



# cimtrak

detecting change throughout the enterprise

## CimTrak™ Integrity & Compliance Suite 4.0

Master Repository  
Web Management Console  
File System Agent  
Network Device Agent  
Command Line Utility  
Ping Utility  
Proxy Utility  
FTP Repository Interface

## User Guidance

---



**CIMCOR**

## LEGAL NOTICES

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

## COPYRIGHT NOTICE

Copyright 2001-2018 CIMCOR, Inc. All Rights Reserved. This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from CIMCOR Inc., 8252 Virginia Street Suite C, Merrillville, IN 46410.

ALL EXAMPLES WITH NAMES, COMPANY NAMES, OR COMPANIES THAT APPEAR IN THIS DOCUMENT ARE IMAGINARY AND DO NOT REFER TO, OR PORTRAY ANY ACTUAL NAMES, COMPANIES, ENTITIES, OR INSTITUTIONS. ANY RESEMBLANCE TO ANY REAL PERSON, COMPANY, ENTITY, OR INSTITUTION IS PURELY COINCIDENTAL.

Every effort has been made to ensure the accuracy of this document. However, CIMCOR Inc. makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. CIMCOR Inc. shall not be liable for any errors or for incidental or consequential damages in connection with the furnishing, performance, or use of this document or the examples herein. The information in this document is subject to change without notice.

## TRADEMARKS

CimTrak™ is a trademark of CIMCOR Inc.

Microsoft, MS, Windows® operating systems are trademarks of Microsoft Corporation in the United States and/or other countries.

Macintosh and Mac OSX are registered trademarks of Apple Inc. in the USA and other countries.

Netscape is a registered trademark and Netscape Communicator is a trademark of Netscape Communications Corporation.

Installbuilder is a registered trademark of BitRock Inc.

Linux is a registered trademark of Linus Torvalds.

Solaris is a registered trademark of Sun Microsystems.

All other products mentioned are trademarks and/or registered trademarks of their respective owners.

Document Released October 9, 2018 CIMCOR™ CimTrak™ Integrity Suite

<b>1.</b>	<b>INTRODUCTION.....</b>	<b>15</b>
1.1.	DOCUMENTATION PURPOSE AND CONVENTIONS.....	15
1.2.	CIMCOR™ CIMTRAK™ INTEGRITY & COMPLIANCE SUITE INTRODUCTION.....	15
1.3.	CIMTRAK™ MASTER REPOSITORY .....	16
1.4.	CIMTRAK™ WEB MANAGEMENT CONSOLE .....	16
1.5.	CIMTRAK™ FILE SYSTEM AGENT .....	16
1.6.	CIMTRAK™ NETWORK DEVICE AGENT .....	17
<b>2.</b>	<b>CONFIGURATION PREREQUISITES .....</b>	<b>18</b>
2.1.	PREREQUISITE OVERVIEW .....	18
<b>3.</b>	<b>CONFIGURING AND USING THE CIMTRAK™ WEB MANAGEMENT CONSOLE.....</b>	<b>19</b>
3.1.	NAVIGATING THE CIMTRAK™ WEB MANAGEMENT CONSOLE.....	21
3.1.1.	UNDERSTANDING THE WEB MANAGEMENT CONSOLE OBJECT GROUP TREE.....	22
3.1.2.	UNDERSTANDING THE WEB MANAGEMENT CONSOLE OBJECT GROUP TREE.....	23
3.1.3.	UNDERSTANDING THE WEB MANAGEMENT CONSOLE INFORMATION DISPLAY AREA .....	23
3.2.	CIMTRAK™ WEB MANAGEMENT CONSOLE: HELP .....	24
3.3.	LEGAL NOTICES .....	25
3.3.1.	END USER LICENSE AGREEMENT (EULA) .....	26
<b>4.</b>	<b>CONFIGURING AND USING THE CIMTRAK™ MASTER REPOSITORY.....</b>	<b>28</b>
4.1.	MANAGING THE MASTER REPOSITORY FROM THE WEB MANAGEMENT CONSOLE .....	28
4.1.1.	MASTER REPOSITORY PROPERTIES.....	28
4.1.1.1.	CONFIGURING LOGGING OPTIONS.....	29
4.1.1.1.1.	CONFIGURING SMTP NOTIFICATIONS .....	31
4.1.1.1.2.	CONFIGURING NITROSECURITY NPP LOGGING.....	32
4.1.1.1.3.	CONFIGURING SNMP LOGGING .....	33
4.1.1.1.4.	CONFIGURING SYSLOG LOGGING .....	33
4.1.1.1.5.	CONFIGURING WEBTRENDS LOGGING .....	34
4.1.1.2.	CONFIGURING MASTER REPOSITORY SETTINGS .....	35
4.1.1.2.1.	CONFIGURING THE MASTER REPOSITORY NAME.....	36
4.1.1.2.3.	CONFIGURING THE WEB MANAGEMENT CONSOLE DISCONNECT TIMEOUT .....	36
4.1.1.2.4.	CONFIGURING THE MASTER REPOSITORY DISK SPACE MONITOR .....	37
4.1.1.2.5.	CONFIGURING THE MASTER REPOSITORY ACCESS RESTRICTIONS .....	37
4.1.1.3.	CONFIGURING MASTER REPOSITORY PERMISSIONS .....	38
4.1.1.3.1.	CONFIGURING THE MASTER REPOSITORY ACCESS RESTRICTIONS .....	39
4.1.1.4.	CONFIGURING MASTER REPOSITORY EMAIL SETTINGS .....	40
4.1.1.4.1.	CONFIGURING THE MASTER REPOSITORY EMAIL SETTINGS .....	42
4.1.1.5.	CONFIGURING THE MASTER REPOSITORY PASSWORD POLICIES.....	42
4.1.1.6.	CONFIGURING THE MASTER REPOSITORY COMMUNICATION SETTINGS.....	44
4.1.1.7.	CONFIGURING THE MASTER REPOSITORY LOGON BANNER .....	45
4.1.1.8.	CONFIGURING ACTIVE DIRECTORY/LDAP USER ACCOUNT INTEGRATION .....	48
4.1.1.8.1.	ADDING/EDITING/DELETING ACTIVE DIRECTORY/LDAP HOSTS .....	49
4.1.2.	MASTER REPOSITORY OPTIONS.....	51
4.1.3.1.	CHANGING ACCOUNT PASSWORD .....	51
4.2.	AUDITING THE MASTER REPOSITORY FROM THE WEB MANAGEMENT CONSOLE .....	52
4.3.1.	MASTER REPOSITORY INFORMATION .....	53
4.3.	CIMTRAK™ WEB MANAGEMENT CONSOLE: HELP .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
4.4.	LEGAL NOTICES .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
4.4.1.	END USER LICENSE AGREEMENT (EULA) .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
4.3.2.1.	FILTERING AND SORTING THE MASTER REPOSITORY EVENT LOG .....	58
4.5.	MASTER REPOSITORY LOGGED ON USERS.....	59

4.6.	MASTER REPOSITORY AREAS .....	60
4.4.1.	CREATING AND DELETING MASTER REPOSITORY AREAS.....	60
4.4.2.	MODIFYING MASTER REPOSITORY AREA PROPERTIES .....	62
4.4.3.	MANAGING AREA PERMISSIONS.....	63
4.4.3.1.	MODIFYING EXISTING USER/GROUP PERMISSIONS .....	64
4.4.3.2.	ADDING AND REMOVING USERS AND GROUPS TO AREA PERMISSIONS .....	65
4.4.4.	AREA EVENT LOG .....	67
4.4.4.1.	FILTERING AND SORTING THE AREA EVENT LOG .....	69
4.7.	MASTER REPOSITORY TEMPLATES.....	69
4.5.1.	MODIFYING EXISTING USER/GROUP PERMISSIONS .....	70
4.5.2.	IMPORTING MASTER REPOSITORY TEMPLATES .....	71
4.5.3.	EXPORTING MASTER REPOSITORY TEMPLATES.....	72
4.5.3.1.	CUSTOMIZING EXPORTED MASTER REPOSITORY TEMPLATES .....	73
<b>5.</b>	<b>CONFIGURING AND USING THE CIMTRAK™ FILE SYSTEM AGENT.....</b>	<b>75</b>
5.1.	MANAGING THE CIMTRAK™ FILE SYSTEM AGENT FROM THE WEB MANAGEMENT CONSOLE ..	75
5.1.1.	FILE SYSTEM AGENT PROPERTIES .....	76
5.1.1.1.	CONFIGURING THE FILE SYSTEM AGENT DESCRIPTION PROPERTIES .....	76
5.1.1.2.	CONFIGURING THE FILE SYSTEM AGENT LOG RETENTION PROPERTIES.....	77
5.1.1.3.	CONFIGURING THE FILE SYSTEM AGENT DISCONNECT WARNING.....	78
5.1.1.4.	CONFIGURING THE FILE SYSTEM AGENT HEARTBEAT AND STATISTIC GATHERING INTERVAL .....	78
5.1.1.5.	CREATING AND EDITING OBJECT GROUP WATCH POLICIES .....	79
5.1.1.5.1.	OBJECT GROUP PROPERTIES .....	80
5.1.1.5.2.	WATCH PROPERTIES.....	85
5.1.1.5.2.1.	CORRECTIVE ACTION .....	87
5.1.1.5.2.2.	AUTHORITATIVE COPY .....	88
5.1.1.5.2.3.	FILE COMPARISON METHOD .....	88
5.1.1.5.2.4.	STORE CHANGES .....	89
5.1.1.5.2.5.	AUTO EXCLUDE .....	89
5.1.1.5.2.6.	OPTIONS.....	90
5.1.1.5.2.7.	EVENT DETECTION METHOD .....	91
5.1.1.5.2.8.	CONNECTION LOSS.....	92
5.1.1.5.2.9.	TUNING WATCH PROPERTIES.....	92
5.1.1.5.2.10.	EXCLUDING AND INCLUDING USING REGULAR EXPRESSIONS .....	94
5.1.1.5.2.10.1.	EXCLUDING FOLDERS USING REGULAR EXPRESSIONS .....	95
5.1.1.5.2.10.2.	EXCLUDING FILES USING REGULAR EXPRESSIONS .....	95
5.1.1.5.2.10.3.	INVERSE EXCLUDING OF FOLDERS USING REGULAR EXPRESSIONS .....	96
5.1.1.5.2.10.4.	INVERSE EXCLUDING OF FILES USING REGULAR EXPRESSIONS .....	97
5.1.1.6.	SAVING OBJECT GROUP WATCH POLICIES TO TEMPLATES .....	98
5.1.1.7.	CREATING OBJECT GROUP WATCH POLICIES USING TEMPLATES .....	99
5.1.1.8.	DELETING OBJECT GROUP WATCH POLICIES.....	100
5.1.1.9.	ENABLING AND DISABLING OBJECT GROUP MONITORING .....	101
5.1.1.10.	SYNCHRONIZING OBJECT GROUP DATA .....	103
5.1.2.	FILE SYSTEM AGENT INFORMATION DISPLAY .....	103
5.1.2.1.	AUDITING FILE SYSTEM AGENT EVENTS.....	104
5.1.2.1.1.	FILTERING AND SORTING THE FILE SYSTEM AGENT EVENT LOG .....	106
5.1.2.2.	FILE SYSTEM AGENT PERMISSIONS .....	106
5.1.2.3.	MODIFYING AN EXISTING USER/GROUP FILE SYSTEM AGENT PERMISSIONS .....	108
5.1.2.4.	ADDING AND REMOVING USERS AND GROUPS TO FILE SYSTEM AGENT PERMISSIONS .....	109
5.1.3.	OBJECT GROUP INFORMATION DISPLAY.....	110
5.1.3.1.	AUDITING OBJECT GROUP EVENTS .....	111
5.1.3.1.1.	FILTERING AND SORTING THE OBJECT GROUP EVENT LOG.....	112
5.1.3.2.	REVIEWING OBJECT GROUP MONITORED CHANGES .....	112
5.1.3.2.1.	FILTERING AND SORTING THE OBJECT GROUP CHANGE LOG .....	114
5.1.3.2.2.	ACCESSING THE CHANGE LOG TAB CONTEXT MENU .....	114
5.1.3.2.2.1.	VIEWING CHANGE CONTENT.....	114
5.1.3.2.2.2.	VIEWING CHANGE FORENSIC DATA .....	115
5.1.3.2.2.3.	DOWNLOADING A COPY OF CHANGE DATA .....	116
5.1.3.2.2.4.	COMPARING CHANGE DATA WITH THE AUTHORITATIVE COPY AT THE TIME OF THE CHANGE	117

5.1.3.2.2.4.1.	UNDERSTANDING THE OBJECT GROUP CHANGE TAB FILE COMPARISON RESULTS DIALOG	117
5.1.3.2.2.4.1.1.	UNDERSTANDING THE FILE COMPARISON RESULTS DIALOG INFORMATION DISPLAY AREA AND TAB BROWSER	118
5.1.3.2.2.5.	COMPARING CHANGE DATA WITH THE CURRENT AUTHORITATIVE COPY	119
5.1.3.2.2.5.1.	UNDERSTANDING THE OBJECT GROUP CHANGE TAB FILE COMPARISON RESULTS DIALOG	119
5.1.3.2.2.5.1.1.	UNDERSTANDING THE FILE COMPARISON RESULTS DIALOG INFORMATION DISPLAY AREA AND TAB BROWSER	119
5.1.3.3.	REVIEWING OBJECT GROUP MONITORING INFORMATION	120
5.1.3.4.	REVIEWING OBJECT GROUP DATA PENDING REPAIR	123
5.1.3.4.1.	FILTERING AND SORTING THE PENDING REPAIR TAB	125
5.1.3.5.	OBJECT GROUP GENERATIONS	125
5.1.3.5.1.	DOWNLOADING GENERATION DATA	127
5.1.3.5.2.	VIEWING AND COMPARING CONTENT OF OBJECT GROUP GENERATIONS	127
5.1.3.5.2.1.	UNDERSTANDING THE OBJECT GROUP CHANGE TAB FILE COMPARISON RESULTS DIALOG	129
5.1.3.5.2.1.1.	UNDERSTANDING THE FILE COMPARISON RESULTS DIALOG INFORMATION DISPLAY AREA AND TAB BROWSER	129
5.1.3.5.3.	DEPLOYING “ROLLING BACK” OBJECT GROUP GENERATIONS	130
5.1.3.6.	OBJECT GROUP PERMISSIONS	131
5.1.3.6.1.	MODIFYING AN EXISTING USER/GROUP OBJECT GROUP PERMISSIONS	133
5.1.3.6.2.	ADDING AND REMOVING USERS AND GROUPS TO OBJECT GROUP PERMISSIONS	134
<b>6.</b>	<b>CONFIGURING AND USING THE CimTrak™ NETWORK DEVICE AGENT</b>	<b>136</b>
6.1.	MANAGING THE CimTrak™ NETWORK DEVICE AGENT FROM THE WEB MANAGEMENT CONSOLE	136
6.1.1.	NETWORK DEVICE AGENT PROPERTIES	137
6.1.1.1.	CONFIGURING THE NETWORK DEVICE AGENT DESCRIPTION PROPERTIES	137
6.1.1.2.	CONFIGURING THE NETWORK DEVICE AGENT LOG RETENTION PROPERTIES	138
6.1.1.3.	CONFIGURING THE NETWORK DEVICE AGENT DISCONNECT WARNING	139
6.1.1.4.	CONFIGURING THE NETWORK DEVICE AGENT HEARTBEAT AND STATISTIC GATHERING INTERVAL	140
6.1.1.5.	CREATING AND EDITING OBJECT GROUP WATCH POLICIES	140
6.1.1.5.1.	OBJECT GROUP PROPERTIES	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.1.5.2.	WATCH PROPERTIES	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.1.5.2.1.	CORRECTIVE ACTION	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.1.5.2.2.	AUTHORITATIVE COPY	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.1.5.2.3.	FILE COMPARISON METHOD	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.1.5.2.4.	STORE CHANGES	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.1.5.2.5.	AUTO EXCLUDE	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.1.5.2.6.	OPTIONS	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.1.5.2.7.	EVENT DETECTION METHOD	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.1.5.2.8.	CONNECTION LOSS	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.1.5.3.	TUNING WATCH PROPERTIES	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.1.5.3.1	EXCLUDING AND INCLUDING USING REGULAR EXPRESSIONS	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.1.5.3.1.1.	EXCLUDING FOLDERS USING REGULAR EXPRESSIONS	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.1.5.3.1.2.	EXCLUDING FILES USING REGULAR EXPRESSIONS	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.1.5.3.1.3.	INVERSE EXCLUDING OF FOLDERS USING REGULAR EXPRESSIONS	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.1.5.3.1.4.	INVERSE EXCLUDING OF FILES USING REGULAR EXPRESSIONS	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.1.6.	SAVING OBJECT GROUP WATCH POLICIES TO TEMPLATES	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.1.7.	CREATING OBJECT GROUP WATCH POLICIES USING TEMPLATES	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.1.8.	DELETING OBJECT GROUP WATCH POLICIES	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.1.9.	ENABLING AND DISABLING OBJECT GROUP MONITORING	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.1.10.	SYNCHRONIZING OBJECT GROUP DATA	<b>ERROR! BOOKMARK NOT DEFINED.</b>

6.1.2.	NETWORK DEVICE AGENT INFORMATION DISPLAY .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
1.1.2.1.	AUDITING NETWORK DEVICE AGENT EVENTS .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.2.1.1.	FILTERING AND SORTING THE NETWORK DEVICE AGENT EVENT LOG .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.2.2.	NETWORK DEVICE AGENT PERMISSIONS.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.2.3.	MODIFYING AN EXISTING USER/GROUP NETWORK DEVICE AGENT PERMISSIONS.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.2.4.	ADDING AND REMOVING USERS AND GROUPS TO NETWORK DEVICE AGENT PERMISSIONS .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.	OBJECT GROUP INFORMATION DISPLAY.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.1.	AUDITING OBJECT GROUP EVENTS .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.1.1.	FILTERING AND SORTING THE OBJECT GROUP EVENT LOG .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.2.	REVIEWING OBJECT GROUP MONITORED CHANGES .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.2.1.	FILTERING AND SORTING THE OBJECT GROUP CHANGE LOG .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.2.2.	ACCESSING THE CHANGE LOG TAB CONTEXT MENU .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.2.2.1.	VIEWING CHANGE CONTENT .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.2.2.2.	VIEWING CHANGE FORENSIC DATA .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.2.2.3.	DOWNLOADING A COPY OF CHANGE DATA .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.2.2.4.	COMPARING CHANGE DATA WITH THE AUTHORITATIVE COPY AT THE TIME OF THE CHANGE .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.2.2.4.1.	UNDERSTANDING THE OBJECT GROUP CHANGE TAB FILE COMPARISON RESULTS DIALOG .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.2.2.4.1.1.	UNDERSTANDING THE FILE COMPARISON RESULTS DIALOG INFORMATION DISPLAY AREA AND TAB BROWSER .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.2.2.5.	COMPARING CHANGE DATA WITH THE CURRENT AUTHORITATIVE COPY .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.2.2.5.1.	UNDERSTANDING THE OBJECT GROUP CHANGE TAB FILE COMPARISON RESULTS DIALOG .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.2.2.5.1.1.	UNDERSTANDING THE FILE COMPARISON RESULTS DIALOG INFORMATION DISPLAY AREA AND TAB BROWSER .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.4.	REVIEWING OBJECT GROUP DATA PENDING REPAIR .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.4.1.	FILTERING AND SORTING THE PENDING REPAIR TAB.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.5.	OBJECT GROUP GENERATIONS .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.5.1.	DOWNLOADING GENERATION DATA .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.5.2.	VIEWING AND COMPARING CONTENT OF OBJECT GROUP GENERATIONS ...	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.5.2.1.	UNDERSTANDING THE OBJECT GROUP CHANGE TAB FILE COMPARISON RESULTS DIALOG .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.5.2.1.1.	UNDERSTANDING THE FILE COMPARISON RESULTS DIALOG INFORMATION DISPLAY AREA AND TAB BROWSER .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.5.3.	DEPLOYING “ROLLING BACK” OBJECT GROUP GENERATIONS .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.6.	OBJECT GROUP PERMISSIONS.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.6.1.	MODIFYING AN EXISTING USER/GROUP OBJECT GROUP PERMISSIONS .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.3.6.2.	ADDING AND REMOVING USERS AND GROUPS TO OBJECT GROUP PERMISSIONS.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
7.	USERS AND GROUPS.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
7.1.	MANAGING MASTER REPOSITORY USERS & GROUPS FROM THE MANAGEMENT CONSOLE .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
7.2.	ADDING A NEW USER.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
7.3.	ADDING AN AD/LDAP USER OR ROLE .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
7.4.	EDITING AN EXISTING CIMTrak USER OR ROLE .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
8.	CREATING, APPLYING, AND USING TAGS .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
8.1.	MANAGING TAGS .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
8.2.	ASSOCIATING PRECONFIGURED TAGS .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>

8.3.	CREATING NEW TAGS .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
8.4.	DELETING TAGS .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
<b>9.</b>	<b>CIMTRAK™ INTEGRATED REPORTING.....</b>	<b>ERROR! BOOKMARK NOT DEFINED.</b>
9.1.	ACCESSING CIMTRAK™ REPORTING .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
9.1.1.	NAVIGATING THE AVAILABLE REPORTS DIALOG AND EXECUTING REPORTS .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
	<b>BOOKMARK NOT DEFINED.</b>	
9.1.1.1.	EXPLAINING AVAILABLE CIMTRAK™ REPORTS .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
9.2.	WORKING WITH CIMTRAK™ REPORT PACKAGES.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
9.3.	UPLOADING ADDITIONAL CIMTRAK™ REPORTS .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
<b>10.</b>	<b>DISPLAYING MULTIPLE REPOSITORIES IN ONE WINDOW.....</b>	<b>ERROR! BOOKMARK NOT DEFINED.</b>
10.1.	ACQUIRING ACCESS TO AN ADDITIONAL REPOSITORY.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
10.1.1.	CREATE AN API KEY ON THE REMOTE REPOSITORY..	<b>ERROR! BOOKMARK NOT DEFINED.</b>
10.1.2.	ADD THE API KEY TO THE LOCAL REPOSITORY .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
10.1.3.	CONFIGURING THE MULTI-REPOSITORY DISPLAY .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
<b>11.</b>	<b>APPENDIX A: DOCUMENT VERSIONING.....</b>	<b>ERROR! BOOKMARK NOT DEFINED.</b>
6.1.5.3.1.	OBJECT GROUP PROPERTIES .....	227
6.1.5.3.2.	WATCH PROPERTIES.....	232
6.1.1.5.2.1.	CORRECTIVE ACTION.....	233
6.1.1.5.2.2.	AUTHORITATIVE COPY .....	234
6.1.1.5.2.3.	FILE COMPARISON METHOD .....	235
6.1.1.5.2.4.	STORE CHANGES .....	235
6.1.1.5.2.5.	AUTO EXCLUDE.....	236
6.1.1.5.2.6.	OPTIONS.....	236
6.1.1.5.2.7.	EVENT DETECTION METHOD .....	237
6.1.1.5.2.8.	CONNECTION LOSS .....	238
6.1.5.3.3.	TUNING WATCH PROPERTIES .....	239
6.1.1.5.3.1	EXCLUDING AND INCLUDING USING REGULAR EXPRESSIONS .....	241
6.1.1.5.3.1.1.	EXCLUDING FOLDERS USING REGULAR EXPRESSIONS .....	241
6.1.1.5.3.1.2.	EXCLUDING FILES USING REGULAR EXPRESSIONS.....	242
6.1.1.5.3.1.3.	INVERSE EXCLUDING OF FOLDERS USING REGULAR EXPRESSIONS.....	243
6.1.1.5.3.1.4.	INVERSE EXCLUDING OF FILES USING REGULAR EXPRESSIONS .....	244
6.1.5.4.	SAVING OBJECT GROUP WATCH POLICIES TO TEMPLATES .....	245
6.1.5.5.	CREATING OBJECT GROUP WATCH POLICIES USING TEMPLATES .....	245
6.1.5.6.	DELETING OBJECT GROUP WATCH POLICIES .....	246
6.1.5.7.	ENABLING AND DISABLING OBJECT GROUP MONITORING .....	247
6.1.5.8.	SYNCHRONIZING OBJECT GROUP DATA .....	249
6.1.4.	NETWORK DEVICE AGENT INFORMATION DISPLAY .....	250
1.1.2.2.	AUDITING NETWORK DEVICE AGENT EVENTS .....	250
6.1.2.1.1.	FILTERING AND SORTING THE NETWORK DEVICE AGENT EVENT LOG .....	252
6.1.2.2.	NETWORK DEVICE AGENT PERMISSIONS.....	252
6.1.2.3.	MODIFYING AN EXISTING USER/GROUP NETWORK DEVICE AGENT PERMISSIONS.....	254
6.1.2.4.	ADDING AND REMOVING USERS AND GROUPS TO NETWORK DEVICE AGENT PERMISSIONS .....	255
6.1.5.	OBJECT GROUP INFORMATION DISPLAY.....	256
6.1.3.1.	AUDITING OBJECT GROUP EVENTS .....	257
6.1.3.1.1.	FILTERING AND SORTING THE OBJECT GROUP EVENT LOG.....	259
6.1.3.2.	REVIEWING OBJECT GROUP MONITORED CHANGES .....	259
6.1.3.2.1.	FILTERING AND SORTING THE OBJECT GROUP CHANGE LOG .....	261
6.1.3.2.2.	ACCESSING THE CHANGE LOG TAB CONTEXT MENU .....	261
6.1.3.2.2.1.	VIEWING CHANGE CONTENT .....	261
6.1.6.2.2.2.	VIEWING CHANGE FORENSIC DATA .....	262
6.1.3.2.2.3.	DOWNLOADING A COPY OF CHANGE DATA .....	263
6.1.3.2.2.4.	COMPARING CHANGE DATA WITH THE AUTHORITATIVE COPY AT THE TIME OF THE CHANGE	264
6.1.3.2.2.4.1.	UNDERSTANDING THE OBJECT GROUP CHANGE TAB FILE COMPARISON RESULTS DIALOG	264
6.1.3.2.2.4.1.1.	UNDERSTANDING THE FILE COMPARISON RESULTS DIALOG INFORMATION DISPLAY AREA AND TAB BROWSER .....	265

6.1.3.2.2.5.	COMPARING CHANGE DATA WITH THE CURRENT AUTHORITATIVE COPY .....	265
6.1.3.2.2.5.1.	UNDERSTANDING THE OBJECT GROUP CHANGE TAB FILE COMPARISON RESULTS DIALOG .....	266
6.1.3.2.2.5.1.1.	UNDERSTANDING THE FILE COMPARISON RESULTS DIALOG INFORMATION DISPLAY AREA AND TAB BROWSER.....	267
6.1.3.4.	REVIEWING OBJECT GROUP DATA PENDING REPAIR .....	270
6.1.3.4.1.	FILTERING AND SORTING THE PENDING REPAIR TAB.....	272
6.1.3.5.	OBJECT GROUP GENERATIONS .....	272
6.1.3.5.1.	DOWNLOADING GENERATION DATA .....	274
6.1.3.5.2.	VUEWING AND COMPARING CONTENT OF OBJECT GROUP GENERATIONS .....	274
6.1.3.5.2.1.	UNDERSTANDING THE OBJECT GROUP CHANGE TAB FILE COMPARISON RESULTS DIALOG .....	277
6.1.3.5.2.1.1.	UNDERSTANDING THE FILE COMPARISON RESULTS DIALOG INFORMATION DISPLAY AREA AND TAB BROWSER .....	277
6.1.3.5.3.	DEPLOYING “ROLLING BACK” OBJECT GROUP GENERATIONS .....	278
6.1.3.6.	OBJECT GROUP PERMISSIONS.....	279
6.1.3.6.1.	MODIFYING AN EXISTING USER/GROUP OBJECT GROUP PERMISSIONS .....	281
6.1.3.6.2.	ADDING AND REMOVING USERS AND GROUPS TO OBJECT GROUP PERMISSIONS.....	282
<b>7.</b>	<b>USERS AND GROUPS.....</b>	<b>284</b>
9.1.	MANAGING MASTER REPOSITORY USERS & GROUPS FROM THE MANAGEMENT CONSOLE .....	284
9.2.	ADDING A NEW USER.....	285
9.3.	ADDING AN AD/LDAP USER OR ROLE .....	286
9.4.	EDITING AN EXISTING CIMTrak USER OR ROLE .....	287
<b>8.</b>	<b>CREATING, APPLYING, AND USING TAGS.....</b>	<b>288</b>
11.1.	MANAGING TAGS.....	288
11.2.	ASSOCIATING PRECONFIGURED TAGS .....	289
11.3.	CREATING NEW TAGS .....	291
8.4.	DELETING TAGS .....	294
<b>9.</b>	<b>CIMTrak™ INTEGRATED REPORTING.....</b>	<b>297</b>
9.4.	ACCESSING CIMTrak™ REPORTING .....	297
9.1.2.	NAVIGATING THE AVAILABLE REPORTS DIALOG AND EXECUTING REPORTS .....	298
9.1.2.1.	EXPLAINING AVAILABLE CIMTrak™ REPORTS .....	303
9.5.	WORKING WITH CIMTrak™ REPORT PACKAGES.....	304
9.6.	UPLOADING ADDITIONAL CIMTrak™ REPORTS .....	306
<b>10.</b>	<b>DISPLAYING MULTIPLE REPOSITORIES IN ONE WINDOW.....</b>	<b>308</b>
10.2.	ACQUIRING ACCESS TO AN ADDITIONAL REPOSITORY.....	308
10.2.1.	CREATE AN API KEY ON THE REMOTE REPOSITORY.....	308
10.2.2.	ADD THE API KEY TO THE LOCAL REPOSITORY .....	309
10.2.3.	CONFIGURING THE MULTI-REPOSITORY DISPLAY .....	310
<b>11.</b>	<b>APPENDIX A: DOCUMENT VERSIONING.....</b>	<b>313</b>
<b>12.</b>	<b>APPENDIX B: FILE SYSTEM AGENT OBJECT GROUP WORKSHEET.....</b>	<b>314</b>
<b>13.</b>	<b>APPENDIX C: NETWORK DEVICE AGENT OBJECT GROUP WORKSHEET .....</b>	<b>315</b>
<b>14.</b>	<b>APPENDIX D: MESSAGE LEVELS AND EXAMPLES .....</b>	<b>316</b>
<b>15.</b>	<b>APPENDIX E: SUPPORT CONTACT INFORMATION.....</b>	<b>319</b>



***This page is intentionally left blank.***

Table 1: Template Environment Variables .....	70
Table 2: Network Device Communication and File Transfer Protocols.....	140
Table 3: Document Versioning.....	227
Table 4: Common Log Messages .....	232

Figure 1: Cimtrak™ Architecture .....	18
Figure 2: CimTrak™ Web Management Console Login Screen.....	19
Figure 3: CimTrak™ Management Console Login Dialog .....	20
Figure 4: CimTrak™ Management Console Login Error.....	20
Figure 5: CimTrak™ Management Console Dashboard .....	21
Figure 6: Object Group Tree Showing Master Repository and Associated CimTrak™ Areas .....	22
Figure 7: CimTrak™ Web Management Console Dashboard.....	22
Figure 8: Object Group Tree Showing Master Repository and Associated CimTrak™ Areas .....	23
Figure 9: CimTrak™ Web Management Console Information Display Area (Master Repository Level).....	24
Figure 10: Cimtrak™ Web Management Console Help dialog screen .....	25
Figure 11: Cimtrak™ Web Management Console Legal Notices dialog screen.....	26
Figure 12: CimTrak™ End User License Agreement .....	27
Figure 13: CimTrak™ Master Repository Properties.....	29
Figure 14: CimTrak™ Master Repository Properties Dialog (Logging Tab) .....	30
Figure 15: CimTrak™ Master Repository Repository Properties Dialog (Repository Settings Tab) .....	35
Figure 16: Permissions for Object Dialog .....	39
Figure 17: Email settings for Object Dialog .....	41
Figure 18: CimTrak™ Master Repository Properties Dialog (Password Policies Tab) ....	43
Figure 19: CimTrak™ Master Repository Properties Dialog (Communication Tab) .....	45
Figure 20: CimTrak™ Master Repository Properties Dialog (Logon Banner Tab) .....	46
Figure 21: CimTrak™ Logon Banner.....	47
Figure 22: Cimtrak™ Master Repository Properties Dialog (AD/LDAP Tab) .....	49
Figure 23: Add AD/LDAP Server Dialog .....	50
Figure 24: Add AD/LDAP Server Error .....	50
Figure 25: Cimtrak™ Master Repository User Maintenance Dialog .....	52
Figure 26: Cimtrak™ Master Repository User Add/Edit Dialog .....	52

Figure 27: CimTrak™ Web Management Console Information Display Area (Master Repository Level).....	53
Figure 28: Cimtrak™ Master Repository Event Log Tab .....	55
Figure 29: Cimtrak™ Master Repository Event Log (Sorted) .....	56
Figure 30: Cimtrak™ Master Repository Logged On Users Tab.....	57
Figure 31: Area dialog .....	58
Figure 32: Object Group Tree showing Area .....	58
Figure 33: Confirm Delete dialog .....	59
Figure 34: Area dialog .....	59
Figure 35: Area Security Permissions dialog.....	61
Figure 36: Add Users dialog .....	63
Figure 37: Area Event Log .....	65
Figure 38: Template Maintenance .....	67
Figure 39: Template Open dialog .....	69
Figure 40: CimTrak™ File System Agent in Object Group Tree.....	72
Figure 41: Cimtrak™ File Sytem Agent Connection Icon .....	72
Figure 42: CimTrak™ Agent Configuration .....	73
Figure 43: File System Agent Description.....	74
Figure 44: Number of Events to Keep settings .....	74
Figure 45: CimTrak™ Agent DB Options settings .....	75
Figure 46: File System Agent Throttling settings.....	76
Figure 47: CimTrak™ Web Management Console's Object Group Tree Showing Object Groups.....	77
Figure 48: Cimtrak™ Object Group Properties Dialog (Attributes Tab) .....	78
Figure 49: File System Agent Object Information .....	78
Figure 50: File System Agent Monitoring Information.....	79
Figure 51: Microsoft Windows Operating System Tree.....	80
Figure 52: Watch notifications.....	80
Figure 53: Watch Properties dialog .....	83
Figure 54: Watch Properties section showing monitored directory.....	84
Figure 55: Corrective Action Properties .....	85
Figure 56: Authoritative Copy Parameter Settings .....	85
Figure 57: File Comparison Method Parameter Settings.....	86
Figure 58: Store Changes Option Checkbox .....	86
Figure 59: Auto Exclude parameter settings.....	87
Figure 60: Options parameter settings .....	87
Figure 61: Log Reads Parameter Checkbox .....	87
Figure 62: Event Detection Method parameter settings .....	88
Figure 63: Connection Loss parameter settings.....	89
Figure 64: Watch Properties section showing monitored data .....	90
Figure 65: Add Regular Expression Exclude dialog.....	91
Figure 66: Regular Expression Folder Exclude .....	92
Figure 67: Regular Expression File Exclude .....	93
Figure 68: Regular Expression Folder Exclude (blue text) .....	94
Figure 69: Regular Expression File Exclude .....	95
Figure 70: Save to Template dialog .....	95

Figure 71: Select Template dialog .....	97
Figure 72: Confirm Delete dialog .....	98
Figure 73: Object Group Lock Process (Event Log) .....	99
Figure 74: Object Group Unlock Process (Event Log).....	100
Figure 75: Object Group Synchronization Process (Event Log) .....	100
Figure 76: File System Agent Information Display Area (Agent Settings Tab Selected).....	101
Figure 77: File System Agent Event Log .....	102
Figure 78: File System Agent Security Permissions dialog.....	104
Figure 79: Add Users dialog .....	106
Figure 80: Object Group Information Display Area.....	107
Figure 81: Object Group Change Log .....	110
Figure 82: File View dialog .....	112
Figure 83: Forensic Data dialog.....	113
Figure 84: File Comparison Results .....	114
Figure 85: File Comparison Results dialog Changes tab.....	115
Figure 86: File Comparison Results .....	116
Figure 87: File Comparison Results dialog Changes tab.....	117
Figure 88: Object Group Monitor Info tab .....	118
Figure 89: Monitor Info Status Window tab.....	120
Figure 90: Monitor Info Summary Window tab .....	120
Figure 91: Monitor Info Details tab .....	120
Figure 92: Pending Repair tab showing 3 pending repairs .....	121
Figure 93: Object Group Generation Tab .....	123
Figure 94: File View dialog (non-binary).....	125
Figure 95: File to Compare Against dialog.....	126
Figure 96: File Comparison Results dialog .....	127
Figure 97: File Comparison Results dialog Changes tab.....	128
Figure 98: Confirm Deploy dialog.....	129
Figure 99: Notes dialog.....	129
Figure 100: Object Group Security Permissions dialog .....	130
Figure 101: Add Users dialog .....	133
Figure 102: CimTrak™ Network Device Agent in Object Group Tree .....	134
Figure 103: Cimtrak™ File Sytem Agent Connection Icon .....	134
Figure 104: CimTrak™ Agent Configuration .....	135
Figure 105: Network Device Agent Description .....	136
Figure 106: Number of Events to Keep settings .....	136
Figure 107: CimTrak™ Agent DB Options settings .....	137
Figure 108: Network Device Agent Throttling settings .....	138
Figure 109: New Network Device dialog .....	139
Figure 110: CimTrak™ Web Management Console's Object Group Tree Showing Object Groups.....	140
Figure 111: Cimtrak™ Network Device Object Group Properties (Attributes Tab).....	141
Figure 112: Network Device Agent Object Information .....	142
Figure 113: Network Device Agent Monitoring Information.....	143
Figure 114: Cisco IOS Operating System Tree .....	143
Figure 115: Watch notifications.....	143

Figure 116: Watch Properties dialog .....	146
Figure 117: Watch Properties section showing monitored directory.....	147
Figure 118: Corrective Action Properties .....	148
Figure 119: Authoritative Copy Parameter Settings.....	148
Figure 120: File Comparison Method Parameter Settings.....	149
Figure 121: Store Changes Option Checkbox .....	149
Figure 122: Auto Exclude parameter settings.....	150
Figure 123: Options parameter settings .....	150
Figure 124: Log Reads Parameter Checkbox .....	150
Figure 125: Event Detection Method parameter settings .....	151
Figure 126: Connection Loss parameter settings.....	152
Figure 127: Watch Properties section showing monitored data .....	153
Figure 128: Add Regular Expression Exclude dialog.....	154
Figure 129: Regular Expression Folder Exclude.....	155
Figure 130: Regular Expression File Exclude .....	156
Figure 131: Regular Expression Folder Exclude (blue text) .....	157
Figure 132: Regular Expression File Exclude .....	158
Figure 133: Save to Template dialog .....	158
Figure 134: Select Template dialog .....	160
Figure 135: Confirm Delete dialog .....	161
Figure 136: Object Group Lock Process (Event Log) .....	162
Figure 137: Object Group Unlock Process (Event Log).....	163
Figure 138: Object Group Synchronization Process (Event Log) .....	163
Figure 139: Network Device Agent Information Display Area (Agent Settings Tab Selected).....	164
Figure 140: Network Device Agent Event Log .....	165
Figure 141: Network Device Agent Security Permissions dialog .....	167
Figure 142: Add Users dialog .....	170
Figure 143: Object Group Information Display Area.....	171
Figure 144: Object Group Change Log .....	174
Figure 145: File View dialog .....	176
Figure 146: Forensic Data dialog.....	177
Figure 147: File Comparison Results .....	178
Figure 148: File Comparison Results dialog Changes tab.....	179
Figure 149: File Comparison Results .....	180
Figure 150: File Comparison Results dialog Changes tab.....	181
Figure 151: Object Group Monitor Info tab .....	182
Figure 152: Monitor Info Status Window tab.....	184
Figure 153: Monitor Info Summary Window tab .....	184
Figure 154: Monitor Info Details tab.....	184
Figure 155: Pending Repair tab showing 3 pending repairs .....	185
Figure 156: Object Group Generation Tab .....	187
Figure 157: File View dialog (non-binary).....	189
Figure 158: File to Compare Against dialog.....	190
Figure 159: File Comparison Results dialog .....	191
Figure 160: File Comparison Results dialog Changes tab.....	192

Figure 161: Confirm Deploy dialog.....	193
Figure 162: Notes dialog.....	193
Figure 163: Object Group Security Permissions dialog .....	194
Figure 164: Add Users dialog.....	197
Figure 165: User Maintenance Dialog.....	198
Figure 166: User Add/Edit dialog.....	199
Figure 167: Add CimTrak™ Role to AD/LDAP Group or User Dialog.....	201
Figure 168: Object Tag Assignment Dialog .....	202
Figure 169: Select Tags dialog screen .....	203
Figure 170: Select Tag dialog screen (tag selected) .....	204
Figure 171: Object Tag Assignments dialog screen (new tag assigned) .....	205
Figure 172: Select Tags dialog screen .....	206
Figure 173: Create/Edit Tag dialog screen .....	207
Figure 174: Create/Edit Tag dialog screen .....	207
Figure 175: Select Tags dialog screen (new tag).....	208
Figure 176: Object Tag Assignments dialog screen (new tag assigned) .....	209
Figure 177: Object Tag Assignment dialog screen (tag deleted).....	210
Figure 178: Available Reports dialog (Master Repository Level).....	213
Figure 179: Report Parameters dialog .....	214
Figure 180: Sample CimTrak™ Report (Page 1 of 2).....	215
Figure 181: Sample CimTrak™ Report (Page 2 of 2).....	216
Figure 182: Report Packages dialog .....	219
Figure 183: Report File Maintenance dialog screen .....	221
Figure 184: Add Repository API Key dialog .....	222
Figure 185: The generated API Key .....	222
Figure 186: Add Repository API Key to Cluster dialog.....	223
Figure 187: Cluster Settings Tab with API key added .....	223
Figure 188: Object tree after adding remote repository.....	224
Figure 189: Multi-repository view options .....	224
Figure 190: Operating System View Option .....	225
Figure 191: IP Range View Option .....	226
Figure 192: Tags View Option .....	226

## 1. Introduction

### 1.1. DOCUMENTATION PURPOSE AND CONVENTIONS

The purpose of this documentation is to provide user guidance to users and administrators of the CimTrak™ Integrity & Compliance Suite. Conformance with this guidance documentation is intended to result in deployment and configuration of the CimTrak™ product consistent with CIMCOR™ recommended best practices.

This guidance document is comprised of sections detailing the configuration options associated with each CimTrak™ component. Additional components, not described in this documentation, may also exist in your region. Contact an authorized CimTrak™ sales representative for more information.



***Occasionally additional notes are relevant to the component being described. These notes are indicated by the “i” information symbol.***

### 1.2. CIMCOR™ CIMTRAK™ INTEGRITY & COMPLIANCE SUITE INTRODUCTION

The CIMCOR™ CimTrak™ Integrity & Compliance Suite application provides a flexible file-based security solution that allows Administrators the capability to protect selected files, operating system components, and network device configurations against unauthorized changes from a centralized location within the network. CimTrak™ immediately identifies the change, determines if it is authorized and then institutes corrective action based on the application configuration. Since CimTrak™ maintains a master set of protected files, unauthorized changes can immediately be reversed to mitigate malicious activity or human error.

CimTrak™ is comprised of a multi-component architecture. The primary CimTrak™ components consist of the Master Repository, Web Management Console, and File System Agent. Additional (optional) CimTrak™ components may be attached to the primary configuration to enhance file and configuration monitoring and remediation.

The CimTrak™ Integrity Suite presents a multifaceted approach to protecting key information system resources and provides comprehensive change control tracking. The application consists of three primary components:

- ❖ CimTrak™ Master Repository
- ❖ CimTrak™ Web Management Console
- ❖ CimTrak™ File System Agent

Additionally the CimTrak™ Integrity Suite has a combination of multiple (optional) components including:

- ❖ CimTrak™ Network Device Agent
- ❖ CimTrak™ Tools

These required and optional components will be discussed in subsequent sections of the documentation.



***Additional CimTrak™ optional components may exist based on your region. Please contact an authorized CimTrak™ sales representative for details.***

### **1.3. CIMTRAK™ MASTER REPOSITORY**

The CimTrak™ Master Repository component maintains a centralized store of protected files and change history within a centralized server. This store provides an isolated, compressed, and encrypted copy of critical files that allows for restoration in the event of unauthorized change and provides a basis for identifying changes made to protected files and configurations within the network. Additionally, the application supports a rollback capability which allows previous versions of a protected file or configuration to be restored at a later date.

### **1.4. CIMTRAK™ WEB MANAGEMENT CONSOLE**

The CimTrak™ Integrity Suite includes a Web Management Console which features a Graphic User Interface (GUI) that allows Administrators the capability to manage and configure the application from a separate Administrator management workstation within the network. The Web Management Console supports the selection of files and configurations on attached components to “lock” and configure an action to take in the event a change is detected. The Web Management Console provides access to a series of reports that detail changes made based on a series of saved baselines stored in the Master Repository. This capability can be used to superimpose changes over the stored baselines to immediately identify what aspects of the “locked” file were changed.

### **1.5. CIMTRAK™ FILE SYSTEM AGENT**

The CimTrak™ File System Agent is installed on protected resources within the Operational Environment. The File System Agent provides real-time or poll based monitoring of protected files and configurations and identifies changes made to protected files. When a change is detected, the File System Agent communicates with the CimTrak™ Master Repository to report change status and (when configured) transfer the master file (Authoritative Copy) from the Master Repository to the File System Agent server to overwrite unauthorized changes. The File System Agent utilizes CimTrak™ configuration data to determine if the change is allowed based on Administrator policy settings for the subject file or configuration. The File System Agent can then institute one of the



following actions on the change: Allow the change and log the event, update the master file baseline stored within the Master Repository, disallow the change and immediately overwrite the change with the master file copy from the Master Repository, or Prompt the authorized user to either allow or disallow the file change attempt. Additionally the CimTrak™ File System Agent can be configured to allow a combination of remediation settings.

In addition to file change detection and remediation, the File System Agent provides configuration monitoring remediation.<sup>1</sup> Windows™ file system configuration monitoring includes:

- ❖ Read Access monitoring
- ❖ Monitoring and remediation of the Windows™ Registry
- ❖ Monitoring of Windows™ Local User accounts
- ❖ Monitoring of Windows™ Local Groups
- ❖ Monitoring of Windows™ Local Security Policy settings
- ❖ Monitoring of Windows™ Local Services
- ❖ Monitoring of Windows™ Local Device Drivers
- ❖ Monitoring of Windows™ Local Installed Software
- ❖ Monitoring of Windows™ Network Share Settings

#### **1.6. CIMTRAK™ NETWORK DEVICE AGENT**

The CimTrak™ Network Device Agent component is installed on device monitoring resources within the Operational Environment. The CimTrak™ Network Device Agent provides real-time (SNMPv3) or poll based (SSHv1, SSHv2, Telnet) monitoring of protected files and identifies changes made to protected files. When a change is detected, the CimTrak™ File System Agent communicates with the CimTrak™ Master Repository to report change status and/or transfer the master file (authoritative copy) from the Master Repository to the Agent Network Host server to overwrite unauthorized changes. The CimTrak™ Network Device Agent utilizes CimTrak™ configuration data to determine if the change is allowed based on Administrator policy settings for the subject file. The Agent can then institute one of the following actions on the change: Allow the change and log the event, Update the master file baseline stored within the Master Repository, Disallow the change and immediately overwrite the change with the master file copy from the Master Repository, or Prompt the authorized user to either allow or disallow the file change attempt.

---

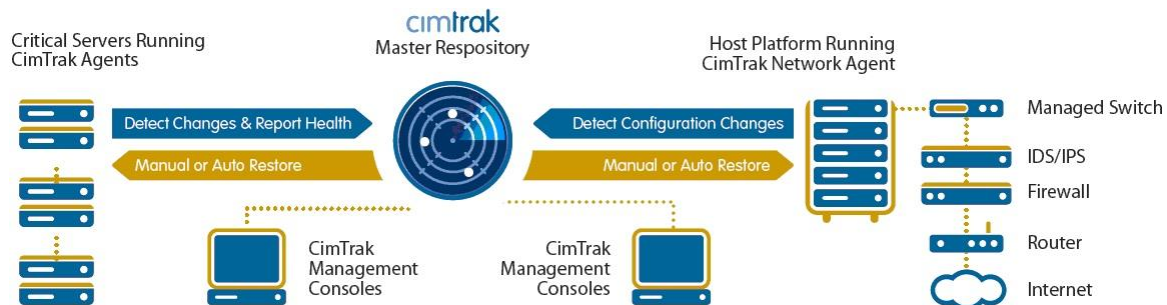
<sup>1</sup> Monitoring of the Windows® registry allows for remediation when changes are detected. All other configuration monitoring features only provide monitoring capabilities.

## 2. Configuration Prerequisites

### 2.1. PREREQUISITE OVERVIEW

Prior to configuring CimTrak™ to monitor and remediate critical system files and configurations it is necessary to install the base CimTrak™ components. Please refer to the CimTrak™ Installation Guidance for additional information on installing CimTrak™ components.

Generally, the CimTrak™ Master Repository is installed on a dedicated server operating system. The CimTrak™ Web Management Console connects remotely to the Master Repository to configure watch policies, view event data, and manage the CimTrak™ application. File System Agents are deployed on critical servers and workstations that require monitoring and remediation. Network Device Agents are deployed on select servers with a logical network connection to organization network devices. A single deployment may have many Master Repositories, Web Management Consoles, File System Agents, and Network Device Agents. It is important to note that a single Web Management Console can manage multiple Master Repositories.



**Figure 1: Cimtrak™ Architecture**

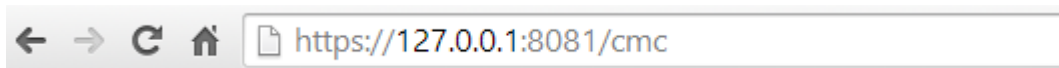
Once all components are installed and communication between the components is established, it is necessary to configure the CimTrak™ Web Management Console to operate with your CimTrak™ Master Repository.

### 3.1. CONNECTING TO THE CIMTRAK™ WEB MANAGEMENT CONSOLE

The Cimtrak™ Web Management Console is hosted from the App Server and can be reached by accessing the server's alternate HTTP port (port 8080) followed by the abbreviation "cmc" (Cimtrak™ Web Management Console) through an internet browser.

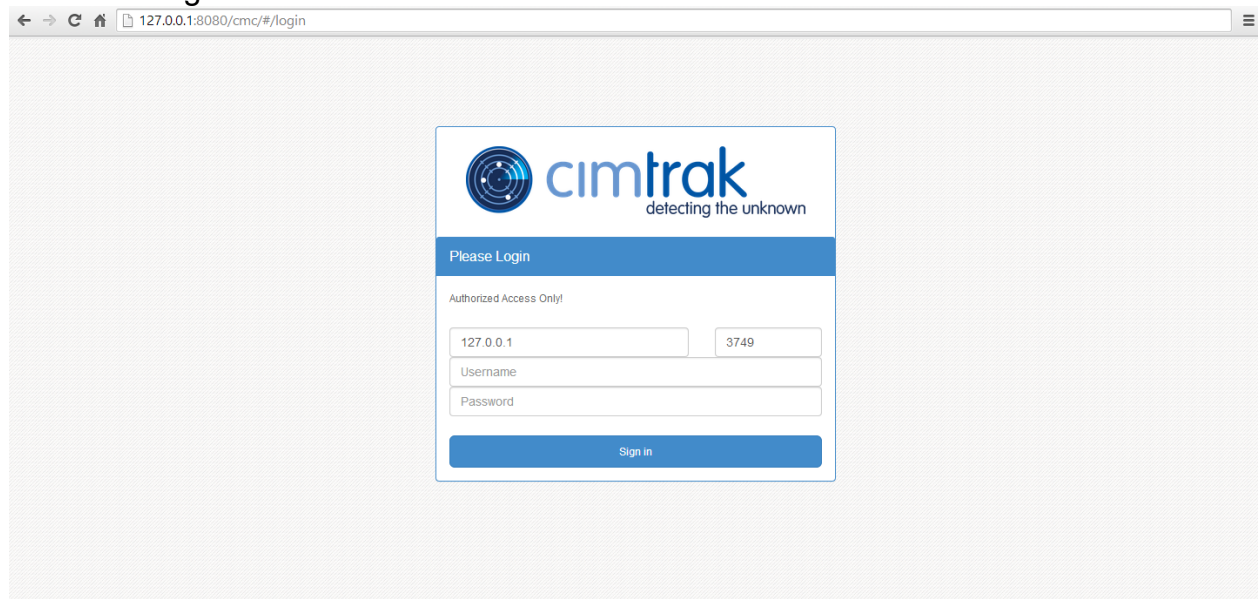


It is suggested that you use the secure HTTPS (port 8081) connection by entering:




***Note: The "loopback": 127.0.0.1; can only be used from the client machine hosting the CimTrak™ App Server. In order to connect to the running CimTrak™ App Server from another machine, please enter the IPv4 address for the machine that the CimTrak App Server is running from.***

You will then be automatically redirected to the Cimtrak™ Web Management Console's login screen.



**Figure 2: CimTrak™ Web Management Console Login Screen**

In order to login to the CimTrak™ Web Management Console, a valid Username and Password is required, as well as the IPv4 address of the Cimtrak™ Master Repository or the Fully Qualified Domain Name (FQDN) of the CimTrak™ Master Repository that you wish to connect to. The port number which you wish to connect to the CimTrak™ Master Repository through is also required.



Please Login

Authorized Users Only

CimTrak Repository IP or FQDN

Port Number

Username

Password

Sign in

Figure 3: CimTrak™ Management Console Login Dialog



***By knowing the IPv4 address, port number, and a valid username and password for a specific CimTrak™ Master Repository, you can connect to that CimTrak™ Master Repository from any other App Server's login screen.***

Entry of an invalid username and/or password for the specified CimTrak™ Master Repository will result in an Authentication Error and the user will be denied access to the CimTrak™ Web Management Console.

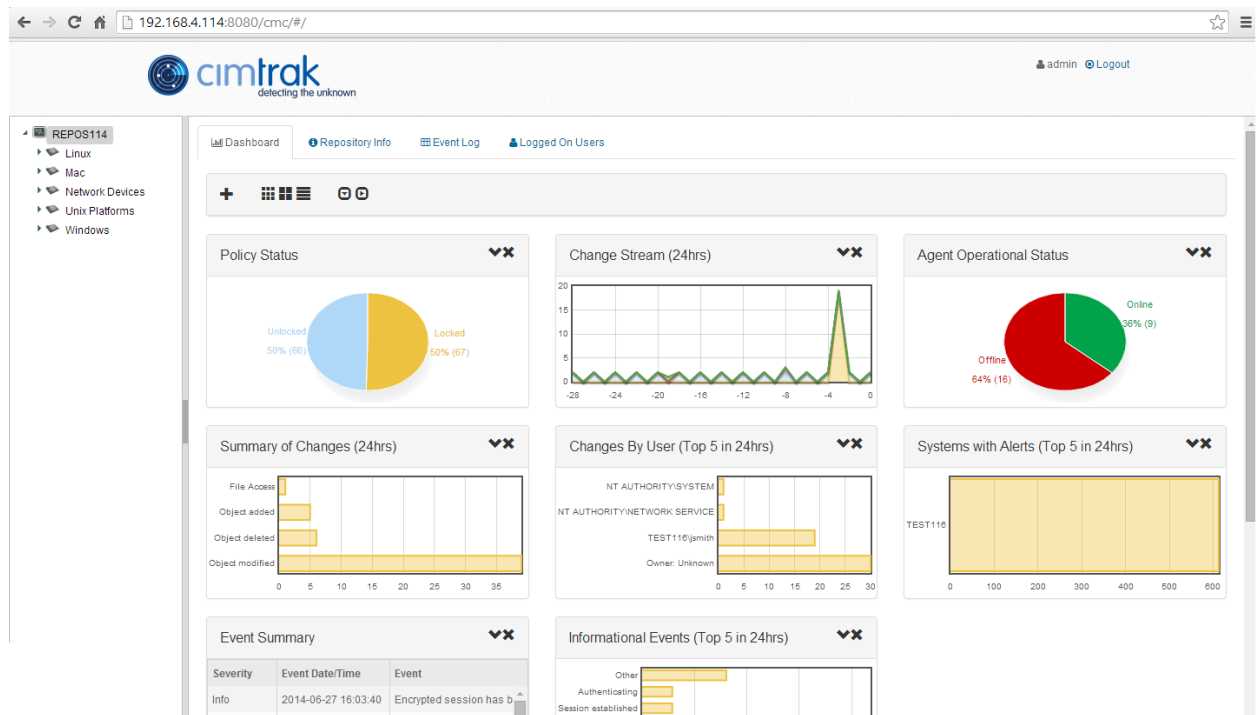
## Authentication Error

Login Error: Invalid Username or Password

OK

**Figure 4: CimTrak™ Management Console Login Error**

Entering valid credentials will result in a connection with the desired CimTrak™ Master Repository and will allow you to continue into the dashboard of the CimTrak™ Web Management Console.



**Figure 5: CimTrak™ Management Console Dashboard**

### 3.1. NAVIGATING THE CIMTRAK™ WEB MANAGEMENT CONSOLE

The CimTrak™ Web Management Console graphical interface is comprised of two primary sections:

- Object Group Tree
- Information Display Area.

Each primary section has specific uses or functions in configuring, maintaining and reviewing the functionality of the CimTrak™ Integrity and Compliance Suite.

### 3.1.1. UNDERSTANDING THE WEB MANAGEMENT CONSOLE OBJECT GROUP TREE

The Object Group tree is a hierarchical view of all CimTrak™ Master Repositories, associated nodes, and Object Group policies. Data contained in the Object Group Tree can be expanded or collapsed by clicking the corresponding ► or ◀ symbol.



Figure 6: Object Group Tree Showing Master Repository and Associated CimTrak™ Areas

Each Object Group Component existing in the Object Group tree has an associated right-click context menu. The associated context menu content changes dynamically with the Object Group Component type. The different context menus will be discussed in the sections corresponding with each Object Group Component type.

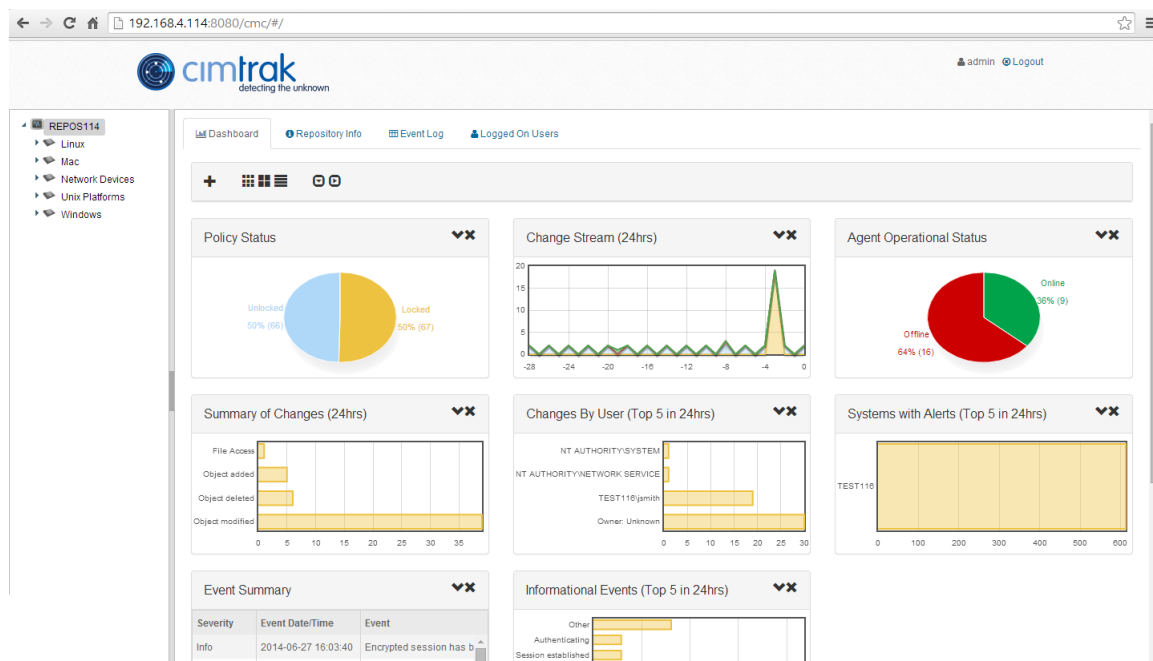


Figure 7: CimTrak™ Web Management Console Dashboard

Each primary section has specific uses or functions in configuring, maintaining and reviewing the functionality of the CimTrak™ Integrity and Compliance Suite.

### 3.1.2. UNDERSTANDING THE WEB MANAGEMENT CONSOLE OBJECT GROUP TREE

The Object Group tree is a hierarchical view of all CimTrak™ Master Repositories, associated nodes, and Object Group policies. Data contained in the Object Group Tree can be expanded or collapsed by clicking the corresponding ► or ◄ symbol.



**Figure 8: Object Group Tree Showing Master Repository and Associated CimTrak™ Areas**

Each Object Group Component existing in the Object Group tree has an associated right-click context menu. The associated context menu content changes dynamically with the Object Group Component type. The different context menus will be discussed in the sections corresponding with each Object Group Component type.

### 3.1.3. UNDERSTANDING THE WEB MANAGEMENT CONSOLE INFORMATION DISPLAY AREA

The Information Display Area displays information for the selected CimTrak™ Object Group Component. The information displayed is often broken up into several tabbed viewing areas. The available tab viewing areas, content, and capabilities vary depending on the Object Group Component type selected. The capabilities of this section will be explained in the sections corresponding with each Object Group Component type.

<div> Dashboard Repository Info Event Log Logged On Users </div>					
Version: 2.0.6.18 Build 7725					
Operating System: Windows Longhorn Service Pack 1 Build 7601					
System Uptime: 5/30/2014 03:38:44 (a month ago)					
Repository Uptime: 6/18/2014 10:50:08 (9 days ago)					
Port: 3749					
Storage Path: E:\Program Files (x86)\Cimcor\CimTrak\CimTrakServer\Storage\					
Agent Connections: 9      Mgmt Console Connections: 1      Total Connections: 12					
Serial Numbers	Agents	Objects	Eval Days	Eval Days Left	+ Add Serial Number
ADCP0819472831000003E8007057	0	10	N/A	N/A	✖ Delete
	Total: 0	Total: 10			
	Used: 0	Used: 3			
CTCP08760364440032044200A241	50	50	N/A	N/A	✖ Delete
	Total: 50	Total: 50			
	Used: 7	Used: 5			
CTCP08760364440032044200A241	50	50	N/A	N/A	✖ Delete
	Total: 50	Total: 50			
	Used: 7	Used: 5			
DBCP0819472932000003E8007053	0	10	N/A	N/A	✖ Delete
	Total: 0	Total: 10			
	Used: 0	Used: 4			

**Figure 9: CimTrak™ Web Management Console Information Display Area (Master Repository Level)**

**3.2. CIMTRAK™ WEB MANAGEMENT CONSOLE: HELP**

The CimTrak™ Web Management Console Help option provides valuable information relating to the CimTrak™ deployment.

The CimTrak™ Help menu can be accessed by clicking the question mark icon “?” in the lower right corner of the CimTrak™ Web Management Console. The Help dialog will show.



Help



E-mail

For technical support, please contact our support group at: [support@cimcor.com](mailto:support@cimcor.com)

Call

For technical support, please contact our support group at: 1-877-424-6267

Licensing

Legal

Close

**Figure 10: Cimtrak™ Web Management Console Help dialog screen**

### 3.3. LEGAL NOTICES

Information relating to CimTrak™ Legal Notices can be accessed by clicking the question mark icon “?” in the lower right corner of the CimTrak™ Web Management Console, followed by clicking the Legal button on the lower left corner or the CimTrak™ Web Management Console Help dialog screen. The Legal Notices dialog will show.



Figure 11: Cimtrak™ Web Management Console Legal Notices dialog screen

3.3.1.            **END USER LICENSE AGREEMENT (EULA)**

Information relating to the CimTrak™ End User License Agreement (EULA) can be accessed by clicking clicking the question mark icon “?” in the lower right corner of the CimTrak™ Web Management Console, followed by clicking the Licensing button on the lower left corner or the Cimtrak™ Web Management Console Help dialog screen. The Licensing dialog will show.

## Licensing



CimTrak Integrity and Compliance Suite End-user License Agreement (EULA)

### 1. GRANT OF LICENSE

1.1 In consideration of payment of the License fee, Cimcor, as Licensor, grants you, the Licensee, a nonexclusive right to use a copy of any of the binaries and other components that comprise the CimTrak Integrity and Compliance Suite (hereinafter the "SOFTWARE").

[Legal](#)[Help](#)[Close](#)

**Figure 12: CimTrak™ End User License Agreement**

## 4. Configuring and Using the CimTrak™ Master Repository

### 4.1. MANAGING THE MASTER REPOSITORY FROM THE WEB MANAGEMENT CONSOLE

Management of the Master Repository requires that the Web Management Console is associated with the Master Repository and that a valid user account has been authenticated. For more information on associating the Web Management Console with the Master Repository please refer to section 3.1.

Once authenticated with the Master Repository multiple configuration, customization, and reporting options are available through the Web Management Console.

#### 4.1.1. MASTER REPOSITORY PROPERTIES

The Master Repository Properties dialog allows authorized CimTrak™ users to perform administrative tasks relating to CimTrak™ internal and external logging, Master Repository connections and data storage, CimTrak™ Password Policies, data communication and storage settings, Logon Banner, and Active Directory/LDAP authentication.

Accessing the CimTrak™ Master Repository Properties dialog by right-clicking on the Master Repository Name/IP Address in the Object Group tree and then select “Properties”.

The CimTrak™ Master Repository Properties dialog is broken down into multiple tabs. Changing between tabs is accomplished by clicking the desired tab. Available tabs include:

- Logging
- Repository Settings
- Password Policies
- Communication
- Logon Banner
- AD/LDAP

The functionality associated with these tabs is explained in subsequent sections.

CimTrak Repository Properties

Logging
Repository Settings
Password Policies
Communication
Logon Banner
AD/LDAP

To enable any of the logging protocols below, fill in the fields for the row matching the desired logging option. To disable a protocol, delete the data in that row. If you want log files formatted for WebTrends generated, check the box for logging to file.

	Server IP	Port	Username	Password	Display Name	From Address	Email Interval	Require TLS
SMTP	smtp.gmail.com	465	manojlovic.jovo.cimcor@grn	Password	Cimtrak_te	CimTrak@	1	<input checked="" type="checkbox"/>

Logging Methods	Server IP	Port	Protocol	Trigger Level
Syslog ▼	192.168.4.220	514	CimTrak UDP	All Events ▼
SNMP ▼	192.168.4.220	162	Community	Public
Off ▼				
Off ▼				
Off ▼				
Off ▼				

☒ Enable Logging To File (WELF Format)
Purge Log Files After
30
days (0 = never)

Number of Events To Keep (0=no limit)
0
Purge Log By # Events ▼
☐ Log Administrative DB Changes

OK
Cancel

**Figure 13: CimTrak™ Master Repository Properties**

#### 4.1.1.1. CONFIGURING LOGGING OPTIONS

The CimTrak™ Integrity and Compliance Suite has various external and internal logging settings that can be customized to meet logging organization log retention requirements.

Accessing the CimTrak™ Master Repository Properties Logging dialog is accomplished by first opening the Master Repository Properties dialog by right-clicking on the Master Repository Name/IP Address in the Object Group tree and selecting “Properties” from the context menu.

CimTrak Repository Properties

Logging Repository Settings Password Policies Communication Logon Banner AD/LDAP

To enable any of the logging protocols below, fill in the fields for the row matching the desired logging option. To disable a protocol, delete the data in that row. If you want log files formatted for WebTrends generated, check the box for logging to file.

	Server IP	Port	Username	Password	Display Name	From Address	Email Interval	Require TLS
SMTP	smtp.gmail.com	465	manojlovic.jovo.cimcor@grn	Password	Cimtrak_te	CimTrak@	1	<input checked="" type="checkbox"/>

Logging Methods	Server IP	Port	Protocol	Trigger Level
Syslog	192.168.4.220	514	CimTrak UDP	All Events
SNMP	192.168.4.220	162	Community	All Events
Off				
Off				
Off				
Off				

☒ Enable Logging To File (WELF Format) Purge Log Files After 30 days (0 = never)

Number of Events To Keep (0=no limit) 0 Purge Log By # Events ☐ Log Administrative DB Changes

OK Cancel

**Figure 14: CimTrak™ Master Repository Properties Dialog (Logging Tab)**

The CimTrak™ Master Repository Properties Logging dialog allows for the configuration of forwarding logging output to various external security information and event management systems (SIEM) and system information management systems (SIM). Additionally logging can be forwarded to a single SMTP server for notification via electronic mail (E-Mail).

The Logging Properties dialog is comprised of the following sections:

#### External Reporting

**SMTP:** *E-Mail configuration settings*

**NitroSecurity NPP:** *NitroSecurity NitroView Plugin Protocol settings*

**SNMP:** *Simple Network Management Protocol (SNMP) Manager settings*

**Syslog:** *Syslog aggregation server settings*

**WebTrends:** *Enable WebTrends logging format output*

- *Optionally CimTrak™ can be configured to purge WebTrends' log files after a user-specified amount of days*

#### Internal Reporting

**Repository Events to Keep:** *Number of CimTrak™ events (days or quantity) to maintain in the CimTrak™ Master Repository Event Log.*

**Log Administrative DB Changes:** *Enable logging of CimTrak™ administrative tasks by authorized users.*



**Logging of Administrative DB Changes is automatically enabled in the FIPS release of CimTrak™ and cannot be disabled. The Enterprise and International releases of CimTrak™ have the option to disable this setting.**

#### 4.1.1.1.1. CONFIGURING SMTP NOTIFICATIONS

CimTrak™ has the capability to export CimTrak-related event notifications over SMTP. SMTP, Simple Mail Transfer Protocol, is a standardized specification for transmission of electronic mail (E-Mail) over the internet protocol enabled networks. Configuring CimTrak™ to send electronic mail involves configuring several authentication and communication settings associated with the facilitating electronic mail server. This configuration is accomplished through the CimTrak™ Master Repository Properties Logging dialog.



***CimTrak™ External Logging properties may have been configured during the initial installation of the CimTrak™ Master Repository.***

Accessing the CimTrak™ Master Repository Properties Logging dialog is accomplished by first opening the Master Repository Properties dialog right-clicking on the Master Repository Name/IP Address in the Object Group tree, selecting “Properties” from the context menu, and then clicking the “Logging” tab.

SMTP email settings required the following associated text boxes be populated with information relating to the electronic mail server CimTrak™ will interact with to send E-Mail messages. The associated text boxes include:

**Server IP:** *IPv4, IPv6, or fully qualified domain name associated with the sending E-Mail Server*

**Port:** *Port number associated with the sending E-Mail server*

**Username:** *Username associated with the E-Mail server who has permission to send electronic mail.*

**Password:** *Password for the username associated with the E-Mail server who has permission to send electronic mail.*

**Display Name:** *Email “From Name” that will appear in the electronic mail message. This name does not need to be a valid E-Mail account on the electronic mail server.*

**From Address:** *Email “From Address” that will appear in the electronic mail message. This name does not need to be a valid E-Mail account on the electronic mail server.*

**Email Interval:** *Interval (in minutes) to send E-Mail messages. Since it is likely multiple CimTrak™ events can occur over a short period of time it is necessary to group E-Mail notifications into a single E-Mail message sent at a user-specified interval.*

**Require TLS:** *Enable transport layer security (TLS) for all E-mail communications. (checkbox)*

Once all SMTP settings have been populated it is necessary to click “OK” to accept the settings. Clicking “Cancel” will abort the changes.

**In order for CimTrak™ to send E-Mail messages three settings must be configured within CimTrak.**



The Master Repository Properties must have SMTP settings configured (this section).

A CimTrak™ User's profile must contain an E-Mail address since alerts are sent to this address. E-Mail messages can be sent to multiple users.

CimTrak™ Object Group Tree Components must have their permissions configured to send E-Mail alerts when changes are detected. Setting additional E-Mail alert settings are discussed in subsequent sections.



The default port associated with SMTP transmissions is “25”.

#### 4.1.1.1.2. CONFIGURING NITROSECURITY NPP LOGGING

CimTrak™ has the capability to export CimTrak-related event notifications over the NitroSecurity Plugin Protocol to NitroSecurity NitroView. Configuring CimTrak™ to send NPP logs involves configuring several authentication and communication settings associated with the facilitating log transmission. This configuration is accomplished through the CimTrak™ Master Repository Properties Logging dialog.



***CimTrak™ External Logging properties may have been configured during the initial installation of the CimTrak™ Master Repository.***

Accessing the CimTrak™ Master Repository Properties Logging dialog is accomplished by first opening the Master Repository Properties dialog by right-clicking on the Master Repository Name/IP Address in the Object Group tree, selecting “Properties” in the context menu, and then clicking the “Logging” tab.

NitroSecurity NPP settings required the following associated text boxes be populated with information relating to the NitroSecurity NitroView system CimTrak™ will interact with. The associated text boxes include:

**Server IP:** *IP Address associated with the NitroSecurity NitroView system.*

**Port:** *Port number associated with NPP transmissions for the NitroSecurity NitroView system.*

**Require TLS:** *Require encrypted NPP transmissions to the NitroSecurity NitroView system. (checkbox)*

**Trigger Level:** *The state of urgency associated with the triggering of this log.*

Once all NitroSecurity NPP settings have been populated it is necessary to click “OK” to accept the settings. Clicking “Cancel” will abort the changes.



#### 4.1.1.1.3. CONFIGURING SNMP LOGGING

CimTrak™ has the capability to export CimTrak-related event notifications to Simple Network Management Protocol (SNMP) managers. Configuring CimTrak™ to send SNMP logs involves configuring several authentication and communication settings associated with the facilitating log transmission. This configuration is accomplished through the CimTrak™ Master Repository Properties Logging dialog.



***CimTrak™ External Logging properties may have been configured during the initial installation of the CimTrak™ Master Repository.***

Accessing the CimTrak™ Master Repository Properties Logging dialog is accomplished by first opening the Master Repository Properties dialog by right-clicking on the Master Repository Name/IP Address in the Object Group tree, selecting “Properties,” and then clicking the “Logging” tab.

SNMP settings required the following associated text boxes be populated with information relating to the SNMP manager CimTrak™ will interact with. The associated text boxes include:

**Server IP:** *IP Address associated with the SNMP manager.*

**Port:** *Port number associated with the SNMP manager.*

**Community:** *Community name associated with the SNMP manager.*

**Trigger Level:** *The state of urgency associated with the triggering of this log.*

Once all SNMP settings have been populated it is necessary to click “OK” to accept the settings. Clicking “Cancel” will abort the changes.



***The default port associated with SNMP transmissions is “162”.***

#### 4.1.1.1.4. CONFIGURING SYSLOG LOGGING

CimTrak™ has the capability to export CimTrak-related event notifications to Syslog servers. Configuring CimTrak™ to send Syslog events involves configuring several authentication and communication settings associated with the facilitating log transmission. This configuration is accomplished through the CimTrak™ Master Repository Properties Logging dialog.



***CimTrak™ External Logging properties may have been configured during the initial installation of the CimTrak™ Master Repository.***

Accessing the CimTrak™ Master Repository Properties Logging dialog is accomplished by first opening the Master Repository Properties dialog by right-clicking on the Master Repository Name/IP Address in the Object Group tree, selecting “Properties” in the context menu, and then clicking the “Logging” tab.

Syslog settings required the following associated text boxes be populated with information relating to the Syslog server CimTrak™ will interact with. The associated text boxes include:

**Server IP:** *IP Address associated with the Syslog server.*

**Port:** *Port number associated with the Syslog manager.*

**Protocol:** *Transmission protocol (TCP or UDP) used to send the Syslog events to the Syslog manager.*

**Trigger Level:** *The state of urgency associated with the triggering of this log.*

Once all Syslog settings have been populated it is necessary to click “OK” to accept the settings. Clicking “Cancel” will abort the changes.



***The default port associated with Syslog transmissions is “514”. Generally, Syslog communications are facilitated via UDP.***

#### **4.1.1.1.5. CONFIGURING WEBTRENDS LOGGING**

CimTrak™ has the capability to save CimTrak-related event notifications to the WebTrends logging format. Configuring CimTrak™ to save WebTrends events is accomplished through the CimTrak™ Master Repository Properties Logging dialog.



***CimTrak™ External Logging properties may have been configured during the initial installation of the CimTrak™ Master Repository.***

Accessing the CimTrak™ Master Repository Properties Logging dialog is accomplished by first opening the Master Repository Properties dialog by Right click on the Master Repository Name/IP Address in the Object Group tree, selecting “Properties” in the context menu, and then clicking the “Logging” tab.

WebTrends logging is enabled by clicking the “Enable Logging to File (WebTrends)” checkbox. Optionally, WebTrends log files can be purged from the system after the user specified number of days.



***By default, WebTrends files are stored in the “C:\Program Files\Cimcor\CimTrak\CimTrakServer\WTLogs” folder on the system containing the CimTrak™ Master Repository.***

Once all WebTrends settings have been populated it is necessary to click “OK” to accept the settings. Clicking “Cancel” will abort the changes.

#### 4.1.1.2. CONFIGURING MASTER REPOSITORY SETTINGS

The CimTrak™ Integrity and Compliance Suite has various connectivity and Master Repository health settings that can be customized to meet organization security requirements. These settings are accomplished through the Master Repository Properties Repository Settings dialog.

Accessing the CimTrak™ Master Repository Properties Repository Settings dialog is accomplished by first opening the Master Repository Properties dialog by right-clicking on the Master Repository Name/IP Address in the Object Group tree, selecting “Properties” from the context menu, and then clicking the “Repository Settings” tab.

The screenshot shows the 'CimTrak Repository Properties' dialog box with the 'Repository Settings' tab selected. The dialog has a title bar and a tabbed interface with the following tabs: 'Logging', 'Repository Settings' (active), 'Password Policies', 'Communication', 'Logon Banner', and 'AD/LDAP'. The 'Repository Settings' tab contains the following fields and controls:

Field	Value	Unit
Name	REPOS114	
Management Console disconnect timeout	720	minutes
Warn if storage drops below	0	%
Deny Agent connection if a MAC address change has been detected	<input type="checkbox"/>	

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

**Figure 15: CimTrak™ Master Repository Repository Properties Dialog (Repository Settings Tab)**

The CimTrak™ Master Repository Properties Repository Settings dialog allows for the configuration of the Master Repository name, Web Management Console timeout interval, Master Repository storage drive space monitoring, and Master Repository access restrictions.

The Repository Settings dialog is comprised of the following sections:

**Name:** *Master Repository Name*

**Web Management Console disconnect timeout:** *Web Management Console idle timeout*

**Warn if storage drops below:** *Master Repository disk space monitoring. An Event Log warning (and optionally external notification) will be sent if the Master Repository disk space falls below the specified threshold.*

**By Default, All Computers Will Be Granted/Denied Access:** *Network access restrictions for connections to the Master Repository.*

#### **4.1.1.2.1. CONFIGURING THE MASTER REPOSITORY NAME**

Setting the CimTrak™ Master Repository name is helpful for uniquely identifying a particular Master Repository in Event Logs and reporting. Setting the Master Repository name is achieved by modifying the “Name” text box located in the Master Repository Properties Repository Settings dialog.

Accessing the CimTrak™ Master Repository Properties Repository Settings dialog is accomplished by first opening the Master Repository Properties dialog by right-clicking on the Master Repository Name/IP Address in the Object Group tree, selecting “Properties,” and then clicking the “Repository Settings” tab.

The Master Repository name can be 50 characters/digits or less.



***By default, the Master Repository name is automatically populated with the host computer's system name.***

Once the Master Repository name has been populated it is necessary to click “OK” to accept the settings. Clicking “Cancel” will abort the changes.

#### **4.1.1.2.3. CONFIGURING THE WEB MANAGEMENT CONSOLE DISCONNECT TIMEOUT**

The CimTrak™ Master Repository can be configured to automatically disconnect an idle Web Management Console connection after a user-specified period of time. Setting a timeout period is essential in ensuring that a connected, inactive Web Management Console session is not assumed by another user. Setting the Web Management Console timeout is achieved by modifying the “Web Management Console Disconnect Timeout” properties located in the Master Repository Properties Repository Settings dialog.

Accessing the CimTrak™ Master Repository Properties Repository Settings dialog is accomplished by first opening the Master Repository Properties dialog by right-clicking on the Master Repository Name/IP Address in the Object Group tree, selecting “Properties,” and then clicking the “Repository Settings” tab.

The Web Management Console timeout can be configured for any value between 2 minutes and 10,000 minutes.



***By default, the Web Management Console timeout is set to 5 minutes.***

Once the Web Management Console timeout is configured it is necessary to click “OK” to accept the settings. Clicking “Cancel” will abort the changes.

#### 4.1.1.2.4. CONFIGURING THE MASTER REPOSITORY DISK SPACE MONITOR

The disk space utilized by the CimTrak™ Master Repository storage location can be monitored for space exhaustion. Monitoring for space exhaustion is essential for maintaining a healthy, functional CimTrak™ Master Repository. Setting the Master Repository disk space monitor is achieved by modifying the “Warn if Storage Drops Below...” properties located in the Master Repository Properties Repository Settings dialog.

Accessing the CimTrak™ Master Repository Properties Repository Settings dialog is accomplished by first opening the Master Repository Properties dialog by right-clicking on the Master Repository Name/IP Address in the Object Group tree, selecting “Properties,” and then clicking the “Repository Settings” tab.

The “Warn if Storage Drops Below...” properties can be configured for any value between 0% and 100%.



***By default, the Master Repository Disk Space Monitor is disabled.***

Once the Master Repository disk space monitor is configured it is necessary to click “OK” to accept the settings. Clicking “Cancel” will abort the changes.

#### 4.1.1.2.5. CONFIGURING THE MASTER REPOSITORY ACCESS RESTRICTIONS

The CimTrak™ Master Repository has the capability to allow or deny connectivity by CimTrak™ Web Management Consoles and connecting Agents. Restricting access to the Master Repository adds an additional layer of security to the Master Repository resulting in additional confidentiality, availability, and integrity of the CimTrak™ Integrity and Compliance Suite. Setting the Master Repository access restrictions is achieved by modifying the “By Default, all Computers will be Granted/Denied Access” properties located in the Master Repository Properties Repository Settings dialog.

Accessing the CimTrak™ Master Repository Properties Repository Settings dialog is accomplished by first opening the Master Repository Properties dialog by right-clicking on the Master Repository Name/IP Address in the Object Group tree, selecting “Properties,” and then clicking the “Repository Settings” tab.

Allowing or restricting access to the Master Repository is accomplished by selecting either the “Granted Access” or “Denied Access” radio buttons and then populating the “Except Those Listed Below” properties.

For example, if an IP address of 192.168.10.5 and Subnet Mask of 255.255.255.0 are specified, all 192.168.10.x IP addresses will be Granted/Denied. In order to Grant/Deny specific IP addresses, the Subnet Mask should be set as 255.255.255.255. Please note that IPv4 and IPv6 IP addresses are valid.



***By default, all IP addresses are allowed access to the Master Repository.***

Once the Master Repository access restrictions are configured it is necessary to click “OK” to accept the settings. Clicking “Cancel” will abort the changes.

