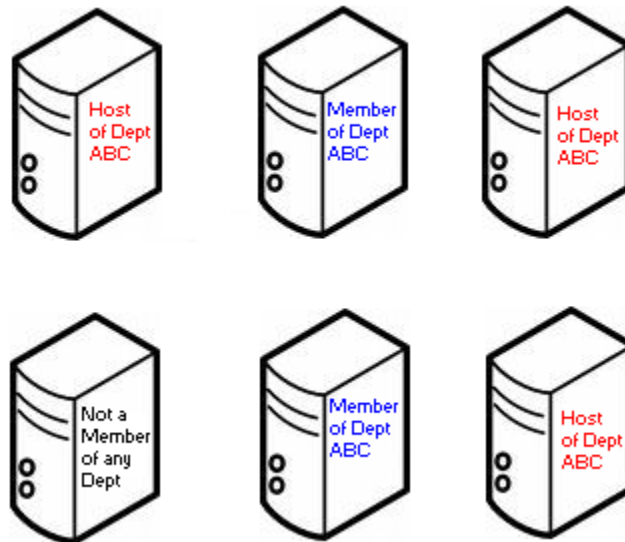
If a CPTRAX server agent is defined as a “Department Host” it becomes a repository for that Department. It also automatically becomes a member of that Department. Multiple servers can host the same Department; each will be a repository for log files destined for that Department.

When a CPTRAX server agent is a Department member it means that server agent will transmit its log files to all servers hosting that Department. All log files transfers rely on TCP/IP – no SMB traffic is generated.

By defining a CPTRAX server agent as a member of a Department, it will send its log files to each Department host. Because a Department may be hosted by multiple servers (each running the CPTRAX server agent), Department members will transmit their complete log files to each server hosting each Department it is a member of. Each Department server will have the same

copy of the transmitted log file. The frequency of log file transfer is defined per server and ranges from every 15 minutes to once a day.

The following figure shows 6 servers, 3 that host Department “ABC” and 2 that are members of the Department “ABC” and one that is neither a Department host nor a member of any Department:



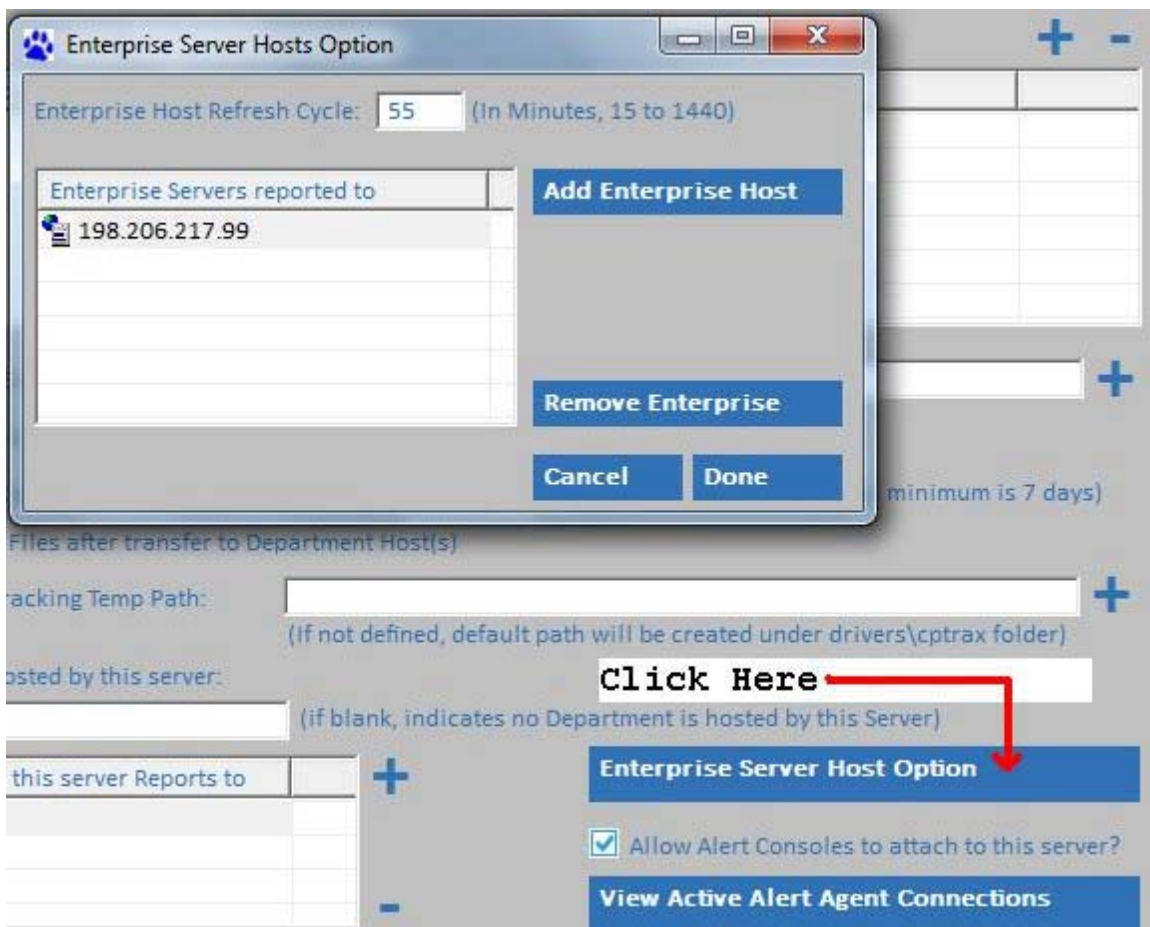
The 3 that host Department “ABC” will contain log files from the 5 servers that are a member of Department “ABC”. Recall that a server that hosts a Department is implicitly a member of that Department. Also recall that it does not matter what Domain or Active Directory Forest any of these servers belong to, the CPTRAX Server Agent on each server will communicate with the others.

The question is, exactly how do these servers “know” about each other? The answer is revealed in the next section.

Defining an Enterprise Host

Because there is no reliable common method for unrelated servers to find each other in a Windows® network, we developed the Enterprise Host model. This was required for CPTRAX Server Agents to find Department Hosts and to find other servers running CPTRAX.

The configuration of the CPTRAX Server Agent on servers includes what we call the “Enterprise Host” or “Enterprise Server”. Please reference the following screen:



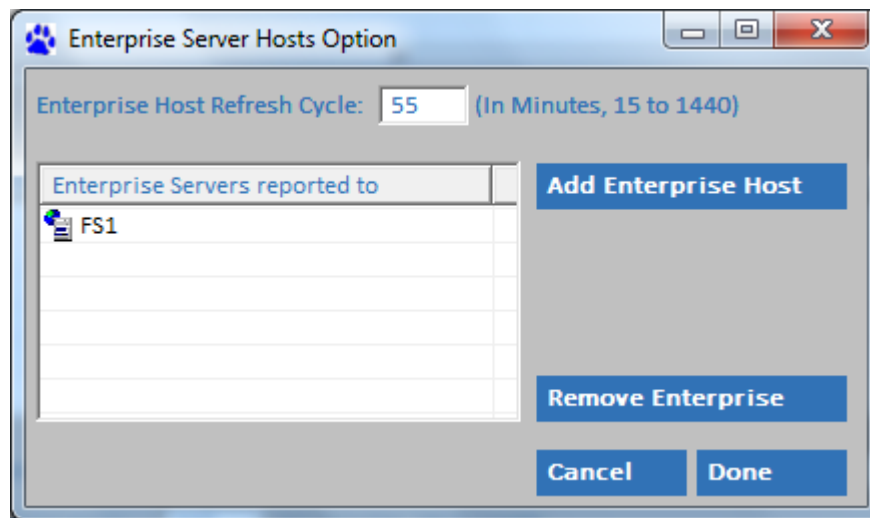
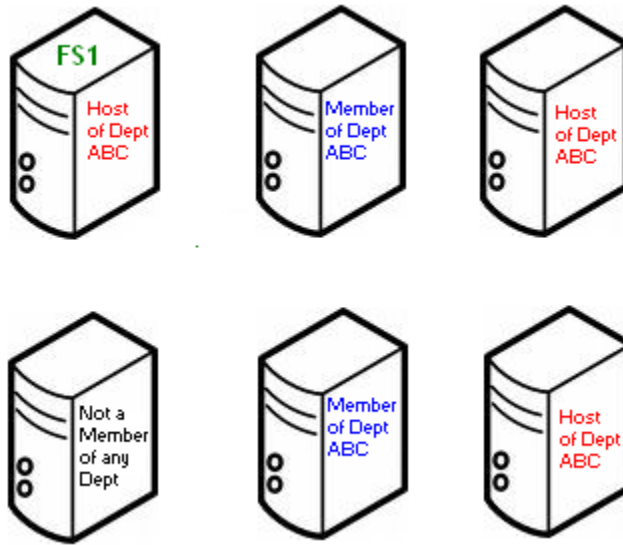
The “Enterprise Servers reported to” list provides the missing ingredient for CPTRAX Server Agents to locate one another. The method employed is simple. CPTRAX on each server can include a list of one or more Enterprise Servers to report their status to. The Enterprise Server name can be specified by its NetBIOS name (*server*), or its IP address (*10.1.1.1*).

Please note that an Enterprise Server is designated as such because you configure other servers to report to it instead of selecting an option that makes a server become an Enterprise Host.

Note: If desired, you must configure the Enterprise Server to report to itself as this is not performed automatically. It is likely you will want the Enterprise Server to send its report logs to itself.

Any server running the CPTRAX Server Agent can be designated as an Enterprise Host.

In the image below, each server is configured to report to FS1:



Notice that the Enterprise Server name can be specified by its IP Address or its NetBIOS name.

The Enterprise Server “FS1” will receive communications from each server configured to connect with it as one of its Enterprise Hosts. Data transmitted includes what Department(s) are hosted as well as its number of ready log files.

Each server that hosts or is a member of a Department will connect with the Enterprise Server(s) and request which servers are hosting that Department and subsequently transmit its activity log files to those servers hosting the named Department.

All CPTRAX Server Agent TCP/IP communications occur on port 4060.

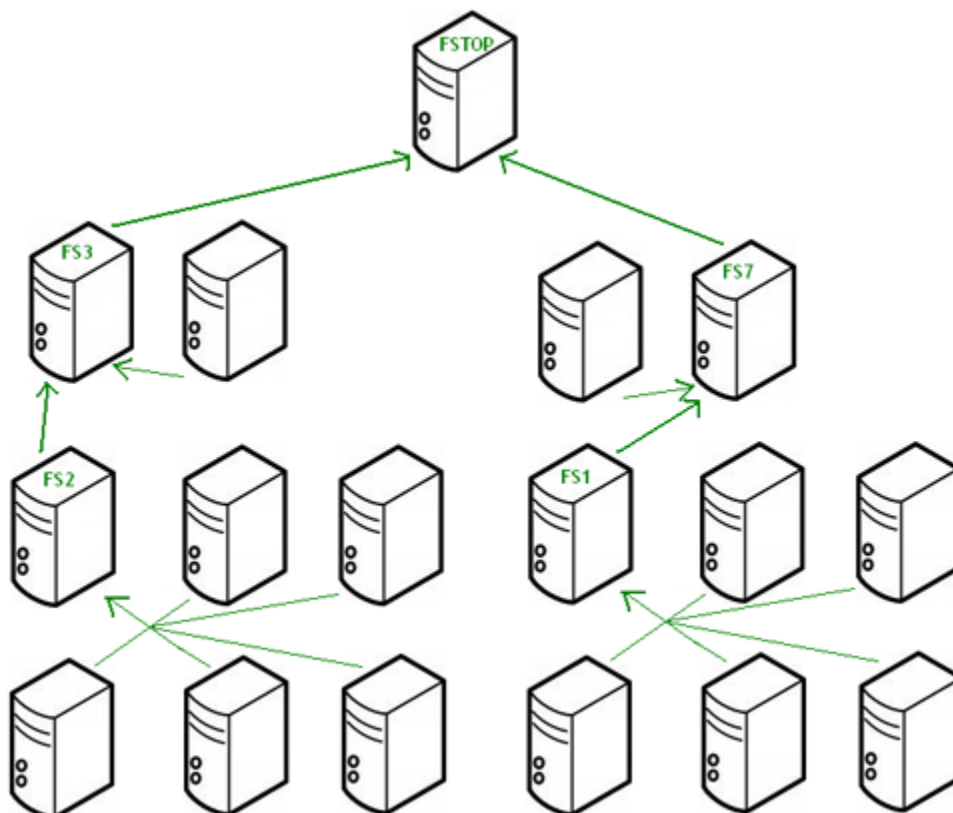
Please note that the CPTRAX Server Agent has been permanently assigned TCP/IP port 4060 (a decimal number) by the Internet Assigned Numbers Authority, see this link:

<http://www.iana.org/assignments/port-numbers>

Combining Enterprise Hosts

If you define servers that are designated as Enterprise Servers to report to other Enterprise Servers, the list of all servers known by each Enterprise Host will be shared with all.

This means, if you query the topmost Enterprise Server you will be able to view all servers below it. This enables you to quickly and easily view part of or all of your CPTRAX installation. Please see the following image:



The server FSTOP is the topmost Enterprise Server that, when queried, will reveal all servers shown in the image as each reports to an Enterprise Host and in turn reports up to (“upstream”) servers that ultimately report to FSTOP.

If you were to query server FS7 you would see only the server that reports to it and all those reporting to server FS1.

FAQ: Department and Enterprise Hosts

Q: Can I define a Department Host but no Enterprise Host?

A: Yes you can but what will occur is no log files (other than those generated locally) will be received by that server defined as a Department Host. This is because the server is not identifying its Department Host configuration to any Enterprise Host and therefore other servers

running CPTRAX that are a member of that same Department will not know about that server and will not consequently transfer log files to it.

Q: Can I define servers with an Enterprise Host(s) to report to but not define a Department and what would that accomplish?

A: Yes you can do this. It is valid because this allows you to easily check the status/health of all servers where you have CPTRAX installed – performed via the ‘Enterprise View’ tab in the CPTRAX Administration console.

Q: What if my selected Enterprise Host is down or otherwise unavailable?

A: There is no limit on the number of servers that can be established as an Enterprise Host – thus, establish more Enterprise Hosts. If your Enterprise Hosts are down/unavailable, CPTRAX Server Agents that depend upon such Enterprise Hosts will store their log files locally until the host(s) are again functioning. Any such affected log file(s) will not be transmitted to any defined Department Hosts because at the time they were created and ‘transmitted’ (that is, moved to the local reporting share) there were no identifiable Department Hosts. Thus, reporting of any such log file(s) will need to be done directly on each server where the logs are found.

Q: What if a Department Host is down or otherwise unavailable?

A: Each member server will “hold” any log files destined for the selected Department Host in its \SystemRoot\System32\Drivers\CPTRAX\Q (or \SystemRoot\SysWow64\Drivers\CPTRAX\Q) folder until such time as the server hosting the Department is available, regardless of how long it takes for that server to come back online.

If a server that hosts a Department is offline for more than 24 hours, the Enterprise server(s) will drop their memory of that Department Host and no further log files will be prepared for delivery to that Department Host server. Only after that server comes back online will any new log files be prepared and transmitted to it.

Chapter 2 – CPTRAX Installation

Installing the CPTRAX Download Package

To begin your installation of CPTRAX, download the installation package from the Visual Click website. You may have received a link to this package in an email or it may have been made available to you in other way such as direct FTP download.

Once retrieved, run the package:

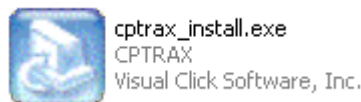


Figure 2-1

You will be presented with a screen similar to the following:

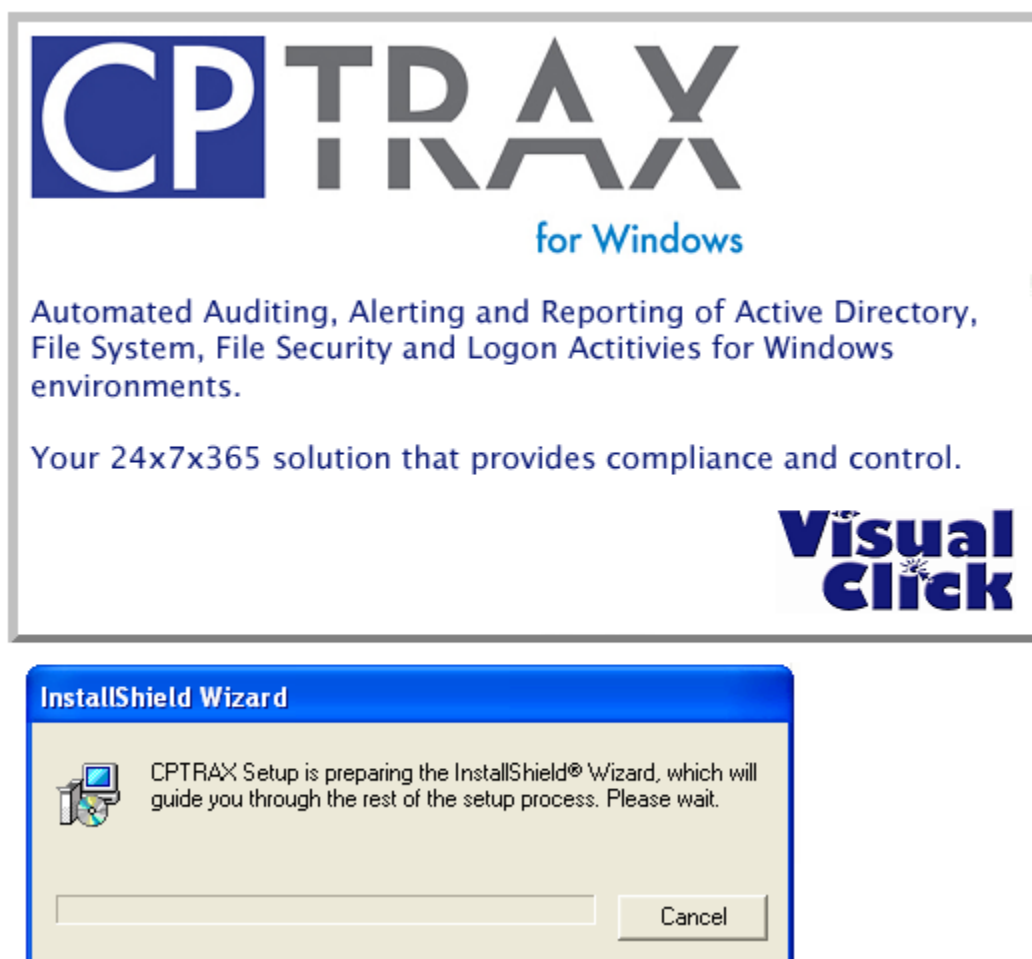


Figure 2-2

Continuing, the following will be shown:

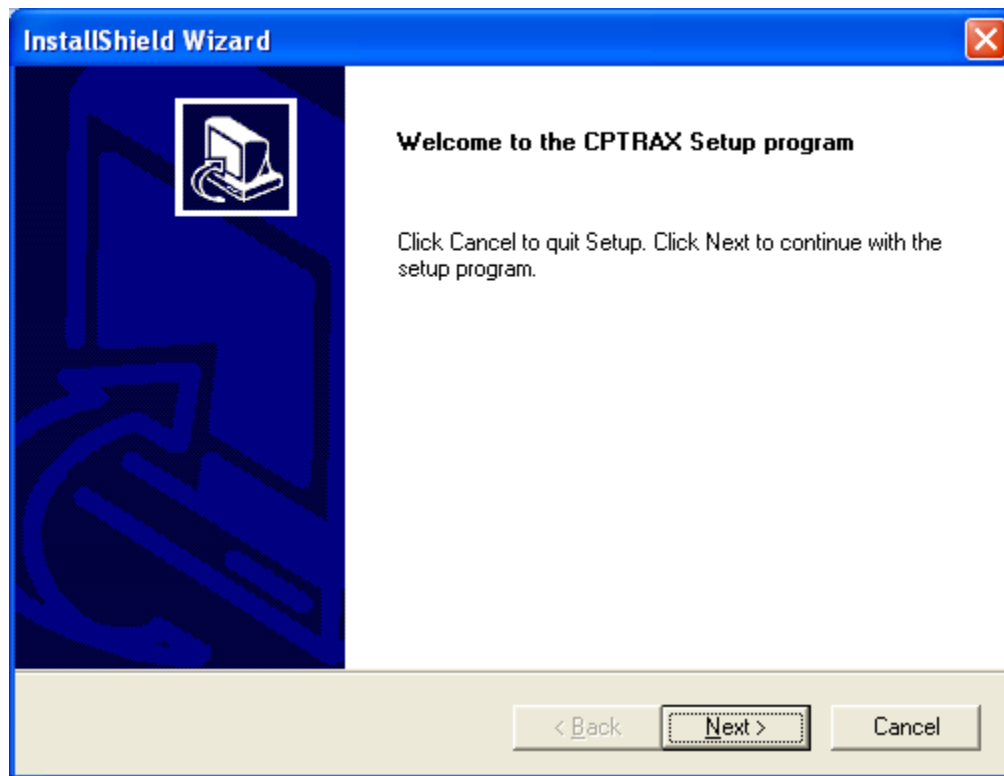


Figure 2-3

After clicking the "Next >" button, the following will be displayed:

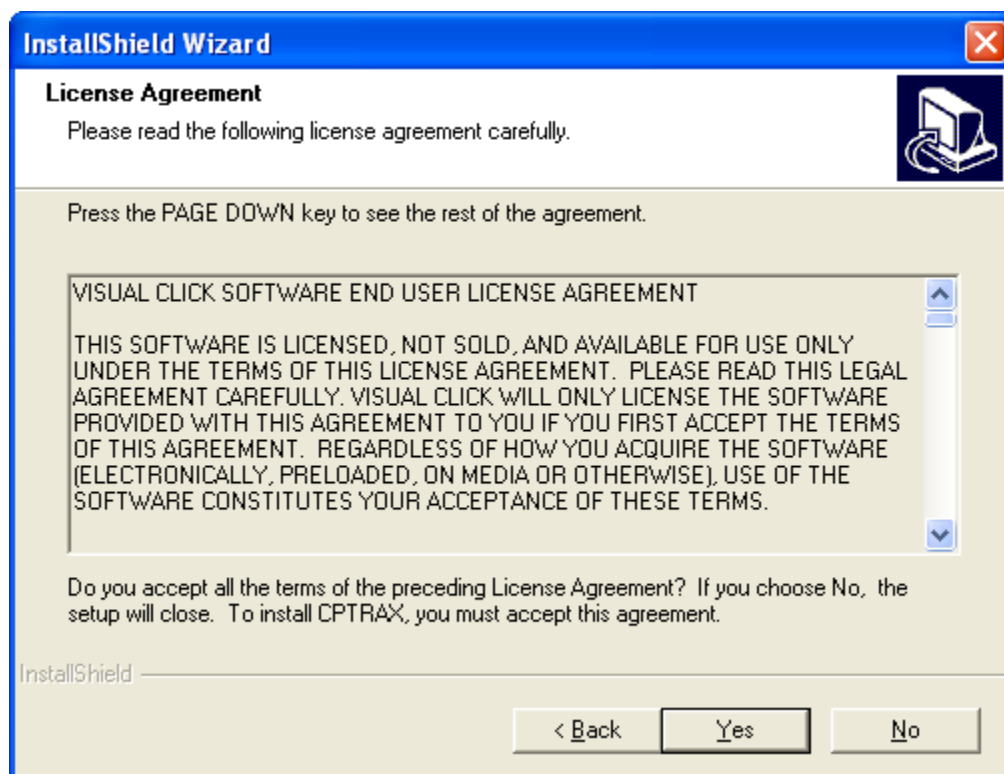


Figure 2-4

The End User License Agreement or EULA shown in figure 2-4 is also found at the [beginning of this guide](#).

Once the “Yes” button has been clicked, the next screen will be:

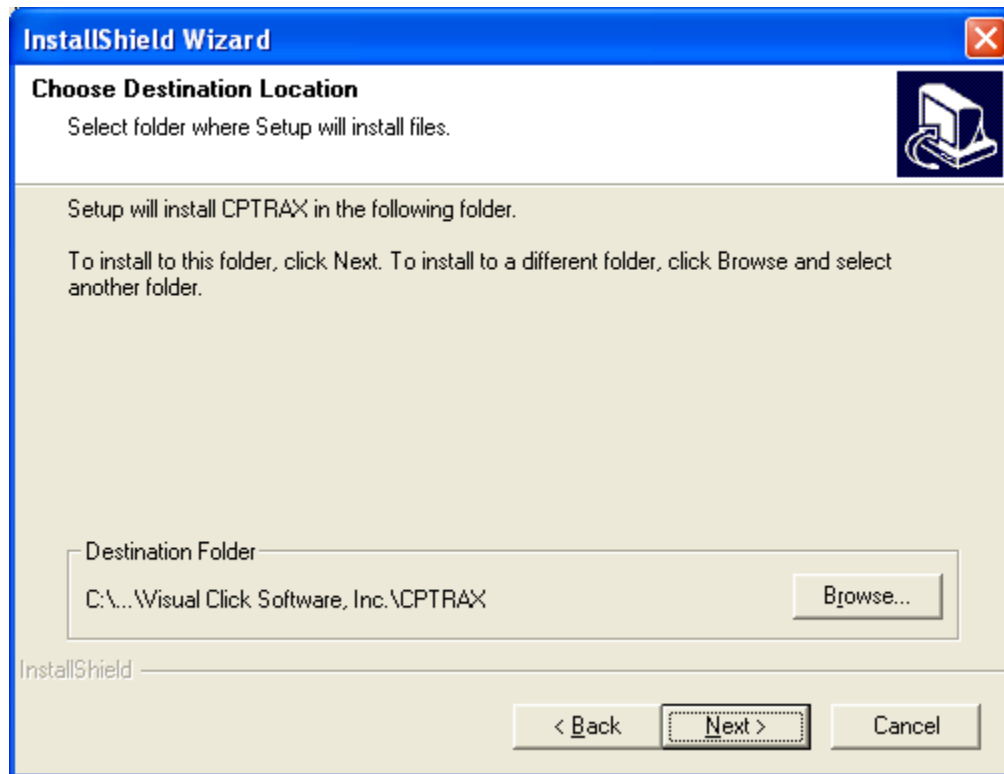


Figure 2-5

The destination folder specified is for placement of the CPTRAX for Windows® Administration Console and server installation files. Actual installation of CPTRAX’s Server Agent on your server(s) will occur separately and at your specific direction. See the [Basic Installation](#) section later in this Chapter for further details.

Once the “Next >” button is clicked the following screen will be shown:



Figure 2-6

After making your selection, click the “Next >” button to reveal:

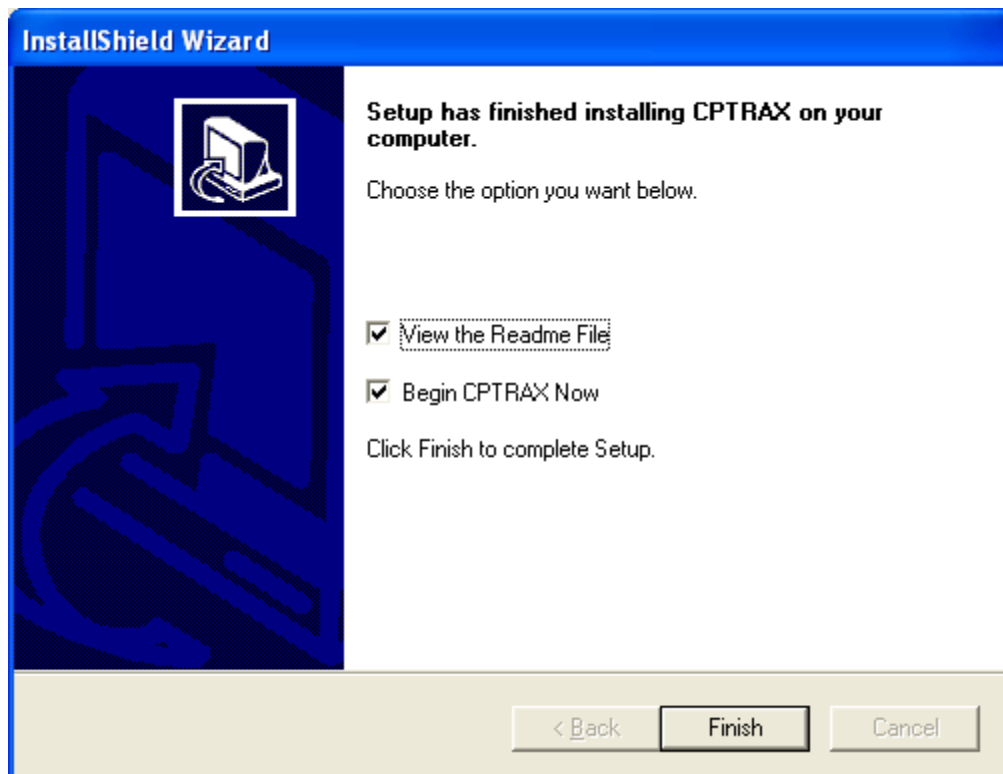


Figure 2-7

If you selected to start “CPTRAX now” you will be presented with the CPTRAX for Windows Administration Console.

CPTRAX Basic Installation

Setting up your first server

After downloading and running the installation package, start the CPTRAX Console (cptrax_console.exe). Once running you will be presented with the following or similar screen:

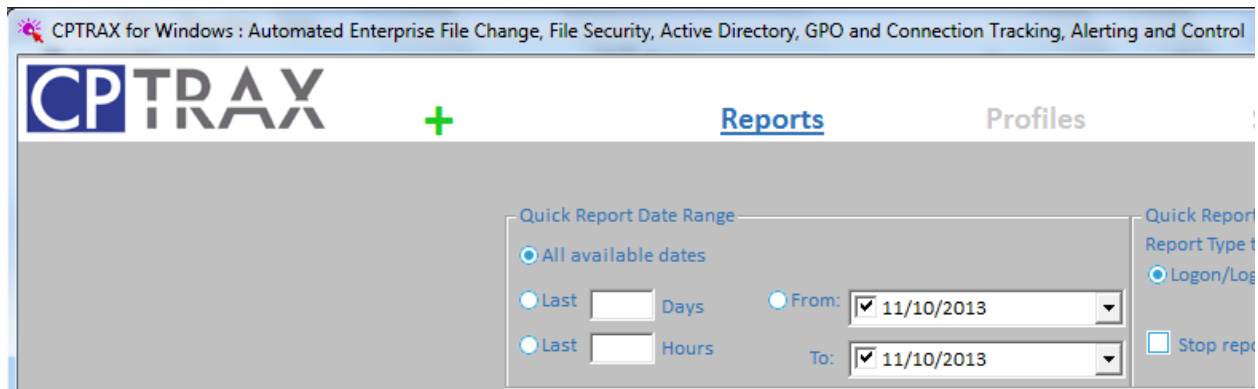


Figure 2-8

Click the green + symbol to begin the process of adding CPTRAX to a selected server or domain controller. The "Add New Server" window appears.



Figure 2-9

Enter the server name or IP Address in the "Name of Server for CPTRAX Installation" field. Separately, in the "Name of Share on selected Server" field, type in CPTRAX_Logs or the name of an existing shared folder to store CPTRAX's log files. You may choose any name for the Share, the name CPTRAX_Logs was selected only for illustrative purposes. Click the "Next" button to continue the installation.

If you are uncertain as to the name of server or existing share, click the "Select Server and Share" button at the lower left.

The selected Share must already exist. The "Add New Server" process does not include creating the Share. If you need to create the Share, please follow the instructions shown in [Appendix C](#). To ensure proper operation of the selected Share, please also refer to [Appendix D](#) and [Appendix E](#).

Continuing CPTRAX Installation after Server and Share selection

Once you have selected the Server and Share as shown in Figure 2-9, click the Next button. Before continuing, the installation process will automatically attempt to connect to the selected server and verify your permissions and presence of the designated Share. If any of these verifications fail you will be notified and the installation will stop until corrected.

Once connectivity and permissions are verified the "Add License" window appears.



Figure 2-10

Click on the "Select License File" button and browse to where your CPTRAX Token file(s) are located. This process only uses one Token file. If your CPTRAX purchase includes multiple Token files you will only choose one for this step. The remaining Token files can be installed after from the Settings tab.

If you are unfamiliar, the CPTRAX Token file's name will be alphanumeric with a .TKN extension. Highlight the Token file and click the "Open" button. Notice the full file path of the selected Token will appear. To continue, click the "Next" button and the "Install Options" window will appear.

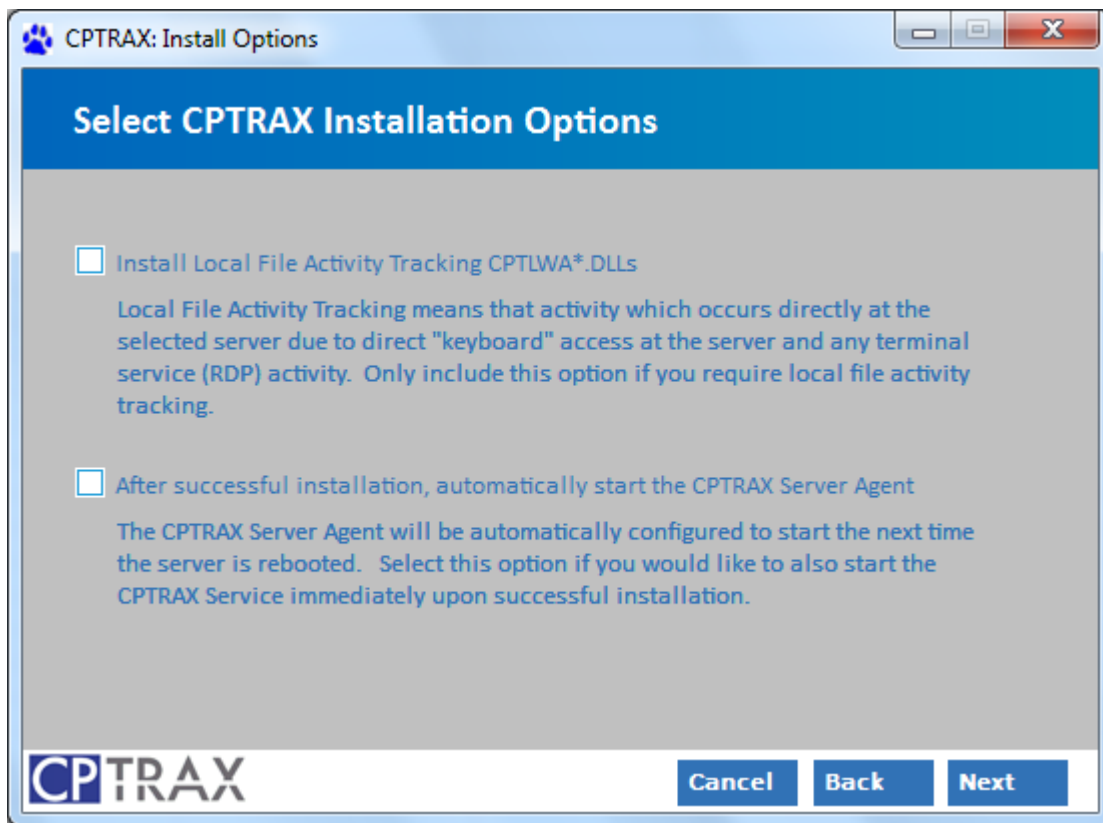


Figure 2-11

There are two option selections. The first option is to "Install Local File Activity Tracking CPTLWA*.DLLs". Only select this option if you require tracking File System and/or Group Policy (GPO) activity that occurs directly via the Server's keyboard/console or via a Remote Desktop Connection.

The second option is "After successful installation, automatically start the CPTRAX Server Agent". Selection of this option will automatically start the CPTRAX Service on the selected Server after the installation process has completed. Whether this option is selected or not, please note that the CPTRAXW Service will be set to automatically start whenever the server is rebooted.

Select the appropriate options for your environment and click the "Next" button.

The "Verify and Begin Installation" window appears.

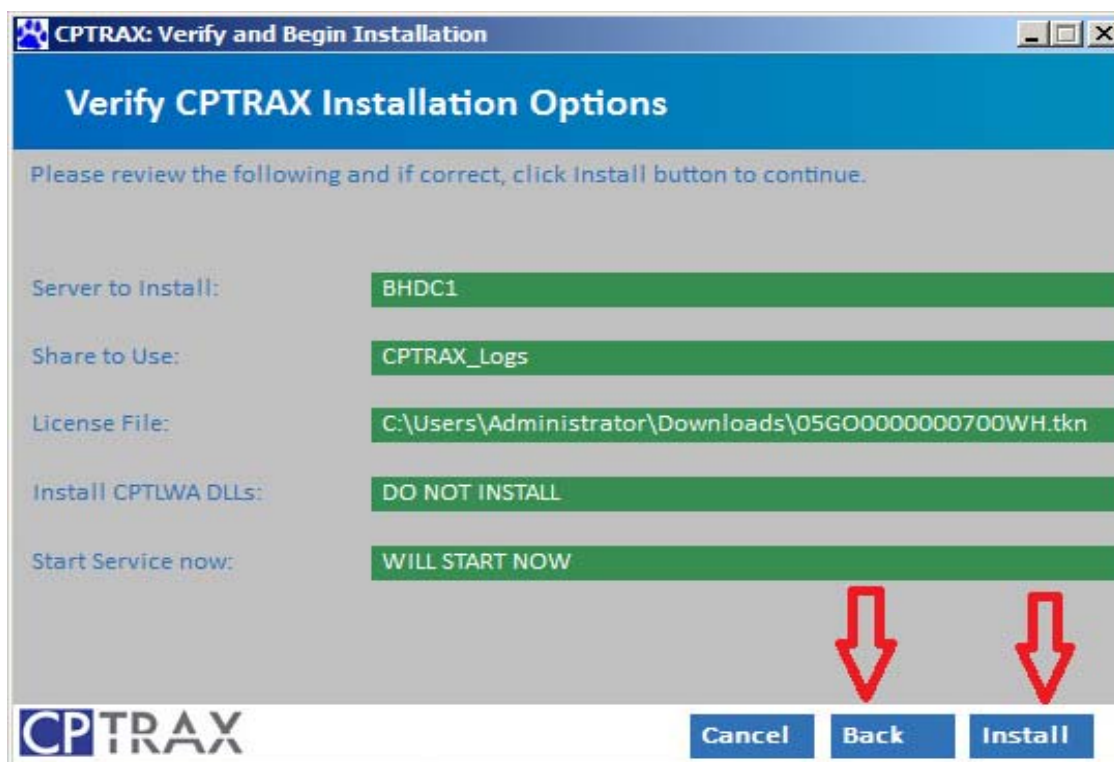


Figure 2-12

Review the configuration settings. If you need to make any changes click the "Back" button and revise. If the configuration is correct click the "Install" button and the “CPTRAX Add New Server Results” window will appear.

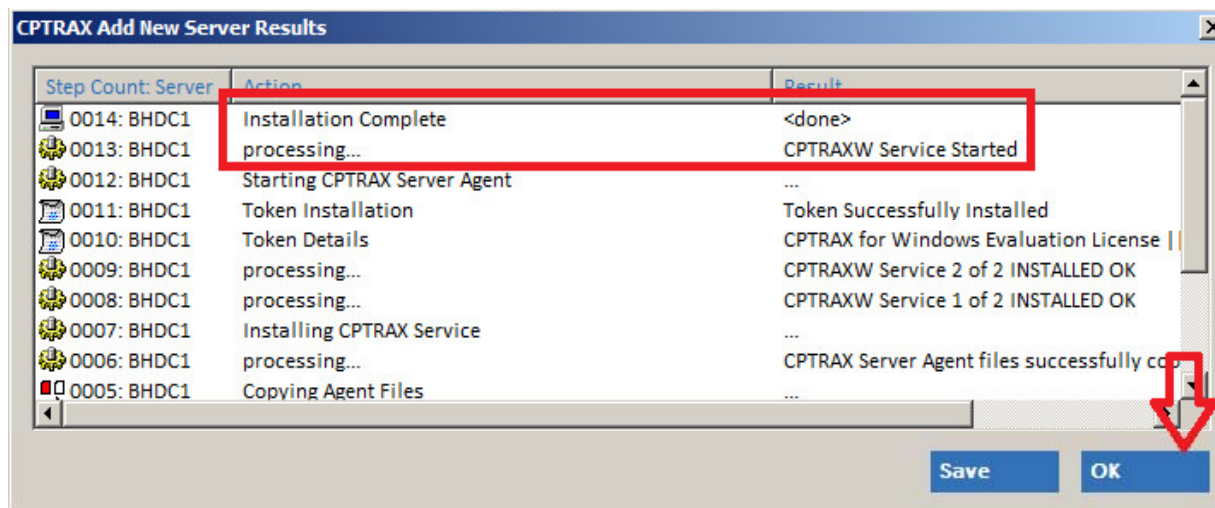


Figure 2-13

Each column can be sorted. The first column can be sorted to reveal each step in order of its progress. The “Save” button can be used to save the installation results.

After you click “OK” on the results window please note the selected Server will appear on the left side of the CPTRAX Console.

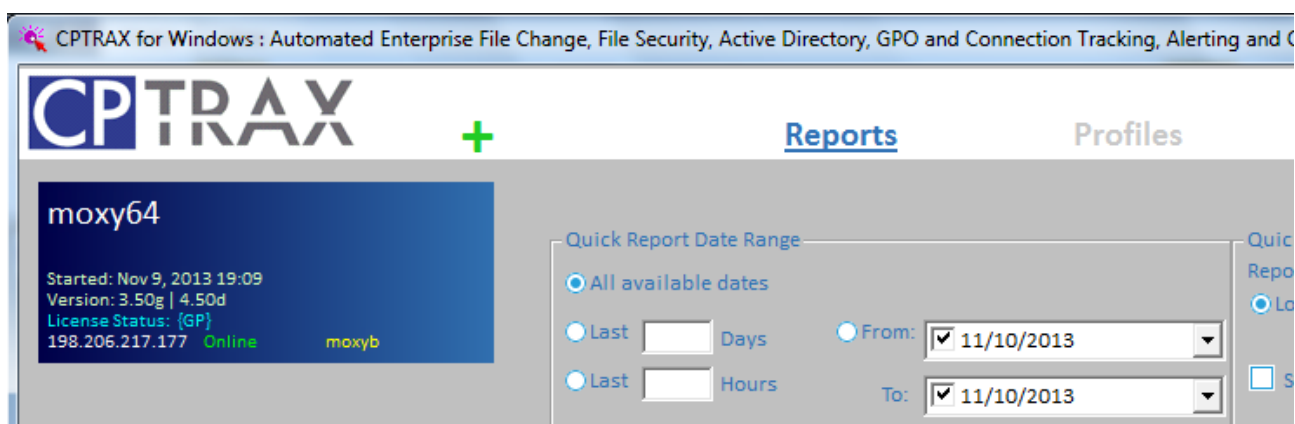


Figure 2-14

Notice the Server Tile will appear. On it you will find the Server name, CPTRAX Agent status and if started, its versions and license status. Also included are the Server's IP Address and status such as "Online".

You may notice the status includes the message "Agent Stopped!". This is normal behavior when the CPTRAX Agent is initially starting. It can take up to 5 minutes for the load to complete. However, the load is usually complete within 2 minutes. If you see "Agent Stopped" when the agent is first started, wait approximately 1 to 2 minutes and the Console will refresh and display the "Started" date and time, CPTRAX "Version" information, and "License Status". If the message "Agent Stopped" persists then exit the Console and restart.

If "Agent Stopped" remains then something has prevented the CPTRAX Agent from starting. Please contact supportw@visualclick.com.

Congratulations! You have successfully installed the CPTRAX for Windows Server Agent.

The next step will be to complete the configuration and start CPTRAX working for you.

CPTRAX Configuring Profiles

With CPTRAX you can pinpoint what you want recorded, alerted and controlled. Define these activities with Profiles. Profiles are stored in the Registry of the selected server that hosts the CPTRAX Agent in the following key:

```
HKEY_LOCAL_MACHINE\Software\Visual Click Software, Inc.\CPTRAX\Profiles
```

Creating and managing Profiles is performed via an encrypted SMB connection to the selected server's Registry. Your logon account at the selected server must be sufficiently privileged to perform Registry modifications in the Registry key defined above:

To define a Profile, start by selecting the 'Profiles' tab located at the center-top in the CPTRAX Administration Console (reference Figure 2-14). Next, click the **+** sign at the top right of the "Profiles" list which will initially be empty. The following window appears:

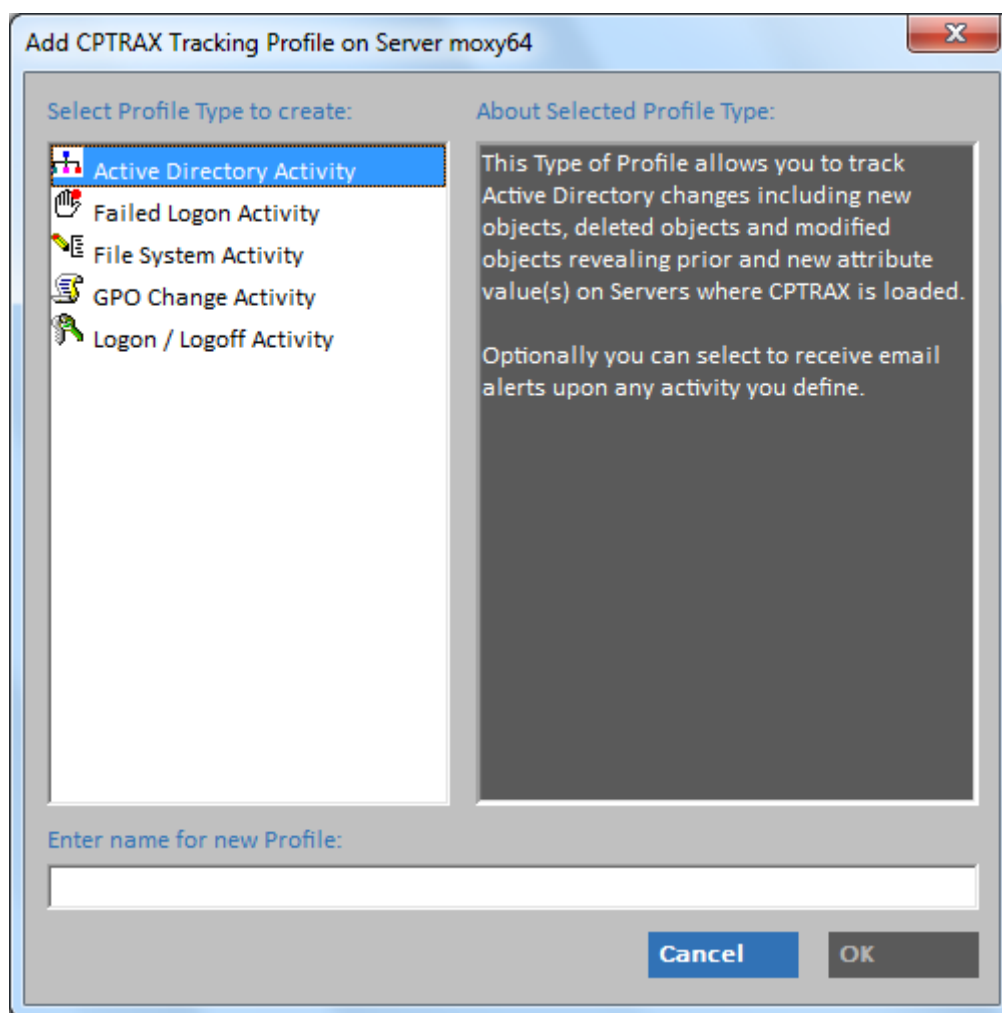


Figure 2-15

File System Activity Profile: Add New

In this first example, select 'File System Activity' and enter the name "FS Test 1".

Click OK, and, you will be immediately presented with the following screen:

Figure 2-16 shows the 'Edit File System Activity Tracking and Control Profile FS Test 1' window. The window has a title bar with a paw print icon and the text 'Edit File System Activity Tracking and Control Profile FS Test 1'. The main area contains a table with the following columns: 'Shares, Folders, Files & Extensions', 'Shares Only?', 'FolderOnly?', 'FileOnly?', 'TrkDel', 'TrkWrt', 'TrkCreate', 'TrkRename', 'TrkOpen', 'TrkACLs', and 'BlkDel'. Below this table is a section for 'Users To Exclude' with columns: 'Users To Exclude', 'Excluded from Tracking?', 'Excluded from Blocking Actions?', and 'SID'. At the bottom, there are two checkboxes: 'Send Email Alerts to Accounts defined on the server configuration screen' and 'Allow Alert Console (cptalert.exe) Users to receive Alerts from this Profile'. There is also a 'Define Email Alert' section with a text input field and two buttons: 'Add Email Address' and 'Revise Email Address'. On the right side of the window, there are several buttons: 'OK', 'Cancel', 'Add', 'Edit', 'Remove', 'Add', 'Remove', 'Remove selected Email Addresses'.

Figure 2-16

All profile editing is per server, there is no option to edit a Profile across multiple servers. You can however, use drag-and-drop to copy Profile(s) to a different server, more on this later in this section.

