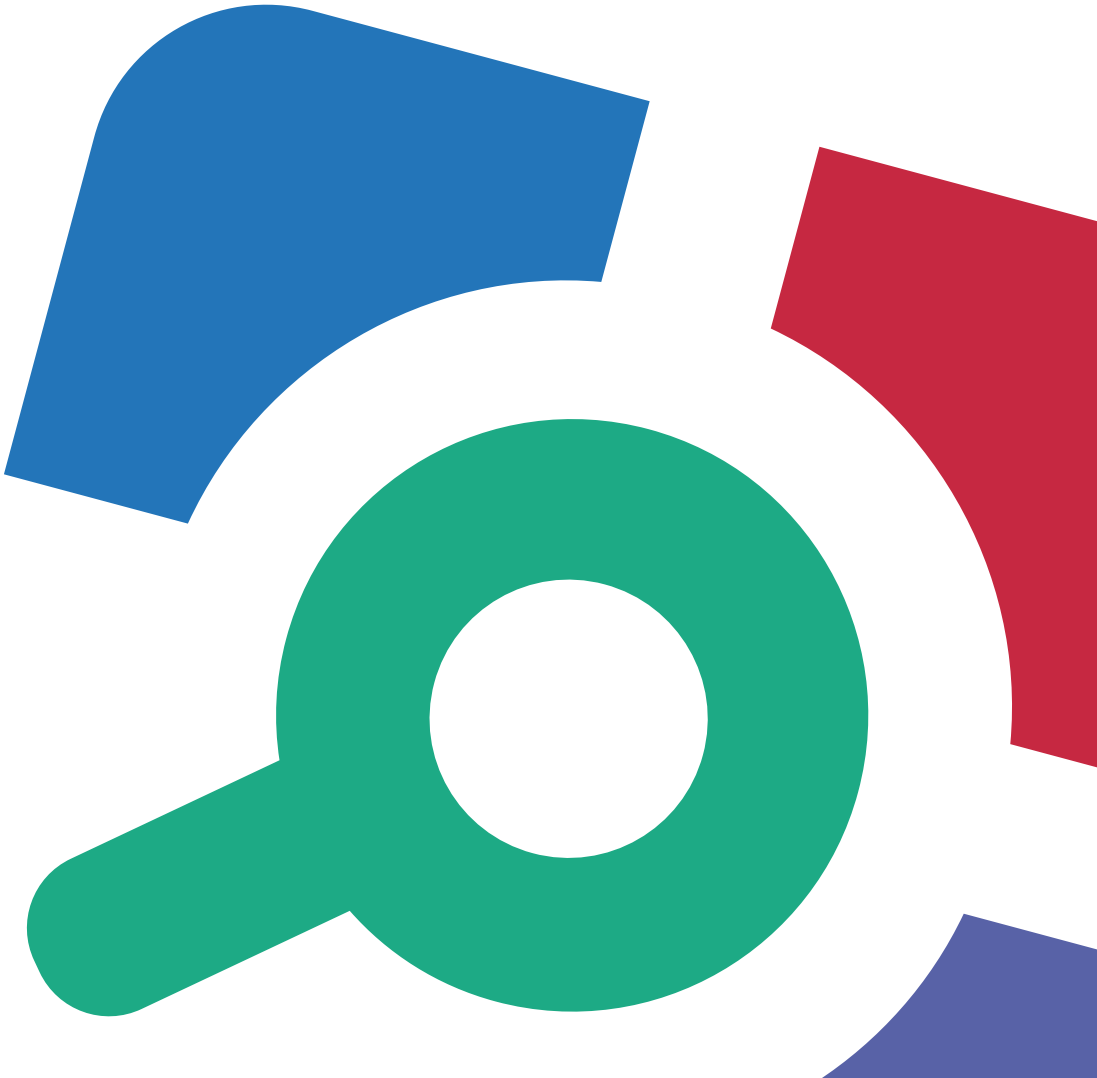
netwrix
#1 for change auditing

Netwrix Auditor

Release Notes

Product version: 6.0
5/14/2014



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, as this publication may describe features or functionality not applicable to the product release or version you are using. Netwrix makes no representations or warranties about the Software beyond what is provided in the License Agreement. Netwrix Corporation assumes no responsibility or liability for the accuracy of the information presented, which is subject to change without notice. If you believe there is an error in this publication, please report it to us in writing.

