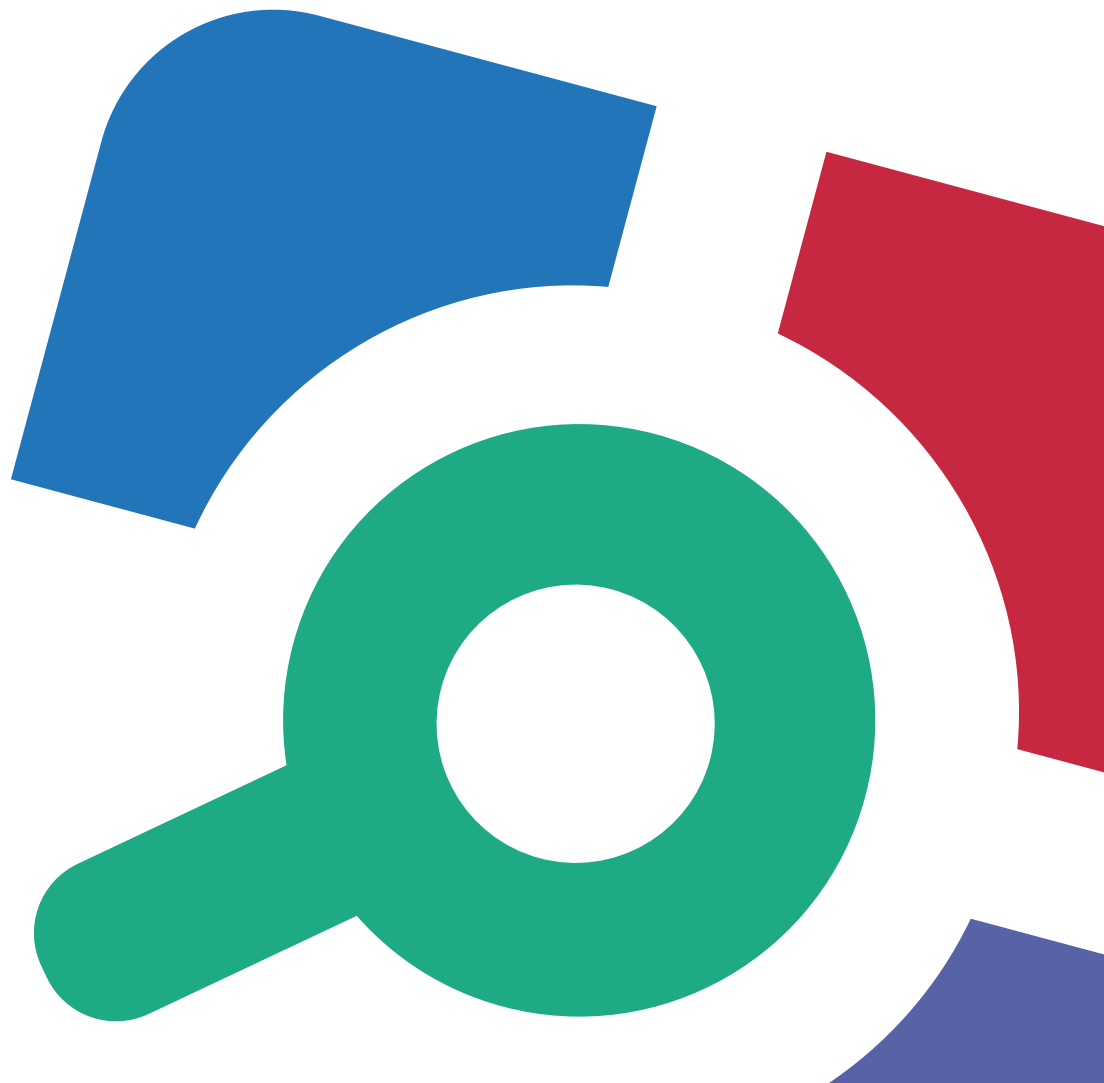


# Netwrix Identity Management Suite

## Features and Requirements

Version: 3.4  
5/30/2014



## **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.

© 2014 Netwrix Corporation.

All rights reserved.

# Table of Contents

1. Netwrix Identity Management Suite Overview .....	4
1.1. Netwrix Identity Management Suite Contents .....	4
1.2. Netwrix Identity Management Suite Overview .....	5
2. Netwrix Identity Management Suite System Requirements .....	7
2.1. Requirements to Managed Environment .....	7
2.2. Requirements to Netwrix Server .....	7
2.2.1. Hardware Requirements .....	7
2.2.2. Software Requirements .....	8
3. How to Install IIS on Different Windows Versions .....	9

# 1. Netwrix Identity Management Suite Overview

## 1.1. Netwrix Identity Management Suite Contents

Netwrix Identity Management Suite 3.4 comprises the following products:

- Netwrix Logon Reporter 2.0
- Netwrix Password Manager 6.5
- Netwrix Password Expiration Notifier 3.4
- Netwrix Inactive Users Tracker 3.3

## 1.2. Netwrix Identity Management Suite Overview

Netwrix Identity Management Suite comprises the solutions that help organizations solve their most pressing account management and password management issues. These solutions help automate and secure the following tasks:

- **Logon Auditing:** automatic consolidation, archiving and reporting on successful and failed logon events from all Active Directory domain controllers, servers and workstations.
- **Restore and reset forgotten passwords:** self-service password management eliminates a great number of help-desk calls and eases the implementation of password policies.
- **Notify remote users on password expiration:** remote (VPN, OWA), as well as Linux and MAC desktops users, who do not have password change prompts, can be notified automatically about expiring passwords by email.
- **De-provisioning of inactive accounts:** inactive user and computer accounts can be tracked and deactivated automatically based on their last logon time.