File System Activity Profile: Add Tracking / Blocking Item

CPTRAX for Windows will track file system activity generated remotely (such as via a mapped share), locally and via terminal services

To continue, click the 'Add' button near the top right side and the following screen will appear:

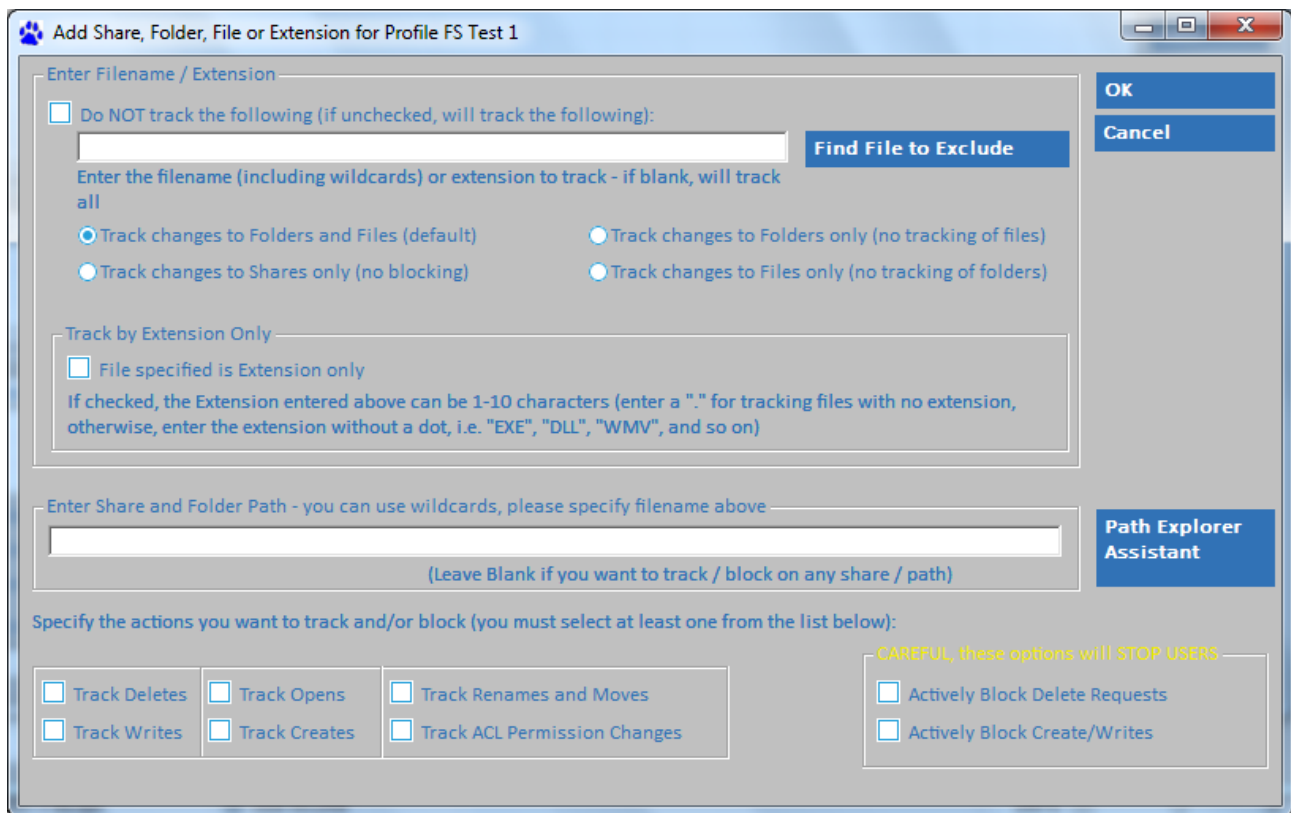


Figure 2-17

On this screen you define the file system path and specific action(s) you want tracked and/or blocked. Details for each data field are provided on screen. The screen shown in Figure 2-17 enables you to get very specific in what you want to occur.

Please note, that in the long edit field described as “Enter Share and Folder Path...” you can also specify the native pathname such as C:\originalPath\sublevel\and_so_on. Click the button ‘Path Explorer Assistant’ to assist in locating the path you want to track/block. It will only show Public Shares. No admin shares such as C\$, D\$ will be shown though you can manually enter them.

The Share path entered is deciphered by the CPTRAX Server Agent to provide tracking/blocking on the native underlying path. The Share path is used by the server agent as a reference point to obtain the native path. Thus, regardless of how the user accesses the file system, the absolute “underlying path” will be known and CPTRAX will provide tracking and/or blocking as defined in each Profile. Tracked user access includes local, terminal server, remote (mapped drive or UNC path), FTP access including access by Macintosh workstations.

When finished, click OK and you will be returned to the main screen for the Profile:

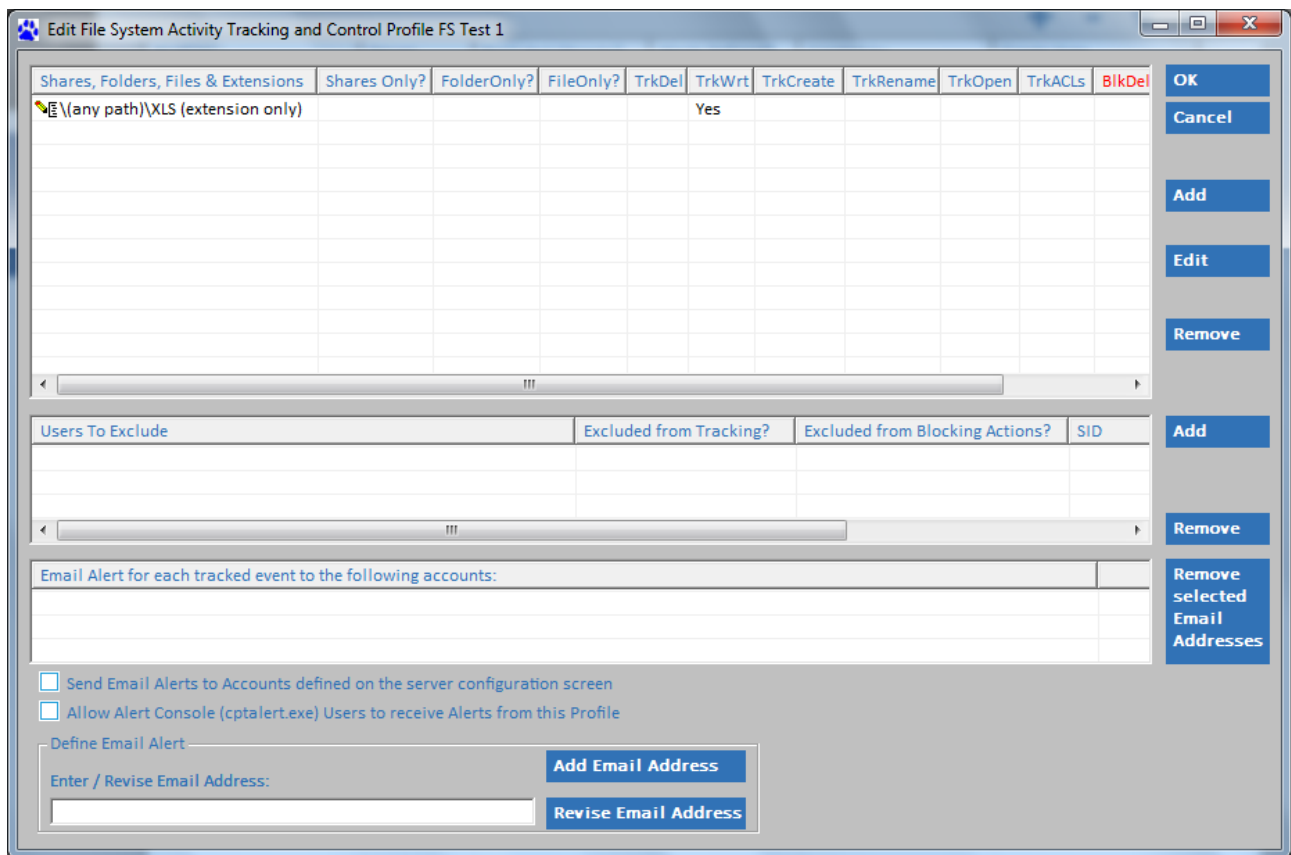


Figure 2-18

In the example above we defined to track all writes to any XLS file anywhere on the server (any share, any path, any volume, any drive).

For each new item you want to track block, click the “Add” button and fill in the resulting screen (as shown in Figure 2-17) as required.

File System Activity Profile: Add Users to Exclude

There are certain accounts where tracking and blocking are not required. For instance, backup user accounts that only perform backup chores typically are not included in tracking or blocking. Additionally you may have accounts you want tracked but to be excluded from blocking actions.

To exclude an account, click on the “Add” button to the right of the ‘Users To Exclude’ view. After you click Add, the following screen will appear:

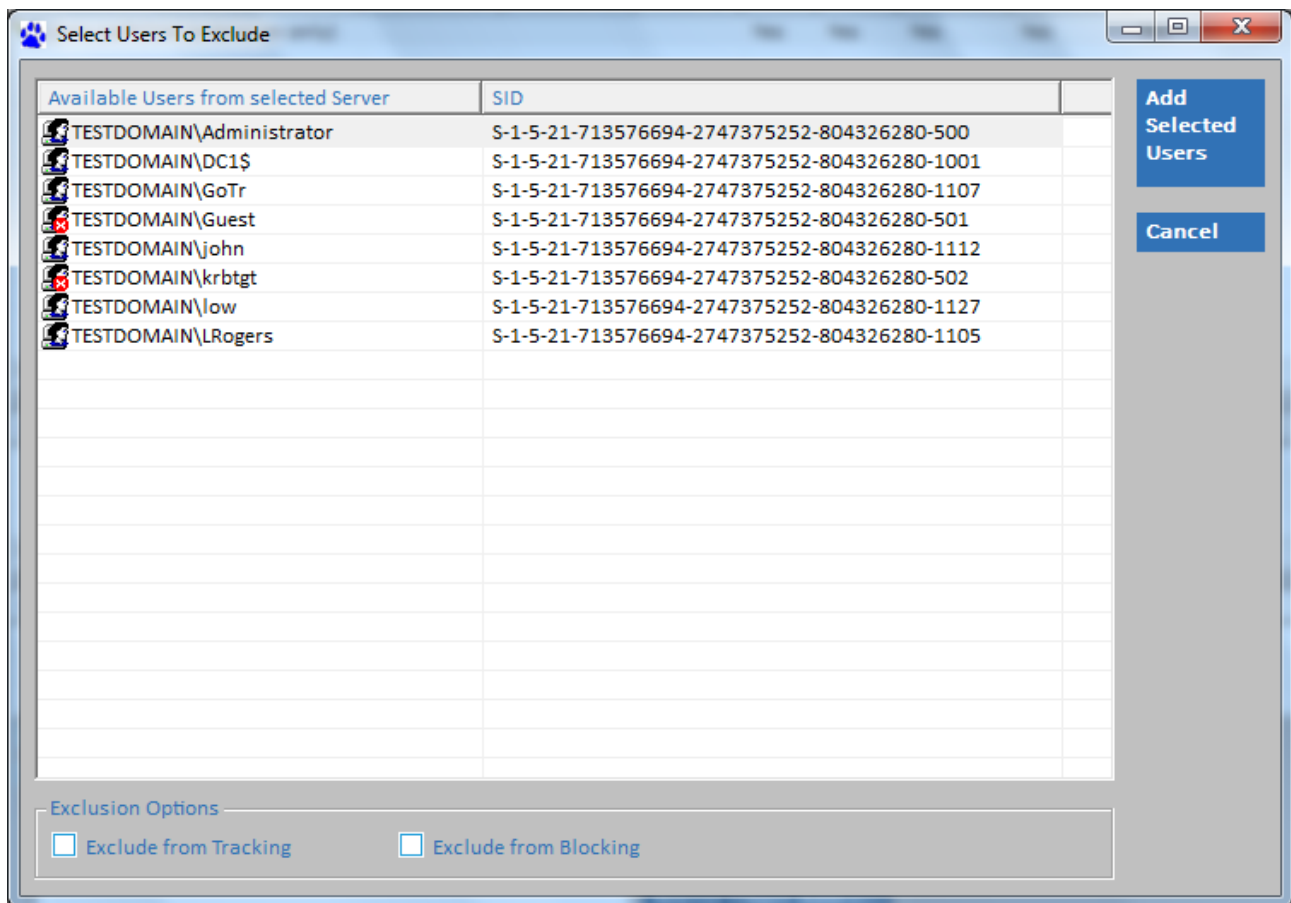


Figure 2-19

The list of accounts presented are all those accounts that are locally known to the server. Select the account(s) you require and check the boxes below to specify the desired type of exclusion. The objects where the icon has a red “x” indicate those accounts that are disabled (and cannot currently logon). To add accounts with different exclusion settings you will need to click ‘Add’ for each desired exclusion variation.

When ready, click ‘Add Selected Users’ and you will be returned to the main screen for the Profile:

Edit File System Activity Tracking and Control Profile FS Test 1

Shares, Folders, Files & Extensions	Shares Only?	FolderOnly?	FileOnly?	TrkDel	TrkWrt	TrkCreate	TrkRename	TrkOpen	TrkACLs	BlkDel
\\(any path)\XLS (extension only)				Yes						

Users To Exclude	Excluded from Tracking?	Excluded from Blocking Actions?	SID
GREENLAND\Superuser	YES	NO	S-1-5-21-1258623138-1789777589

Email Alert for each tracked event to the following accounts:

☐ Send Email Alerts to Accounts defined on the server configuration screen
☐ Allow Alert Console (cptalert.exe) Users to receive Alerts from this Profile

Define Email Alert

Enter / Revise Email Address: Add Email Address Revise Email Address

Figure 2-20

File System Activity Profile: Alerts

There are two methods to receive alerts from the CPTRAX Server Agent. The first is via email. The second is the [Alert Console](#). To define email alerts, enter the destination email address in the “Enter / Revise Email Address” field and click on the “Add Email Address” button.

You may also check the “Send Email Alerts to Accounts defined on the server configuration screen” and “Allow Alert Console Users to receive Alerts from this Profile”.

Note: For email alerts to be sent, the server configuration screen must define the “sending” email account. This is discussed later in this [Chapter 4, Settings](#).

The Alert Console is further discussed at the [end of this chapter](#).

An alert is generated for each capture event. Alerts are sent in real-time.

File System Activity Profile: Done

When finished editing the File System Activity Profile, click on the “OK” button (clicking “Cancel” will abort all changes). If the CPTRAX Server Agent is active it will realize the change has occurred and will wait 2 minutes for all changes to be processed and then it will re-read all Profiles and begin acting on them as defined.

Important Notes about Server Agent Startup:

When the CPTRAX Server Agent is started it can take up to 10 minutes before initializations are complete and it is ready to act on Profiles.

For Remote File System Tracking and Control:

For users connecting via workstations and are **not** logging in locally or via terminal services please note that due to the methods utilized by the CPTRAX Server Agent, you may need to reboot or Logoff/logoff from your workstations to be accurately tracked and controlled. When in general use, the CPTRAX Server Agent is started at the same time the server is starting so there is usually no need to ensure workstations have reboot or logged off. However, if you are evaluating or upgrading the CPTRAX Server Agent please ensure you reboot or completely logoff /log back on your workstations that you are expecting to track and control

For Local and Terminal Services File System Tracking and Control:

For users connecting locally at the server and via terminal services, there is no requirement to logoff and logon for the CPTRAX Server Agent to effectively track and control, however, the 10 minute initialization period must be allowed to complete before the server agent is ready.

Logon / Logoff Activity Profile: Add New

CPTRAX for Windows provides Logon / Logoff tracking for all connections, remote (via NTLM, NTLMSSP, Kerberos and FTP), local and terminal services.

Note: If you require tracking of who is logging into individual workstations (versus who is logging into servers and terminal servers) you will want to refer to our [Technology Partner Integrity Software](#) and its SofTrack product. SofTrack includes local workstation activity tracking.

In this second example, from the ‘Profiles’ tab located at the center-top in the CPTRAX Administration Console (Figure 2-14), click the + sign at the top right of the “Profiles” list and then select ‘Logon / Logoff Activity’ and enter the name “LL Test 1”:

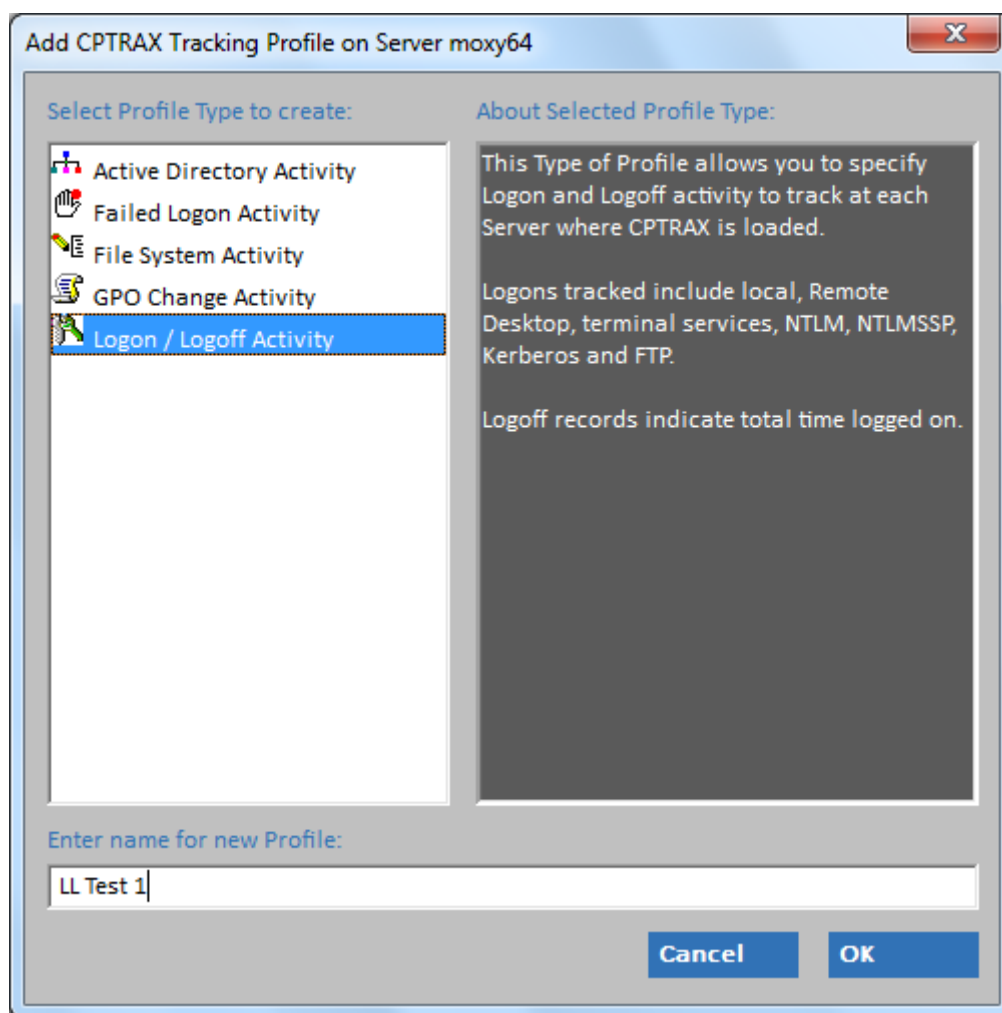


Figure 2-21

Click OK, and you will be immediately presented with the following screen:

Edit Logon / Logoff Activity Tracking Profile LL Test 1

IP Ranges to Include & Exclude	Exclude IP Range?

Define IP Range

☐ Exclude IP Range (uncheck to Include IP Range)

Start with this IP address: End with this IP address:

Save New **Revise Existing**

Email Alert for each successful logon event (not logoffs) to the following accounts:

Define Email Alert

Enter / Revise Email Address:

Add Email Address **Revise Email Address**

☐ Send Email Alerts to Accounts defined in the server settings

☐ Allow Alert Console (cptalert.exe) Users to receive Alerts from this Profile

Remove selected IP Range(s)

Remove selected Email Addresses

Figure 2-22

All profile editing is per server, there is no option to edit a Profile across multiple servers. You can however, use drag-and-drop to copy Profile(s) to a different server, more on this later in this section.

Logon / Logoff Activity Profile: Add IP Range

When you first create a Logon / Logoff Activity Profile there is no IP Range defined. You could stop here and all Logon / Logoff activity will be tracked on the selected server. However, if you want the profile to capture only logons from selected IP addresses / range, enter the range and click “Save New”:

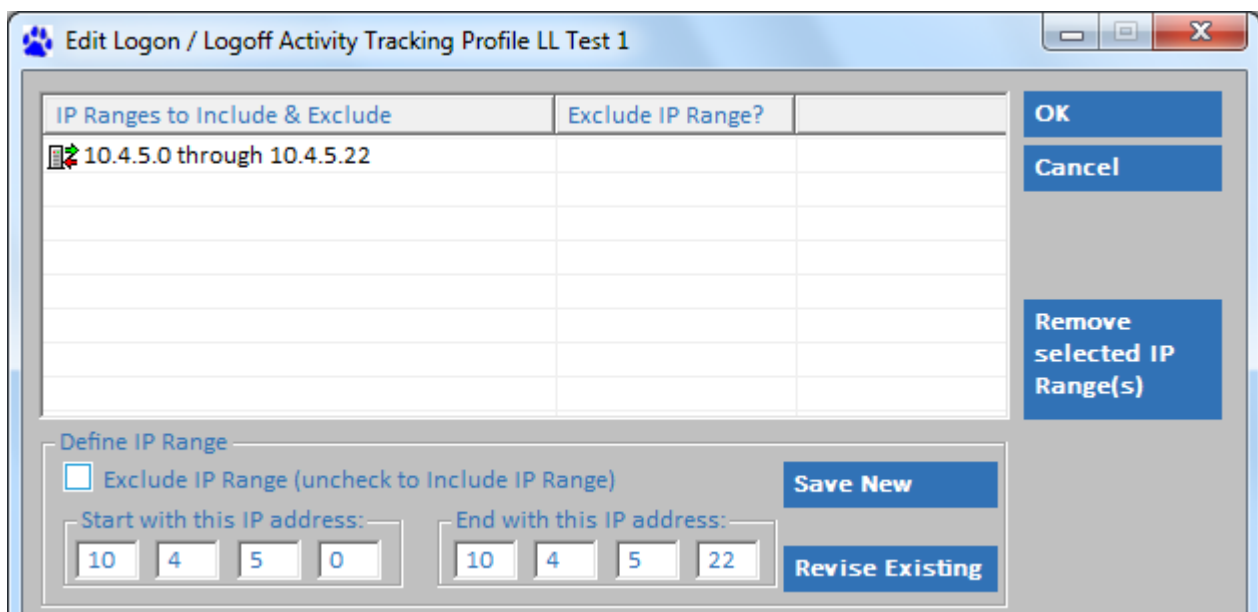


Figure 2-23

Note: Local and Terminal Server logons are only filtered if the IP Address(es) of the server running the CPTRAX Server Agent is defined by the IP Address Range. This includes terminal service sessions that originate at a separate IP Address than the server.

If you want to exclude an IP Range, check the “Exclude IP Range” option:

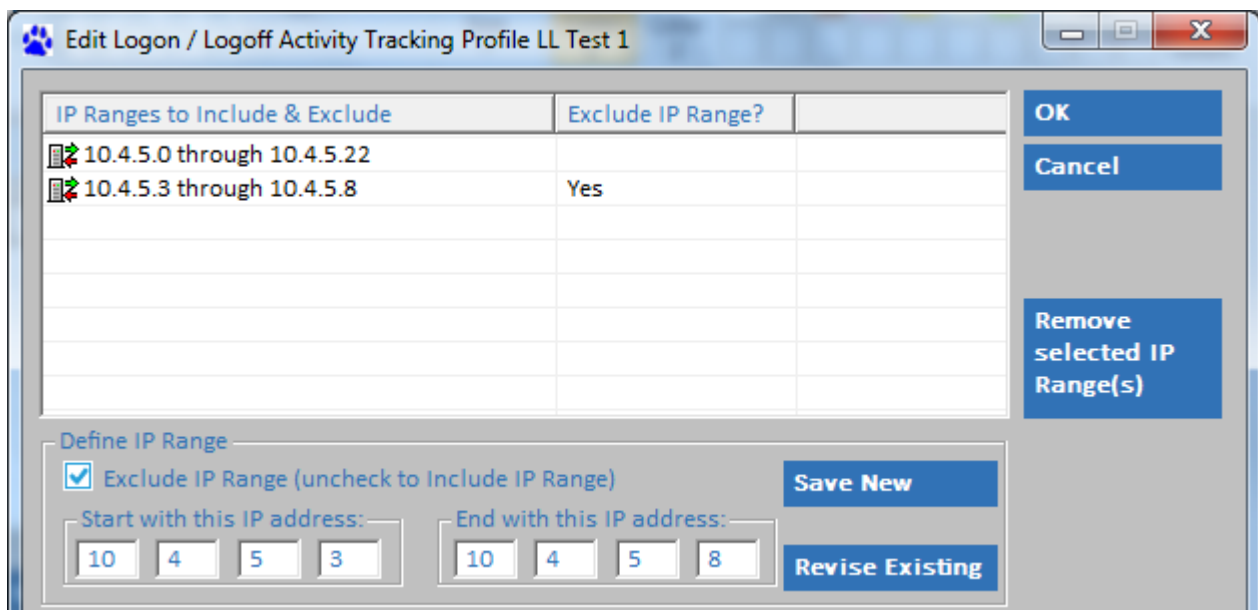


Figure 2-24

Logon / Logoff Activity Profile: Alerts

There are two methods to receive alerts from the CPTRAX Server Agent. The first is via email. The second is the [Alert Console](#). To define email alerts, enter the destination email address in the “Enter / Revise Email Address” field and click on the “Add Email Address” button. You

may also check the “Send Email Alerts to Accounts defined on the server configuration screen” and “Allow Alert Console Users to receive Alerts from this Profile”.

Note: For email alerts to be sent, the server configuration screen must define the “sending” email account. This is discussed in [Chapter 4, Settings](#).

The Alert Console is further discussed at the [end of this chapter](#).

An alert is generated for each captured event. Alerts are sent in real-time.

Logon / Logoff Activity Profile: Done

When finished editing the Logon / Logoff Activity Profile, click on the “OK” button (clicking “Cancel” will abort all changes). If the CPTRAX Server Agent is active it will realize the change has occurred and will wait 2 minutes for all changes to be processed and then it will re-read all Profiles and begin acting on them as defined.

Important Note about Server Agent Startup:

When the CPTRAX Server Agent is started it can take up to 10 minutes before initializations are complete and it is ready to act on Profiles.

Any users currently logged on locally or via terminal services, and where there is a matching Logon / Logoff Activity Profile, will have their logon recorded immediately (even if they logged on prior to starting the CPTRAX Server Agent).

Failed Logon Activity Profile: Add New

CPTRAX for Windows provides Failed Logon tracking for remote connections using NTLM, NTLMSSP, Kerberos and FTP only and **not** for local and terminal services.

In this third example, from the ‘Profiles’ tab located at the center-top in the CPTRAX Administration Console (Figure 2-14), click the + sign at the top right of the “Profiles” list and then select ‘Failed Logon Activity’ and enter the name “FL Test 1”:

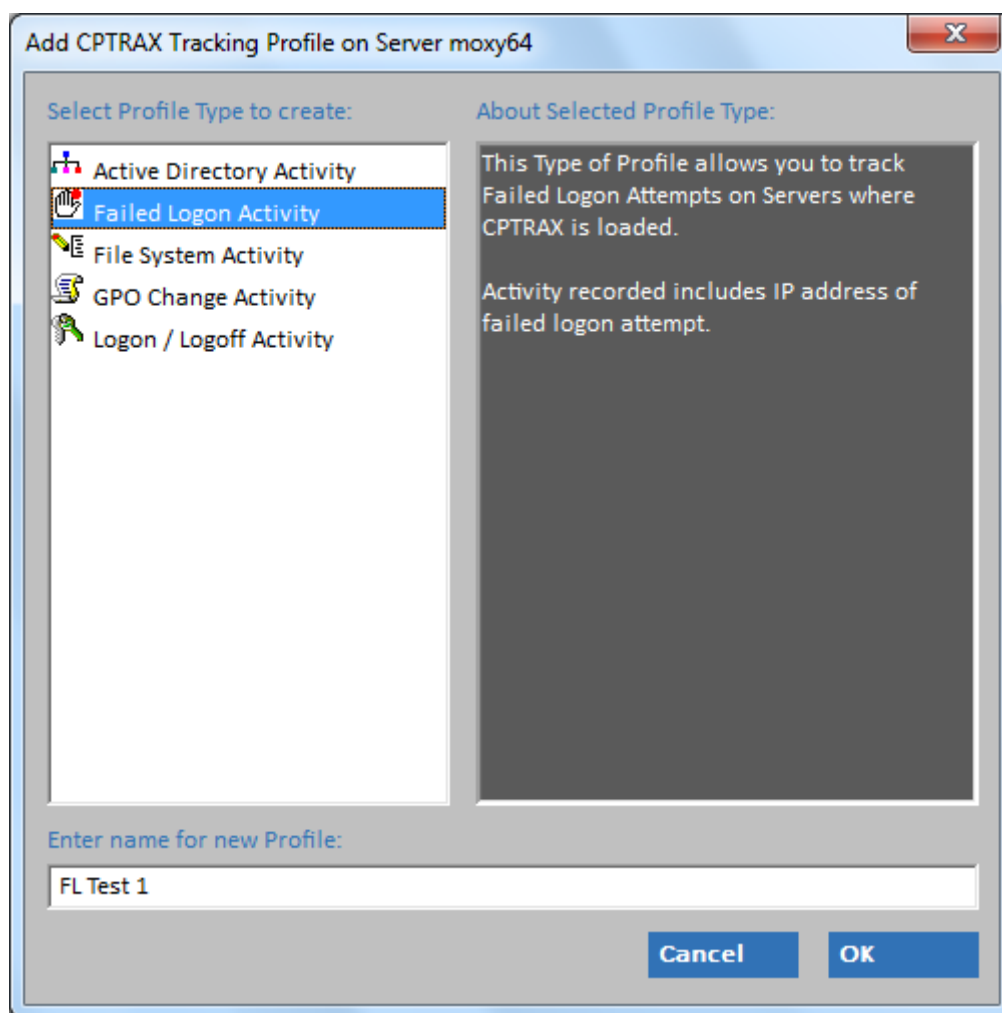
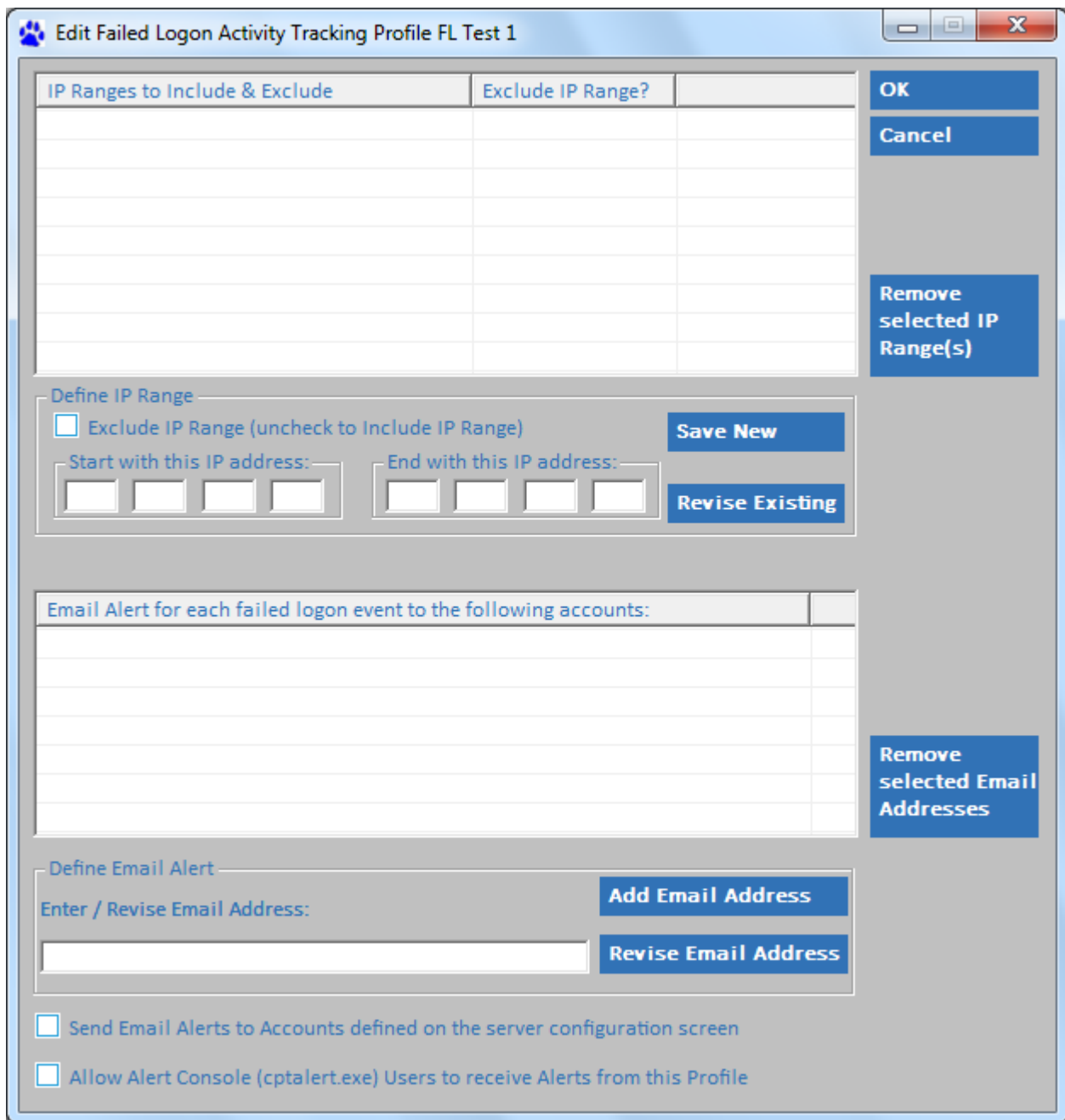


Figure 2-25

Click OK, and you will be immediately presented with the following screen:



Edit Failed Logon Activity Tracking Profile FL Test 1

IP Ranges to Include & Exclude	Exclude IP Range?

Define IP Range

☐ Exclude IP Range (uncheck to Include IP Range)

Start with this IP address:

End with this IP address:

Save New **Revise Existing**

Email Alert for each failed logon event to the following accounts:

Define Email Alert

Enter / Revise Email Address:

Add Email Address **Revise Email Address**

☐ Send Email Alerts to Accounts defined on the server configuration screen

☐ Allow Alert Console (cptalert.exe) Users to receive Alerts from this Profile

Figure 2-26

All profile editing is per server, there is no option to edit a Profile across multiple servers. You can however, use drag-and-drop to copy Profile(s) a different server, more on this later in this section.

Failed Logon Activity Profile: Add IP Range

When you first create a Failed Logon Activity Profile there is no IP Range defined. You could stop here and all remote Failed Logon activity will be tracked on the selected server. However, if you want the profile to capture only logons from selected IP addresses / range, enter the range and click “Save New”:

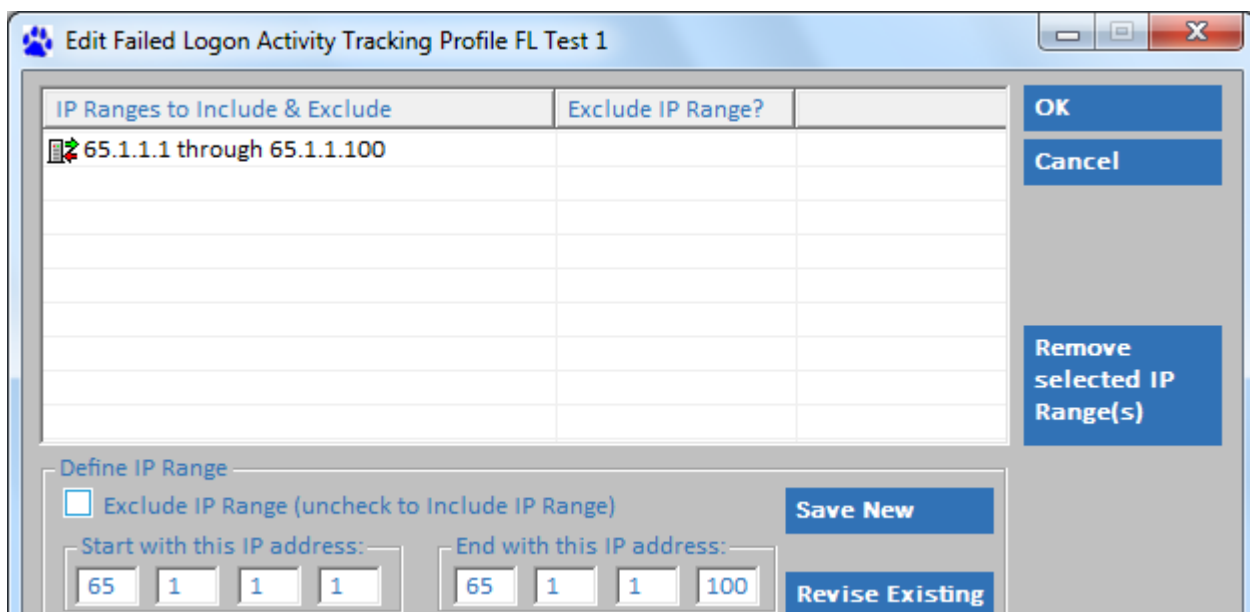


Figure 2-27

If you want to exclude an IP Range, check the “Exclude IP Range” option:

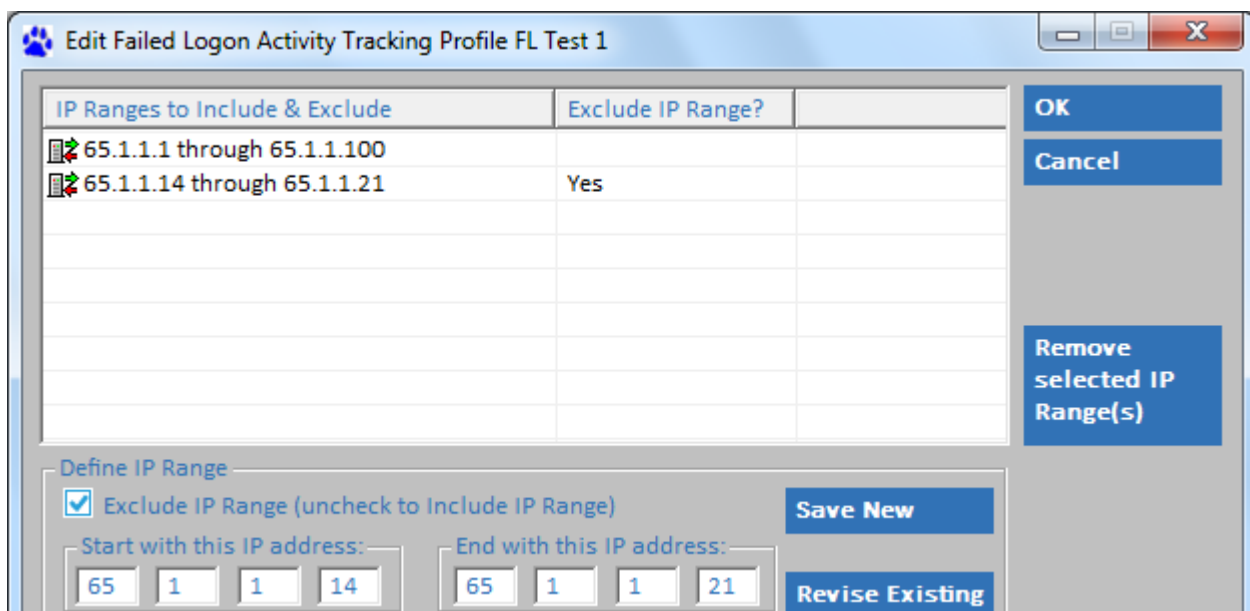


Figure 2-28

Failed Logon Activity Profile: Alerts

There are two methods to receive alerts from the CPTRAX Server Agent. The first is via email. The second is the [Alert Console](#). To define email alerts, enter the destination email address in the “Enter / Revise Email Address” field and click on the “Add Email Address” button. You may also check the “Send Email Alerts to Accounts defined on the server configuration screen” and “Allow Alert Console Users to receive Alerts from this Profile”.

Note: For email alerts to be sent, the server configuration screen must define the “sending” email account. This is discussed in [Chapter 4, Settings](#).

The Alert Console is further discussed at the [end of this chapter](#).

An alert is generated for each captured event. Alerts are sent in real-time.

Failed Logon Activity Profile: Done

When finished editing the Failed Logon Activity Profile, click on the “OK” button (clicking “Cancel” will abort all changes). If the CPTRAX Server Agent is active it will realize the change has occurred and will wait 2 minutes for all changes to be processed and then it will re-read all Profiles and begin acting on them as defined.

Important Note about Server Agent Startup:

When the CPTRAX Server Agent is started it can take up to 10 minutes before initializations are complete and it is ready to act on Profiles.

Once this initialization has completed, the CPTRAX Server Agent will immediately track Failed Logon Activity made via NTLM, NTLMSSP, Kerberos and FTP authentication methods.

Active Directory Activity Profile: Add New

CPTRAX for Windows provides full auditing of Active Directory activity.

To begin, select ‘Active Directory Activity’ and enter the name “AD Test 1”:

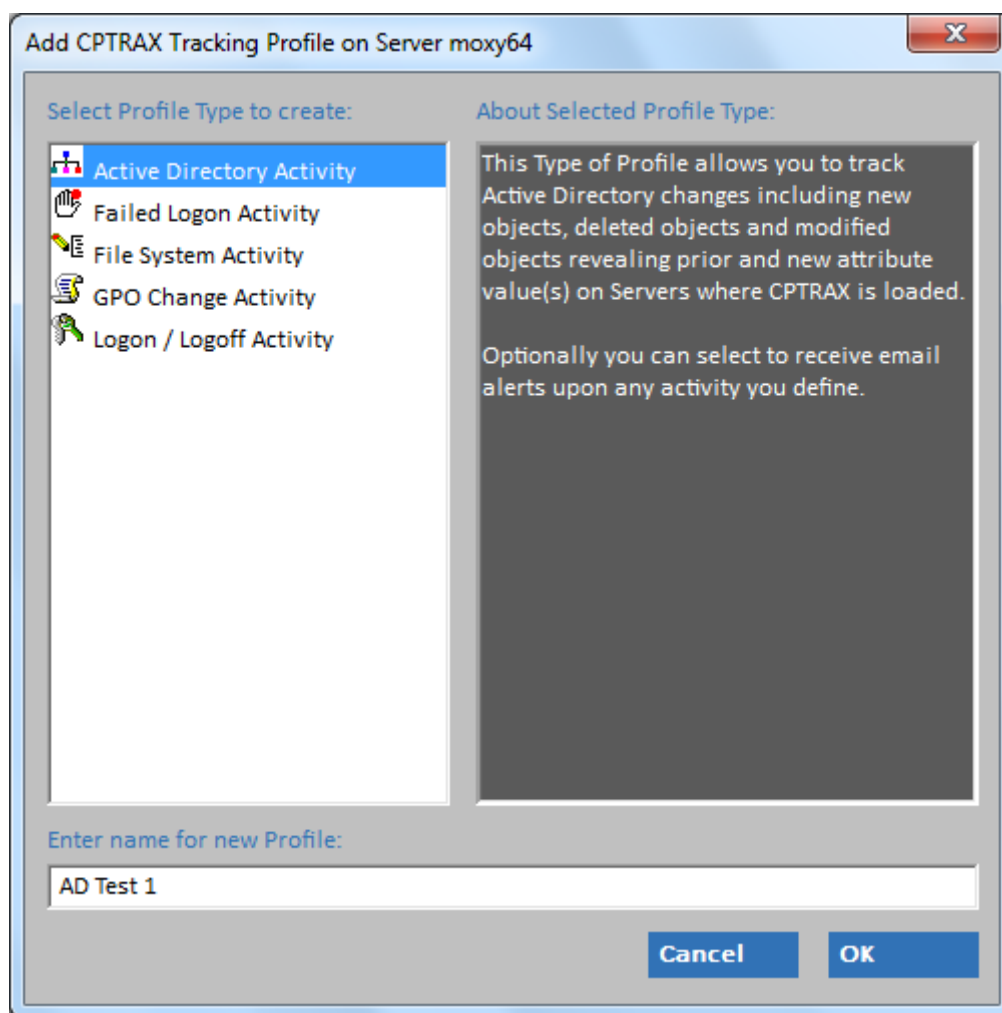


Figure 2-29

Click OK, and you will be immediately presented with the following screen:

The screenshot shows the 'Edit Active Directory Tracking Profile AD Test 1' window. It features two main tables for configuration:

Object Classes to be tracked	Creations?	Deletions?	Modifications?

Attributes to be tracked	Additions?	Deletions?	Do not track?

Active Directory Objects to be tracked	Object Only? (only if wildcards not used)

Email Alert for each tracked event to the following accounts:

Buttons: Add, Remove, Add, Remove, Add, Remove, Remove selected Email Addresses.

Define Email Alert

Enter / Revise Email Address: Add Email Address Revise Email Address

☐ Send Email Alerts to Accounts defined on the server configuration screen

☐ Allow Alert Console (cptalert.exe) Users to receive Alerts from this Profile

Figure 2-30

All profile editing is per server, there is no option to edit a Profile across multiple servers. You can however, use drag-and-drop to copy Profile(s) to a different server, more on this later in this section.

Active Directory Activity Profile: Add Object Class to Track

CPTRAX for Windows can be configured to track selected or all Object Classes. Further refinements include tracking of Creations, Deletions and Modifications of selected object classes.

To begin, click the 'Add' button near the center top of the screen shown in Figure 2-30 and the following screen will appear:

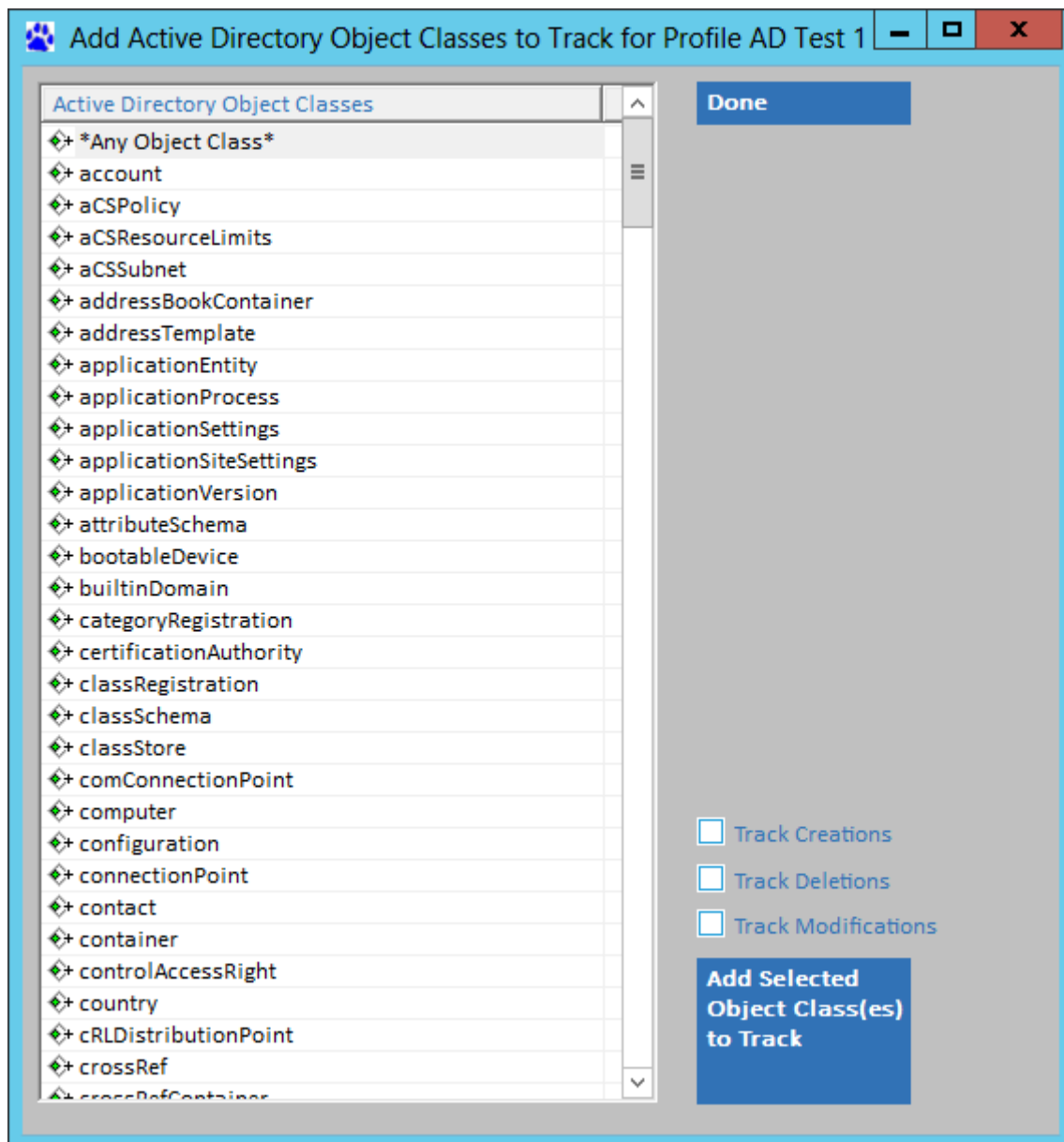


Figure 2-31

On this screen you select the desired Object Classes to track regardless of location. To continue, click the checkbox for each desired tracking action. Finally click the 'Add' button to place your selection(s) in the profile. Notice that each selected Object Class will be removed from the available list and placed into the profile's list.

When finished, click the 'Done' button and you will be returned to the main screen for the Profile.

Note: Selection of Object Classes to track is not required. You can instead select only Attributes to track. When no Object Classes are selected, any Attributes chosen will be tracked regardless of the Object Class.

Active Directory Activity Profile: Add Attribute to Track

CPTRAX for Windows can be configured to track selected or all Attributes regardless of the Directory Object. Further refinements include tracking of Additions, Deletions and ‘do not track’ selected Attributes. Most Attribute value changes include reporting of the value being added or deleted.