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. What's New

The new Netwrix Auditor 6.0 features are:

- **Enterprise Overview dashboards**: Netwrix Auditor provides complete visibility into what is happening in your IT infrastructure, and allows to drill down to details on every change across all audited systems.
  - Provide a high-level overview of changes across all audited systems.
  - Show activity trends by date, user, server or IT system with detailed drill-down capabilities.
  - Aggregate change events across all kinds of audited systems (Active Directory, File Servers, SharePoint, etc.) into one single view.
- **Comprehensive SharePoint auditing**: Netwrix Auditor further extends the range of audited systems, providing the broadest coverage on the market.
  - Supports SharePoint 2010 and SharePoint 2013.
  - Provides visibility into farm configuration and security changes, including modifications of permissions and permission inheritance, SharePoint group membership, permission levels, and security policies.
  - Reports on creation, deletion and modification of any SharePoint content, including sites, lists and libraries, folders, documents and list items.
- **Over 25 enhancements and fixed issues**, including scalability, performance and usability.

2. Known Issues

This section provides a list of all currently known issues that customers may experience with Netwrix Auditor 6.0. For each issue, there is a brief description and a workaround for the problem.

2.1. Netwrix Auditor for Active Directory

ID	Issue Description	Workaround
10401	Changes made through the Exchange Management Console in the Organization Configuration node (Federation Trust, Organization Relationships and Hybrid Configuration tabs) may be displayed in an internal Active Directory format that can be difficult to interpret.	Contact Netwrix Technical Support for information on how to resolve this issue.
10831	Since the AD Configuration partition is common for all domains in a forest, any change to this partition will be reported by the product for each of the audited domains. The name of the user who made the change will only be displayed for the domain where the change was made. Product reports for other audited domains will show the "System" value in the "Who Changed" column.	Ignore entries with the "System" value in the "Who Changed" column for other domains.
10956	If a user made a change and then this user's account was renamed, moved or deleted within a short period of time (less than 10 minutes), Active Directory audit reports will display a canonical user name in the "Who Changed" column. As a result, reports filtered by this user's name may contain incorrect audit data.	This is going to be fixed in the future product versions.
11090	If changes to group membership are made through Exchange Control Panel, the product will report on addition and deletion of all group members in addition to these changes.	This is going to be fixed in the future product versions.
11433	If an AD object is created using the Exchange Management Console, and then renamed through Active Directory Users and Computers within a short period of time (less than 10 minutes), the product will show duplicate entries for this change. One will show the Exchange Server name in the "Who Changed" column, and the other - the name of the user who made the change.	Ignore the duplicate entry with the Exchange Server account in the "Who Changed" field.