#### **4.1.1.3. CONFIGURING MASTER REPOSITORY PERMISSIONS**

The CimTrak™ Master Repository can be configured to restrict access to children objects based on permission settings. Accessing Master Repository permissions is accomplished by first clicking once on the Repository Name in the Object Tree to select it and then right-clicking and selecting Permission. The Permissions for Object dialog will display.

By default each Area will have the following permissions:

##### **Administrators**

**Create Objects:** *Create Object Groups.*

**Edit:** *Edit Object Group settings.*

**Lock:** *Enable active monitoring of Object Group data.*

**Reports:** *View reports relating to children objects.*

**Unlock:** *Disable active monitoring of Object Group Data.*

**View:** *View contents and configurations relating to children data.*

##### **Auditors**

**Reports:** *View reports relating to children objects.*

**View:** *View contents and configurations relating to children data.*

##### **Installers**

*Attach CimTrak™ Agents to a Master Repository.*

Default access permissions associated with the Administrators, Auditors, and Installers User Groups cannot be changed.

Additional information relating to these alert types is described in a subsequent section.

Permissions for Object

Add

Group or User Names

Group	Administrators
Group	Auditors
Group	Installers

Permissions	Allow	Deny
Create Objects	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Edit	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lock	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Reports	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Unlock	<input checked="" type="checkbox"/>	<input type="checkbox"/>
View	<input checked="" type="checkbox"/>	<input type="checkbox"/>

☒ Apply permissions to children recursively

OK

Cancel

**Figure 16: Permissions for Object Dialog**

#### 4.1.1.3.1. CONFIGURING THE MASTER REPOSITORY ACCESS RESTRICTIONS

It is possible to modify existing user and group Permissions. Accessing Master Repository permissions is accomplished by first clicking once on the Master Repository Name in the Object Tree to select it and then right-clicking and selecting Permissions. The Permissions for Object dialog will display.

Select the existing user or role by clicking once on the CimTrak™ User or Role name in the Role or User Names section of the Permissions for Object dialog. The Permissions section of the Permissions for Object dialog will update to show the permissions currently assigned to the selected user or group.





***Selecting a role will apply the selected permissions to all members of the role. Selecting a single user will apply the selected permissions to only that single user account.***

To add or remove permissions click the “Allow” or “Deny” checkbox corresponding to the permission being configured. Available permissions include:

**Create Objects:** *Create Object Groups.*

**Edit:** *Edit Object Group settings.*

**Lock:** *Enable active monitoring of Object Group data.*

**Reports:** *View reports relating to children objects.*

**Unlock:** *Disable active monitoring of Object Group Data.*

**View:** *View contents and configurations relating to children data.*

To apply the permission settings to all children objects, ensure that the Apply permissions to children recursively checkbox is selected.

When completed, click “OK” to apply the permissions. Click “Cancel” to abort the security permission configuration.



***Permissions can be inherited from parent objects (such as the Master Repository) if the permissions are created at a parent level.***



***Permissions are not automatically inherited for new objects. It will be necessary to manually assign the permissions and notification settings to the object.***

In order to add a User or Group to the Permissions dialog that does not currently appear in the Permissions dialog, click the Add button. The Select Users or Roles dialog will appear. To select a User or Role, select the checkbox corresponding to the User or Role and click Ok. The User or Role will now appear in the Permissions dialog.

#### **4.1.1.4. CONFIGURING MASTER REPOSITORY EMAIL SETTINGS**

The CimTrak™ Master Repository email settings can be configured per User or Role. Accessing Master Repository email settings is accomplished by first clicking once on the Repository Name in the Object Tree to select it and then right-clicking and selecting Email. The Email Settings for Object dialog will display.

By default, no User or Role has specially defined email settings. When the Email Settings for Object dialog is first opened, no User or Role will be listed.



Email Settings for Object

Add

Group or User Names

☒ Apply permissions to children recursively

OK

Cancel

**Figure 17: Email settings for Object Dialog**

In order to add a User or Group to the Email Settings for Object dialog that does not currently appear in the Email Settings for Object dialog, click the Add button. The Select Users or Roles dialog will appear. To select a User or Role, select the checkbox corresponding to the User or Role and click Ok. The User or Role will now appear in the Email Settings for Object dialog. Now, the email settings for the selected User or Role can be set for the selected object.

#### 4.1.1.4.1. CONFIGURING THE MASTER REPOSITORY EMAIL SETTINGS

It is possible to modify existing user and group Email Settings. Accessing Master Repository email settings is accomplished by first clicking once on the Master Repository Name in the Object Tree to select it and then right-clicking and selecting Email. The Email Settings for Object dialog will display.

Select the existing user or role by clicking once on the CimTrak™ User or Role name in the Role or User Names section of the Email Settings for Object dialog. The settings section of the Email Settings for Object dialog will update to show the settings currently assigned to the selected user or group.



***Selecting a role will apply the selected email settings to all members of the role. Selecting a single user will apply the selected email settings to only that single user account.***

To add or remove email settings click the “Send” checkbox corresponding to the email setting being configured. Available email notification settings include:

**Emergency:** *Receive alerts relating to emergency level notifications.*

**Alert:** *Receive alerts relating to alert level notifications.*

**Critical:** *Receive alerts relating to critical level notifications.*

**Error:** *Receive alerts relating to error level notifications.*

**Warning:** *Receive alerts relating to warning level notifications.*

**Notice:** *Receive alerts relating to notice level notifications.*

**Information:** *Receive alerts relating to information level notifications.*

To apply the email settings to all children objects, ensure that the Apply email settings to children recursively checkbox is selected.

When completed, click “OK” to apply the email settings. Click “Cancel” to abort the email setting configuration.



***Email notification settings can be inherited from parent objects (such as the Master Repository) if the email settings are created at a parent level.***



***Email notification settings are not automatically inherited for new objects. It will be necessary to manually assign the email settings to the object.***

#### 4.1.1.5. CONFIGURING THE MASTER REPOSITORY PASSWORD POLICIES

The CimTrak™ Master Repository has the capability to enforce password complexity requirements for CimTrak™ user account passwords. Password complexity requirements settings allow authorized CimTrak™ administrators the capability to configure CimTrak™ to require password complexities meeting organizational requirements.

CimTrak Repository Properties

Logging Repository Settings Password Policies Communication Logon Banner AD/LDAP

☒ None  
☐ Advanced Password Policy (AR 25-2 Compliant) - User-entered password  
☐ Advanced Password Policy (AR 25-2 Compliant) - Randomly-generated password  
☐ Custom  
☐ Require 2 lower case, 2 upper case, 2 numbers, and 2 special characters  
☐ Random Password Generation  
☐ Check against password dictionary  
 Require minimum password length of   
 Passwords expire after  days (0 = never)  
 Prevent use of the last  passwords  
 Lock out account after  login failures (0 = never)  
 Lock out account for  minutes (0 = indefinite)

OK Cancel

**Figure 18: CimTrak™ Master Repository Properties Dialog (Password Policies Tab)**

Accessing the CimTrak™ Master Repository Properties Password Policies dialog is accomplished by first opening the Master Repository Properties dialog by right-click on the Master Repository Name/IP Address in the Object Group tree, selecting “Properties,” and then clicking the “Password Policies” tab.

CimTrak™ has the capability to enforce four primary password complexity categories. Enforcing password complexity requirements is accomplished by selected the applicable password complexity requirement:

**None**

*No password complexity requirements are enforced.*

**Advanced Password Policy (AR 25-2 Compliant) User-entered Password:**

*Meeting or exceeding user-generated password complexity requirements prescribed by United States Army Information Assurance Regulation 25-2*

- *Require 2 lower case, 2 upper case, 2 numbers, and 2 special characters*
- *Check against password dictionary*
- *Require minimum password length of 10 alpha-numeric characters/symbols*
- *Passwords expire after 30 days*
- *Prevent use of the last 10 passwords*
- *Lock out the account after 3 logon failures*
- *Locked out accounts are indefinite (until unlocked by an authorized CimTrak™ administrator.*

**Advanced Password Policy (AR 25-2 Compliant) – Randomly-generated password:**

*Meeting or exceeding password complexity requirements prescribed by United States Army Information Assurance Regulation 25-2. Passwords are randomly generated.*

- *Require 2 lower case, 2 upper case, 2 numbers, and 2 special characters*
- *Random Password Generation*
- *Check against password dictionary*
- *Require minimum password length of 10 alpha-numeric characters/symbols*
- *Passwords expire after 30 days*
- *Prevent use of the last 10 passwords*
- *Lock out the account after 3 logon failures*
- *Locked out accounts are indefinite (until unlocked by an authorized CimTrak™ administrator).*

**Custom:**

*Allows for the configuration of custom password policies. Complexity options available for the custom setting include:*

- *Require 2 lower case, 2 upper case, 2 numbers, and 2 special characters*
- *Random Password Generation*
- *Check against password dictionary*
- *Require minimum password length of alpha-numeric characters/symbols*
  - ◆ *(Minimum = 0, Maximum = 50)*
- *Passwords expire after # days*
  - ◆ *(Never = 0, Minimum = 1, Maximum = 365)*
- *Prevent use of the last ## passwords*
  - ◆ *(Minimum = 0, Maximum = 30)*
- *Lock out the account after ## logon failures*
  - ◆ *(Never = 0, Minimum = 1, Maximum = 10)*
- *Locked out accounts for ## minutes*
  - ◆ *(0 = Indefinite until unlocked by an authorized CimTrak™ administrator, Minimum = 1, Maximum = 4320)*

Once the Master Repository Password Policies are configured it is necessary to click “OK” to accept the settings. Clicking “Cancel” will abort the changes.

#### **4.1.1.6. CONFIGURING THE MASTER REPOSITORY COMMUNICATION SETTINGS**

The CimTrak™ Master Repository communication encryption settings can be changed for any data communications directed to or from the CimTrak™ Master Repository. It is important to have the capability to change encryption settings in the event a used communication cipher/encryption type has been publicly compromised.

CimTrak Repository Properties

Logging
Repository Settings
Password Policies
Communication
Logon Banner
AD/LDAP

Encryption Type	AES	
Encryption Key Length	256	
HMAC	SHA1	

Communication Settings	DHE-RSA-AES256-SHA	
Key Renegotiation Interval	0	seconds (0 = off)

NOTE: Changes to the communication settings will not be reflected until the Agents and Management Consoles reconnect to the Repository

OK Cancel

**Figure 19: CimTrak™ Master Repository Properties Dialog (Communication Tab)**

Accessing the CimTrak™ Master Repository Properties Communication dialog is accomplished by first opening the Master Repository Properties dialog by right-clicking on the Master Repository Name/IP Address in the Object Group tree, selecting “Properties,” and then clicking the “Communication” tab.



***Encryption settings for data stored in the Master Repository cannot be changed after installation.***

To select the communication settings for all data-in-transit communications to/from the CimTrak™ Master Repository, select the appropriate cipher string from the “Communication Settings” dropdown.



***Available cipher strings are dependant on the CimTrak™ release type. Available cipher strings are outlined in the Installation Documentation.***



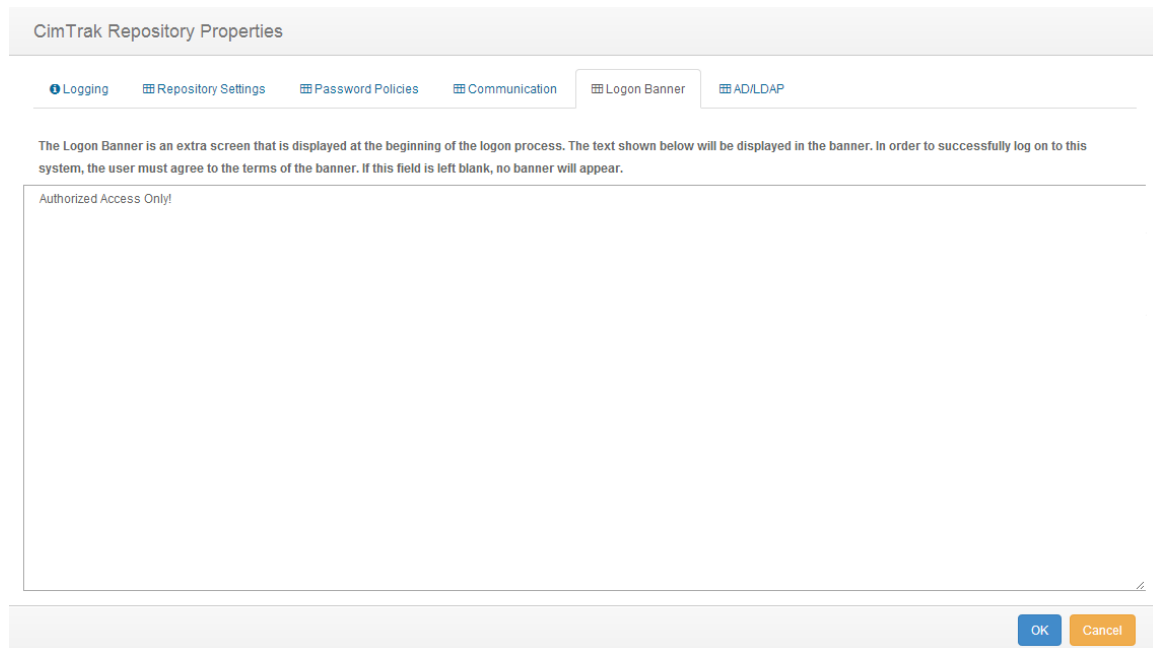
***Changes to the Master Repository communication settings will not be reflected until all entities connected to the Master Repository reconnect.***

Once the Master Repository Communication Settings are configured it is necessary to click “OK” to accept the settings. Clicking “Cancel” will abort the changes.

#### **4.1.1.7. CONFIGURING THE MASTER REPOSITORY LOGON BANNER**

The CimTrak™ Master Repository supports logon banners. Logon banners are used to inform connecting users of any restrictions, policies, or disclaimers

relating to the use of an application. The logon banner is displayed whenever any user interface attaches to the Master Repository. The user must accept the logon banner before using the application.



**Figure 20: CimTrak™ Master Repository Properties Dialog (Logon Banner Tab)**

Accessing the CimTrak™ Master Repository logon banner dialog is accomplished by first opening the Master Repository Properties dialog by right-clicking on the Master Repository Name/IP Address in the Object Group tree, selecting "Properties," and then clicking the "Logon Banner" tab.



The image shows a login banner for Cimtrak. At the top left is a circular logo with a stylized 'C' and dots. To its right is the text 'cimtrak' in a large, blue, sans-serif font, with the tagline 'detecting the unknown' in a smaller, grey font below it. Below the logo and text is a blue horizontal bar with the text 'Please Login' in white. Underneath this bar is a light blue rectangular box containing the text 'Authorized Access Only!'. Below this box are two input fields: the first contains the IP address '192.168.4.114' and the second contains the port number '3749'. Below these are two more input fields labeled 'Username' and 'Password'. At the bottom is a large blue button with the text 'Sign in' in white.

**Figure 21: CimTrak™ Logon Banner**

To enter a logon banner, type the desired information in the provided text box. To disable the logon banner, delete all contents of the logon banner text box.

Right-clicking anywhere in the logon banner text box provides additional text editing functionality for additional logon banner customization. Additional functionality includes:

- Undo
- Cut
- Copy
- Paste
- Delete
- Select All
- Right to left Reading order
- Show Unicode control characters
- Insert Unicode control character
  - LRM: Left-to-right mark
  - RLM: Right-to-left mark

ZWJ: Zero width joiner  
ZWNJ: Zero width non-joiner  
LRE: Start of left-to-right embedding  
RLE: Start of right-to-left embedding  
LRO: Start of left-to-right override  
RLO: Start of right-to-left override  
PDF: Pop directional formatting  
NADS: National digit shapes substitution  
NODS: Nominal (European) digit shapes  
ASS: Active symmetric swapping  
ISS: Inhibit symmetric swapping  
AAFS: Active Arabic form shaping  
IAFS: Inhibit Arabic form shaping  
RS: Record Separator (Block separator)  
US: Unit Separator (Segment separator)  
Close IME  
Reconversion



***The Logon Banner accepts between 0 and 3,999 alphanumeric/symbol characters.***

Once the Master Repository Logon Banner Settings are configured it is necessary to click “OK” to accept the settings. Clicking “Cancel” will abort the changes.

#### **4.1.1.8. CONFIGURING ACTIVE DIRECTORY/LDAP USER ACCOUNT INTEGRATION**

CimTrak™ supports local user accounts and Active Directory/LDAP integrated user accounts. Using Active Directory/LDAP user accounts simplifies the administrative task of adding additional user accounts to the CimTrak™ Master Repository. Active Directory/LDAP integration allows the CimTrak™ Master Repository to authenticate and authorize users directly with the Active Directory/LDAP Server. Additionally, using Active Directory/LDAP integration helps maintain a consistent password policy, facilitates single sign-on, and enables the use of CAC cards for authentication and authorization.

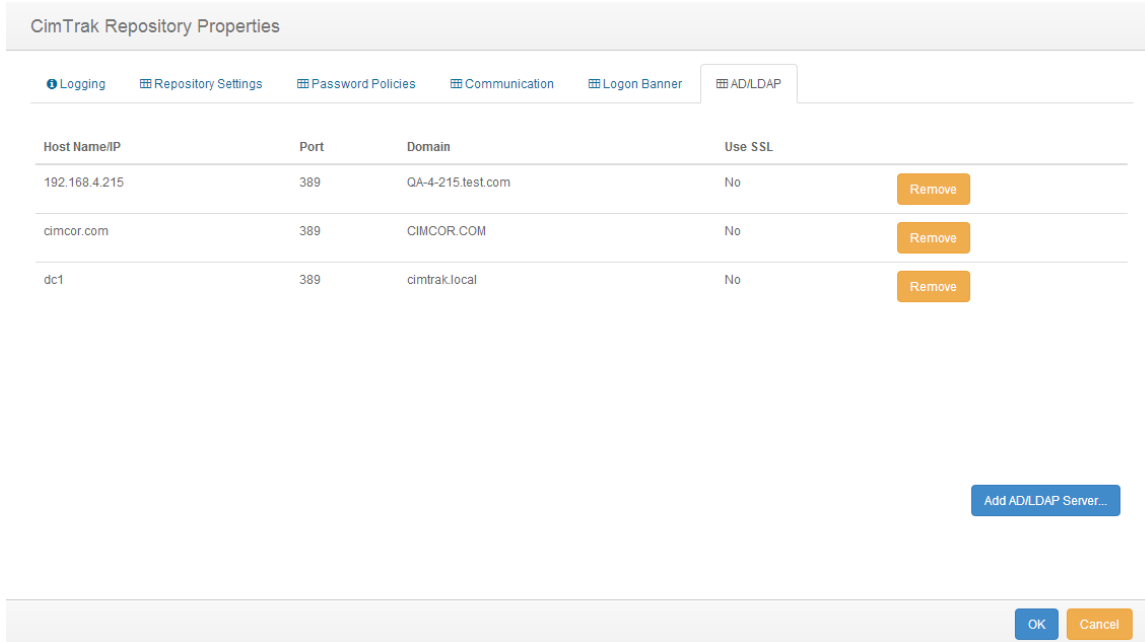


***Unlike the other tabs in the CimTrak™ Master Repository Properties dialog, all changes made in the AD/LDAP tab are updated in the Master Repository automatically. For this reason the “Cancel” button is not available once the AD/LDAP tab is selected.***



***The computer hosting the Master Repository does not need to be a member of the domain before the Master Repository connects to the AD/LDAP server. The Master Repository must have full communication with the domain server.***





**Figure 22: Cimtrak™ Master Repository Properties Dialog (AD/LDAP Tab)**

Accessing the CimTrak™ Master Repository AD/LDAP dialog is accomplished by first opening the Master Repository Properties dialog by right-clicking on the Master Repository Name/IP Address in the Object Group tree, selecting “Properties,” and then clicking the “AD/LDAP” tab.

The AD/LDAP dialog is broken into two sections:

- Configure AD/LDAP Hosts
- Configure AD/LDAP Users

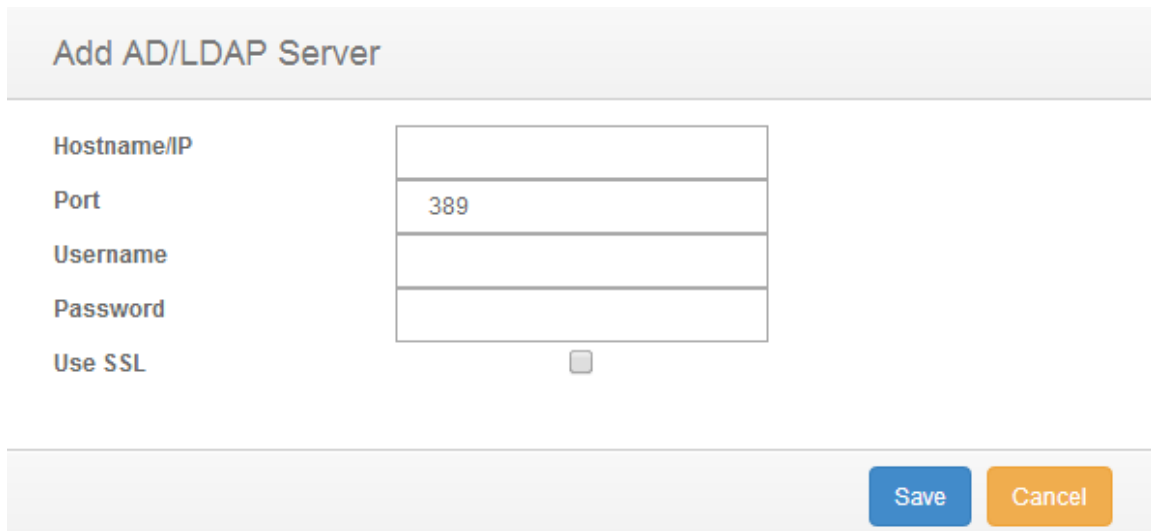
The Configure AD/LDAP Hosts section displays all Active Directory/LDAP hosts the CimTrak™ Master Repository is currently authenticated with. Selecting the AD/LDAP host will populate the Configure AD/LDAP Users section with all added user accounts.

#### **4.1.1.8.1. ADDING/EDITING/DELETING ACTIVE DIRECTORY/LDAP HOSTS**

Adding Active Directory/LDAP hosts is accomplished through the Master Repository properties AD/LDAP dialog.

Accessing the CimTrak™ Master Repository Properties AD/LDAP dialog is accomplished by first opening the Master Repository Properties dialog by right-clicking on the Master Repository Name/IP Address in the Object Group tree, selecting “Properties” from the context menu, and then clicking the “AD/LDAP” tab.

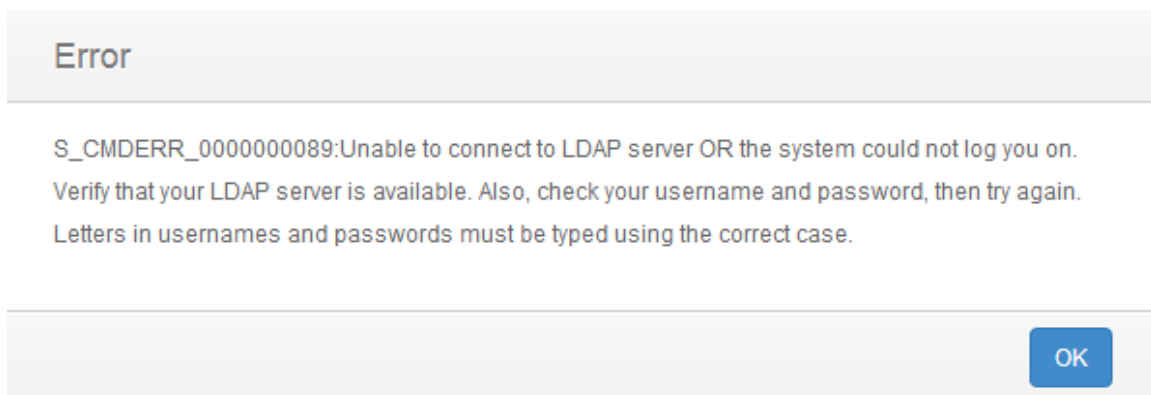
Adding an AD/LDAP host is accomplished by clicking the “Add...” button located in the Configure AD/LDAP Hosts section of the AD/LDAP dialog. The AD/LDAP Hosts dialog will appear.

The image shows a dialog box titled "Add AD/LDAP Server". It contains a form with the following fields: "Hostname/IP" (empty), "Port" (containing "389"), "Username" (empty), and "Password" (empty). Below these fields is a checkbox labeled "Use SSL" which is currently unchecked. At the bottom right of the dialog are two buttons: "Save" (blue) and "Cancel" (orange).

**Figure 23: Add AD/LDAP Server Dialog**

Populate the Host Name/IP Address, Port number, SSL requirements, Username, and Password associated with the AD/LDAP host. Click “OK” when completed. Clicking “Cancel” will abort the host configuration process.

Invalid settings or communication errors are indicated with a CimTrak™ Web Management Console alert dialog.

The image shows an error dialog box with a title bar that says "Error". The main text area contains the following message: "S\_CMDERR\_0000000089:Unable to connect to LDAP server OR the system could not log you on. Verify that your LDAP server is available. Also, check your username and password, then try again. Letters in usernames and passwords must be typed using the correct case." At the bottom right of the dialog is a single blue button labeled "OK".

**Figure 24: Add AD/LDAP Server Error**

Successful authentication with the AD/LDAP host will be indicated by the Host Name/IP, Port, Domain, and Use SSL columns being populated in the Configure AD/LDAP Hosts section of the AD/LDAP dialog.



***It is possible to add additional AD/LDAP Hosts by repeating the processes in this section.***

Once the Master Repository Logon Banner Settings are configured it is necessary to configure AD/LDAP users before continuing.

Deleting AD/LDAP Hosts is accomplished by selecting the Host Name/IP associated with the AD/LDAP host in the Configure AD/LDAP Hosts section and then clicking the “Remove” button.

#### **4.1.2. MASTER REPOSITORY OPTIONS**

The Master Repository allows for the configuration of user-specific options. These options are dependent on the Master Repository the CimTrak™ user is authenticated with. These options include the capability to change account passwords and customize preferences.

Accessing CimTrak™ Master Repository Options is accomplished by right-clicking the Master Repository in the Object Tree and selecting “User Maintenance” in the context menu.

##### **4.1.3.1. CHANGING ACCOUNT PASSWORD**

The attached user has the capability of changing their password. Passwords can only be changed by local CimTrak™ Users. AD/LDAP users must change their password following the instructions provided by their domain.

Changing a CimTrak™ User password is accomplished by right-clicking the Master Repository in the Object Tree, selecting “User Maintenance” in the context menu, and selecting the user that you wish to modify preferences for. The “User Maintenance” dialog will display.

User Maintenance

Search

Type	CimTrak Role	User	First Name	Last Name	Notes
User	Administrators	aaaa			
User	Administrators	admin			
User	Administrators	alberts	Dave	Alberts	
User	Administrators	aniken	Aniken	Skywalker	
User	Administrators	CIMCOR.COM\Administrator			Built-in account for administering the computer/domain
Group	Administrators	CIMCOR.COM\Developers			
User	Administrators	CIMCOR.COM\reister.kenneth	Kenneth	Reister	
Group	Administrators	cimtrak.local\Domain Admins			Designated administrators of the domain
User	Administrators	cimtrak.local\jovo	Jovo	Manojlovic	
Group	Administrators	cimtrak.local\Users			Users are prevented from making accidental or intentional system-wide changes and can run most applications
User	Administrators	Fridge	Refridgerator	Perry	

Add User...
Add AD/LDAP User/Group...
Close

**Figure 25: Cimtrak™ Master Repository User Maintenance Dialog**

Upon selecting a user to modify preferences for, the “User Preferences” dialog will display.

User Add/Edit

Username

aaaa

Role

Administrators

Password

Password

Confirm Password

Confirmed Password

First Name

First Name

Last Name

Last Name

Title

Title

Address

Address

City

City

State

State

Zip

Zip

Email Address

Email Address

Phone

Phone

Extension

Extension

Fax

Fax

Alt. Phone

Alt. Phone

Alt. Extension

Alt. Extension

Pager

Pager

Delete
Save
Cancel

**Figure 26: Cimtrak™ Master Repository User Add/Edit Dialog**

## 4.2. AUDITING THE MASTER REPOSITORY FROM THE WEB MANAGEMENT CONSOLE

Each CimTrak™ Master Repository installation has the capability to be audited via the CimTrak™ Web Management Console Information Display Area. Auditing of the Master Repository provides authorized CimTrak™ Administrators a list of events occurring on components connected to the Master Repository. The Auditing capabilities are broken into four primary categories:

- Repository Information
- Event Log
- Notes

## Logged On Users

Auditing capabilities are accessed by selecting the Master Repository name/IP Address in the Web Management Console Object Group Tree. The auditing capabilities will display in the Web Management Console Information Display Area.

Dashboard Repository Info Event Log Logged On Users

Version: 2.0.6.18 Build 7725

Operating System: Windows Longhorn Service Pack 1 Build 7601

System Uptime: 5/30/2014 03:38:44 (a month ago)

Repository Uptime: 6/18/2014 10:50:08 (9 days ago)

Port: 3749

Storage Path: E:\Program Files (x86)\Cimcor\CimTrak\CimTrakServer\Storage\

Agent Connections: 9 Mgmt Console Connections: 1 Total Connections: 12

Serial Numbers	Agents	Objects	Eval Days	Eval Days Left	+ Add Serial Number
ADCP0819472831000003E8007057	0	10	N/A	N/A	Delete
	Total: 0	Total: 10			
	Used: 0	Used: 3			
CTCP08760364440032044200A241	50	50	N/A	N/A	Delete
	Total: 50	Total: 50			
	Used: 7	Used: 5			
CTCP08760364440032044200A241	50	50	N/A	N/A	Delete
	Total: 50	Total: 50			
	Used: 7	Used: 5			
DBCP0819472932000003E8007053	0	10	N/A	N/A	Delete
	Total: 0	Total: 10			
	Used: 0	Used: 4			

Figure 27: CimTrak™ Web Management Console Information Display Area (Master Repository Level)

### 4.3.1. MASTER REPOSITORY INFORMATION

The Master Repository Information Tab displays information about the Master Repository Host Operating System, Master Repository Uptime, and connection information. The Master Repository Information Tab is accessed from the Web Management Console in the Information Display Area by clicking the “Repository Info” tab. See Figure 9: CimTrak™ Web Management Console Information Display Area (Master Repository Level)

### 4.3. CIMTRAK™ WEB MANAGEMENT CONSOLE: HELP

The CimTrak™ Web Management Console Help option provides valuable information relating to the CimTrak™ deployment.

The CimTrak™ Help menu can be accessed by clicking the question mark icon “?” in the lower right corner of the CimTrak™ Web Management Console. The Help dialog will show.

Help



E-mail

For technical support, please contact our support group at: [support@cimcor.com](mailto:support@cimcor.com)

Call

For technical support, please contact our support group at: 1-877-424-6267

Licensing

Legal

Close

**Figure 10: Cimtrak™ Web Management Console Help dialog screen**

#### **4.4. LEGAL NOTICES**

Information relating to CimTrak™ Legal Notices can be accessed by clicking the question mark icon “?” in the lower right corner of the CimTrak™ Web Management Console, followed by clicking the Legal button on the lower left corner or the CimTrak™ Web Management Console Help dialog screen. The Legal Notices dialog will show.



**Figure 11: Cimtrak™ Web Management Console Legal Notices dialog screen**

#### **4.4.1. END USER LICENSE AGREEMENT (EULA)**

Information relating to the CimTrak™ End User License Agreement (EULA) can be accessed by clicking clicking the question mark icon “?” in the lower right corner of the CimTrak™ Web Management Console, followed by clicking the Licensing button on the lower left corner or the Cimtrak™ Web Management Console Help dialog screen. The Licensing dialog will show.



Figure 12: CimTrak™ End User License Agreement

The Master Repository Information Tab is divided into 3 sections:

**Master Repository Information**  
**Master Repository Connections**

The Master Repository Information section displays information relating to:

**Version:** *Version and build number associated with the CimTrak™ Master Repository*

**Operating System:** *Operating system of the host the CimTrak™ Master Repository is installed on.*

**System Uptime:** *Master Repository host system uptime.*

**Repository Uptime:** *Master Repository uptime.*

**Port:** *Communication port used by the Master Repository.*

**File Storage Path:** *Location of the file storage used by the Master Repository to store authoritative copy and intrusion data.*

The Master Repository Connections section displays information about external agents and Web Management Console connections currently associated with the Master Repository.

#### 4.3.2. MASTER REPOSITORY EVENT LOG



Master Repository Event Log provides audit information relating to events occurring in the Master Repository and objects connected to the Master Repository. Accessing the Master Repository Event Log is accomplished by first clicking once on the Master Repository name/IP Address in the Object Group Tree to select it followed by clicking the Event Log tab in the Web Management Console Information Display Area.

The Master Repository Event Log displays details of all events that have occurred on the Master Repository and objects connected to the Master Repository. The level of detail displayed is dependent on the auditing level configured in the Master Repository Properties Log Administrative DB Changes. See section 0 for additional information.

For each recorded event, the Master Repository Event Log will display information corresponding to the following:

**Event Date/Time:** *The exact date and time of the detected event.*

**Event:** *Brief description of the detected event.*

**Correction:** *The action taken on the detected event.*

**Performed by:** *CimTrak™ User Account responsible for the detected event.*

**Modified by:** *File System User responsible for the detected event..*

**Absolute Path:** *File path affected by the detected event.*

**Completion Date/Time:** *Date and time the correction response completed.*

**Event Code:** *Internal CimTrak™ Event Code corresponding to the detected event.*

**Path:** *Object Tree Path to the affected CimTrak™ object.*

DashboardRepository InfoEvent LogLogged On Users

Drag a column header here and drop it to group by that column.

Severity	Event Date/Time	Event	Correction	CimTrak ID	Modified By	Process	Absolute path
Warning	6/27/2014 14:37:37	* [ warning] [vmusr:vmusr] Error in the RP...		TEST116((n...	TEST116js...	VMware Tools	\\LogMonitor\EventLog\Application
Warning	6/27/2014 14:37:35	* [ warning] [vmusr:vmusr] Error in the RP...		TEST116((n...	TEST116js...	VMware Tools	\\LogMonitor\EventLog\Application
Warning	6/27/2014 14:37:34	* [ warning] [vmusr:vmusr] Error in the RP...		TEST116((n...	TEST116js...	VMware Tools	\\LogMonitor\EventLog\Application
Warning	6/27/2014 14:37:33	* [ warning] [vmusr:vmusr] Error in the RP...		TEST116((n...	TEST116js...	VMware Tools	\\LogMonitor\EventLog\Application
Warning	6/27/2014 14:37:32	* [ warning] [vmusr:vmusr] Error in the RP...		TEST116((n...	TEST116js...	VMware Tools	\\LogMonitor\EventLog\Application
Warning	6/27/2014 14:37:31	* [ warning] [vmusr:vmusr] Error in the RP...		TEST116((n...	TEST116js...	VMware Tools	\\LogMonitor\EventLog\Application
Warning	6/27/2014 14:37:30	* [ warning] [vmusr:vmusr] Error in the RP...		TEST116((n...	TEST116js...	VMware Tools	\\LogMonitor\EventLog\Application
Warning	6/27/2014 14:37:28	* [ warning] [vmusr:vmusr] Error in the RP...		TEST116((n...	TEST116js...	VMware Tools	\\LogMonitor\EventLog\Application
Warning	6/27/2014 14:37:27	* [ warning] [vmusr:vmusr] Error in the RP...		TEST116((n...	TEST116js...	VMware Tools	\\LogMonitor\EventLog\Application
Warning	6/27/2014 14:37:26	* [ warning] [vmusr:vmusr] Error in the RP...		TEST116((n...	TEST116js...	VMware Tools	\\LogMonitor\EventLog\Application
Warning	6/27/2014 14:37:26	* [ warning] [vmusr:vmusr] Error in the RP...		TEST116((n...	TEST116js...	VMware Tools	\\LogMonitor\EventLog\Application
Warning	6/27/2014 14:37:24	* [ warning] [vmusr:vmusr] Error in the RP...		TEST116((n...	TEST116js...	VMware Tools	\\LogMonitor\EventLog\Application
Warning	6/27/2014 14:37:23	* [ warning] [vmusr:vmusr] Error in the RP...		TEST116((n...	TEST116js...	VMware Tools	\\LogMonitor\EventLog\Application
Warning	6/27/2014 14:37:22	* [ warning] [vmusr:vmusr] Error in the RP...		TEST116((n...	TEST116js...	VMware Tools	\\LogMonitor\EventLog\Application
Warning	6/27/2014 14:37:21	* [ warning] [vmusr:vmusr] Error in the RP...		TEST116((n...	TEST116js...	VMware Tools	\\LogMonitor\EventLog\Application
Warning	6/27/2014 14:37:20	* [ warning] [vmusr:vmusr] Error in the RP...		TEST116((n...	TEST116js...	VMware Tools	\\LogMonitor\EventLog\Application
Warning	6/27/2014 14:37:19	* [ warning] [vmusr:vmusr] Error in the RP...		TEST116((n...	TEST116js...	VMware Tools	\\LogMonitor\EventLog\Application

Total Items: 49081

CSV Export

Page Size: 100

1 / 491

Figure 28: Cimtrak™ Master Repository Event Log Tab

Each Event Log message type has a corresponding icon that allows for quick visual reference to the urgency level of the event. These urgency levels are important to note when configuring E-Mail alert permissions. E-Mail alert permissions are explained in a subsequent section.

**Emergency:** *System is unusable. Highest level of event.*

**Alert:** *Take action immediately.*

**Critical:** *Critical conditions have occurred.*

**Error:** *Error conditions.*

**Warning:** *Warning conditions.*

**Notice:** *Normal condition that requires attention.*

**Information:** *Informational message.*

**Debug:** *Debug-level message. Lowest level of event.*

Specifics relating to message types are discussed in the Appendix of this documentation.



***Data displayed in the Management Console Event Log will not actively refresh as new events occur. Click the Refresh button to update the Event Log.***

#### **4.3.2.1. FILTERING AND SORTING THE MASTER REPOSITORY EVENT LOG**

The Master Repository Event Log can be filtered to only show events matching the specified criteria. Accessing the Master Repository Event Log is accomplished by first clicking once on the Master Repository name/IP Address in the Object Group Tree to select it followed by clicking the Event Log tab in the Web Management Console Information Display Area.

To filter the information displayed in the Master Repository Event Log, drag and drop a column header into the area labelled “Drag a column header here and drop it to group by that column.”

Severity x							
Severity	Event Date/Time	Event	Correction	CimTrak ID	Modified By	Process	Absolute path
Critical (100)							
Critical	3/6/2014 07:50:29	File Modified	Unable to comple...	test112			C:\Windows\System32\wdi\LogFiles\Wdi
Critical	2/28/2014 17:37:14	Directory Added	Unable to comple...	QA-4-109	Owner: Unk...		C:\Windows\SysWOW64\config\systempr
Critical	3/7/2014 13:06:42	File Modified	Unable to comple...	QA-4-109	Owner: Unk...		C:\Windows\System32\wuauclt.exe
Critical	1/28/2014 12:57:36	File Added	Unable to comple...	QA-6672_x86	QA-6672\Ad...	explorer.exe	C:\Documents and Settings\Administrato
Critical	3/7/2014 13:06:43	File Modified	Unable to comple...	QA-4-109	Owner: Unk...		C:\Windows\System32\wucltux.dll
Critical	2/28/2014 17:37:14	Directory Added	Unable to comple...	QA-4-109	Owner: Unk...		C:\Windows\SysWOW64\config\systempr
Critical	3/7/2014 13:06:42	File Modified	Unable to comple...	QA-4-109	Owner: Unk...		C:\Windows\System32\wuaueng.dll
Critical	3/5/2014 13:20:06	File Modified	Unable to comple...	test112			C:\Windows\System32\wdi\LogFiles\Wdi
Critical	3/7/2014 13:26:03	File Deleted	Unable to comple...	QA-4-109	Owner: Unk...		C:\Windows\System32\wuups2.dll
Critical	2/28/2014 17:37:14	Directory Added	Unable to comple...	QA-4-109	Owner: Unk...		C:\Windows\SysWOW64\config\systempr
Critical	3/7/2014 13:11:42	Directory Added	Unable to comple...	QA-4-109	Owner: Unk...		C:\Windows\SysWOW64\config\systempr
Critical	1/3/2014 14:58:21	Directory Added	Unable to comple...	QA-4-109	Owner: Unk...		C:\Windows\SysWOW64\config\systempr
Critical	3/7/2014 13:12:02	Directory Added	Unable to comple...	QA-4-109	Owner: Unk...		C:\Windows\SysWOW64\config\systempr
Critical	2/28/2014 17:37:31	Directory Added	Unable to comple...	QA-4-109	Owner: Unk...		C:\Windows\SysWOW64\config\systempr
Critical	3/7/2014 13:12:02	Directory Added	Unable to comple...	QA-4-109	Owner: Unk...		C:\Windows\SysWOW64\config\systempr
Critical	12/19/2013 13:48:05	Directory Added	Unable to comple...	QA-4-109	Owner: Unk...		C:\Windows\SysWOW64\config\systempr

Total Items: 48819    CSV Export    Page Size: 100    1 / 489

**Figure 29: Cimtrak™ Master Repository Event Log (Sorted)**

#### 4.5. MASTER REPOSITORY LOGGED ON USERS

The Master Repository Logged On Users Tab allows CimTrak™ Administrators the capability to view and modify existing CimTrak™ user connections to the Master Repository. Accessing the Master Repository Logged on Users Tab is accomplished by first clicking once on the Master Repository name/IP Address in the Object Group Tree to select it followed by clicking the Logged On Users tab in the Web Management Console Information Display Area.

The Logged On Users Tab displays information pertaining to any CimTrak™ User connection with the Master Repository. Pertaining information includes:

**Username:** *CimTrak™ Account Username*

**Name:** *Full first and last name associated with the CimTrak™ user account.*

**IP Address:** *IP Address the connection with the Master Repository has been established from.*

**Connect Time:** *Date and Time the connection with the Master Repository occurred.*

Right-clicking on any user account displayed in the Logged On Users Tab allows for additional functionality by means of a context menu. Using the context menu authorized CimTrak™ Administrators have the capability to Edit and Disconnect users.

To edit a currently connected user account, right-click on the user account and select "Edit User". The Edit User dialog will display.

To disconnect a currently connected user account, right-click on the user account and select “Disconnect”. The user will instantly be disconnected without notice.

Username	First Name	Last Name	IP Address	Connect Time
admin			192.168.4.114	6/27/2014 09:52:53
admin			192.168.4.114	6/27/2014 10:51:10
admin			192.168.4.114	6/27/2014 11:03:40

Total Items: 3

Figure 30: Cimtrak™ Master Repository Logged On Users Tab

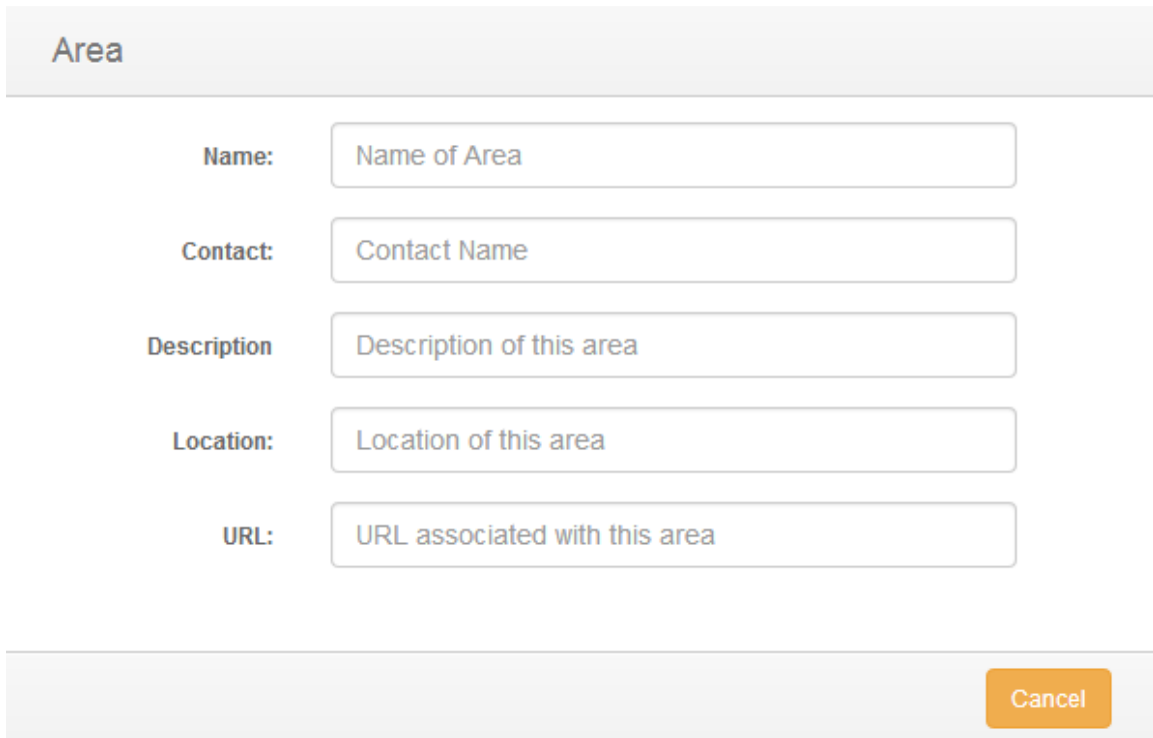
## 4.6. MASTER REPOSITORY AREAS

CimTrak™ allows for the creation of logical Areas in the Web Management Console Object Group Tree. Areas are created to organize Document Control Objects and attached Agents in a logical order. Event logs, permissions, and reports can be ran and configured in unison for all components contained within an Area.

### 4.4.1. CREATING AND DELETING MASTER REPOSITORY AREAS

CimTrak™ allows for the creation of logical Areas in the Web Management Console Object Group Tree. To create an Area, right-click on the Master Repository name/IP Address in the Web Management Console Object Group Tree and then select **New** → **Area**. The Area dialog will display.

The Area dialog allows for the configuration of details relating to a CimTrak™ Area. The only required field is the Name textbox. All additional fields are optional. Populate the fields of the Area dialog and then click OK to create the Area. Click Cancel to abort the Area creation process.

The image shows a dialog box titled "Area". It contains five input fields, each with a label to its left: "Name:" with the placeholder "Name of Area", "Contact:" with the placeholder "Contact Name", "Description:" with the placeholder "Description of this area", "Location:" with the placeholder "Location of this area", and "URL:" with the placeholder "URL associated with this area". At the bottom right of the dialog is an orange button labeled "Cancel".

Area

Name: Name of Area

Contact: Contact Name

Description: Description of this area

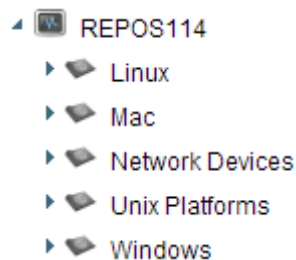
Location: Location of this area

URL: URL associated with this area

Cancel

**Figure 31: Area dialog**

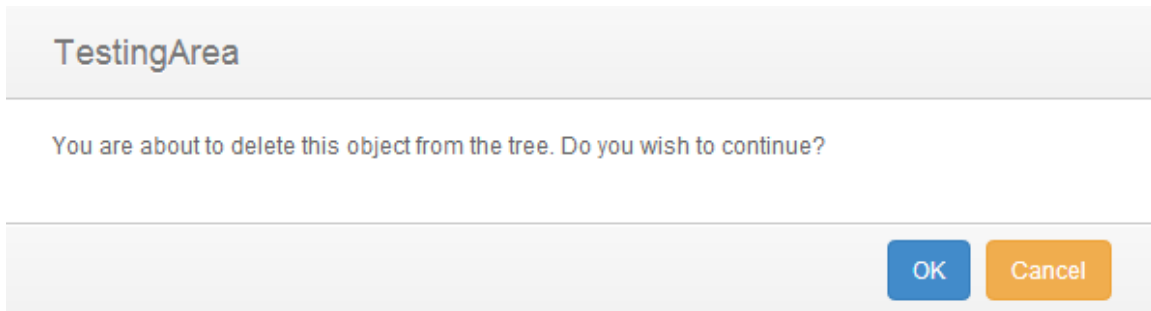
The Area will display in the Object Group Tree.



**Figure 32: Object Group Tree showing Area**

Objects can be removed from Areas by moving the component back to the Master Repository level.

To delete an Area, right-click on the Area and select Delete. The Confirm Delete dialog will display. Click Ok to delete the area or Cancel to abort the deletion.



TestingArea

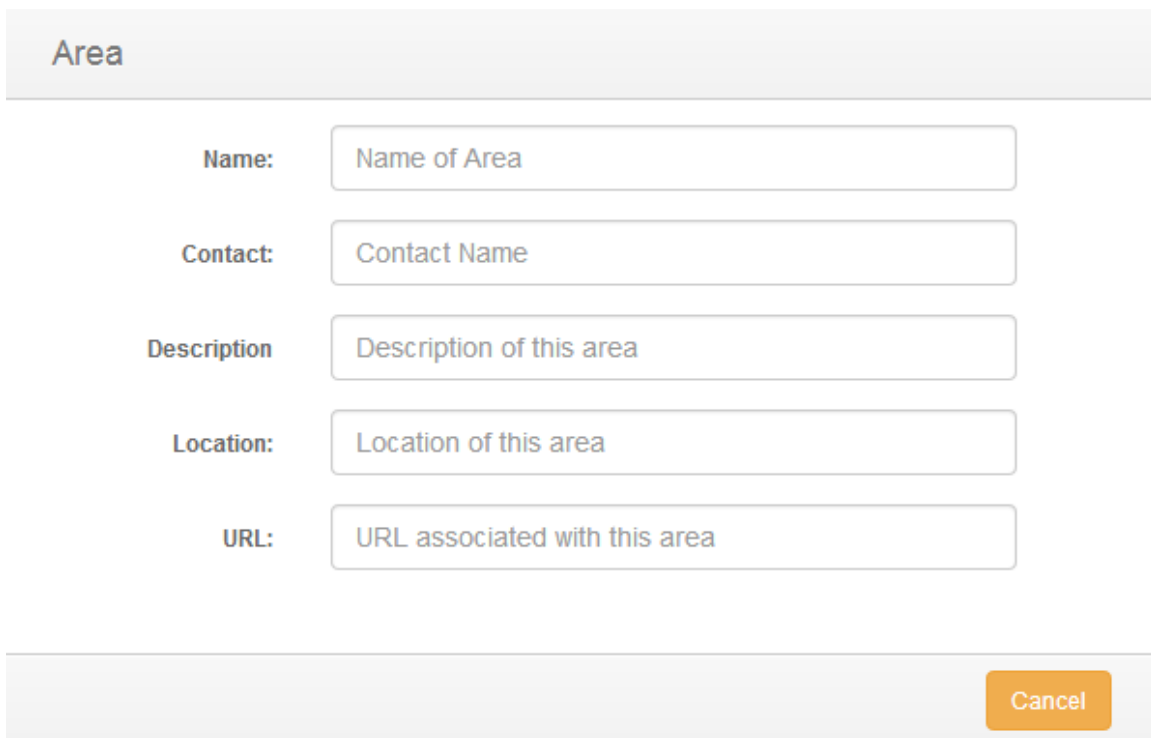
You are about to delete this object from the tree. Do you wish to continue?

OK Cancel

Figure 33: Confirm Delete dialog

#### 4.4.2. MODIFYING MASTER REPOSITORY AREA PROPERTIES

CimTrak™ allows for the editing of properties associated with logical Areas in the Web Management Console Object Group Tree. To edit the properties of an Area, right-click on the Master Repository name/IP Address in the Web Management Console Object Group Tree and then Properties. The Area dialog will display.



Area

Name:

Contact:

Description:

Location:

URL:

Cancel

Figure 34: Area dialog

The Area dialog allows for the configuration of details relating to a CimTrak™ Area. The only required field is the Name textbox. All additional fields are optional. Populate the fields of the Area dialog and then click OK to update the Area. Click Cancel to abort the Area creation process.



***CimTrak™ Areas can be renamed by right-clicking the Area in the Web Management Console Object Group Tree and then selecting Rename.***

#### 4.4.3. MANAGING AREA PERMISSIONS

CimTrak™ Areas can be configured restrict access to children objects based on permission settings. Additionally, event notifications can be configured to notify CimTrak™ Users about events relating to the Area and children objects. Accessing Area permissions is accomplished by first clicking once on the Area in the Object Group Tree to select it and then right-clicking and selecting Permissions. The Security Permissions dialog will display.

By default each Area will have the following permissions:

##### **Administrators**

**Create Objects:** *Create Object Groups.*

**Edit:** *Edit Object Group settings.*

**Lock:** *Enable active monitoring of Object Group data.*

**Reports:** *View reports relating to children objects.*

**Unlock:** *Disable active monitoring of Object Group Data.*

**View:** *View contents and configurations relating to children data.*

##### **Auditors**

**Reports:** *View reports relating to children objects.*

**View:** *View contents and configurations relating to children data.*

##### **Installers**

*Attach CimTrak™ Agents to a Master Repository.*

Default access permissions associated with the Administrators, Auditors, and Installers User Groups cannot be changed. It is possible to modify E-mail alert notices for Administrator and Auditor user groups. Available E-mail alert types include:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Information

Additional information relating to these alert types is described in a subsequent section.

Permissions for Object

Add

Group or User Names

Group	Administrators
Group	Auditors
Group	Installers

Permissions	Allow	Deny
Create Objects	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Edit	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lock	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Reports	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Unlock	<input checked="" type="checkbox"/>	<input type="checkbox"/>
View	<input checked="" type="checkbox"/>	<input type="checkbox"/>

☒ Apply permissions to children recursively

OK

Cancel

**Figure 35: Area Security Permissions dialog**

#### 4.4.3.1. MODIFYING EXISTING USER/GROUP PERMISSIONS

It is possible to modify existing user and group Permissions and E-mail notification settings. Accessing Area permissions is accomplished by first clicking once on the Master Repository IP Address/Name in the Object Group Tree to select it and then right-clicking and selecting “Permissions” from the context menu. The Security Permissions dialog will display.

Select the existing user or group by clicking once on the CimTrak™ User or Group name in the Group or User Names section of the Security Permissions dialog. The Permissions section of the Security Permissions dialog will update to show the permissions currently assigned to the selected user or group.





***Selecting a group will apply the selected permissions and E-mail notification settings to all members of the group. Selecting a single user will apply the selected permissions and E-mail notification settings to only that single user account.***

To add or remove permissions click the “Allow” or “Deny” checkbox corresponding to the permission being configured. Available permissions include:

**Create Objects:** *Create Object Groups.*

**Edit:** *Edit Object Group settings.*

**Lock:** *Enable active monitoring of Object Group data.*

**Reports:** *View reports relating to children objects.*

**Unlock:** *Disable active monitoring of Object Group Data.*

**View:** *View contents and configurations relating to children data.*

**Create Objects:** *Create Object Groups.*

**Edit:** *Edit Object Group settings.*

**Lock:** *Enable active monitoring of Object Group data.*

**Reports:** *View reports relating to children objects.*

**Unlock:** *Disable active monitoring of Object Group Data.*

**View:** *View contents and configurations relating to children data.*

**Email Emergency:** *Receive alerts relating to emergency level notifications.*

**Email Alert:** *Receive alerts relating to alert level notifications.*

**Email Critical:** *Receive alerts relating to critical level notifications.*

**Email Error:** *Receive alerts relating to error level notifications.*

**Email Warning:** *Receive alerts relating to warning level notifications.*

**Email Notice:** *Receive alerts relating to notice level notifications.*

**Email Information:** *Receive alerts relating to information level notifications.*

To apply the permission settings to all children objects, ensure that the Apply permissions to children recursively checkbox is selected.

When completed, click “OK” to apply the permission and alert settings. Click “Cancel” to abort the security permission configuration.



***Permissions and notification settings can be inherited from parent objects (such as the Master Repository) if the permissions are created at a parent level.***



***Permissions and notification settings are not automatically inherited for new objects. It will be necessary to manually assign the permissions and notification settings to the object.***

#### **4.4.3.2. ADDING AND REMOVING USERS AND GROUPS TO AREA PERMISSIONS**

It is possible to add additional users and groups to the Security Permissions dialog so that Area Permissions and E-mail notification settings can be assigned

or changed. Accessing Master Repository permissions is accomplished by first clicking once on the Master Repository IP Address/name in the Object Group Tree to select it and then right-clicking and selecting Permissions. The Security Permissions dialog will display.

To add a new local CimTrak™ User or Group, click the Add button. The Add Users dialog will display listing all available local users and groups.

Select Users or Groups

Q Search

	Type	Name
<input type="checkbox"/>	User	test2
<input type="checkbox"/>	User	wade
<input type="checkbox"/>	User	knightrider
<input type="checkbox"/>	User	payton
<input type="checkbox"/>	User	Pippen
<input type="checkbox"/>	User	Hanks
<input type="checkbox"/>	User	Rose
<input type="checkbox"/>	User	Garnett
<input type="checkbox"/>	User	Fridge
<input type="checkbox"/>	User	alberts
<input type="checkbox"/>	User	aaaa

OK

Cancel

**Figure 36: Add Users dialog**

Select the local CimTrak™ User or Group to add by selecting the checkbox to the left of the name. Click “OK” to add the User or Group. Click “Cancel” to abort the addition process. The selected user or group will now display in the Group or User Names section of the Security Permissions dialog.

The User or Group is now available to have permissions and notification settings assigned.

The Search String(s) textbox provides a space for entering the users or groups that should be searched for additional options. It is possible to search for multiple objects by separating each name/group with a semicolon. The following are syntax examples:

**Display Name:** John Smith

**User Name:** smith.john

**Group Name:** Domain Admins

Once completed entering the search criteria click "Search". Clicking "Cancel" will abort the AD/LDAP user search.

#### **4.4.4. AREA EVENT LOG**

The Area Event Log provides audit information relating to events occurring in the Area and objects connected to the Area. Accessing the Area Event Log is accomplished by first clicking once on the Area name in the Object Group Tree to select it followed by clicking the Event Log tab in the Web Management Console Information Display Area.

The Area Event Log displays details of all events that have occurred on the Area and objects connected to the Area. The level of detail displayed is dependent on the auditing level configured in the Master Repository Properties Log Administrative DB Changes. See section 0 for additional information.

For each recorded event, the Area Event Log will display information corresponding to the following:

**Event Date/Time:** *The exact date and time of the detected event.*

**Event:** *Brief description of the detected event.*

**Correction:** *The action taken on the detected event.*

**Performed by:** *CimTrak™ User Account responsible for the detected event.*

**Modified by:** *File System User responsible for the detected event..*

**Absolute Path:** *File path affected by the detected event.*

**Completion Date/Time:** *Date and time the correction response completed.*

**Event Code:** *Internal CimTrak™ Event Code corresponding to the detected event.*

**Path:** *Object Tree Path to the affected CimTrak™ object.*

Severity	Event Date/Time	Event	Correction	CimTrak ID	Modified By	Process	Absolute path
Critical	6/18/2014 10:53:24	Agent REPOS114->Windows->Windows ...					
Critical	6/18/2014 10:53:20	Agent REPOS114->Windows->Windows ...					
Critical	6/18/2014 10:53:17	Agent REPOS114->Windows->Windows ...					
Critical	6/16/2014 10:34:45	Agent REPOS114->Windows->Windows ...					
Critical	6/16/2014 10:34:45	Agent REPOS114->Windows->Windows ...					
Critical	6/16/2014 10:34:45	Agent REPOS114->Windows->Windows ...					
Critical	6/13/2014 10:15:20	Agent REPOS114->Windows->Windows ...					
Critical	6/13/2014 10:15:20	Agent REPOS114->Windows->Windows ...					
Critical	6/13/2014 10:15:19	Agent REPOS114->Windows->Windows ...					
Critical	6/12/2014 11:50:45	Agent REPOS114->Windows->Windows ...					
Critical	6/12/2014 11:50:44	Agent REPOS114->Windows->Windows ...					
Critical	6/12/2014 11:50:44	Agent REPOS114->Windows->Windows ...					
Warning	6/6/2014 09:56:12	Agent REPOS114->Windows->Windows ...					
Warning	6/6/2014 09:56:09	Agent REPOS114->Windows->Windows ...					
Warning	6/6/2014 09:56:07	Agent REPOS114->Windows->Windows ...					
Warning	6/4/2014 10:12:10	Agent REPOS114->Windows->Windows ...					
Warning	6/4/2014 10:12:08	Agent REPOS114->Windows->Windows ...					

**Figure 37: Area Event Log**

Each Event Log message type has a corresponding icon that allows for quick visual reference to the urgency level of the event. These urgency levels are important to note when configuring E-Mail alert permissions. E-Mail alert permissions are explained in a subsequent section.

**Emergency:** *System is unusable. Highest level of event.*

**Alert:** *Take action immediately.*

**Critical:** *Critical conditions have occurred.*

**Error:** *Error conditions.*

**Warning:** *Warning conditions.*

**Notice:** *Normal condition that requires attention.*

**Information:** *Informational message.*

**Debug:** *Debug-level message. Lowest level of event.*

Specifics relating to message types are discussed in a subsequent section.



***Data displayed in the Area Event Log will not actively refresh as new events occur. Click the Refresh button to update the Event Log.***

#### **4.4.4.1. FILTERING AND SORTING THE AREA EVENT LOG**

The Area Event Log can be filtered to only show events matching the specified criteria. Accessing the Area Event Log is accomplished by first clicking once on the Area in the Object Group Tree to select it followed by clicking the Event Log tab in the Web Management Console Information Display Area.

To filter/sort the information displayed in the Area Event Log, drag and drop a column header into the area labelled “Drag a column header here and drop it to group by that column.”





















#### **4.7. MASTER REPOSITORY TEMPLATES**


Certain CimTrak™ components, such as Agents, have the capability to store pre-configured policies in the form of Templates. Templates can be imported, exported, and deleted to/from Master Repositories. Template maintenance is performed using the Template Maintenance dialog access by right-clicking the Master Repository in the Object Tree and selecting “Template Maintenance” from the context menu.

Template Maintenance

Q

Search

Template Name	Export	Delete
109	 Export	 Delete
AD+SQL+FSA	 Export	 Delete
jovotest-progfiles	 Export	 Delete
Linux Operating System	 Export	 Delete
linux with etc store	 Export	 Delete
new policy	 Export	 Delete
program files	 Export	 Delete
services	 Export	 Delete
services v2	 Export	 Delete
test1-oktodelete	 Export	 Delete

 Import

Close

**Figure 38: Template Maintenance**

By default, CimTrak™ is preconfigured with a CimTrak™ File System Agent Windows Directory template. Using templates to create Object Groups is discussed in subsequent sections.

#### 4.5.1. MODIFYING EXISTING USER/GROUP PERMISSIONS

It is possible to modify existing user and group Permissions and E-mail notification settings. Accessing Master Repository permissions is accomplished by first clicking once on the Master Repository IP Address/Name in the Object Group Tree to select it and then right-clicking and selecting “Permissions” in the context menu. The Security Permissions dialog will display.

Select the existing user or group by clicking once on the CimTrak™ User or Group name in the Group or User Names section of the Security Permissions

dialog. The Permissions section of the Security Permissions dialog will update to show the permissions currently assigned to the selected user or group.



***Selecting a group will apply the selected permissions and E-mail notification settings to all members of the group. Selecting a single user will apply the selected permissions and E-mail notification settings to only that single user account.***

To add or remove permissions click the “Allow” or “Deny” checkbox corresponding to the permission being configured. Available permissions include:

**Create Objects:** *Create Object Groups.*

**Edit:** *Edit Object Group settings.*

**Lock:** *Enable active monitoring of Object Group data.*

**Reports:** *View reports relating to children objects.*

**Unlock:** *Disable active monitoring of Object Group Data.*

**View:** *View contents and configurations relating to children data.*

To apply the permission settings to all children objects, ensure that the Apply permissions to children recursively checkbox is selected.

When completed, click “OK” to apply the permission and alert settings. Click “Cancel” to abort the security permission configuration.



***Permissions and notification settings can be inherited from parent objects (such as the Master Repository) if the permissions are created at a parent level.***



***Permissions and notification settings are not automatically inherited for new objects. It will be necessary to manually assign the permissions and notification settings to the object.***

#### **4.5.2. IMPORTING MASTER REPOSITORY TEMPLATES**

CimTrak™ has the capability to import Object Group Templates from other Master Repositories. Importing of Templates is performed using the Template Maintenance dialog accessed from the CimTrak™ Web Management Console Menu Bar by right-clicking the Master Repository in the Object Tree and selecting “Template Maintenance” from the context menu.

To import a single template or multiple templates click the Import button and then click the button labelled “Choose Files”. The Import Template(s) dialog will display. Click the Add button to browse the file system for CimTrak™ templates. The Open File dialog will display. Select the template file and then click Open to import the template or Cancel to abort the import process.

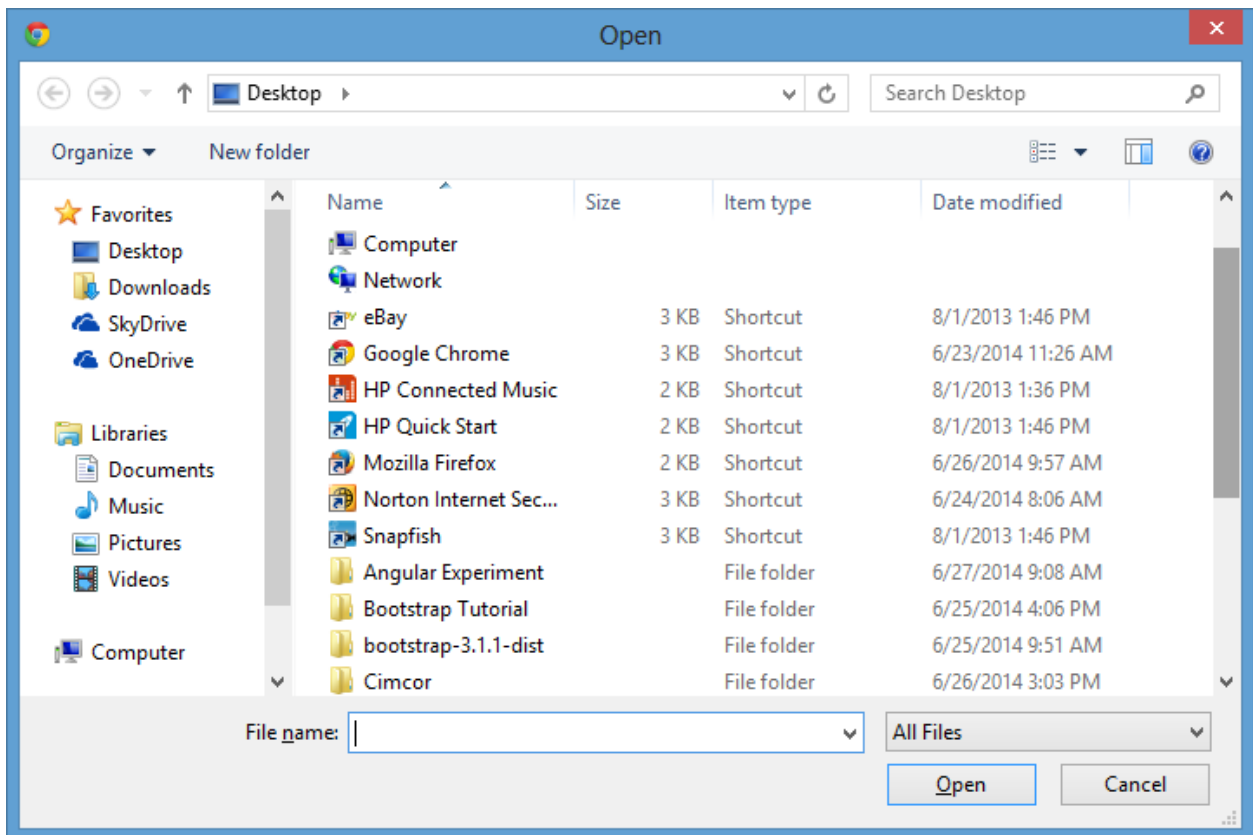


Figure 39: Template Open dialog

The selected template will display in the Import Template(s) dialog. Click Add to add additional templates or Remove to remove templates. When completed click OK to return to the Templates Maintenance dialog. Clicking cancel will abort the import process.



**Select the Private Checkbox to make the imported template only accessible to your CimTrak™ user account.**

#### 4.5.3. EXPORTING MASTER REPOSITORY TEMPLATES

CimTrak™ has the capability to export Object Group Templates from the Master Repository. Exporting of Templates is performed using the Template Maintenance dialog accessed by right-clicking the Master Repository in the Object Tree and selecting “Template Maintenance” from the context menu.

To export a template, select the appropriate template and then click the Export button.

Exported templates can be imported into another Master Repository using the Import feature discussed in section 4.5.2. Optionally, exported templates can be modified in a text editor to enable custom configurations.



#### 4.5.3.1. CUSTOMIZING EXPORTED MASTER REPOSITORY TEMPLATES

It is possible to modify Object Group Templates that have been exported from the Master Repository. Once a Template has been modified it can then be imported into a Master Repository. Exporting of Templates is explained in section 4.5.3. Importing of Templates is explained in section 4.5.2.

Templates created for CimTrak™ File System Agent monitoring of Microsoft Windows operating system folders can be customized to include environment variables. The use of environment variables is important when deploying templates across multiple systems that may not have consistent file system structures. For example, one system's Windows Directory may be "C:\WINNT" while another may be "C:\Windows". Customizing the Template with environment variables can help facilitate this scenario.

After exporting the Template open it in a text editor. Navigate to the line beginning with the path parameter. If the path parameter value is "C:\Windows" change it to "<WindowsDirectory>".

Save the changes and import the template back into the Master Repository. This template can now be used to monitor the Windows directory in any supported version of Microsoft Windows. Additional environment variables exist for additional customization.

Environment Variable	Windows 2000 Example	Windows XP Example
<SystemDirectory>	C:\WINNT\system32	C:\Windows\system32
<WindowsDirectory>	C:\WINNT	C:\Windows
<SystemWindowsDirectory>	C:\WINNT	C:\Windows

**Table 1: Template Environment Variables**

Additionally, templates can be customized using regular expressions. If a Template is used to create an Object Group, and the Template has specified files and folders to be excluded, the files within the locked folder that match the excluded files in the Template are automatically excluded. However, the excluded entries are case sensitive. For example, if the Template file lists "C:\data\exclude.txt" as an excluded file, and the actual filename path is "C:\data\Exclude.txt", the file will not be excluded.

It is possible to modify the Template replacing the static path and filename of a file with dynamic Regular Expressions. This will make the Excluded file or directory case insensitive.

For example, the case sensitive path and filename:

```
Excludepath1 = C:\WINDOWS\system32\  
Excludefile1 = wpa.dbl  
Excludetype1 = File
```

...can be modified to a case insensitive path and filename:

Excludepath1 = [a-zA-Z]:\\.+\\[sS][yY][sS][tT][eE][mM]32\\

Excludefile1 = [wW][pP][aA]+\\. [dD][bB][!L]\$

Excludetype1 = Regular Expression

Please note that the first entry set specifically lists the exact path of the file; the second lists a Regular Expression wildcard path before the \system32\ directory. Using wildcards the wpa.dbl file can be locked in various versions of Windows.

## 5. Configuring and Using the CimTrak™ File System Agent

### 5.1. MANAGING THE CIMTRAK™ FILE SYSTEM AGENT FROM THE WEB MANAGEMENT CONSOLE

Management of the CimTrak™ File System Agent requires that the Web Management Console is associated with the Master Repository and that a valid user account has been authenticated. For more information on associating the Web Management Console with the Master Repository please refer to section 3.1.

Once authenticated with the Master Repository multiple configuration, customization, and reporting options are available through the Web Management Console.

File System Agents that have been installed and associated with the selected Master Repository will display in the CimTrak™ Web Management Console's Object Group Tree.

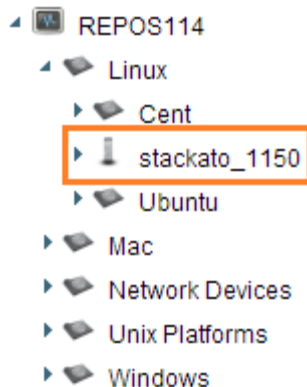


Figure 40: CimTrak™ File System Agent in Object Group Tree

The connection status of the CimTrak™ File System Agent can be confirmed by the associated icon.



Figure 41: Cimtrak™ File Sytem Agent Connection Icon

5.1.1. FILE SYSTEM AGENT PROPERTIES

The File System Agent Properties dialog allows authorized CimTrak™ users to perform administrative tasks relating to CimTrak™ File System Agent logging, throttling, heartbeat and statistic transmissions and health monitoring parameters.

Accessing the CimTrak™ File System Agent Properties dialog is accomplished by right-clicking on the File System Agent name in the Object Group tree and then selecting “Properties.” The CimTrak™ Agent Configuration dialog will display.

The CimTrak™ Agent Configuration dialog consists of several functional sections including:

- Description
- Agent Throttling
- Number of Events to Keep
- DB Options
- Poll Intervals

The functionality associated with these sections is explained in subsequent sections.

Agent Properties

Name	stackato_1150		Date In Service		
Location			Description		
URL			Contact		
Events to Keep	0	Ever (0=no limit)	Cancel Lock when exceeds	200000	objects (0=no limit)
Agent Throttling	1		Agent Stats Interval	10	seconds
HeartBeat Interval	30	seconds	Offline Event Cache	Off	
Warn if Disconnected	0	minutes			
Whitelist Mode	Off				

OK

Cancel

Figure 42: CimTrak™ Agent Configuration

5.1.1.1. CONFIGURING THE FILE SYSTEM AGENT DESCRIPTION PROPERTIES

The CimTrak™ File System Agent Description and associated information can be customized through the CimTrak™ Agent Configuration dialog. Accessing the CimTrak™ Agent Configuration dialog is accomplished by right-clicking on the File System Agent name in the Object Group tree and then selecting “Properties.” The CimTrak™ Agent Configuration dialog will display.

Name	stackato_1150	Date In Service	
Location		Description	
URL		Contact	

**Figure 43: File System Agent Description**

**File System Agent Description Information:**

**Name:** *Used to indicate a unique name for the File System Agent.*  
**Date in Service:** *Optional Date and Time associated with the in-service date of the File System Agent*  
**Location:** *Optional File System Agent Location information.*  
**Description:** *Optional File System Agent Description information.*  
**URL:** *Optional URL information associated with the File System Agent..*  
**Contact:** *Optional Contact information associated with the File System Agent.*

Once all sections have been populated, click the “OK” button to save the File System Agent Description Information. Click “Cancel” to abort the File System Agent properties modification.



***A File System Agent can be renamed by either changing the name in the Name textbox or by right-clicking the File System Agent in the Object Group Tree and selecting “Rename”.***

**5.1.1.2. CONFIGURING THE FILE SYSTEM AGENT LOG RETENTION PROPERTIES**

The CimTrak™ File System Agent log retention settings can be customized through the CimTrak™ Agent Configuration dialog. Accessing the CimTrak™ Agent Configuration dialog is accomplished by right-clicking on the File System Agent name in the Object Group tree and then selecting “Properties.” The CimTrak™ Agent Configuration dialog will display.

The Number of Events to Keep section of the dialog allows for the configuration of File System Agent Event Log data retention. The event log can be configured to flush older records on a day interval or message quantity limit.

Events to Keep	0	Ever ▼	(0=no limit)
----------------	---	--------	--------------

**Figure 44: Number of Events to Keep settings**

**Days:** The event log will automatically remove event messages older than the indicated value. Entering “0” will store event messages indefinitely. (Maximum Days: 10,000)

**Quantity:** The event log will automatically remove older event messages as the amount of messages exceeds the indicated value. Entering “0” will store event messages indefinitely. (Maximum Quantity: 10,000)



***Storing an unlimited number of events has the potential to exhaust all available disk space on the Master Repository and degrade system performance.***

Once the data retention settings have been selected, click the “OK” button to save the File System Agent properties configuration. Click “Cancel” to abort the File System Agent properties configuration.

#### **5.1.1.3. CONFIGURING THE FILE SYSTEM AGENT DISCONNECT WARNING**

The CimTrak™ File System Agent must remain in communication with the Master Repository at all times. If configured a failure to communicate with the Master Repository can generate an auditable event. Setting of disconnection notices is performed in the CimTrak™ Agent Configuration dialog. Accessing the CimTrak™ Agent Configuration dialog is accomplished by right-clicking on the File System Agent name in the Object Group tree and then selecting “Properties.” The CimTrak™ Agent Configuration dialog will display.

The DB Options section of the dialog allows for the configuration of Agent disconnection warnings. Warnings are generated if the Agent is out of communication with the Master Repository for a time period longer than the specified time in minutes. Accepted values (in minutes) include 1 through 4,194,304. Setting the “Warn if Disconnected” minute value to 0 disables the warning.

Warn if Disconnected  minutes

Figure 45: CimTrak™ Agent DB Options settings



***The notification of the disconnect occurs at the nearest heartbeat transmission. For example, if a heartbeat is set to 30 seconds and the disconnect is set to 2 minutes the alert will occur between 2 minutes and 2 minutes, 30 seconds depending on where the event occurs in the heartbeat cycle.***

Once the DB Options settings have been selected, click the “OK” button to save the File System Agent properties configuration. Click “Cancel” to abort the File System Agent properties configuration.

#### **5.1.1.4 CONFIGURING THE FILE SYSTEM AGENT HEARTBEAT AND STATISTIC GATHERING INTERVAL**

The CimTrak™ File System Agent communications can be throttled to control the speed of communications with the Master Repository. This capability is useful in limiting network bandwidth requirements and CPU cycles on the Agent host operating system. Setting of Agent Throttling is performed through the CimTrak™ Agent Configuration dialog. Accessing the CimTrak™ Agent Configuration dialog

is accomplished by right-clicking on the File System Agent name in the Object Group tree and then selecting “Properties.” The CimTrak™ Agent Configuration dialog will display.



**Figure 46: File System Agent Throttling settings**

Setting Agent Throttling does not delay the remediation capabilities of the File System Agent. The Throttle is applied to communication transfer relating to events. The Throttle indicates the wait time between file transmissions and/or 60 KB data transmission.

The Throttle applies to the following scenarios:

- Sending Watch Data and Files to the Master Repository
- Syncing Watch Directories
- Locking Directories

Sliding the Agent Throttling slider to the left reduces the throttling (speeds up communications). Sliding the Agent Throttling slider to the right increases the throttling (slows down communications). By default, the Agent Throttling is set one tick right of Off.

Once the Agent Throttling settings have been selected, click the “OK” button to save the File System Agent properties configuration. Click “Cancel” to abort the File System Agent properties configuration.

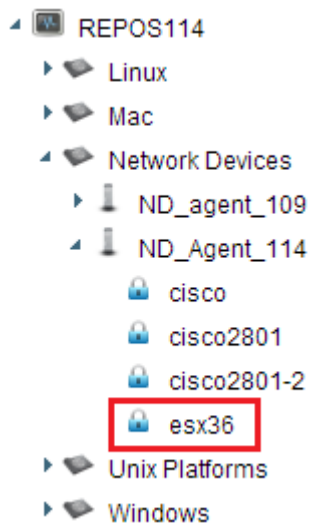
#### **5.1.1.5 CREATING AND EDITING OBJECT GROUP WATCH POLICIES**

The File System Agent has the capability to monitor critical files and operating system configurations on the host system containing the File System Agent or remote file shares. For many monitored files and configurations, CimTrak™ has the capability to remediate detected changes. To enable monitoring the CimTrak™ File System Agent must have Object Group Policies created and enabled.

To create a new Object Group Watch Policy, select the File System Agent of the system to monitor by clicking it once in the Web Management Console’s Object Group Tree, right-click and select **New** → **Object Group** in the Context menu. The Object Group Properties dialog will display.

To edit an Object Group Watch Policy, select the Object Group Policy to modify by right-clicking its name in the Object Group Tree. Select **Properties** in the Context menu. The Object Group Properties dialog will display.

Once the Object Group has been created it will display in the CimTrak™ Web Management Console’s Object Group Tree.



**Figure 47: CimTrak™ Web Management Console's Object Group Tree Showing Object Groups**

To enable monitoring of the Object Group it must be “locked”. Detailed information about creating Object Group Watch Policies and enabling/disabling monitoring is explained in subsequent sections.

#### **5.1.1.5.1. OBJECT GROUP PROPERTIES**

The process of creating a new or editing an Object Group Watch Policy can be initiated by selecting the File System Agent of the system to monitor by clicking it once in the Web Management Console's Object Group Tree, clicking the “New” drop-down button in the Menu Bar, followed by Object Group. The Object Group Properties dialog will display.

To edit an Object Group Watch Policy, select the Object Group Policy to modify by right-clicking its name in the Object Group Tree. Select **Properties** in the Context menu. The Object Group Properties dialog will display.

The Object Group Properties dialog is comprised of several sections. Each of these sections has specific functionality relating to the monitoring performed by the File System Agent.



Object Group Properties

**Policy** | **Attributes**

Location: [Location]  
 Description: [Description]  
 Date Put In Service: 2013-09-10 14:59:13  
 Contact: [Name of Contact]  
 URL: [ ]

Notes: [ ]  
 Require Notes On Lock: ☐

Number of Intrusions to Keep: 250  
 Keep Intrusion Size (in KB): 500  
 Number of Revisions to Keep: 250  
 Warn if Unlocked (in minutes): 0  
 Events To Keep (0=no limit): 250 Events

Watched in this group ■  
 Watched elsewhere ■

OK Cancel

**Figure 48: Cimtrak™ Object Group Properties Dialog (Attributes Tab)**

**Object Information**  
**Private Key Implementation**  
**Monitoring Information**  
**Operating System Tree**  
**Watch Properties**

### File System Agent Object Information:

Object Information provides CimTrak™ Users and Administrators detailed information pertaining to the Object Group Watch Policy. The “Object Group Name” is the only required field. Object Group Names must be unique and may contain between 1 and 49 characters.

Location: [Location]  
 Description: [Description]  
 Date Put In Service: 2013-09-10 14:59:13  
 Contact: [Name of Contact]  
 URL: [ ]

Notes: [ ]  
 Require Notes On Lock: ☐

**Figure 49: File System Agent Object Information**

**Location:** *Optional Object Group Location information.*  
**Description:** *Optional Object Group Description information.*  
**Date Put in Service:** *Optional Date and Time associated with the in-service date of the Object Group.*  
**Contact:** *Optional Contact information associated with the Object Group.*  
**URL:** *Optional URL information associated with the Object Group.*  
**Notes:** *Optional dialog to enter administrative notes associated with the Object Group.*

Optionally, the Object Group Watch Policy has the capability to require CimTrak™ Users and Administrators to enter notes when enabling monitoring of the Object Group Watch Policy. Enabling of required notes is performed by selecting the Require Notes on Lock checkbox.

