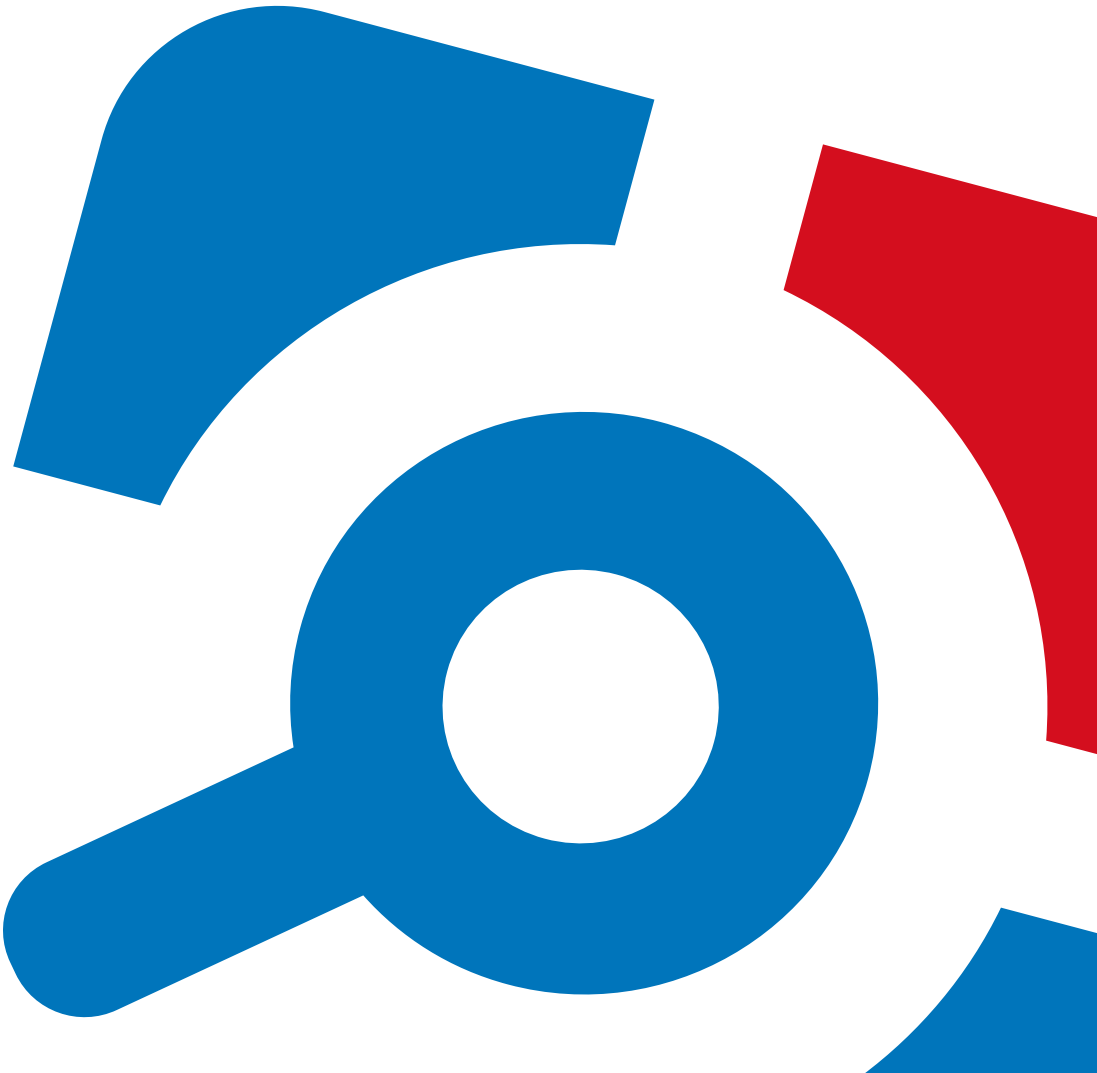
netwrix
#1 for change auditing

Netwrix All-in-One Suite Features and Requirements

Version: 5.0
5/21/2015



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.