ID	Issue Description	Workaround
11537	If a user is added through Active Directory Users and Computers, and then a mailbox is created for this user through the Exchange Management Console within a short period of time (less than 10 minutes), the product will show duplicate entries for the mailbox creation event. One change will show the Exchange Server name in the "Who Changed" column, and the other - the name of the user who made this change.	Ignore the duplicate entry with the Exchange Server account in the "Who Changed" field.
13619	If a change is made to the audited domain through Exchange Server 2010 or 2013 installed in another domain, the originating workstation for such changes will be reported as "Unknown".	This is going to be fixed in the future product versions.
13854	If a user who belongs to the audited domain is also a member of any groups in a different domain from another forest, the product will not be able to collect the information on the latter user group membership, and these groups will not be available in report filters.	This is going to be fixed in the future product versions.
13855	If a user who belongs to the audited domain is also a member of the Domain Local Group of a different domain in the same forest, the product will not be able to collect the information on the latter user group membership, and this group will not be available in report filters.	This is going to be fixed in the future product versions.
14291	If changes to Active Directory objects are made through Exchange 2010 or 2013 Management Console or Exchange Control Panel, the "Workstation" field in reports showing the computer from which a change was made may contain several workstations.	This is going to be fixed in the future product versions.
12895	When upgrading from Netwrix Auditor 5.0.x to Netwrix Auditor6.0, the list of installed programs may contain multiple entries for the Inactive User Tracking feature.	This does not affect the product operability. Uninstall the older version of this feature.
11988	If you are auditing a non-trusted domain, and the version of the ADSI in the audited domain is higher than in the domain where Netwrix Auditor is installed, reports may return errors or contain incomplete or incorrect data.	Install an Netwrix Auditor instance in the audited domain, or migrate the product to a computer with the same ADSI version as in

ID	Issue Description	Workaround
		the audited domain.
12896	When upgrading from Netwrix Auditor 5.0.x to Netwrix Auditor6.0, the list of installed programs may contain multiple entries for the Password Expiration Alerting feature.	This does not affect the product operability. Uninstall the older version of this feature.

2.2. Netwrix Auditor for Exchange

ID	Issue Description	Workaround
11527	In Microsoft Exchange Server 2010 SP2, after a mailbox is restored using the Active Directory Object Restore wizard shipped with Netwrix Auditor, it will be inaccessible for several hours through Microsoft Outlook or Outlook Web App.	Wait for several hours before using this mailbox. For details on this issue, refer to the following Microsoft Knowledge Base Article: You cannot access a mailbox for several hours after you disconnect and then reconnect the mailbox in an Exchange Server 2010 SP2 environment
11110	For Microsoft Exchange Server 2010, changes to text strings that have line breaks will contain the before and after values only for the text fragment before the line break. The fact of the change itself will be reported for the whole text string.	Check the resulting value through Active Directory Users and Computers or other tools.
10956	If a user made a change and then this user's account was renamed, moved or deleted within a short period of time (less than 10 minutes), Exchange Server audit reports will display a canonical user name in the "Who Changed" column. As a result, reports filtered by this user's name may contain incorrect audit data.	This is going to be fixed in the future product versions.
10897	The product does not report on changes made on an Exchange Server with the Edge Transport role.	Contact Netwrix Technical Support for information on how to resolve this issue.
10896	For Microsoft Exchange Server 2010, changes made to its	Contact Netwrix Technical

ID	Issue Description	Workaround
	configuration using certain cmdlets may be displayed with the Exchange Server name in the "Who Changed" column instead of a user name.	Support for information on how to resolve this issue.
10762	For Microsoft Exchange Server 2010 and 2013, the previous values for some modified attributes will not be reported.	Contact Netwrix Technical Support for information on how to resolve this issue.
10590	For Microsoft Exchange Server 2010, changes to the inetOrgPerson object type will be reported in the Exchange Server audit reports with the "user" value in the "Object Type" column.	Contact Netwrix Technical Support for information on how to resolve this issue.
10431	If a previously disconnected mailbox is reconnected to a user, the Exchange Server audit reports will display the mailbox GUID instead of a canonical user name in the "Object Name" column. If, as a result of this operation, the email address of this user is modified, this change will be reported in the Active Directory Auditing reports with the Exchange Server name in the "Who Changed" column.	If you need to get a canonical user name in an Exchange Server Audit report, look for the "User" attribute in the "Details" field of the reconnected mailbox change entry. If you need to get the "Who Changed" value for the email address change entry, open the Exchange Server Auditing report for the same time period and look for the entry reflecting the mailbox reconnection event. The user who reconnected the mailbox is the same user who initiated the email address change event. You can match the email notification entry with the mailbox reconnection entry by comparing the ObjectPath field in the Active Directory audit report with the User attribute in the "Details" field of the Exchange Server audit