### **Monitoring Information:**

**Number of Intrusions to Keep:** *Number of added files/configurations to keep in the Change Log. A zero placed in this field indicates unlimited changes will be stored. Maximum accepted value of 10,000 changes.*

**Keep Intrusion Size (in KB):** *The maximum file size an added file can be for it to be stored in the Change Log. Files exceeding this change size limit are still detected but cannot be compared or retrieved. Maximum accepted value of 4,194,304 KB.*

**Number of Revisions to Keep:** *Number of revisions to keep for each change to files and configurations monitored by the Object Group. A zero placed in this field indicates unlimited changes will be stored. Maximum accepted value of 10,000 revisions*

**Warn if Unlocked (in minutes):** *Generate a notice if monitoring of the Object Group has been disabled for more than the indicated time. A zero placed in this field disables the warning. Maximum accepted value of 10,000 minutes.*

**Number of Events to Keep:** *Quantity or Days to store Object Group Event Log audit records. Maximum accepted value of 10,000 events.*



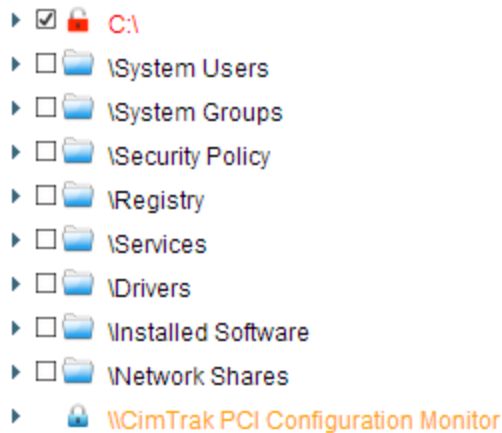
***Storing an unlimited number of events, revisions, or changes has the potential to exhaust all available disk space on the Master Repository and degrade system performance.***

Number of Intrusions to Keep	<input type="text" value="250"/>	Number of Revisions to Keep	<input type="text" value="250"/>	Events To Keep (0=no limit)	<input type="text" value="250"/>	<input type="text" value="Events"/>
Keep Intrusion Size (in KB)	<input type="text" value="500"/>	Warn if Unlocked (in minutes)	<input type="text" value="0"/>			

**Figure 50: File System Agent Monitoring Information**

### **Operating System Tree**

The Operating System Tree, located at the lower left corner of the Object Group Properties dialog, contains a listing of all files, folders, and operating system configurations that can be monitored by the CimTrak™ File System Agent. The contents of the Operating System Tree are system specific. Additionally, external CimTrak™ Plug-ins attached to the File System Agent will appear in the Operating System Tree.

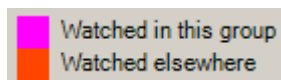


**Figure 51: Microsoft Windows Operating System Tree**

Selecting data to monitor is accomplished by checking the checkbox next to the system component. The contents of the Operating System Tree can be expanded or collapsed by clicking the ► or ◄ symbols corresponding with each monitor type. Selecting any monitor data results in the Watch Properties dialog to display. See a subsequent section for more information on setting Watch Properties.



***Content that is monitored in the current Object Group is displayed in the File System Tree in a pink font color. Content that is monitored elsewhere is displayed in a orange font color.***



**Figure 52: Watch notifications**

### **Microsoft Windows File System Agents have the capability to monitor:**

**Drivers:** *Drivers are specialized programs designed to run in the background of a system and to control specific hardware. This feature allows security professionals the capability to monitor drivers for changes, additions, or deletions. Remediation capability is not available for monitoring of system drivers. The recommended monitoring mode is “Update Baseline”. This feature supports polling detection.*

**Installed Software:** *Installed Software monitoring detects any software that has been installed using a standard installation tool. This mode displays any software that is registered in Microsoft Windows to display in the “Add/Remove Programs” dialog. This feature allows security professionals the capability to monitor if new or additional software has been installed or uninstalled. Remediation capability is not available for monitoring of installed software. The recommended monitoring mode is “Update Baseline”. This feature supports polling detection.*

**Network Shares:** Monitoring of Network Shares allows security professionals the capability to monitor the share settings associated with files and folders on a Windows operating system. This mode allows for remediation of any detected changes. The recommended monitoring mode is “Restore from Repository”. This feature supports polling detection.

**Registry:** Windows Registry monitoring allows security professionals the capability to define a preset list of registry keys to monitor. CimTrak™ will detect any modifications to this preset list of keys or values. The recommended monitoring mode is “Restore from Repository”. This feature supports polling or real-time detection.

**Security Policy:** Monitoring of the local Security Policy allows security professionals the capability to monitor the settings associated with the local security policy. Local security policies are relevant even if the system is attached to a domain since the local security policies are executed before group policies. Locking the Security Policy helps ensure that the intended local security policies of an organization are maintained. The recommended monitoring mode is “Update Baseline”. This feature supports polling detection.

**Services:** Services are specialized programs designed to run in the background of a system. This feature allows security professionals the capability to monitor when new or additional services have been started or configurations of existing services have been modified. The recommended monitoring mode is “Update Baseline”. This feature supports polling detection.

**System Groups:** Monitoring of local system groups allows security professionals the capability to detect changes to all local user groups existing on the monitored system. CimTrak™ detects when groups are added, deleted, or modified. The recommended monitoring mode is “Update Baseline”. This feature supports polling detection.

**System Users:** Monitoring of local system users allows security professionals the capability to detect when local user accounts are added, deleted, or modified on the system. Using this feature is important even if the system is attached to a domain as additional or modified local user accounts can create a system vulnerability. The recommended monitoring mode is “Update Baseline”. This feature supports polling detection.

**Local File System:** Monitoring of the local file system will detect (and optionally remediate) any addition, deletion, or modification to files and folders on the monitored system. This feature supports polling or real-time detection.

**Network File System:** Using the optional “Network Drive Enabler” allows for the detection (and optionally remediation) of any addition, deletion, or modification to files and folders to monitored network share data. This feature supports polling detection.

**Linux, UNIX, and Macintosh File System Agents have the capability to monitor:**

**System Groups:** *Monitoring of local system groups allows security professionals the capability to detect changes to all local user groups existing on the monitored system. CimTrak™ detects when groups are added, deleted, or modified. The recommended monitoring mode is “Update Baseline”. This feature supports polling detection.*

**System Users:** *Monitoring of local system users allows security professionals the capability to detect when local user accounts are added, deleted, or modified on the system. Using this feature is important even if the system is attached to a domain as additional or modified local user accounts can create a system vulnerability. The recommended monitoring mode is “Update Baseline”. This feature supports polling detection.*

**Local File System:** *Monitoring of the local file system will detect (and optionally remediate) any addition, deletion, or modification to files and folders on the monitored system. This feature supports polling or real-time detection.*

**Network File System:** *Monitoring of mounted shares allows for the detection (and optional remediation) of any addition, deletion, or modification to files and folders on monitored network shares. This feature supports polling detection.*

### **Watch Properties**

The Watch Properties section shows any currently monitored files, folders, and configurations. Additionally, excluded or included paths and files are displayed. The Watch Properties are explained in detail in subsequent sections.

#### **5.1.1.5.2. WATCH PROPERTIES**

Selecting any object listed in the Object Group Properties File System Tree results in the Watch Properties dialog to display. See section 0 for more information on accessing Object Group Properties.

Watch Properties

When a change occurs

☐ Restore from Repository
☒ Log
☐ Update Baseline
☐ Prompt for Approval
☐ Deny Access

Some software, such as backup utilities or virus detection software, modify various file attributes, which will signal an intrusion to CimTrak.

☒ Ignore Archive Flag
☐ Ignore Read-only Flag
☐ Ignore SACL
☐ Ignore Owner Security
☐ Ignore Alternate Stream Data
☐ Ignore DACL
☐ Ignore Group Security
☐ Ignore File Dates

Authoritative Copy

☐ Store authoritative copy of all files in the CimTrak Repository. This will allow CimTrak to restore files back to their original state.
☒ Don't Store authoritative copy

Event Detection Method

☒ Real-time Detection
☐ Poll Detection (interval)
☐ Poll at Specific Time (Local Time)
☐ Poll at Specific Time (Agent Time)

Store Changes

☐ Store a copy of added/changed files

Other

☐ Log Reads

File Comparison Method

MD5

Connection Loss Strategy

☐ Wait for User Approval on Sync

Auto Exclude

Auto exclude files that have changed 0 times in 60 minutes (0 changes = disabled)

OK

Cancel

**Figure 53: Watch Properties dialog**

The Watch Properties dialog allows for the configuration of detection and reaction parameters. The Watch Properties dialog is comprised of several different sections:

**Corrective Action**  
**Authoritative Copy**  
**File Comparison Method**  
**Store Changes**  
**Options**  
**Event Detection Method**  
**Connection Loss**  
**Auto Exclude**

These sections are explained in detail in subsequent sections. After completing the Watch Properties configuration click OK to accept the changes or Cancel to abort and discard the changes. The Watch Properties dialog will close and the Object Group Properties dialog will display showing the configured Watch Properties in the Watch Properties section.



Optionally, the Custom configuration mode exists allowing for any combination of the primary modes of remediation. For example, when a file is added the administrator may choose to update the baseline; when a file is deleted the administrator may choose to restore the file; when a file is modified the administrator may choose to log the change.

#### When a change occurs

- ☐ Restore from Repository
- ☒ Log
- ☐ Update Baseline
- ☐ Prompt for Approval
- ☐ Deny Access

Figure 55: Corrective Action Properties

Selection of the remediation mode is accomplished by selecting the corresponding radio button.

#### 5.1.1.5.2.2. AUTHORITATIVE COPY

Depending on the Corrective Action used, CimTrak™ has the capability to alter the storage of Authoritative Copy data. The Authoritative Copy refers to a saved copy of “locked” file system/configuration data stored in the Master Repository for the purpose of restoring files to the last known approved state. Additionally, Authoritative Copy data can be used to compare the contents of monitored files and configurations. Authoritative Copy data is stored in the Master Repository using the user configured cryptology and compressed.

#### Authoritative Copy

- ☐ Store authoritative copy of all files in the CimTrak Repository. This will allow CimTrak to restore files back to their original state.
- ☒ Don't Store authoritative copy

Figure 56: Authoritative Copy Parameter Settings



***The compression ratio used by CimTrak™ varies with the type of content being monitored (i.e., images, documents, text files). Generally, the authoritative copy data is stored with a 20-25% compression ratio.***

#### 5.1.1.5.2.3. FILE COMPARISON METHOD

Each file, folder, and configuration monitored by CimTrak™ has a calculated hash value stored in the CimTrak™ Master Repository. The File Comparison



Method parameter setting allows for authorized CimTrak™ Administrators to modify the comparison algorithm used. By default the most powerful method is selected. The methods allowed vary based on the CimTrak™ Cryptology release.

#### File Comparison Method

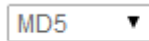


Figure 57: File Comparison Method Parameter Settings

To change the File Comparison Method, select the method to use from the File Comparison Method dropdown.

#### 5.1.1.5.2.4. STORE CHANGES

Depending on the Corrective Action used, CimTrak™ has the capability to alter the storage of change data. Change data refers to a saved copy of modified file system/configuration data stored in the Master Repository for the purpose of compare the contents with the Authoritative Copy. Change data is stored in the Master Repository using the user configured cryptology and compressed.

#### Store Changes

☐ Store a copy of added/changed files

Figure 58: Store Changes Option Checkbox



***The compression ratio used by CimTrak™ varies with the type of change stored (i.e., images, documents, text files). Generally, the change data is stored with a 20-25% compression ratio.***

Selecting the checkbox labelled “Store Changes” will store the change data to the Master Repository using the user configured cryptology and compressed.

#### 5.1.1.5.2.5. AUTO EXCLUDE

When creating an Object Group Watch Policy it is important to tune the configuration to exclude files that are dynamic and need to change. CimTrak™ has the capability to auto-tune the Watch Policy by automatically excluding file that change more times than the designated threshold and interval. The Auto Exclude threshold and interval is configured in the File System Agent Watch Properties dialog.



***The Auto Exclude feature should only be enabled during the initial Object Group Policy tuning process. Leaving this***

***feature enabled indefinitely could result in CimTrak™ missing legitimate system changes.***

By default the Auto Exclude feature is disabled. To enable the Auto Exclude feature, specify the threshold by indicated the amount of times a file or configuration is allowed to change over a specified time in minutes.

#### Auto Exclude

Auto exclude files that have changed  times in  minutes (0 changes = disabled)

**Figure 59: Auto Exclude parameter settings**

Acceptable change values must be between 0 (disabled) and 1,000. The time value must be between 1 minute and 1,440 minutes.

#### 5.1.1.5.2.6. OPTIONS

The CimTrak™ File System Agent Watch Properties has additional customization options available to reduce the number of detected false changes. These additional options are useful to allow CimTrak™ to function properly with backup utilities and source control utilities. Additionally options exist to enable additional monitoring capabilities. The Option settings are available in the File System Agent Watch Properties dialog.

Some software, such as backup utilities or virus detection software, modify various file attributes, which will signal an intrusion to CimTrak.

- |                                                         |                                                |
|---------------------------------------------------------|------------------------------------------------|
| <input checked="" type="checkbox"/> Ignore Archive Flag | <input type="checkbox"/> Ignore Read-only Flag |
| <input type="checkbox"/> Ignore SACL                    | <input type="checkbox"/> Ignore DACL           |
| <input type="checkbox"/> Ignore Owner Security          | <input type="checkbox"/> Ignore Group Security |
| <input type="checkbox"/> Ignore Alternate Stream Data   | <input type="checkbox"/> Ignore File Dates     |

**Figure 60: Options parameter settings**

#### Other

- ☐ Log Reads

**Figure 61: Log Reads Parameter Checkbox**

Option parameter settings are enabled by clicking the corresponding checkbox. Options are disabled when unchecked. The Options parameter settings allow for the custom configuration of the following:

- Ignore Archive Flag: When checked the CimTrak™ File System Agent will ignore any changes that occur to the archive flag.

- Ignore Read-only Flag: When checked the CimTrak™ File System Agent will ignore any changes that occur to the Read-only flag.
- Log Reads: When checked CimTrak™ has the capability to monitor specific files and folders for any form of access. Using this feature will generate audit events whenever a file is viewed or copied.



***Logging of reads requires the File System Agent Forensic Driver. This driver is installed during the installation of the Windows File System Agent.***

#### 5.1.1.5.2.7. EVENT DETECTION METHOD

The CimTrak™ File System Agent has the capability to monitor Object Group Policies in real-time (when supported) or on a polling interval. Configuration of the Event detection method is available in the File System Agent Watch Properties dialog.

##### Event Detection Method

- ☒ Real-time Detection
- ☐ Poll Detection (interval)
- ☐ Poll at Specific Time (Local Time)
- ☐ Poll at Specific Time (Agent Time)

**Figure 62: Event Detection Method parameter settings**

Available event detection methods include:

- **Real-time Detection:** *Real-time Detection will report detected changes immediately when they are performed. The configured remediation mode will automatically initiate immediately upon the detection of a change.*
- **Poll-based Detection:** *Poll-based Detection will report any changes that have occurred since the last poll-based scan. Acceptable values range between 0 (poll only when force-synced) and 1,440 minutes.*



***The Windows File System Agent Forensic Driver will not show forensic assisting information for changes detected using the Poll-based Detection.***



***Scheduled polling is accomplished by setting the Poll-based Detection interval to 0 and scripting the synchronization using the CimTrak™ Command Line Interface. These scripts can then be scheduled using Windows Task Scheduler or Linux/UNIX Cron jobs. The Command Line Interface is explained in section Error! Reference source not found..***

#### 5.1.1.5.2.8. CONNECTION LOSS

Occasionally the CimTrak™ Master Repository may lose connectivity with attached File System Agents due to network errors or mobile devices. When this occurs the option exists to automatically perform Object Group synchronization when the connection is re-established. Setting the Connection Loss settings are available through the Object Group Properties Watch Properties dialog.

##### Connection Loss Strategy

☐ Wait for User Approval on Sync

**Figure 63: Connection Loss parameter settings**

To enable synchronization after a connection loss, select the User Approval on Sync checkbox. To disable synchronization, de-select the User Approval on Sync checkbox.

When User Approval on Sync is enabled, the CimTrak™ Administrator is prompted for the desired action to take on detected changes made during the non-connectivity period. The CimTrak™ Administrator utilizes the Changes Pending Approval Web Management Console dialog to authorize or deny these changes. The Changes Pending Approval dialog is explained in a subsequent section.

The User Approval on Sync dialog has the following default and customizable settings for each of the following corrective actions:

- **Restore from Repository:** *Option can be enabled or disabled. By default this option is disabled.*
- **Log:** *Option is disabled by default and cannot be changed.*
- **Update Baseline:** *Option is disabled by default and cannot be changed.*
- **Prompt for Approval:** *Option is enabled by default and cannot be changed.*

#### 5.1.1.5.2.9. TUNING WATCH PROPERTIES

When an operating system folder or configuration is selected in the Object Group Properties dialog, all children files, folders, and configurations are also selected. Often certain files need to be excluded or included in the particular watch policy. CimTrak™ has the capability to create exclude or include rules for files, folders, and configurations. Creating these advanced rules is accomplished in the selected Object Group's Watch Properties. Accessing the Object Group Properties is accomplished during the creation or editing of an Object Group's Watch Policy. See section 0 for more information on creating Watch Policies.

Monitored folders, files, and configurations will display in the Object Group Properties Watch Properties section. Each displayed item will include the following information:

- **Path:** *The operating system location of the parent folder or configuration.*
- **Object Type:** *The Object Type being monitored (i.e. Directory).*
- **Type:** *Action performed by the Watch Property detail (i.e. Watch, Exclude, etc.).*
- **Store Files:** *Indication of whether or not Authoritative Copy data will be stored in the CimTrak™ Master Repository.*
- **Corrective Action:** *The Corrective Action chosen during the creation of the Object Group Watch Policy.*
- **Detection:** *Indication of the mode of detection (Real-time, Polling).*
- **Ignore Archive Flag:** *Indication of whether or not changes to the Archive Flag will be ignored.*
- **Ignore Read-only Flag:** *Indication of whether or not changes to the Read-only Flag will be ignored.*
- **Comparison Method:** *Displays the comparison method selected in the Object Group's Watch Properties.*
- **Quarantine:** *Indication of whether or not Change Data will be stored in the CimTrak™ Master Repository.*

Path	Object Type	Type	Store Files	Corrective Ac...	Detection	C
▲ C:\testabc (2 )						
C:\testabc	Directory	Watch	No	Log	Real-time	M
[a-zA-Z]:\.\+\\[sS][yY][sS][tT][eE][m...	Regular Expr...	Exclude				

Figure 64: Watch Properties section showing monitored data

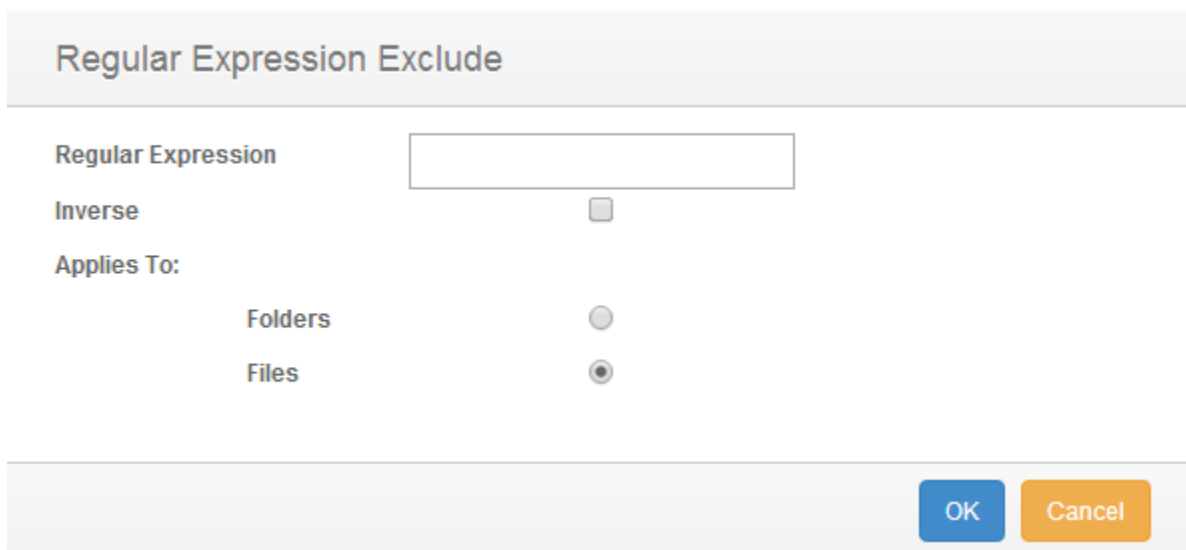
Each column of information can be sorted by column criteria by clicking once on the column title.

Right clicking on any item showing in the Watch Properties section results in a context menu to display showing additional configuration and navigation options. Context menu options include:

- **Edit Watch Properties:** *Modify the watch properties associated with the selected Watch data. Opens the Watch Properties dialog.*
- **Remove Watch:** *Disable the selected Watch data by unselecting it in the Object Group Properties dialog File System Tree.*
- **Add Regular Expression Exclude:** *Create customized excludes to prevent or enable of specific folder, file, or configuration criteria.*

#### 5.1.1.5.2.10. EXCLUDING AND INCLUDING USING REGULAR EXPRESSIONS

Occasionally a CimTrak™ Object Group Policy may need to exclude monitor or only monitor data based on file extensions, file names, folder names, configuration names, or various other types of information. Setting these custom watch rules is performed by creating Regular Express Excludes. The process of creating a Regular Expression Exclude is performed through the Add Regular Expression Exclude dialog accessed by right-clicking Watch data and then selecting Add Regular Expression Exclude from the context menu. Accessing the Object Group Properties is accomplished during the creation or editing of an Object Group's Watch Policy. See section 0 for more information on creating Watch Policies.



The image shows a screenshot of the 'Regular Expression Exclude' dialog box. The dialog has a title bar with the text 'Regular Expression Exclude'. Below the title bar, there is a text input field labeled 'Regular Expression'. To the right of this field is a checkbox labeled 'Inverse'. Below these, there is a section labeled 'Applies To:' with two radio buttons: 'Folders' and 'Files'. The 'Files' radio button is selected. At the bottom right of the dialog are two buttons: 'OK' and 'Cancel'.

Figure 65: Add Regular Expression Exclude dialog

The Add Regular Expression Exclude dialog has the capability to exclude files and folders. Additionally, the Add Regular Expression Exclude dialog can create inverse regular expressions excludes to only monitor certain files or folders based on the criteria entered.

**5.1.1.5.2.10.1. EXCLUDING FOLDERS USING REGULAR EXPRESSIONS**

The process of creating a Regular Expression Exclude is performed through the Add Regular Expression Exclude dialog accessed by right-clicking Watch data and then selecting Add Regular Expression Exclude from the context menu. Accessing the Object Group Properties is accomplished during the creation or editing of an Object Group’s Watch Policy. See section 0 for more information on creating Watch Policies.

To create a Regular Expression folder exclude, enter the folder information to exclude (i.e. \temp). Ensure that the Folders radio button is selected and then click OK. Click Cancel to abort the changes and return to the Object Group Properties dialog. Clicking OK will automatically return to the Object Group Properties dialog. Note that the regular expression exclude is displayed in the Watch Properties data section.

Regular Expression Folder Excludes can become very complex. It is possible to create custom exclusions using regular expressions. For instance, a regular expression exclude can be created to ignore case:

**C:\WINDOWS\system32\**

*can be entered as...*

**[a-zA-Z]:\\.+\\[sS][yY][sS][tT][eE][mM]32\\**

C:\testabc	Directory	Watch	No	Log	Real-time
[a-zA-Z]:\\.+\\[sS][yY][sS][tT][eE][m...	Regular Expr...	Exclude			

**Figure 66: Regular Expression Folder Exclude**

To add additional Regular Express folder excludes, repeat the same steps. To remove Regular Expression Excludes, right-click on the Exclude information in the Watch Properties data section and then select Remove Exclude(s). When completed, click the OK button to save the changes. Click the Cancel button to abort the configuration and discard any changes.

**5.1.1.5.2.10.2. EXCLUDING FILES USING REGULAR EXPRESSIONS**

The process of creating a Regular Expression Exclude is performed through the Add Regular Expression Exclude dialog accessed by right-clicking Watch data and then selecting Add Regular Expression Exclude from the context menu. Accessing the Object Group Properties is accomplished during the creation or

editing of an Object Group’s Watch Policy. See section 0 for more information on creating Watch Policies.

To create a Regular Expression file exclude, enter the file type information to exclude (i.e. .log). Ensure that the Files radio button is selected and then click OK. Click Cancel to abort the changes and return to the Object Group Properties dialog. Clicking OK will automatically return to the Object Group Properties dialog. Note that the regular expression exclude is displayed in the Watch Properties data section.

Regular Expression Folder Excludes can become very complex. It is possible to create custom exclusions using regular expressions. For instance, a regular expression exclude can be created to ignore case:

**.log**

*can be entered as...*

**.[lL][oO][gG]\$**

C:\testabc	Directory	Watch	No	Log	Real-time
[a-zA-Z]:\+\\[sS][yY][sS][tT][eE][m...	Regular Expr...	Exclude			

**Figure 67: Regular Expression File Exclude**

To add additional Regular Express file excludes, repeat the same steps. To remove Regular Expression Excludes, right-click on the Exclude information in the Watch Properties data section and then select Remove Exclude(s). When completed, click the OK button to save the changes. Click the Cancel button to abort the configuration and discard any changes.

**5.1.1.5.2.10.3. INVERSE EXCLUDING OF FOLDERS USING REGULAR EXPRESSIONS**

The process of creating an Inverse Regular Expression Exclude is performed through the Add Regular Expression Exclude dialog accessed by right-clicking Watch data and then selecting Add Regular Expression Exclude from the context menu. Accessing the Object Group Properties is accomplished during the creation or editing of an Object Group’s Watch Policy. See section 0 for more information on creating Watch Policies.

Inverse regular expressions can be used to “include” information to monitor. To create an Inverse Regular Expression folder exclude, enter the folder information to watch (i.e. \temp). Ensure that the Folders radio button and the Inverse checkbox are selected and then click OK. Click Cancel to abort the changes and



return to the Object Group Properties dialog. Clicking OK will automatically return to the Object Group Properties dialog. Note that the Inverse regular expression exclude is displayed in the Watch Properties data section.

Inverse Regular Expression Folder Excludes can become very complex. It is possible to create custom inverse exclusions using inverse regular expressions. For instance, an inverse regular expression exclude can be created to ignore case:

**C:\WINDOWS\system32\**

*can be entered as...*

**[a-zA-Z]:\.\+\\[sS][yY][sS][tT][eE][mM]32\**

C:\testabc	Directory	Watch	No	Log	Real-time
[a-zA-Z]:\.\+\\[sS][yY][sS][tT][eE][mM]32\	Inverse Regul...	Exclude			

**Figure 68: Regular Expression Folder Exclude (blue text)**

To add additional Inverse Regular Express folder excludes, repeat the same steps. To remove Inverse Regular Expression Excludes, right-click on the Exclude information in the Watch Properties data section and then select Remove Exclude(s). When completed, click the OK button to save the changes. Click the Cancel button to abort the configuration and discard any changes.

**5.1.1.5.2.10.4. INVERSE EXCLUDING OF FILES USING REGULAR EXPRESSIONS**  
The process of creating an Inverse Regular Expression to include specified files or extensions is performed through the Add Regular Expression Exclude dialog accessed by right-clicking Watch data and then selecting Add Regular Expression Exclude from the context menu. Accessing the Object Group Properties is accomplished during the creation or editing of an Object Group's Watch Policy. See section 0 for more information on creating Watch Policies.

To create an Inverse Regular Expression file exclude, enter the file type information to exclude (i.e. .log). Ensure that the Files radio button and Inverse checkbox are selected and then click OK. Click Cancel to abort the changes and return to the Object Group Properties dialog. Clicking OK will automatically return to the Object Group Properties dialog. Note that the inverse regular expression exclude is displayed in the Watch Properties data section.

Inverse Regular Expression Folder Excludes can become very complex. It is possible to create custom exclusions using regular expressions. For instance, an inverse regular expression exclude can be created to ignore case:

**.log**

*can be entered as...*

**.[!L][oO][gG]\$**

C:\testabc	Directory	Watch	No	Log	Real-time
[a-zA-Z]:\.\+\[sS][yY][sS][tT][eE][m...	Inverse Regul...	Exclude			

**Figure 69: Regular Expression File Exclude**

To add additional Inverse Regular Express file excludes, repeat the same steps. To remove Inverse Regular Expression Excludes, right-click on the Exclude information in the Watch Properties data section and then select Remove Exclude(s). When completed, click the OK button to save the changes. Click the Cancel button to abort the configuration and discard any changes.

#### **5.1.1.6. SAVING OBJECT GROUP WATCH POLICIES TO TEMPLATES**

Once an Object Group Watch Policy has been created it is possible to save the policy configurations to a template. Using a template can assist in creating identical watch data for other CimTrak™ File System Agents. See section 4.7 for more information on CimTrak™ Templates.

To create a template, right-click on the Object Group name in the CimTrak™ Web Management Console's Object Group Tree and then select Save to Template. The Save to Template dialog will display. Enter a unique name for the template. If you would like this template to be private to your CimTrak™ account be sure to select the Private option by selecting the Private checkbox. When completed entering the required information click the OK button. Click the cancel button to abort the template creation. A template name can be between 1 and 512 characters.

Save Policy Settings To A Template

Template Name:

Name of Template

Private:

☐

OK

Cancel

**Figure 70: Save to Template dialog**

In addition to being able to create Templates for single Object Groups CimTrak™ has the capability to create Templates for multiple Object Groups at the File System Agent level. To create a File System Agent template, right-click on the File System Agent name in the CimTrak™ Web Management Console's Object Group Tree and then select Save to Template. The Save to Template dialog will display. Enter a unique name for the template. If you would like this template to be private to your CimTrak™ account be sure to select the Private option by selecting the Private checkbox. When completed entering the required information click the OK button. Click the cancel button to abort the template creation. A template name can be between 1 and 512 characters.

#### **5.1.1.7. CREATING OBJECT GROUP WATCH POLICIES USING TEMPLATES**

Once an Object Group Watch Policy has been created it is possible to save the policy configurations to a template. Using a template can assist in creating identical watch data for other CimTrak™ File System Agents. See section 4.7 for more information on CimTrak™ Templates.

To create an Object Group from template (or multiple Object Groups from a single template) right-click on the File System Agent name in the CimTrak™ Web Management Console's Object Group Tree and then select New Object Group(s) from Template. The Select Template dialog will display.

Select Template

Search

Template Name

109

AD+SQL+FSA

jovotest-progfiles

Linux Operating System

linux with etc store

new policy

program files

services

services v2

test1-oktodelete

test112

test171-template

Close

**Figure 71: Select Template dialog**

Select the template the Object Group will be based off of and then click OK. Click Cancel to abort the Object Group creation. If OK is selected the Select Template dialog will close and the newly created Object Group(s) will display in the CimTrak™ Web Management Consoles Object Group Tree.

**5.1.1.8. DELETING OBJECT GROUP WATCH POLICIES**

Once an Object Group Watch Policy has been created it is possible to delete the Object Group. Once an Object Group is deleted it cannot be undone.

To delete an Object Group Watch Policy right-click on its name in the CimTrak™ Web Management Console's Object Group Tree and then select Delete. The Confirm Delete dialog will display.

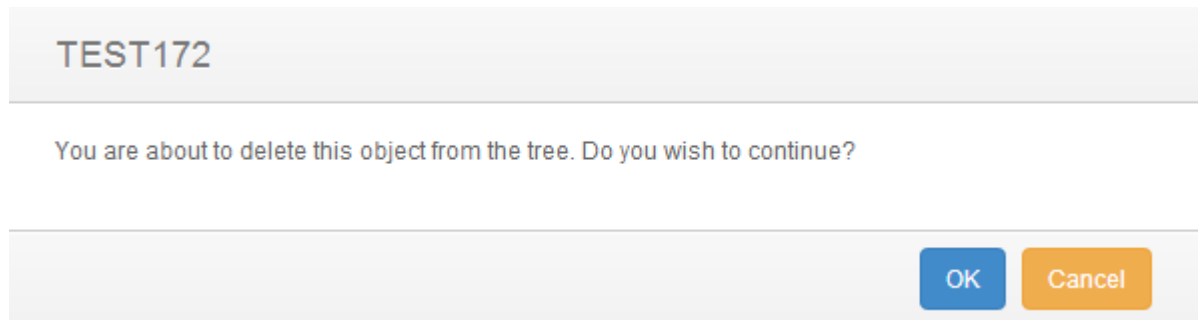


Figure 72: Confirm Delete dialog

Select “Yes” to delete the Object Group, select No to abort the deletion. Select the Do not show this again checkbox to suppress this message from future deletions. Clicking Yes results in the Object Group being deleted.



***The Object Group must be unlocked (monitoring disabled) before the Object Group can be deleted. Unlocking an Object Group is explained in a subsequent section.***

#### 5.1.1.9. ENABLING AND DISABLING OBJECT GROUP MONITORING

Before a CimTrak™ File System Agent can monitor an Object Group Watch Policy the Object Group must be “Locked”. To disable monitoring the Object Group Watch Policy must be “Unlocked”. The monitoring status of an Object Group can be determined by the associated icon in the CimTrak™ Web Management Console's Object Group Tree. See section 0 for more information on creating Object Group Watch Policies. Possible associated statuses are as follows:



**Unlocked:** *The Object Group Watch Policy is not currently being enforced.*



**Locked:** *The Object Group Watch Policy is currently enforcing the configured Corrective Action.*

Locking an Object Group is accomplished by selecting the Object Group to lock in the CimTrak™ Web Management Console's Object Group Tree, right-clicking and then selecting Lock and Digitally Sign.

When an Object Group is locked (or locking) it will show the locking and synchronization process in the Master Repository, Area, Agent, and Object

Group Event Logs. The process of locking and synchronization creates Information level events.

Severity	Event Date/Time	Event	Correction	CimTrak ID	Event Log	Created By	Process	Absolute path
Info	6/10/2014 15:37:35	Sync Complete		TEST172(T...				C:\testabc
Info	6/10/2014 15:37:32	Lock Completed		admin				
Info	6/10/2014 15:37:32	Sync Started		TEST172(T...				C:\testabc
Info	6/10/2014 15:37:22	Lock Started		admin				
Error	6/10/2014 15:37:17	Unlocked Object		admin				

**Figure 73: Object Group Lock Process (Event Log)**



***Multiple Object Groups can be locked simultaneously by selecting the File System Agent in the Web Management Console's Object Group Tree and then either right-clicking and selecting Lock and Digitally Sign in the context menu.***

Locking the Object Group will instruct the File System Agent to create digital signatures for each file included in the watch policy. If a Restore from Repository or Update Baseline Corrective Action is assigned, the File System Agent will create Authoritative Copies of the monitored files. All digital signatures and Authoritative Copy data is compressed, encrypted, and then transmitted to the CimTrak™ Master Repository.

While an Object Group is in the process of locking the lock process can be aborted by right-clicking on the Object Group in the CimTrak™ Web Management Console's Object Group Tree and selecting Cancel Lock in the context menu.

When the locking of an Object Group is "Stopped" it will show the stop locking process in the Master Repository, Area, Agent, and Object Group Event Logs. The process of Stopping creates error level events.



***The Locking of Multiple Object Groups can be stopped simultaneously by selecting the File System Agent in the Web Management Console's Object Group Tree and then right-clicking and selecting Cancel Lock in the context menu.***

Before configuration settings associated with an Object Group Watch Policy can be modified, an Object Group is deleted, or simply to temporarily disable Object Group monitoring the Object Group must be "Unlocked". Unlocking an Object Group is accomplished by selecting the Object Group to unlock in the CimTrak™ Web Management Console's Object Group Tree, right-clicking and then selecting Unlock and Allow Changes.

When an Object Group is Unlocked it will show the unlock process in the Master Repository, Area, Agent, and Object Group Event Logs. The process of unlocking creates error level events.

Severity	Event Date/Time	Event	Correction	CimTrak ID	Event Log	Created By	Process	Absolute path
Info	6/10/2014 15:37:35	Sync Complete		TEST172(T...				C:\testabc
Info	6/10/2014 15:37:32	Lock Completed		admin				
Info	6/10/2014 15:37:32	Sync Started		TEST172(T...				C:\testabc
Info	6/10/2014 15:37:22	Lock Started		admin				
Error	6/10/2014 15:37:17	Unlocked Object		admin				

**Figure 74: Object Group Unlock Process (Event Log)**



**Multiple Object Groups can be unlocked simultaneously by selecting the File System Agent in the Web Management Console's Object Group Tree and then right-clicking and selecting Unlock and Allow Changes in the context menu.**

#### 5.1.1.10. SYNCHRONIZING OBJECT GROUP DATA

Data being monitored by a CimTrak™ File System Agent is monitored either in real-time or at a polling interval. To force the polling interval to expire immediately, CimTrak™ has the capability to synchronize monitored data on demand by means of Force Sync.

Synchronizing an Object Group Watch Policy is performed by right-clicking on the Object Group in the CimTrak™ Web Management Console's Object Group Tree and selecting Force Sync in the context menu.



**Multiple Object Groups can be synchronized simultaneously by selecting the File System Agent in the Web Management Console's Object Group Tree and then right-clicking and selecting Force Sync in the context menu.**

When an Object Group is synchronized it will show the synchronization process in the Master Repository, Area, Agent, and Object Group Event Logs. The process of synchronizing creates information level events.

Severity	Event Date/Time	Event	Correction	CimTrak ID	Event Log	Created By	Process	Absolute path
Info	6/10/2014 15:37:35	Sync Complete		TEST172(T...				C:\testabc
Info	6/10/2014 15:37:32	Lock Completed		admin				
Info	6/10/2014 15:37:32	Sync Started		TEST172(T...				C:\testabc
Info	6/10/2014 15:37:22	Lock Started		admin				
Error	6/10/2014 15:37:17	Unlocked Object		admin				

**Figure 75: Object Group Synchronization Process (Event Log)**

#### 5.1.2. FILE SYSTEM AGENT INFORMATION DISPLAY

The CimTrak™ Web Management Console's Information Display Area displays information for the selected CimTrak™ File System Agent. The information displayed provides Event Log data.

- **Agent Settings:** *Settings and system information associated with the selected File System Agent.*

- **Event Log:** Event audit log associated with the File System Agent and children Object Groups of the selected File System Agent.
- **Stats:** System statistics associated with the system hosting the File System Agent.
- **Notes:** Administrative notes associated with the File System Agent.
- **Overview:** Object Group status information for all Object Groups associated with the File System Agent.

Event Log

Drag a column header here and drop it to group by that column.

Severity	Event Date/Time	Event	Correction	CimTrak ID	Modified By	Process	Absolute path
Info	7/11/2014 10:51:54	Sync Complete		TEST172(T...			C:\testabc
Info	7/11/2014 10:51:51	Lock Completed		admin			
Info	7/11/2014 10:51:51	Sync Started		TEST172(T...			C:\testabc
Info	7/11/2014 10:51:47	Lock Started		admin			
Error	7/11/2014 10:51:41	Unlocked Object		admin			
Info	7/11/2014 10:50:09	Sync Complete		TEST172(T...			C:\testabc
Info	7/11/2014 10:50:07	Sync Started		TEST172(T...			C:\testabc
Info	7/11/2014 10:50:06	Lock Completed		admin			
Info	7/11/2014 10:50:02	Lock Started		admin			
Error	7/11/2014 10:49:48	Unlocked Object		admin			
Info	7/11/2014 10:48:59	Sync Complete		TEST172(T...			C:\testabc
Info	7/11/2014 10:48:56	Lock Completed		admin			

Total Items: 5701

CSV Export

Page Size: 100

1 / 58

**Figure 76: File System Agent Information Display Area (Agent Settings Tab Selected)**

The information associated with the File System Agent Information Display Area tabs is explained in subsequent sections.

#### 5.1.2.1. AUDITING FILE SYSTEM AGENT EVENTS

The File System Agent Event Log provides audit information relating to events occurring in the File System Agent and Object Groups connected to the File System Agent. Accessing the File System Agent Event Log is accomplished by first clicking once on the File System Agent name in the Object Group Tree to select it followed by clicking the Event Log tab in the Web Management Console Information Display Area.

The File System Agent Event Log displays details of all events that have occurred on the File System Agent and Object Groups connected to the File System Agent. The level of detail displayed is dependent on the auditing level configured in the Master Repository Properties Log Administrative DB Changes. See section 0 for additional information.



For each recorded event, the File System Agent Event Log will display information corresponding to the following:

**Event Date/Time:** *The exact date and time of the detected event.*

**Event:** *Brief description of the detected event.*

**Absolute Path:** *File path affected by the detected event.*

**Completion Date/Time:** *Date and time the correction response completed.*

**Event Code:** *Internal CimTrak™ Event Code corresponding to the detected event.*

**Path:** *Object Tree Path to the affected CimTrak™ object.*

Event Log							
Drag a column header here and drop it to group by that column.							
Severity	Event Date/Time	Event	Correction	CimTrak ID	Modified By	Process	Absolute path
Info	7/11/2014 10:51:54	Sync Complete		TEST172(T...			C:\testabc
Info	7/11/2014 10:51:51	Lock Completed		admin			
Info	7/11/2014 10:51:51	Sync Started		TEST172(T...			C:\testabc
Info	7/11/2014 10:51:47	Lock Started		admin			
Error	7/11/2014 10:51:41	Unlocked Object		admin			
Info	7/11/2014 10:50:09	Sync Complete		TEST172(T...			C:\testabc
Info	7/11/2014 10:50:07	Sync Started		TEST172(T...			C:\testabc
Info	7/11/2014 10:50:06	Lock Completed		admin			
Info	7/11/2014 10:50:02	Lock Started		admin			
Error	7/11/2014 10:49:48	Unlocked Object		admin			
Info	7/11/2014 10:48:59	Sync Complete		TEST172(T...			C:\testabc
Info	7/11/2014 10:48:56	Lock Completed		admin			
Total Items: 5701 CSV Export Page Size: 100 1 / 58							

**Figure 77: File System Agent Event Log**

Each Event Log message type has a corresponding icon that allows for quick visual reference to the urgency level of the event. These urgency levels are important to note when configuring E-Mail alert permissions. E-Mail alert permissions are explained in a subsequent section.

**Emergency:** *System is unusable. Highest level of event.*

**Alert:** *Take action immediately.*

**Critical:** *Critical conditions have occurred.*

**Error:** *Error conditions.*

**Warning:** *Warning conditions.*

**Notice:** *Normal condition that requires attention.*

**Information:** *Informational message.*

**Debug:** *Debug-level message. Lowest level of event.*

Specifics relating to message types are discussed in a subsequent sections.

#### **5.1.2.1.1. FILTERING AND SORTING THE FILE SYSTEM AGENT EVENT LOG**

The File System Agent Event Log can be filtered to only show events matching the specified criteria. Accessing the File System Agent Event Log is accomplished by first clicking once on the File System Agent in the Object Group Tree to select it followed by clicking the Event Log tab in the Web Management Console Information Display Area.

To filter the information displayed in the File System Agent Event Log, drag and drop one of the column headers into the section labelled “Drag a column header here and drop it to group by that column.”

#### **5.1.2.2. FILE SYSTEM AGENT PERMISSIONS**

File System Agents can be configured restrict access based on permission settings. Additionally, event notifications can be configured to notify CimTrak™ Users about events relating to the File System Agent. Accessing File System Agent permissions is accomplished by first clicking once on the File System Agent in the Object Group Tree to select it and then right-clicking and selecting “Permissions”. The Security Permissions dialog will display.

By default each File System Agent will have the following permissions:

##### **Administrators**

**Create Objects:** *Create File System Agent Object Groups.*

**Edit:** *Edit File System Agent settings.*

**Lock:** *Enable active monitoring of Object Group Data.*

**Reports:** *View reports relating to the File System Agent contents.*

**Unlock:** *Disable active monitoring of Object Group Data.*

**View:** *View contents and configurations relating to the File System Agent.*

##### **Auditors**

**Reports:** *View reports relating to File System Agent contents.*

**View:** *View contents and configurations relating to the File System Agent.*

##### **Installers**

*Attach CimTrak™ Agents to a Master Repository.*

Permissions for Object

Add

Group or User Names

Group	Administrators	
Group	Auditors	
Group	Email_Testing	Remove
Group	Installers	

Permissions	Allow	Deny
Create Objects	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Edit	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lock	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Reports	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Unlock	<input checked="" type="checkbox"/>	<input type="checkbox"/>
View	<input checked="" type="checkbox"/>	<input type="checkbox"/>

☒ Apply permissions to children recursively

OKCancel

**Figure 78: File System Agent Security Permissions dialog**

Default access permissions associated with the Administrators, Auditors, and Installers User Groups cannot be changed. It is possible to modify E-mail alert notices for Administrator and Auditor user groups.

#### 5.1.2.3. MODIFYING AN EXISTING USER/GROUP FILE SYSTEM AGENT PERMISSIONS

It is possible to modify existing user and group File System Agent Permissions and E-mail notification settings. Accessing File System Agent permissions is accomplished by first clicking once on the File System Agent in the Object Group Tree to select it and then right-clicking and selecting “Permissions”. The Security Permissions dialog will display.

Select the existing user or group by clicking once on the CimTrak™ User or Group name in the Group or User Names section of the Security Permissions dialog. The Permissions section of the Security Permissions dialog will update to show the permissions currently assigned to the selected user or group.



***Selecting a group will apply the selected permissions and E-mail notification settings to all members of the group. Selecting a single user will apply the selected permissions and E-mail notification settings to only that single user account.***

To add or remove permissions click the “Allow” or “Deny” checkbox corresponding to the permission being configured. Available permissions include:

**Create Objects:** Create File System Agent Object Groups.

**Edit:** Edit File System Agent/Object Group control contents.

**Lock:** Enable active monitoring of Object Group Data

**Reports:** View reports relating to File System Agent contents.

**Unlock:** Disable active monitoring of Object Group Data

**View:** View contents and configurations relating to the File System Agent.

To apply the permission settings to all children objects, ensure that the Apply permissions to children recursively checkbox is selected.

When completed, click “OK” to apply the permission and alert settings. Click “Cancel” to abort the security permission configuration.



***Permissions and notification settings can be inherited from parent objects (such as the Master Repository) if the permissions are created at a parent level.***

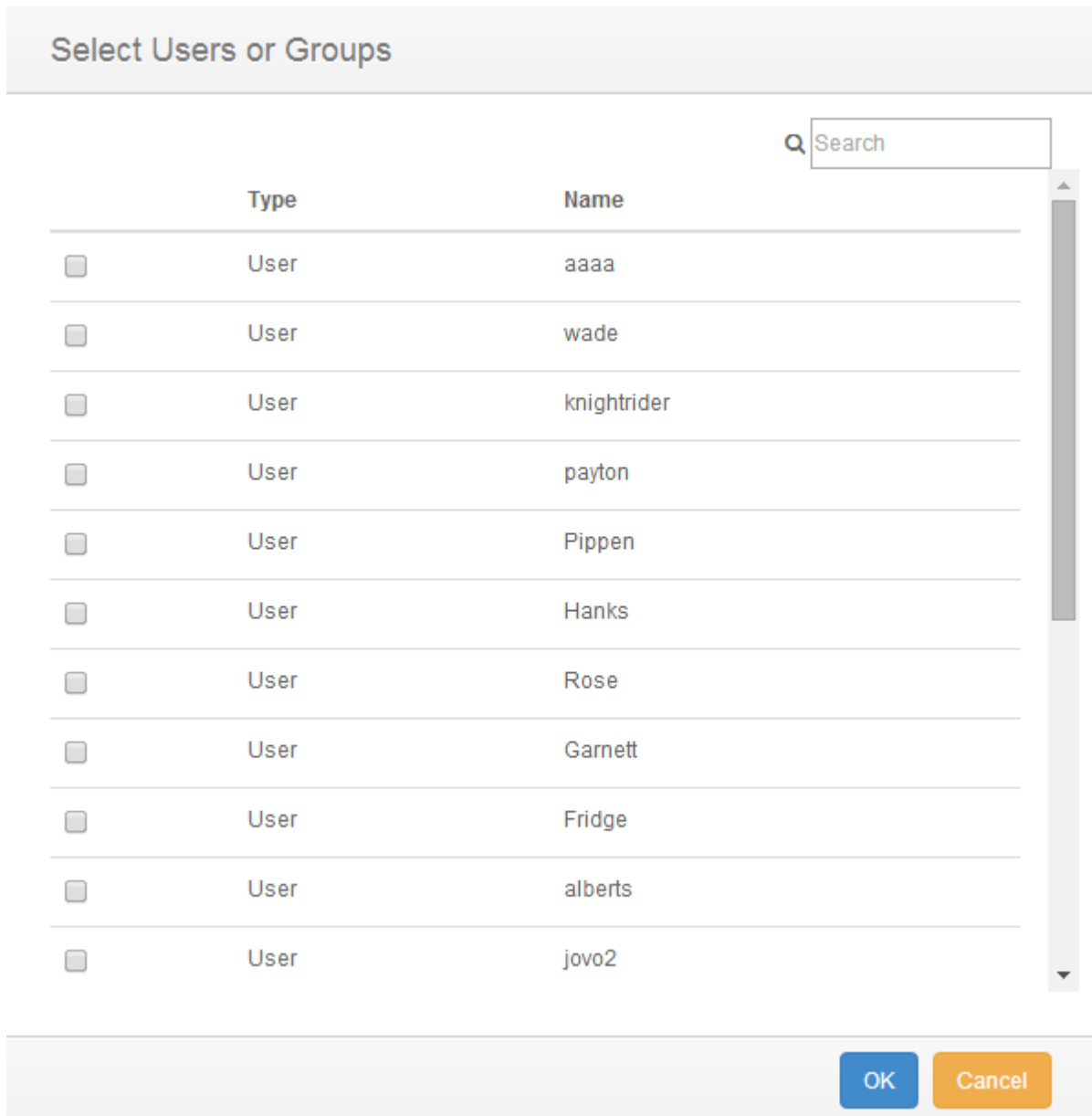


***Permissions and notification settings are not automatically inherited for new objects. It will be necessary to manually assign the permissions and notification settings to the object.***

#### 5.1.2.4. ADDING AND REMOVING USERS AND GROUPS TO FILE SYSTEM AGENT PERMISSIONS

It is possible to add additional users and groups to the Security Permissions dialog so that File System Agent Permissions and E-mail notification settings can be assigned or changed. Accessing File System Agent permissions is accomplished by first clicking once on the File System Agent in the Object Group Tree to select it and then right-clicking and selecting “Permissions.” The Security Permissions dialog will display.

To add a new local CimTrak™ User or Group, click the Add button. The Add Users dialog will display listing all available local users and groups.



	Type	Name
<input type="checkbox"/>	User	aaaa
<input type="checkbox"/>	User	wade
<input type="checkbox"/>	User	knightrider
<input type="checkbox"/>	User	payton
<input type="checkbox"/>	User	Pippen
<input type="checkbox"/>	User	Hanks
<input type="checkbox"/>	User	Rose
<input type="checkbox"/>	User	Garnett
<input type="checkbox"/>	User	Fridge
<input type="checkbox"/>	User	alberts
<input type="checkbox"/>	User	jovo2

Figure 79: Add Users dialog

Select the local CimTrak™ User or Group to add by selecting the checkbox to the left of the name. Click “OK” to add the User or Group. Click “Cancel” to abort the addition process. The selected user or group will now display in the Group or User Names section of the Security Permissions dialog.

The User or Group is now available to have permissions and notification settings assigned.

### 5.1.3. OBJECT GROUP INFORMATION DISPLAY

The CimTrak™ Web Management Console’s Information Display Area displays information for the selected CimTrak™ File System Agent Object Groups. The information displayed is often broken up into several tabbed viewing areas.

- **Event Log:** *Event audit log associated with the File System Agent and children Object Groups of the selected File System Agent.*
- **Change Log:** *Detected changes of watched directories.*
- **Monitor Info:** *Description and statistical standing of Watch Parameters within the Object Group.*
- **Pending Repair:** *Displays queue information associated with the remediation of folder, file and configuration data.*
- **Generation:** *Displays revision information for changes occurring to files, folders, operating system configurations contained in a File System Agent Object Group.*

Severity	Event Date/Time	Event	Correction	CimTrak ID	Event Log	Created By	Process	Absolute path
Info	6/10/2014 15:37:35	Sync Complete		TEST172(T...				C:\testabc
Info	6/10/2014 15:37:32	Lock Completed		admin				
Info	6/10/2014 15:37:32	Sync Started		TEST172(T...				C:\testabc
Info	6/10/2014 15:37:22	Lock Started		admin				
Error	6/10/2014 15:37:17	Unlocked Object		admin				
Info	3/24/2014 23:04:52	Sync Complete		TEST172(T...				C:\testabc
Info	3/24/2014 23:04:38	Sync Started		TEST172(T...				C:\testabc
Info	3/24/2014 10:47:09	Sync Complete		TEST172(T...				C:\testabc
Info	3/24/2014 10:46:53	Sync Started		TEST172(T...				C:\testabc
Info	3/19/2014 11:17:53	Sync Complete		TEST172(T...				C:\testabc
Info	3/19/2014 11:17:38	Sync Started		TEST172(T...				C:\testabc
Info	3/19/2014 10:18:17	Sync Complete		TEST172(T...				C:\testabc

Figure 80: Object Group Information Display Area

The information associated with the Object Group Information Display Area tabs is explained in subsequent sections.

#### 5.1.3.1. AUDITING OBJECT GROUP EVENTS

The Object Group Event Log provides audit information relating to events occurring in the Object Groups connected to the File System Agent. Accessing the Object Group Event Log is accomplished by first clicking once on the Object Group name in the Object Group Tree to select it followed by clicking the Event Log tab in the Web Management Console Information Display Area.

The Object Group Event Log displays details of all events that have occurred on the Object Groups connected to the File System Agent. The level of detail displayed is dependent on the auditing level configured in the Master Repository Properties Log Administrative DB Changes. See section 0 for additional information.

For each recorded event, the Object Group Event Log will display information corresponding to the following:

**Event Date/Time:** *The exact date and time of the detected event.*

**Event:** *Brief description of the detected event.*

**Correction:** *The Corrective Action performed on the detected event.*

**Performed By (Cimtrak™ ID):** *The File System Agent detecting the event and performing the remediation.*

**Modified By:** *The File System User responsible for the detected event.*

**Absolute Path:** *File path affected by the detected event.*

**Completion Date/Time:** *Date and time the correction response completed.*

**Event Code:** *Internal CimTrak™ Event Code corresponding to the detected event.*

Each Event Log message type has a corresponding icon that allows for quick visual reference to the urgency level of the event. These urgency levels are important to note when configuring E-Mail alert permissions. E-Mail alert permissions are explained in a subsequent section.

**Emergency:** *System is unusable. Highest level of event.*

**Alert:** *Take action immediately.*

**Critical:** *Critical conditions have occurred.*

**Error:** *Error conditions.*

**Warning:** *Warning conditions.*

**Notice:** *Normal condition that requires attention.*

**Information:** *Informational message.*

**Debug:** *Debug-level message. Lowest level of event.*

Specifics relating to message types are discussed in a subsequent section.

#### **5.1.3.1.1. FILTERING AND SORTING THE OBJECT GROUP EVENT LOG**

The Object Group Event Log can be filtered to only show events matching the specified criteria. Accessing the Object Group Event Log is accomplished by first clicking once on the Object Group in the Object Group Tree to select it followed by clicking the Event Log tab in the Web Management Console Information Display Area.

To filter the information displayed in the File System Agent Event Log, drag and drop one of the column headers into the section labelled “Drag a column header here and drop it to group by that column.”

#### **5.1.3.2. REVIEWING OBJECT GROUP MONITORED CHANGES**

The Object Group Change Log provides detailed change event audit information relating to change events occurring in the Object Groups connected to the File System Agent. Accessing the Object Group Change Log is accomplished by first clicking once on the Object Group name in the Object Group Tree to select it followed by clicking the Change Log tab in the Web Management Console Information Display Area.

The Object Group Change Log displays details of all addition, deletion, and change events that have occurred on the Object Groups connected to the File System Agent.

For each recorded event, the Object Group Change Log will display information corresponding to the following:

**Event Date/Time:** *The exact date and time of the detected event.*

**Storage Status:** *Information indicating if the change is stored in the Master Repository.*

**Absolute Path:** *File path affected by the detected event.*

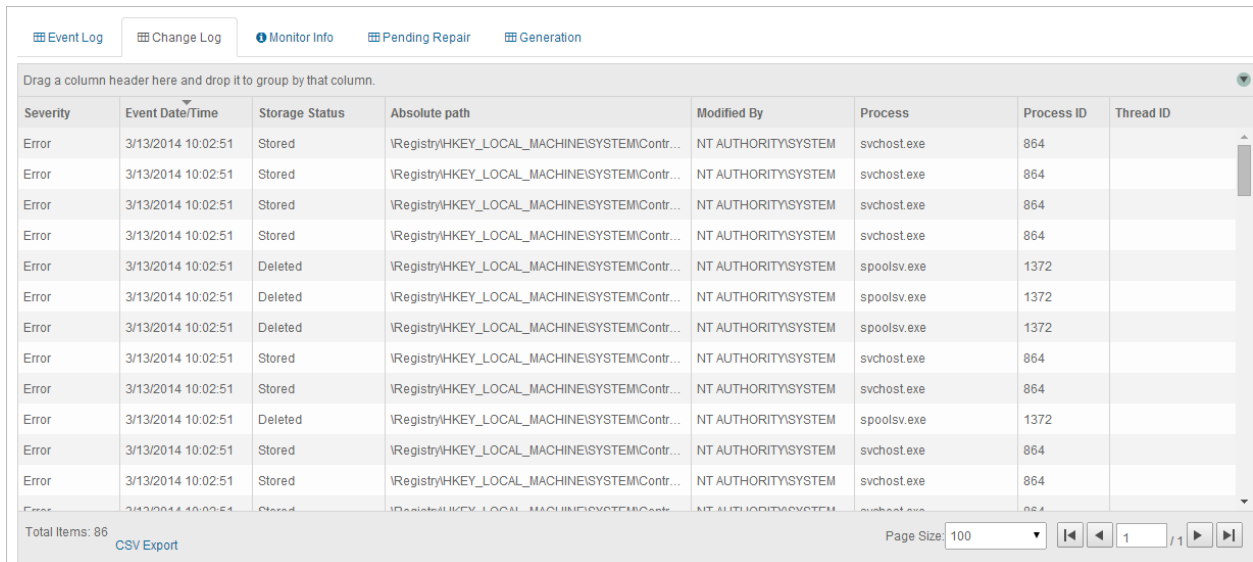
**Modified By:** *The File System User responsible for the detected event (Windows File System Agent with Driver only).*



**Process:** The process used to initiate the detected event (Windows File System Agent with Driver only).

**Process ID:** Windows Process ID associated with the initiating process (Windows File System Agent with Driver only).

**Thread ID:** Process Thread ID associated with the initiating process (Windows File System Agent with Driver only).



Severity	Event Date/Time	Storage Status	Absolute path	Modified By	Process	Process ID	Thread ID
Error	3/13/2014 10:02:51	Stored	\Registry\HKEY_LOCAL_MACHINE\SYSTEM\Contr...	NT AUTHORITY\SYSTEM	svchost.exe	864	
Error	3/13/2014 10:02:51	Stored	\Registry\HKEY_LOCAL_MACHINE\SYSTEM\Contr...	NT AUTHORITY\SYSTEM	svchost.exe	864	
Error	3/13/2014 10:02:51	Stored	\Registry\HKEY_LOCAL_MACHINE\SYSTEM\Contr...	NT AUTHORITY\SYSTEM	svchost.exe	864	
Error	3/13/2014 10:02:51	Stored	\Registry\HKEY_LOCAL_MACHINE\SYSTEM\Contr...	NT AUTHORITY\SYSTEM	svchost.exe	864	
Error	3/13/2014 10:02:51	Deleted	\Registry\HKEY_LOCAL_MACHINE\SYSTEM\Contr...	NT AUTHORITY\SYSTEM	spoolsv.exe	1372	
Error	3/13/2014 10:02:51	Deleted	\Registry\HKEY_LOCAL_MACHINE\SYSTEM\Contr...	NT AUTHORITY\SYSTEM	spoolsv.exe	1372	
Error	3/13/2014 10:02:51	Deleted	\Registry\HKEY_LOCAL_MACHINE\SYSTEM\Contr...	NT AUTHORITY\SYSTEM	spoolsv.exe	1372	
Error	3/13/2014 10:02:51	Stored	\Registry\HKEY_LOCAL_MACHINE\SYSTEM\Contr...	NT AUTHORITY\SYSTEM	svchost.exe	864	
Error	3/13/2014 10:02:51	Stored	\Registry\HKEY_LOCAL_MACHINE\SYSTEM\Contr...	NT AUTHORITY\SYSTEM	svchost.exe	864	
Error	3/13/2014 10:02:51	Deleted	\Registry\HKEY_LOCAL_MACHINE\SYSTEM\Contr...	NT AUTHORITY\SYSTEM	spoolsv.exe	1372	
Error	3/13/2014 10:02:51	Stored	\Registry\HKEY_LOCAL_MACHINE\SYSTEM\Contr...	NT AUTHORITY\SYSTEM	svchost.exe	864	
Error	3/13/2014 10:02:51	Stored	\Registry\HKEY_LOCAL_MACHINE\SYSTEM\Contr...	NT AUTHORITY\SYSTEM	svchost.exe	864	

**Figure 81: Object Group Change Log**

Each Change Log message type has a corresponding icon that allows for quick visual reference to the urgency level of the event. These urgency levels are important to note when configuring E-Mail alert permissions. E-Mail alert permissions are explained in a subsequent section.

**Emergency:** System is unusable. Highest level of event.

**Alert:** Take action immediately.

**Critical:** Critical conditions have occurred.

**Error:** Error conditions.

**Warning:** Warning conditions.

**Notice:** Normal condition that requires attention.

**Information:** *Informational message.*

**Debug:** *Debug-level message. Lowest level of event.*

Generally change events are associated with the Error level. Specifics relating to message types are discussed in a subsequent section.

#### **5.1.3.2.1. FILTERING AND SORTING THE OBJECT GROUP CHANGE LOG**

The Object Group Change Log can be filtered to only show events matching the specified criteria. Accessing the Object Group Change Log is accomplished by first clicking once on the Object Group in the Object Group Tree to select it followed by clicking the Change Log tab in the Web Management Console Information Display Area.

To filter the information displayed in the Object Group Change Log, drag and drop one of the column headers into the section labelled “Drag a column header here and drop it to group by that column.”

#### **5.1.3.2.2. ACCESSING THE CHANGE LOG TAB CONTEXT MENU**

Right-clicking on any event listed in the Change Log tab provides a context menu allowing for change related actions. The Change Log tab is accessed by selecting the Object Group in the Web Management Console’s Object Group Tree and then selecting the Change Log tab in the Information Display Area.

The Change Log Context Menu allows for additional actions to be taken on stored changes including:

**View:** *View the content and attributes associated with the stored change.*

**View as Binary:** *View the content associated with the stored change in a hexadecimal format.*

**View Forensic Data:** *View the IP Address and Port number associated with the change process. (Windows File System Agent with Driver only).*

**Download:** *Download a copy of the stored intrusion.*

**Compare with Authoritative Copy (at time of change):** *Compare the content of the detected change with the known, authoritative copy stored in the Master Repository at the time of the change.*

**Compare with Authoritative Copy (current):** *Compare the content of the detected change with the current known, authoritative copy stored in the Master Repository currently.*

**Add to Excludes:** *Disable monitoring of the selected file or configuration.*

Details associated with these context menu options are discussed in subsequent sections.

##### **5.1.3.2.2.1. VIEWING CHANGE CONTENT**

Right-clicking on any event listed in the Change Log tab provides a context menu allowing for change related actions. Selecting View from the context menu allows authorized CimTrak™ administrators the capability to review content associated with a detected change. The Change Log tab is accessed by selecting the Object Group in the Web Management Console's Object Group Tree and then selecting the Change Log tab in the Information Display Area.

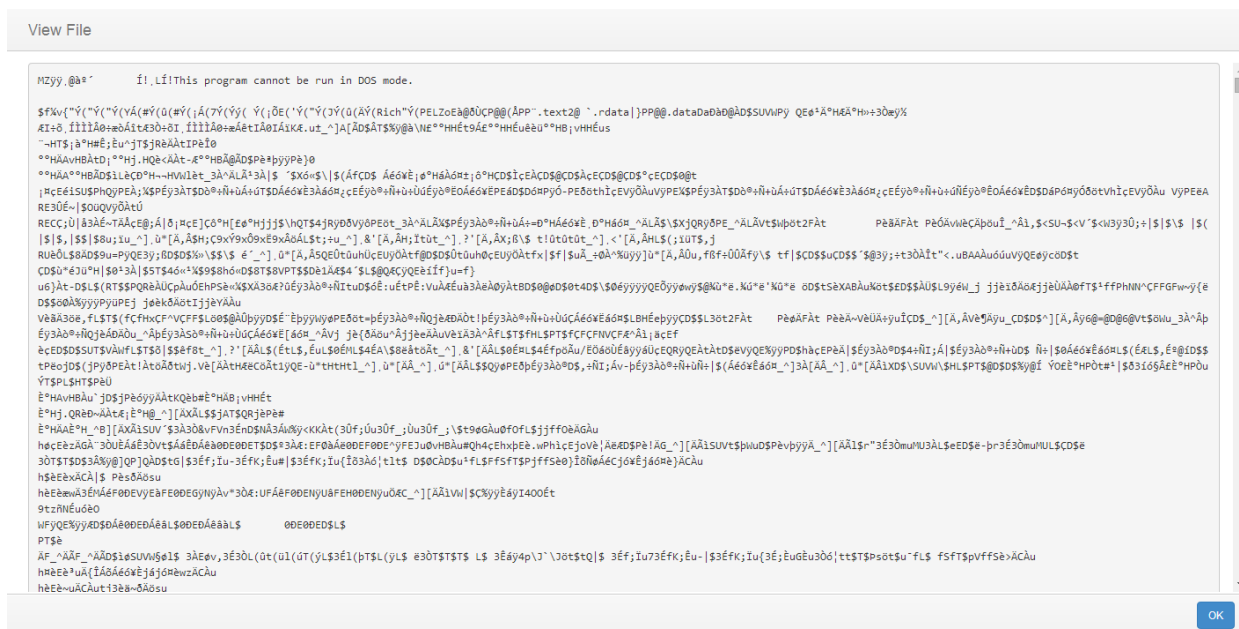


Figure 82: File View dialog



**Viewing of Change data requires the Object Group Policy is configured to store changes. Additionally, the change must not exceed the specified “Keep Change Size (in KB)” indicated in Object Group Properties Monitoring Information. See sections 0 and 5.1.1.5.2.4 for more information.**



**Viewing the content of non-binary files is supported. Binary files cannot be viewed at this time.**

Click the Close button to exit the File View dialog.

#### 5.1.3.2.2.2. VIEWING CHANGE FORENSIC DATA

Right-clicking on any event listed in the Change Log tab provides a context menu allowing for change related actions. Selecting View Forensic Data from the context menu allows authorized CimTrak™ administrators the capability to review connections associated with the offending change process at the time of the change. The Change Log tab is accessed by selecting the Object Group in the Web Management Console's Object Group Tree and then selecting the Change Log tab in the Information Display Area.

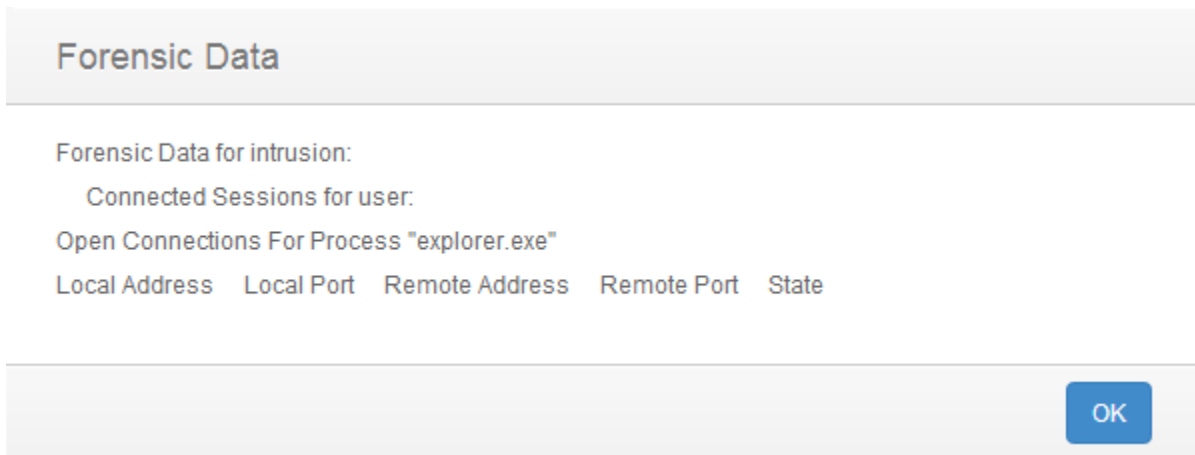


Figure 83: Forensic Data dialog



***Forensic data is only available for remote connections.***



***Viewing of forensic data is only supported on Windows File Systems with the File System Agent Driver installed.***

The Forensic Data dialog displays the following information:

Mount Points: The Windows Mount Point Name the change occurred on.\*?\*

Process: The Windows Process name responsible for initiating the detected change. Remote changes display as “System”.

Local Address: IP Address on the affected system the process utilized to make the change.

Local Port: Port number on the affected system the process utilized to make the change.

Remote Address: IP Address of the remote system that attached to the local process to make the change.

Remote Port: Port number of the remote system used to connect to the local system.

State: State of the current connection (i.e., Listen or Established).

Click the Close button to exit the Forensic Data dialog.

#### **5.1.3.2.2.3. DOWNLOADING A COPY OF CHANGE DATA**

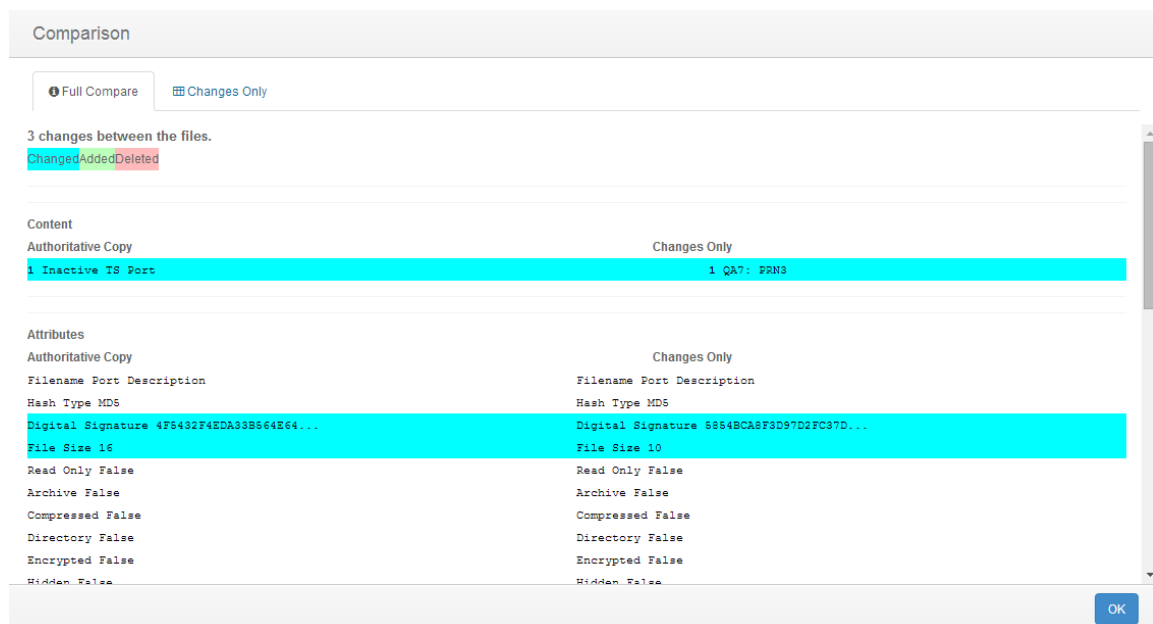
Right-clicking on any event listed in the Change Log tab provides a context menu allowing for change related actions. Selecting Download from the context menu

allows authorized CimTrak™ administrators the capability to download a copy of the actual change file. The Change Log tab is accessed by selecting the Object Group in the Web Management Console's Object Group Tree and then selecting the Change Log tab in the Information Display Area.

Clicking the Download option in the Change Log tab context menu results in the file being downloaded and saved in the Download folder, or in your default location for downloaded files.

#### 5.1.3.2.2.4. COMPARING CHANGE DATA WITH THE AUTHORITATIVE COPY AT THE TIME OF THE CHANGE

Right-clicking on any event listed in the Change Log tab provides a context menu allowing for change related actions. Selecting Compare with Authoritative Copy (at time of change) allows authorized CimTrak™ administrators the capability to perform a side-by-side comparison of the changed file with its authoritative copy stored in the Master Repository. The Change Log tab is accessed by selecting the Object Group in the Web Management Console's Object Group Tree and then selecting the Change Log tab in the Information Display Area.



**Figure 84: File Comparison Results**

Click the Close button to exit the File Comparison Results dialog.

#### 5.1.3.2.2.4.1. UNDERSTANDING THE OBJECT GROUP CHANGE TAB FILE COMPARISON RESULTS DIALOG

The File Comparison Results dialog displays anytime a comparison is performed between a detected change and the authoritative copy associated with watch properties. See section 0 for more information on performing file comparisons.

The File Comparison dialog is comprised of two tabs:

**Full Compare:** A comparison of both files are shown with all content and attributes listed.

**Changes only:** A comparison of both file are shown with only the content and attributes which the changes affected listed.

#### 5.1.3.2.2.4.1.1. UNDERSTANDING THE FILE COMPARISON RESULTS DIALOG INFORMATION DISPLAY AREA AND TAB BROWSER

The File Comparison Results dialog Tab Browser and Information Display Area allows authorized CimTrak™ users the capability visualize generation comparison data. The File Comparison Results dialog is accessible by accessing the context menu and selected Compare with Authoritative Copy (at time of Change) in the Object Group Change Tab. See section 0 for more information on performing file comparisons.

The File Comparison Results dialog Information Display Area shows a side-by-side comparison of one generation revision of a detected change to the Master Repository Authoritative Copy. Lines that have been modified are highlighted in blue, lines that have been added are highlighted in green, and lines that have been deleted are highlighted in red.

By default, the “Full Compare” tab is selected. The “Full Compare” tab shows all lines of a selected comparison. Selecting the “Changes Only” tab displays only the lines that have differences between the compared generations.

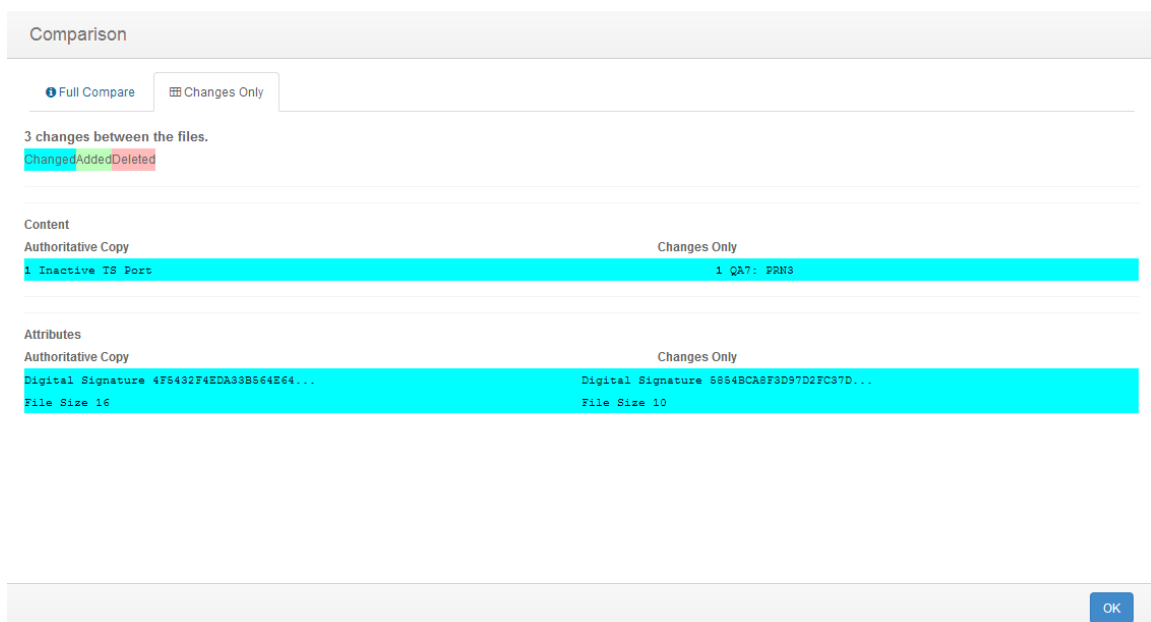


Figure 85: File Comparison Results dialog Changes tab

Click the Close button to exit the File Comparison Results dialog.

5.1.3.2.2.5. COMPARING CHANGE DATA WITH THE CURRENT AUTHORITATIVE COPY

Right-clicking on any event listed in the Change Log tab provides a context menu allowing for change related actions. Selecting Compare with Authoritative Copy (Current) allows authorized CimTrak™ administrators the capability to perform a side-by-side comparison of the changed file with an authoritative copy stored in the Master Repository. The Change Log tab is accessed by selecting the Object Group in the Web Management Console’s Object Group Tree and then selecting the Change Log tab in the Information Display Area.

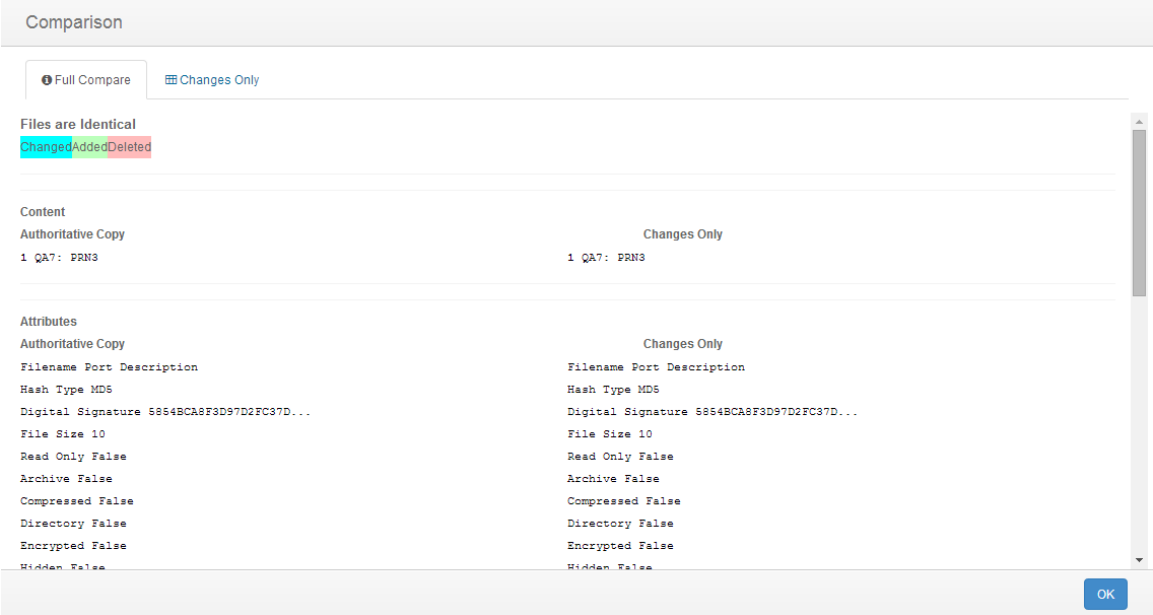


Figure 86: File Comparison Results

Click the Close button to exit the File Comparison Results dialog.

5.1.3.2.2.5.1. UNDERSTANDING THE OBJECT GROUP CHANGE TAB FILE COMPARISON RESULTS DIALOG

The File Comparison Results dialog displays anytime a comparison is performed between a detected change and the authoritative copy associated with watch properties. See section 0 for more information on performing file comparisons.

The File Comparison dialog is comprised of two tabs:

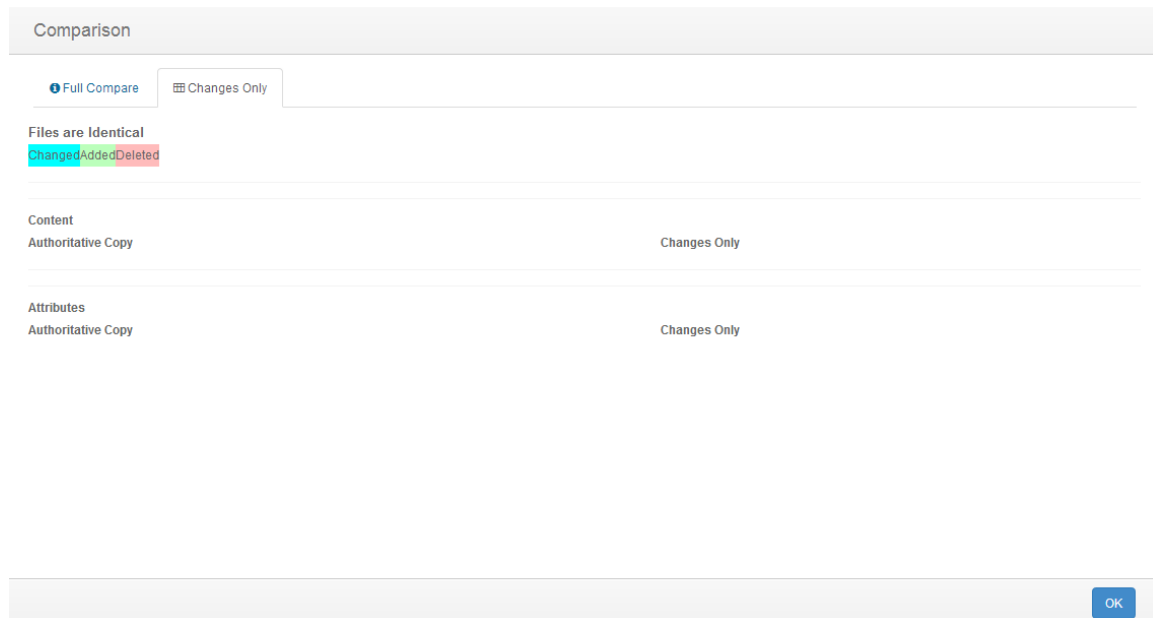
- Full Compare:** A comparison of both files are shown with all content and attributes listed.
- Changes only:** A comparison of both file are shown with only the content and attributes which the changes affected listed.

5.1.3.2.2.5.1.1. UNDERSTANDING THE FILE COMPARISON RESULTS DIALOG INFORMATION DISPLAY AREA AND TAB BROWSER

The File Comparison Results dialog Tab Browser and Information Display Area allows authorized CimTrak™ users the capability visualize generation comparison data. The File Comparison Results dialog is accessible by accessing the context menu and selected Compare with Authoritative Copy (Current) in the Object Group Change Tab. See section 0 for more information on performing file comparisons.

The File Comparison Results dialog Information Display Area shows a side-by-side comparison of one generation revision of a detected change to the Master Repository Authoritative Copy. Lines that have been modified are highlighted in blue, lines that have been added are highlighted in green, and lines that have been deleted are highlighted in red.

By default, the “Full Compare” tab is selected. The “Full Compare” tab shows all lines of a selected comparison. Selecting the “Changes Only” tab displays only the lines that have differences between the compared generations.



**Figure 87: File Comparison Results dialog Changes tab**

Click the Close button to exit the File Comparison Results dialog.

