netwrix

Keeping Tabs on the Top 5 Critical Changes in Active Directory with Netwrix Auditor

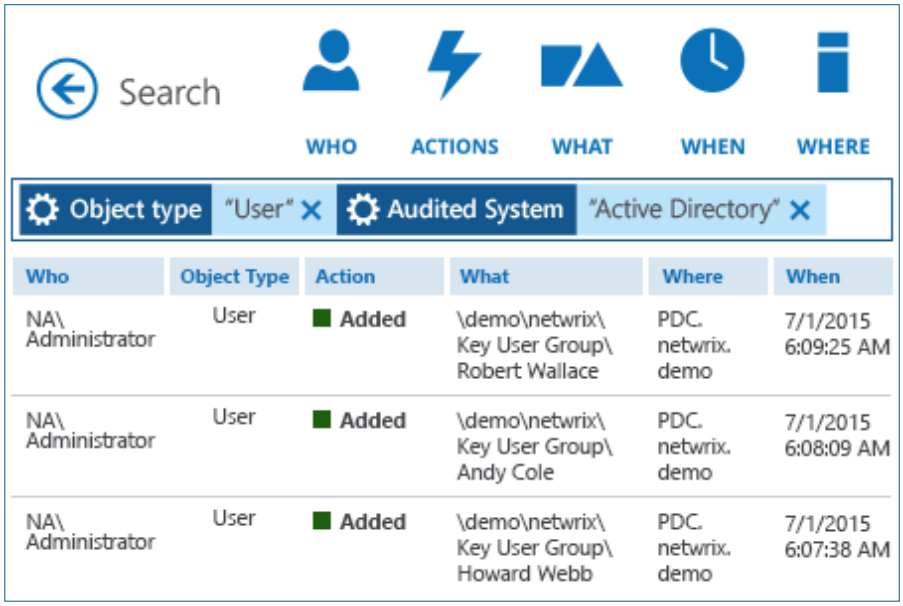
www.netwrix.com | **Toll-free**: 888.638.9749

Table of Contents

#1: Creation of User Accounts

Accounts created outside normal controls may enable unauthorized users to access the system. Netwrix Auditor tracks all newly created accounts and helps answer the following questions:

- What user accounts were created?
- Who created each new user account?
- When was each account created?
- Which domain does each new account belong to?

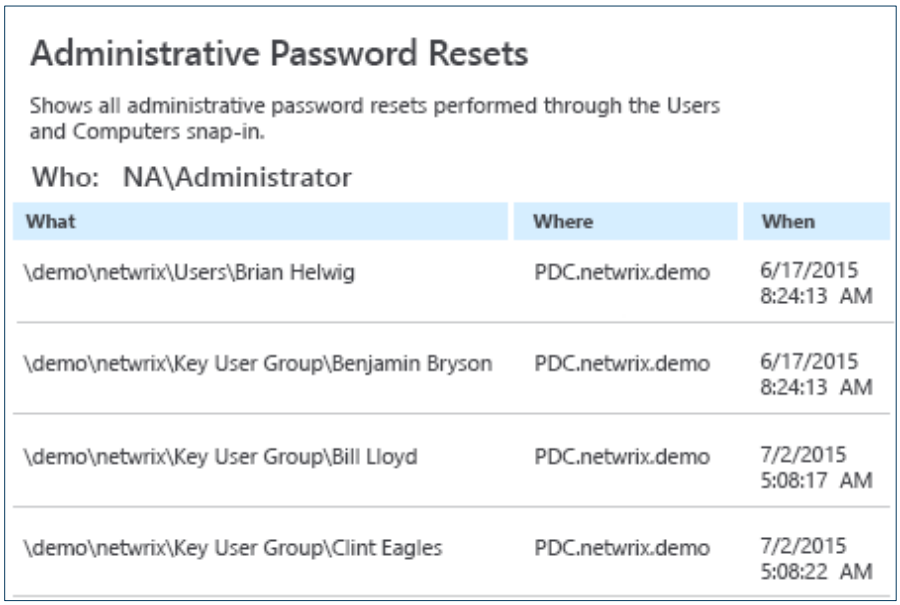


Who	Object Type	Action	What	Where	When
NA\ Administrator	User	Added	\demo\netwrix\ Key User Group\ Robert Wallace	PDC. netwrix. demo	7/1/2015 6:09:25 AM
NA\ Administrator	User	Added	\demo\netwrix\ Key User Group\ Andy Cole	PDC. netwrix. demo	7/1/2015 6:08:09 AM
NA\ Administrator	User	Added	\demo\netwrix\ Key User Group\ Howard Webb	PDC. netwrix. demo	7/1/2015 6:07:38 AM

#2: Administrative Password Resets

A user account password reset made behind the back of an IT administrator may be a sign that an unauthorized user has received access to an administrator's account.
Netwrix Auditor tracks all administrative password resets and helps answer the following questions:

- Which user account passwords were reset?
- Which IT administrator reset each user account password?
- In which domain was each password reset?
- When was each password reset?



Administrative Password Resets

Shows all administrative password resets performed through the Users and Computers snap-in.

