netwrix

Keeping Tabs on the Top 5 Critical Exchange Server Changes with Netwrix Auditor

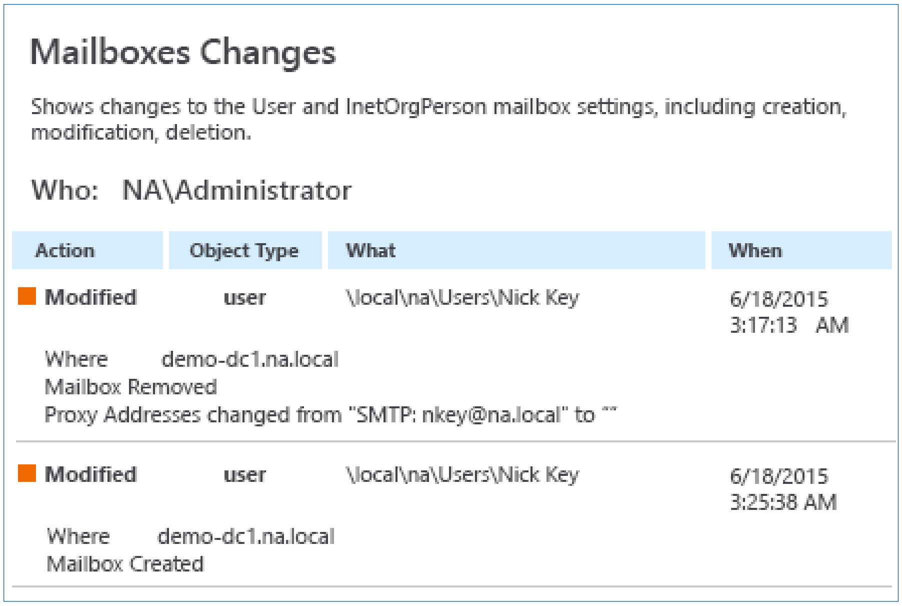
www.netwrix.com | **Toll-free**: 888.638.9749

Table of Contents

#1: Mailbox Changes

If a user mailbox is improperly modified or deleted, the user might lose access to it. Unauthorized creation of a mailbox can be a sign that a malefactor is trying to get access to your Exchange Server to perform spam and phishing attacks.
Netwrix Auditor tracks all mailbox changes and helps answer the following questions:

- Who made mailbox changes?
- Which mailboxes were changed?
- What changes were made to each mailbox?
- When was the mailbox changed?
- In which Exchange Server was the changed mailbox located?



Mailboxes Changes

Shows changes to the User and InetOrgPerson mailbox settings, including creation, modification, deletion.

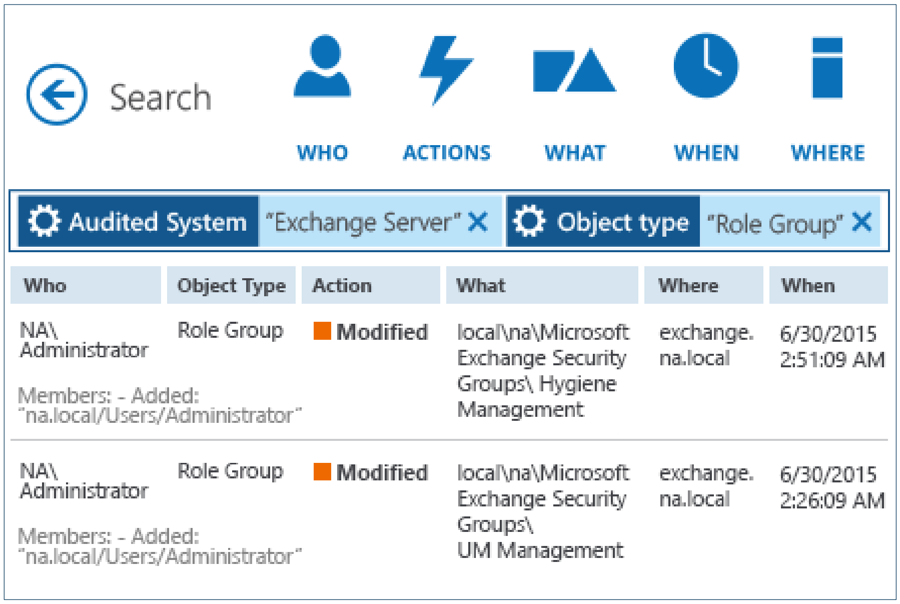
Who: NA\Administrator

Action	Object Type	What	When
🟧 **Modified**	**user**	\local\na\Users\Nick Key	6/18/2015 3:17:13 AM
Where demo-dc1.na.local Mailbox Removed Proxy Addresses changed from "SMTP: nkey@na.local" to ""			
🟧 **Modified**	**user**	\local\na\Users\Nick Key	6/18/2015 3:25:38 AM
Where demo-dc1.na.local Mailbox Created			

#2: Changes to Exchange Role Groups

Adding a user to a management role group on an Exchange Server gives that user full control over that server. The user can delete mailbox databases, edit send/receive connectors and change mailbox permissions, any of which can lead to a security breach.
Netwrix Auditor tracks all changes to Exchange role groups and helps answer the following questions:

- Who changed an Exchange role group?
- Which groups were changed?
- Who was added to or removed from each group?
- How was the Exchange role group changed?
- In which Exchange Server was the changed group located?
- When was the group changed?



