

ChangeAuditor® 5.5

What's New

**© 2011 Quest Software, Inc.
ALL RIGHTS RESERVED.**

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software, Inc.

The information in this document is provided in connection with Quest products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest products. EXCEPT AS SET FORTH IN QUEST'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software World Headquarters
LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
email: legal@quest.com

Refer to our Web site for regional and international office information.

Trademarks

Quest, Quest Software, the Quest Software logo, ActiveRoles, ChangeAuditor, Defender, GPOAdmin, InTrust, and Quest Authentication Services are trademarks and registered trademarks of Quest Software, Inc in the United States of America and other countries. For a complete list of Quest Software's trademarks, please see <http://www.quest.com/legal/trademark-information.aspx>. Other trademarks and registered trademarks are property of their respective owners.

Third Party Contributions

ChangeAuditor contains some third party components. For a complete list, see the Third Party Components page in the ChangeAuditor online help.

ChangeAuditor What's New March 2011 Version 5.5

TABLE OF CONTENTS

| | |
|---|-----------|
| About Quest Software Corporation | 5 |
| Contacting Quest Software. | 5 |
| Contacting Quest Support | 5 |
| What's New In ChangeAuditor 5.5 | 6 |
| EMC Auditing and Event Logging. | 6 |
| NetApp Auditing and Event Logging. | 6 |
| Software Development Kit (SDK) | 6 |
| Capture Originating IP/Workstation in Events | 6 |
| Exclude Accounts from Object Protection | 6 |
| Expanded Coverage of Exchange Auditing | 7 |
| Expanded Exchange 2010 Auditing | 7 |
| Entourage Support | 7 |
| New Built-in Searches | 7 |
| What's New In ChangeAuditor 5.1 | 8 |
| SQL Server Auditing and Event Logging | 8 |
| LDAP Query Auditing | 8 |
| Exchange 2010 Auditing | 8 |
| Integration with Quest Defender. | 8 |
| Ability to Construct Searches and Alerts Using Wildcard Expressions | 8 |
| SQL Reporting Services Templates | 9 |
| Enhancements to Object Protection Feature | 9 |
| Enhancements to Customize Alert Emails. | 9 |
| Ability to Search for Blank Comments | 9 |
| User Interface Enhancements. | 9 |
| What's New in ChangeAuditor 5.0 | 10 |
| What's New for ChangeAuditor Users. | 10 |
| Event Logging | 10 |
| Originating Workstation. | 10 |
| Reporting Services Integration. | 10 |
| Object Protection | 10 |
| What's New for InTrust Plug-in Users | 11 |
| In-depth Auditing for Registry, Local Users and Groups, and Services. | 11 |
| Single Download Package | 11 |
| Internal Auditing | 11 |
| Enhanced User Interface | 12 |
| Filtering and Grouping. | 12 |
| Dashboards / Executive Summary | 12 |
| Integration with Recovery Manager for AD (RMAD). | 13 |
| System Center Operations Manager (SCOM) Integration | 13 |
| What's New for both ChangeAuditor and InTrust Plug-in Users | 13 |
| Role-based Access | 13 |

| | |
|--|----|
| Auto Agent Deployment | 14 |
| Support for Windows Server 2008 R2 and Windows 7 | 14 |
| Integration with Quest Authentication Services | 14 |

About Quest Software Corporation

Quest Software simplifies and reduces the cost of managing IT for more than 100,000 customers worldwide. Our innovative solutions make solving the toughest IT management problems easier, enabling customers to save time and money across physical, virtual and cloud environments. For more information about Quest go to www.quest.com.

Contacting Quest Software

| | |
|----------|---|
| Phone | 949.754.8000 (United States and Canada) |
| Email | info@quest.com |
| Mail | Quest Software, Inc. World Headquarters 5 Polaris Way Aliso Viejo, CA 92656 USA |
| Web site | www.quest.com |

Please refer to our Web site for regional and international office information.

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a Quest product and have a valid maintenance contract. Quest Support provides unlimited 24x7 access to SupportLink, our self-service portal. Visit SupportLink at <http://support.quest.com>.

From SupportLink, you can do the following:

- Review thousands of solutions from our online Knowledgebase
- Download the latest releases and service packs
- Create, update and review Support cases

View the **Global Support Guide** for a detailed explanation of support programs, online services, contact information, and policy and procedures. The guide is available at: <http://support.quest.com>.

What's New In ChangeAuditor 5.5

EMC Auditing and Event Logging

ChangeAuditor for EMC helps ensure the security, compliance and control of files and folders by tracking, auditing, reporting and alerting on EMC Celerra changes in real time. With ChangeAuditor for EMC, administrators can report on and analyze events and changes without the complexity and time required by native auditing or concerns over system performance.

