NETWRIX PASSWORD MANAGER
QUICK-START GUIDE

Product Version: 6.5

November 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 first-time users of Netwrix Password Manager. It contains an overview of the product functionality, instructions on how to install and setup the product, and explains how to start using Netwrix Password Manager by providing step-by-step procedures for some basic operations.

This guide can be used 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 Netwrix Password Manager
- Enroll into the system
- Reset a password (as an end-user and as a help desk operator)
- View reports on users' activities
- Configure password management options for end-users

Note: This guide only covers basic installation and configuration options. For full information, please refer to Netwrix Password Manager Administrator's Guide.

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: the current chapter. It explains the purpose of this document, defines its audience and explains its structure.
- Chapter 2 Product Overview provides an overview of the product features, and explains the system's architecture and deployment structure. It also contains information on licensing.
- Chapter 3 Installing Netwrix Password Manager provides detailed instructions on the installation of the Password Manager Service and Client applications.
- Chapter 4 Configuring Netwrix Password Manager contains an overview of the configuration options available through the Administrative Portal.
- Chapter 5 Enrolling into the System provides step-by-step instructions on different enrollment options.
- Chapter 6 Resetting a Password explains how to reset a password as an end-user and as a help-desk operator.
- Chapter 7 Viewing Reports explains how to generate and view reports on users' activities and enrollment events, and provides report examples.
- Appendix: lists all documentation published to support Netwrix Password Manager.

1.3. Free Pre-Sales Support

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

2. PRODUCT OVERVIEW

2.1. Key Features and Benefits

In an Active Directory environment, administration of user passwords includes multiple tasks, such as enforcing password security requirements through Group Policy, help-desk activities, and batch configuration of user account management options. Often, these operations are decentralized, and account owners are left out of account management.

Netwrix Password Manager is a solution that helps reduce help-desk and administration workload by achieving the following goals:

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

Netwrix Password Manager is a role-based application that allows its users to have the certain level of permissions. The following three roles are distinguished:

- End-users
- Help-desk operators
- Administrators

By assigning these roles to groups and single users, you can control who can perform which password management operations.

2.2. Product Architecture

Netwrix Password Manager consists of the following three components:

- **Web Application**: supports the web portals that provide the Password Manager functionality:
  - Administrative Portal: allows configuring password policies and user options, importing user account data for batch enrollment, etc.
  - Help-Desk Portal: allows centralized management and reporting on the enrolled users' accounts.
  - Self-Service Portal: a web-interface for end users to perform password management operations without contacting the help-desk.
- **Password Manager Service**: executes the operations requested through the web portals.
- **Password Manager Client** (also referred to as Windows Logon Prompt Extension*): extends the standard Windows logon prompt and pops up a dialog box that allows end-users to perform self-service password management operations. It also supports the enrollment wizard.

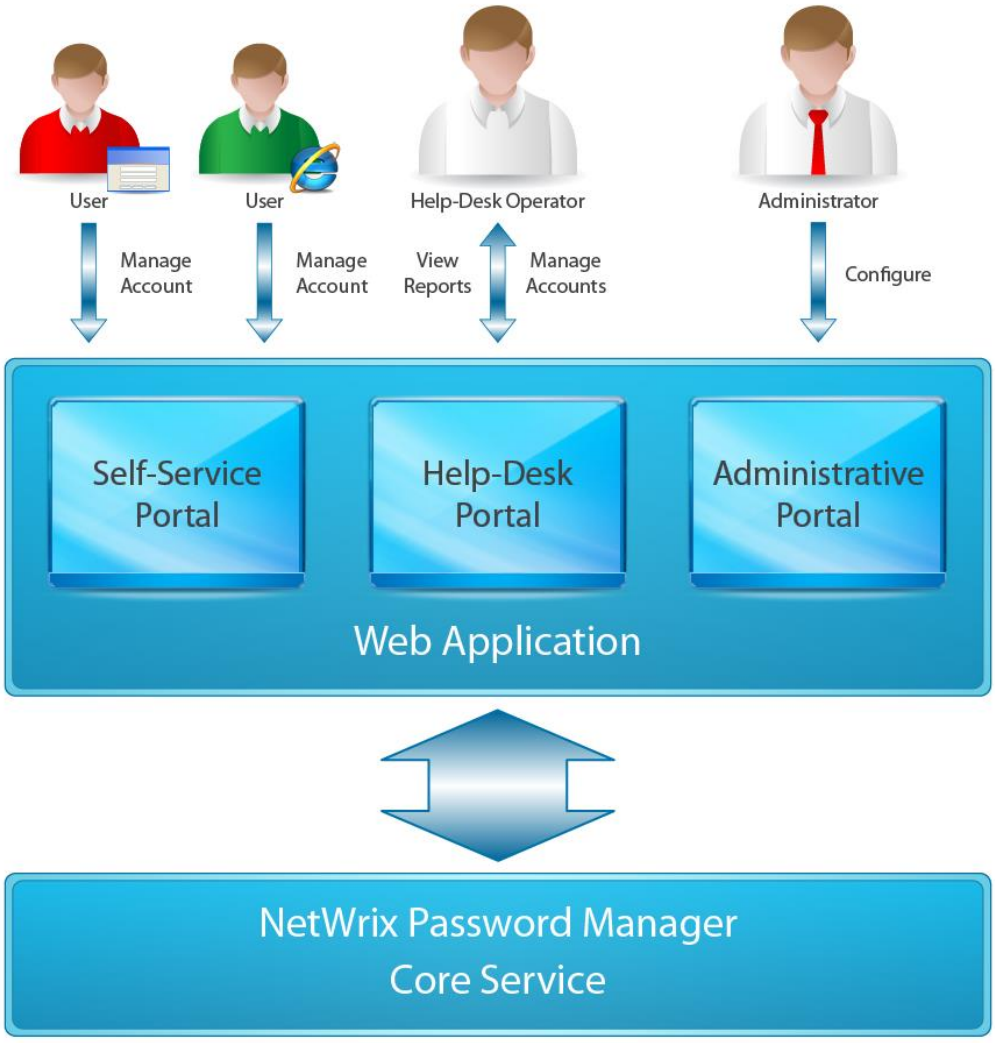
* *It is referred to as 'GINA extension' on pre Windows Vista systems and as 'Credentials Provider' on Windows Vista and Windows Server 2008 or above.*

