NETWRIX PASSWORD MANAGER

ADMINISTRATOR'S GUIDE

Product Version: 6.5

February/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 system administrators and integrators. It contains a detailed product overview, instructions on how to install the product and information about security installation and configuration options. It also explains how to setup and use NetWrix Password Manager.

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 NetWrix Password Manager features, and explains the system's architecture and deployment structure. It also contains information on licensing.
- Chapter 3 Installing NetWrix Password Manager contains detailed instructions that will guide you through the installation process of the Password Manager Service and Client applications. It explains different installation scenarios, and also provides information on how to upgrade from previous product versions.
- Chapter 4 Configuring Password Manager Security explains different configuration and deployment options that provide for enhanced application security. It contains detailed instructions on how to setup the product for maximum performance and security.
- Chapter 5 Configuring Password Manager Settings explains how to configure the Self-Service Portal and the options available to users, how to enforce verification questions policies and apply password restrictions, etc.
- Chapter 6 Enrolling Users for Self-Service lists and explains different enrollment options, and provides guidance for administrators on which option to choose.
- Chapter 7 Troubleshooting NetWrix Password Manager lists the issues that may be encountered while using NetWrix Password Manager, and contains detailed instructions on how to resolve them.
- Appendix: Supporting Data contains reference information, such a list of all registry keys that provide additional options for NetWrix Password Manager configuration, a glossary and the list of all documentation published to support NetWrix Password Manager.

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 doing the following:

- 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 the kinds of passwords that can be used, and to apply security policies and identity verification procedures to the managed domains.

To achieve this, 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.

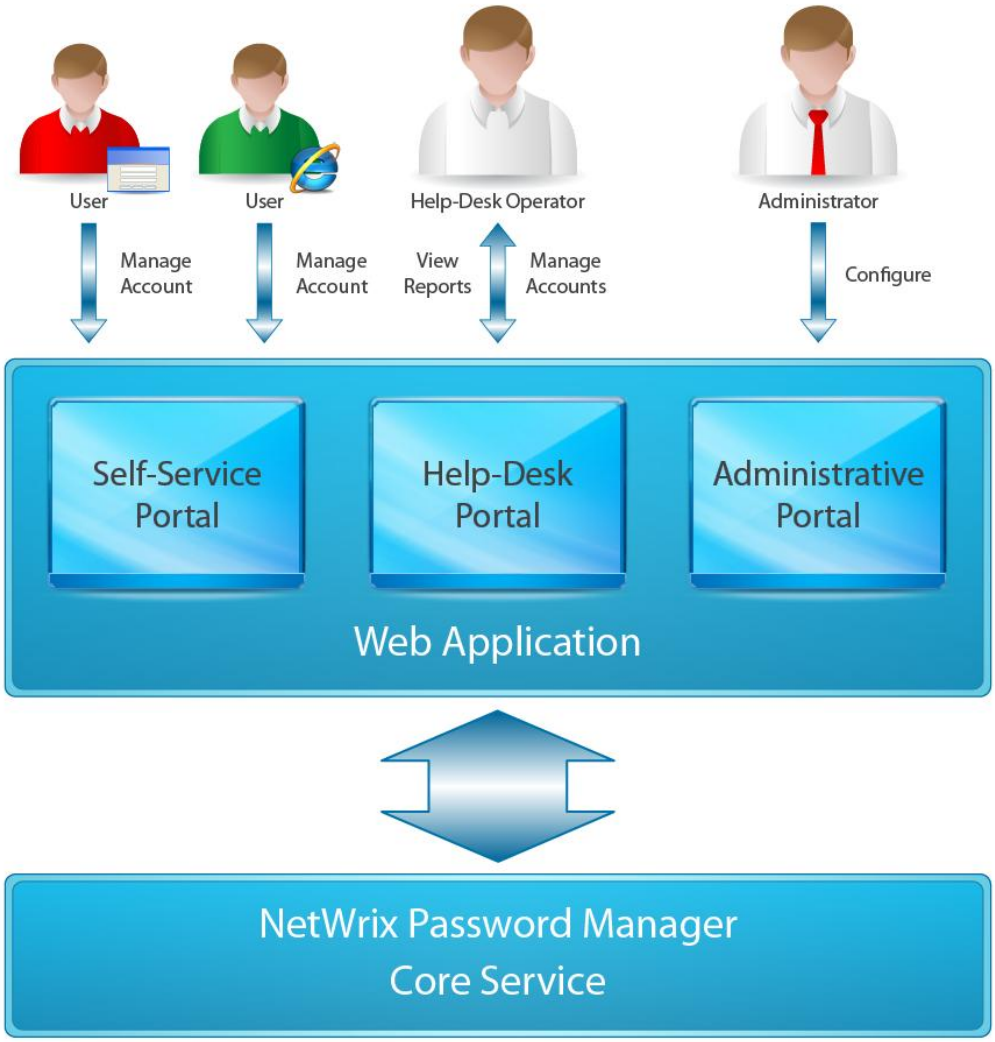
* *It is referred to as 'GINA extension' on pre Windows Vista systems and as 'Credentials Provider' on Windows Vista and Windows Server 2008 or higher.*

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 NetWrix 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. Web Application is installed on the same computer where Password Manager Service is installed. The Administrative, Help-Desk and Self-Service portals provided by Web Application are available from anywhere in the domain, and, optionally, from the Internet.

Note: If you want to install Web Application in a DMZ (demilitarized zone), so that the web portals are accesible from anywhere on the Internet, you may want to install 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, refer to Section 4.4 Installing Web Application in a DMZ.

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

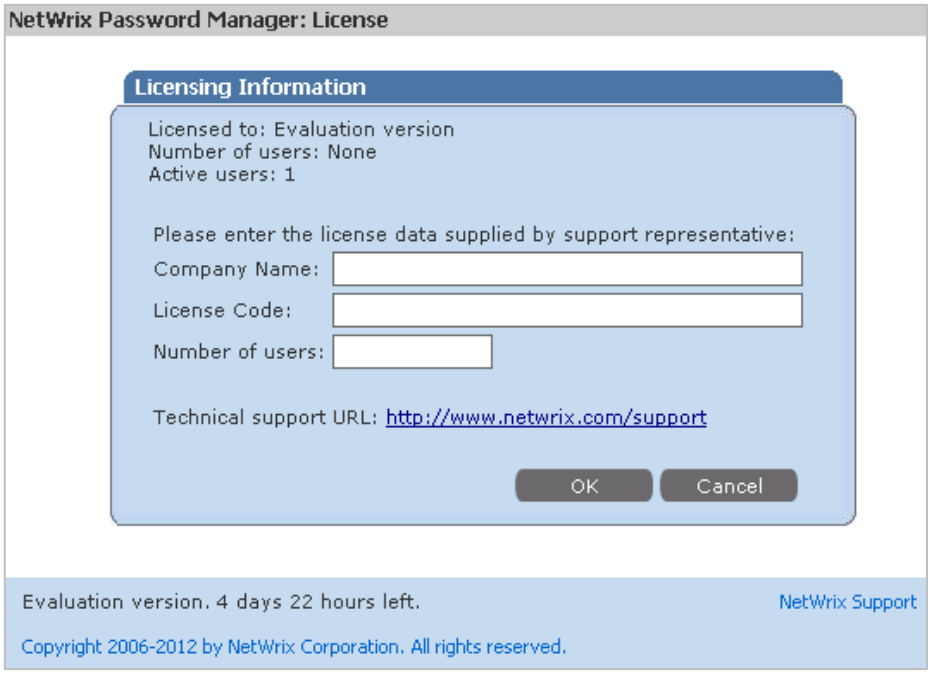
Note: The Password Manager Client and the Self-Service Portal are identical in terms of the functions they provide. Depending on your policies, you can choose not to deploy the Password Manager Client, and not sacrifice any functionality; or you can deploy it to give end users more self-service access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

2.4. Licensing Information

NetWrix Password Manager is licensed for a free 20-days evaluation period. To register the product with a permanent commercial license purchased from NetWrix, take the following steps:

1. Purchase the license code (it can be requested from the product page).
2. Install the product following the instructions in Chapter 3 Installing NetWrix Password Manager.
3. Open the Administrative Portal (for instructions refer to Section 5.1 Accessing the Administrative Portal) and click **License**. The **Licensing Information** page will be displayed:

Figure 2: Licensing Information Page



4. Fill in the fields and click **OK**.

3. INSTALLING NETWRIX PASSWORD MANAGER

This chapter guides you through the installation process of Password Manager Service, Web Application and Password Manager Client. It contains the following sections:

- Installation Prerequisites
- Installing Password Manager Service and Web Application
- Installing Password Manager Client
- Upgrading from Previous Versions
- Migrating to Another Server

3.1. Installation Prerequisites

3.1.1. Hardware Requirements

Before installing NetWrix Password Manager, make sure that the computers, where Password Manager Service and Web Application are going to be installed, meet the following hardware requirements:

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

3.1.2. Software Requirements

Make sure that this software has been installed on the corresponding computers before proceeding with the installation.

Table 1: Password Manager Software Requirements

Product Component	Required Software
Password Manager Service and Web Application	Platform: Intel x86, AMD 32 or 64 bit
	General requirements: • Windows XP SP3 or above • .NET Framework 3.5 SP1 • Windows Installer 3.1 or above • 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
	IIS 6.0 or above (Web Server 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 For instructions on how to install the Web Server role, please refer to the following article: Installing the Web Server Role.
Password Manager Client	OS: Windows XP SP3 or above
	Web browser: Microsoft Internet Explorer 6.0 or above

Make sure that the end user's computers have one of the following web browsers installed:

- Microsoft Internet Explorer 6.0 or above
- Mozilla Firefox 2.0 or above
- Apple Safari 2.0 or above
- Google Chrome 4.0 or later

3.2. Installing Password Manager Service and Web Application

Procedure 1. To install Password Manager Service and Web Application

1. Run the product setup file called prm_setup.exe on a member server or a workstation.
2. In a simple scenario, 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. For details on the service account privileges, refer to Section 4.3 Configuring Service Account Permissions.
3. Follow the instructions of the wizard to complete the installation.

As a result, once 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 Password Manager Service is installed. For details on how to enable encryption for IIS, refer to the following documentation:

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

For the advanced installation scenario (installation on an Internet-facing DMZ server), refer to Section 4.4 Installing Web Application in a DMZ.

3.3. Installing Password Manager Client

Password Manager Client can be installed manually or automatically through Group Policy. Installation through Group Policy is recommended when you need to deploy Password Manager Client on a large number of client computers. If you want to perform silent installation, you can do it via the command prompt by using the msiexec component with any of its options enabled.

See the procedures below for instructions on the installation options:

- Procedure 2 To install Password Manager Client manually
- Procedure 3 To install Password Manager Client via the command prompt
- Procedure 4 To install Password Manager Client via Group Policy

Procedure 2. To install Password Manager Client manually

1. Run the prm_client.msi installation package (located in the Password Manager installation folder) on all computers where you want to deploy the Password Manager Client (Windows 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.

Procedure 3. To install Password Manager Client via the command prompt

1. Run the following command in the command prompt:

```
msiexec.exe /I prm_client.msi  PM_URL=https://localhost/pm
/quiet.
```

2. To check all available options, type in "msiexec/help" and press **Enter**.
3. To enable the required Password Manager self-service option, add its name and a value to the command prompt when installing the client. The available options are as follows:

   - PM_NOLPE: can be "true" or "false", quotes needed. If "true", only the enrollment wizard is installed, without the logon prompt extension, which helps reset a password from the logon screen.
   - PM_URL: URL of the Password Manager server, by default http://%PRMservername%/pm.
   - ALLUSERS: can be "1" or "2", if 1 – the enrollment wizard is installed for all users.
   - PM_NOREBOOT=- can be "true" or "false", quotes needed. If true, Windows XP/2003 machines will not reboot after installation.

   The options should be added in the following format:

```
msiexec /i <file name>.msi <option name=%option value%>
/quiet
```

   Example:

```
msiexec.exe /i prm_client.msi ALLUSERS="1"
PM_URL=https://localhost/pm /quiet.
```

   To add several options, separate them by a space in the following format:

```
msiexec /i <file name>.msi <option1 name=%option1 value%>
<option2 name=%option2 value%> quiet
```

   Example:

```
msiexec.exe /i prm_client.msi ALLUSERS="1" PM_NOLPE="false"
PM_URL=https://localhost/pm PM_NOREBOOT="true" /quiet.
```

Procedure 4. To install Password Manager Client via Group Policy

1. Verify that:

   - Password Manager Service and Web Application are installed on the server.
   - The Group Policy Management Console (GPMC) is installed on the target computer.

   Note: The Group Policy Management Console is a free download from Microsoft, and can be obtained from the following link: http://go.microsoft.com/fwlink/?linkid=58541

2. Start the GPMC by going to **Start → Control Panel → Administrative Tools → Group Policy Management**.
3. Right-click the OU (organizational unit), or the entire domain, that your client computers belong to, and select **Create and Link a GPO Here**. Enter the name of the new GPO (Group Policy Object), for example 'NetWrix Password Manager'.
4. Right-click the newly created GPO and select **Edit** to start Group Policy Object Editor.

5. Navigate to the **Computer Configuration → Administrative Templates** node, right click it and select the **Add/Remove Templates** option. Click **Add** and browse to the netwrixpm.adm file (by default installed to C:\ProgramFiles\NetWrix Password Manager).
6. Navigate to the **Computer Configuration → Administrative Templates → NetWrix Password Manager** node and double-click **Password Manager server URL** in the right pane. In the dialog that opens, select the **Enabled** option, and enter the Self-Service Portal URL.
7. Adjust the advanced options (for example **Suppress Enrollment Errors**, **Reset Local Credentials Cache**, and others) if necessary.
8. Place the prm_client.msi package in a network share, e.g. \\MYSERVER\Share.

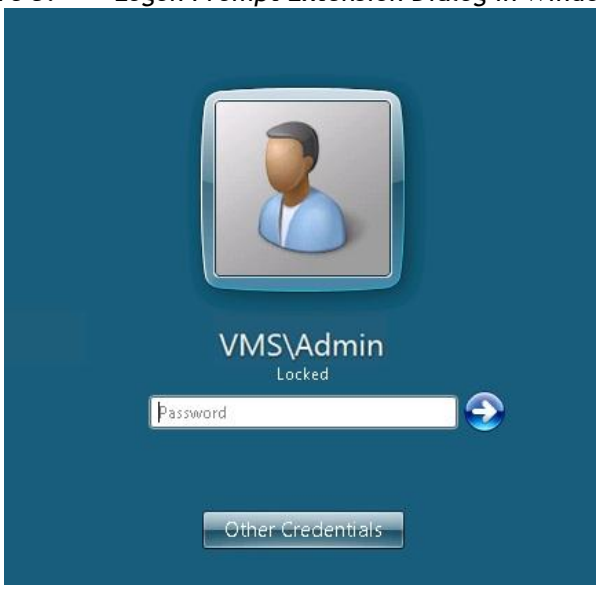
   Note: This share and its contents must be available to all users.
9. Navigate to **Computer Configuration → Policies → Software Settings**. Right-click **Software Installation**, and select **New → Package**.
10. Select the package from the share. In the **Deploy Software** dialog select **Assigned** (the default value), and click **OK**.

The Password Manager Client will be deployed automatically on end users' computers during the next startup. They will be restarted automatically after the installation.

Note: If later the Password Manager Web Application is moved to another server, the Password Manager URL must be updated.

