NETWRIX PASSWORD EXPIRATION NOTIFIER

QUICK-START GUIDE

Product Version: 3.3.247

March 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. INTRODUCTION

1.1. Overview

Netwrix Password Expiration Notifier is a tool for automatic detection of expiring accounts and passwords.

It monitors the managed domain and detects which domain accounts and passwords are to expire in a specified number of days, and sends notifications to users and reports to administrators and/or user managers.

1.2. Licensing

Netwrix Password Expiration Notifier is a freeware product with an unlimited license.

1.3. How It Works

The product data collection and reporting workflow is as follows:

1. An administrator sets the parameters for automated data collection.
2. A dedicated scheduled task which is launched daily checks the managed domain and collects data on expiring accounts and passwords.
3. The product sends notifications to users that their passwords are about to expire. It also generates summary reports on expiring accounts and passwords and delivers them to the specified recipients.

2. Install Netwrix Password Expiration Notifier

2.1. Installation Prerequisites

This section provides hardware and software requirements necessary to install Netwrix Password Expiration Notifier, and recommendations on how to deploy this product.

2.1.1. Deployment Options

Netwrix Password Expiration Notifier can be installed on any computer in the managed domain. If you want to monitor a different domain, you will need to specify an account that will collect data from that domain. This account must have the same rights and permissions as the account used to run the product scheduled task (for details, see Chapter 3 Configure Rights and Permissions)

2.1.2. Hardware Requirements

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

Table 1: Netwrix Password Expiration Notifier Hardware Requirements

Hardware Component	Minimum	Recommended
Processor	Intel or AMD 32 bit, 500MHz	Intel or AMD 64 bit, 3GHz Note: The Itanium (IA64) processor is not supported.
Memory*	512MB RAM	2GB RAM
Disk space	50MB	20GB

2.1.3. Software Requirements

Before installing Netwrix Password Expiration Notifier, make sure that your system meets the following software requirements:

Table 2: Netwrix Password Expiration Notifier Software Requirements

Component	Requirement
Operating System	Windows XP SP3 or above
Framework	.NET Framework 3.5
Additional Software	Windows Installer 3.1 or above

2.1.4. Supported Environments

Netwrix Password Expiration Notifier supports Active Directory domains (all domain and forest functional levels). The following domain controller OS versions are supported:

- Windows Server 2000 SP4
- Windows Server 2003 SP2
- Windows Server 2003 R2 SP2
- Windows Server 2008 SP2

- Windows Server 2008 R2 SP1

2.2. Install Netwrix Password Expiration Notifier

To install Netwrix Password Expiration Notifier, download and run the Netwrix_Password_Expiration_Notifier.msi file. Follow the instructions of the installation wizard. When prompted, accept the license agreement and specify the installation folder.