Both Password Manager Client and the web clients connect to the web service via the HTTP or

HTTPS protocol. The web service, in turn, connects to Password Manager Service via the RPC protocol. Password Manager Service holds a secure profile database in the local file system, and communicates with Active Directory via encrypted LDAP and RPC channels.

The figure below illustrates Password Manager architecture and workflows:

Figure 1: Password Manager Architecture



2.3. Deployment Structure

Netwrix Password Manager components are typically distributed as follows:

I. Password Manager Service runs on a member server in an Active Directory domain.

Note: Installation of the Service on domain controllers is possible but not recommended.

II. The Web Application is installed on the same computer as the Service.

Note: If you want to install the Web Application in a Error! Reference source not ound., so that the web portals are accesible from anywhere in the Internet, you may want to install the Core Password Manager Service on a different machine behind your firewall as a more secure configuration option. For information on this installation scenario and detailed instructions, please refer to Section 4.4 of Netwrix Password Manager Administrator's Guide.

III. The Password Manager Client is installed on end-users' computers (this component is optional).

Note: The Password Manager Client and the Self-Service Portal are identical in terms of the functions they provide. Depending on your policies, you can choose not to deploy the Password Manager Client, and not sacrifice any functionality; or you can deploy it to give end-users more self-service access options.

2.4. Licensing Information

The product is licensed for a free 20-days evaluation period.

The product can be sued as freeware when limited to managing 50 or less users. Otherwise a commercial license is required. For license types and pricing information, please refer to Netwrix Password Manager web page.

3. INSTALLING NETWRIX PASSWORD MANAGER

This chapter guides you through the installation process of Password Manager Service application and Password Manager Client.

3.1. Installation Prerequisites

3.1.1. Hardware Requirements

Before installing Netwrix Password Manager, make sure that that the machine where the Core Service and the Web Application are going to be installed meets the following hardware requirements:

- Minimum 20 Mbytes of free hard disk space
- Minimum 512 Mbytes of RAM

3.1.2. Software Requirements

Table 1 Password Manager Software Requirements below lists the minimum software requirements for Netwrix Password Manager components. Make sure that this software has been installed on the corresponding machines before proceeding with the installation.

Table 1: Password Manager Software Requirements

Product Component	Required Software
Core Service and Web Application	Platform: Intel x86, AMD 32 or 64 bit
	OS: Windows XP Service Pack 3 or above .Net Framework 3.5 Service Pack 1
	Error! Reference source not found. 6.0 or above (Web erver role for Windows Server 2008) The following features must be enabled prior to the installation: • IIS 6 Management Compatibility • ASP extension • Windows Integrated Authentication • Anonymous Authentication • ASP.NET
Web client	Web browsers: Microsoft Internet Explorer 6.0 or above / Mozilla FireFox 2.0 or above / Apple Safari 2.0 or above / Google Chrome 4.0 or above
Password Manager Client	OS: Windows XP SP3 or above
	Web browser: Microsoft Internet Explorer 6.0 or above

3.2. Installing Password Manager Service and Web Application

Procedure 1. To install Password Manager Core Service and Web Application

1. Run prm_setup.exe on a member server or a workstation.

2. Accept the default settings and specify the service account in the **DOMAIN\user** format. The service account must have the appropriate access rights to your domain accounts to be able to reset passwords and unlock accounts.
3. Follow the instructions of the wizard to complete the installation.

After the installation is complete, the Administrative Portal will be started in the default web browser.

For security considerations, it is recommended to enable the HTTPS protocol for the Web Server on the machine where the Password Manager Core Service is installed. For details on how to enable encryption for IIS, please refer to the following documentation:

- How to implement SSL in IIS
- How to Set Up SSL on IIS 7

For the advanced installation scenario (i.e. installing on an Internet-facing DMZ server), please refer to Netwrix Password Manager Administrator's Guide.

3.3. Installing the Password Manager Client

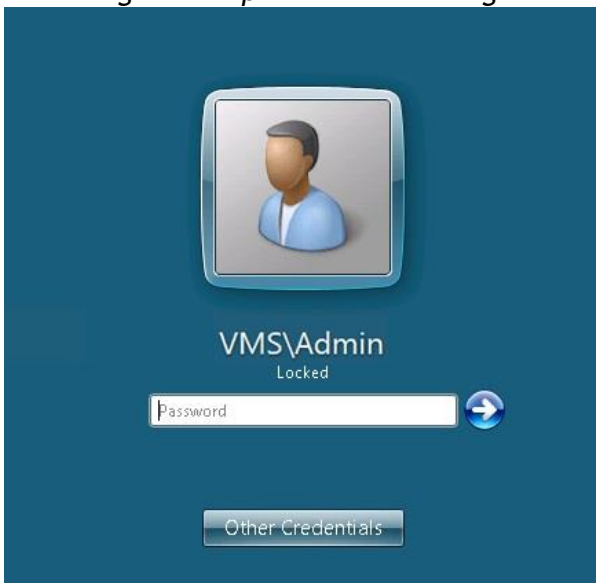
The Password Manager Client can be installed in several ways. This guide only covers a simple manual installation. For more installation options, please refer to Netwrix Password Manager Administrator's Guide.

