myPassword

Administrator's Guide

namescape

Copyright © 2004-2018 Namescape Corporation

5110 N 40th St

Suite P100

Phoenix, Arizona 85018

www.namescape.com

Trademarks

Namescape® rDirectory®, myPassword® and Password Policy Guardian™ are registered trademarks of the Namescape Corporation or its assigns. All other trademarks used or referred to in the document are the property of their respective owners.

Proprietary Rights

Namescape has prepared this document for use by Namescape personnel, agents, licensees and customers. The information contained in this document is the property of Namescape. You may not reproduce, translate or transmit it in any form or by any means, electronically or mechanically, without prior written permission from Namescape.

Disclaimer of Liability

Namescape makes no representation or warranties of any kind, either expressed or implied, with respect to the contents of this manual, including but not limited to typographical errors and technical completeness. Namescape reserves the right to revise this publication and to make changes in its content without obligation to notify any person of such revision or changes.

Document Revision History

myPassword 3.0	January, 2011
myPassword 3.1	October, 2011
myPassword 3.2	December, 2011
myPassword 3.3	May, 2012
myPassword 3.4	July, 2012
myPassword 3.5	October, 2012
myPassword 3.7	June, 2013
myPassword 4.0	April, 2014
myPassword 4.2	February, 2016
myPassword 4.2.2	September, 2016

Table of Contents

Overview **7**
Prerequisites 7

myPassword Features **8**
Language Support 8
rDirectory Integration 8
Password Policy Guardian Integration 8
Access Methods 9
Security Features 10
Cross Browser Support 13
Themeable User Interface 13
Customizable Landing Page 13

Configuring myPassword **14**
Log on to rDirectory 14
The Namescape Designer 15
myPassword Administration 16

Accessing myPassword **32**
Access Methods 32
Entry Pages 34
Access Modes and Arguments 36
Customizing the Web Client and Main Menu Landing Page 38

Using myPassword 40
Main Page 40
CAPTCHA 41
Reset my Password 42
Unlock my Account 47
Change my Password 48
Edit my Profile 49
Enforcing Enrollment 50
On rDirectory access 50
On Logon with ProfileValidator.exe 50
Reporting in myPassword 51
Configuring Report Access 51
Using the Report Console 54
Appendix A – Customizing myPassword 59
Client Customization 59
Adding a myPassword link to the Outlook Web Access Logon Page 61
Redirecting the IWA failed logon page to the myPassword site 66
How to change the language in myPassword 68

Overview

This Administrator's Guide covers the configuration and use, but not the installation, of myPassword. For information concerning the installation of myPassword, please refer to:

Installation and Setup Guide for rDirectory and myPassword.pdf

myPassword is designed to work immediately upon installation, provided a default Proxy Account has been configured in the Site Manager.

Because myPassword shares many key technologies with rDirectory, the administration of myPassword is done via the Namescape Designer, accessible through rDirectory. Even if myPassword is the only product licensed, the installation of rDirectory is required. In this case, rDirectory will be limited to only those features needed to administer myPassword.

Prerequisites

The configuration of myPassword requires:

1. An installation of both myPassword and rDirectory.
2. The assignment of a Proxy Account using the Site Manager
3. An Active Directory logon account that can log into rDirectory and has been granted the Namescape Designer role
4. A myPassword license key applied using the Site Manager

For more information on any of these prerequisites, please refer to the installation and setup guide.

myPassword Features

Language Support

myPassword ships with English, German, Spanish and French language support. To display myPassword in one of these languages, simply change your browser settings to display the desired language. If you require a language that is not included, please see *How to Change the Language in myPassword* in Appendix A – Customizing myPassword.

rDirectory Integration

Although myPassword may be licensed and used without rDirectory, the natural synergy of these two products forms an even more powerful password management solution. Combining rDirectory with myPassword provides the following additional benefits:

Help Desk Password Management Solution

With rDirectory integration, you get a complete Help Desk password management solution that allows your help desk staff to quickly locate a user profile and securely verify the user's identity before resetting their password or unlocking their account. Audit logs and email notices record who reset which account and when, and since delegation is done through rDirectory, the Help Desk staff does not require administrator permissions. In addition, features such as group management can also be easily delegated to the Help Desk.

Flexible Delegation of Password Management

The flexible Role Based Access Control (RBAC) model of rDirectory provides many more delegation options than just allowing members of a help desk group to manage everyone's passwords. For example, you can also grant access to manage passwords and accounts based on relationships, such as a user's manager.

Enforced Profile Data Integrity Check

When coupled only with myPassword, the ProfileValidator tool can be configured to require users to fill in their Question and Answer Password Reset Profile upon logon. However, when myPassword is combined with rDirectory, the ProfileValidator tool can also require users to fill in or correct virtually any other attribute in their profiles.

Password Policy Guardian Integration

When Password Policy Guardian is installed alongside myPassword, users will receive an immediate, detailed explanation why a password does not meet the applicable complexity policies in the event a password change or reset fails.

Access Methods

myPassword supports multiple access methods for users who need to reset or change their password.

Windows Logon Form - GINA-Enabled or GINA-Free

Users can access myPassword directly from their Windows Logon Form, using either the GINA-Enabled or GINA-Free access methods. The myPassword GINA.dll will modify the user's Windows Logon Form, providing the user with a convenient, direct link to myPassword, without the need to log on to Windows. However, since using GINA extensions can be problematic in some environments, myPassword also includes a GINA-Free method to access myPassword directly from the Windows Logon Form using a Restricted Access Account.

The Restricted Access Account method is a best practice recommended by Microsoft, and has significant advantages over the traditional GINA.dll method. With a Restricted Access Account, users can log on using these alternate credentials, yet be securely limited to only the myPassword site. The key advantages of this method are centralized management, simplified access for roaming and mobile users, and because a replacement GINA.dll is no longer required, the possibility of a conflict with other authorization extensions, such as biometrics or network drivers, is eliminated.

A Windows Logon Prompt utility is provided when using the GINA-free access method, allowing you to add a custom message to the user's Windows Logon Form, instructing them to log on as the Restricted Access Account when they need to reset their password.

Outlook Web Access Logon Form

A link to myPassword can be added directly to the Outlook Web Access Logon form using the ReturnURL Access Mode. This access method provides remote users with the same access to myPassword as users who log on using the Windows Logon Form. Remote users can edit their Password Reset Profile, unlock their account and change or reset their password.

Portal or Web Pages

Since myPassword is web based, it's easy to integrate into an existing portal or corporate web site. Using the ReturnURL Access Mode, myPassword can be configured to return users to the originating page upon completion of a password modification or inactivity timeout.

Mobile Access

myPassword also includes full support for password management using smartphones or tablets. When the URL is accessed by a phone or tablet browser, myPassword will

automatically detect a mobile device and display the customizable web app, rather than the standard desktop site, without further configuration.

Direct Access Methods

All of the standard direct access methods, such as kiosk or workstation, are also available. The security features of myPassword also allow you to confidently make myPassword available publicly on the internet.

Web Front End

The myPassword Web Front End (WFE) is a simple web client designed to reside on an IIS server located in your DMZ. Coupled to an appropriately configured myPassword Proxy Server located on your internal network, the WFE allows users to change or reset their passwords from the internet, without fear of externally exposing your Active Directory.