In addition to real-time auditing, you can also enable event logging to capture EMC Celerra events locally in a Windows event log. These event logs can then be collected using Quest InTrust to satisfy long-term storage requirements.

NetApp Auditing and Event Logging

ChangeAuditor for NetApp helps ensure the security, compliance and control of files and folders by tracking, auditing, reporting and alerting on NetApp filer changes in real time. With ChangeAuditor for NetApp, administrators can report on and analyze events and changes without the complexity and time required by native auditing or concerns over system performance.

In addition to real-time auditing, you can also enable event logging to capture NetApp filer events locally in a Windows event log, which can then be collected using Quest InTrust to satisfy long-term storage requirements.

Software Development Kit (SDK)

The new Software Development Kit in ChangeAuditor 5.5 provides a powerful tool that enables administrators to capture user-defined audit events generated from third-party applications. These audited events can then be displayed either in the ChangeAuditor Client or another application's console.

Capture Originating IP/Workstation in Events

Since ChangeAuditor 5.0, the event details for most audited events include the workstation name or IP address of the originating system (workstation or server). Now in ChangeAuditor 5.5, this same originating IP/workstation information is also available for Account Lockout and SQL events.

Exclude Accounts from Object Protection

ChangeAuditor now allows you to protect objects from being accessed by specified accounts. That is, using this feature you can specify to allow everyone to access the resource except those listed in the protection template.

Expanded Coverage of Exchange Auditing

Expanded Exchange 2010 Auditing

ChangeAuditor for Exchange now supports Exchange 2010 SP1. In addition, new events associated with Exchange 2010 and Exchange 2010 SP1 have been added, such as:

- User Mailbox Properties
 - Calendar settings
 - Remove meeting forward notifications to the Deleted Items Folder
 - Remove old meeting requests and responses
 - Mark new meeting requests as Tentative
 - Process meeting requests and responses originating outside the Exchange organization
- Room, Linked, Equipment Mailbox Properties
 - Resource General – Tab section
 - Resource Policy – Tab section
 - Resource Information – Tab section
 - Resource In-Policy Requests
 - Resource Out-of-Policy Requests
- Mobile Devices
 - List the mobile phones or devices for a specific user
 - Initiate remote wipes on mobile phones or devices
 - Remove old mobile phone or device partnerships
 - Create a rule for all users of a specific mobile phone or device or mobile phone type
 - Allow or block a specific mobile phone or device for the specific user

Entourage Support

ChangeAuditor for Exchange now supports Entourage for Exchange Web Services (EWS), the Microsoft email client developed for the Macintosh.

New Built-in Searches

Additional built-in searches provide more coverage of LDAP activities. For example, the new LDAP searches are designed to assist with Active Directory forest migrations and query optimizations.

What's New In ChangeAuditor 5.1

SQL Server Auditing and Event Logging

ChangeAuditor for SQL Server provides database auditing to secure SQL database assets with extensive, customizable auditing and reporting for all critical SQL Server changes including broker, database, object, performance, and transaction events, plus errors and warnings. ChangeAuditor for SQL Server helps tighten enterprise-wide change and control policies by tracking user and administrator activity such as database additions and deletions, granting and removing SQL access, etc.

LDAP Query Auditing

ChangeAuditor for LDAP monitors directory access across all domain controllers in the environment and aggregates that information in a central database identifying LDAP-enabled applications and how they use Active Directory. The LDAP access data gathered by ChangeAuditor for LDAP can then be used during Active Directory forest migration and restructuring projects.

Exchange 2010 Auditing

With the release of 5.1, the ChangeAuditor for Exchange module has been expanded to proactively audit the activities taking place in your Exchange 2010 environment.

Integration with Quest Defender

Quest Defender enhances security by enabling two-factor authentication to network, Web, and applications-based resources. Defender was designed to base all administration and identity management on an organization's existing investment in Active Directory and eliminates the costs and time involved in setting up and maintaining proprietary databases. ChangeAuditor for Defender tracks changes to user accounts enabled with Defender tokens in Active Directory.

Ability to Construct Searches and Alerts Using Wildcard Expressions

Using ChangeAuditor, you have always been able to run detailed searches and enable alerts based on user-defined criteria and customize the report templates to fit the needs of your organization. However, now in ChangeAuditor 5.1, you can use wildcard expressions to construct searches and alerts. That is, you can specify either the Like or Not Like comparison operator and a pattern (character string and * wildcard character) to be used to search for an Active Directory or Group Policy object, user or group, or an agent, domain or site.