3. Configure Rights and Permissions

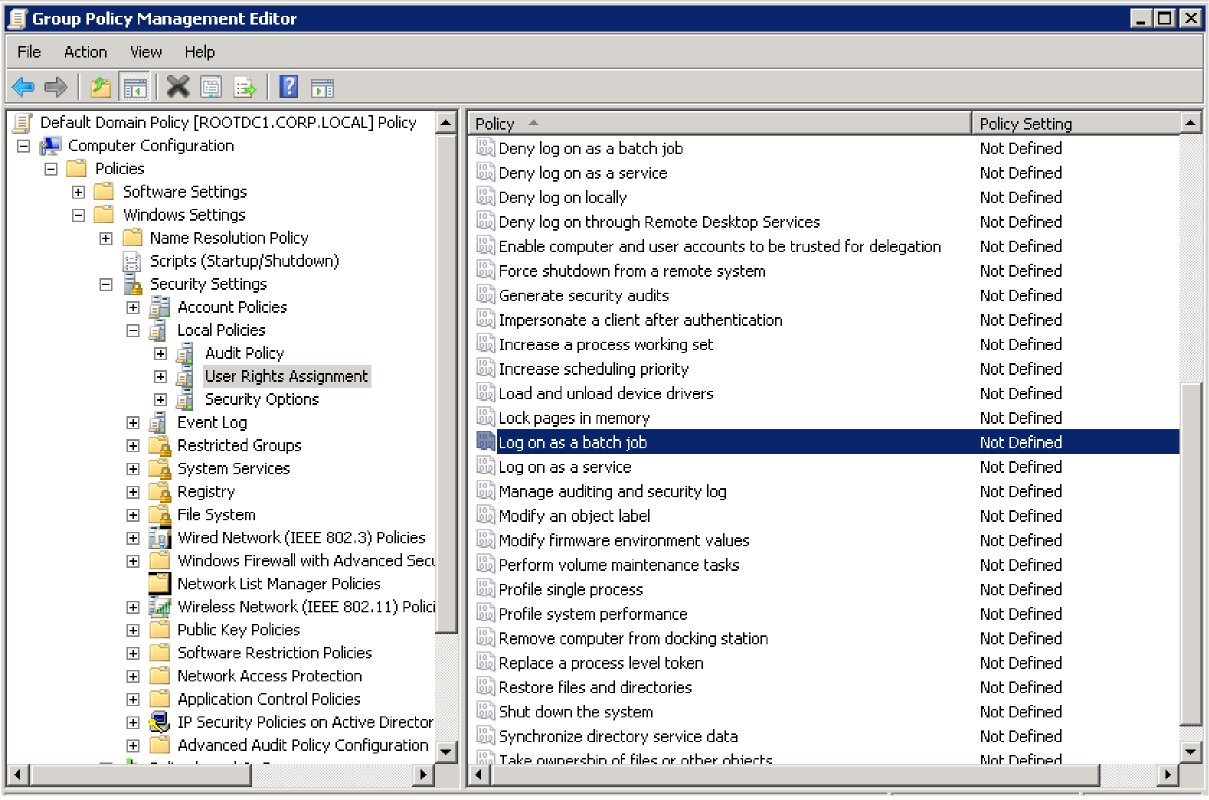
The account under which Netwrix Password Expiration Notifier collects data from the managed domain must have the following rights and permissions:

- The account must be a member of the **Domain Administrators** group.
- The **Log on as a batch job** policy must be defined for this account (see Procedure 1 To define the Log on as a batch job policy)

Procedure 1. To define the Log on as a batch job policy

1. Open the **Group Policy Management** console on any domain controller in the monitored domain: navigate to **Start** → **Administrative Tools** → **Group Policy Management**.
2. In the left pane, navigate to **Forest: <domain_name>** → **Domains** → **<domain_name>**, right-click **Default Domain Policy** and select **Edit** from the pop-up menu.
3. In the **Group Policy Management Editor** dialog, expand the **Computer Configuration** node on the left and navigate to **Policies** → **Windows Settings** → **Security Settings** → **Local Policies** → **User Rights Assignment** and locate the **Log on as a batch job** policy:

Figure 1: Group Policy Management Editor


Group Policy Management Editor
File
Action
View
Help
Default Domain Policy [ROOTDC1.CORP.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Wireless Network (IEEE 802.11) Polici
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Director
Advanced Audit Policy Configuration

Policy	Policy Setting
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined
Deny log on locally	Not Defined
Deny log on through Remote Desktop Services	Not Defined
Enable computer and user accounts to be trusted for delegation	Not Defined
Force shutdown from a remote system	Not Defined
Generate security audits	Not Defined
Impersonate a client after authentication	Not Defined
Increase a process working set	Not Defined
Increase scheduling priority	Not Defined
Load and unload device drivers	Not Defined
Lock pages in memory	Not Defined
Log on as a batch job	Not Defined
Log on as a service	Not Defined
Manage auditing and security log	Not Defined
Modify an object label	Not Defined
Modify firmware environment values	Not Defined
Perform volume maintenance tasks	Not Defined
Profile single process	Not Defined
Profile system performance	Not Defined
Remove computer from docking station	Not Defined
Replace a process level token	Not Defined
Restore files and directories	Not Defined
Shut down the system	Not Defined
Synchronize directory service data	Not Defined
Take ownership of files or other objects	Not Defined

4. Double-click this policy, select **Define these policy settings** and click **Add User or Group**. Specify the account that you want to define this policy for.
5. Navigate to **Start** → **Run** and type `cmd`. Input the gpupdate /force command and click **Enter** to update the group policy.