Security Features

While a self-service password reset product like myPassword can save countless hours of time for end users and help desk staff, it can also be a target for intruders seeking to take unauthorized control of someone's account. For this reason, myPassword is designed with security in mind and includes the following security features:

Force Two Factor Authentication with External Email Address or SMS

In addition to profile validation, myPassword can force the use of external email verification or SMS validation to a mobile device before a user is allowed to unlock their account or reset their password.

To force these forms of authentication, three conditions must be met in the myPassword configuration:

1. The feature is enabled in the designer.
2. *Deny For Users with No Profile* is enabled (Email verification only).
3. *If Profile Exists, Require Answers* is selected.

If these three conditions are met, a user attempting to unlock their account or reset their password must first answer their profile validation questions. Once the questions have been answered correctly, an email will be generated and sent to an external email address defined on their user account, or an SMS verification code will be sent to the mobile number defined on their user account. The user must click the link in the email or enter the SMS verification code, and only then will they be allowed to perform the **Unlock** or **Reset** action.

Both the SMS number and external email address are encrypted and stored in the Password Reset Profile. Once encrypted, the values will not be viewable by any users.

Intrusion Detection

myPassword incorporates several means of deterring, detecting, and blocking access to intruders who may attempt to use myPassword to gain illicit access to an account. If excessive failures are detected when answering questions or authenticating an account (used in Profile Edit, Password Change, or Vouching), access to myPassword can be restricted by blocking the intruder's IP address, blocking the compromised account, and/or sending email alerts to immediately notify security personnel of a potential attack.

Question Presentation

Questions are presented sequentially for additional security. In other products, all questions are presented on a single page, giving an intruder the opportunity to immediately know the information needed to successfully modify a password. By presenting only a single question at a time, socially engineering answers becomes much more difficult and time consuming.

Inactivity Timer

An inactivity timer provides additional security to myPassword by automatically logging the current user out of myPassword and returning them to the main menu if a keystroke or mouse movement is not detected for a predefined period of time. In kiosk mode, the inactivity timer guarantees myPassword is returned to the main menu when left unattended. If myPassword is using the GINA-free access method with a Restricted Access Account, the inactivity timer will log off of the Restricted Access Account and return to the normal windows logon when the timer expires.

Audit Logging / Email Notification

myPassword records the 'who, what, when, and where' of all myPassword related activity and can be configured to store this valuable data in both the server event logs and the myPassword reporting database.

myPassword can also be configured to send email notifications to the modified account, their manager, or an administrator for additional security. A special email notification is generated when a potential intrusion is detected and can be sent to an administrator or security personnel.

Password Reset Profile Rules

With myPassword, you can create rule sets to apply unique Password Profile Policies to determine the questions and requirements for creating a Password Reset Profile. This allows a more stringent Password Reset Profile requirement for sensitive accounts, while allowing simpler Password Reset Profiles for those with lower security requirements.

Password Generator

An optional Password Generator can be used to automatically create new passwords. By default, the password generation feature uses a customizable dictionary of case-sensitive words that are appended with numbers (and additional words and numbers as necessary) until the minimum password length is obtained. In addition, myPassword can generate a series of random characters for use as a temporary password.

When used with the **Force Password Change on next Logon** setting enabled, the generated password becomes a one-time-use password that can be as complex as required.

When integrated with Namescape's Password Policy Guardian, the password generator will automatically create a password that is compliant with any applicable password policies.

Voucher Rules

Vouching is an optional feature that allows someone who has not completed their Password Reset Profile, or has forgotten their answers, to get another authorized user to vouch for them, allowing their password to be reset. With myPassword, you can set up rules where different users may be allowed different vouchers, and receive different messages to indicate who can vouch for them. Since vouching rules leverage customizable relationship based roles, a voucher may also be based on relationships defined in the directory, such as Manager or any other custom relationship.

Cross Browser Support

myPassword supports the following browsers to reset or change passwords, create Password Reset Profiles, or unlock accounts:

- Microsoft Edge
- Microsoft Internet Explorer 7.0 or later
- Safari 5.0.3 or later
- Mozilla Firefox 3.6.3 or later
- Chrome 8.0 or later
- Opera 10.62 or later

To configure myPassword, the Namescape Designer supports Microsoft Internet Explorer 7.0 or later.

Themeable User Interface

myPassword includes a number of preinstalled themes that allow an administrator to change the element colors in the client with a few clicks. In addition, myPassword also supports custom logos, text and languages.

Customizable Landing Page

The main landing page of the myPassword client may be changed to better suit your business needs. A number of template landing pages are included by default, and new ones may be added by simply creating a new html page and adding it to the templates directory.

Configuring myPassword

The configuration and administration of myPassword is accomplished using the Namescape Designer, included with the rDirectory and myPassword installation. To configure myPassword, log on to the rDirectory website with an account that has been granted the Namescape Designer role.

Log on to rDirectory

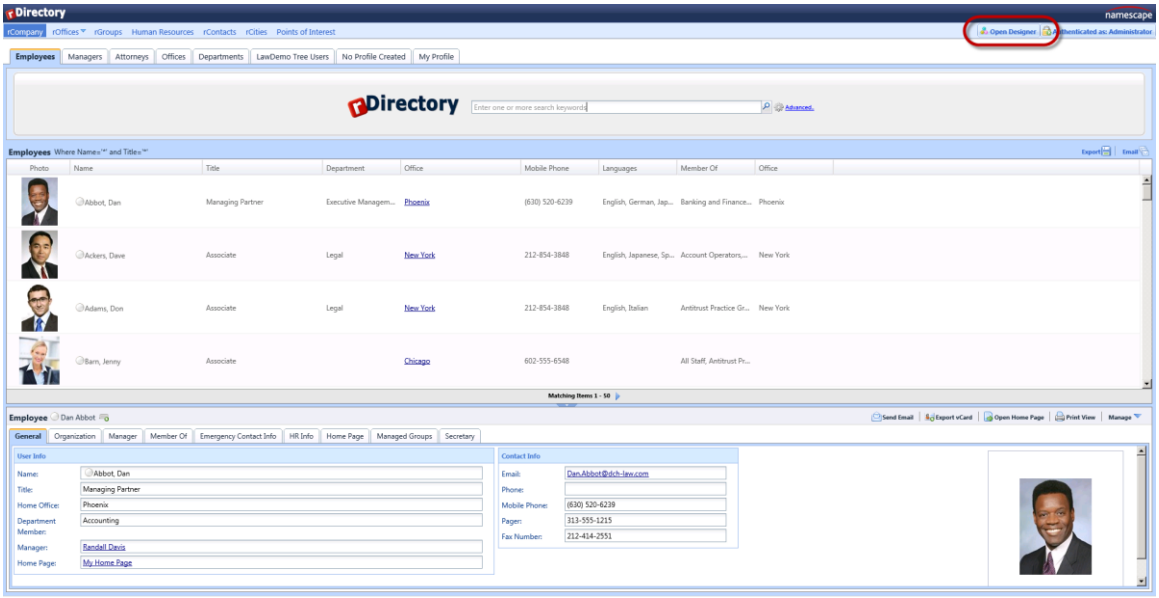
If **Forms Authentication** is configured for the rDirectory website using the Site Manager, you will see the above logon screen when the site is accessed. If **Windows Authentication** is configured for the rDirectory website, you will not see the logon screen and will be automatically authenticated.

In either case, you are required to log on with an account that has been granted the Designer role in the site manager.