To begin, click the ‘Add’ button near the left top of the screen shown in Figure 2-22 and the following screen will appear:

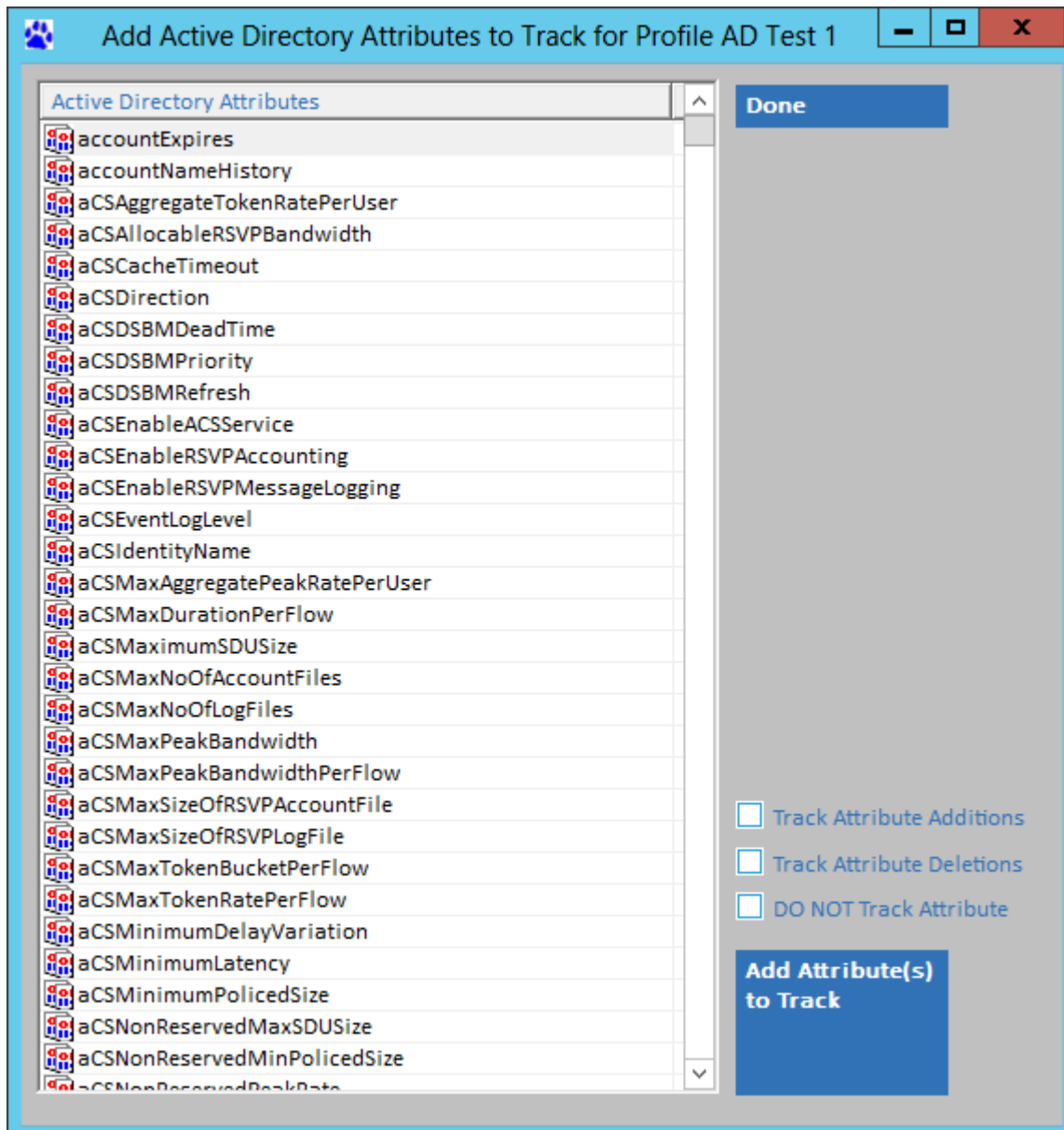


Figure 2-32

The list of Attributes includes all in the Schema of the currently selected server – including any custom attributes may have defined such as those created by Microsoft Exchange.

If you have selected an Object Class(es) to track Modification thereof, by default, all Attribute changes will be tracked. You can eliminate unwanted ‘noise’ attributes such as whenChanged, uSNChanged, dnsRecord, dsCorePropogation and so on from being included by merely selecting those attributes and checking the “DO NOT Track Attribute” checkbox and then clicking the ‘Add Attribute’ button. If you click OK to save the Profile and no attributes are selected you will be presented with a prompt to automatically include attributes to “not track”:

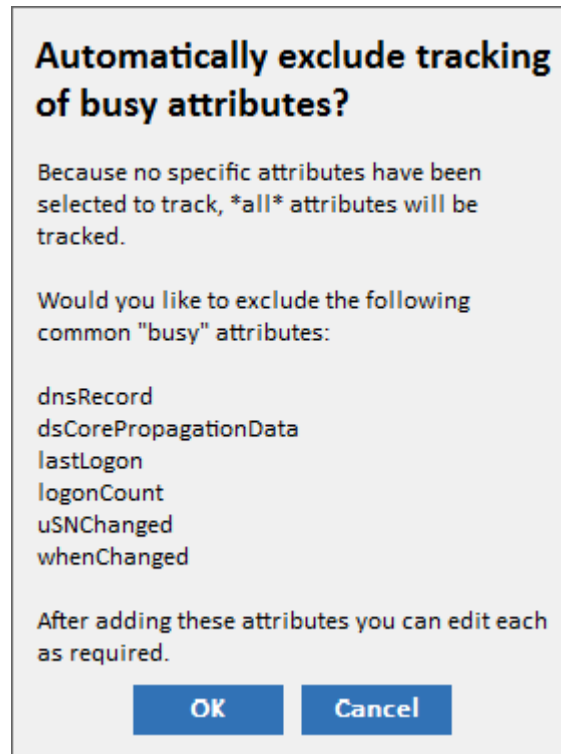


Figure 2-33

Alternatively you can define only Attributes to Track without selecting any Object Classes to track.

Active Directory Activity Profile: Add Directory Objects to Track

In addition to selecting Object Classes and Attributes to track CPTRAX for Windows gives you the ability to select Directory Objects by name. Both fully formed names and partial names can be defined.

To begin, click the ‘Add’ button near the center-right of the screen shown in Figure 2-30 and the following screen will appear:

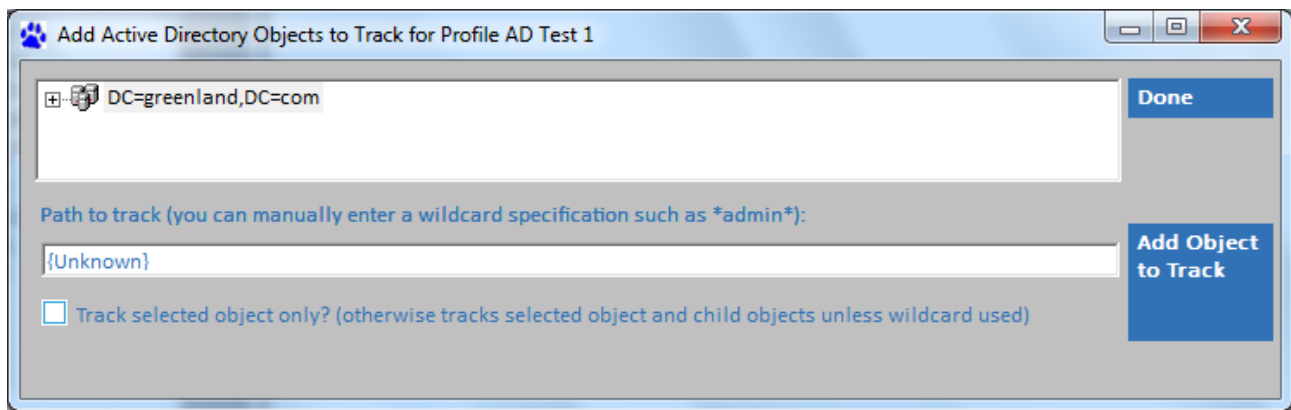


Figure 2-34

On this screen you can directly select any single Directory Object to track. You can also modify the name with wildcards * and ?. As you click the ‘Add Object to Track’ button the entry will be immediately placed into the profile and you can select additional objects.

Active Directory Activity Profile: Alerts

There are two methods to receive alerts from the CPTRAX Server Agent. The first is via email. The second is the [Alert Console](#). To define email alerts, enter the destination email address in the “Enter / Revise Email Address” field and click on the “Add Email Address” button.

You may also check the “Send Email Alerts to Accounts defined on the server configuration screen” and “Allow Alert Console Users to receive Alerts from this Profile”.

Note: For email alerts to be sent, the server configuration screen must define the “sending” email account. This is discussed later in this [Chapter 4, Settings](#).

The Alert Console is further discussed at the [end of this chapter](#).

An alert is generated for each capture event. Alerts are sent in real-time.

Active Directory Activity Profile: Done

When finished editing the Active Directory Activity Profile, click on the “OK” button (clicking “Cancel” will abort all changes). If the CPTRAX Server Agent is active it will realize the change has occurred and will wait 2 minutes for all changes to be processed and then it will re-read all Profiles and begin acting on them as defined.

GPO Change Activity Profile: Add New

CPTRAX for Windows provides auditing of Group Policy Object (GPO) change activity.

To begin, select ‘GPO Change Activity’ and enter the name “GP Test 1”:

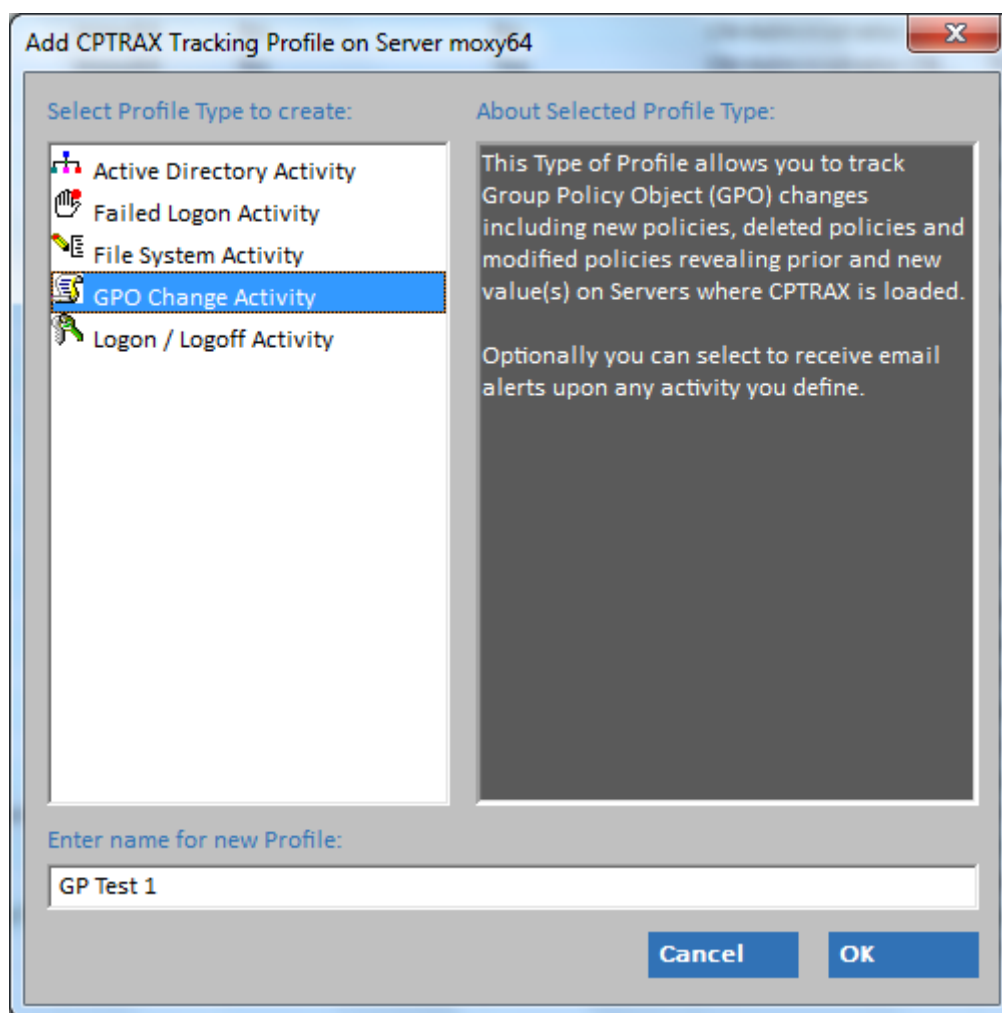


Figure 2-35

Click OK, and you will be immediately presented with the following screen:

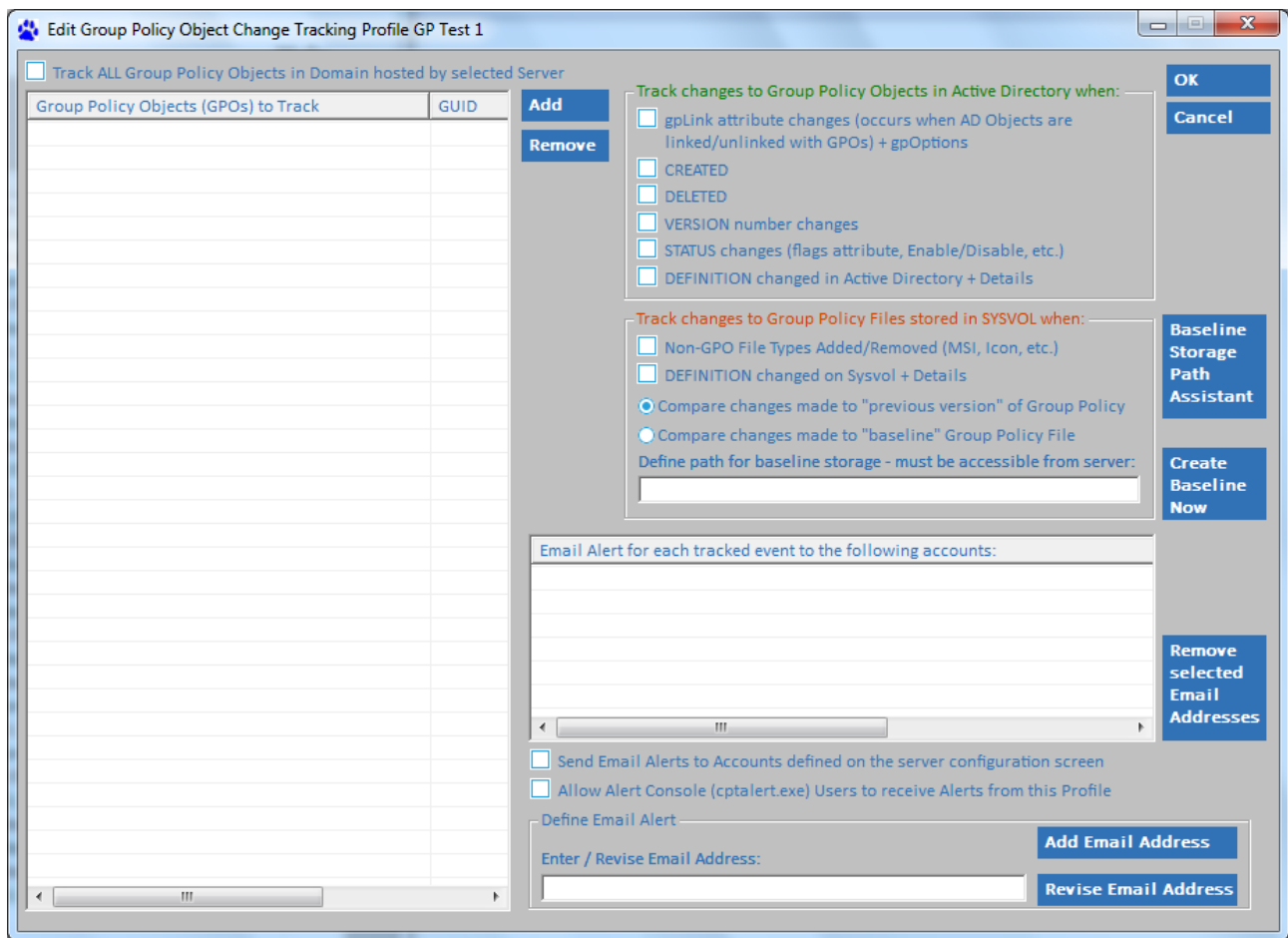


Figure 2-36

All profile editing is per server, there is no option to edit a Profile across multiple servers. You can however, use drag-and-drop to copy Profile(s) to a different server, more on this later in this section.

GPO Change Activity Profile: Add GPO to Track

CPTRAX for Windows can be configured to track selected or all Group Policy Objects (GPOs). Further refinements include tracking of Creations, Deletions and Modification details.

You can either Track All GPOs or selected GPOs. To Track All, simply click the checkbox at the top left.

To track selected GPOs, click the 'Add' button near the center top of the screen shown in Figure 2-36 and the following screen will appear:

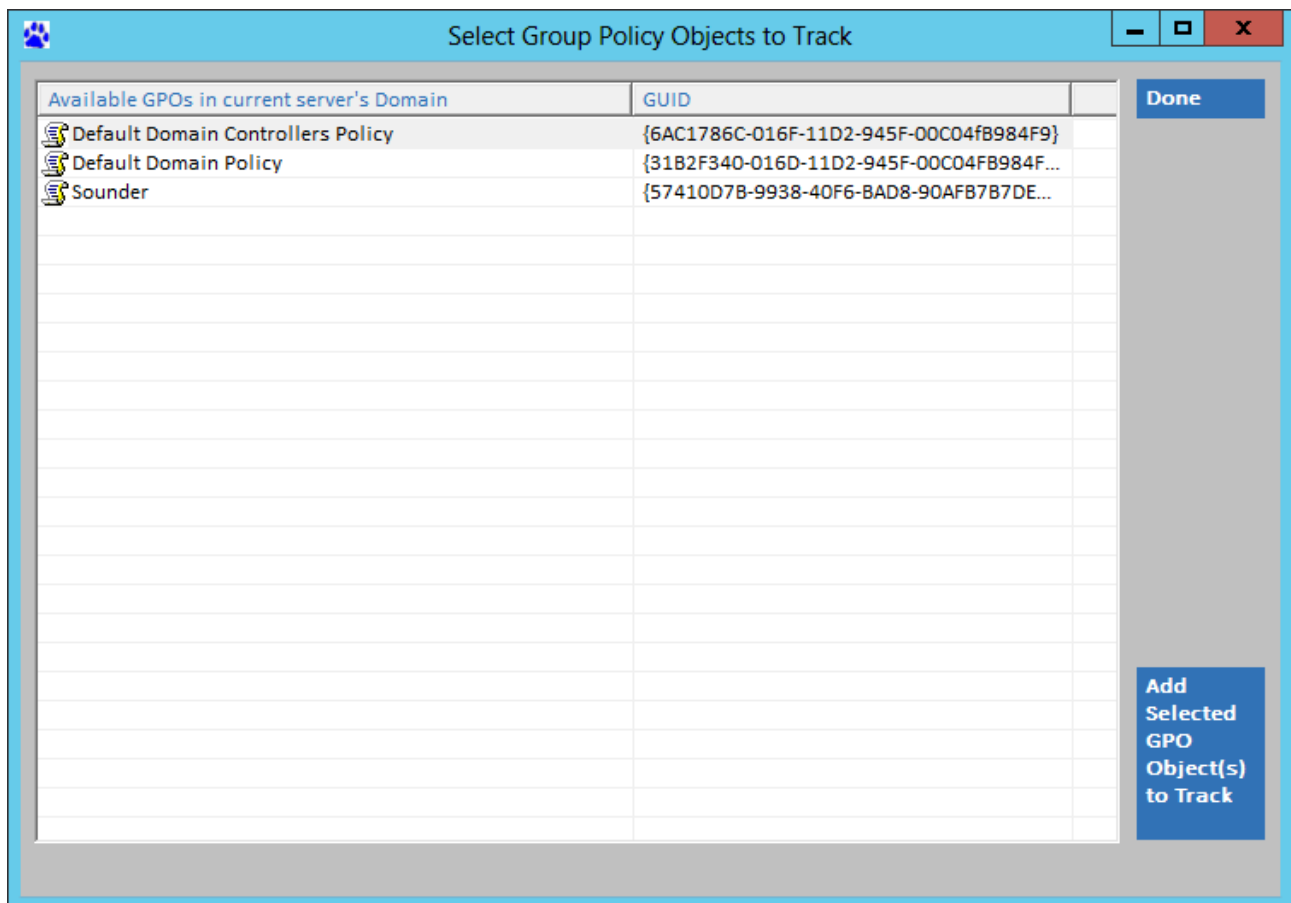


Figure 2-37

On this screen you select the desired GPOs to track. Once selected click the ‘Add Selected GPO Object(s) to Track’ button to place your selection(s) in the profile. Notice that each selected GPOs will be removed from the available list and placed into the profile’s list.

When finished, click the ‘Done’ button and you will be returned to the main screen for the Profile.

GPO Change Activity Profile: Active Directory Tracking Options

As you may know, Group Policy Objects definitions are stored in both Active Directory and in the Sysvol file system location at each Domain Controller. The CPTRAX GPO Change Activity Tracking Profile provides you tracking granularity that differentiates between each.

When a GPO is created, it is created in Active Directory first and Sysvol Policy file structure merely accompanies that primary Active Directory object and serves to store most but not all Policy definitions.

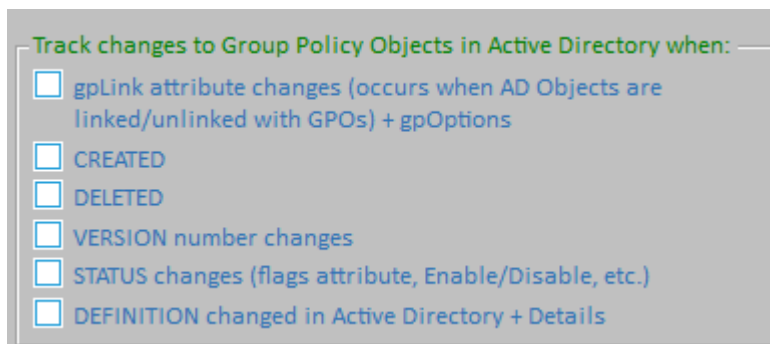


Figure 2-38

GPO Change Tracking Options shown in Figure 2-38 include:

- (a) gpLink and gpOptions change tracking : These are the names of Active Directory attributes. The gpLink attribute is attached to each container object where GPOs are linked. Change details recorded include whenever a change in links occur. The gpOptions attribute is attached to each container and indicates if inheritance of GPOs will be allowed or not.
- (b) Creation of GPOs : please note, for this option to function the Profile must define to “Track ALL Group Policy Objects in Domain...”
- (c) Deletion of GPOs
- (d) version change tracking : The “version” Active Directory attribute stores a revision sequence number for the GPO object. Whenever the GPO Active Directory object is modified the version attribute is incremented
- (e) Status changes to the GPO include whenever the Computer Configuration or User Configuration options are enabled or disabled
- (f) Because portions of GPOs are stored in Active Directory the Definition changed option will decipher what exactly changed. Some GPO policies such as the Wireless policy are stored in Active Directory as XML strings and this option will reveal what actually changed

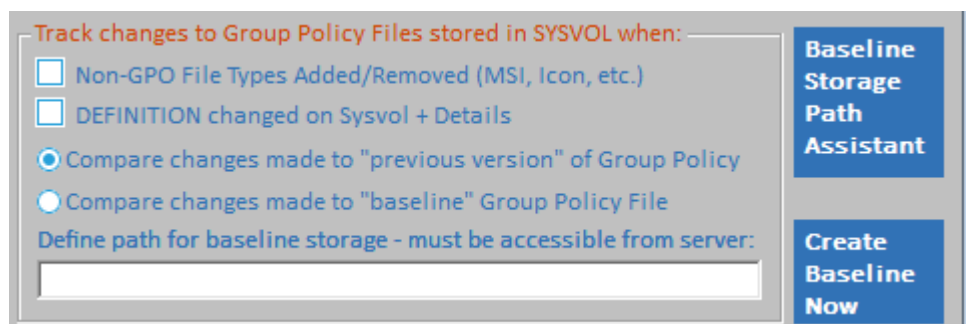


Figure 2-39

GPO Change Tracking Options shown in Figure 2-39 include:

- (a) Non-GPO File Types : What is indicated by non-GPO file types are those files that are stored in the Sysvol GPO location but are not directly “GPO Policy Files”. For instance, icon or MSI files. These sorts of non-GPO file types are used in the application of GPO policies but do not actually define the policy, hence, non-GPO

file types. For such files, simple file tracking is performed, such as file created, deleted, renamed.

- (b) For GPO Policy files stored in Sysvol, the Definition changed option will decipher what exactly changed. The policy file path is included for each change recorded. This path serves as a reference for where in the Group Policy the change was made.
- (i) If Definition changes are desired you can use either the previous version of the file that changed or a baseline file. The default option is to compare against the previous version of the file. Please see Chapter 4, GPO Change Tracking Temp Path for important information on where the previous version of each GPO file will be stored for comparison.
 - (ii) You can also choose to compare the GPO Sysvol-located changes to a baseline of GPO files. When you select this option you will need to select(create) a Baseline path . Click the “Baseline Storage Path Assistant” button to select. Once the path is selected, click the “Create Baseline Now” button and a “progress window” will appear to reveal the copy progress:

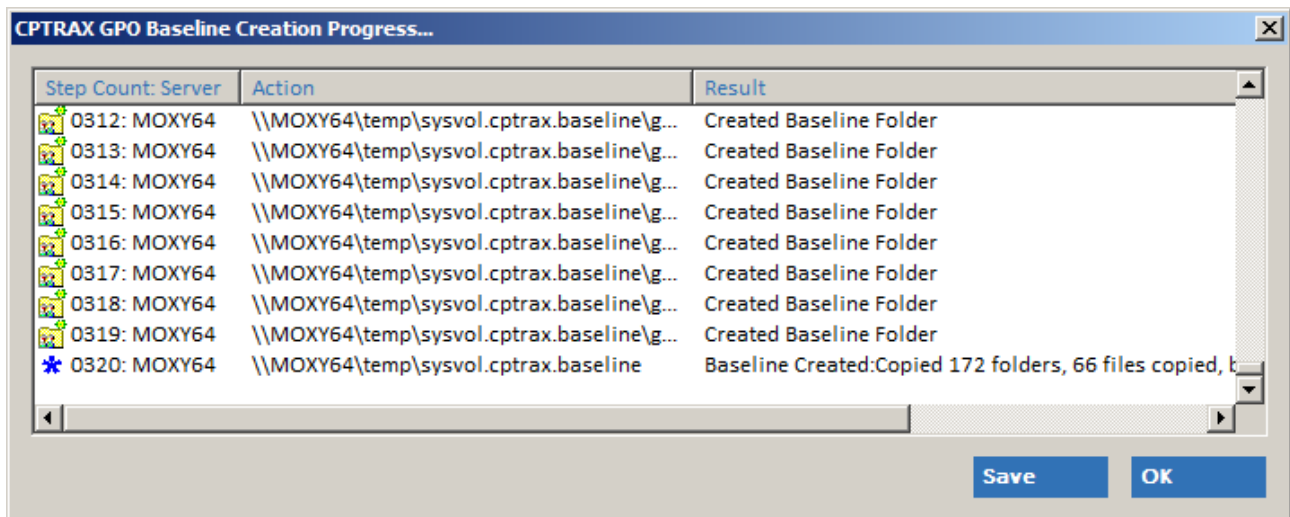


Figure 2-40

When copy is complete you can sort on the “Step Count: Server” column. Note that all current GPOs are copied, there is no exception. Because only actual GPO Policy files are being copied the actual file size copied will be small, generally between 10KB and 50KB per GPO.

If you receive an error message as the baseline copy process initiates:

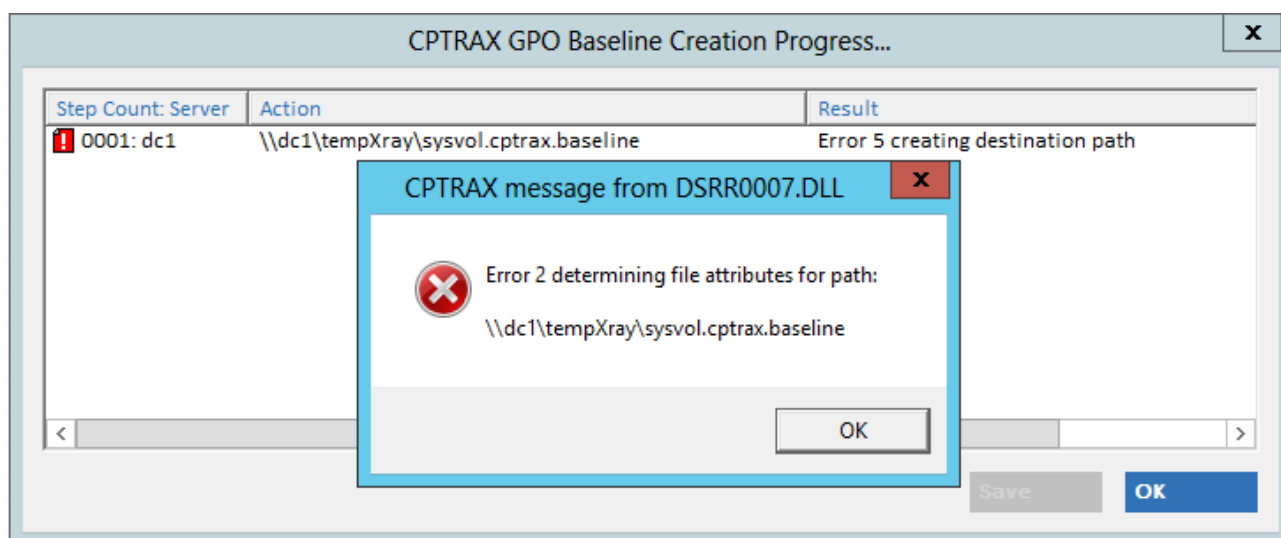


Figure 2-41

It likely indicates your current logon account is sufficiently credentialed to perform the indicated actions. Note “Error 5 creating destination path” in the “Result” column, this indicates access was denied. And then “Error 2” indicates the path was not found (because it could not be created).

Group Policy Activity Profile: Alerts

There are two methods to receive alerts from the CPTRAX Server Agent. The first is via email. The second is the [Alert Console](#). To define email alerts, enter the destination email address in the “Enter / Revise Email Address” field and click on the “Add Email Address” button.

You may also check the “Send Email Alerts to Accounts defined on the server configuration screen” and “Allow Alert Console Users to receive Alerts from this Profile”.

Note: For email alerts to be sent, the server configuration screen must define the “sending” email account. This is discussed later in this [Chapter 4, Settings](#).

The Alert Console is further discussed at the [end of this chapter](#).

An alert is generated for each capture event. Alerts are sent in real-time.

Group Policy Activity Profile: Done

When finished editing the Active Directory Activity Profile, click on the “OK” button (clicking “Cancel” will abort all changes). If the CPTRAX Server Agent is active it will realize the change has occurred and will wait 2 minutes for all changes to be processed and then it will re-read all Profiles and begin acting on them as defined.

CPTRAX Additional Installation Options

Configuring Email Addresses for Alerting

If you have defined email addresses for alerting in any Profile, you will need to also configure the CPTRAX Server Agent to send the alerts. From the ‘Settings’ tab in the Administration Console select the server and click the “Email Server Configuration” button:

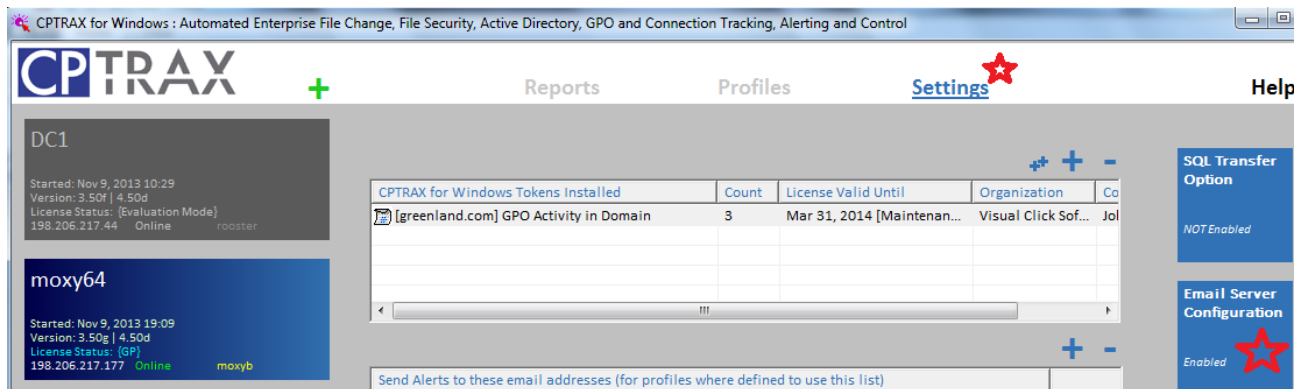


Figure 2-42

And the following window will be presented:

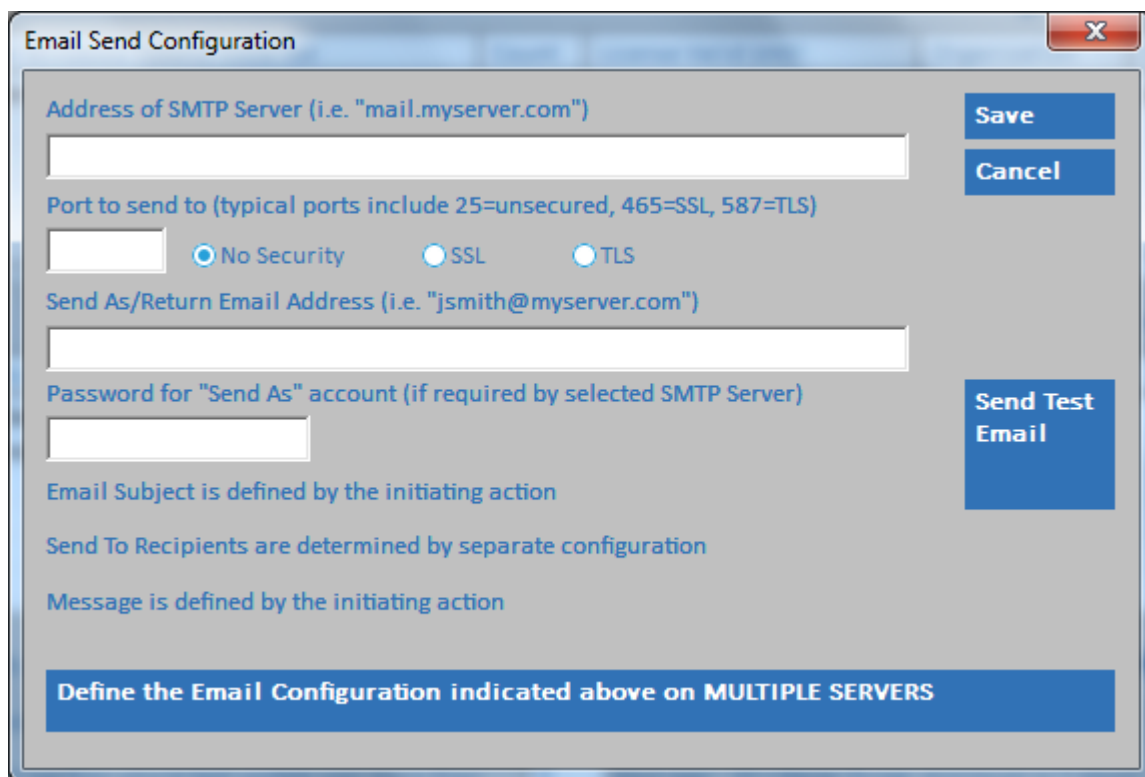


Figure 2-43

Fill in the fields as labeled. Click the “Send Test Email” button to confirm operation. Click “Save” to ensure the values entered are retained. Please note, a ***Password is required***, the CPTRAX Server Agent will not send emails where the “Send Configuration” defines a blank password.

After you click “Save” and return to the prior screen, use the “Send Alerts to these email addresses...” section to add specific email addresses of those to receive email alerts from the CPTRAX Server Agent on the selected server.

This email address list provides a centralized list of email addresses that can be quickly included in any CPTRAX Activity Tracking Profile.

Using the Alert Console – Configuring the CPTRAX Server Agent

If you would like to use the Alert Console you must configure the CPTRAX Server Agent to enable Alert Agents to connect to it and receive alerts.

From the ‘Settings’ tab in the Administration Console select the server and click the “Allow Alert Consoles to attach to this server?” checkbox.

Using the Alert Console – Configuring the workstation Alert Agent

In the product installation directory you will find a file `CPTALERT.EXE`, this is the CPTRAX Alert Agent. It is comprised of a single file (`CPTALERT.EXE`) and when loaded minimizes itself to the system tray.

When first run, the alert console will put its icon in the system tray, no screen will appear.

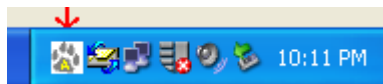


Figure 2-44

To activate, right click on the icon:

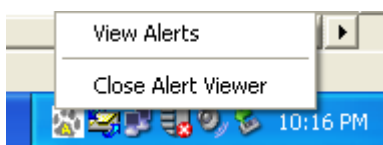


Figure 2-45

and select “View Alerts” and the following screen appears:

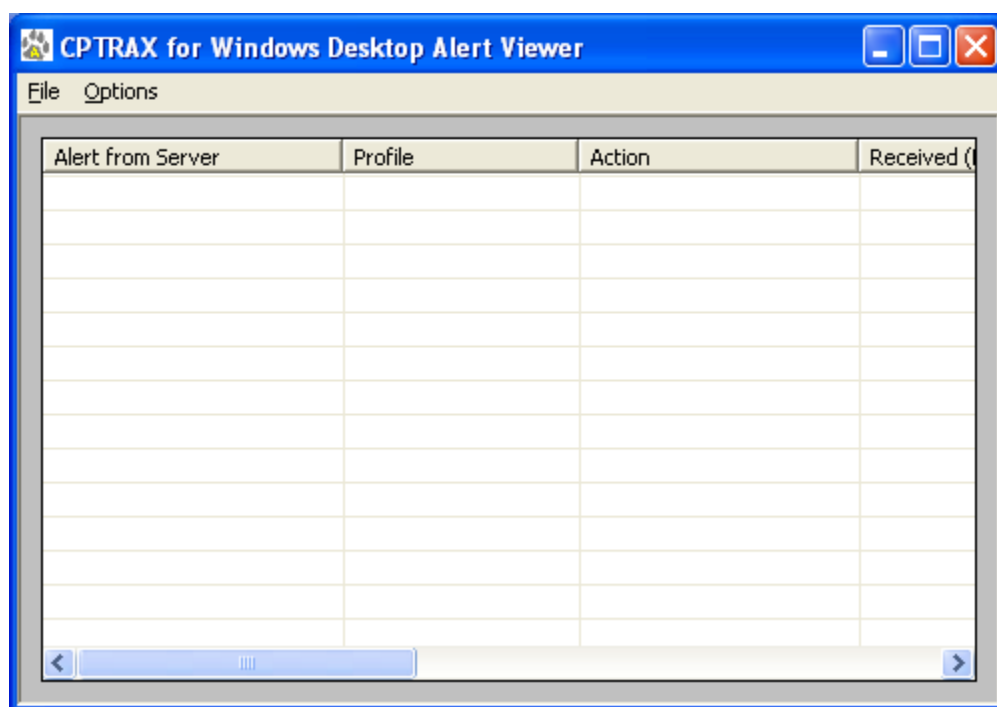


Figure 2-46

To connect to a server hosting the CPTRAX Server Agent, click on “File” and select “Connect to Windows Server”. At the prompt that follows, enter the NetBIOS name or IP Address of the server to connect. Repeat for each server where alerts may be generated.

Various options can be found under the “Options” menu selection.

In addition to alerts you define, the Alert Console will also receive an alert when the CPTRAX Server Agent is being unloaded.

Note: If the CPTRAX Server Agent is restarted you will need to instruct the Alert Console to re-connect. The re-connect option is under the “Options” menu item.

You can re-size the Alert Console by dragging from any side. To remove the Alert Console from view, click the red X at the top right corner. It will remain active in the system tray. To stop the Alert Console, <right click> its icon in the system tray and select “Close Alert Viewer”. The Alert Console communicates with the CPTRAX Server Agent via TCP/IP.

The Alert Console configuration settings are stored in the local machine’s Registry under the key:

```
HKEY_CURRENT_USER\Software\Visual Click Software, Inc.\CPTRAX\AlertConsole
```

In the CPTRAX Administration Console you can view current Alert Console (Alert Agent) users in the server configuration screen (only available when selecting one server) under the “Alert Consoles” tab

The following screenshot shows captured alerts in the Alert Console (zoom in to see detail):

Alert ...	Pro...	Action	Received (Local Time)	User	W...	Share Folder Object	File Object Cla...	New Name Rename Object on ACL Attribute Value
DC1	gs01	Local File Copy for GPO:Sounder	Sat Nov 09 10:29:49 2013	Administrator	DC1	\\testdomain.local\SysVo...	GptTmplInf	\\testdomain.local\SysVol\testdomain.local\Policies\{57...
DC1	gs01	Local File Copy for GPO:Sounder	Sat Nov 09 10:30:04 2013	Administrator	DC1	C:\Users\ADMINI~1\AppData...	sce64224.tmp	\\testdomain.local\SysVol\testdomain.local\Policies\{57...
DC1	gs01	Delete File for GPO:Sounder	Sat Nov 09 10:30:04 2013	Administrator	DC1	\\testdomain.local\SysVo...	GptTmpl.tmp	\\testdomain.local\SysVol\testdomain.local\Policies\{57...
DC1	gs01	Local File Copy for GPO:Sounder	Sat Nov 09 10:30:04 2013	Administrator	DC1	\\testdomain.local\SysVo...	GptTmplInf	\\testdomain.local\SysVol\testdomain.local\Policies\{57...
DC1	gs01	Local File Copy for GPO:Sounder	Sat Nov 09 10:30:04 2013	Administrator	DC1	C:\Users\ADMINI~1\AppData...	sce50091.tmp	\\testdomain.local\SysVol\testdomain.local\Policies\{57...
DC1	gs01	Delete File for GPO:Sounder	Sat Nov 09 10:30:04 2013	Administrator	DC1	\\testdomain.local\SysVo...	GptTmpl.tmp	
DC1	gs01	Group Policy Remove Item for GPO:Sounder	Sat Nov 09 10:30:04 2013	Administrator	DC1	C:\Windows\SYSVOL\sys...	GptTmplInf	Event Audit Section: REMOVE ITEM AuditObjectAccess =
DC1	gs01	Group Policy Add Item for GPO:Sounder	Sat Nov 09 10:30:04 2013	Administrator	DC1	C:\Windows\SYSVOL\sys...	GptTmplInf	Event Audit Section: ADD ITEM AuditObjectAccess = 1
DC1	gs01	GPO AD Other Add Attribute Value for GPO:Sounder	Sat Nov 09 10:30:04 2013	CN=Administ...	DC1	cn={57410D7B-9938-40F6...	versionNumber	524361
DC1	gs01	GPO AD Other Delete Attribute Value for GPO:Sounder	Sat Nov 09 10:30:04 2013	CN=Administ...	DC1	cn={57410D7B-9938-40F6...	versionNumber	524359

Figure 2-47

To save Alert Console results, <right click> over the list of alerts and from the resulting popup menu select “Save Alerts to File”. With this same popup menu you can erase all alerts currently shown.

Using SQL Transfer – Configuring the CPTRAX Server Agent for SQL Server

Use the SQL Transfer option to enable the CPTRAX Server Agent to send all activity records it captures to an *existing* Microsoft SQL Server of your selection. This option is used to identify the SQL Server instance to use and will create the CPTRAX_for_Windows database as well as tables. This option does not install SQL Server, it is presumed the SQL Server has already been installed and is functional.

Important: Before you continue, please ensure your current login credentials have sufficient permissions on the SQL Server to Create a Database and Add Tables to the new database.

To begin, from the ‘Settings’ tab, select the desired server and click the “SQL Transfer Option” button.

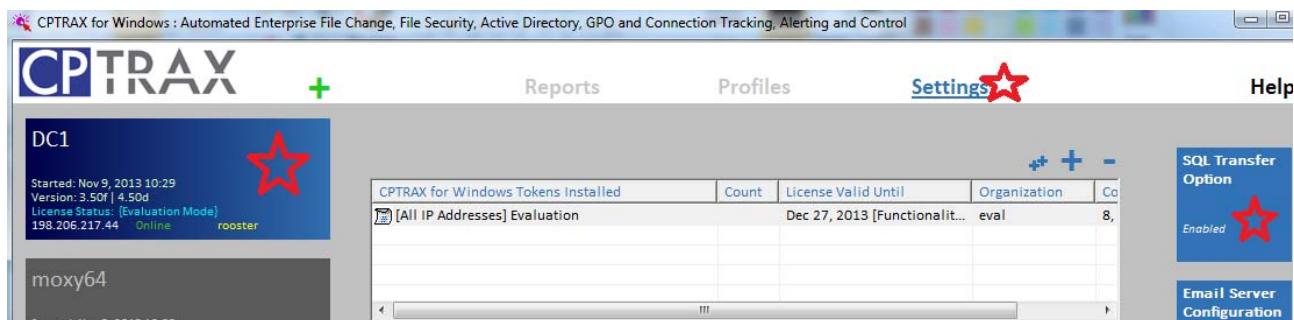
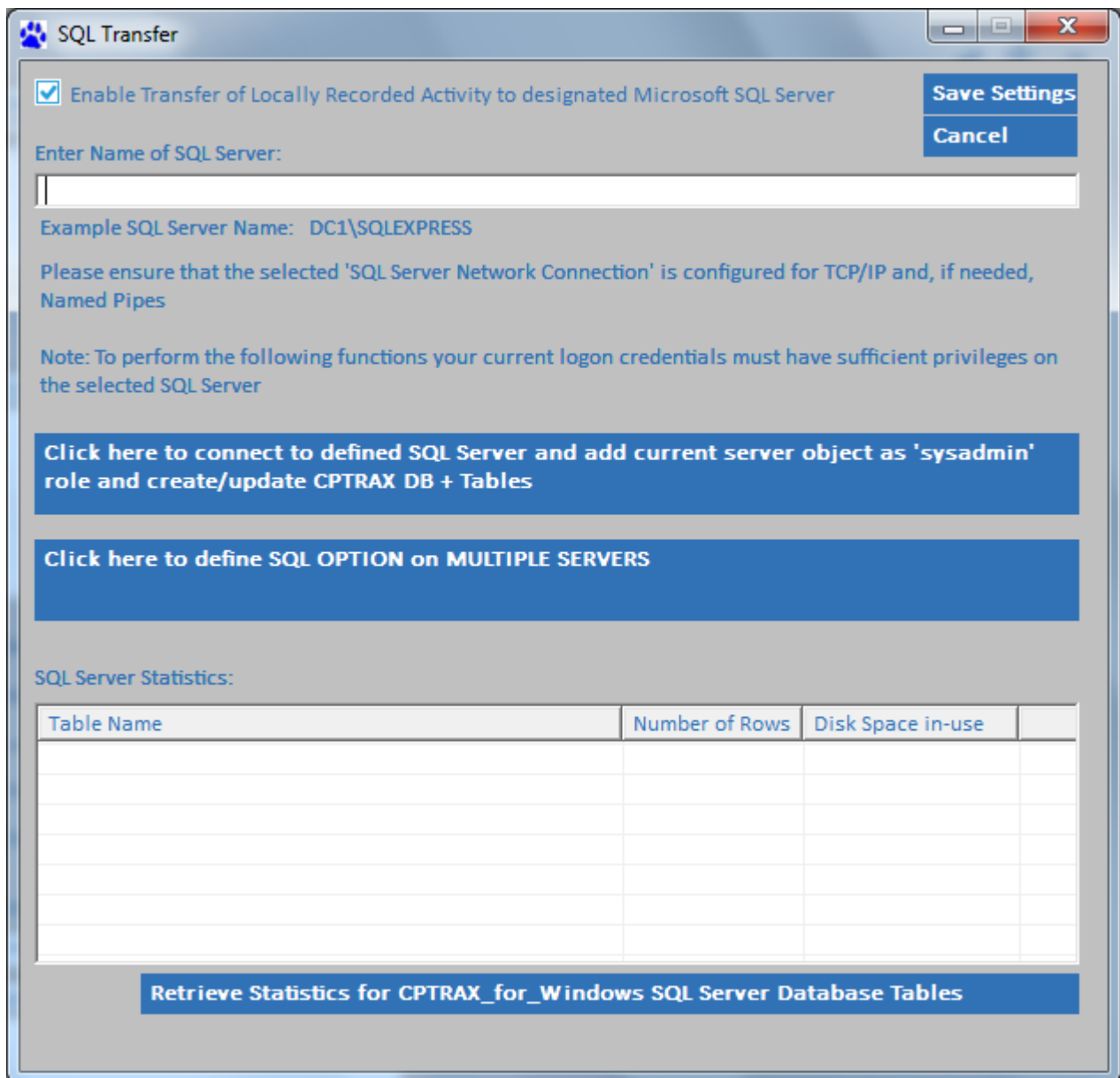


Figure 2-48

The following window will be presented:



SQL Transfer

☒ Enable Transfer of Locally Recorded Activity to designated Microsoft SQL Server

Enter Name of SQL Server:

Example SQL Server Name: DC1\SQLEXPRESS

Please ensure that the selected 'SQL Server Network Connection' is configured for TCP/IP and, if needed, Named Pipes

Note: To perform the following functions your current logon credentials must have sufficient privileges on the selected SQL Server

Click here to connect to defined SQL Server and add current server object as 'sysadmin' role and create/update CPTRAX DB + Tables

Click here to define SQL OPTION on MULTIPLE SERVERS

SQL Server Statistics:

Table Name	Number of Rows	Disk Space in-use	

Retrieve Statistics for CPTRAX_for_Windows SQL Server Database Tables

Figure 2-49

Notice in Figure 2-49 the checkbox labeled “Enable Transfer of Locally Recorded Activity to designated Microsoft SQL Server” has been checked. The default is unchecked. When this checkbox is selected and field below contains a valid SQL Server Name the CPTRAX Server Agent will attempt to send all activity it gathers from any [Profile](#) to the SQL Server.

Note: Because the SQL Transfer option only sends activity captured on the selected server by the CPTRAX Server Agent you must define the SQL Transfer option on each server that hosts a CPTRAX Server Agent where you want its recorded activity sent to your SQL Server.

Recorded activity is sent to the designated SQL Server approximately once a minute. Recorded activity transfers to the SQL Server are performed by the CPTSQLXF.EXE process that is automatically spawned by the CPTRAX Server Agent when the SQL Transfer option is defined.

To complete the SQL Transfer option setup, specify the Name of your SQL Server to use. Then, click the “Connect to defined SQL Server and add current server object as ‘dbcreator’ role and create/update CPTRAX DB + Tables” button.

When you click this button you will be presented with a “results window” similar to the following:

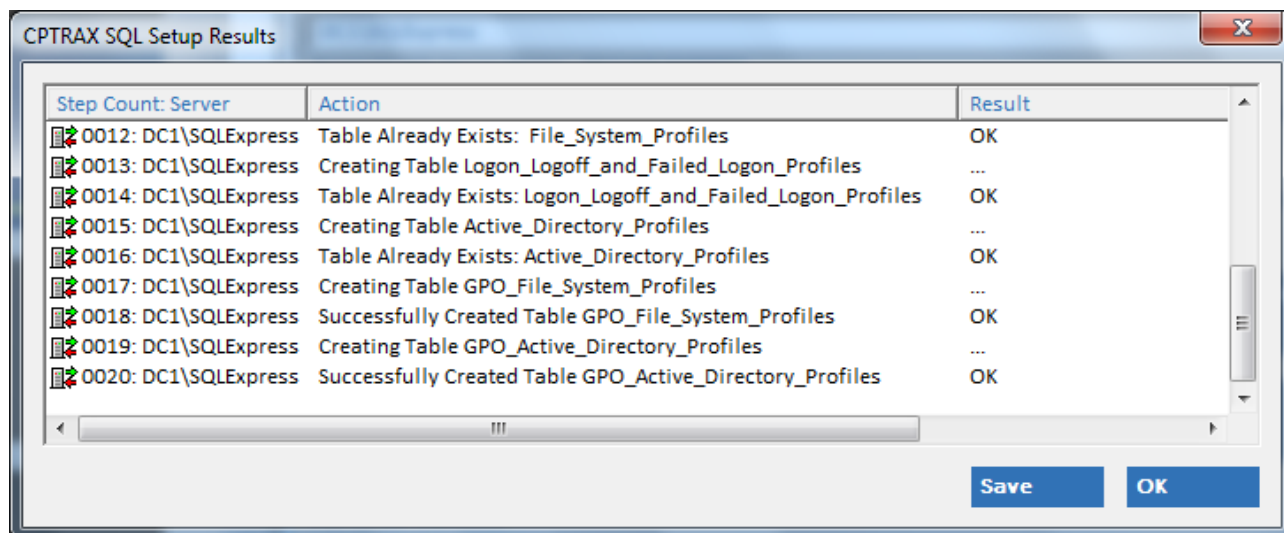


Figure 2-50

Notice that the first column specifies numbers, these are included to ensure you can sort on that column to view the results in order of occurrence.