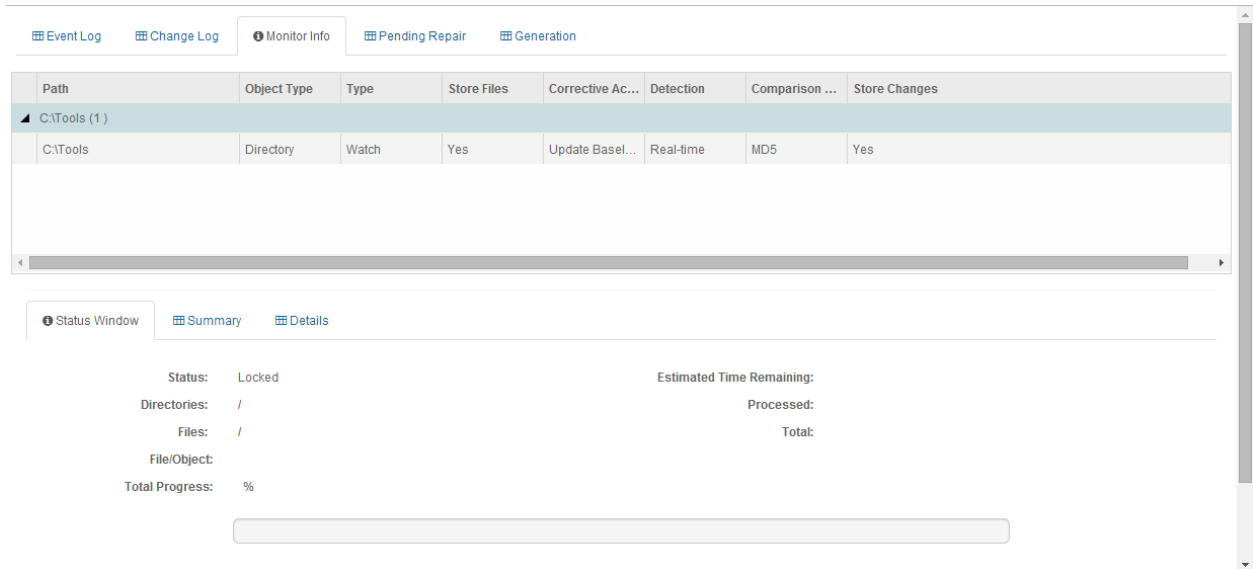
#### **5.1.3.3. REVIEWING OBJECT GROUP MONITORING INFORMATION**

The Object Group Monitor Info tab provides Object Group monitoring and status information relating to Object Groups connected to the File System Agent. Accessing the Object Group Monitor Info is accomplished by first clicking once on the Object Group name in the Object Group Tree to select it followed by clicking the Monitor Info tab in the Web Management Console Information Display Area.



The Object Group Monitor Info tab is comprised of two sections:

## Path Status Windows/Details



**Figure 88: Object Group Monitor Info tab**

The Path section displays watch path and exclude information pertaining to the select Object Group.

The Status Window/Details section is comprised of three tabs:

- **Status Window:** Displays current lock status information associated with the Object Group Watch Policy. (i.e. Lock, Locking, Unlocked)
- **Summary:**
- **Details:** Displays details associated with the Object Group Watch Policy Configuration including:
  - **Type:** Object Group policy type (generally Watch).
  - **Detection Mode:** The change detection mode enabled (Real-time or polling)
  - **File Comparison Method:** The hash type performed on monitored data.
  - **User Approval on Sync:** Require user intervention for changes detected while the File System Agent was disconnected from the Master Repository. (True, False)
  - **Store Files:** Store authoritative copy data in the Master Repository (True, False).
  - **Store Changes:** Store change data in the Master Repository (True, False).
  - **Ignore Archive Flag:** Monitor the archive flag associated with file system watch data. (True, False)

- **Ignore Read-only Flag:** Monitor the read-only flag associated with the file system watch data. (True, False)
- **Ignore SACL Flag:** Monitor the SACL flag associated with the file system watch data. (True, False)
- **Ignore DACL Flag:** Monitor the DACL flag associated with the file system watch data. (True, False)
- **Ignore Owner Security Flag:** Monitor the Owner Security flag associated with the file system watch data. (True, False)
- **Ignore Group Security Flag:** Monitor the Group Security flag associated with the file system watch data. (True, False)
- **Ignore Alternate Data Flag:** Monitor the Alternate Data flag associated with the file system watch data. (True, False)
- **Ignore File Dates Flag:** Monitor the File Dates flag associated with the file system watch data. (True, False)
- **Block Writes Flag:** Monitor the Block Writes flag associated with the file system watch data. (True, False)
- **Auto Exclude Files that have changed Flag:** Monitor the Auto Exclude Files that have changed flag associated with the file system watch data. (Enabled, Disabled)
- **Log Reads Flag:** Monitor the Log Reads flag associated with the file system watch data. (True, False)
- **Number of Intrusions to Keep:**
- **Keep Intrusion Size (in KB):**
- **Number of Revisions to Keep:**
- **Warn if Unlocked (in minutes):**
- **Number of Events to Keep:**
- **Corrective Action (On Add, On Change, On Delete):** The Corrective Action mode specified in the Object Group Watch Policy. (Restore, Update Baseline, Log, Prompt, Ignore)
- **Run (On Add, On Change, On Delete):** Custom script that is ran when an add, change, or delete action has occurred on monitored watch data. (Path/File Name)
- **Wait (On Add, On Change, On Delete):** Use remediation timeout period enforced on custom scripts that are ran when an add, change, or deleted action has occurred on the monitored watch data. (True, False)
- **Timeout (On Add, On Change, On Delete):** Remediation timeout period enforced on custom scripts that are ran when an add, change, or deleted action has occurred on the monitored watch data.
- **Parameters (On Add, On Change, On Delete):** Pass filed and action parameters to the attached script ran on add, change, or delete actions.

Status Window

Summary

Details

Status:

Locked

Estimated Time Remaining:

Directories:

/

Processed:

Files:

/

Total:

File/Object:

Total Progress:

%

**Figure 89: Monitor Info Status Window tab**

Status Window

Summary

Details

Detection Mode:

Real-time

Comparison Method:

MD5

Type:

Watched Directory

Store Files:

Yes

Store Changes:

Yes

Approval on Sync:

No

Block Writes:

No

Log Reads:

No

# Intrusions to Keep:

250

# Revisions to Keep:

250

# Events to Keep:

250 Events

Keep Intrusion Size:

500 (kb)

Warn if Unlocked:

0 min.

Auto exclude files:

Disabled

On Add:

Update Baseline

On Change:

Update Baseline

On Delete:

Update Baseline

**Figure 90: Monitor Info Summary Window tab**

Status Window

Summary

Details

Setting Name	Current Setting
Type	Watched Directory
Detection Mode	Real-time
File Comparison Method	MD5
User Approval on Sync	X
Store Files	✓
Store Changes	✓
Ignore Archive Flag	✓

**Figure 91: Monitor Info Details tab**

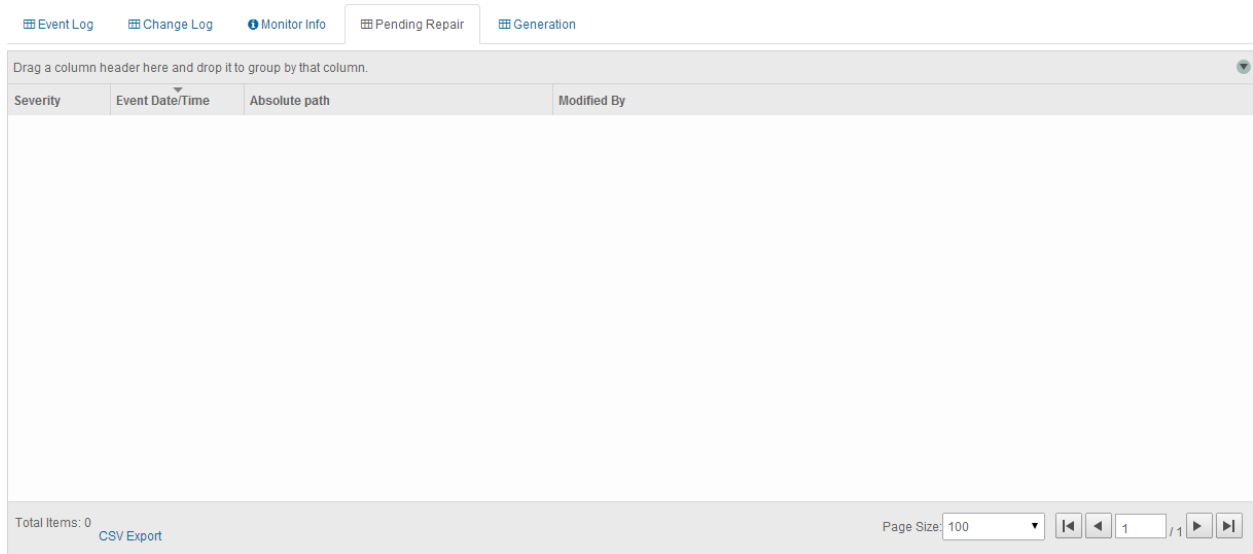
#### 5.1.3.4. REVIEWING OBJECT GROUP DATA PENDING REPAIR

The Pending Repair tab displays queue information associated with the remediation of folder, file and configuration data. The Pending Repair tab will append the number of pending repairs to the tab title. As changes are repaired they are automatically removed from the Pending Repair tab. Accessing the Object Group Pending Repair tab is accomplished by first clicking once on the Object Group name in the Object Group Tree to select it followed by clicking the Pending Repair tab in the Web Management Console Information Display Area.



***The Pending Repair tab also displays changes requiring CimTrak™ Administrator intervention. Intervention is required if the Prompt for Approval corrective action is enabled or the User Approval on Sync has been enabled and there was a***

## ***communication failure between the File System Agent and the Master Repository.***



Event Log Change Log Monitor Info Pending Repair Generation

Drag a column header here and drop it to group by that column.

Severity	Event Date/Time	Absolute path	Modified By
----------	-----------------	---------------	-------------

Total Items: 0 CSV Export Page Size: 100 1 / 1

**Figure 92: Pending Repair tab showing 3 pending repairs**

For each recorded event, the Object Group Pending Repair tab will display information corresponding to the following:

**Severity:** *The state of the pending repair.*

**Event Date/Time:** *The exact date and time of the detected event.*

**Absolute Path:** *File path affected by the detected event.*

**Modified By:** *The File System User responsible for the detected event.*

Generally, the items contained in the Pending Repair tab will automatically cycle out as the folders, files, and configurations are remediated on the monitored system. The Pending Repair tab will automatically refresh based on the Pending Repair Refresh Interval specified in the Master Repository Preferences dialog. See section 0 for additional information.

In the event the Pending Repairs exist due to the Prompt for Approval Corrective Action or a triggered User Approval on Sync the Changes Pending Approval dialog must be referenced. See a subsequent section for additional information on the Changes Pending Approval dialog.

Each Pending Repair message type has a corresponding icon that allows for quick visual reference to the urgency level of the event. These urgency levels are important to note when configuring E-Mail alert permissions. E-Mail alert permissions are explained in a subsequent section.

**Emergency:** *System is unusable. Highest level of event.*

**Alert:** *Take action immediately.*

**Critical:** *Critical conditions have occurred.*

**Error:** *Error conditions.*

**Warning:** *Warning conditions.*

**Notice:** *Normal condition that requires attention.*

**Information:** *Informational message.*

**Debug:** *Debug-level message. Lowest level of event.*

Specifics relating to message types are discussed in a subsequent section.

#### **5.1.3.4.1. FILTERING AND SORTING THE PENDING REPAIR TAB**

The Pending Repair Tab can be filtered to only show events matching the specified criteria. Accessing the Object Group Event Log is accomplished by first clicking once on the Object Group in the Object Group Tree to select it followed by clicking the Pending Repair tab in the Web Management Console Information Display Area.

To filter the information displayed in the Pending Repair Tab, drag and drop one of the column headers into the section labelled “Drag a column header here and drop it to group by that column.”

#### **5.1.3.5. OBJECT GROUP GENERATIONS**

The Object Group Generation Tab provides revision information for changes occurring to files, folders, operating system configurations contained in a File System Agent Object Group. Accessing the Object Group Generations Tab is accomplished by first clicking once on the Object Group in the Object Group Tree to select it followed by clicking the Generation tab in the Web Management Console Information Display Area.

The Generation Tab is broken into two sections:

**Revisions Table**

**Revision Details**

Event Log

Change Log

Monitor Info

Pending Repair

Generation

Revision	Sub-revision	Date/Time	Changed by	# of Dirs	# of Files	Total Size(bytes)
0000019	0000001	3/19/2014 10:18:15	admin	3	14	40757180
0000018	0000001	3/13/2014 11:03:27	admin	3	14	40757180
0000017	0000025	3/13/2014 10:08:23	admin	Calculating...	Calculating...	Calculating...
0000017	0000024	3/13/2014 10:08:20	admin	Calculating...	Calculating...	Calculating...

Total Items: 43

CSV Export

Page Size: 100

1

1

Revision Information

Details

Change From Previous

Date of Revision:

3/13/2014 11:03:27

Revised by:

admin

Revision:

0000018

Sub-Revision:

0000001

Number of Files:

14

Number of Directories:

3

Notes:

Lock Request

**Figure 93: Object Group Generation Tab**

The Revisions Table displays overview information relating to each generation revision. Selecting a specific generation revision in the Revision Table will populate the corresponding information in the Revision Details section.

Information in the Revisions Table includes:

**Revision:** Primary revision number indicating the number of the generation.

**Sub-revision:** Secondary revision number indicating the number of events that have occurred since the primary generation was created.

**Date/Time:** Date and time associated with the creation of the revision or sub-revision.

**Changed by:** The CimTrak™ User account responsible for the creation of the revision or sub-revision.

**# of Dirs:** Quantity of directories contained in the revision or sub-revision.

**# of Files:** Quantity of files contained in the revision or sub-revision.

**Total Size (bytes):** The total amount of disk space utilized by the contents of the revision or sub-revision.

The Revision Details section displays detailed information relating to a revision or sub-revision. The Revision Details section has three tabs:

**Revision Information:** Details of the revision or sub-revision such as the date of the revision, revising user account, number of revisions, number of sub-revisions, number of files, number of directories, and notes.

**Details:** Complete list of all files and folders contained in a generation. Files and folders indicate their generation status such as “Added”, “Deleted”, and “Modified”.

**Change from Previous:** Partial file list showing what files were “Added”, “Deleted” or “Modified” in the selected generation.

#### 5.1.3.5.1. DOWNLOADING GENERATION DATA

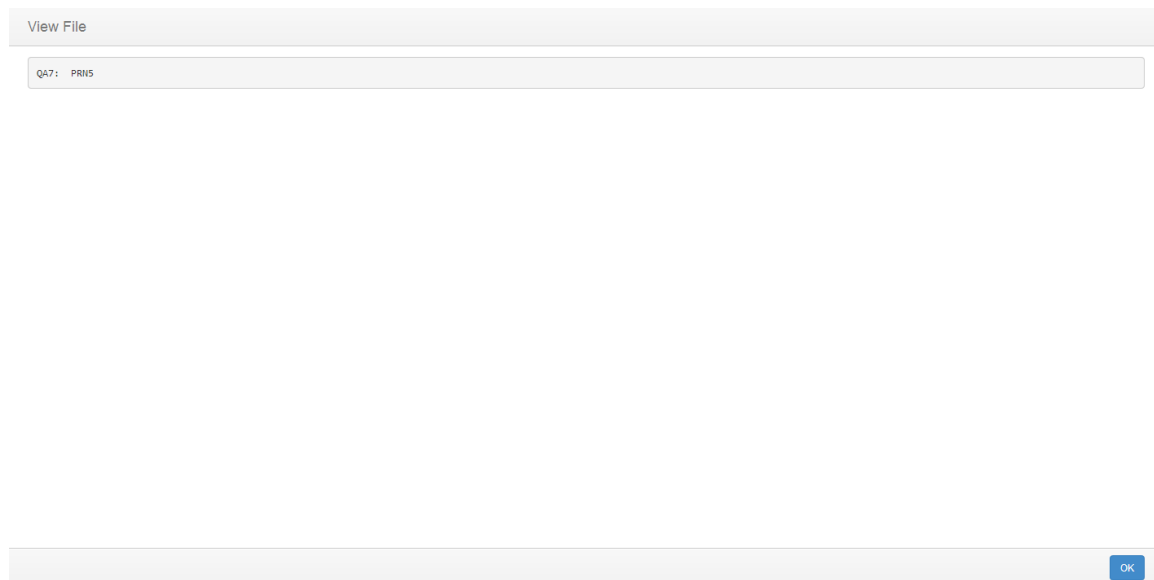
Each file stored in an Object Group generation has the capability to be downloaded and copied to a local system. An Object Group generation can be accessed by first clicking once on the Object Group in the Object Group Tree to select it followed by clicking the Generation tab in the Web Management Console Information Display Area.

Copies of generation data can be downloaded by right-clicking on the Revisions Table generation and selecting “Download” from the context menu. Additionally, copies of generation data can also be downloaded from the Revision Details Details tab or Change from Previous tab by right-clicking on the file or folder to download and then clicking “Download”.

#### 5.1.3.5.2. VIEWING AND COMPARING CONTENT OF OBJECT GROUP GENERATIONS

Folders, files, and configurations monitored within an Object Group generation have the capability to be viewed and compared with other generations. An Object Group generation can be accessed by first clicking once on the Object Group in the Object Group Tree to select it followed by clicking the Generation tab in the Web Management Console Information Display Area.

To view the non-binary file contents associated with a file, select either the Details or Change from Previous tab in the Object Group Generation Revision Details section. Right-click on the file and then select “View”. The File View dialog will display.

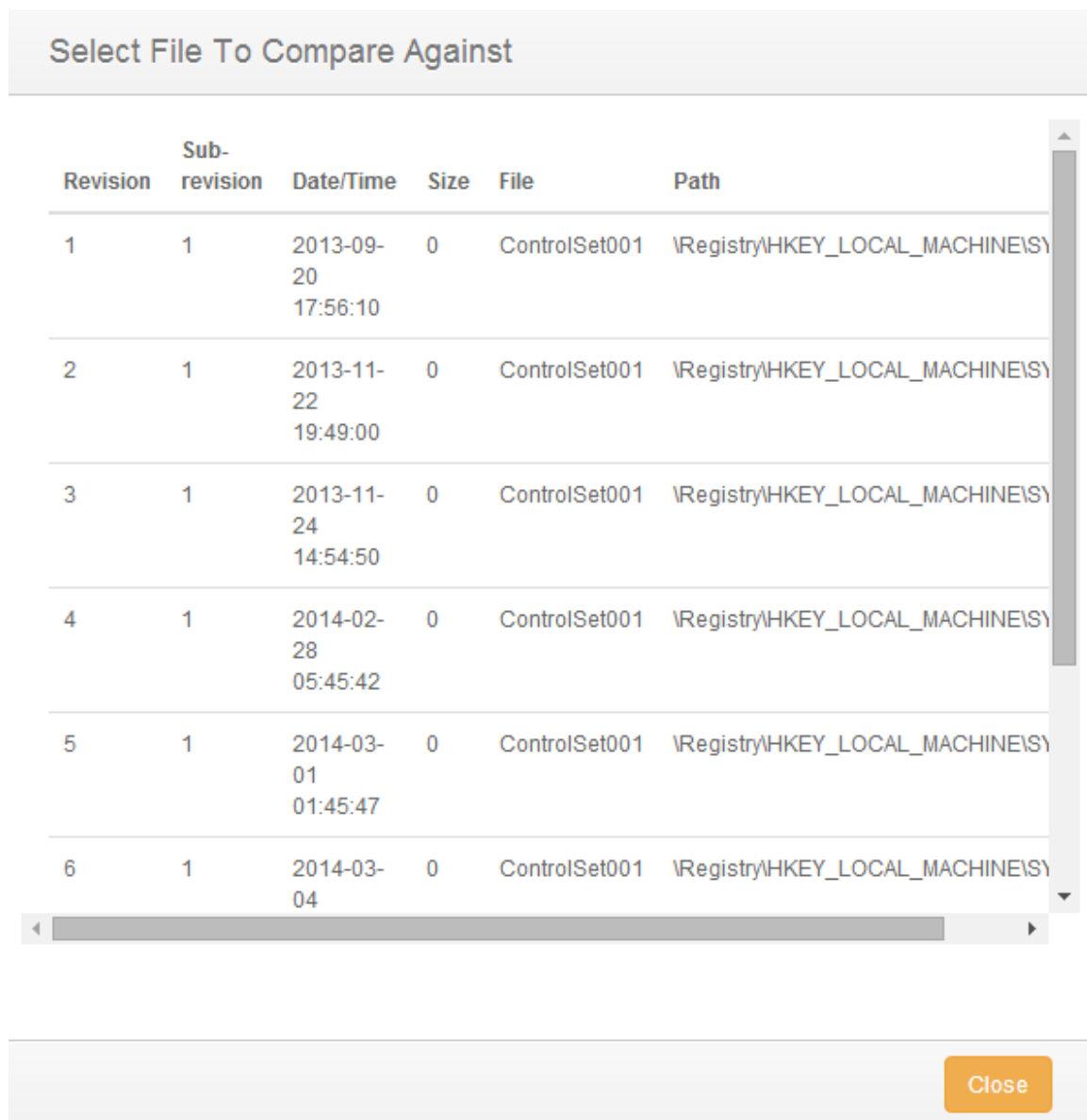


**Figure 94: File View dialog (non-binary)**

Click “Close” to exit the File View dialog.

The Object Group Generations tab has the capability to compare previous generations with the current state of the file stored within the Master Repository to the local system. To compare a generation, click the “Object Group” node in the Web Management Console Object Group Tree. Select the generations tab.

To compare the file, from either the Details or Change from Previous tab, right-click on the file and then select either “Compare with Other Generation” or “Compare with Authoritative Copy (current)”. If “Compare with Other Generation” is selected the Select File to Compare Against dialog will display. Select the generation to compare with by clicking once on the revision. Click “OK” to perform the comparison or click “Cancel” to abort the comparison process. The File Comparison Results dialog will display.



**Figure 95: File to Compare Against dialog**



In the event “Compare with Authoritative Copy (current)” is selected the File Comparison Results will display comparing the current file content with the most current baseline.

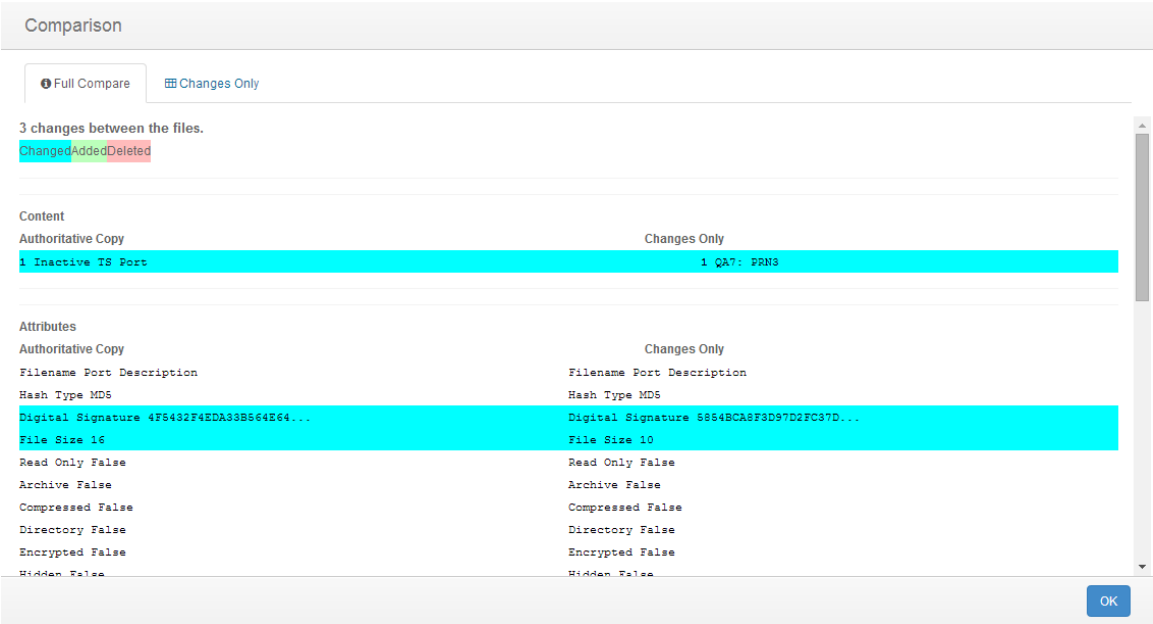


Figure 96: File Comparison Results dialog

Click the “Close” button to exit the File Comparison Results dialog.

#### 5.1.3.5.2.1. UNDERSTANDING THE OBJECT GROUP CHANGE TAB FILE COMPARISON RESULTS DIALOG

The File Comparison Results dialog displays anytime a comparison is performed between a detected change and the authoritative copy associated with watch properties. See section 0 for more information on performing file comparisons.

The File Comparison dialog is comprised of two primary sections.

**Information Display Area**  
**Tab Browser**

#### 5.1.3.5.2.1.1. UNDERSTANDING THE FILE COMPARISON RESULTS DIALOG INFORMATION DISPLAY AREA AND TAB BROWSER

The File Comparison Results dialog Tab Browser and Information Display Area allows authorized CimTrak™ users the capability visualize generation comparison data. The File Comparison Results dialog is accessible by accessing the context menu and selected Compare with Authoritative Copy (Current) in the Object Group Change Tab. See section 0 for more information on performing file comparisons.

The File Comparison Results dialog Information Display Area shows a side-by-side comparison of one generation revision of a detected change to the Master Repository Authoritative Copy. Lines that have been modified are highlighted in blue, lines that have been added are highlighted in green, and lines that have been deleted are highlighted in red.

By default, the Complete tab is selected in the File Comparison Results Tab Browser. The Complete tab shows all lines of a selected comparison. Selecting the Changes tab displays only the lines that have differences between the compared generations.

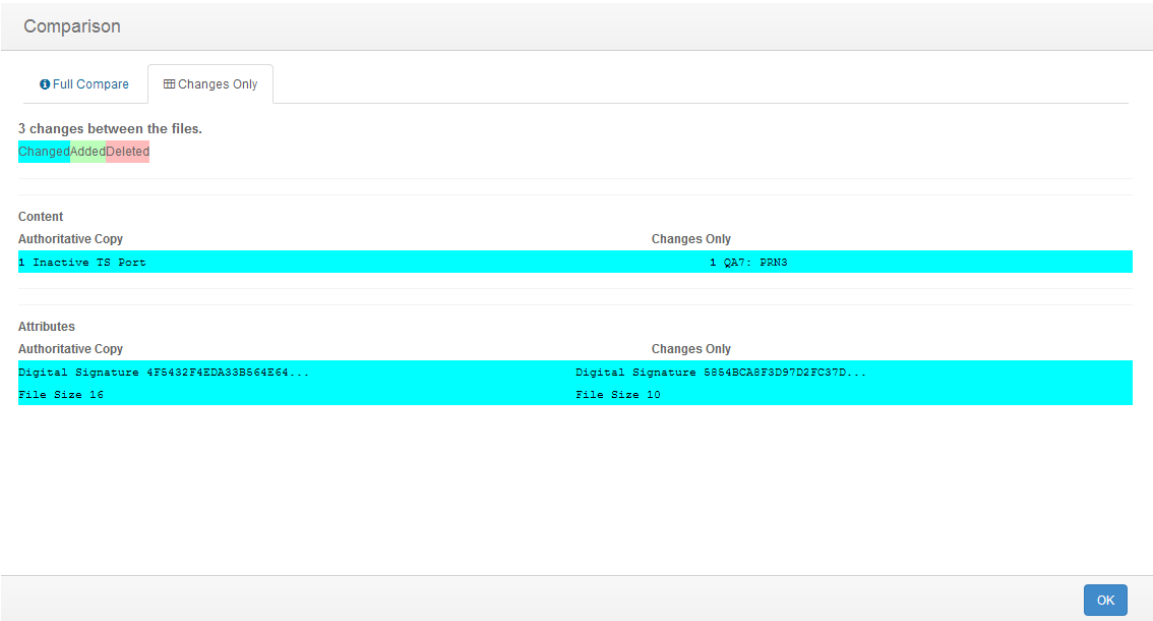


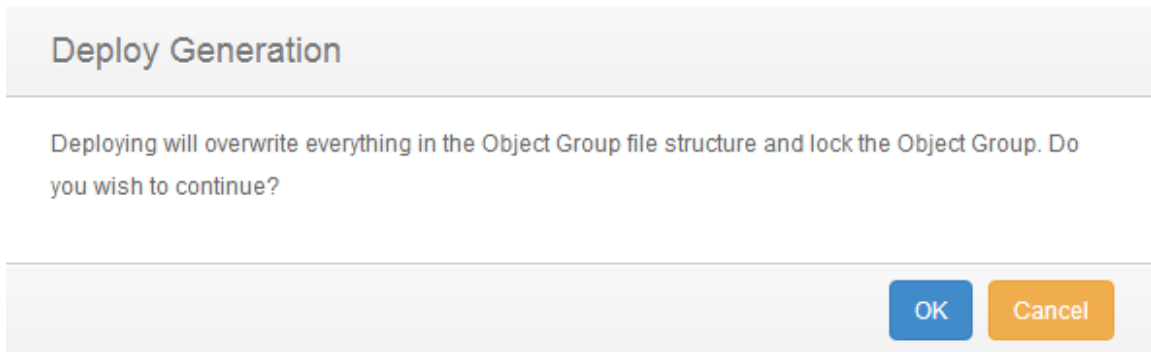
Figure 97: File Comparison Results dialog Changes tab

Click the Close button to exit the File Comparison Results dialog.

#### 5.1.3.5.3. DEPLOYING “ROLLING BACK” OBJECT GROUP GENERATIONS

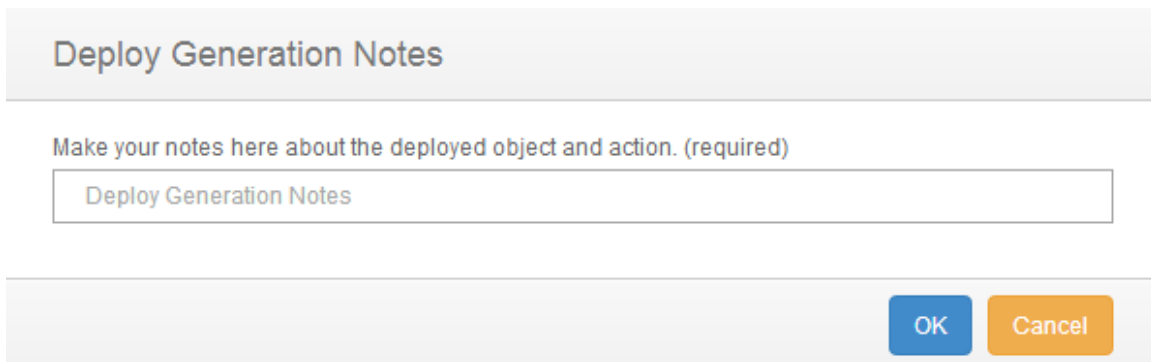
Depending on the remediation capabilities of the monitoring Object Group, the Generations tab may have the capability to deploy previous generations back to the File System. An Object Group generation can be accessed by first clicking once on the Object Group in the Object Group Tree to select it followed by clicking the Generation tab in the Web Management Console Information Display Area.

To deploy “roll back” a generation, select the generation in the Generation Tab Revisions Table, right-click, and then select “Deploy”. The Confirm Deploy dialog will display warning that deploying will overwrite everything in the Document Control with the content of this generation. Click “Yes” to proceed or “Cancel” to abort the operation.



**Figure 98: Confirm Deploy dialog**

Upon clicking “Yes” on the Confirm Deploy dialog the Notes dialog will appear. Enter any administrative notes relating to this deployment and then click “OK”. Click “Cancel” to abort the deployment.



**Figure 99: Notes dialog**

A new generation revision will be created with the rolled-back content. This newly created generation is the current generation.

#### **5.1.3.6. OBJECT GROUP PERMISSIONS**

Object Groups can be configured restrict access based on permission settings. Additionally, event notifications can be configured to notify CimTrak™ Users about events relating to the Object Group. Accessing Object Group permissions is accomplished by first clicking once on the File Object Group in the Object Group Tree to select it and then right-clicking and selecting “Permissions.” The Security Permissions dialog will display.

By default each Object Group will have the following permissions:

##### **Administrators**

**Create Objects:** *Create File System Agent Object Groups.*

**Edit:** *Edit File System Agent settings.*

**Lock:** *Enable active monitoring of Object Group Data.*

**Reports:** *View reports relating to the Object Group contents.*

**Unlock:** *Disable active monitoring of Object Group Data.*

**View:** *View contents and configurations relating to the Object Group.*

##### **Auditors**

**Reports:** View reports relating to Object Group contents.

**View:** View contents and configurations relating to the Object Group..

**Installers**

Attach CimTrak™ Agents to a Master Repository. (Not applicable for Object Groups).

Permissions for Object

Add

Group or User Names

Group	Administrators	
Group	Auditors	
Group	Email_Testing	Remove
Group	Installers	

Permissions	Allow	Deny
Create Objects	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Edit	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lock	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Reports	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Unlock	<input checked="" type="checkbox"/>	<input type="checkbox"/>
View	<input checked="" type="checkbox"/>	<input type="checkbox"/>

☒ Apply permissions to children recursively

OKCancel

**Figure 100: Object Group Security Permissions dialog**

Default access permissions associated with the Administrators, Auditors, and Installers User Groups cannot be changed. It is possible to modify E-mail alert notices for Administrator and Auditor user groups. Available E-mail alert types include:

Emergency  
Alert

Critical  
Error  
Warning  
Notice  
Information

Additional information relating to these alert types is described in a subsequent section.

#### **5.1.3.6.1. MODIFYING AN EXISTING USER/GROUP OBJECT GROUP PERMISSIONS**

It is possible to modify existing user and group Object Group Permissions and E-mail notification settings. Accessing Object Group permissions is accomplished by first clicking once on the Object Group in the Object Group Tree to select it and then right-clicking and selecting “Permissions.” The Security Permissions dialog will display.

Select the existing user or group by clicking once on the CimTrak™ User or Group name in the Group or User Names section of the Security Permissions dialog. The Permissions section of the Security Permissions dialog will update to show the permissions currently assigned to the selected user or group.



***Selecting a group will apply the selected permissions and E-mail notification settings to all members of the group. Selecting a single user will apply the selected permissions and E-mail notification settings to only that single user account.***

To add or remove permissions click the “Allow” or “Deny” checkbox corresponding to the permission being configured. Available permissions include:

**Create Objects:** *Create File System Agent Object Groups.*

**Edit:** *Edit Object Group control contents.*

**Lock:** *Enable active monitoring of Object Group Data*

**Reports:** *View reports relating to Object Group contents.*

**Unlock:** *Disable active monitoring of Object Group Data*

**View:** *View contents and configurations relating to the Object Group.*

**Email Emergency:** *Receive alerts relating to emergency level notifications.*

**Email Alert:** *Receive alerts relating to alert level notifications.*

**Email Critical:** *Receive alerts relating to critical level notifications.*

**Email Error:** *Receive alerts relating to error level notifications.*

**Email Warning:** *Receive alerts relating to warning level notifications.*

**Email Notice:** *Receive alerts relating to notice level notifications.*

**Email Information:** *Receive alerts relating to information level notifications.*

To apply the permission settings to all children objects, ensure that the Apply permissions to children recursively checkbox is selected.

When completed, click “OK” to apply the permission and alert settings. Click “Cancel” to abort the security permission configuration.



***Permissions and notification settings can be inherited from parent objects (such as the File System Agent) if the permissions are created at a parent level.***



***Permissions and notification settings are not automatically inherited for new objects. It will be necessary to manually assign the permissions and notification settings to the object.***

#### **5.1.3.6.2.    ADDING AND REMOVING USERS AND GROUPS TO OBJECT GROUP PERMISSIONS**

It is possible to add additional users and groups to the Security Permissions dialog so that Object Group Permissions and E-mail notification settings can be assigned or changed. Accessing Object Group permissions is accomplished by first clicking once on the Object Group in the Object Group Tree to select it and then right-clicking and selecting “Permissions.” The Security Permissions dialog will display.

To add a new local CimTrak™ User or Group, click the Add button. The Add Users dialog will display listing all available local users and groups.

Select Users or Groups

Q Search

	Type	Name
<input type="checkbox"/>	User	aaaa
<input type="checkbox"/>	User	wade
<input type="checkbox"/>	User	knightrider
<input type="checkbox"/>	User	payton
<input type="checkbox"/>	User	Pippen
<input type="checkbox"/>	User	Hanks
<input type="checkbox"/>	User	Rose
<input type="checkbox"/>	User	Garnett
<input type="checkbox"/>	User	Fridge
<input type="checkbox"/>	User	alberts
<input type="checkbox"/>	User	jovo2

OKCancel

**Figure 101: Add Users dialog**

Select the local CimTrak™ User or Group to add by selecting the checkbox to the left of the name. Click “OK” to add the User or Group. Click “Cancel” to abort the addition process. The selected user or group will now display in the Group or User Names section of the Security Permissions dialog.

The User or Group is now available to have permissions and notification settings assigned. See section 0 for more information.

## 6. Configuring and Using the CimTrak™ Network Device Agent

### 6.1. MANAGING THE CIMTRAK™ NETWORK DEVICE AGENT FROM THE WEB MANAGEMENT CONSOLE

Management of the CimTrak™ Network Device Agent requires that the Web Management Console is associated with the Master Repository and that a valid user account has been authenticated. For more information on associating the Web Management Console with the Master Repository please refer to section 3. For more information on authenticating with the Master Repository please refer to section 3.1.

Once authenticated with the Master Repository multiple configuration, customization, and reporting options are available through the Web Management Console.

Network Device Agents that have been installed and associated with the selected Master Repository will display in the CimTrak™ Web Management Console's Object Group Tree.



Figure 102: CimTrak™ Network Device Agent in Object Group Tree

The connection status of the CimTrak™ Network Device Agent can be confirmed by the associated icon.



Figure 103: Cimtrak™ File System Agent Connection Icon



6.1.1. NETWORK DEVICE AGENT PROPERTIES

The Network Device Agent Properties dialog allows authorized CimTrak™ users to perform administrative tasks relating to CimTrak™ Network Device Agent logging, throttling, heartbeat and statistic transmissions and health monitoring parameters.

Accessing the CimTrak™ Network Device Agent Properties dialog is accomplished by right-clicking on the Network Device Agent name in the Object Group tree and then selecting “Properties.” The CimTrak™ Agent Configuration dialog will display.

The CimTrak™ Agent Configuration dialog consists of several functional sections including:

- Description
- Agent Throttling
- Number of Events to Keep
- DB Options
- Poll Intervals

The functionality associated with these sections is explained in subsequent sections.

Agent Properties

Name	stackato_1150		Date In Service		
Location			Description		
URL			Contact		
Events to Keep	0	Ever (0=no limit)	Cancel Lock when exceeds	200000	objects (0=no limit)
Agent Throttling	1		Agent Stats Interval	10	seconds
HeartBeat Interval	30	seconds	Offline Event Cache	Off	
Warn if Disconnected	0	minutes			
Whitelist Mode	Off				

OK

Cancel

Figure 104: CimTrak™ Agent Configuration

6.1.1.1. CONFIGURING THE NETWORK DEVICE AGENT DESCRIPTION PROPERTIES

The CimTrak™ Network Device Agent Description and associated information can be customized through the CimTrak™ Agent Configuration dialog. Accessing the CimTrak™ Agent Configuration dialog is accomplished by right-clicking on the Network Device Agent name in the Object Group tree and then selecting “Properties.” The CimTrak™ Agent Configuration dialog will display.

Name	stackato_1150	Date In Service	
Location		Description	
URL		Contact	

**Figure 105: Network Device Agent Description**

#### **Network Device Agent Description Information:**

**Name:** *Used to indicate a unique name for the Network Device Agent.*

**Date in Service:** *Optional Date and Time associated with the in-service date of the Network Device Agent*

**Location:** *Optional Network Device Agent Location information.*

**Description:** *Optional Network Device Agent Description information.*

**URL:** *Optional URL information associated with the Network Device Agent.*

**Contact:** *Optional Contact information associated with the Network Device Agent.*

Once all sections have been populated, click the “OK” button to save the Network Device Agent Description Information. Click “Cancel” to abort the Network Device Agent properties modification.



***A Network Device Agent can be renamed by either changing the name in the Name textbox or by right-clicking the Network Device Agent in the Object Group Tree and selecting “Rename”.***

#### **6.1.1.2. CONFIGURING THE NETWORK DEVICE AGENT LOG RETENTION PROPERTIES**

The CimTrak™ Network Device Agent log retention settings can be customized through the CimTrak™ Agent Configuration dialog. Accessing the CimTrak™ Agent Configuration dialog is accomplished by right-clicking on the Network Device Agent name in the Object Group tree and then selecting “Properties.” The CimTrak™ Agent Configuration dialog will display.

The “Number of Events to Keep” section of the dialog allows for the configuration of Network Device Agent Event Log data retention. The event log can be configured to flush older records on a day interval or message quantity limit.

Events to Keep	0	Ever ▼	(0=no limit)
----------------	---	--------	--------------

**Figure 106: Number of Events to Keep settings**

**Days:** The event log will automatically remove event messages older than the indicated value. Entering “0” will store event messages indefinitely. (Maximum Days: 10,000)

Quantity: The event log will automatically remove older event messages as the amount of messages exceeds the indicated value. Entering “0” will store event messages indefinitely. (Maximum Quantity: 10,000)



***Storing an unlimited number of events has the potential to exhaust all available disk space on the Master Repository and degrade system performance.***

Once the data retention settings have been selected, click the “OK” button to save the Network Device Agent properties configuration. Click “Cancel” to abort the Network Device Agent properties configuration.

#### **6.1.1.3. CONFIGURING THE NETWORK DEVICE AGENT DISCONNECT WARNING**

The CimTrak™ Network Device Agent must remain in communication with the Master Repository at all times. If configured a failure to communicate with the Master Repository can generate an auditable event. Setting of disconnection notices is performed in the CimTrak™ Agent Configuration dialog. Accessing the CimTrak™ Agent Configuration dialog is accomplished by right-clicking on the Network Device Agent name in the Object Group tree and then selecting “Properties.” The CimTrak™ Agent Configuration dialog will display.

The DB Options section of the dialog allows for the configuration of Agent disconnection warnings. Warnings are generated if the Agent is out of communication with the Master Repository for a time period longer than the specified time in minutes. Accepted values (in minutes) include 1 through 4,194,304. Setting the “Warn if Disconnected” minute value to 0 disables the warning.

Warn if Disconnected  minutes

Figure 107: CimTrak™ Agent DB Options settings



***The notification of the disconnect occurs at the nearest heartbeat transmission. For example, if a heartbeat is set to 30 seconds and the disconnect is set to 2 minutes the alert will occur between 2 minutes and 2 minutes, 30 seconds depending on where the event occurs in the heartbeat cycle.***

Once the DB Options settings have been selected, click the “OK” button to save the Network Device Agent properties configuration. Click “Cancel” to abort the Network Device Agent properties configuration.

#### 6.1.1.4. CONFIGURING THE NETWORK DEVICE AGENT HEARTBEAT AND STATISTIC GATHERING INTERVAL

The CimTrak™ Network Device Agent communications can be throttled to control the speed of communications with the Master Repository. This capability is useful in limiting network bandwidth requirements and CPU cycles on the Agent host operating system. Setting of Agent Throttling is performed through the CimTrak™ Agent Configuration dialog. Accessing the CimTrak™ Agent Configuration dialog is accomplished by right-clicking on the Network Device Agent name in the Object Group tree and then selecting “Properties.” The CimTrak™ Agent Configuration dialog will display.



Figure 108: Network Device Agent Throttling settings

Setting Agent Throttling does not delay the remediation capabilities of the Network Device Agent. The Throttle is applied to communication transfer relating to events. The Throttle indicates the wait time between file transmissions and/or 60 KB data transmission.

The Throttle applies to the following scenarios:

- Sending Watch Data and Files to the Master Repository
- Syncing Watch Directories
- Locking Directories

Sliding the Agent Throttling slider to the left reduces the throttling (speeds up communications). Sliding the Agent Throttling slider to the right increases the throttling (slows down communications). By default, the Agent Throttling is set one tick right of Off.

Once the Agent Throttling settings have been selected, click the “OK” button to save the Network Device Agent properties configuration. Click “Cancel” to abort the Network Device Agent properties configuration.

#### 6.1.1.5. CREATING AND EDITING OBJECT GROUP WATCH POLICIES

The Network Device Agent has the capability to monitor critical files and operating system configurations on the host system containing the Network Device Agent or remote file shares. For many monitored files and configurations, CimTrak™ has the capability to remediate detected changes. To enable monitoring the CimTrak™ Network Device Agent must have Object Group Policies created and enabled.

To edit an Object Group Watch Policy, select the Object Group Policy to modify by right-clicking its name in the Object Group Tree. Select **Properties** in the Context menu. The New Network Device dialog will display.

Plugin Properties

Device Type Cisco NEXUS ▼

Cisco Nexus

Protocol: SSH ▼

IP Address:

Port: 22

Username:

Password:

Enable Password (If Required):

Configuration Transfer Protocol: SSH ▼

OK

Cancel

Figure 109: New Network Device dialog

The Network Device dialog allows for the communication and data transfer configurations associated with the monitored network device. Default supported network devices, communication methods, and file transfer methods are outlined in Table 2: Network Device Communication and File Transfer Protocols

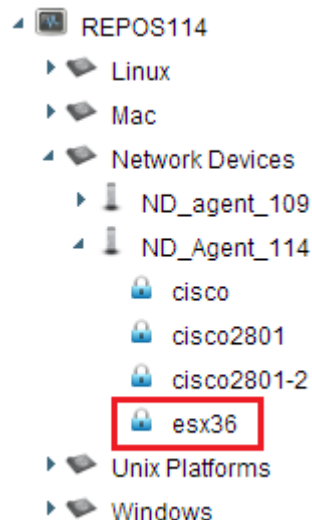
Additional supported network devices may be available in your region. Contact an authorized CimTrak™ Sales Representative for more information.

*Monitoring and communicating with Cisco IOS devices supporting SNMPv2c or SNMPv3 requires additional configuration on the monitored network device. See a subsequent section for configuration details.*

Populating the Network Device dialog and clicking the OK button results in the Object Group Properties dialog to display. To abort the Network Device Configuration click the Cancel button.

To edit an Object Group Watch Policy, select the Object Group Policy to modify by right-clicking its name in the Object Group Tree. Select **Properties** in the Context menu. The Object Group Properties dialog will display.

Once the Object Group has been created it will display in the CimTrak™ Web Management Console's Object Group Tree.



**Figure 110: CimTrak™ Web Management Console's Object Group Tree Showing Object Groups**

To enable monitoring of the Object Group it must be “locked”. Detailed information about creating Object Group Watch Policies and enabling/disabling monitoring is explained in subsequent sections.

#### **6.1.1.5.1. OBJECT GROUP PROPERTIES**

The process of creating a new or editing an Object Group Watch Policy can be initiated by selecting the Network Device Agent of the system to monitor by clicking it once in the Web Management Console's Object Group Tree, clicking the “New” drop-down button in the Menu Bar, followed by Object Group. The Object Group Properties dialog will display.

To edit an Object Group Watch Policy, select the Object Group Policy to modify by right-clicking its name in the Object Group Tree. Select **Properties** in the Context menu. The Object Group Properties dialog will display.

The Object Group Properties dialog is comprised of several sections. Each of these sections has specific functionality relating to the monitoring performed by the Network Device Agent.

Object Group Properties

Policy Attributes

Location: Location

Description: Description

Date Put In Service: 2013-09-10 14:59:13

Contact: Name of Contact

URL:

Notes:

Require Notes On Lock: ☐

Number of Intrusions to Keep: 250

Keep Intrusion Size (in KB): 500

Number of Revisions to Keep: 250

Warn if Unlocked (in minutes): 0

Events To Keep (0=no limit): 250

Events:

Watched in this group: ■

Watched elsewhere: ■

OK Cancel

**Figure 111: Cimtrak™ Network Device Object Group Properties (Attributes Tab)**

**Object Information**  
**Private Key Implementation**  
**Monitoring Information**  
**Operating System Tree**  
**Watch Properties**

### **Network Device Agent Object Information:**

Object Information provides CimTrak™ Users and Administrators detailed information pertaining to the Object Group Watch Policy. The “Object Group Name” is the only required field. Object Group Names must be unique and may contain between 1 and 49 characters.

Location: Location

Description: Description

Date Put In Service: 2013-09-10 14:59:13

Contact: Name of Contact

URL:

Notes:

Require Notes On Lock: ☐

**Figure 112: Network Device Agent Object Information**

**Location:** *Optional Object Group Location information.*

**Description:** *Optional Object Group Description information.*

**Date Put in Service:** *Optional Date and Time associated with the in-service date of the Object Group.*

**Contact:** *Optional Contact information associated with the Object Group.*

**URL:** *Optional URL information associated with the Object Group.*

**Notes:** *Optional dialog to enter administrative notes associated with the Object Group.*

Optionally, the Object Group Watch Policy has the capability to require CimTrak™ Users and Administrators to enter notes when enabling monitoring of the Object Group Watch Policy. Enabling of required notes is performed by selecting the Require Notes on Lock checkbox.

### **Monitoring Information:**

**Number of Intrusions to Keep:** *Number of added files/configurations to keep in the Change Log. A zero placed in this field indicates unlimited changes will be stored. Maximum accepted value of 10,000 changes.*

**Keep Intrusion Size (in KB):** *The maximum file size an added file can be for it to be stored in the Change Log. Files exceeding this change size limit are still detected but cannot be compared or retrieved. Maximum accepted value of 4,194,304 KB.*

**Number of Revisions to Keep:** *Number of revisions to keep for each change to files and configurations monitored by the Object Group. A zero placed in this field indicates unlimited changes will be stored. Maximum accepted value of 10,000 revisions*

**Warn if Unlocked (in minutes):** *Generate a notice if monitoring of the Object Group has been disabled for more than the indicated time. A zero placed in this field disables the warning. Maximum accepted value of 10,000 minutes.*

**Number of Events to Keep:** *Quantity or Days to store Object Group Event Log audit records. Maximum accepted value of 10,000 events.*

***Storing an unlimited number of events, revisions, or changes has the potential to exhaust all available disk space on the Master Repository and degrade system performance.***

Number of Intrusions to Keep	<input type="text" value="250"/>	Number of Revisions to Keep	<input type="text" value="250"/>	Events To Keep (0=no limit)	<input type="text" value="250"/>	<input type="text" value="Events"/>
Keep Intrusion Size (in KB)	<input type="text" value="500"/>	Warn if Unlocked (in minutes)	<input type="text" value="0"/>			

**Figure 113: Network Device Agent Monitoring Information**

### **Operating System Tree**

The Operating System Tree, located at the lower left corner of the Object Group Properties dialog, contains a listing of all files, folders, and operating system configurations that can be monitored by the CimTrak™ Network Device Agent. The contents of the Operating System Tree are system specific. Additionally, external CimTrak™ Plug-ins attached to the Network Device Agent will appear in the Operating System Tree.

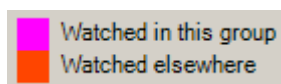


**Figure 114: Cisco IOS Operating System Tree**



Selecting data to monitor is accomplished by checking the checkbox next to the system component. The contents of the Operating System Tree can be expanded or collapsed by clicking the ► or ◄ symbols corresponding with each monitor type. Selecting any monitor data results in the Watch Properties dialog to display. See a subsequent section for more information on setting Watch Properties.

***Content that is monitored in the current Object Group is displayed in the File System Tree in a pink font color. Content that is monitored elsewhere is displayed in a orange font color.***



**Figure 115: Watch notifications**

**Microsoft Windows Network Device Agents have the capability to monitor:**

**Drivers:** *Drivers are specialized programs designed to run in the background of a system and to control specific hardware. This feature allows security professionals the capability to monitor drivers for changes, additions, or deletions. Remediation capability is not available for monitoring of system drivers. The recommended monitoring mode is “Update Baseline”. This feature supports polling detection.*

**Installed Software:** *Installed Software monitoring detects any software that has been installed using a standard installation tool. This mode displays any software that is registered in Microsoft Windows to display in the “Add/Remove Programs” dialog. This feature allows security professionals the capability to monitor if new or additional software has been installed or uninstalled. Remediation capability is not available for monitoring of installed software. The recommended monitoring mode is “Update Baseline”. This feature supports polling detection.*

**Network Shares:** *Monitoring of Network Shares allows security professionals the capability to monitor the share settings associated with files and folders on a Windows operating system. This mode allows for remediation of any detected changes. The recommended monitoring mode is “Restore from Repository”. This feature supports polling detection.*

**Registry:** *Windows Registry monitoring allows security professionals the capability to define a preset list of registry keys to monitor. CimTrak™ will detect any modifications to this preset list of keys or values. The recommended monitoring mode is “Restore from Repository”. This feature supports polling or real-time detection.*

**Security Policy:** *Monitoring of the local Security Policy allows security professionals the capability to monitor the settings associated with the local security policy. Local security policies are relevant even if the system is attached to a domain since the local security policies are*

*executed before group policies. Locking the Security Policy helps ensure that the intended local security policies of an organization are maintained. The recommended monitoring mode is “Update Baseline”. This feature supports polling detection.*

**Services:** *Services are specialized programs designed to run in the background of a system. This feature allows security professionals the capability to monitor when new or additional services have been started or configurations of existing services have been modified. The recommended monitoring mode is “Update Baseline”. This feature supports polling detection.*

**System Groups:** *Monitoring of local system groups allows security professionals the capability to detect changes to all local user groups existing on the monitored system. CimTrak™ detects when groups are added, deleted, or modified. The recommended monitoring mode is “Update Baseline”. This feature supports polling detection.*

**System Users:** *Monitoring of local system users allows security professionals the capability to detect when local user accounts are added, deleted, or modified on the system. Using this feature is important even if the system is attached to a domain as additional or modified local user accounts can create a system vulnerability. The recommended monitoring mode is “Update Baseline”. This feature supports polling detection.*

**Local File System:** *Monitoring of the local file system will detect (and optionally remediate) any addition, deletion, or modification to files and folders on the monitored system. This feature supports polling or real-time detection.*

**Network File System:** *Using the optional “Network Drive Enabler” allows for the detection (and optionally remediation) of any addition, deletion, or modification to files and folders to monitored network share data. This feature supports polling detection.*

**Linux, UNIX, and Macintosh Network Device Agents have the capability to monitor:**

**System Groups:** *Monitoring of local system groups allows security professionals the capability to detect changes to all local user groups existing on the monitored system. CimTrak™ detects when groups are added, deleted, or modified. The recommended monitoring mode is “Update Baseline”. This feature supports polling detection.*

**System Users:** *Monitoring of local system users allows security professionals the capability to detect when local user accounts are added, deleted, or modified on the system. Using this feature is important even if the system is attached to a domain as additional or modified local user accounts can create a system vulnerability. The recommended monitoring mode is “Update Baseline”. This feature supports polling detection.*

**Local File System:** *Monitoring of the local file system will detect (and optionally remediate) any addition, deletion, or modification to files and folders on the monitored system. This feature supports polling or real-time detection.*

**Network File System:** *Monitoring of mounted shares allows for the detection (and optional remediation) of any addition, deletion, or modification to files and folders on monitored network shares. This feature supports polling detection.*

### **Watch Properties**

The Watch Properties section shows any currently monitored files, folders, and configurations. Additionally, excluded or included paths and files are displayed. The Watch Properties are explained in detail in subsequent sections.

#### **6.1.1.5.2. WATCH PROPERTIES**

Selecting any object listed in the Object Group Properties File System Tree results in the Watch Properties dialog to display.

Watch Properties

When a change occurs

☐ Restore from Repository

☐ Log

☒ Update Baseline

☐ Prompt for Approval

Some software, such as backup utilities or virus detection software, modify various file attributes, which will signal an intrusion to CimTrak.

☒ Ignore Archive Flag

☐ Ignore Read-only Flag

☐ Ignore SACL

☐ Ignore DACL

☐ Ignore Owner Security

☐ Ignore Group Security

☐ Ignore Alternate Stream Data

☐ Ignore File Dates

Authoritative Copy

☒ Store authoritative copy of all files in the CimTrak Repository. This will allow CimTrak to restore files back to their original state.

☐ Don't Store authoritative copy

Event Detection Method

☐ Real-time Detection

☒ Poll Detection (interval)

☐ Poll at Specific Time (Local Time)

☐ Poll at Specific Time (Agent Time)

Poll Interval (Hours and Minutes)

02 : 00

Store Changes

☒ Store a copy of added/changed files

Other

☐ Log Reads

File Comparison Method

MD5

Connection Loss Strategy

☐ Wait for User Approval on Sync

Auto Exclude

Auto exclude files that have changed 0 times in 60 minutes (0 changes = disabled)

OK Cancel

**Figure 116: Watch Properties dialog**

The Watch Properties dialog allows for the configuration of detection and reaction parameters. The Watch Properties dialog is comprised of several different sections:

### **Corrective Action Authoritative Copy**

**File Comparison Method**  
**Store Changes**  
**Options**  
**Event Detection Method**  
**Connection Loss**  
**Auto Exclude**

These sections are explained in detail in subsequent sections. After completing the Watch Properties configuration click OK to accept the changes or Cancel to abort and discard the changes. The Watch Properties dialog will close and the Object Group Properties dialog will display showing the configured Watch Properties in the Watch Properties section.

Path	Object Type	Type	Store Files	Corrective Ac...	Detection	C
▲ /DeviceRoot (1 )						
/DeviceRoot	Directory	Watch	Yes	Update Basel...	Poll	M

**Figure 117: Watch Properties section showing monitored directory**

#### 6.1.1.5.2.1. CORRECTIVE ACTION

Defining the corrective action associated with a Network Device Agent Object Group Policy is accomplished through the Watch Properties dialog. CimTrak™ supports four primary modes of remediation when changes to modified files/configurations are detected. Additionally, CimTrak™ has the capability to perform customized remediation actions.

Primary modes of remediation include:

**Restore from Repository:** *Stored authoritative (original) data files are used to restore files and folders that have been changed.*

**Log:** *All detected change events are only logged. No authoritative (original) file data is stored.*

**Update Baseline:** *Changes are allowed to occur. Each change results in an incremental backup being performed on the watch data. When applicable, previous baselines can be pushed back to the monitored system.*

**Prompt for Approval:** *Changes are allowed to occur. The CimTrak™ Administrator is given the option to allow or undo the detected changes.*

**Deny Access:** *Changes are not allowed to occur.*

Optionally, the Custom configuration mode exists allowing for any combination of the primary modes of remediation. For example, when a file is added the administrator may choose to update the baseline; when a file is deleted the administrator may choose to restore the file; when a file is modified the administrator may choose to log the change.

When a change occurs

- ☐ Restore from Repository
- ☒ Log
- ☐ Update Baseline
- ☐ Prompt for Approval
- ☐ Deny Access

**Figure 118: Corrective Action Properties**

Selection of the remediation mode is accomplished by selecting the corresponding radio button.

#### **6.1.1.5.2.2. AUTHORITATIVE COPY**

Depending on the Corrective Action used, CimTrak™ has the capability to alter the storage of Authoritative Copy data. The Authoritative Copy refers to a saved copy of “locked” file system/configuration data stored in the Master Repository for the purpose of restoring files to the last known approved state. Additionally, Authoritative Copy data can be used to compare the contents of monitored files and configurations. Authoritative Copy data is stored in the Master Repository using the user configured cryptology and compressed.

#### Authoritative Copy

- ☐ Store authoritative copy of all files in the CimTrak Repository. This will allow CimTrak to restore files back to their original state.
- ☒ Don't Store authoritative copy

Figure 119: Authoritative Copy Parameter Settings

***The compression ratio used by CimTrak™ varies with the type of content being monitored (i.e., images, documents, text files). Generally, the authoritative copy data is stored with a 20-25% compression ratio.***

#### 6.1.1.5.2.3. FILE COMPARISON METHOD

Each file, folder, and configuration monitored by CimTrak™ has a calculated hash value stored in the CimTrak™ Master Repository. The File Comparison Method parameter setting allows for authorized CimTrak™ Administrators to modify the comparison algorithm used. By default the most powerful method is selected. The methods allowed vary based on the CimTrak™ Cryptology release.

#### File Comparison Method

MD5 ▼

Figure 120: File Comparison Method Parameter Settings

To change the File Comparison Method, select the method to use from the File Comparison Method dropdown.

#### 6.1.1.5.2.4. STORE CHANGES

Depending on the Corrective Action used, CimTrak™ has the capability to alter the storage of change data. Change data refers to a saved copy of modified file system/configuration data stored in the Master Repository for the purpose of compare the contents with the Authoritative Copy. Change data is stored in the Master Repository using the user configured cryptology and compressed.

#### Store Changes

- ☐ Store a copy of added/changed files

Figure 121: Store Changes Option Checkbox

***The compression ratio used by CimTrak™ varies with the type of change stored (i.e., images, documents, text files).***

***Generally, the change data is stored with a 20-25% compression ratio.***

Selecting the checkbox labelled “Store Changes” will store the change data to the Master Repository using the user configured cryptology and compressed.

#### **6.1.1.5.2.5. AUTO EXCLUDE**

When creating an Object Group Watch Policy it is important to tune the configuration to exclude files that are dynamic and need to change. CimTrak™ has the capability to auto-tune the Watch Policy by automatically excluding file that change more times than the designated threshold and interval. The Auto Exclude threshold and interval is configured in the Network Device Agent Watch Properties dialog.

***The Auto Exclude feature should only be enabled during the initial Object Group Policy tuning process. Leaving this feature enabled indefinitely could result in CimTrak™ missing legitimate system changes.***

By default the Auto Exclude feature is disabled. To enable the Auto Exclude feature, specify the threshold by indicated the amount of times a file or configuration is allowed to change over a specified time in minutes.

##### **Auto Exclude**

Auto exclude files that have changed 0 times in 60 minutes (0 changes = disabled)

**Figure 122: Auto Exclude parameter settings**

Acceptable change values must be between 0 (disabled) and 1,000. The time value must be between 1 minute and 1,440 minutes.

#### **6.1.1.5.2.6. OPTIONS**

The CimTrak™ Network Device Agent Watch Properties has additional customization options available to reduce the number of detected false changes. These additional options are useful to allow CimTrak™ to function properly with backup utilities and source control utilities. Additionally options exist to enable additional monitoring capabilities. The Option settings are available in the Network Device Agent Watch Properties dialog.

Some software, such as backup utilities or virus detection software, modify various file attributes, which will signal an intrusion to CimTrak.

- |                                                         |                                                |
|---------------------------------------------------------|------------------------------------------------|
| <input checked="" type="checkbox"/> Ignore Archive Flag | <input type="checkbox"/> Ignore Read-only Flag |
| <input type="checkbox"/> Ignore SACL                    | <input type="checkbox"/> Ignore DACL           |
| <input type="checkbox"/> Ignore Owner Security          | <input type="checkbox"/> Ignore Group Security |
| <input type="checkbox"/> Ignore Alternate Stream Data   | <input type="checkbox"/> Ignore File Dates     |

**Figure 123: Options parameter settings**

Other

- ☐ Log Reads

**Figure 124: Log Reads Parameter Checkbox**

Option parameter settings are enabled by clicking the corresponding checkbox. Options are disabled when unchecked. The Options parameter settings allow for the custom configuration of the following:

- Ignore Archive Flag: When checked the CimTrak™ Network Device Agent will ignore any changes that occur to the archive flag.
- Ignore Read-only Flag: When checked the CimTrak™ Network Device Agent will ignore any changes that occur to the Read-only flag.
- Log Reads: When checked CimTrak™ has the capability to monitor specific files and folders for any form of access. Using this feature will generate audit events whenever a file is viewed or copied.

***Logging of reads requires the Network Device Agent Forensic Driver. This driver is installed during the installation of the Windows Network Device Agent.***

#### **6.1.1.5.2.7. EVENT DETECTION METHOD**

The CimTrak™ Network Device Agent has the capability to monitor Object Group Policies in real-time (when supported) or on a polling interval. Configuration of the Event detection method is available in the Network Device Agent Watch Properties dialog.



#### Event Detection Method

☐ Real-time Detection

☒ Poll Detection (interval)

☐ Poll at Specific Time (Local Time)

☐ Poll at Specific Time (Agent Time)

#### Poll Interval (Hours and Minutes)

02 : 00

Figure 125: Event Detection Method parameter settings

Available event detection methods include:

- **Real-time Detection:** *Real-time Detection will report detected changes immediately when they are performed. The configured remediation mode will automatically initiate immediately upon the detection of a change.*
- **Poll-based Detection:** *Poll-based Detection will report any changes that have occurred since the last poll-based scan. Acceptable values range between 0 (poll only when force-synced) and 1,440 minutes.*

***The Windows Network Device Agent Forensic Driver will not show forensic assisting information for changes detected using the Poll-based Detection.***

***Scheduled polling is accomplished by setting the Poll-based Detection interval to 0 and scripting the synchronization using the CimTrak™ Command Line Interface. These scripts can then be scheduled using Windows Task Scheduler or Linux/UNIX Cron jobs. The Command Line Interface is explained in section Error! Reference source not found..***

#### 6.1.1.5.2.8. CONNECTION LOSS

Occasionally the CimTrak™ Master Repository may lose connectivity with attached Network Device Agents due to network errors or mobile devices. When this occurs the option exists to automatically perform Object Group synchronization when the connection is re-established. Setting the Connection Loss settings are available through the Object Group Properties Watch Properties dialog.

#### Connection Loss Strategy

☐ Wait for User Approval on Sync

Figure 126: Connection Loss parameter settings

To enable synchronization after a connection loss, select the User Approval on Sync checkbox. To disable synchronization, de-select the User Approval on Sync checkbox.

When User Approval on Sync is enabled, the CimTrak™ Administrator is prompted for the desired action to take on detected changes made during the non-connectivity period. The CimTrak™ Administrator utilizes the Changes Pending Approval Web Management Console dialog to authorize or deny these changes. The Changes Pending Approval dialog is explained in a subsequent section.

The User Approval on Sync dialog has the following default and customizable settings for each of the following corrective actions:

- **Restore from Repository:** *Option can be enabled or disabled. By default this option is disabled.*
- **Log:** *Option is disabled by default and cannot be changed.*
- **Update Baseline:** *Option is disabled by default and cannot be changed.*
- **Prompt for Approval:** *Option is enabled by default and cannot be changed.*

#### 6.1.1.5.3. TUNING WATCH PROPERTIES

When an operating system folder or configuration is selected in the Object Group Properties dialog, all children files, folders, and configurations are also selected. Often certain files need to be excluded or included in the particular watch policy. CimTrak™ has the capability to create exclude or include rules for files, folders, and configurations. Creating these advanced rules is accomplished in the selected Object Group's Watch Properties. Accessing the Object Group Properties is accomplished during the creation or editing of an Object Group's Watch Policy. See section 6.1.5.3.2 for more information on creating Watch Policies.

Monitored folders, files, and configurations will display in the Object Group Properties Watch Properties section. Each displayed item will include the following information:

- **Path:** *The operating system location of the parent folder or configuration.*
- **Object Type:** *The Object Type being monitored (i.e. Directory).*
- **Type:** *Action performed by the Watch Property detail (i.e. Watch, Exclude, etc.).*
- **Store Files:** *Indication of whether or not Authoritative Copy data will be stored in the CimTrak™ Master Repository.*
- **Corrective Action:** *The Corrective Action chosen during the creation of the Object Group Watch Policy.*
- **Detection:** *Indication of the mode of detection (Real-time, Polling).*

- **Ignore Archive Flag:** *Indication of whether or not changes to the Archive Flag will be ignored.*
- **Ignore Read-only Flag:** *Indication of whether or not changes to the Read-only Flag will be ignored.*
- **Comparison Method:** *Displays the comparison method selected in the Object Group's Watch Properties.*
- **Quarantine:** *Indication of whether or not Change Data will be stored in the CimTrak™ Master Repository.*

Path	Object Type	Type	Store Files	Corrective Ac...	Detection	C
▲ /DeviceRoot (2 )						
/DeviceRoot	Directory	Watch	Yes	Update Basel...	Poll	M
[/Cc][li][Ss][Cc][Oo] [li][Oo][Ss]/	Regular Expr...	Exclude				

**Figure 127: Watch Properties section showing monitored data**

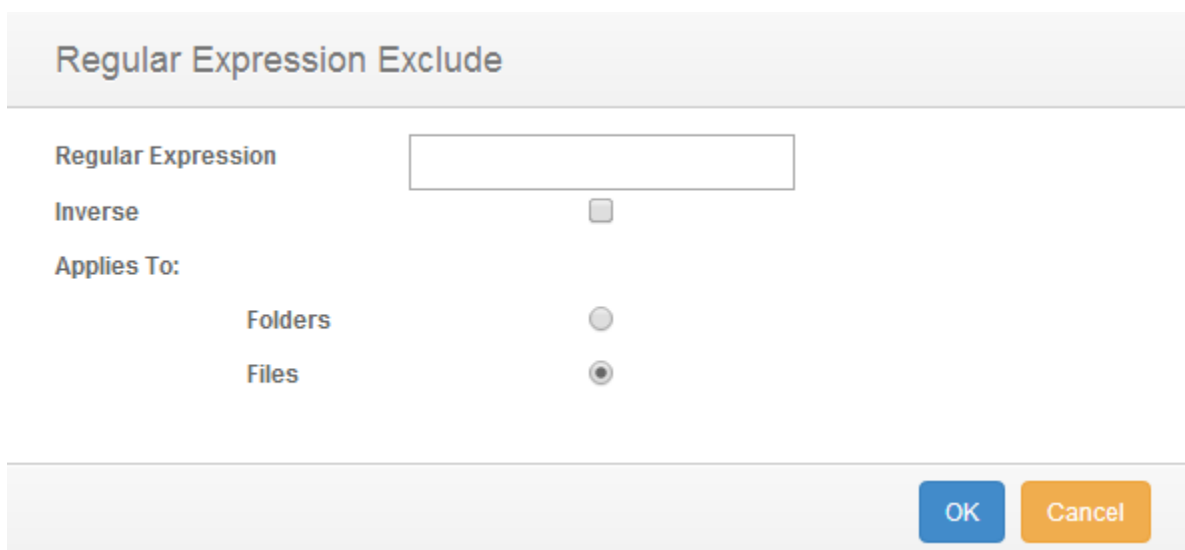
Each column of information can be sorted by column criteria by clicking once on the column title.

Right clicking on any item showing in the Watch Properties section results in a context menu to display showing additional configuration and navigation options. Context menu options include:

- **Edit Watch Properties:** *Modify the watch properties associated with the selected Watch data. Opens the Watch Properties dialog.*
- **Remove Watch:** *Disable the selected Watch data by unselecting it in the Object Group Properties dialog File System Tree.*
- **Add Regular Expression Exclude:** *Create customized excludes to prevent or enable of specific folder, file, or configuration criteria.*

#### 6.1.1.5.3.1 EXCLUDING AND INCLUDING USING REGULAR EXPRESSIONS

Occasionally a CimTrak™ Object Group Policy may need to exclude monitor or only monitor data based on file extensions, file names, folder names, configuration names, or various other types of information. Setting these custom watch rules is performed by creating Regular Express Exclude. The process of creating a Regular Expression Exclude is performed through the Add Regular Expression Exclude dialog accessed by right-clicking Watch data and then selecting Add Regular Expression Exclude from the context menu. Accessing the Object Group Properties is accomplished during the creation or editing of an Object Group's Watch Policy. See section 6.1.5.3.2 for more information on creating Watch Policies.



Regular Expression Exclude

Regular Expression

Inverse ☐

Applies To:

Folders ☐

Files ☒

OK Cancel

**Figure 128: Add Regular Expression Exclude dialog**

The Add Regular Expression Exclude dialog has the capability to exclude files and folders. Additionally, the Add Regular Expression Exclude dialog can create inverse regular expressions excludes to only monitor certain files or folders based on the criteria entered.

##### 6.1.1.5.3.1.1. EXCLUDING FOLDERS USING REGULAR EXPRESSIONS

The process of creating a Regular Expression Exclude is performed through the Add Regular Expression Exclude dialog accessed by right-clicking Watch data and then selecting Add Regular Expression Exclude from the context menu. Accessing the Object Group Properties is accomplished during the creation or editing of an Object Group's Watch Policy. See section 6.1.5.3.2 for more information on creating Watch Policies.

To create a Regular Expression folder exclude, enter the folder information to exclude (i.e. \temp). Ensure that the Folders radio button is selected and then click OK. Click Cancel to abort the changes and return to the Object Group Properties dialog. Clicking OK will automatically return to the Object Group Properties dialog. Note that the regular expression exclude is displayed in the Watch Properties data section.

Regular Expression Folder Excludes can become very complex. It is possible to create custom exclusions using regular expressions. For instance, a regular expression exclude can be created to ignore case:

**/Cisco IOS**

*can be entered as...*

**//[Cc][Ii][Ss][Cc][Oo] [Ii][Oo][Ss]//**

/DeviceRoot	Directory	Watch	Yes	Update Basel...	Poll
//[Cc][Ii][Ss][Cc][Oo] [Ii][Oo][Ss]//	Regular Expr...	Exclude			

**Figure 129: Regular Expression Folder Exclude**

To add additional Regular Express folder excludes, repeat the same steps. To remove Regular Expression Excludes, right-click on the Exclude information in the Watch Properties data section and then select Remove Exclude(s). When completed, click the OK button to save the changes. Click the Cancel button to abort the configuration and discard any changes.

#### **6.1.1.5.3.1.2. EXCLUDING FILES USING REGULAR EXPRESSIONS**

The process of creating a Regular Expression Exclude is performed through the Add Regular Expression Exclude dialog accessed by right-clicking Watch data and then selecting Add Regular Expression Exclude from the context menu. Accessing the Object Group Properties is accomplished during the creation or editing of an Object Group's Watch Policy. See section 6.1.5.3.2 for more information on creating Watch Policies.

To create a Regular Expression file exclude, enter the file type information to exclude (i.e. .log). Ensure that the Files radio button is selected and then click OK. Click Cancel to abort the changes and return to the Object Group Properties dialog. Clicking OK will automatically return to the Object Group Properties dialog. Note that the regular expression exclude is displayed in the Watch Properties data section.

Regular Expression Folder Excludes can become very complex. It is possible to create custom exclusions using regular expressions. For instance, a regular expression exclude can be created to ignore case:

## running-config

can be entered as...

[Rr][Uu][Nn][Nn][Ii][Nn][Gg]-[Cc][Oo][Nn][Ff][Ii][Gg]

/DeviceRoot	Directory	Watch	Yes	Update Basel...	Poll
[Rr][Uu][Nn][Nn][Ii][Nn][Gg]-[Cc][Oo][Nn][Ff][Ii][Gg]	Regular Expr...	Exclude			

**Figure 130: Regular Expression File Exclude**

To add additional Regular Express file excludes, repeat the same steps. To remove Regular Expression Excludes, right-click on the Exclude information in the Watch Properties data section and then select Remove Exclude(s). When completed, click the OK button to save the changes. Click the Cancel button to abort the configuration and discard any changes.

### 6.1.1.5.3.1.3. INVERSE EXCLUDING OF FOLDERS USING REGULAR EXPRESSIONS

The process of creating an Inverse Regular Expression Exclude is performed through the Add Regular Expression Exclude dialog accessed by right-clicking Watch data and then selecting Add Regular Expression Exclude from the context menu. Accessing the Object Group Properties is accomplished during the creation or editing of an Object Group's Watch Policy. See section 6.1.5.3.2 for more information on creating Watch Policies.

Inverse regular expressions can be used to "include" information to monitor. To create an Inverse Regular Expression folder exclude, enter the folder information to watch (i.e. \temp). Ensure that the Folders radio button and the Inverse checkbox are selected and then click OK. Click Cancel to abort the changes and return to the Object Group Properties dialog. Clicking OK will automatically return to the Object Group Properties dialog. Note that the Inverse regular expression exclude is displayed in the Watch Properties data section.

Inverse Regular Expression Folder Excludes can become very complex. It is possible to create custom inverse exclusions using inverse regular expressions. For instance, an inverse regular expression exclude can be created to ignore case:

## /Cisco IOS

can be entered as...

//[Cc][Ii][Ss][Cc][Oo] [Ii][Oo][Ss]//

/DeviceRoot	Directory	Watch	Yes	Update Basel...	Poll
//[Cc][Ii][Ss][Cc][Oo] [Ii][Oo][Ss]//	Inverse Regul...	Exclude			

**Figure 131: Regular Expression Folder Exclude (blue text)**

To add additional Inverse Regular Express folder excludes, repeat the same steps. To remove Inverse Regular Expression Excludes, right-click on the Exclude information in the Watch Properties data section and then select Remove Exclude(s). When completed, click the OK button to save the changes. Click the Cancel button to abort the configuration and discard any changes.

**6.1.1.5.3.1.4. INVERSE EXCLUDING OF FILES USING REGULAR EXPRESSIONS**

The process of creating an Inverse Regular Expression to include specified files or extensions is performed through the Add Regular Expression Exclude dialog accessed by right-clicking Watch data and then selecting Add Regular Expression Exclude from the context menu. Accessing the Object Group Properties is accomplished during the creation or editing of an Object Group's Watch Policy. See section 6.1.5.3.2 for more information on creating Watch Policies.

To create an Inverse Regular Expression file exclude, enter the file type information to exclude (i.e. .log). Ensure that the Files radio button and Inverse checkbox are selected and then click OK. Click Cancel to abort the changes and return to the Object Group Properties dialog. Clicking OK will automatically return to the Object Group Properties dialog. Note that the inverse regular expression exclude is displayed in the Watch Properties data section.

Inverse Regular Expression Folder Excludes can become very complex. It is possible to create custom exclusions using regular expressions. For instance, an inverse regular expression exclude can be created to ignore case:

**running-config**  
*can be entered as...*  
[Rr][Uu][Nn][Nn][Ii][Nn][Gg]-[Cc][Oo][Nn][Ff][Ii][Gg]

/DeviceRoot	Directory	Watch	Yes	Update Basel...	Poll
[Rr][Uu][Nn][Nn][Ii][Nn][Gg]-[Cc][Oo][Nn][Ff][Ii][Gg]	Inverse Regul...	Exclude			

**Figure 132: Regular Expression File Exclude**

To add additional Inverse Regular Express file excludes, repeat the same steps. To remove Inverse Regular Expression Excludes, right-click on the Exclude information in the Watch Properties data section and then select Remove Exclude(s). When completed, click the OK button to save the changes. Click the Cancel button to abort the configuration and discard any changes.



#### 6.1.1.6. SAVING OBJECT GROUP WATCH POLICIES TO TEMPLATES

Once an Object Group Watch Policy has been created it is possible to save the policy configurations to a template. Using a template can assist in creating identical watch data for other CimTrak™ Network Device Agents. See section 4.7 for more information on CimTrak™ Templates.

To create a template, right-click on the Object Group name in the CimTrak™ Web Management Console's Object Group Tree and then select Save to Template. The Save to Template dialog will display. Enter a unique name for the template. If you would like this template to be private to your CimTrak™ account be sure to select the Private option by selecting the Private checkbox. When completed entering the required information click the OK button. Click the cancel button to abort the template creation. A template name can be between 1 and 512 characters.

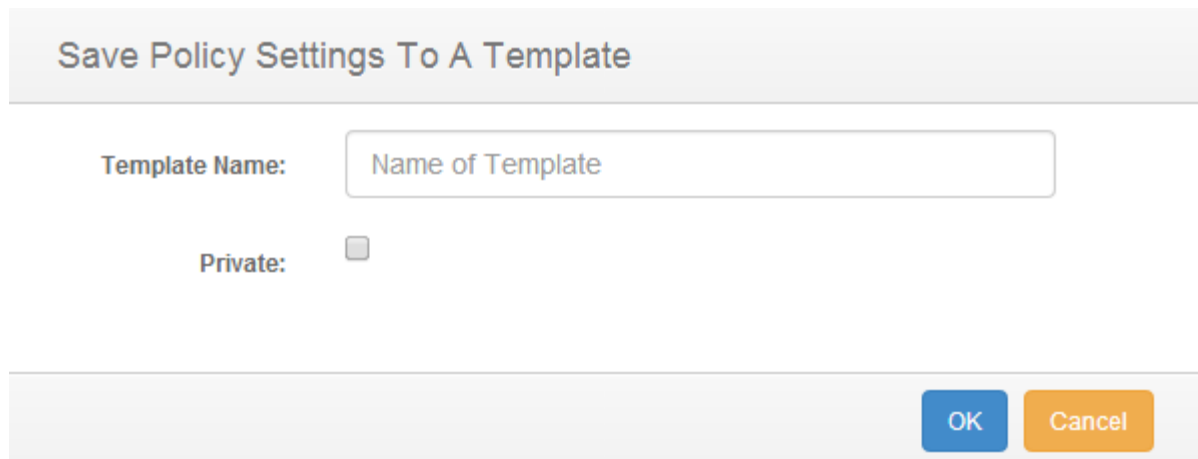
The image shows a dialog box titled "Save Policy Settings To A Template". It has a light gray header bar with the title in blue text. Below the header, there is a label "Template Name:" followed by a text input field containing the placeholder text "Name of Template". Below this, there is a label "Private:" followed by an unchecked checkbox. At the bottom right of the dialog, there are two buttons: a blue "OK" button and an orange "Cancel" button.