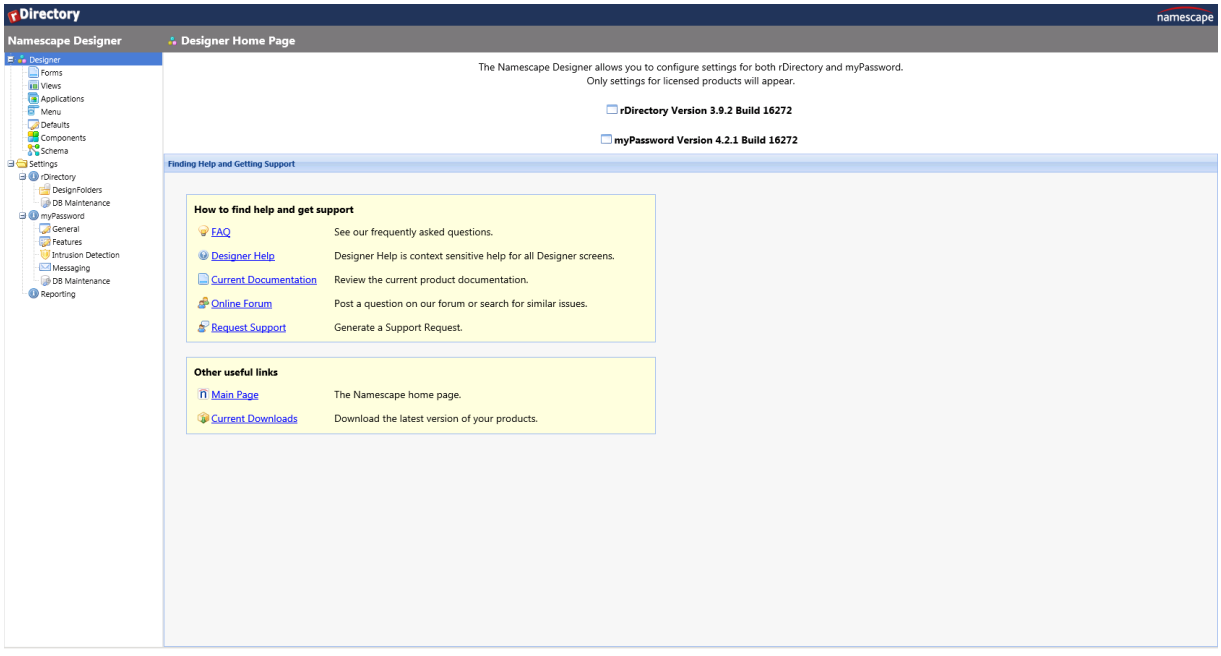
NOTE: *If rDirectory is not licensed, you will be immediately redirected to the Namescape Designer after authentication and presented with a partial Designer view containing only the tree nodes appropriate for myPassword.*

The Namescape Designer

The type of applied license determines what is displayed when you access rDirectory. If rDirectory is licensed, and you are authorized to access the Namescape Designer, you will see the rDirectory website with a toolbar containing an **Open Designer** button in the upper right:



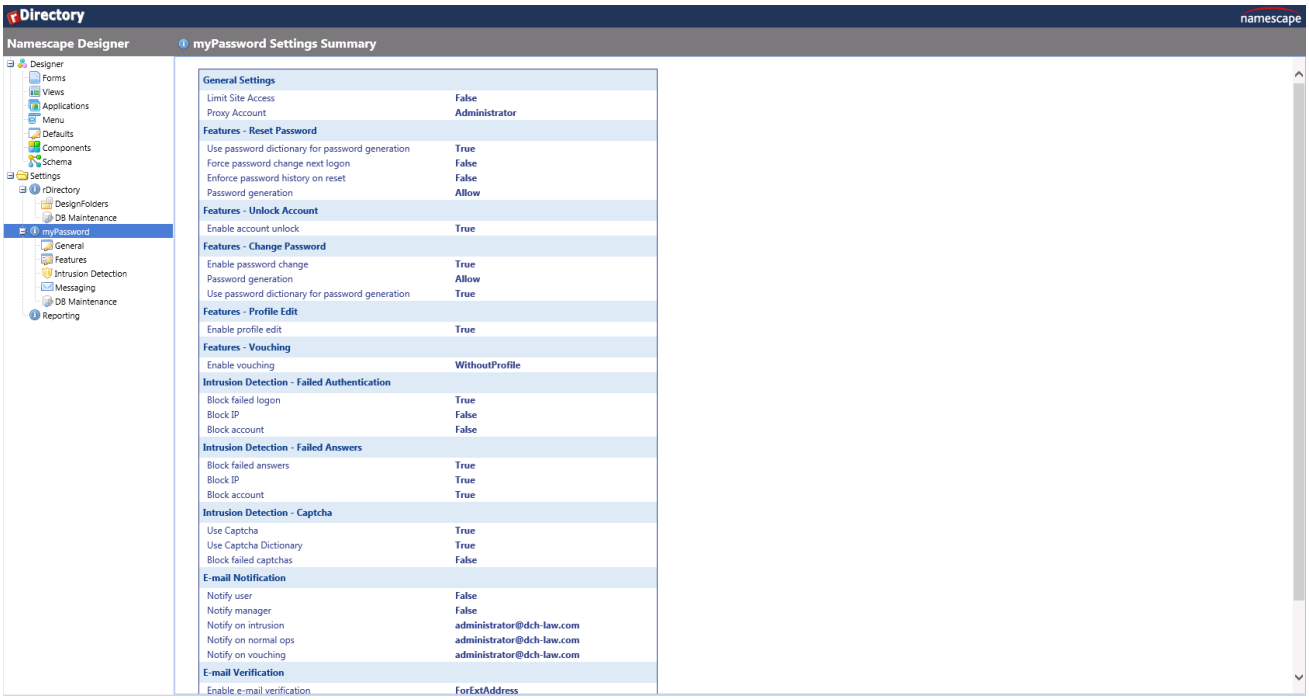
Click the **Open Designer** button to access the Namescape Designer.



If you have questions or difficulty using features in the Namescape Designer, select **Designer Help** on the Designer Home Page to access the context sensitive help.

myPassword Administration

In the Namescape Designer tree menu, expand the **Settings** node and select **myPassword.**

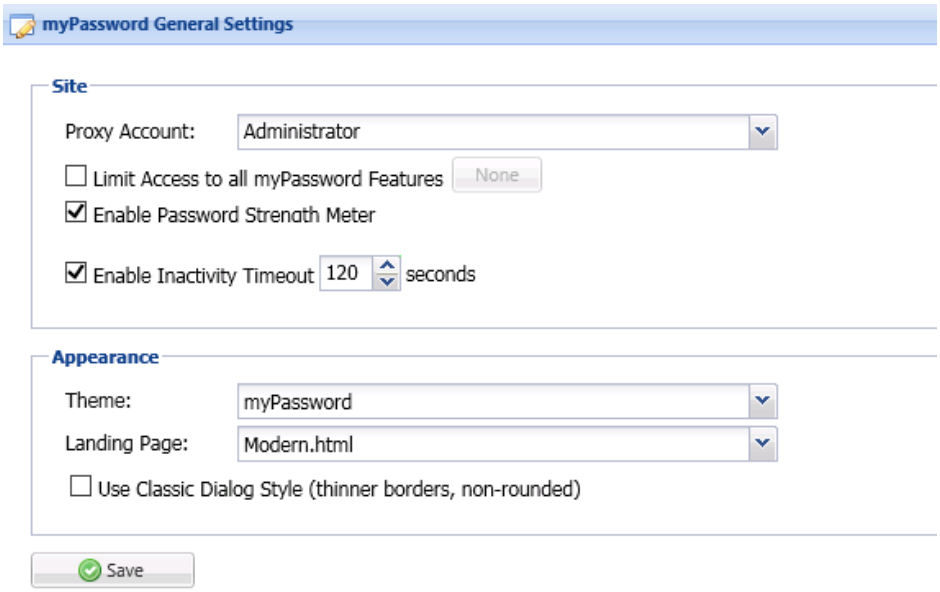


You will be presented with a summarized settings view for the current installation of myPassword.

myPassword settings may be configured by selecting one of the following subordinate nodes:

General

In the tree navigation menu, click **General** to change the proxy settings, limit access to myPassword with roles, and to enable the password strength meter. Here, you may also select the coloring theme and landing page you wish to use.