The table below explains the functionality of the products forming Netwrix Identity Management Suite:

Product	Description
Netwrix Logon Reporter	<p>The product automatically consolidates and archives all types of logon events from all Active Directory domain workstations and servers. It collects data from event logs from multiple computers across the network and stores it centrally in a compressed format, enabling convenient analysis and rich reporting capabilities.</p> <p>Product reports reflect successful and failed logons and logoffs for the following event types: interactive, network, batch, service, unlock, network clear text, new credentials, remote interactive, cached interactive, user initiated logoff, account password changes and resets, account lockouts and unlocks.</p>
Netwrix Password Manager	<p>This is a tool for automated password management. The product does the following:</p> <ul style="list-style-type: none"><li>• Provides end-users with self-service web access to common password management tasks.</li><li>• Allows help-desk operators to manage user accounts and view reports on their status through a simple web interface.</li><li>• 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.</li></ul>

Product	Description
Netwrix Password Expiration Notifier	<p>The product checks which domain account and/or passwords are to expire in the specified number of days, and sends notifications to users via email or text messages (SMS). It also generates summary reports that can be delivered to system administrators and the users' managers. The product also allows checking the effects of a password policy change before applying it to the managed domain.</p>
Netwrix Inactive Users Tracker	<p>This is a tool for automatic tracking of inactive user and computer accounts. The products performs the following tasks:</p> <ul style="list-style-type: none"><li>• Checks domains or specific organizational units by inquiring all domain controllers, and notifies managers and administrators about the accounts that have been inactive for the specified number of days.</li><li>• Automatically deactivates inactive accounts by setting a random password, disabling, deleting or moving them to a specified organizational unit.</li></ul>

## 2. Netwrix Identity Management Suite System Requirements

### 2.1. Requirements to Managed Environment

This section lists the requirements to the environment that is going to be managed with the Netwrix products forming Netwrix Identity Management Suite:

- Active Directory (domain and forest functional levels)
- Domain controller OS versions:
  - Windows Server 2000 SP4
  - Windows Server 2003 SP2
  - Windows Server 2003 R2 SP2
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1
  - Windows Server 2012
  - Windows Server 2012 R2

### 2.2. Requirements to Netwrix Server

This section provides the requirements to the computer where Netwrix Identity Management suite is going to be installed.

#### 2.2.1. Hardware Requirements

Before installing Netwrix Identity Management Suite 3.4, make sure that your system meets the following hardware requirements:

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

Hardware Component	Minimum	Recommended
Hard Disk	50 MB for each product	2 drives with 50 GB of free space in total

## 2.2.2. Software Requirements

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

Component	Requirements
Operating System	<ul style="list-style-type: none"><li>• Desktop OS: Windows 7 (32 and 64-bit) and above</li><li>• Server OS: Windows Server 2008 R2 and above</li></ul>
Framework	<ul style="list-style-type: none"><li>• <a href="#">.Net Framework 3.5 SP1</a></li></ul>
Additional software	<ul style="list-style-type: none"><li>• <a href="#">Windows Installer 3.1 or above</a></li><li>• IIS 6.0 or above*</li><li>• Microsoft Internet Explorer 6.0 or later/Mozilla FireFox 2.0 or later/Apple Safari 2.0 or later/Google Chrome 4.0 or later*</li></ul> <p>*Only required for Netwrix Password Manager Core Service and Web Application. Refer to <a href="#">How to Install IIS on Different Windows Versions</a> for detailed instructions on</p>



## 3. 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 7](#)
- [To install IIS on Windows Server 2008/2008 R2](#)
- [To install IIS on Windows Server 2012](#)

### *To install IIS on Windows 7*

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 Management Compatibility** under **Web Management Tools**
  - **ASP and ASP.NET** under **World Wide Web Services\Application Development Features**
  - **Windows Authentication** under **World Wide Web Services\Security**.
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 → Control Panel → Programs and Features**.
2. Double-click **Turn Windows features on or off**.
3. In the left pane, right-click **Roles** and select **Add Roles**.
4. In the **Add Roles** wizard proceed to the **Server Roles** page and select **Web Server (IIS)**.

5. 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 Management Compatibility** under **Management Tools**
6. On the **Confirm Installation Selections** step, verify your choice and click **Install**.
7. After the installation has completed successfully, navigate to **Start → Control Panel → Administrative Tools → Internet Information Services (IIS) Manager**.
8. In the left pane, select the server node and double-click **Authentication** under **IIS** in the right pane.
9. 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*

1. Open Server Manager.
2. Under the **Manage** menu, select **Add Roles and Features**.
3. Select **Role-based or feature-based installation**.
4. Select the server (localhost is selected by default).
5. Select the **Web Server (IIS)** check-box.
6. In the **Add Roles and Features** wizard, click **Add Features**.
7. Click **Next** on the **Select features** and the **Web Server Role (IIS)** steps.
8. On the **Select role services** step, select the following features:
  - **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 Management Compatibility** under **Management Tools**
9. On the **Confirm installation selections** step, review your choices and click **Install**.
10. In the Server Manager dialog, select **Local Server** on the left.
11. In the main menu click **Tools** and select **Internet Information Services (IIS) Manager**.
12. 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.

13. On the **Authencation** page, make sure that **Anonymous Authentication** is enabled. If it is disabled, right-click it and select **Enable**.