ID	Issue Description	Workaround
		report.
9744 10037	If the Mailbox Access Auditing feature is disabled and then re-enabled after some time, or an upgrade is performed, data will start to be collected only after the first scheduled data collection task is run (at 3:00 AM by default). As a result, events that occur after the feature is re-enabled or upgraded and before the first scheduled task will not be reported.	Launch the scheduled data collection task manually immediately after the feature is reenabled or upgraded. To do this, navigate to **Start** → Administrative Tools → Task Scheduler or **Start** → **Control Panel** → **Scheduled Tasks** (depending on your Windows version), locate the task titled "Netwrix Non-owner Mailbox Access Reporter for Exchange" and launch it.
9688	The Mailbox Access Auditing feature does not report on actions performed with attachments to email messages. The fact of accessing a message containing an attachment, as well as all other actions performed with this message, will be reflected in reports.	This is going to be fixed in the future product versions.
9889	The Mailbox Access Auditing feature does not report on renaming of mail folders. The fact of accessing a mail folder, as well as all other actions performed with it, will be reflected in reports.	This is going to be fixed in the future product versions.

2.3. Netwrix Auditor for File Servers

ID	Issue Description	Workaround
2871 762	Windows native audit does not write folder creation operations to the event log. As a result, Netwrix Auditor, which relies on native audit, will report these changes with the "System" value in the "Who Changed" column, or not reported at all if the **Large server support** option is enabled.	This is going to be fixed in the future product versions.
6462	If a switch between the active and the passive node occurred on a clustered file server, the changes that took place	If you plan a switch, manually launch a data

ID	Issue Description	Workaround
	between the last data collection and the switch will be reported with the "System" value in the "Who Changed" column, or not reported at all if the **Large server support** option is enabled.	collection task (click the **Run** button in the Netwrix Auditor console on your Managed Object page), wait until it has completed and then perform the switch. If the switch is unplanned, contact Netwrix Technical Support.
6615	If you apply granular audit configuration (available on Windows Vista or later) to the Object Access policy that must be configured to log audit data, the product will be unable to verify these audit settings. As a result, you will be getting warning messages saying that audit has been configured incorrectly.	Ignore these warning messages as they do not affect the product functionality. This is going to be fixed in the next product version. For more information on the granular audit configuration, refer to the following Netwrix article: How to Configure Granular Audit Policy on a File Server Monitored by Netwrix Auditor.
8496	If the **Attach the email reports as a CSV file** option is enabled, and an attachment is opened in Microsoft Excel, non-ASCII symbols may not be rendered correctly.	Instead of double-clicking an attached report, save the file, then in Microsoft Excel navigate to **Data→From Text** and select the file you want to view.
9450 9208 8887	If the **Large server support** option is enabled, viewing an object's security properties may be reported as a change to these properties.	This is going to be fixed in the future product versions.
10000	The product cannot detect overwriting of the security event log on a NetApp Filer appliance.	Configure the scheduled data collection task to run several times a day, or enable automatic log archiving. For instructions refer to Netwrix Auditor

ID	Issue Description	Workaround
		Administrator's Guide.
9514	Audit of NetApp Filer appliances cannot be configured in the Netwrix Auditor console, and is only available through the Standard configuration mode.	This is going to be fixed in the next product version. For detailed instructions on how to audit of NetApp Filer appliances, refer to Netwrix Auditor Administrator's Guide.
1734	The product cannot verify the current audit policy settings on an EMC VNX/VNXe/Celerra appliance. As a result, if the audit policy is configured incorrectly, you will be setting empty or incorrect reports with no warning.txt file attached explaining the reason for the problem.	For instructions on how to configure audit to monitor an EMC VNX/VNXe/Celerra appliance, refer to Netwrix Auditor Installation and Configuration Guide.
9512	Audit of EMC VNX/VNXe/Celerra appliances cannot be configured in the Netwrix Auditor console, and is only available through the Standard configuration mode.	This is going to be fixed in the next product version. For detailed instructions on how to audit of NetApp Filer appliances, refer to Netwrix Auditor Administrator's Guide.