Site

Proxy Account

A Proxy Account is required for all Password Reset and Profile Edit operations and is configured using the Site Manager.

The account specified must have permissions to reset passwords for all users who may be using the Password Reset feature. If Profile Editing is enabled, this account must also have permissions to edit the Password Reset Profile Attribute for all users who may be using the Profile Editing feature.

Limit Access to myPassword with Roles

If *Limit Access to myPassword with Roles* is checked, and the roles are set, only users who satisfy the roles specified will be allowed to use features on the myPassword site.

Enable Password Strength Meter

If *Enable Password Strength Meter* is checked, the relative strength of the password will dynamically update in the strength meter as characters are entered. The strength of a password is based on Microsoft's password complexity requirement.

Enable Inactivity Timeout

If checked, this setting allows you to specify the time (in seconds) before myPassword will time out due to user inactivity. Upon timeout, the user will be returned to the main menu.

Appearance

Theme

myPassword includes a set of color themes that can be used to alter the appearance of the myPassword client. Changing a theme does not affect customized graphics, text or styles. If you desire a color theme not included with the product, please contact Namescape support for assistance.

Landing Page

myPassword includes a number of templates that may be used as the main landing page of the client. Additional landing pages may be added by simply adding your own custom html file into the templates directory where myPassword is installed, and selecting the new template from the drop down list in the designer.

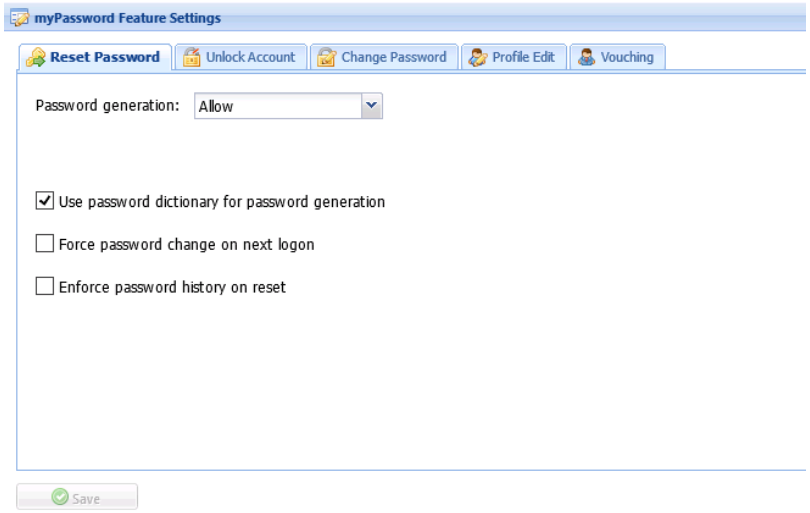
Use Classic Dialogue Style

When enabled, all dialogue boxes will be displayed with the style of previous versions of myPassword. This includes thinner borders and non-rounded boxes.

Features

The Features node allows you to control the feature settings for the main myPassword page.

Reset Password



Password Generation

The *Password Generation* setting determines if automatic password generation is allowed, required (Always) or not available (Never) for Password Reset operations. For more information see *Password Generator*.

Use password dictionary for password generation

If checked, this setting will generate passwords based on the words, numbers or characters specified in the password dictionary.

Force Password Change on Next Logon

If checked, this setting requires users who have reset their password to change their password upon next logon.

> ***NOTE:*** *If password history is enforced, this feature is recommended. The password reset function of Active Directory does not enforce password history, potentially allowing re-use of old passwords if this feature is not enabled. Active Directory only enforces password history on the password change function, so when users are forced to change their password on next logon, their history will re-enforce.*

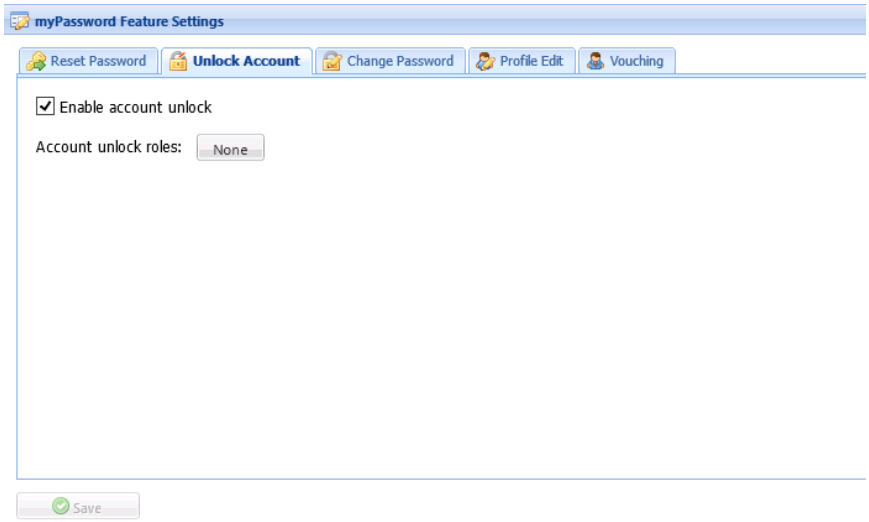
Enforce Password History on Reset

If checked, this setting enforces password history on a reset and prevents the user from changing their password back to a previously used password. We recommend modifying your

Domain Security Policy to increase the number of passwords remembered (at least 2x default value).

NOTE: *If you set the minimum password age in your Domain Password Policy, and a user forgets their password within the minimum age, they will not be able to use myPassword to reset their password.*

Unlock Account



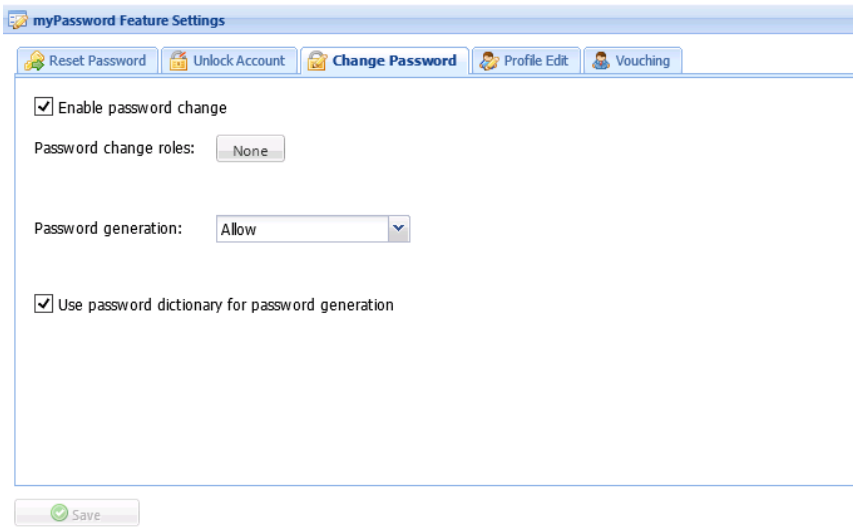
Enable Account Unlock

If the *Enable Account Unlock* setting is checked, the Unlock my Account feature will be available on the main myPassword page.