Procedure 2. To install the Password Manager client manually

1. Run the prm_client.msi installation package (located in Password Manager installation folder) on all computers where you want to deploy the Password Manager Client (Logon Prompt Extension). The installation wizard will start.
2. When prompted, specify the installation path and the path to the Self-Service Portal.
3. Follow the instructions of the wizard to complete the installation.

Figure 2: and Figure 4: below show the logon dialog for Windows 7 and Windows XP with the Logon Prompt Extension that will now be displayed each time you log into the system:

Figure 2: Logon Prompt Extension Dialog in Windows 7



Note: If you cannot log on the system, click the **Other Credentials** button, and then select the **Can't log on? Click HERE for assistance** icon:

Figure 3: The logon assistance icon

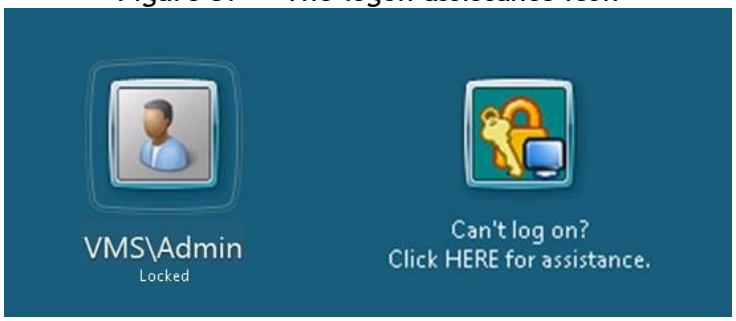


Figure 4: Logon Prompt Extension Dialog in Windows XP/2000

Now, to perform password management operations via the Logon Prompt Extension, you can click on the **Can't log on? Click here for assistance** link or the **Logon Assistance** button (depending on your Windows version).

4. Configuring Netwrix Password Manager Settings

Netwrix Password Manager is installed with the default configuration options (such as the domain name, password security settings, options available to end-users, verification questions policies, etc.). However, you can always modify the default configuration settings when needed through the Administrative Portal.

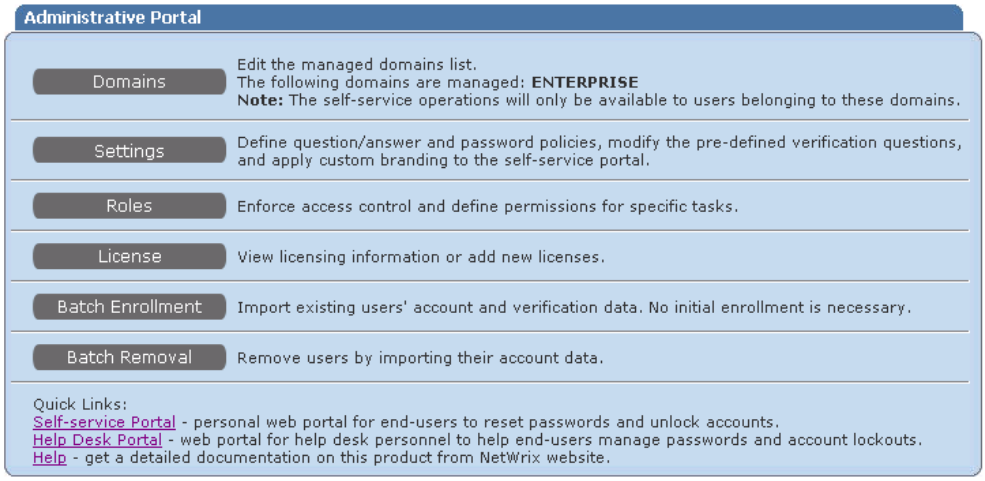
This chapter provides an overview of the configuration options available through the Administrative Portal. For detailed step-by-step instructions on each configuration setting, please refer to Netwrix Password Manager Administrator's Guide.

Note: You do not have to perform any additional configuration to execute the procedures explained in the chapters below in this guide. To try and test the product, the default configuration settings are sufficient.

4.1. Accessing the Administrative Portal

To access the Administrative Portal, go to **Start** > **All Programs** > **Netwrix** > **Password Manager** > **Administrative Portal** on the machine where the Password Manager Core Service is installed. The Administrative Portal web application will open in the default web browser:

Figure 5: Administrative Portal Main Page



Note: If the web page cannot be displayed due to authentication problems, add the Password Manager site to the Local Intranet zone. To do this, go to **Start** > **Control Panel** > **Internet Options**. In the **Internet Properties** dialog box select the **Security** tab. Click on **Local Intranet**, press the **Sites** button and add the Administrative Portal URL to the list.

4.2. Configuration Options Overview

The Administrative Portal supports the following configuration options:

- **Domains:** allows adding, removing or modifying domains in the managed domains list.
- **Settings:** allows configuring the Self-Service Portal. Administrators can define settings for the following:
  - Branding (company name and logo, support contacts, and others);
  - User Options (password management options available to end users);
  - Predefined Questions used for verification;

  - Questions Policy (question and answer length, the minimum number of questions required for verification, and so on);
  - Password Policy (password length);
  - Alerts (alert triggers and alert recipients);
  - Product updates
- **Roles:** allows assigning different roles to users (Administrators / Help-Desk Operators / Self-Service Access)
- **License:** allows managing product licenses.
- **Batch Enrollment:** allows administrators to enroll users by importing their account information from a file.
- **Batch Removal:** allows administrators to remove users in a batch by importing their account information from a file.

