netwrix
#1 for configuration auditing

NETWRIX AUDITOR FOR PASSWORD EXPIRATION

QUICK-START GUIDE

Product Version: 5.0

December 2013

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 discussed. Netwrix Corporation assumes no responsibility or liability for the accuracy of the information presented, which is subject to change without notice.

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. Introduction

1.1. Overview

This guide is intended for the first-time users of Netwrix Auditor for Password Expiration. It is designed for evaluation purposes, therefore, it is recommended to read it sequentially, and follow the instructions in the order they are provided. After reading this guide you will be able to:

- Install and configure Netwrix Auditor for Password Expiration
- Create a Managed Object
- Get a notification about password/account expiration
- Receive a summary listing all passwords/accounts that are about to expire.

For evaluation purposes, this guide only covers basic configuration and usage options of the Password Expiration Alerting feature. For advanced configuration options and usage scenarios, refer to the corresponding documentation (see Appendix: Related Documentation for links).

1.2. How This Guide is Organized

This section explains how this guide is organized and provides a brief overview of each chapter.

- Chapter 1 Introduction is the current chapter. It explains the purpose of this document, defines its audience and explains its structure. This chapter also provides an overview of Netwrix Auditor for Password Expiration, lists its main features and benefits, and explains the product workflow.
- Chapter 2 Installing Netwrix Auditor for Password Expiration lists all hardware and software requirements for the Netwrix Auditor for Password Expiration installation and explains how to setup the product.
- Chapter 3 Configuring Managed Object explains how to configure a Managed Object that represents the audited AD domain.
- Chapter 4 Monitoring Audited Domain for Password Expiration explains how to run data collection and receive user notifications and administrator summary reports.
- A Appendix: Related Documentation contains a list of all documents published to support Netwrix Auditor for Active Directory.

1.3. Free Pre-Sales Support

You are eligible for free technical support during the evaluation period. If you encounter any problems, or would like assistance with the installation, configuration or implementation of Netwrix Auditor for Password Expiration, contact Netwrix support specialists.

1.4. Key Features and Benefits

Netwrix Auditor for Password Expiration checks which domain accounts and/or passwords are about to expire in the specified number of days, and sends notifications to non-interactive users, for example, who have Active Directory accounts only for VPN, Outlook Web Access and file shares and never log on interactively and do not receive the standard Windows notification.

It also generates summary reports that can be delivered to system administrators and/or users managers and allows checking the effects of a password policy change before applying it to the managed domain.

1.5. Product Workflow

A typical Netwrix Auditor for Password Expiration data collection and reporting workflow is as follows:

1. An administrator configures Managed Objects and sets the parameters for automated data collection and reporting on passwords and accounts expiry.
2. Netwrix Auditor for Password Expiration daily checks which accounts and passwords are about to reach their expiry threshold, and sends user notifications and/or summary reports to managers/administrators.

2. Installing Netwrix Auditor for Password Expiration

2.1. Installation Prerequisites

Netwrix Auditor for Password Expiration can be installed on any computer in the monitored domain.

2.1.1. Hardware Requirements

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

Table 1: Netwrix Auditor for Password Expiration Hardware Requirements

Hardware Component	Minimum	Recommended
Processor	Intel or AMD 32 bit, 2GHz	Intel Core 2 Duo 2x 64 bit, 2GHz
Memory	2GB RAM	8GB RAM
Disk space	250MB physical disk space for product installation.	Two physical drives with a total of 50GB free space

2.1.2. Software Requirements

This section lists the minimum software requirements for Netwrix Auditor for Password Expiration. Make sure that this software has been installed before proceeding with the installation.

Table 2: Netwrix Auditor for Password Expiration Software Requirements

Component	Requirement
Operating System	• Windows XP SP3 (both 32-bit and 64-bit systems) and above
Additional software	• .NET Framework 3.5 • Windows Installer 3.1 or above

2.1.3. Supported Environments

This section lists the requirements to the audited environment:

Table 3: Requirements to the Audited Environment

Feature	Supported Environments
Password Expiration Alerting	• Active Directory (all 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

2.2. Installing Netwrix Auditor for Password Expiration

Procedure 1. To install Netwrix Auditor for Password Expiration

1. Download Netwrix Auditor 5.0.

   Unpack the Netwrix_Auditor_Enterprise_Edition package.

2. Click the **Install** button.
3. Follow the instructions of the installation wizard. When prompted, accept the license agreement and specify the installation folder.
4. On the last step, click **Finish** to complete the installation.