© 2015 Netwrix Corporation.

All rights reserved.

Table of Contents

1. Netwrix All-in-One Suite Overview 4
   1.1. Netwrix Auditor Overview 4
   1.2. Netwrix Password Manager Overview 6
2. System Requirements 7
   2.1. Netwrix Auditor System Requirements 7
      2.1.1. Requirements for Audited System 7
      2.1.2. Requirements to Install Netwrix Auditor 8
         2.1.2.1. Hardware Requirements 8
         2.1.2.2. Software Requirements 9
      2.1.3. Supported Microsoft SQL Server Versions 10
   2.2. Netwrix Password Manager System Requirements 11
      2.2.1. Hardware Requirements 11
      2.2.2. Software Requirements 12
3. Appendix: Supporting Data 13
   3.1. Install Microsoft SQL Server 13
      3.1.1. Install Microsoft SQL Server 2012 Express 13
      3.1.2. Verify Reporting Services Installation 13
   3.2. How to Install IIS on Different Windows Versions 14

1. Netwrix All-in-One Suite Overview

Netwrix All-in-One Suite 5.0 combines Netwrix products into one integrated platform aimed at sustaining security and compliance across your IT infrastructure. The suite contains configuration and change auditing, and password management solutions that facilitate and streamline most administrative tasks of an IT department in any organization.

Netwrix All-in-One Suite 5.0 comprises the following products:

- Netwrix Auditor 7.0
- Netwrix Password Manager 6.5

1.1. Netwrix Auditor Overview

Netwrix Auditor is a change and configuration auditing platform that streamlines compliance, strengthens security and simplifies root cause analysis across the entire IT infrastructure.

Netwrix Auditor enables complete visibility into both security configuration and data access by providing actionable audit data about *who* did *what*, *when*, and *where*, and *who* has access to *what*. Netwrix Auditor helps prevent security breaches caused by insider attacks, pass audits and minimize compliance costs or just keep tabs on what privileged users are doing in the environment and why.

With over 6,000 customers from 28 industries and more than 70 industry awards, Netwrix Auditor is the only platform that combines both security configuration management and data access governance across the broadest variety of IT systems, including Active Directory, Exchange, File Servers, SharePoint, SQL Server, VMware, Windows Server and others. It also supports privileged user activity monitoring on all other systems, even if they do not produce any logs, via user activity video recording with the ability to search and replay.

Netwrix Auditor brings AuditIntelligence™ with:

- Change and access auditing: determine *who* changed *what*, *when*, and *where*.
- AuditIntelligence search: browse audit data, investigate incidents and keep track of changes.
- Configuration assessment: analyze current and past configurations with the state–in–time reports.
- Predefined reports: pass audits with a variety of out–of–the–box reports and stay compliant with international standards.

Netwrix Auditor employs AuditAssurance™, a patent–pending technology that does not have the disadvantages of native auditing or SIEM (Security Information and Event Management) solutions that rely on a single source of audit data. Netwrix Auditor utilizes an efficient, enterprise–grade architecture that

consolidates audit data from multiple independent sources and scalable two–tiered Audit Archive (file–based local Long–Term Archive and short-term SQL-based Audit Database) holding consolidated audit data for 10 years or more.

The table below provides an overview of each Netwrix Auditor solution:

Solution	Features
Netwrix Auditor for Active Directory	Netwrix Auditor for Active Directory detects and reports on all changes made to the managed Active Directory domain, including AD objects, Group Policy configuration, directory partitions and more. It also makes daily snapshots of the managed domain's structure that can be used to assess its state at present or at any moment in the past. In addition, Netwrix Auditor for Active Directory provides a built–in Active Directory Object Restore tool that allows reverting unwanted changes to AD objects down to their attribute level.
Netwrix Auditor for Exchange	Netwrix Auditor for Exchange detects and reports on all changes made to Microsoft Exchange configuration and permissions.
Netwrix Auditor for File Servers	Netwrix Auditor for File Servers detects and reports on all changes made to Windows–based file servers, EMC storages and NetApp Filer appliances, including modifications of files, folders, shares and permissions, as well as failed and successful access attempts.
Netwrix Auditor for SharePoint	Netwrix Auditor for SharePoint detects and reports on all changes made to SharePoint farms, servers and sites, including modifications of content, security settings and permissions.
Netwrix Auditor for SQL Server	Netwrix Auditor for SQL Server detects and reports on all changes to SQL Server configuration and database content.
Netwrix Auditor for VMware	Netwrix Auditor for VMware detects and reports on all changes made to ESX servers, folders, clusters, resource pools, virtual machines and their virtual hardware configuration.
Netwrix Auditor for Windows Server	Netwrix Auditor for Windows Server detects and reports on all changes made to Windows–based servers' configuration, including hardware devices, drivers, software, services, applications, networking settings, registry settings, DNS, and more. It also provides automatic consolidation and archiving of event logs data. Netwrix Auditor collects Windows event logs and syslog events from multiple computers across the network, stores them centrally in a compressed format, and enables convenient analysis of event log data. In addition, Netwrix Auditor for Windows Server can be configured to capture a video of users' activity on the audited computers.

1.2. Netwrix Password Manager Overview

Netwrix Password Manager is a solution that helps reduce help-desk and administration workload when addressing password issues. The product does the following:

- Provides end-users with self-service web access to common password management tasks.
- Allows help-desk operators to manage user accounts and view reports on their status through a simple web interface.
- Allows administrators to enforce restrictions on what kind of passwords can be used, and to apply security policies and identity verification procedures to the managed domain.

2. System Requirements

2.1. Netwrix Auditor System Requirements

This section lists the requirements for the systems that are going to be audited with Netwrix Auditor, and for the computer where the product is going to be installed. Refer to the following sections for detailed information:

- Requirements for Audited System
- Requirements to Install Netwrix Auditor

2.1.1. Requirements for Audited System

The table below provides the requirements for the systems that can be audited with Netwrix Auditor:

Audited System	Supported Versions
Active Directory	Domain Controller OS versions: • Windows Server 2008/2008 R2 • Windows Server 2012/2012 R2
Exchange	• Exchange 2007 • Exchange 2010 • Exchange 2013
File Servers	• Windows Desktop OS: Windows Vista SP2 (32 and 64-bit) and above • Windows Server OS: Windows Server 2008 SP2 (32 and 64-bit) and above • EMC VNX/VNXe/Celerra families (CIFS configuration only) • NetApp Filer (CIFS configuration only)
SharePoint	• SharePoint Foundation 2010 and SharePoint Server 2010 • SharePoint Foundation 2013 and SharePoint Server 2013
SQL Server	• SQL Server 2005 • SQL Server 2008 • SQL Server 2008 R2

Audited System	Supported Versions
	• SQL Server 2012 • SQL Server 2014
VMware	• VMware ESXi 4.x and above • vSphere vCenter 4.x and above
Windows Server	• Desktop OS: Windows Vista SP2 (32 and 64-bit) and above • Server OS: Windows Server 2008 SP2 (32 and 64-bit) and above
Cisco	Cisco ASA 5500 Series Adaptive Security Appliance Software Release 8.0
DNS	• Desktop OS: Windows Vista SP2 (32 and 64-bit) and above • Server OS: Windows Server 2008 SP2 (32 and 64-bit) and above
Event Log	• Desktop Windows OS: Windows Vista SP2 (32 and 64-bit) and above • Server Windows OS: Windows Server 2008 SP2 (32 and 64-bit) and above • Any Linux system using Syslog (event collection rules must be created manually)
IIS	IIS 7.0 (integrated with Windows Server 2008 R2)
User Activity	• Desktop OS: Windows Vista SP2 (32 and 64-bit) and above • Server OS: Windows Server 2008 SP2 (32 and 64-bit) and above