Figure 133: Save to Template dialog

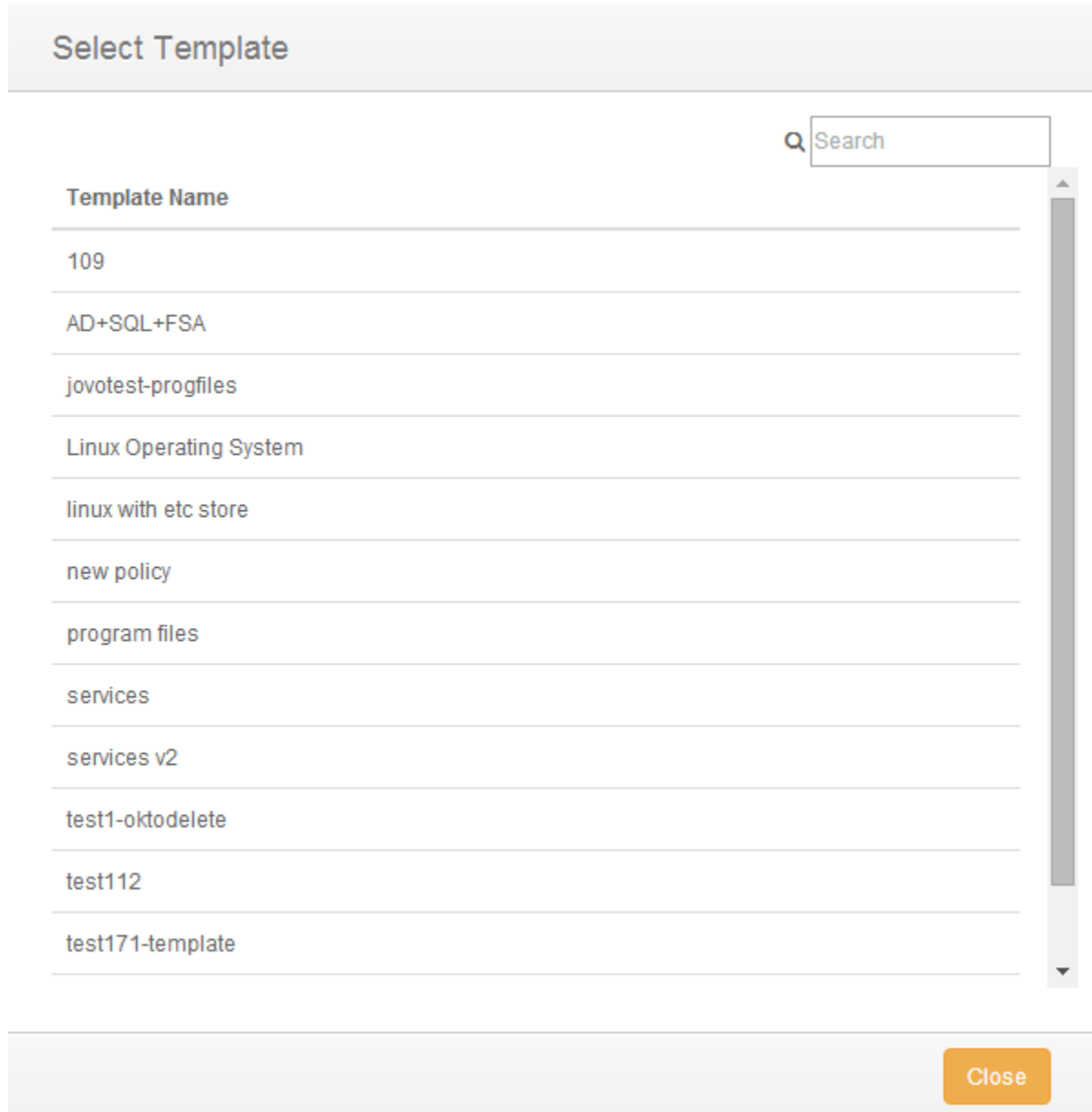
In addition to being able to create Templates for single Object Groups CimTrak™ has the capability to create Templates for multiple Object Groups at the Network Device Agent level. To create a Network Device Agent template, right-click on the Network Device Agent name in the CimTrak™ Web Management Console's Object Group Tree and then select Save to Template. The Save to Template dialog will display. Enter a unique name for the template. If you would like this template to be private to your CimTrak™ account be sure to select the "Private" option by selecting the "Private" checkbox. When completed entering the required information click the OK button. Click the cancel button to abort the template creation. A template name can be between 1 and 512 characters.

#### 6.1.1.7. CREATING OBJECT GROUP WATCH POLICIES USING TEMPLATES

Once an Object Group Watch Policy has been created it is possible to save the policy configurations to a template. Using a template can assist in creating identical watch data for other CimTrak™ Network Device Agents. See section 4.7 for more information on CimTrak™ Templates.



To create an Object Group from template (or multiple Object Groups from a single template) right-click on the Network Device Agent name in the CimTrak™ Web Management Console's Object Group Tree and then select New Object Group(s) from Template. The Select Template dialog will display.

The image shows a 'Select Template' dialog box. At the top, there is a search bar with a magnifying glass icon and the word 'Search'. Below the search bar is a list of templates. The list has a header 'Template Name' and contains the following items: '109', 'AD+SQL+FSA', 'jovotest-progfiles', 'Linux Operating System', 'linux with etc store', 'new policy', 'program files', 'services', 'services v2', 'test1-oktodelete', 'test112', and 'test171-template'. A vertical scrollbar is on the right side of the list. At the bottom right of the dialog box is an orange button labeled 'Close'.

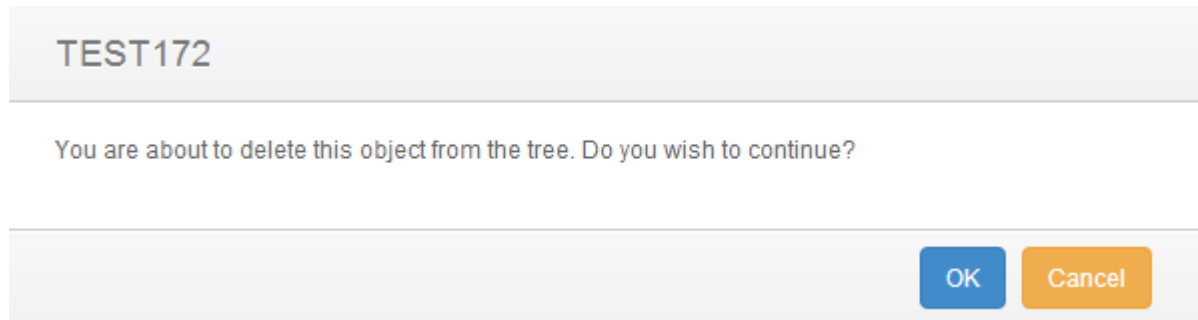
**Figure 134: Select Template dialog**

Select the template the Object Group will be based off of and then click OK. Click Cancel to abort the Object Group creation. If OK is selected the Select Template dialog will close and the newly created Object Group(s) will display in the CimTrak™ Web Management Consoles Object Group Tree.

#### **6.1.1.8. DELETING OBJECT GROUP WATCH POLICIES**

Once an Object Group Watch Policy has been created it is possible to delete the Object Group. Once an Object Group is deleted it cannot be undone.

To delete an Object Group Watch Policy right-click on its name in the CimTrak™ Web Management Console's Object Group Tree and then select Delete. The Confirm Delete dialog will display.



**Figure 135: Confirm Delete dialog**

Select Yes to delete the Object Group, select No to abort the deletion. Select the Do not show this again checkbox to suppress this message from future deletions. Clicking Yes results in the Object Group being deleted.

***The Object Group must be unlocked (monitoring disabled) before the Object Group can be deleted. Unlocking an Object Group is explained in a subsequent section.***

#### **6.1.1.9. ENABLING AND DISABLING OBJECT GROUP MONITORING**

Before a CimTrak™ Network Device Agent can monitor an Object Group Watch Policy the Object Group must be “Locked”. To disable monitoring the Object Group Watch Policy must be “Unlocked”. The monitoring status of an Object Group can be determined by the associated icon in the CimTrak™ Web Management Console's Object Group Tree. See section 6.1.1.5 for more information on creating Object Group Watch Policies. Possible associated statuses are as follows:



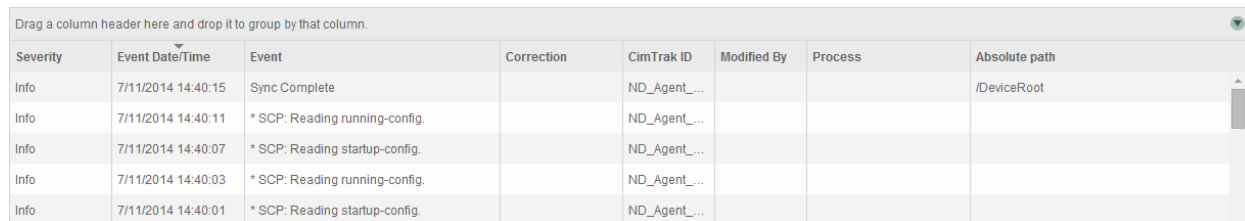
**Unlocked:** *The Object Group Watch Policy is not currently being enforced.*



**Locked:** *The Object Group Watch Policy is currently enforcing the configured Corrective Action.*

Locking an Object Group is accomplished by selecting the Object Group to lock in the CimTrak™ Web Management Console's Object Group Tree, right-clicking and then selecting Lock and Digitally Sign.

When an Object Group is locked (or locking) it will show the locking and synchronization process in the Master Repository, Area, Agent, and Object Group Event Logs. The process of locking and synchronization creates Information level events.



Severity	Event Date/Time	Event	Correction	CimTrak ID	Modified By	Process	Absolute path
Info	7/11/2014 14:40:15	Sync Complete		ND_Agent_...			/DeviceRoot
Info	7/11/2014 14:40:11	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:40:07	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 14:40:03	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:40:01	* SCP: Reading startup-config.		ND_Agent_...			

**Figure 136: Object Group Lock Process (Event Log)**

***Multiple Object Groups can be locked simultaneously by selecting the Network Device Agent in the Web Management Console's Object Group Tree and then either right-clicking and selecting Lock and Digitally Sign in the context menu.***

Locking the Object Group will instruct the Network Device Agent to create digital signatures for each file included in the watch policy. If a Restore from Repository or Update Baseline Corrective Action is assigned, the Network Device Agent will create Authoritative Copies of the monitored files. All digital signatures and Authoritative Copy data is compressed, encrypted, and then transmitted to the CimTrak™ Master Repository.

While an Object Group is in the process of locking the lock process can be aborted by right-clicking on the Object Group in the CimTrak™ Web Management Console's Object Group Tree and selecting Cancel Lock in the context menu.

When the locking of an Object Group is "Stopped" it will show the stop locking process in the Master Repository, Area, Agent, and Object Group Event Logs. The process of Stopping creates error level events.

***The Locking of Multiple Object Groups can be stopped simultaneously by selecting the Network Device Agent in the Web Management Console's Object Group Tree and then right-clicking and selecting Cancel Lock in the context menu.***

Before configuration settings associated with an Object Group Watch Policy can be modified, an Object Group is deleted, or simply to temporarily disable Object Group monitoring the Object Group must be "Unlocked". Unlocking an Object Group is accomplished by selecting the Object Group to unlock in the CimTrak™

Web Management Console's Object Group Tree, right-clicking and then selecting Unlock and Allow Changes.

When an Object Group is Unlocked it will show the unlock process in the Master Repository, Area, Agent, and Object Group Event Logs. The process of unlocking creates error level events.

Drag a column header here and drop it to group by that column.

Severity	Event Date/Time	Event	Correction	CimTrak ID	Modified By	Process	Absolute path
Info	7/11/2014 14:40:15	Sync Complete		ND_Agent_...			/DeviceRoot
Info	7/11/2014 14:40:11	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:40:07	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 14:40:03	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:40:01	* SCP: Reading startup-config.		ND_Agent_...			

**Figure 137: Object Group Unlock Process (Event Log)**

***Multiple Object Groups can be unlocked simultaneously by selecting the Network Device Agent in the Web Management Console's Object Group Tree and then right-clicking and selecting Unlock and Allow Changes in the context menu.***

#### 6.1.1.10. SYNCHRONIZING OBJECT GROUP DATA

Data being monitored by a CimTrak™ Network Device Agent is monitored either in real-time or at a polling interval. To force the polling interval to expire immediately, CimTrak™ has the capability to synchronize monitored data on demand by means of Force Sync.

Synchronizing an Object Group Watch Policy is performed by right-clicking on the Object Group in the CimTrak™ Web Management Console's Object Group Tree and selecting Force Sync in the context menu.

***Multiple Object Groups can be synchronized simultaneously by selecting the Network Device Agent in the Web Management Console's Object Group Tree and then right-clicking and selecting Force Sync in the context menu.***

When an Object Group is synchronized it will show the synchronization process in the Master Repository, Area, Agent, and Object Group Event Logs. The process of synchronizing creates information level events.

Drag a column header here and drop it to group by that column.

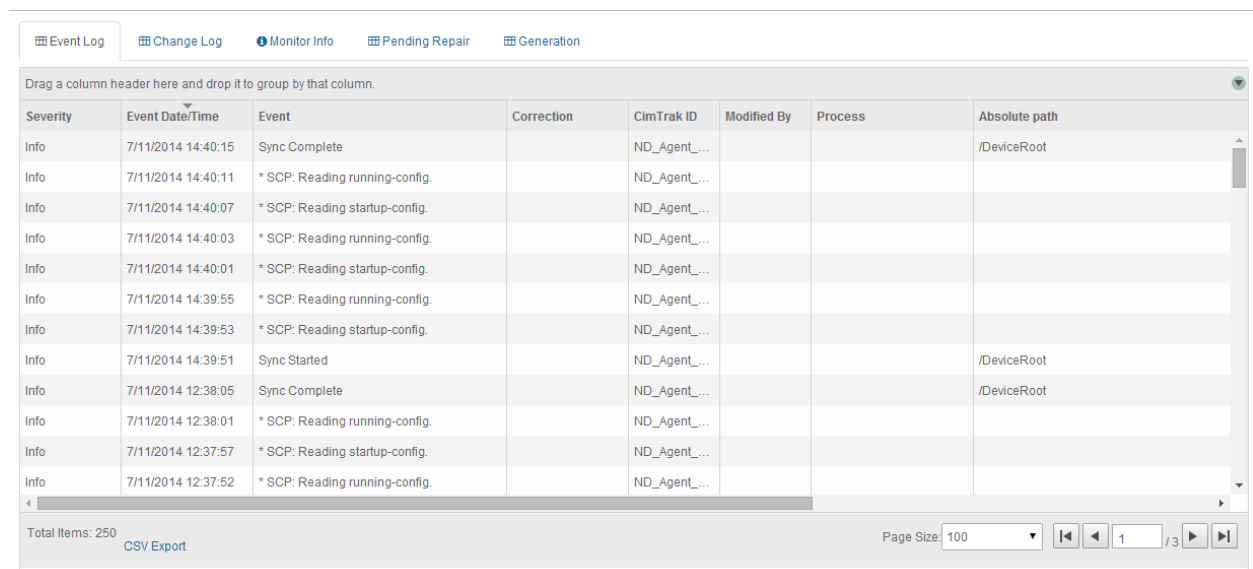
Severity	Event Date/Time	Event	Correction	CimTrak ID	Modified By	Process	Absolute path
Info	7/11/2014 14:40:15	Sync Complete		ND_Agent_...			/DeviceRoot
Info	7/11/2014 14:40:11	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:40:07	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 14:40:03	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:40:01	* SCP: Reading startup-config.		ND_Agent_...			

**Figure 138: Object Group Synchronization Process (Event Log)**

### 6.1.2. NETWORK DEVICE AGENT INFORMATION DISPLAY

The CimTrak™ Web Management Console's Information Display Area displays information for the selected CimTrak™ Network Device Agent. The information displayed provides Event Log data.

- **Agent Settings:** *Settings and system information associated with the selected Network Device Agent.*
- **Event Log:** *Event audit log associated with the Network Device Agent and children Object Groups of the selected Network Device Agent.*
- **Stats:** *System statistics associated with the system hosting the Network Device Agent.*
- **Notes:** *Administrative notes associated with the Network Device Agent.*
- **Overview:** *Object Group status information for all Object Groups associated with the Network Device Agent.*



Severity	Event Date/Time	Event	Correction	CimTrak ID	Modified By	Process	Absolute path
Info	7/11/2014 14:40:15	Sync Complete		ND_Agent_...			/DeviceRoot
Info	7/11/2014 14:40:11	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:40:07	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 14:40:03	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:40:01	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 14:39:55	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:39:53	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 14:39:51	Sync Started		ND_Agent_...			/DeviceRoot
Info	7/11/2014 12:38:05	Sync Complete		ND_Agent_...			/DeviceRoot
Info	7/11/2014 12:38:01	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 12:37:57	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 12:37:52	* SCP: Reading running-config.		ND_Agent_...			

**Figure 139: Network Device Agent Information Display Area (Agent Settings Tab Selected)**

The information associated with the Network Device Agent Information Display Area tabs is explained in subsequent sections.

#### 1.1.2.1. AUDITING NETWORK DEVICE AGENT EVENTS

The Network Device Agent Event Log provides audit information relating to events occurring in the Network Device Agent and Object Groups connected to the Network Device Agent. Accessing the Network Device Agent Event Log is accomplished by first clicking once on the Network Device Agent name in the Object Group Tree to select it followed by clicking the Event Log tab in the Web Management Console Information Display Area.

The Network Device Agent Event Log displays details of all events that have occurred on the Network Device Agent and Object Groups connected to the Network Device Agent. The level of detail displayed is dependent on the auditing level configured in the Master Repository Properties Log Administrative DB Changes. See section 0 for additional information.

For each recorded event, the Network Device Agent Event Log will display information corresponding to the following:

**Event Date/Time:** *The exact date and time of the detected event.*

**Event:** *Brief description of the detected event.*

**Absolute Path:** *File path affected by the detected event.*

**Completion Date/Time:** *Date and time the correction response completed.*

**Event Code:** *Internal CimTrak™ Event Code corresponding to the detected event.*

**Path:** *Object Tree Path to the affected CimTrak™ object.*

Event Log

Drag a column header here and drop it to group by that column.

Severity	Event Date/Time	Event	Correction	CimTrak ID	Modified By	Process	Absolute path
Info	7/11/2014 16:11:39	Sync Complete		ND_Agent_...			/DeviceRoot
Info	7/11/2014 16:11:31	Sync Started		ND_Agent_...			/DeviceRoot
Info	7/11/2014 14:42:51	Sync Complete		ND_Agent_...			/DeviceRoot
Warning	7/11/2014 14:42:47	File Modified	Baseline Updated	ND_Agent_...	Owner: Unk...		/DeviceRoot/vmware/backup.counter
Warning	7/11/2014 14:42:17	File Modified	Baseline Updated	ND_Agent_...	Owner: Unk...		/DeviceRoot/ntp.drift
Info	7/11/2014 14:41:06	Sync Started		ND_Agent_...			/DeviceRoot
Info	7/11/2014 14:40:15	Sync Complete		ND_Agent_...			/DeviceRoot
Info	7/11/2014 14:40:11	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:40:07	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 14:40:03	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:40:01	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 14:39:55	* SCP: Reading running-config.		ND_Agent_...			

Total Items: 3964 CSV Export Page Size: 100 1 / 40

**Figure 140: Network Device Agent Event Log**

Each Event Log message type has a corresponding icon that allows for quick visual reference to the urgency level of the event. These urgency levels are important to note when configuring E-Mail alert permissions. E-Mail alert permissions are explained in a subsequent section.

**Emergency:** *System is unusable. Highest level of event.*

**Alert:** *Take action immediately.*

**Critical:** *Critical conditions have occurred.*

**Error:** *Error conditions.*

**Warning:** *Warning conditions.*

**Notice:** *Normal condition that requires attention.*

**Information:** *Informational message.*

**Debug:** *Debug-level message. Lowest level of event.*

Specifics relating to message types are discussed in a subsequent sections.

#### **6.1.2.1.1. FILTERING AND SORTING THE NETWORK DEVICE AGENT EVENT LOG**

The Network Device Agent Event Log can be filtered to only show events matching the specified criteria. Accessing the Network Device Agent Event Log is accomplished by first clicking once on the Network Device Agent in the Object Group Tree to select it followed by clicking the Event Log tab in the Web Management Console Information Display Area.

To filter the information displayed in the Network Device Agent Event Log, drag and drop one of the column headers into the section labelled “Drag a column header here and drop it to group by that column.”

#### **6.1.2.2. NETWORK DEVICE AGENT PERMISSIONS**

Network Device Agents can be configured restrict access based on permission settings. Additionally, event notifications can be configured to notify CimTrak™ Users about events relating to the Network Device Agent. Accessing Network Device Agent permissions is accomplished by first clicking once on the Network Device Agent in the Object Group Tree to select it and then right-clicking and selecting “Permissions”. The Security Permissions dialog will display.

By default each Network Device Agent will have the following permissions:

##### **Administrators**

**Create Objects:** *Create Network Device Agent Object Groups.*

**Edit:** *Edit Network Device Agent settings.*

**Lock:** *Enable active monitoring of Object Group Data.*

**Reports:** *View reports relating to the Network Device Agent contents.*

**Unlock:** *Disable active monitoring of Object Group Data.*

**View:** *View contents and configurations relating to the Network Device Agent.*

## **Auditors**

**Reports:** View reports relating to Network Device Agent contents.

**View:** View contents and configurations relating to the Network Device Agent.

## **Installers**

Attach CimTrak™ Agents to a Master Repository.

### Permissions for Object

Add

Group or User Names

Group	Administrators	
Group	Auditors	
Group	Email_Testing	Remove
Group	Installers	

Permissions	Allow	Deny
Create Objects	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Edit	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lock	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Reports	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Unlock	<input checked="" type="checkbox"/>	<input type="checkbox"/>
View	<input checked="" type="checkbox"/>	<input type="checkbox"/>

☒ Apply permissions to children recursively

OKCancel

**Figure 141: Network Device Agent Security Permissions dialog**

Default access permissions associated with the Administrators, Auditors, and Installers User Groups cannot be changed. It is possible to modify E-mail alert notices for Administrator and Auditor user groups. Available E-mail alert types include:

Emergency



Alert  
Critical  
Error  
Warning  
Notice  
Information

Additional information relating to these alert types is described in a subsequent section.

#### **6.1.2.3. MODIFYING AN EXISTING USER/GROUP NETWORK DEVICE AGENT PERMISSIONS**

It is possible to modify existing user and group Network Device Agent Permissions and E-mail notification settings. Accessing Network Device Agent permissions is accomplished by first clicking once on the Network Device Agent in the Object Group Tree to select it and then right-clicking and selecting “Permissions”. The Security Permissions dialog will display.

Select the existing user or group by clicking once on the CimTrak™ User or Group name in the Group or User Names section of the Security Permissions dialog. The Permissions section of the Security Permissions dialog will update to show the permissions currently assigned to the selected user or group.

***Selecting a group will apply the selected permissions and E-mail notification settings to all members of the group. Selecting a single user will apply the selected permissions and E-mail notification settings to only that single user account.***

To add or remove permissions click the “Allow” or “Deny” checkbox corresponding to the permission being configured. Available permissions include:

**Create Objects:** *Create Network Device Agent Object Groups.*

**Edit:** *Edit Network Device Agent/Object Group control contents.*

**Lock:** *Enable active monitoring of Object Group Data*

**Reports:** *View reports relating to Network Device Agent contents.*

**Unlock:** *Disable active monitoring of Object Group Data*

**View:** *View contents and configurations relating to the Network Device Agent.*

**Email Emergency:** *Receive alerts relating to emergency level notifications.*

**Email Alert:** *Receive alerts relating to alert level notifications.*

**Email Critical:** *Receive alerts relating to critical level notifications.*

**Email Error:** *Receive alerts relating to error level notifications.*

**Email Warning:** *Receive alerts relating to warning level notifications.*

**Email Notice:** *Receive alerts relating to notice level notifications.*

**Email Information:** *Receive alerts relating to information level notifications.*

To apply the permission settings to all children objects, ensure that the Apply permissions to children recursively checkbox is selected.

When completed, click “OK” to apply the permission and alert settings. Click “Cancel” to abort the security permission configuration.

***Permissions and notification settings can be inherited from parent objects (such as the Master Repository) if the permissions are created at a parent level.***

***Permissions and notification settings are not automatically inherited for new objects. It will be necessary to manually assign the permissions and notification settings to the object.***

#### **6.1.2.4. ADDING AND REMOVING USERS AND GROUPS TO NETWORK DEVICE AGENT PERMISSIONS**

It is possible to add additional users and groups to the Security Permissions dialog so that Network Device Agent Permissions and E-mail notification settings can be assigned or changed. Accessing Network Device Agent permissions is accomplished by first clicking once on the Network Device Agent in the Object Group Tree to select it and then right-clicking and selecting “Permissions.” The Security Permissions dialog will display.

To add a new local CimTrak™ User or Group, click the Add button. The Add Users dialog will display listing all available local users and groups.

Select Users or Groups

Search

	Type	Name
<input type="checkbox"/>	User	aaaa
<input type="checkbox"/>	User	wade
<input type="checkbox"/>	User	knightrider
<input type="checkbox"/>	User	payton
<input type="checkbox"/>	User	Pippen
<input type="checkbox"/>	User	Hanks
<input type="checkbox"/>	User	Rose
<input type="checkbox"/>	User	Garnett
<input type="checkbox"/>	User	Fridge
<input type="checkbox"/>	User	alberts
<input type="checkbox"/>	User	jovo2

OKCancel

Figure 142: Add Users dialog

Select the local CimTrak™ User or Group to add by selecting the checkbox to the left of the name. Click “OK” to add the User or Group. Click “Cancel” to abort the addition process. The selected user or group will now display in the Group or User Names section of the Security Permissions dialog.

The User or Group is now available to have permissions and notification settings assigned.

6.1.3. OBJECT GROUP INFORMATION DISPLAY

The CimTrak™ Web Management Console's Information Display Area displays information for the selected CimTrak™ Network Device Agent Object Groups. The information displayed is often broken up into several tabbed viewing areas.

- **Event Log:** *Event audit log associated with the Network Device Agent and children Object Groups of the selected Network Device Agent.*
- **Change Log:** *Detected changes of watched directories.*
- **Monitor Info:** *Description and statistical standing of Watch Parameters within the Object Group.*
- **Pending Repair:** *Displays queue information associated with the remediation of folder, file and configuration data.*
- **Generation:** *Displays revision information for changes occurring to files, folders, operating system configurations contained in a File System Agent Object Group.*

Severity	Event Date/Time	Event	Correction	CimTrak ID	Modified By	Process	Absolute path
Info	7/11/2014 14:40:15	Sync Complete		ND_Agent_...			/DeviceRoot
Info	7/11/2014 14:40:11	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:40:07	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 14:40:03	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:40:01	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 14:39:55	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:39:53	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 14:39:51	Sync Started		ND_Agent_...			/DeviceRoot
Info	7/11/2014 12:38:05	Sync Complete		ND_Agent_...			/DeviceRoot
Info	7/11/2014 12:38:01	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 12:37:57	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 12:37:52	* SCP: Reading running-config.		ND_Agent_...			

Total Items: 250    CSV Export    Page Size: 100    1 / 3

**Figure 143: Object Group Information Display Area**

The information associated with the Object Group Information Display Area tabs is explained in subsequent sections.

### 6.1.3.1. AUDITING OBJECT GROUP EVENTS

The Object Group Event Log provides audit information relating to events occurring in the Object Groups connected to the Network Device Agent. Accessing the Object Group Event Log is accomplished by first clicking once on the Object Group name in the Object Group Tree to select it followed by clicking the Event Log tab in the Web Management Console Information Display Area.

The Object Group Event Log displays details of all events that have occurred on the Object Groups connected to the Network Device Agent. The level of detail displayed is dependent on the auditing level configured in the Master Repository

Properties Log Administrative DB Changes. See section 0 for additional information.

For each recorded event, the Object Group Event Log will display information corresponding to the following:

**Event Date/Time:** *The exact date and time of the detected event.*

**Event:** *Brief description of the detected event.*

**Correction:** *The Corrective Action performed on the detected event.*

**Performed By (Cimtrak™ ID):** *The Network Device Agent detecting the event and performing the remediation.*

**Modified By:** *The File System User responsible for the detected event.*

**Absolute Path:** *File path affected by the detected event.*

**Completion Date/Time:** *Date and time the correction response completed.*

**Event Code:** *Internal CimTrak™ Event Code corresponding to the detected event.*

Each Event Log message type has a corresponding icon that allows for quick visual reference to the urgency level of the event. These urgency levels are important to note when configuring E-Mail alert permissions. E-Mail alert permissions are explained in a subsequent section.

**Emergency:** *System is unusable. Highest level of event.*

**Alert:** *Take action immediately.*

**Critical:** *Critical conditions have occurred.*

**Error:** *Error conditions.*

**Warning:** *Warning conditions.*

**Notice:** *Normal condition that requires attention.*

**Information:** *Informational message.*

**Debug:** *Debug-level message. Lowest level of event.*

Specifics relating to message types are discussed in a subsequent section.

#### **6.1.3.1.1. FILTERING AND SORTING THE OBJECT GROUP EVENT LOG**

The Object Group Event Log can be filtered to only show events matching the specified criteria. Accessing the Object Group Event Log is accomplished by first clicking once on the Object Group in the Object Group Tree to select it followed by clicking the Event Log tab in the Web Management Console Information Display Area.

To filter the information displayed in the Network Device Agent Event Log, drag and drop one of the column headers into the section labelled “Drag a column header here and drop it to group by that column.”

#### **6.1.3.2. REVIEWING OBJECT GROUP MONITORED CHANGES**

The Object Group Change Log provides detailed change event audit information relating to change events occurring in the Object Groups connected to the Network Device Agent. Accessing the Object Group Change Log is accomplished by first clicking once on the Object Group name in the Object Group Tree to select it followed by clicking the Change Log tab in the Web Management Console Information Display Area.

The Object Group Change Log displays details of all addition, deletion, and change events that have occurred on the Object Groups connected to the Network Device Agent.

For each recorded event, the Object Group Change Log will display information corresponding to the following:

**Event Date/Time:** *The exact date and time of the detected event.*

**Storage Status:** *Information indicating if the change is stored in the Master Repository.*

**Absolute Path:** *File path affected by the detected event.*

**Modified By:** *The File System User responsible for the detected event (Windows Network Device Agent with Driver only).*

**Process:** *The process used to initiate the detected event (Windows Network Device Agent with Driver only).*

**Process ID:** *Windows Process ID associated with the initiating process (Windows Network Device Agent with Driver only).*

**Thread ID:** *Process Thread ID associated with the initiating process (Windows Network Device Agent with Driver only).*

Event Log Change Log Monitor Info Pending Repair Generation

Drag a column header here and drop it to group by that column.

Severity	Event Date/Time	Storage Status	Absolute path	Modified By	Process	Process ID	Thread ID
Warning	7/11/2014 14:42:47	Stored	/DeviceRoot/vmware/backup.counter	Owner: Unknown		0	
Warning	7/11/2014 14:42:17	Stored	/DeviceRoot/ntp.drift	Owner: Unknown		0	
Warning	7/11/2014 12:39:18	Stored	/DeviceRoot/vmware/backup.counter	Owner: Unknown		0	
Warning	7/11/2014 12:38:48	Stored	/DeviceRoot/ntp.drift	Owner: Unknown		0	
Warning	7/11/2014 10:35:45	Stored	/DeviceRoot/vmware/backup.counter	Owner: Unknown		0	
Warning	7/11/2014 10:35:15	Stored	/DeviceRoot/ntp.drift	Owner: Unknown		0	
Warning	7/11/2014 08:32:15	Stored	/DeviceRoot/vmware/backup.counter	Owner: Unknown		0	
Warning	7/11/2014 08:31:46	Stored	/DeviceRoot/ntp.drift	Owner: Unknown		0	
Warning	7/11/2014 06:28:45	Stored	/DeviceRoot/vmware/backup.counter	Owner: Unknown		0	
Warning	7/11/2014 06:28:16	Stored	/DeviceRoot/ntp.drift	Owner: Unknown		0	
Warning	7/11/2014 04:25:17	Stored	/DeviceRoot/vmware/backup.counter	Owner: Unknown		0	
Warning	7/11/2014 04:24:48	Stored	/DeviceRoot/ntp.drift	Owner: Unknown		0	
Warning	7/11/2014 03:24:48	Stored	/DeviceRoot/vmware/backup.counter	Owner: Unknown		0	

Total Items: 125 CSV Export Page Size: 100 1 / 2

Figure 144: Object Group Change Log

Each Change Log message type has a corresponding icon that allows for quick visual reference to the urgency level of the event. These urgency levels are important to note when configuring E-Mail alert permissions. E-Mail alert permissions are explained in a subsequent section.

**Emergency:** *System is unusable. Highest level of event.*

**Alert:** *Take action immediately.*

**Critical:** *Critical conditions have occurred.*

**Error:** *Error conditions.*

**Warning:** *Warning conditions.*

**Notice:** *Normal condition that requires attention.*

**Information:** *Informational message.*

**Debug:** *Debug-level message. Lowest level of event.*

Generally change events are associated with the Error level. Specifics relating to message types are discussed in a subsequent section.

#### **6.1.3.2.1. FILTERING AND SORTING THE OBJECT GROUP CHANGE LOG**

The Object Group Change Log can be filtered to only show events matching the specified criteria. Accessing the Object Group Change Log is accomplished by first clicking once on the Object Group in the Object Group Tree to select it followed by clicking the Change Log tab in the Web Management Console Information Display Area.

To filter the information displayed in the Object Group Change Log, drag and drop one of the column headers into the section labelled “Drag a column header here and drop it to group by that column.”

#### **6.1.3.2.2. ACCESSING THE CHANGE LOG TAB CONTEXT MENU**

Right-clicking on any event listed in the Change Log tab provides a context menu allowing for change related actions. The Change Log tab is accessed by selecting the Object Group in the Web Management Console’s Object Group Tree and then selecting the Change Log tab in the Information Display Area.

The Change Log Context Menu allows for additional actions to be taken on stored changes including:

**View:** *View the content and attributes associated with the stored change.*

**View as Binary:** *View the content associated with the stored change in a hexadecimal format.*

**View Forensic Data:** *View the IP Address and Port number associated with the change process. (Windows Network Device Agent with Driver only).*

**Download:** *Download a copy of the stored intrusion.*

**Compare with Authoritative Copy (at time of change):** *Compare the content of the detected change with the known, authoritative copy stored in the Master Repository at the time of the change.*

**Compare with Authoritative Copy (current):** *Compare the content of the detected change with the current known, authoritative copy stored in the Master Repository currently.*

**Add to Excludes:** *Disable monitoring of the selected file or configuration.*

Details associated with these context menu options are discussed in subsequent sections.

#### **6.1.3.2.2.1. VIEWING CHANGE CONTENT**

Right-clicking on any event listed in the Change Log tab provides a context menu allowing for change related actions. Selecting View from the context menu allows authorized CimTrak™ administrators the capability to review content associated with a detected change. The Change Log tab is accessed by



selecting the Object Group in the Web Management Console's Object Group Tree and then selecting the Change Log tab in the Information Display Area.

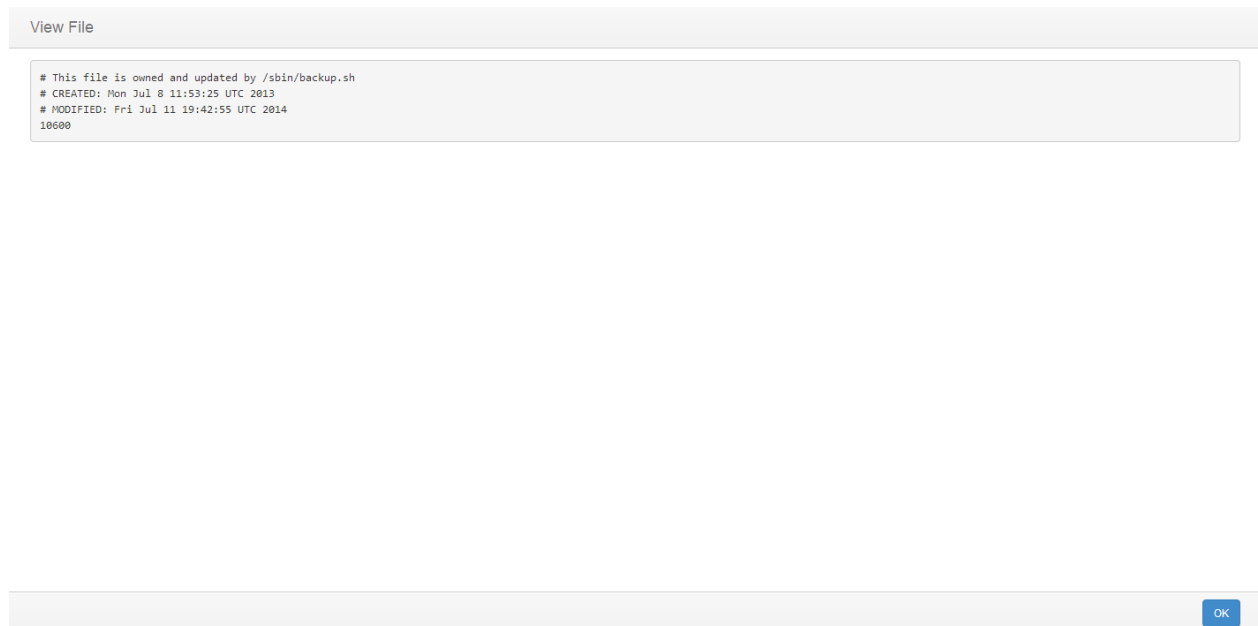


Figure 145: File View dialog

***Viewing of Change data requires the Object Group Policy is configured to store changes. Additionally, the change must not exceed the specified “Keep Change Size (in KB)” indicated in Object Group Properties Monitoring Information.***

***Viewing the content of non-binary files is supported. Binary files cannot be viewed at this time.***

Click the Close button to exit the File View dialog.

#### **6.1.6.2.2.2. VIEWING CHANGE FORENSIC DATA**

Right-clicking on any event listed in the Change Log tab provides a context menu allowing for change related actions. Selecting View Forensic Data from the context menu allows authorized CimTrak™ administrators the capability to review connections associated with the offending change process at the time of the change. The Change Log tab is accessed by selecting the Object Group in the Web Management Console's Object Group Tree and then selecting the Change Log tab in the Information Display Area.

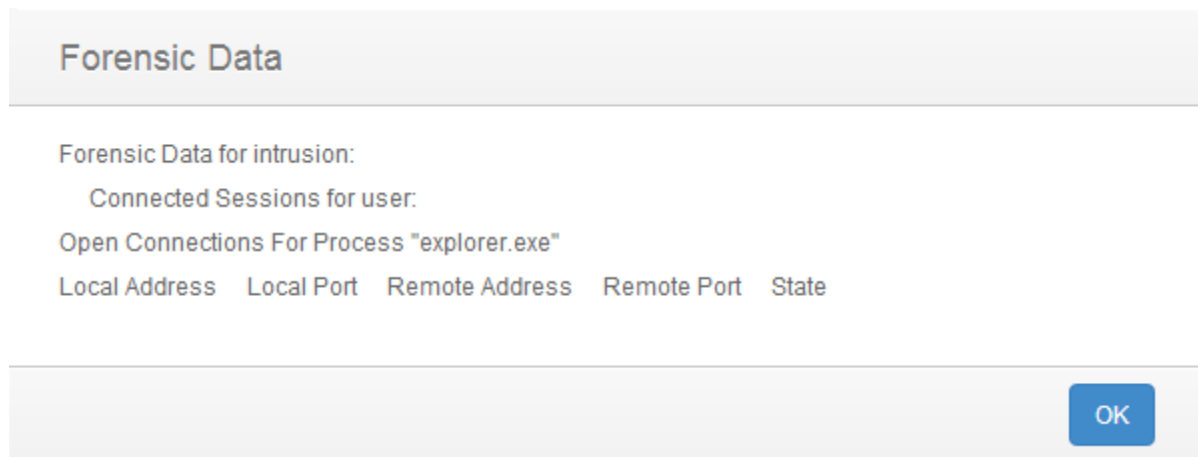


Figure 146: Forensic Data dialog

***Forensic data is only available for remote connections.***

***Viewing of forensic data is only supported on Windows File Systems with the Network Device Agent Driver installed.***

The Forensic Data dialog displays the following information:

Mount Points: The Windows Mount Point Name the change occurred on.\*?\*

Process: The Windows Process name responsible for initiating the detected change. Remote changes display as "System".

Local Address: IP Address on the affected system the process utilized to make the change.

Local Port: Port number on the affected system the process utilized to make the change.

Remote Address: IP Address of the remote system that attached to the local process to make the change.

Remote Port: Port number of the remote system used to connect to the local system.

State: State of the current connection (i.e., Listen or Established).

Click the Close button to exit the Forensic Data dialog.

#### **6.1.3.2.2.3. DOWNLOADING A COPY OF CHANGE DATA**

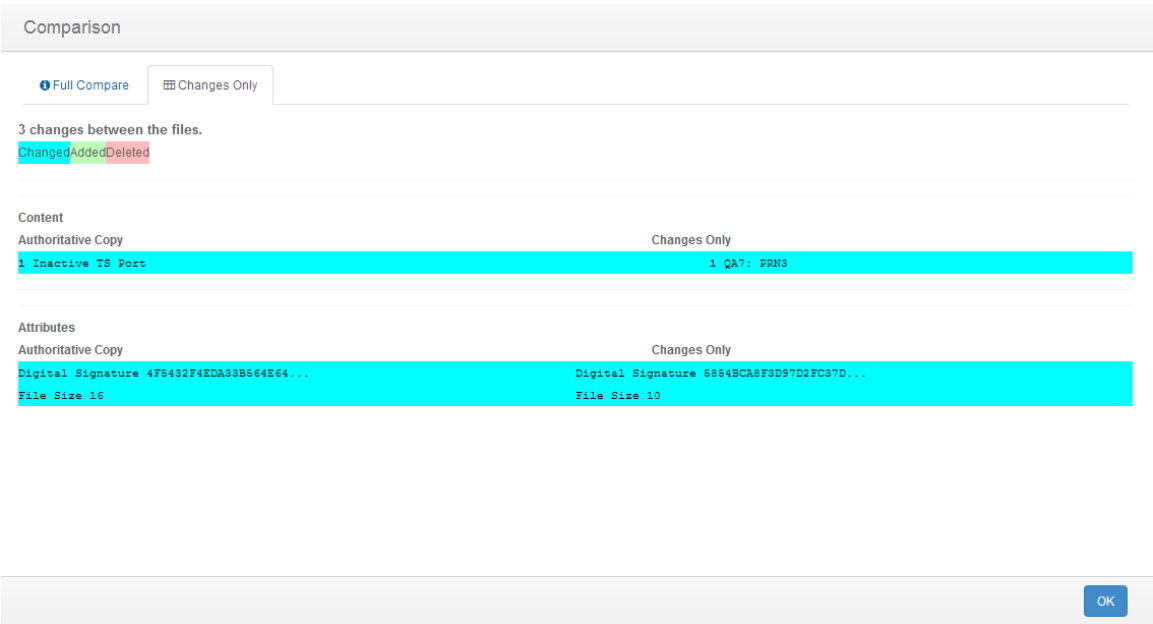
Right-clicking on any event listed in the Change Log tab provides a context menu allowing for change related actions. Selecting Download from the context menu allows authorized CimTrak™ administrators the capability to download a copy of

the actual change file. The Change Log tab is accessed by selecting the Object Group in the Web Management Console's Object Group Tree and then selecting the Change Log tab in the Information Display Area.

Clicking the Download option in the Change Log tab context menu results in the file being downloaded and saved in the Download folder, or in your default location for downloaded files.

**6.1.3.2.2.4. COMPARING CHANGE DATA WITH THE AUTHORITATIVE COPY AT THE TIME OF THE CHANGE**

Right-clicking on any event listed in the Change Log tab provides a context menu allowing for change related actions. Selecting Compare with Authoritative Copy (at time of change) allows authorized CimTrak™ administrators the capability to perform a side-by-side comparison of the changed file with it authoritative copy stored in the Master Repository. The Change Log tab is accessed by selecting the Object Group in the Web Management Console's Object Group Tree and then selecting the Change Log tab in the Information Display Area.



**Figure 147: File Comparison Results**

**6.1.3.2.2.4.1. UNDERSTANDING THE OBJECT GROUP CHANGE TAB FILE COMPARISON RESULTS DIALOG**

The File Comparison Results dialog displays anytime a comparison is performed between a detected change and the authoritative copy associated with watch properties. See section 0 for more information on performing file comparisons.

The File Comparison dialog is comprised of two tabs:

**Full Compare:** A comparison of both files are shown with all content and attributes listed.

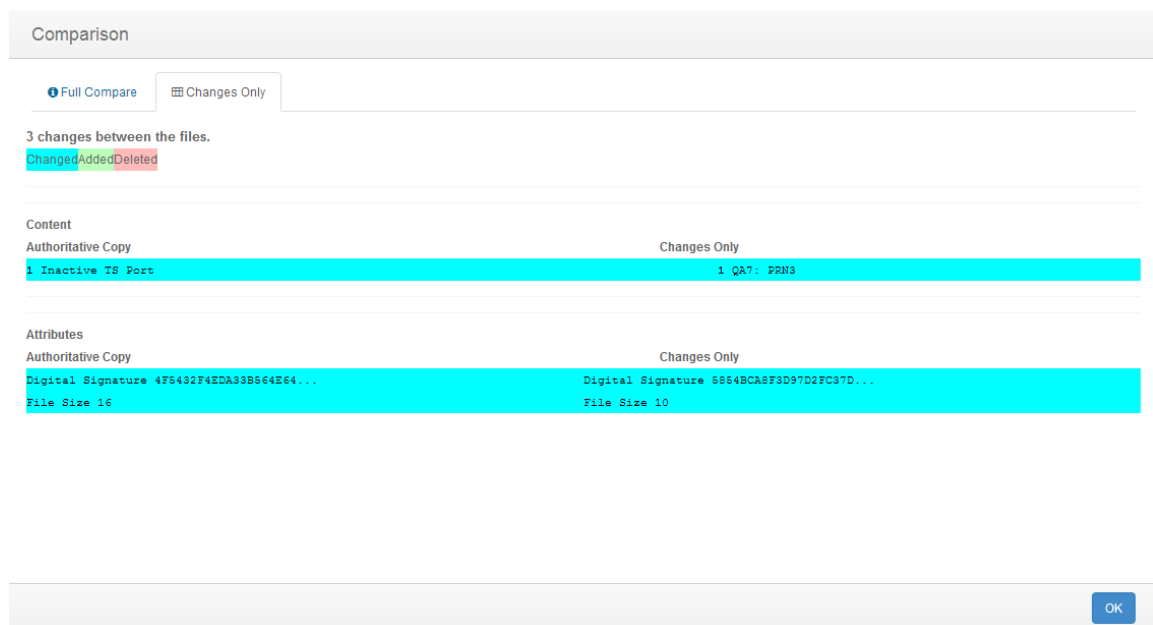
**Changes only:** A comparison of both file are shown with only the content and attributes which the changes affected listed.

#### 6.1.3.2.4.1.1. UNDERSTANDING THE FILE COMPARISON RESULTS DIALOG INFORMATION DISPLAY AREA AND TAB BROWSER

The File Comparison Results dialog Tab Browser and Information Display Area allows authorized CimTrak™ users the capability visualize generation comparison data. The File Comparison Results dialog is accessible by accessing the context menu and selected Compare with Authoritative Copy (at time of Change) in the Object Group Change Tab. See section 0 for more information on performing file comparisons.

The File Comparison Results dialog Information Display Area shows a side-by-side comparison of one generation revision of a detected change to the Master Repository Authoritative Copy. Lines that have been modified are highlighted in blue, lines that have been added are highlighted in green, and lines that have been deleted are highlighted in red.

By default, the “Full Compare” tab is selected. The “Full Compare” tab shows all lines of a selected comparison. Selecting the “Changes Only” tab displays only the lines that have differences between the compared generations.

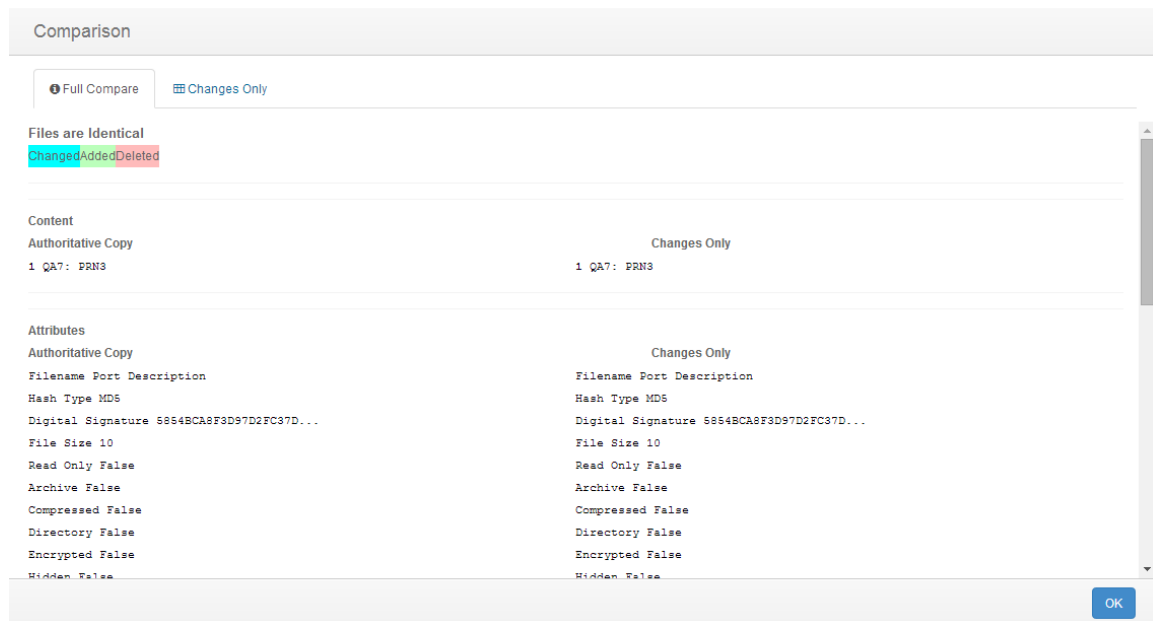


**Figure 148: File Comparison Results dialog Changes tab**

Click the Close button to exit the File Comparison Results dialog.

#### 6.1.3.2.2.5. COMPARING CHANGE DATA WITH THE CURRENT AUTHORITATIVE COPY

Right-clicking on any event listed in the Change Log tab provides a context menu allowing for change related actions. Selecting Compare with Authoritative Copy (Current) allows authorized CimTrak™ administrators the capability to perform a side-by-side comparison of the changed file with an authoritative copy stored in the Master Repository. The Change Log tab is accessed by selecting the Object Group in the Web Management Console's Object Group Tree and then selecting the Change Log tab in the Information Display Area.



**Figure 149: File Comparison Results**

Click the Close button to exit the File Comparison Results dialog.

#### 6.1.3.2.2.5.1. UNDERSTANDING THE OBJECT GROUP CHANGE TAB FILE COMPARISON RESULTS DIALOG

The File Comparison Results dialog displays anytime a comparison is performed between a detected change and the authoritative copy associated with watch properties. See section 0 for more information on performing file comparisons.

The File Comparison dialog is comprised of two tabs:

**Full Compare:** A comparison of both files are shown with all content and attributes listed.

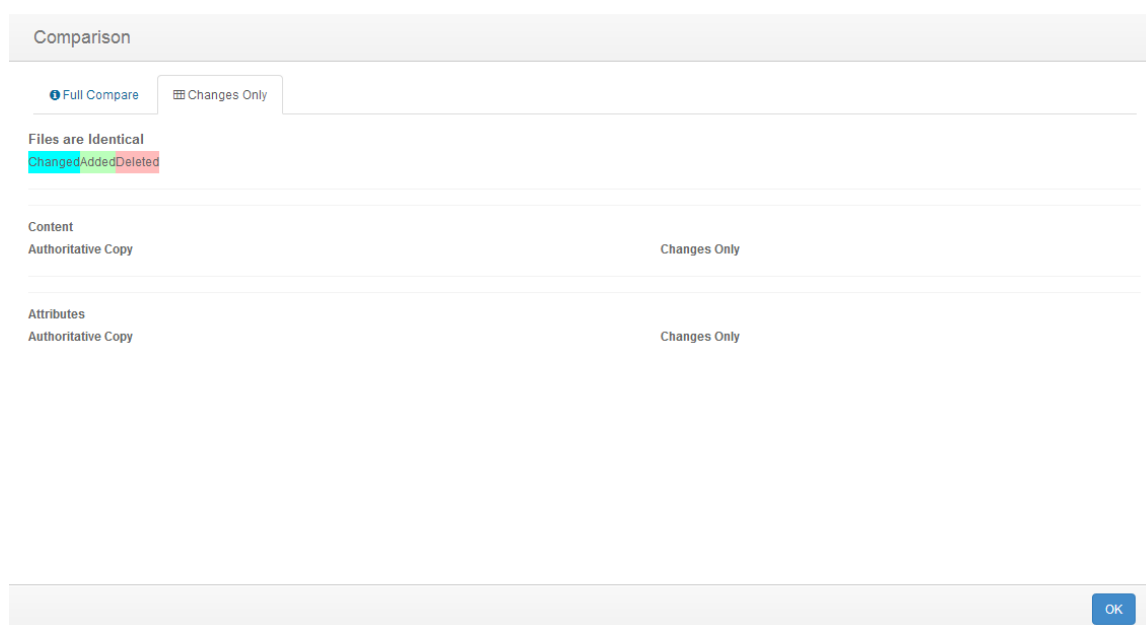
**Changes only:** A comparison of both file are shown with only the content and attributes which the changes affected listed.

#### 6.1.3.2.2.5.1.1. UNDERSTANDING THE FILE COMPARISON RESULTS DIALOG INFORMATION DISPLAY AREA AND TAB BROWSER

The File Comparison Results dialog Tab Browser and Information Display Area allows authorized CimTrak™ users the capability visualize generation comparison data. The File Comparison Results dialog is accessible by accessing the context menu and selected Compare with Authoritative Copy (Current) in the Object Group Change Tab. See section 0 for more information on performing file comparisons.

The File Comparison Results dialog Information Display Area shows a side-by-side comparison of one generation revision of a detected change to the Master Repository Authoritative Copy. Lines that have been modified are highlighted in blue, lines that have been added are highlighted in green, and lines that have been deleted are highlighted in red.

By default, the “Full Compare” tab is selected. The “Full Compare” tab shows all lines of a selected comparison. Selecting the “Changes Only” tab displays only the lines that have differences between the compared generations.



**Figure 150: File Comparison Results dialog Changes tab**

Click the Close button to exit the File Comparison Results dialog.

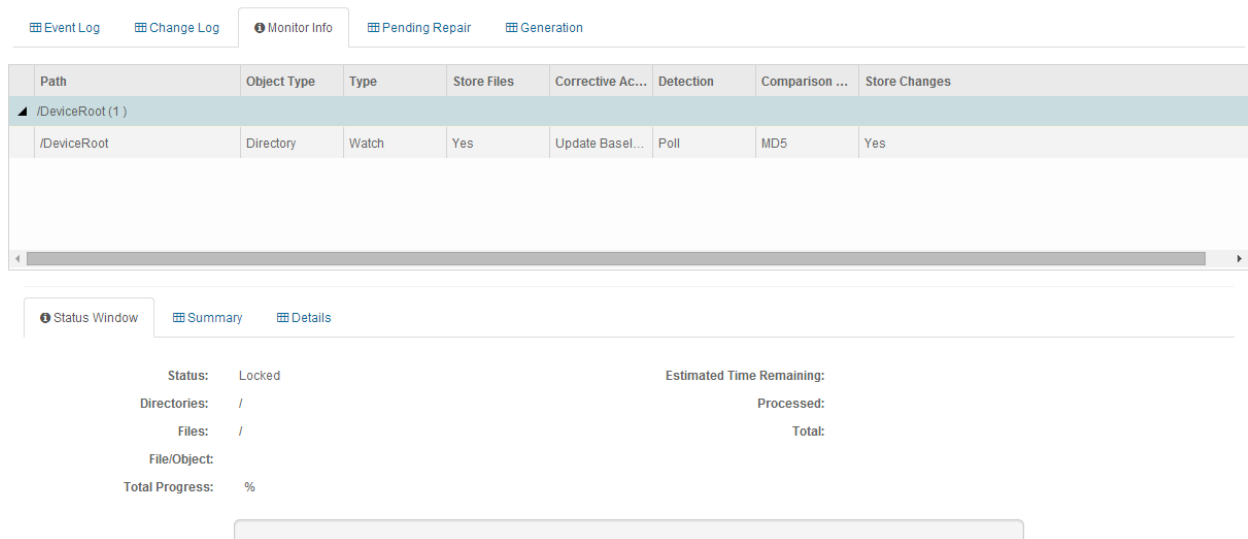
#### 6.1.3.3. REVIEWING OBJECT GROUP MONITORING INFORMATION

The Object Group Monitor Info tab provides Object Group monitoring and status information relating to Object Groups connected to the Network Device Agent. Accessing the Object Group Monitor Info is accomplished by first clicking once on the Object Group name in the Object Group Tree to select it followed by

clicking the Monitor Info tab in the Web Management Console Information Display Area.

The Object Group Monitor Info tab is comprised of two sections:

## Path Status Windows/Details



**Figure 151: Object Group Monitor Info tab**

The Path section displays watch path and exclude information pertaining to the select Object Group.

The Status Window/Details section is comprised of three tabs:

- **Status Window:** *Displays current lock status information associated with the Object Group Watch Policy. (i.e. Lock, Locking, Unlocked)*
- **Summary:**
- **Details:** *Displays details associated with the Object Group Watch Policy Configuration including:*
  - **Type:** *Object Group policy type (generally Watch).*
  - **Detection Mode:** *The change detection mode enabled (Real-time or polling)*
  - **File Comparison Method:** *The hash type performed on monitored data.*
  - **User Approval on Sync:** *Require user intervention for changes detected while the Network Device Agent was disconnected from the Master Repository. (True, False)*
  - **Store Files:** *Store authoritative copy data in the Master Repository (True, False).*

- **Store Changes:** *Store change data in the Master Repository (True, False).*
- **Ignore Archive Flag:** *Monitor the archive flag associated with file system watch data. (True, False)*
- **Ignore Read-only Flag:** *Monitor the read-only flag associated with the file system watch data. (True, False)*
- **Ignore SACL Flag:** *Monitor the SACL flag associated with the file system watch data. (True, False)*
- **Ignore DACL Flag:** *Monitor the DACL flag associated with the file system watch data. (True, False)*
- **Ignore Owner Security Flag:** *Monitor the Owner Security flag associated with the file system watch data. (True, False)*
- **Ignore Group Security Flag:** *Monitor the Group Security flag associated with the file system watch data. (True, False)*
- **Ignore Alternate Data Flag:** *Monitor the Alternate Data flag associated with the file system watch data. (True, False)*
- **Ignore File Dates Flag:** *Monitor the File Dates flag associated with the file system watch data. (True, False)*
- **Block Writes Flag:** *Monitor the Block Writes flag associated with the file system watch data. (True, False)*
- **Auto Exclude Files that have changed Flag:** *Monitor the Auto Exclude Files that have changed flag associated with the file system watch data. (Enabled, Disabled)*
- **Log Reads Flag:** *Monitor the Log Reads flag associated with the file system watch data. (True, False)*
- **Number of Intrusions to Keep:**
- **Keep Intrusion Size (in KB):**
- **Number of Revisions to Keep:**
- **Warn if Unlocked (in minutes):**
- **Number of Events to Keep:**
- **Corrective Action (On Add, On Change, On Delete):** *The Corrective Action mode specified in the Object Group Watch Policy. (Restore, Update Baseline, Log, Prompt, Ignore)*
- **Run (On Add, On Change, On Delete):** *Custom script that is ran when an add, change, or delete action has occurred on monitored watch data. (Path/File Name)*
- **Wait (On Add, On Change, On Delete):** *Use remediation timeout period enforced on custom scripts that are ran when an add, change, or deleted action has occurred on the monitored watch data. (True, False)*
- **Timeout (On Add, On Change, On Delete):** *Remediation timeout period enforced on custom scripts that are ran when an add, change, or deleted action has occurred on the monitored watch data.*



- **Parameters (On Add, On Change, On Delete):** *Pass filed and action parameters to the attached script ran on add, change, or delete actions.*

The screenshot shows the 'Status Window' tab with the following information:

Status:	Locked	Estimated Time Remaining:	
Directories:	/	Processed:	
Files:	/	Total:	
File/Object:			
Total Progress:	%		

Below the text is a horizontal progress bar.

**Figure 152: Monitor Info Status Window tab**

The screenshot shows the 'Summary' tab with the following configuration settings:

Detection Mode:	Real-time	Comparison Method:	MD5	Type:	Watched Directory
Store Files:	Yes	Store Changes:	Yes	Approval on Sync:	No
Block Writes:	No	Log Reads:	No		
# Intrusions to Keep:	250	# Revisions to Keep:	250	# Events to Keep:	250 Events
Keep Intrusion Size:	500 (kb)	Warn if Unlocked:	0 min.	Auto exclude files:	Disabled
On Add:	Update Baseline	On Change:	Update Baseline	On Delete:	Update Baseline

**Figure 153: Monitor Info Summary Window tab**

The screenshot shows the 'Details' tab with a table of settings:

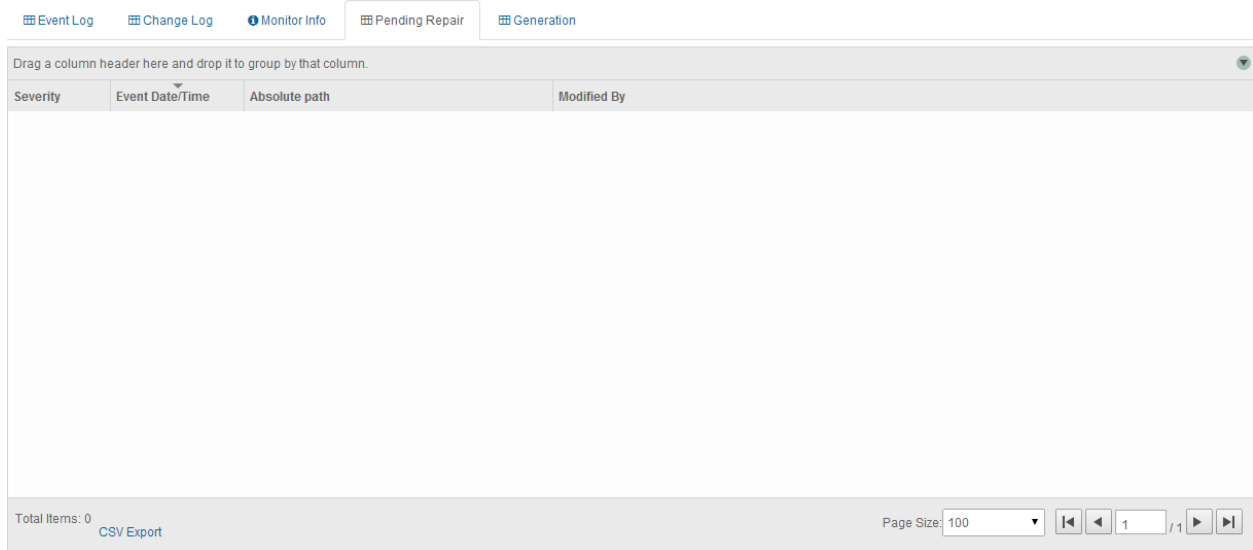
Setting Name	Current Setting
Type	Watched Directory
Detection Mode	Real-time
File Comparison Method	MD5
User Approval on Sync	<input checked="" type="checkbox"/>
Store Files	<input checked="" type="checkbox"/>
Store Changes	<input checked="" type="checkbox"/>
Ignore Archive Flag	<input checked="" type="checkbox"/>

**Figure 154: Monitor Info Details tab**

#### 6.1.3.4. REVIEWING OBJECT GROUP DATA PENDING REPAIR

The Pending Repair tab displays queue information associated with the remediation of folder, file and configuration data. The Pending Repair tab will append the number of pending repairs to the tab title. As changes are repaired they are automatically removed from the Pending Repair tab. Accessing the Object Group Pending Repair tab is accomplished by first clicking once on the Object Group name in the Object Group Tree to select it followed by clicking the Pending Repair tab in the Web Management Console Information Display Area.

***The Pending Repair tab also displays changes requiring CimTrak™ Administrator intervention. Intervention is required if the Prompt for Approval corrective action is enabled or the User Approval on Sync has been enabled and there was a communication failure between the Network Device Agent and the Master Repository.***



Severity	Event Date/Time	Absolute path	Modified By
Total Items: 0			

**Figure 155: Pending Repair tab showing 3 pending repairs**

For each recorded event, the Object Group Pending Repair tab will display information corresponding to the following:

**Severity:** *The state of the pending repair.*

**Event Date/Time:** *The exact date and time of the detected event.*

**Absolute Path:** *File path affected by the detected event.*

**Modified By:** *The File System User responsible for the detected event.*

Generally, the items contained in the Pending Repair tab will automatically cycle out as the folders, files, and configurations are remediated on the monitored system. The Pending Repair tab will automatically refresh based on the Pending Repair Refresh Interval specified in the Master Repository Preferences dialog.

In the event the Pending Repairs exist due to the Prompt for Approval Corrective Action or a triggered User Approval on Sync the Changes Pending Approval dialog must be referenced. See a subsequent section for additional information on the Changes Pending Approval dialog.

Each Pending Repair message type has a corresponding icon that allows for quick visual reference to the urgency level of the event. These urgency levels are important to note when configuring E-Mail alert permissions. E-Mail alert permissions are explained in a subsequent section.

**Emergency:** *System is unusable. Highest level of event.*

**Alert:** *Take action immediately.*

**Critical:** *Critical conditions have occurred.*

**Error:** *Error conditions.*

**Warning:** *Warning conditions.*

**Notice:** *Normal condition that requires attention.*

**Information:** *Informational message.*

**Debug:** *Debug-level message. Lowest level of event.*

Specifics relating to message types are discussed in a subsequent section.

#### **6.1.3.4.1. FILTERING AND SORTING THE PENDING REPAIR TAB**

The Pending Repair Tab can be filtered to only show events matching the specified criteria. Accessing the Object Group Event Log is accomplished by first clicking once on the Object Group in the Object Group Tree to select it followed by clicking the Pending Repair tab in the Web Management Console Information Display Area.

To filter the information displayed in the Pending Repair Tab, drag and drop one of the column headers into the section labelled “Drag a column header here and drop it to group by that column.”

#### **6.1.3.5. OBJECT GROUP GENERATIONS**

The Object Group Generation Tab provides revision information for changes occurring to files, folders, operating system configurations contained in a Network Device Agent Object Group. Accessing the Object Group Generations Tab is accomplished by first clicking once on the Object Group in the Object Group Tree to select it followed by clicking the Generation tab in the Web Management Console Information Display Area.

The Generation Tab is broken into two sections:

## Revisions Table

### Revision Details

Event Log

Change Log

Monitor Info

Pending Repair

Generation

Revision	Sub-revision	Date/Time	Changed by	# of Dirs	# of Files	Total Size(bytes)
0000019	0000001	3/19/2014 10:18:15	admin	3	14	40757180
0000018	0000001	3/13/2014 11:03:27	admin	3	14	40757180
0000017	0000025	3/13/2014 10:08:23	admin	Calculating...	Calculating...	Calculating...
0000017	0000024	3/13/2014 10:08:20	admin	Calculating...	Calculating...	Calculating...

Total Items: 43

CSV Export

Page Size: 100 / 1

Revision Information

Details

Change From Previous

Date of Revision:

3/13/2014 11:03:27

Revised by:

admin

Revision:

0000018

Sub-Revision:

0000001

Number of Files:

14

Number of Directories:

3

Notes:

Lock Request

**Figure 156: Object Group Generation Tab**

The Revisions Table displays overview information relating to each generation revision. Selecting a specific generation revision in the Revision Table will populate the corresponding information in the Revision Details section.

Information in the Revisions Table includes:

**Revision:** Primary revision number indicating the number of the generation.

**Sub-revision:** Secondary revision number indicating the number of events that have occurred since the primary generation was created.

**Date/Time:** Date and time associated with the creation of the revision or sub-revision.

**Changed by:** The CimTrak™ User account responsible for the creation of the revision or sub-revision.

**# of Dirs:** Quantity of directories contained in the revision or sub-revision.

**# of Files:** Quantity of files contained in the revision or sub-revision.

**Total Size (bytes):** The total amount of disk space utilized by the contents of the revision or sub-revision.

The Revision Details section displays detailed information relating to a revision or sub-revision. The Revision Details section has three tabs:

**Revision Information:** Details of the revision or sub-revision such as the date of the revision, revising user account, number of revisions, number of sub-revisions, number of files, number of directories, and notes.

**Details:** *Complete list of all files and folders contained in a generation. Files and folders indicate their generation status such as “Added”, “Deleted”, and “Modified”.*

**Change from Previous:** *Partial file list showing what files were “Added”, “Deleted” or “Modified” in the selected generation.*

#### **6.1.3.5.1. DOWNLOADING GENERATION DATA**

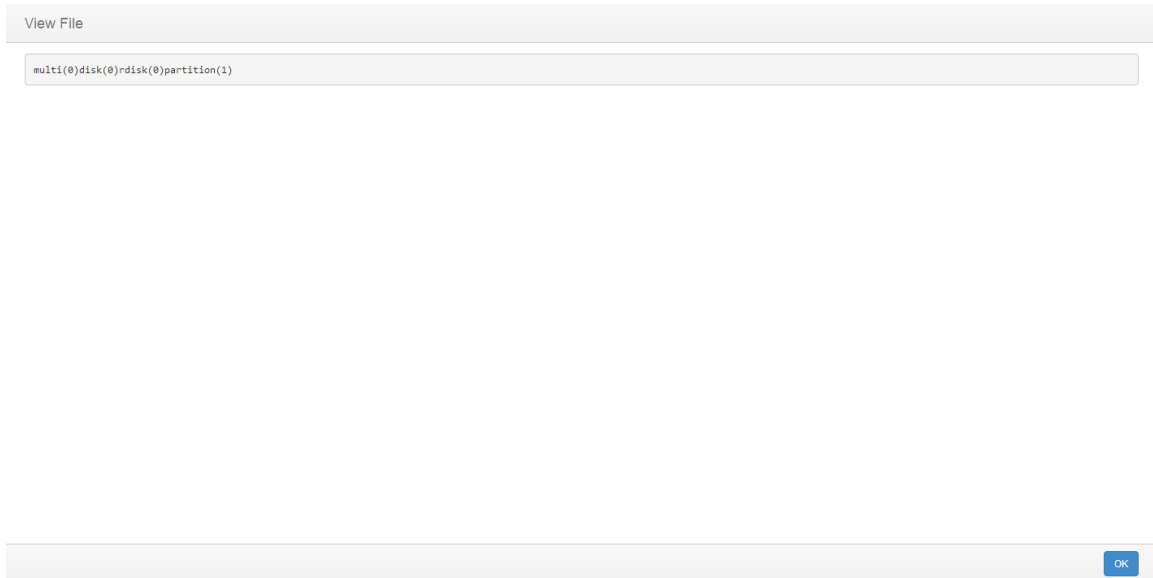
Each file stored in an Object Group generation has the capability to be downloaded and copied to a local system. An Object Group generation can be accessed by first clicking once on the Object Group in the Object Group Tree to select it followed by clicking the Generation tab in the Web Management Console Information Display Area.

Copies of generation data can be downloaded by right-clicking on the Revisions Table generation and selecting “Download” from the context menu. Additionally, copies of generation data can also be downloaded from the Revision Details Details tab or Change from Previous tab by right-clicking on the file or folder to download and then clicking “Download”.

#### **6.1.3.5.2. VIEWING AND COMPARING CONTENT OF OBJECT GROUP GENERATIONS**

Folders, files, and configurations monitored within an Object Group generation have the capability to be viewed and compared with other generations. An Object Group generation can be accessed by first clicking once on the Object Group in the Object Group Tree to select it followed by clicking the Generation tab in the Web Management Console Information Display Area.

To view the non-binary file contents associated with a file, select either the Details or Change from Previous tab in the Object Group Generation Revision Details section. Right-click on the file and then select “View”. The File View dialog will display.

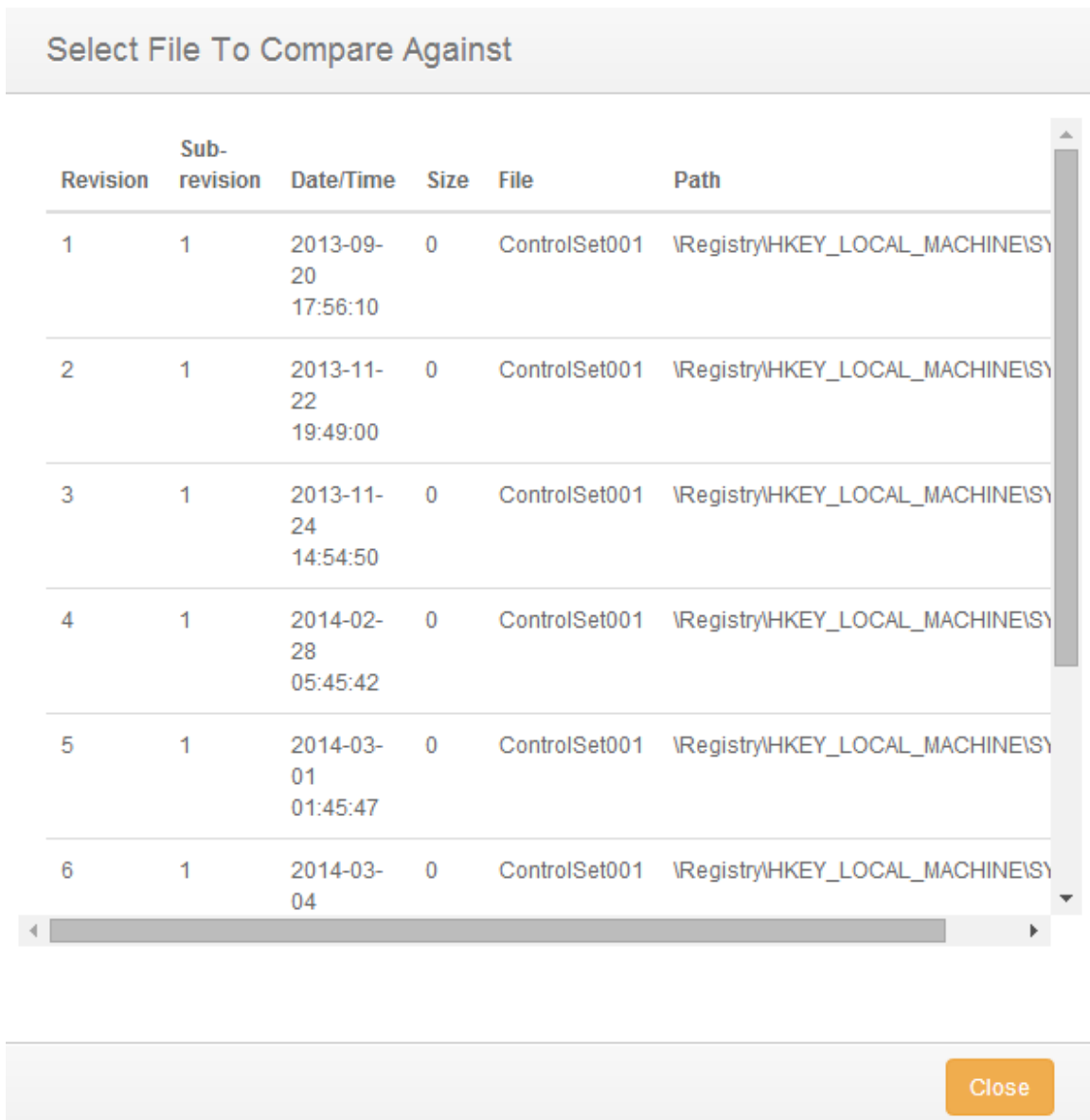


**Figure 157: File View dialog (non-binary)**

Click “Close” to exit the File View dialog.

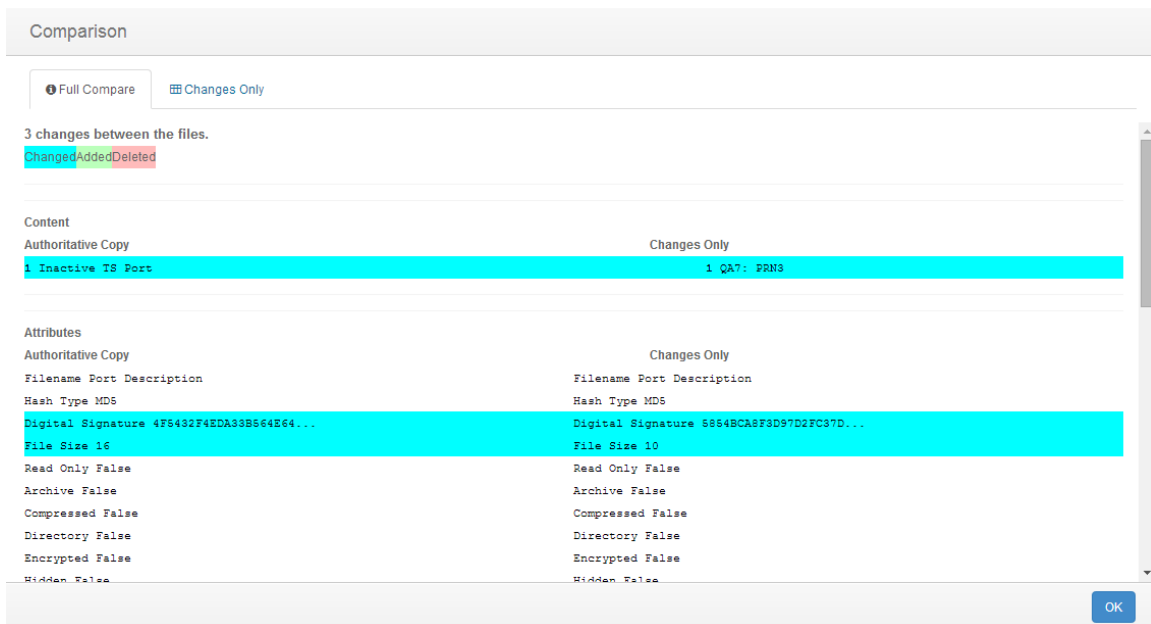
The Object Group Generations tab has the capability to compare previous generations with the current state of the file stored within the Master Repository to the local system. To compare a generation, click the “Object Group” node in the Web Management Console Object Group Tree. Select the generations tab.

To compare the file, from either the Details or Change from Previous tab, right-click on the file and then select either “Compare with Other Generation” or “Compare with Authoritative Copy (current)”. If “Compare with Other Generation” is selected the Select File to Compare Against dialog will display. Select the generation to compare with by clicking once on the revision. Click “OK” to perform the comparison or click “Cancel” to abort the comparison process. The File Comparison Results dialog will display.



**Figure 158: File to Compare Against dialog**

In the event “Compare with Authoritative Copy (current)” is selected the File Comparison Results will display comparing the current file content with the most current baseline.



**Figure 159: File Comparison Results dialog**

Click the “Close” button to exit the File Comparison Results dialog.

#### **6.1.3.5.2.1. UNDERSTANDING THE OBJECT GROUP CHANGE TAB FILE COMPARISON RESULTS DIALOG**

The File Comparison Results dialog displays anytime a comparison is performed between a detected change and the authoritative copy associated with watch properties. See section 0 for more information on performing file comparisons.

The File Comparison dialog is comprised of two primary sections.

**Information Display Area**  
**Tab Browser**

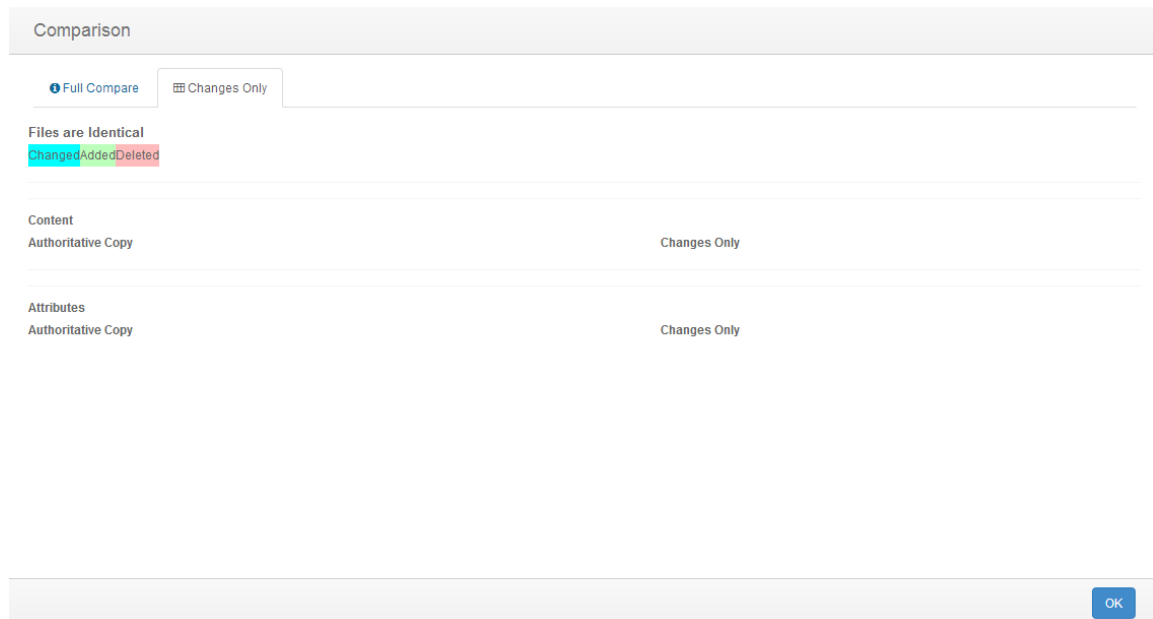
##### **6.1.3.5.2.1.1. UNDERSTANDING THE FILE COMPARISON RESULTS DIALOG INFORMATION DISPLAY AREA AND TAB BROWSER**

The File Comparison Results dialog Tab Browser and Information Display Area allows authorized CimTrak™ users the capability visualize generation comparison data. The File Comparison Results dialog is accessible by accessing the context menu and selected Compare with Authoritative Copy (Current) in the Object Group Change Tab. See section 0 for more information on performing file comparisons.

The File Comparison Results dialog Information Display Area shows a side-by-side comparison of one generation revision of a detected change to the Master Repository Authoritative Copy. Lines that have been modified are highlighted in blue, lines that have been added are highlighted in green, and lines that have been deleted are highlighted in red.



By default, the “Full Compare” tab is selected in the File Comparison Results Tab Browser. The “Full Compare” tab shows all lines of a selected comparison. Selecting the “Changes Only” tab displays only the lines that have differences between the compared generations.



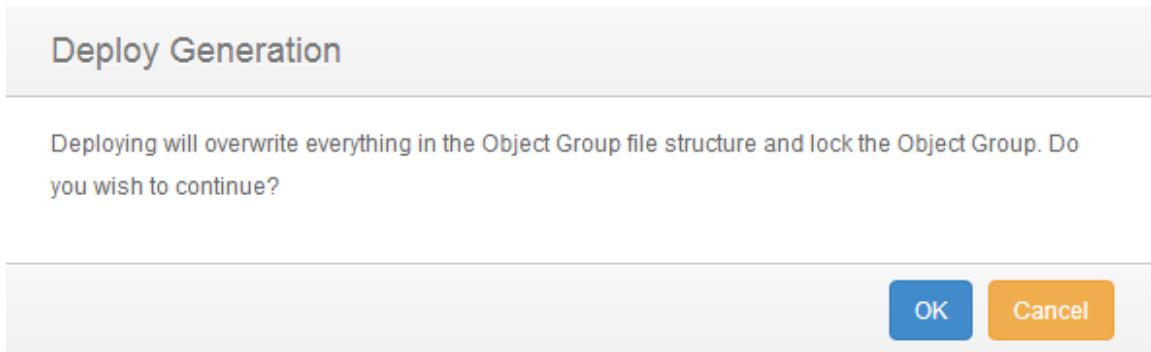
**Figure 160: File Comparison Results dialog Changes tab**

Click the Close button to exit the File Comparison Results dialog.

#### **6.1.3.5.3. DEPLOYING “ROLLING BACK” OBJECT GROUP GENERATIONS**

Depending on the remediation capabilities of the monitoring Object Group, the Generations tab may have the capability to deploy previous generations back to the File System. An Object Group generation can be accessed by first clicking once on the Object Group in the Object Group Tree to select it followed by clicking the Generation tab in the Web Management Console Information Display Area.

To deploy “roll back” a generation, select the generation in the Generation Tab Revisions Table, right-click, and then select “Deploy”. The Confirm Deploy dialog will display warning that deploying will overwrite everything in the Document Control with the content of this generation. Click “Yes” to proceed or “Cancel” to abort the operation.



**Figure 161: Confirm Deploy dialog**

Upon clicking “Yes” on the Confirm Deploy dialog the Notes dialog will appear. Enter any administrative notes relating to this deployment and then click “OK”. Click “Cancel” to abort the deployment.



