NETWRIX ACTIVE DIRECTORY CHANGE REPORTER

USER GUIDE

Product Version: 7.2

January 2013

Legal Notice

The information in this publication is furnished for information use only, and does not constitute a commitment from NetWrix Corporation of any features or functions discussed. NetWrix Corporation assumes no responsibility or liability for the accuracy of the information presented, which is subject to change without notice.

NetWrix is a registered trademark of NetWrix Corporation. The NetWrix logo and all other NetWrix product or service names and slogans are registered trademarks or trademarks of NetWrix Corporation. Active Directory is a trademark of Microsoft Corporation. All other trademarks and registered trademarks are property of their respective owners.

Disclaimers

This document may contain information regarding the use and installation of non-NetWrix products. Please note that this information is provided as a courtesy to assist you. While NetWrix tries to ensure that this information accurately reflects the information provided by the supplier, please refer to the materials provided with any non-NetWrix product and contact the supplier for confirmation. NetWrix Corporation assumes no responsibility or liability for incorrect or incomplete information provided about non-NetWrix products.

Table of Contents

1. INTRODUCTION

1.1. Overview

This guide is intended for end users of NetWrix Active Directory Change Reporter. It contains the information on the product reporting capabilities, lists all available report types and report output formats, and explains how these reports can be viewed and interpreted.

This guide can be used by auditors, company management or anyone who wants to view audit reports on the monitored environment.

1.2. How This Guide is Organized

This section explains how this guide is organized and provides a brief overview of each chapter.

- Chapter 1 Introduction: the current chapter. It explains the purpose of this document, defines its audience and outlines its structure.
- Chapter 2 Product Overview provides an overview of the NetWrix Active Directory Change Reporter functionality.
- Chapter 3 Change Summary shows a Change Summary example and explains what information a Change Summary contains.
- Chapter 4 Reports contains an overview of the Reports functionality, lists all reports available in NetWrix Active Directory Change Reporter and provides their descriptions, and explains how to view reports in a web browser or receive them by email.
- Chapter 5 Real-Time Alerts provides an example and description of a Real-Time Alert.
- Appendix: Related Documentation contains a list of all documentation published to support NetWrix Active Directory Change Reporter.

2. PRODUCT OVERVIEW

Microsoft Active Directory change auditing has become a mission-critical activity in business networks. Unauthorized changes and errors in Active Directory configuration can put your organization at risk introducing security breaches and compliance issues. Native Active Directory auditing is often inadequate when it comes to supporting such business needs as troubleshooting, security auditing, change monitoring, and reporting, many of which are driven by the necessity for organizations to comply with external industry and legislative requirements.

NetWrix Active Directory Change Reporter fills this functional gap by tracking all additions, deletions, and modifications made to Active Directory users, groups, computers, OUs, group memberships, permissions, domain trusts, AD sites, FSMO roles, AD schema, Group Policy and Exchange objects, settings and permissions.

The product collects data on changes made to the monitored Active Directory domain and generates audit reports showing the before and after values for WHO changed WHAT, WHEN and WHERE in a human-readable format without the overhead of resolving complicated native identifiers.