2.1.2. Requirements to Install Netwrix Auditor

This section provides the requirements for the computer where Netwrix Auditor is going to be installed. Refer to the following sections for detailed information:

- Hardware Requirements
- Software Requirements

2.1.2.1. Hardware Requirements

Before installing Netwrix Auditor, make sure that your hardware meets the following requirements:

Hardware Component	Minimum	Recommended
Processor	Intel or AMD 32 bit, 2 GHz	Intel Core 2 Duo 2x 64 bit, 3 GHz
RAM	2 GB	8 GB
Disk space	• Full installation—1 TB The disk space required for Netwrix Auditor to function properly depends on the average number of changes per day in the audited environment, Audit Database location and Long-Term Archive retention settings. **NOTE:** Netwrix Auditor informs you if you are running out of space on a system disk where Long-Term Archive is stored by default. You will see events in the **Netwrix Auditor System Health** log once the free disk space starts approaching minimum level. When the free disk space is less than 3 GB all Netwrix services will be stopped. • Client installation—200 MB	
Screen resolution	1280 x 1024	1920 x 1080 and higher

2.1.2.2. Software Requirements

The table below lists the minimum software requirements for the Netwrix Auditor installation:

Component	Full installation	Client installation (only Netwrix Auditor client)
Operating system	• Desktop OS: Windows 7 SP1 (64-bit) and above • Server OS: Windows Server 2008 R2 SP1 and above **NOTE:** 32-bit operating systems are not supported.	• Desktop OS: Windows 7 SP1 (32 and 64-bit) and above • Server OS: Windows Server 2008 R2 SP1 and above **NOTE:** Both 32 and 64-bit operating systems are supported.
Framework	• .Net Framework 3.5 SP1	
Additional software	• Windows Installer 3.1 and above • Windows Media Player (only required to audit user activity)	• Windows Installer 3.1 and above

Component	Full installation	Client installation (only Netwrix Auditor client)
	• Group Policy Management Console (only required to audit Group Policy changes) Download Remote Server Administration Tools that include GPMC for: • Windows 7 • Windows 8 • Windows 8.1 For Windows Server 2008/2008 R2/2012/2012 R2, Group Policy Management is turned on as a Windows feature.	

2.1.3. Supported Microsoft SQL Server Versions

Microsoft SQL Server provides Reporting Services that enables creating reports based on data stored in Audit Database. Netwrix Auditor uses Reporting Services to run data searches and generate reports on changes to the audited environment and on the point-in-time configuration.

To take advantage of reports and search capabilities of the Netwrix Auditor client, SQL Server must be deployed on the same computer where Netwrix Auditor is installed, or on a computer that can be accessed by the product.

The following SQL Server versions are supported:

Version	Edition
SQL Server 2008	Standard or Enterprise Edition **NOTE:** SQL Server Reporting Services 2008 is not supported. In this case you have to install and configure Reporting Services 2008 R2 and above manually.
SQL Server 2008 R2	Express Edition with Advanced Services Standard or Enterprise Edition
SQL Server 2012	Express Edition with Advanced Services

Version	Edition
	Standard or Enterprise Edition
SQL Server 2014	Express Edition with Advanced Services Standard or Enterprise Edition

The following SQL Server Reporting Services versions are supported: 2008 R2 and above.

NOTE: It is recommended to consider the maximum database size in different SQL Server versions, and make your choice based on the size of the environment you are going to monitor, the number of users and other factors. Note that the maximum database size in SQL Server Express editions may be insufficient.

SQL Server is not included in the product installation package and must be installed manually or automatically through the **AuditIntelligence Settings** wizard. This wizard automatically installs SQL Server 2012 Express Edition with Advanced Services and configures Reporting Services.

For your convenience, Netwrix provides instructions on the manual installation of Microsoft SQL Server with Advanced Services. See Install Microsoft SQL Server for more information. For full installation and configuration details, refer to the documentation provided by Microsoft.