The setup attempts to perform the following:

1. Connect to the named SQL Server
2. Create the database “CPTRAX_for_Windows”

Note: This CPTRAX installation setup process does not define a database file location or any other particulars, it leaves all details up to SQL Server to decide. If you prefer, you can create the “CPTRAX_for_Windows” database via a tool of your choice and select database file path location and other technical details to better suite your particular needs. If you create the database separately, this step will recognize that the database already exists and will use it instead of creating a new instance.
3. Add Login for “NT AUTHORITY\SYSTEM”

This is the local service account on the computer hosting the SQL Server, in this case, a computer named DC1; “Add Login” simply means adding this account name to the list of accounts recognized by the SQL Server, it does not actually create the account, the account must already exist in the Domain. This account is added in case the CPTRAX Server Agent is run on the same computer that hosts the SQL Server so it can communicate with it. For further details read the Microsoft article: [Testing a connection to SQL Server from a service running under Local System Account](#).
4. Add the database role “sysadmin” for “NT AUTHORITY\SYSTEM”

This is performed so this account can modify the CPTRAX_for_Windows database.

5. Add Login for “DOMAIN\COMPUTER\$”

This is the Domain name of the currently selected Windows computer that will host the CPTRAX Server Agent. This login is added because the CPTRAX Server Agent, when it is active, is known to remote computers by its Domain name. Therefore, if the SQL Server is on a computer that is remote to that where the CPTRAX Server Agent is running, it will connect to that remote SQL Server host via its Domain name.

Note: If the computer hosting the SQL Server is in a different Domain than the computer hosting the CPTRAX Server Agent, the two Domains must trust one another. Therefore, if no “trust” currently exists a *two-way trust* must be established. You can use the Windows-provided “domain.msc” applet to configure trust relationships between domains. [Click here to learn more about creating an External Trust between Domains](#), if the link provided has been abandoned by Microsoft, find it by searching Microsoft’s website for the topic “Create an External Trust”.

6. Add the database role “sysadmin” for “DOMAIN\COMPUTER\$”

This is performed so this account can modify the CPTRAX_for_Windows database. Please note that the ‘dbcreator’ role is insufficient for this purpose.

7. The following tables are created:

- a. File_System_Profiles
- b. Logon_Logoff_and_Failed_Logon_Profiles
- c. Active_Directory_Profiles
- d. GPO_Active_Directory_Profiles
- e. GPO_File_System_Profiles

For more comprehensive SQL installation instructions please refer to [Appendix F](#).

SQL Server Table Column (Field) Definitions

The following sections detail each CPTRAX SQL Table created and its specific field definitions.

File_System_Profiles Table

The **CREATE TABLE** statement creates the following columns (fields)

[GUID] [uniqueIdentifier] NOT NULL DEFAULT NEWSEQUENTIALID()

This column is created to ensure each record is unique and can be uniquely located. The data in this column is a GUID and is not part of the activity recorded by the CPTRAX Server Agent.

[FromServer] [varchar](128) NOT NULL

This column is the name of the Windows Computer where the CPTRAX Server Agent captured the recorded activity.

[RecType] [varchar](64) NOT NULL

This column specifies the Profile Type of the recorded activity. Value will be:
FILE SYSTEM PROFILE

[ProfileName] [varchar](128) NOT NULL

This column specifies the name of the CPTRAX Profile that recorded this row's activity.

[Action] [varchar](64) NOT NULL

This column defines the exact type of recorded activity this row (record) defines.

[TimeOccurred] [smalldatetime] NOT NULL

This column indicates the local time on the Windows computer that this row's recorded activity was captured. An example *smalldatetime* format is '20130304 11:05' indicating March 4, 2013, 11:05am.

[UserName] [varchar](512) NULL

This column indicates the name of the logged in user that performed the activity identified by this row. The name specified can be in a variety of formats. This field can be blank, usually this is due to a Windows system account performing the activity and not an actual user.

[UserLDAPName] [varchar](512) NULL

This column indicates the LDAP name of the logged in user that performed the activity. For instance, CN=Joe,OU=ACME,DC=COMPANY,DC=COM

[TSStation] [varchar](32) NULL

This column indicates the Terminal Services Station name (if was used), the Station Name is usually the same as the Windows computername of the computer used as the source of the Terminal Services connection.

[TSRemoteAddr] [varchar](32) NULL

This column indicates the Terminal Services Remote Address (if was used), the Remote Address, if available, is usually an IP-address used by the computer that was the source of the Terminal Services Connection.

[UserSID] [varchar](88) NULL

This column indicates the SID of the object named in the UserName column.

[IPv4From] [varchar](20) NULL

This column indicates the IP version 4 address of the computer where the activity originated (example: 10.1.1.51)

[IPv6From] [varchar](64) NULL

This column indicates the IP version 6 address of the computer where the activity originated (example: 2002:c6ce:d905::c6ce:d905)

[isDirectory] [varchar](16) NULL

This column indicates if the file activity was for a Directory/Folder, the value is either TRUE or FALSE.

[wasBlocked] [varchar](16) NULL

This column indicates if the file activity was blocked, the value is either TRUE or FALSE.

[ACetype] [varchar](10) NULL

This column is only used with File System Permissions changes (ACE=Access Control Entry), for such activity the value will be ALLOW or DENY. This column, when set, indicates a File Permissions activity occurred and additional details will be included in follow on columns occurring later in this row.

[FullFilePath] [varchar](1200) NULL

This column indicates the full file path of the file affected by this row's activity.

[ShareName] [varchar](128) NULL

This column indicates the name of the file system share used to access the file indicated by this row. If the access was performed locally and not via a share it will instead indicate <local access>.

[FileNameOnly] [varchar](512) NULL

This column indicates the name of the file affected by this row's activity.

[NewPathName] [varchar](1200) NULL

This column indicates the new name of the file affected by this row's activity. This is used for file (or folder) renames as well as local file copies.

[SIDOfNewOwner] [varchar](88) NULL

This column indicates the SID of the new owner, this is only used when file/folder's ownership has been changed and does not contain a value when a file/folder is newly created.

[ACLObjectLDAPName] [varchar](512) NULL

This column is only used with File System Permissions changes (ACL=Access Control List). This column, when set, indicates the LDAP name of the object receiving specified permissions to the indicated file/folder.

[ACLObjectDomain] [varchar](50) NULL

This column is only used with File System Permissions changes (ACL=Access Control List). This column, when set, indicates the Domain name of the object receiving specified permissions to the indicated file/folder.

[ACLObjectName] [varchar](512) NULL

This column is only used with File System Permissions changes (ACL=Access Control List). This column, when set, indicates the Object name of the object receiving specified permissions to the indicated file/folder.

[ACLMask] [varchar](512) NULL

This column is only used with File System Permissions changes (ACL=Access Control List). This column, when set, indicates the ACL Mask of the permissions activity, the

value can be long and indicates each discrete permission included such as “List Folders, DeleteChild, Traverse” and so on.

[ACLFlags] [varchar](64) NULL

This column is only used with File System Permissions changes (ACL=Access Control List). This column, when set, indicates the ACL Flags of the permissions activity, the value indicates where the permissions defined by the ACLMask column will be placed, for example: this folder, subfolders and files.

[ACLObjectType] [varchar](32) NULL

This column is only used with File System Permissions changes (ACL=Access Control List). This column, when set, indicates the object type of the object receiving the permissions change, for instance “FILE OBJECT” or “FILE SHARE”

The **CREATE TABLE** statement also creates a clustered primary key for the File_System_Profiles Table:

```
CONSTRAINT [CPTRAX_FSP_PK_DATE_SERVER_GUID] PRIMARY KEY CLUSTERED
([TimeOccurred] ASC,[FromServer] ASC,[RecType] ASC,[GUID] ASC)WITH (PAD_INDEX
= OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS
= ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]) ON [PRIMARY]"
```

Logon_Logoff_and_Failed_Logon_Profiles Table

The **CREATE TABLE** statement creates the following columns (fields)

[GUID] [uniqueIdentifier] NOT NULL DEFAULT NEWSEQUENTIALID()

This column is created to ensure each record is unique and can be uniquely located. The data in this column is a GUID and is not part of the activity recorded by the CPTRAX Server Agent.

[FromServer] [varchar](128) NOT NULL

This column is the name of the Windows Computer where the CPTRAX Server Agent captured the recorded activity.

[RecType] [varchar](64) NOT NULL

This column specifies the Profile Type of the recorded activity. Possible values include:
FAILED LOGON PROFILE
LOGON LOGOFF PROFILE

[ProfileName] [varchar](128) NOT NULL

This column specifies the name of the CPTRAX Profile that recorded this row’s activity.

[Action] [varchar](64) NOT NULL

This column defines the exact type of recorded activity this row (record) defines.

[TimeOccurred] [smalldatetime] NOT NULL

This column indicates the local time on the Windows computer that this row's recorded activity was captured. An example *smalldatetime* format is '20130304 11:05' indicating March 4, 2013, 11:05am.

[FailCodeValue] [int] NULL

This column indicates the numeric code of the Login Failure record types.

[FailCodeText] [varchar](128) NULL

This column indicates the "readable" version of the FailCodeValue of Login Failure record types.

[IPv4From] [varchar](20) NULL

This column indicates the IP version 4 address of the computer where the activity originated (example: 10.1.1.51)

[IPv6From] [varchar](64) NULL

This column indicates the IP version 6 address of the computer where the activity originated (example: 2002:c6ce:d905::c6ce:d905)

[LogonTime] [smalldatetime] NULL

This column indicates the local time on the Windows computer that the Logon occurred for this row's recorded activity. An example *smalldatetime* format is '20130304 11:05' indicating March 4, 2013, 11:05am.

[LogoffTime] [smalldatetime] NULL

This column indicates the local time on the Windows computer that the Logoff occurred for this row's recorded activity. An example *smalldatetime* format is '20130304 11:05' indicating March 4, 2013, 11:05am.

[NumberOfSecondsLoggedOn] [int] NULL

This column indicates the number of seconds that occurred between the Logon and Logoff Times, only used in Logoff records.

[UserName] [varchar](512) NULL

This column indicates the exact name typed in by the remote user attempting to logon. It can be in any acceptable format.

[UserLDAPName] [varchar](512) NULL

This column indicates the LDAP name of the logged in object. Value here is determined after successful logon.

[UserSID] [varchar](88) NULL

This column indicates the SID of the logged in object. Value here is determined after successful logon.

[TSUserName] [varchar](512) NULL

This column indicates the Terminal Services User Name of the logged in object. Value here is determined after successful logon.

[TSStation] [varchar](32) NULL

This column indicates the Terminal Services Station Name of the logged in object. This value is typically the Windows computername of the remote device used for logon. Value here is determined after successful logon.

[TSRemoteAddr] [varchar](32) NULL

This column indicates the Terminal Services Remote Address of the logged in object. This value is typically the IP address of the remote device used for logon. Value here is determined after successful logon.

[TSSessionName] [varchar](64) NULL

This column indicates the Terminal Services Session Name of the logged in object. This value is provided by Windows and an example is "RDP-Tcp#1". Value here is determined after successful logon.

[LogonDomain] [varchar](64) NULL

This column indicates the "logon domain" as defined by Windows that was conveyed by the remote device during remote logon.

[LogonZone] [varchar](64) NULL

This column indicates the "logon zone" as defined by Windows that was conveyed by the remote device during remote logon.

The **CREATE TABLE** statement also creates a clustered primary key for the Logon_Logoff_and_Failed_Logon_Profiles Table:

```
CONSTRAINT [CPTRAX_LLFLP_PK_DATE_SERVER_GUID] PRIMARY KEY CLUSTERED
([TimeOccurred] ASC, [FromServer] ASC, [RecType] ASC, [GUID] ASC) WITH
(PAD_INDEX = OFF, STATISTICS NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]) ON [PRIMARY]
```

Active_Directory_Profiles Table

The **CREATE TABLE** statement creates the following columns (fields)

[GUID] [uniqueIdentifier] NOT NULL DEFAULT NEWSEQUENTIALID()

This column is created to ensure each record is unique and can be uniquely located. The data in this column is a GUID and is not part of the activity recorded by the CPTRAX Server Agent.

[FromServer] [varchar](128) NOT NULL

This column is the name of the Windows Computer where the CPTRAX Server Agent captured the recorded activity.

[RecType] [varchar](64) NOT NULL

This column specifies the Profile Type of the recorded activity. Value will be:
ACTIVE DIRECTORY PROFILE

[ProfileName] [varchar](128) NOT NULL

This column specifies the name of the CPTRAX Profile that recorded this row's activity.

[Action] [varchar](64) NOT NULL

This column defines the exact type of recorded activity this row (record) defines.

[TimeOccurred] [smalldatetime] NOT NULL

This column indicates the local time on the Windows computer that this row's recorded activity was captured. An example *smalldatetime* format is '20130304 11:05' indicating March 4, 2013, 11:05am.

[ObjectClass] [varchar](128) NOT NULL

This column indicates the Active Directory Schema Object Class of the object affected by this row's activity.

[ObjectAffected] [varchar](1024) NOT NULL

This column indicates the LDAP name of the Active Directory object affected by this row's activity.

[ObjectNewName] [varchar](1024) NULL

This column indicates the **ObjectAffected's** new LDAP name that is the result of an Active Directory move / rename object activity.

[AttributeAffected] [varchar](128) NULL

This column indicates the name of the Active Directory Schema Attribute affected by this row's activity.

[WasAttributeRemoved] [varchar](20) NULL

This column indicates if the **AttributeAffected** was entirely removed, value is TRUE or FALSE.

[AttributeValueAdded] [varchar](1024) NULL

This column indicates the new value of added to the **AttributeAffected**.

[AdditionalDetailRegardingSelectedAttributes] [varchar](4024) NULL

This column indicates additional details regarding the new/modified value of the **AttributeAffected**. Currently the UserAccountControl and LastLogon attributes are further detailed

[AttributeValueRemoved] [varchar](1024) NULL

This column indicates the value removed from the **AttributeAffected**.

[PerformedByUserName] [varchar](1024) NULL

This column indicates the LDAP name of the Active Directory object (typically a user) that requested the change detailed by this row's activity.

[TSStation] [varchar](32) NULL

This column indicates the Terminal Services Station name (if was used), the Station Name is usually the same as the Windows computername of the computer used as the source of the Terminal Services connection.

[TSRemoteAddr] [varchar](32) NULL

This column indicates the Terminal Services Remote Address (if was used), the Remote Address, if available, is usually an IP-address used by the computer that was the source of the Terminal Services Connection.

[IPv4From] [varchar](20) NULL

This column indicates the IP version 4 address of the computer where the activity originated (example: 10.1.1.51)

[IPv6From] [varchar](64) NULL

This column indicates the IP version 6 address of the computer where the activity originated (example: 2002:c6ce:d905::c6ce:d905)

The **CREATE TABLE** statement also creates a clustered primary key for the **Active_Directory_Profiles** Table:

```
CONSTRAINT [CPTRAX_ADP_PK_DATE_SERVER_GUID] PRIMARY KEY CLUSTERED
([TimeOccurred] ASC, [FromServer] ASC, [RecType] ASC, [GUID] ASC) WITH
(PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]) ON [PRIMARY]
```

GPO_Active_Directory_Profiles Table

The **CREATE TABLE** statement creates the following columns (fields)

[GUID] [uniqueIdentifier] NOT NULL DEFAULT NEWSEQUENTIALID()

This column is created to ensure each record is unique and can be uniquely located. The data in this column is a GUID and is not part of the activity recorded by the CPTRAX Server Agent.

[FromServer] [varchar](128) NOT NULL

This column is the name of the Windows Computer where the CPTRAX Server Agent captured the recorded activity.

[RecType] [varchar](64) NOT NULL

This column specifies the Profile Type of the recorded activity. Value will be:
GPO ACTIVE DIRECTORY PROFILE

[ProfileName] [varchar](128) NOT NULL

This column specifies the name of the CPTRAX Profile that recorded this row's activity.

[Action] [varchar](64) NOT NULL

This column defines the exact type of recorded activity this row (record) defines.

[TimeOccurred] [smalldatetime] NOT NULL

This column indicates the local time on the Windows computer that this row's recorded activity was captured. An example *smalldatetime* format is '20130304 11:05' indicating March 4, 2013, 11:05am.

[GPODisplayName] [varchar](256) NULL

This column indicates the Display Name of the Group Policy object affected by this row's activity.

[GPOGuid] [varchar](88) NULL

This column indicates the GUID of the Group Policy object affected by this row's activity.

[ObjectClass] [varchar](128) NOT NULL

This column indicates the Active Directory Schema Object Class of the object affected by this row's activity.

[ObjectAffected] [varchar](1024) NOT NULL

This column indicates the LDAP name of the Active Directory object affected by this row's activity.

[ObjectNewName] [varchar](1024) NULL

This column indicates the **ObjectAffected's** new LDAP name that is the result of an Active Directory move / rename object activity.

[AttributeAffected] [varchar](128) NULL

This column indicates the name of the Active Directory Schema Attribute affected by this row's activity.

[WasAttributeRemoved] [varchar](20) NULL

This column indicates if the **AttributeAffected** was entirely removed, value is TRUE or FALSE.

[AttributeValueAdded] [varchar](1024) NULL

This column indicates the new value of added to the **AttributeAffected**.

[AdditionalDetailRegardingSelectedAttributes] [varchar](4024) NULL

This column indicates additional details regarding the new/modified value of the **AttributeAffected**. Currently the UserAccountControl and LastLogon attributes are further detailed

[AttributeValueRemoved] [varchar](1024) NULL

This column indicates the value removed from the **AttributeAffected**.

[PerformedByUserName] [varchar](1024) NULL

This column indicates the LDAP name of the Active Directory object (typically a user) that requested the change detailed by this row's activity.

[TSStation] [varchar](32) NULL

This column indicates the Terminal Services Station name (if was used), the Station Name is usually the same as the Windows computername of the computer used as the source of the Terminal Services connection.

[TSRemoteAddr] [varchar](32) NULL

This column indicates the Terminal Services Remote Address (if was used), the Remote Address, if available, is usually an IP-address used by the computer that was the source of the Terminal Services Connection.

[IPv4From] [varchar](20) NULL

This column indicates the IP version 4 address of the computer where the activity originated (example: 10.1.1.51)

[IPv6From] [varchar](64) NULL

This column indicates the IP version 6 address of the computer where the activity originated (example: 2002:c6ce:d905::c6ce:d905)

[GPOADSectionName] [varchar](128) NULL

This column indicates the name of the Policy Section of the Group Policy object affected by this row's activity.

[GPOADChangeAction] [varchar](16) NULL

This column indicates the Change Action of the Group Policy object affected by this row's activity. Values include Add, Remove, Change.

[GPOADChangeDetails] [varchar](4096) NULL

This column indicates further details regarding the specific changes to the Group Policy object affected by this row's activity.

The **CREATE TABLE** statement also creates a clustered primary key for the **GPO_Active_Directory_Profiles** Table:

```
CONSTRAINT [CPTRAX_GPO_AD_PK_DATE_SERVER_GUID] PRIMARY KEY CLUSTERED
([TimeOccurred] ASC, [FromServer] ASC, [RecType] ASC, [GUID] ASC) WITH
(PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]) ON [PRIMARY]
```

GPO_File_System_Profiles Table

The **CREATE TABLE** statement creates the following columns (fields)

[GUID] [uniqueIdentifier] NOT NULL DEFAULT NEWSEQUENTIALID()

This column is created to ensure each record is unique and can be uniquely located. The data in this column is a GUID and is not part of the activity recorded by the CPTRAX Server Agent.

[FromServer] [varchar](128) NOT NULL

This column is the name of the Windows Computer where the CPTRAX Server Agent captured the recorded activity.

[RecType] [varchar](64) NOT NULL

This column specifies the Profile Type of the recorded activity. Value will be:
GPO FILE SYSTEM PROFILE

[ProfileName] [varchar](128) NOT NULL

This column specifies the name of the CPTRAX Profile that recorded this row's activity.

[Action] [varchar](64) NOT NULL

This column defines the exact type of recorded activity this row (record) defines.

[TimeOccurred] [smalldatetime] NOT NULL

This column indicates the local time on the Windows computer that this row's recorded activity was captured. An example *smalldatetime* format is '20130304 11:05' indicating March 4, 2013, 11:05am.

[UserName] [varchar](512) NULL

This column indicates the name of the logged in user that performed the activity identified by this row. The name specified can be in a variety of formats. This field can be blank, usually this is due to a Windows system account performing the activity and not an actual user.

[UserLDAPName] [varchar](512) NULL

This column indicates the LDAP name of the logged in user that performed the activity. For instance, CN=Joe,OU=ACME,DC=COMPANY,DC=COM

[TSStation] [varchar](32) NULL

This column indicates the Terminal Services Station name (if was used), the Station Name is usually the same as the Windows computername of the computer used as the source of the Terminal Services connection.

[TSRemoteAddr] [varchar](32) NULL

This column indicates the Terminal Services Remote Address (if was used), the Remote Address, if available, is usually an IP-address used by the computer that was the source of the Terminal Services Connection.

[UserSID] [varchar](88) NULL

This column indicates the SID of the object named in the UserName column.

[IPv4From] [varchar](20) NULL

This column indicates the IP version 4 address of the computer where the activity originated (example: 10.1.1.51)

[IPv6From] [varchar](64) NULL

This column indicates the IP version 6 address of the computer where the activity originated (example: 2002:c6ce:d905::c6ce:d905)

[GPODisplayName] [varchar](256) NULL

This column indicates the Display Name of the Group Policy object affected by this row's activity.

[GPOGuid] [varchar](88) NULL

This column indicates the GUID of the Group Policy object affected by this row's activity.

[isDirectory] [varchar](16) NULL

This column indicates if the file activity was for a Directory/Folder, the value is either TRUE or FALSE.

[isGPOCoreFile] [varchar](16) NULL

This column indicates if the file activity was for a Directory/Folder, the value is either CORE or NON-CORE.

[GPOPolicyFilePath] [varchar](256) NULL

This column indicates the Sysvol file path starting at the {GUID} for the Group Policy File affected by this row's activity.

[GPOFullLocalFilePath] [varchar](756) NULL

This column indicates the full local file path for the Group Policy File affected by this row's activity. For instance,
"C:\windows\sysvol\sysvol\domain.local\Policies\{GUID}\...."

[GPOPolicyFileName] [varchar](128) NULL

This column indicates the file name only for the Group Policy File affected by this row's activity. For instance, "install.ins"

[NewPathName] [varchar](756) NULL

This column indicates the new name of the file affected by this row's activity. This is used for file (or folder) renames as well as local file copies.

[GPOChangeDescription] [varchar](1024) NULL

This column indicates an overall description of the specific change to the Group Policy File affected by this row's activity.

[ShareName] [varchar](128) NULL

This column indicates the name of the file system share used to access the file indicated by this row. If the access was performed locally and not via a share it will instead indicate <local access>.

[GPOFileSectionName] [varchar](64) NULL

This column indicates section name for the portion of the Group Policy File with the change recorded by this row's activity.

[GPOFileChangeAction] [varchar](16) NULL

This column indicates the change action for the specific change to the Group Policy File recorded by this row's activity. Values can be ADD ITEM or REMOVE ITEM.

[GPOFileSectionParameterName] [varchar](128) NULL

This column indicates parameter name for the portion of the Group Policy File with the change recorded by this row's activity.

[GPOFileSectionOther] [varchar](128) NULL

This column indicates other parameter name for the portion of the Group Policy File with the change recorded by this row's activity.

[GPOFileSectionValue01] [varchar](128) NULL

This column indicates the registry value type for the portion of the Group Policy File with the change recorded by this row's activity. Values include "REG_SZ", "REG_DWORD" and so on. For instance, used by Policies that affect Registry settings.

[GPOFileSectionValue02] [varchar](64) NULL

This column indicates the length of GPOFileSectionValue01's type for the portion of the Group Policy File with the change recorded by this row's activity. For instance, used by Policies that affect Registry settings.

[GPOFileSectionString] [varchar](128) NULL

This column indicates a value associated with the change to the Group Policy File affected by this row's activity.

[GPOFileSectionStringSubValue] [varchar](2048) NULL

This column indicates a value associated with the change to the Group Policy File affected by this row's activity.

The **CREATE TABLE** statement also creates a clustered primary key for the GPO_File_System_Profiles Table:

```
CONSTRAINT [CPTRAX_GPO_FSP_PK_DATE_SERVER_GUID] PRIMARY KEY CLUSTERED
([TimeOccurred] ASC, [FromServer] ASC, [RecType] ASC, [GUID] ASC) WITH
(PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]) ON [PRIMARY]
```

Viewing SQL Server Statistics

In the following Figure 2-51, within the SQL Transfer Option, click the “Retrieve Statistics for CPTRAX_for_Windows SQL Database Tables” button. When performed, the CPTRAX_CONSOLE will attempt to connect to the named SQL Server and, from the CPTRAX_for_Windows database it will retrieve current statistics for each Table. The results shown are current at the button is clicked. Click the button again to retrieve updated current statistics.

The screenshot shows a window titled "SQL Transfer" with a standard Windows interface. At the top, there is a checkbox labeled "Enable Transfer of Locally Recorded Activity to designated Microsoft SQL Server" which is checked. To the right of this checkbox are two buttons: "Save Settings" and "Cancel". Below the checkbox is a text field labeled "Enter Name of SQL Server:" containing the text "DC1\SQLEXPRESS". Underneath this field, it says "Example SQL Server Name: DC1\SQLEXPRESS". A note follows: "Please ensure that the selected 'SQL Server Network Connection' is configured for TCP/IP and, if needed, Named Pipes". Another note states: "Note: To perform the following functions your current logon credentials must have sufficient privileges on the selected SQL Server". Below these notes are two large blue buttons. The first button says "Click here to connect to defined SQL Server and add current server object as 'sysadmin' role and create/update CPTRAX DB + Tables". The second button says "Click here to define SQL OPTION on MULTIPLE SERVERS". Below these buttons is a section titled "SQL Server Statistics:". It contains a table with the following data:

Table Name	Number of Rows	Disk Space in-use
CPTRAX Active_Directory_Profiles	3160	816 KB
CPTRAX File_System_Profiles	117	40 KB
CPTRAX GPO_Active_Directory_Profiles	144	72 KB
CPTRAX GPO_File_System_Profiles	109	56 KB
CPTRAX Logon_Logoff_and_Failed_Logon_Profiles	0	0 KB

At the bottom of the window is a large blue button labeled "Retrieve Statistics for CPTRAX_for_Windows SQL Server Database Tables".

Figure 2-51

Chapter 3 – CPTRAX Quick Reports

About Quick Reports

Accessed via the CPTRAX Administration console (`cptrax_console.exe`), Quick Reports provide an immediate method to view all capture records for each Profile ([described in Chapter 2](#)) created.

CPTRAX for Windows stores all captured activity in log files that are uniquely named for the Profile, Server (where captured) and Date (of the activity). These log files are fully encrypted to maintain the integrity of the data contained within. There is no required backend database or other reporting tools. The CPTRAX for Windows Administration console provides all you need for complete reporting. See [Chapter 5](#) for Custom Reporting options.

Because there is only one log file per *Profile + Server + Date* it is possible for “today’s” log file to grow throughout the day – depending on the volume of activity being captured.

Quick Report Console

To access Quick Reports, click on the “Reports” tab at the top center-left of the console and the following will appear:

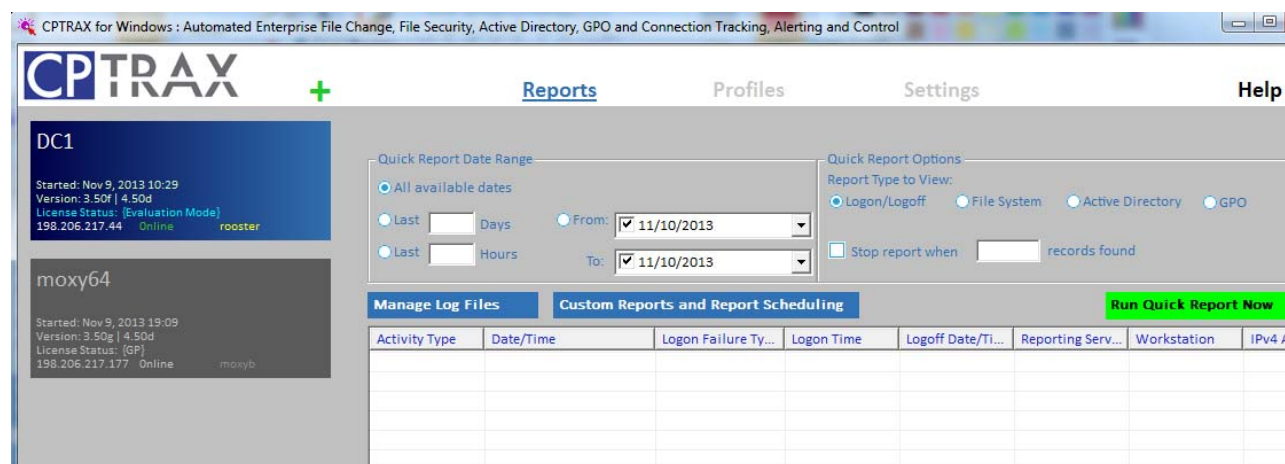


Figure 3-1

Select the desired server and fill in the desired options and click “Run Quick Report Now”.

Once report generation begins the “Run Quick Report Now” button will change and can be used to abort the report generation.

The Quick Report supports up to 100,000 records. To view larger reports click the “Custom Reports and Report Scheduling” button.

Use the “Report Type to View” selectors (they are “radio buttons”) to switch which report type is viewed. As the Quick Report is generated each record processed is automatically inserted into the screen matching its record type.

Custom Reporting

Custom Reporting is detailed in [Chapter 5](#). Custom reporting enables filtering on desired data including any of the columns shown. Custom reports can also be saved as stand-alone executables. Lastly, custom reports can be scheduled to be directly run by the CPTRAX Server Agent with output going directly to a file.

Manage Log Files

At the left side of the screen, the “Manage Log Files” button when clicked, will present a screen similar to the following:

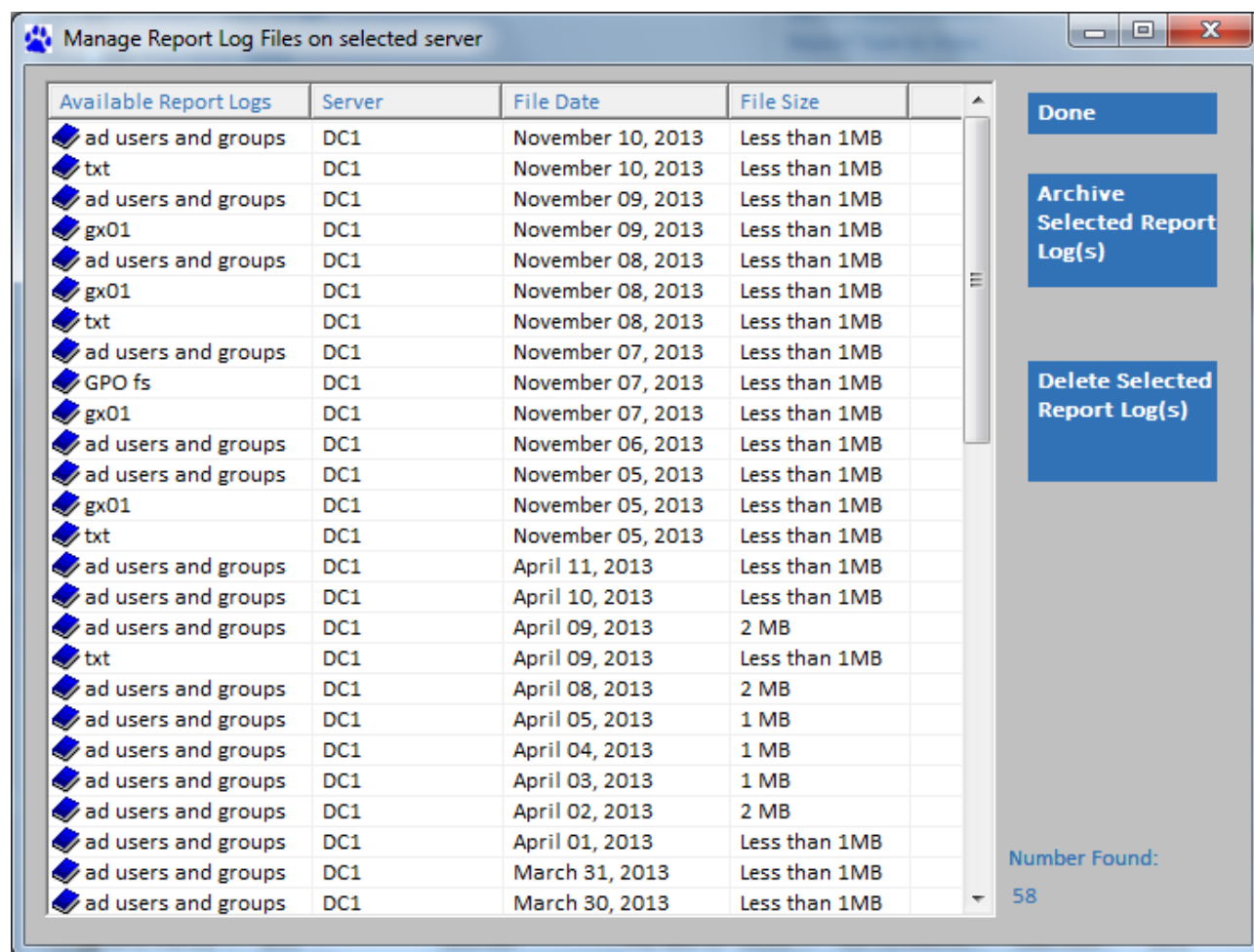


Figure 3-2

As shown in Figure 3-2, log files stored on the selected server are presented. You can sort on any of the columns as needed. There are two options, Archive and Delete.

The Archive button will archive any selected log files. What archiving does is *move* the selected file(s) to a subfolder named “**archived_logs**” – this subfolder is under the “**cptlogs**” folder that contains the logs files listed. If a log file by the same filename already exists in the archived_logs subfolder, it is concatenated to the existing archive log file so no data is lost. Once successfully archived, the log file is deleted from the “**cptlogs**” folder and from the list of available report logs.

To receive reports from an archived log file you must manually move the desired archived log file(s) back to the “**cptlogs**” folder.

Please note, when using the “Archive” and “Delete” buttons, the actions are immediately effective, there is no undo or cancel.

Chapter 4 – CPTRAX Administration Console

This chapter will review the CPTRAX Administration Console (`cptrax_console.exe`) and detail many of its options. When accessing via a lower resolution screen use the alternate CPTRAX Administration Console (`cptrax_console_1024.exe`).

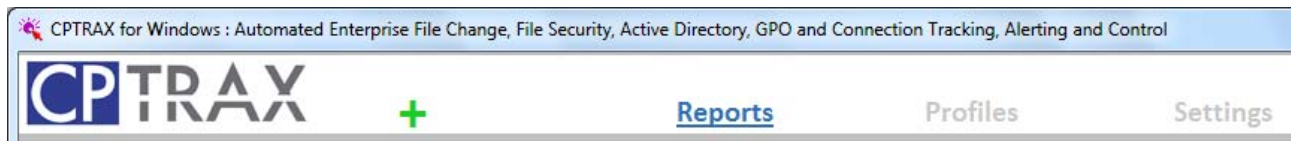


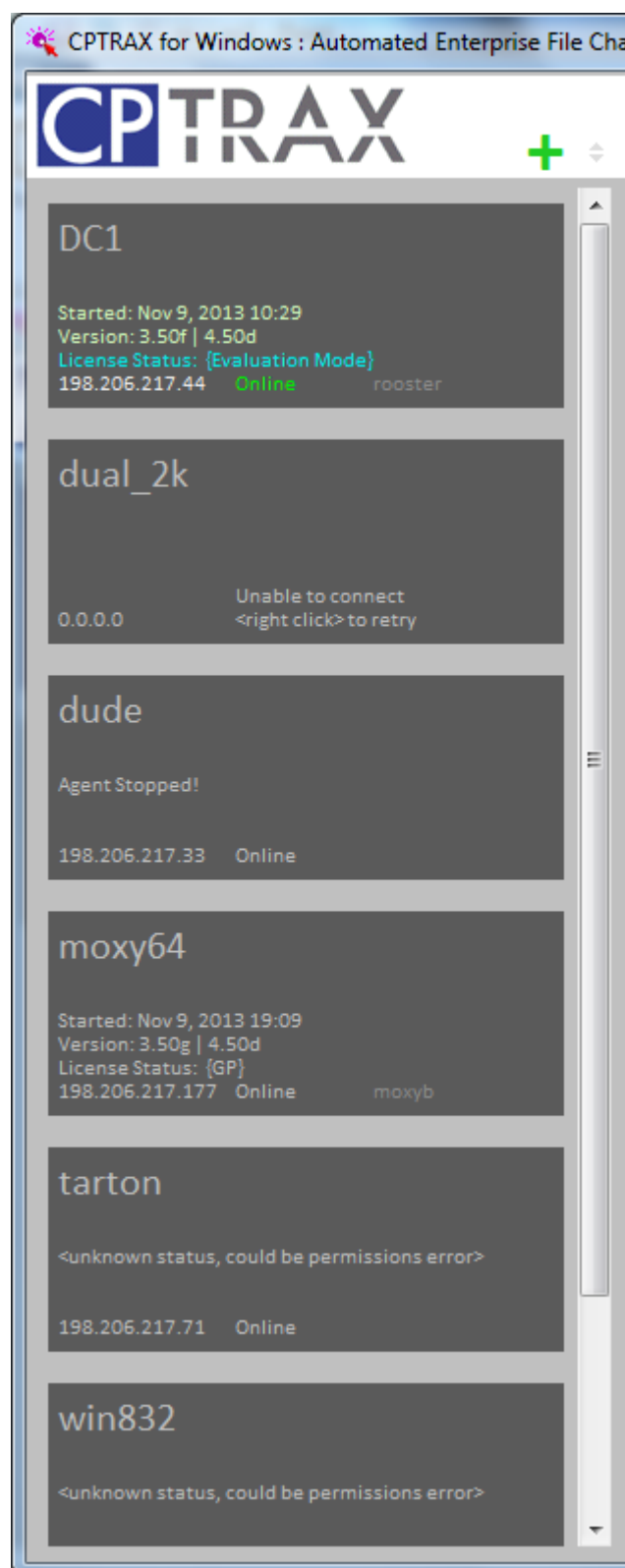
Figure 4-1

As shown in Figure 4-1, there are 3 tabs in the administration console. The `cptrax_console.exe` will remember the last tab when exiting the application. When next used on the same workstation and while logged on as the same user, that last tab will be presented first. The last tab is saved on the local machine in the following Registry key:

```
HKEY_CURRENT_USER\Software\Visual Click Software, Inc.\CPTRAX
```


Servers Managed

Servers Managed



When you first run the console (cptrax_console.exe) the list of My Servers will be populated, and an attempt will be made to connect with each server . The list of My Servers is stored on the local machine under the following registry key:

```
HKEY_CURRENT_USER\Software\Visual  
Click Software,  
Inc.\CPTRAX\MY_SERVERS
```

Each time a server is added it is automatically added to the list of My Servers.

At the top of the list you will always see a green + symbol and if there are more than 5 servers in the list a “sort” symbol appears next to the green + symbol. Click it to reverse the sort of the list of servers.

When you <right click> over the list of servers shown or anywhere on the left side of the console the following menu or similar will appear:

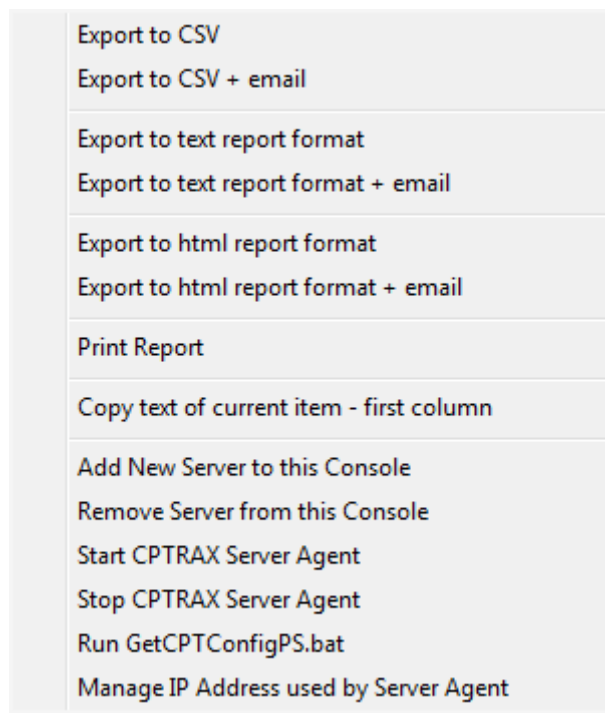


Figure 4-2

The first option “Export to CSV” will export a list of all servers plus all the details you see on each tile.

To add a new server select the “Add New Server to this Console” and the following screen will be presented:

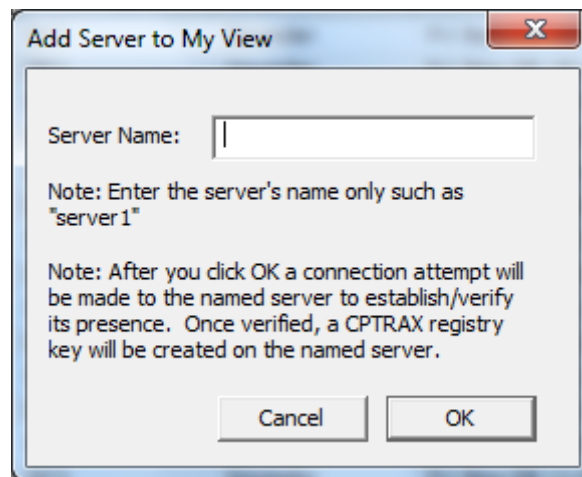


Figure 4-3

Enter the NetBIOS or SAM {Security Account Manager} name of the server. This is the same name you would use if mapping a drive or UNC path (\\server\share\path). As indicated in Figure 4-3, when you click OK a connection will be attempted with the named server. If connection is made and your logon account is sufficiently privileged, the following registry key and underlying structure will be created (if not already present):

```
HKEY_LOCAL_MACHINE\Software\Visual Click Software, Inc.\CPTRAX
```

Regardless of whether a connection is made, the server name you entered will be added to the list of “my servers”.

As shown in Figure 4-2 you can also “Remove Server from this Console” – this only removes the server from your “view” it does not uninstall CPTRAX on the selected server. To uninstall, use the “Uninstall CPTRAX Server Agent” button found on the ‘Settings’ tab. This button will be further discussed later in this chapter.

Start CPTRAX Server Agent

The two other major options in Figure 4-2 are “Start CPTRAX Server Agent” and “Stop CPTRAX Server Agent”.

If you select “Start CPTRAX Server Agent” the console will immediately attempt to initiate contact via an SMB connection with the selected server(s). If your logon account is sufficiently privileged it will then attempt to start the CPTRAX Server Agent.

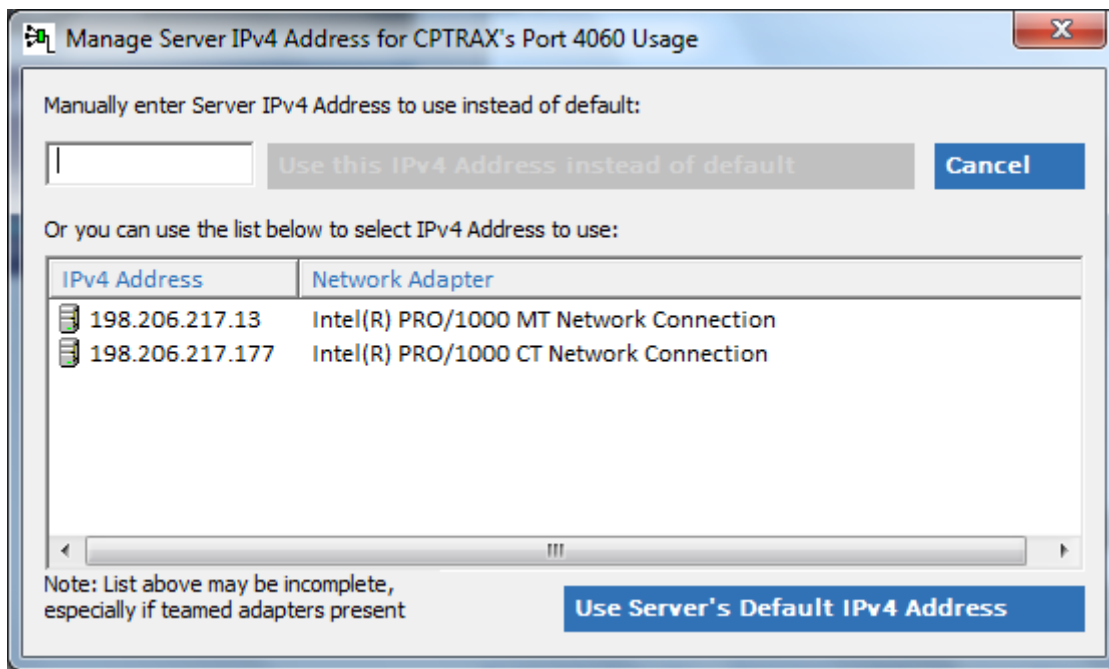
Stop CPTRAX Server Agent

If from the menu shown in Figure 4-2 you select “Stop CPTRAX Server Agent” the console will immediately attempt to initiate contact via an SMB connection with the selected server(s), and if your logon account is sufficiently privileged will attempt to stop the CPTRAX Server Agent.

Manage IP Address used by Server Agent

The final option shown in Figure 4-2 is “Manage IP Address used by Server Agent”. This option is required when the server/domain controller hosting the CPTRAX Server Agent hosts multiple IP addresses. By default, the CPTRAX Server Agent will simply choose the “first” IP address hosted and bind to it for its activities such as transmitting log files and notifying CPTALERT agents. However, in some instances this is not preferred, particularly when the host machine is using its IP addresses for specific purposes.

To overcome this default this option is used. When selected a window similar to the following will appear:



Notice the entry field at top left is initially blank. This indicates default behavior will occur as defined above.

To force the CPTRAX Server Agent to *only* bind to a particular IP address on its host machine either manually enter the address or select from the list shown. Please note that the list shown may be incomplete, particularly if teamed adapters are used. It does not matter if the desired IP address appears in the list. However, the desired IP address must be present at the host. The list shown is collected from the selected server's registry.

To restore default behavior, simply click the "User Server's Default IPv4 Address".

"Agent Running?" responses

As shown in the figure to the left of Figure 4-2, there are number of different details shown for each server. The following are possible License (also known as "Token") States:

- {Evaluation Mode}
 - Evaluation License is installed – even if other tokens are present, evaluation takes priority
- {No Valid Token}
 - May take up to 2 minutes to reflect any change in token status
- {FS}
 - Valid File System Tracking Token present and no other valid Tokens found
- {LL}
 - Valid Logon+Logoff Tracking Token present and no other valid Tokens found
- {AD}
 - Valid Active Directory Tracking Token present and no other valid Tokens found
- {GP}

- Valid GPO Change Tracking Token present and no other valid Tokens found
- {FS} {LL}
 - Fully Licensed for File System Tracking and Logon+Logoff Tracking
- {FS} {LL} {AD}
 - Fully Licensed for File System Tracking, Logon+Logoff Tracking and Active Directory Tracking
- {FS} {LL} {AD} {GP}
 - Fully Licensed for File System Tracking, Logon+Logoff Tracking, Active Directory Tracking and GPO Change Tracking
- Yes {ExceedFS} {ExceedLL}
 - Valid tokens found for File System Tracking and Logon+Logoff Tracking but each license has been exceeded – usually because the token(s) has been installed on more than the licensed number of servers
- Yes {ExceedFS} {LL}
 - Valid tokens found for File System Tracking and Logon+Logoff Tracking but the license for File System Tracking has been exceeded – usually because the token(s) has been installed on more than the licensed number of servers
- Yes {FS} {ExceedLL}
 - Valid tokens found for File System Tracking and Logon+Logoff Tracking but the license for Logon+Logoff Tracking has been exceeded – usually because the token(s) has been installed on more than the licensed number of servers
- Yes {...} {ExceedAD}
 - The Active Directory token(s) installed are insufficient and tracking has been disabled
- Yes {...} {ExceedGP}
 - The GPO Change Tracking token(s) installed are insufficient and tracking has been disabled
- Yes {Auditor}
 - Indicates an Auditor token is installed. In Auditor / report only mode the CPTRAX Server Agent does not act on any defined Profile. This means no activity will be captured or blocked. When in Auditor / report only mode the agent will only receive log files from other servers hosting the CPTRAX Server Agent - but only if defined as a Department Host. More on Department Hosts can be found in [Chapter 1](#).
- No
 - Server Agent not running or your logon account does not have sufficient privileges to receive a response

Agent Version, Driver Version

As shown in the figure to the left of Figure 4-2 among details shown can include “Agent Version” used to indicate the versions of the components of the CPTRAXW Server Agent currently in-use at the selected server.

Note that the CPTRAX Server Agent will not load Kernel Driver (CPTW_K32.SYS/CPTW_K64.SYS/CPTWK646.SYS if an Auditor token is installed as this file is not used when that token type is present.

For more information regarding the Auditor token type, review the License Tokens section of [Chapter 4, Settings tab](#).

Start Time and IP Address

The “Started” value indicates when `CPTRAXW.EXE` was most recently started on the selected server.

The “IP Address” value indicates the IP Address that the server is known by for your workstation. The server itself can have multiple IP Addresses but your workstation would likely only use one of those IP Addresses to connect to that server.