Figure 3: and Figure 5: below show the logon dialog for Windows 7 and Windows XP/2000 with the Logon Prompt Extension that will now be displayed each time you log on the system:

Figure 3: 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 4: The logon assistance icon

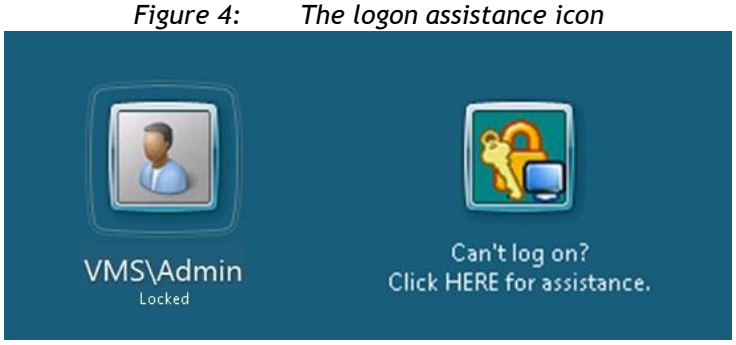


Figure 5: Logon Prompt Extension Dialog in Windows XP/2000

3.4. Upgrading from Previous Versions

Procedure 5. To upgrade Password Manager Service and Web Application

1. Back up the three .bin files in the product installation folder (alinfo.bin, inv_logon.bin and secrets.bin).
2. Install a new version in the same way as explained in Section 3.2 Installing Password Manager Service and Web Application above.

All current product settings will be preserved, and no reconfiguration is required.

Note: If you applied some specific IIS settings to your previous NetWrix Password Manager version, verify them and reconfigure if necessary.

Procedure 6. To upgrade Password Manager Client via Group Policy

1. Upload the latest prm_client.msi file to a network share as explained in Procedure 4 To install Password Manager Client via Group Policy.
2. Navigate to **Start → Control Panel → Administrative Tools → Group Policy Management**. To locate the required Domain Policy, expand the **Forest <forest_name> → Domains → <domain_name> → Group Policy Objects** node. Right-click the node and select **Edit**.

3. Navigate to **Computer Configuration** → **Policies** → **Software Settings**, right-click Password Manager Client package and select **All Tasks** → **Redeploy Application**.

The Password Manager Client will be reinstalled on all computers where the Group Policy applies.

3.5. Migrating to Another Server

Procedure 7. To migrate NetWrix Password Manager to another server

1. Install NetWrix Password Manager on a new server.
2. Stop NetWrix Password Manager Service on the server where the product was installed initially.
3. On the old server, navigate to the product installation directory (the default path is C:\ProgramFiles(x86)\NetWrix Password Manager) and copy the following files to the same location on the new server:
   - alinfo.bin
   - secrets.bin
   - PredefinedQuestions.txt
   - the entire **Templates** folder
4. Start Password Manager Service on the new server.
5. If you are using NetWrix Password Manager Client, change NetWrix Password Manager server address as follows:
   a. Navigate to **Start** → **Administrative Tools** → **Group Policy Management Console**.
   b. Right-click the GPO created for NetWrix Password Manager and select **Edit** from the pop-up menu.
   c. In the dialog that opens, navigate to **Computer Configuration** → **Administrative Templates** → <**Your_Password_Manager_Template**>.
   d. In the right pane, specify the new server URL in the **Password Manager Server URL** entry field.

4. CONFIGURING PASSWORD MANAGER SECURITY

There are several ways to enhance Password Manager operational security. This chapter explains the available security options and provides detailed instructions on how to configure them.

This chapter covers:

4.1. Configuring Web Application Security

The Web Application component does not have any inner security logic: it acts merely as a communication and presentation layer between the Web Portals/Password Manager Client and the Password Manager Service. All security checks and policy enforcements are realized on the Password Manager Service side.

However, to provide for secure communications, SSL (Secure Sockets Layer) is required to prevent data eavesdropping and tampering. You must install an SSL certificate (for example, obtained from http://www.verisign.com) on your web server, and enable the HTTPS protocol at port 443. It is recommended to disable the non-secure HTTP protocol on port 80.

To install an SSL certificate, perform one of the procedures below depending on your IIS version:

To redirect users from any page of your website right to the Password Manager Portal, or to create redirection from an http address to an https address, follow the procedure below:

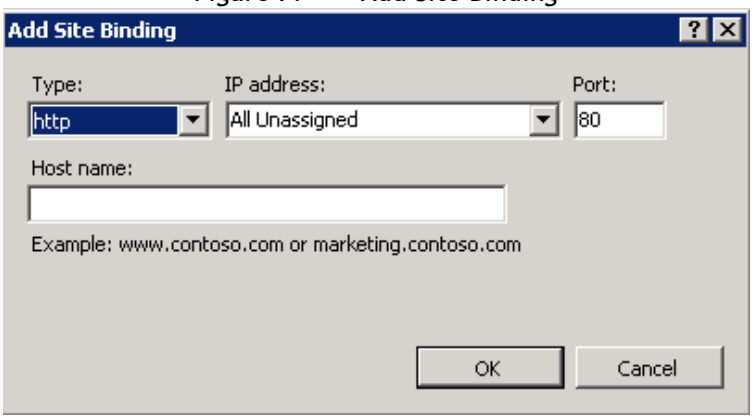
Procedure 8. To install an SSL certificate on IIS7

1. On the Password Manager server, navigate to **Start → Control Panel → Administrative Tools → Internet Information Services (IIS) Manager**. In the left pane, select the computer where the Password Manager Web Application is installed.
2. In the center pane, double-click **Server Certificates**.
3. In the **Server Certificate** dialog that opens, select one of the options in the Actions pane depending on the action you want to take: import an existing certificate, request a certificate, or create a certificate:

Figure 6: Server Certificate: Actions Tab

4. When a certificate has been installed, in the left pane select the default web site where your PRM folder is displayed.
5. In the **Actions** pane, click **Bindings,** and then click **Add**. The following dialog will be displayed:

Figure 7: Add Site Binding



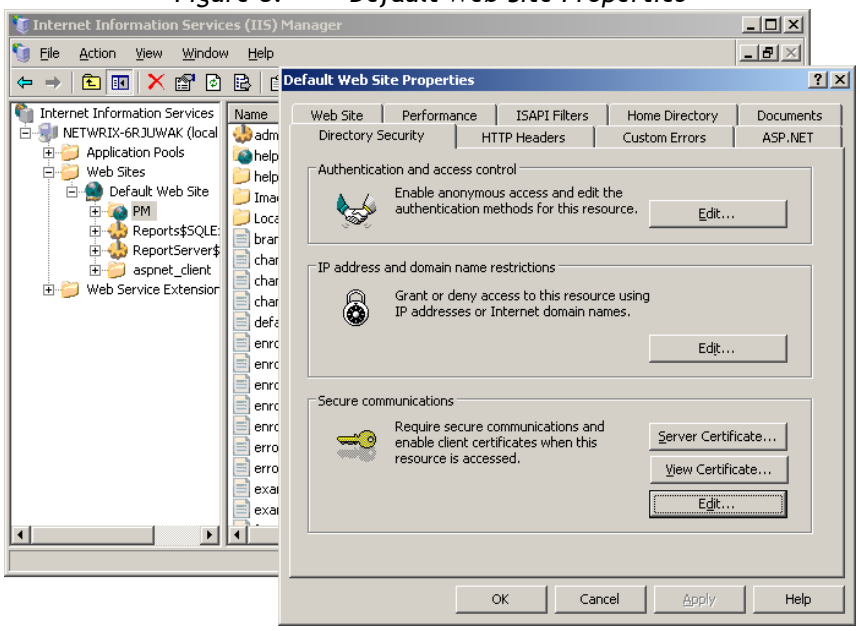
6. In the **Type** drop-down list, select 'https', specify your SSL certificate, and click **OK**.

Procedure 9. To install an SSL certificate on IIS6

1. On the NetWrix Password Manager server, navigate to **Start → Control Panel → Administrative Tools → Internet Information Services (IIS) Manager → <computer_name> → Web Sites → Default Web Site**, where your PRM folder is displayed.

2. Right-click the web site folder and switch to the **Properties** → **Directory Security** tab:

Figure 8: Default Web Site Properties

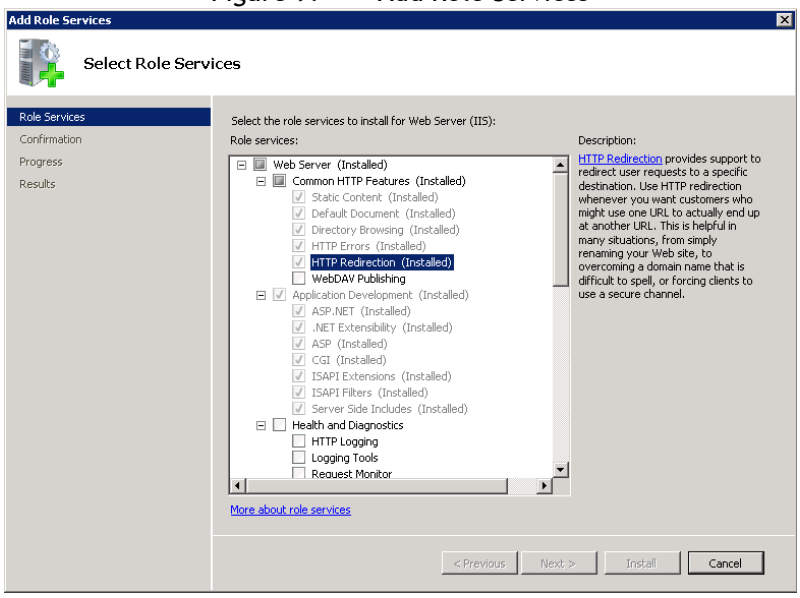


3. Click the **Server Certificate** button and follow the **Web Server Certificate Wizard** by specifying your certificate.

Procedure 10. To create a redirect in IIS

1. On the Password Manager server, make sure you have installed the HTTP Redirect feature for IIS: navigate to **Start** → **Control Panel** → **Programs and Features** and select **Turn Windows features on or off**.
2. In the **Server Manager** dialog, select **Web Server (IIS)** and click **Add Role Services** on the right.
3. In the **Add Role Services** dialog, make sure the **HTTP Redirection** service is selected. Otherwise proceed with installing it.

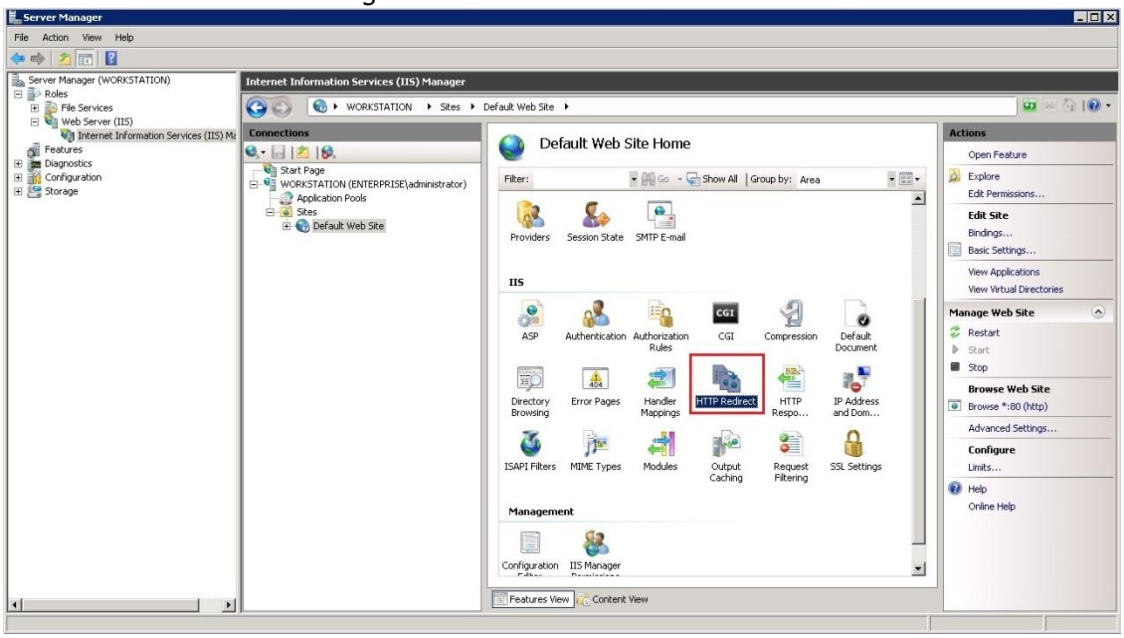
Figure 9: Add Role Services



4. In **Server Manager**, open **Internet Information Services (IIS) Manager** under **Web Server (IIS)**.

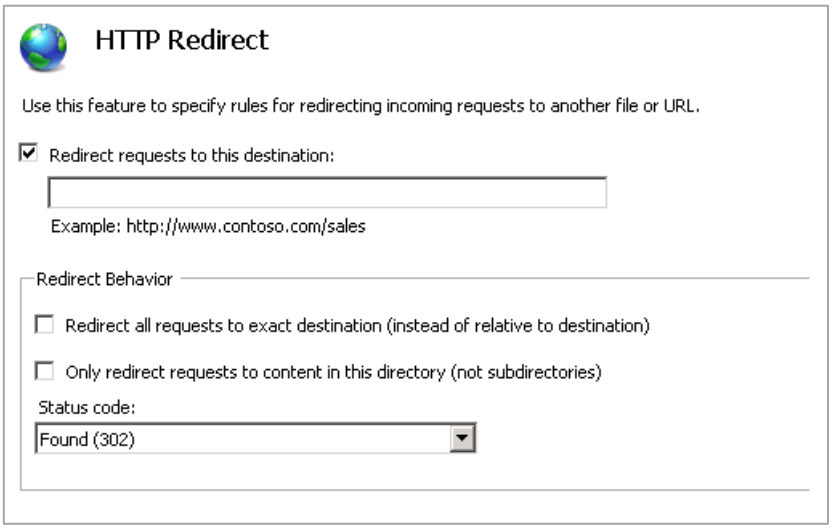
5. In the **Connections** pane, navigate to <**your computer name**> → **Sites** → **Default Web Site** and double-click the **HTTP Redirect** feature on the right.

Figure 10: HTTP Redirect Feature



6. In the **HTTP Redirect** window, select the **Redirect requests to this destination** check box and enter the Password Manager portal address, by default https://localhost/PM.

7. HTTP Redirect Feature



4.2. Configuring Roles

Password Manager Service authenticates Help-Desk Operators and Administrators by means of integrated Windows authentication.

No Windows authentication is implemented for users with the Self-Service role. This is done to enable password resets based on verification questions, without logging in.

Roles (including the security roles) are assigned in the Administrative Portal. For detailed instructions, refer to 5.6 Assigning Roles.

4.3. Configuring Service Account Permissions

The service account specified on installation must be powerful enough to unlock accounts and reset passwords in the managed domains, since all self-service and help-desk password management operations are performed under this account. This account must also be given local Admin access on the computer where Password Manager Service is installed.

The following rights must be delegated to the service account on the managed OUs:

- Change Password
- Reset Password
- Read Account Restrictions
- Write Account Restrictions
- Read *pwdLastSet*
- Write *pwdLastSet*
- Read *lockoutTime*
- Write *lockoutTime*

For instructions on how to delegate specific rights to the service account, refer to the following articles on the Microsoft support website:

- How To Delegate the Unlock Account Right
- How to grant help-desk personnel the specific right to unlock locked user accounts

4.4. Installing Web Application in a DMZ

If you want the web portals to be accessible from anywhere on the Internet, as an additional security measure, you may want to separate the Internet-facing Web Application from Password Manager Service acting as a back-end for interfacing with Active Directory domain accounts and passwords. This measure decreases the potential attack surface and improves overall security.

For step-by-step instructions on the deployment scenarios, refer to the following sections:

- Configuring a DMZ Server that is an AD Domain Member
- Configuring a DMZ Server that is not an AD Domain Member

Note: The DMZ Server must have ASP installed.

