



# NetWrix Password Expiration Notifier Quick Start Guide

Introduction.....	3
Licensing .....	3
Getting Started .....	4
System Requirements.....	4
Setup.....	5
Next Steps.....	7
Providing Access to Self-Service Password Management .....	7
Filtering Accounts .....	7
Editing Notification Templates .....	7
Running an On-Demand Report .....	8
Advanced Options .....	9
Contacting NetWrix Support .....	11

## Introduction

Password expiration is a frequent cause of many IT support issues. Passwords that are not changed before they expire can cause helpdesk calls from end users as well as productivity losses. Windows automatically notifies users of impending password expiration during interactive logon, but in some scenarios—for example, when users have AD accounts only for VPN, Outlook Web Access (OWA), and file shares—users never actually log on interactively and see this standard Windows notification.

The Password Expiration Notifier periodically checks all domain users to detect those whose passwords are about to expire in a specified number of days and then sends them friendly reminders. Armed with this tool, administrators can proactively resolve password expiration issues and implement strong password policies without additional drawbacks.

## Licensing

Password Expiration Notifier comes in two variants: freeware and commercial. The table below outlines the differences between them.

Feature	Freeware Version	Commercial Version
Scheduling	Yes	Yes
Account filtering	Only by account name	By organizational unit, groups, and account name
Administrator reports	Yes	Yes
Notification of end users	Yes	Yes
Customizable notification templates	No	Yes
On-demand administrator reports	Yes	Yes
Technical support	<a href="#">Support forum</a>	Phone, email
Licensing	Free of charge	Per managed AD domain or site license, please request a quote

The free version can be used by businesses and individuals for an **unlimited** time, at no charge. The commercial version can be evaluated free of charge for **20** days.

# Getting Started

Follow the instructions below to install and configure the Password Expiration Notifier.

## System Requirements

One of the following operating systems:

- ⑩ Windows XP (32-bit or 64-bit)
- ⑩ Windows Server 2003 (32-bit or 64-bit)
- ⑩ Windows Vista (32-bit or 64-bit)
- ⑩ Windows Server 2008 (32-bit or 64-bit)

Additional software:

- ⑩ .Net Framework 2.0 or later
- ⑩ Windows Installer 3.1 or later

You can install the program on any computer that is a member of the domain you want to manage, not necessarily a domain controller.

In Windows Server 2003 and Windows Server 2008 domains, all functional levels are supported. Fine-grained password policies of Windows Server 2008 are fully supported.

## Setup

To install the Password Expiration Notifier, run the setup program on the computer you have chosen (this can be any computer that belong the managed domain). On the last step of the installation wizard, the configuration dialog box opens:



Basic configuration steps:

- ⑩ Specify the name of the managed domain in the NetBIOS (for example, **acme**) or FQDN (for example, **example.com**) format. If you have several domains you may want to take a look at the Enterprise Edition of this product which is a part of the [NetWrix Enterprise Management Console](#) offering.
- ⑩ Enable administrator report, if necessary, and the report filter criteria (number of days before password expiration). For example, if you specify 10 days, all users whose passwords expire in 10 days or sooner will be reported to the administrator.
- ⑩ Select whether you want to notify the end users. You might want to turn this option after the administrator report is tested. You have two basic options: send password reminders every day starting with specific days (e.g. 14th day, 13<sup>th</sup> day, and so on until the password finally expires or changes), or just send 3 reminders on specified days (e.g. 14<sup>th</sup>, 7<sup>th</sup> and 3<sup>rd</sup> day before expiration).
- ⑩ SMTP server settings: name, port, from (sender) address.