2.1. Key Benefits

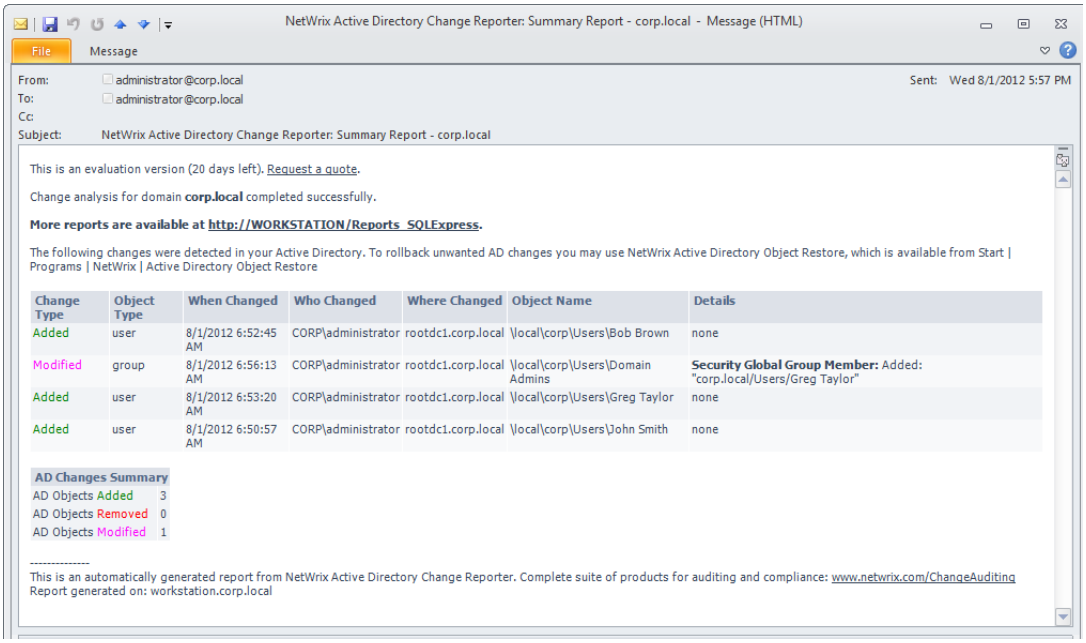
NetWrix Active Directory Change Reporter is a tool for automated auditing and reporting on changes to the monitored Active Directory environment. It allows you to do the following:

- **Monitor day-to-day administrative activities**: the product captures detailed information on all changes made to the monitored Active Directory environment, including the information on WHO changed WHAT, WHEN and WHERE. Audit reports and real-time email notifications facilitate review of daily activities.
- **Sustain compliance** by using in-depth change information. Audit data can be archived and stored for more than 7 years to be used for reports generation.
- **Streamline change control**: the integrated Active Directory Object Restore tool streamlines the restore of any undesired or potentially harmful changes to your Active Directory environment.
- **Integrate with SIEM systems**: the product can be integrated with multiple SIEM systems, including RSA enVision®, ArcSight® Logger™, Novell® Sentinel™, NetIQ® Security Manager™, IBM Tivoli® Security Information and Event Manager™ and more. The product can also be configured to feed data to Microsoft System Center Operations Manager, thus providing organizations that use SCOM with fully automated Active Directory auditing and helping protect these investments.

3. CHANGE SUMMARY

Each day (at 3:00 AM by default), NetWrix Active Directory Change Reporter generates a Change Summary that contains the information on changes that occurred in the last 24 hours and emails it to the specified recipients:

Figure 1: Change Summary Example



The example Change Summary reflects the following changes to the monitored AD domain:

- User Bob Brown has been added
- User Greg Taylor has been added
- User Greg Taylor has been added to the Domain Admins group
- User John Smith has been added

The Change Summary provides the following information for each change:

Table 1: Change Summary Fields

Parameter	Description
Change Type	Shows the type of action that was performed on the AD object. The possible values are Added/Removed/Modified.
Object Type	Shows the type of the AD object that was changed, e.g. “user”.
When Changed	Shows the exact time when the change occurred.
Who Changed	Shows the name of the account under which the change was made.
Where Changed	Shows the name of the domain controller where the change was made.
Object Name	Shows the path to the AD object that was changed.
Details	Shows the before and after values for the modified object.

To receive daily Change Summary emails, ask your system administrator to add your email address to the Change Summary Recipients list.

4. REPORTS

NetWrix Active Directory Change Reporter allows generating reports based on Microsoft SQL Server Reporting Services (SSRS). The product provides a wide variety of predefined report templates that will help you stay compliant with various standards and regulations (GLBA, HIPAA, PCI, SOX, and many others). You can use different output formats for your reports, such as PDF, XLS, and so on.

In NetWrix Active Directory Change Reporter, two types of reports are available:

- **Snapshot Reports**: allow generating reports on your AD domain configuration state at a specific moment of time.
- **Change Reports**: show changes to the monitored Active Directory domain filtered by different parameters (date, user and so on) and in different formats (table or chart):

You can view audit reports through a web browser, or you can ask your system administrator to configure a subscription to the selected reports to receive them by email. For details on these options, refer to the following sections:

- 4.2 Viewing Reports in a Web Browser
- 4.3 Receiving Reports by Email

4.1. Reports List

NetWrix Active Directory Change Reporter provides over 70 predefined report templates. If none of these reports suits your needs, ask your system administrator to create custom report templates, or order them from NetWrix.