For step-by-step procedures on how to configure these settings, please refer to Netwrix Password Manager Administrator's Guide.

5. ENROLLING INTO THE SYSTEM

Once you have installed Netwrix Password Manager, you can test the product functionality.

Before users can perform any self-service password management operations, they must complete a procedure referred to as enrollment. This involves selecting the verification questions and answering them as an identity verification mechanism.

Netwrix Password Manager supports the following enrollment options:

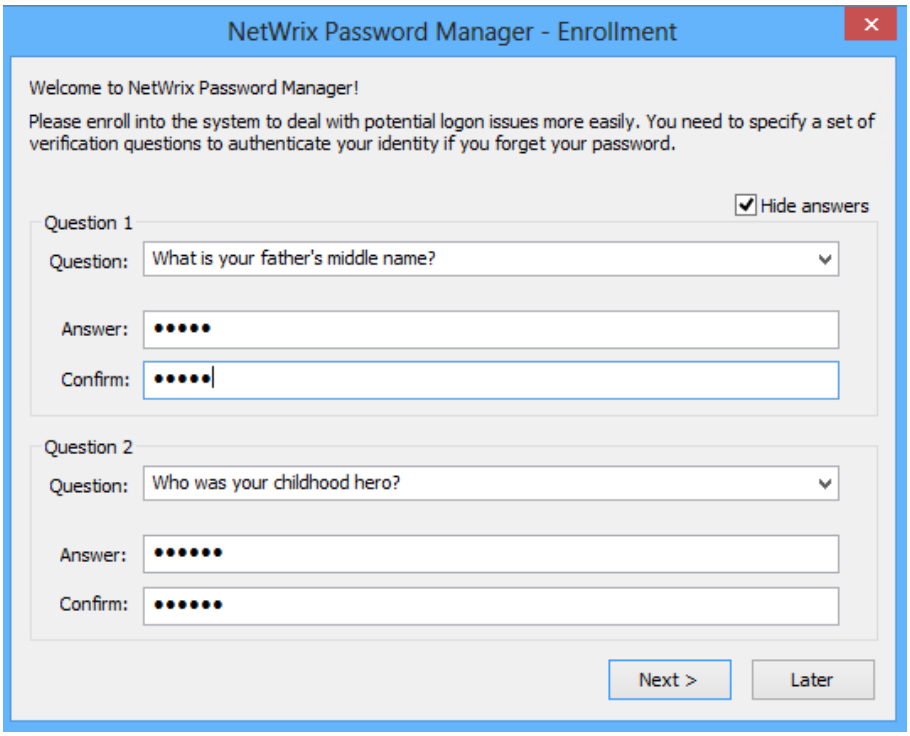
- **Automatic enrollment**: users are automatically prompted to enroll into the system at logon. For details, see 5.1 Enrolling with the Password Manager Client.
- **Manual enrollment**: users must go to the Self-Service Portal and perform the enrollment procedure. For details, see Section 5.2 Enrolling in the Self-Service Portal.
- **Batch enrollment**: administrators can pre-enroll users based on existing account and verification data (for example, taken from the HR database).

Please see the following sections below for detailed instructions on both enrollment options:

5.1. Enrolling with the Password Manager Client

If the Password Manager Client has been installed on your client machine, the Enrollment Wizard will start automatically after the installation is complete:

Figure 6: Enrollment Wizard



Perform the following procedure to enroll into the system:

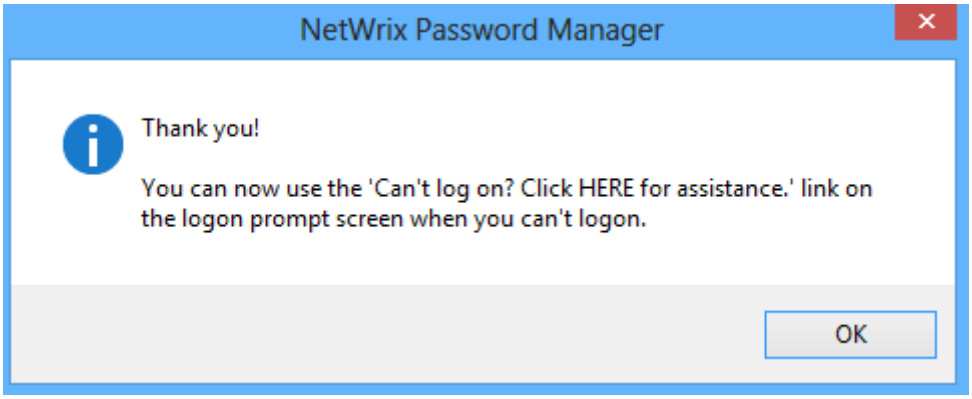
Procedure 3. To enroll with the Password Manager Client

1. In the **Enrollment** dialog select verification questions from the drop-down list, or provide your own custom question (if this option is enabled in the Administrative Portal).
2. Type your answer and confirm it. The **Hide Answers** option is selected by default. If you want to see your answers as you type, disable this option.

Note: If more than one question is required for authentication, this step will be repeated until you have selected and answered the required number of questions. The number of questions is set in **Administrative Portal** > **Settings** > **Questions Policy**.