In order to allow connections to NetWrix Password Manager deployed in a DMZ, make sure your firewall settings comply with the following rules:

Table 2: Firewall Settings Rules

	Local Ports	Remote Ports	Remote Machine	Protocol	Application	Action
On DMZ Inbound	80, 443, 135	Any RPC range*	Any Backend	TCP TCP	Any Any	Allow Allow

On DMZ Outbound	RPC Range	135-139	Backend, all DCs	TCP, UDP	Any	Allow
	RPC Range	88, 389, 464	All DCs	TCP, UDP	Any	Allow
	RPC Range	DCOM range	Backend	TCP	Any	Allow
	RPC Range	53	DNS	UDP	Any	Allow
On Backend Inbound	DCOM range	RPC range	DMZ	TCP	Any	Allow
	135-139	RPC range	DMZ	TCP, UDP	Any	Allow
On Backend Outbound	RPC range	135-139	DMZ, all DCs	TCP, UDP	Any	Allow
	RPC range	88, 389, 464	All DCs	TCP, UDP	Any	Allow
	RPC range	53	DNS	UDP	Any	Allow
	RPC range	RPC range	All DCs	TCP	Lsass.exe*	Allow
	RPC range	25	Mail Server	TCP	Any	Allow
On DCs Inbound	88, 389, 464	RPC range	DMZ, Backend	TCP, UDP	Any	Allow
	135-139	RPC range	Backend	TCP, UDP	Any	Allow
	RPC dynamics	RPC range	Backend	TCP	Lsass.exe*	Allow
On DCs Outbound: no rules required						
Additional: DNS Inbound	53	Any	Any	UDP	Any	Allow
Mail Server Inbound	25	Any	Any	TCP	Any	Allow

*The RPC range is 1024 – 65535 (Windows NT/XP/2003), or 49152 – 65535 (Windows Vista/2008/7/2k8r2)

**Lsass.exe is %systemroot%\System32\lsass.exe

Note: All inbound and outbound connections on all servers are blocked, if they do not match these rules.

4.4.1. Configuring a DMZ Server that is an AD Domain Member

For this deployment scenario, perform the following procedures:

- Install Password Manager Service on the back-end server

Note: It is not recommended to use a domain controller as a back-end server.

- Install Web Application on the front-end
- Test the configuration

Procedure 11. To install Password Manager Service on the back-end server

1. Install the Password Manager Application using the `/dmz` command-line parameter under a domain account with the necessary permissions and rights (for details on permissions, see Section 4.3 Configuring Service Account Permissions).

Note: The `/dmz` key implies that IIS is not required, and no web interface is installed on the back-end server.

2. Navigate to **Start → Control Panel → Administrative Tools → Active Directory Users and Computers**, and locate the account for the machine that you want to act as a server in the DMZ. Select the **Trust this computer for delegation** option.

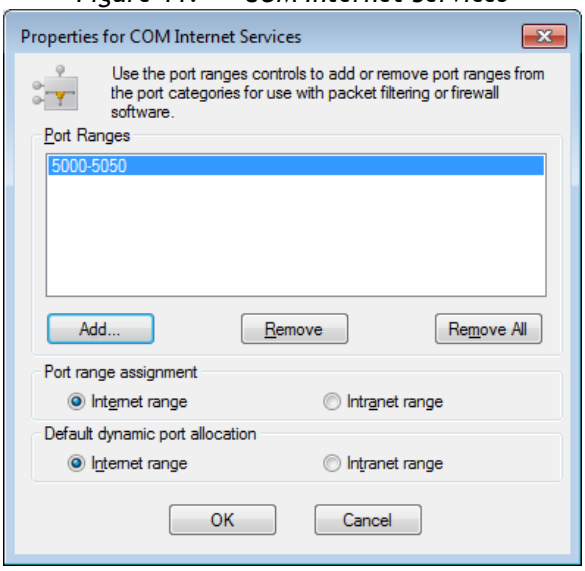
3. Create a new domain account called IUSR_NetWrix_DMZ and include it in the following local groups on the back-end server: **Guests** and **Distributed COM Users**.

4. To the **Distributed COM Users** group, also add all users that are members of the Administrators and Help-Desk Operators Roles (for details on how to assign roles to users, refer to Section 5.6 Assigning Roles).

   Note: Users that belong to the Local Administrators group, already have all the necessary permissions and access rights, so you do not have to add them to the **Distributed COM Users** group.

5. On the back-end server, navigate to **Start → Run** and execute the `dcomcnfg.exe` command to run **Component Services**. In the **Component Services** snap-in navigate to **Console Root → Component Services → Computers → My Computer**, right-click it and select **Properties**. Navigate to the **Default Protocols** tab, and select **Connection-oriented TCP/IP**. Click **Properties**, the **Add** button and specify a range of at least fifty ports, e.g. 5000-5050.

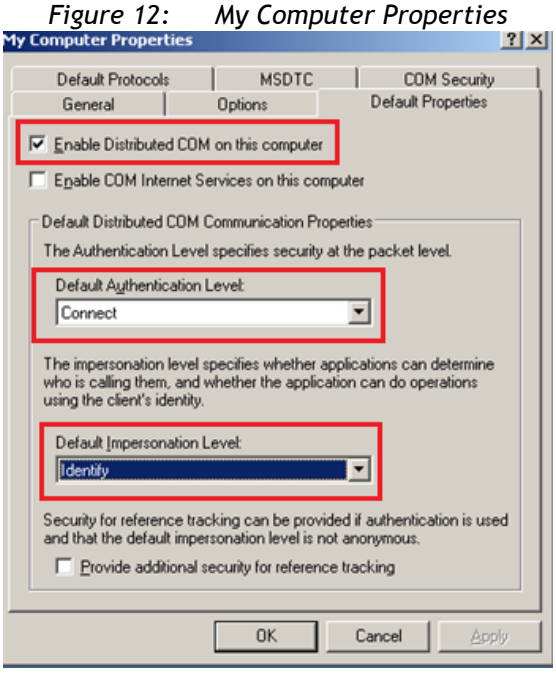
Figure 11: COM Internet Services



6. In the firewall settings between the DMZ and the internal network, allow network connections from the DMZ server to the backend server for port 135 (TCP) and the port range configured above.

7. In the **My Computer Properties** dialog, select the **Default Properties** tab and make sure that everything is configured as shown in the figure below:

Figure 12: My Computer Properties

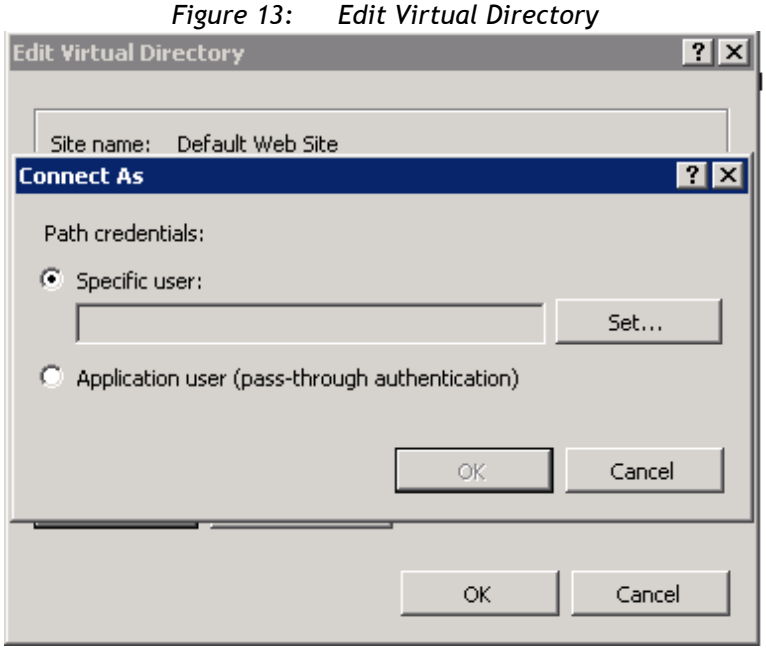


8. Restart the back-end server.

Procedure 12. To install Web Application on the front-end (DMZ)

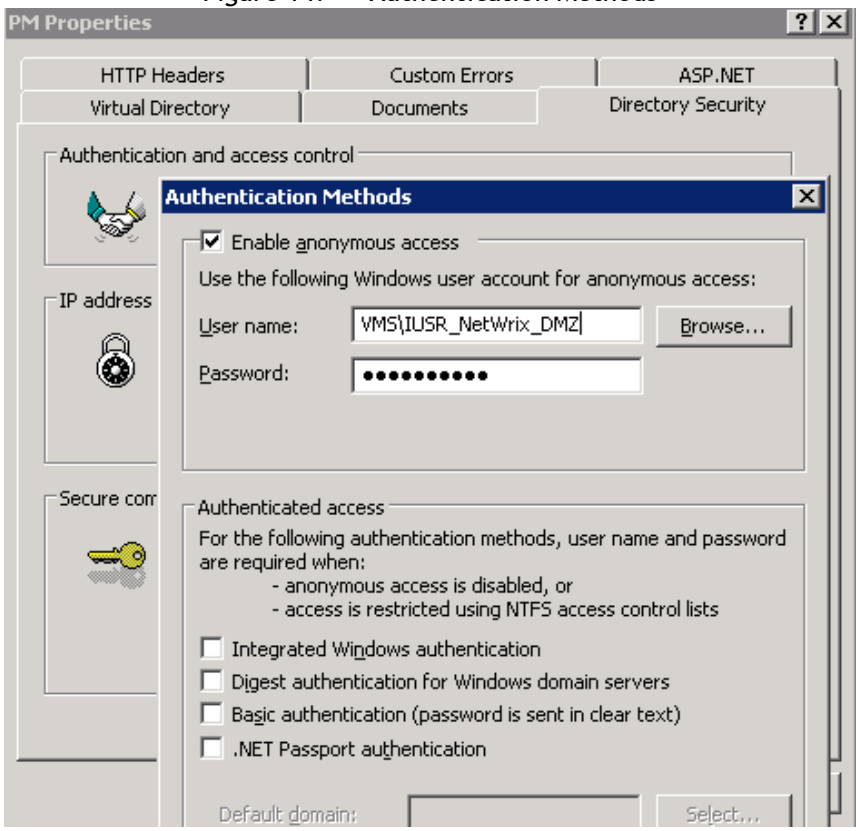
1. Install NetWrix Password Manager as described in Section 3.2 Installing Password Manager Service and Web Application under any domain account.
2. Navigate to **Start → Control Panel → Administrative Tools → Services**, and stop the service named **NetWrix Password Manager**. Then set its startup mode to 'Disabled'.
3. Navigate to the product folder and remove the prmservice.exe file. This is done since the local service may still be in use, and if the DMZ configuration is wrong, the local COM server may be started instead of the remote one.
4. Navigate to **Start → Control Panel → Administrative Tools → Component Services → Computers → My Computer → DCOM Config**. Right-click **NetWrix Password Manager** and select **Properties**. Go to the **Location** tab and disable the **Run application on this computer** check box. Then enable the **Run application on the following computer** option, and enter the name of the back-end server you have installed, click **OK**.
5. Run the IIS Manager snap-in (**Start → Control Panel → Administrative Tools → Internet Information Services (IIS) Manager**). Do one of the following, depending on your IIS version:
   - For IIS7: In the left pane, locate the virtual directory created on installation (normally named 'PM'). In the **Actions** pane on the right, click **Basic Settings**. In the dialog that opens, click the **Connect as** button, select the **Specific user** option and specify the domain account in step three of Procedure 11 To install Password Manager Service on the back-end server in the domain\account format. Enter the password and click **OK**.

Figure 13: Edit Virtual Directory



- For IIS6: In the left pane, locate the virtual directory created on installation (normally named 'PM'), right-click it and select **Properties**. Open the **Directory Security** tab, click **Edit** in the **Authentication and access control** section. In the dialog that opens, enter the name of the domain account created in step three of Procedure 11 To install Password Manager Service on the back-end server in the domain\account format. Enter the current password and click **OK**.

Figure 14: Authentication Methods



Anonymous logons will be now impersonated as the specified user.

Procedure 13. To test the configuration

1. Navigate to Password Manager Self-Service Portal (running on the DMZ server) from an outside network.
2. Perform some basic actions, such as enrolling and resetting a user's password (for instructions on how to perform these operations, refer to the Self-Service Portal help).

4.4.2. Configuring a DMZ Server that is not an AD Domain Member

For this deployment scenario, perform the following procedures:

- Install Password Manager Service on the back-end server

Note: It is not recommended to use a domain controller as a back-end server.

- Install Web Application on the front-end
- Test the configuration

Procedure 14. To install Password Manager Service on the back-end server

1. Install NetWrix Password Manager using the `/dmz` command-line parameter under a domain account with the necessary permissions and rights (for details on permissions see Section 4.3 Configuring Service Account Permissions).

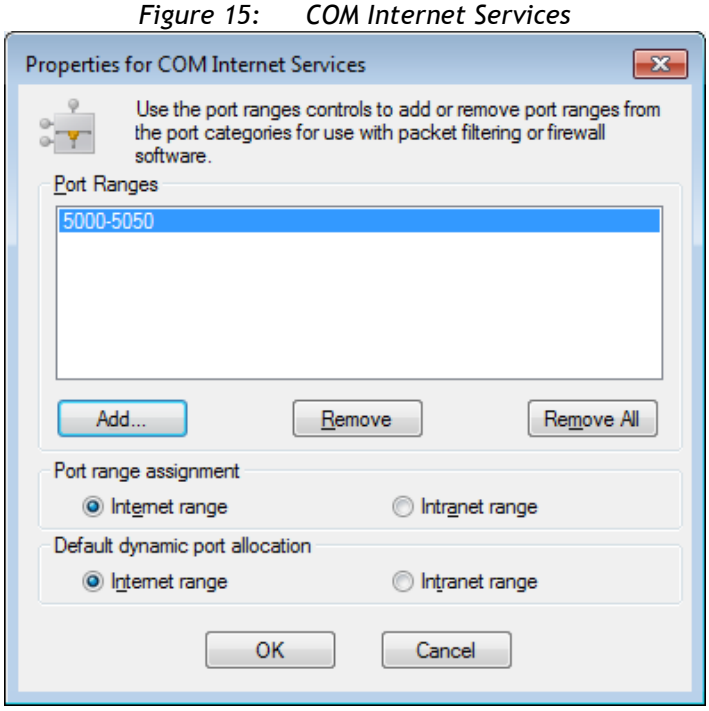
   Note: The `/dmz` key implies that IIS is not required, and no web interface is installed on the back-end server.

2. Create a new local account called IUSR_NetWrix_DMZ and include it in the following local groups on the back-end server: **Guests** and **Distributed COM Users**.
3. To the Distributed COM Users group, also add all users that are members of the Administrators and Help-Desk Operators Roles (for details on how to assign roles to users, refer to Section 5.6 Assigning Roles).

   Note: Users that belong to the Local Administrators group, already have all the necessary permissions and access rights, so you do not have to add them to the **Distributed COM Users** group.

4. On the back-end server, go to **Start** → **Run** and execute the dcomcnfg.exe command to run **Component Services**. In the **Component Services** snap-in go to **Console Root** → **Component Services** → **Computers** → **My Computer**, right-click it and select **Properties**. Go to the **Default Protocols** tab, and select **Connection-oriented TCP/IP**. Click **Properties**, the **Add** button and specify a range of at least fifty ports, e.g. 5000-5050.