**Figure 162: Notes dialog**

A new generation revision will be created with the rolled-back content. This newly created generation is the current generation.

#### **6.1.3.6. OBJECT GROUP PERMISSIONS**

Object Groups can be configured restrict access based on permission settings. Additionally, event notifications can be configured to notify CimTrak™ Users about events relating to the Object Group. Accessing Object Group permissions is accomplished by first clicking once on the File Object Group in the Object Group Tree to select it and then right-clicking and selecting “Permissions.” The Security Permissions dialog will display.

By default each Object Group will have the following permissions:

##### **Administrators**

**Create Objects:** *Create Network Device Agent Object Groups.*

**Edit:** *Edit Network Device Agent settings.*

**Lock:** *Enable active monitoring of Object Group Data.*

**Reports:** *View reports relating to the Object Group contents.*

**Unlock:** *Disable active monitoring of Object Group Data.*

**View:** *View contents and configurations relating to the Object Group.*

##### **Auditors**

**Reports:** View reports relating to Object Group contents.

**View:** View contents and configurations relating to the Object Group..

**Installers**

Attach CimTrak™ Agents to a Master Repository. (Not applicable for Object Groups).

Permissions for Object

Add

Group or User Names

Group	Administrators	
Group	Auditors	
Group	Email_Testing	Remove
Group	Installers	

Permissions	Allow	Deny
Create Objects	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Edit	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lock	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Reports	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Unlock	<input checked="" type="checkbox"/>	<input type="checkbox"/>
View	<input checked="" type="checkbox"/>	<input type="checkbox"/>

☒ Apply permissions to children recursively

OKCancel

**Figure 163: Object Group Security Permissions dialog**

Default access permissions associated with the Administrators, Auditors, and Installers User Groups cannot be changed. It is possible to modify E-mail alert notices for Administrator and Auditor user groups. Available E-mail alert types include:

Emergency  
Alert

Critical  
Error  
Warning  
Notice  
Information

Additional information relating to these alert types is described in a subsequent section.

#### **6.1.3.6.1. MODIFYING AN EXISTING USER/GROUP OBJECT GROUP PERMISSIONS**

It is possible to modify existing user and group Object Group Permissions and E-mail notification settings. Accessing Object Group permissions is accomplished by first clicking once on the Object Group in the Object Group Tree to select it and then right-clicking and selecting “Permissions.” The Security Permissions dialog will display.

Select the existing user or group by clicking once on the CimTrak™ User or Group name in the Group or User Names section of the Security Permissions dialog. The Permissions section of the Security Permissions dialog will update to show the permissions currently assigned to the selected user or group.

***Selecting a group will apply the selected permissions and E-mail notification settings to all members of the group. Selecting a single user will apply the selected permissions and E-mail notification settings to only that single user account.***

To add or remove permissions click the “Allow” or “Deny” checkbox corresponding to the permission being configured. Available permissions include:

**Create Objects:** *Create Network Device Agent Object Groups.*

**Edit:** *Edit Object Group control contents.*

**Lock:** *Enable active monitoring of Object Group Data*

**Reports:** *View reports relating to Object Group contents.*

**Unlock:** *Disable active monitoring of Object Group Data*

**View:** *View contents and configurations relating to the Object Group.*

**Email Emergency:** *Receive alerts relating to emergency level notifications.*

**Email Alert:** *Receive alerts relating to alert level notifications.*

**Email Critical:** *Receive alerts relating to critical level notifications.*

**Email Error:** *Receive alerts relating to error level notifications.*

**Email Warning:** *Receive alerts relating to warning level notifications.*

**Email Notice:** *Receive alerts relating to notice level notifications.*

**Email Information:** *Receive alerts relating to information level notifications.*

To apply the permission settings to all children objects, ensure that the Apply permissions to children recursively checkbox is selected.

When completed, click “OK” to apply the permission and alert settings. Click “Cancel” to abort the security permission configuration.

***Permissions and notification settings can be inherited from parent objects (such as the Network Device Agent) if the permissions are created at a parent level.***

***Permissions and notification settings are not automatically inherited for new objects. It will be necessary to manually assign the permissions and notification settings to the object.***

#### **6.1.3.6.2.    ADDING AND REMOVING USERS AND GROUPS TO OBJECT GROUP PERMISSIONS**

It is possible to add additional users and groups to the Security Permissions dialog so that Object Group Permissions and E-mail notification settings can be assigned or changed. Accessing Object Group permissions is accomplished by first clicking once on the Object Group in the Object Group Tree to select it and then right-clicking and selecting “Permissions.” The Security Permissions dialog will display.

To add a new local CimTrak™ User or Group, click the Add button. The Add Users dialog will display listing all available local users and groups.

Select Users or Groups

Q Search

	Type	Name
<input type="checkbox"/>	User	aaaa
<input type="checkbox"/>	User	wade
<input type="checkbox"/>	User	knightrider
<input type="checkbox"/>	User	payton
<input type="checkbox"/>	User	Pippen
<input type="checkbox"/>	User	Hanks
<input type="checkbox"/>	User	Rose
<input type="checkbox"/>	User	Garnett
<input type="checkbox"/>	User	Fridge
<input type="checkbox"/>	User	alberts
<input type="checkbox"/>	User	jovo2

OKCancel

Figure 164: Add Users dialog

Select the local CimTrak™ User or Group to add by selecting the checkbox to the left of the name. Click “OK” to add the User or Group. Click “Cancel” to abort the addition process. The selected user or group will now display in the Group or User Names section of the Security Permissions dialog.

## 7.1. MANAGING MASTER REPOSITORY USERS & GROUPS FROM THE MANAGEMENT CONSOLE

To help improve the functionality, deployment, and security of the Master Repository, CimTrak™ supports the creation of additional user accounts. User accounts and groups support prescribing differing access permissions based on the purpose and the account.

During the installation of the CimTrak™ Master Repository a single user account was created. This first user account was automatically added to the “Administrators” group. For functionality reasons, at least one administrator-level account must exist at all times.

The Users dialog provides the functionality to view, edit, delete, and add CimTrak™ users and groups. Accessing the User Maintenance dialog can be accomplished by first clicking once on the Master Repository in the Object Group Tree to select it and then right-clicking and selecting “User Maintenance.” The User Maintenance dialog will display.

User Maintenance

Search

Type	CimTrak Role	User	First Name	Last Name	Notes
User	Administrators	admin			
User	Administrators	Other Admin			
User	Administrators	Sam	Sam	Conley	
User	Standard	Justin	Justin	Chandler	
User	Standard	Rob	Robert	Johnson	
User	Standard	Ryan	Ryan	Rutkin	Notes?

Add User...

Add AD/LDAP User/Role...

Role Maintenance...

Close

**Figure 165: User Maintenance Dialog**

Each CimTrak™ user will be listed upon entering the CimTrak™ User Maintenance dialog.

From the CimTrak™ User Maintenance dialog, there are various actions that may be taken involving users.

## 7.2. ADDING A NEW USER

A new CimTrak™ user can be created by clicking the “Add User” button in the CimTrak™ User Maintenance dialog. For more information about the CimTrak™ User Maintenance dialog, please refer to section 0. Upon clicking the “Add User” button in the CimTrak™ User Maintenance dialog, the User Add/Edit dialog will appear.

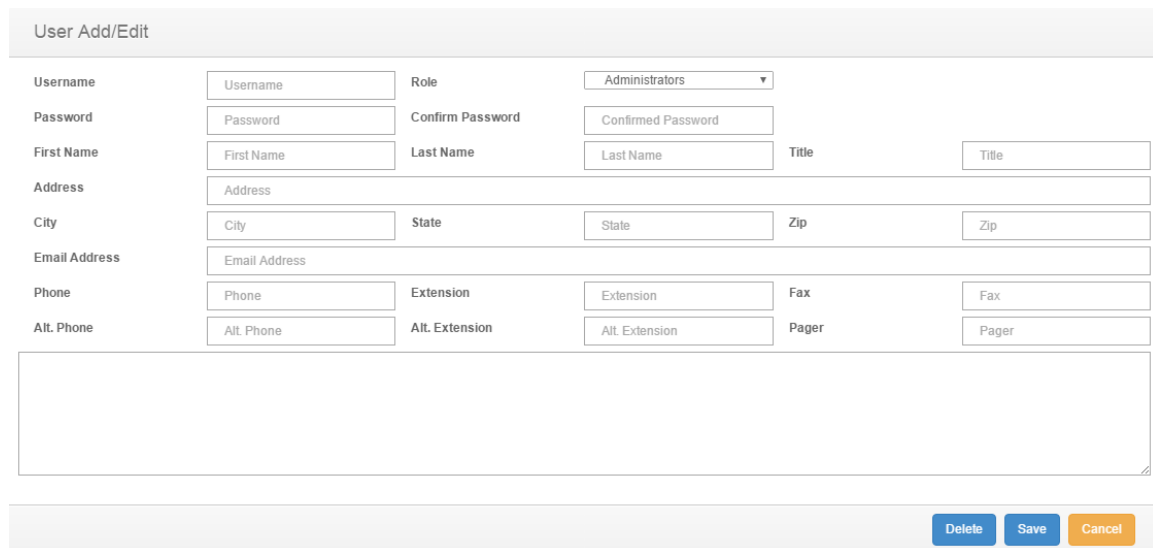
The image shows a 'User Add/Edit' dialog box. It has a title bar at the top. Below the title bar, there are several input fields arranged in a grid-like fashion. The fields are: Username (text box), Role (dropdown menu with 'Administrators' selected), Password (text box), Confirm Password (text box), First Name (text box), Last Name (text box), Title (text box), Address (text box), City (text box), State (text box), Zip (text box), Email Address (text box), Phone (text box), Extension (text box), Fax (text box), Alt. Phone (text box), Alt. Extension (text box), and Pager (text box). Below these fields is a large empty text area. At the bottom right of the dialog, there are three buttons: 'Delete' (blue), 'Save' (blue), and 'Cancel' (orange).

Figure 166: User Add/Edit dialog

The CimTrak™ User Add/Edit dialog provides various fields, allowing the user to associate different data with a specific user. These fields are.

- **Username\***: The name of the CimTrak™ user. This will be used to log into CimTrak™.
- **Role\***: The CimTrak™ role of the CimTrak™ user.
- **Password\***: The password for the CimTrak™ user. This will be used to log into CimTrak™.
- **Confirm Password\***: Confirmation of the entered user password. The value entered into this field must match the value entered into the Password field.
- **First Name**: The first name of the user.
- **Last Name**: The last name of the user.
- **Title**: The title of the user.
- **Address**: The address of the user.
- **City**: The city where the user lives.
- **State**: The state where the user lives.
- **Zip**: The zip code of the area where the user lives.
- **Email Address**: The email address of the user.
- **Phone**: The phone number of the user.
- **Extension**: The phone extension of the user.



- **Fax:** The fax number of the user.
- **Alt. Phone:** The alternate phone number for the user.
- **Alt. Extension:** The phone extension for the alternate phone number of the user.
- **Pager:** The pager number for the user.
- **Note:** Additional notes to be associated with the user.

*Fields marked with a “\*” are required.*

Once the required data has been entered, the configuration for the new user can be saved. To save the configuration for the new CimTrak™ user, click the Save button at the bottom of the screen. The new user will be added to CimTrak™ and the User Add/Edit dialog will close.

### **7.3. ADDING AN AD/LDAP USER OR ROLE**

A new CimTrak™ user can be created by clicking the “Add AD/LDAP User/Role” button in the CimTrak™ User Maintenance dialog. For more information about the CimTrak™ User Maintenance dialog, please refer to section 0. Upon clicking the “Add AD/LDAP User/Role” button in the CimTrak™ User Maintenance dialog, the Search AD/LDAP for Users and Groups dialog will appear.

In the Search AD/LDAP for Users and Groups dialog is an array of field used to search for the AD/LDAP User or Group. These field are:

- **Domain:** The domain of the AD/LDAP Server.
- **Member of Group (optional):** A field which will filter the result set of the search to only users who belong to the group listed in this field. This field is optional.
- **Search Groups/Search Users:** Two checkboxes which denote whether the search will be performed for Users or Groups. One of these checkboxes must be checked.
- **Search for String(s):** A search string that will be used to query to AD/LDAP Server with. This field may be a TODO separated list of search strings.

After entering the required information, you may search the AD/LDAP Server for a User or Group by clicking the Search button in the bottom right-hand corner of the screen. Upon clicking the Search button the Add CimTrak Role to AD/LDAP Group or User dialog will appear containing the results of your search.

Add CimTrak Role To AD/LDAP Group or User

Q
Search

	Type	CimTrak Role	Username	First Name	Last Name	Notes
<input type="checkbox"/>	User	None	cimtrak.local\admin	Ad	Min	
<input type="checkbox"/>	User	None	cimtrak.local\Administrator			Built-in account for administering the computer/domain
<input type="checkbox"/>	User	None	cimtrak.local\cimcor	cimcor	admin	default
<input type="checkbox"/>	User	None	cimtrak.local\ef46-admin	ef46-admin	ef46-admin	

Please verify CimTrak role to apply to this User(s)/Group(s)
Administrators
Add with the selected role
Close

**Figure 167: Add CimTrak™ Role to AD/LDAP Grou or User Dialog**

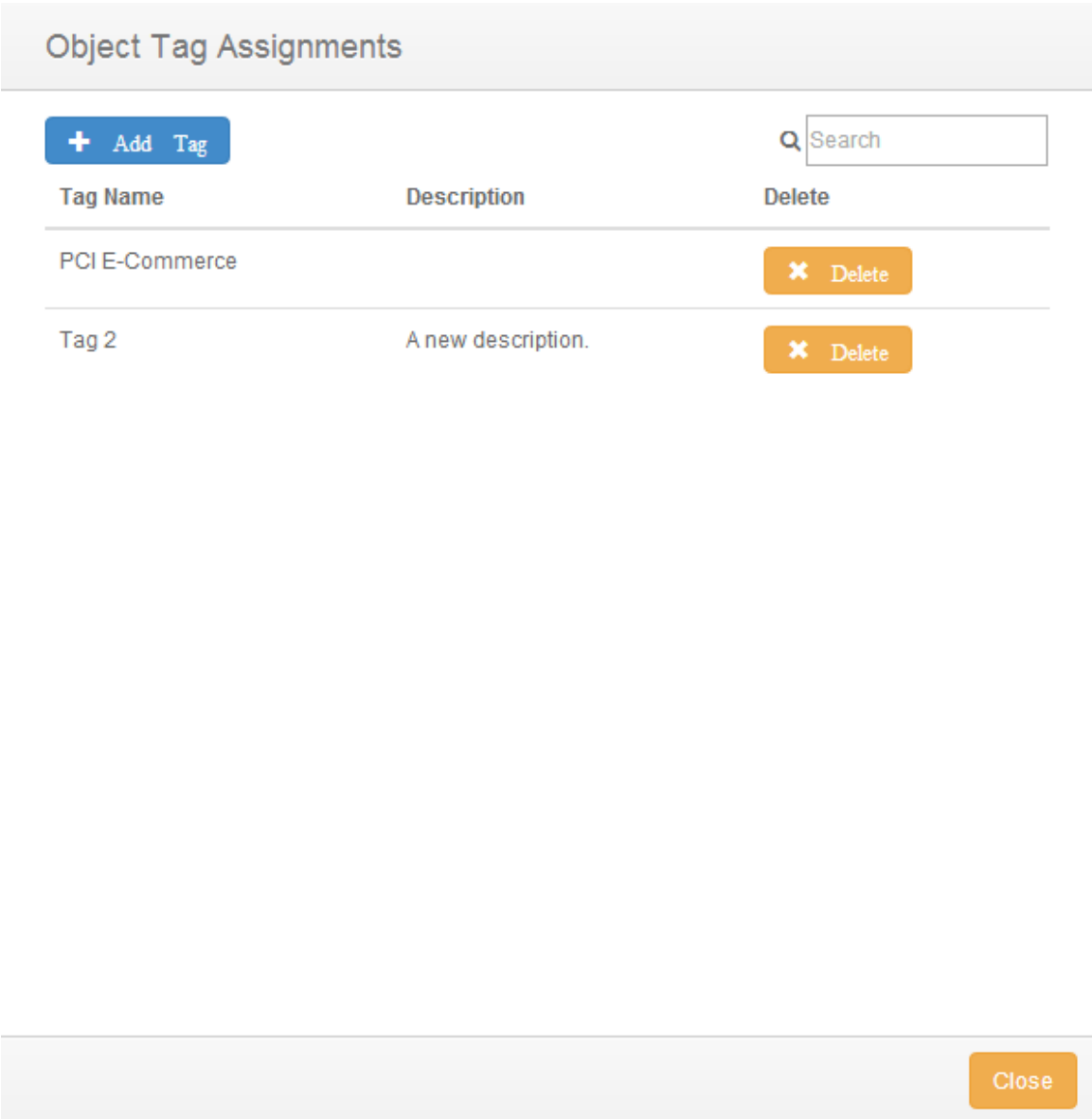
To apply a User or Group from your search results to a CimTrak Role, select the search result by checking the checkbox for that result and click the “Add with selected role” button in the bottom right-hand corner of the screen. The selected search result will be applied to the selected CimTrak role. A CimTrak role for application can be selected by the select box in the bottom of the screen.

**7.4. EDITING AN EXISTING CIMTRAK USER OR ROLE**

A CimTrak™ User or Role can be edited by first entering the User Maintenance dialog and clicking on the User or Role you wish to edit. For more information on the User Maintenance dialog, please refer to section 0. Upon clicking the User or Role you wish to edit, the User Add/Edit dialog will appear with the User or Role’s current data populating the fields of this screen. For more information on the User Add/Edit dialog, please refer to section 9.2. The data within these fields can be edited. Once the desired changes have been made to the selected CimTrak™ User or Role, you may save these changes by clicking the Save button in the bottom right-hand corner of the screen. To delete the selected user, click the Delete button in the bottom right-hand corner of the screen.

**8.1. MANAGING TAGS**

It is possible to associate a “tag” with an agent from the Object Group Tree for grouping and/or filtering. Tags can later be to filter the associated items under “Bulk Operations” when applying templates or modifying Agent Properties. Tags are added, created, or modified by right-clicking on an area in the Object Group Tree and selecting “Tags” from the context menu. The Object Tag Assignment dialog will appear.



**Figure 168: Object Tag Assignment Dialog**

**8.2. ASSOCIATING PRECONFIGURED TAGS**

A preconfigured Tag can be associated to a Cimtrak™ Agent from the Object Tab Assignment Dialog screen. The Object Tag Assignment screen can be accessed by right-clicking on a Cimtrak™ Agent in the Object Group Tree and selecting “Tags.” For more information about accessing the Object Tag Assignment screen, please refer to section 11.1.

To associate a preconfigured tag with the selected Cimtrak™ Agent, click the “Add Tag” button near the top of the Object Tag Assignment dialog screen. The Select Tag dialog will appear.

Select Tags

Search

Select	Tag Name	Description
<input type="checkbox"/>	another tag	This is another tag
<input type="checkbox"/>	jovowashere	
<input type="checkbox"/>	myTag	my description
<input type="checkbox"/>	newTag	A new description.
<input type="checkbox"/>	newtag3	newtag3 description
<input type="checkbox"/>	newtag4	newtag4 description
<input type="checkbox"/>	testTag	This is a test tag.

Create New Tag

Add

Cancel

**Figure 169: Select Tags dialog screen**

You can apply a preconfigured tag to a Cimtrak™ Agent by clicking the checkbox under the “Select” column that is associated with the desired tag.

Select Tags

Q Search

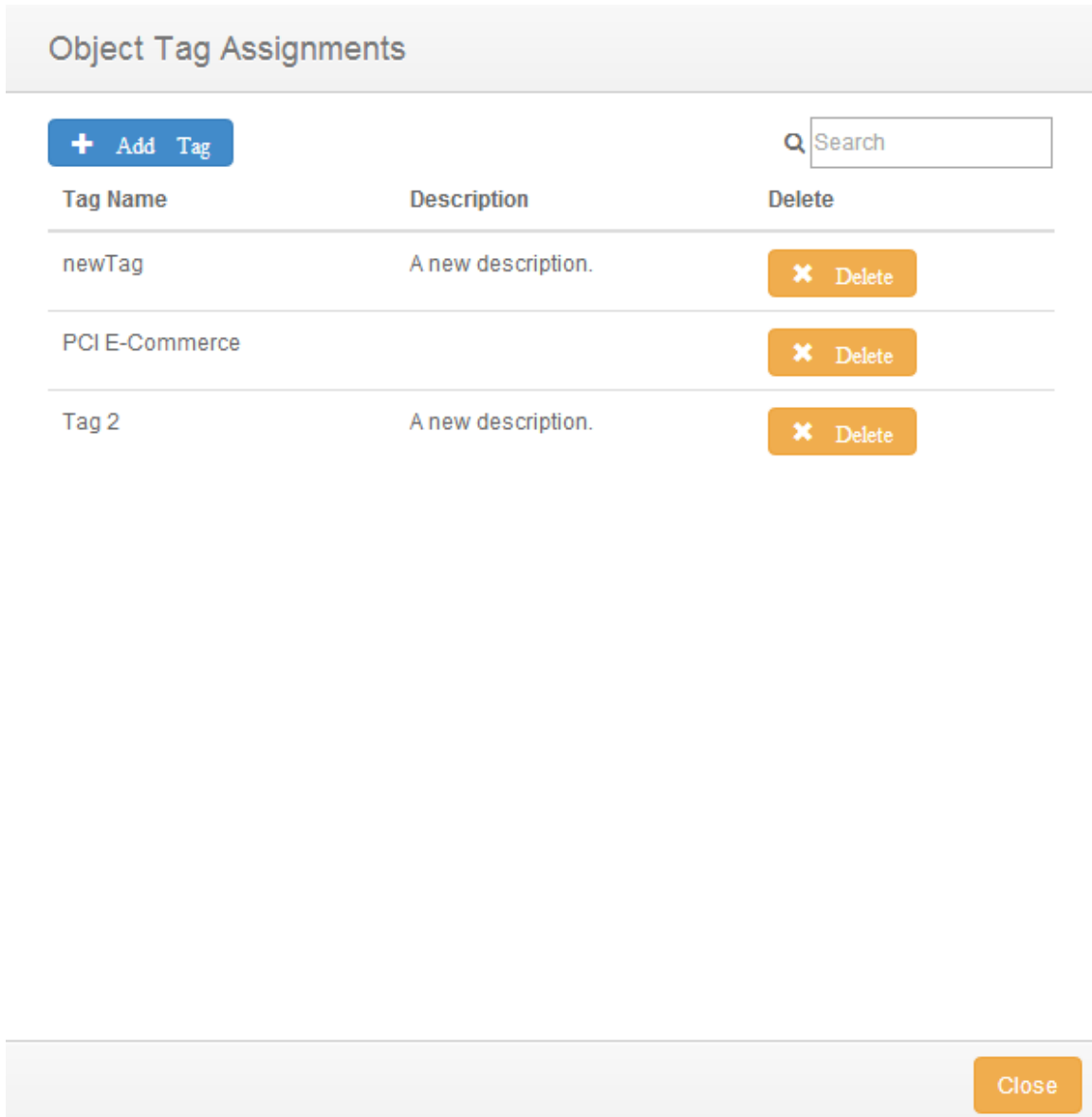
Select	Tag Name	Description
<input type="checkbox"/>	another tag	This is another tag
<input type="checkbox"/>	jovowashere	
<input type="checkbox"/>	myTag	my description
<input checked="" type="checkbox"/>	newTag	A new description.
<input type="checkbox"/>	newtag3	newtag3 description
<input type="checkbox"/>	newtag4	newtag4 description
<input type="checkbox"/>	testTag	This is a test tag.

Create New Tag

AddCancel

Figure 170: Select Tag dialog screen (tag selected)

Once the desired tag has been selected, click the “Add” button in the lower-left corner of the Select Tag dialog screen to add the selected tag to the selected Cimtrak™ Agent. The Object Tag Assignments dialog screen will appear with the newly assigned tag showing in the Assigned Tags section.



**Figure 171: Object Tag Assignments dialog screen (new tag assigned)**

### **8.3. CREATING NEW TAGS**

A new Tag can be created from the Object Tag Assignment Dialog screen. The Object Tag Assignment screen can be accessed by right-clicking on an agent in the Object Group Tree and selecting “Tags.” For more information about accessing the Object Tag Assignment screen, please refer to section 11.1.

To create a new tag, continue to the Select Tag dialog screen by clicking the “Add Tag” button near the top of the Object Tag Assignment dialog screen. The Select Tag dialog will appear.

Select Tags

Q Search

Select	Tag Name	Description
<input type="checkbox"/>	another tag	This is another tag
<input type="checkbox"/>	jovowashere	
<input type="checkbox"/>	myTag	my description
<input type="checkbox"/>	newTag	A new description.
<input type="checkbox"/>	newtag3	newtag3 description
<input type="checkbox"/>	newtag4	newtag4 description
<input type="checkbox"/>	testTag	This is a test tag.

Create New Tag

AddCancel

Figure 172: Select Tags dialog screen

From the Select Tag dialog screen, click the Create New Tag button on the lower-left corner of the dialog screen to continue to the Create/Edit Tag screen.

Create/Edit Tag

Tag Name:

Description:

OK Cancel

**Figure 173: Create/Edit Tag dialog screen**

The Create/Edit Tag dialog screen is comprised of two primary sections:

- **Tag Name (Required):** The desired name which you will associate to the newly created tag. This name will show in the Select Tag dialog screen.
- **Description (Optional):** The desired description which you will associate to the newly created tag. This description will show in the Select Tag dialog screen.

Once you have populated the fields of the Create/Edit Tag dialog screen, click Ok to complete the tag creation. The tag will now show in the Select Tag dialog screen.

Create/Edit Tag

Tag Name:

Description:

OK Cancel

**Figure 174: Create/Edit Tag dialog screen**



Select Tags

Q

Search

Select	Tag Name	Description
<input type="checkbox"/>	another tag	This is another tag
<input type="checkbox"/>	jovowashere	
<input type="checkbox"/>	myTag	my description
<input type="checkbox"/>	newtag3	newtag3 description
<input type="checkbox"/>	newtag4	newtag4 description
<input type="checkbox"/>	tagTest	This is a test of the create tag function.
<input type="checkbox"/>	testTag	This is a test tag.

Create New Tag

Add

Cancel

**Figure 175: Select Tags dialog screen (new tag)**

The newly created tag can be assigned to a Cimtrak™ Agent from the Select Tag dialog screen. For more information about assigning a tag to a Cimtrak™ Agent, please refer to section 11.2.

#### 8.4. DELETING TAGS

A tag can be disassociated from a CimTrak™ Agent through the Object Tab Assignment Dialog screen. The Object Tag Assignment screen can be accessed by right-clicking on an agent in the Object Group Tree and selecting “Tags.” For more information about accessing the Object Tag Assignment screen, please refer to section 11.1.

To disassociate a tag from a CimTrak™ Agent, click the Delete button that is associated with the tag that you wish to disassociate.

Object Tag Assignments

+ Add Tag

Q

Search

Tag Name	Description	Delete
newTag	A new description.	<div><div>×</div>Delete</div>
PCI E-Commerce		<div><div>×</div>Delete</div>
Tag 2	A new description.	<div><div>×</div>Delete</div>

Close

**Figure 176: Object Tag Assignments dialog screen (new tag assigned)**

Upon clicking the Delete button of an associated tag, the tag will be disassociated from the Cimtrak™ Agent and the tag will no longer be shown in the Object Tag Assignments dialog screen.

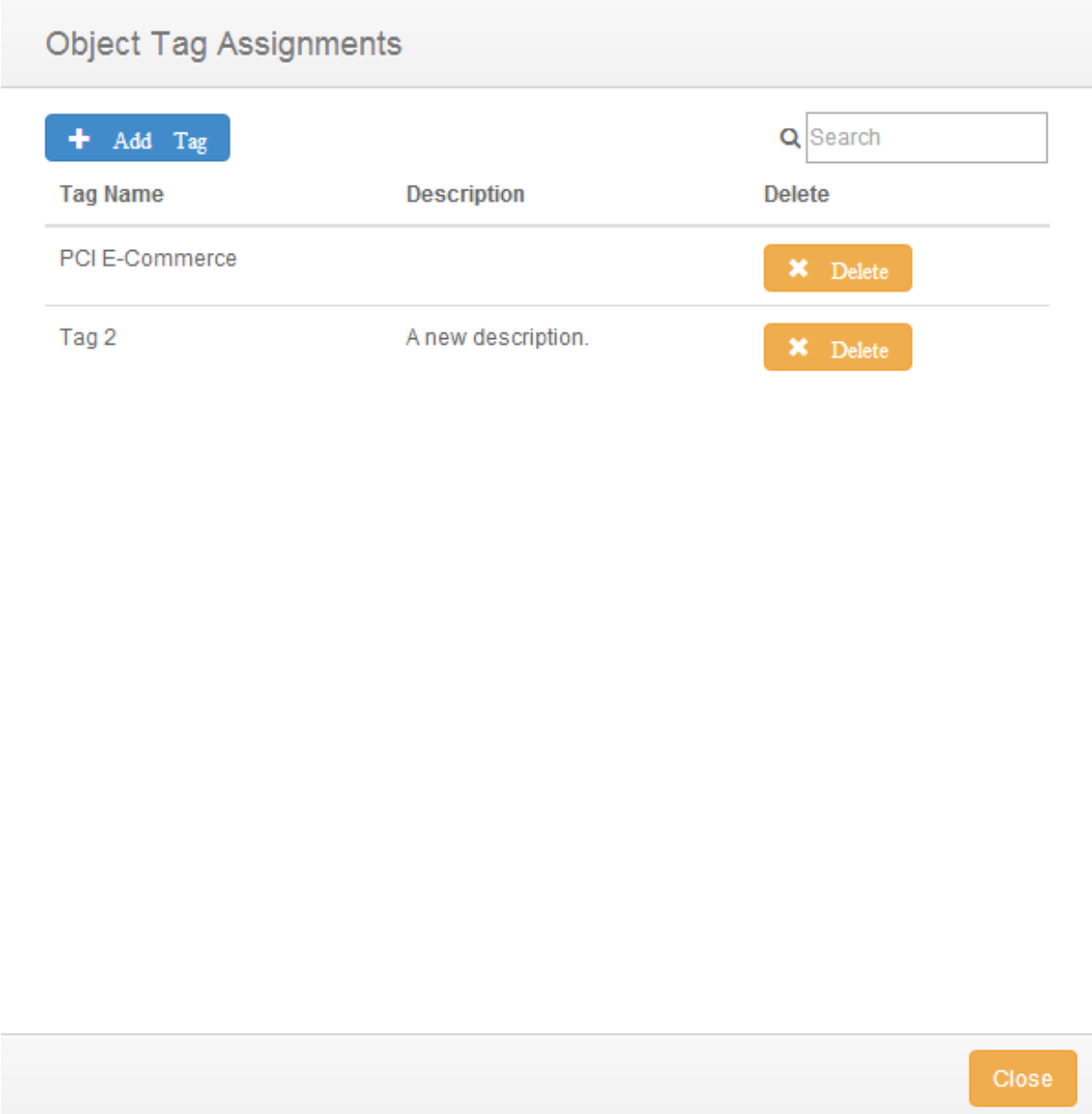


Figure 177: Object Tag Assignment dialog screen (tag deleted)

### 9.1. ACCESSING CIMTRAK™ REPORTING

Authorized CimTrak™ Administrators, Users, and Auditors have the capability to execute and download reports to display audit log and event information. Reports can be executed via the CimTrak™ Web Management Console Graphical User Interface or using the CimTrak™ Command Line Tool. See section **Error! Reference source not found.** for information explaining running reports from the Command Line Tool.

Reports are accessible for each level of Object listed in the Web Management Console's Object Group Tree. Information on accessing CimTrak™ Reports based on the Object level is as follows. Executing each of these methods will display the corresponding Available Reports dialog.

#### **CimTrak™ Master Repository:**

- On the Web Management Console Menu Bar click **Reports**→ **View Reports**

#### **CimTrak™ Area:**

- Right-click on the Area name in the Object Group tree and select Reports in the context menu.

#### **CimTrak™ File System/Network Device Agent:**

- Right-click on the CimTrak™ Agent name in the Object Group tree and select Reports in the context menu.

#### **CimTrak™ Object Group:**

- Right-click on the Object Group name in the Object Group tree and select Reports in the context menu.

#### **CimTrak™ Document Control:**

- Right-click on the Document Control name in the Object Group tree and select Reports in the context menu.

Additionally, other CimTrak™ components not listed execute reports using the methods outlined above.

Reports run or downloaded for a selected Object level show results for all children object of the corresponding level. For instance, reports run or downloaded at the Master Repository level display information associated to all children Objects including:

- **CimTrak™ Master Repository**
- **All CimTrak™ Areas**

- **All CimTrak™ File System/Network Device Agents**
- **All CimTrak™ Object Groups**
- **All CimTrak™ Document Controls**

Reports run at an Area Level will display information associated to all children Objects of the specified Area including:

- **Specified CimTrak™ Area**
- **CimTrak™ File System/Network Device Agents contained in the specified Area**
- **CimTrak™ Object Groups contained in the specified Area**
- **CimTrak™ Document Controls contained in the specified Area**

Reports run at an Agent Level will display information associated to all children Objects of the specified Agent including:

- **Specified CimTrak™ File System/Network Device Agent**
- **CimTrak™ Object Groups contained in the specified CimTrak™ Agent**
- **CimTrak™ Document Controls contained in the specified CimTrak™ Agent**

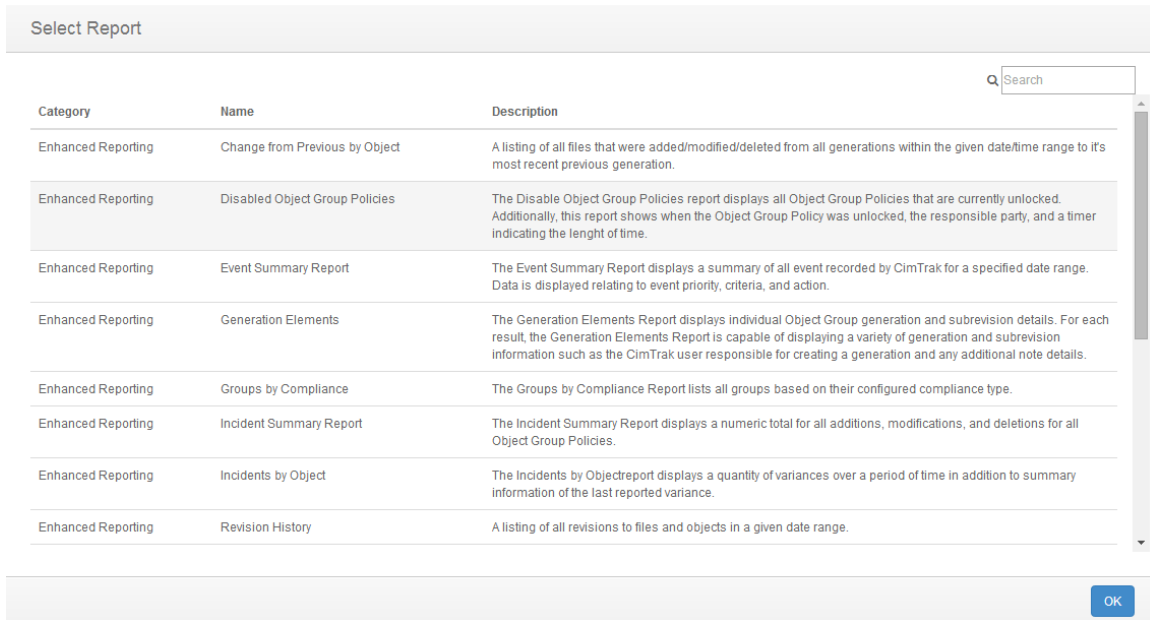
Reports run at an Object Group Level will only display information for the selected Object Group. Reports run at a Document Control level only display information for the selected Document Control.

The Available Reports dialog is explained in section 9.1.2.

#### **9.1.1. NAVIGATING THE AVAILABLE REPORTS DIALOG AND EXECUTING REPORTS**

Authorized CimTrak™ Administrators, Users, and Auditors have the capability to execute and download reports to display audit log and event information. Executing reports from the Web Management Console is performed using the Available Reports dialog.

Reports are accessible for each level of Object listed in the Web Management Console's Object Group Tree. Information on accessing CimTrak™ Reports based on the Object level is explained in section 9.4.



**Figure 178: Available Reports dialog (Master Repository Level)**

The Available Reports dialog displays all reports available for the selected Object level. Each report is classified into a general level or can be queried to match a specific tag. For more information on tags, refer to section 0.

Reports included in the CimTrak™ Reports level are used to audit CimTrak™ Web Management Console and Master Repository health, access, and user accounts. Reports included in the Enhanced Reporting level are used to audit change events detected (and optionally remediated) by CimTrak™. Details of these associated reports are explained in a section 9.1.2.1.

To execute a report navigate the Available Reports dialog to find the intended report. Select the report by clicking it once and then clicking the Generate Report button. The selected report will display.

CimTrak™ support staff has the capability to generate reports to perform custom functions for customer-specific requests. Additionally CimTrak™ Administrators with a programming background can modify reports. Generally CimTrak™ Reports consist of embedded HTML, SQL, JavaScript and LUA. To download the reports unexecuted code, navigate the Available Reports dialog to find the intended report. Select the report by clicking it once and then clicking the Download button. The Save As dialog will display. Select the location to save the report to. Once the report is modified it must be uploaded to the Master Repository. Uploading reports to the Master Repository is described in a section 9.6.

***When executing some reports a parameters dialog will display. The Parameters dialog allows for the specification of report parameters such as the date range, private key, chart type, and***

***optional query criteria. Populate the parameters dialog with appropriate information relating to the intended report criteria.***

### Report - Incident Summary Report

The Incident Summary Report displays a numeric total for all additions, modifications, and deletions for all Object Group Policies.

Start Date/Time:

End Date/Time:

Chart Type:

Pie Chart

Generate Report

OK

**Figure 179: Report Parameters dialog**

Once the report parameters are specified and the Continue button is clicked the selected report will generate.





## Incident Summary Report

All Object Groups: TSS-9910



Incident Count	Description	Response
55	Service Changed	Baseline Updated
20	*File Read	*NA
4	File Deleted	Replaced from Repository
3	File Modified	Replaced from Repository
2	Device Configuration Changed	Pending User Approval
1	File Changed	Baseline Updated
1	File Added	File Removed and Stored
1	Directory Added	Directory Removed
1	User Changed	Baseline Updated
1	File Added	Baseline Updated

aboutblank

6/14/2011

Figure 181: Sample CimTrak™ Report (Page 2 of 2)

***CimTrak™ Utilizes Microsoft Windows Internet Explorer installed on the Web Management Console's operating system. Graphical information will not display in Internet Explorer versions less than 8.0.***

#### 9.1.1.1. EXPLAINING AVAILABLE CIMTRAK™ REPORTS

Authorized CimTrak™ Administrators, Users, and Auditors have the capability to execute and download reports to display audit log and event information. Executing reports from the Web Management Console is performed using the Available Reports dialog.

Reports are accessible for each level of Object listed in the Web Management Console's Object Group Tree. Information on accessing CimTrak™ Reports based on the Object level is explained in section 9.4.

General Reports are contained in the CimTrak™ Reports and Enhanced Reporting Report Groups. Expanding Report Groups is possible by clicking the corresponding "+". Clicking the corresponding "-" will collapse the selected Report Group.

#### **Enhanced CimTrak™ Reports:**

- **Diagnostic Analysis:** *The Diagnostic Analysis is intended for support purposes to determine database availability/integrity, version information, process information, incident totals.*
- **Object Group Configuration:** *The Object Group Configuration report displays configuration settings for all Objects in the Object Group tree.*
- **Active User Listing:** *The Active User Listing Report lists all CimTrak™ users that are currently active.*
- **Added User Listing:** *The Added User Listing Report lists all added CimTrak™ users that are currently active.*
- **Deleted User Listing:** *The Deleted User Listing Report lists all deleted CimTrak™ users.*
- **Failed Logon Attempts:** *The Failed Logon Attempts Report provides a detail listing of failed logon attempts over a user specified period of time.*
- **Locked Out Users:** *The Locked Out Users Report provides a detailed listing of all locked out CimTrak™ user accounts.*
- **Successful Logons (Administrators):** *The Successful Logons (Administrators) Report provides a detailed listing of successful authentications with the CimTrak™ Master Repository by CimTrak™ user accounts.*
- **Successful Logons (All Users):** *The Successful Logons (All Users) Report provides a detailed listing of successful authentications with the CimTrak™ Master Repository by CimTrak™ user accounts.*
- **Successful Logons (Auditors):** *The Successful Logons (Auditors) Report provides a detailed listing of successful authentications with the CimTrak™ Master Repository by CimTrak™ user accounts.*
- **Successful Logons (Installers):** *The Successful Logons (Installers) Report provides a detailed listing of successful authentications with the CimTrak™ Master Repository by CimTrak™ user accounts.*
- **Successful Logons (Other Users):** *The Successful Logons (Other Users) Report provides a detailed listing of successful authentications with the CimTrak™ Master Repository by CimTrak™ user accounts.*

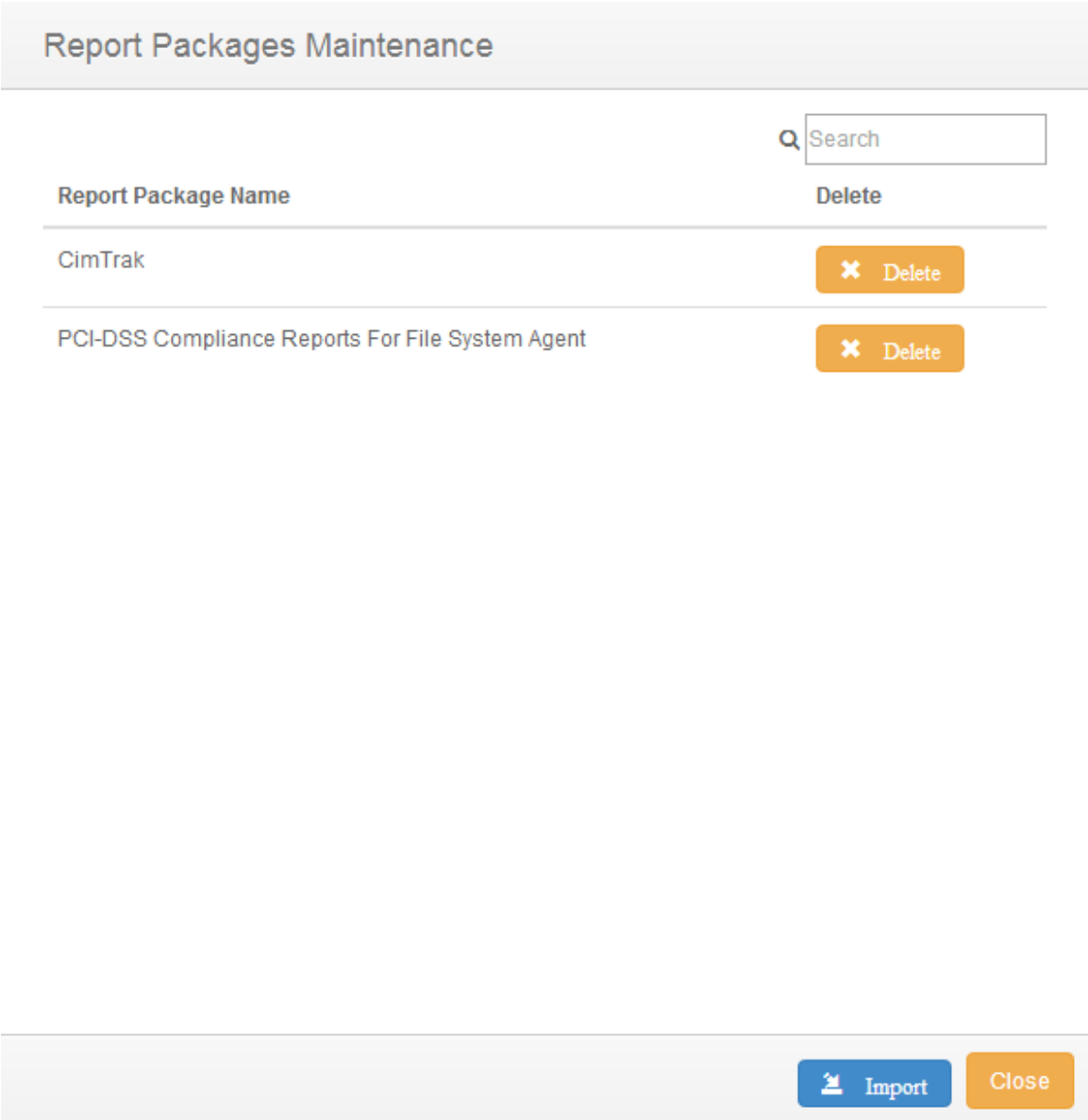
### **Enhanced Reporting:**

- **Disabled Object Group Policies:** *The Disabled Object Group Policies report displays all Object Group Policies that are currently unlocked. Additionally, this report shows when the Object Group Policy was unlocked, the responsible party, and a timer indicating the length of time.*
- **Event Summary Report:** *The Event Summary Report displays a summary of all events recorded by CimTrak™ for a specified date range. Data is displayed relating to event priority, criteria, and action.*
- **Generation Elements:** *The Generation Elements Report displays individual Object Group generation and sub-revision details. For each result, the Generation Elements Report is capable of displaying a variety of generation and sub-revision information such as the CimTrak™ user responsible for creating a generation and any additional note details.*
- **Groups by Compliance:** *The Groups by Compliance Report lists all groups based on their configured compliance type.*
- **Incidents by Object:** *The Incidents by Object report displays a quantity of variances over a period of time in addition to summary information of the last reported variance.*
- **Incident Summary Report:** *The Incident Summary Report displays a numeric total for all additions, modifications, and deletions for all Object Group Policies.*
- **Variance by Quantity:** *The Variance by Quantity Report displays a total of Object Group contents that have been added, modified, and/or removed from the monitored system.*
- **Variance Detail Report:** *The Variance Detail Report displays Object Group contents that have been added, modified, and/or removed from the monitored system. For each result, the Variance Detail Report is capable of displaying a variety of forensic-assisting information such as the operating system user responsible for the change, the responsible process, and associated change details.*
- **Variance Summary Report:** *The Variance Summary Report displays Object Group contents that have been added, modified, and/or removed from the monitored system. For each result, the Variance Detail Report is capable of displaying a variety of forensic-assisting information such as the operating system user responsible for the change and the responsible process.*
- **Variance Window Report:** *The Variance Window Report calculates the quantity of detected intrusions on locked objects during a specified period of time.*
- **Baseline Comparison Report:** *Only available at the Object Group Level, the Baseline Comparison report evaluates files/directories contained in one object group against the object group specified. The Baseline Comparison report requires that the original, authoritative baseline Object Group has the Audit Baseline Compliance Flag selected.*

## **9.2. WORKING WITH CIMTRAK™ REPORT PACKAGES**

Authorized CimTrak™ Administrators have the capability to add additional report packages to the CimTrak™ Master Repository. Additional report packages are often distributed with additional CimTrak™ components.

To add additional report packages, log into the CimTrak® Web Management Console using an Administrator account. Navigate to the Report Package Manager by right-clicking the Master Repository in the Object Group Tree and selecting “Report Packages . . .”



**Figure 182: Report Packages dialog**

By default, the CimTrak™ reporting package is installed. Click the Add button to navigate the Web Management Console host file system to select additional report packages to install. Select the appropriate report package and then click

Open. The selected report package will now be displayed in the Report Packages dialog. Click the OK button to complete the report package installation.

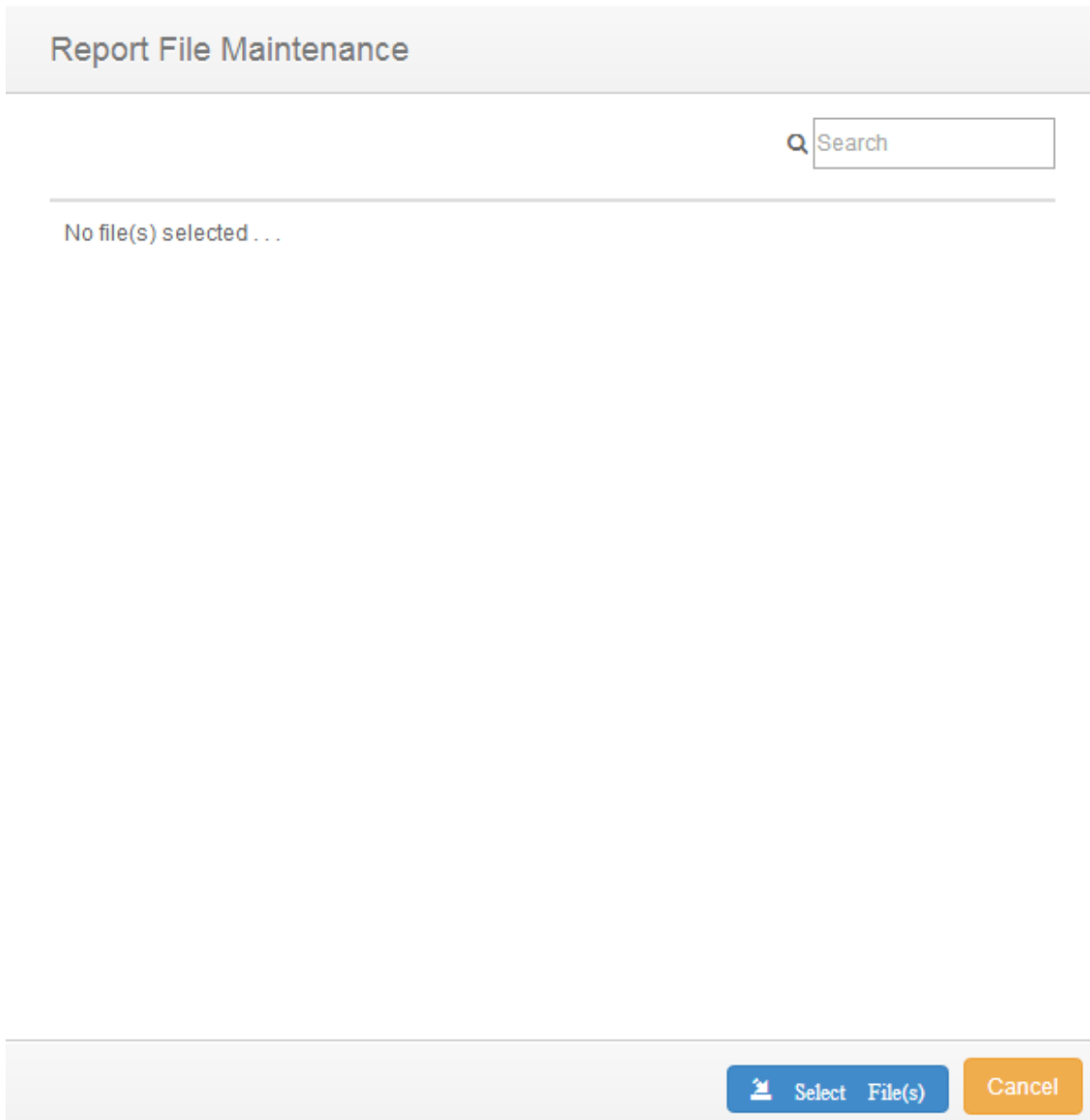
Removing a report package is achieved by selecting the Report package name in the Report Packages dialog and then clicking the Remove button. Click the OK button to complete the report package removal.

***Additional report packages may be available in your region. Contact an authorized CimTrak™ sales representative to acquire additional reporting packages.***

### **9.3. UPLOADING ADDITIONAL CIMTRAK™ REPORTS**

Authorized CimTrak™ Administrators have the capability to add additional individual reports to the CimTrak™ Master Repository. Additional reports are often distributed with additional CimTrak™ components.

Log into the CimTrak® Web Management Console using an Administrator account. Navigate to the Report File Upload Manager by right-clicking the Master Repository in the Object Group Tree and then selecting “Upload Report File . . .” The Report File Maintenance dialog will display.



**Figure 183: Report File Maintenance dialog screen**

To upload a Report File, click the “Select File(s)” button. The Open dialog will show.

Browse the Web Management Console’s host operating system and select the report to upload. Click Open to upload the report to the Master Repository. Click Cancel button to abort the upload process.

### **10.1. ACQUIRING ACCESS TO AN ADDITIONAL REPOSITORY.**

The Web Management Console can display more than one repository. Configuring an additional repository can be done by a user that has object creation permission on the primary repository.

#### **10.1.1. CREATE AN API KEY ON THE REMOTE REPOSITORY.**

Logon to the remote repository as a user with object creation permission on the repository. Open the repository properties dialog. Click the Repository API Key tab. Click the “Generate API Key for this Repository” button and the dialog shown below pops up. Type a description for the API key in the text box and then click the “Generate API Key” button.

An API key with the entered description will show up in the Repository API Key tab. This API Key will be entered into the other repository.

#### **10.1.2. ADD THE API KEY TO THE LOCAL REPOSITORY**

Logon to the local repository as a user with object creation permissions. Open the repository properties dialog. Click the Cluster Settings tab. Click the “Add CimTrak Repository API Key” button. The dialog below will pop up.

In the API Key text box, enter the API key generated for the remote repository. Add a description for the remote repository in the Repository Display Name box. Enter the IP address or FQDN for the App server used to access the remote repository in the App Server IP/FQDN box. Enter the App Server listening port, Repository Server IP/FQDN, and the Repository Server port in the boxes provided. If SSL (https) is used to access the App Server, check the “Use SSL” check box. Once this information is entered, click the “Add Cluster Entry” button to add the API key to the local repository's cluster. It should then show up on the Cluster Settings tab as shown below.

#### **10.1.3. CONFIGURING THE MULTI-REPOSITORY DISPLAY**

Clicking the “OK” button on the repository properties dialog closes it. The contents of the object tree pane has changed. It now has two top level nodes in addition to the repository node. The new node at the top is “Consolidated View” and the other additional node is the added remote repository (using the display name entered in the “Add Repository API Key to Cluster” dialog). Under the added repository node are the area, agent, and object group structure from the remote repository.

The Consolidated View node will contain all of the areas, agents, and object groups from both repositories. When this node is selected, the dashboard widgets will report data for all of the connected repositories. The display of the node structure can be configured. Right-clicking one of the top-level nodes presents the “Change View” option. The “Change View” sub-menu has the options, “Custom”, “Operating System”, “IP Range”, and “Tags”.

The view option selected determines how the agent and area nodes are grouped under the repository nodes as well as the consolidated view node. The “Custom” view option is the display mode that shows up by default when multiple repositories get configured. The “Operating System” view option adds second level nodes for each operating system that the agents are running on, ie. “Windows”, “Linux”, etc. and the agents from each repository are grouped by the operating system that they run on.

The “IP Range” view option groups the agents by the IP address range (defined by the first 2 octets of the IP address ie 192.168.xxx.xxx) of the machines that the agents run on.

The “Tags” view groups the agents by the tags assigned to the agents.





### A.1 CIMTRAK™ USER GUIDANCE DOCUMENTATION HISTORY

The following table outlines the history of this documentation.

Date	Version	Editor	Modification
15 June 2011	DOC_2.0.0	David Wheeler, CIMCOR™ Technical Support	Document Creation
5 June 2011	DOC_2.0.1	Sam Conley CIMCOR™ Support Engineer	Minor editing
5 August 2014	DOC_2.1.0	Ryan Rutkin CIMCOR™ Software Engineer	Complete Document Overhaul
1 April 2013	DOC_3.0.0	Sam Conley CIMCOR™ Technical Support	Document Update
2 Feb 2017	DOC_3.0.1	Sam Conley, CIMCOR Technical Support	Document Upgrade
5 Feb 2018	DOC_3.0.2	Richard Slaughter CIMCOR™ Software Engineer	Document Update

Table 3: Document Versioning

.

Device Type	Communication Options	Detection Options	Configuration Transfer Options
Cisco IOS	SSH Telnet SNMPv3 SNMPv2c	Polling SNMPv3 SNMPv2c	SCP TFTP
Cisco ASA	SSH Telnet	Polling	SCP TFTP
Cisco PIX	SSH Telnet	Polling	SCP TFTP
Juniper ScreenOS	SSH Telnet	Polling	SCP TFTP
Juniper JunOS	SSH Telnet	Polling	SCP TFTP

Table 2: Network Device Communication and File Transfer Protocols

Additional supported network devices may be available in your region. Contact an authorized CimTrak™ Sales Representative for more information.

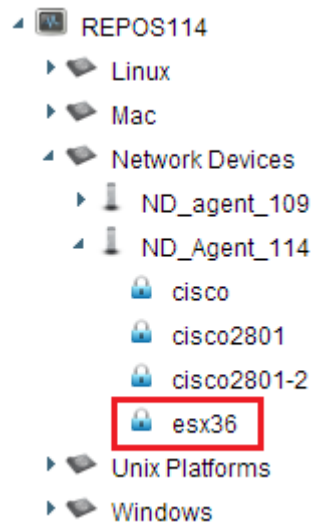


***Monitoring and communicating with Cisco IOS devices supporting SNMPv2c or SNMPv3 requires additional configuration on the monitored network device. See a subsequent section for configuration details.***

Populating the Network Device dialog and clicking the OK button results in the Object Group Properties dialog to display. To abort the Network Device Configuration click the Cancel button.

To edit an Object Group Watch Policy, select the Object Group Policy to modify by right-clicking its name in the Object Group Tree. Select **Properties** in the Context menu. The Object Group Properties dialog will display.

Once the Object Group has been created it will display in the CimTrak™ Web Management Console's Object Group Tree.



**Figure 110: CimTrak™ Web Management Console's Object Group Tree Showing Object Groups**

To enable monitoring of the Object Group it must be “locked”. Detailed information about creating Object Group Watch Policies and enabling/disabling monitoring is explained in subsequent sections.

#### **6.1.5.3.1. OBJECT GROUP PROPERTIES**

The process of creating a new or editing an Object Group Watch Policy can be initiated by selecting the Network Device Agent of the system to monitor by clicking it once in the Web Management Console's Object Group Tree, clicking the “New” drop-down button in the Menu Bar, followed by Object Group. The Object Group Properties dialog will display.

To edit an Object Group Watch Policy, select the Object Group Policy to modify by right-clicking its name in the Object Group Tree. Select **Properties** in the Context menu. The Object Group Properties dialog will display.

The Object Group Properties dialog is comprised of several sections. Each of these sections has specific functionality relating to the monitoring performed by the Network Device Agent.

Object Group Properties

PolicyAttributes

Location

Description

Date Put In Service

Contact

URL

Location

Description

2013-09-10 14:59:13

Name of Contact

Notes

Require Notes On Lock

Number of Intrusions to Keep

250

Number of Revisions to Keep

250

Events To Keep (0=no limit)

250

Events

Keep Intrusion Size (in KB)

500

Warn if Unlocked (in minutes)

0

Watched in this group

Watched elsewhere

OKCancel

Figure 111: Cimtrak™ Network Device Object Group Properties (Attributes Tab)

- Object Information
- Private Key Implementation
- Monitoring Information
- Operating System Tree
- Watch Properties

**Network Device Agent Object Information:**

Object Information provides CimTrak™ Users and Administrators detailed information pertaining to the Object Group Watch Policy. The “Object Group Name” is the only required field. Object Group Names must be unique and may contain between 1 and 49 characters.

Location

Description

Date Put In Service

Contact

URL

Location

Description

2013-09-10 14:59:13

Name of Contact

Notes

Require Notes On Lock

Figure 112: Network Device Agent Object Information

**Location:** *Optional Object Group Location information.*  
**Description:** *Optional Object Group Description information.*  
**Date Put in Service:** *Optional Date and Time associated with the in-service date of the Object Group.*  
**Contact:** *Optional Contact information associated with the Object Group.*  
**URL:** *Optional URL information associated with the Object Group.*  
**Notes:** *Optional dialog to enter administrative notes associated with the Object Group.*

Optionally, the Object Group Watch Policy has the capability to require CimTrak™ Users and Administrators to enter notes when enabling monitoring of the Object Group Watch Policy. Enabling of required notes is performed by selecting the Require Notes on Lock checkbox.

### **Monitoring Information:**

**Number of Intrusions to Keep:** *Number of added files/configurations to keep in the Change Log. A zero placed in this field indicates unlimited changes will be stored. Maximum accepted value of 10,000 changes.*

**Keep Intrusion Size (in KB):** *The maximum file size an added file can be for it to be stored in the Change Log. Files exceeding this change size limit are still detected but cannot be compared or retrieved. Maximum accepted value of 4,194,304 KB.*

**Number of Revisions to Keep:** *Number of revisions to keep for each change to files and configurations monitored by the Object Group. A zero placed in this field indicates unlimited changes will be stored. Maximum accepted value of 10,000 revisions*

**Warn if Unlocked (in minutes):** *Generate a notice if monitoring of the Object Group has been disabled for more than the indicated time. A zero placed in this field disables the warning. Maximum accepted value of 10,000 minutes.*

**Number of Events to Keep:** *Quantity or Days to store Object Group Event Log audit records. Maximum accepted value of 10,000 events.*



***Storing an unlimited number of events, revisions, or changes has the potential to exhaust all available disk space on the Master Repository and degrade system performance.***

Number of Intrusions to Keep	<input type="text" value="250"/>	Number of Revisions to Keep	<input type="text" value="250"/>	Events To Keep (0=no limit)	<input type="text" value="250"/>	Events <input type="button" value="▼"/>
Keep Intrusion Size (in KB)	<input type="text" value="500"/>	Warn if Unlocked (in minutes)	<input type="text" value="0"/>			

**Figure 113: Network Device Agent Monitoring Information**

### **Operating System Tree**

The Operating System Tree, located at the lower left corner of the Object Group Properties dialog, contains a listing of all files, folders, and operating system configurations that can be monitored by the CimTrak™ Network Device Agent. The contents of the Operating System Tree are system specific. Additionally,

external CimTrak™ Plug-ins attached to the Network Device Agent will appear in the Operating System Tree.

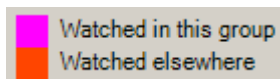


**Figure 114: Cisco IOS Operating System Tree**

Selecting data to monitor is accomplished by checking the checkbox next to the system component. The contents of the Operating System Tree can be expanded or collapsed by clicking the ► or ◄ symbols corresponding with each monitor type. Selecting any monitor data results in the Watch Properties dialog to display. See a subsequent section for more information on setting Watch Properties.



***Content that is monitored in the current Object Group is displayed in the File System Tree in a pink font color. Content that is monitored elsewhere is displayed in a orange font color.***



**Figure 115: Watch notifications**

#### **Microsoft Windows Network Device Agents have the capability to monitor:**

**Drivers:** *Drivers are specialized programs designed to run in the background of a system and to control specific hardware. This feature allows security professionals the capability to monitor drivers for changes, additions, or deletions. Remediation capability is not available for monitoring of system drivers. The recommended monitoring mode is “Update Baseline”. This feature supports polling detection.*

**Installed Software:** *Installed Software monitoring detects any software that has been installed using a standard installation tool. This mode displays any software that is registered in Microsoft Windows to display in the “Add/Remove Programs” dialog. This feature allows security professionals the capability to monitor if new or additional software has been installed or uninstalled. Remediation capability is not available for monitoring of installed software. The recommended monitoring mode is “Update Baseline”. This feature supports polling detection.*

**Network Shares:** *Monitoring of Network Shares allows security professionals the capability to monitor the share settings associated with files and folders on a Windows operating system. This mode allows for remediation of any detected changes. The recommended monitoring mode is “Restore from Repository”. This feature supports polling detection.*

**Registry:** *Windows Registry monitoring allows security professionals the capability to define a preset list of registry keys to monitor. CimTrak™ will detect any modifications to this preset list of keys or values. The*

*recommended monitoring mode is “Restore from Repository”. This feature supports polling or real-time detection.*

**Security Policy:** *Monitoring of the local Security Policy allows security professionals the capability to monitor the settings associated with the local security policy. Local security policies are relevant even if the system is attached to a domain since the local security policies are executed before group policies. Locking the Security Policy helps ensure that the intended local security policies of an organization are maintained. The recommended monitoring mode is “Update Baseline”. This feature supports polling detection.*

**Services:** *Services are specialized programs designed to run in the background of a system. This feature allows security professionals the capability to monitor when new or additional services have been started or configurations of existing services have been modified. The recommended monitoring mode is “Update Baseline”. This feature supports polling detection.*

**System Groups:** *Monitoring of local system groups allows security professionals the capability to detect changes to all local user groups existing on the monitored system. CimTrak™ detects when groups are added, deleted, or modified. The recommended monitoring mode is “Update Baseline”. This feature supports polling detection.*

**System Users:** *Monitoring of local system users allows security professionals the capability to detect when local user accounts are added, deleted, or modified on the system. Using this feature is important even if the system is attached to a domain as additional or modified local user accounts can create a system vulnerability. The recommended monitoring mode is “Update Baseline”. This feature supports polling detection.*

**Local File System:** *Monitoring of the local file system will detect (and optionally remediate) any addition, deletion, or modification to files and folders on the monitored system. This feature supports polling or real-time detection.*

**Network File System:** *Using the optional “Network Drive Enabler” allows for the detection (and optionally remediation) of any addition, deletion, or modification to files and folders to monitored network share data. This feature supports polling detection.*

## **Linux, UNIX, and Macintosh Network Device Agents have the capability to monitor:**

**System Groups:** *Monitoring of local system groups allows security professionals the capability to detect changes to all local user groups existing on the monitored system. CimTrak™ detects when groups are added, deleted, or modified. The recommended monitoring mode is “Update Baseline”. This feature supports polling detection.*

**System Users:** *Monitoring of local system users allows security professionals the capability to detect when local user accounts are added, deleted, or modified on the system. Using this feature is important even if the system is attached to a domain as additional or modified local user*

accounts can create a system vulnerability. The recommended monitoring mode is “Update Baseline”. This feature supports polling detection.

**Local File System:** Monitoring of the local file system will detect (and optionally remediate) any addition, deletion, or modification to files and folders on the monitored system. This feature supports polling or real-time detection.

**Network File System:** Monitoring of mounted shares allows for the detection (and optional remediation) of any addition, deletion, or modification to files and folders on monitored network shares. This feature supports polling detection.

### **Watch Properties**

The Watch Properties section shows any currently monitored files, folders, and configurations. Additionally, excluded or included paths and files are displayed. The Watch Properties are explained in detail in subsequent sections.

#### **6.1.5.3.2. WATCH PROPERTIES**

Selecting any object listed in the Object Group Properties File System Tree results in the Watch Properties dialog to display.

Watch Properties

When a change occurs

☐ Restore from Repository

☐ Log

☒ Update Baseline

☐ Prompt for Approval

Some software, such as backup utilities or virus detection software, modify various file attributes, which will signal an intrusion to CimTrak.

☒ Ignore Archive Flag

☐ Ignore Read-only Flag

☐ Ignore SACL

☐ Ignore DACL

☐ Ignore Owner Security

☐ Ignore Group Security

☐ Ignore Alternate Stream Data

☐ Ignore File Dates

Authoritative Copy

☒ Store authoritative copy of all files in the CimTrak Repository. This will allow CimTrak to restore files back to their original state.

☐ Don't Store authoritative copy

Event Detection Method

☐ Real-time Detection

☒ Poll Detection (interval)

☐ Poll at Specific Time (Local Time)

☐ Poll at Specific Time (Agent Time)

Poll Interval (Hours and Minutes)

02 : 00

Store Changes

☒ Store a copy of added/changed files

Other

☐ Log Reads

File Comparison Method

MD5

Connection Loss Strategy

☐ Wait for User Approval on Sync

Auto Exclude

Auto exclude files that have changed 0 times in 60 minutes (0 changes = disabled)

OK Cancel

**Figure 116: Watch Properties dialog**



The Watch Properties dialog allows for the configuration of detection and reaction parameters. The Watch Properties dialog is comprised of several different sections:

**Corrective Action**  
**Authoritative Copy**  
**File Comparison Method**  
**Store Changes**  
**Options**  
**Event Detection Method**  
**Connection Loss**  
**Auto Exclude**

These sections are explained in detail in subsequent sections. After completing the Watch Properties configuration click OK to accept the changes or Cancel to abort and discard the changes. The Watch Properties dialog will close and the Object Group Properties dialog will display showing the configured Watch Properties in the Watch Properties section.

Path	Object Type	Type	Store Files	Corrective Ac...	Detection	C
▲ /DeviceRoot (1 )						
/DeviceRoot	Directory	Watch	Yes	Update Basel...	Poll	M

**Figure 117: Watch Properties section showing monitored directory**

#### 6.1.1.5.2.1. CORRECTIVE ACTION

Defining the corrective action associated with a Network Device Agent Object Group Policy is accomplished through the Watch Properties dialog. CimTrak™ supports four primary modes of remediation when changes to modified

files/configurations are detected. Additionally, CimTrak™ has the capability to perform customized remediation actions.

Primary modes of remediation include:

**Restore from Repository:** *Stored authoritative (original) data files are used to restore files and folders that have been changed.*

**Log:** *All detected change events are only logged. No authoritative (original) file data is stored.*

**Update Baseline:** *Changes are allowed to occur. Each change results in an incremental backup being performed on the watch data. When applicable, previous baselines can be pushed back to the monitored system.*

**Prompt for Approval:** *Changes are allowed to occur. The CimTrak™ Administrator is given the option to allow or undo the detected changes.*

**Deny Access:** *Changes are not allowed to occur.*

Optionally, the Custom configuration mode exists allowing for any combination of the primary modes of remediation. For example, when a file is added the administrator may choose to update the baseline; when a file is deleted the administrator may choose to restore the file; when a file is modified the administrator may choose to log the change.

#### When a change occurs

- ☐ Restore from Repository
- ☒ Log
- ☐ Update Baseline
- ☐ Prompt for Approval
- ☐ Deny Access

**Figure 118: Corrective Action Properties**

Selection of the remediation mode is accomplished by selecting the corresponding radio button.

#### 6.1.1.5.2.2. AUTHORITY COPY

Depending on the Corrective Action used, CimTrak™ has the capability to alter the storage of Authoritative Copy data. The Authoritative Copy refers to a saved copy of “locked” file system/configuration data stored in the Master Repository for the purpose of restoring files to the last known approved state. Additionally, Authoritative Copy data can be used to compare the contents of monitored files

and configurations. Authoritative Copy data is stored in the Master Repository using the user configured cryptology and compressed.

#### Authoritative Copy

- ☐ Store authoritative copy of all files in the CimTrak Repository. This will allow CimTrak to restore files back to their original state.
- ☒ Don't Store authoritative copy

Figure 119: Authoritative Copy Parameter Settings



***The compression ratio used by CimTrak™ varies with the type of content being monitored (i.e., images, documents, text files). Generally, the authoritative copy data is stored with a 20-25% compression ratio.***

#### 6.1.1.5.2.3. FILE COMPARISON METHOD

Each file, folder, and configuration monitored by CimTrak™ has a calculated hash value stored in the CimTrak™ Master Repository. The File Comparison Method parameter setting allows for authorized CimTrak™ Administrators to modify the comparison algorithm used. By default the most powerful method is selected. The methods allowed vary based on the CimTrak™ Cryptology release.

#### File Comparison Method

MD5 ▼

Figure 120: File Comparison Method Parameter Settings

To change the File Comparison Method, select the method to use from the File Comparison Method dropdown.

#### 6.1.1.5.2.4. STORE CHANGES

Depending on the Corrective Action used, CimTrak™ has the capability to alter the storage of change data. Change data refers to a saved copy of modified file system/configuration data stored in the Master Repository for the purpose of compare the contents with the Authoritative Copy. Change data is stored in the Master Repository using the user configured cryptology and compressed.

#### Store Changes

- ☐ Store a copy of added/changed files

Figure 121: Store Changes Option Checkbox



***The compression ratio used by CimTrak™ varies with the type of change stored (i.e., images, documents, text files). Generally, the change data is stored with a 20-25% compression ratio.***

Selecting the checkbox labelled “Store Changes” will store the change data to the Master Repository using the user configured cryptology and compressed.

#### **6.1.1.5.2.5. AUTO EXCLUDE**

When creating an Object Group Watch Policy it is important to tune the configuration to exclude files that are dynamic and need to change. CimTrak™ has the capability to auto-tune the Watch Policy by automatically excluding file that change more times than the designated threshold and interval. The Auto Exclude threshold and interval is configured in the Network Device Agent Watch Properties dialog.



***The Auto Exclude feature should only be enabled during the initial Object Group Policy tuning process. Leaving this feature enabled indefinitely could result in CimTrak™ missing legitimate system changes.***

By default the Auto Exclude feature is disabled. To enable the Auto Exclude feature, specify the threshold by indicated the amount of times a file or configuration is allowed to change over a specified time in minutes.

##### **Auto Exclude**

Auto exclude files that have changed  times in  minutes (0 changes = disabled)

**Figure 122: Auto Exclude parameter settings**

Acceptable change values must be between 0 (disabled) and 1,000. The time value must be between 1 minute and 1,440 minutes.

#### **6.1.1.5.2.6. OPTIONS**

The CimTrak™ Network Device Agent Watch Properties has additional customization options available to reduce the number of detected false changes. These additional options are useful to allow CimTrak™ to function properly with backup utilities and source control utilities. Additionally options exist to enable additional monitoring capabilities. The Option settings are available in the Network Device Agent Watch Properties dialog.

Some software, such as backup utilities or virus detection software, modify various file attributes, which will signal an intrusion to CimTrak.

- |                                                         |                                                |
|---------------------------------------------------------|------------------------------------------------|
| <input checked="" type="checkbox"/> Ignore Archive Flag | <input type="checkbox"/> Ignore Read-only Flag |
| <input type="checkbox"/> Ignore SACL                    | <input type="checkbox"/> Ignore DACL           |
| <input type="checkbox"/> Ignore Owner Security          | <input type="checkbox"/> Ignore Group Security |
| <input type="checkbox"/> Ignore Alternate Stream Data   | <input type="checkbox"/> Ignore File Dates     |

**Figure 123: Options parameter settings**

Other

- ☐ Log Reads

**Figure 124: Log Reads Parameter Checkbox**

Option parameter settings are enabled by clicking the corresponding checkbox. Options are disabled when unchecked. The Options parameter settings allow for the custom configuration of the following:

- Ignore Archive Flag: When checked the CimTrak™ Network Device Agent will ignore any changes that occur to the archive flag.
- Ignore Read-only Flag: When checked the CimTrak™ Network Device Agent will ignore any changes that occur to the Read-only flag.
- Log Reads: When checked CimTrak™ has the capability to monitor specific files and folders for any form of access. Using this feature will generate audit events whenever a file is viewed or copied.



***Logging of reads requires the Network Device Agent Forensic Driver. This driver is installed during the installation of the Windows Network Device Agent.***

#### **6.1.1.5.2.7. EVENT DETECTION METHOD**

The CimTrak™ Network Device Agent has the capability to monitor Object Group Policies in real-time (when supported) or on a polling interval. Configuration of the Event detection method is available in the Network Device Agent Watch Properties dialog.

#### Event Detection Method

☐ Real-time Detection

☒ Poll Detection (interval)

☐ Poll at Specific Time (Local Time)

☐ Poll at Specific Time (Agent Time)

#### Poll Interval (Hours and Minutes)

02 : 00

Figure 125: Event Detection Method parameter settings

Available event detection methods include:

- **Real-time Detection:** *Real-time Detection will report detected changes immediately when they are performed. The configured remediation mode will automatically initiate immediately upon the detection of a change.*
- **Poll-based Detection:** *Poll-based Detection will report any changes that have occurred since the last poll-based scan. Acceptable values range between 0 (poll only when force-synced) and 1,440 minutes.*



***The Windows Network Device Agent Forensic Driver will not show forensic assisting information for changes detected using the Poll-based Detection.***



***Scheduled polling is accomplished by setting the Poll-based Detection interval to 0 and scripting the synchronization using the CimTrak™ Command Line Interface. These scripts can then be scheduled using Windows Task Scheduler or Linux/UNIX Cron jobs. The Command Line Interface is explained in section Error! Reference source not found..***

#### 6.1.1.5.2.8. CONNECTION LOSS

Occasionally the CimTrak™ Master Repository may lose connectivity with attached Network Device Agents due to network errors or mobile devices. When this occurs the option exists to automatically perform Object Group synchronization when the connection is re-established. Setting the Connection Loss settings are available through the Object Group Properties Watch Properties dialog.

#### Connection Loss Strategy

☐ Wait for User Approval on Sync

Figure 126: Connection Loss parameter settings

To enable synchronization after a connection loss, select the User Approval on Sync checkbox. To disable synchronization, de-select the User Approval on Sync checkbox.

When User Approval on Sync is enabled, the CimTrak™ Administrator is prompted for the desired action to take on detected changes made during the non-connectivity period. The CimTrak™ Administrator utilizes the Changes Pending Approval Web Management Console dialog to authorize or deny these changes. The Changes Pending Approval dialog is explained in a subsequent section.

The User Approval on Sync dialog has the following default and customizable settings for each of the following corrective actions:

- **Restore from Repository:** *Option can be enabled or disabled. By default this option is disabled.*
- **Log:** *Option is disabled by default and cannot be changed.*
- **Update Baseline:** *Option is disabled by default and cannot be changed.*
- **Prompt for Approval:** *Option is enabled by default and cannot be changed.*

#### 6.1.5.3.3. TUNING WATCH PROPERTIES

When an operating system folder or configuration is selected in the Object Group Properties dialog, all children files, folders, and configurations are also selected. Often certain files need to be excluded or included in the particular watch policy. CimTrak™ has the capability to create exclude or include rules for files, folders, and configurations. Creating these advanced rules is accomplished in the selected Object Group's Watch Properties. Accessing the Object Group Properties is accomplished during the creation or editing of an Object Group's Watch Policy. See section 6.1.5.3.2 for more information on creating Watch Policies.

Monitored folders, files, and configurations will display in the Object Group Properties Watch Properties section. Each displayed item will include the following information:

- **Path:** *The operating system location of the parent folder or configuration.*
- **Object Type:** *The Object Type being monitored (i.e. Directory).*
- **Type:** *Action performed by the Watch Property detail (i.e. Watch, Exclude, etc.).*
- **Store Files:** *Indication of whether or not Authoritative Copy data will be stored in the CimTrak™ Master Repository.*
- **Corrective Action:** *The Corrective Action chosen during the creation of the Object Group Watch Policy.*
- **Detection:** *Indication of the mode of detection (Real-time, Polling).*

- **Ignore Archive Flag:** *Indication of whether or not changes to the Archive Flag will be ignored.*
- **Ignore Read-only Flag:** *Indication of whether or not changes to the Read-only Flag will be ignored.*
- **Comparison Method:** *Displays the comparison method selected in the Object Group's Watch Properties.*
- **Quarantine:** *Indication of whether or not Change Data will be stored in the CimTrak™ Master Repository.*

Path	Object Type	Type	Store Files	Corrective Ac...	Detection	C
▲ /DeviceRoot (2 )						
/DeviceRoot	Directory	Watch	Yes	Update Basel...	Poll	M
[/Cc][li][Ss][Cc][Oo] [li][Oo][Ss]/	Regular Expr...	Exclude				

**Figure 127: Watch Properties section showing monitored data**

Each column of information can be sorted by column criteria by clicking once on the column title.

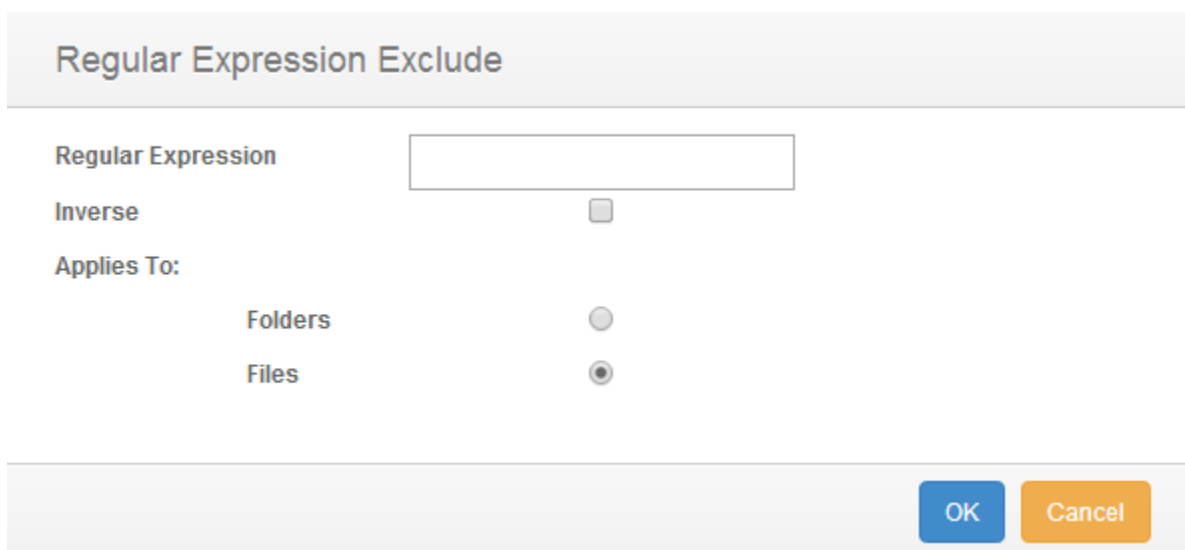
Right clicking on any item showing in the Watch Properties section results in a context menu to display showing additional configuration and navigation options. Context menu options include:

- **Edit Watch Properties:** *Modify the watch properties associated with the selected Watch data. Opens the Watch Properties dialog.*
- **Remove Watch:** *Disable the selected Watch data by unselecting it in the Object Group Properties dialog File System Tree.*
- **Add Regular Expression Exclude:** *Create customized excludes to prevent or enable of specific folder, file, or configuration criteria.*



#### 6.1.1.5.3.1 EXCLUDING AND INCLUDING USING REGULAR EXPRESSIONS

Occasionally a CimTrak™ Object Group Policy may need to exclude monitor or only monitor data based on file extensions, file names, folder names, configuration names, or various other types of information. Setting these custom watch rules is performed by creating Regular Express Exclude. The process of creating a Regular Expression Exclude is performed through the Add Regular Expression Exclude dialog accessed by right-clicking Watch data and then selecting Add Regular Expression Exclude from the context menu. Accessing the Object Group Properties is accomplished during the creation or editing of an Object Group's Watch Policy. See section 6.1.5.3.2 for more information on creating Watch Policies.



Regular Expression Exclude

Regular Expression

Inverse ☐

Applies To:

Folders ☐

Files ☒

OK Cancel

**Figure 128: Add Regular Expression Exclude dialog**

The Add Regular Expression Exclude dialog has the capability to exclude files and folders. Additionally, the Add Regular Expression Exclude dialog can create inverse regular expressions excludes to only monitor certain files or folders based on the criteria entered.

##### 6.1.1.5.3.1.1. EXCLUDING FOLDERS USING REGULAR EXPRESSIONS

The process of creating a Regular Expression Exclude is performed through the Add Regular Expression Exclude dialog accessed by right-clicking Watch data and then selecting Add Regular Expression Exclude from the context menu. Accessing the Object Group Properties is accomplished during the creation or editing of an Object Group's Watch Policy. See section 6.1.5.3.2 for more information on creating Watch Policies.