Netwrix Auditor shortcuts will be added to the **Start** menu and the Netwrix Auditor console will open.

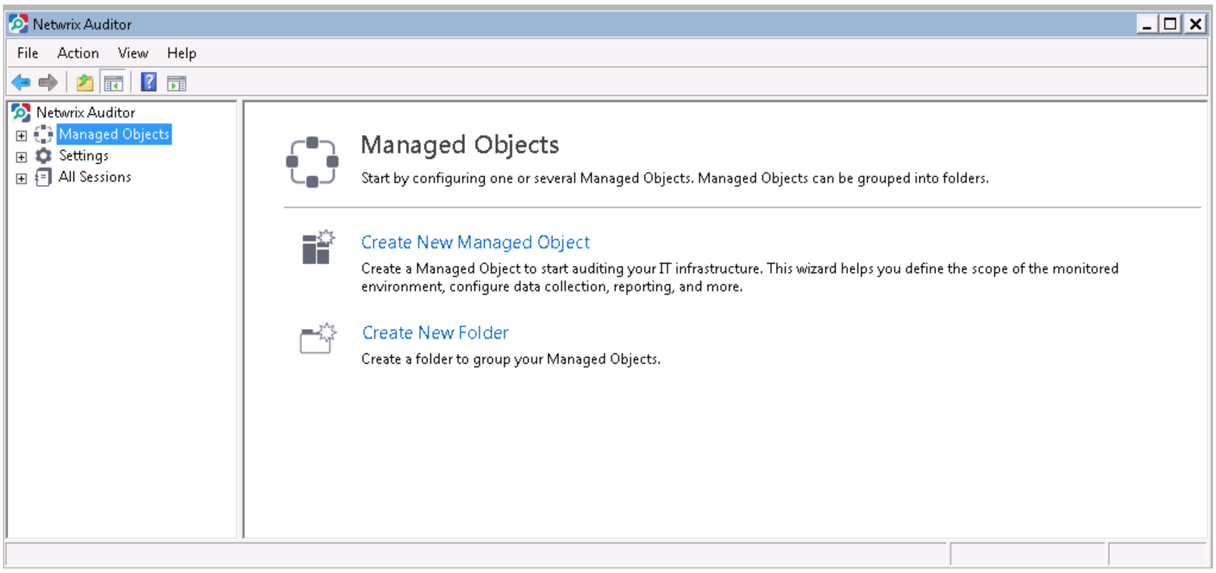
3. Configuring Managed Object

To start monitoring your Active Directory domain for expiring accounts and/or passwords, , you need to configure a Managed Object to define the scope of the monitored environment.

Procedure 2. To create and configure a Managed Object

1. In the Netwrix Auditor console, select the **Managed Objects** node in the left pane. The Managed Objects page will be displayed:

Figure 1: Managed Objects Page



Managed Objects

Start by configuring one or several Managed Objects. Managed Objects can be grouped into folders.

Create New Managed Object

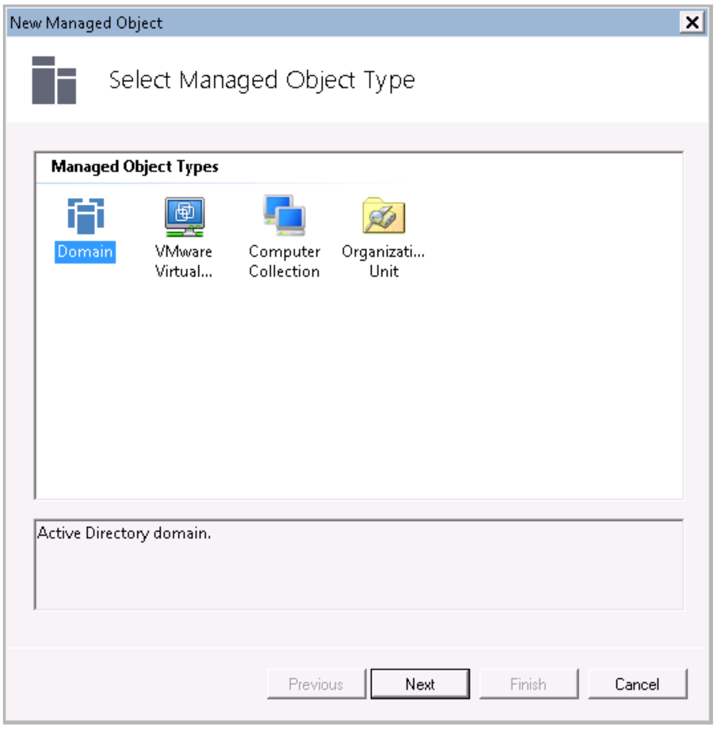
Create a Managed Object to start auditing your IT infrastructure. This wizard helps you define the scope of the monitored environment, configure data collection, reporting, and more.