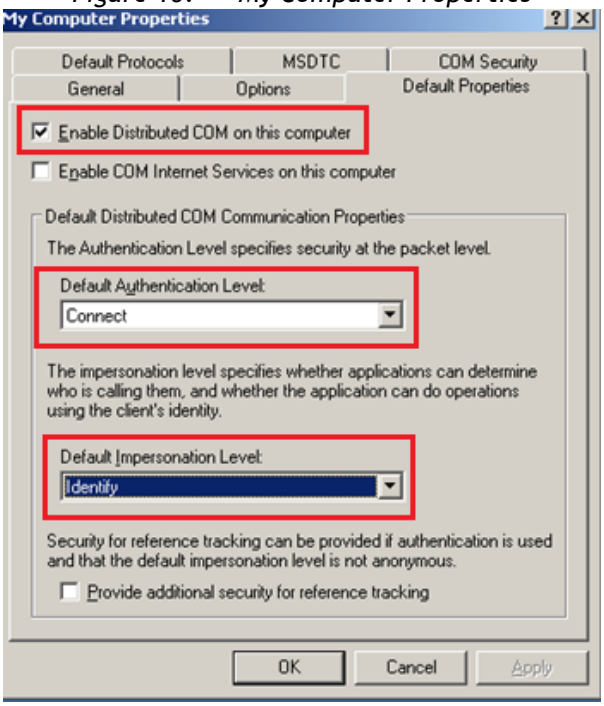
Figure 15: COM Internet Services



5. In the firewall settings between the DMZ and the internal network allow network connections from the DMZ server to the backend server for port 135 (TCP) and the port range configured above.

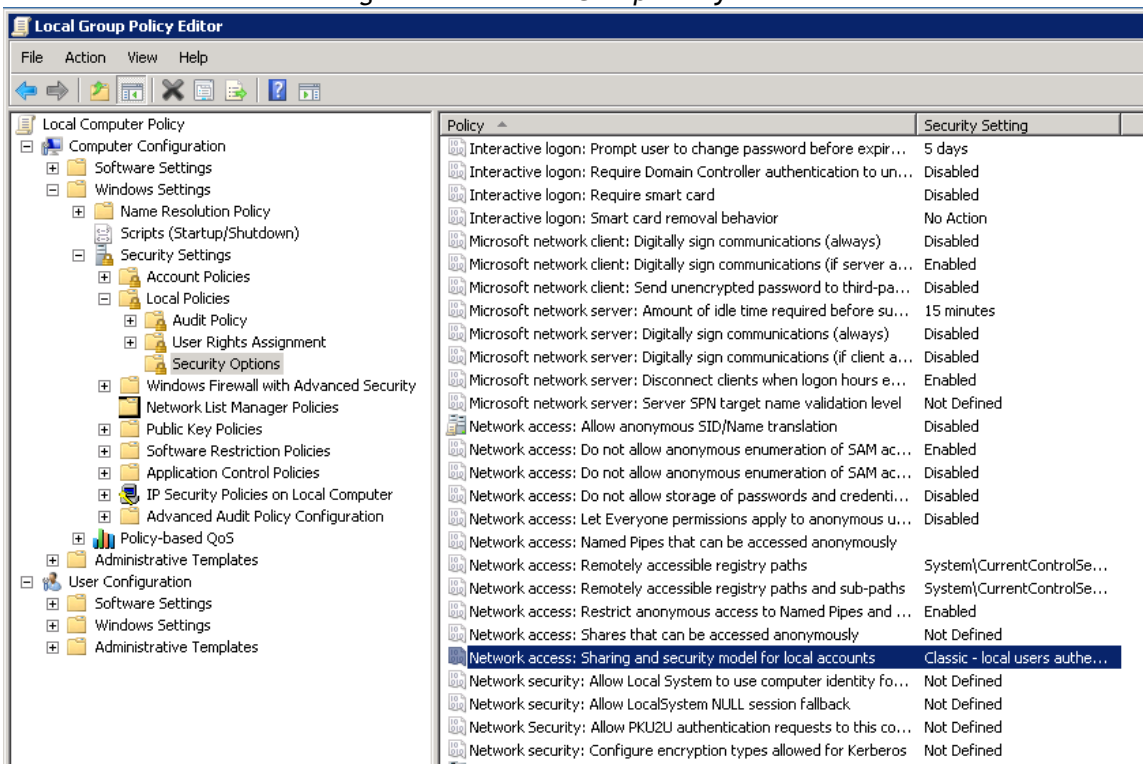
6. In the **My Computer Properties** dialog, select the **Default Properties** tab and make sure that everything is configured as shown in the figure below:

Figure 16: My Computer Properties



7. Open the Local Group Policy Editor (navigate to **Start** → **Run** and execute the `gpedit.msc` command). Expand the **Windows Settings** → **Security Settings** → **Local Policies** → **Security Options** node and locate the **Network access: Sharing and security model for local accounts** policy in the right pane:

Figure 17: Local Group Policy Editor



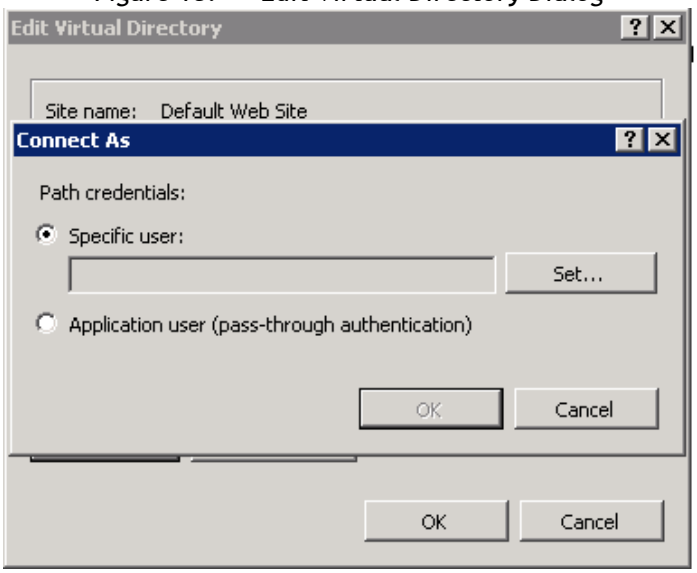
8. Double-click this policy and make sure that it is set to 'Classic – local users authenticate as themselves'.
9. Restart the back-end server.

Procedure 15. To install Web Application on the front-end (DMZ)

1. Install the Password Manager Application as described in Section 3.2 Installing Password Manager Service and Web Application under a Local Administrator account.
2. Navigate to **Start → Control Panel → Administrative Tools → Services**, and stop the service named **NetWrix Password Manager**. Then set its startup mode to 'Disabled'.
3. Navigate to the product folder and remove the prmservice.exe file. This is done since the local service may still be in use, and if the DMZ configuration is wrong, the local COM server may be started instead of the remote one.
4. Create a new local account called IUSR_NetWrix_DMZ (user name and password must be identical to the ones you have created on the back-end server), and include it in the following local groups on the back-end server: **Guests** and **Distributed COM Users**.
5. Navigate to **Start → Control Panel → Administrative Tools → Component Services → Computers → My Computer → DCOM Config**. Right-click **NetWrix Password Manager** and select **Properties**. Go to the **Location** tab and disable the **Run application on this computer** check box. Then enable the **Run application on the following computer** option, and enter the name of the back-end server you have installed. Then click **OK**.
6. Run the IIS Manager snap-in (**Start → Control Panel → Administrative Tools → Internet Information Services (IIS) Manager**). Do one of the following, depending on your IIS version:

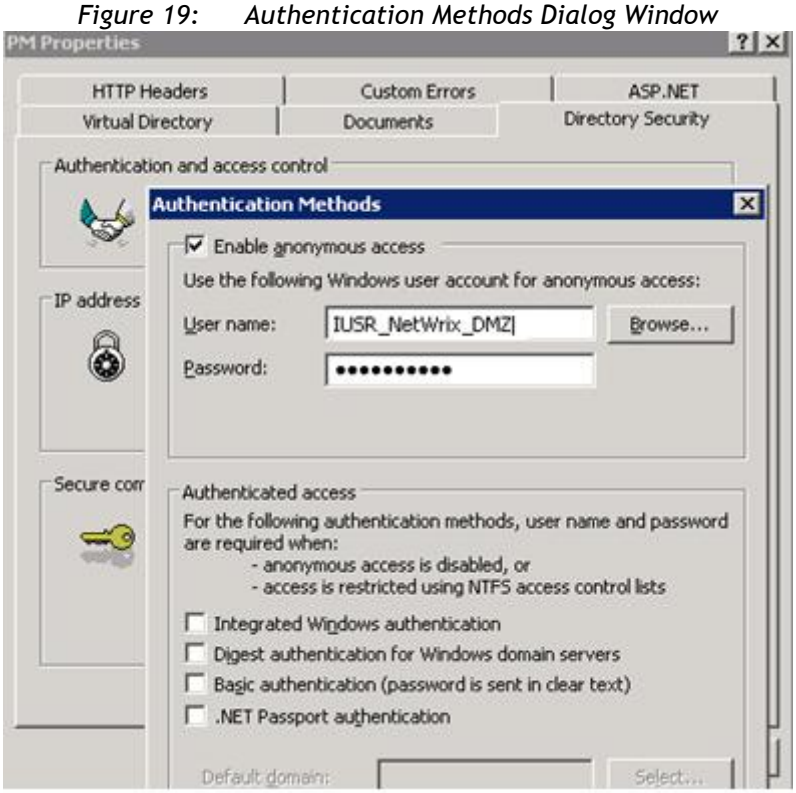
- For IIS7: In the left pane, locate the virtual directory created on installation (normally named 'PM'). In the **Actions** pane on the right, click **Basic Settings**. In the dialog that opens, press the **Connect as** button, select the **Specific user** option and specify the local account created in step 4 above (without the domain name). Enter the password and click **OK**.

Figure 18: Edit Virtual Directory Dialog



- For IIS6: In the left pane, locate the virtual directory created on installation (normally named 'PM'), right-click it and select **Properties**. Open the **Directory Security** tab, click **Edit** in **the Authentication and access control** section. In the dialog window that opens, enter the name of the local account created in step 4 above (without the domain name). Enter the current password and click **OK**.

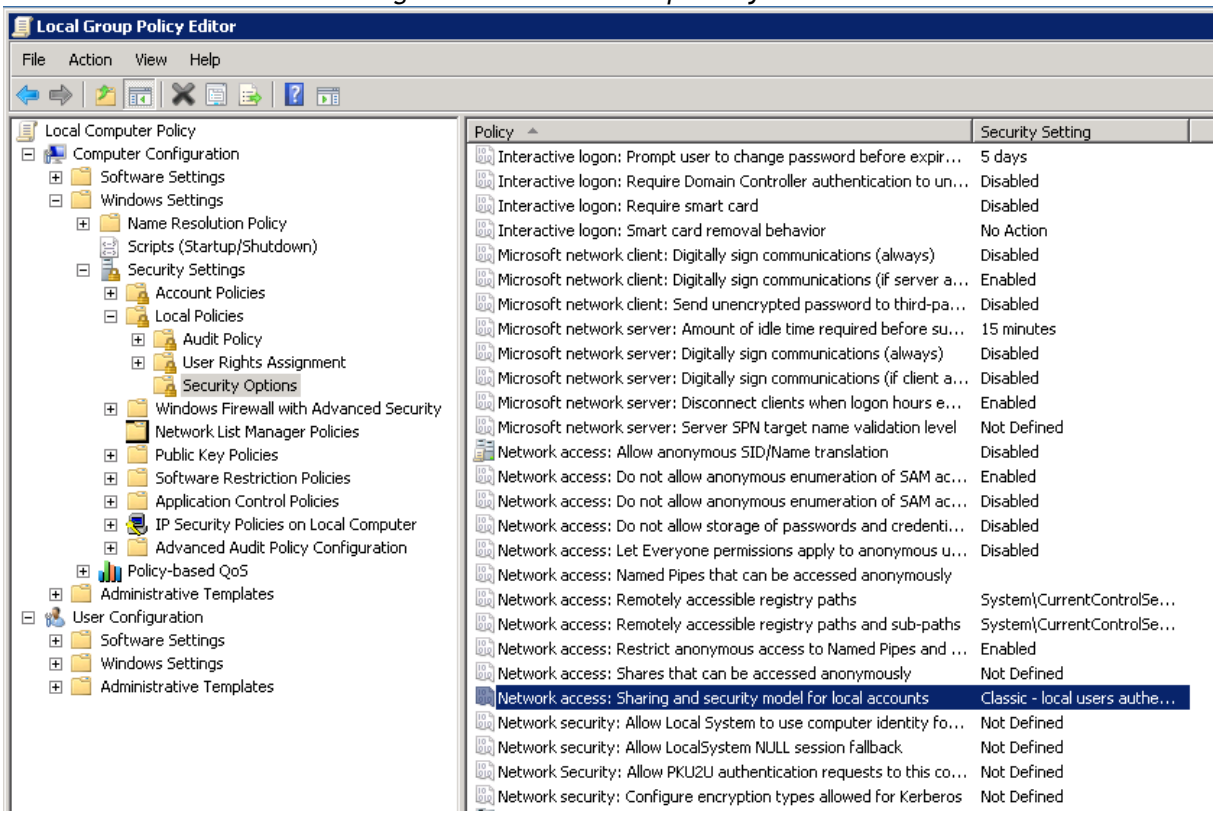
Figure 19: Authentication Methods Dialog Window



Anonymous logons will be now impersonated as the specified user.

7. Open the Local Group Policy Editor (navigate to **Start → Run** and execute the `gpedit.msc` command). Expand the **Windows Settings → Security Settings → Local Policies → Security Options** node and locate the **Network access: Sharing and security model for local accounts** policy in the right pane:

Figure 20: Local Group Policy Editor



8. Double-click this policy and make sure that it is set to 'Classic – local users authenticate as themselves'.
9. Restart the front-end server.

Procedure 16. To test the configuration

1. Navigate to the Password Manager Self-Service Portal (running on the DMZ server) from an outside network.
2. Perform some basic actions, such as enrolling and resetting a user's password (for instructions on how to perform these operations, refer to Self-Service Portal help).

4.5. Clustering for Enhanced Stability

This chapter provides tips on how to improve NetWrix Password Manager performance.

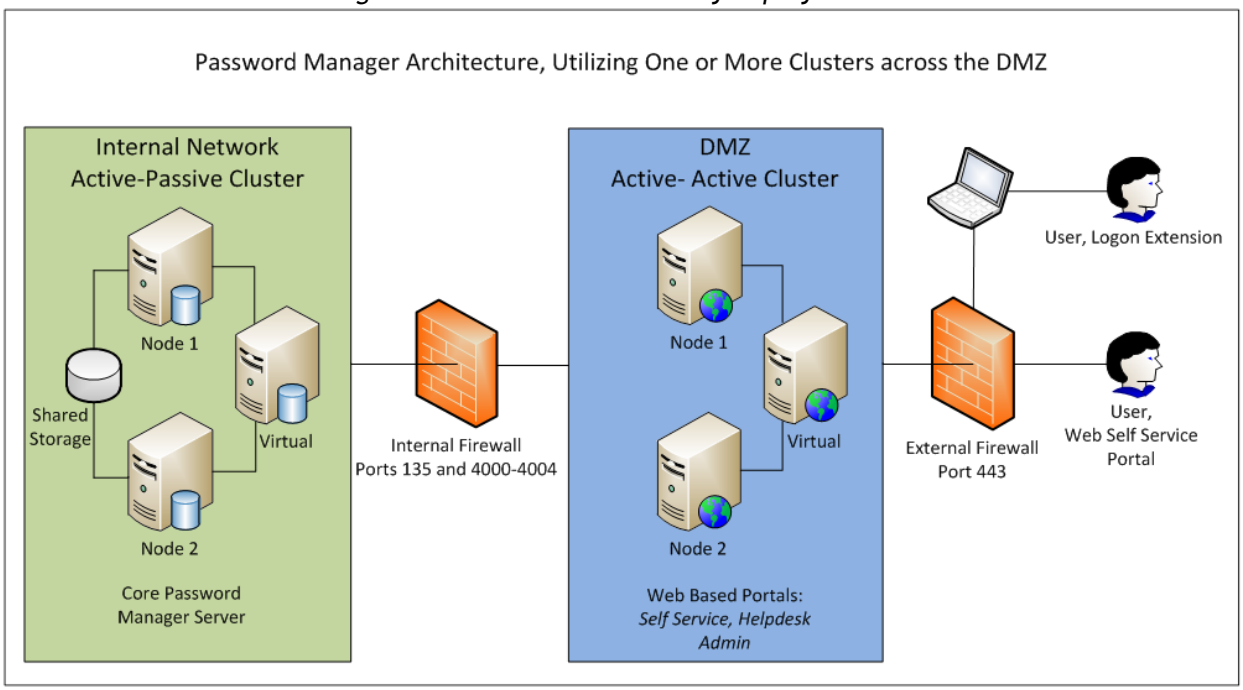
Password Manager Service and/or the front-end may be spread separately to clusters of multiple servers. While the front-end cluster represents a load-balanced server network, the service cluster is a failover one.