The table below lists all available reports and provides their descriptions:

Table 2: Reports List

Report Name	Description
AD Snapshot Reports	
Computer Account Reports	
All Computer Accounts Enabled and Disabled	Shows all computers (including their path, name and status). Data can be filtered by the domain name, status and computer name.
Service Principal Names	Shows all computers (including their path, service principal name and operating system). Data can be filtered by the domain name, path and property name.
Domain Controller Reports	
All Domain Controllers	Shows all domain controllers (including their path, service principal name and operating system). Data can be filtered by the domain name, path and property name.
Group Reports	
All Active Directory Groups	Shows all groups (such as domain local groups, global groups, universal groups, etc.). Data can be filtered by the domain name, group type and group name.
All Groups without Members	Shows all groups without members. Data can be filtered by the domain name and group name.
Group Members	Shows all members (users, groups, etc.) of the selected groups.
Sensitive Group Members	Shows all members (users, groups, etc.) of the Domain Admins and Enterprise Admins groups.

Users without Distribution Group Membership	Shows all accounts that do not belong to any distribution group.
Organizational Unit Reports	
Organizational Unit Accounts	Shows users, computers and inetOrgPersons from the selected organizational units and the “Users” and “Built-in” containers, including their usernames and account statuses (enabled/disabled).
User Account Reports	
All User Accounts Enabled and Disabled	Shows all users (including their path, name, logon name and status) filtered by the domain name, status and logon name.
All User Accounts Last Logons	Shows all users (including their paths, status and last logon time) filtered by path, status and last logon time.
All User Accounts whose Password Never Expired	Shows all users (including their path and status) whose password policy is set to “Password Never Expires”. Data can be filtered by path and status.
All User Accounts with Group Membership	Shows all users and their group membership. Data can be filtered by the user path, group path and group type.
Expired User Accounts	Shows all user accounts that have expired. Data can be filtered by user name, logon name and expiration date.
Locked User Accounts	Shows all user accounts in the lock-out state. Data can be filtered by user name and logon name.
All Changes Reports	
All Active Directory Changes (Chart)	A chart report showing all changes to AD objects, permissions and configuration grouped by change type. Data can be filtered by date range and domain name.
All Active Directory Changes by Date (Chart)	A chart report showing all changes to AD objects, permissions and configuration grouped by date. Data can be filtered by date range and domain name.
All Active Directory Changes by Date	Shows all changes to AD objects, permissions and configuration grouped by date. Data can be filtered by date range and the name of the user who made the changes.
All Active Directory Changes by Object Type	Shows all changes to AD objects, permissions and configuration grouped by object type (e.g. User or Group). Data can be filtered by date range and the name of the user who made the changes.
All Active Directory Changes by User (Chart)	A chart report showing all changes to AD objects, permissions and configuration grouped by the users who made the changes. Data can be filtered by date range.
All Active Directory Changes by User	Shows all changes to AD objects, permissions and configuration grouped by the users who made the changes. Data can be filtered by date range and the name of the user who made the changes.
All Active Directory Changes	Shows all changes made to AD objects, permissions and configuration. Data can be filtered by date range and the name of the user who made the changes.
All Active Directory Configuration Changes	Shows all changes made to objects inside the AD Configuration container, such as domains, domain controllers, sites, etc.
All Active Directory Schema Changes	Shows all changes made to the AD Schema container (classes and attributes).
All Active Directory Site Changes	Shows all changes made to AD sites.
Best Practice Reports	
AD Structure	
Organizational Unit Setting	Shows changes to organizational units (name, description,