Create New Folder

Create a folder to group your Managed Objects.

2. Click **Create New Managed Object** in the right pane. Alternatively, right-click the **Managed Objects** node and select **New Managed Object** from the popup menu to start the **New Managed Object** wizard.
3. On the **Select Managed Object Type** step, select **Domain** as the Managed Object type and click **Next**.

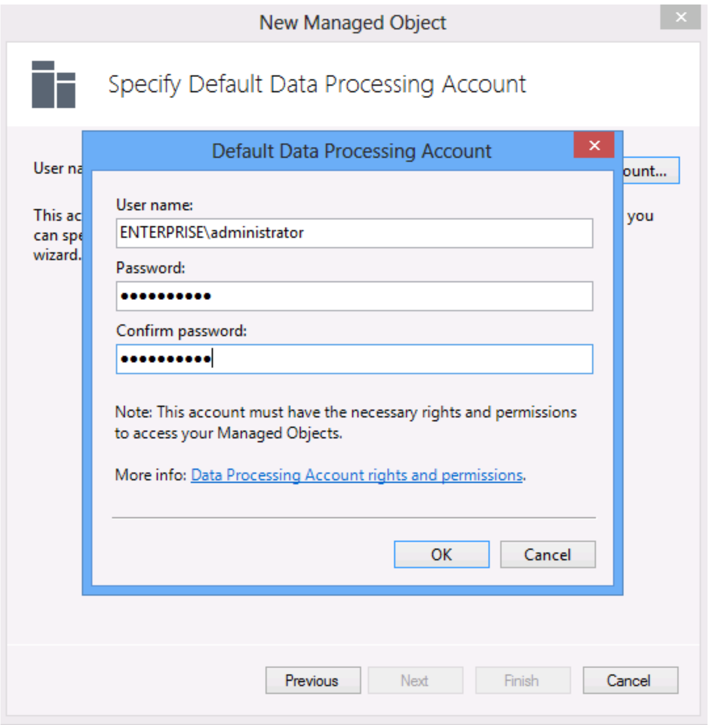
Figure 2: New Managed Object: Select Managed Object Type



Active Directory domain.

4. On the **Specify Default Data Processing Account** step, click the **Specify Account** button. In the dialog that opens, enter the default Data Processing Account credentials that will be used by Netwrix Auditor for data collection. The name should be specified in the following format: domain_name\account_name. For evaluation purposes, it is recommended to specify a domain admin account. For details on the rights and permissions required for this account, refer to the following KB article: Data Processing Account Rights and Permissions.

Figure 3: New Managed Object: Specify Default Data Processing Account



User name: ENTERPRISE\administrator

Password: ••••••••••

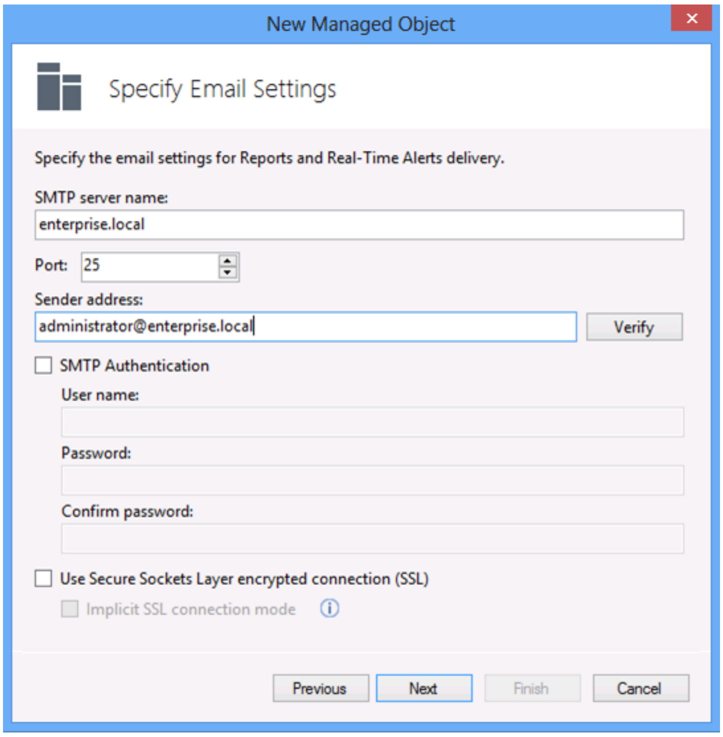
Confirm password: ••••••••••

Note: This account must have the necessary rights and permissions to access your Managed Objects.