Several clustering options are possible:

- One front-end (DMZ) server and two (or more) failover back-end servers with a common configuration database storage. This configuration provides only service failover and is more secure.
- Two or more load-balanced front-end (DMZ) servers and one back-end server. This configuration allows decreasing the load on the web portals, but does not provide any failover, as there is still one service which provides the core functionality.
- Two or more load-balanced front-end (DMZ) servers and two or more failover back-end servers with a common configuration database storage. This configuration provides both for web portals load decrease and service failover.

The figure below illustrates the third deployment option:

Figure 21: Enhanced Stability Deployment



4.6. Configuring Password Manager Client Security

The Password Manager Client (Windows Logon Prompt Extension) connects to Password Manager Service using the same mechanism as Microsoft Internet Explorer: the HTTPS protocol. Therefore, the same security considerations apply: make sure that you specify an https-prefixed Self-Service Portal URL during installation and configuration.

The Password Manager Client (Windows Logon Prompt Extension) supports a disconnected operation mode, which means that no actual connection to the domain is required after a password has been reset using the Password Manager Client.

Note: After logging into the system, users must initiate a network connection and change their passwords again for Active Directory and locally stored passwords to synchronize. If there is connection to the Self-Service Portal, the passwords will be synchronized automatically.

4.7. Configuring Profile Database Security

The Profile Database is maintained by Password Manager Service. All users' answers to verification questions are stored using a non-reversible encryption (MD5). Only the first and

the last letter of each answer can be decrypted by Password Manager Services to enable manual user verification by Help-Desk operators.

The profile database is stored in binary files named alinfo.bin, inv_logon.bin and secrets.bin located in the installation folder. You can apply NTFS permissions and encryption settings to these files for additional security.

It is strongly recommended to backup profile database files regularly to avoid potential data loss. Database backups must be encrypted when copied to a backup media. In the simplest case, use password-protected .zip files).

4.8. Configuring Built-In Security Policies

NetWrix Password Manager provides a number of built-in security policies configurable from the Administrative Portal. The following settings are highly recommended:

- **Self-Service Role**: allow end users to perform password resets and account unlocks in a self-service fashion (for detailed instructions on how to configure roles, refer to Section 5.6 Assigning Roles).

Note: Do not assign this role to domain administrators and other sensitive users, since this can compromise their security (for example, by answer-guessing or account hijacking attempts).

- **Questions/Answers Policy**: configure these settings to make sure that users provide secure question-answer pairs (enforce minimum answer length, prohibit duplicates, etc.). For detailed instructions on how to configure these settings, refer to Section 5.5.4 Questions Policy.
- **Prevent answer-guessing** so that an account is locked after a certain number of invalid answers entered during a self-service password management operation. For details refer to Section 5.3 Configuring the Managed Domains.
- **E-mail Notifications**: account owners and/or administrators, whose e-mails are listed in the alerts configuration section, are warned by e-mail if someone tries to perform a self-service operation against their account. For detailed instructions on how to configure these settings, refer to Section 5.5.7 Alerts.
- **Audit Trail**: the product creates full audit trail reports on all user account activities. It is recommended to review these reports regularly. For more information, refer to the Help-Desk Portal help.

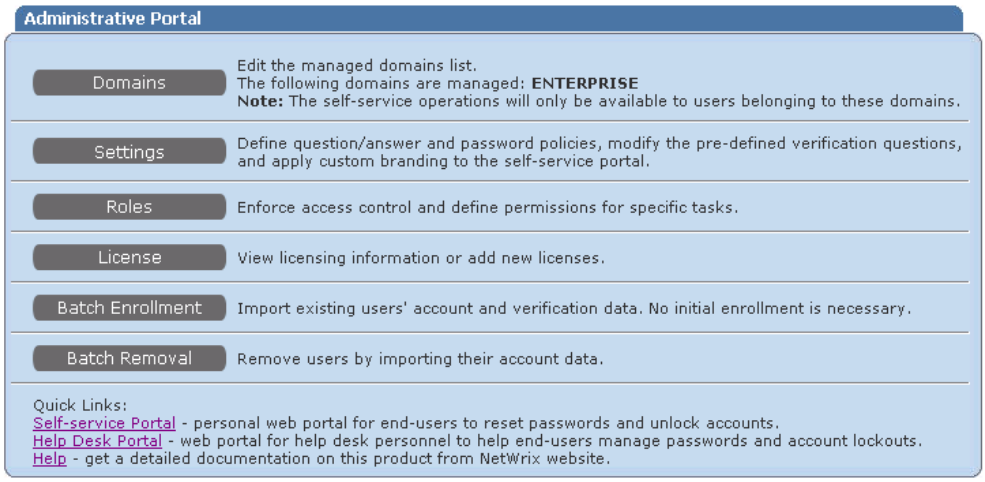
5. CONFIGURING PASSWORD MANAGER SETTINGS

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, and so on). However, you can always modify the default configuration settings when needed through the Administrative Portal.

5.1. Accessing the Administrative Portal

To access the Administrative Portal, go to **Start → All Programs → NetWrix → Password Manager → Administrative Portal** on the computer where NetWrix Password Manager is installed. The Administrative Portal web application will open in the default web browser:

Figure 22: Administrative Portal



Note: If the web page cannot be displayed due to authentication problems, add the Password Manager site to the Local Intranet zone: navigate to **Start → Control Panel → Internet Options**. In the **Internet Properties** dialog select the **Security** tab. Select **Local Intranet**, click the **Sites** button and add the Administrative Portal URL to the list.

5.2. Configuration Options Overview

The Administrative Portal supports the following configuration options:

- **Domains**: allows adding, removing or modifying domains in the managed domains list. For details, refer to Section 5.3 Configuring the Managed Domains.
- **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.

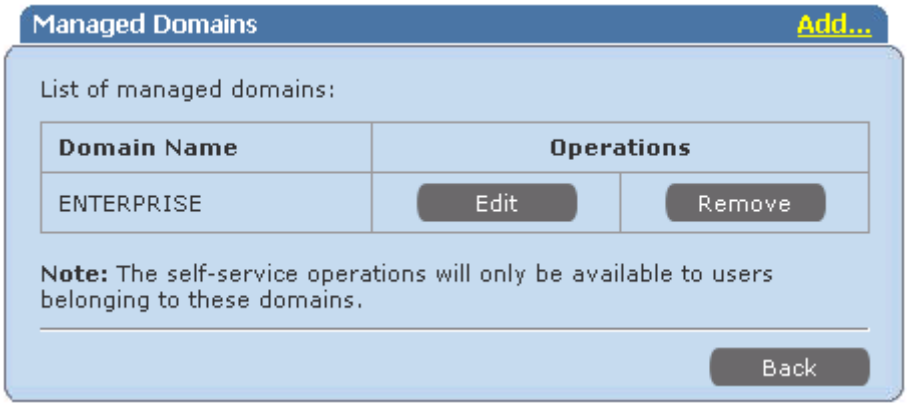
For details on the configuration settings, refer to Section 5.5 Customizing the Self-Service Portal.

- **Roles**: allows assigning different roles to users (Administrators / Help-Desk Operators / Self-Service Access). For details, refer to Section 5.6 Assigning Roles.
- **License**: allows managing product licenses. For details, refer to Section 2.4 Licensing Information.
- **Batch Enrollment**: allows administrators to enroll users by importing their account information from a file. For details, refer to Section 6.3 Batch Enrollment.
- **Batch Removal**: allows administrators to remove users in a batch by importing their account information from a file. For details, refer to Section 6.4 Batch Removal.

5.3. Configuring the Managed Domains

To configure the managed domains, click **Domains** on the Administrative Portal main page. The following page will be displayed:

Figure 23: Managed Domains



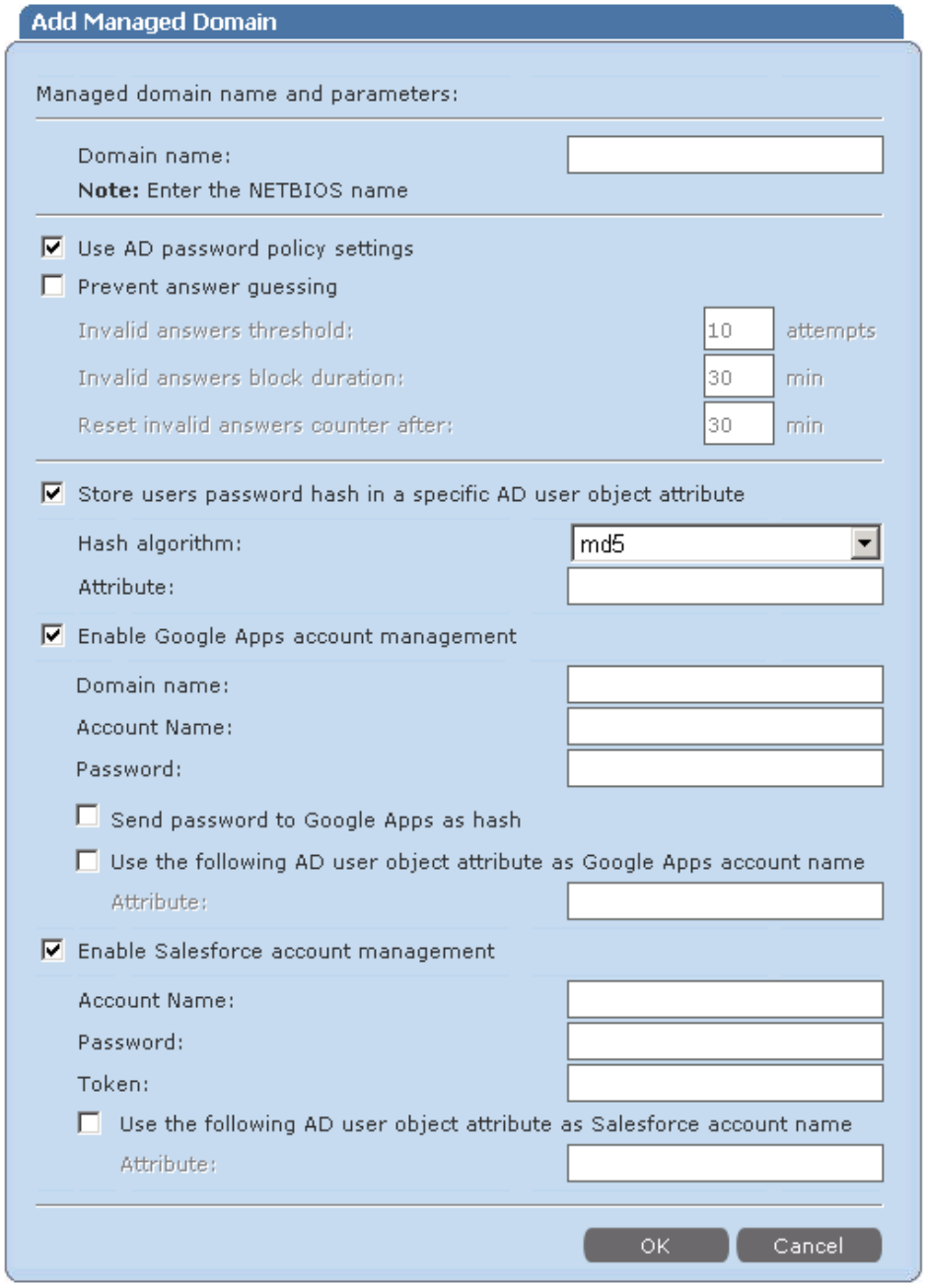
You can do the following:

- Add a domain to the list of managed domains
- Edit the settings for an existing domain
- Remove a domain from the list of managed domains

Procedure 17. To add a domain

1. Click the **Add** link on top of the **Managed Domains** page. The **Add Managed Domain** page will be displayed:

Figure 24: Add Managed Domain



2. Specify the following parameters:

Table 3: Managed Domain Parameters

Parameter	Description
Domain name	Target domain NETBIOS name
Use AD password policy settings	Select this check box if you want Password Manager to apply the effective Active Directory password policy settings instead of its custom policy. **NOTE:** If the custom policy is stricter than the AD password policy, it will override the AD settings.
Prevent answer guessing	Select this check box to enforce limitations on invalid attempts to answer the verification questions: • Invalid answers threshold: determines how many invalid answers are allowed before the account is blocked.

	• Invalid answers block duration: determines the period of time during which the user who failed to answer the authentication questions cannot reset or unlock their account. • Reset invalid answers counter after: determines the period of time after which the invalid answers counter will be reset.
Store users password hash in a specific AD user object attribute	Select this check box if you want Google Apps passwords to be stored securely in one of the user object attributes. • Hash algorithm • Attribute
Enable Google Apps account management	Select this check box to allow users to manage their Google Apps accounts together with their domain accounts (all password resets will be applied to both accounts). Specify the following parameters: • Domain name as defined in Google settings. • Account Name: Google Apps admin account name. **NOTE**: Just the admin account name must be specified, without '@<domain_name>', for example, 'administrator'. • Password of the Google Apps admin account. For the **Google Apps account management** option, additional configuration is required. For details refer to Section 5.3.1 Configuring Google Apps Settings. **NOTE**: Google Apps accounts cannot be monitored separately, without having the corresponding AD accounts.
Send password to Google Apps as hash	Select this check box to send password to Google Apps as hash.
Use the following AD user object attribute as Google Apps account name	Select this check box if you want the specified attribute value to act as Google account name.
Enable Salesforce account management	Select this check box to allow users to manage their Salesforce accounts together with their domain accounts (all password resets will be applied to both accounts). Specify the following Salesforce account parameters: • Account Name • Password • Token
Use the following AD user object attribute as Salesforce account name	Select this check box if you want the specified attribute value to act as Salesforce account name.

3. Click **OK**. The new domain will appear in the managed domains list.

Procedure 18. To edit a domain

1. Select the domain you want to edit in the **Managed Domains** page and click **Edit**. A page will be displayed showing the selected domain's parameters.
2. Modify the necessary parameters and click **OK**.

Procedure 19. To remove a domain

- Select the domain you want to remove in the Managed Domains page and click **Remove**. The selected domain will be removed from the list of managed domains.