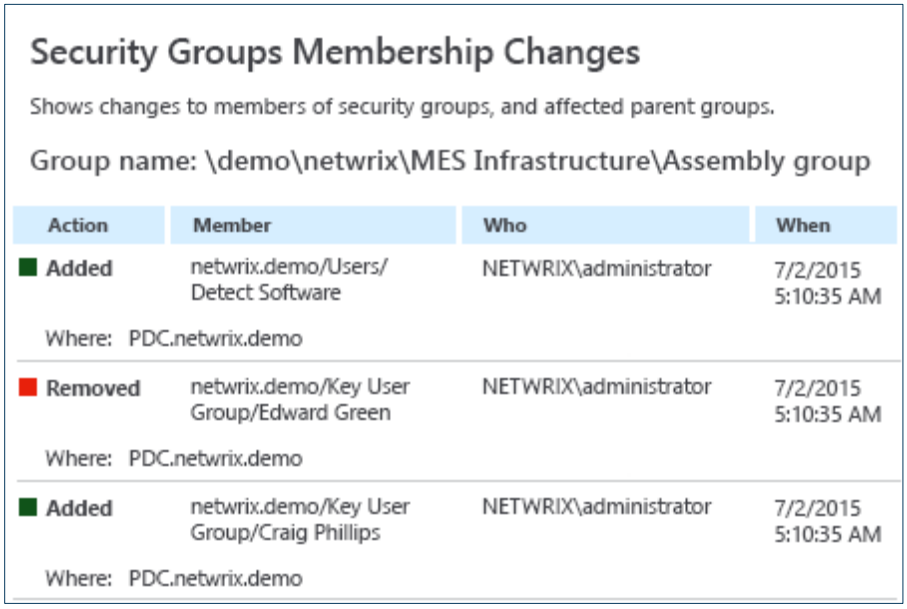
Who: NA\Administrator

What	Where	When
\demo\netwrix\Users\Brian Helwig	PDC.netwrix.demo	6/17/2015 8:24:13 AM
\demo\netwrix\Key User Group\Benjamin Bryson	PDC.netwrix.demo	6/17/2015 8:24:13 AM
\demo\netwrix\Key User Group\Bill Lloyd	PDC.netwrix.demo	7/2/2015 5:08:17 AM
\demo\netwrix\Key User Group\Clint Eagles	PDC.netwrix.demo	7/2/2015 5:08:22 AM

#3: Changes to Security Group Membership

Any unauthorized user added, for example, to the Domain Admins Group receives full control over the Active Directory and gets access to all IT systems that use Windows authentication.
Netwrix Auditor tracks all security group membership changes and helps answer the following questions:

- Who was added to or removed from a security group?
- Who made each change to a security group?
- Which domain was the changed security group in?
- When was each change to a security group made?



Security Groups Membership Changes

Shows changes to members of security groups, and affected parent groups.

Group name: \demo\netwrix\MES Infrastructure\Assembly group

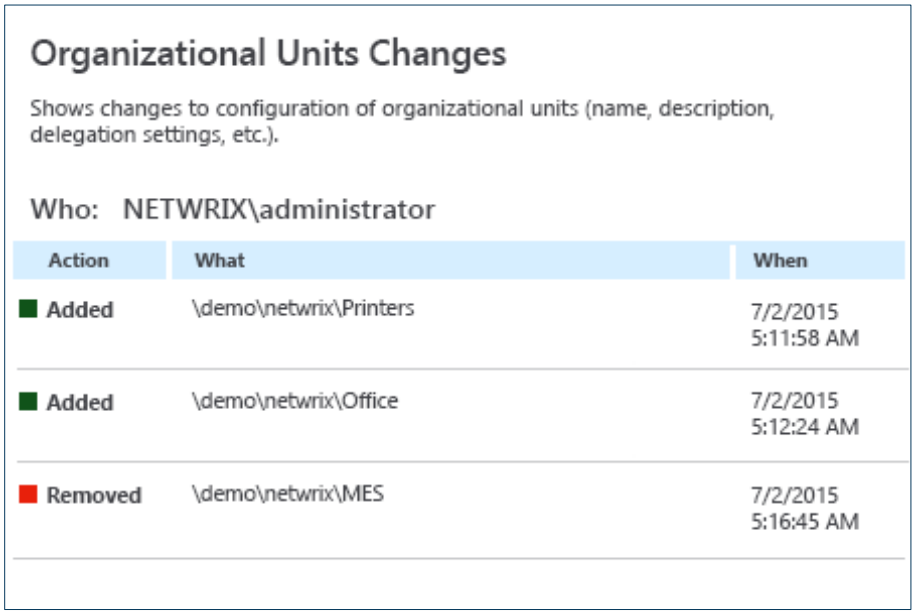
Action	Member	Who	When
Added	netwrix.demo/Users/ Detect Software	NETWRIX\administrator	7/2/2015 5:10:35 AM
Where: PDC.netwrix.demo			
Removed	netwrix.demo/Key User Group/Edward Green	NETWRIX\administrator	7/2/2015 5:10:35 AM
Where: PDC.netwrix.demo			
Added	netwrix.demo/Key User Group/Craig Phillips	NETWRIX\administrator	7/2/2015 5:10:35 AM
Where: PDC.netwrix.demo			

#4: Deleted Organizational Units

Improper deletions of organizational units (OUs) will increase the pressure on the IT department. Some users will not be able to log in, while others will have a hard time accessing email, Messenger, SharePoint, etc.