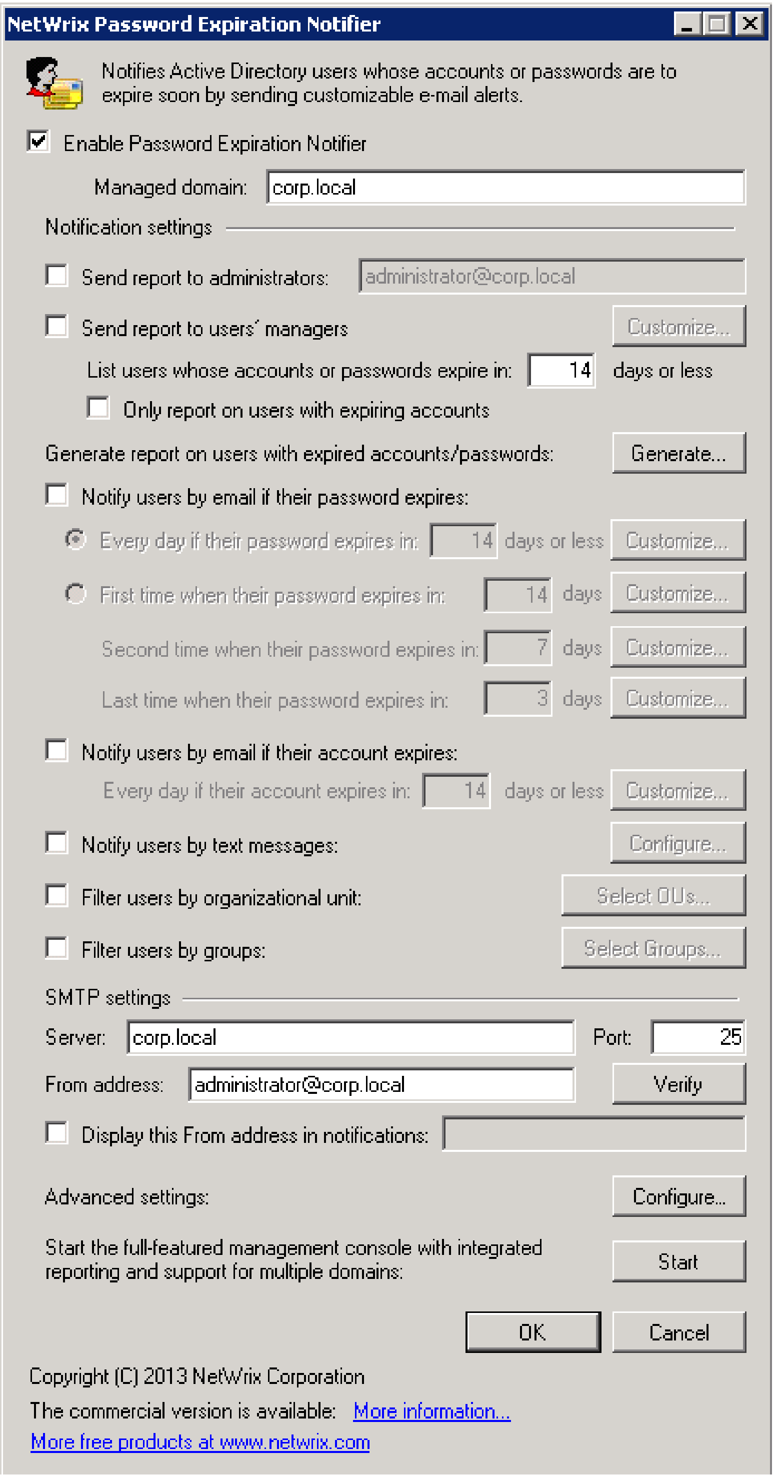
4. Configure Netwrix Password Expiration Notifier

After Netwrix Password Expiration Notifier has been installed, you need to configure the product settings.