2.4. Netwrix Auditor for SharePoint

ID	Issue Description	Workaround
1549	SharePoint Central Administration URL specified on Managed Object creation cannot exceed 80 characters.	If your SharePoint Central Administration URL exceeds 80 characters, create a short name and specify it in the Alternate Access Mappings, and create a Site Binding in IIS for SharePoint Central Administration v4.
9165	If you move an Item between Lists using the **Move** menu option on the **Site Settings - Site Content and Structure** page, audit reports and Change Summaries will contain two	Ignore the multiple change entries.

ID	Issue Description	Workaround
	change entries associated with this event: List Item Removed and List Item Added.	
12683	When a lot of SharePoint changes are made within a short period of time (15-20 changes per second), some events may be lost and not reflected in audit reports and Change Summaries because of the default IIS recycle settings (the IIS Worker Process that accumulates data on changes is restarted before all data is written to the audit database).	Modify the default IIS recycle settings to keep data when the process is restarted. For details on how to configure recycling, refer to the following Microsoft article: Recycling Settings for an Application Pool.
12883	The timestamp for SharePoint farm configuration changes in audit reports and email Change Summaries is the time when Netwrix Auditor generates the daily Change Summary, not the actual event time.	This is going to be fixed in the future product versions.
9133	When you activate the Publishing Feature, SharePoint audit reports may contain a number of internal changes associated with this event.	This is going to be fixed in the future product versions.
13445	The following changes are reported by the product with the "Unknown" value in the "Who Changed" column: • Automatic creation of SharePoint groups on site creation if it uses unique permissions instead of inheriting them • All changes made under the "Anonymous" user if the security policy permits such changes	This is going to be fixed in the future product versions.
13455	When a web application is created or when Service Accounts are modified, SharePoint audit reports and Change Summaries may contain a number of internal security changes for the following site collection: *http://%centraladministration%/sites/help*.	This is going to be fixed in the future product versions.
13918	The following changes are reported with the "SHAREPOINT\system" value in the "Who Changed" column: • Changes made under an account that belongs to Farm Admins • Changes made under an account that is a Managed account for the Web Application Pool	This is going to be fixed in the future product versions.

ID	Issue Description	Workaround
	• Changes made under an account that is specified in the User Policy of the modified Web Application with the **"Operates as a system"** option enabled • Changes resulting from SharePoint Workflows	
13923	Creation, deletion and modification of folders in SharePoint Libraries will be reported by the product with the "List Item" value in the "Object Type" column. Creation, deletion and modification of sub-folders and documents inside these sub-folders will be reported with the path to the list instead of the folder path in the "Object Path" column.	This is going to be fixed in the future product versions.
13926	The following changes are reported by the product with the "Not applicable" value in the "Who Changed" column: • Addition and removal of servers, changes to service status • Web application creation and deletion, changes to key web application settings • Changes to the following web application security policies: anonymous access policy, user policy, security policy levels • Site collection creation and deletion, changes to key site collection settings • Addition, removal and deployment of SharePoint solutions • Addition and removal, activation and deactivation of farm-wide features	This is going to be fixed in the future product versions.

13977	The following changes are reported with the "Not applicable" value in the "Workstation" field in the Change Summary emails (in audit reports the "Workstation" field will be missing for these changes):
	• Content Security changes
	  • Assignment of permissions to SharePoint sites, lists, libraries, folders, documents or items
	  • Permission inheritance break or restore on any
		This is going to be fixed in the future product versions.