To create a Regular Expression folder exclude, enter the folder information to exclude (i.e. \temp). Ensure that the Folders radio button is selected and then click OK. Click Cancel to abort the changes and return to the Object Group Properties dialog. Clicking OK will automatically return to the Object Group Properties dialog. Note that the regular expression exclude is displayed in the Watch Properties data section.

Regular Expression Folder Excludes can become very complex. It is possible to create custom exclusions using regular expressions. For instance, a regular expression exclude can be created to ignore case:

#### **/Cisco IOS**

*can be entered as...*

**//[Cc][Ii][Ss][Cc][Oo] [Ii][Oo][Ss]//**

/DeviceRoot	Directory	Watch	Yes	Update Basel...	Poll
//[Cc][Ii][Ss][Cc][Oo] [Ii][Oo][Ss]//	Regular Expr...	Exclude			

**Figure 129: Regular Expression Folder Exclude**

To add additional Regular Express folder excludes, repeat the same steps. To remove Regular Expression Excludes, right-click on the Exclude information in the Watch Properties data section and then select Remove Exclude(s). When completed, click the OK button to save the changes. Click the Cancel button to abort the configuration and discard any changes.

#### **6.1.1.5.3.1.2. EXCLUDING FILES USING REGULAR EXPRESSIONS**

The process of creating a Regular Expression Exclude is performed through the Add Regular Expression Exclude dialog accessed by right-clicking Watch data and then selecting Add Regular Expression Exclude from the context menu. Accessing the Object Group Properties is accomplished during the creation or editing of an Object Group's Watch Policy. See section 6.1.5.3.2 for more information on creating Watch Policies.

To create a Regular Expression file exclude, enter the file type information to exclude (i.e. .log). Ensure that the Files radio button is selected and then click OK. Click Cancel to abort the changes and return to the Object Group Properties dialog. Clicking OK will automatically return to the Object Group Properties dialog. Note that the regular expression exclude is displayed in the Watch Properties data section.

Regular Expression Folder Excludes can become very complex. It is possible to create custom exclusions using regular expressions. For instance, a regular expression exclude can be created to ignore case:

## running-config

can be entered as...

```
[Rr][Uu][Nn][Nn][Ii][Nn][Gg]-[Cc][Oo][Nn][Ff][Ii][Gg]
```

/DeviceRoot	Directory	Watch	Yes	Update Basel...	Poll
[Rr][Uu][Nn][Nn][Ii][Nn][Gg]-[Cc][Oo][Nn][Ff][Ii][Gg]	Regular Expr...	Exclude			

**Figure 130: Regular Expression File Exclude**

To add additional Regular Express file excludes, repeat the same steps. To remove Regular Expression Excludes, right-click on the Exclude information in the Watch Properties data section and then select Remove Exclude(s). When completed, click the OK button to save the changes. Click the Cancel button to abort the configuration and discard any changes.

### 6.1.1.5.3.1.3. INVERSE EXCLUDING OF FOLDERS USING REGULAR EXPRESSIONS

The process of creating an Inverse Regular Expression Exclude is performed through the Add Regular Expression Exclude dialog accessed by right-clicking Watch data and then selecting Add Regular Expression Exclude from the context menu. Accessing the Object Group Properties is accomplished during the creation or editing of an Object Group's Watch Policy. See section 6.1.5.3.2 for more information on creating Watch Policies.

Inverse regular expressions can be used to "include" information to monitor. To create an Inverse Regular Expression folder exclude, enter the folder information to watch (i.e. \temp). Ensure that the Folders radio button and the Inverse checkbox are selected and then click OK. Click Cancel to abort the changes and return to the Object Group Properties dialog. Clicking OK will automatically return to the Object Group Properties dialog. Note that the Inverse regular expression exclude is displayed in the Watch Properties data section.

Inverse Regular Expression Folder Excludes can become very complex. It is possible to create custom inverse exclusions using inverse regular expressions. For instance, an inverse regular expression exclude can be created to ignore case:

## /Cisco IOS

can be entered as...

```
//[Cc][Ii][Ss][Cc][Oo] [Ii][Oo][Ss]//
```

/DeviceRoot	Directory	Watch	Yes	Update Basel...	Poll
//[Cc][Ii][Ss][Cc][Oo] [Ii][Oo][Ss]//	Inverse Regul...	Exclude			

**Figure 131: Regular Expression Folder Exclude (blue text)**

To add additional Inverse Regular Express folder excludes, repeat the same steps. To remove Inverse Regular Expression Excludes, right-click on the Exclude information in the Watch Properties data section and then select Remove Exclude(s). When completed, click the OK button to save the changes. Click the Cancel button to abort the configuration and discard any changes.

**6.1.1.5.3.1.4. INVERSE EXCLUDING OF FILES USING REGULAR EXPRESSIONS**

The process of creating an Inverse Regular Expression to include specified files or extensions is performed through the Add Regular Expression Exclude dialog accessed by right-clicking Watch data and then selecting Add Regular Expression Exclude from the context menu. Accessing the Object Group Properties is accomplished during the creation or editing of an Object Group's Watch Policy. See section 6.1.5.3.2 for more information on creating Watch Policies.

To create an Inverse Regular Expression file exclude, enter the file type information to exclude (i.e. .log). Ensure that the Files radio button and Inverse checkbox are selected and then click OK. Click Cancel to abort the changes and return to the Object Group Properties dialog. Clicking OK will automatically return to the Object Group Properties dialog. Note that the inverse regular expression exclude is displayed in the Watch Properties data section.

Inverse Regular Expression Folder Excludes can become very complex. It is possible to create custom exclusions using regular expressions. For instance, an inverse regular expression exclude can be created to ignore case:

**running-config**  
*can be entered as...*  
[Rr][Uu][Nn][Nn][Ii][Nn][Gg]-[Cc][Oo][Nn][Ff][Ii][Gg]

/DeviceRoot	Directory	Watch	Yes	Update Basel...	Poll
[Rr][Uu][Nn][Nn][Ii][Nn][Gg]-[Cc][Oo][Nn][Ff][Ii][Gg]	Inverse Regul...	Exclude			

**Figure 132: Regular Expression File Exclude**

To add additional Inverse Regular Express file excludes, repeat the same steps. To remove Inverse Regular Expression Excludes, right-click on the Exclude information in the Watch Properties data section and then select Remove Exclude(s). When completed, click the OK button to save the changes. Click the Cancel button to abort the configuration and discard any changes.

#### 6.1.5.4. SAVING OBJECT GROUP WATCH POLICIES TO TEMPLATES

Once an Object Group Watch Policy has been created it is possible to save the policy configurations to a template. Using a template can assist in creating identical watch data for other CimTrak™ Network Device Agents. See section 4.7 for more information on CimTrak™ Templates.

To create a template, right-click on the Object Group name in the CimTrak™ Web Management Console's Object Group Tree and then select Save to Template. The Save to Template dialog will display. Enter a unique name for the template. If you would like this template to be private to your CimTrak™ account be sure to select the Private option by selecting the Private checkbox. When completed entering the required information click the OK button. Click the cancel button to abort the template creation. A template name can be between 1 and 512 characters.

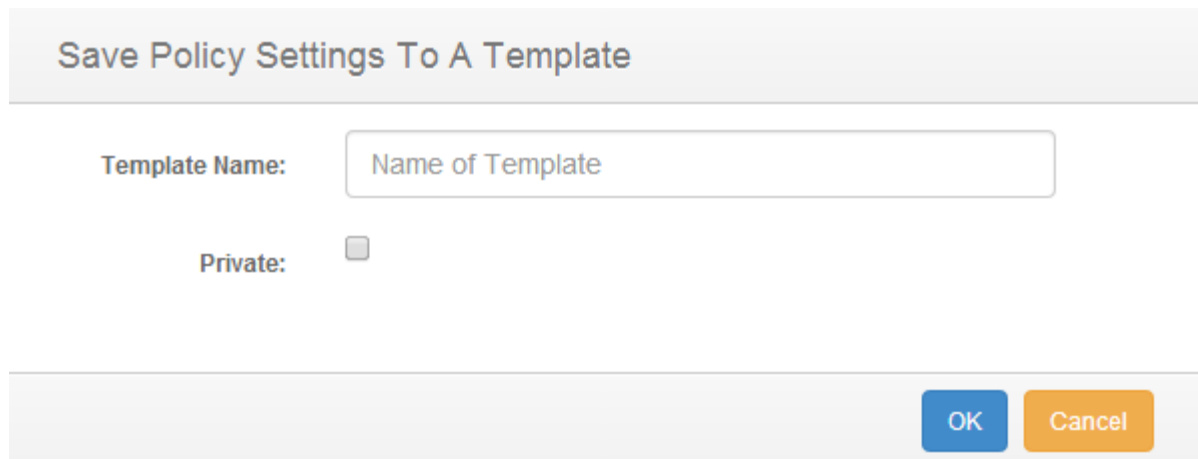
The image shows a dialog box titled "Save Policy Settings To A Template". It has a light gray header bar with the title in blue text. Below the header, there is a label "Template Name:" followed by a text input field containing the placeholder text "Name of Template". Below this, there is a label "Private:" followed by an unchecked checkbox. At the bottom right of the dialog, there are two buttons: a blue "OK" button and an orange "Cancel" button.

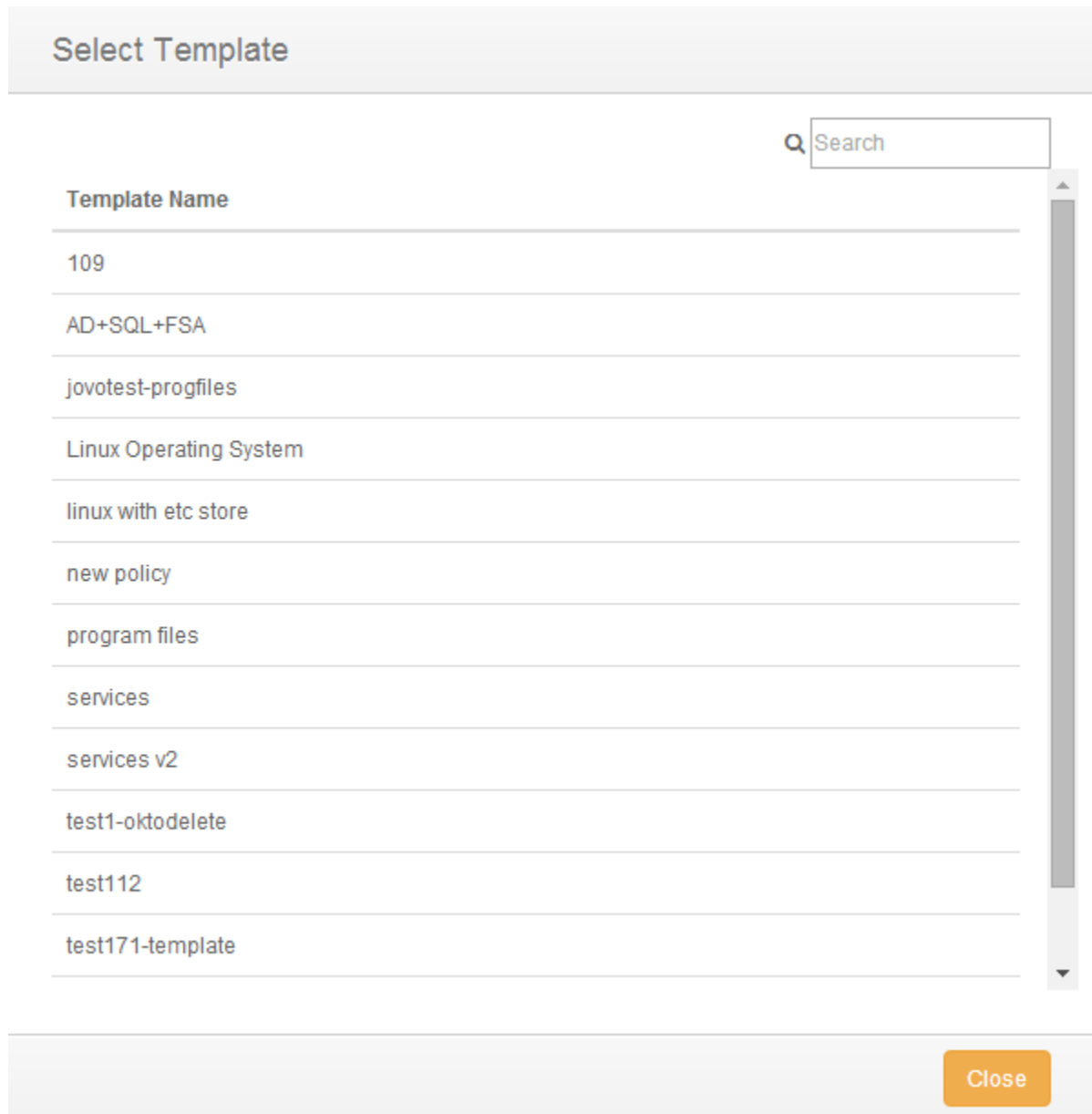
Figure 133: Save to Template dialog

In addition to being able to create Templates for single Object Groups CimTrak™ has the capability to create Templates for multiple Object Groups at the Network Device Agent level. To create a Network Device Agent template, right-click on the Network Device Agent name in the CimTrak™ Web Management Console's Object Group Tree and then select Save to Template. The Save to Template dialog will display. Enter a unique name for the template. If you would like this template to be private to your CimTrak™ account be sure to select the "Private" option by selecting the "Private" checkbox. When completed entering the required information click the OK button. Click the cancel button to abort the template creation. A template name can be between 1 and 512 characters.

#### 6.1.5.5. CREATING OBJECT GROUP WATCH POLICIES USING TEMPLATES

Once an Object Group Watch Policy has been created it is possible to save the policy configurations to a template. Using a template can assist in creating identical watch data for other CimTrak™ Network Device Agents. See section 4.7 for more information on CimTrak™ Templates.

To create an Object Group from template (or multiple Object Groups from a single template) right-click on the Network Device Agent name in the CimTrak™ Web Management Console's Object Group Tree and then select New Object Group(s) from Template. The Select Template dialog will display.

The image shows a 'Select Template' dialog box. At the top, there is a title bar with the text 'Select Template'. Below the title bar, on the right side, is a search bar with a magnifying glass icon and the word 'Search'. The main area of the dialog is a list of templates. The list has a header 'Template Name' and contains the following items: '109', 'AD+SQL+FSA', 'jovotest-progfiles', 'Linux Operating System', 'linux with etc store', 'new policy', 'program files', 'services', 'services v2', 'test1-oktodelete', 'test112', and 'test171-template'. A vertical scrollbar is on the right side of the list. At the bottom right of the dialog, there is an orange button labeled 'Close'.

**Figure 134: Select Template dialog**

Select the template the Object Group will be based off of and then click OK. Click Cancel to abort the Object Group creation. If OK is selected the Select Template dialog will close and the newly created Object Group(s) will display in the CimTrak™ Web Management Consoles Object Group Tree.

#### **6.1.5.6. DELETING OBJECT GROUP WATCH POLICIES**

Once an Object Group Watch Policy has been created it is possible to delete the Object Group. Once an Object Group is deleted it cannot be undone.

To delete an Object Group Watch Policy right-click on its name in the CimTrak™ Web Management Console's Object Group Tree and then select Delete. The Confirm Delete dialog will display.

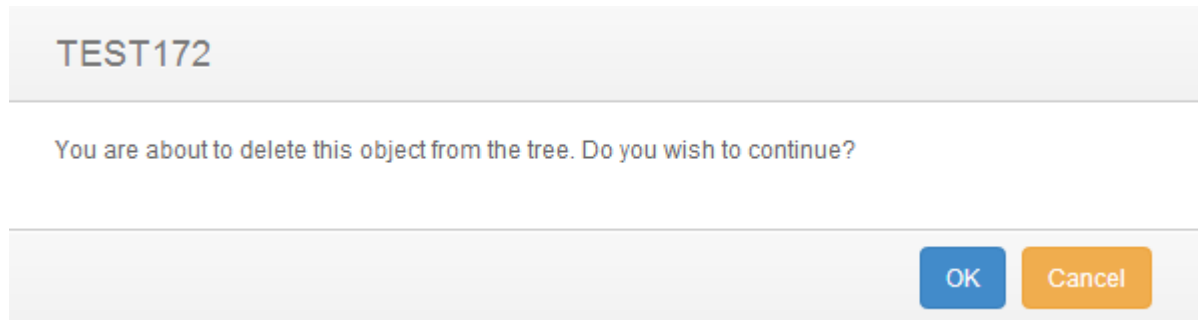


Figure 135: Confirm Delete dialog

Select Yes to delete the Object Group, select No to abort the deletion. Select the Do not show this again checkbox to suppress this message from future deletions. Clicking Yes results in the Object Group being deleted.



***The Object Group must be unlocked (monitoring disabled) before the Object Group can be deleted. Unlocking an Object Group is explained in a subsequent section.***

#### 6.1.5.7. ENABLING AND DISABLING OBJECT GROUP MONITORING

Before a CimTrak™ Network Device Agent can monitor an Object Group Watch Policy the Object Group must be “Locked”. To disable monitoring the Object Group Watch Policy must be “Unlocked”. The monitoring status of an Object Group can be determined by the associated icon in the CimTrak™ Web Management Console's Object Group Tree. See section 6.1.1.5 for more information on creating Object Group Watch Policies. Possible associated statuses are as follows:



**Unlocked:** *The Object Group Watch Policy is not currently being enforced.*



**Locked:** *The Object Group Watch Policy is currently enforcing the configured Corrective Action.*

Locking an Object Group is accomplished by selecting the Object Group to lock in the CimTrak™ Web Management Console's Object Group Tree, right-clicking and then selecting Lock and Digitally Sign.

When an Object Group is locked (or locking) it will show the locking and synchronization process in the Master Repository, Area, Agent, and Object Group Event Logs. The process of locking and synchronization creates Information level events.

Drag a column header here and drop it to group by that column.

Severity	Event Date/Time	Event	Correction	CimTrak ID	Modified By	Process	Absolute path
Info	7/11/2014 14:40:15	Sync Complete		ND_Agent_...			/DeviceRoot
Info	7/11/2014 14:40:11	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:40:07	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 14:40:03	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:40:01	* SCP: Reading startup-config.		ND_Agent_...			

**Figure 136: Object Group Lock Process (Event Log)**



***Multiple Object Groups can be locked simultaneously by selecting the Network Device Agent in the Web Management Console's Object Group Tree and then either right-clicking and selecting Lock and Digitally Sign in the context menu.***

Locking the Object Group will instruct the Network Device Agent to create digital signatures for each file included in the watch policy. If a Restore from Repository or Update Baseline Corrective Action is assigned, the Network Device Agent will create Authoritative Copies of the monitored files. All digital signatures and Authoritative Copy data is compressed, encrypted, and then transmitted to the CimTrak™ Master Repository.

While an Object Group is in the process of locking the lock process can be aborted by right-clicking on the Object Group in the CimTrak™ Web Management Console's Object Group Tree and selecting Cancel Lock in the context menu.

When the locking of an Object Group is "Stopped" it will show the stop locking process in the Master Repository, Area, Agent, and Object Group Event Logs. The process of Stopping creates error level events.



***The Locking of Multiple Object Groups can be stopped simultaneously by selecting the Network Device Agent in the Web Management Console's Object Group Tree and then right-clicking and selecting Cancel Lock in the context menu.***

Before configuration settings associated with an Object Group Watch Policy can be modified, an Object Group is deleted, or simply to temporarily disable Object Group monitoring the Object Group must be "Unlocked". Unlocking an Object Group is accomplished by selecting the Object Group to unlock in the CimTrak™



Web Management Console's Object Group Tree, right-clicking and then selecting Unlock and Allow Changes.

When an Object Group is Unlocked it will show the unlock process in the Master Repository, Area, Agent, and Object Group Event Logs. The process of unlocking creates error level events.

Drag a column header here and drop it to group by that column.

Severity	Event Date/Time	Event	Correction	CimTrak ID	Modified By	Process	Absolute path
Info	7/11/2014 14:40:15	Sync Complete		ND_Agent_...			/DeviceRoot
Info	7/11/2014 14:40:11	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:40:07	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 14:40:03	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:40:01	* SCP: Reading startup-config.		ND_Agent_...			

**Figure 137: Object Group Unlock Process (Event Log)**



***Multiple Object Groups can be unlocked simultaneously by selecting the Network Device Agent in the Web Management Console's Object Group Tree and then right-clicking and selecting Unlock and Allow Changes in the context menu.***

#### 6.1.5.8. SYNCHRONIZING OBJECT GROUP DATA

Data being monitored by a CimTrak™ Network Device Agent is monitored either in real-time or at a polling interval. To force the polling interval to expire immediately, CimTrak™ has the capability to synchronize monitored data on demand by means of Force Sync.

Synchronizing an Object Group Watch Policy is performed by right-clicking on the Object Group in the CimTrak™ Web Management Console's Object Group Tree and selecting Force Sync in the context menu.



***Multiple Object Groups can be synchronized simultaneously by selecting the Network Device Agent in the Web Management Console's Object Group Tree and then right-clicking and selecting Force Sync in the context menu.***

When an Object Group is synchronized it will show the synchronization process in the Master Repository, Area, Agent, and Object Group Event Logs. The process of synchronizing creates information level events.

Drag a column header here and drop it to group by that column.

Severity	Event Date/Time	Event	Correction	CimTrak ID	Modified By	Process	Absolute path
Info	7/11/2014 14:40:15	Sync Complete		ND_Agent_...			/DeviceRoot
Info	7/11/2014 14:40:11	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:40:07	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 14:40:03	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:40:01	* SCP: Reading startup-config.		ND_Agent_...			

**Figure 138: Object Group Synchronization Process (Event Log)**

#### 6.1.4. NETWORK DEVICE AGENT INFORMATION DISPLAY

The CimTrak™ Web Management Console's Information Display Area displays information for the selected CimTrak™ Network Device Agent. The information displayed provides Event Log data.

- **Agent Settings:** *Settings and system information associated with the selected Network Device Agent.*
- **Event Log:** *Event audit log associated with the Network Device Agent and children Object Groups of the selected Network Device Agent.*
- **Stats:** *System statistics associated with the system hosting the Network Device Agent.*
- **Notes:** *Administrative notes associated with the Network Device Agent.*
- **Overview:** *Object Group status information for all Object Groups associated with the Network Device Agent.*

Severity	Event Date/Time	Event	Correction	CimTrak ID	Modified By	Process	Absolute path
Info	7/11/2014 14:40:15	Sync Complete		ND_Agent_...			/DeviceRoot
Info	7/11/2014 14:40:11	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:40:07	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 14:40:03	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:40:01	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 14:39:55	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:39:53	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 14:39:51	Sync Started		ND_Agent_...			/DeviceRoot
Info	7/11/2014 12:38:05	Sync Complete		ND_Agent_...			/DeviceRoot
Info	7/11/2014 12:38:01	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 12:37:57	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 12:37:52	* SCP: Reading running-config.		ND_Agent_...			

**Figure 139: Network Device Agent Information Display Area (Agent Settings Tab Selected)**

The information associated with the Network Device Agent Information Display Area tabs is explained in subsequent sections.

#### 1.1.2.2. AUDITING NETWORK DEVICE AGENT EVENTS

The Network Device Agent Event Log provides audit information relating to events occurring in the Network Device Agent and Object Groups connected to the Network Device Agent. Accessing the Network Device Agent Event Log is accomplished by first clicking once on the Network Device Agent name in the Object Group Tree to select it followed by clicking the Event Log tab in the Web Management Console Information Display Area.

The Network Device Agent Event Log displays details of all events that have occurred on the Network Device Agent and Object Groups connected to the Network Device Agent. The level of detail displayed is dependent on the auditing level configured in the Master Repository Properties Log Administrative DB Changes. See section 0 for additional information.

For each recorded event, the Network Device Agent Event Log will display information corresponding to the following:

**Event Date/Time:** *The exact date and time of the detected event.*

**Event:** *Brief description of the detected event.*

**Absolute Path:** *File path affected by the detected event.*

**Completion Date/Time:** *Date and time the correction response completed.*

**Event Code:** *Internal CimTrak™ Event Code corresponding to the detected event.*

**Path:** *Object Tree Path to the affected CimTrak™ object.*

Event Log

Drag a column header here and drop it to group by that column.

Severity	Event Date/Time	Event	Correction	CimTrak ID	Modified By	Process	Absolute path
Info	7/11/2014 16:11:39	Sync Complete		ND_Agent_...			/DeviceRoot
Info	7/11/2014 16:11:31	Sync Started		ND_Agent_...			/DeviceRoot
Info	7/11/2014 14:42:51	Sync Complete		ND_Agent_...			/DeviceRoot
Warning	7/11/2014 14:42:47	File Modified	Baseline Updated	ND_Agent_...	Owner: Unk...		/DeviceRoot/vmware/backup.counter
Warning	7/11/2014 14:42:17	File Modified	Baseline Updated	ND_Agent_...	Owner: Unk...		/DeviceRoot/http.drift
Info	7/11/2014 14:41:06	Sync Started		ND_Agent_...			/DeviceRoot
Info	7/11/2014 14:40:15	Sync Complete		ND_Agent_...			/DeviceRoot
Info	7/11/2014 14:40:11	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:40:07	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 14:40:03	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:40:01	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 14:39:55	* SCP: Reading running-config.		ND_Agent_...			

Total Items: 3964

CSV Export

Page Size: 100

1 / 40

**Figure 140: Network Device Agent Event Log**

Each Event Log message type has a corresponding icon that allows for quick visual reference to the urgency level of the event. These urgency levels are important to note when configuring E-Mail alert permissions. E-Mail alert permissions are explained in a subsequent section.

**Emergency:** *System is unusable. Highest level of event.*

**Alert:** *Take action immediately.*

**Critical:** *Critical conditions have occurred.*

**Error:** *Error conditions.*

**Warning:** *Warning conditions.*

**Notice:** *Normal condition that requires attention.*

**Information:** *Informational message.*

**Debug:** *Debug-level message. Lowest level of event.*

Specifics relating to message types are discussed in a subsequent sections.

#### **6.1.2.1.1. FILTERING AND SORTING THE NETWORK DEVICE AGENT EVENT LOG**

The Network Device Agent Event Log can be filtered to only show events matching the specified criteria. Accessing the Network Device Agent Event Log is accomplished by first clicking once on the Network Device Agent in the Object Group Tree to select it followed by clicking the Event Log tab in the Web Management Console Information Display Area.

To filter the information displayed in the Network Device Agent Event Log, drag and drop one of the column headers into the section labelled “Drag a column header here and drop it to group by that column.”

#### **6.1.2.2. NETWORK DEVICE AGENT PERMISSIONS**

Network Device Agents can be configured restrict access based on permission settings. Additionally, event notifications can be configured to notify CimTrak™ Users about events relating to the Network Device Agent. Accessing Network Device Agent permissions is accomplished by first clicking once on the Network Device Agent in the Object Group Tree to select it and then right-clicking and selecting “Permissions”. The Security Permissions dialog will display.

By default each Network Device Agent will have the following permissions:

##### **Administrators**

**Create Objects:** *Create Network Device Agent Object Groups.*

**Edit:** *Edit Network Device Agent settings.*

**Lock:** *Enable active monitoring of Object Group Data.*

**Reports:** *View reports relating to the Network Device Agent contents.*

**Unlock:** *Disable active monitoring of Object Group Data.*

**View:** *View contents and configurations relating to the Network Device Agent.*

## **Auditors**

**Reports:** View reports relating to Network Device Agent contents.

**View:** View contents and configurations relating to the Network Device Agent.

## **Installers**

Attach CimTrak™ Agents to a Master Repository.

### Permissions for Object

Add

Group or User Names

Group	Administrators	
Group	Auditors	
Group	Email_Testing	Remove
Group	Installers	

Permissions	Allow	Deny
Create Objects	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Edit	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lock	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Reports	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Unlock	<input checked="" type="checkbox"/>	<input type="checkbox"/>
View	<input checked="" type="checkbox"/>	<input type="checkbox"/>

☒ Apply permissions to children recursively

OKCancel

**Figure 141: Network Device Agent Security Permissions dialog**

Default access permissions associated with the Administrators, Auditors, and Installers User Groups cannot be changed. It is possible to modify E-mail alert notices for Administrator and Auditor user groups. Available E-mail alert types include:

Emergency

Alert  
Critical  
Error  
Warning  
Notice  
Information

Additional information relating to these alert types is described in a subsequent section.

### 6.1.2.3. MODIFYING AN EXISTING USER/GROUP NETWORK DEVICE AGENT PERMISSIONS

It is possible to modify existing user and group Network Device Agent Permissions and E-mail notification settings. Accessing Network Device Agent permissions is accomplished by first clicking once on the Network Device Agent in the Object Group Tree to select it and then right-clicking and selecting “Permissions”. The Security Permissions dialog will display.

Select the existing user or group by clicking once on the CimTrak™ User or Group name in the Group or User Names section of the Security Permissions dialog. The Permissions section of the Security Permissions dialog will update to show the permissions currently assigned to the selected user or group.



***Selecting a group will apply the selected permissions and E-mail notification settings to all members of the group. Selecting a single user will apply the selected permissions and E-mail notification settings to only that single user account.***

To add or remove permissions click the “Allow” or “Deny” checkbox corresponding to the permission being configured. Available permissions include:

**Create Objects:** Create Network Device Agent Object Groups.

**Edit:** Edit Network Device Agent/Object Group control contents.

**Lock:** Enable active monitoring of Object Group Data

**Reports:** View reports relating to Network Device Agent contents.

**Unlock:** Disable active monitoring of Object Group Data

**View:** View contents and configurations relating to the Network Device Agent.

**Email Emergency:** Receive alerts relating to emergency level notifications.

**Email Alert:** Receive alerts relating to alert level notifications.

**Email Critical:** Receive alerts relating to critical level notifications.

**Email Error:** Receive alerts relating to error level notifications.

**Email Warning:** Receive alerts relating to warning level notifications.

**Email Notice:** Receive alerts relating to notice level notifications.

**Email Information:** *Receive alerts relating to information level notifications.*

To apply the permission settings to all children objects, ensure that the Apply permissions to children recursively checkbox is selected.

When completed, click “OK” to apply the permission and alert settings. Click “Cancel” to abort the security permission configuration.



***Permissions and notification settings can be inherited from parent objects (such as the Master Repository) if the permissions are created at a parent level.***



***Permissions and notification settings are not automatically inherited for new objects. It will be necessary to manually assign the permissions and notification settings to the object.***

#### **6.1.2.4. ADDING AND REMOVING USERS AND GROUPS TO NETWORK DEVICE AGENT PERMISSIONS**

It is possible to add additional users and groups to the Security Permissions dialog so that Network Device Agent Permissions and E-mail notification settings can be assigned or changed. Accessing Network Device Agent permissions is accomplished by first clicking once on the Network Device Agent in the Object Group Tree to select it and then right-clicking and selecting “Permissions.” The Security Permissions dialog will display.

To add a new local CimTrak™ User or Group, click the Add button. The Add Users dialog will display listing all available local users and groups.

Select Users or Groups

Search

	Type	Name
<input type="checkbox"/>	User	aaaa
<input type="checkbox"/>	User	wade
<input type="checkbox"/>	User	knightrider
<input type="checkbox"/>	User	payton
<input type="checkbox"/>	User	Pippen
<input type="checkbox"/>	User	Hanks
<input type="checkbox"/>	User	Rose
<input type="checkbox"/>	User	Garnett
<input type="checkbox"/>	User	Fridge
<input type="checkbox"/>	User	alberts
<input type="checkbox"/>	User	jovo2

OKCancel

**Figure 142: Add Users dialog**

Select the local CimTrak™ User or Group to add by selecting the checkbox to the left of the name. Click “OK” to add the User or Group. Click “Cancel” to abort the addition process. The selected user or group will now display in the Group or User Names section of the Security Permissions dialog.

The User or Group is now available to have permissions and notification settings assigned.

#### 6.1.5. OBJECT GROUP INFORMATION DISPLAY



The CimTrak™ Web Management Console's Information Display Area displays information for the selected CimTrak™ Network Device Agent Object Groups. The information displayed is often broken up into several tabbed viewing areas.

- **Event Log:** *Event audit log associated with the Network Device Agent and children Object Groups of the selected Network Device Agent.*
- **Change Log:** *Detected changes of watched directories.*
- **Monitor Info:** *Description and statistical standing of Watch Parameters within the Object Group.*
- **Pending Repair:** *Displays queue information associated with the remediation of folder, file and configuration data.*
- **Generation:** *Displays revision information for changes occurring to files, folders, operating system configurations contained in a File System Agent Object Group.*

Severity	Event Date/Time	Event	Correction	CimTrak ID	Modified By	Process	Absolute path
Info	7/11/2014 14:40:15	Sync Complete		ND_Agent_...			/DeviceRoot
Info	7/11/2014 14:40:11	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:40:07	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 14:40:03	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:40:01	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 14:39:55	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 14:39:53	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 14:39:51	Sync Started		ND_Agent_...			/DeviceRoot
Info	7/11/2014 12:38:05	Sync Complete		ND_Agent_...			/DeviceRoot
Info	7/11/2014 12:38:01	* SCP: Reading running-config.		ND_Agent_...			
Info	7/11/2014 12:37:57	* SCP: Reading startup-config.		ND_Agent_...			
Info	7/11/2014 12:37:52	* SCP: Reading running-config.		ND_Agent_...			

Total Items: 250    CSV Export    Page Size: 100    1 / 3

**Figure 143: Object Group Information Display Area**

The information associated with the Object Group Information Display Area tabs is explained in subsequent sections.

### 6.1.3.1. AUDITING OBJECT GROUP EVENTS

The Object Group Event Log provides audit information relating to events occurring in the Object Groups connected to the Network Device Agent. Accessing the Object Group Event Log is accomplished by first clicking once on the Object Group name in the Object Group Tree to select it followed by clicking the Event Log tab in the Web Management Console Information Display Area.

The Object Group Event Log displays details of all events that have occurred on the Object Groups connected to the Network Device Agent. The level of detail displayed is dependent on the auditing level configured in the Master Repository

Properties Log Administrative DB Changes. See section 0 for additional information.

For each recorded event, the Object Group Event Log will display information corresponding to the following:

**Event Date/Time:** *The exact date and time of the detected event.*

**Event:** *Brief description of the detected event.*

**Correction:** *The Corrective Action performed on the detected event.*

**Performed By (Cimtrak™ ID):** *The Network Device Agent detecting the event and performing the remediation.*

**Modified By:** *The File System User responsible for the detected event.*

**Absolute Path:** *File path affected by the detected event.*

**Completion Date/Time:** *Date and time the correction response completed.*

**Event Code:** *Internal CimTrak™ Event Code corresponding to the detected event.*

Each Event Log message type has a corresponding icon that allows for quick visual reference to the urgency level of the event. These urgency levels are important to note when configuring E-Mail alert permissions. E-Mail alert permissions are explained in a subsequent section.

**Emergency:** *System is unusable. Highest level of event.*

**Alert:** *Take action immediately.*

**Critical:** *Critical conditions have occurred.*

**Error:** *Error conditions.*

**Warning:** *Warning conditions.*

**Notice:** *Normal condition that requires attention.*

**Information:** *Informational message.*

**Debug:** *Debug-level message. Lowest level of event.*

Specifics relating to message types are discussed in a subsequent section.

#### **6.1.3.1.1. FILTERING AND SORTING THE OBJECT GROUP EVENT LOG**

The Object Group Event Log can be filtered to only show events matching the specified criteria. Accessing the Object Group Event Log is accomplished by first clicking once on the Object Group in the Object Group Tree to select it followed by clicking the Event Log tab in the Web Management Console Information Display Area.

To filter the information displayed in the Network Device Agent Event Log, drag and drop one of the column headers into the section labelled “Drag a column header here and drop it to group by that column.”

#### **6.1.3.2. REVIEWING OBJECT GROUP MONITORED CHANGES**

The Object Group Change Log provides detailed change event audit information relating to change events occurring in the Object Groups connected to the Network Device Agent. Accessing the Object Group Change Log is accomplished by first clicking once on the Object Group name in the Object Group Tree to select it followed by clicking the Change Log tab in the Web Management Console Information Display Area.

The Object Group Change Log displays details of all addition, deletion, and change events that have occurred on the Object Groups connected to the Network Device Agent.

For each recorded event, the Object Group Change Log will display information corresponding to the following:

**Event Date/Time:** *The exact date and time of the detected event.*

**Storage Status:** *Information indicating if the change is stored in the Master Repository.*

**Absolute Path:** *File path affected by the detected event.*

**Modified By:** *The File System User responsible for the detected event (Windows Network Device Agent with Driver only).*

**Process:** *The process used to initiate the detected event (Windows Network Device Agent with Driver only).*

**Process ID:** *Windows Process ID associated with the initiating process (Windows Network Device Agent with Driver only).*

**Thread ID:** *Process Thread ID associated with the initiating process (Windows Network Device Agent with Driver only).*

<a href="#">Event Log</a>	<a href="#">Change Log</a>	<a href="#">Monitor Info</a>	<a href="#">Pending Repair</a>	<a href="#">Generation</a>
---------------------------	----------------------------	------------------------------	--------------------------------	----------------------------

Drag a column header here and drop it to group by that column.

Severity	Event Date/Time	Storage Status	Absolute path	Modified By	Process	Process ID	Thread ID
Warning	7/11/2014 14:42:47	Stored	/DeviceRoot/vmware/backup.counter	Owner: Unknown		0	
Warning	7/11/2014 14:42:17	Stored	/DeviceRoot/ntp.drift	Owner: Unknown		0	
Warning	7/11/2014 12:39:18	Stored	/DeviceRoot/vmware/backup.counter	Owner: Unknown		0	
Warning	7/11/2014 12:38:48	Stored	/DeviceRoot/ntp.drift	Owner: Unknown		0	
Warning	7/11/2014 10:35:45	Stored	/DeviceRoot/vmware/backup.counter	Owner: Unknown		0	
Warning	7/11/2014 10:35:15	Stored	/DeviceRoot/ntp.drift	Owner: Unknown		0	
Warning	7/11/2014 08:32:15	Stored	/DeviceRoot/vmware/backup.counter	Owner: Unknown		0	
Warning	7/11/2014 08:31:46	Stored	/DeviceRoot/ntp.drift	Owner: Unknown		0	
Warning	7/11/2014 06:28:45	Stored	/DeviceRoot/vmware/backup.counter	Owner: Unknown		0	
Warning	7/11/2014 06:28:16	Stored	/DeviceRoot/ntp.drift	Owner: Unknown		0	
Warning	7/11/2014 04:25:17	Stored	/DeviceRoot/vmware/backup.counter	Owner: Unknown		0	
Warning	7/11/2014 04:24:48	Stored	/DeviceRoot/ntp.drift	Owner: Unknown		0	
Warning	7/11/2014 03:24:49	Stored	/DeviceRoot/vmware/backup.counter	Owner: Unknown		0	

Total Items: 125

[CSV Export](#)

Page Size:

### Figure 144: Object Group Change Log

Each Change Log message type has a corresponding icon that allows for quick visual reference to the urgency level of the event. These urgency levels are important to note when configuring E-Mail alert permissions. E-Mail alert permissions are explained in a subsequent section.

**Emergency:** *System is unusable. Highest level of event.*

**Alert:** *Take action immediately.*

**Critical:** *Critical conditions have occurred.*

**Error:** *Error conditions.*

**Warning:** *Warning conditions.*

**Notice:** *Normal condition that requires attention.*

**Information:** *Informational message.*

**Debug:** *Debug-level message. Lowest level of event.*

Generally change events are associated with the Error level. Specifics relating to message types are discussed in a subsequent section.

#### **6.1.3.2.1. FILTERING AND SORTING THE OBJECT GROUP CHANGE LOG**

The Object Group Change Log can be filtered to only show events matching the specified criteria. Accessing the Object Group Change Log is accomplished by first clicking once on the Object Group in the Object Group Tree to select it followed by clicking the Change Log tab in the Web Management Console Information Display Area.

To filter the information displayed in the Object Group Change Log, drag and drop one of the column headers into the section labelled “Drag a column header here and drop it to group by that column.”

#### **6.1.3.2.2. ACCESSING THE CHANGE LOG TAB CONTEXT MENU**

Right-clicking on any event listed in the Change Log tab provides a context menu allowing for change related actions. The Change Log tab is accessed by selecting the Object Group in the Web Management Console’s Object Group Tree and then selecting the Change Log tab in the Information Display Area.

The Change Log Context Menu allows for additional actions to be taken on stored changes including:

**View:** *View the content and attributes associated with the stored change.*

**View as Binary:** *View the content associated with the stored change in a hexadecimal format.*

**View Forensic Data:** *View the IP Address and Port number associated with the change process. (Windows Network Device Agent with Driver only).*

**Download:** *Download a copy of the stored intrusion.*

**Compare with Authoritative Copy (at time of change):** *Compare the content of the detected change with the known, authoritative copy stored in the Master Repository at the time of the change.*

**Compare with Authoritative Copy (current):** *Compare the content of the detected change with the current known, authoritative copy stored in the Master Repository currently.*

**Add to Excludes:** *Disable monitoring of the selected file or configuration.*

Details associated with these context menu options are discussed in subsequent sections.

#### **6.1.3.2.2.1. VIEWING CHANGE CONTENT**

Right-clicking on any event listed in the Change Log tab provides a context menu allowing for change related actions. Selecting View from the context menu allows authorized CimTrak™ administrators the capability to review content associated with a detected change. The Change Log tab is accessed by

selecting the Object Group in the Web Management Console's Object Group Tree and then selecting the Change Log tab in the Information Display Area.

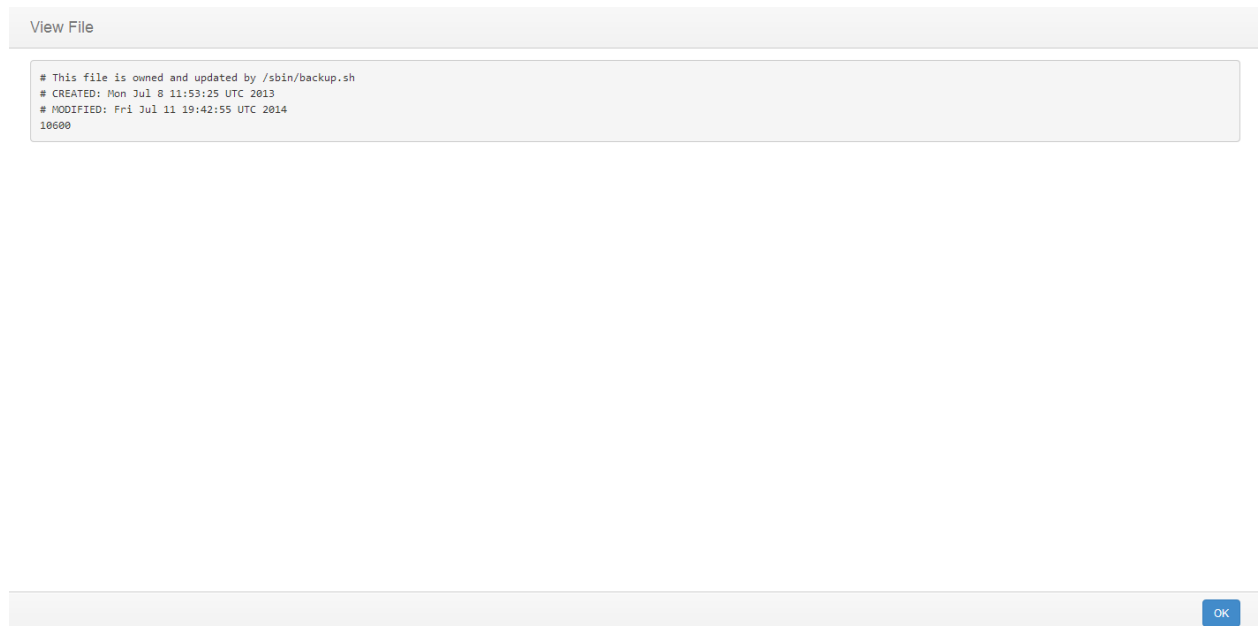


Figure 145: File View dialog



***Viewing of Change data requires the Object Group Policy is configured to store changes. Additionally, the change must not exceed the specified “Keep Change Size (in KB)” indicated in Object Group Properties Monitoring Information.***



***Viewing the content of non-binary files is supported. Binary files cannot be viewed at this time.***

Click the Close button to exit the File View dialog.

#### **6.1.6.2.2.2. VIEWING CHANGE FORENSIC DATA**

Right-clicking on any event listed in the Change Log tab provides a context menu allowing for change related actions. Selecting View Forensic Data from the context menu allows authorized CimTrak™ administrators the capability to review connections associated with the offending change process at the time of the change. The Change Log tab is accessed by selecting the Object Group in the Web Management Console's Object Group Tree and then selecting the Change Log tab in the Information Display Area.

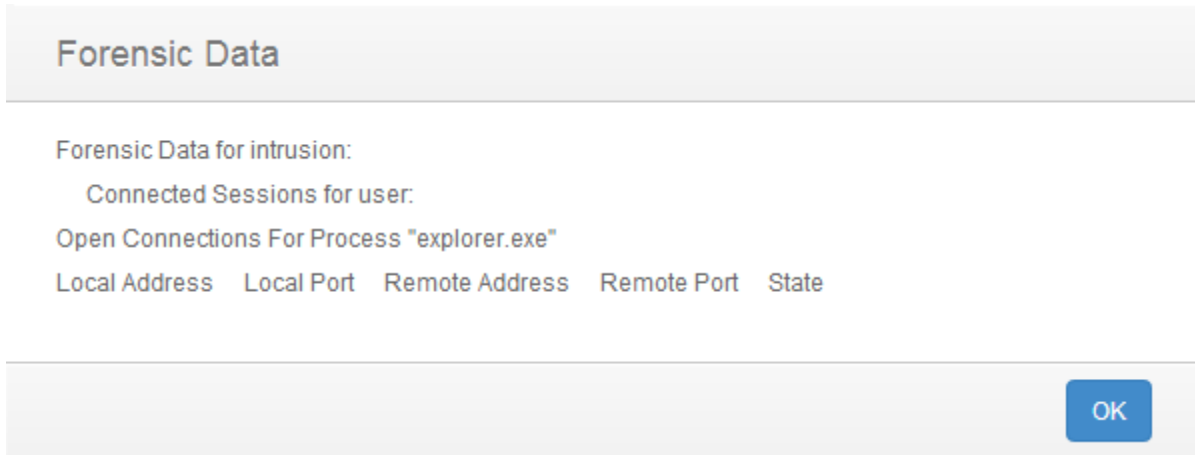


Figure 146: Forensic Data dialog



***Forensic data is only available for remote connections.***



***Viewing of forensic data is only supported on Windows File Systems with the Network Device Agent Driver installed.***

The Forensic Data dialog displays the following information:

Mount Points: The Windows Mount Point Name the change occurred on.\*?\*

Process: The Windows Process name responsible for initiating the detected change. Remote changes display as “System”.

Local Address: IP Address on the affected system the process utilized to make the change.

Local Port: Port number on the affected system the process utilized to make the change.

Remote Address: IP Address of the remote system that attached to the local process to make the change.

Remote Port: Port number of the remote system used to connect to the local system.

State: State of the current connection (i.e., Listen or Established).

Click the Close button to exit the Forensic Data dialog.

#### **6.1.3.2.2.3. DOWNLOADING A COPY OF CHANGE DATA**

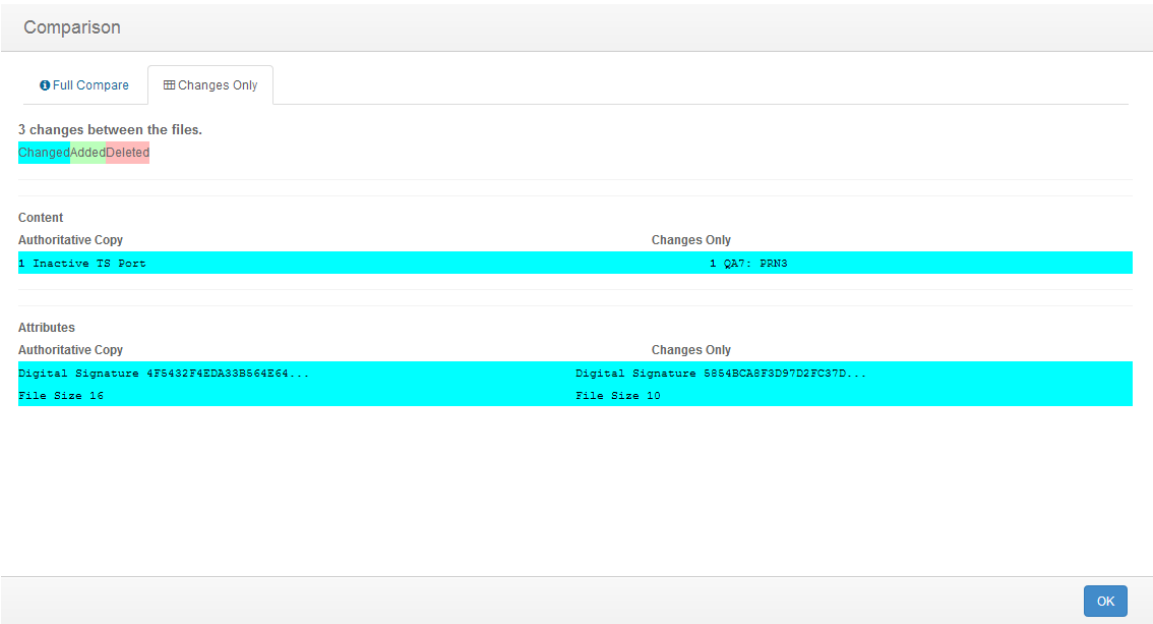
Right-clicking on any event listed in the Change Log tab provides a context menu allowing for change related actions. Selecting Download from the context menu allows authorized CimTrak™ administrators the capability to download a copy of

the actual change file. The Change Log tab is accessed by selecting the Object Group in the Web Management Console's Object Group Tree and then selecting the Change Log tab in the Information Display Area.

Clicking the Download option in the Change Log tab context menu results in the file being downloaded and saved in the Download folder, or in your default location for downloaded files.

**6.1.3.2.2.4. COMPARING CHANGE DATA WITH THE AUTHORITATIVE COPY AT THE TIME OF THE CHANGE**

Right-clicking on any event listed in the Change Log tab provides a context menu allowing for change related actions. Selecting Compare with Authoritative Copy (at time of change) allows authorized CimTrak™ administrators the capability to perform a side-by-side comparison of the changed file with its authoritative copy stored in the Master Repository. The Change Log tab is accessed by selecting the Object Group in the Web Management Console's Object Group Tree and then selecting the Change Log tab in the Information Display Area.



**Figure 147: File Comparison Results**

**6.1.3.2.2.4.1. UNDERSTANDING THE OBJECT GROUP CHANGE TAB FILE COMPARISON RESULTS DIALOG**

The File Comparison Results dialog displays anytime a comparison is performed between a detected change and the authoritative copy associated with watch properties. See section 0 for more information on performing file comparisons.

The File Comparison dialog is comprised of two tabs:

**Full Compare:** A comparison of both files are shown with all content and attributes listed.



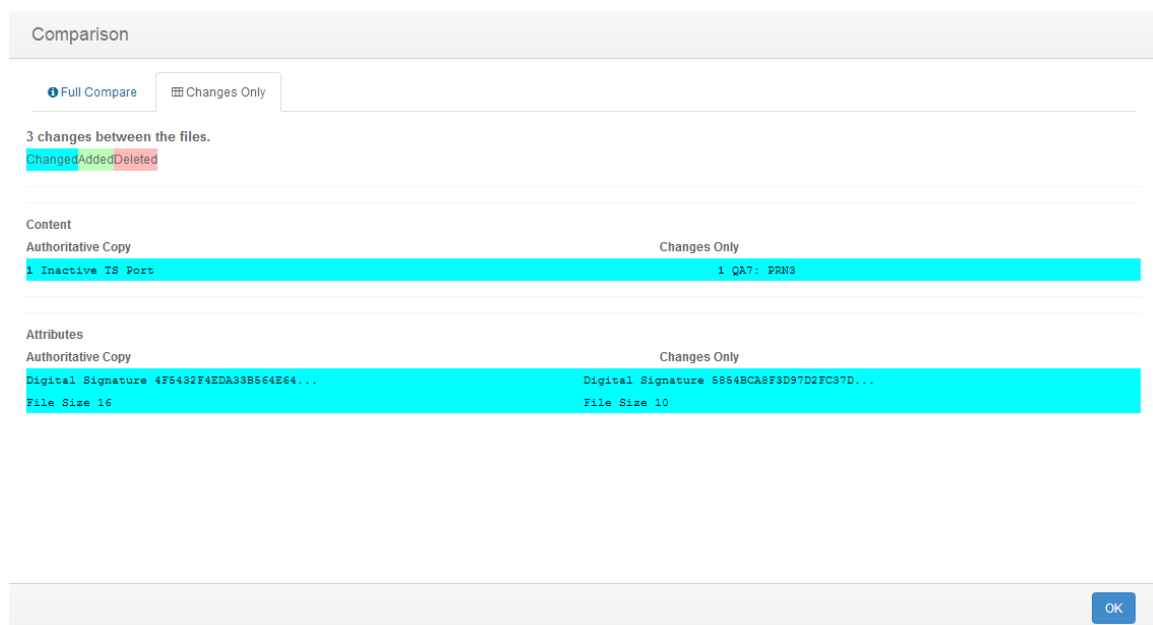
**Changes only:** A comparison of both file are shown with only the content and attributes which the changes affected listed.

#### 6.1.3.2.2.4.1.1. UNDERSTANDING THE FILE COMPARISON RESULTS DIALOG INFORMATION DISPLAY AREA AND TAB BROWSER

The File Comparison Results dialog Tab Browser and Information Display Area allows authorized CimTrak™ users the capability visualize generation comparison data. The File Comparison Results dialog is accessible by accessing the context menu and selected Compare with Authoritative Copy (at time of Change) in the Object Group Change Tab. See section 0 for more information on performing file comparisons.

The File Comparison Results dialog Information Display Area shows a side-by-side comparison of one generation revision of a detected change to the Master Repository Authoritative Copy. Lines that have been modified are highlighted in blue, lines that have been added are highlighted in green, and lines that have been deleted are highlighted in red.

By default, the “Full Compare” tab is selected. The “Full Compare” tab shows all lines of a selected comparison. Selecting the “Changes Only” tab displays only the lines that have differences between the compared generations.



**Figure 148: File Comparison Results dialog Changes tab**

Click the Close button to exit the File Comparison Results dialog.

#### 6.1.3.2.2.5. COMPARING CHANGE DATA WITH THE CURRENT AUTHORITATIVE COPY

Right-clicking on any event listed in the Change Log tab provides a context menu allowing for change related actions. Selecting Compare with Authoritative Copy (Current) allows authorized CimTrak™ administrators the capability to perform a side-by-side comparison of the changed file with an authoritative copy stored in the Master Repository. The Change Log tab is accessed by selecting the Object Group in the Web Management Console's Object Group Tree and then selecting the Change Log tab in the Information Display Area.

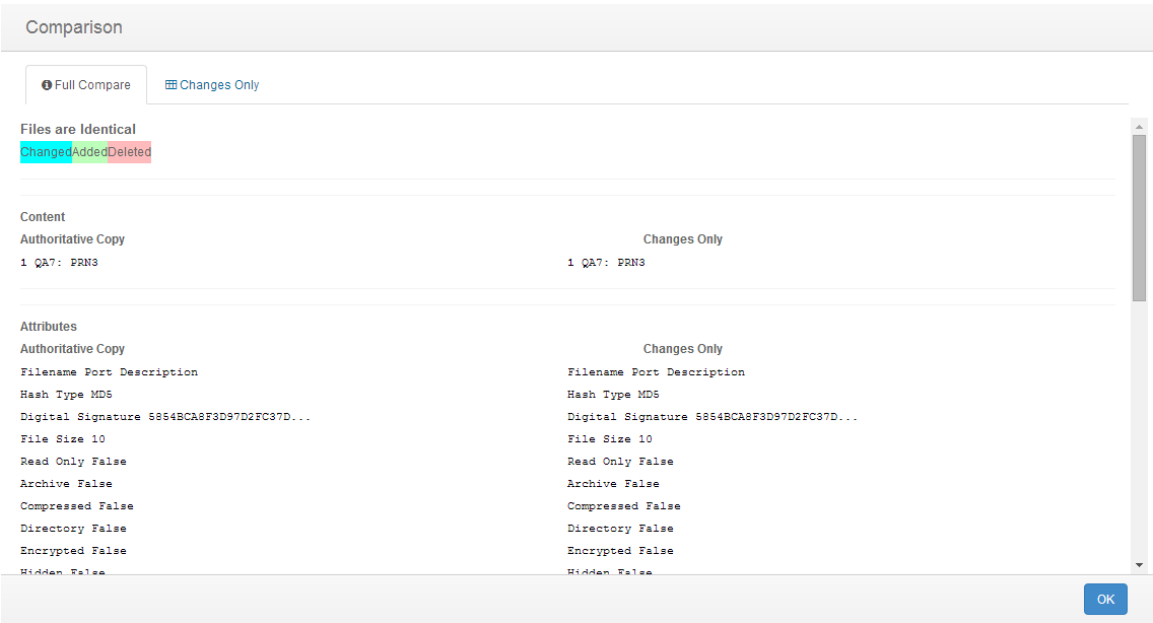


Figure 149: File Comparison Results

Click the Close button to exit the File Comparison Results dialog.

#### 6.1.3.2.2.5.1. UNDERSTANDING THE OBJECT GROUP CHANGE TAB FILE COMPARISON RESULTS DIALOG

The File Comparison Results dialog displays anytime a comparison is performed between a detected change and the authoritative copy associated with watch properties. See section 0 for more information on performing file comparisons.

The File Comparison dialog is comprised of two tabs:

**Full Compare:** A comparison of both files are shown with all content and attributes listed.

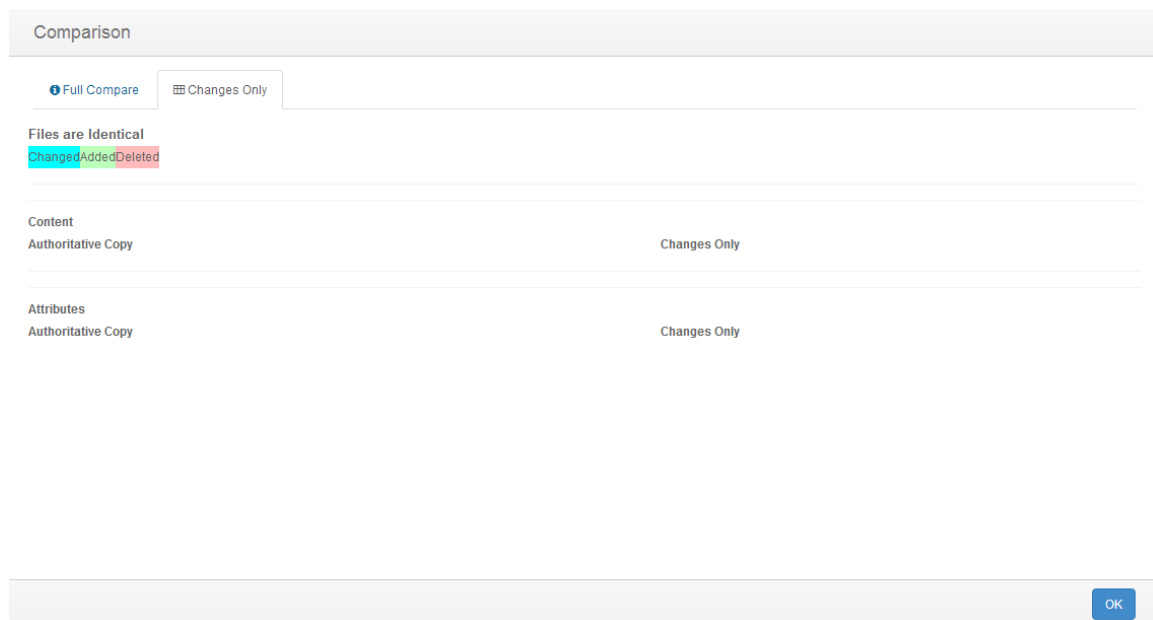
**Changes only:** A comparison of both file are shown with only the content and attributes which the changes affected listed.

#### 6.1.3.2.2.5.1.1. UNDERSTANDING THE FILE COMPARISON RESULTS DIALOG INFORMATION DISPLAY AREA AND TAB BROWSER

The File Comparison Results dialog Tab Browser and Information Display Area allows authorized CimTrak™ users the capability visualize generation comparison data. The File Comparison Results dialog is accessible by accessing the context menu and selected Compare with Authoritative Copy (Current) in the Object Group Change Tab. See section 0 for more information on performing file comparisons.

The File Comparison Results dialog Information Display Area shows a side-by-side comparison of one generation revision of a detected change to the Master Repository Authoritative Copy. Lines that have been modified are highlighted in blue, lines that have been added are highlighted in green, and lines that have been deleted are highlighted in red.

By default, the “Full Compare” tab is selected. The “Full Compare” tab shows all lines of a selected comparison. Selecting the “Changes Only” tab displays only the lines that have differences between the compared generations.



**Figure 150: File Comparison Results dialog Changes tab**

Click the Close button to exit the File Comparison Results dialog.

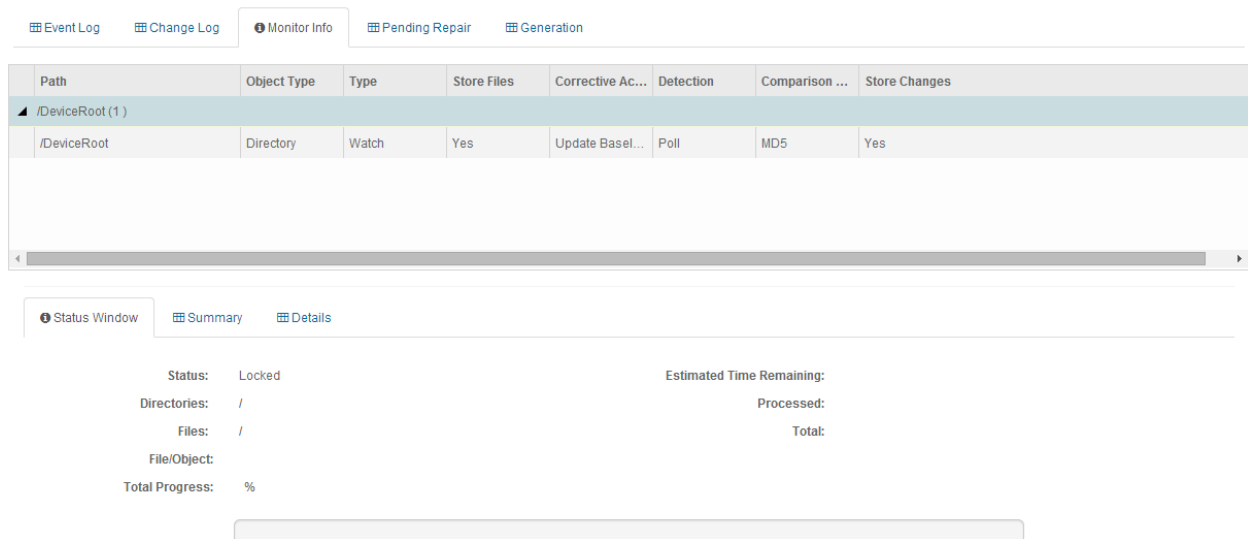
#### 6.1.3.3. REVIEWING OBJECT GROUP MONITORING INFORMATION

The Object Group Monitor Info tab provides Object Group monitoring and status information relating to Object Groups connected to the Network Device Agent. Accessing the Object Group Monitor Info is accomplished by first clicking once on the Object Group name in the Object Group Tree to select it followed by

clicking the Monitor Info tab in the Web Management Console Information Display Area.

The Object Group Monitor Info tab is comprised of two sections:

## Path Status Windows/Details



**Figure 151: Object Group Monitor Info tab**

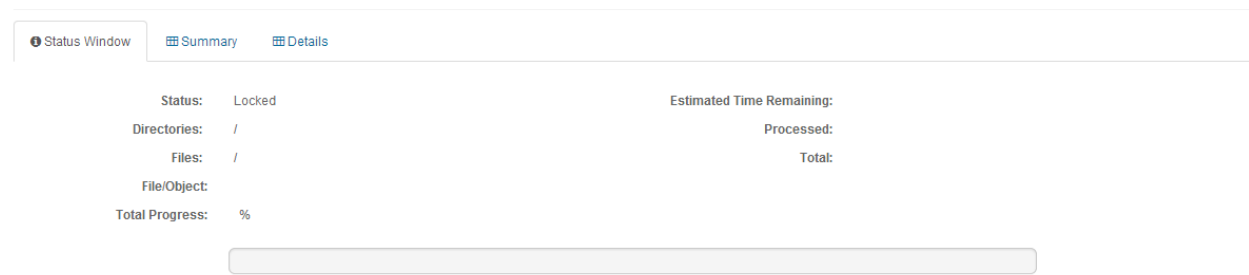
The Path section displays watch path and exclude information pertaining to the select Object Group.

The Status Window/Details section is comprised of three tabs:

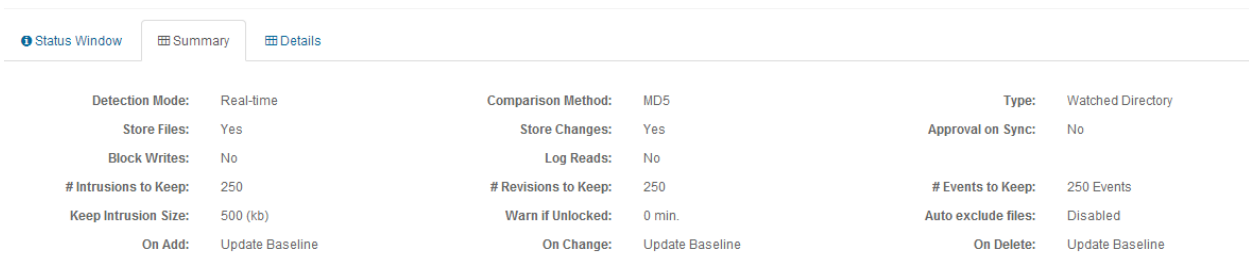
- **Status Window:** *Displays current lock status information associated with the Object Group Watch Policy. (i.e. Lock, Locking, Unlocked)*
- **Summary:**
- **Details:** *Displays details associated with the Object Group Watch Policy Configuration including:*
  - **Type:** *Object Group policy type (generally Watch).*
  - **Detection Mode:** *The change detection mode enabled (Real-time or polling)*
  - **File Comparison Method:** *The hash type performed on monitored data.*
  - **User Approval on Sync:** *Require user intervention for changes detected while the Network Device Agent was disconnected from the Master Repository. (True, False)*
  - **Store Files:** *Store authoritative copy data in the Master Repository (True, False).*

- **Store Changes:** Store change data in the Master Repository (True, False).
- **Ignore Archive Flag:** Monitor the archive flag associated with file system watch data. (True, False)
- **Ignore Read-only Flag:** Monitor the read-only flag associated with the file system watch data. (True, False)
- **Ignore SACL Flag:** Monitor the SACL flag associated with the file system watch data. (True, False)
- **Ignore DACL Flag:** Monitor the DACL flag associated with the file system watch data. (True, False)
- **Ignore Owner Security Flag:** Monitor the Owner Security flag associated with the file system watch data. (True, False)
- **Ignore Group Security Flag:** Monitor the Group Security flag associated with the file system watch data. (True, False)
- **Ignore Alternate Data Flag:** Monitor the Alternate Data flag associated with the file system watch data. (True, False)
- **Ignore File Dates Flag:** Monitor the File Dates flag associated with the file system watch data. (True, False)
- **Block Writes Flag:** Monitor the Block Writes flag associated with the file system watch data. (True, False)
- **Auto Exclude Files that have changed Flag:** Monitor the Auto Exclude Files that have changed flag associated with the file system watch data. (Enabled, Disabled)
- **Log Reads Flag:** Monitor the Log Reads flag associated with the file system watch data. (True, False)
- **Number of Intrusions to Keep:**
- **Keep Intrusion Size (in KB):**
- **Number of Revisions to Keep:**
- **Warn if Unlocked (in minutes):**
- **Number of Events to Keep:**
- **Corrective Action (On Add, On Change, On Delete):** The Corrective Action mode specified in the Object Group Watch Policy. (Restore, Update Baseline, Log, Prompt, Ignore)
- **Run (On Add, On Change, On Delete):** Custom script that is ran when an add, change, or delete action has occurred on monitored watch data. (Path/File Name)
- **Wait (On Add, On Change, On Delete):** Use remediation timeout period enforced on custom scripts that are ran when an add, change, or deleted action has occurred on the monitored watch data. (True, False)
- **Timeout (On Add, On Change, On Delete):** Remediation timeout period enforced on custom scripts that are ran when an add, change, or deleted action has occurred on the monitored watch data.

- **Parameters (On Add, On Change, On Delete):** *Pass filed and action parameters to the attached script ran on add, change, or delete actions.*



**Figure 152: Monitor Info Status Window tab**



**Figure 153: Monitor Info Summary Window tab**



**Figure 154: Monitor Info Details tab**

#### 6.1.3.4. REVIEWING OBJECT GROUP DATA PENDING REPAIR

The Pending Repair tab displays queue information associated with the remediation of folder, file and configuration data. The Pending Repair tab will append the number of pending repairs to the tab title. As changes are repaired they are automatically removed from the Pending Repair tab. Accessing the Object Group Pending Repair tab is accomplished by first clicking once on the Object Group name in the Object Group Tree to select it followed by clicking the Pending Repair tab in the Web Management Console Information Display Area.



***The Pending Repair tab also displays changes requiring CimTrak™ Administrator intervention. Intervention is required if the Prompt for Approval corrective action is enabled or the User Approval on Sync has been enabled and there was a communication failure between the Network Device Agent and the Master Repository.***

Severity	Event Date/Time	Absolute path	Modified By
----------	-----------------	---------------	-------------

**Figure 155: Pending Repair tab showing 3 pending repairs**

For each recorded event, the Object Group Pending Repair tab will display information corresponding to the following:

**Severity:** *The state of the pending repair.*

**Event Date/Time:** *The exact date and time of the detected event.*

**Absolute Path:** *File path affected by the detected event.*

**Modified By:** *The File System User responsible for the detected event.*

Generally, the items contained in the Pending Repair tab will automatically cycle out as the folders, files, and configurations are remediated on the monitored system. The Pending Repair tab will automatically refresh based on the Pending Repair Refresh Interval specified in the Master Repository Preferences dialog.

In the event the Pending Repairs exist due to the Prompt for Approval Corrective Action or a triggered User Approval on Sync the Changes Pending Approval dialog must be referenced. See a subsequent section for additional information on the Changes Pending Approval dialog.

Each Pending Repair message type has a corresponding icon that allows for quick visual reference to the urgency level of the event. These urgency levels are important to note when configuring E-Mail alert permissions. E-Mail alert permissions are explained in a subsequent section.

**Emergency:** *System is unusable. Highest level of event.*

**Alert:** *Take action immediately.*

**Critical:** *Critical conditions have occurred.*

**Error:** *Error conditions.*

**Warning:** *Warning conditions.*

**Notice:** *Normal condition that requires attention.*

**Information:** *Informational message.*

**Debug:** *Debug-level message. Lowest level of event.*

Specifics relating to message types are discussed in a subsequent section.

#### **6.1.3.4.1. FILTERING AND SORTING THE PENDING REPAIR TAB**

The Pending Repair Tab can be filtered to only show events matching the specified criteria. Accessing the Object Group Event Log is accomplished by first clicking once on the Object Group in the Object Group Tree to select it followed by clicking the Pending Repair tab in the Web Management Console Information Display Area.

To filter the information displayed in the Pending Repair Tab, drag and drop one of the column headers into the section labelled “Drag a column header here and drop it to group by that column.”

#### **6.1.3.5. OBJECT GROUP GENERATIONS**

The Object Group Generation Tab provides revision information for changes occurring to files, folders, operating system configurations contained in a Network Device Agent Object Group. Accessing the Object Group Generations Tab is accomplished by first clicking once on the Object Group in the Object Group Tree to select it followed by clicking the Generation tab in the Web Management Console Information Display Area.



The Generation Tab is broken into two sections:

## Revisions Table

### Revision Details

The screenshot displays the 'Generation' tab in a software interface. At the top, there are navigation tabs: 'Event Log', 'Change Log', 'Monitor Info', 'Pending Repair', and 'Generation'. The 'Generation' tab is active, showing a table with the following columns: Revision, Sub-revision, Date/Time, Changed by, # of Dirs, # of Files, and Total Size(bytes). The table contains five rows of data, with the second row (Revision 0000018) highlighted. Below the table, there is a 'Total Items: 43' label and a 'CSV Export' link. To the right, there is a 'Page Size' dropdown set to '100' and navigation buttons. Below the table, there is a 'Revision Information' section with three tabs: 'Revision Information', 'Details', and 'Change From Previous'. The 'Revision Information' tab is active, displaying the following details: Date of Revision: 3/13/2014 11:03:27, Revised by: admin, Revision: 0000018, Sub-Revision: 0000001, Number of Files: 14, Number of Directories: 3, and Notes: Lock Request.

Revision	Sub-revision	Date/Time	Changed by	# of Dirs	# of Files	Total Size(bytes)
0000019	0000001	3/19/2014 10:18:15	admin	3	14	40757180
0000018	0000001	3/13/2014 11:03:27	admin	3	14	40757180
0000017	0000025	3/13/2014 10:08:23	admin	Calculating...	Calculating...	Calculating...
0000017	0000024	3/13/2014 10:08:20	admin	Calculating...	Calculating...	Calculating...

Total Items: 43 [CSV Export](#)

Page Size: 100 1 / 1

**Revision Information** **Details** **Change From Previous**

Date of Revision: 3/13/2014 11:03:27  
 Revised by: admin  
 Revision: 0000018  
 Sub-Revision: 0000001  
 Number of Files: 14  
 Number of Directories: 3  
 Notes: Lock Request

**Figure 156: Object Group Generation Tab**

The Revisions Table displays overview information relating to each generation revision. Selecting a specific generation revision in the Revision Table will populate the corresponding information in the Revision Details section.

Information in the Revisions Table includes:

**Revision:** Primary revision number indicating the number of the generation.

**Sub-revision:** Secondary revision number indicating the number of events that have occurred since the primary generation was created.

**Date/Time:** Date and time associated with the creation of the revision or sub-revision.

**Changed by:** The CimTrak™ User account responsible for the creation of the revision or sub-revision.

**# of Dirs:** Quantity of directories contained in the revision or sub-revision.

**# of Files:** Quantity of files contained in the revision or sub-revision.

**Total Size (bytes):** The total amount of disk space utilized by the contents of the revision or sub-revision.

The Revision Details section displays detailed information relating to a revision or sub-revision. The Revision Details section has three tabs:

**Revision Information:** Details of the revision or sub-revision such as the date of the revision, revising user account, number of revisions, number of sub-revisions, number of files, number of directories, and notes.

**Details:** *Complete list of all files and folders contained in a generation. Files and folders indicate their generation status such as “Added”, “Deleted”, and “Modified”.*

**Change from Previous:** *Partial file list showing what files were “Added”, “Deleted” or “Modified” in the selected generation.*

#### **6.1.3.5.1. DOWNLOADING GENERATION DATA**

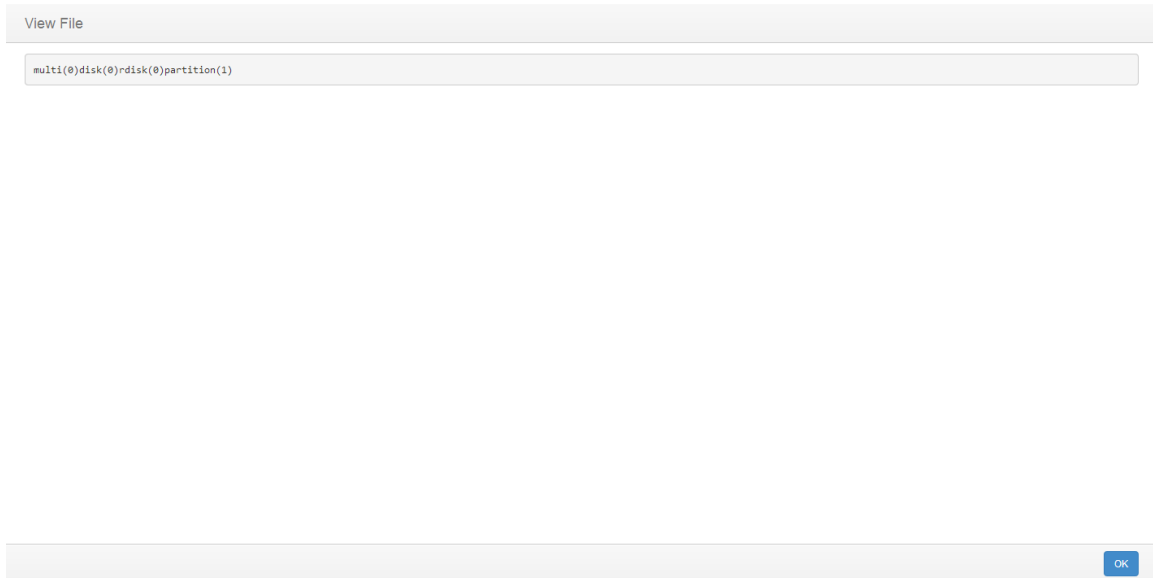
Each file stored in an Object Group generation has the capability to be downloaded and copied to a local system. An Object Group generation can be accessed by first clicking once on the Object Group in the Object Group Tree to select it followed by clicking the Generation tab in the Web Management Console Information Display Area.

Copies of generation data can be downloaded by right-clicking on the Revisions Table generation and selecting “Download” from the context menu. Additionally, copies of generation data can also be downloaded from the Revision Details Details tab or Change from Previous tab by right-clicking on the file or folder to download and then clicking “Download”.

#### **6.1.3.5.2. VIEWING AND COMPARING CONTENT OF OBJECT GROUP GENERATIONS**

Folders, files, and configurations monitored within an Object Group generation have the capability to be viewed and compared with other generations. An Object Group generation can be accessed by first clicking once on the Object Group in the Object Group Tree to select it followed by clicking the Generation tab in the Web Management Console Information Display Area.

To view the non-binary file contents associated with a file, select either the Details or Change from Previous tab in the Object Group Generation Revision Details section. Right-click on the file and then select “View”. The File View dialog will display.

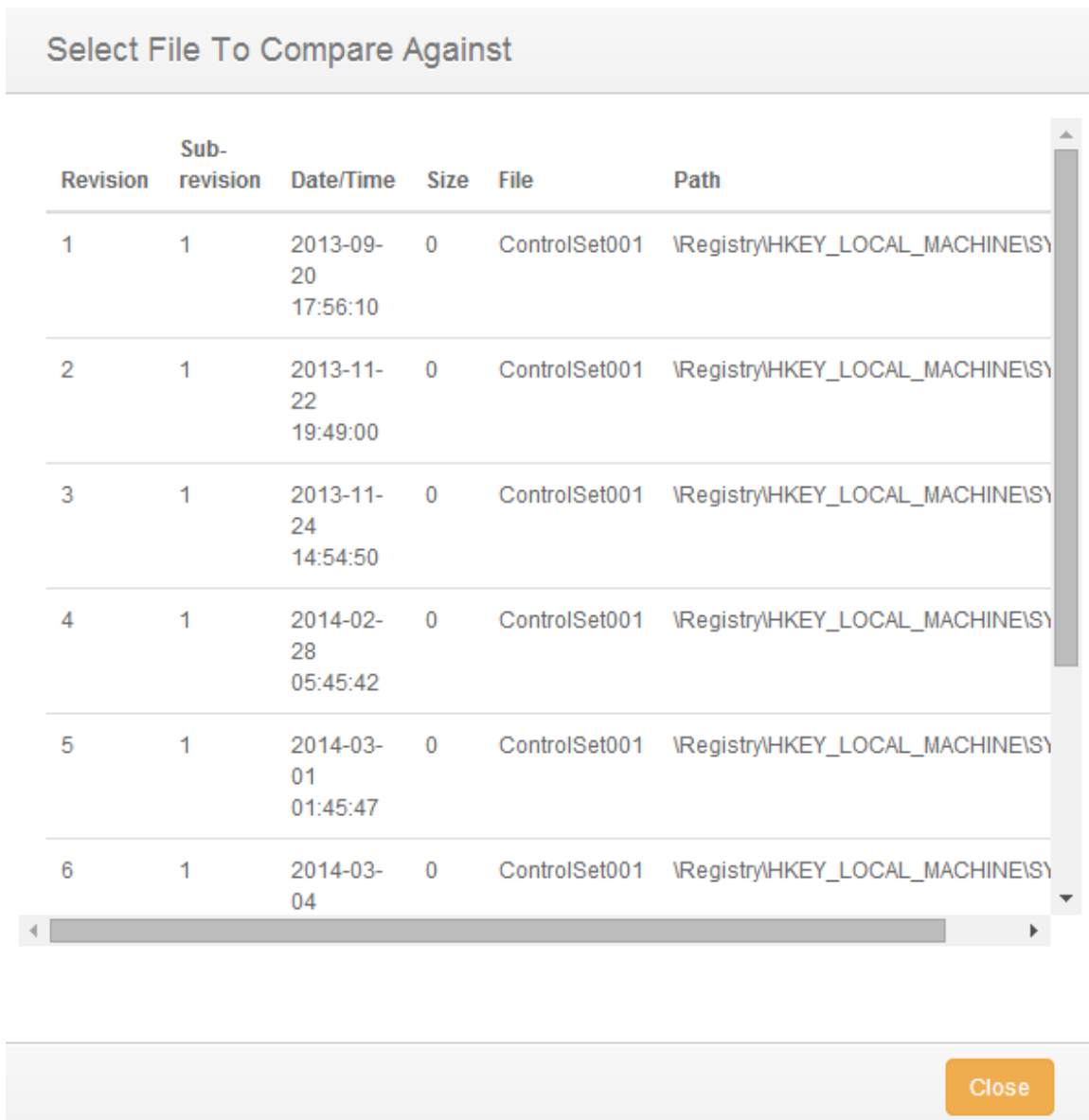


**Figure 157: File View dialog (non-binary)**

Click “Close” to exit the File View dialog.