3. Click **Finish** to complete the enrollment procedure. The following confirmation dialog will be displayed:

Figure 7: Successful Enrollment Confirmation



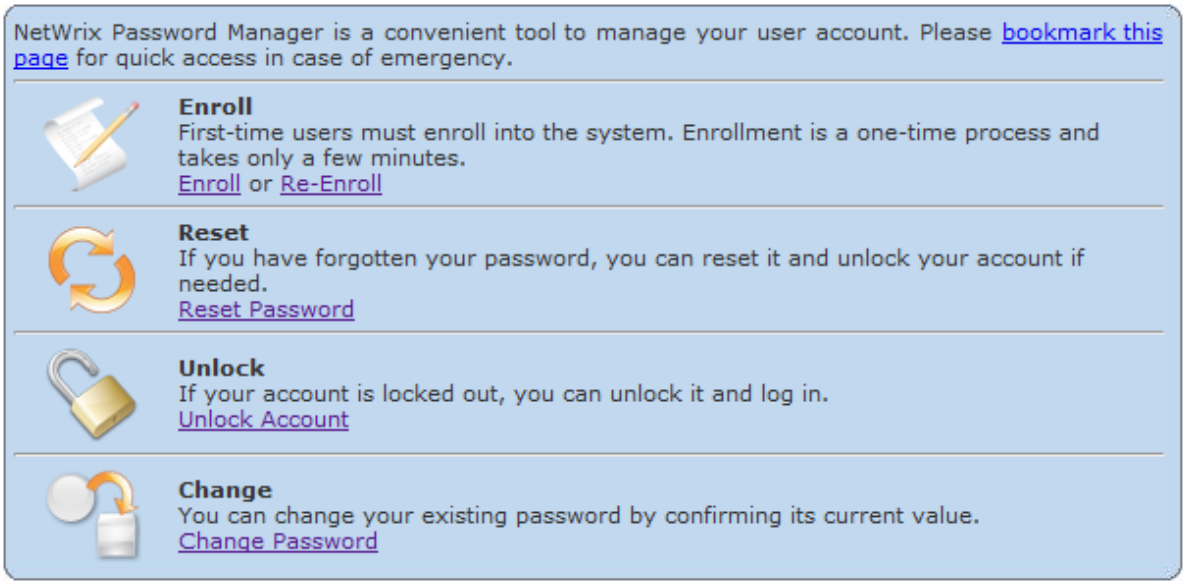
5.2. Enrolling in the Self-Service Portal

To enroll into the system through the Self-Service portal, perform the following procedure:

Procedure 4. To enroll in the Self-Service Portal

1. On the machine where the Web Application is installed, open the Self-Service Portal. To do this, go to **Start** > **All Programs** > **Netwrix** > **Password Manager** > **Self-Service Portal**. The main page of the Self-Service Portal will open in the default web-browser:

Figure 8: Self-Service Portal Main Page



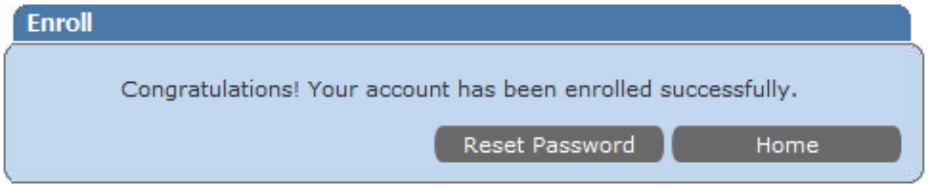
Note: If the web page cannot be displayed due to authentication problemts, add the Password Manager site to the Local Intranet zone.

2. Click on **Enroll** in the **Enroll** section. In the page that opens, enter your account name and current password and click **Next** to proceed.
3. On the next step, select a verification question from the drop-down list and type you answer following the tips provided on this page. Click **Next** to proceed.

Note: If more than one question is required for authentication, this step will be repeated until you have selected and answered the required number of questions.

The following page will be displayed after you have completed the enrollment procedure:

Figure 9: Successful Enrollment Confirmation



Once you have enrolled into the system, you can perform the self-service password management operations, such as:

- Resetting your password
- Unlocking your account
- Changing your password

For detailed step-by-step instructions on how to perform these operations, please refer to the product online help. So that you can try the product's functionality, Chapter 6 Resetting a Password below explains how to perform the password reset operation.

5.3. Batch Enrollment

If your organization has an HR database with user-specific data, such as Social Security numbers, birth places, and so on, you can preload the existing verification data in a batch, so that users can perform self-service password management operations without having to take any extra steps.

This way you can ensure that all users are enrolled for self-service, which minimizes the load on the help-desk. For more information on importing user account data, refer to Netwrix Password Manager Administrator's Guide.

6. RESETTING A PASSWORD

In this chapter you will try resetting a password. This operation can be performed by end users or by help-desk operators (if for some reason a user has no access to the Self-Service Portal or the Logon Prompt Extension).

So that you can test different aspects of the product, this chapter provides instructions on both password reset options.