More info: Data Processing Account rights and permissions.

5. On the **Specify Email Settings** step, specify the SMTP settings that will be used for Change Summary delivery:

Figure 4: New Managed Object: Specify Email Settings



New Managed Object

Specify Email Settings

Specify the email settings for Reports and Real-Time Alerts delivery.

SMTP server name: enterprise.local

Port: 25

Sender address: administrator@enterprise.local

□ SMTP Authentication

User name:

Password:

Confirm password:

□ Use Secure Sockets Layer encrypted connection (SSL)

□ Implicit SSL connection mode

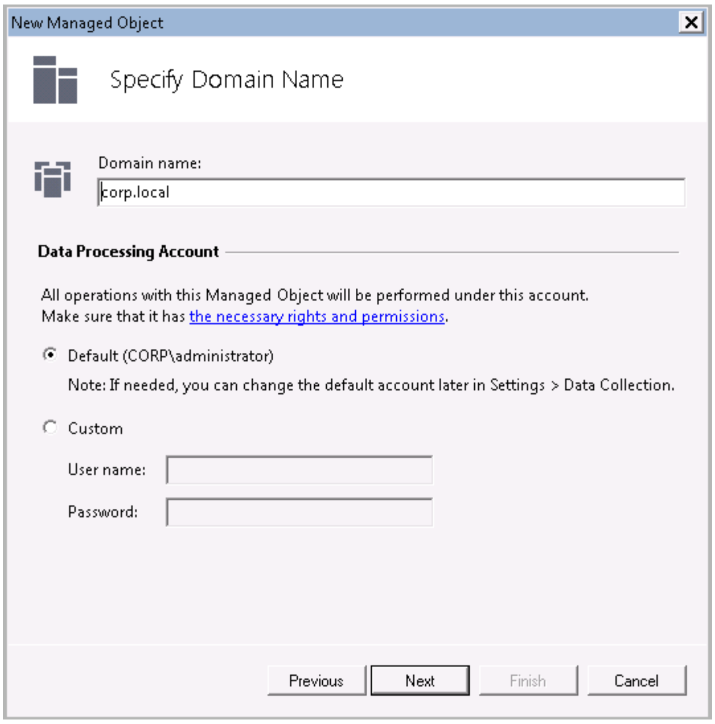
The following parameters must be specified:

Table 4: Email Settings Parameters

Parameter	Description
SMTP server name	Enter your SMTP server name.
Port	Specify your SMTP server port number.
Sender address	Enter the address that will appear in the "From" field in Reports and Change Summaries. To check the email address, click **Verify**. The system will send a test message to the specified address and will inform you if any problems are detected.
Use SMTP authentication	Select this check box if your mail server requires the SMTP authentication.
User name	Enter a user name for the SMTP authentication.
Password	Enter a password for the SMTP authentication.
Confirm password	Confirm the password.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
Use Implicit SSL connection mode	Select this checkbox if the implicit SSL mode is used, which means that an SSL connection is established before any meaningful data is sent.

6. On the **Specify Domain Name** step, specify your domain name in the FQDN format:

Figure 5: New Managed Object: Specify Domain Name



New Managed Object

Specify Domain Name

Domain name: corp.local

Data Processing Account

All operations with this Managed Object will be performed under this account.
Make sure that it has the necessary rights and permissions.

● Default (CORP\administrator)

Note: If needed, you can change the default account later in Settings > Data Collection.