When you have finished configuration, click **OK**. You will be prompted for the credentials to use for

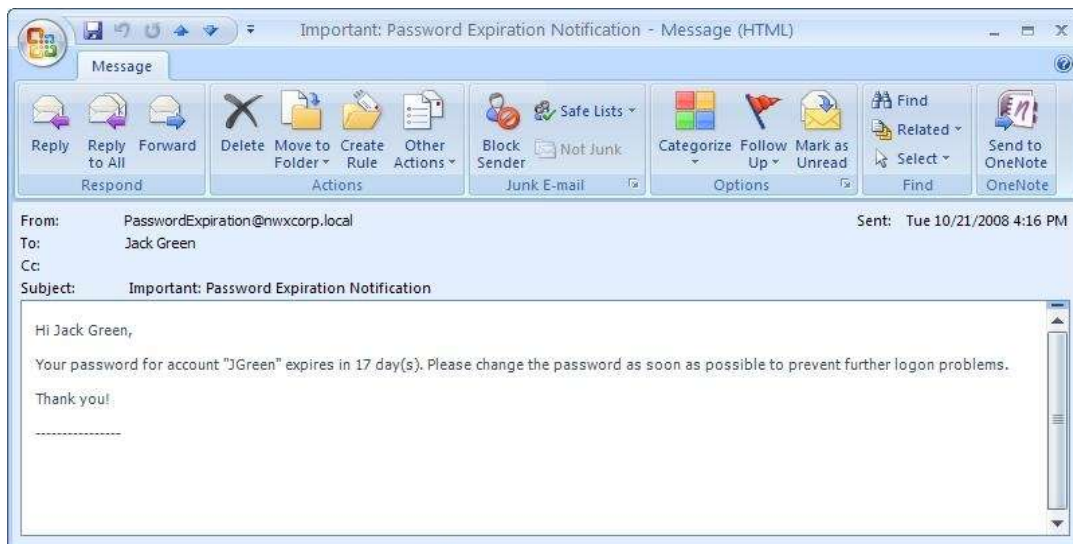
©2009 NetWrix Corporation. All rights reserved. NetWrix, Password Expiration Notifier, and Password Manager are trademarks of NetWrix Corporation and/or one or more of its subsidiaries, and may be registered in the U.S. Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are the property of their respective owners.

accessing Active Directory. Specify an account with sufficient privileges to read user account settings from Active Directory—for example, a member of the **Domain Admins** group, though it's recommended to run under a limited account with read access to the following attributes:

- ⑩ At the domain level: **maxPwdAge** attribute
- ⑩ For each user: **sAMAccountName**, **passwordAge** and **mail** attributes.

The account you specify will be used to run the scheduled task called **NetWrix Password Expiration Notifier** that performs the Active Directory search and sends notifications. The default schedule for this task is 3 AM daily, but you can change the schedule by clicking the **Schedule** button in the [Advanced Options](#) (see below). You can also run this scheduled task manually.

Now, if you have enabled both notification options, the result of this task will be a reminder for each user whose account is about to expire, as shown in the screenshot below, and a message to the administrator with a list of such accounts.



## Next Steps

This section tells you how to control the operation of the Password Expiration Notifier beyond the initial configuration.

## Providing Access to Self-Service Password Management

The password expiration notifications that the program sends to account owners can be more useful if they tell the addressees how to change their passwords. To make password self-service easy, we recommend using the [NetWrix Password Manager](#) or [NetWrix Web-based Password Change for AD](#).

If one these products are deployed in your environment, your notification templates should include a link to the password change URL. For example, for the [Password Manager](#) it would be [https://webservername/PM/change\\_password.asp](https://webservername/PM/change_password.asp).

## Filtering Accounts

You can fine-tune the scope of accounts that you want to watch: accounts with a specific pattern in their names or accounts from particular organizational units. For that, use the **Filter by organizational unit**, **Filter by group**, or **Filter by account name** options.

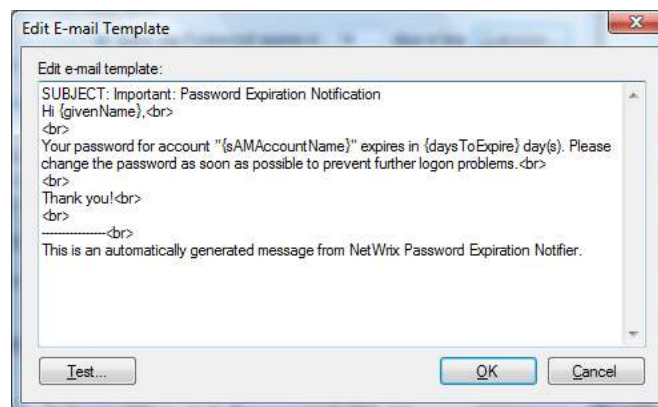
When you filter by organizational unit, clicking **Select OUs** prompts you for a list of OUs. Add the OUs you want to the list one by one in the **domain\_name/OU\_name** format (e. g. **example.com/Users**). Filtering by organizational unit is available only in the commercial version of the program.