Procedure 2. To Configure Password Expiration Notifier

1. Navigate to **Start → All Programs → Netwrix Freeware → Netwrix Password Expiration Notifier**. The product configuration dialog will open:

Figure 2: The Netwrix Password Expiration Notifier Configuration Dialog



NetWrix Password Expiration Notifier

Notifies Active Directory users whose accounts or passwords are to expire soon by sending customizable e-mail alerts.

☑ Enable Password Expiration Notifier

Managed domain: corp.local

Notification settings

□ Send report to administrators: administrator@corp.local

□ Send report to users´ managers [Customize...]

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

□ Only report on users with expiring accounts

Generate report on users with expired accounts/passwords: [Generate...]

□ Notify users by email if their password expires:

● Every day if their password expires in: 14 days or less [Customize...]

○ First time when their password expires in: 14 days [Customize...]

Second time when their password expires in: 7 days [Customize...]

Last time when their password expires in: 3 days [Customize...]

□ Notify users by email if their account expires:

Every day if their account expires in: 14 days or less [Customize...]

□ Notify users by text messages: [Configure...]

□ Filter users by organizational unit: [Select OUs...]

□ Filter users by groups: [Select Groups...]

SMTP settings

Server: corp.local Port: 25

From address: administrator@corp.local [Verify]

□ Display this From address in notifications:

Advanced settings: [Configure...]

Start the full-featured management console with integrated reporting and support for multiple domains: [Start]

[OK] [Cancel]

Copyright (C) 2013 NetWrix Corporation

The commercial version is available: More information...

More free products at www.netwrix.com

2. Specify the following settings and parameters:

Table 3: Netwrix Password Expiration Notifier Settings

Parameter	Instruction
Enable Password Expiration Notifier	Select this option to start monitoring your domain for expiring accounts and passwords.
Managed domain	Specify the managed domain name in the FQDN format.
Send report to administrators	Enable this option if, in addition, to user notifications you want the product to generate a summary report and deliver it to administrators. You can specify several email addresses separated by a semicolon.
Send report to users' managers	Enable this option if you want to deliver summary reports to the users' group managers. The managers are specified in the **Managed By** tab of the AD users group **Properties** dialog.
List users whose accounts or passwords expire in x days or less	Specify the expiration period for accounts and/or passwords to be included in the administrator and manager reports.
Only report on users with expiring accounts	Enable this option if you want to exclude the information on expiring passwords from administrator and manager reports.
Generate report on users with expired accounts/passwords	Click **Generate** to generate an on-demand report on accounts and passwords that are about to expire (for details, see Procedure 4 To generate an on-demand report).
Notify users by email if their password expires	Select this option to notify users that their passwords are about to expire.
Every day if their password expires in x days or less	Select this option to notify users daily that their passwords are going to expire, and specify the number of days before the expiration date.
First time when their password expires in x days	Select this option to notify users three times, and specify the number of days before the expiration date for each of the three notifications.
Second time when their password expires in x days	Specify the number of days before the expiration date when you want to notify users the second time.
Last time when their password expires in x days	Specify the number of days before the expiration date when you want to notify users the third time.
Notify users by email if their account expires	Select this option to notify users daily that their account are going to expire, and specify the number of days before the expiration date.
Every day if their account expires in x days or less	Select this option to notify users that their accounts are about to expire.
Server	Enter the SMTP server name.
Port	Specify the SMTP port number.
From address	Enter the email address that will appear in the "From" field in administrator and manager summary reports.
Display this From address in notifications	Enable this option if you want a different address to be displayed in the "From" field in user notifications, and specify this address.
Advanced settings	Click **Configure** to fine-tune the product settings (see below)
• Modify scheduled task start time	
• Include data on expiring	Select this option for the administrator and manager reports to contain the information not only on expiring