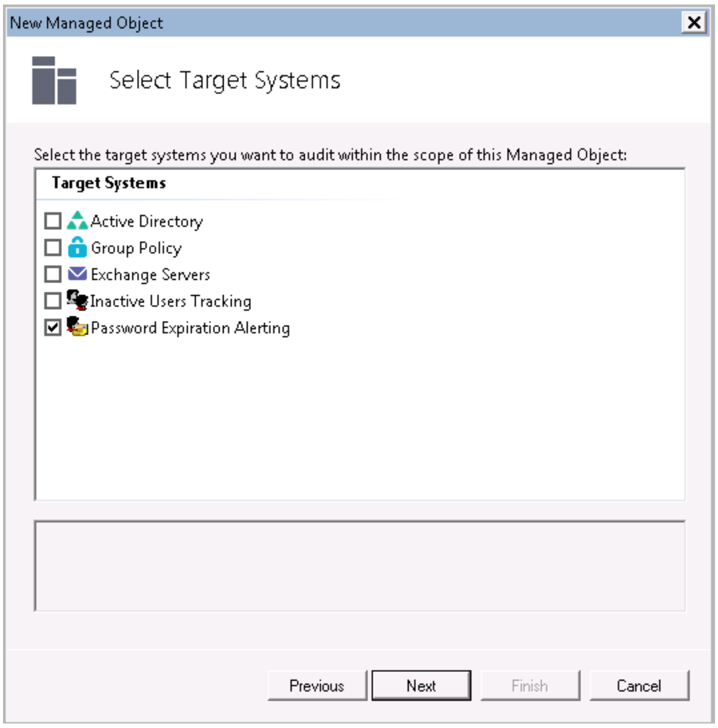
○ Custom

User name:

Password:

7. On the **Select Target Systems** step, make sure that Password Expiration Alerting is selected under **Target Systems**:

Figure 6: New Managed Object: Select Target Systems



New Managed Object

Select Target Systems

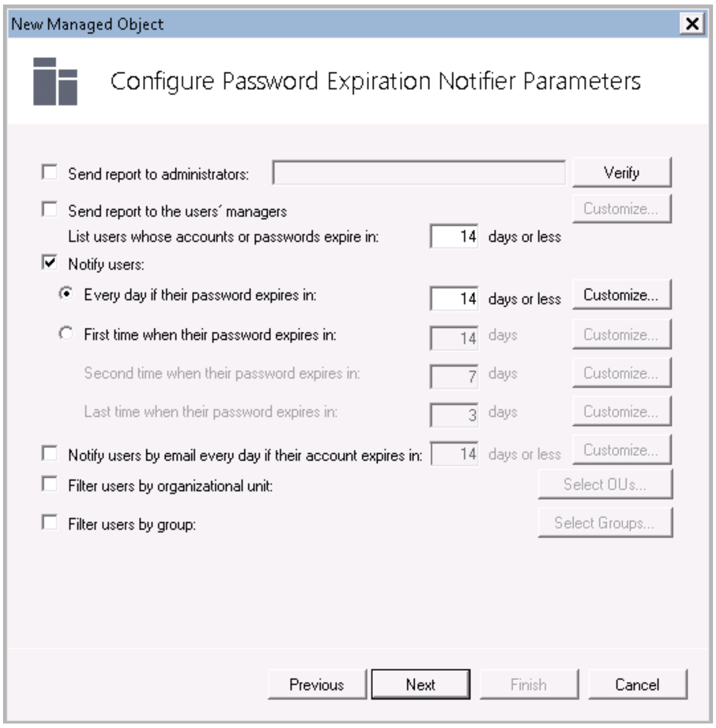
Select the target systems you want to audit within the scope of this Managed Object:

Target Systems

- □ Active Directory
- □ Group Policy
- □ Exchange Servers
- □ Inactive Users Tracking
- ☑ Password Expiration Alerting

8. On the **Configure Password Expiration Notifier Parameters** step, specify the reporting options:

Figure 7: New Managed Object: Configure Password Expiration Notifier Parameters



□ Send report to administrators:

□ Send report to the users' managers

List users whose accounts or passwords expire in: 14 days or less

☑ Notify users:

● Every day if their password expires in: 14 days or less

○ First time when their password expires in: 14 days

Second time when their password expires in: 7 days

Last time when their password expires in: 3 days

□ Notify users by email every day if their account expires in: 14 days or less

□ Filter users by organizational unit:

□ Filter users by group:

Table 5: Password Expiration Notifier Parameters

Parameter	Description
Send report to administrators	Select this option and specify your email address. A summary listing the users whose accounts/passwords are going to expire in the specified number of days will be delivered to this address. To check the email address, click **Verify**. The system will send a test message to the specified address and will inform you if any problems are detected.
Send report to the users' managers	Enable this option for reports to be delivered to the users' group managers. The managers are specified in the **Managed By** tab of the AD users group **Properties** dialog. **NOTE**: To edit the report template, click the **Customize** button.
List users whose accounts or passwords expire in <> days or less	Specify the expiration period for accounts and/or passwords to be included in the administrators and managers reports.
Notify users:	Select this option to notify users that their passwords and/or accounts are about to expire.
Every day if their password expires in <> days or less	Select this option for users to be notified daily that their passwords are going to expire, and specify the number of days before the expiration date. **NOTE:** To edit the report template, click the **Customize** button.
First time when their password expires in <> days	Select this option for users to be notified three times, and specify the number of days before the expiration date for each of three notifications. **NOTE**: To edit the report template, click the **Customize** button.
Notify users by email every day if their account expires in:	Select this option for users to be notified daily that their account is going to expire, and specify the number of days before the expiration date.

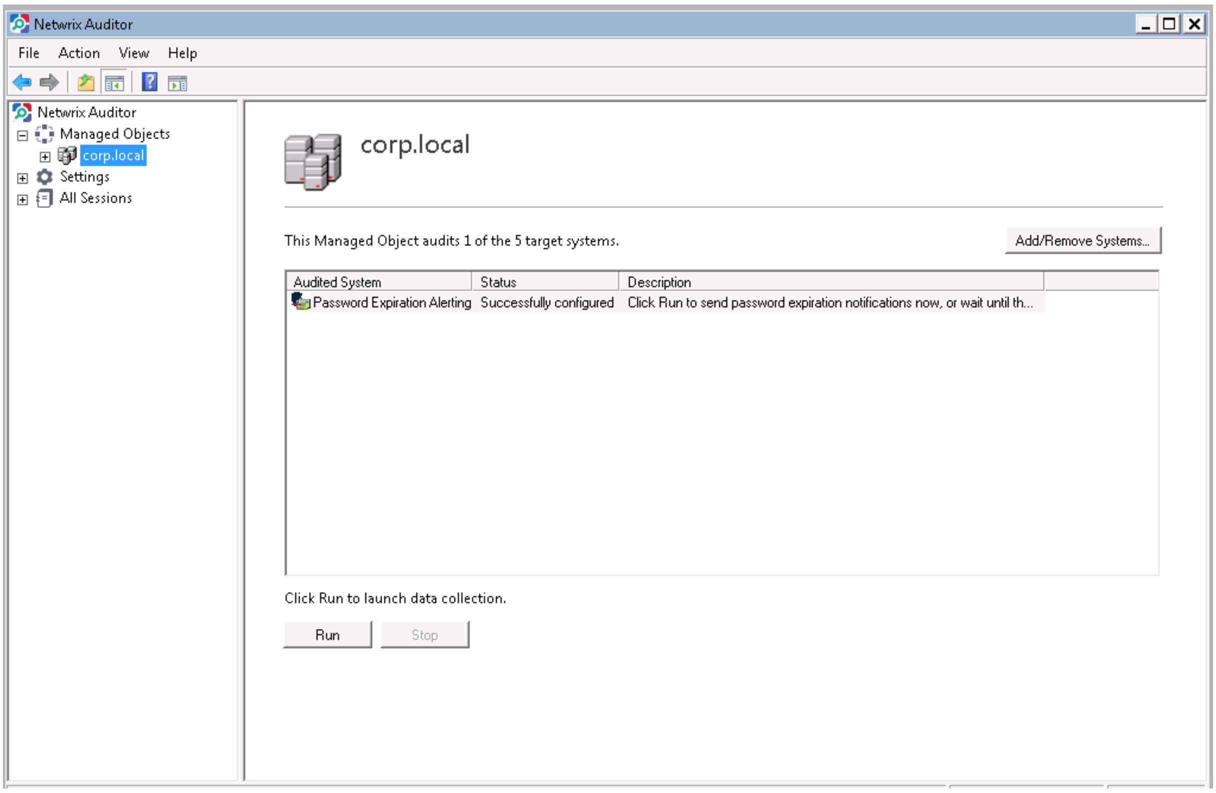
Filter users by organizational unit	To monitor users for expiring accounts/passwords that belong to certain organizational units within your Active Directory domain, select this option and click the **Select OUs** button. In the dialog that opens, specify the OUs that you want to monitor. Only users belonging to these OUs will be notified and included in the administrators and managers reports.
Filter users by group	To monitor users for expiring accounts/passwords that belong to certain groups within your Active Directory domain, select this option and click the **Select OUs** button. In the dialog that opens, specify the groups that you want to monitor. Only users belonging to these groups will be notified and included in the administrators and managers reports.