Modifications	delegation, etc.), except for changes made to child objects.
Organizational Units Created	Shows newly created organizational units.
Organizational Units Removed	Shows deleted organizational units. Shows deleted organizational units.
Computer Account	
Computer Account Modifications	Shows all changes to computer accounts (e.g. renames, delegation settings, etc.)
Computer Accounts Created	Shows all computer accounts created automatically when they join the domain.
Computer Accounts Removed with Details	Shows removed computer accounts with detailed information.
Computer Accounts Removed	Shows removed computer accounts.
Service Packs Applied to Computers	Shows OS service packs installations on DCs, member servers and workstations.
Contact Account	
All Contact Changes	Shows all changes to Contact objects, their permissions and configuration. Data can be filtered by date range and the name of the user who made the changes.
Domain	
Changes in Domain Trust Relationships	Shows all changes to the domain trusts. Data can be filtered by date range and the name of the user who made the changes.
Changes in Domain-Wide Operations Master Roles	Shows FSMO role transfers inside the domain (e.g. PDC and RID Master).
Changes in Forest-Wide Operations Master Roles	Shows forest-wide FSMO role transfers (e.g. Schema Master).
New Servers Added with Details	Shows computer accounts created automatically when servers join the domain.
Domain Controller	
Domain Controller Modifications	Shows changes do domain controllers configuration.
Doman Controllers Demoted	Shows all removed domain controllers.
Domain Controllers Promoted	Shows additions of new domain controllers to the domain.
Group Membership	
Administrative Group Membership Changes	Shows changes to membership in the following administrative groups: Domain Admins, Enterprise Admins, Schema Admins, Account Operators, Administrators, Backup Operators, Incoming Forest Trust Builders, Server Operators.
All Changes by Group Members	Shows all changes made by members of a selected group.
Distribution Group Modifications	Shows changes to distribution groups properties, including group membership.
Distribution Groups Created	Shows newly created distribution groups.
Distribution Groups Removed	Shows all deleted distribution groups.
Security Group Membership Changes	Shows changes to security groups membership.
Security Group Modifications	Shows all types of changes to security groups, including changes to their name, description, membership and permissions.
Security Groups Created	Shows newly created security groups, including local, global and universal groups.
Security Groups Removed	Shows deleted security groups, including local, global and universal groups.

Object Security	
Administrative Group Membership Changes	Shows changes to membership in the following administrative groups: Domain Admins, Enterprise Admins, Schema Admins, Account Operators, Administrators, Backup Operators, Incoming Forest Trust Builders, Server Operators.
All Changes by Group Members	Shows all changes made by members of a selected group.
Object Security Changes	Shows changes to object permissions and audit settings.
User Account	
Account Expiration Modifications	Shows changes to account expiration settings. Data can be filtered by date range.
Accounts Enabled or Disabled	Shows accounts that have been enabled or disabled.
Administrative Password Resets by User	Shows all password resets performed by IT personnel filtered by user.
All User Changes with Advanced Attributes	Shows all changes to AD user objects, their permissions and configuration. Data can be filtered by date range and the name of the user who made the changes.
Dial-in Access Modifications	Shows changes to dial-in and VPB access rights.
Logon Hours Modifications	Shows changes to the Logon Hours settings that controls the allowed logon time range.
Logon Workstations Modifications	Shows changes to the Allowed Logon workstations on the user account level.
Password Changes by User	Shows all successful password resets performed by users.
User Account Modifications	Shows changes made to user account attributes (e.g. name, contact info, dial-in permissions, manager, etc.).
User Accounts Created with Details	Shows all newly created user accounts with detailed information.
User Accounts Created	Shows all newly created user accounts.
User Accounts Deleted with Details	Shows all deleted user accounts with detailed information.
User Accounts Deleted	Shows all deleted user accounts.
User Accounts Lockouts	Shows all account lockout events.
User Accounts Renamed	Shows all renamed user accounts.
User Accounts Unlocked	Shows all user accounts unlocked manually.
Users Disabled	Shows all disabled user accounts.
Users Enabled	Shows all enabled user accounts.