SQL Reporting Services Templates

ChangeAuditor allows you to define SQL Reporting Services (SRS) templates that define all the necessary Report Server and ChangeAuditor data source information for publishing reports. These templates can then be made available to users to publish ChangeAuditor reports to SRS. That is, when an authorized user attempts to publish a ChangeAuditor report to SRS using the **Create Report(s) Using SQL Reporting Services** right-click command on the Searches page, they can use the **Import SRS Settings** button on the Reporting Services Setup dialog to import the settings defined in an SQL Reporting Services template to publish their reports.

Enhancements to Object Protection Feature

The Active Directory and Group Policy protection wizards now include an additional page that allow you to optionally assign template ownership to another user or group.

In addition, you can now use ChangeAuditor for Windows File Servers to protect file shares.

Enhancements to Customize Alert Emails

Using the Alert Custom Email dialog you can now send alerts to:

- the user who initiated the change that triggered the alert
- the Exchange Mailbox owner whose mailbox was accessed by another user. (This feature only applies to Exchange Mailbox Monitoring, which is available in ChangeAuditor for Exchange.)

Ability to Search for Blank Comments

In addition to searching for a string of characters in a comment, you can now search for blank comments or comments that do not contain a specific string of characters.

User Interface Enhancements

The ChangeAuditor client has undergone some enhancements, including:

- **Ability to Hide Unlicensed Components** - when on the Administration Tasks tab, you can use the **Action | Hide Unlicensed Components** menu command to hide unlicensed components from the Administration Tasks tab and unavailable events throughout the client.
- **Redesign of Navigation Pane in Administration Tasks Tab** - using the new redesigned navigation pane, you can open individual task lists. In addition, you can quickly see which templates are global and which ones need to be assigned to an agent configuration.
- **Ability to Show Count of Events of License Type** - an additional Overview pane is now available on the Overview page where you can show the number of events generated per licensed component.

What's New in ChangeAuditor 5.0

ChangeAuditor provides total auditing and security coverage for Microsoft infrastructures including Active Directory, Exchange and Windows File Servers. ChangeAuditor audits the activities taking place in your infrastructure and, with real-time alerts, delivers detailed information about vital changes and activities as they occur.

What's New for ChangeAuditor Users

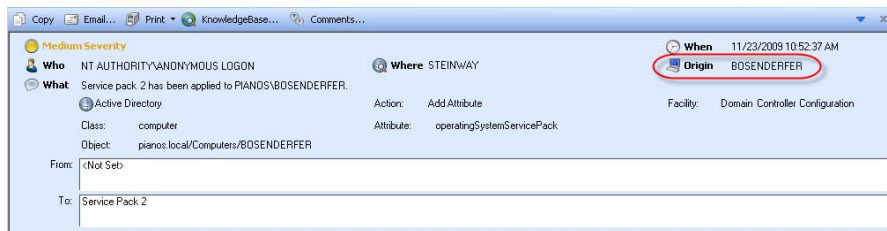
For existing ChangeAuditor customers, ChangeAuditor 5.0 includes the following new features:

Event Logging

With ChangeAuditor 5.0, in addition to real-time event auditing, you can optionally enable event logging to capture all activity locally in a Windows event log. These event logs can then be captured by Quest InTrust and stored in the InTrust Repository for efficient long term retention.

Originating Workstation

ChangeAuditor's enhanced audit data now includes the workstation name or IP address of the originating system (workstation or server).



Reporting Services Integration

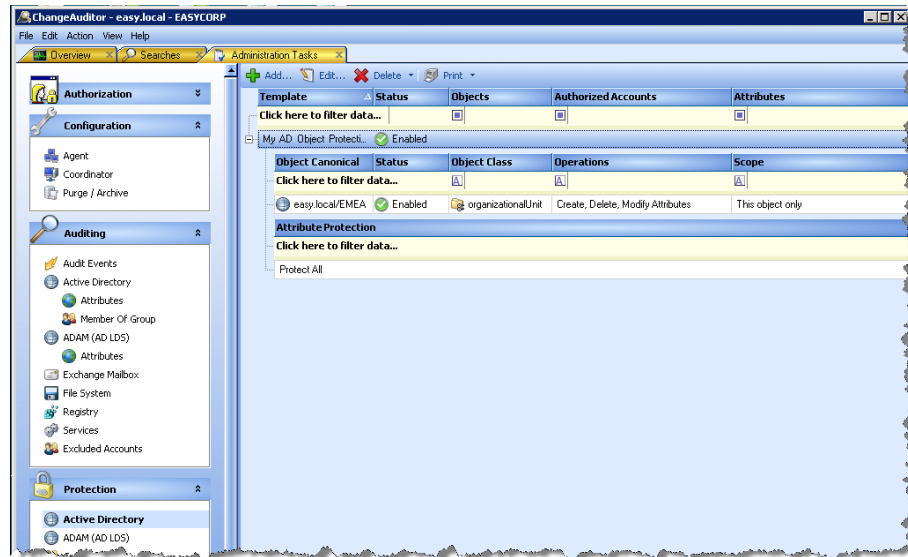
ChangeAuditor reports can now be published to Quest Knowledge Portal in addition to SQL Reporting Services for streamlined report generation and automated delivery.