When you filter by security group, clicking **Select Groups** prompts you for a list of groups. Pick one or more groups (security or distribution) and click **OK**. Note that filtering by group is available only in the commercial version of the program

Filtering by account names is useful for testing and described in the [Advanced Options](#) section below..

## Editing Notification Templates

You can edit templates for the notification e-mail messages sent to the end users. Click the **Customize** button next to the corresponding option:



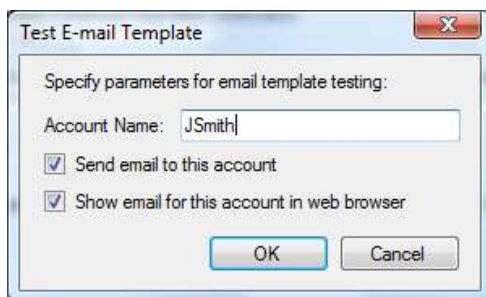
©2009 NetWrix Corporation. All rights reserved. NetWrix, Password Expiration Notifier, and Password Manager are trademarks of NetWrix Corporation and/or one or more of its subsidiaries, and may be registered in the U.S. Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are the property of their respective owners.

The template must include "SUBJECT:" section on the first line and the rest has HTML format and contains variables for which actual values are substituted when the messages are sent. Note that line breaks must be specified using the <br> tag. The following variables are supported:

- ⑩ Names of Active Directory attributes enclosed in brackets—for example, **{sAMAccountName}** or **{description}**
- ⑩ **{daysToExpire}**, an internal variable in Password Expiration Notifier defined by the program settings
- ⑩ References to the parent object attributes: **{parent!distinguishedName}**. Parent is usually an organizational unit.
- ⑩ Note that "SUBJECT:" section must be the first line in the template and cannot contain HTML tags.

Here is a sample snippet from the body of an account owner notification template: "Your password for account "{sAMAccountName}" expires in {daysToExpire} days."

You can quickly test your templates by clicking **Test** and specifying an account name to test on. Note that you need to specify a login name without domain name (e.g. JSmith, not ACME\JSmith):



Note that notification template editing is available only in the commercial version of the Password Expiration Notifier. Administrator reports can also be customized, please refer to [Advanced Options](#) section below.