Audited System "Exchange Server" ✕ Object type "Role Group" ✕

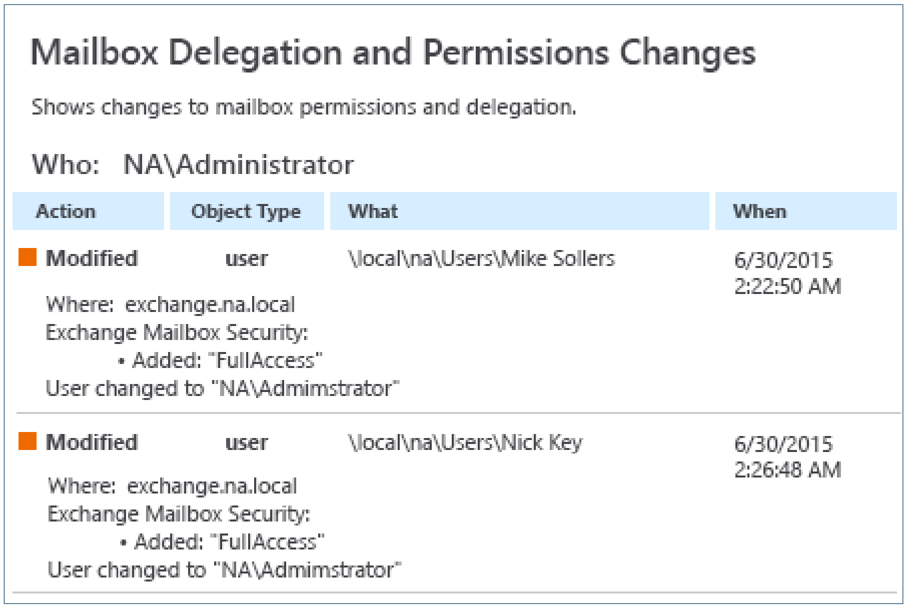
Who	Object Type	Action	What	Where	When
NA\ Administrator Members: - Added: "na.local/Users/Administrator"	Role Group	🟧 **Modified**	local\na\Microsoft Exchange Security Groups\ Hygiene Management	exchange. na.local	6/30/2015 2:51:09 AM
NA\ Administrator Members: - Added: "na.local/Users/Administrator"	Role Group	🟧 **Modified**	local\na\Microsoft Exchange Security Groups\ UM Management	exchange. na.local	6/30/2015 2:26:09 AM

#3: Changes to Mailbox Delegation and Permissions

Having full access permissions to an Exchange mailbox gives a user access to all mailbox content. This includes reading or deleting content, moving content to another location and sending phishing e-mails on behalf of the mailbox owner. Therefore, misuse of full access permissions can lead to loss of sensitive data.

Netwrix Auditor tracks all mailbox delegation and permission changes and helps answer the following questions:

- Who made changes to mailbox delegation and permissions?
- Which mailboxes were affected?
- In which Exchange Server was each change made?
- When was each change to mailbox delegation and permissions made?
- What changes were made?



Mailbox Delegation and Permissions Changes

Shows changes to mailbox permissions and delegation.

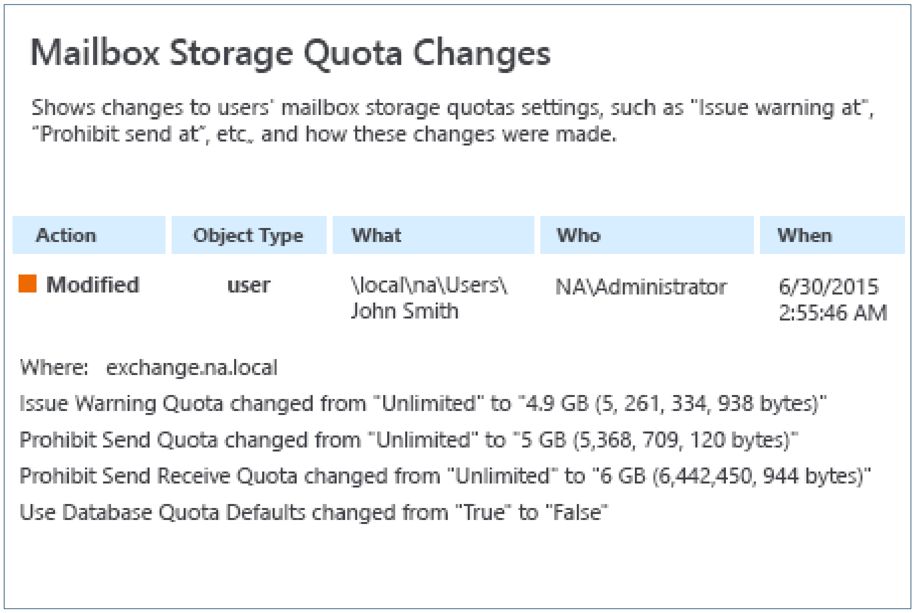
Who: NA\Administrator

Action	Object Type	What	When
🟧 **Modified**	**user**	\local\na\Users\Mike Sollers	6/30/2015 2:22:50 AM
Where: exchange.na.local Exchange Mailbox Security: • Added: "FullAccess" User changed to "NA\Admimstrator"			
🟧 **Modified**	**user**	\local\na\Users\Nick Key	6/30/2015 2:26:48 AM
Where: exchange.na.local Exchange Mailbox Security: • Added: "FullAccess" User changed to "NA\Admimstrator"			