To use this extended reporting capability, you must enable event logging within the ChangeAuditor Client. These event logs can then be collected using the Quest InTrust framework and imported into the InTrust database for forensic analysis from the Quest Knowledge Portal.

Object Protection

The object protection features new to ChangeAuditor 5.0 enable administrators to prevent accidental and unauthorized modifications and deletions to critical object in Active Directory by effectively securing these objects against potentially dangerous changes (add, move, modify, delete).

ChangeAuditor provides proactive protection against unwanted changes to critical Active Directory objects, Group Policy objects, ADAM (AD LDS) objects, Exchange mailboxes, and Windows files and folders.



What's New for InTrust Plug-in Users

For existing InTrust Plug-in customers, ChangeAuditor 5.0 includes the following new features:

In-depth Auditing for Registry, Local Users and Groups, and Services

ChangeAuditor provides extensive auditing coverage for registry, local users and groups, and Windows services. With these auditing features, ChangeAuditor ensures that administrators can track, alert and identify these type of changes, providing unprecedented visibility into the changes that are made and the impact those changes have on the environment.

In addition, you can optionally enable event logging for Registry, Service and/or Local Account events -- writing them to a Windows event log which can be gathered by Quest InTrust and Quest Knowledge Portal for further processing and reporting.

Single Download Package

Similar to the InTrust Plug-ins, ChangeAuditor uses a modular approach which allows for separate product deployment and management for key environments including Active Directory, Exchange and Windows File Servers. However, all ChangeAuditor modules are included in one package and it is the license keys that unlock the features specific to the different modules. Therefore, you now only need to download and install a single product instead of separate plug-in modules.

Internal Auditing

All administrative activity performed within the ChangeAuditor Client is automatically captured and can optionally be recorded to a Windows event log. This event log can then be collected using Quest InTrust to satisfy long-term storage requirements.

Enhanced User Interface

ChangeAuditor gives you the power to audit your Windows network's most visible and business-critical applications - all from a single client. The ChangeAuditor Client shows all events captured in real-time simplifying troubleshooting and analysis.

Once ChangeAuditor captures an audited event, it provides several flexible ways to generate meaningful reports. All audited event information is displayed in ChangeAuditor's Client and its 'built-in' reports provide views for the most common and complex requests. You can view configuration changes from a variety of perspectives.

- You can view all changes at a particular site.
- You can view changes made during a specific time frame.
- You can view the changes performed by a particular administrator.

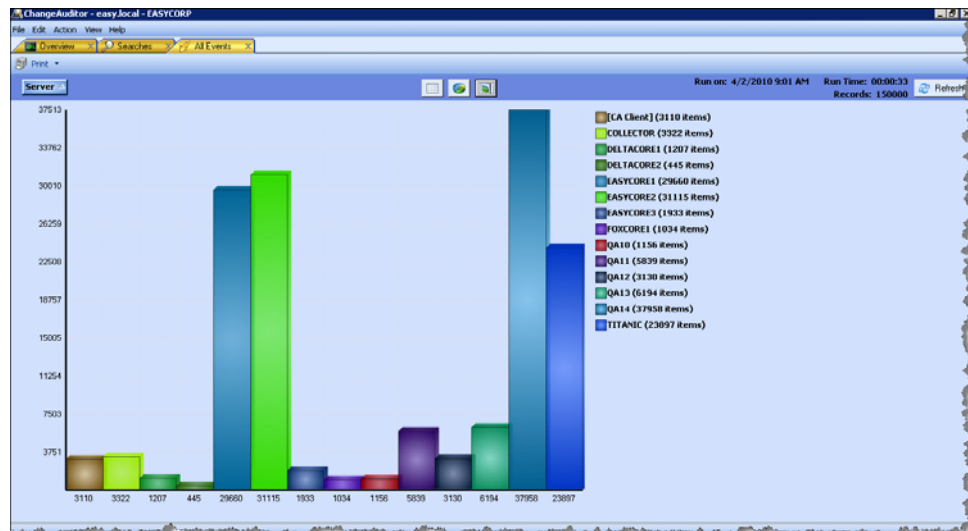
You can even run detailed searches based on user-defined criteria and customize the report templates to fit the needs of your organization.