Account Unlock Roles

If any *Account Unlock Roles* are set, only users who satisfy these roles will be allowed to use this feature.

Change Password



Enable Password Change

If checked, this setting enables the Password Change feature for all users who satisfy any roles set under *Password Change Roles*. If *Password Change Roles* are not set, all users may use the Password Change function.

Password Change Roles

The *Password Change Roles* setting indicates if any roles are set for the Password Change feature. If roles are not set, all users may use the Password Change feature when it is enabled.

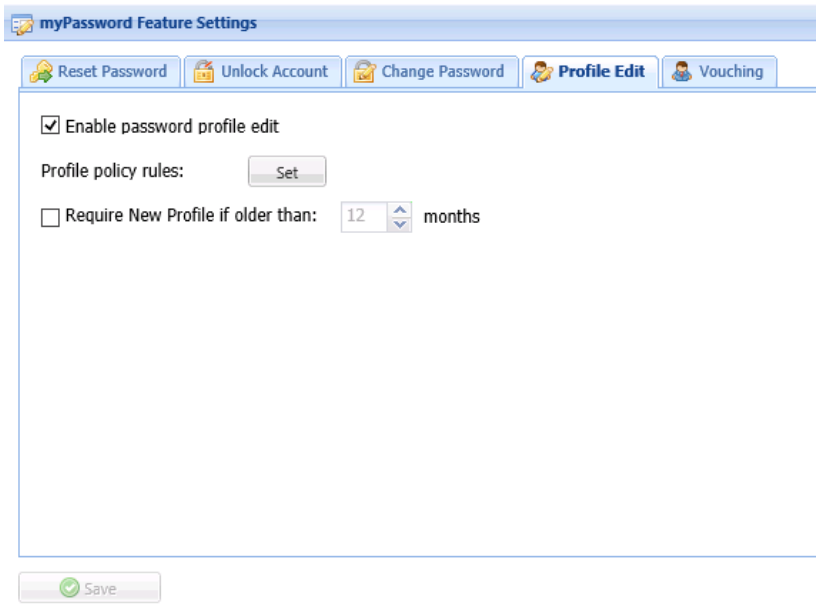
Password Generation

The *Password Generation* setting determines if Password Generation is allowed, required (Always) or not available (Never) for Password Change operations. For more information see Password Generator.

Use password dictionary for password generation

If checked, this setting will generate passwords based on the words, numbers or characters specified in the password dictionary.

Profile Edit



Enable Password Profile Edit

If selected, and at least one *Profile Policy Rule* is set, users will be allowed to create and edit a Password Profile containing their questions and answers.

Profile Policy Rules

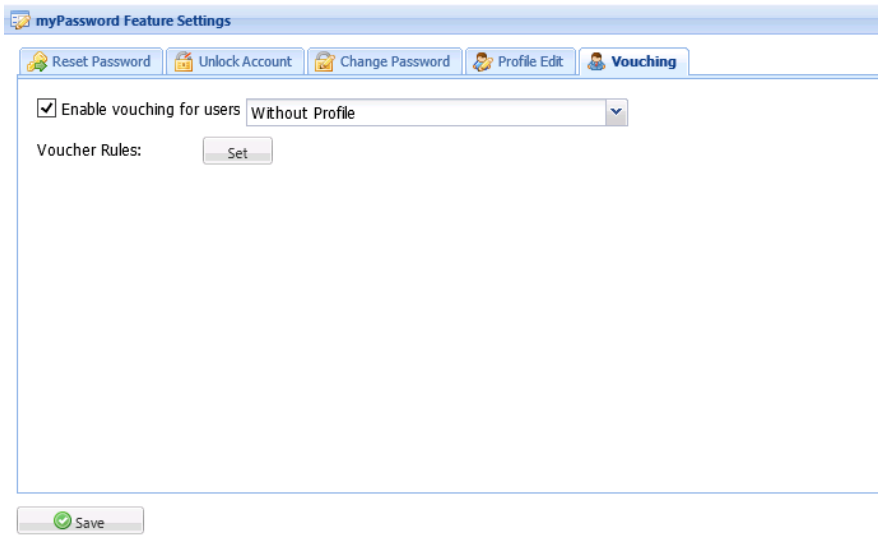
The *Profile Policy Rules* button indicates if any Password Profile Rules are set and when selected, launches the Password Profile Rules Editor. If *Enable Password Profile Edit* is checked, at least one Password Profile Rule must be set.

Profile Policy rules can be defined in the Namescape Designer under **Components | Policies**.

Require New Profile if older than X months

Enabling this setting will cause myPassword to prompt users for updated profile questions every *X* months. By default, this setting is disabled.

Vouching



Enable Vouching for Users

If vouching is enabled, and at least one Voucher Rule is set, users will be allowed to have someone to vouch for them, rather than being required to answer the questions in their Password Reset Profile. Users who have the option of someone vouching for them are limited with the following settings:

Without Profile

Only users who do not have a Password Reset Profile are allowed to have someone vouch for them.

With Profile

Only users who have a Password Reset Profile are allowed to have someone vouch for them (I.e. in case they can't remember their answers).

Both

All users, regardless of whether they have a Password Reset Profile, are allowed to have someone vouch for them.

Voucher Rules

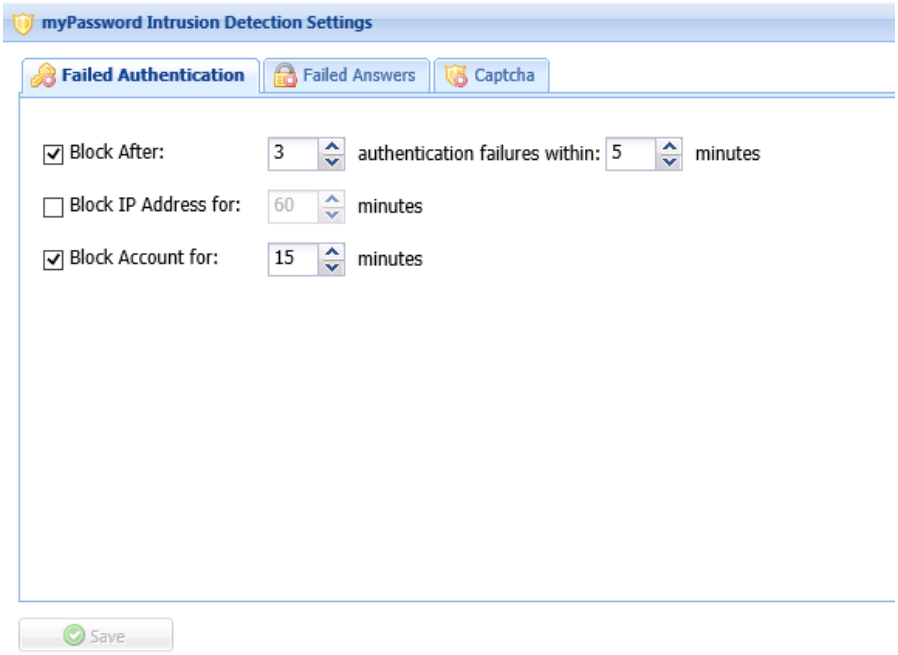
The *Voucher Rules* button indicates if any Voucher Rules are set, and when selected, launches the Voucher Rules Editor. If vouching is enabled, at least one Voucher Rule must be set.