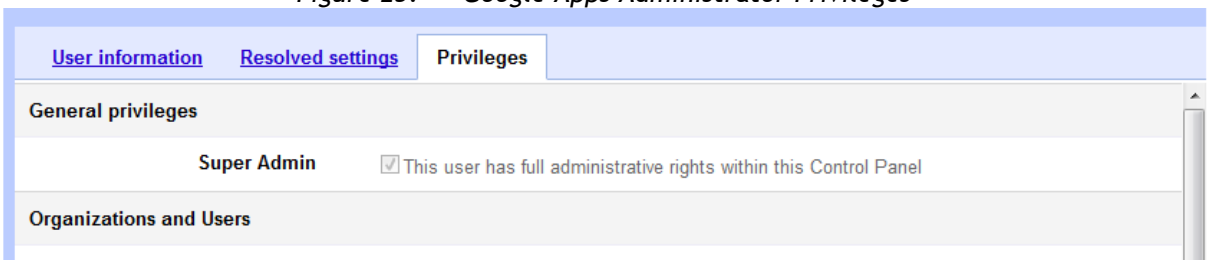
5.3.1. Configuring Google Apps Settings

For the Google Apps account management feature to function properly, some additional configuration of Google Apps is required. Please perform the following procedure if you have enabled this option:

Procedure 20. To configure Google Apps

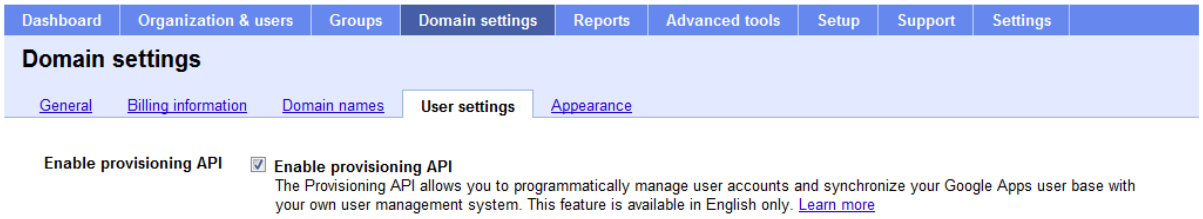
1. Open **Google Apps** and select **Organizations & users** from the top menu.
2. Click the admin account name you entered in the Password Manager Administrative Portal when adding a managed domain.
3. Select **Privileges** and make sure the **Super Admin** check box is selected:

Figure 25: Google Apps Administrator Privileges



4. Select **Domain settings** from the top menu. Navigate to **User settings** and make sure that the **Enable provisioning API** option is selected:

Figure 26: Google Apps Domain Settings



5. Click **Save changes**.

5.4. Editing Email Notification Templates

Procedure 21. To edit email notification template

1. Navigate to the **Templates** folder with all product templates, which is by default stored in the program installation folder: C:\ProgramFiles(x86)\NetWrix Password Manager.
2. Select the required template name basing on the following criteria:
   - Which operation this notification is for:
     - **Action**: a notification is sent for additional user's authentication if the **Enable additional authentication using the user email** check box is selected on the **Authentication Policy** tab of the Administrative portal.
     - **Change**: a notification is sent on an account password change.
     - **Enroll**: a notification is sent when an account has been enrolled with NetWrix Password Manager to enable self-service account management.
     - **Reset**: the notification is sent on a successful or failed account reset attempt. The attempt result is shown in the **Result** field of the notification.
     - **Unlock**: the notification is sent on of a successful or failed account unlock attempt. The result of this attempt is shown in the **Result** field of the notification.
     - **Verification**: the notification is sent in case of a failed self-service operation attempt with the failure reason specified as "Invalid verification answers".
   - Which part of the notification you want to edit - subject or body:
     - to edit an email subject, select a template containing "subject" in its name
     - to edit an email body, select a template containing "body" in its name
   - Who the notification recipients are - administrators or users:
     - for the notification sent to administrators, select the required template with the "_adm" ending in its name
     - for the notification sent to the users whose action triggered an email delivery, select the required template without the "_adm" ending in its name
   - Finally, select a template for the required language:
     - **English:** this is the default language, templates do not have any special labels in their names.
     - **German:** templates in German have names ending with "de"
     - **French**: templates in French have names ending with "fr"
     - **Japanese:** templates in Japanese have names ending with "jp"
     - **Korean:** templates in Korean have names ending with "ko"
     - **Russian:** templates in Russian have names ending with "ru"
     - **Chinese:** templates in Chinese have names ending with "zh"

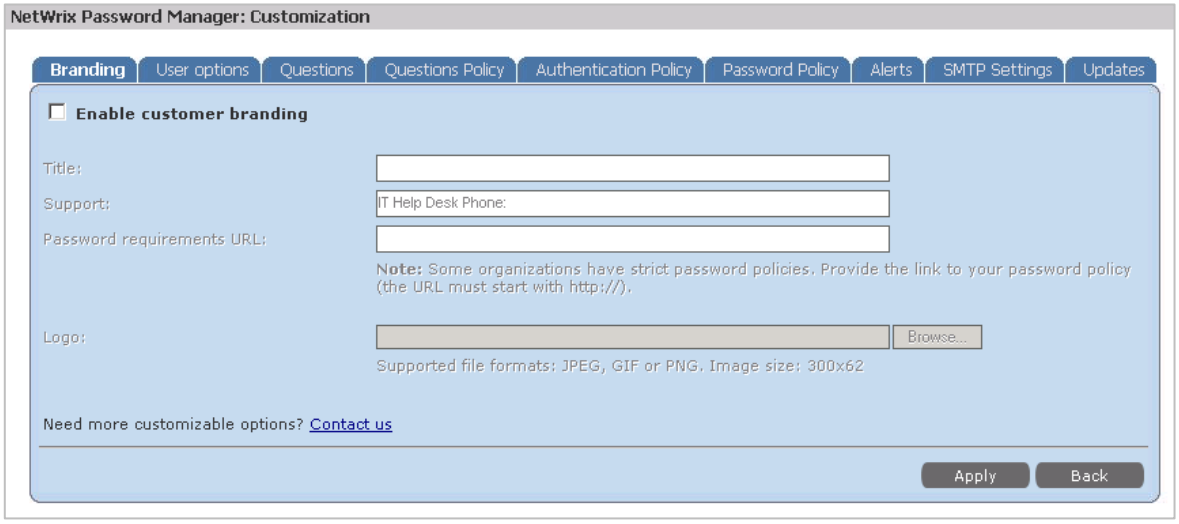
   Example: the template name: "reset_body_template_adm"
3. Edit the required template in Notepad and save the changes.

5.5. Customizing the Self-Service Portal

The Self-Service Portal allows users to perform password management operations, such as password reset, account unlock, and so on.

To customize the Self-Service Portal, click **Settings** on the Administrative Portal main page. The following page will be displayed:

Figure 27: Customization Tabs



Administrators can configure the following settings for the Self-Service Portal:

- Branding
- User Options
- Questions
- Questions Policy
- Authentication Policy
- Password Policy
- Alerts
- SMTP Settings
- Updates

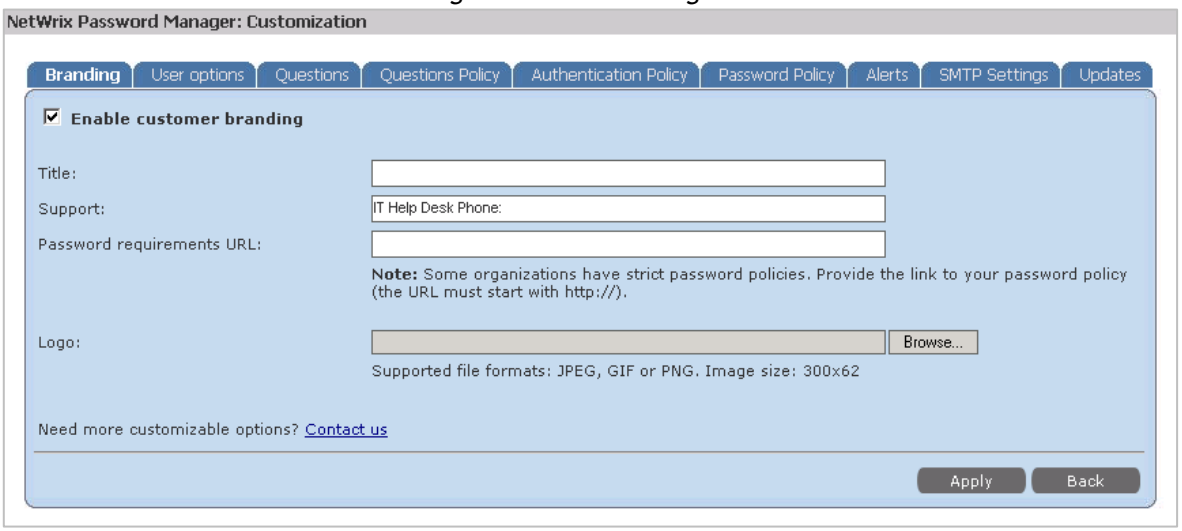
5.5.1. Branding

This option allows customizing the appearance of the Self-Service Portal and personalizing its interface by adding company-specific information (such as company logo, support information and link to a web-page with password policies).

Procedure 22. To configure branding

1. Select the **Branding** tab in the Self-Service Portal customization page. The following page will be displayed:

Figure 28: Branding Tab



2. Select the **Enable Customer Branding** option and specify the following parameters:

Table 4: Branding Parameters

Parameter	Description
Title	Specify your company name as it should appear in the Self-Service Portal.
Support	Enter the phone number or a hyperlink to reach your company's technical support.
Password requirements URL	Specify the URL of the web page where your company's password policies are explained.
Logo	Upload a file with your company's logo that will be displayed in the Self-Service Portal.

3. Click **Apply** to save the changes.

Note: In order to avoid any issues with adding the custom logo, disable UAC (User Account Control) via local security policy.

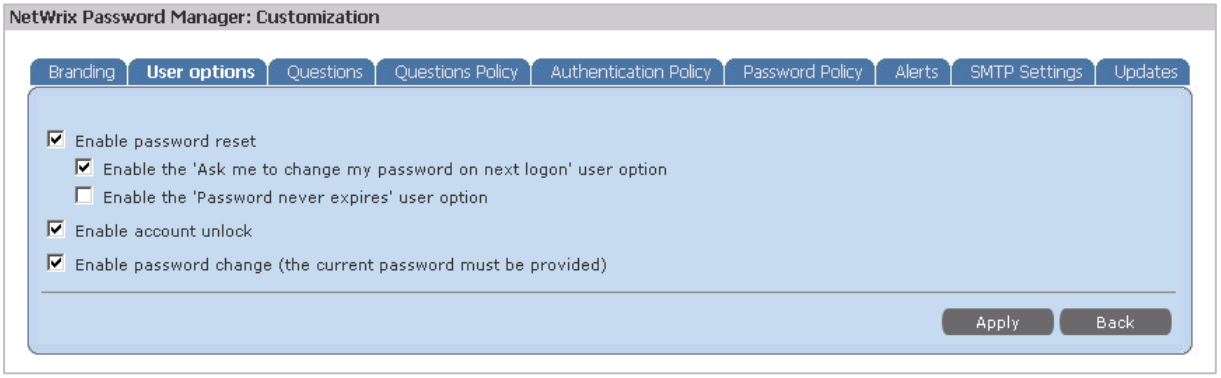
5.5.2. User Options

This option allows enabling or disabling certain features available to end users from the Self-Service Portal or the Password Manager Client (Windows Logon Prompt Extension).

Procedure 23. To configure user options

1. Select the **User Options** tab in the Customization section of the Administrative portal. The following page will be displayed:

Figure 29: User Options Tab



2. Select or clear the following user options:

Table 5: User Options

Parameter	Instruction
Enable password reset	Select this check box to allow users to reset their passwords in the Self-Service Portal.
Enable the 'Ask me to change my password on next logon' user option	Select this check box if you want to allow users to select this option when resetting their passwords.
Enable the 'Password never expires' user option	Select this check box to allow users to decide if they want their passwords to be valid for an unlimited period of time.
Enable account unlock	Select this check box to allow users to unlock their accounts in the Self-Service Portal.
Enable password change	Select this check box to allow users to change their passwords in the Self-Service Portal.

3. Click **Apply** to save the changes.

5.5.3. Predefined Questions

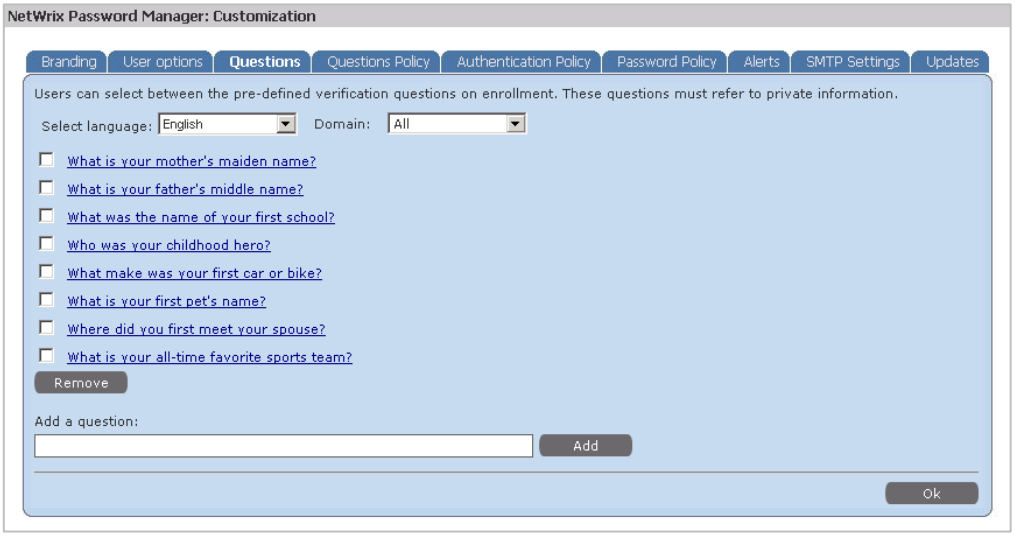
The *reset password* and *unlock account* self-service operations require answering identity verification questions as a secure authentication mechanism. When enrolling into the system, users must answer a set of verification questions. When a user has correctly answered these questions, they receive an email with a link to the password reset operation. The answers are stored separately for each user in the account database.

Administrators can configure which verification questions a user will be asked. A set of questions can be applied to a single domain, or to all managed domains.

Procedure 24. To configure questions

1. Select the **Questions** tab in the Self-Service Portal customization page. The following page will be displayed:

Figure 30: Questions Tab



2. If necessary, select the language from the drop-down list.
3. Select the domain to which this set of predefined questions will be applied. If you want to apply the selected questions to all managed domains, select **All**.
4. Select the questions that users will be asked by ticking the corresponding check boxes.
5. You can edit a question by clicking on it, or remove a question from the list by selecting the corresponding box and clicking **Remove**.
6. To add a new custom question to the list, type it in the **Add a question** entry field, and click **Add**.
7. Click **OK** to save the changes.

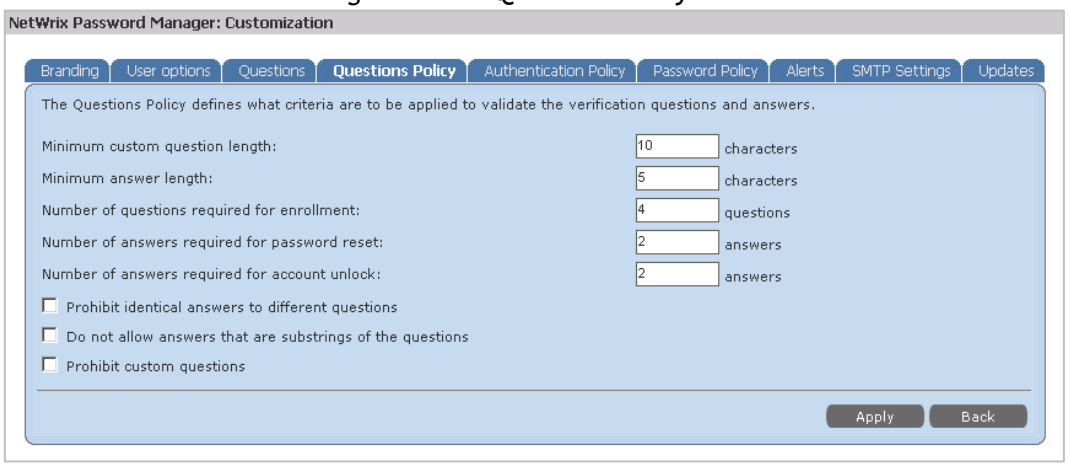
5.5.4. Questions Policy

This option allows applying constraints to verification questions and answers.