accounts in reports	passwords, but also on expiring accounts.
• Ignore users with “Change password at next logon” option enabled	Select this option to exclude users with the “Change password at next logon” option enabled from the administrator and manager reports.
• Ignore users with “Password never expires” option enabled	Select this option to exclude users with the “Password never expires” option enabled from the administrator and manager reports.
• Ignore users who do not have email accounts	Select this option to exclude users who have no email accounts from the administrator and manager reports.
• Ignore users whose passwords have already expired	Select this option to exclude users whose passwords have already expired from the administrator and manager reports.
• Filter by account name	Select this option to filter users included in the administrator and manager reports by their account names.
• Specify the account that will be used for data collection from the managed domain	If you are going to collect data from a different domain from the one where Netwrix Password Expiration Notifier is installed, select this option and specify the account that has access to user information in the managed domain. This account must have the same rights and permissions as the account used to run the product scheduled task (for details, see Chapter 3 Configure Rights and Permissions).
• User name	Enter the user name.
• Password	Enter the account password.
• Only report on users with Fine Grained Policy settings	Select this option to exclude all users from the administrator and manager reports except for the users with the Fine Grained Policy settings.

3. Save your configuration by clicking the **OK** button. The **Scheduled Task Credentials** dialog will be displayed.

4. Specify the account under which the product scheduled task will collect audit data. Make sure that this account has the necessary rights and permissions (see Chapter 3 Configure Rights and Permissions).

5. Enter and confirm the account password and click **OK**.

Note: To modify the product settings later, launch the product configuration dialog from the **Start** menu.

5. MONITOR YOUR DOMAIN FOR ACCOUNT/PASSWORD EXPIRATION

5.1. Data Collection

When the product has been configured, it starts collecting data on users whose accounts and passwords are about to expire. By default, the data collection task is launched daily at 3:00 AM. If required, you can launch the product scheduled task manually or modify its schedule.

Procedure 3. To launch the product scheduled task manually:

1. Launch **Task Scheduler**.
2. In the left pane, expand the **Task Scheduler Library** node. In the right pane, select the task called ***Netwrix Management Console - Password Expiration Notifier - <managed domain name>***.
3. Right-click the task and select **Run** from the drop-down list. Alternatively, use the **Run** option from the **Actions** menu.

Procedure 4. To generate an on-demand report

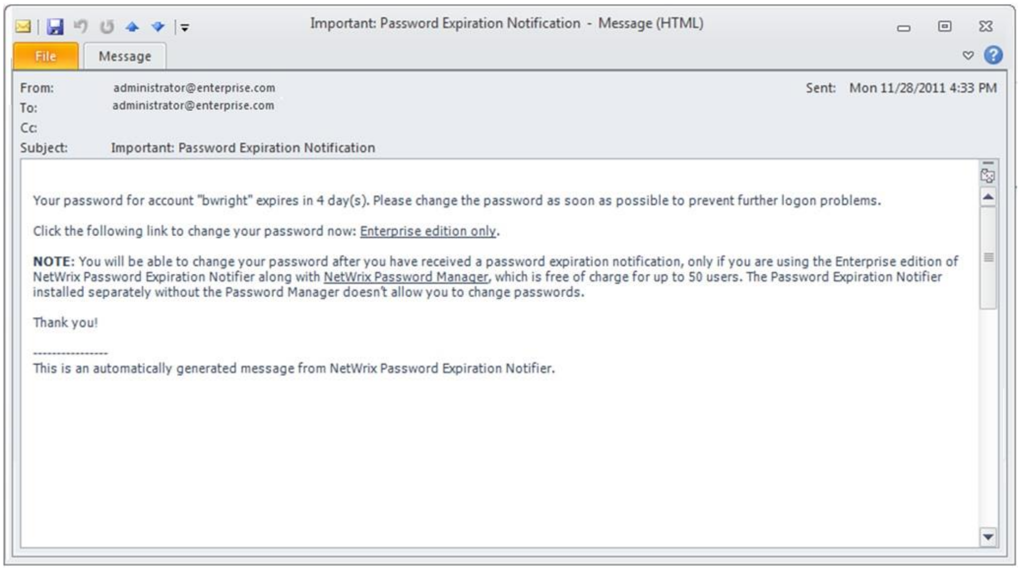
1. In the product configuration dialog, click **Configure** next to **Advanced settings**.
2. In the dialog that opens, click **Modify** next to **Modify scheduled task start time**.
3. Adjust the data collection schedule and click **OK** to save the changes.

5.2. Reports and Notifications

5.2.1. Notifications

After a data collection task has completed, a notification is sent to users whose accounts and/or passwords are about to expire:

Figure 3: 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.