NOTE: If you install Netwrix Auditor on a read-only domain controller, SQL Server installation will fail (both manual or automatic through the **AuditIntelligence Settings** wizard). This is a known issue, for details refer to the following Microsoft Knowledge base article: You may encounter problems when installing SQL Server on a domain controller. To fix the issue, install Netwrix Auditor on another computer, or install SQL Server manually on a different computer that can be accessed by the product.

You can also configure Netwrix Auditor to use an exiting SQL Server instance.

NOTE: If you have more than one Netwrix Auditor Server running in your network, make sure to configure them to use different SQL Server instances. The same SQL Server instance cannot be used to store audit data collected by several Netwrix Auditor Servers.

2.2. Netwrix Password Manager System Requirements

2.2.1. Hardware Requirements

Before installing Netwrix Password Manager, make sure that the computers, where Netwrix Password Manager is going to be installed, meet the following hardware requirements:

Hardware Component	Minimum	Recommended
Processor	Intel or AMD 32 bit, 2 GHz	Intel or AMD 64 bit, 3 GHz, Core
Memory	512 MB	4 GB
Hard Disk	20 MB	50 GB

2.2.2. Software Requirements

The table below lists the software requirements for Netwrix Password Manager. Make sure that this software has been installed on the Netwrix server before proceeding with the installation.

Component	Password Manager Service Web Application	Password Manager Client
Operating system	• Desktop OS: Windows Vista SP2 and above • Server OS: Windows Server 2008 SP2 and above	
Web browser	• Microsoft Internet Explorer 6.0 and above • Mozilla FireFox 2.0 and above • Apple Safari 2.0 and above • Google Chrome 4.0 and above	
Framework	.Net Framework 3.5 SP1	not required
IIS	IIS 7.0 and above (Web Server role) The following features must be enabled prior to the installation: • IIS 6 Metabase Compatibility • ASP • ASP.NET • Windows Authentication • HTTP Redirection See How to Install IIS on Different Windows Versions for more information.	not required
Additional software	Windows Installer 3.1 and above	not required

3. Appendix: Supporting Data

3.1. Install Microsoft SQL Server

This section provides instructions on how to:

- Install Microsoft SQL Server 2012 Express
- Verify Reporting Services Installation

3.1.1. Install Microsoft SQL Server 2012 Express

This section only provides instructions on how to install SQL Server 2012 with Advanced Services and configure the Reporting Services required for Netwrix Auditor to function properly. For full installation and configuration instructions, refer to Microsoft documentation.

1. Download SQL Server 2012.
2. Run the installation package and follow the instructions of the wizard until you get to the **Feature Selection** page. On this page, ensure that the **Reporting Services** option is selected under **Instance Features**.
3. Proceed with the wizard until you get to the **Server Configuration** page. On this page, ensure that the **SQL Server Reporting Services** will run under the **Network Service account**, and its startup type is set to *"Automatic"*.
4. Follow the instructions of the wizard to complete the installation.

3.1.2. Verify Reporting Services Installation

As a rule, Netwrix Auditor can use Reporting Services installed with the default settings. However, to ensure that Reporting Services is properly configured, it is recommended to perform the following procedure:

NOTE: You must be logged in as a member of the **local Administrators** group on the computer where SQL Server 2012 Express is installed.

1. Depending on SQL Server version installed, navigate to **Start** → **All Programs** → **Microsoft SQL Server 2012** → **Configuration Tools** → **Reporting Services Configuration Manager.**
2. In the **Reporting Services Configuration Connection** dialog, make sure that your local report server instance (for example SQLExpress) is selected and click **Connect**.
3. In the **Reporting Services Configuration Manager** left pane, select **Web Service URL**. Make sure that **Virtual Directory** is set to *"ReportServer_ <YourSqlServerInstanceName>"* (for example

ReportServer_SQLEXPRESS for SQLEXPRESS instance) and **TCP Port** is set to *"80"*.