Procedure 25. To configure questions policy

1. Select the **Questions Policy** tab in the Customization section of the Administrative portal. The following page will be displayed:

Figure 31: Questions Policy Tab



2. Specify the following parameters:

Table 6: Questions Policy Parameters

Parameter	Description
Minimum custom question length	Specify the minimum number of characters a custom user-defined question must contain.
Minimum answer length	Specify the minimum number of characters an answer must contain.
Number of questions required for enrollment	Specify the number of questions a user must answer during the enrollment procedure.
Number of answers required for password reset	Specify the number of correct answers that a user must give to perform the password reset operation.
Number of answers required for account unlock	Specify the number of correct answers that a user must give to perform the account unlock operation.
Prohibit identical answers to different questions	Select this option to prevent users from providing the same answers to different questions. This option is recommended for security reasons.
Do not allow answers that are substrings of the questions	Select this option to prevent users from providing answers that are identical to the question or its part. This option is recommended for security reasons.
Prohibit custom questions	Select this option if you want to prohibit users to create their own custom questions on enrollment.

3. Click **Apply** to save the changes.

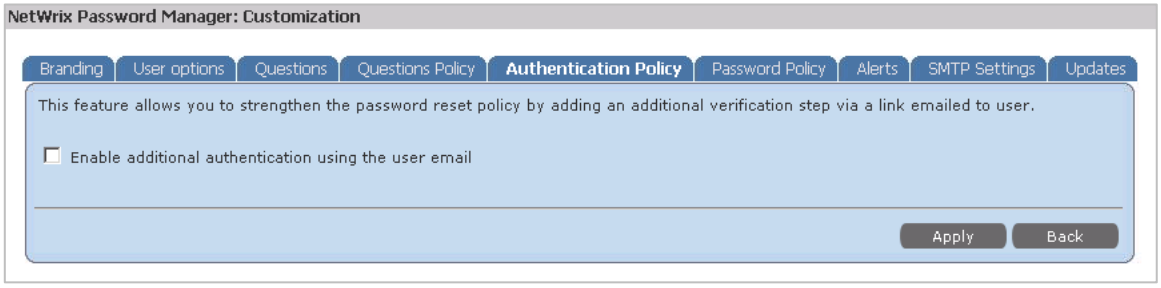
5.5.5. Authentication Policy

The Authentication Policy option allows you to strengthen the password reset policy by adding an additional verification step via a link emailed to users.

Procedure 26. To enable authentication policy

1. Open the **Authentication Policy** tab in the Self-Service Portal customization page. The following page will be displayed:

Figure 32: Authentication Policy Tab



2. Select the **Enable additional authentication using the user email** check box to enable the option.

5.5.6. Password Policy

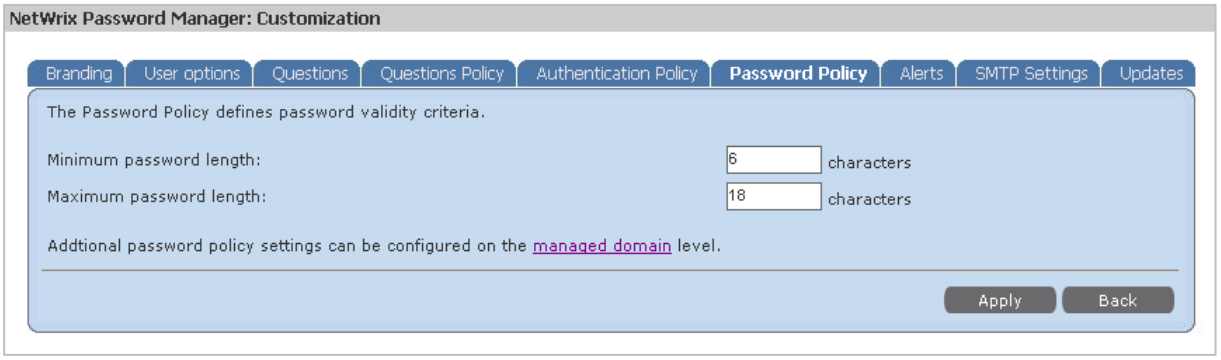
This option allows applying limitations on password length.

Note: These settings apply to all managed domains. For details on how to apply AD password settings to a single domain, refer to Section 5.3 Configuring the Managed Domains. Note that if the AD password policy is less strict than the password settings specified in the Password Manager Administrative Portal, it will be overriden.

Procedure 27. To configure password policy

1. Select the **Password Policy** tab in the Self-Service Portal customization page. The following page will be displayed:

Figure 33: Password Policy Tab



2. Specify the minimum and maximum allowed password length and click **Apply** to save the changes.

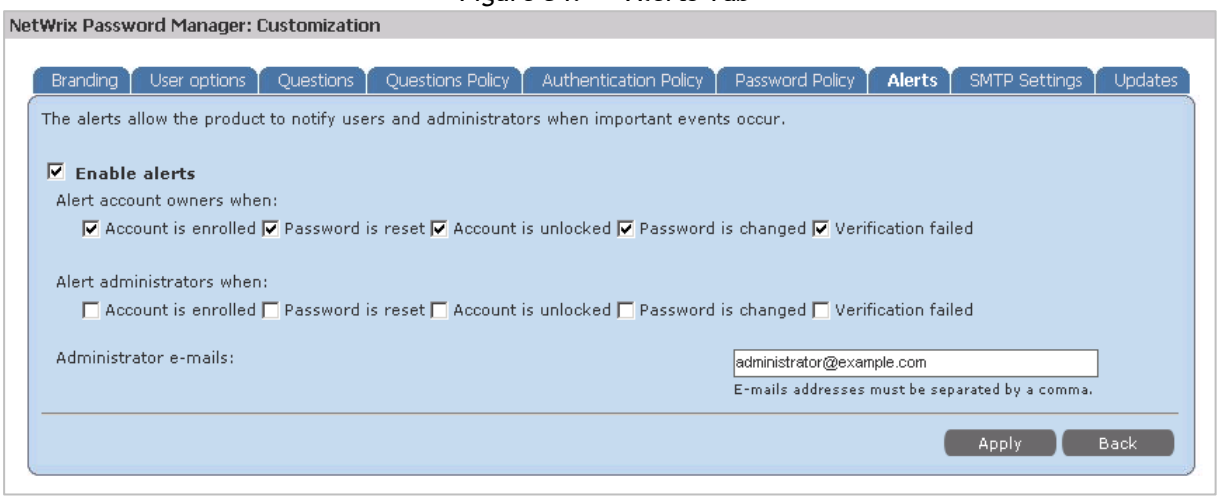
5.5.7. Alerts

This option allows configuring Password Manager to send email notifications triggered by certain events related to user accounts.

Procedure 28. To configure alerts

1. Select the **Alerts** tab in the Customization section of the Administrative portal. The following page will be displayed:

Figure 34: Alerts Tab



2. Specify the following parameters:

Table 7: Alerts Parameters

Parameter	Description
Enable alerts	Select this option to enable e-mail notifications.
Alert account owners when	Select the events that you want account owners to be notified about.
Alert administrators when	Select the events that you want administrators to be notified about.
Administrator e-mails	Enter administrator(s)' email addresses that you want notifications to be sent to. Addresses must be separated by a comma.

3. Click **Apply** to save the changes.

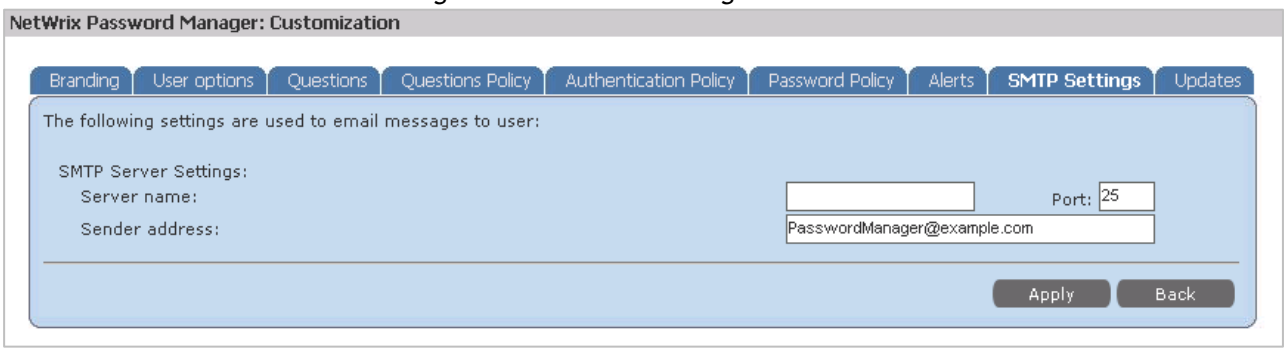
5.5.8. SMTP Settings

This option allows configuring the SMTP settings for email delivery.

Procedure 29. To configure SMTP Settings

1. Select the **SMTP Settings** tab in the Customization section of the Administrative portal. The following page will be displayed:

Figure 35: SMTP Settings Tab



2. Specify the following parameters:

Table 8: SMTP Settings

Parameter	Description
Server name	Specify the SMTP server name.
Port	Specify the SMTP server port.
Sender address	Specify the address that will appear in the 'from' field in the email notifications.

3. Click **Apply** to save the changes.

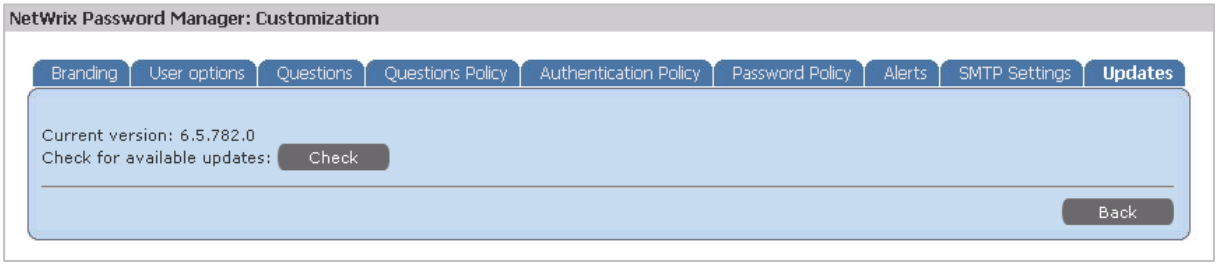
5.5.9. Updates

This option allows checking if your NetWrix Password Manager version is the latest one, or if a more recent product version is available.

Procedure 30. To check for updates

1. Select the **Updates** tab in the Customization section of the Administrative portal. The following page will be displayed:

Figure 36: Updates



2. Click the **Check** button to see if updates are available.

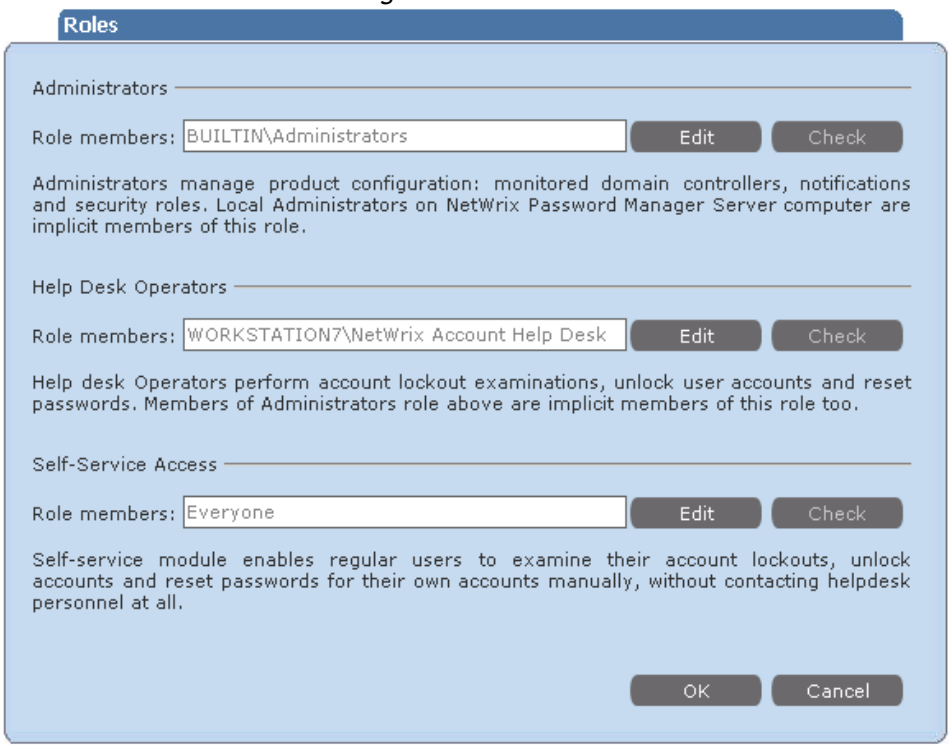
5.6. Assigning Roles

This configuration option allows assigning different roles (Administrators, Help-Desk Operators, Self-Service Access) to account owners.

Procedure 31. To assign roles to users

1. Click **Roles** in the Administrative Portal main page. The following page will be displayed:

Figure 37: Roles



2. Click **Edit** to modify the list of account owners to whom a role is assigned. Account names must be separated by a semi-colon. To verify if the account names you specified are valid, click **Check**.
3. Click **OK** to save the changes.

6. Enrolling Users for Self-Service

Before users can perform any password management operations in the self-service mode, they must enroll into the system.

NetWrix Password Manager supports the following three enrollment options:

- **Manual enrollment**: users must go to the Self-Service Portal and perform the enrollment procedure. For details, see section 6.1 Manual Enrollment.
- **Automatic enrollment**: users are automatically prompted to enroll into the system at logon. For details, see Section 6.2 Automatic Enrollment.
- **Batch enrollment**: administrators can pre-enroll users based on existing account and verification data (for example, taken from the HR database). For details, see Section 6.3 Batch Enrollment.

6.1. Manual Enrollment

Manual enrollment is performed by users in the Self-Service Portal.

After you have deployed and configured NetWrix Password Manager, you must send an introductory email message to end users explaining the purpose of the system and containing brief instructions on how to use it and the Self-Service Portal URL. You must instruct users to follow the link and perform the enrollment procedure before they can perform any password management operations.

The main advantage of this enrollment option is that no client software deployment is required.

However, many users will not follow the link (they may be too busy, or may not understand the importance of this action), which will result in additional help-desk calls when they face account issues.

6.2. Automatic Enrollment

Automatic enrollment takes place if the Password Manager Client Application has been deployed on end users' computers.

The first time users log on to their computers after the deployment, an **Enrollment Wizard** will pop up automatically, forcing them to enroll into the system.

The main advantage of this enrollment option is that it will minimize the number of help-desk calls.