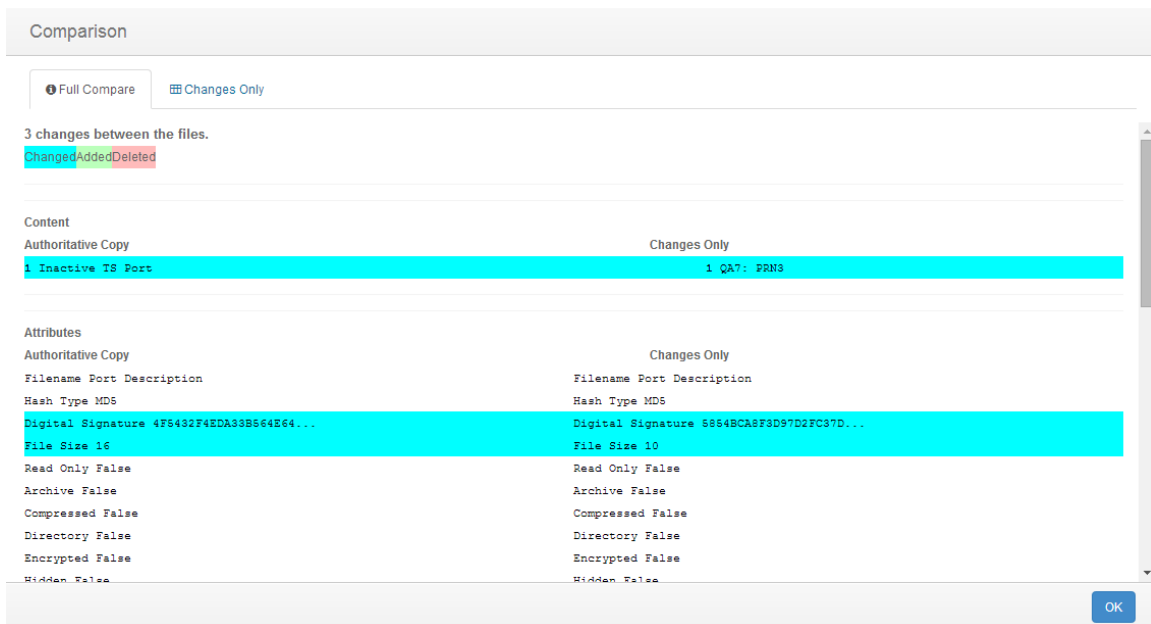
The Object Group Generations tab has the capability to compare previous generations with the current state of the file stored within the Master Repository to the local system. To compare a generation, click the “Object Group” node in the Web Management Console Object Group Tree. Select the generations tab.

To compare the file, from either the Details or Change from Previous tab, right-click on the file and then select either “Compare with Other Generation” or “Compare with Authoritative Copy (current)”. If “Compare with Other Generation” is selected the Select File to Compare Against dialog will display. Select the generation to compare with by clicking once on the revision. Click “OK” to perform the comparison or click “Cancel” to abort the comparison process. The File Comparison Results dialog will display.



**Figure 158: File to Compare Against dialog**

In the event “Compare with Authoritative Copy (current)” is selected the File Comparison Results will display comparing the current file content with the most current baseline.



**Figure 159: File Comparison Results dialog**

Click the “Close” button to exit the File Comparison Results dialog.

#### **6.1.3.5.2.1. UNDERSTANDING THE OBJECT GROUP CHANGE TAB FILE COMPARISON RESULTS DIALOG**

The File Comparison Results dialog displays anytime a comparison is performed between a detected change and the authoritative copy associated with watch properties. See section 0 for more information on performing file comparisons.

The File Comparison dialog is comprised of two primary sections.

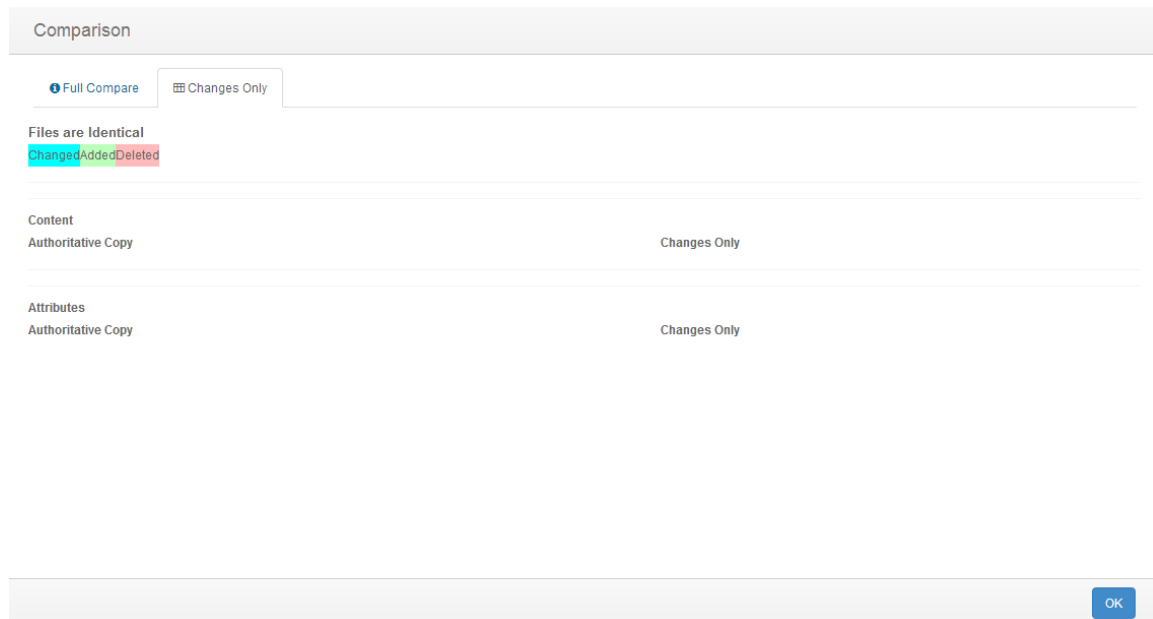
**Information Display Area**  
**Tab Browser**

##### **6.1.3.5.2.1.1. UNDERSTANDING THE FILE COMPARISON RESULTS DIALOG INFORMATION DISPLAY AREA AND TAB BROWSER**

The File Comparison Results dialog Tab Browser and Information Display Area allows authorized CimTrak™ users the capability visualize generation comparison data. The File Comparison Results dialog is accessible by accessing the context menu and selected Compare with Authoritative Copy (Current) in the Object Group Change Tab. See section 0 for more information on performing file comparisons.

The File Comparison Results dialog Information Display Area shows a side-by-side comparison of one generation revision of a detected change to the Master Repository Authoritative Copy. Lines that have been modified are highlighted in blue, lines that have been added are highlighted in green, and lines that have been deleted are highlighted in red.

By default, the “Full Compare” tab is selected in the File Comparison Results Tab Browser. The “Full Compare” tab shows all lines of a selected comparison. Selecting the “Changes Only” tab displays only the lines that have differences between the compared generations.



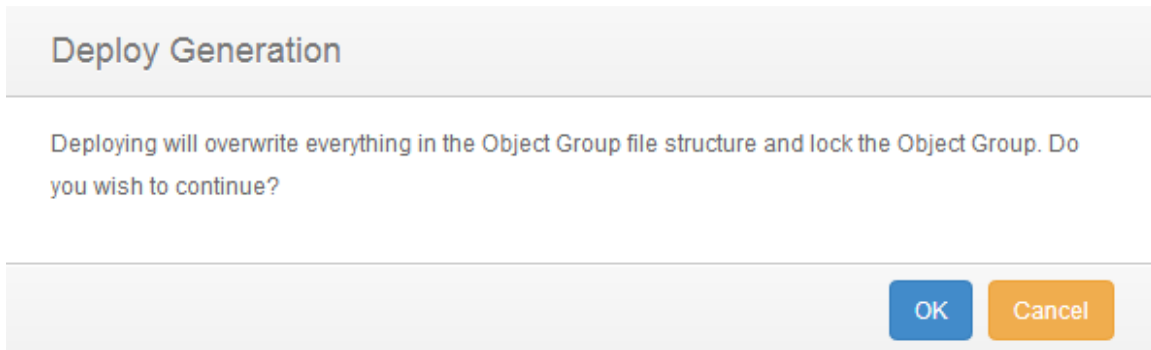
**Figure 160: File Comparison Results dialog Changes tab**

Click the Close button to exit the File Comparison Results dialog.

#### **6.1.3.5.3. DEPLOYING “ROLLING BACK” OBJECT GROUP GENERATIONS**

Depending on the remediation capabilities of the monitoring Object Group, the Generations tab may have the capability to deploy previous generations back to the File System. An Object Group generation can be accessed by first clicking once on the Object Group in the Object Group Tree to select it followed by clicking the Generation tab in the Web Management Console Information Display Area.

To deploy “roll back” a generation, select the generation in the Generation Tab Revisions Table, right-click, and then select “Deploy”. The Confirm Deploy dialog will display warning that deploying will overwrite everything in the Document Control with the content of this generation. Click “Yes” to proceed or “Cancel” to abort the operation.



**Figure 161: Confirm Deploy dialog**

Upon clicking “Yes” on the Confirm Deploy dialog the Notes dialog will appear. Enter any administrative notes relating to this deployment and then click “OK”. Click “Cancel” to abort the deployment.



**Figure 162: Notes dialog**

A new generation revision will be created with the rolled-back content. This newly created generation is the current generation.

#### **6.1.3.6. OBJECT GROUP PERMISSIONS**

Object Groups can be configured restrict access based on permission settings. Additionally, event notifications can be configured to notify CimTrak™ Users about events relating to the Object Group. Accessing Object Group permissions is accomplished by first clicking once on the File Object Group in the Object Group Tree to select it and then right-clicking and selecting “Permissions.” The Security Permissions dialog will display.

By default each Object Group will have the following permissions:

##### **Administrators**

**Create Objects:** *Create Network Device Agent Object Groups.*

**Edit:** *Edit Network Device Agent settings.*

**Lock:** *Enable active monitoring of Object Group Data.*

**Reports:** *View reports relating to the Object Group contents.*

**Unlock:** *Disable active monitoring of Object Group Data.*

**View:** *View contents and configurations relating to the Object Group.*

##### **Auditors**

**Reports:** View reports relating to Object Group contents.

**View:** View contents and configurations relating to the Object Group..

**Installers**

Attach CimTrak™ Agents to a Master Repository. (Not applicable for Object Groups).

Permissions for Object

Add

Group or User Names

Group	Administrators	
Group	Auditors	
Group	Email_Testing	Remove
Group	Installers	

Permissions	Allow	Deny
Create Objects	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Edit	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lock	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Reports	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Unlock	<input checked="" type="checkbox"/>	<input type="checkbox"/>
View	<input checked="" type="checkbox"/>	<input type="checkbox"/>

☒ Apply permissions to children recursively

OKCancel

**Figure 163: Object Group Security Permissions dialog**

Default access permissions associated with the Administrators, Auditors, and Installers User Groups cannot be changed. It is possible to modify E-mail alert notices for Administrator and Auditor user groups. Available E-mail alert types include:

Emergency  
Alert



Critical  
Error  
Warning  
Notice  
Information

Additional information relating to these alert types is described in a subsequent section.

#### **6.1.3.6.1. MODIFYING AN EXISTING USER/GROUP OBJECT GROUP PERMISSIONS**

It is possible to modify existing user and group Object Group Permissions and E-mail notification settings. Accessing Object Group permissions is accomplished by first clicking once on the Object Group in the Object Group Tree to select it and then right-clicking and selecting “Permissions.” The Security Permissions dialog will display.

Select the existing user or group by clicking once on the CimTrak™ User or Group name in the Group or User Names section of the Security Permissions dialog. The Permissions section of the Security Permissions dialog will update to show the permissions currently assigned to the selected user or group.



***Selecting a group will apply the selected permissions and E-mail notification settings to all members of the group. Selecting a single user will apply the selected permissions and E-mail notification settings to only that single user account.***

To add or remove permissions click the “Allow” or “Deny” checkbox corresponding to the permission being configured. Available permissions include:

**Create Objects:** *Create Network Device Agent Object Groups.*

**Edit:** *Edit Object Group control contents.*

**Lock:** *Enable active monitoring of Object Group Data*

**Reports:** *View reports relating to Object Group contents.*

**Unlock:** *Disable active monitoring of Object Group Data*

**View:** *View contents and configurations relating to the Object Group.*

**Email Emergency:** *Receive alerts relating to emergency level notifications.*

**Email Alert:** *Receive alerts relating to alert level notifications.*

**Email Critical:** *Receive alerts relating to critical level notifications.*

**Email Error:** *Receive alerts relating to error level notifications.*

**Email Warning:** *Receive alerts relating to warning level notifications.*

**Email Notice:** *Receive alerts relating to notice level notifications.*

**Email Information:** *Receive alerts relating to information level notifications.*

To apply the permission settings to all children objects, ensure that the Apply permissions to children recursively checkbox is selected.

When completed, click “OK” to apply the permission and alert settings. Click “Cancel” to abort the security permission configuration.



***Permissions and notification settings can be inherited from parent objects (such as the Network Device Agent) if the permissions are created at a parent level.***



***Permissions and notification settings are not automatically inherited for new objects. It will be necessary to manually assign the permissions and notification settings to the object.***

#### **6.1.3.6.2.    ADDING AND REMOVING USERS AND GROUPS TO OBJECT GROUP PERMISSIONS**

It is possible to add additional users and groups to the Security Permissions dialog so that Object Group Permissions and E-mail notification settings can be assigned or changed. Accessing Object Group permissions is accomplished by first clicking once on the Object Group in the Object Group Tree to select it and then right-clicking and selecting “Permissions.” The Security Permissions dialog will display.

To add a new local CimTrak™ User or Group, click the Add button. The Add Users dialog will display listing all available local users and groups.

Select Users or Groups

Q Search

	Type	Name
<input type="checkbox"/>	User	aaaa
<input type="checkbox"/>	User	wade
<input type="checkbox"/>	User	knightrider
<input type="checkbox"/>	User	payton
<input type="checkbox"/>	User	Pippen
<input type="checkbox"/>	User	Hanks
<input type="checkbox"/>	User	Rose
<input type="checkbox"/>	User	Garnett
<input type="checkbox"/>	User	Fridge
<input type="checkbox"/>	User	alberts
<input type="checkbox"/>	User	jovo2

OKCancel

Figure 164: Add Users dialog

Select the local CimTrak™ User or Group to add by selecting the checkbox to the left of the name. Click “OK” to add the User or Group. Click “Cancel” to abort the addition process. The selected user or group will now display in the Group or User Names section of the Security Permissions dialog.

## 7. Users and Groups

### 9.1. MANAGING MASTER REPOSITORY USERS & GROUPS FROM THE MANAGEMENT CONSOLE

To help improve the functionality, deployment, and security of the Master Repository, CimTrak™ supports the creation of additional user accounts. User accounts and groups support prescribing differing access permissions based on the purpose and the account.

During the installation of the CimTrak™ Master Repository a single user account was created. This first user account was automatically added to the “Administrators” group. For functionality reasons, at least one administrator-level account must exist at all times.

The Users dialog provides the functionality to view, edit, delete, and add CimTrak™ users and groups. Accessing the User Maintenance dialog can be accomplished by first clicking once on the Master Repository in the Object Group Tree to select it and then right-clicking and selecting “User Maintenance.” The User Maintenance dialog will display.

User Maintenance

Q

Search

Type	CimTrak Role	User	First Name	Last Name	Notes
User	Administrators	admin			
User	Administrators	Other Admin			
User	Administrators	Sam	Sam	Conley	
User	Standard	Justin	Justin	Chandler	
User	Standard	Rob	Robert	Johnson	
User	Standard	Ryan	Ryan	Rutkin	Notes?

Add User...

Add AD/LDAP User/Role...

Role Maintenance...

Close

**Figure 165: User Maintenance Dialog**

Each CimTrak™ user will be listed upon entering the CimTrak™ User Maintenance dialog.

From the CimTrak™ User Maintenance dialog, there are various actions that may be taken involving users.

## 9.2. ADDING A NEW USER

A new CimTrak™ user can be created by clicking the “Add User” button in the CimTrak™ User Maintenance dialog. For more information about the CimTrak™ User Maintenance dialog, please refer to section 0. Upon clicking the “Add User” button in the CimTrak™ User Maintenance dialog, the User Add/Edit dialog will appear.

User Add/Edit

Username	<input type="text"/>	Role	Administrators		
Password	<input type="password"/>	Confirm Password	<input type="password"/>		
First Name	<input type="text"/>	Last Name	<input type="text"/>	Title	<input type="text"/>
Address	<input type="text"/>				
City	<input type="text"/>	State	<input type="text"/>	Zip	<input type="text"/>
Email Address	<input type="text"/>				
Phone	<input type="text"/>	Extension	<input type="text"/>	Fax	<input type="text"/>
Alt. Phone	<input type="text"/>	Alt. Extension	<input type="text"/>	Pager	<input type="text"/>

Figure 166: User Add/Edit dialog

The CimTrak™ User Add/Edit dialog provides various fields, allowing the user to associate different data with a specific user. These fields are.

- **Username\***: The name of the CimTrak™ user. This will be used to log into CimTrak™.
- **Role\***: The CimTrak™ role of the CimTrak™ user.
- **Password\***: The password for the CimTrak™ user. This will be used to log into CimTrak™.
- **Confirm Password\***: Confirmation of the entered user password. The value entered into this field must match the value entered into the Password field.
- **First Name**: The first name of the user.
- **Last Name**: The last name of the user.
- **Title**: The title of the user.
- **Address**: The address of the user.
- **City**: The city where the user lives.
- **State**: The state where the user lives.
- **Zip**: The zip code of the area where the user lives.
- **Email Address**: The email address of the user.
- **Phone**: The phone number of the user.
- **Extension**: The phone extension of the user.

- **Fax:** The fax number of the user.
- **Alt. Phone:** The alternate phone number for the user.
- **Alt. Extension:** The phone extension for the alternate phone number of the user.
- **Pager:** The pager number for the user.
- **Note:** Additional notes to be associated with the user.

*Fields marked with a “\*” are required.*

Once the required data has been entered, the configuration for the new user can be saved. To save the configuration for the new CimTrak™ user, click the Save button at the bottom of the screen. The new user will be added to CimTrak™ and the User Add/Edit dialog will close.

### **9.3. ADDING AN AD/LDAP USER OR ROLE**

A new CimTrak™ user can be created by clicking the “Add AD/LDAP User/Role” button in the CimTrak™ User Maintenance dialog. For more information about the CimTrak™ User Maintenance dialog, please refer to section 0. Upon clicking the “Add AD/LDAP User/Role” button in the CimTrak™ User Maintenance dialog, the Search AD/LDAP for Users and Groups dialog will appear.

In the Search AD/LDAP for Users and Groups dialog is an array of field used to search for the AD/LDAP User or Group. These field are:

- **Domain:** The domain of the AD/LDAP Server.
- **Member of Group (optional):** A field which will filter the result set of the search to only users who belong to the group listed in this field. This field is optional.
- **Search Groups/Search Users:** Two checkboxes which denote whether the search will be performed for Users or Groups. One of these checkboxes must be checked.
- **Search for String(s):** A search string that will be used to query to AD/LDAP Server with. This field may be a TODO separated list of search strings.

After entering the required information, you may search the AD/LDAP Server for a User or Group by clicking the Search button in the bottom right-hand corner of the screen. Upon clicking the Search button the Add CimTrak Role to AD/LDAP Group or User dialog will appear containing the results of your search.

Add CimTrak Role To AD/LDAP Group or User

Q Search

	Type	CimTrak Role	Username	First Name	Last Name	Notes
<input type="checkbox"/>	User	None	cimtrak.local\admin	Ad	Min	
<input type="checkbox"/>	User	None	cimtrak.local\Administrator			Built-in account for administering the computer/domain
<input type="checkbox"/>	User	None	cimtrak.local\cimcor	cimcor	admin	default
<input type="checkbox"/>	User	None	cimtrak.local\ef46-admin	ef46-admin	ef46-admin	

Please verify CimTrak role to apply to this User(s)/Group(s)
Administrators
Add with the selected role
Close

**Figure 167: Add CimTrak™ Role to AD/LDAP Grou or User Dialog**

To apply a User or Group from your search results to a CimTrak Role, select the search result by checking the checkbox for that result and click the “Add with selected role” button in the bottom right-hand corner of the screen. The selected search result will be applied to the selected CimTrak role. A CimTrak role for application can be selected by the select box in the bottom of the screen.

**9.4. EDITING AN EXISTING CIMTRAK USER OR ROLE**

A CimTrak™ User or Role can be edited by first entering the User Maintenance dialog and clicking on the User or Role you wish to edit. For more information on the User Maintenance dialog, please refer to section 0. Upon clicking the User or Role you wish to edit, the User Add/Edit dialog will appear with the User or Role’s current data populating the fields of this screen. For more information on the User Add/Edit dialog, please refer to section 9.2. The data within these fields can be edited. Once the desired changes have been made to the selected CimTrak™ User or Role, you may save these changes by clicking the Save button in the bottom right-hand corner of the screen. To delete the selected user, click the Delete button in the bottom right-hand corner of the screen.

## 8. Creating, Applying, and Using Tags

### 11.1. MANAGING TAGS

It is possible to associate a “tag” with an agent from the Object Group Tree for grouping and/or filtering. Tags can later be used to filter the associated items under “Bulk Operations” when applying templates or modifying Agent Properties. Tags are added, created, or modified by right-clicking on an area in the Object Group Tree and selecting “Tags” from the context menu. The Object Tag Assignment dialog will appear.

### Object Tag Assignments

Add Tag

Search

Tag Name	Description	Delete
PCI E-Commerce		<div><div></div>Delete</div>
Tag 2	A new description.	<div><div></div>Delete</div>

Close

Figure 168: Object Tag Assignment Dialog



## 11.2. ASSOCIATING PRECONFIGURED TAGS

A preconfigured Tag can be associated to a Cimtrak™ Agent from the Object Tab Assignment Dialog screen. The Object Tag Assignment screen can be accessed by right-clicking on a Cimtrak™ Agent in the Object Group Tree and selecting “Tags.” For more information about accessing the Object Tag Assignment screen, please refer to section 11.1.

To associate a preconfigured tag with the selected Cimtrak™ Agent, click the “Add Tag” button near the top of the Object Tag Assignment dialog screen. The Select Tag dialog will appear.

Select Tags

Search

Select	Tag Name	Description
<input type="checkbox"/>	another tag	This is another tag
<input type="checkbox"/>	jovowashere	
<input type="checkbox"/>	myTag	my description
<input type="checkbox"/>	newTag	A new description.
<input type="checkbox"/>	newtag3	newtag3 description
<input type="checkbox"/>	newtag4	newtag4 description
<input type="checkbox"/>	testTag	This is a test tag.

Create New Tag

Add

Cancel

Figure 169: Select Tags dialog screen

You can apply a preconfigured tag to a Cimtrak™ Agent by clicking the checkbox under the “Select” column that is associated with the desired tag.

Select Tags

Q

Search

Select	Tag Name	Description
<input type="checkbox"/>	another tag	This is another tag
<input type="checkbox"/>	jovowashere	
<input type="checkbox"/>	myTag	my description
<input checked="" type="checkbox"/>	newTag	A new description.
<input type="checkbox"/>	newtag3	newtag3 description
<input type="checkbox"/>	newtag4	newtag4 description
<input type="checkbox"/>	testTag	This is a test tag.

Create New Tag

Add

Cancel

**Figure 170: Select Tag dialog screen (tag selected)**

Once the desired tag has been selected, click the “Add” button in the lower-left corner of the Select Tag dialog screen to add the selected tag to the selected Cimtrak™ Agent. The Object Tag Assignments dialog screen will appear with the newly assigned tag showing in the Assigned Tags section.

Object Tag Assignments

+ Add Tag

Q

Search

Tag Name	Description	Delete
newTag	A new description.	<div><div>×</div>Delete</div>
PCI E-Commerce		<div><div>×</div>Delete</div>
Tag 2	A new description.	<div><div>×</div>Delete</div>

Close

Figure 171: Object Tag Assignments dialog screen (new tag assigned)

11.3. CREATING NEW TAGS

A new Tag can be created from the Object Tab Assignment Dialog screen. The Object Tag Assignment screen can be accessed by right-clicking on an agent in the Object Group Tree and selecting “Tags.” For more information about accessing the Object Tag Assignment screen, please refer to section 11.1.

To create a new tag, continue to the Select Tag dialog screen by clicking the “Add Tag” button near the top of the Object Tag Assignment dialog screen. The Select Tag dialog will appear.

Select Tags

Search

Select	Tag Name	Description
<input type="checkbox"/>	another tag	This is another tag
<input type="checkbox"/>	jovowashere	
<input type="checkbox"/>	myTag	my description
<input type="checkbox"/>	newTag	A new description.
<input type="checkbox"/>	newtag3	newtag3 description
<input type="checkbox"/>	newtag4	newtag4 description
<input type="checkbox"/>	testTag	This is a test tag.

Create New Tag

AddCancel

**Figure 172: Select Tags dialog screen**

From the Select Tag dialog screen, click the Create New Tag button on the lower-left corner of the dialog screen to continue to the Create/Edit Tag screen.

Create/Edit Tag

Tag Name:

Description:

OK Cancel

**Figure 173: Create/Edit Tag dialog screen**

The Create/Edit Tag dialog screen is comprised of two primary sections:

- **Tag Name (Required):** The desired name which you will associate to the newly created tag. This name will show in the Select Tag dialog screen.
- **Description (Optional):** The desired description which you will associate to the newly created tag. This description will show in the Select Tag dialog screen.

Once you have populated the fields of the Create/Edit Tag dialog screen, click Ok to complete the tag creation. The tag will now show in the Select Tag dialog screen.

Create/Edit Tag

Tag Name:

Description:

OK Cancel

**Figure 174: Create/Edit Tag dialog screen**

Select Tags

Q Search

Select	Tag Name	Description
<input type="checkbox"/>	another tag	This is another tag
<input type="checkbox"/>	jovowashere	
<input type="checkbox"/>	myTag	my description
<input type="checkbox"/>	newtag3	newtag3 description
<input type="checkbox"/>	newtag4	newtag4 description
<input type="checkbox"/>	tagTest	This is a test of the create tag function.
<input type="checkbox"/>	testTag	This is a test tag.

Create New Tag

Add

Cancel

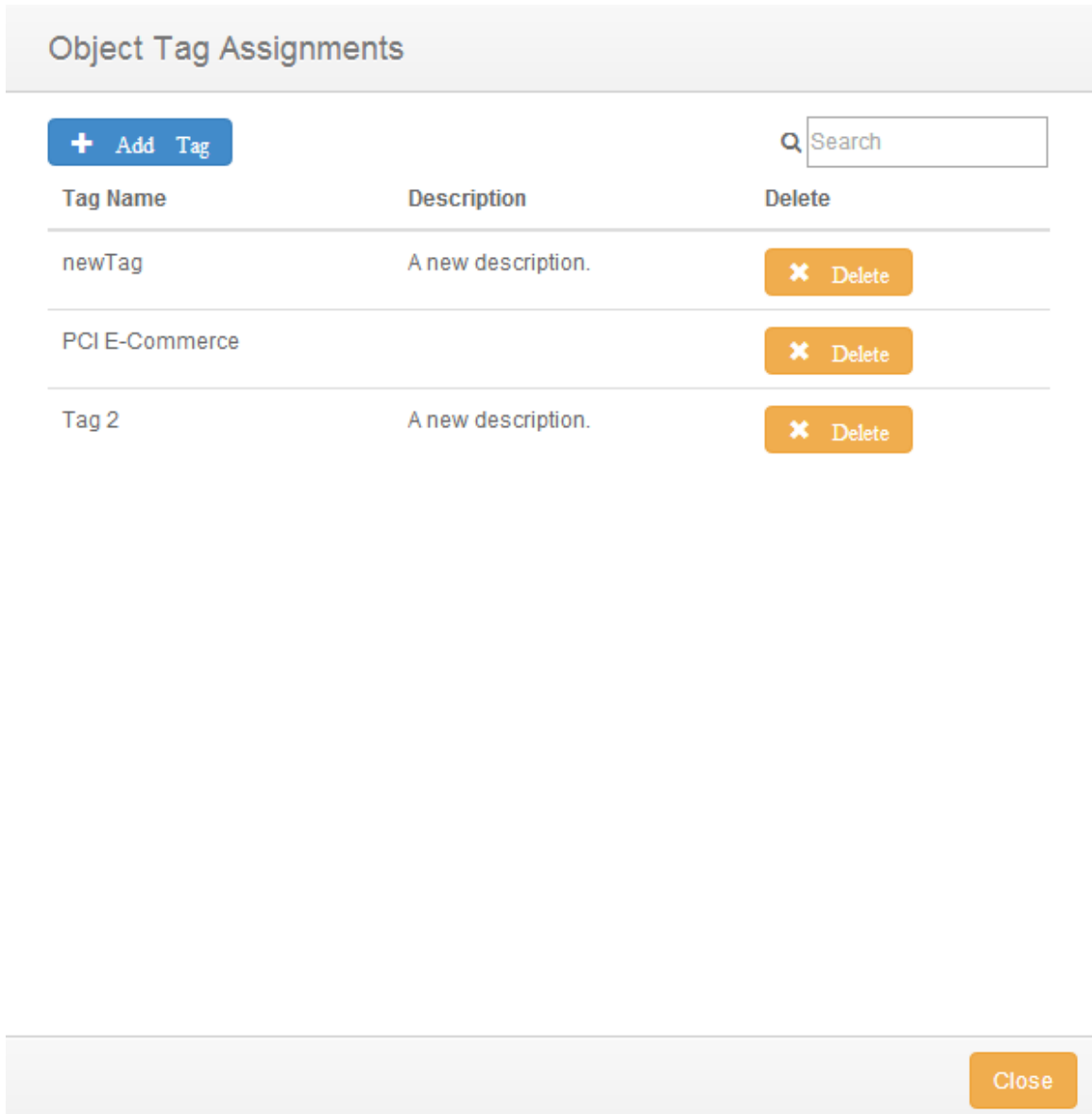
**Figure 175: Select Tags dialog screen (new tag)**

The newly created tag can be assigned to a Cimtrak™ Agent from the Select Tag dialog screen. For more information about assigning a tag to a Cimtrak™ Agent, please refer to section 11.2.

#### 8.4. DELETING TAGS

A tag can be disassociated from a CimTrak™ Agent through the Object Tab Assignment Dialog screen. The Object Tag Assignment screen can be accessed by right-clicking on an agent in the Object Group Tree and selecting “Tags.” For more information about accessing the Object Tag Assignment screen, please refer to section 11.1.

To disassociate a tag from a CimTrak™ Agent, click the Delete button that is associated with the tag that you wish to disassociate.



**Figure 176: Object Tag Assignments dialog screen (new tag assigned)**

Upon clicking the Delete button of an associated tag, the tag will be disassociated from the Cimtrak™ Agent and the tag will no longer be shown in the Object Tag Assignments dialog screen.

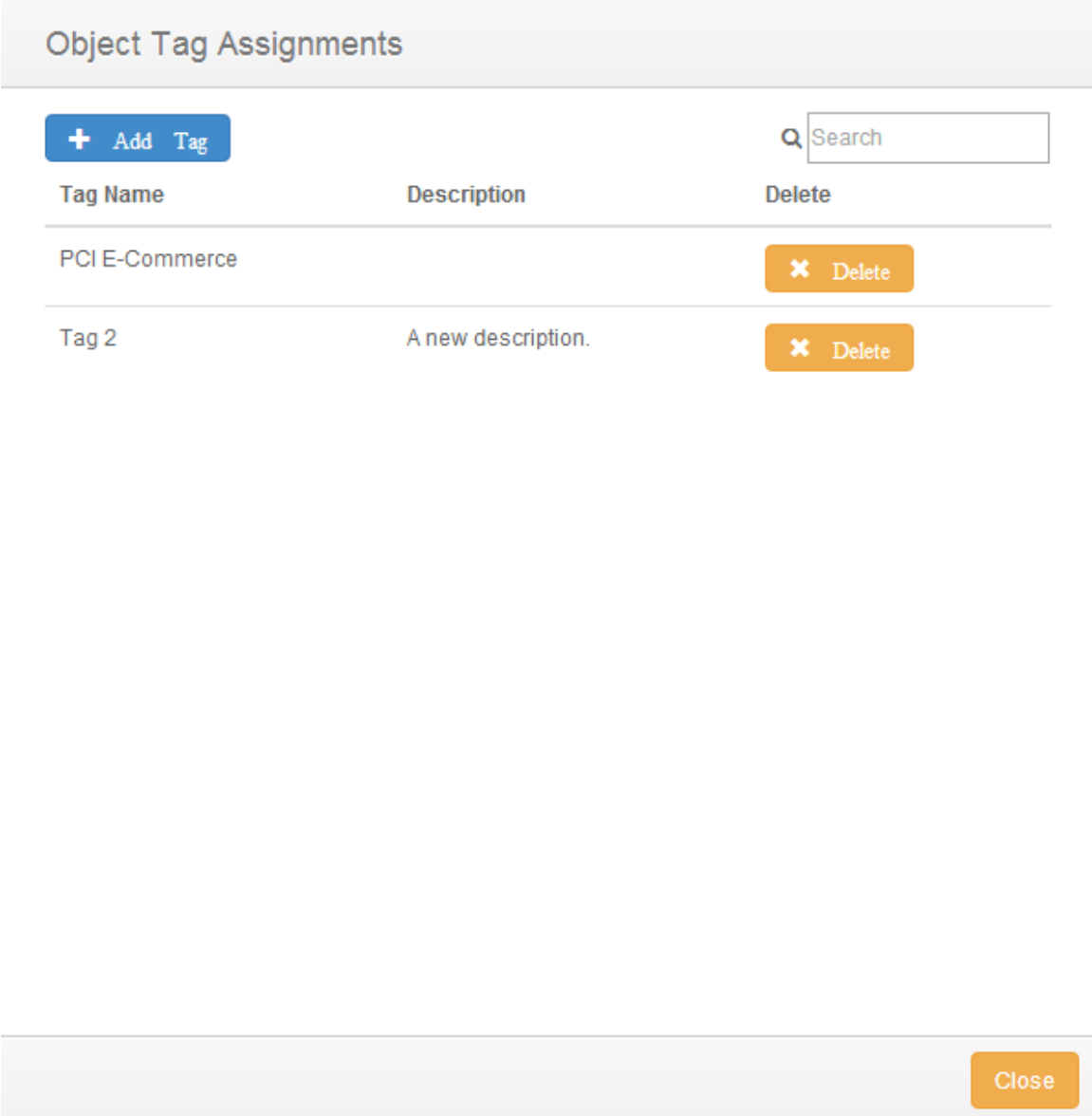


Figure 177: Object Tag Assignment dialog screen (tag deleted)



## 9. CimTrak™ Integrated Reporting

### 9.4. ACCESSING CIMTRAK™ REPORTING

Authorized CimTrak™ Administrators, Users, and Auditors have the capability to execute and download reports to display audit log and event information. Reports can be executed via the CimTrak™ Web Management Console Graphical User Interface or using the CimTrak™ Command Line Tool. See section **Error! Reference source not found.** for information explaining running reports from the Command Line Tool.

Reports are accessible for each level of Object listed in the Web Management Console's Object Group Tree. Information on accessing CimTrak™ Reports based on the Object level is as follows. Executing each of these methods will display the corresponding Available Reports dialog.

#### **CimTrak™ Master Repository:**

- On the Web Management Console Menu Bar click **Reports**→ **View Reports**

#### **CimTrak™ Area:**

- Right-click on the Area name in the Object Group tree and select Reports in the context menu.

#### **CimTrak™ File System/Network Device Agent:**

- Right-click on the CimTrak™ Agent name in the Object Group tree and select Reports in the context menu.

#### **CimTrak™ Object Group:**

- Right-click on the Object Group name in the Object Group tree and select Reports in the context menu.

#### **CimTrak™ Document Control:**

- Right-click on the Document Control name in the Object Group tree and select Reports in the context menu.

Additionally, other CimTrak™ components not listed execute reports using the methods outlined above.

Reports run or downloaded for a selected Object level show results for all children object of the corresponding level. For instance, reports run or downloaded at the Master Repository level display information associated to all children Objects including:

- **CimTrak™ Master Repository**
- **All CimTrak™ Areas**

- **All CimTrak™ File System/Network Device Agents**
- **All CimTrak™ Object Groups**
- **All CimTrak™ Document Controls**

Reports run at an Area Level will display information associated to all children Objects of the specified Area including:

- **Specified CimTrak™ Area**
- **CimTrak™ File System/Network Device Agents contained in the specified Area**
- **CimTrak™ Object Groups contained in the specified Area**
- **CimTrak™ Document Controls contained in the specified Area**

Reports run at an Agent Level will display information associated to all children Objects of the specified Agent including:

- **Specified CimTrak™ File System/Network Device Agent**
- **CimTrak™ Object Groups contained in the specified CimTrak™ Agent**
- **CimTrak™ Document Controls contained in the specified CimTrak™ Agent**

Reports run at an Object Group Level will only display information for the selected Object Group. Reports run at a Document Control level only display information for the selected Document Control.

The Available Reports dialog is explained in section 9.1.2.

### **9.1.2. NAVIGATING THE AVAILABLE REPORTS DIALOG AND EXECUTING REPORTS**

Authorized CimTrak™ Administrators, Users, and Auditors have the capability to execute and download reports to display audit log and event information. Executing reports from the Web Management Console is performed using the Available Reports dialog.

Reports are accessible for each level of Object listed in the Web Management Console's Object Group Tree. Information on accessing CimTrak™ Reports based on the Object level is explained in section 9.4.

Select Report

Q Search

Category	Name	Description
Enhanced Reporting	Change from Previous by Object	A listing of all files that were added/modified/deleted from all generations within the given date/time range to it's most recent previous generation.
Enhanced Reporting	Disabled Object Group Policies	The Disable Object Group Policies report displays all Object Group Policies that are currently unlocked. Additionally, this report shows when the Object Group Policy was unlocked, the responsible party, and a timer indicating the lenght of time.
Enhanced Reporting	Event Summary Report	The Event Summary Report displays a summary of all event recorded by CimTrak for a specified date range. Data is displayed relating to event priority, criteria, and action.
Enhanced Reporting	Generation Elements	The Generation Elements Report displays individual Object Group generation and subrevision details. For each result, the Generation Elements Report is capable of displaying a variety of generation and subrevision information such as the CimTrak user responsible for creating a generation and any additional note details.
Enhanced Reporting	Groups by Compliance	The Groups by Compliance Report lists all groups based on their configured compliance type.
Enhanced Reporting	Incident Summary Report	The Incident Summary Report displays a numeric total for all additions, modifications, and deletions for all Object Group Policies.
Enhanced Reporting	Incidents by Object	The Incidents by Objectreport displays a quantity of variances over a period of time in addition to summary information of the last reported variance.
Enhanced Reporting	Revision History	A listing of all revisions to files and objects in a given date range.

OK

**Figure 178: Available Reports dialog (Master Repository Level)**

The Available Reports dialog displays all reports available for the selected Object level. Each report is classified into a general level or can be queried to match a specific tag. For more information on tags, refer to section 0.

Reports included in the CimTrak™ Reports level are used to audit CimTrak™ Web Management Console and Master Repository health, access, and user accounts. Reports included in the Enhanced Reporting level are used to audit change events detected (and optionally remediated) by CimTrak™. Details of these associated reports are explained in a section 9.1.2.1.

To execute a report navigate the Available Reports dialog to find the intended report. Select the report by clicking it once and then clicking the Generate Report button. The selected report will display.

CimTrak™ support staff has the capability to generate reports to perform custom functions for customer-specific requests. Additionally CimTrak™ Administrators with a programming background can modify reports. Generally CimTrak™ Reports consist of embedded HTML, SQL, JavaScript and LUA. To download the reports unexecuted code, navigate the Available Reports dialog to find the intended report. Select the report by clicking it once and then clicking the Download button. The Save As dialog will display. Select the location to save the report to. Once the report is modified it must be uploaded to the Master Repository. Uploading reports to the Master Repository is described in a section 9.6.



***When executing some reports a parameters dialog will display. The Parameters dialog allows for the specification of report parameters such as the date range, private key, chart type, and***

***optional query criteria. Populate the parameters dialog with appropriate information relating to the intended report criteria.***

### Report - Incident Summary Report

The Incident Summary Report displays a numeric total for all additions, modifications, and deletions for all Object Group Policies.

Start Date/Time:

End Date/Time:

Chart Type:

Pie Chart

Generate Report

OK

**Figure 179: Report Parameters dialog**

Once the report parameters are specified and the Continue button is clicked the selected report will generate.

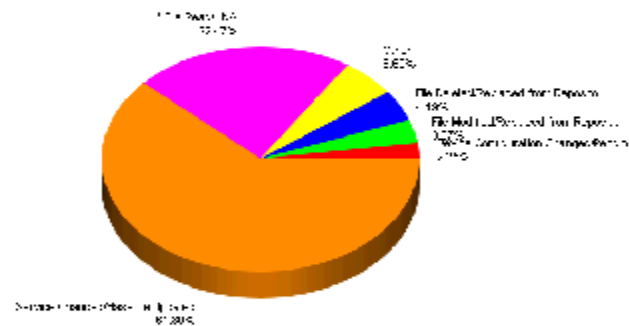
## Incident Summary Report

All Object Groups: TSS-9910



Report Generation Date/Time:	Tuesday June 14, 2011 at 20:55:02
Report Start Date/Time:	Wednesday June 01, 2011 at 13:00:00
Report End Date/Time:	Tuesday June 14, 2011 at 20:52:53
Report Generated By:	admin
Chart Type:	Pie Chart
Query File:	All Files
Query User:	All Users
Query Process:	All Processes
Query Forensic:	All Forensic Data

### Incidents Detected



Device Configuration Changed/Endpoint...	File Modified/Replaced from Repository
File Deleted/Replaced from Repository	Other
File Deleted/Replaced from Repository	Service Changed/Device Upgraded
File Deleted/Replaced from Repository	

Figure 180: Sample CimTrak™ Report (Page 1 of 2)

## Incident Summary Report

All Object Groups: TSS-9910



Incident Count	Description	Response
55	Service Changed	Baseline Updated
20	*File Read	*NA
4	File Deleted	Replaced from Repository
3	File Modified	Replaced from Repository
2	Device Configuration Changed	Pending User Approval
1	File Changed	Baseline Updated
1	File Added	File Removed and Stored
1	Directory Added	Directory Removed
1	User Changed	Baseline Updated
1	File Added	Baseline Updated

aboutblank

6/14/2011

Figure 181: Sample CimTrak™ Report (Page 2 of 2)



***CimTrak™ Utilizes Microsoft Windows Internet Explorer installed on the Web Management Console's operating system. Graphical information will not display in Internet Explorer versions less than 8.0.***

#### 9.1.2.1. EXPLAINING AVAILABLE CIMTRAK™ REPORTS

Authorized CimTrak™ Administrators, Users, and Auditors have the capability to execute and download reports to display audit log and event information. Executing reports from the Web Management Console is performed using the Available Reports dialog.

Reports are accessible for each level of Object listed in the Web Management Console's Object Group Tree. Information on accessing CimTrak™ Reports based on the Object level is explained in section 9.4.

General Reports are contained in the CimTrak™ Reports and Enhanced Reporting Report Groups. Expanding Report Groups is possible by clicking the corresponding "+". Clicking the corresponding "-" will collapse the selected Report Group.

#### **Enhanced CimTrak™ Reports:**

- **Diagnostic Analysis:** *The Diagnostic Analysis is intended for support purposes to determine database availability/integrity, version information, process information, incident totals.*
- **Object Group Configuration:** *The Object Group Configuration report displays configuration settings for all Objects in the Object Group tree.*
- **Active User Listing:** *The Active User Listing Report lists all CimTrak™ users that are currently active.*
- **Added User Listing:** *The Added User Listing Report lists all added CimTrak™ users that are currently active.*
- **Deleted User Listing:** *The Deleted User Listing Report lists all deleted CimTrak™ users.*
- **Failed Logon Attempts:** *The Failed Logon Attempts Report provides a detail listing of failed logon attempts over a user specified period of time.*
- **Locked Out Users:** *The Locked Out Users Report provides a detailed listing of all locked out CimTrak™ user accounts.*
- **Successful Logons (Administrators):** *The Successful Logons (Administrators) Report provides a detailed listing of successful authentications with the CimTrak™ Master Repository by CimTrak™ user accounts.*
- **Successful Logons (All Users):** *The Successful Logons (All Users) Report provides a detailed listing of successful authentications with the CimTrak™ Master Repository by CimTrak™ user accounts.*
- **Successful Logons (Auditors):** *The Successful Logons (Auditors) Report provides a detailed listing of successful authentications with the CimTrak™ Master Repository by CimTrak™ user accounts.*
- **Successful Logons (Installers):** *The Successful Logons (Installers) Report provides a detailed listing of successful authentications with the CimTrak™ Master Repository by CimTrak™ user accounts.*
- **Successful Logons (Other Users):** *The Successful Logons (Other Users) Report provides a detailed listing of successful authentications with the CimTrak™ Master Repository by CimTrak™ user accounts.*

### **Enhanced Reporting:**

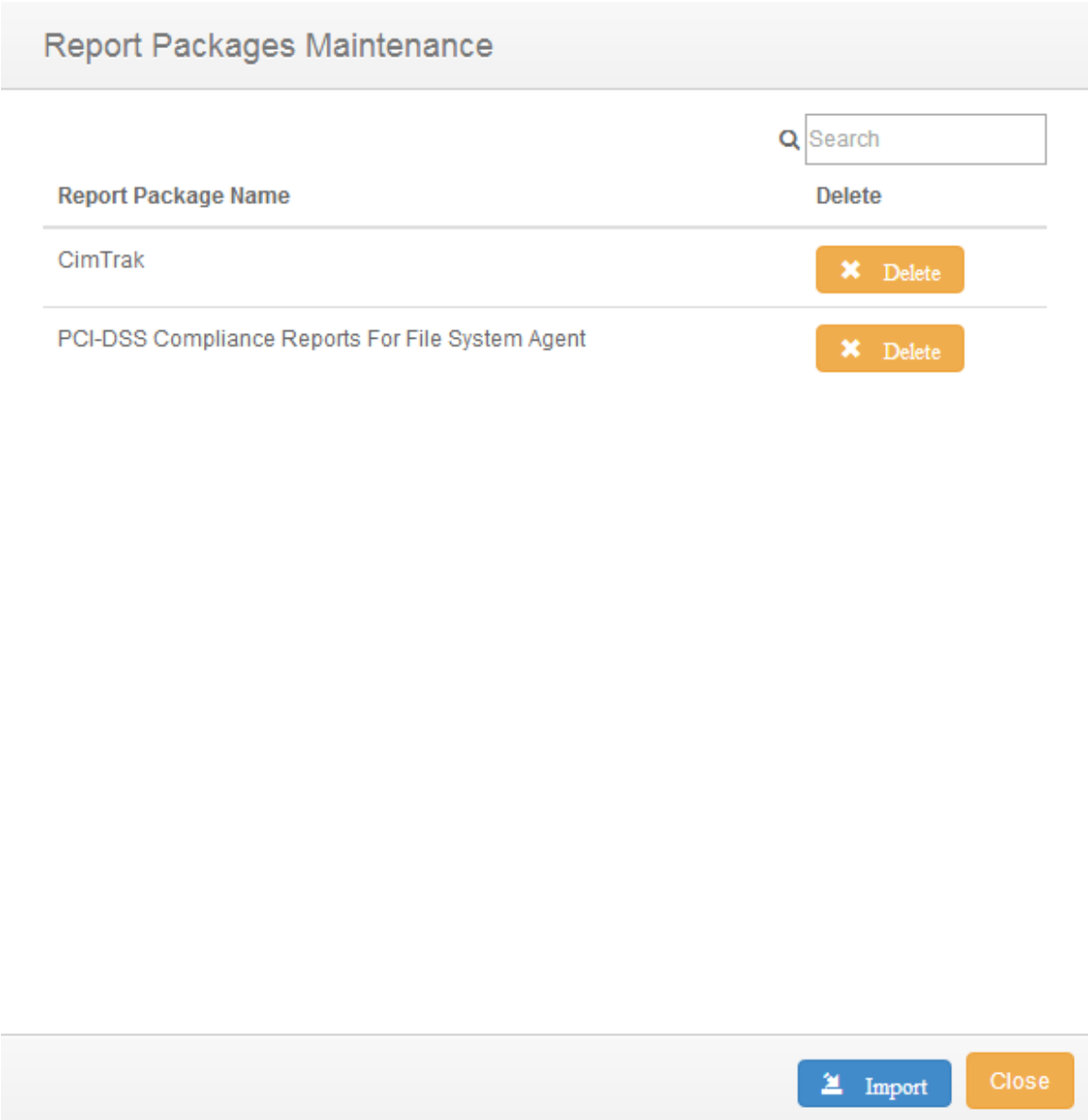
- **Disabled Object Group Policies:** *The Disabled Object Group Policies report displays all Object Group Policies that are currently unlocked. Additionally, this report shows when the Object Group Policy was unlocked, the responsible party, and a timer indicating the length of time.*
- **Event Summary Report:** *The Event Summary Report displays a summary of all events recorded by CimTrak™ for a specified date range. Data is displayed relating to event priority, criteria, and action.*
- **Generation Elements:** *The Generation Elements Report displays individual Object Group generation and sub-revision details. For each result, the Generation Elements Report is capable of displaying a variety of generation and sub-revision information such as the CimTrak™ user responsible for creating a generation and any additional note details.*
- **Groups by Compliance:** *The Groups by Compliance Report lists all groups based on their configured compliance type.*
- **Incidents by Object:** *The Incidents by Object report displays a quantity of variances over a period of time in addition to summary information of the last reported variance.*
- **Incident Summary Report:** *The Incident Summary Report displays a numeric total for all additions, modifications, and deletions for all Object Group Policies.*
- **Variance by Quantity:** *The Variance by Quantity Report displays a total of Object Group contents that have been added, modified, and/or removed from the monitored system.*
- **Variance Detail Report:** *The Variance Detail Report displays Object Group contents that have been added, modified, and/or removed from the monitored system. For each result, the Variance Detail Report is capable of displaying a variety of forensic-assisting information such as the operating system user responsible for the change, the responsible process, and associated change details.*
- **Variance Summary Report:** *The Variance Summary Report displays Object Group contents that have been added, modified, and/or removed from the monitored system. For each result, the Variance Detail Report is capable of displaying a variety of forensic-assisting information such as the operating system user responsible for the change and the responsible process.*
- **Variance Window Report:** *The Variance Window Report calculates the quantity of detected intrusions on locked objects during a specified period of time.*
- **Baseline Comparison Report:** *Only available at the Object Group Level, the Baseline Comparison report evaluates files/directories contained in one object group against the object group specified. The Baseline Comparison report requires that the original, authoritative baseline Object Group has the Audit Baseline Compliance Flag selected.*

### **9.5. WORKING WITH CIMTRAK™ REPORT PACKAGES**



Authorized CimTrak™ Administrators have the capability to add additional report packages to the CimTrak™ Master Repository. Additional report packages are often distributed with additional CimTrak™ components.

To add additional report packages, log into the CimTrak® Web Management Console using an Administrator account. Navigate to the Report Package Manager by right-clicking the Master Repository in the Object Group Tree and selecting “Report Packages . . .”



**Figure 182: Report Packages dialog**

By default, the CimTrak™ reporting package is installed. Click the Add button to navigate the Web Management Console host file system to select additional report packages to install. Select the appropriate report package and then click

Open. The selected report package will now be displayed in the Report Packages dialog. Click the OK button to complete the report package installation.

Removing a report package is achieved by selecting the Report package name in the Report Packages dialog and then clicking the Remove button. Click the OK button to complete the report package removal.

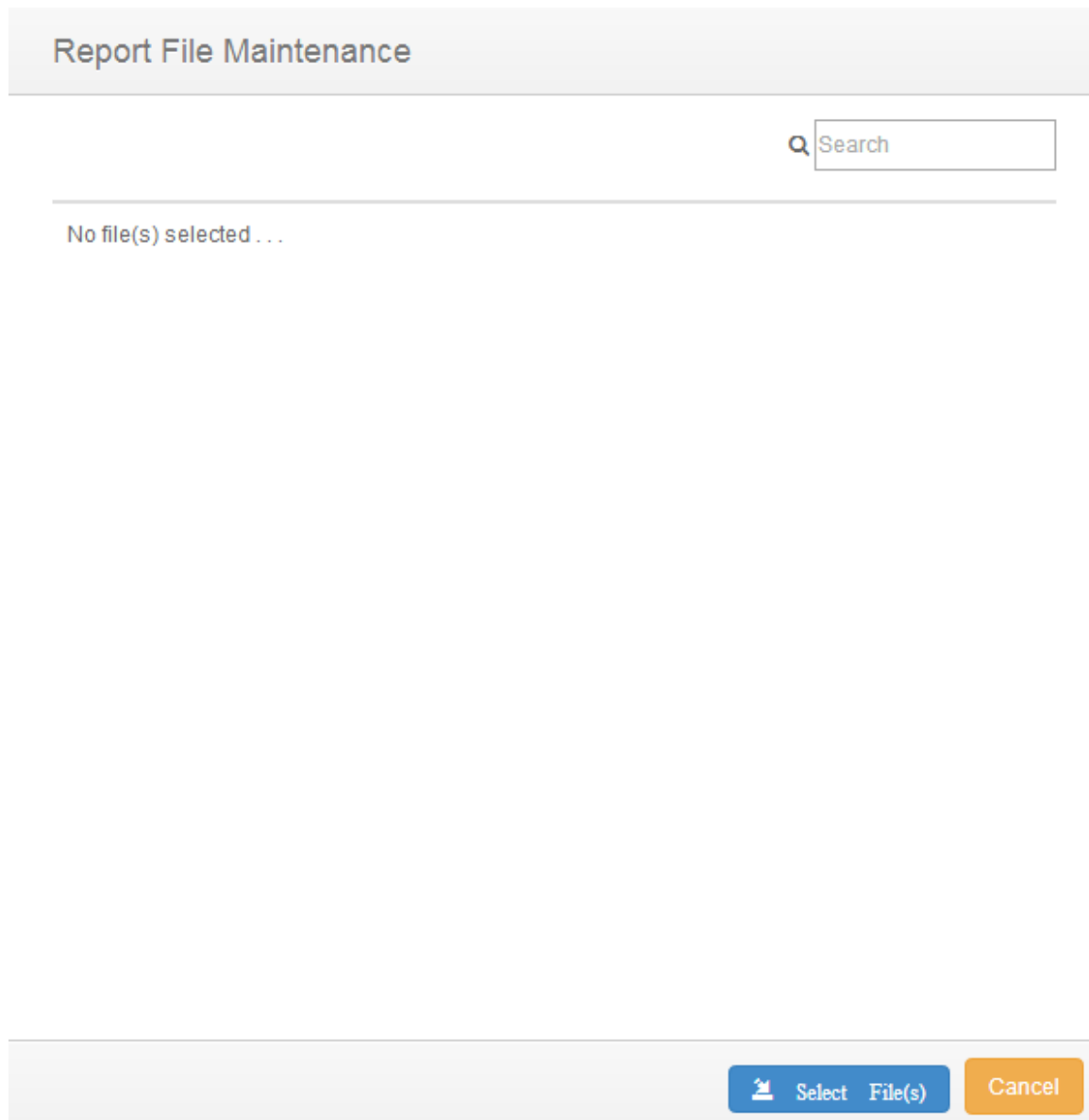


***Additional report packages may be available in your region. Contact an authorized CimTrak™ sales representative to acquire additional reporting packages.***

#### **9.6. UPLOADING ADDITIONAL CIMTRAK™ REPORTS**

Authorized CimTrak™ Administrators have the capability to add additional individual reports to the CimTrak™ Master Repository. Additional reports are often distributed with additional CimTrak™ components.

Log into the CimTrak® Web Management Console using an Administrator account. Navigate to the Report File Upload Manager by right-clicking the Master Repository in the Object Group Tree and then selecting “Upload Report File . . .” The Report File Maintenance dialog will display.



**Figure 183: Report File Maintenance dialog screen**

To upload a Report File, click the “Select File(s)” button. The Open dialog will show.

Browse the Web Management Console’s host operating system and select the report to upload. Click Open to upload the report to the Master Repository. Click Cancel button to abort the upload process.

## 10. Displaying Multiple Repositories in One Window

### 10.2. ACQUIRING ACCESS TO AN ADDITIONAL REPOSITORY.

The Web Management Console can display more than one repository. Configuring an additional repository can be done by a user that has object creation permission on the primary repository.

#### 10.2.1. CREATE AN API KEY ON THE REMOTE REPOSITORY.

Logon to the remote repository as a user with object creation permission on the repository. Open the repository properties dialog. Click the Repository API Key tab. Click the “Generate API Key for this Repository” button and the dialog shown below pops up. Type a description for the API key in the text box and then click the “Generate API Key” button.

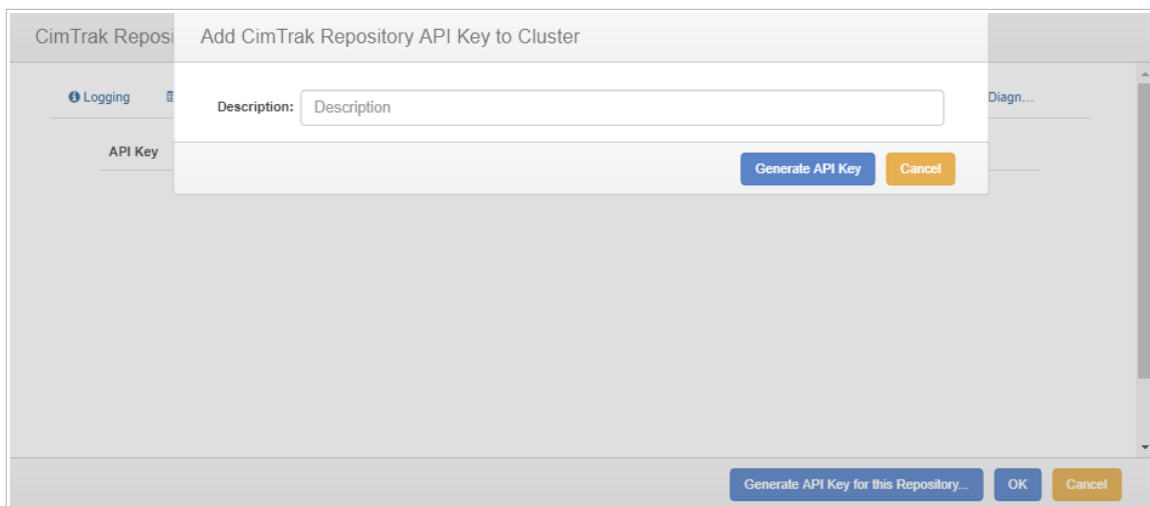


Figure 184: Add Repository API Key dialog

An API key with the entered description will show up in the Repository API Key tab. This API Key will be entered into the other repository.

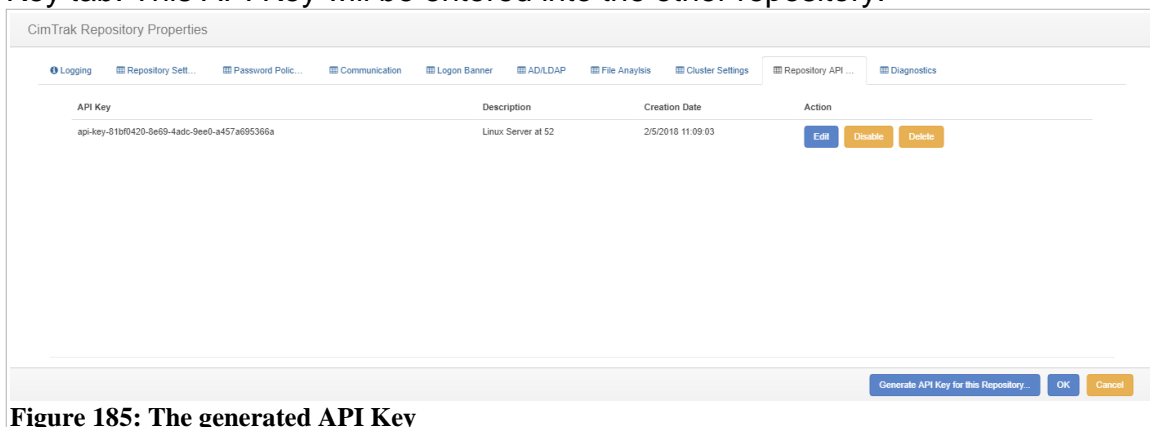
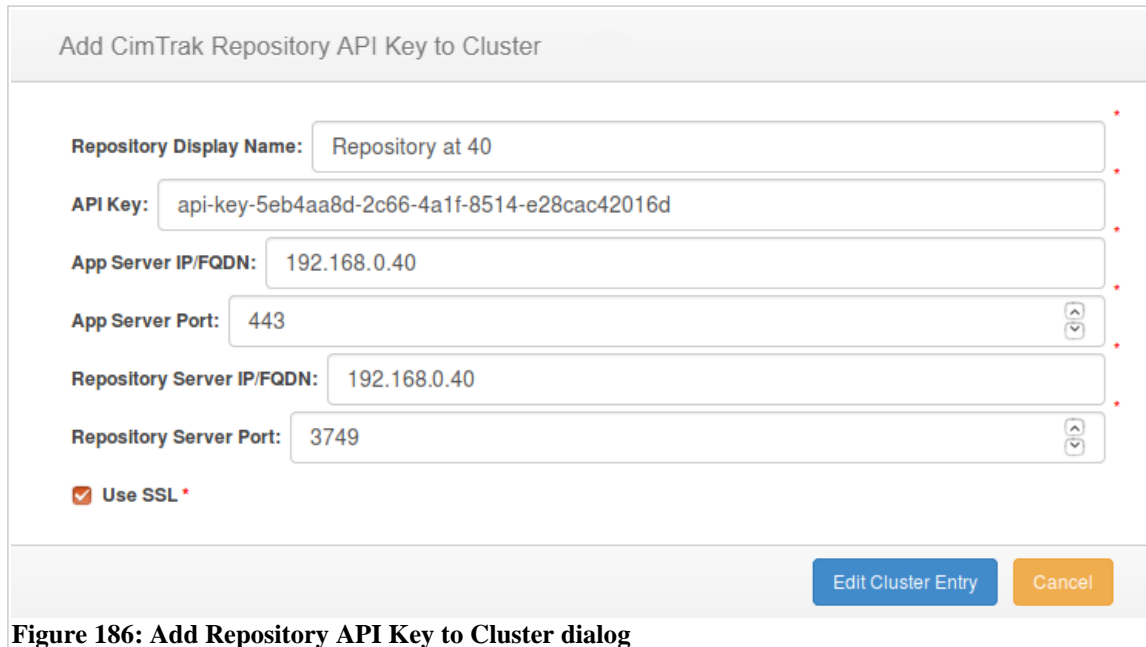


Figure 185: The generated API Key

### 10.2.2. ADD THE API KEY TO THE LOCAL REPOSITORY

Logon to the local repository as a user with object creation permissions. Open the repository properties dialog. Click the Cluster Settings tab. Click the “Add CimTrak Repository API Key” button. The dialog below will pop up.

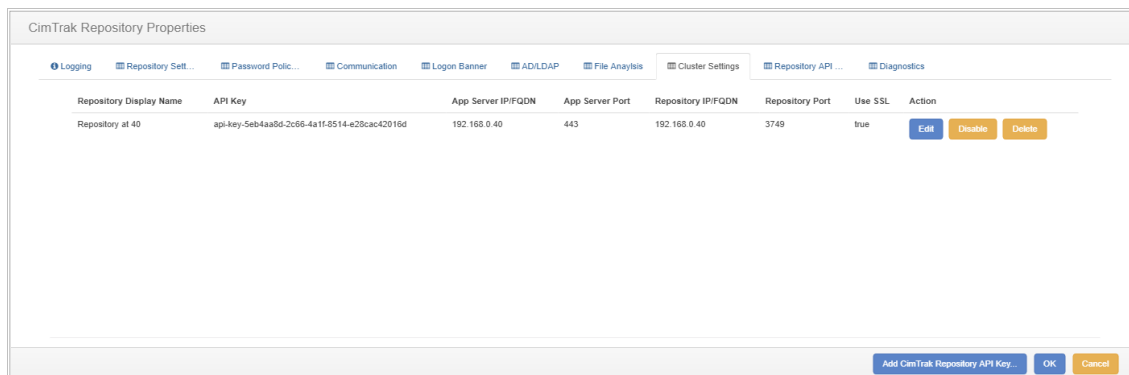


The dialog titled "Add CimTrak Repository API Key to Cluster" contains the following fields and controls:

- Repository Display Name:** Repository at 40
- API Key:** api-key-5eb4aa8d-2c66-4a1f-8514-e28cac42016d
- App Server IP/FQDN:** 192.168.0.40
- App Server Port:** 443
- Repository Server IP/FQDN:** 192.168.0.40
- Repository Server Port:** 3749
- ☒ **Use SSL**
- Buttons:** Edit Cluster Entry (blue), Cancel (orange)

Figure 186: Add Repository API Key to Cluster dialog

In the API Key text box, enter the API key generated for the remote repository. Add a description for the remote repository in the Repository Display Name box. Enter the IP address or FQDN for the App server used to access the remote repository in the App Server IP/FQDN box. Enter the App Server listening port, Repository Server IP/FQDN, and the Repository Server port in the boxes provided. If SSL (https) is used to access the App Server, check the “Use SSL” check box. Once this information is entered, click the “Add Cluster Entry” button to add the API key to the local repository's cluster. It should then show up on the Cluster Settings tab as shown below.



The "CimTrak Repository Properties" dialog shows the "Cluster Settings" tab. It contains a table with the following data:

Repository Display Name	API Key	App Server IP/FQDN	App Server Port	Repository IP/FQDN	Repository Port	Use SSL	Action
Repository at 40	api-key-5eb4aa8d-2c66-4a1f-8514-e28cac42016d	192.168.0.40	443	192.168.0.40	3749	true	<a href="#">Edit</a> <a href="#">Disable</a> <a href="#">Delete</a>

At the bottom of the dialog, there are buttons: "Add CimTrak Repository API Key" (blue), "OK" (blue), and "Cancel" (orange).

Figure 187: Cluster Settings Tab with API key added

### 10.2.3. CONFIGURING THE MULTI-REPOSITORY DISPLAY

Clicking the "OK" button on the repository properties dialog closes it. The contents of the object tree pane has changed. It now has two top level nodes in addition to the repository node. The new node at the top is "Consolidated View" and the other additional node is the added remote repository (using the display name entered in the "Add Repository API Key to Cluster" dialog). Under the added repository node are the area, agent, and object group structure from the remote repository.

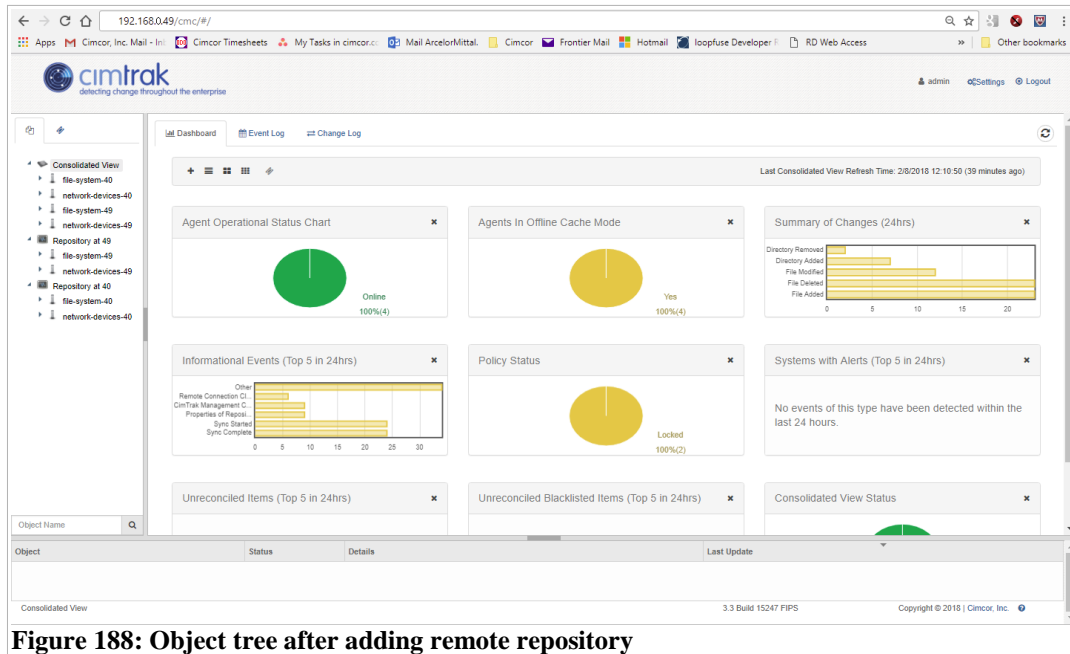


Figure 188: Object tree after adding remote repository

The Consolidated View node will contain all of the areas, agents, and object groups from both repositories. When this node is selected, the dashboard widgets will report data for all of the connected repositories. The display of the node structure can be configured. Right-clicking one of the top-level nodes presents the "Change View" option. The "Change View" sub-menu has the options, "Custom", "Operating System", "IP Range", and "Tags".

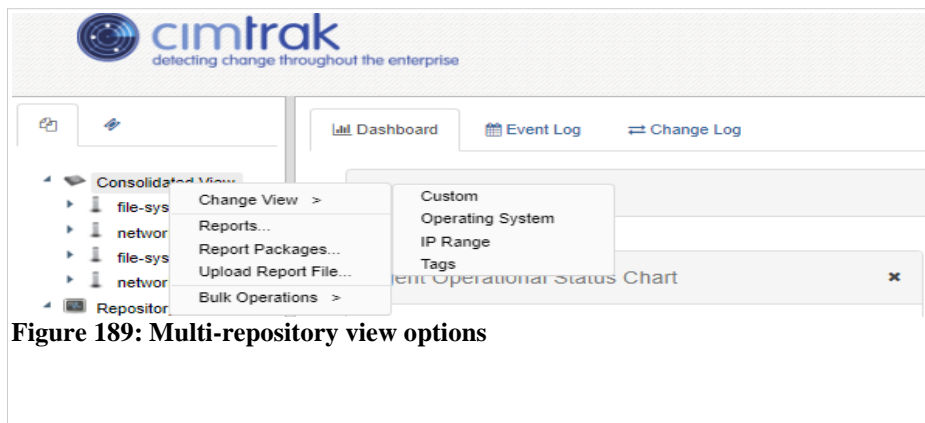
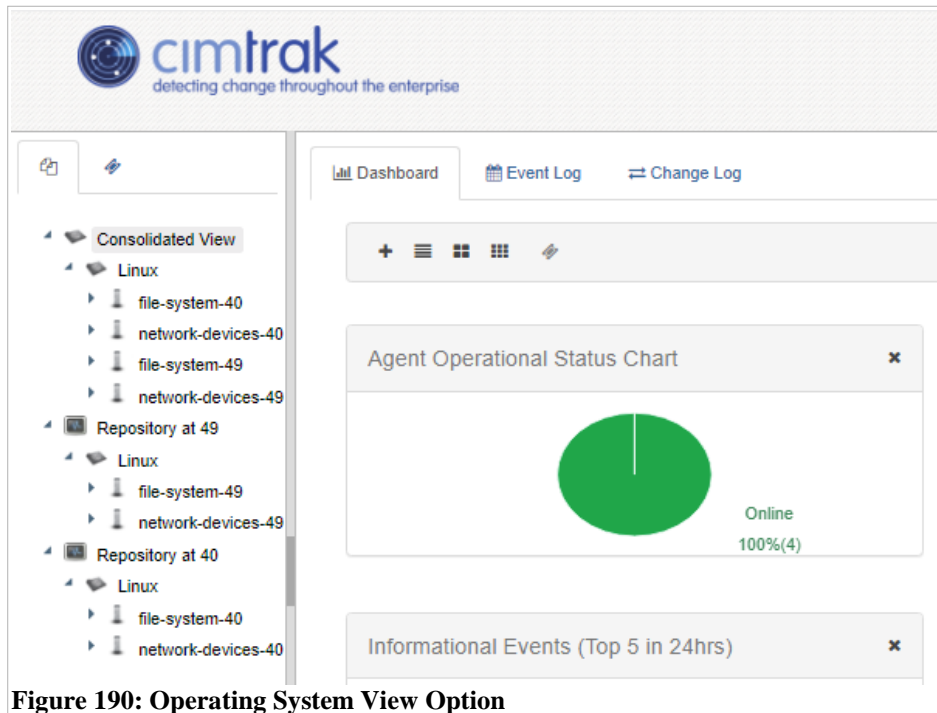


Figure 189: Multi-repository view options

The view option selected determines how the agent and area nodes are grouped under the repository nodes as well as the consolidated view node. The “Custom” view option is the display mode that shows up by default when multiple repositories get configured. The “Operating System” view option adds second level nodes for each operating system that the agents are running on, ie. “Windows”, “Linux”, etc. and the agents from each repository are grouped by the operating system that they run on.



**Figure 190: Operating System View Option**

The “IP Range” view option groups the agents by the IP address range (defined by the first 2 octets of the IP address ie 192.168.xxx.xxx) of the machines that the agents run on.

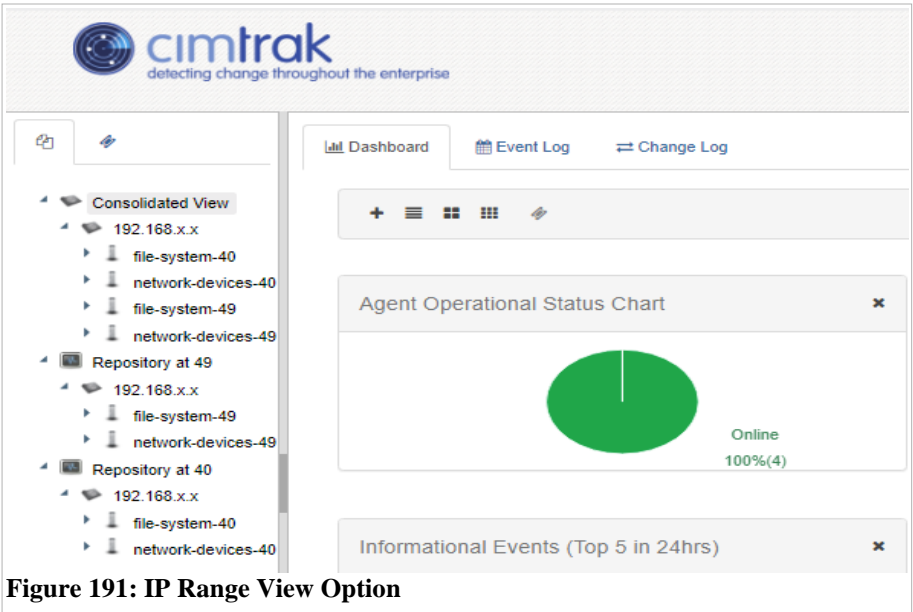


Figure 191: IP Range View Option

The “Tags” view groups the agents by the tags assigned to the agents.

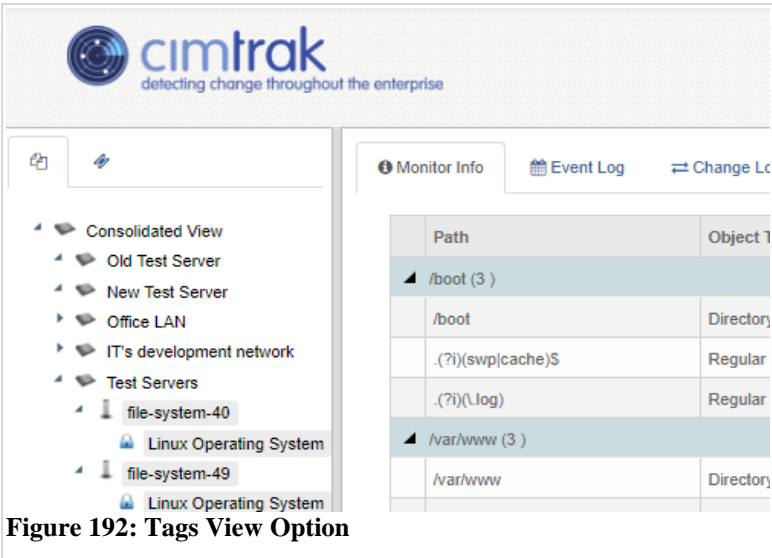


Figure 192: Tags View Option



## Appendix A: Document Versioning

### A.1 CIMTRAK™ USER GUIDANCE DOCUMENTATION HISTORY

The following table outlines the history of this documentation.

Date	Version	Editor	Modification
15 June 2011	DOC_2.0.0	David Wheeler, CIMCOR™ Technical Support	Document Creation
5 June 2011	DOC_2.0.1	Sam Conley CIMCOR™ Support Engineer	Minor editing
5 August 2014	DOC_2.1.0	Ryan Rutkin CIMCOR™ Software Engineer	Complete Document Overhaul
1 April 2013	DOC_3.0.0	Sam Conley CIMCOR™ Technical Support	Document Update
2 Feb 2017	DOC_3.0.1	Sam Conley, CIMCOR Technical Support	Document Upgrade
5 Feb 2018	DOC_3.0.2	Richard Slaughter CIMCOR™ Software Engineer	Document Update

Table 3: Document Versioning

## Appendix B: File System Agent Object Group Worksheet

### B.1 OBJECT GROUP WORKSHEET

The following worksheet can be used to keep a physical log of Object Group configurations.

**Object Group Name:** \_\_\_\_\_

**Location:** \_\_\_\_\_

**Description:** \_\_\_\_\_

**Contact:** \_\_\_\_\_

**URL:** \_\_\_\_\_

**Notes:** \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

**A zero in any of the following fields means no limit:**

- **Number of Revisions to Keep:** \_\_\_\_\_
  - Default is 250
- **Number of Changes to Keep:** \_\_\_\_\_
  - Default is 250
- **Number of Event to Keep:** \_\_\_\_\_
  - Default is 250
- **Stored Change Size (in KB):** \_\_\_\_\_
  - Default is 250

## Appendix C: Network Device Agent Object Group Worksheet

### C.1 OBJECT GROUP WORKSHEET

The following worksheet can be used to keep a physical log of Object Group configurations.

**Object Group Name:** \_\_\_\_\_

**Device Type:** \_\_\_\_\_

**IP Address of Device:** \_\_\_\_\_

**Location:** \_\_\_\_\_

**Description:** \_\_\_\_\_

**Contact:** \_\_\_\_\_

**URL:** \_\_\_\_\_

**Notes:** \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

A zero in any of the following fields means no limit:

- **Number of Revisions to Keep:** \_\_\_\_\_
  - Default is 250
- **Number of Changes to Keep:** \_\_\_\_\_
  - Default is 250
- **Number of Event to Keep:** \_\_\_\_\_
  - Default is 250
- **Stored Change Size (in KB):** \_\_\_\_\_
  - Default is 250

## Appendix D: Message Levels and Examples

### D.1 OBJECT GROUP WORKSHEET

Each Event Log message type has a corresponding icon that allows for quick visual reference to the urgency level of the event. These urgency levels are important to note when configuring E-Mail alert permissions. E-Mail alert permissions are explained in a subsequent section.

**Emergency:** *System is unusable. Highest level of event.*

**Alert:** *Take action immediately.*

**Critical:** *Critical conditions have occurred.*

**Error:** *Error conditions.*

**Warning:** *Warning conditions.*

**Notice:** *Normal condition that requires attention.*

**Information:** *Informational message.*

**Debug:** *Debug-level message. Lowest level of event.*

The following table contains examples of common log messages and their associated message levels.

Message	Message Level
CimTrak™ Repository Loading Startup Values Failed	LOG_CRITICAL
Attributes Reset	LOG_ERROR
Baseline Update	LOG_ERROR
Baseline Updated	LOG_ERROR
CimTrak™ Repository Unable to Close Sockets during shutdown	LOG_ERROR
Directory Added	LOG_ERROR
Directory Modified	LOG_ERROR
Directory Removed	LOG_ERROR
Failed To Start Deploy	LOG_ERROR
File Added	LOG_ERROR
File Deleted	LOG_ERROR
File Modified	LOG_ERROR
File Removed	LOG_ERROR
File Removed And Stored	LOG_ERROR
Lock Cancelled By User	LOG_ERROR
Lock Failed.	LOG_ERROR
Monitor Only	LOG_ERROR
Pending Repair	LOG_ERROR
Pending User Approval	LOG_ERROR
Repair Aborted	LOG_ERROR
Replaced From Repository	LOG_ERROR
Unlocked object	LOG_ERROR
Repaired by later event	LOG_WARNING
%s "%s" was %s.	LOG_NOTICE
%s "%s" was added to Object "%s".	LOG_NOTICE
%s "%s" was deleted from Object "%s".	LOG_NOTICE
Agent "%s" was %s.	LOG_NOTICE
An Object Note was added for Object "%s".	LOG_NOTICE
IP: %s, Subnet Mask: %s was added to the grant/deny access list.	LOG_NOTICE
IP: %s, Subnet Mask: %s was removed from the grant/deny access list.	LOG_NOTICE
Object "%s" was deleted.	LOG_NOTICE
Permissions for user "%s" on Object "%s" were revoked.	LOG_NOTICE
Permissions for user "%s" were modified for Object "%s".	LOG_NOTICE
Properties of %s "%s" on Object "%s" were modified.	LOG_NOTICE
Properties of %s %s were modified.	LOG_NOTICE
Properties of Master Repository were modified.	LOG_NOTICE
Properties were modified for Agent "%s".	LOG_NOTICE
Properties were modified for Object "%s".	LOG_NOTICE
User %s was granted permissions on Object "%s".	LOG_NOTICE
%s Checked In	LOG_INFO

%s Checked Out	LOG_INFO
%s was moved to %s	LOG_INFO
CimTrak™ File System Agent Connected Username %s	LOG_INFO
CimTrak™ File System Agent Failed Connecting Username %s	LOG_INFO
CimTrak™ File System Agent Logoff Requested	LOG_INFO
CimTrak™ Client Connected Username %s	LOG_INFO
CimTrak™ Client Failed Connecting Username %s	LOG_INFO
CimTrak™ Client Logoff Requested	LOG_INFO
CimTrak™ Repository Accepting A Remote Connection from %s.	LOG_INFO
CimTrak™ Repository Loading Startup Values	LOG_INFO
CimTrak™ Repository Loading Startup Values Completed	LOG_INFO
CimTrak™ Repository rejected A Remote Connection from %s.	LOG_INFO
CimTrak™ Repository Starting	LOG_INFO
CimTrak™ Repository Stopped	LOG_INFO
CimTrak™ Repository Stopping	LOG_INFO
File Added	LOG_INFO
File Deleted	LOG_INFO
File Modified	LOG_INFO
Lock Completed	LOG_INFO
Lock Started	LOG_INFO
Remote Connection Close Abnormally from %s.	LOG_INFO
Remote Connection Close Normally from %s.	LOG_INFO
Sync Complete	LOG_INFO
Sync Started	LOG_INFO
System being deployed	LOG_INFO
User %s has exceeded maximum logon attempts and the account has been locked.	LOG_INFO
User %s uploaded file "%s" to the repository.	LOG_INFO

**Table 4: Common Log Messages**

## Appendix E: Support Contact Information

### E.1 CIMTRAK™ TECHNICAL SUPPORT SERVICES

CimTrak™ Technical Support Services are here to help. Should you have any problems or questions please contact us using one of the following contact methods.

### E.2 SUPPORT VIA ELECTRONIC MAIL

CimTrak™ Technical Support electronic mail: [support@CIMCOR™.com](mailto:support@CIMCOR™.com)

Please be sure to include the following information in your message:

- Product name, version, and serial number
- Operating system, version, and service pack number
- Description of what you were doing when the error message occurred and exactly what the error message stated.
- Any other pertinent information

### E.3 SUPPORT VIA FAX

Should you choose this method, fax the same information as above to: CIMCOR™, Inc. (219) 736-4401

In addition to the above information please be sure to include the following:

- Your name and organization
- Return phone number
- Return fax number
- Your E-mail address

### E.4 SUPPORT VIA PHONE

Call CimTrak™ Technical Support at (877) 424-6267 Ext. 2

Hours: Monday thru Friday 9 AM – 5 PM Central Standard Time

Voice Mail: Leave a voice mail during off hours

Include in your voice mail:

- Your name and organization
- Your phone number
- Your question or a description of the problem
- Your E-mail address

Our technical support staff will contact you with an answer as soon as possible.