6.1. Resetting a Password as an End-User

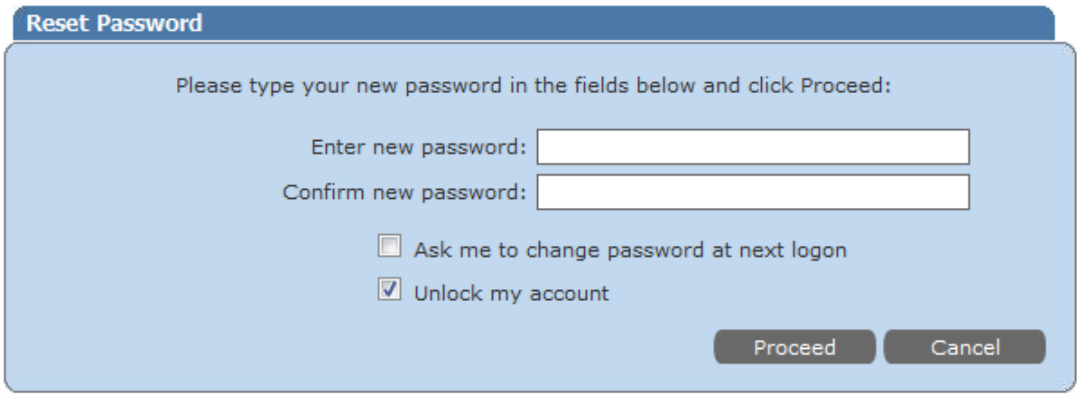
Users can reset their passwords in the Self-Service Portal or with the help of the Password Manager Client (Logon Prompt Extension) if the Password Manager Client has been installed on their machines. See the following procedures below for detailed instructions:

- Procedure 5 To reset a password in the Self-Service Portal
- Procedure 6 To reset a password via the Logon Prompt Extension

Procedure 5. To reset a password in the Self-Service Portal

1. Access the Self-Service Portal main page as explained in Section 5.2 Enrolling in the Self-Service Portal.
2. Click on **Reset Password** in the **Reset** Section.
3. In the page that opens, enter the name of the account that you want to reset the password for, and specify the domain. Then click **Next**.
4. The verification question selected on enrollment will be displayed. Type the answer to this question and click **Next** to proceed.
5. If you have answered the question correctly, the following page will be displayed:

Figure 10: Password Reset Page

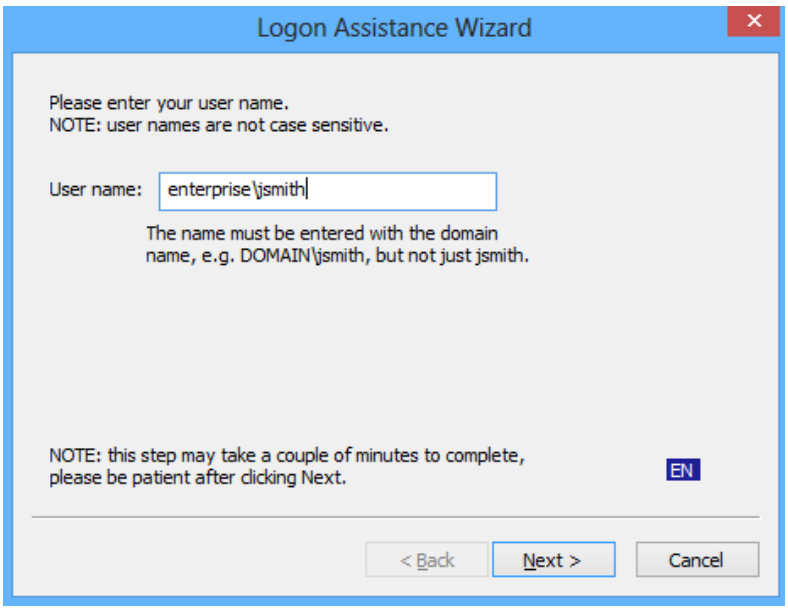


6. Enter the new password and retype it for confirmation.
   - If you want to be prompted to change your password at next logon, activate the corresponding checkbox.
   - If your account had been locked (for example, due to unsuccessful logon attempts), select the **Unlock my account** option.
7. Click **Proceed**. Your password will be reset.

Procedure 6. To reset a password via the Logon Prompt Extension

1. Log off the system or lock your computer. Pressing Ctrl + Alt + Del to call the logon page.
2. Depending on your Windows version, click the **Can't log on? Click here for assistance** link or the **Logon Assistance** button. The **Logon Assistant Wizard** will start:

Figure 11: Logon Assistance Wizard



3. Enter your account name in the domain\account name format and click **Next** to proceed.
4. On the next step, select the Reset password option, enter the new password and retype it for confirmation.
   - If your account had been locked (for example, due to unsuccessful logon attempts), select the **Unlock account** option.
   - If you want your password to be valid for an unlimited period of time, select the **Password never expires** option.

   Note: This option can be disabled by an administrator in the Administrative Portal.
5. On the next step, you will be asked to answer the verification question selected on enrollment. Type your answer and click **Finish**. Your password will be reset.