Intrusion Detection

Access to myPassword by an IP address or compromised account can be blocked for excessive failed answers and/or excessive failed authentications. myPassword may also be configured to require a CAPTCHA entry to prevent automated intrusion attempts.

Examples of a failed authentication include a bad logon name or password for any logon screen, a failed password change, a failed password reset profile edit or an invalid voucher logon.

Both the **Failed Authentication** and the **Failed Answers** tabs contain the following settings:



Block After X Authentication Failures within X Minutes

If enabled, the IP address or compromised account will be blocked if the specified number of authentication failures or failed answers occurs within the time frame specified. This event can initiate an email notice, block access from the IP address for a specified time, or block access to the compromised account for the specified time.

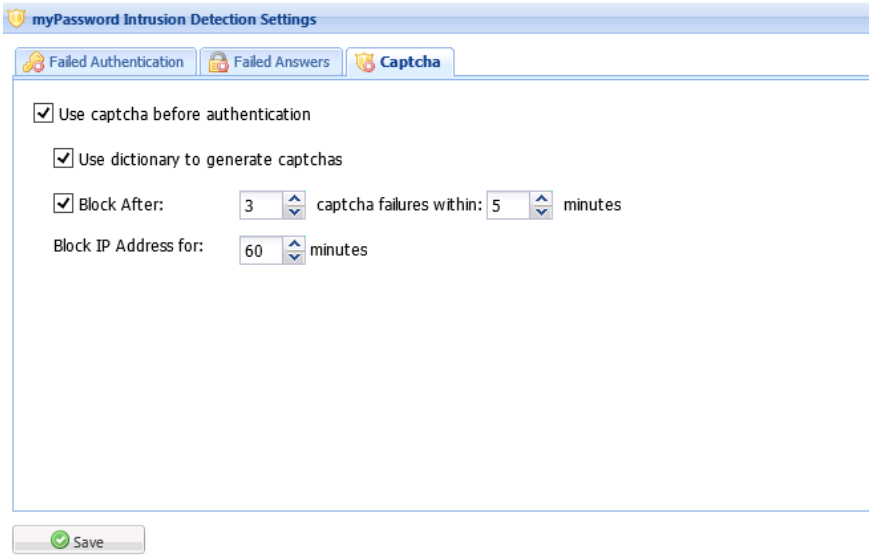
Block IP Address for X minutes

If enabled, the originating IP address is blocked for the specified time period if an authentication failure or failed answer occurs.

Block Account for X minutes

If enabled, the compromised account is blocked from being accessed via myPassword for the specified time period if an authentication failure or failed answer occurs.

CAPTCHA



CAPTCHA may be required in order to validate a user as a person, and is designed to prevent automated attacks.

Use CAPTCHA before authentication

If enabled, a user will be presented with a CAPTCHA page prior to being allowed to enter their credentials. A number of options are available when configuring the CAPTCHA page:

Use dictionary to generate CAPTCHAs

When enabled, the customizable myPassword word dictionary will be used to generate CAPTCHAs. If this setting is not enabled, any CAPTCHAs presented will be a random combination of letters and numbers.

Block After

An IP address may be blocked from accessing myPassword after a user incorrectly enters a defined number of CAPTCHAs within a given time period.

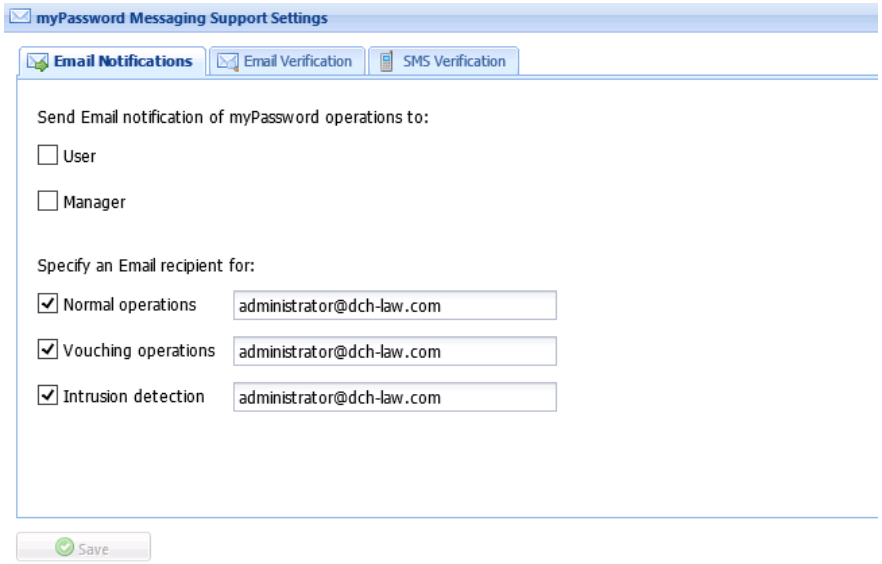
Block IP address for X minutes

The IP address of the potential intruder will be blocked for a defined period of time.

Messaging

Messaging allows you to configure email messaging and SMS for myPassword.

Email Notification



User

If checked, an email notice is sent to the email address of the user for all password resets, password changes and Password Reset Profile modifications made to their account.

Manager

If checked, an email notice is sent to the user's manager for all password resets, password changes and Password Reset Profile modifications made against the user's account, provided the account being accessed has a manager, and the manager has an email address.

Normal Operations

If checked, an email notice is sent to the email address specified for all password resets, password changes and Password Reset Profile modifications made via myPassword.

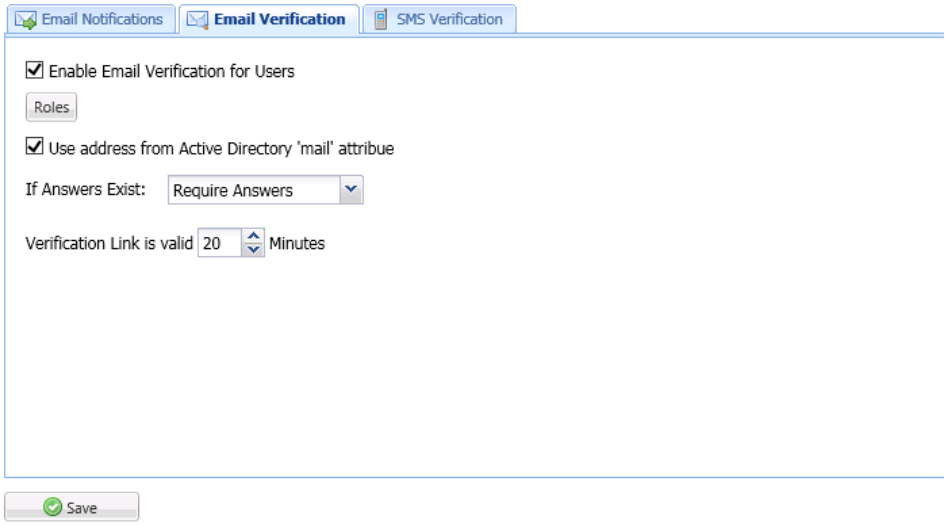
Vouching Operations

If checked, an email notice is sent to the email address specified whenever the vouching feature is used to authorize a password reset.