#4: Changes to Mailbox Storage Quotas

Unauthorized increases in mailbox storage quotas can lead to uncontrolled growth of data on the Exchange Server. Lack of available space can cause the server to become unstable and even result in server downtime during which users cannot receive or send email. Netwrix Auditor tracks all changes to mailbox storage quotas and helps answer the following questions:

- Who changed mailbox storage quotas?
- Which quotas were changed?
- How was each mailbox storage quota changed?
- In which Exchange Server was the quota changed?
- When was the storage mailbox quota changed?



Mailbox Storage Quota Changes

Shows changes to users' mailbox storage quotas settings, such as "Issue warning at", "Prohibit send at", etc., and how these changes were made.

Action	Object Type	What	Who	When
🟧 Modified	user	\local\na\Users\ John Smith	NA\Administrator	6/30/2015 2:55:46 AM

Where: exchange.na.local

Issue Warning Quota changed from "Unlimited" to "4.9 GB (5, 261, 334, 938 bytes)"

Prohibit Send Quota changed from "Unlimited" to "5 GB (5,368, 709, 120 bytes)"

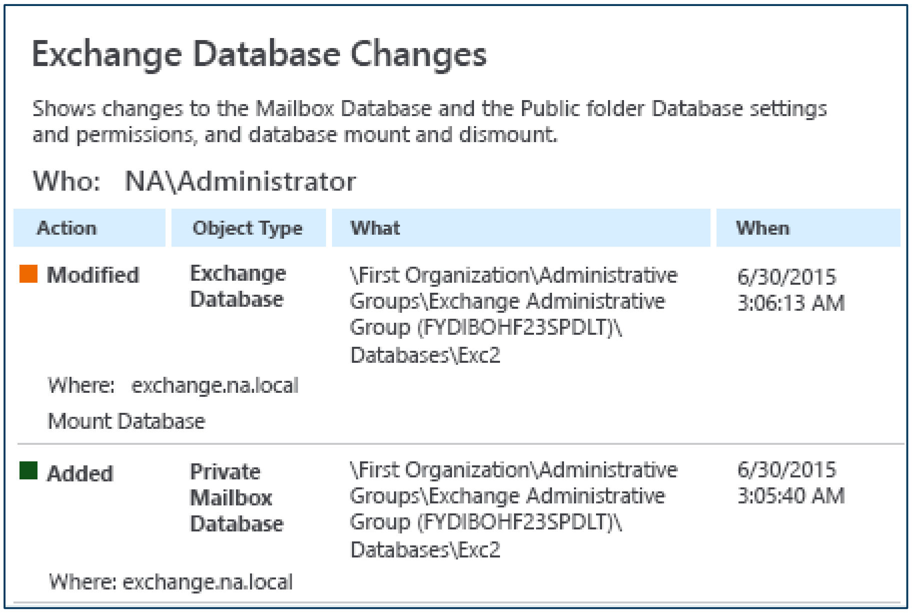
Prohibit Send Receive Quota changed from "Unlimited" to "6 GB (6,442,450, 944 bytes)"

Use Database Quota Defaults changed from "True" to "False"

#5: Exchange Database Changes

Unauthorized deletion of an Exchange database can result in users being unable to access their mailboxes or receive email. A database created outside normal controls may be a sign of a hacker trying to gain access to email messages that contain sensitive data.
Netwrix Auditor tracks all changes to Exchange databases and helps answer the following questions:

- Who changed an Exchange database?
- Which Exchange databases were changed?
- What was changed in each Exchange database?
- In which Exchange Server was each database that was changed?
- When was the Exchange database changed?



Exchange Database Changes

Shows changes to the Mailbox Database and the Public folder Database settings and permissions, and database mount and dismount.

Who: NA\Administrator

Action	Object Type	What	When
🟧 Modified	Exchange Database	\First Organization\Administrative Groups\Exchange Administrative Group (FYDIBOHF23SPDLT)\Databases\Exc2	6/30/2015 3:06:13 AM
Where: exchange.na.local Mount Database			
🟩 Added	Private Mailbox Database	\First Organization\Administrative Groups\Exchange Administrative Group (FYDIBOHF23SPDLT)\Databases\Exc2	6/30/2015 3:05:40 AM
Where: exchange.na.local			

About Netwrix Auditor

Netwrix Auditor is an IT auditing software that 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