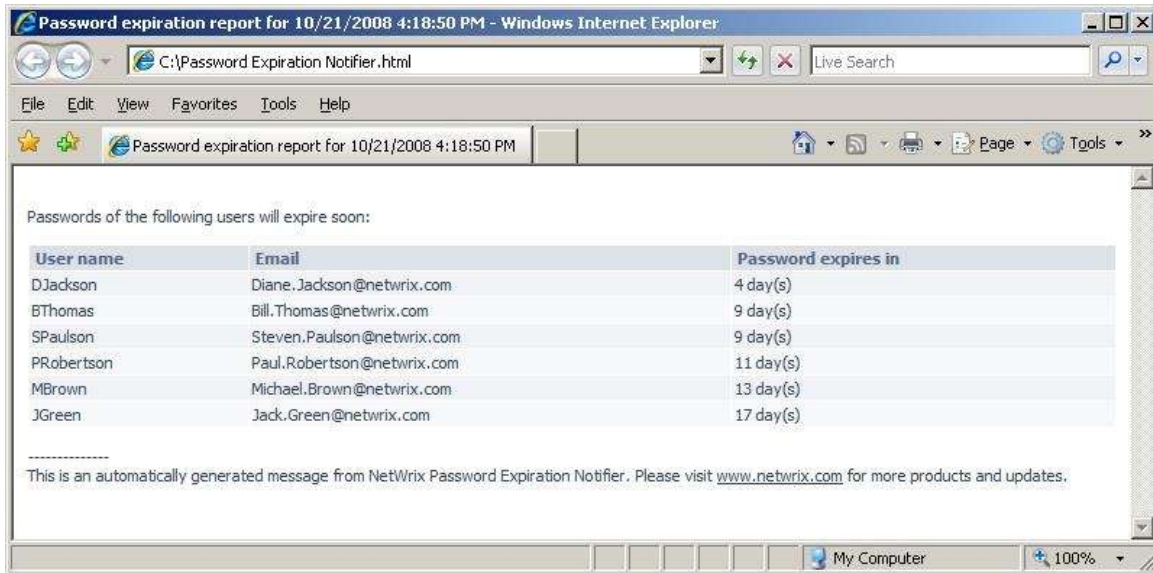
## Running an On-Demand Report

To get a report on whether any accounts have passwords that are about to expire, click **Generate** next to the administrator report settings. You will be prompted to use the current password policy from your domain or specify a custom value. Custom value can be useful if you don't have password expiration policy enabled in your domain yet and want to analyze the impact of turning it on:





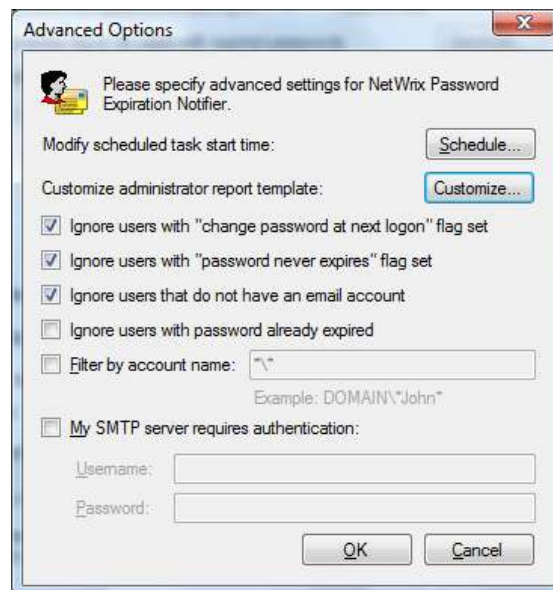
After selecting the password policy option you will be asked for report file name. The program will perform the check using selected settings and open the report file automatically:



Note that not notifications will be sent to end users when you generate on-demand reports.

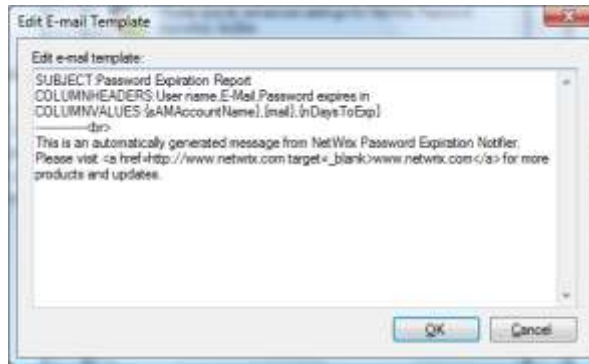
## Advanced Options

Advanced options are available by clicking **Advanced** on the main dialog box:



- **Schedule** button allows you to override the default schedule (3:00am).

- **Customize** button (not available in freeware) opens the template customization dialog box which is similar to notification templates for end users but has a bit different format: it requires additional COLUMNHEADERS and COLUMNVALUES sections to generate a table-like HTML report. COLUMNHEADERS section contains comma-separated list of column names and COLUMNVALUES refers to AD attributes of user accounts and parent OUs, similar to user templates:



Note that SUBJECT, COLUMNHEADERS, and COLUMNVALUES must be placed in the fixed order and cannot contain HTML tags; the rest of template has HTML format. Note that line breaks must be specified using the <br> tag.

- A set of **Ignore** options are self-explanatory and can be configured depending on your requirements.
- **Filter by account name** option is useful for testing and allows using wildcards (\*). For example, entering **svc\*** will match all accounts whose names start with “svc”.
- **SMTP server authentication** allows to specify login and password to send e-mails. This option is not available in the freeware version of the tool.

## Contacting NetWrix Support

If you have any questions please feel free to contact NetWrix support team at [www.netwrix.com/support](http://www.netwrix.com/support). NetWrix provides unlimited phone and e-mail support for commercial version (including evaluation) and limited free of charge support for freeware version on NetWrix Support Forum.