Settings Tab: Overview

At the top right of Console is the Settings tab:

The screenshot displays the 'Settings' tab in the CPTRAX console. At the top, there are four tabs: 'Reports', 'Profiles', 'Settings' (which is active and underlined), and 'Help'. The main content area is divided into several sections. The top section features a table titled 'CPTRAX for Windows Tokens Installed' with columns for 'Count', 'License Valid Until', 'Organization', and 'Co'. Below this is a section for email alerts, including a text input for 'Send Alerts to these email addresses (for profiles where defined to use this list)' and a checkbox for 'Retain Log Files after transfer to Department Host(s)'. Further down are configuration fields for 'Log File Path (Share)', 'Log File Transfer Frequency' (set to 15 minutes), 'Purge report log files where last update was more than 0 days ago', and 'GPO Change Tracking Temp Path'. A 'Department Hosted by this server' section includes a text input and a checkbox for 'Allow Alert Consoles to attach to this server?'. On the right side, a vertical sidebar contains several blue buttons: 'SQL Transfer Option' (with a 'NOT Enabled' status), 'Email Server Configuration' (with a 'NOT Enabled' status), 'Update CPTRAX Server Agent', 'Uninstall CPTRAX Server Agent' (with a 'Requires Confirmation' status), and 'Restore CPTRAX Registry Settings'. At the bottom of the main area are three buttons: 'Enterprise Server Host Option', 'View Active Alert Agent Connections', and 'Save Changes'.

Figure 4-4

Settings Tab: SQL Transfer Option

This option is detailed in [Chapter 2](#).

Settings Tab: Email Server Configuration

This option is detailed in [Chapter 2](#).

Settings Tab: Update CPTRAX Server Agent

This button will attempt to update the CPTRAX Server Agent for the currently selected server. When this button is clicked, the following screen will appear:

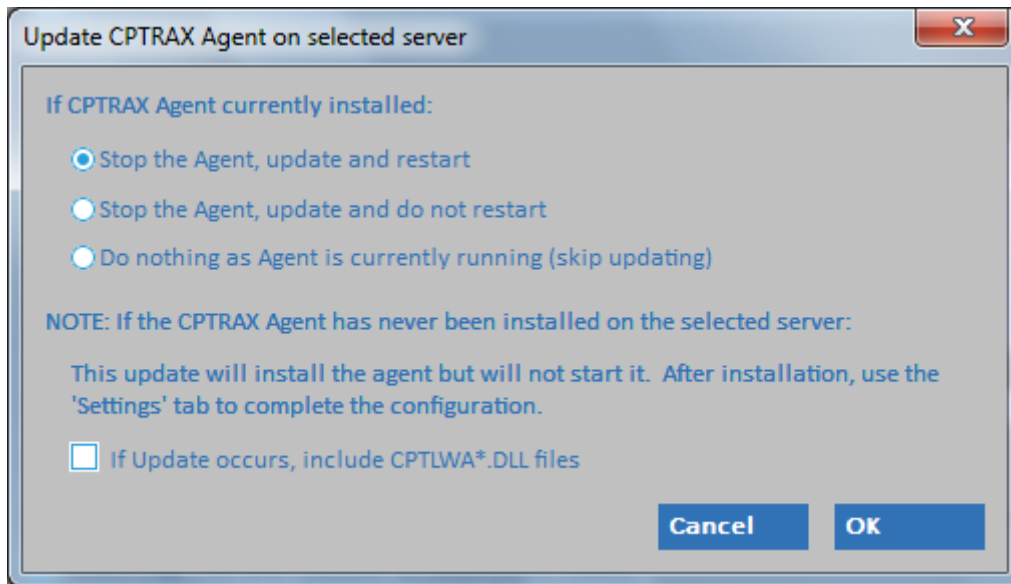


Figure 4-5

As shown in Figure 4-5, select the appropriate option and click OK to begin the update. During the update, the following screen will be presented:

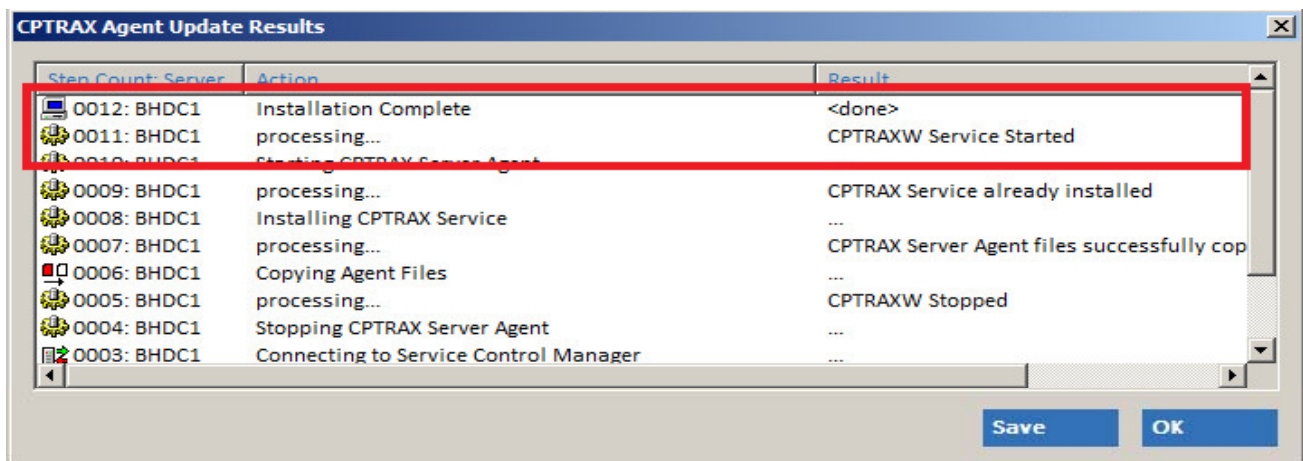


Figure 4-6

Be sure to click on the first column “Step Count: Server” to sort the rows in order of progression.

At the lower right in Figure 4-6 there is a “Save” button . This button will save the full text of the results of the updates. Before saving, be sure to click on the “Step Count: Server” column to sequence the results in the order of occurrence.

Uninstall CPTRAX Server Agent

This button will attempt to uninstall the CPTRAX Server Agent for the currently selected server. When this button is clicked, the following warning will appear:

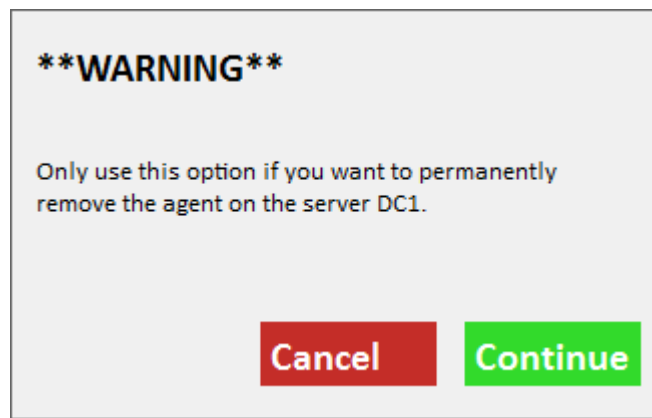


Figure 4-7

If you click “Continue” the following screen will appear:

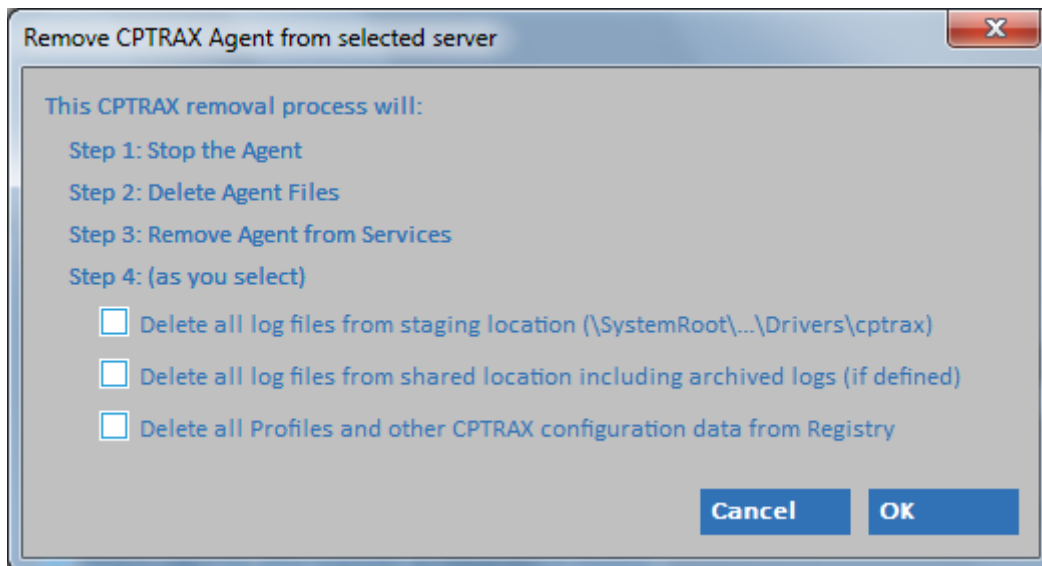


Figure 4-8

As shown in Figure 4-8, select the appropriate options and click OK to begin the uninstall process. During the removal, a progress screen will be presented that details the removal actions as each occurs on the selected server.

Log File Path (Share)

The Log File Path Share or “reporting share” is a *share* and optional path within the share where the selected server will place its report ready log files. Please note that a subfolder named “**cptlogs**” will always be created under the path specified. Only those users producing reports require access to the selected *share\path\cptlogs*. If the currently selected server has no public shares or if you are not certain of the names of the available public shares, click the “Path Assistance” button.

Typical Windows installations offer several options to create file system shares, some require you to be present at the actual server console. Remote file system share creation can be accomplished via the WMIC tool (Windows Management Instrumentation Command line tool).

And the Windows resource kit includes the `rmtshare.exe` command line tool that can be used to remotely create shares.

For Windows 2008 and later the native Windows ‘Computer Management’ interface can be used to create remote shares.

If there is no Log File Path Share defined, the *default* of:

```
\SystemRoot\System32\Drivers\CPTRAX\cptlogs
```

or on 64-bit systems:

```
\SystemRoot\SysWow64\Drivers\CPTRAX\cptlogs
```

will be used. If this *default* occurs you will not be able to view any log file activity as the `cptrax_console.exe` as it requires the Local Log File Path to be defined. If this occurs, you will need to manually copy any existing log files from this *default* location to the Local Log File Path (**cptlogs** subfolder).

[See Appendix C](#) for the procedure to confirm appropriate file permissions are set on the share and optional path.

NOTE:

If you change the “Log File Path Share”, any existing log files will remain in their current location and must be manually moved if you want them to be available for reporting. There is no automatic relocation of log files if you change the reporting share. There are no special instructions for moving existing log files, just copy them to the new reporting share’s “**cptlogs**” folder. The same is true for any archived log files.

Log File Space Considerations

It is recommended that the “**cptlogs**” subfolder created within the selected “Local Log File Path” have File Compression enabled. Windows File Compression is easy to set up and has very good performance. To enable file compression, simply start a Windows Explorer session and right click on the “**cptlogs**” folder and select “Properties”; then click on the “Advanced...” button and check the “Compress contents to save disk space” or similarly named option and click OK.

In general, CPTRAX for Windows log files:

- Use approximately 2000 bytes per record for Logon+Logoff Profiles
- Use approximately 5500 bytes per record for File System and Active Directory Profiles
- Use approximately 4000 bytes per record for GPO Change Tracking Profiles
- 180,000 - 500,000 records per gigabyte of disk space
- 18 - 50 million records per terabyte of disk space

With compression enabled you will be able to store more than double the number of records per gigabyte as with compression disabled.

Log File Transfer Frequency

The “Log File Transfer Frequency” indicates how often log files are transferred from the selected server to servers hosting [Departments](#) that the server agent belongs to. The minimum frequency is every 15 minutes and the maximum is once a day or 1440 minutes. Any ready log files will have their transmission initiated at the beginning of the next transfer cycle.

You can view ready log files in the folder

```
\SystemRoot\System32\Drivers\CPTRAX
```

or, on 64bit systems

```
\SystemRoot\SysWow64\Drivers\CPTRAX
```

on the selected server. Ready log files have a file extension of [TXY](#). See [Appendix A](#) for more details regarding the files used by the CPTRAX Server Agent.

Log files are securely transferred directly between CPTRAX Server Agents via TCP/IP. Log files are not transferred via SMB/CIFS to the “reporting share” path defined. Therefore, there is no requirement for remote servers to have access to a defined “reporting share”. The “reporting share” is only used for users producing reports.

Retain Log Files

The “Retain Log Files after transfer to Department Host(s)” checkbox, if set, will place a copy of each ready log file in the **cptlogs** subfolder of the [Log File Path Share](#). This option is redundant if the selected server is defined as a Department Host (for any Department). Ordinarily you would use this option if the selected server as not a Department host but you wanted it to retain a copy of each log file it created.

Purging Log Files

The “Purge report log files where last update was more than N days ago” option defaults to zero or never purge. The purging of log files means the complete erasure of any matching log files. The value of N days ago is based on the date the file was last updated/modified. The minimum value is 7 days; the maximum value is 9999 days. A value of 0 indicates never purge.

Managing Log Files

Please refer to details in [Chapter 3](#).

Restore CPTRAXC Registry Values

The CPTRAX Server Agent retrieves its configuration settings from the Registry of the machine hosting the agent. The Registry key used is:

```
HKEY_LOCAL_MACHINE\Software\Visual Click Software, Inc.\CPTRAX
```

While the CPTRAX Server Agent is active, if any change is made within this key or its subkeys, the agent will set a 2 minute timer after which it will archive this Registry key and all subkeys. The agent will also archive this Registry key and all subkeys each time the agent is started, even if there have not been any changes.

The file:

```
CPTRAXW_00000000.savekey
```

always contains the most recent copy of the CPTRAX Server Agent Registry key and subkeys.

Except for the '00000000' save key, these Registry archives are automatically purged after 7 days. There is no option for altering the 7 day purge, it is predefined.

The Registry archives are stored on the same machine hosting the agent in the folder:

```
\SystemRoot\System32\Drivers\CPTRAX (32bit systems)
-or-
\SystemRoot\SysWow64\Drivers\CPTRAX (64bit systems)
```

Each archive is encrypted to maintain its integrity.

To restore a Registry archive, click on “Restore Registry values from archive” button found at the bottom right of the server configuration screen. When clicked, this button will present a screen similar to:

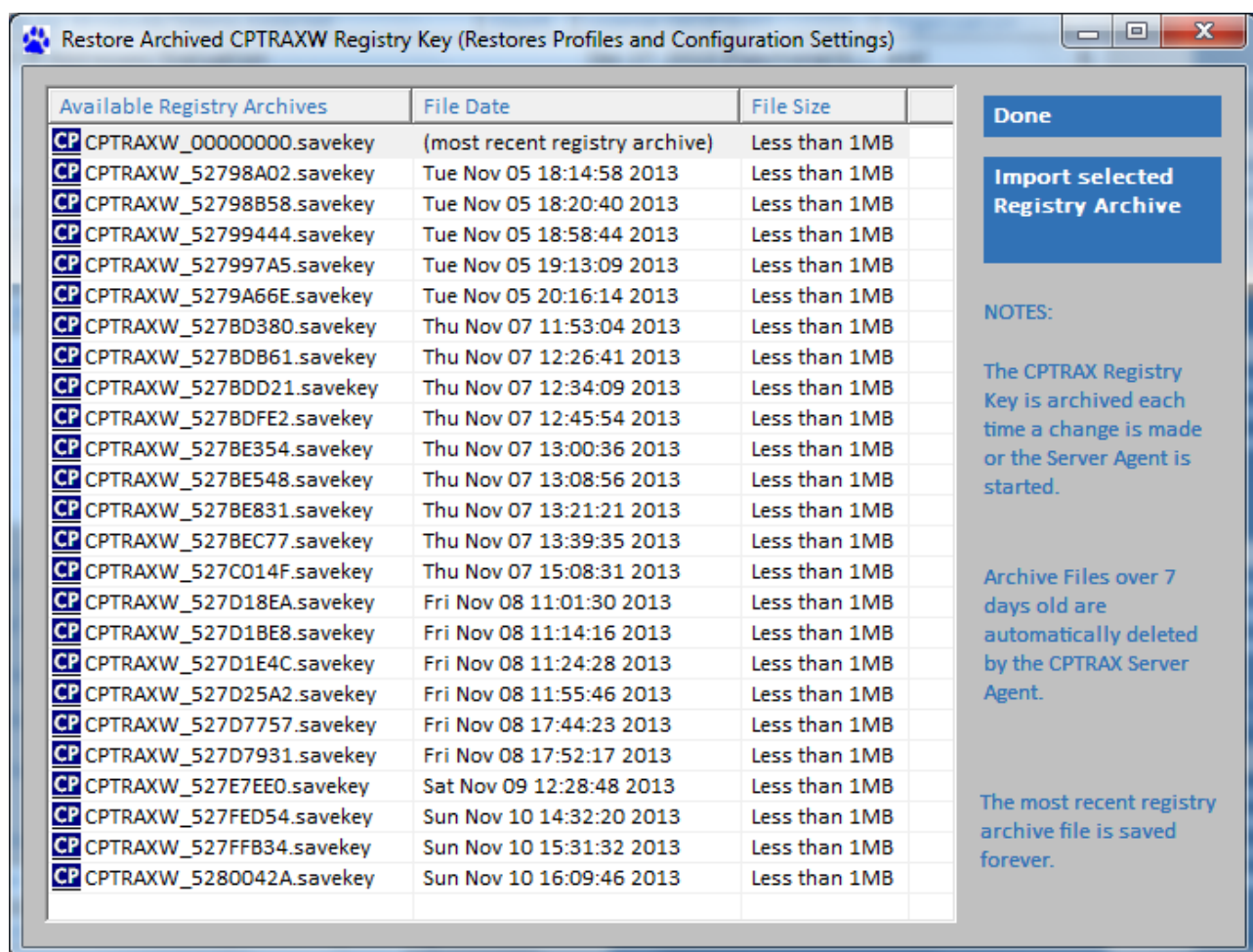


Figure 4-9

As mentioned previously, the first file, CPTRAXW_00000000.savekey is always the most recent copy of the CPTRAX Server Agent Registry key structure.

The remaining Registry archives have a File Date that indicates when each was created.

Why would you want to restore a Registry archive? Several reasons including:

- Accidental deletion of a Profile, Custom Report, Scheduled Activity and so on
- Server was restored after a critical error and the CPTRAX Registry entries were erased
- You can also use this function to quickly establish a new server with the same definitions as another server – to accomplish this, simply copy the selected savekey file to the \SystemRoot\System32\Drivers\CPTRAX (or \SystemRoot\SysWow64\Drivers\CPTRAX) folder of the new server and use the CPTRAX Administration Console to import the savekey file.

Please note, the savekey file is not the same as a .reg file and cannot be used by REGEDIT's import function.

Department Hosted

Departments are discussed in-depth in [Chapter 1](#). If the “Department Hosted by this server” field has a value then the selected server will be a Department Host for the named Department. If the “Department Hosted” field empty then the server does not host a department. A server can only host one Department. A server can be a member of several Departments.

In short, a Department Host will act as a repository for log files created on it and on any other server that either Hosts the same Department or is a member of the same Department. The name specified in the ”Department Hosted” field is not case sensitive.

Departments Reports To (Department Membership)

The “Departments this server Reports to” list indicates those Departments the currently selected server is a member of. When a server is a member of a Department it indicates that any recorded activity (activity logs) will be transmitted to each server that hosts that Department. Please note, that if a server is defined to be a Department Host it is also, implicitly, a member of that Department.

Use the ‘Add Department ‘ and “Remove Department” buttons to alter Departments Reported to (Department Membership).

Departments are discussed in-depth in [Chapter 1](#).

Enterprise Server Host Option

When you click the “Enterprise Server Host Refresh Option” button the following screen will appear:

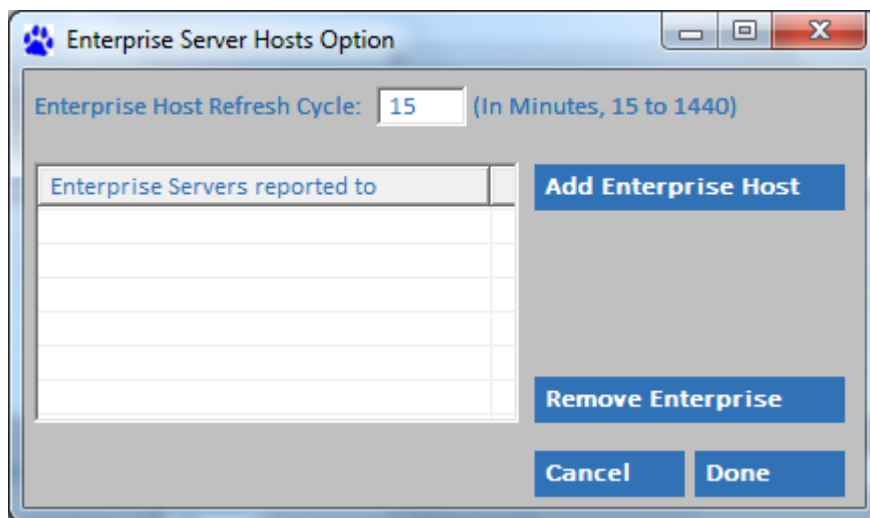


Figure 4-10

The “Enterprise Host Refresh Cycle” field allows you to define how often the CPTRAX for Windows Server Agent, when active, on the currently selected server will update each

configured Enterprise Host. If the field is empty the default value of 15 minutes will be used. The maximum is once a day or 1440 minutes. If a value greater than 1440 is entered it will be set to 1440.

For each Refresh Cycle, the Server Agent will, via TCP/IP (port 4060) communicate its current status. This communication could range from 1000 bytes to 10,000 bytes depending on how many server agents on other servers are reporting to the currently selected server. If the Server Agent has no servers reporting to it the communication size will be approximately 1000 bytes. If the Server Agent is configured to be an Enterprise Host (by other servers defined to report to it as such) it will also relay status of each Server Agent it is actively aware of, this could range up to 10,000 bytes per Refresh Cycle.

Use the ‘Add Enterprise Host ‘ and “Remove Enterprise Host” buttons to alter Enterprise Servers Reported to. The server name specified must either be the NetBIOS name (also known as its SAM Name) such as ‘FS1’ or that server’s IPv4 address.

Typically you would use this option when you have a network where servers reporting to one another are not in the same Active Directory Forest.

Enterprise Hosts are further discussed in-depth in [Chapter 1](#).

Alert Consoles

When the “Allow Alert Consoles to attach to this server?” checkbox is selected users using CPTALERT.EXE will be allowed to attach to the selected server’s CPTRAX Server Agent to receive alerts for any Profiles defined to send alerts.

The “Allow Alert Consoles to attach to selected server?” checkbox is, by default, unchecked. When unchecked, Alert Agent consoles are prevented from connecting to the server. When checked, new connections by Alert Agent consoles will be allowed. Alerts generated by Profiles will be sent if the selected Profiles are defined to allow alerts to be sent to [Alert Agent consoles](#). If unchecked while Alert Agent consoles are currently connected to the server, they will remain connected to the server agent but will no longer receive alerts from Profiles. They will still receive alerts from the server agent – the only alert received will be if the server agent unloads.

When you click the “View Active Alert Connections” a screen similar to the following will appear:

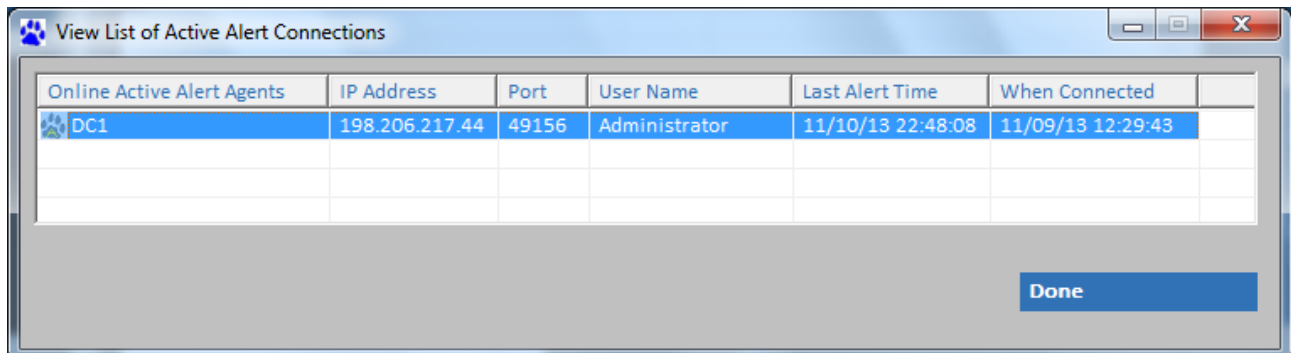


Figure 4-11

The values therein are retrieved directly from the CPTRAX Server Agent on the selected server via TCP/IP communication on Port 4060. The list presented are Alert Agent consoles ([use of described at the end of Chapter 2](#)) currently connected to that server agent. There is no option to disconnect Alert Agent consoles. Each connected Alert Agent console can only be disconnected by selecting the disconnect option at the client end in the Alert Agent console.

The details shown include:

- Workstation Name
- IP Address of the Workstation
- TCP/IP Port open at the Workstation – in use for receipt of alerts from server agent
- User that started the Alert Agent on that Workstation
- Last time an Alert was sent to the workstation
- Time the Alert Agent connected to the server agent

If the server agent is unloaded, all Alert Agent consoles are automatically disconnected and will need to reconnect to the server agent after it is restarted.

There is no restriction on who can use an Alert Agent console.

License Tokens

At the top of the ‘Settings’ tab you will find the “CPTRAX for Windows Tokens Installed” list

This list will reveal all tokens (licenses) installed on the selected server. Use the blue + symbol above-right to Add a License Token. Use the blue – symbol to Remove a License Token. Please note that the CPTRAX for Windows Server Agent, when active, will automatically remove any invalid or expired tokens. For instance, if the token installed is for a specific IPv4 address range and the server does not host an IP address within that range, that token will be automatically removed. Likewise, tokens that specify a specific server name, will automatically be removed if the name of the server where installed does not match.

When installed, the token(s) are stored in the Registry of the selected server in the key:

```
HKEY_CURRENT_USER\Software\Visual Click Software, Inc.
```

Tokens are additive. Therefore if you have multiple tokens installed, the “Count” of each is accumulated.

If you are importing the CPTRAX for Windows Registry key from another server, any tokens installed in that key will be available. And, when active, any invalid or expired tokens will be automatically removed by the Server Agent.

Please note, when using the “Add” and “Remove” buttons to manage tokens, unlike all other fields and values on the Settings tab, **changes are implemented immediately**. All other fields and values are only implemented if the “Save Changes” button is clicked.

Auditor Tokens and Auditor Mode

If any Auditor tokens are installed, the CPTRAX for Windows Server Agent will automatically operate in Auditor mode *only*. Auditor mode means the Server Agent will not act on any Profiles defined (no tracking or controlling) it will only receive log files. And, to receive log files the server operating in Auditor mode must be defined as a [Department Host](#) and servers gathering activity log files must be configured to be a member of the Department the Auditor workstation hosts.

Token License Scan [AD Domain, LDAP path or AD Container]

For any tokens installed that include an AD Domain, LDAP path (or DNS name) or AD Container path, the CPTRAX for Windows Server Agent will confirm license compliance at various times each day. When the installed tokens are being verified the Server Agent will scan the Global Catalog for the CPTRAXW serviceConnectionPoint objects that each Server Agent maintains. If this object is not present the Server Agent will cease functioning but remain loaded. Each such object will be verified via TCP/IP. Violation Alerts will be sent to each connected [Alert Console](#). If an Evaluation Token is installed, a license scan *will not* be performed.

Token License Scan [AD Object Count]

For any Active Directory tokens installed, the CPTRAX for Windows Server Agent will confirm license compliance at various times each day. The object count(s) defined by the installed token(s) will be verified. For this type of token there is no inter-server verification. Violation Alerts will be sent to each connected [Alert Console](#). If an Evaluation Token is installed, a license scan *will not* be performed.

Ethernet Switches and ARP Tables

For any tokens using an IP Range, if any of the nodes being pinged do not actually exist, the intervening Ethernet switch(es) will build an ARP entry (ARP = Address Resolution Protocol). Please note that this action is true of any software that scans network nodes.

We have found that some Ethernet switches will switch from hardware switching to software switching if the ARP Table grows beyond an internal limit. If this occurs, any workstations and servers connected to the intervening switches will begin operating very slowly. Most will recover after a few minutes.

If you experience unexpected slowness or timeouts on your network when the CPTRAX for Windows Server agent is active and has token(s) installed that specify an IP address range you may be experiencing “software switching” mode of your switches.

Remedies include:

- Flushing the ARP Cache on the switch(es)
 - Slow network, network dropout, network timeout, workstation timeout
- Power cycling the switch(es) (if unable to flush the ARP Cache)
- Upgrading switches to those with higher ARP Table limits or no limit

Generally, once the ARP Cache is flushed the switch will perform “at speed” for a long time to come. We have found that such switches have been in-use for months (or years) without ever flushing the ARP Cache and after a flush will take a long time to overflow the ARP Table again.

About Profile Management Access

Creating and managing Profiles is performed via an encrypted SMB connection to the selected server’s Registry. Your logon account at the selected server must be sufficiently privileged to perform Registry modifications in the following Registry key at the server:

```
HKEY_LOCAL_MACHINE\Software\Visual Click Software, Inc.\CPTRAX\Profiles
```

Add New Profile to selected Server

This button is fully described in [Chapter 2](#).

Rename Profile on selected Server

The “Rename Profile” acts on a single Profile. If multiple Profiles are selected only the first one will be renamed. If the CPTRAX Server Agent is active on the selected servers it will recognize the rename and begin using the new Profile name for activity log files within 15 minutes.

When a Profile is renamed its existing activity log files remain under the old name, they are not renamed. There is no option to rename old activity log files. The Profile’s log files remain available for reporting both in [Quick Reports \(Chapter 3\)](#) and in Custom Reports (Chapter 5) via its [wildcard option](#).

If there are any existing [Custom Reports](#) that specifically include the renamed Profile, each such Custom Report will need to be updated with the new Profile name as there is no automatic update of Custom Reports with new Profile names.

Delete Profile on selected Server

When a Profile is deleted it is removed from the Registry key at the selected server. If the CPTRAX Server Agent is active on the selected server it will stop acting on that Profile after 2 minutes (as there is a preset 2 minute delay from when the Profile is deleted until the agent acts on it).

When a Profile is deleted its activity log files remain, they are not deleted. To delete activity log files use the “Manage Log Files” button on the ‘Reports’ Tab. See [Chapter 3](#) for additional details.

The deleted Profile’s log files remain available for reporting both in [Quick Reports \(Chapter 3\)](#) and in Custom Reports (Chapter 5) via its [wildcard option](#).

If there are any existing [Custom Reports](#) that specifically include the deleted Profile (created prior to the Profile's deletion), each such Custom Report will still "find" all log files for that Profile. This happens because the Custom Report will seek any log files with the now deleted Profile's name. Remember, any existing log files for a delete Profile remain available for reporting.

Disable / Enable Profiles on selected Server

If you click and select a Profile and then <right click> you will be presented with a pop up menu:

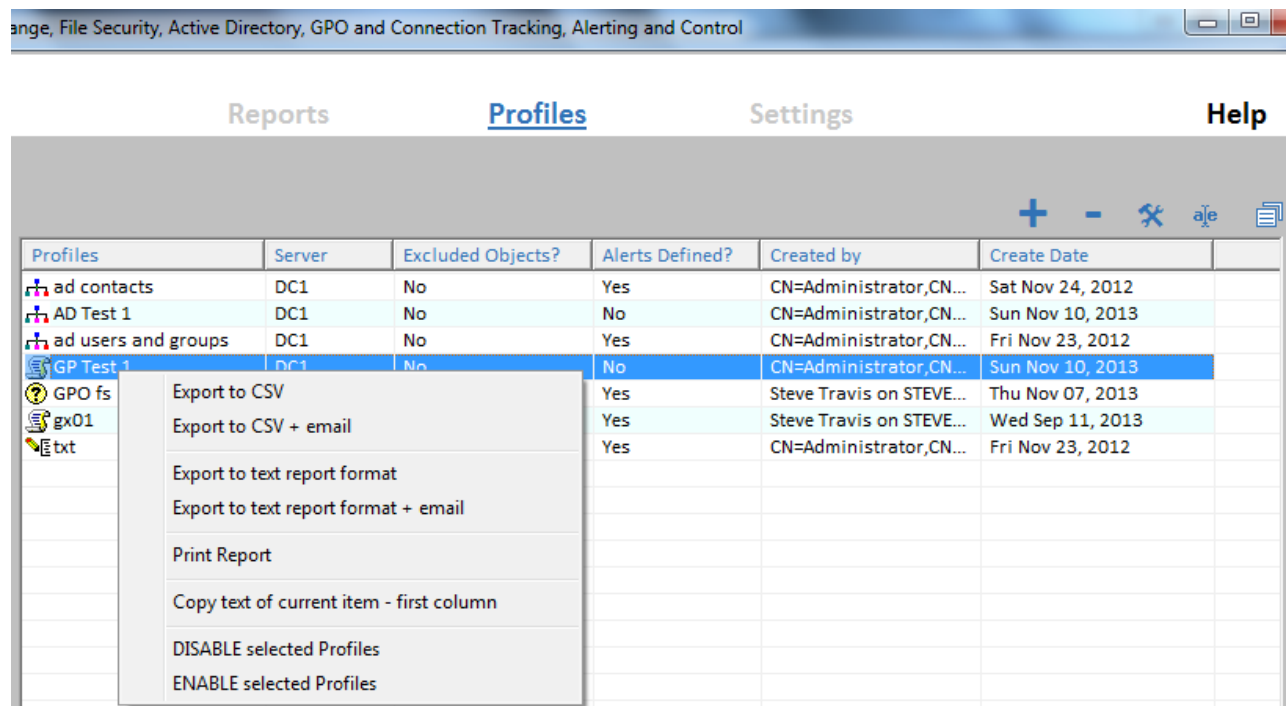


Figure 4-12

At the bottom of the menu you will find the options to Disable or Enable. When you Disable a Profile, its definition remains, the CPTRAX Server Agent, after a 2 minute delay, will stop performing that specific Profile's definition. And, when you Enable a disabled Profile, the CPTRAX Server Agent, after a 2 minute delay, start/resume performing that specific Profile's definition.

Copy Profiles to other Servers

Any Profiles listed can be easily copied via drag-and-drop to another server.

Here is the procedure:

First, select the server and Profiles you want to copy:

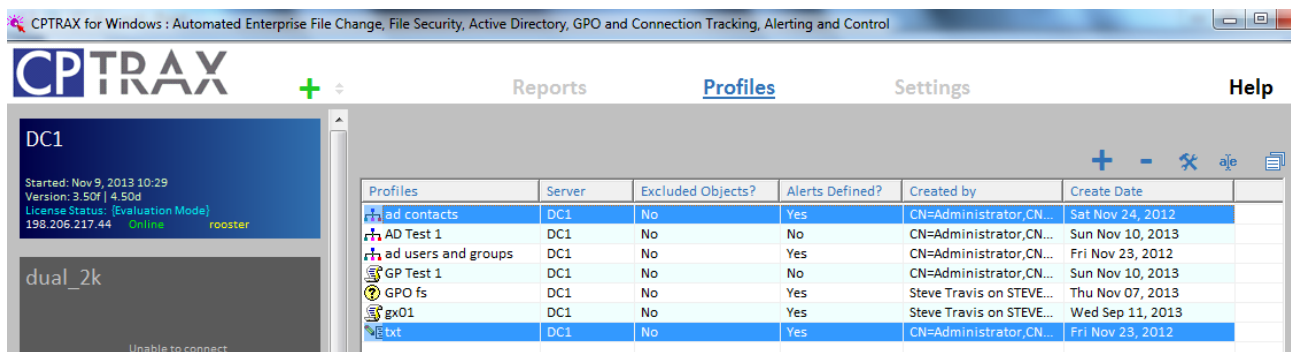


Figure 4-13

Click on the icon of one of the selected Profiles and while holding down the left mouse button position the cursor over the desired destination server and release.

Note that only the first selected Profile will be “shown” as it is being dragged – just the same, all selected Profiles are being dragged.

Once you release the left mouse button over the desired destination server the following window will appear:

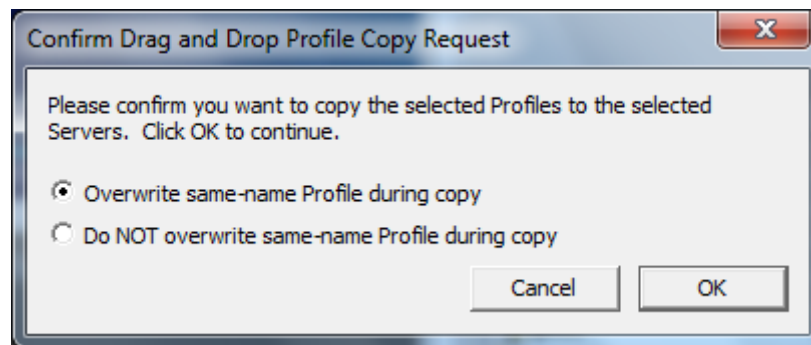


Figure 4-14

Select your response and click OK to continue or Cancel to abort.

If you select OK a results window will appear that details how the copy request is proceeding. Be sure to click on the first column labeled “Step Count: Server” to sort the events in order of progression.

Chapter 5 – CPTRAX Custom Reports

Custom Reports Creation

This chapter will provide a review of custom reporting options of the CPTRAX Administration Console (cptrax_console.exe).

To begin, select the ‘Reports’ tab and click “Custom Reports” button:

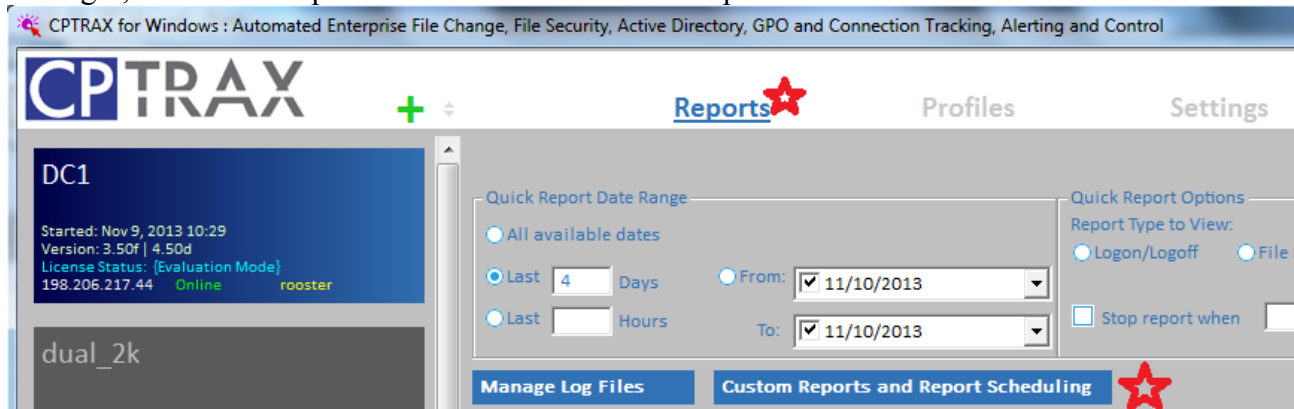


Figure 5-1

The following screen will appear:

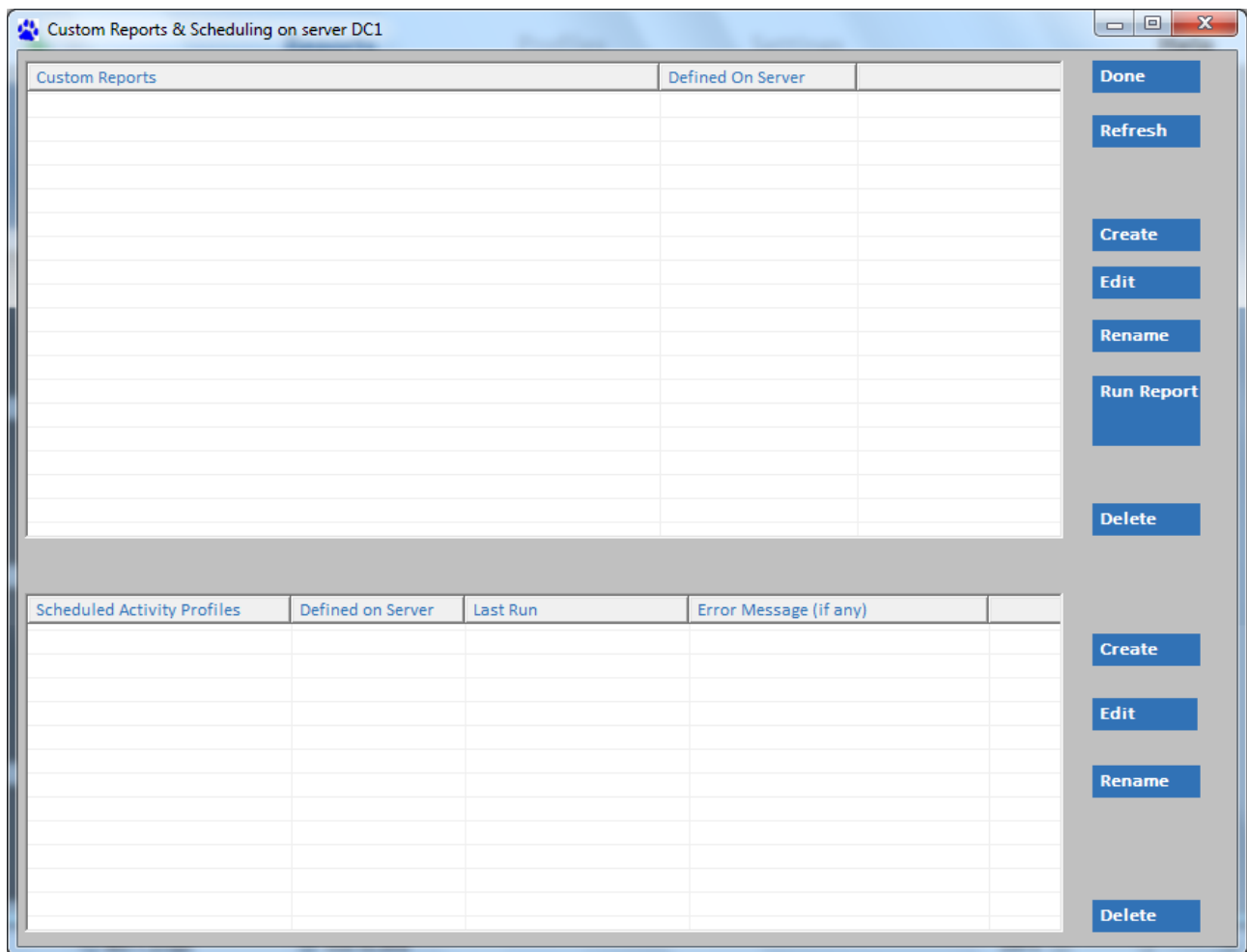


Figure 5-2

The list of Custom Reports will initially be empty.

Custom Reports are stored at each server hosting the CPTRAX Server Agent in the Registry key:

HKEY_LOCAL_MACHINE\Software\Visual Click Software, Inc.\CPTRAX\Reports

Actions are as follows:

- [Create](#)
 - Will launch the CPTRAX Custom Reports Designer (CPTWDES.EXE) for the selected server.
- [Edit](#)
 - Will launch the CPTRAX Custom Reports Designer (CPTWDES.EXE) for the selected Custom Report. If multiple custom reports are selected only the first one will be presented for editing.
- Refresh
 - Will refresh display of available Custom Report definitions.
- Rename
 - Will present a window to rename the selected custom report.
- [Run Report](#)

- Will immediately run the selected Custom Report. If multiple custom reports are selected only the first one will be run.
- Delete
 - Will present a confirming window. Once deleted, if the Custom Report was included in any [Scheduled Activities](#) its entry will be automatically removed.

Creating a new Custom Report

To begin, click the “Create” button and you will be presented with the following:

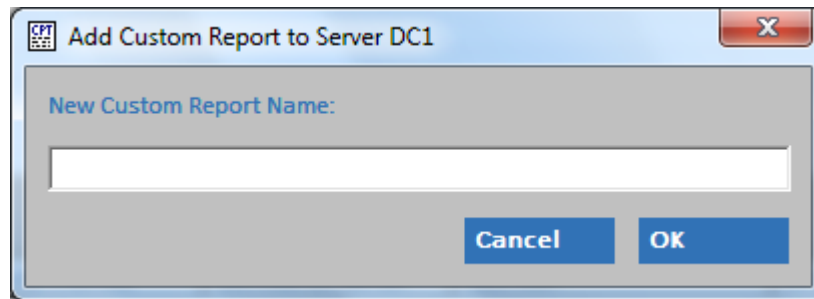


Figure 5-3

Enter the new Custom Report name – it can be up to 250 characters long.

After you click OK the CPTRAX Custom Reports Designer (CPTWDES.EXE) will be launched and the following prompt will be presented:

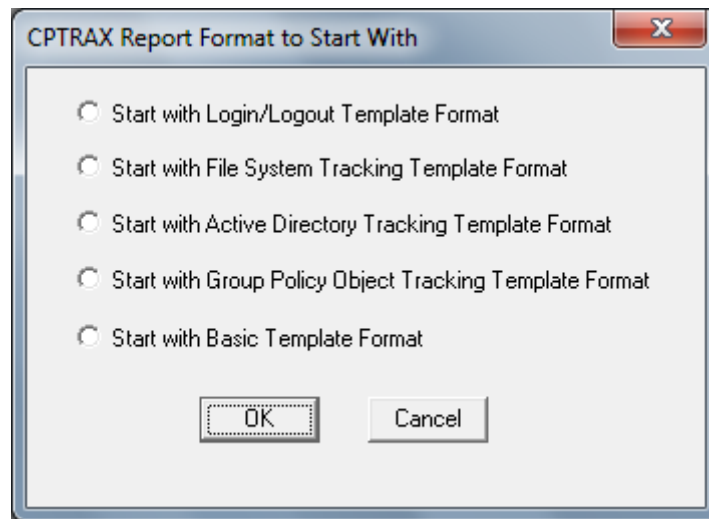


Figure 5-4

For this example, select “Start with File System Tracking Template Format” and click OK and the following will be presented:

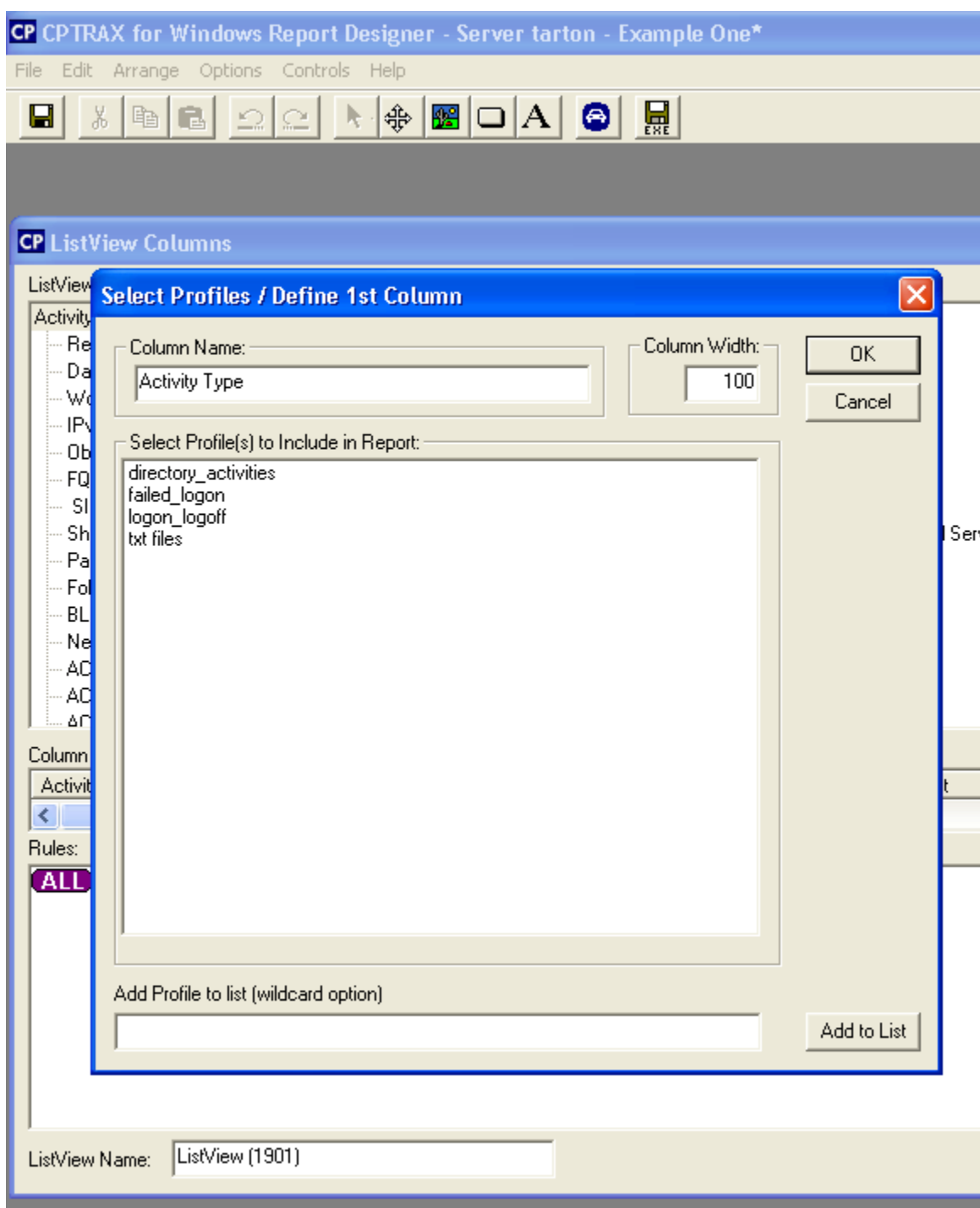


Figure 5-5

If you are familiar with our [DSRAZOR®](#) or [DSMETER®](#) products you will recognize the Custom Report Designer as it is largely based on those products' designer interfaces.

In Figure 5-5 the “Select Profiles / Define 1st Column” prompts you to select the Profile(s) to include in this Custom Report. You can change the selection at any time.

The “Column Name” field is predefined as “Activity Type” and can be changed. Likewise, the “Column Width” field, predefined as 100 (pixels) can be directly entered or, later, [can be sized](#) without knowing the appropriate number.

At the bottom of the screen is the “Add Profile to list (wildcard option)”. Use this prompt if you need to report from a Profile that has been deleted or is not otherwise present on the selected Server.