If you do not want to deploy Password Manager Client on end users' computers, you can still enforce automatic enrollment through Group Policy scripts. To do this, perform the following procedure:

Procedure 32. To enforce automatic enrollment through Group Policy

1. Temporarily install the Password Manager Client on any computer.
2. Copy the prmmain.exe file (located in the installation folder) and the .dll language files that you are going to use to a file server share that can be accessed by all users, for example, \\pmserver\Enroll\prmmain.exe.
3. Open the **Default Domain Policy** or create a new Group Policy object using the standard Microsoft tools - GPMC or ADUC (Active Directory Users and Computers).

4. Navigate to **User Configuration → Windows Settings → Scripts (Logon/Logoff)** and add a new logon script that starts prmmain.exe without any arguments.
5. Through GPO, set the following Windows registry value on the client machines:
6. HKLM\SOFTWARE\Policies\NetWrix\PasswordManager
   PRM_Server=<Self_Service_Portal_URL>, for example http://corp.local/pm.

   Note: Make sure that this URL is accessible from the client machines.
7. Alternatively, you can use the netwrixpm.adm file to distribute this value. To do this, execute the following steps:
   - Start the GPMC by going to **Start → Control Panel → Administrative Tools → Group Policy Management**.
   - Locate the OU (or the entire domain) that your client machines belong to and the Password Manager GPO (if you have not created it previously, you can do it now by right-clicking the OU and selecting the **Create and Link a GPO Here** option).
   - Right-click the GPO and select **Edit** to start the Group Policy Object Editor.
   - Navigate to the **Computer Configuration → Administrative Templates** node, right-click it and select the **Add/Remove Templates** option. Click **Add** and browse to the netwrixpm.adm file (by default installed to C:\ProgramFiles\NetWrix Password Manager).
   - Navigate to the **Computer Configuration → Administrative Templates → NetWrix Password Manager** node and double-click **Installation URL** in the right pane. Select the **Enabled** option, and enter the Self-Service Portal URL.

6.3. 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.

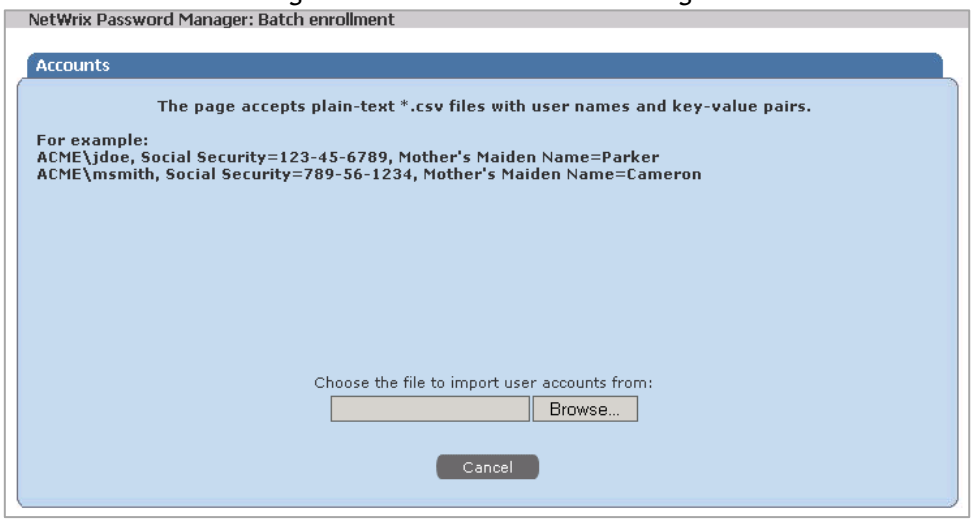
This way you can ensure that all users are enrolled for self-service, which minimizes the load on the help-desk.

To import user account data from a file for batch enrollment, perform the following procedure:

Procedure 33. To enroll users by importing their account data

1. Click **Batch Enrollment** on the Administrative Portal main page. The following page will be displayed:

Figure 38: Batch Enrollment Page



2. Select the file that you want to import account data from, and click **Next**.

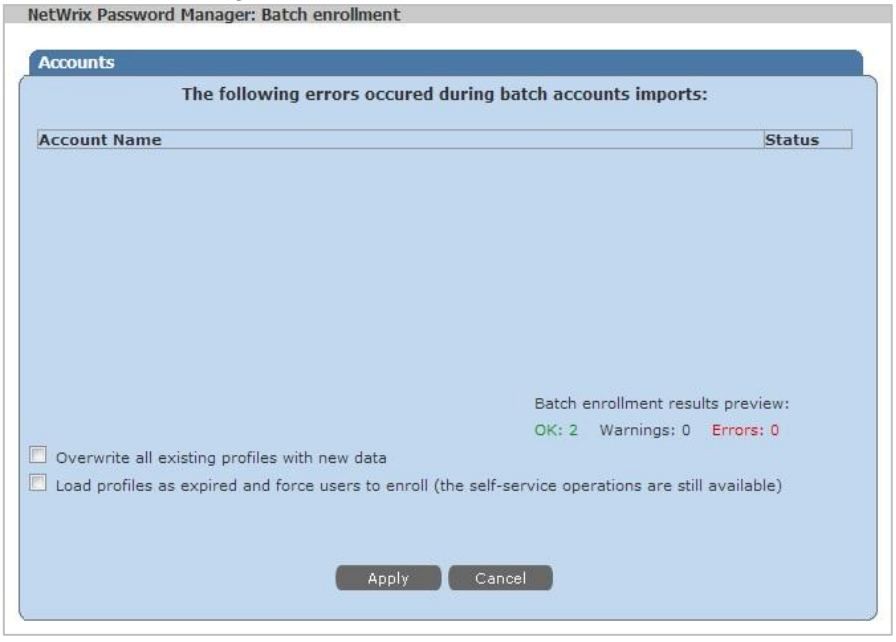
   Note: Plain-text Unicode .csv files are accepted containing user names and key-value pairs. For example:

   ```
   ACME\jdoe, Social Security=123-45-6789, Mother's Maiden
   Name=Parker

   ACME\msmith, Social Security=789-56-1234, Mother's Maiden
   Name=Cameron
   ```

3. The results of the operation will be displayed:

Figure 39: Batch Enrollment Results



4. Select one of the following options:

   - **Overwrite all existing profiles with new data** if the data you imported contains more relevant and up-to-date information than the existing records.
   - **Load profiles as expired and force users to enroll (the self-service operations are still available)**. This option is recommended for security reasons.

5. Click **Apply** to save the changes.

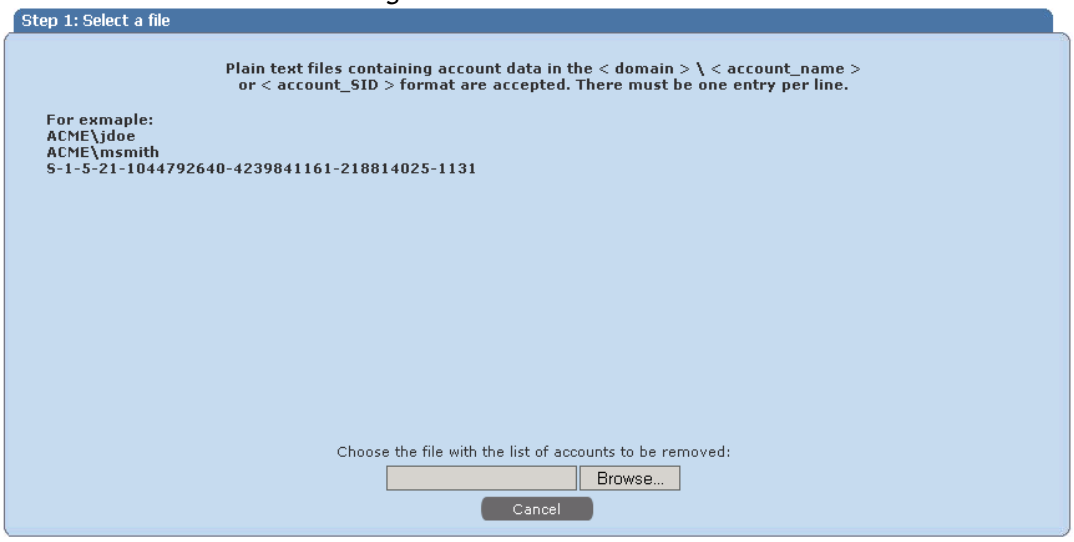
6.4. Batch Removal

This feature enables administrators to import a file with a list of users to be removed, instead of removing each separate user manually.

Procedure 34. To remove users by importing their account data

1. Click **Batch Removal** on the Administrative Portal main page. The following page will be displayed:

Figure 40: Batch Removal



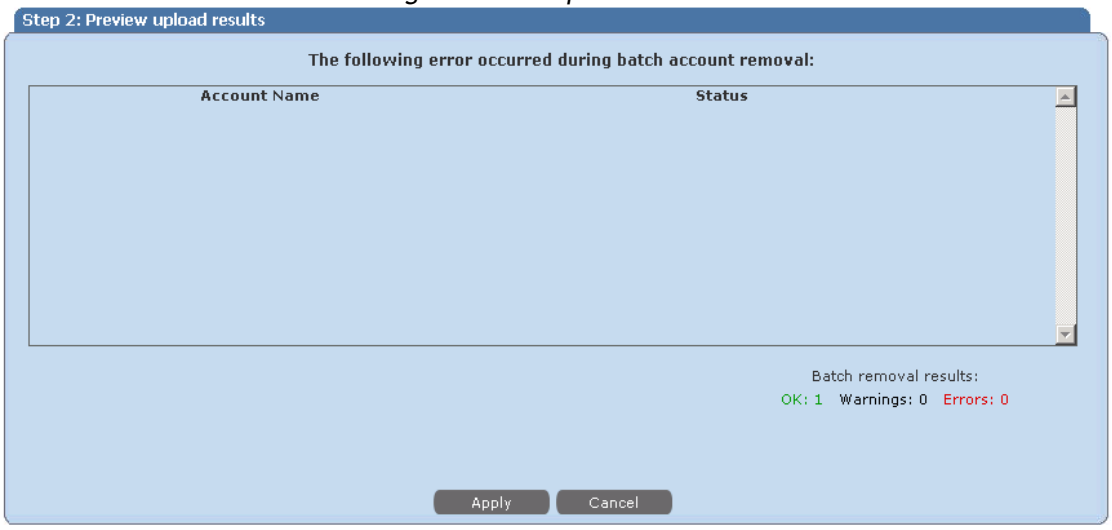
2. Select the file with the list of accounts to be removed, and click **Next**.

Note: Plain-text files are accepted containing user account data in the <domain>\<account_name> or <account_SID> format. For example:

```
ACME\jdoe
ACME\msmith
S-1-5-21-1044792640-4239841161-218814025-1131
```

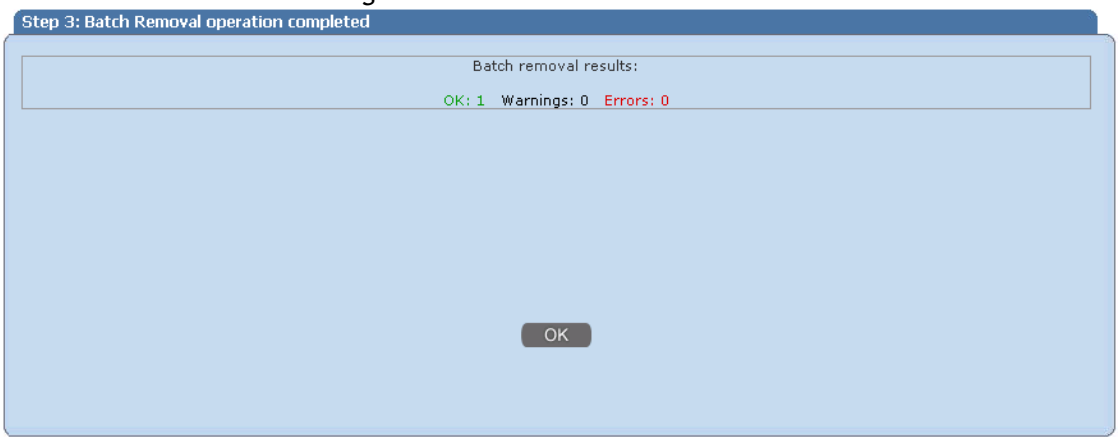
3. On the next step, preview the upload results:

Figure 41: Upload Results



4. To proceed with batch removal, click **Apply**. Review the results of the operation, and click **OK**:

Figure 42: Batch Removal Results



7. TROUBLESHOOTING NETWRIX PASSWORD MANAGER

This chapter lists the issues that you may encounter while using NetWrix Password Manager, and suggests a workaround to resolve them.

7.1. Error 401

7.1.1. Issue Description

When the Logon Prompt Extension tries to start, the following error occurs on the end user's computer:

```
Automatic user enrollment failed: Unauthorized (Error code: 401,
URL: http://mywebserver/pm/gina_isprofilecreated.asp)
```

7.1.2. How to Fix

Make sure through Group Policy that the Password Manager Self-Service Portal URL is present in the Local Intranet zone. To do this, execute the following steps:

1. Use the **Group Policy Object Editor** to open the GPO that manages the deployment of the Password Manager Client to the domain.
2. Navigate to the **User Configuration** → **Administrative Templates** → **Windows Components** → **Internet Explorer** → **Internet Control Panel** → **Security Page** node.
3. Open the properties of the **Site to Zone Assignment List** entry in the right pane.
4. In the dialog that opens, select **Enabled** and click **Show**.
5. In the **Show Contents** dialog box, click **Add**. Add the Self-Service Portal URL and set the value 1 (Intranet Sites zone). Then click **OK**.

Note: Client computers must be restarted in order for these changes to take effect.

The same configuration can be created using the registry. This is useful, for example, if you want to create offline images for remote employees who are not affected by Group Policy. To do this, execute the following steps:

1. Navigate to:

   HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains.
2. Create a key with the same name as your domain name (for instance, example.com).
3. Under the newly created key, create a child key with the same name as your server name (for instance, if the full name is myserver.example.com the value name is myserver).
4. Create a DWORD value named https and set it to 1.
5. Repeat the operation for

   KEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains.

A APPENDIX: SUPPORTING DATA

A.1 NetWrix Password Manager Registry Keys

This section contains a description of NetWrix Password Manager registry keys, their types and values. If you want to modify the product's settings for which these keys are responsible, create the corresponding key in HKEY_LOCAL_MACHINE\SOFTWARE\NetWrix\Password Manager and set its value. Otherwise, the settings correspond to the key's default value.

Note: Incorrect modification of registry keys may lead to the product's incorrect behavior or failure.

Table 9: NetWrix Password Manager Registry Keys

Registry Key	Type	Description/Value
HKEY_LOCAL_MACHINE\SOFTWARE\NetWrix\Password Manager		
loglevel	REG_DWORD	Used to include detailed information into the product log. 100 – include detailed information 0 – do not include detailed information
AllowRemoveByHelpdesk	REG_DWORD	Used to enable users that belong to the Help-Desk Operators role to delete users from the Help-Desk Portal. 1 – allow 0 – do not allow
PRM_SuppressEnrollmentErrors	REG_DWORD	Used to disable appearance of error messages on the system autorun. 1 – disable 0 - do not disable
PRM_SuppressLaterEnrollment	REG_DWORD	Used to prevent users from closing the enrollment wizard until they complete the enrollment procedure. 1 – prevent closing the wizard 0 – do not prevent closing the wizard

A.2 Related Documentation

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

Table 10: Product Documentation

Document Name	Overview
NetWrix Password Manager Administrator's Guide	The current document.
NetWrix Password Manager Quick-Start Guide	Explains how to quickly install and configure NetWrix Password Manager, and provides step-by-step instructions for some basic password management operations. This guide can be used for evaluation purposes.

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.