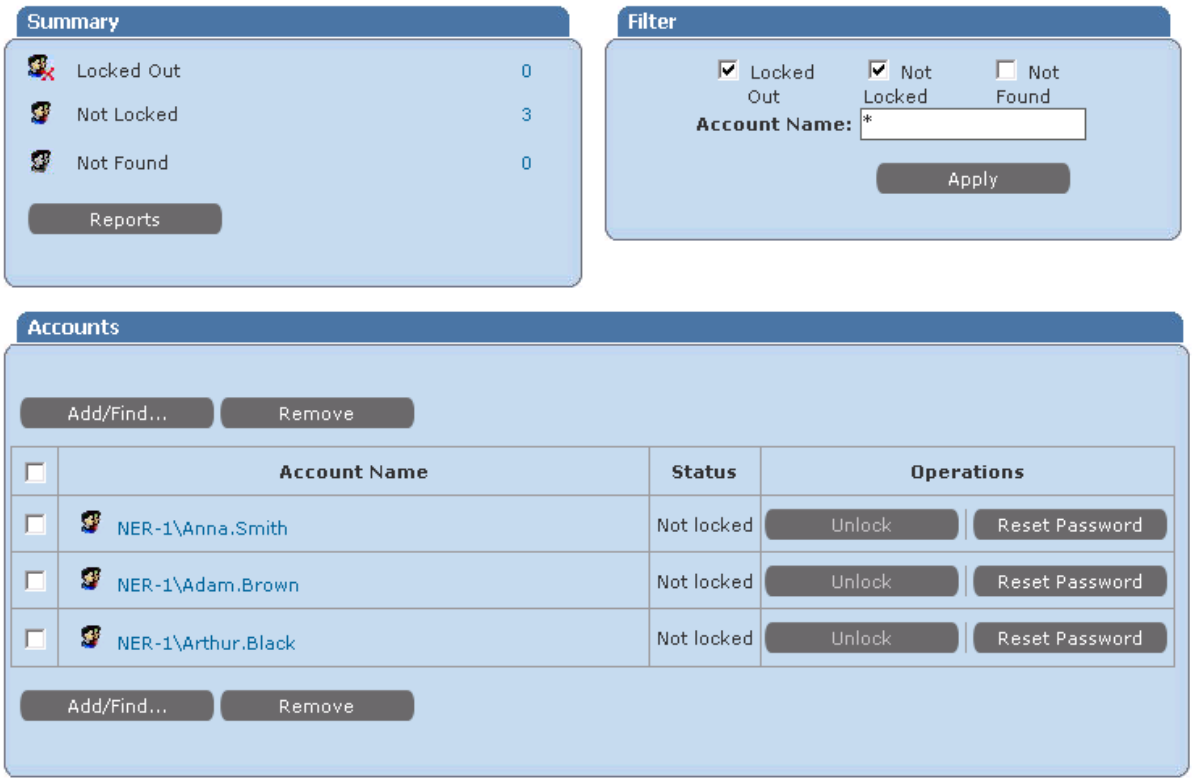
6.2. Resetting a Password as a Help-Desk Operator

If users cannot access the Self-Service Portal or the Logon Prompt Extension, they can call a help-desk operator and ask to reset their password. This section tells you how to reset a user's password through the Help-Desk Portal.

Procedure 7. To reset a password as a help-desk operator

1. Open the Help-Desk Portal. To do this, go to **Start** > **All Programs** > **Netwrix** > **Password Manager** > **Help-Desk Portal**. The main page of the Help-Desk Portal will open in the default web-browser:

Figure 12: Help-Desk Portal Main Page



Note: If the web page cannot be displayed due to authentication problemts, add the Password Manager site to the Local Intranet zone.

2. Select the user whose password you want to reset, and press the **Reset Password** button next to this account name. To search for a user, enter the account name in the Filter section.
3. The **User Identity Verification** page will be displayed containing a verification question that the user selected on enrollment.
4. Make sure that the user has answered the question correctly and click **Next**.
5. In the next page enter the new password for this user and retype it for confirmation. Select the available options if necessary and click **Next**. The password for the selected user will be reset.

7. VIEWING REPORTS

This chapter describes how to generate and view reports. Two types of reports are available:

- **User Activity** report shows all users' activities during a specified period of time.
- **User Enrollment** report shows a summary of the enrollment events for all users in the managed domains.

To generate and view these reports, execute the following procedure:

Procedure 8. To generate and view reports

1. Go to the Help-Desk Portal as explained in Section 6.2 Resetting a Password as a Help-Desk Operator.
2. Click on the **Reports** button in the **Summary** section.
3. Select the type of report you want to generate and click on the **Generate report** button. The report will be generated and displayed in your browser.

Figure 13: and Figure 14: below show example User Activity and User Enrollment reports:

Figure 13: User Activity Report Example

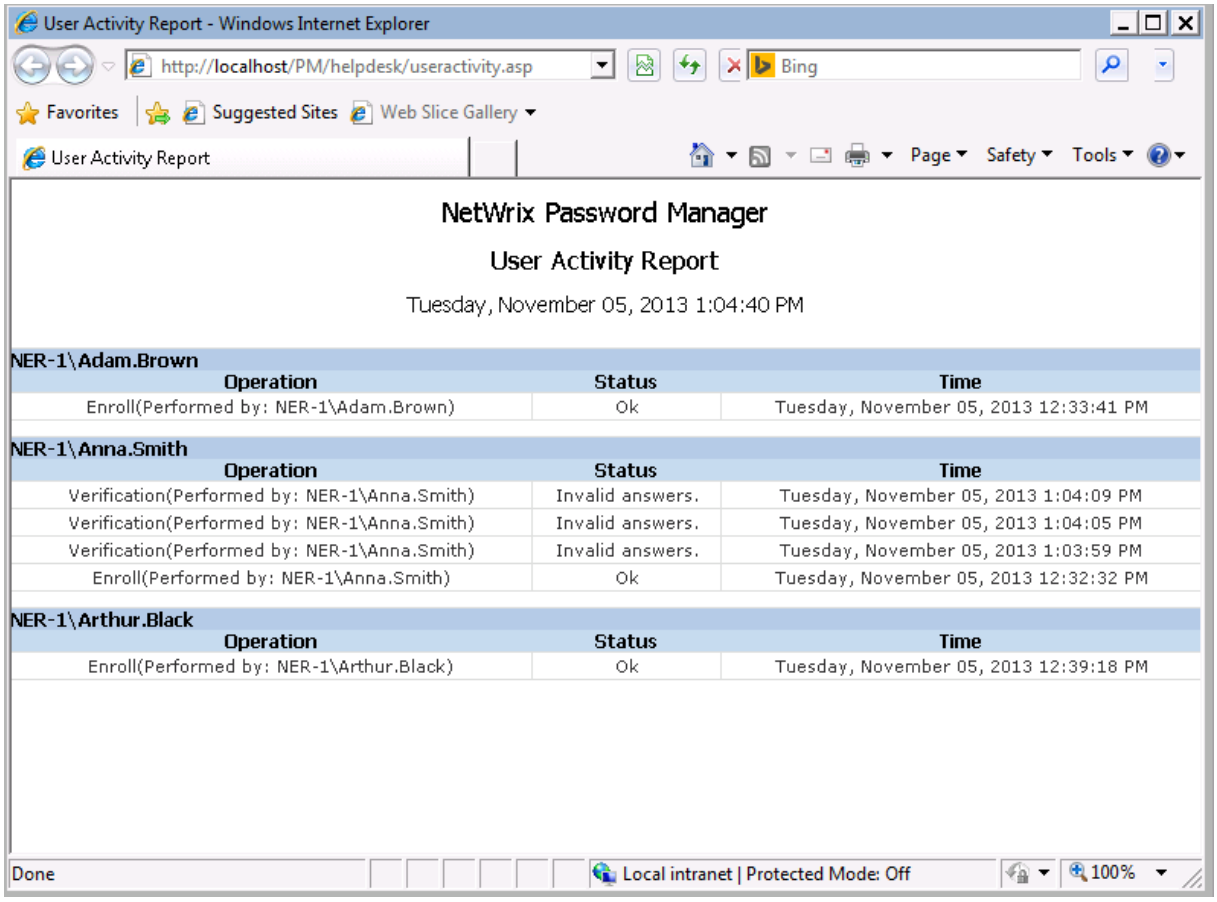
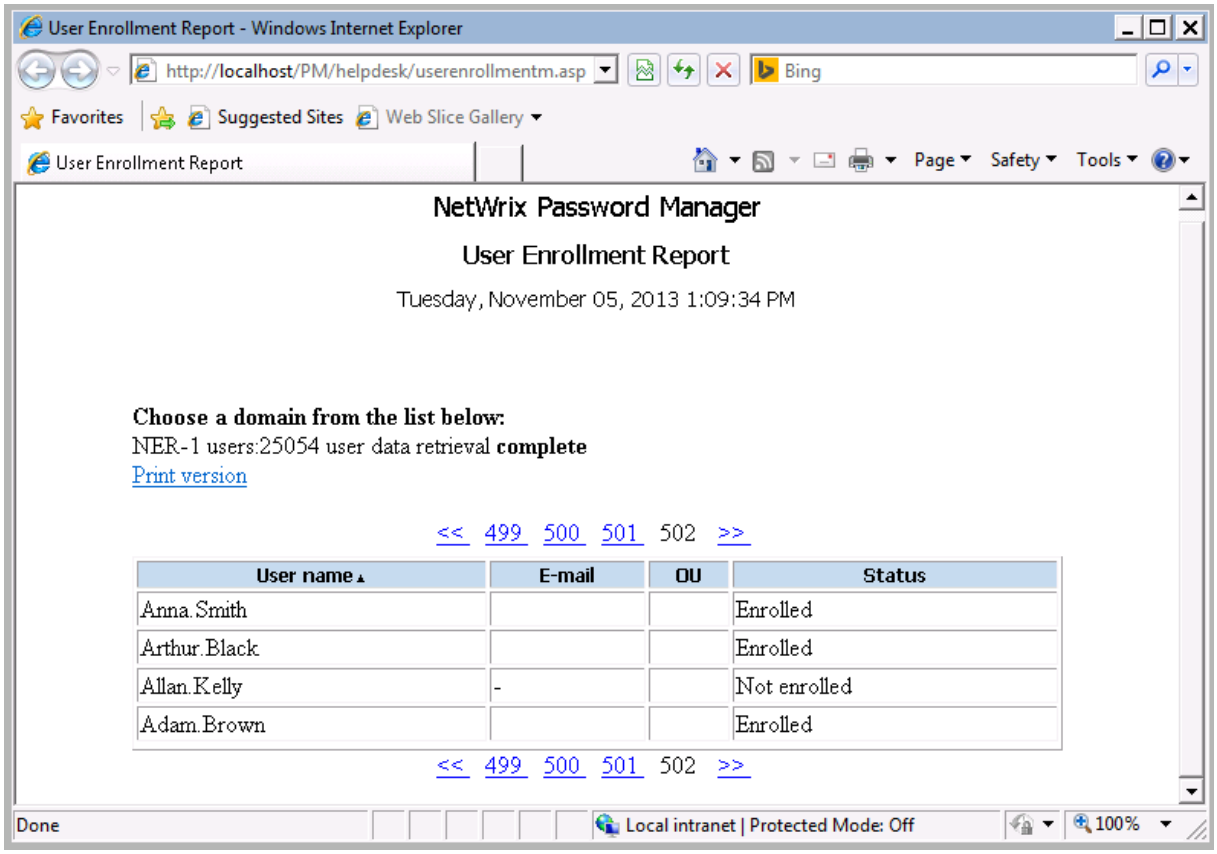


Figure 14: User Enrollment Report Example



A APPENDIX: RELATED DOCUMENTATION

The table below lists all documents available to support Netwrix Password Manager:

Table 2: Product Documentation

Document Name	Overview
Netwrix Password Manager Quick-Start Guide	The present document
Netwrix Password Manager Administrator's Guide	Provides information on various deployment scenarios and details all configuration options.
Self-Service Portal Help	Provides tips and step-by-step instructions on how to perform self-service password management operations. Accessible from the Self-Service Portal.
Help-Desk Portal Help	Provides tips and step-by-step instructions on how to perform password management operations and view reports. Accessible from the Help-Desk Portal.