Filtering and Grouping

The ChangeAuditor Client provides advanced filtering and grouping capabilities that allow users to modify the results of a search without changing the original search -- making it easy for users to find the events they are looking for and ultimately reducing the need to build the same search multiple times with minor customizations.

Dashboards / Executive Summary

Every search can quickly render the results into a pie chart or bar graph perfect for upper-level management to quickly see what's going on.



Integration with Recovery Manager for AD (RMAD)

By installing ChangeAuditor for Active Directory in Recovery Manager's home forest, administrators can run reports from the RMAD console to show who modified or deleted specific Active Directory objects. To be more specific, through this integration, the Recovery Manager comparison reports on Active Directory objects can include who (which user account) modified the objects being reported.

System Center Operations Manager (SCOM) Integration

ChangeAuditor includes an extremely efficient and robust SCOM Management Pack which can be configured to complement SCOM and send ChangeAuditor audited events and alert information to the SCOM console.

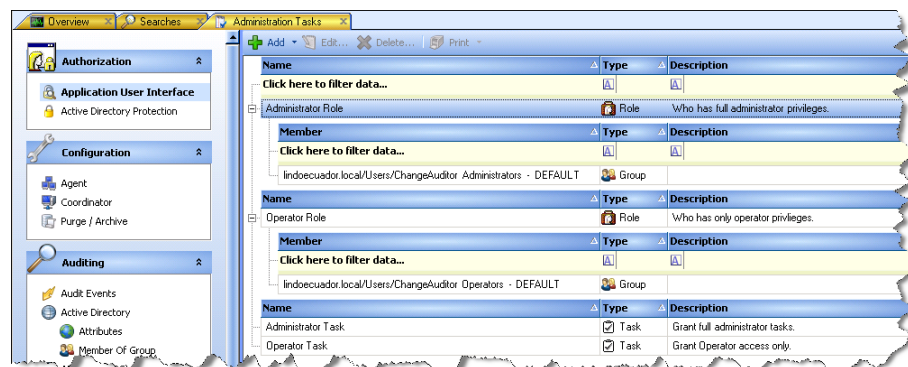
What's New for both ChangeAuditor and InTrust Plug-in Users

In addition to the features mentioned above, ChangeAuditor 5.0 provides the following new features and product enhancements to both ChangeAuditor and InTrust Plug-in customers:

Role-based Access

ChangeAuditor now allows administrators to control user access through granular, role-based permissions to ensure users are permitted to access only what they need in the ChangeAuditor Client. Using the Authorization tasks available on the Administration Tasks tab, administrators can restrict access as follows:

- Using the Application User Interface Authorization feature administrators can define who is authorized to perform the different operations available within the ChangeAuditor Client.
- Using the Active Directory Protection Authorization feature administrators can specify who is authorized to define Active Directory protection for a given domain or organizational unit.



Auto Agent Deployment

Integrated within the ChangeAuditor Client, administrators can install and upgrade agents on demand or on a schedule. The Auto Agent Deployment feature allows administrators to automatically deploy a ChangeAuditor Agent to any new servers that are added to the forest. Administrators can automatically deploy agents to all new servers or those in selected containers, based on OU membership for instance.

Support for Windows Server 2008 R2 and Windows 7

ChangeAuditor 5.0 provides support for Windows Server 2008 R2 and Windows 7, as follows:

- The ChangeAuditor Client can be installed on Windows Server 2008 R2 or Windows 7 computers.
- The ChangeAuditor Coordinator can be installed on Windows Server 2008 R2 computers.
- ChangeAuditor Agents can be deployed to Windows Server 2008 R2 computers.

Integration with Quest Authentication Services

Quest Authentication Services (formerly Vintela Authentication Services) is patented technology that enables organizations to extend the security and compliance of Active Directory to Unix, Linux and Mac platforms and enterprise applications. Leveraging ChangeAuditor for Quest Authentication Services, users of Authentication Services can now track, audit, report and alert on all critical changes to:

- Unix/Linux/Mac-related data for Active Directory users, groups, computers, NIS objects and QAS personalities
- Unix/Linux/Mac settings in Group Policy Objects