Intrusion Detection

If checked, an email notice is sent to the email address specified whenever an intrusion detection event occurs. An intrusion detection event is triggered by a failed answer, failed authentication or failed CAPTCHA entries.

Email Verification



Email Verification allows mail-enabled users with an external email address to be sent a time sensitive email. The email includes a link that, when clicked, returns the user to the final page in the password reset process where they can set their new password.

This feature is intended for mail-enabled users with external email accounts only. This feature should not be used with mailbox-enabled accounts where the user is required to log on to Active Directory in order to access their mailbox.

The external email address will be encrypted and added to the users Password Reset Profile when the Profile Edit Policy is appropriately configured.

NOTE: *In Exchange terminology, a mailbox-enabled user is someone who has an exchange mailbox. Whereas a mail-enabled user or contact has an email address that points to an external mail system or domain. A mail-enabled user or contact can show up in the Global Address List, and you can send email to them which will be directed to their external email address. When you mail-enable a user or contact using the Exchange tools, or using rDirectory and the Provisioning Agent for*

Exchange, the external email address is populated in both the normal 'mail' attribute, as well as the 'External Target Address' attribute.

Enable Email Verification for Users

This setting enables email verification for the password reset, password change and account unlock operation.

When enabled, all users with a properly configured and completed Password Reset Profile will automatically use Email Verification. A user's Password Reset Profile may be updated by opening the myPassword client and selecting **Edit my Profile.**

Roles

If set, only users assigned one of the approved roles may use Email Verification.

Use address from Active Directory *mail* attribute

If enabled, the address used for email verification will be retrieved from the user's *mail* attribute in Active Directory, rather than the encrypted Password Reset Profile.

If Answers Exist

If a user has a completed Password Profile, this setting determines the following behavior:

Require Answers

This setting requires users with a Password Reset Profile to successfully answer their challenge/response questions before they are sent an email link. They need to click on the link sent to them to complete the operation.

Always Skip

This setting always skips the process of requiring users to answer their challenge/response questions, and sends them an email link to verify their identity.

Allow Skip

This setting allows users with a Password Reset Profile the option of either answering their challenge/response questions, or using the email link feature for identification.

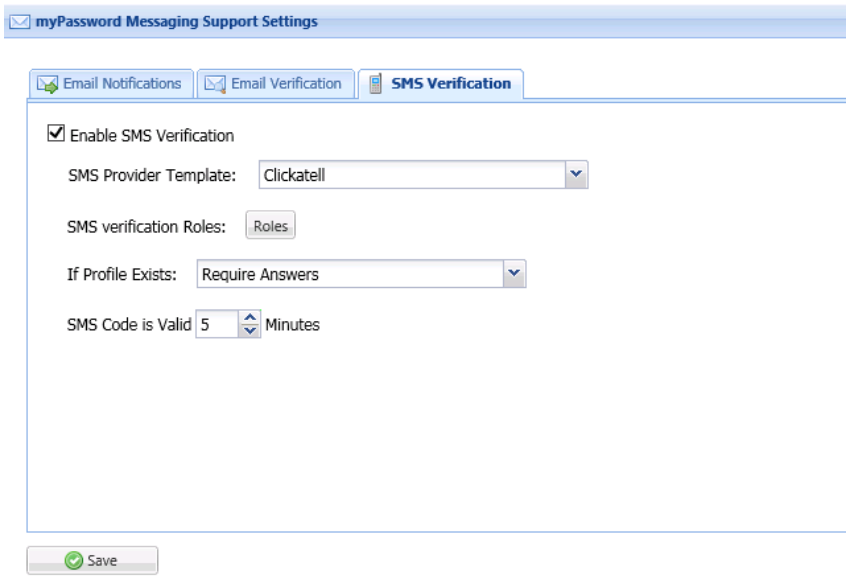
Link Timeout

This value determines how long a user has to respond to the link sent in a verification email. If a user clicks on the link after this time period expires, they will receive a message saying the link is no longer valid.

NOTE: *For security reasons, the link sent to a user simply contains a GUID. This GUID is used to store and retrieve information about each specific Email Verification session in the application cache. This information is removed from the cache after this amount of time. Should the server reboot, or the application pool of the myPassword web site recycled, the information is lost for all past email verification links sent.*

SMS Verification

SMS Verification allows you to set up a secondary authentication method for resetting passwords. When SMS is configured, a verification code will be generated and sent to the mobile number stored in the user's properly configured and completed Password Reset Profile. The user will then be prompted to enter that code into the myPassword client in order to proceed.



Enable SMS Verification

When checked, this setting enables SMS verification in myPassword. See *Installation and Setup rDirectory and myPassword: Chapter 7: Configuring myPassword for SMS Verification* for more information on configuring your SMS gateway account to work with the included myPassword SMS gateway templates.

NOTE: *If both SMS and email verification are enabled, the user may be given a choice of authentication method. Otherwise, SMS will always take precedence.*

SMS Provider Template

This setting defines the SMS gateway provider template to be used when generating an SMS text. By default, the included gateway provider templates are Clickatell and Red Oxygen.

NOTE: *You must have a fully configured and funded SMS gateway provider account prior to using myPassword SMS verification. Namescape is not responsible for the setup and maintenance of this SMS gateway provider account.*

SMS Verification Roles

This setting defines which users will be allowed or denied the use of SMS verification when resetting a password. If no claims or groups are defined, all users will be presented SMS verification, if enabled.

If Profile Exists

This setting defines how myPassword should behave if a user has a profile created and SMS verification is enabled.

Require Answers

If the user has a completed profile, they will be required to answer all security questions correctly, in addition to entering the correct SMS verification code, before proceeding.

Always Skip

The profile questions will always be skipped and the user will only be required to enter the SMS verification code to proceed.

Allow Skip

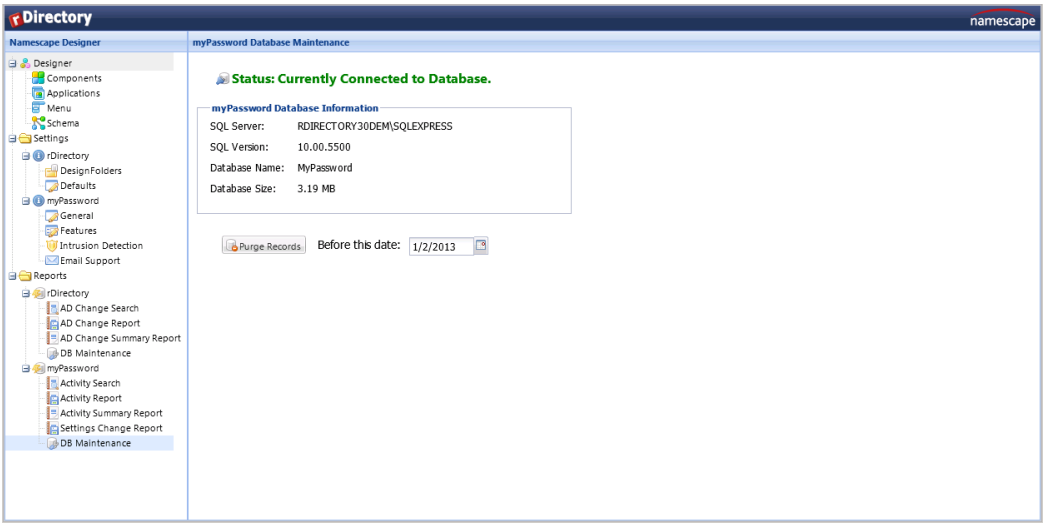
The user will be given the option to answer the security questions in their profile, but will be allowed to skip to the SMS verification if desired.