ID	Issue Description	Workaround
	SharePoint object • Creation and deletion of SharePoint groups, as well as changes to group membership • Creation, deletion and modification of permission levels • Farm configuration changes • Changes to the Farm administrators group membership • Addition and removal of servers, changes to service status • Web application creation and deletion, changes to key web application settings • Changes to the following web application security policies: anonymous access policy, user policy, security policy levels • Site collection creation and deletion, changes to key site collection settings • Addition, removal and deployment of SharePoint solutions • Addition and removal, activation and deactivation of farm-wide features The "Workstation" field is not reported for content changes if they were made in one of the following ways: • Through powershell cmdlets • Through the **Site settings** → **Content and Structure** menu • Through Microsoft servers and Office applications integrated with SharePoint • Through SharePoint workflows • Through the **Upload Multiple Files** menu option • Through the **Open With Explorer** menu option • Through a shared folder • Deletion of items through the context menu	

ID	Issue Description	Workaround
14009	If an object was deleted within 30 minutes after its permissions were modified, permission modifications will be reported by the product with the "SharePoint Object" value in the "Object Type" column.	This is going to be fixed in the future product versions.
14591	When you create a SharePoint site based on a SharePoint 2010 template, SharePoint audit reports may contain change entries for the creation of all default Lists and Items that belong to this site. This applies to the following SharePoint 2010 templates: • Access Services Site • Assets Web Database • Charitable Contributions Web Database • Projects Web Database • Issues Web Database • Collaboration Portal	This is going to be fixed in the future product versions.
15051	If you create a site collection based on the SharePoint 2010 template on SharePoint 2013, and then update the template to SharePoint 2013, audit reports and Change Summaries will contain a number of internal changes associated with this event.	This is going to be fixed in the future product versions.
15342	When upgrading from Netwrix Auditor 5.0.80 or below to Netwrix Auditor 6.0, the list of installed programs may contain multiple entries for the SharePoint Auditing feature.	This does not affect the product operability. Uninstall the older version of this feature.

2.5. Netwrix Auditor for SQL Server

ID	Issue Description	Workaround
3133 7688 7769 7871	The following changes are reported with the "System" value in the "Who Changed" column: • Modifications to Server Instance, Application Role, Database, Stored Procedure and Tables on a SQL Server 2000 instance	This is going to be fixed in the future product versions.

ID	Issue Description	Workaround
	• Backup operations • Removal of an SQL Job together with unused schedules • Database restore from backup to a new database	
3117	If you are auditing a SQL Server 2000 instance installed on an x64-bit system, automatic audit configuration will fail (you will receive a warning message).	Manually specify the path to SQL trace logs. For instructions on how to do this, refer to the following Netwrix KB article: How I can change the SQL Server Change Reporter log path on the SQL Server?
6789	With the Database Content Audit option enabled for the SQL Server Auditing feature, when you try to perform the UPDATE/INSERT/DELETE operations in an audited database, an error is returned stating that the statements cannot be executed because the database owner SID cannot be resolved or SIDs do not match. **NOTE:** Database backup and restore may lead to unresolved or not matching SIDs.	For detailed information about the issue and for a solution, refer to the following Netwrix KB article: An error is returned stating that you have problems accessing an audited database.

2.6. Netwrix Auditor for VMware

ID	Issue Description	Workaround
13168	When upgrading from Netwrix Auditor 5.0.x to Netwrix Auditor 6.0, the list of installed programs may contain multiple entries for the VMware Auditing feature.	This does not affect the product operability. Uninstall the older version of this feature.

2.7. Netwrix Auditor for Windows Server

ID	Issue Description	Workaround
12743 12765	The following changes will be reported with the "System" value in the "Who Changed" column:	This is going to be fixed in the future product versions.