4. In the **Reporting Services Configuration Manager** left pane, select **Database**. Make sure that the **SQL Server Name** and **Database Name** fields contain correct values. If the fields contain incorrect values, click **Change Database** and complete the **Report Server Database Configuration** wizard.
5. In the **Reporting Services Configuration Manager** left pane, select **Report Manager URL**. Make sure **Virtual Directory** is set correctly, and that the URL is valid.

3.2. How to Install IIS on Different Windows Versions

This section provides step-by-step instructions on how to install Internet Information Services (IIS) on different Windows versions. Refer to the following sections for instructions:

- To install IIS on Windows Vista and above
- To install IIS on Windows Server 2008/2008 R2
- To install IIS on Windows Server 2012 and above

To install IIS on Windows Vista and above

1. Navigate to **Start** → **Control Panel** → **Programs** and click **Turn Windows features on or off** under **Programs and Features**.
2. In the **Windows Features** dialog, select **Internet Information Services**.
3. Expand the **Internet Information Services** node and enable the following features prior to the installation:
   - **IIS 6 Metabase Compatibility** under **IIS 6 Management Compatibility** → **Web Management Tools**
   - **ASP** and **ASP.NET** under **World Wide Web Services\Application Development Features**
   - **Windows Authentication** under **World Wide Web Services\Security**
   - **HTTP Redirection** under **Common HTTP Features**
4. After the installation has completed successfully, navigate to **Control Panel** → **System and Security** → **Administrative Tools** and double-click **Internet Information Services (IIS) Manager**.
5. In the left pane, select the server node and double-click **Authentication** under **IIS** in the right pane.
6. On the **Authentication** page, enable the following authentication types (right-click them and select **Enable**):
   - **Anonymous Authentication**
   - **Windows Authentication**

To install IIS on Windows Server 2008/2008 R2

1. Navigate to **Start** → **Administrative Tools** → **Server Manager**.
2. In the left pane, select the **Roles** node and click **Add Roles** in the right pane.
3. In the **Add Roles** wizard proceed to the **Server Roles** page and select **Web Server (IIS)**.
4. On the **Select Role Services** step, enable the following features:
   - **ASP** and **ASP.NET** under **Application Development** (click **Add Required Role Services** in the **Add Roles** wizard that appears)
   - **Windows Authentication** under **Security**
   - **IIS 6 Metabase Compatibility** under **IIS 6 Management Compatibility** → **Management Tools**
   - **HTTP Redirection** under **Common HTTP Features**
5. On the **Confirm Installation Selections** step, verify your choice and click **Install**.
6. After the installation has completed successfully, navigate to **Start** → **Control Panel** → **Administrative Tools** → **Internet Information Services (IIS) Manager**.
7. In the left pane, select the server node and double-click **Authentication** under **IIS** in the right pane.
8. On the **Authentication** page, enable the following authentication types (right-click them and select **Enable**):
   - **Anonymous Authentication**
   - **Windows Authentication**

To install IIS on Windows Server 2012 and above

1. Open **Server Manager**.
2. Under the **Manage** menu at the right, select **Add Roles and Features**.
3. In the **Add Roles and Features** wizard, navigate to the **Installation Type** tab and select **Role-based or feature-based installation**.
4. Select the server (localhost is selected by default).
5. Select the **Web Server (IIS)** checkbox and the following roles:
   - **ASP** and **ASP.NET 3.5** under **Application Development** (click **Add Features** in the **Add Roles and Features** dialog that appears)
   - **Windows Authentication** under **Security**
   - **IIS 6 Metabase Compatibility** under **IIS 6 Management Compatibility** → **Management Tools**
   - **HTTP Redirection** under **Common HTTP Features**

6. Proceed with the wizard. On the **Confirm installation selections** step, review your choices and click **Install**.
7. In the Server Manager dialog, select **Local Server** on the left.
8. In the main menu click **Tools** and select **Internet Information Services (IIS) Manager**.
9. In the **Internet Information Services (IIS) Manager** window, select the server node on the left and double-click **Authentication** under **IIS** in the right pane.
10. On the **Authentication** page, make sure that **Anonymous Authentication** is enabled. If it is disabled, right-click it and select **Enable**.