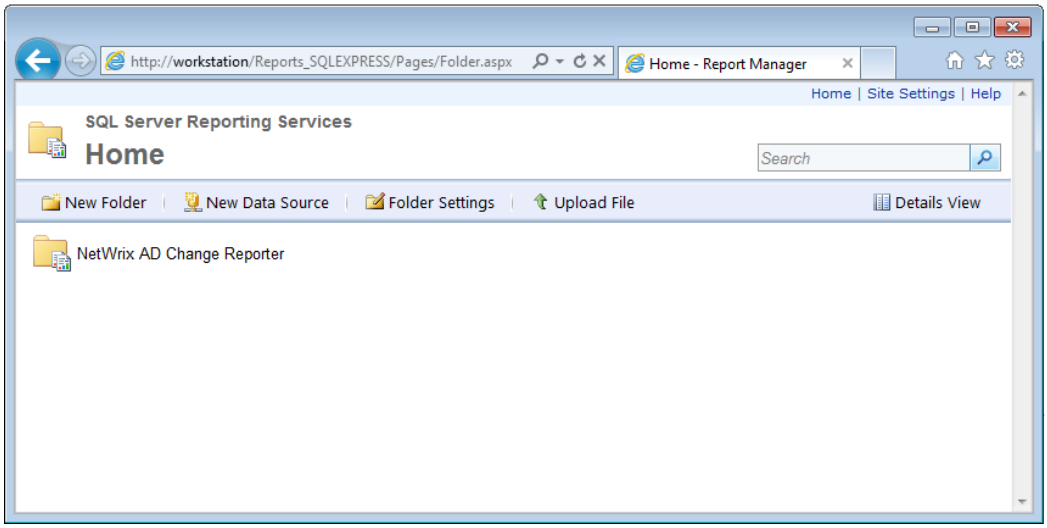
4.2. Viewing Reports in a Web Browser

To be able to view reports in your web browser, ask your system administrator to provide you with the Report Manager URL.

Procedure 1. To view reports in a web browser

1. In your web browser, type the Report Manager URL in the address line and press **Enter**. The SQL Server Reporting Services Home page will open:

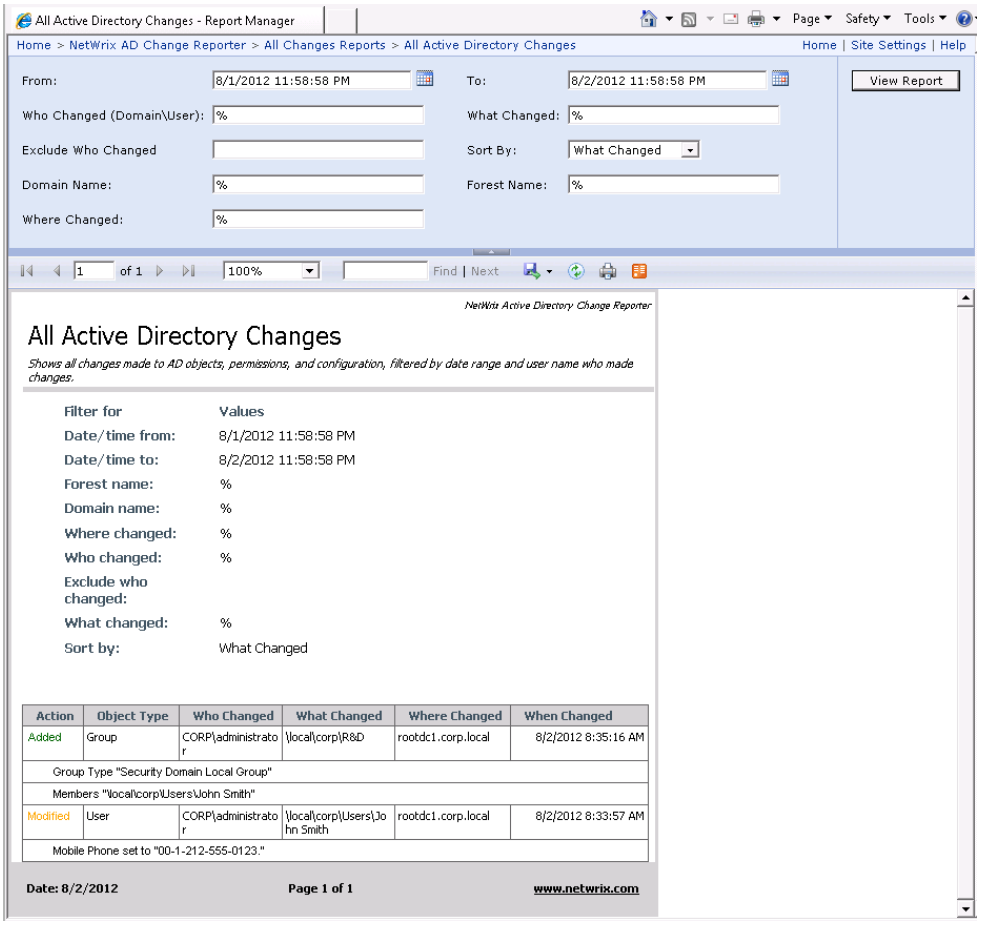
Figure 2: Report Manager Home Page



2. Click the **NetWrix AD Change Reporter** folder and navigate to the report you want to generate.

3. Click the report name. The report will be displayed showing the changes that occurred in the last 24 hours. On the report page, you can specify filters to the selected report and click the **View Report** button (**View Chart** for chart reports) to apply them:

Figure 3: All Active Directory Changes Report (Web Browser)



Note: Report filters may vary depending on the selected report.

4.3. Receiving Reports by Email

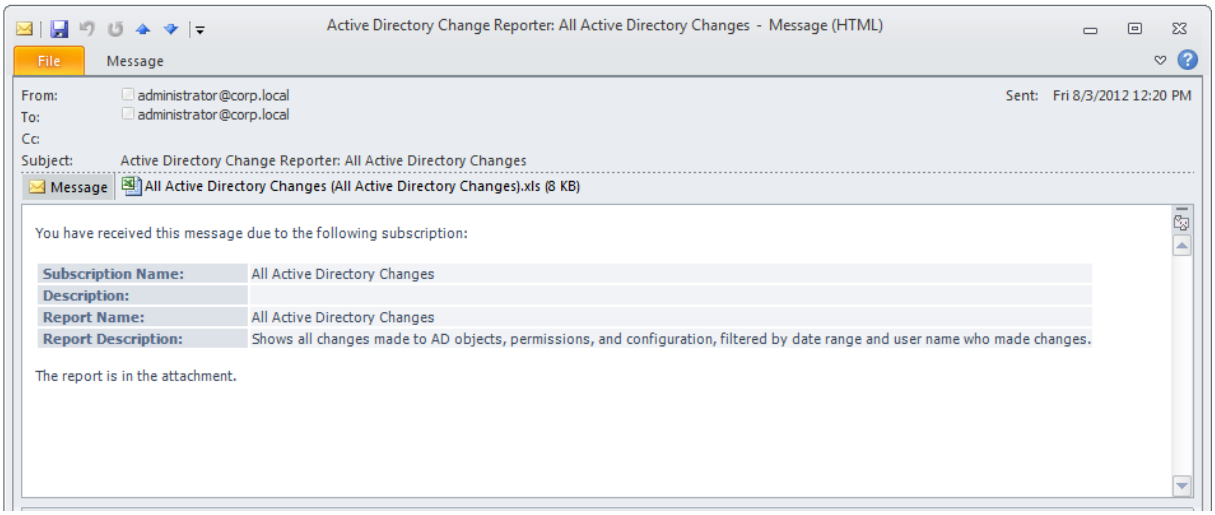
If you want to receive reports by email, ask your system administrator to configure a subscription to the selected reports. The administrator can configure report filters, so that you only receive the information you need, and select report output format: Excel, Word or PDF.

Reports can be delivered on one of the following schedules:

- On a daily basis (reports will be delivered at the specified interval of days at 3:00 AM);
- On a weekly basis (reports will be delivered on the specified days of the week at 3:00 AM);
- On a monthly basis (reports will be delivered in the specified months on a selected date at 3:00 AM).

Reports will be delivered as email attachments in the selected format:

Figure 4: Report Delivered by Subscription

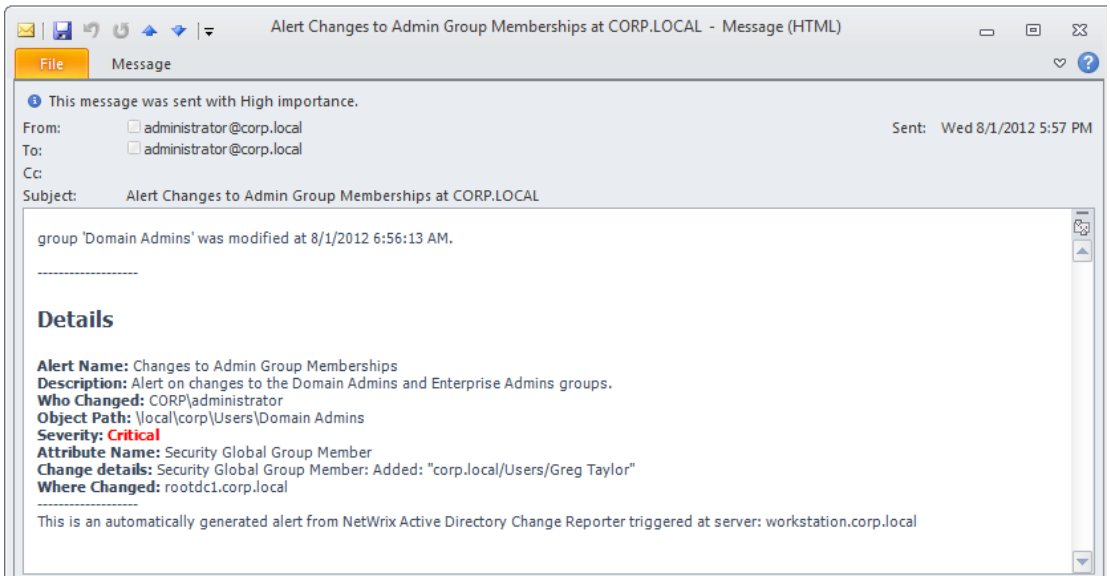


5. Real-Time Alerts

If you want to be notified immediately about changes to certain objects, you can ask your system administrator to configure Real-Time Alerts that will be triggered by specific events. Alerts are emailed immediately after the specified event has been detected.

The example below shows an alert triggered by additions to the Domain Admins and Enterprise Admins groups. This alert notifies you that user Greg Taylor has been added to the Domain Admins group:

Figure 5: Real-Time Alert Example



A APPENDIX: RELATED DOCUMENTATION

The table below lists all documents available to support NetWrix Active Directory Change Reporter:

Table 3: Product Documentation

Document Name	Overview
NetWrix Active Directory Change Reporter User Guide	The current document
NetWrix Active Directory Change Reporter Installation and Configuration Guide	Provides detailed instructions on how to install NetWrix Active Directory Change Reporter, NetWrix Group Policy Change Reporter and NetWrix Exchange Change Reporter, and explains how to configure the target AD domain for auditing.
NetWrix Active Directory Change Reporter Quick-Start Guide	Provides an overview of the product functionality and instructions on how to install, configure and start using the product. This guide can be used for evaluation purposes.
NetWrix Active Directory Change Reporter Administrator's Guide	Provides a detailed explanation of the NetWrix Active Directory Change Reporter features and step-by-step instructions on how to configure and use the product.
NetWrix Active Directory Change Reporter Freeware Edition Quick-Start Guide	Provides instructions on how to install, configure and use NetWrix Active Directory Change Reporter, NetWrix Group Policy Change Reporter and NetWrix Exchange Change Reporter Freeware Edition.
NetWrix Active Directory Change Reporter Release Notes	Contains a list of the known issues that customers may experience with NetWrix Active Directory Change Reporter 7.2, and suggests workarounds for these issues.
Troubleshooting Incorrect Reporting of the "Who Changed" Parameter	Step-by-step instructions on how to troubleshoot incorrect reporting of the 'who changed' parameter.
Configuring Real-Time Alerts in NetWrix Active Directory Change Reporter	This technical article provides detailed instructions on how to configure real-time alerts, as well as an algorithm for selecting the correct attribute for the type of change you want to track. It also contains step-by-step procedures that will guide you through configuration of some most commonly used alerts.
Installing Microsoft SQL Server and Configuring the Reporting Services	This technical article provides instructions on how to install Microsoft SQL Server 2005/2008 R2/2012 Express and configure the Reporting Services.
How to Subscribe to SSRS Reports	This technical article explains how to configure a subscription to SSRS reports using the Report Manager.
Integration with Third Party SIEM Systems	This article explains how to enable integration with third-party Security Information and Event Management (SIEM) systems.
Native AD Auditing Cheat Sheet	Provides an Active Directory auditing configuration checklist.