ID	Issue Description	Workaround
12795 13365	• Creation of new scheduled tasks on computers running Windows 2003. • Renaming a scheduled task on computers running Windows XP/2003 if no other parameters are modified for the renamed task. • Changes to child registry keys (i.e. the keys that other keys link to). • Renaming a network connection on computers running Windows XP/2003 (for Windows Vista/7/2008/2012, the "Who Changed" column will contain the target computer name). • Creation of a new registry key if no value has been set for it.	
12740	If you browse for an Active Directory container when adding items to the audited Computer Collection, child domains of trusted domains will not appear in this list.	User a different choice option (computer name / IP address range / import from file) to specify target computers.
12745	Software upgrade is reported by the product as two consecutive changes: software removal and software installation. The entry for software removal will have the "System" value in the "Who Changed" column.	Look for the user name in the entry for software installtion to determine who performed the upgrade.
12936	No audit data is collected from computers running Windows XP/2003 if they are specified in the audited Computer Collection as CNAME records.	Specify the actual name of the target computer.
11637	Although you can configure the product to write video only if certain applications are activated, the whole desktop will be captured, not just the application windows that trigger a video recording session.	In the future product versions a choice option is going to be implemented to select whether the whole desktop must be captured, or only the selected applications and windows.
12100	On Windows XP/2003, the information on the launch of applications through the "Run as different user" menu option is not written to the detailed activity log (reports	This is going to be fixed in the future product versions.

ID	Issue Description	Workaround
	metadata). As a result, it will be unavailable for data search and positioning inside video files.	
12182	If a monitored user connects via an RDP session to a computer that is not monitored by Netwrix Auditor (i.e. the agent is not installed on the remote computer), the information on the launch of applications and opening windows inside this RDP session is not written to the detailed activity log (reports metadata). As a result, data search and positioning inside video files will be unavailable for such video recording sessions. All activity inside such RDP session will still be captured and will be availbale for playback.	To get a detailed activity log, configure the product to monitor the computer accesed through an RDP connection. When a computer is added to the audited computer collection, the Netwrix Auditor agent will be installed on it that will collect both video and a detailed activity log (metadata).
12451	Video capture of an RDP session will be termindated if this session is taken over by another user.	This is going to be fixed in the future product versions.
12776 11838	On computers running Windows XP/2003/Vista/2008, if a console application (i.e. an application that does not have its own grpahical user interface and is executed via a command line interface) is launched, the information about this launch and the command line parameters are not written to the detailed activity log (reports metadata). Therefore, data search and positioning inside video files will be unavailable for such applications. The command line parameters and the launch of the application will still be captured and will be available for playback.	This is going to be fixed in the future product versions.
12763	Links to video recordings will not open from reports saved in the doc/xls format, or reports received by subscription and attached to emails in one of these formats.	Save reports in the PDF format and select this format when configuring a subscription to a report.
12770	If integration of video records into audit reports for different audited systems is enabled, the Active Directory, Group Policy and Exchange Server audit reports called "All Changes with Video" contain audit data for Active Directory *and* Exchange Server *and* Group Policy changes.	Contact Netwrix Technical Support to get separate reports for each type of audit data.
12807	On Windows 8/Windows Server 2012, the information on	This is going to be fixed in

ID	Issue Description	Workaround
	the launch of Windows Store (Metro-style) applications is not written to the detailed activity log (reports metadata), as applications in a tile-based interface do not have application descriptions or window titles. Therefore, data search or positioning inside video files will be unavailable for such applications. A video recording session will no start before the user accesses their desktop for the first time.	the future product versions.
12951	If an Activity Records summary is generated with the **Show detailed user activity log** option enabled, and then saved in the HTML format, clicking the links for different timestamps will start video playback from the beginning.	For positioning and data search, watch Activity Records summaries from the Netwrix Auditor console.
10029	After a Managed Object with the Event Log Management feature enabled for it is deleted from the Netwrix Auditor console, a scheduled task associated with this Managed Object will not be deleted automatically.	Delete the task manually in the Task Scheduler. The task name is "Netwrix Management console - Event Log Manager - <managed_ object_name>".
10305	If you launch data collection manually for the Event Log Management feature (by clicking the **Run** button on your Managed Object page in the Netwrix Auditor console), and there is an invalid email address in the **Events Summary Recipients** list, email delivery will fail to all addresses, not just the invalid one.	When you add a new address to the **Events Summary Recipients** list, it is recommended to click the **Verify** button to check if this address is valid.