9. On the **Configure Real-Time Alerts** step, you can enable or disable predefined Real-

10. On the last step, review your Managed Object settings and click **Finish** to exit the wizard. A confirmation message will be displayed.

The newly created Managed Object will appear under the **Managed Objects** node, and its details will be displayed in the right pane:

Figure 8: Managed Object Page



This Managed Object audits 1 of the 5 target systems.

Audited System	Status	Description
Password Expiration Alerting	Successfully configured	Click Run to send password expiration notifications now, or wait until th...

Click Run to launch data collection.

4. MONITORING AUDITED DOMAIN FOR PASSWORD EXPIRATION

4.1. Running Data Collection

When you have added and configured a Managed Object, Netwrix Auditor for Password Expiration starts monitoring the audited domain for account/password expiration.

After you have configured a Managed Object, launch data collection manually to avoid waiting for a scheduled run.

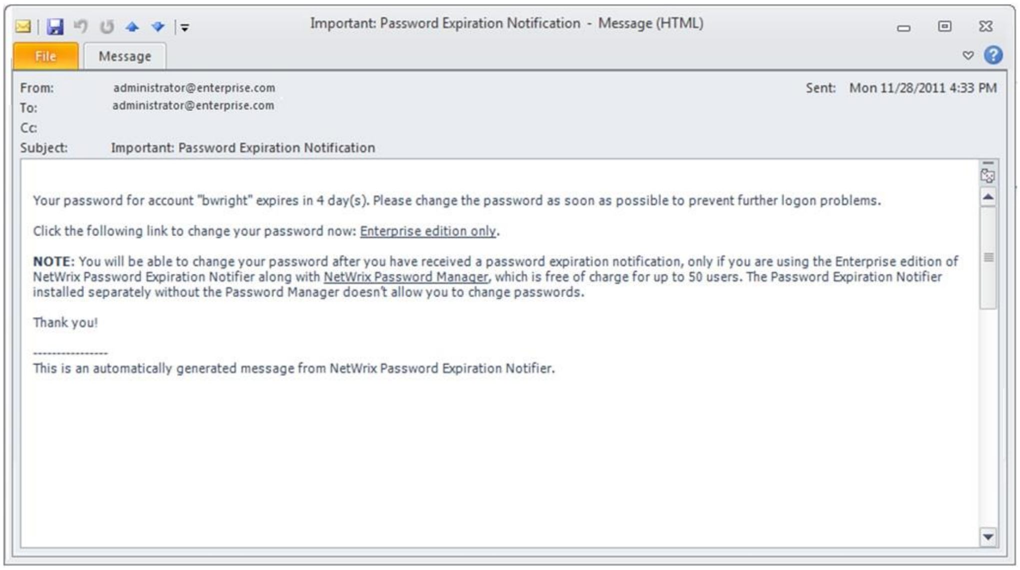
Procedure 3. To launch a data collection task

1. In the Netwrix Auditor console, expand the **Managed Objects** node, and select your Managed Object.
2. In the details pane, click **Run**.

4.2. Receiving Notifications and Reports

After each data collection, Netwrix Auditor for Password Expiration sends email notifications to the users whose passwords and/or accounts are about to expire. Below is an example of a user notification:

Figure 9: Notification Example



Important: Password Expiration Notification - Message (HTML)
File
Message

From: administrator@enterprise.com

To: administrator@enterprise.com

Cc:

Subject: Important: Password Expiration Notification

Sent: Mon 11/28/2011 4:33 PM

Your password for account "bwright" expires in 4 day(s). Please change the password as soon as possible to prevent further logon problems.

Click the following link to change your password now: Enterprise edition only.