Netwrix Auditor tracks all deleted organizational units and helps answer the following questions:

- Which OUs were deleted?
- Who deleted each OU?
- Which domain was the OU deleted from?
- When was each OU deleted?



Organizational Units Changes

Shows changes to configuration of organizational units (name, description, delegation settings, etc.).

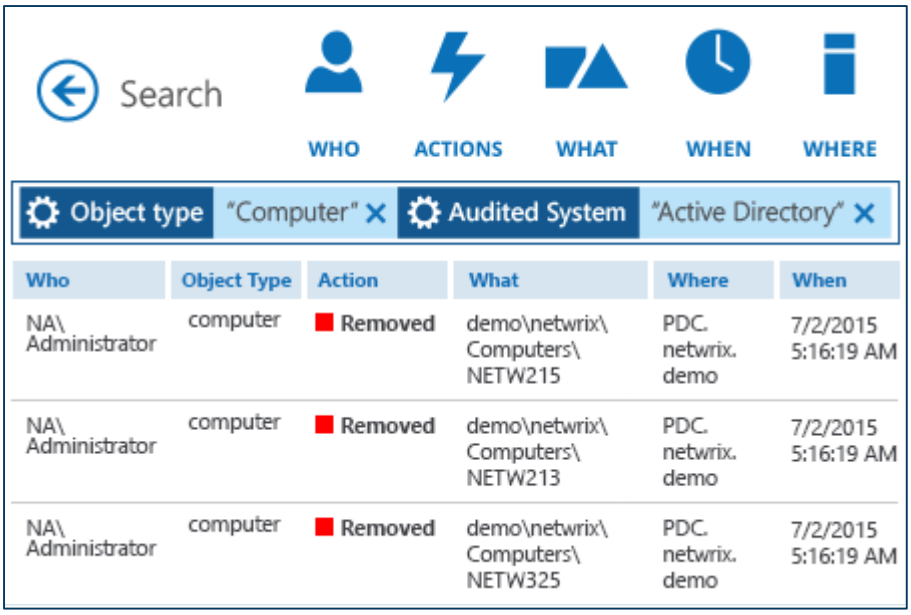
Who: NETWRIX\administrator

Action	What	When
Added	\demo\netwrix\Printers	7/2/2015 5:11:58 AM
Added	\demo\netwrix\Office	7/2/2015 5:12:24 AM
Removed	\demo\netwrix\MES	7/2/2015 5:16:45 AM

#5: Deleted Computer Accounts

Users whose computer accounts have been deleted cannot log into IT systems using domain authentication or access e-mail, SharePoint, SQL Server, shared folders, etc.
Netwrix Auditor tracks all recently deleted computer accounts and helps answer the following questions:

- Which computer accounts were deleted?
- Who deleted each computer account?
- Which domain was the computer account deleted from?
- When was each computer account deleted?



Who	Object Type	Action	What	Where	When
NA\ Administrator	computer	Removed	demo\netwrix\ Computers\ NETW215	PDC. netwrix. demo	7/2/2015 5:16:19 AM
NA\ Administrator	computer	Removed	demo\netwrix\ Computers\ NETW213	PDC. netwrix. demo	7/2/2015 5:16:19 AM
NA\ Administrator	computer	Removed	demo\netwrix\ Computers\ NETW325	PDC. netwrix. demo	7/2/2015 5:16:19 AM

About Netwrix Auditor

Netwrix Auditor delivers **complete visibility** into IT infrastructure changes and data access by providing actionable audit data about **who changed what**, **when and where each change was made**, and **who has access to what**. Netwrix Auditor helps organizations prevent security breaches caused by insider attacks, pass compliance audits with far less effort and expense, and keep tabs on what privileged users are doing in the environment.

Netwrix Auditor enables auditing of the broadest variety of IT systems, including Active Directory, Exchange, file servers, SharePoint, SQL Server, VMware and Windows Server. It also supports monitoring of privileged user activity in all other systems, even if they do not produce any logs, by enabling video recording of user screen activity and later search and replay.

More than 160,000 IT departments worldwide rely on Netwrix Auditor to secure IT infrastructure, prove compliance and increase operational efficiency. The product has earned over 70 awards from leading industry publications, including SC Magazine, Windows IT Pro, Redmond Magazine and WindowSecurity.com.

Download Free Trial: www.netwrix.com/auditor.html

Netwrix Corporation, 300 Spectrum Center Drive,
Suite 1100, Irvine, CA 92618, US

netwrix.com/social

Toll-free: 888-638-9749 **Int'l:** +1 (949) 407-5125 **EMEA:** +44 (0) 203-318-0261