Note regarding the wildcard option

CPTRAX Profile activity log files outlive the Profile. That is, when (and if) you [delete a Profile](#) its log files are *not removed*. The **wildcard option** gives you the ability to report from Profiles that are no longer present on the server, have been [renamed](#) or for Profile activity log files received from other servers. Remember that [Department Host](#) servers can receive log files from other servers that have different Profiles defined.

Example wildcard names includes:

Actions*

log

??gather*

In the screenshot below we entered the wildcard name *log*:

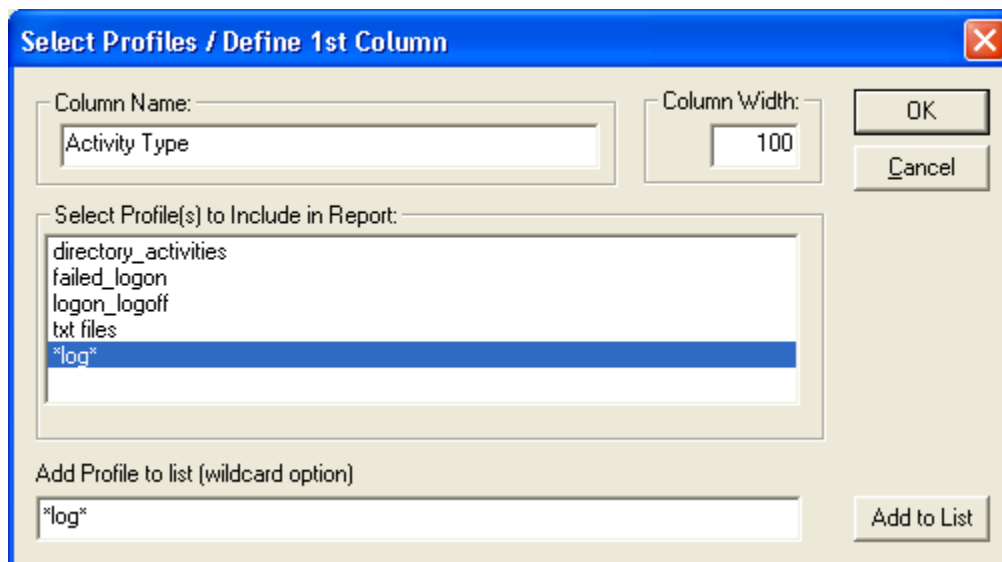


Figure 5-6 (screen reduced in height for illustration here)

The wildcard names entered (by clicking on “Add to List” button) will appear in the list of available Profiles to include in the report. The wildcard names you entered will only be present at the time you enter them. Once the OK or Cancel button is clicked, any wildcard names entered that are *not highlighted* will need to be reentered.

When selecting Profiles to include it is okay to select Profiles that contain different record types. For instance, you can combine records from Logon+Logoff Profiles with those from File System Activity Profiles. For any columns where data is not available, a blank or phrase “not available” will be presented. For instance, there is no “filename” in a Logon record and there is no “Logon Failure Type” for a File System Activity record.

Continuing from Figure 5-6, when you click OK or Cancel you will be presented with the following screen:

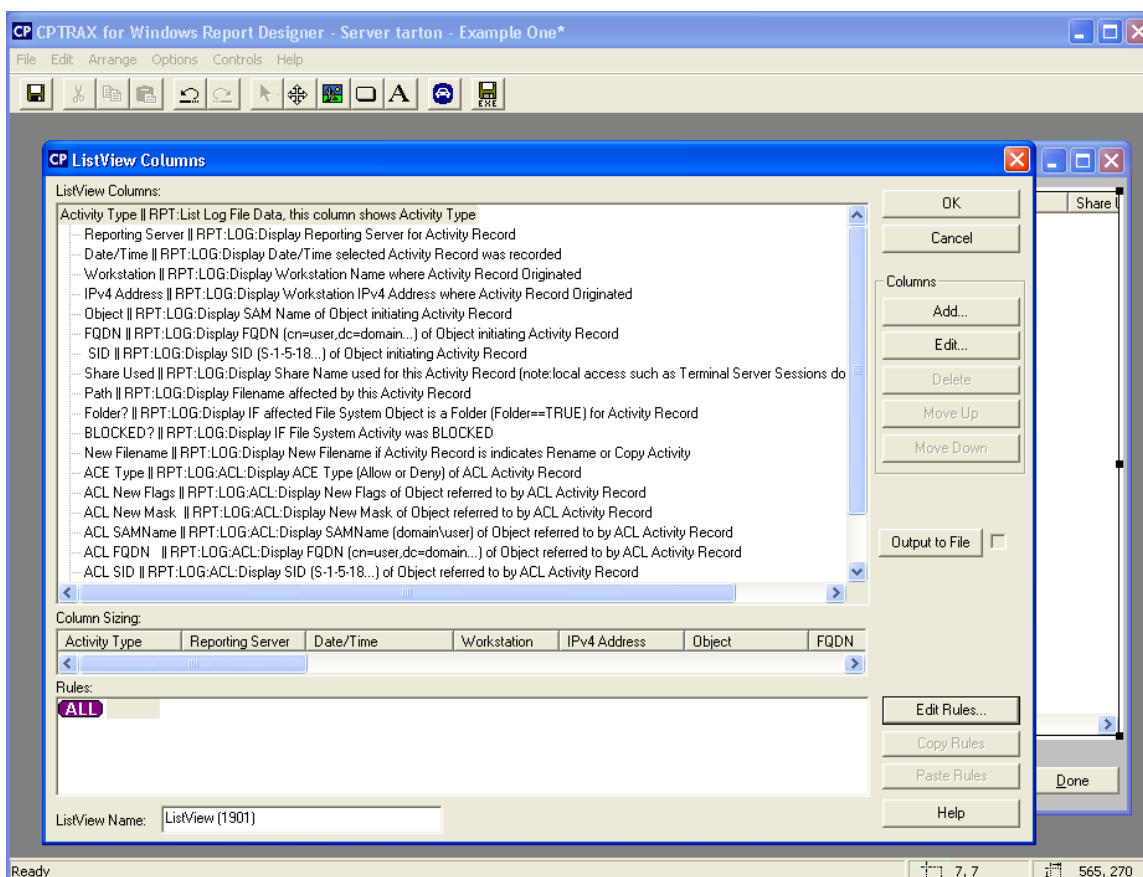


Figure 5-7

This screen has two main components; the first is the toolbar (Figure 5-8), the second is the report design (Figure 5-9).

Custom Report Toolbar

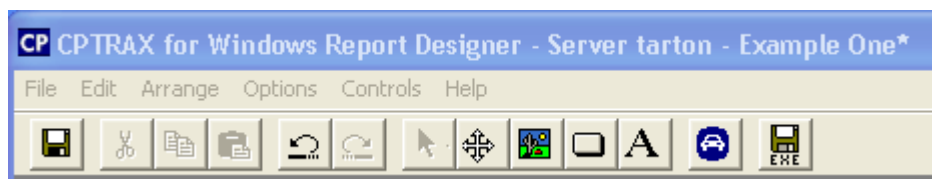


Figure 5-8

The toolbar (above) presents several familiar functions and some new ones.

Starting at the right, the button that depicts a floppy disk and the letters “EXE” will save the Custom Report currently being edited as a stand-alone executable file (EXE). When a Custom Report is saved as an EXE you can run it directly from your desktop or from a scheduler service such as available via Windows “AT” command (<http://support.microsoft.com/kb/313565>).

The next button to the left depicts an automobile image in a blue surround. This *test drive* button, when clicked, will immediately run the Custom Report currently being edited.

The next three buttons, when clicked, will enable you to drop a control on the face of the Custom Report. The *A* is for a text item, the *button* is a button and the *image* is for a bitmap. There are very few functions available for these toolbar buttons and it is possible to create a Custom Report and never use them.

The other toolbar buttons provide functions similar to many Windows products.

The “save” button works a little differently as the Custom Report is not saved to a file but, rather is saved directly to the Registry of the server selected (server name is noted in the caption bar, in this case the name is “tarton”). If you use “Save As” you can save the Custom Report to a new name on the same server.

If the server is not available or your logon account on that server does not have sufficient permissions to modify that server’s Registry key:

```
HKEY_LOCAL_MACHINE\Software\Visual Click Software, Inc.\CPTRAX\Reports
```

then the Custom Report will be saved to the LOCAL_MACHINE (your workstation) in the same Registry key. This is intentional to ensure your Custom Report is saved. If the Custom Report is saved to your workstation you can retrieve it in the CPTRAX Administration Console. More on this in the [LOCAL_MACHINE section](#).

Custom Report – Report Design

The Custom Report design is presented in a listview control – with a main column, “Activity Type”, and any columns you require. When first creating a new Custom Report the option to select the Report Template ([Figure 5-7](#)) will determine the columns that are initially presented. Except for the first column, all columns can be modified, added and deleted and the order changed to suite your purposes. The first column, the “Activity Type” represents a record “row” from an activity log file. Every Custom Report must have at least one column, the “Activity Type”. The label for the column can be changed to whatever is required.

The following screenshot shows what you will see when selecting the “File System Tracking” Report Template:

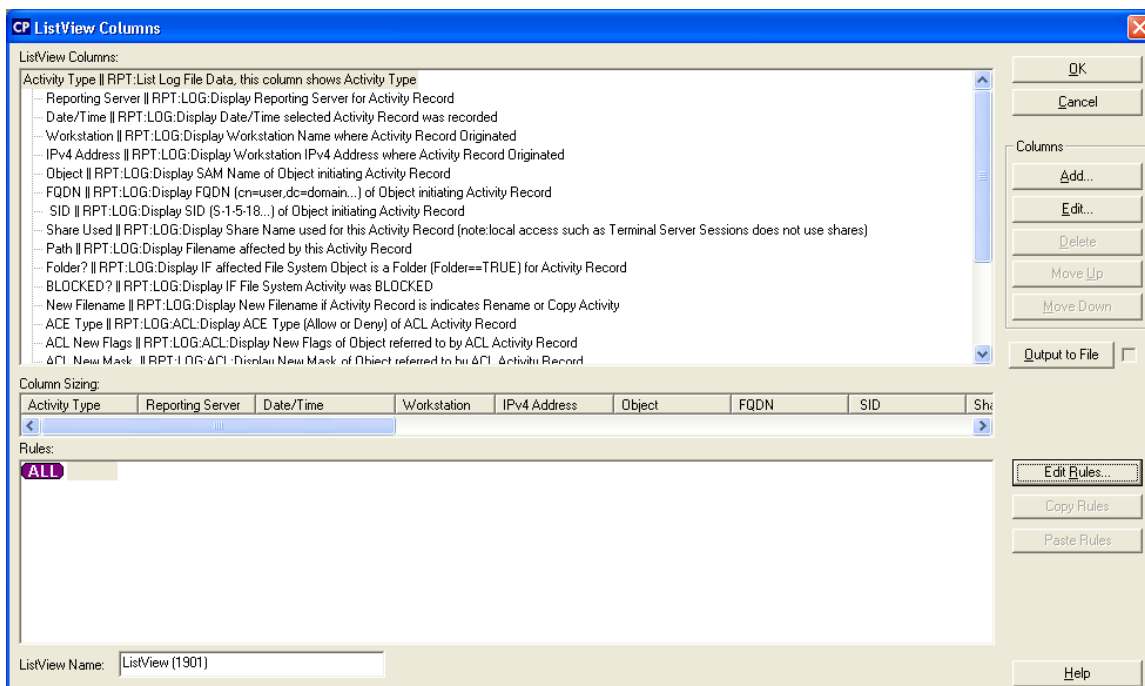


Figure 5-9

What you are viewing in Figure 5-10 is not an actual report but the layout of the report you want.

If you click OK you will be returned to a screen similar to:

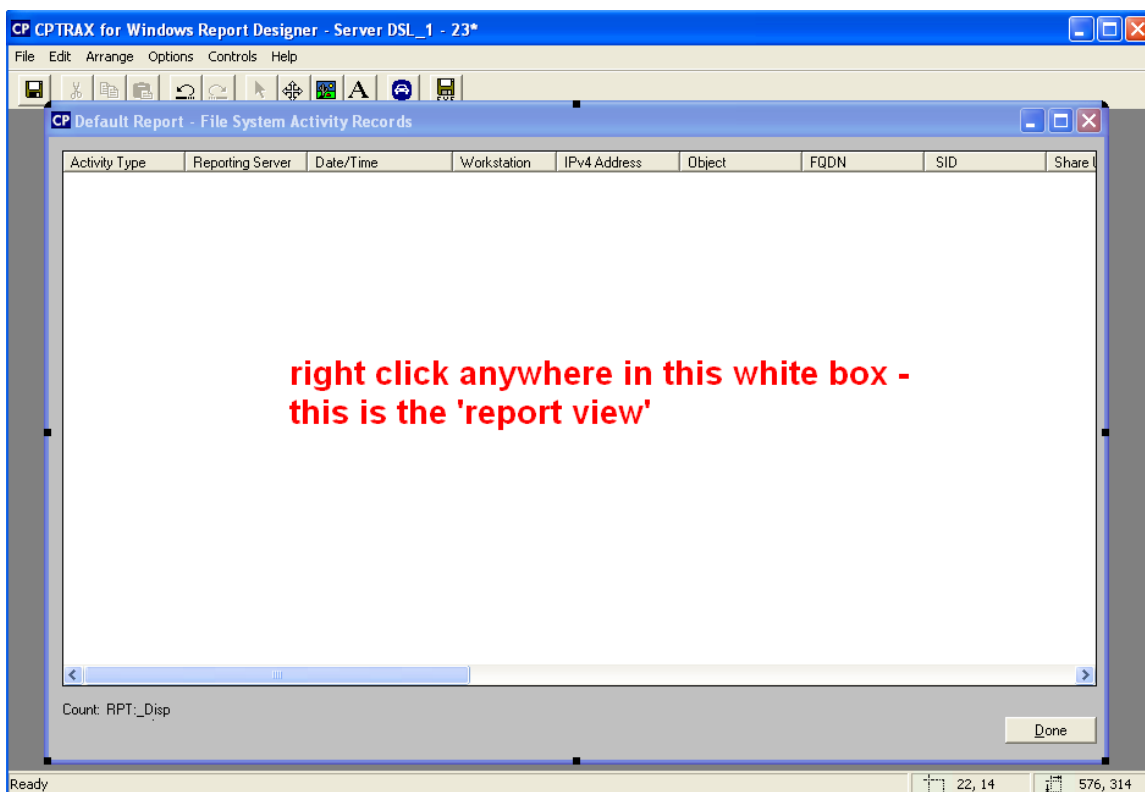


Figure 5-10

From this screen you can ‘re-enter’ editing the report by positioning the mouse cursor over the report view and clicking the *right-mouse* button.

Adding Comments

As shown in Figure 5-10, if you right click on the title bar (window caption) for the report view:



Figure 5-11

You will be presented with the following:

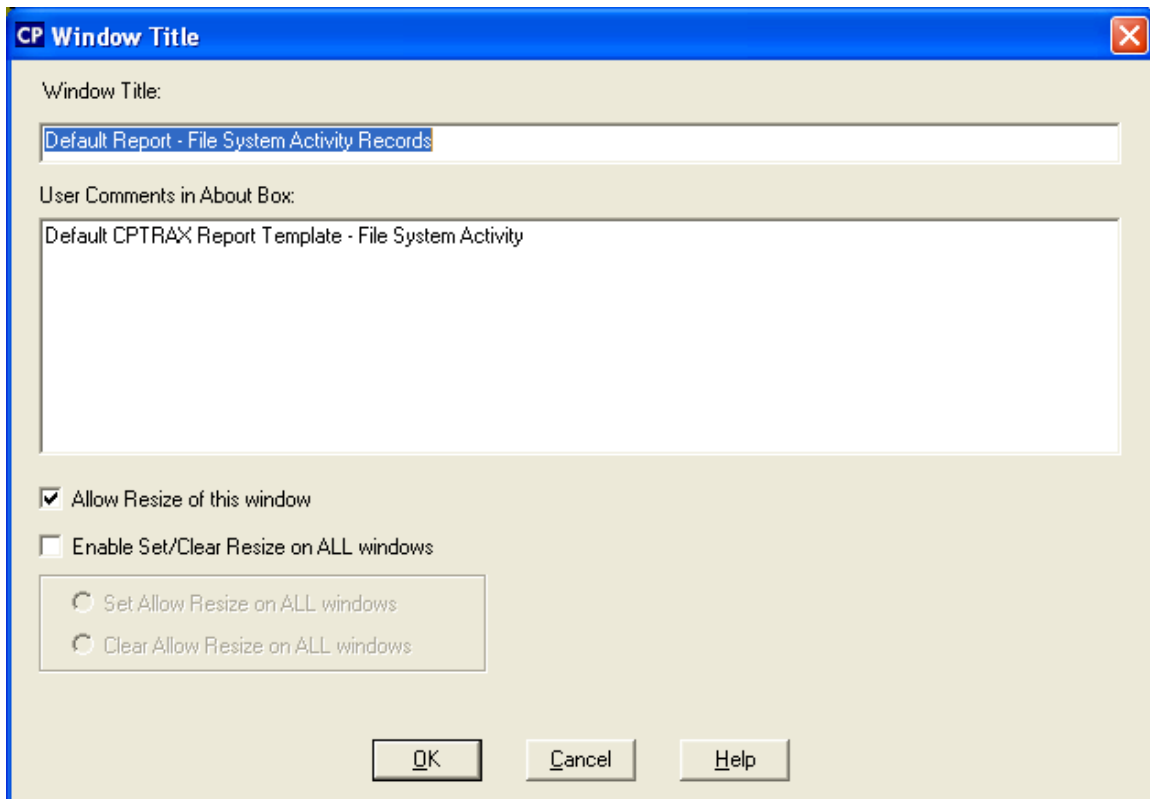


Figure 5-12

On this screen you can change the title of the Custom Report window and add comments as desired. There are also two checkboxes present:

- Allow Resize of this window
 - If checked, will allow report window to be resized at runtime
- Enable Set/Clear Resize on ALL windows
 - At present, reports are only contained on a single window, as such, this checkbox does not provide any noticeable functionality

Sizing Columns

If not already viewing the screen similar to [Figure 5-9](#), right click on the report view as shown in [Figure 5-10](#) to be returned to editing the Custom Report.

In the middle of the screen you will find the “Column Sizing” area:

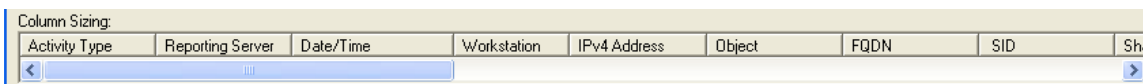


Figure 5-13

This area allows you to resize columns by positioning the mouse cursor over the “divider” between each column and dragging it to the left or right. Columns can also be resized when editing columns (discussed in the next section).

Note: You can resize the columns while viewing report data, that is, when you run a Custom Report (or [Quick Report](#)).

Editing Columns

The area above the column sizing area is a listing of all columns the report contains. For each line shown there are two text areas:

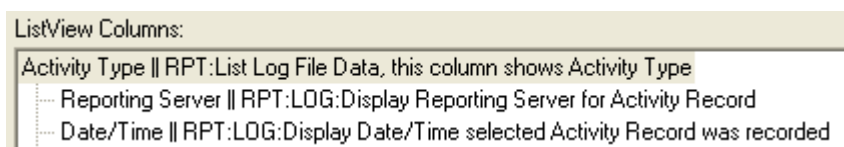


Figure 5-14

The first text area is to the left of the || divider. This is the text that will be shown as the column name when running the Custom Report. In Figure 5-9 the phrases “Activity Type”, “Reporting Server” and “Date/Time” are all column names. The text to the right of the || divider is the name of the actual Custom Report service that will be used to determine what data to present. For instance, the text “RPT:LOG:Display Date/Time selected Activity Record was recorded” will not shown when running the report, it is the service that will be used to present the data for that column.

To edit a column, use the mouse cursor to select it and then click on the “Edit...” button at the right side of the screen.

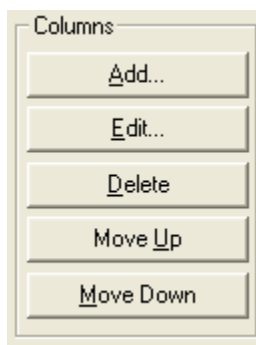


Figure 5-15

If you select the line containing the text “RPT:LOG:Display Date/Time selected Activity Record was recorded” and click “Edit...” the following will be presented:

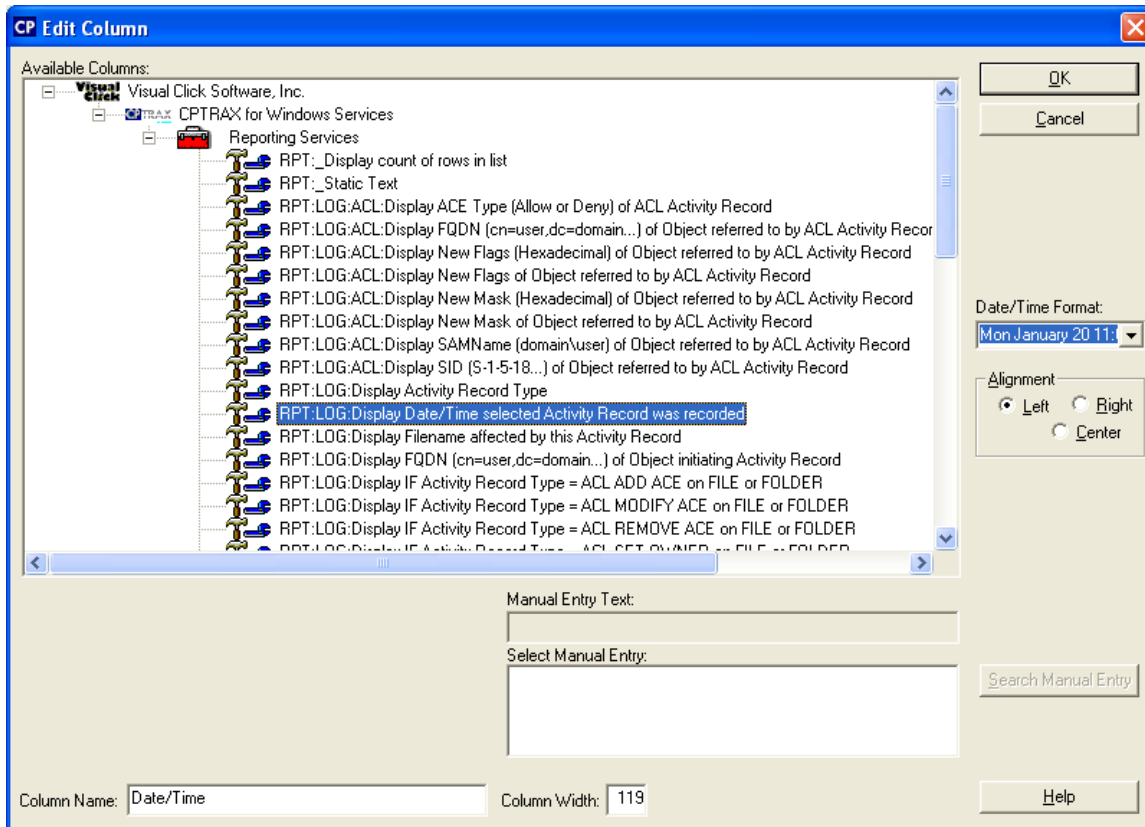


Figure 5-16

What Figure 5-16 shows are the services available and the currently selected service is highlighted.

Because the service selected displays the date/time there is an additional option at the right side, “Date/Time Format”. This is a drop down list that allows you to select the format for the values shown when running the report. Figure 5-21 shows all available date and time formats.

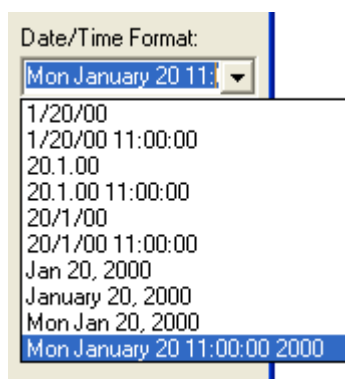


Figure 5-21

At the lower left corner in Figure 5-16 is the “Column Name” field. The value here will become the column name in the Custom Report.

Immediately to the right of the “Column Name” field is the “Column Width” field. This field contains a number that represents how wide the column is in pixels. If you enter a new value here, once you click OK and are returned to the previous screen you will see the new column width in the “Column Sizing” area. To resize a column you can enter the number of pixels as explained here or use the mouse cursor to dynamically drag the column width in the “Column Sizing” area as shown in [Figure 5-9](#).

Also shown in Figure 5-16 are two other fields, “Manual Entry Text” and “Select Manual Entry”. Both of these fields are used when [editing Rules](#) and are disabled when editing and adding columns.

Adding and Changing Columns

With the Custom Report Designer you can Add, Delete, Modify and rearrange columns. You can use the “Add...”, “Delete”, “Move Up” and “Move Down” buttons as shown previously in Figure 5-15, but repeated here as Figure 5-22.

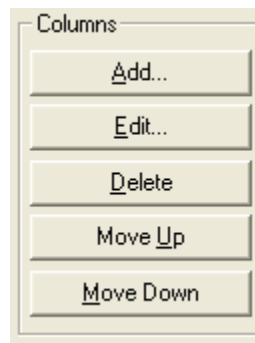


Figure 5-22

When you click the “Add...” button you will be presented with a screen similar to the following:

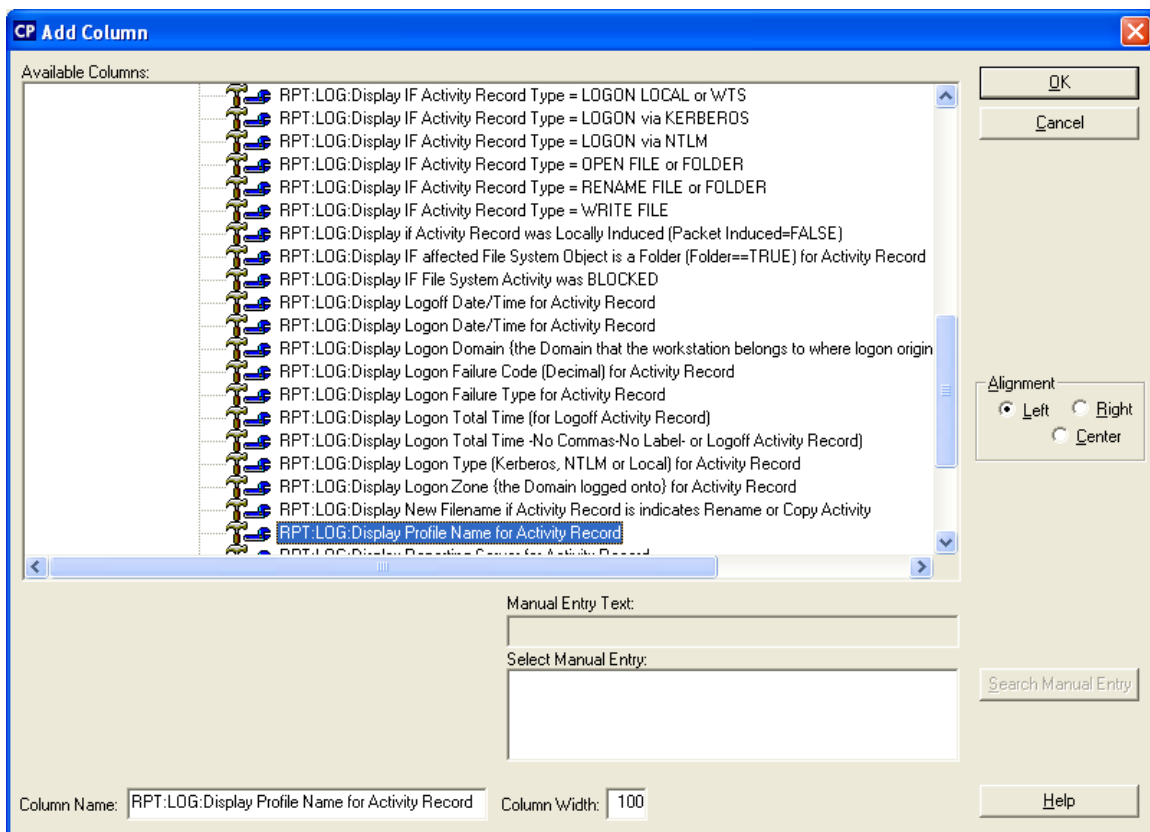


Figure 5-23

A default selection will be highlighted. Each selection represents data available to add to the Custom Report. These selections are sometimes referred to as “services”.

Select the data you want to add to the report. Each selection is named to indicate what you will receive. Refer to [Appendix B](#) for a complete listing of all available data columns/services. Edit the “Column Name” to be as required (a default name is provided that is the description of the data that will be provided). When you edit the “Column Name” for one of the selections, the new value entered will be remembered when editing or adding columns in the current or other Custom Reports.

Expediting Custom Reports by Filtering Report Data with Rules

When creating and modifying Custom Reports you can set filters to restrict the data returned.

There are 3 different rule filters that will *limit the number of log files* that will be read-through to produce the report output. By using these three rule filters you can speed up report performance, that is, the amount of time required to generate the report.

These 3 rule filters that can expedite reporting performance are:

- Profile(s) to include
- Server(s) to include (where activity was gathered)
- Date/Time of activity (when activity occurred)

The first “rule filter” was made when you selected the [Profile\(s\) to include in the report](#). And can be re-accessed by editing the “Activity Type” column as shown in [Figure 5-6](#).

Just prior to [clicking Create](#) you selected the server where the Custom Report will be stored. This is different than choosing which servers to include the report. The difference is that activity log files located on a specific server may have originated from multiple servers. This is presumed to be true for [Department Host servers](#).

It is simple to establish a rule to limit reporting to be from specific servers. To begin, from the screen shown in [Figure 5-16](#) select the “Activity Type” and then click the “Edit Rules...” button:

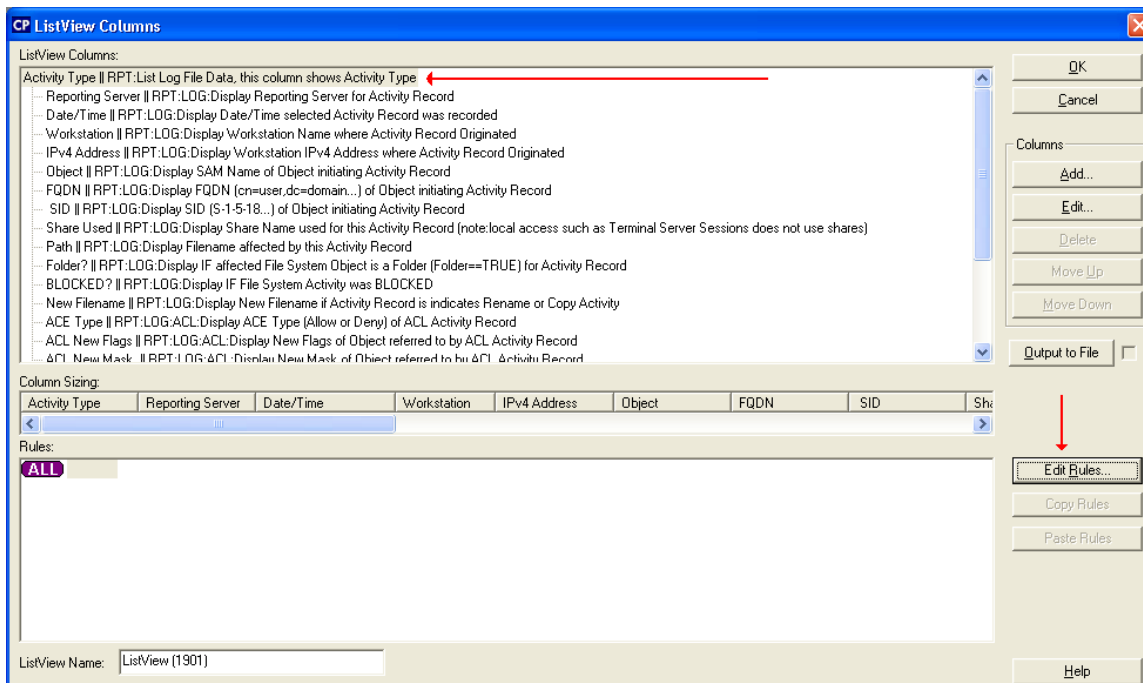


Figure 5-24

After clicking the “Edit Rules...” button the following screen will appear:

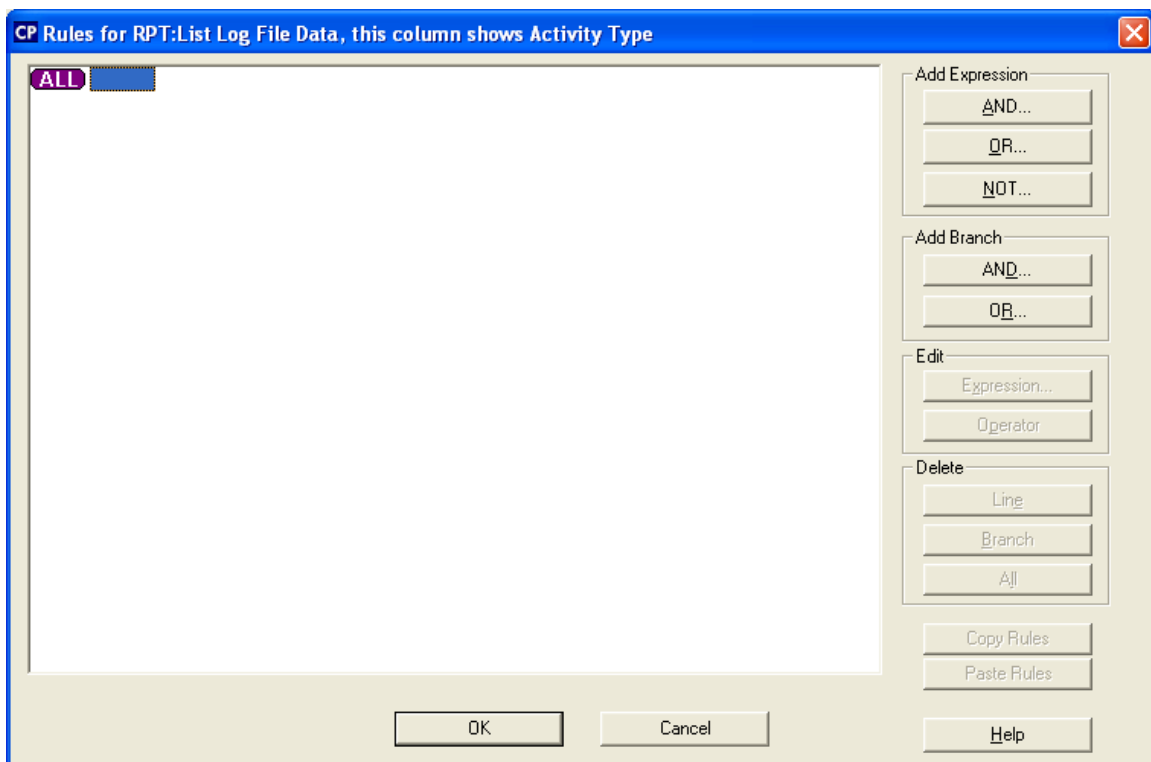


Figure 5-25

Notice at the top of the screen the caption indicates:

Rules for RPT:List Log File Data, this column shows Activity Type

This screen allows you to construct simple to complex rules to filter the report data to be exactly as required.

Reporting from selected Servers

To restrict the report to be from selected servers, click the “AND...” button in the “Add Expression’ section:

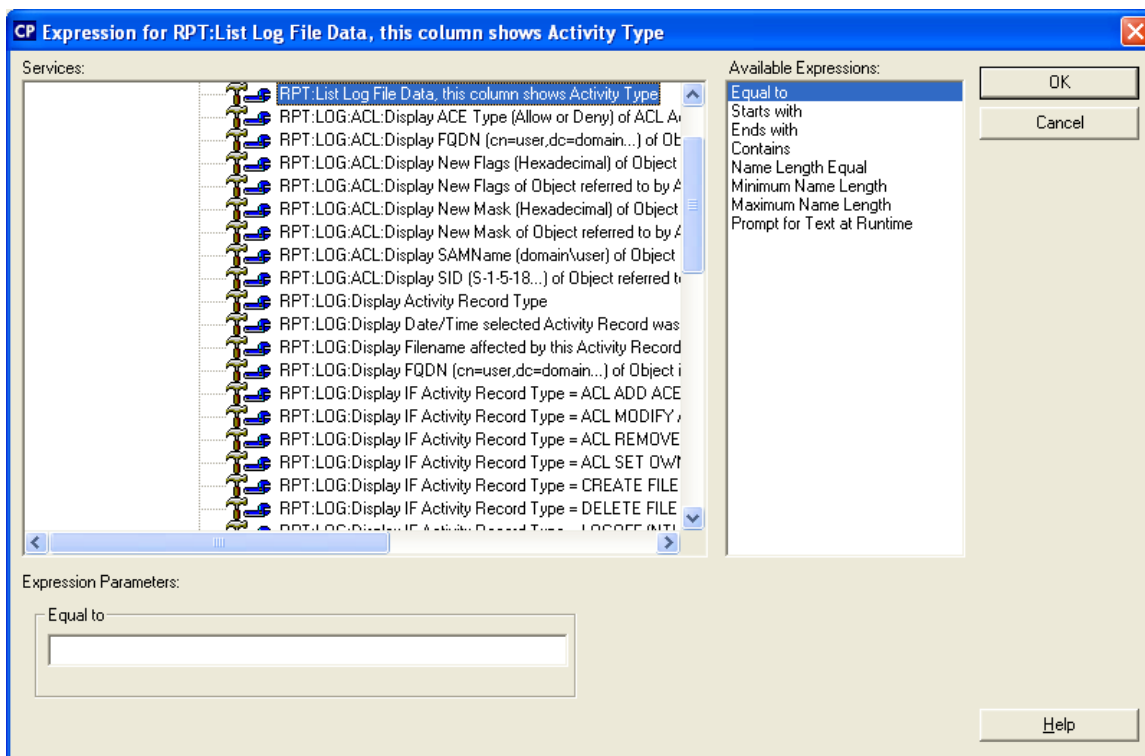


Figure 5-26

The initial highlighted selection will always equal to the report data column you are editing. To restrict by the originating or “reporting” server select the following service from the list:

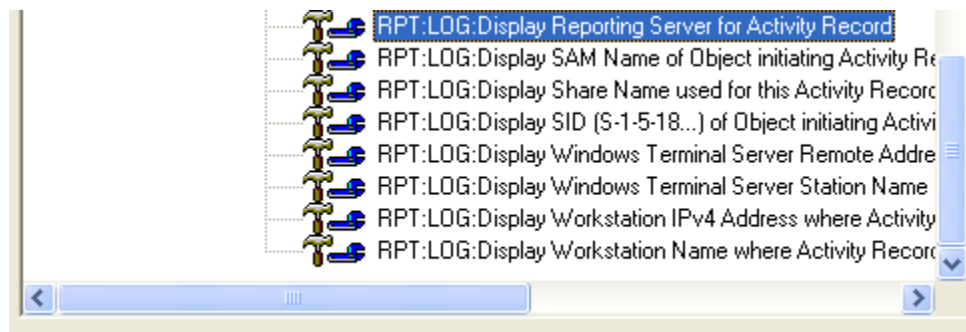


Figure 5-27

At the upper right of this screen there are several options:

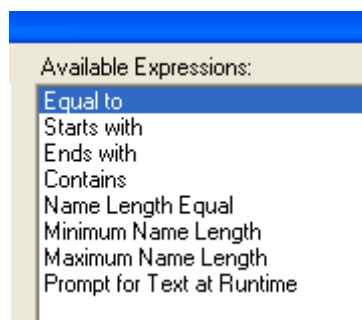


Figure 5-28

Select the appropriate expression, use “Equal to” if specifying the exact server name. Enter the NetBIOS-based server name in the “Expression Parameters” field. Please note that the server name entered **must be** equal to the NetBIOS name (same as the SAM name) of the gathering server, the IP address will not be interpreted.

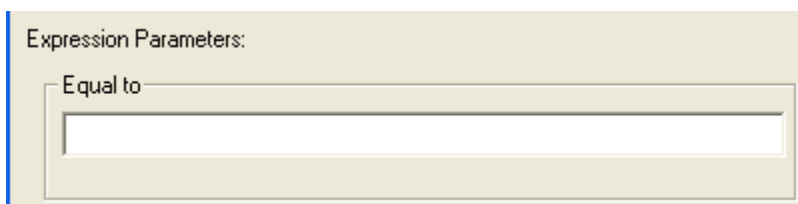


Figure 5-29

Click OK after you have entered the server name and you will be returned to this screen:

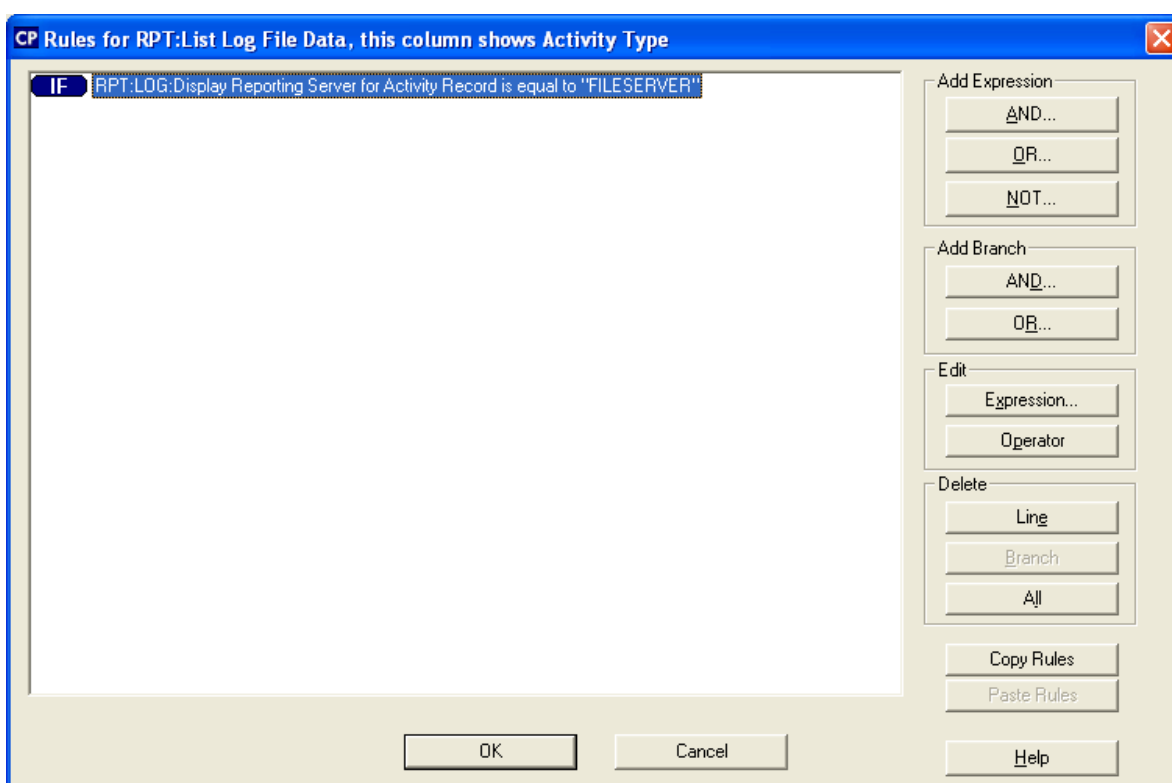


Figure 5-30

In the example above we used the server name “FILESERVER”.

To add a second server, click the “OR...” button and enter the “next” server to include and click OK, the result will appear similar to:

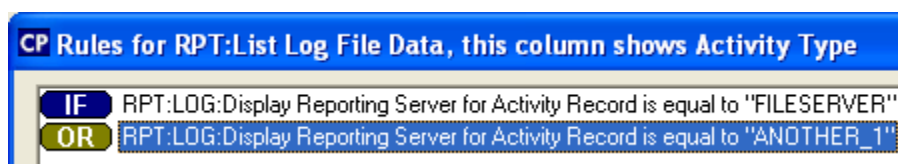


Figure 5-31

Be sure to use the “OR” expression, if you use the “AND” expression as shown here:

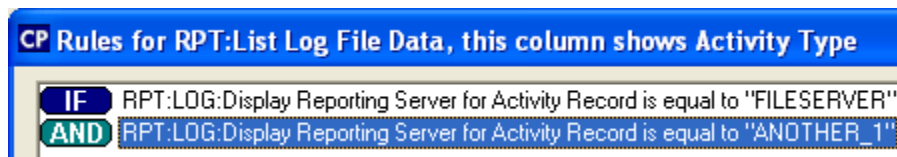


Figure 5-32

Then your report will be empty as it is not possible for a single record to have been gathered on two separate servers. This is what the “AND” operator indicates.

If you did use the AND operator you can easily change it by clicking on the “Edit | Operator” button:

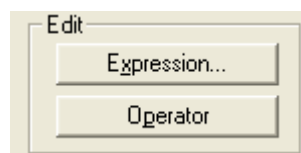


Figure 5-33

Alternatively you can use the NOT operator to report from all but the specified servers:

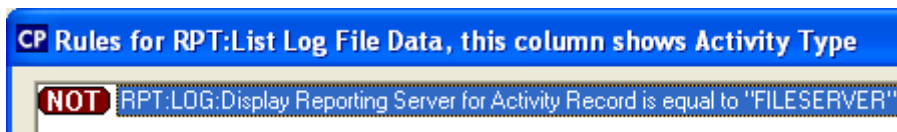


Figure 5-34

Reporting for selected Dates

To restrict the report to be for selected Date/Time periods, click the “AND...” button ([Figure 5-30](#)) in the “Add Expression” section:

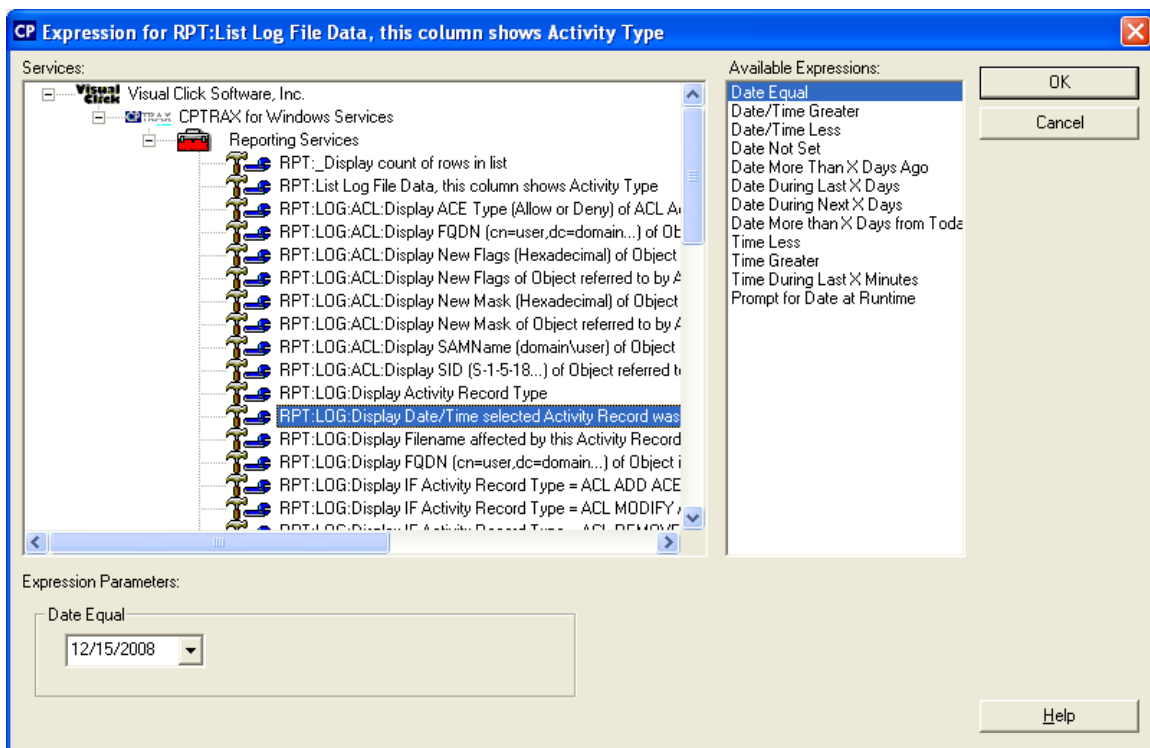


Figure 5-35

And select the “RPT:LOG:Display Date/Time selected Activity Record was recorded” service (as shown in Figure 5-34).

Notice the “Available Expressions” for the Date/Time service:

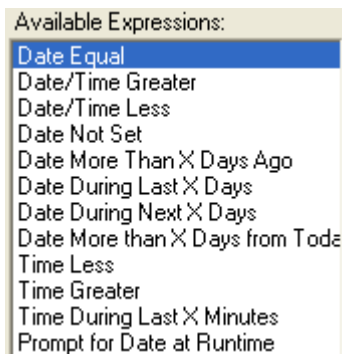


Figure 5-36

In the “Expression Parameters” field you can specify the date:

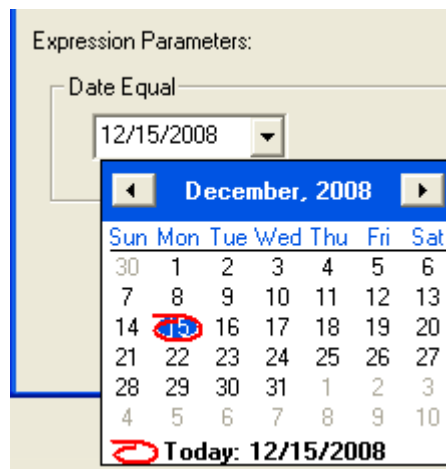


Figure 5-37

If you select the “Expression” ***Date During Last X Days*** you will be presented with an edit field to enter a number:

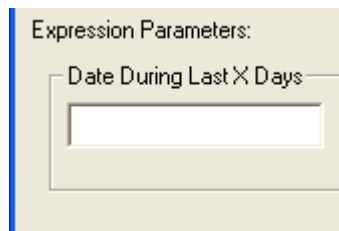


Figure 5-39

If you would prefer the Date be selected dynamically when interactively running the report, select the “Expression” ***Prompt for Date at Runtime***:

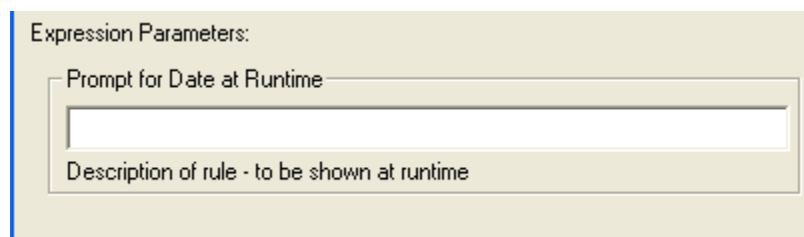


Figure 5-40

Enter a description to be shown to the report user in the edit field presented.