3. What Has Been Fixed

This section lists all issues that have been fixed in Netwrix Auditor 6.0.

ID	Issue Description
Netwrix Auditor for Active Directory	
9821	It takes Netwrix Auditor a long time to write Group Policy changes to the audit database.
13659	In large environments with a great number of changes (around 5000 per day) it takes Netwrix Auditor a long time to process audit data. Change Summary generation may take up to 15 hours.
14132 14171 14648 15309 15312	It takes Netwrix Auditor a long time to process logon events.
7655 8205 11638 12523 12536	Netwrix Auditor may hang up when collecting or processing audit data.
8067	If a modified Active Directory object contains the ' symbol as part of it name, the corresponding configuration snapshot will not be updated.
8071	It takes Netwrix Auditor a long time to process events "4740: A user account was locked out".
8926	It takes Netwrix Auditor a long time to import a configuration snapshot into the audit database on a SQL Server.
9234	Netwrix Auditor fails to deliver daily Active Directory and Group Policy email Change Summaries when omitting errors through the omitreporterrors.txt file is configured.
9461	Netwrix Auditor fails to delete temporary snapshot and timestamp files from the %Temp% folder.

ID	Issue Description
10596 11387 11405	Some changes are reported with the "system" value in the "Who Changed" field.
10611	Email Change Summaries may contain duplicate entries for the same change.
11367	Email Change Summaries may contain network errors that do not affect the integrity of collected audit data.
12391	Some Active Directory changes are displayed in daily Change Summaries, but are not saved into the SQL database.
20285	Netwrix Auditor fails to send administrator notifications on users' inactivity to multiple recipients.
22663	The Inactive User Tracking feature fails to move an account to the specified organizational unit.
23296	Poor performance (the product fails to process domains/OUs with a large number of users).
23296	Netwrix Auditor fails to process accounts information if the queried DC is highly loaded.
6651	If the MemoryPageSize registry key is set to a value different from zero, Netwrix Auditor fails to collect data on inactive accounts.
40566	Netwrix Auditor does not always correctly process the last logon time in environments with a large number of domain controllers.
8195	The Password Expiration Alerting feature fails if a managed organizational unit contains the / symbol as part of its name.
12206	The Password Expiration Alerting feature fails to save SMS notification settings.
Netwrix Auditor for Exchange	
9240	It takes Netwrix Auditor a long time to collect Administrator Audit Logging events from the audited Exchange organization.
Netwrix Auditor for SQL Server	
30099	Netwrix Auditor fails to inform users about database content audit errors on non-English Windows versions.

ID	Issue Description
8163	If connection to an audited SQL Server is lost, or it is disconnected during audit data collection, Netwrix Auditor returns fake "Add/Remove" events in audit reports and Change Summaries.
9632	If backup events are excluded from the Netwrix Auditor reports on SQL Server changes, the product fails to write audit data to the reporting SQL database.
12762	If the Database Content Audit option is seleted, Netwrix Auditor by default enables database content audit on all databases stored on the audited SQL Server.
Netwrix Auditorfor VMware	
12931	If the time zone on the audited vCenter server is different from UTC, audit data on changes may be incomplete.
Netwrix Auditor for Windows Server	
5574	Netwrix Auditor fails when collecting audit data from DNS servers with a large number of resource records.
9426	Netwrix Auditor returns false warnings about event log overwrites that did not occur.
12258	No support for user profiles stored in a different volume from the Netwrix Auditor agent repository where files with audit data are stored.
26215	Netwrix Auditor writes the "Default" value in the Event Log field in the SQL audit database, instead of the actual log name (Security, Application, System, etc.)
25745	Netwrix Auditor fails to process Event log backups stored in a non-default location (the default directory is %SystemRoot%\system32\winevt\Logs\
7585	Netwrix Auditor cannot process syslog events that contain the # symbol.
9426	Netwrix Auditor returns false warnings about event log overwrites that did not occur.