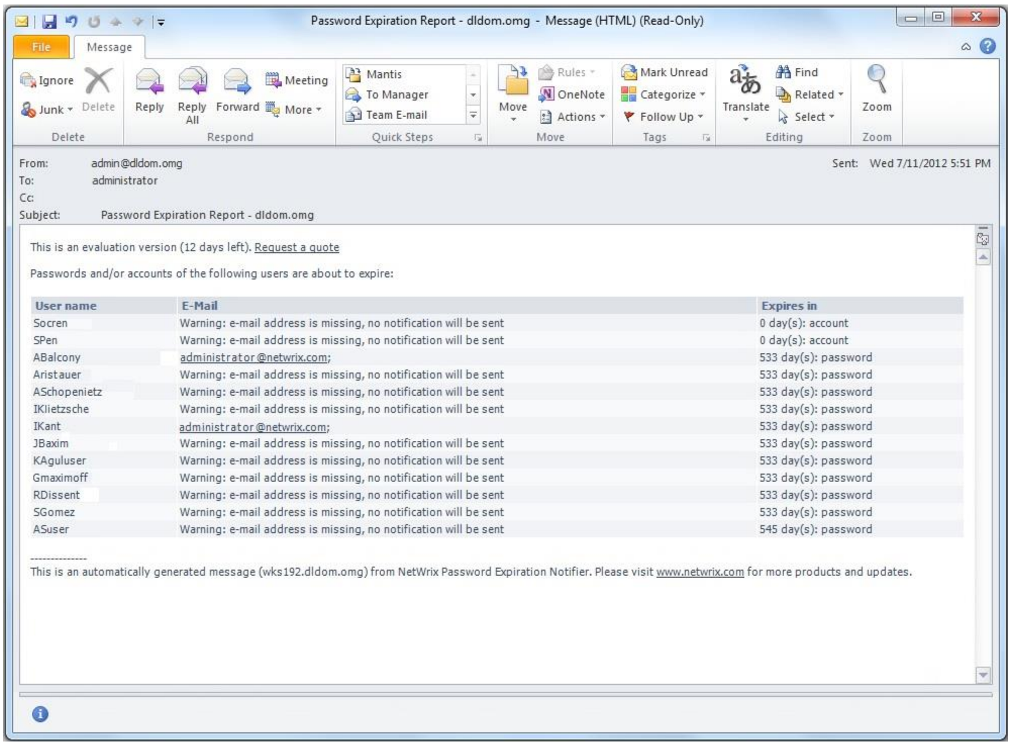
NOTE: You will be able to change your password after you have received a password expiration notification, only if you are using the Enterprise edition of NetWrix Password Expiration Notifier along with NetWrix Password Manager, which is free of charge for up to 50 users. The Password Expiration Notifier installed separately without the Password Manager doesn't allow you to change passwords.

Thank you!

This is an automatically generated message from NetWrix Password Expiration Notifier.

If you also select to send a summary report to administrators, it will be generated and delivered daily:

Figure 10: Summary Report



From: admin@dldom.omg
To: administrator
Cc:
Subject: Password Expiration Report - dldom.omg
Sent: Wed 7/11/2012 5:51 PM

This is an evaluation version (12 days left). Request a quote

Passwords and/or accounts of the following users are about to expire:

User name	E-Mail	Expires in
Socren	Warning: e-mail address is missing, no notification will be sent	0 day(s): account
SPen	Warning: e-mail address is missing, no notification will be sent	0 day(s): account
ABalcony	administrator@netwrix.com;	533 day(s): password
Aristauer	Warning: e-mail address is missing, no notification will be sent	533 day(s): password
ASchopenietz	Warning: e-mail address is missing, no notification will be sent	533 day(s): password
IKlietzsche	Warning: e-mail address is missing, no notification will be sent	533 day(s): password
IKant	administrator@netwrix.com;	533 day(s): password
JBaxim	Warning: e-mail address is missing, no notification will be sent	533 day(s): password
KAguluser	Warning: e-mail address is missing, no notification will be sent	533 day(s): password
Gmaximoff	Warning: e-mail address is missing, no notification will be sent	533 day(s): password
RDissent	Warning: e-mail address is missing, no notification will be sent	533 day(s): password
SGomez	Warning: e-mail address is missing, no notification will be sent	533 day(s): password
ASuser	Warning: e-mail address is missing, no notification will be sent	545 day(s): password

----
This is an automatically generated message (wks192.dldom.omg) from NetWrix Password Expiration Notifier. Please visit www.netwrix.com for more products and updates.

A APPENDIX: RELATED DOCUMENTATION

The table below lists all documents available to support Netwrix Auditor for Password Expiration:

Table 6: Product Documentation

Document Name	Overview
Netwrix Auditor for Password Expiration Installation and Configuration Guide	Provides detailed instructions on how to install and set up Netwrix Auditor for Password Expiration Active Directory.
Netwrix Auditor for Password Expiration Administrator's Guide	Provides a detailed explanation of the Netwrix Auditor: Active Directory features and step-by-step instructions on how to configure and use the product.