When actually running the report the result will appear similar to:

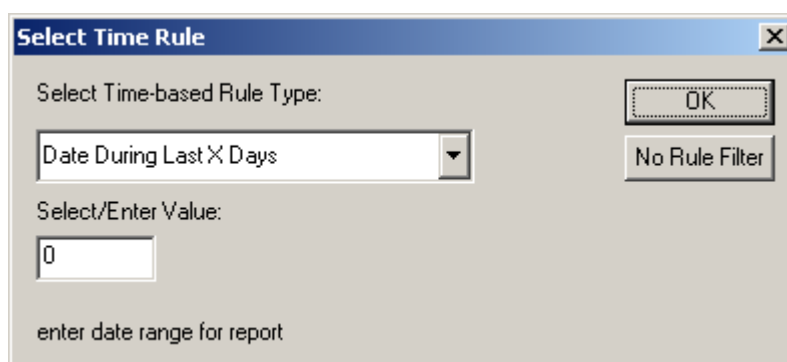


Figure 5-41

In Figure 5-40 the “description” entered was “enter date range for report”.

The “Expression” ***Prompt for Date at Runtime*** is available for all rules except the Profile name(s) to include.

Special note about midnight activity and Date/Time Rules

Because CPTRAX for Windows saves activity log files in individual files for each day there can be some overlap if recorded activity occurs around midnight (local time at the server). To ensure your reports include all activity for a specific date that includes activity generated within 30 minutes before or after midnight (local time at the server where recorded) include the “day before” or “day after” in the date range.

For instance, if you want to all activity for December 15, the date range for the report should be from December 14 until December 16.

This section has reviewed the three rule filters (Profile(s) to include, Server(s) to include and Date/Time Range to include) to expedite Custom Report performance by limiting the number of activity log files that will be read.

Customizing Custom Report output using Boolean Rule Trees

This section reviews variations when adding Boolean rules to your Custom Report.

Beyond the [3 rule filters that can expedite report performance](#) there are essentially an unlimited number of rules you can assemble to craft the specific report you require.

The following three figures show example Boolean rule trees you can construct to retrieve just the data important to you:

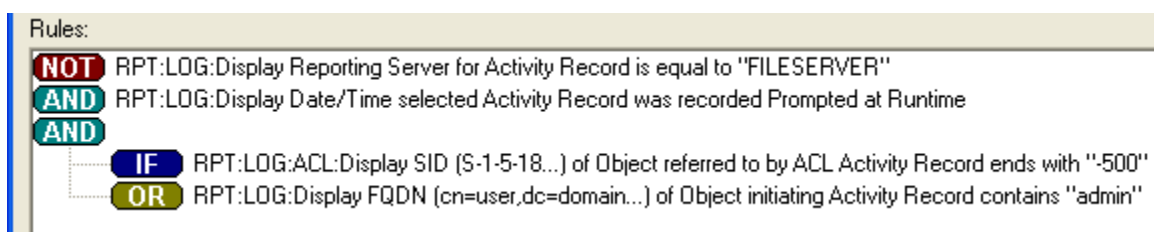


Figure 5-42

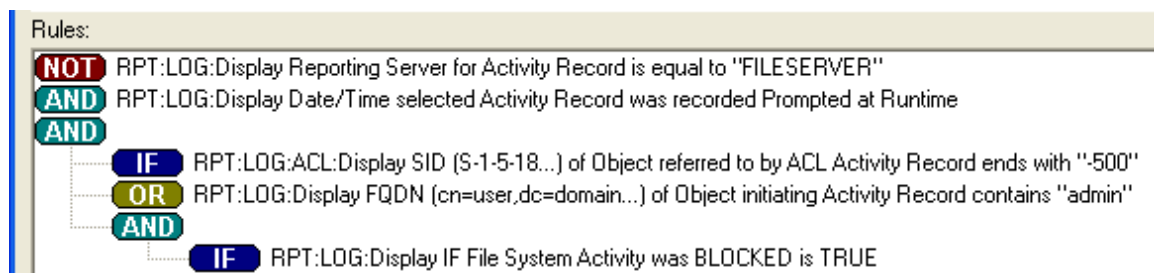


Figure 5-43

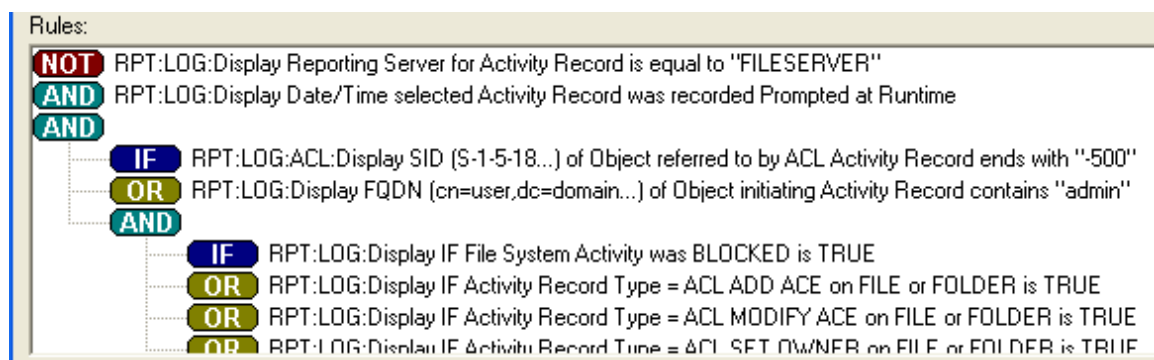


Figure 5-44

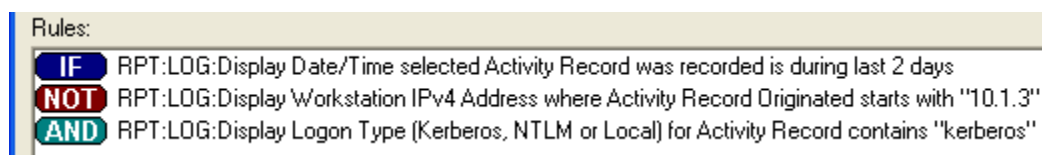


Figure 5-45

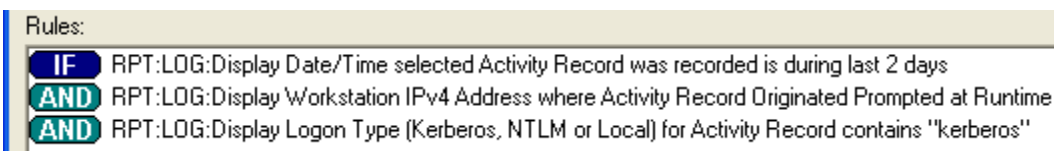


Figure 5-46

Reporting directly to File versus Screen

There are two basic ways CPTRAX Custom Reports can be run. Either interactively where the results are presented directly on screen:

Activity Type	Reporting Server	Date/Time	Workstation	IPv4 Address	Object	FQDN	SID	Share Used	Path
Open Folder	DUAL-2K	Tue Dec 02 22:09:45 2008	XPPOWER	198.206.217.203	DUAL_2K\Admi...	CN=Administrato...	S-1-5-21-164552...	DX	D:\Program Files...
Open Folder	DUAL-2K	Tue Dec 02 22:09:45 2008	XPPOWER	198.206.217.203	DUAL_2K\Admi...	CN=Administrato...	S-1-5-21-164552...	DX	D:\Program Files...
Open Folder	DUAL-2K	Tue Dec 02 22:10:00 2008	XPPOWER	198.206.217.203	DUAL_2K\Admi...	CN=Administrato...	S-1-5-21-164552...	DX	D:\Program Files...
Block Delete ...	DUAL-2K	Thu Dec 04 21:53:26 2008	XPPOWER	198.206.217.203	DUAL_2K\Admi...	CN=Administrato...	S-1-5-21-164552...	DX	D:\Program Files...
Block Delete ...	DUAL-2K	Thu Dec 04 21:53:26 2008	XPPOWER	198.206.217.203	DUAL_2K\Admi...	CN=Administrato...	S-1-5-21-164552...	DX	D:\Program Files...
Block Delete ...	DUAL-2K	Thu Dec 04 21:53:26 2008	XPPOWER	198.206.217.203	DUAL_2K\Admi...	CN=Administrato...	S-1-5-21-164552...	DX	D:\Program Files...
Block Delete ...	DUAL-2K	Thu Dec 04 21:53:27 2008	XPPOWER	198.206.217.203	DUAL_2K\Admi...	CN=Administrato...	S-1-5-21-164552...	DX	D:\Program Files...
Block Delete ...	DUAL-2K	Thu Dec 04 21:53:27 2008	XPPOWER	198.206.217.203	DUAL_2K\Admi...	CN=Administrato...	S-1-5-21-164552...	DX	D:\Program Files...
Block Delete ...	DUAL-2K	Thu Dec 04 21:53:27 2008	XPPOWER	198.206.217.203	DUAL_2K\Admi...	CN=Administrato...	S-1-5-21-164552...	DX	D:\Program Files...
Block Delete ...	DUAL-2K	Thu Dec 04 21:53:28 2008	XPPOWER	198.206.217.203	DUAL_2K\Admi...	CN=Administrato...	S-1-5-21-164552...	DX	D:\Program Files...
Block Delete ...	DUAL-2K	Thu Dec 04 21:53:28 2008	XPPOWER	198.206.217.203	DUAL_2K\Admi...	CN=Administrato...	S-1-5-21-164552...	DX	D:\Program Files...
Block Delete ...	DUAL-2K	Thu Dec 04 21:53:28 2008	XPPOWER	198.206.217.203	DUAL_2K\Admi...	CN=Administrato...	S-1-5-21-164552...	DX	D:\Program Files...

Count: 13

Done

Figure 5-47

Or CPTRAX Custom Reports can be run where the output is sent directly to a file.

Reasons why to define a Custom Report to be sent directly to a file rather than to the screen include:

- Results could exceed 50,000 lines
 - Windows® runs out of system resources when report output exceeds 50,000 lines
- Report will be used in a [Scheduled Activity](#) (at the server)
- Report will be saved as a stand-alone EXE file

To set a Custom Report to report directly to file, edit the Custom Report and on the screen shown in [Figure 5-9](#). Click on the “Output to File” button:

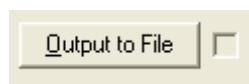


Figure 5-48

The “greyed out” checkbox next to the button indicates if the Output to File option has been engaged. After clicking this button, the following will be presented:

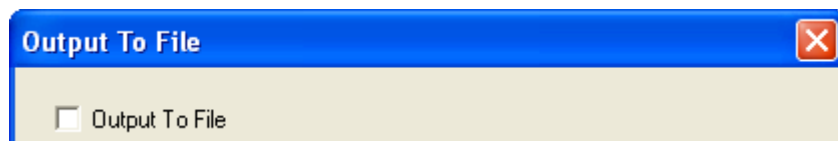


Figure 5-49

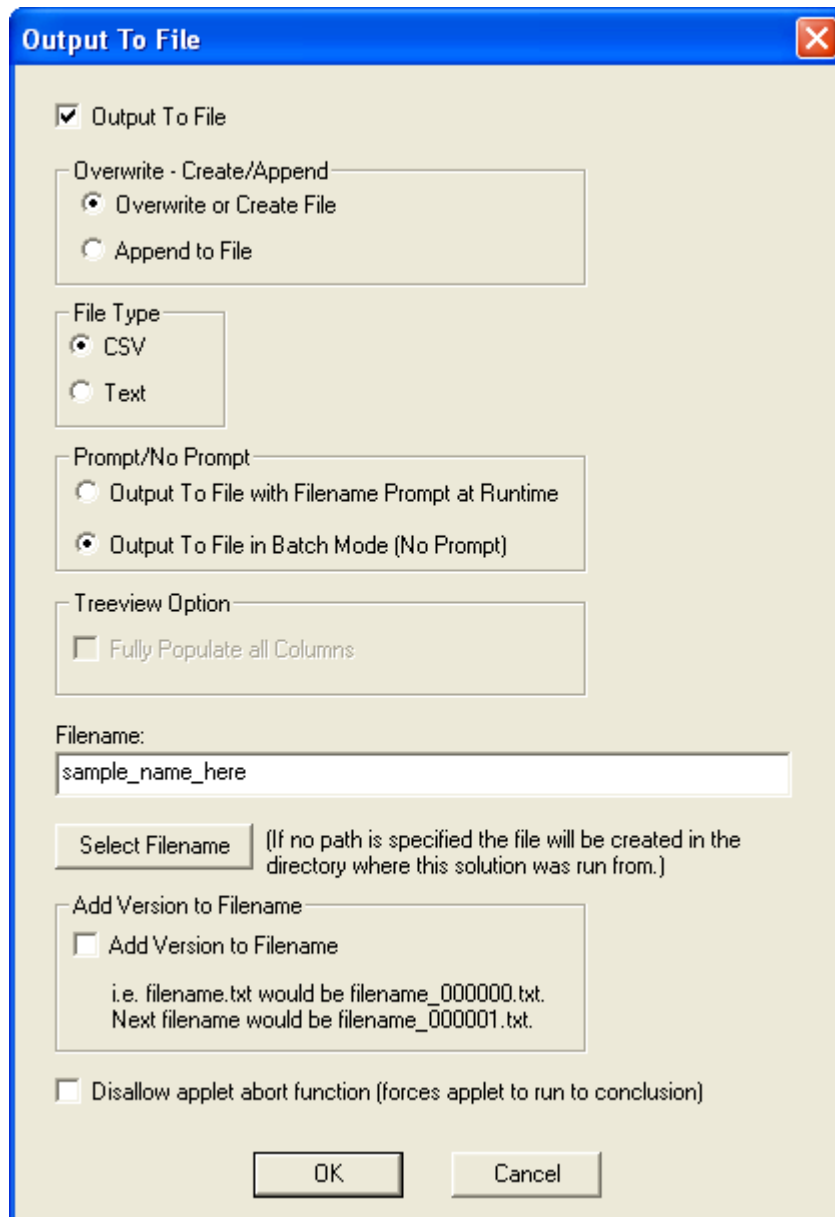


Figure 5-50

By setting these options the Custom Report will be configured to send its output directly to a file.

Viewing list of Custom Reports

To begin, click on the checkbox “Output To File”-to disable this option, uncheck it

Select Overwrite or Append

CSV=Comma Delimited Output, Text = as shown when running interactively

Use “No Prompt” for ‘silent’ running of report

Treeview Option is not available

Enter Filename and optionally the Path

Optional: Add version to filename

Block interactive aborting of report

To update the list of reports to show your new Custom Report, refer to [Figure 5-2](#) and click the “Refresh” button.

Any time you create a Custom Report you will need to click the “Refresh” button to refresh the list as the list is *not* automatically refreshed.

Editing an existing Custom Report

To edit an existing Custom Report, refer to [Figure 5-1](#) and [Figure 5-2](#) for how to navigate to the Custom Reports management screen. Next, click on the Custom Report to edit and click the “Edit” button. The Custom Report Designer is presented and you can edit the Custom Report.

Running a Custom Report

There are 4 methods to run a CPTRAX Custom Report:

- From the CPTRAX Administration Console
- From the Custom Report Designer (Test Drive Button)
- As a stand-alone executable (when saved as an EXE from the Designer)
- As a [scheduled activity on a specific server](#)

Custom Report Scheduling

Any Custom Report you create can be scheduled to be run automatically by the CPTRAX for Windows Server Agent. As with Custom Reports, Scheduled Activities are stored in the Registry of the server hosting the CPTRAX Server Agent in the following key:

```
HKEY_LOCAL_MACHINE\Software\Visual Click Software, Inc.\CPTRAX\Reports
```

Because this is the same Registry key that is used to store Custom Reports, any Scheduled Activity you create cannot use the same name as used by an exiting Custom Report on that server.

When running a scheduled activity, the CPTRAX Server Agent launches CPTWCCR.EXE (plus DSRR0007.DLL) from the \SystemRoot\System32\Drivers (or \SystemRoot\SysWow64\Drivers) folder.

The process to create a Scheduled Activity is straightforward and is explained in the following steps.

Start by running the CPTRAX for Windows Administration Console and refer to [Figure 5-1](#) and [Figure 5-2](#) for how to navigate to the Custom Reports management screen. Please note the “Scheduled Activity Profiles” list at the lower half of the following screen:

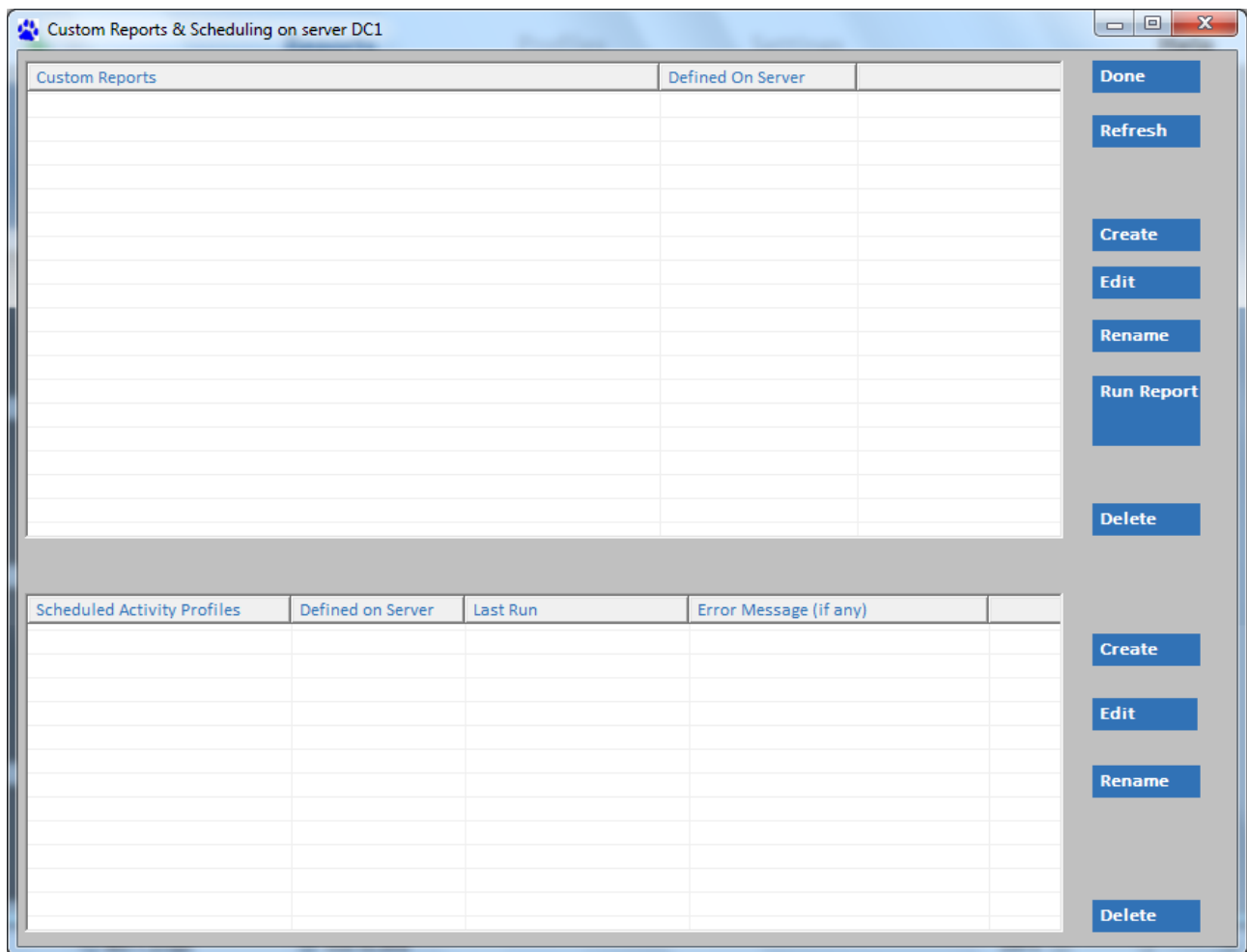


Figure 5-51

Creating a Scheduled Activity

To create a new Schedule Activity, click the “Create” button:

Figure 5-52

As shown in Figure 5-52, give the Scheduled Activity a name:

Figure 5-53

Note: The name used *cannot be* the same as a Custom Report defined on the same server.

Use the “Add New Scheduled Time” area to define times to start the selected activity.

Figure 5-54

The time of day to start is provided in 15-minute increments:

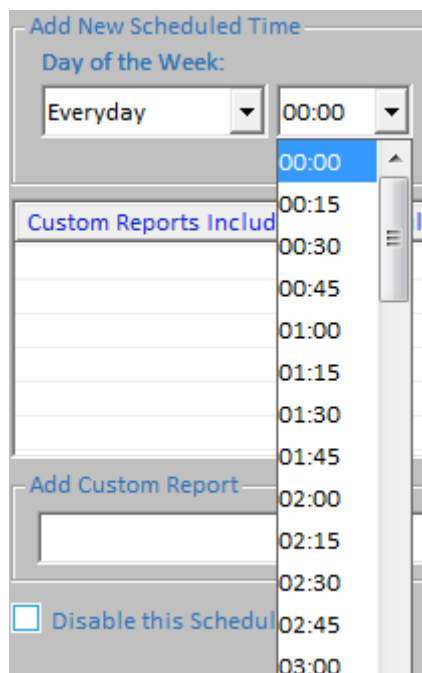


Figure 5-55

Click the “Add” button to enter your selection:

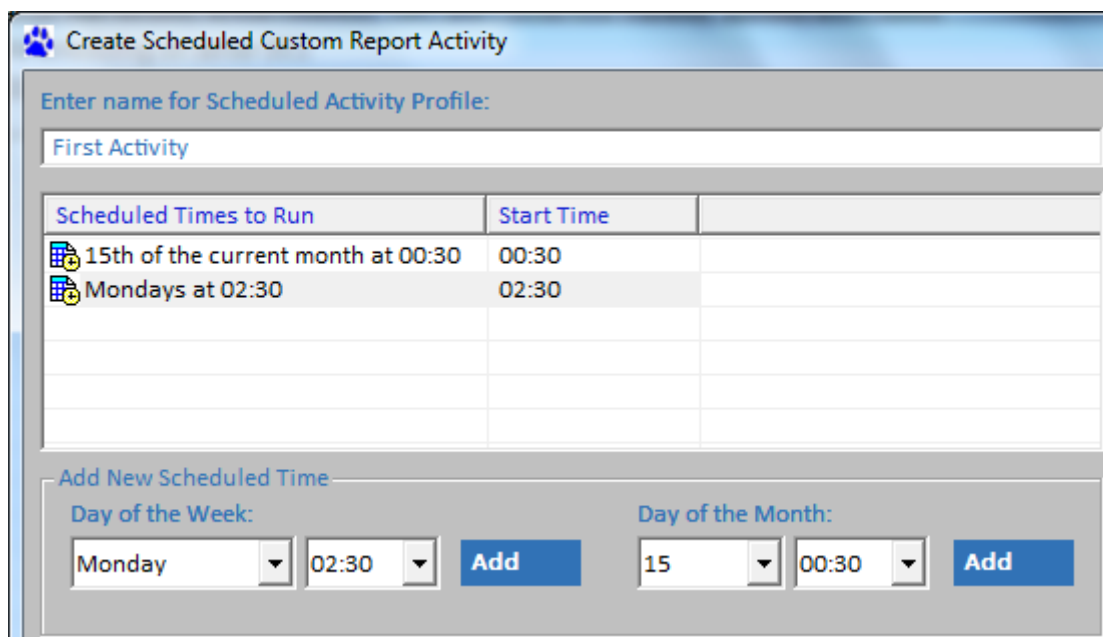


Figure 5-56

There is no limit on the number of “Scheduled Times to Run” are specified.

Next, choose the Custom Report(s) to run with this Scheduled Activity:

Add New Scheduled Time

Day of the Week: Everyday 00:00 Add

Day of the Month: 1 00:00 Add

Custom Reports Included in Scheduled Activity Profile		From Server
AD Test Report		DC1
GPO Check		DC1

Add Custom Report

AD Test Report Add

☐ **Disable this Scheduled Report**

Figure 5-57

There is no limit on the number of Custom Reports that can be included.

Important:

Custom Report(s) included in a Scheduled Activity should be set to [report directly to a file](#).

If not, you may notice `CPTWCCR.EXE` in the process (task) list at the server. Because Custom Reports, when run by the CPTRAX Server Agent, are run in the background there is no method to view on-screen report results.

You will need to manually terminate any `CPTWCCR.EXE` processes in the task list at the server hosting the CPTRAX Server Agent that are not configured to report directly to a file.

The `CPTWCCR.EXE` process will auto-terminate if the report it is building contains no results or if it is reporting directly to a file and it is finished.

Lastly you can set this activity to be Disabled. When disabled this activity will not be run, if currently running it will run to completion and then will not be rescheduled to run again. Later, you can edit this activity to disable or re-enable it.

Once complete, click on the “Create Custom Report Scheduled Activity” button and you will be returned to the previous screen ([Figure 5-51](#)). The new Scheduled Activity will automatically be included in the list.

Viewing current Scheduled Activities

Start by running the CPTRAX for Windows Administration Console and refer to [Figure 5-1](#) and [Figure 5-2](#) for how to navigate to the Custom Reports management screen. Please note the “Scheduled Activity Profiles” list at the lower half of the following screen:



Scheduled Activity Profiles	Defined on Server	Last Run	Error Message (if any)
 First Activity	DC1	<never>	
 Second Activity	DC1	<never>	

Figure 5-58

The icon shown indicates whether the activity is disabled. The orange time clock icon indicates disabled. The blue time clock icon indicates is not disabled. The “Last Run” column indicates the last time the activity was run by the CPTRAX Server Agent.. If there was an error message associated with the latest running of the activity it will be noted in the “Error Message (if any)” column.

Copying Scheduled Activities

There is no option to copy Scheduled Activities.

Appendix A – CPTRAX File Extensions

The CPTRAX for Windows Server Agent uses the following file extensions. Files using the following extensions (except *.CPT) are found in the

```
\SystemRoot\System32\Drivers\CPTRAX (32bit systems)
-or-
\SystemRoot\SysWow64\Drivers\CPTRAX (64bit systems)
```

and

```
\SystemRoot\System32\Drivers\CPTRAX\Q (32bit systems)
-or-
\SystemRoot\System32\Drivers\CPTRAX\Q (64bit systems)
```

folders at servers hosting the CPTRAX Server Agent.

See [Appendix C](#) for the procedure to confirm appropriate file permissions are set.

Note: If an [Auditor token](#) is installed, the CPTRAX Server Agent uses only the TXZ and CPT file extensions (listed below).

*.Q = initial staging files made by CPTRAXW.EXE

*.QS = initial staging files made by CPTW_K32.SYS/CPTW_K64.SYS

These files exist for approximately 2 minutes and then are renamed immediately to:

*.Q1 = 2nd stage, for CPTRAXW.EXE log records

*.Q2 = 2nd stage, for CPTW_K32.SYS/CPTW_K64.SYS log records

=====Extensions below are all generated by CPTRAXW.EXE=====

Q1 and Q2 files are combined into TXQ files (these are intermediate log files when renamed to TXR are ready for transmission)

*.TXW files when ready, are renamed TXY. TXW files are a combination of TXR files for transmission to department hosts

*.TXY files are those files completely ready to be transmitted – they are named for each destination server ([Department Hosts](#))

*.TXV files are those files that were in the process of being transmitted via TCP/IP but the CPTRAX Server Agent was stopped before the transmission was complete. When the Server Agent is restarted it will rename any existing TXV files to be TXY.

*.TXZ files are those files that were in the process of being *RECEIVED* via TCP/IP but transmission was aborted, so, when found these orphaned files are completely deleted and transmission is presumed to be auto-restarted by the sending server's CPTRAX Server Agent.

*.CPT files are found in the [“cptlogs” folder](#) and contain ready to report from log files.

Appendix B – All Custom Report Data Services

The following table includes all services that provide data for CPTRAX Custom Reports ([Chapter 5](#)). The “AD” column indicates data available associated with [Active Directory Tracking](#) Profiles. The “Logon” column indicates data available associated with [Logon+Logoff](#) and [Failed Logon](#) Profiles. The “File” column indicates data available associated with [File System Activity Tracking](#) Profiles. A checkmark is used to indicate which services are available for the selected Profile type.

AD	Logon	File	Column Service Description
✓	✓	✓	RPT:LOG:Display Reporting Server for Activity Record
✓	✓	✓	RPT:LOG:Display Profile Name for Activity Record
✓	✓	✓	RPT:LOG:Display Date/Time selected Activity Record was recorded
✓	✓	✓	RPT:LOG:Display Workstation Name where Activity Record Originated
✓	✓	✓	RPT:LOG:Display Workstation IPv4 Address where Activity Record Originated
✓	✓	✓	RPT:LOG:Display SAM Name of Object initiating Activity Record
✓	✓	✓	RPT:LOG:Display FQDN (cn=user,dc=domain...) of Object initiating Activity Record
✓	✓	✓	RPT:LOG:Display SID (S-1-5-18...) of Object initiating Activity Record
✓	✓	✓	RPT:LOG:Display Activity Record Type
✓	✓	✓	RPT:LOG:Display if Activity Record was Locally Induced (Packet Induced=FALSE)
✓	✓	✓	RPT:LOG:Display Windows Terminal Server Station Name (if known, typically is same as workstation name) for Activity Record
✓	✓	✓	RPT:LOG:Display Windows Terminal Server Remote Address used for Activity Record
✓	✓	✓	RPT:_Display count of rows in list <i>This service is meant to be displayed in a Text field outside the list containing the report</i>
✓	✓	✓	RPT:_Static Text <i>This service is meant to be displayed in a Text field outside the list containing the report</i>
✓	✓	✓	RPT:Display name of Server where selected Rpt Log is physically located
	✓		RPT:LOG:Display IF Activity Record Type = LOGON via NTLM
	✓		RPT:LOG:Display IF Activity Record Type = LOGON via KERBEROS
	✓		RPT:LOG:Display IF Activity Record Type = LOGOFF (NTLM or KERBEROS)
	✓		RPT:LOG:Display IF Activity Record Type = LOGON LOCAL or WTS
	✓		RPT:LOG:Display IF Activity Record Type = LOGON LOCAL or WTS
	✓		RPT:LOG:Display IF Activity Record Type = LOGON FAILED via NTLM
	✓		RPT:LOG:Display Logon Type (Kerberos, NTLM or Local) for Activity Record
	✓		RPT:LOG:Display Logon Total Time (for Logoff Activity Record)
	✓		RPT:LOG:Display Logon Failure Type for Activity Record
	✓		RPT:LOG:Display Logon Failure Code (Decimal) for Activity Record
	✓		RPT:LOG:Display Logon Date/Time for Activity Record
	✓		RPT:LOG:Display Logoff Date/Time for Activity Record
	✓		RPT:LOG:Display Logon Zone {the Domain logged onto} for Activity Record
	✓		RPT:LOG:Display Logon Domain {the Domain that the workstation belongs to where logon originated} for Activity Record
	✓		RPT:LOG:Display Logon Total Time -No Commas-No Label- (for Logoff Activity Record)
		✓	RPT:LOG:Display IF Activity Record Type = DELETE FILE or FOLDER
		✓	RPT:LOG:Display IF Activity Record Type = WRITE FILE

		✓	RPT:LOG:Display IF Activity Record Type = CREATE FILE or FOLDER
		✓	RPT:LOG:Display IF Activity Record Type = RENAME FILE or FOLDER
		✓	RPT:LOG:Display IF Activity Record Type = OPEN FILE or FOLDER
		✓	RPT:LOG:Display IF Activity Record Type = ACL SET OWNER on FILE or FOLDER
		✓	RPT:LOG:Display IF Activity Record Type = ACL REMOVE ACE on FILE or FOLDER
		✓	RPT:LOG:Display IF Activity Record Type = ACL MODIFY ACE on FILE or FOLDER
		✓	RPT:LOG:Display IF Activity Record Type = ACL ADD ACE on FILE or FOLDER
		✓	RPT:LOG:Display Filename affected by this Activity Record
		✓	RPT:LOG:Display IF affected File System Object is a Folder (Folder==TRUE) for Activity Record
		✓	RPT:LOG:Display IF File System Activity was BLOCKED
		✓	RPT:LOG:Display New Filename if Activity Record is indicates Rename or Copy Activity
		✓	RPT:LOG:ACL:Display SID (S-1-5-18...) of Object referred to by ACL Activity Record
		✓	RPT:LOG:ACL:Display FQDN (cn=user,dc=domain...) of Object referred to by ACL Activity Record
		✓	RPT:LOG:ACL:Display New Mask of Object referred to by ACL Activity Record
		✓	RPT:LOG:ACL:Display New Mask (Hexadecimal) of Object referred to by ACL Activity Record
		✓	RPT:LOG:ACL:Display New Flags of Object referred to by ACL Activity Record
		✓	RPT:LOG:ACL:Display New Flags (Hexadecimal) of Object referred to by ACL Activity Record
		✓	RPT:LOG:Display Share Name used for this Activity Record (note:local access such as Terminal Server Sessions do not use shares)
		✓	RPT:LOG:ACL:Display SAMName (domain\user) of Object referred to by ACL Activity Record
		✓	RPT:LOG:ACL:Display ACE Type (Allow or Deny) of ACL Activity Record
✓			RPT:LOG:Display Active Directory Object name affected by this Activity Record
✓			RPT:LOG:Display Active Directory Object "Object Class" affected by this Activity Record
✓			RPT:LOG:Display Active Directory Object Attribute affected by this Activity Record
✓			RPT:LOG:Display Active Directory Object Attribute "New Value" in this Activity Record
✓			RPT:LOG:Display Active Directory Object Attribute "Deleted Value" in this Activity Record
✓			RPT:LOG:Display IF Active Directory Attribute is Single Valued
✓			RPT:LOG:Display IF Active Directory Attribute is a Binary Value
✓			RPT:LOG:Display Active Directory Attribute "COMMENT" for selected Activity Record

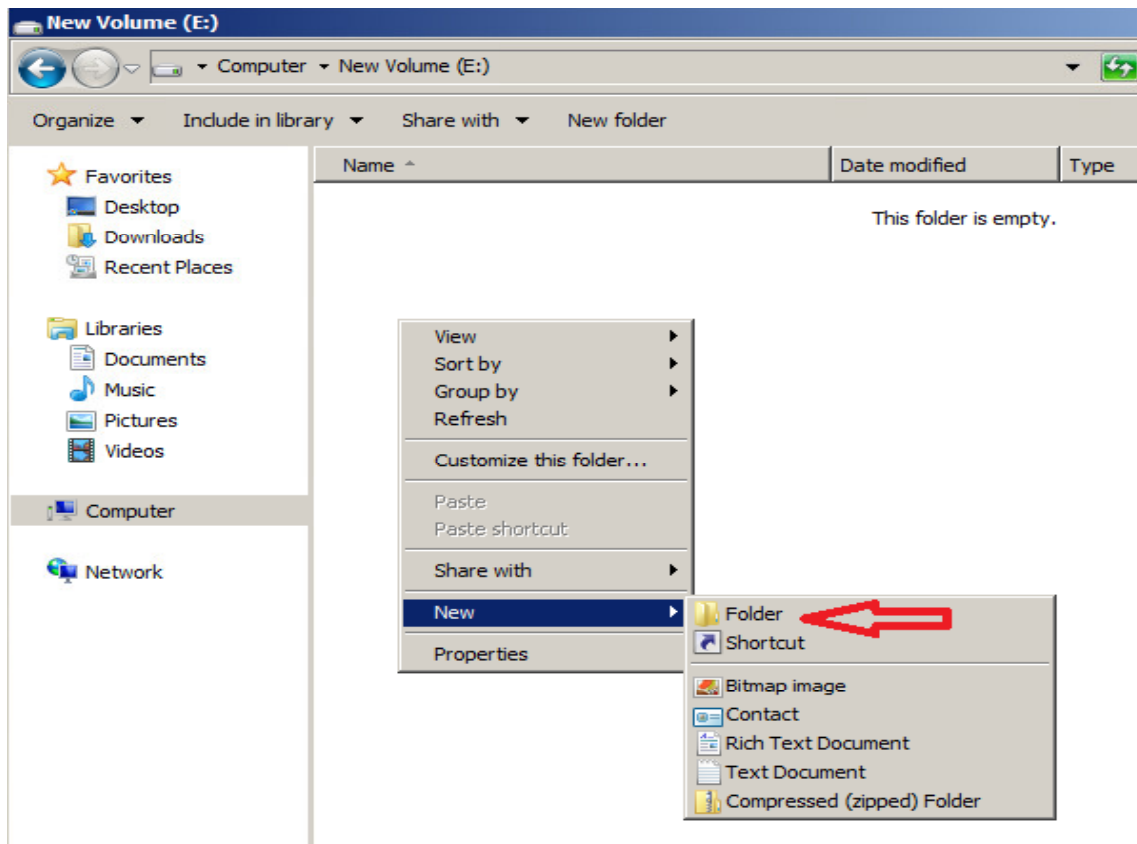
Appendix C – Creating Shared Folder for CPTRAX reporting

Please follow these instructions if you need to create a shared folder on the server or domain controller where you will be installing CPTRAX. This Share will be used by the CPTRAX Service to store logs files for reporting. Any users needing the ability to create CPTRAX reports will require read access to the selected Share. Regular users who are not responsible for generating CPTRAX reports will not require access to the defined Share.

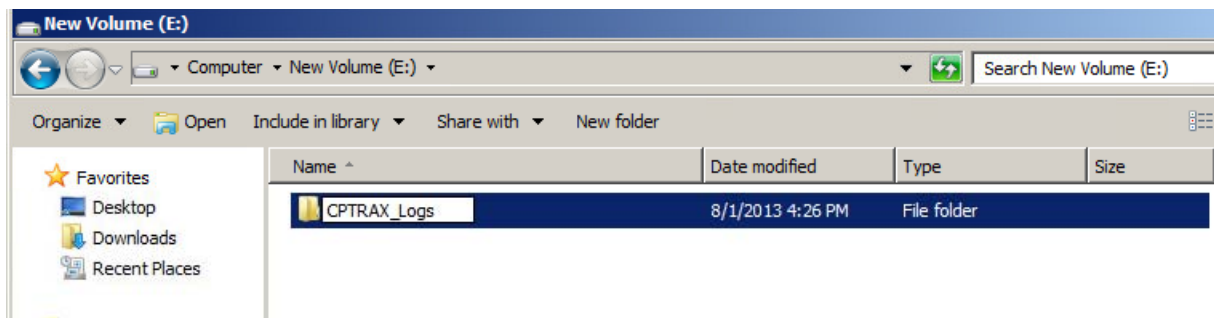
The minimum share level and NTFS permissions needed to the shared folder are READ for user accounts or groups that will be viewing CPTRAX reports stored in the log files. The folder you create to store the log files will need to be created on a drive local to the selected server.

The following steps must be performed from the server console (keyboard local to the server or Remote Desktop session) where CPTRAX will be installed.

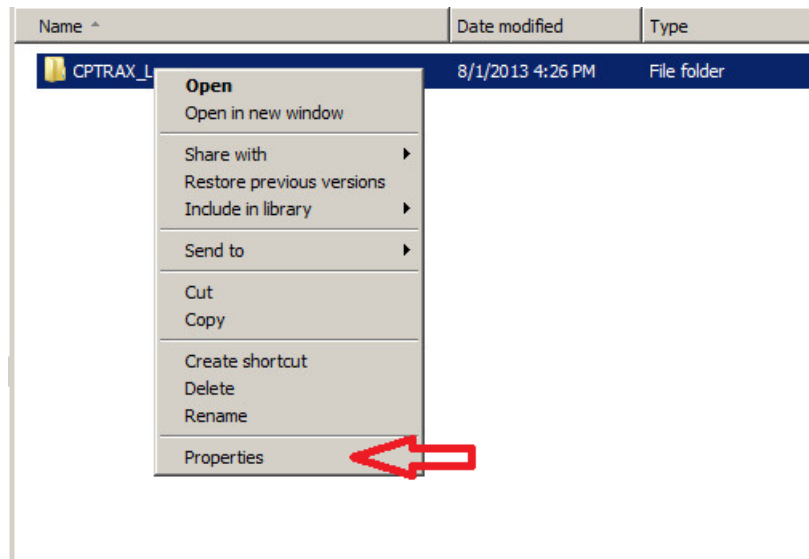
Open Windows Explorer and select the drive where you will store the CPTRAX Log files. Right click the content pane and select “New -> Folder”.



Enter “CPTRAX_Logs” for the folder name.

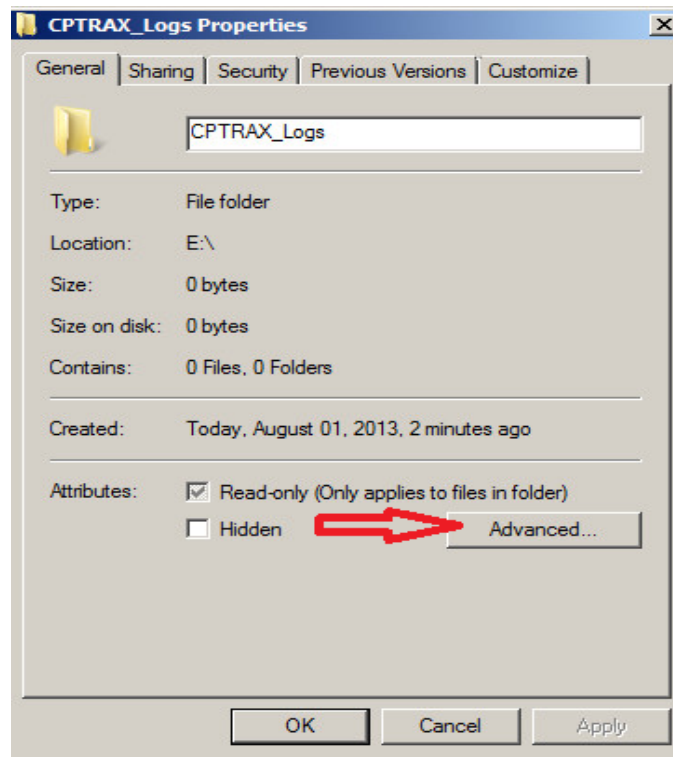


Highlight the CPTRAX_Logs folder, then right click the highlight folder and select “Properties”.

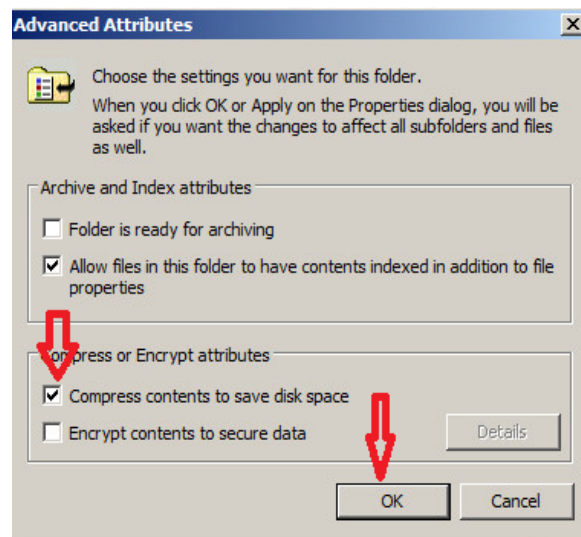


Windows includes the innate ability to compress files. It is recommended that the contents of the CPTRAX_Logs folder engage the compress option to reduce log file storage footprint.

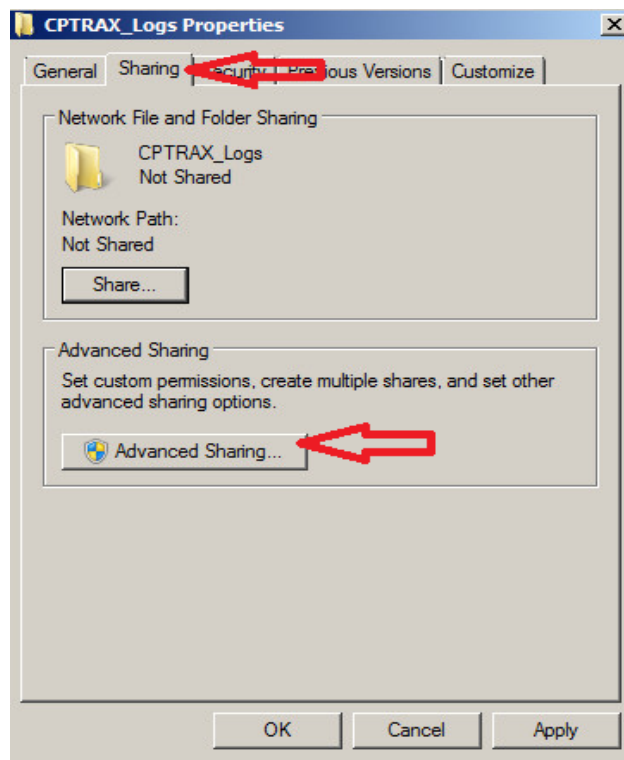
To enable compression on the CPTRAX_Logs folder click the “Advanced” button.



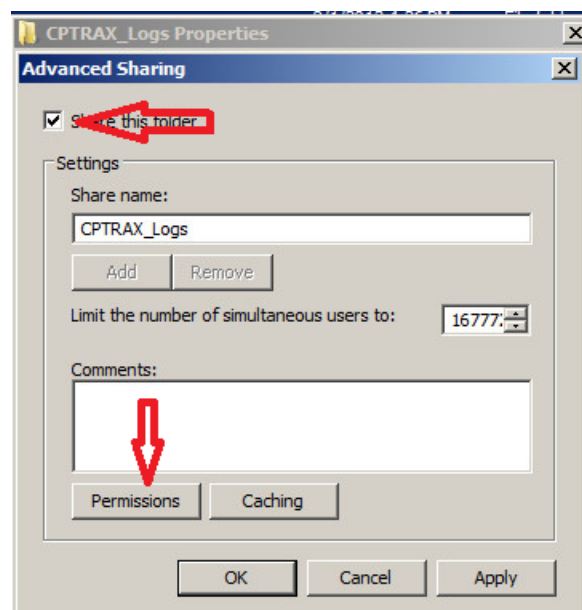
Check the box next to “Compress contents to save disk space” check box and click the “OK” button to close the Advanced Attributes window.



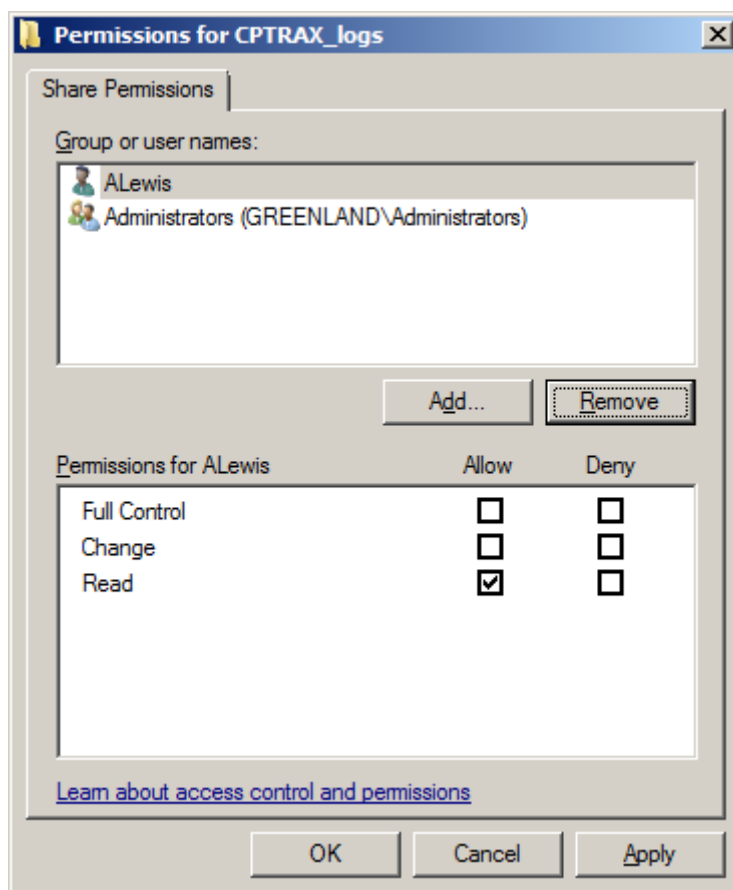
To share the CPTRAX_Logs folder click the “Sharing” tab and click the “Advanced Sharing” button.



Check the box “Share this Folder” check box and click the “Permissions” button.

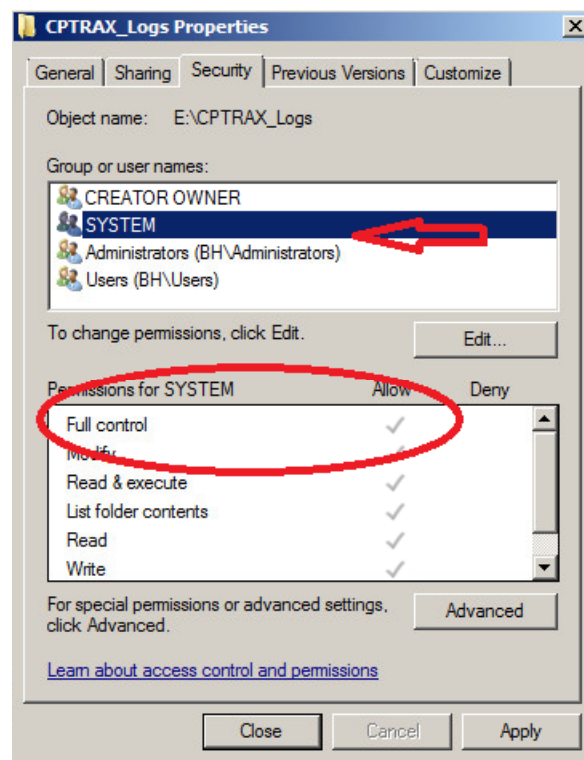


The minimum share level permissions need to view CPTRAX log files is READ. This should be assigned to the user account(s) or group(s) that will generate CPTRAX reports and thus view the log file contents.