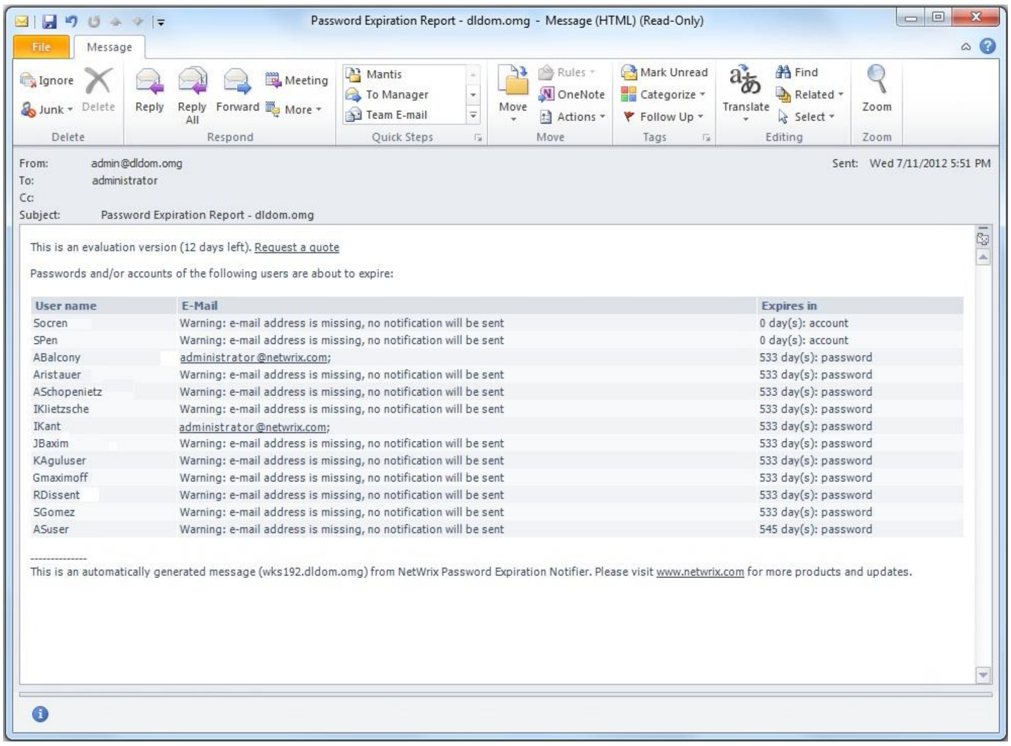
Thank you!

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

5.2.2. Reports

If you selected to send administrator and/or manager reports, reports will be generated and delivered to the specified recipients after each data collection task has completed:

Figure 4: On-Demand Report Example



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

----

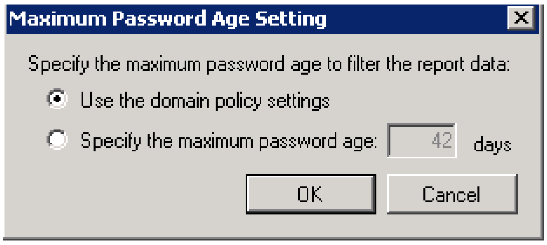
This is an automatically generated message (wks192.dldom.omg) from NetWrix Password Expiration Notifier. Please visit www.netwrix.com for more products and updates.

If you do not want to wait until a scheduled delivery, you can generate an on-demand report.

Procedure 5. To generate an on-demand report

1. In the product configuration dialog, click **Generate** next to **Generate report on users with expired accounts/passwords**.
2. The following dialog will be displayed allowing you to filter data:

Figure 5: Maximum Password Age Setting



Specify the maximum password age to filter the report data:

● Use the domain policy settings

○ Specify the maximum password age: 42 days

3. Select one of the following options:
   - **User the domain policy settings**: if this option is selected, the report will contain data on the users whose passwords and accounts are about to expire in accordance with the domain policy settings.
   - **Specify the maximum password age**: if this option is selected, the report will contain data on the users whose passwords and accounts are about to expire after the specified number of days.
4. Click **OK**. The report will be displayed in your default web browser.