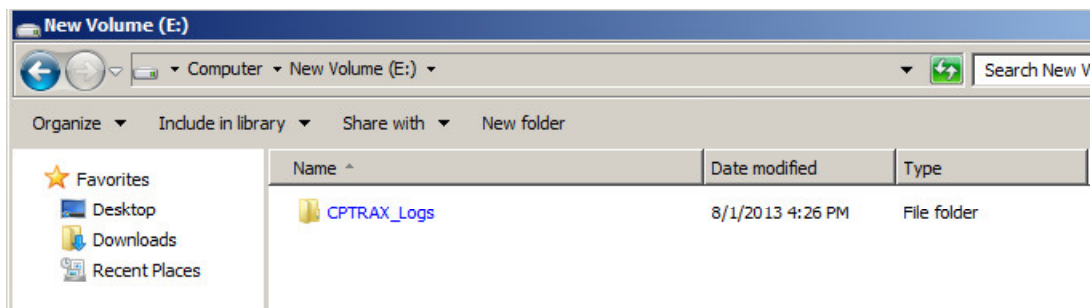


Please note that CPTRAX log files are encrypted and you will not be able to view or change the contents of the log files directly, however they can be manually deleted from the folder. Do not assign permissions to any user who should not be able to view the log files. Click the “OK” button once you have configured you permissions. Click the “OK” button to close the “Advanced Sharing” window.

Click the “Security” tab to verify and configure NTFS Permissions. You will need to verify the “SYSTEM” account has “Full Control” permissions to the CPTRAX_Logs folder. These permissions are the assigned default permissions but need to be verified for CPTRAX to function properly.



Once permissions are verified and/or added, click the “Close” button to return to Windows Explorer.



Once completed, you can immediately select and use the Share.

If non-administrative accounts will be used to generate CPTRAX reports, please refer to [Appendix E](#) for instructions to grant non-admin users remote registry access for generating CPTRAX reports.

Appendix D – Setting SYSTEM Account File Permissions

Confirming permissions on the *drivers* folder

The CPTRAX for Windows Server Agent, by *default*, logons on to the host server with the Local System Account. If you have installed the server agent and it is not creating files as expected the **SYSTEM** account may have insufficient permissions to the following paths:

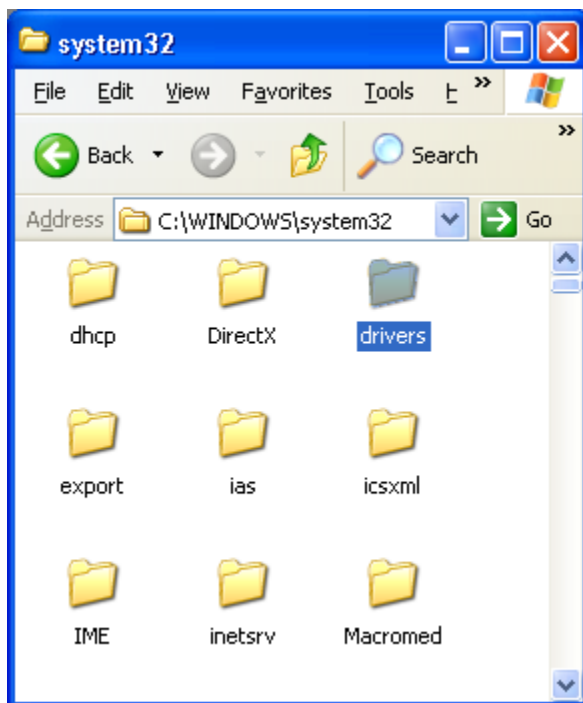
```
\SystemRoot\System32\Drivers    (32bit systems)
-or-
\SystemRoot\SysWow64           (64bit systems)
```

and

the Local Path hosting the “cptlogs” share as defined when installing the server agent ([reference Chapter 2](#)).

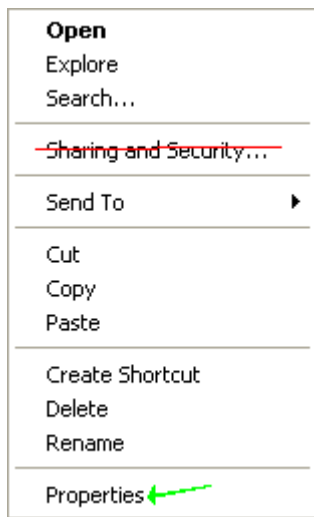
If the server agent is not creating activity log files as expected, please confirm that the **SYSTEM** account has sufficient permissions.

Step one: Checking **SYSTEM** account permissions to the “drivers” folder. It is preferable to check and set permissions *while you are at the server’s keyboard* and not accessing via a share.



Select the “drivers” folder and then *right click* on it, a pop up menu will be presented

Figure D-1



from the resulting popup menu select “Properties” this will open a new window as shown in the next figure

(do not select “Sharing and Security”)

Figure D-2

Step two: After selecting *Properties* on the pop up menu you will be presented with the following screen:

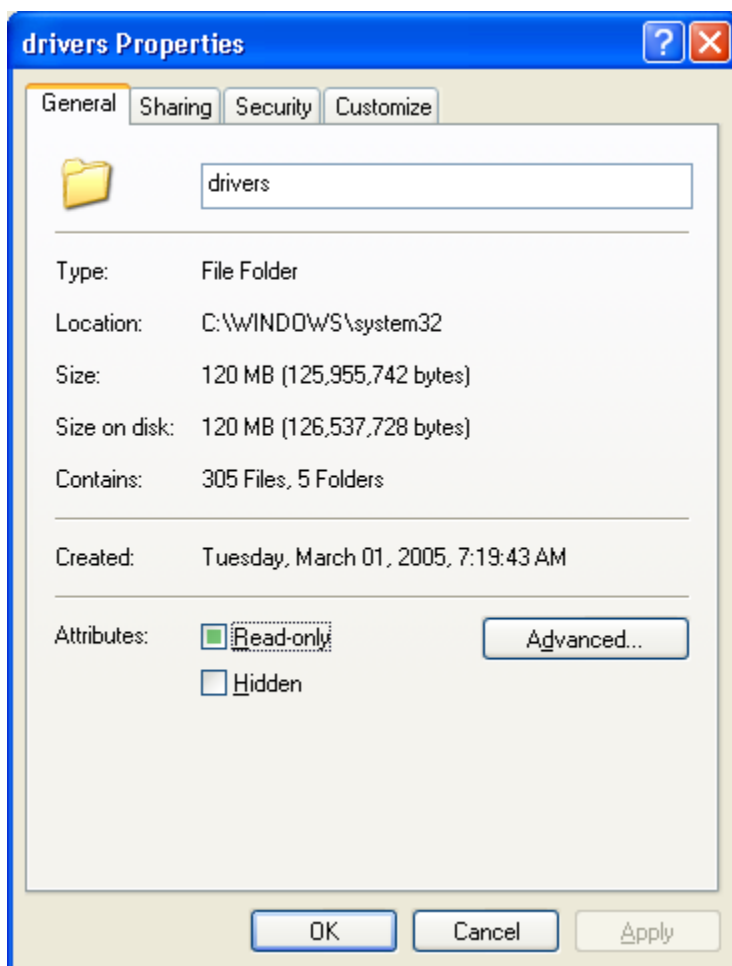


Figure D-3

Step three: Click on the “Security” tab to reveal the next image:

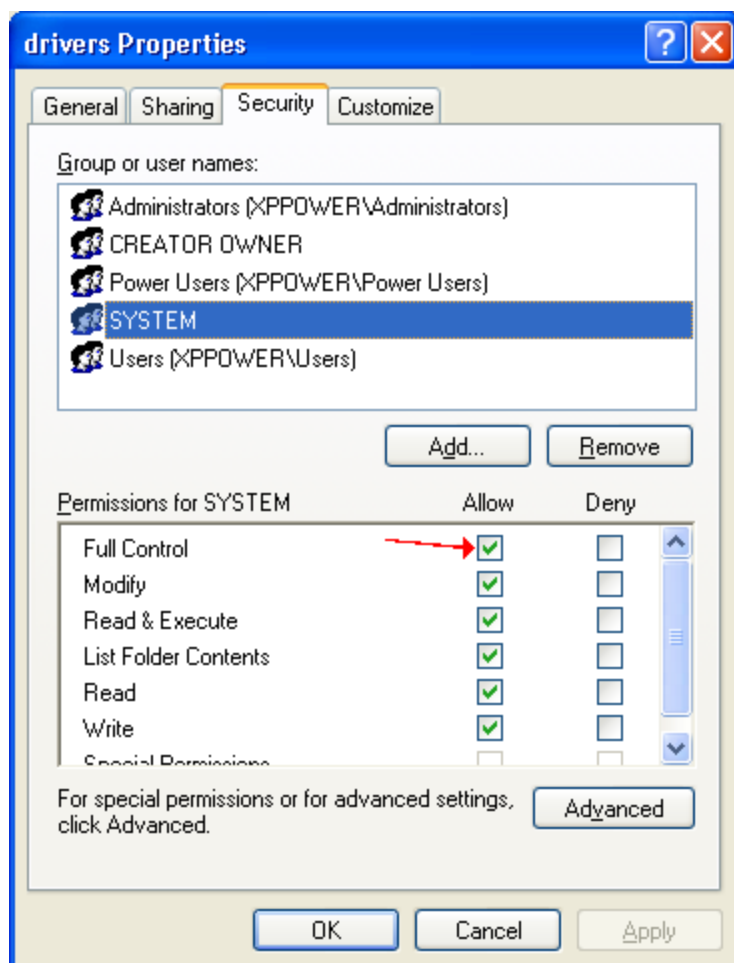


Figure D-4

Step four: Highlight the **SYSTEM** account from the list of names and ensure “Full Control” is set to “Allow”.

Confirming permissions on the Share for Activity Log Files

After confirming the **SYSTEM** account’s permission on the “drivers” folder (listed above), perform these same 4 steps for the folder on the server that is defined to be the share for activity log files – do not set the permissions on the “cptlogs” folder within, set permissions for the **SYSTEM** account on the parent folder (the one that is actually ‘shared’).

Note: When viewing permissions for the **SYSTEM** account they may appear grayed out as shown in the next figure:

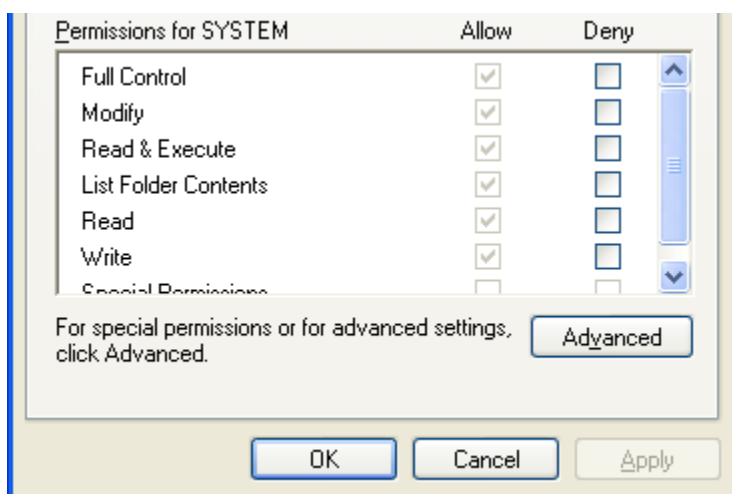


Figure D-5

This indicates that permissions were set at a higher-level folder and have been inherited from that folder to the current one. Confirm the permissions are set for “Allow Full Control”, if they are not, you will need to edit the security on the folder where permissions were directly given. To do this, you will need to know which folder that is, to find out, click on the “Advanced” button, a screen similar to the following will be presented:

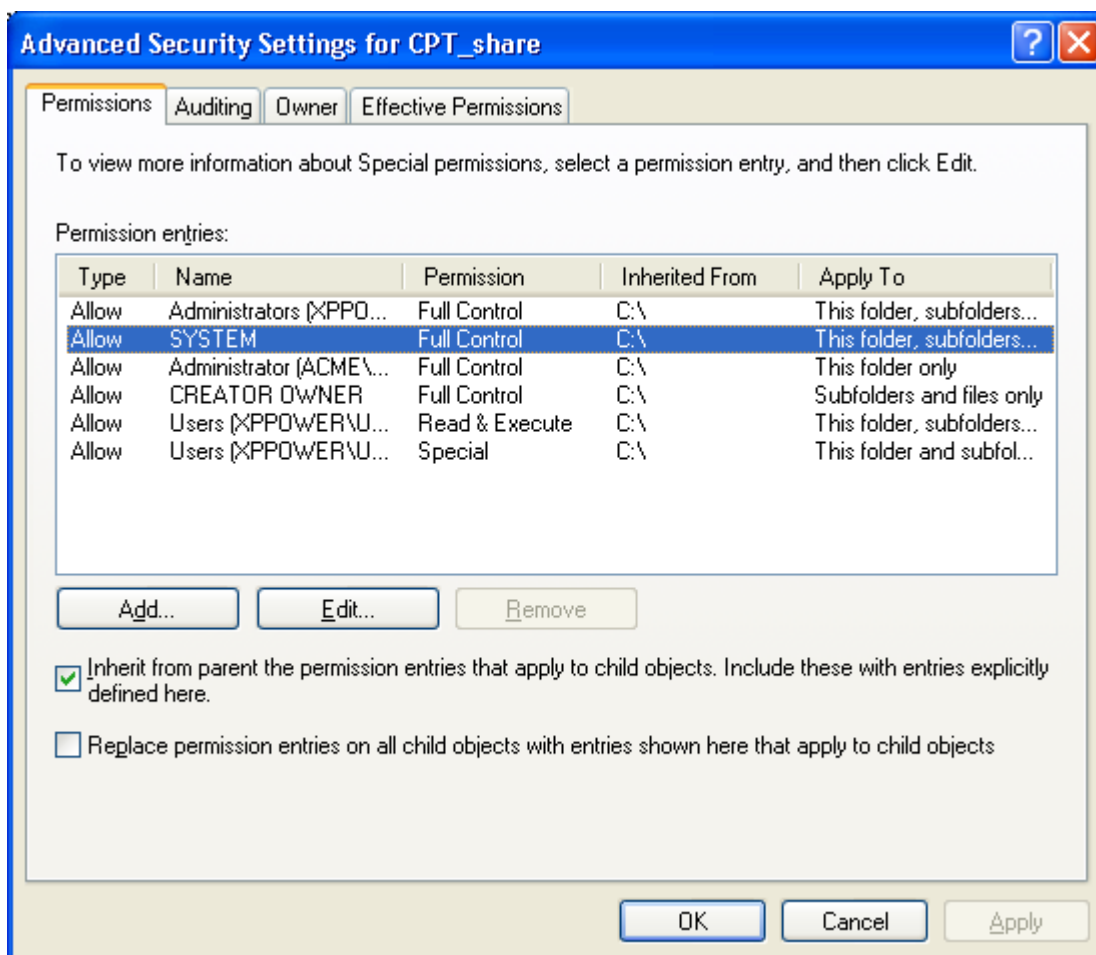


Figure D-6

The highlighted line (for the **SYSTEM** account) reveals that permissions were directly given at the root of C: drive (“C:\”). You will need to set “Allow Full Control” permissions on that folder for the **SYSTEM** account to have Full Control to the folder being shared that is used for CPTRAX’s Activity Log Files.

Appendix E - Granting non-admin users access for generating CPTRAX reports

If non-administrator user accounts will be generating CPTRAX for Windows reports, remote registry access and read access to the selected servers' registry (CPTRAX keys) will be required.

You must also ensure that the user has sufficient privileges to access the log file share on the server. They need to have NTFS permissions and Share-Level permissions. You can test this access by using Windows Explorer from their workstation while logged on as the user.

To establish the necessary registry access please following article link or refer to the text below:

<http://support.microsoft.com/kb/314837>

Option 1 of 2

The following instructions are one method of establishing the necessary access permissions for non-administrator users. This method will provide 'general read access' to the selected server's registry. For more restricted registry access please refer to option 2 below.

First, ensure that the "Remote Registry" service is running and set to "Automatic" on the server.

To create the registry key to allow non-administrator user access to the registry:

Start Registry Editor (`regedit.exe` or `regedt32.exe`) and go to the following subkey:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
```

On the Edit menu, click Add Key. Enter the following values:

Key Name: SecurePipeServers

Class: REG_SZ

Go to the following subkey:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers
```

On the Edit menu, click Add Key. Enter the following values:

Key Name: winreg

Class: REG_SZ

Go to the following subkey:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
```

On the Edit menu, click Add Value. Enter the following values:

Value Name: Description

Data Type: REG_SZ

String: Registry Server

Go to the following subkey.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
```

Select "winreg". Click Security and then click Permissions. Add users or groups to which you want to grant access. If you at a later stage want to change the list of users that can access the local server's registry, repeat steps 10-12. To be in effect, the server must be restarted.

Option 2 of 2

For environments with a high level of security, non-administrator user accounts will require, at a minimum, the granting of READ ACCESS permission to the following two keys on the server hosting CPTRAX log files.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Visual Click Software, Inc.  
HKEY_LOCAL_MACHINE\SOFTWARE\Visual Click Software, Inc.\CPTRAX
```

For 64-bit servers:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Visual Click Software, Inc.  
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Visual Click Software, Inc.\CPTRAX
```

Once you have added READ ACCESS permission for the selected non-administrator users to the above referenced registry keys you will also need to perform the following:

Ensure that the "Remote Registry" service is running and set to "Automatic" on the server.

Make the CPTRAX registry keys available for Remote Registry Access by modifying the registry.

To start, open `regedit.exe` on the server and go to:

```
HKEY_LOCAL_MACHINE\SYSTEM\  
CurrentControlSet\Control\SecurePipeServers\winreg\AllowedPaths
```

There will likely be a value present named "Machine" with multiple paths. Select "Edit" and then "Modify" and add the following values:

```
SOFTWARE\Visual Click Software, Inc.  
SOFTWARE\Visual Click Software, Inc.\CPTRAX
```

For 64-bit servers:

```
SOFTWARE\Wow6432Node\Visual Click Software, Inc.  
SOFTWARE\Wow6432Node\Visual Click Software, Inc.\CPTRAX
```

And save the changes. This change should allow the non-administrator users read access to the selected registry keys.

To be in effect, the server may need to be restarted.

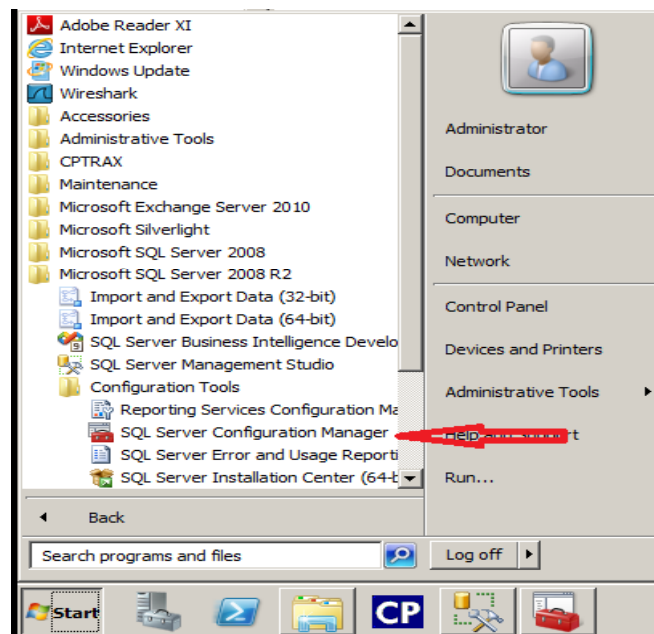
Appendix F – CPTRAX to SQL Configuration

Comprehensive installation details

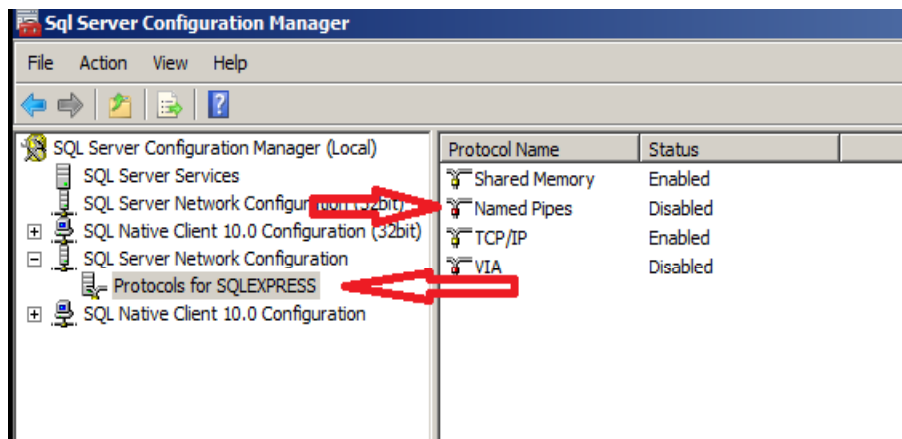
The steps below will walk you through the process of configuring the CPTRAX Service on the server(s) you wish to track activities on to connect to and store log data in an SQL Database. In addition you will need to be logged in as **the Administrator** or a member of the **Domain Admins** group in order to make the registry changes needed to successfully update and configure CPTRAX and create the CPTRAX Database and Tables in SQL. The following process is based upon SQL Express 2008R2...your steps may vary.

Configuring Protocols for SQL Server (performed at SQL Server Host)

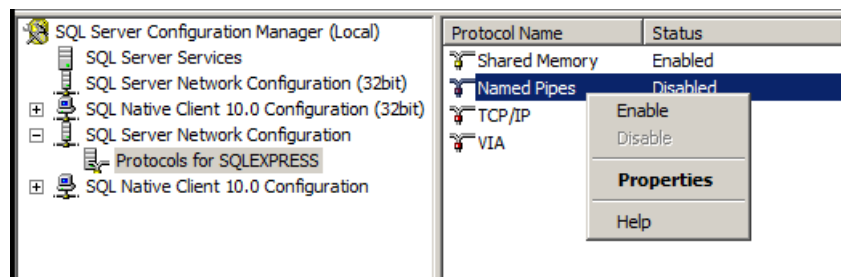
Click Start -> All Programs -> Microsoft SQL Server 2008 R2 -> Configuration Tools -> SQL Server Configuration Manager



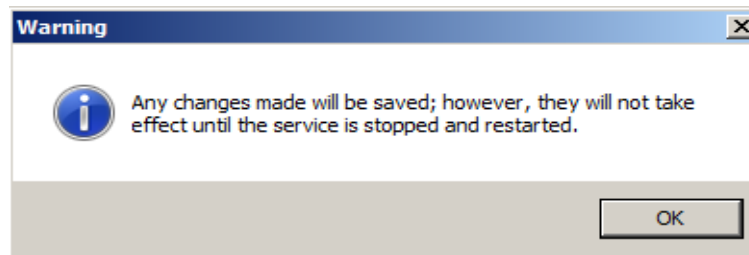
Expand SQL Server Network Configuration -> Protocols for SQLEXPRESS



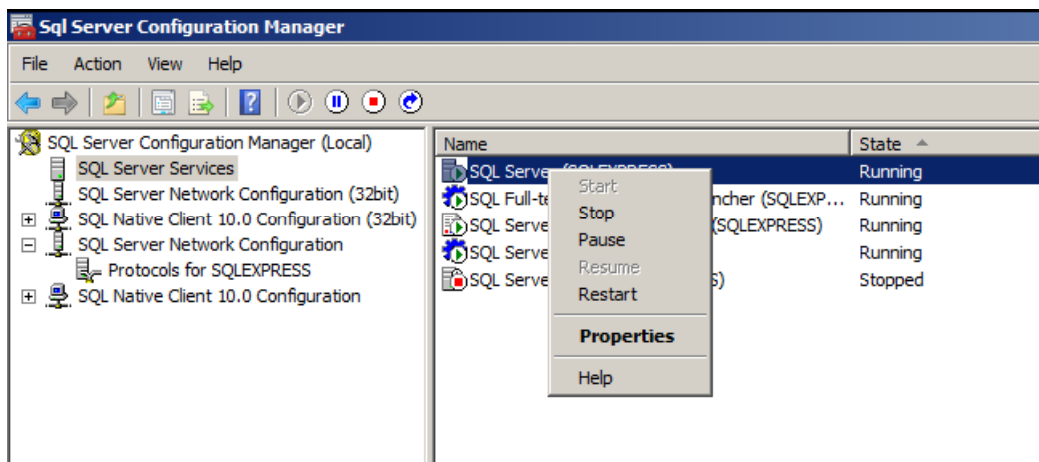
If Named Pipes is not enabled -> Right click “Named Pipes” in the right hand pane of the SQL Configuration Manager and select “Enable” to enable Named Pipes. Complete the steps a second time to enable the “TCP/IP” protocol if not already enabled.



You should receive the following Warning message that changes will not take effect until the service is stopped and restarted. Click the “OK” button.



To restart the SQL Server services from within SQL Server Manager -> highlight SQL Server Services in the left hand pane. In the right hand pane right click the SQL Server (SQLEXPRESS) and select “Restart”

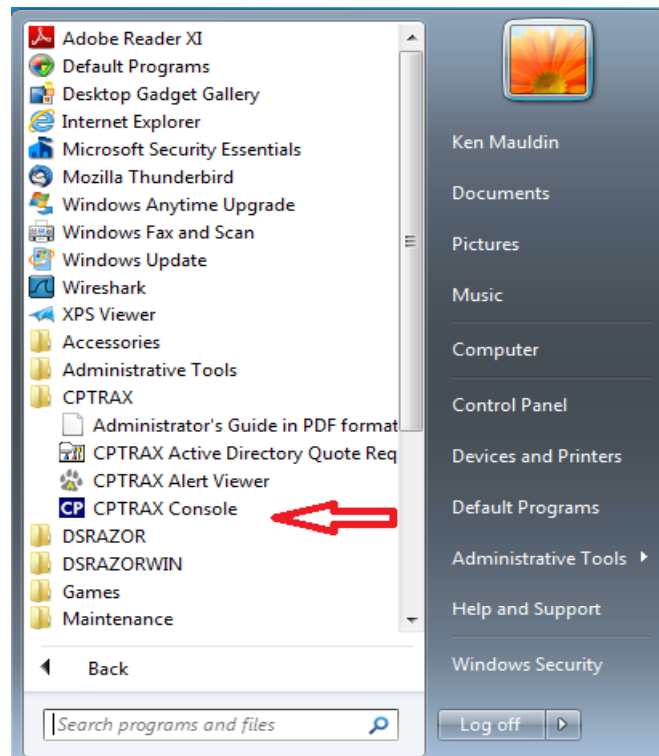


Close the SQL Configuration Manager Management Console.

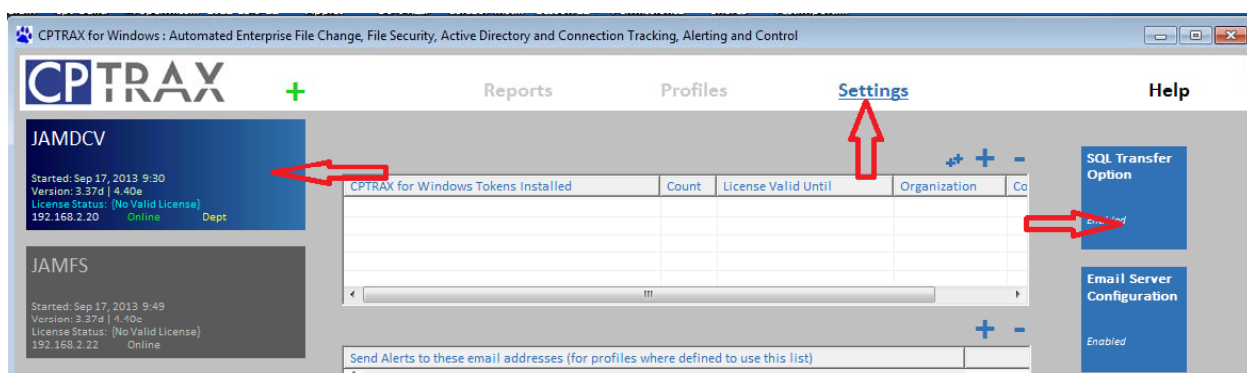
Configuring CPTRAX for SQL Server

The steps below will walk you through the process of configuring CPTRAX to create the CPTRAX_for_Windows database and connect to the SQL Server. The following steps are based upon SQL Express 2008R2...your steps may vary.

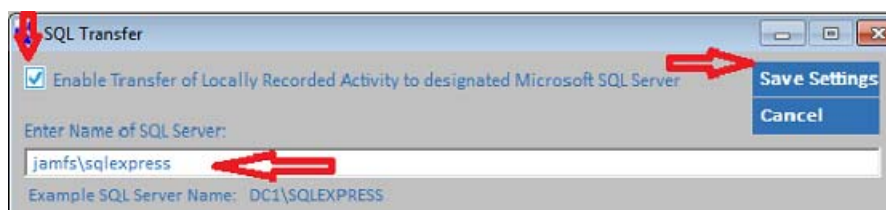
Click Start -> All Programs -> CPTRAX -> CPTRAX Console



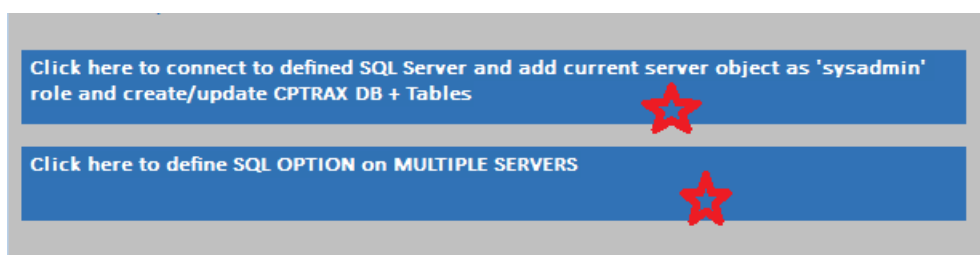
Highlight the server on the left side of the CPTRAX Console -> Click the “Settings” link in the top right side of the console -> Click the “SQL Transfer Option” button on the right side of the CPTRAX Console.



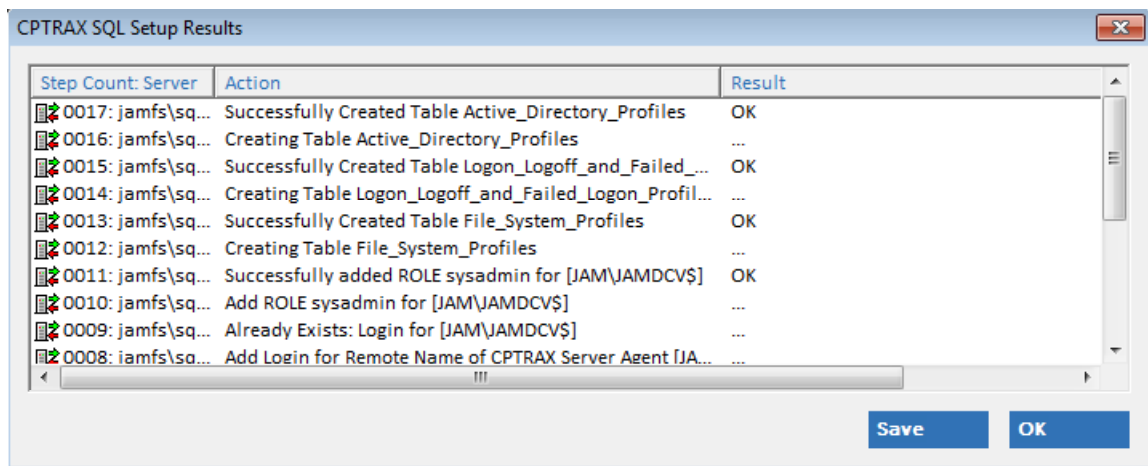
In the “SQL Transfer” windows -> check the box next to “Enable Transfer of Locally Recorded Activity to designated Microsoft SQL Server”. In the “Enter Name of SQL Server” box enter the SQL Server name and SQL Server Instance. (ServerName\InstanceName)



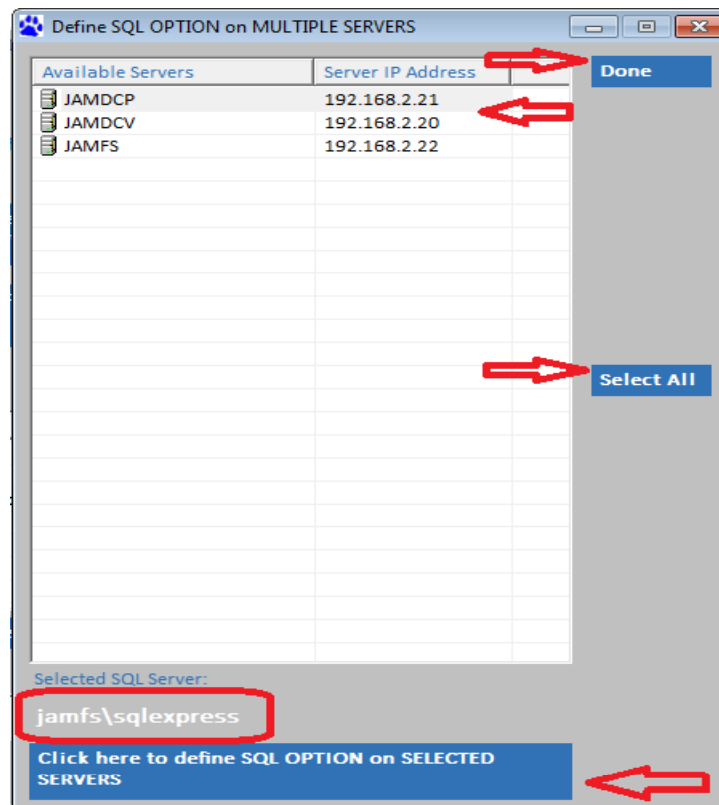
If you have CPTRAX installed on a single server and you would like the CPTRAX log files to be stored in an SQL Server click the “Click here to connect to defined SQL Server.....” button. If you have CPTRAX installed on multiple servers and you would like the CPTRAX log files to be stored in an SQL Server click the “Click here to define SQL Option on Multiple Servers” button.



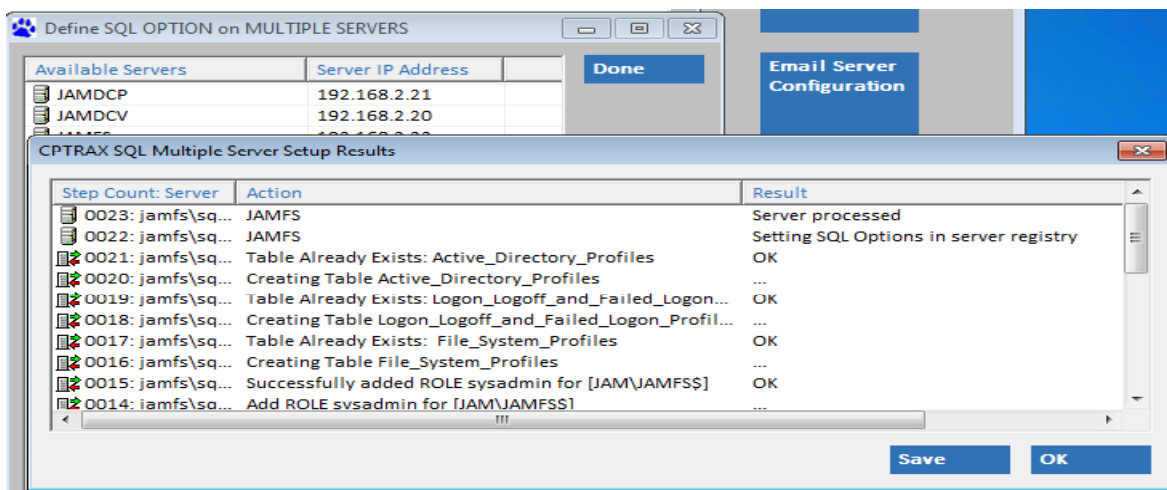
If you click the “Click here to connect to defined SQL Server...” button the “CPTRAX SQL Setup Results” window appears and you will see the status showing the database creation, table creation, logon added, and sysadmin role added. Click the “OK” button to close the status window.



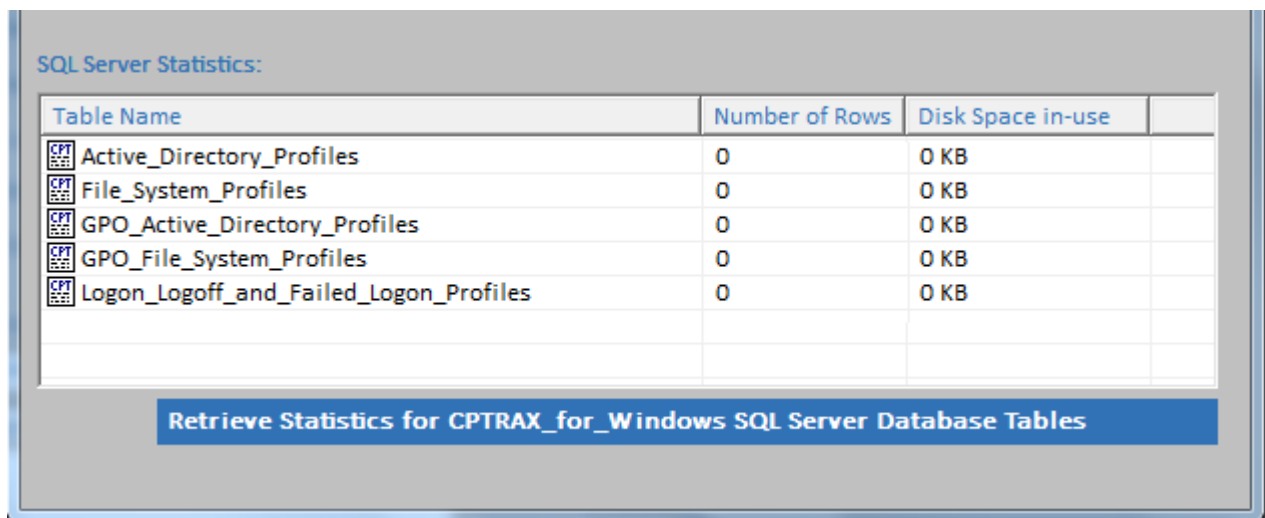
If you click the “Click here to define SQL Option on Multiple Servers” button the “Define SQL Option on Multiple Servers” window appears. You can highlight servers individually or click the “Select All” button to configure some or all servers to store their log files in SQL. Once you have highlight the servers you wish to configure click the “Click here to define SQL Options on Selected Servers” button at the bottom of the windows.



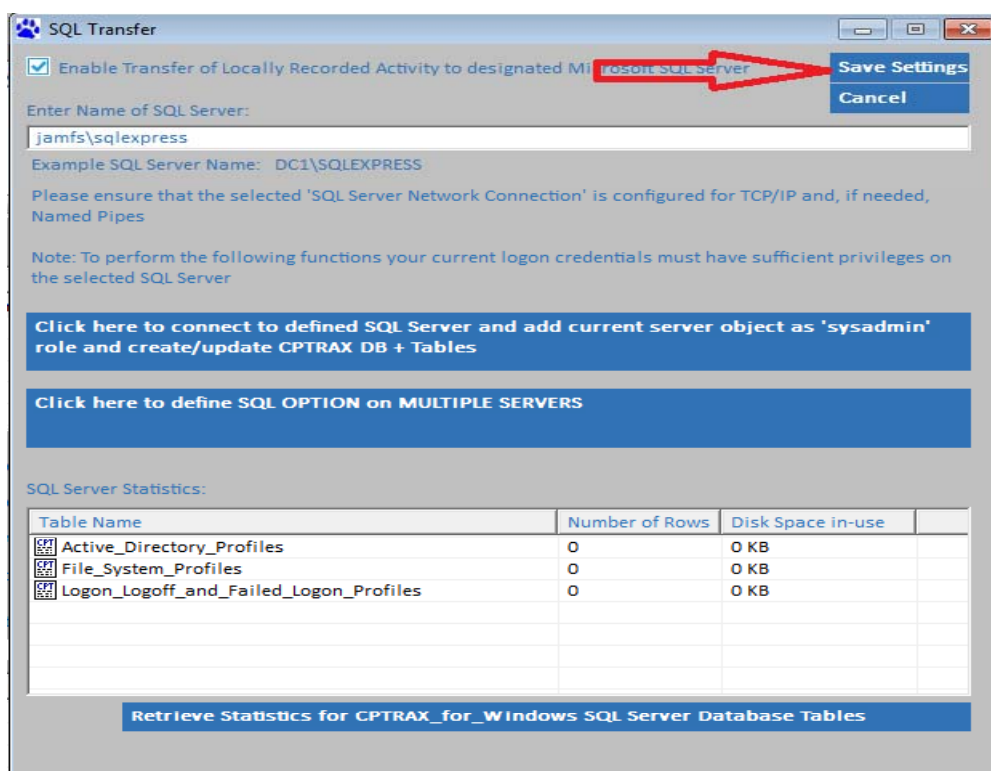
You will see the status showing the database creation, table creation, logon added, and sysadmin role added. Click the “OK” button to close the status window and click the “Done” button on the top right side of the window to close the windows.



To view if the tables were created successfully click the “Retrieve Statistics for CPTRAX_for_Windows SQL Server Database Tables” button at the bottom of the “SQL Transfer” window. You should see five tables: Active_Directory_Profiles, File_System_Profiles, GPO_Active_Directory_Profiles, GPO_File_System_Profiles, and Logon_Logoff_and_Failed_Logon_Profiles.



Click the “Save Settings” button on the top right of the “SQL Transfer” window to save your settings and close the window.

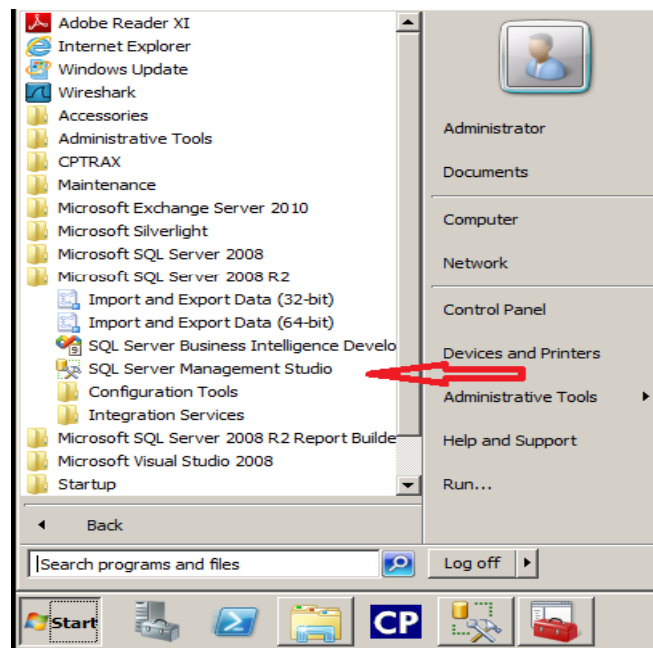


Please contact the Visual Click Windows Support Team if you have any questions or receive any error messages at any time during the configuration of the SQL Transfer process at [Visual Click Support](#).

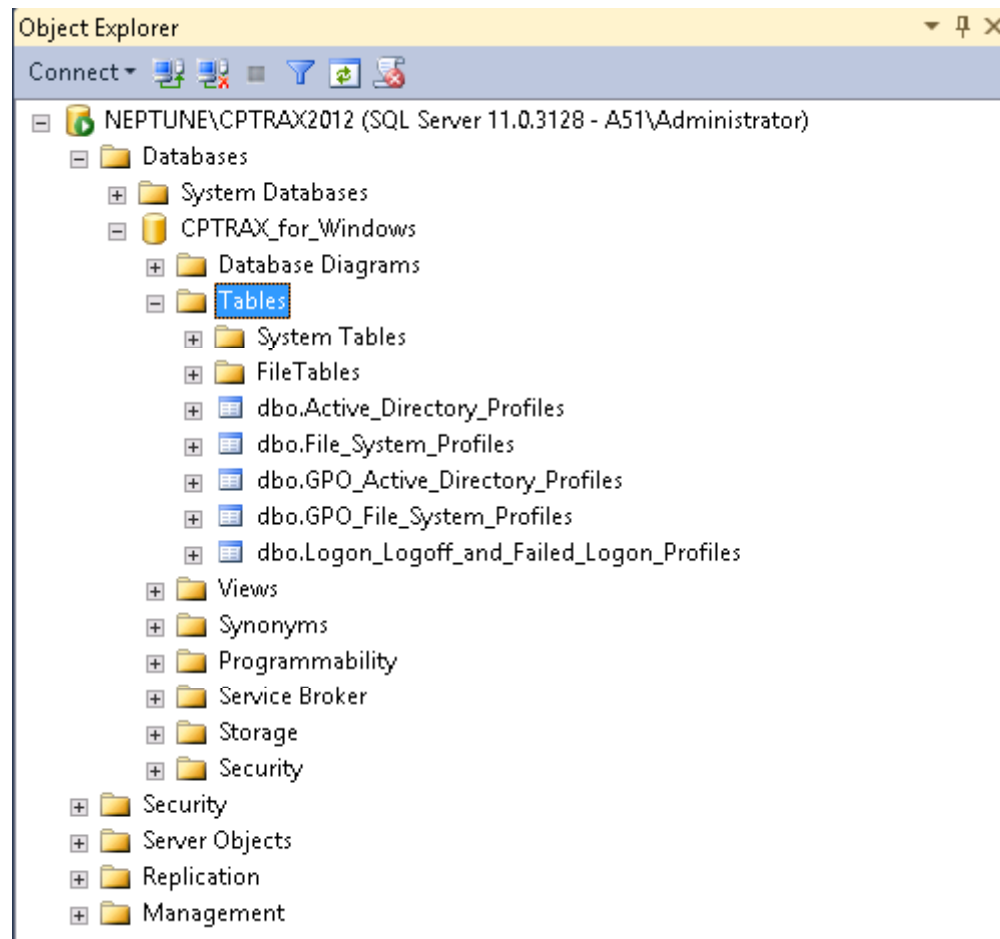
Verifying CPTRAX for SQL Server installation

The steps below will walk you through the process of verifying the CPTRAX_for_Windows database and the three tables from SQL Server Management Studio. The following steps are based upon SQL Express 2008R2...your steps may vary.

Click Start -> All Programs -> Microsoft SQL Server 2008 R2 -> SQL Server Management Studio.



Expand the Databases folder to locate the CPTRAX_for_Windows database. Expand the CPTRAX_for_Windows database -> Expand the “Tables” folder to view the five CPTRAX tables.



Appendix G – Features FAQ

Selected Q & A

Question: I am installing CPTRAX for Windows and would like to know what additional performance overhead will be occur, for instance: memory usage, CPU power, and how quickly and large log files get.

Answer: There is no immediately response regarding specific numbers. The only way to know how it will affect their environment is to install it and try it.

Detailed Answer: Every server and network is different. CPTRAX is designed to run as a low-priority background service. The CPTRAX server agent should never take more than a few percentage of CPU utilization and less than 100MB of RAM. CPTRAX always captures/ queues activity in real-time. Activity capture is done with low resource utilization. Afterwards, CPTRAX uses background processes to further process captured data (including arrangement into encrypted log files and setup for transfer) and, actual transfer of log files to their final destination(s). Log file growth depends on how much activity is being monitored including how many users access those monitored resources, and how often. CPTRAX's log files are transaction-based, so log file growth is determined by the settings selected. [General guidance is this: you can store 180,000 to 500,000 records on a gigabyte of uncompressed disk space.](#) By utilizing Windows native file compression you can expect an increase of at least 50% in the amount of records that can be stored.

Question: Regarding the "Block File System Activity" feature, does CPTRAX for Windows have an option to Block "Moving" of a folder? Reportedly this is a common issue, that is, where a user accidentally drags a folder to another and it is reported as being deleted and the helpdesk staff restores the folder first without checking to see if it was moved. Thus two copies of the same folder will be present.

If you do have that option, can it be limited to specific users or groups or is it an all or nothing kind of setup. Can the limitations be made granular?

Answer: It all depends on where the folder "is" and where it being moved "to".

If the folder is being moved around on the same "volume"(disk drive) then YES you can block the rename if you set the profile to "Block Creates/Writes" (on "Folders only") for a path that contains the existing folder(s) you want to prevent from being moved/renamed.

If the folder is being moved/renamed to a different volume (which includes "to a different server/workstation") then no, that is not an actual "move/rename" operation but is instead a copy operation followed by a delete operation (for each affected folder and files).

As for granularity, the file activity tracking profiles have a field that allows you to exclude accounts from the profile. By default, the profile will apply to everyone, however you can exclude local user and Domain accounts.

Question: I have defined a File Activity profile in CPTRAX to track only FILE DELETES, however, in the resulting report I was surprised to see FILE CREATE actions as well as FILE DELETE actions. What happened?

Answer: The SMB/CIFS protocol for file actions includes five (5) different options when creating a file:

- ✓ Create Always
- ✓ Create New
- ✓ Truncate Existing
- ✓ Open Existing
- ✓ Open Always

The first three (3) options will automatically DELETE an existing file and because CPTRAX is tracking requested actions and is not verifying the presence of an existing file those action options are recorded as being delete actions/requests as they are considered implicit delete actions.

Checking for the presence of existing files during such operations would incur overhead that would slow the performance of system from the user's point of view.

Solution: CPTRAX includes custom reporting that can be used to define a rules filter to eliminate any undesired actions from being shown in any reports you create. Use of CPTRAX's custom reporting can ensure that only actual delete requests are shown.

Troubleshooting Index

<i>ARP Cache</i>	98
<i>ARP Table</i>	98
<i>HKEY_CURRENT_USER\Software\Visual Click Software, Inc.</i>	13, 96
<i>HKEY_CURRENT_USER\Software\Visual Click Software, Inc.\CPTRAX</i>	80
<i>HKEY_CURRENT_USER\Software\Visual Click Software, Inc.\CPTRAX\AlertConsole</i>	59
<i>HKEY_CURRENT_USER\Software\Visual Click Software, Inc.\CPTRAX\MY_SERVERS</i>	81
<i>HKEY_LOCAL_MACHINE\Software\Visual Click Software, Inc.</i>	12
<i>HKEY_LOCAL_MACHINE\Software\Visual Click Software, Inc.\CPTRAX</i>	82, 92
<i>HKEY_LOCAL_MACHINE\Software\Visual Click Software, Inc.\CPTRAX\Profiles</i>	29, 98
<i>HKEY_LOCAL_MACHINE\Software\Visual Click Software, Inc.\CPTRAX\Reports</i>	102, 107, 125
<i>network dropout</i>	98
Prompt for Date at Runtime	120, 121
<i>Server Agent Startup</i>	36
<i>Slow network</i>	98
<i>Special note about midnight activity and Date/Time Rules</i>	121
<i>SYSTEM Account - Required File System Permissions</i>	141, 148, 156
<i>SystemRoot\System32\Drivers</i>	12, 125, 141
<i>SystemRoot\System32\Drivers\CPTRAX</i>	91, 92, 93, 131
<i>SystemRoot\System32\Drivers\CPTRAX\cptlogs</i>	90
<i>SystemRoot\System32\Drivers\CPTRAX\Q</i>	19, 131
<i>workstation timeout</i>	98