Minutes SMS Code is Valid

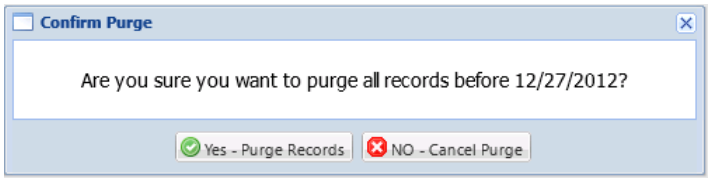
This setting defines the length of time a sent SMS verification code will remain valid. Once a code is expired, it may no longer be used, and the user will need to generate a new code before proceeding. (*Default: 5 minutes*)

DB Maintenance

The DB (database) Maintenance screen displays SQL database information and status, and allows you to purge user activity from the SQL database.



Click **Purge Records** to mark any records prior to the defined date as inactive. You will be prompted to confirm the records will be purged.



Click ***Yes – Purge Records*** to mark all selected records as inactive.

Accessing myPassword

Access Methods

Several access methods are available with myPassword, including Normal/Kiosk, Mobile Web App, Web Front End, ReturnURL and AutoClose. Any of these access methods may be set with additional URL arguments and directly linked entry pages. The behavior and button text of myPassword will vary depending on the method in use, and which entry page the user first accesses.

From the Windows Logon Form

myPassword provides both GINA-enabled and GINA-free methods of allowing users to access myPassword directly from their Windows Logon Form.

NOTE: *A GINA (Graphical Identification and Authentication) is a DLL that is pushed out to each workstation and modifies the user's logon form, providing a prompt and a direct access link to myPassword. The management of the GINA method is not considered to be a best practice by Microsoft. However, it is preferred in certain environments, so we provide both GINA-enabled and GINA-free methods. Both methods are compatible with the ProfileValidator tool.*

GINA-free access

NOTE: *The GINA-free access method is only compatible with the WindowsXP operating system. All other versions of Windows must use the GINA-enabled access method.*

The GINA-free access method combines a Restricted Access Account with a Windows Logon Form prompt message.

A Restricted Access Account is a well-known account that anyone can use to log on, but which has very limited access. Using this method, a user logging in with a Restricted Access Account is taken directly to the myPassword site, without being granted additional access to any local files or resources on the PC or other web sites.

To complement the Restricted Access Account method, Namescape also provides a means to include a custom message prompt at the top of each user's logon screen, reminding them to use the Restricted Access Account should they forget their password.

The GINA-free access method provides a number of advantages over the GINA method, including centralized management and eliminating potential conflicts that a GINA.DLL may create.

For more details, see:

Installation – myPassword Restricted Access Account.pdf

Installation – myPassword WinLogon Prompt.pdf

GINA-enabled access

The myPassword GINA will modify the logon screen using a custom GINA.dll installed on every workstation, and will prominently place a customizable message and link to the myPassword website.

For more details, see:

Installation – myPassword GINA.pdf

Outlook Web Access Logon Page

A link to myPassword can be added to the Outlook Web Access (OWA) Logon page, granting remote users access to myPassword. Using this method, the ReturnURL is configured to return the user to the Outlook Web Access Logon page upon completion of a password modification or inactivity timeout in myPassword.

For more details, see *Appendix A – Adding a myPassword Link to the Outlook Web Access Logon Page*.

Company portal or web page

A direct link to myPassword can be added to a company portal or web page, granting remote users access to myPassword. Using this method, the ReturnURL is configured to return the user to the originating portal or web page upon completion of a password modification or inactivity timeout in myPassword.

Web Front End\Public internet access

The strong security features of myPassword make it suitable for public availability. When using the externally facing Web Front End, a simple client is installed on an IIS server located in your DMZ. This client is then configured to securely communicate with an instance of the myPassword Proxy Server service that is deployed on an internal installation of myPassword. This architecture allows for secure password modifications, without the fear of externally exposing your Active Directory. The Normal/Kiosk Access Method is used when myPassword is publicly accessible, and the user is returned to the entry page upon completion of a password modification or inactivity timeout.

Dedicated kiosk

A dedicated, centrally located workstation, or Kiosk, with access to myPassword is a solution many companies find desirable. In this scenario, the Normal/Kiosk Access Method is used, and the user is returned to the entry page upon completion of a password modification or inactivity timeout.

Shared console

A user may simply go to a co-worker or manager's workstation to access myPassword, which may be preferred if the Voucher feature is enabled.

Mobile access

myPassword also includes a web app display mode, allowing users on smartphones or tablets to perform any of the standard myPassword operations in a smaller, mobile device friendly format. The web app is created alongside the normal myPassword site during installation and does not require additional configuration. When a user accesses the myPassword site with a smartphone or tablet device, the device type will be automatically detected and the user will be shown the appropriate view. Because this is a web app, and not a native mobile app, no further installation or configuration on the mobile device is required.

Entry Pages

There are five possible entry pages for myPassword. The main menu page is the default Entry Page when the base URL for myPassword is used. For example:

//<servername>/myPassword

The remaining four possible entry pages each represent one of the primary features found on the main menu page.

Main Menu Page

If the Change Password, Password Reset, Unlock Account, and Password Profile Edit features are all enabled, users accessing the main page of myPassword will see the choices shown below.

Selecting **Change my Password**, **Reset my Password**, **Unlock my Account**, or **Edit my Profile** directs the user, respectively, to the following pages:

//<servername>/myPassword/PasswordChange.aspx

//<servername>/myPassword/PasswordReset.aspx

//<servername>/myPassword/AccountUnlock.aspx

//<servername>/myPassword/EditProfile.aspx

If enabled, each of these pages can also be accessed directly. When accessed directly, these pages are considered the Entry Page for that user, rather than the main page.

Access Modes and Arguments

There are three Access Modes that modify the behavior of myPassword on completion of a password modification or inactivity timeout. Each mode will have unique text displayed on the Timeout/Return button, as described by the table below:

Access Mode	Action on Completion or Timeout	Timeout/Return Button Text
Normal/Kiosk	Return to Entry Page	Return to <Name of Entry Page> Now
ReturnURL	Returns to URL specified	Return to <Return Page Name> Now
AutoClose	Close Browser	Return to Windows Logon Now

In all modes, the **Cancel** button returns the user to their respective entry page.

Normal/Kiosk

Normal or Kiosk is the default access mode used when additional URL arguments are **not** passed into the Entry Page.

In this access mode, the user always returns to their respective entry page when the Timeout/Return button is clicked, an action is completed, or an inactivity timeout occurs. The Timeout/Return button text appears as one of the following depending on the entry page for that user:

Return to the Main Menu

Return to the Password Reset Page

Return to the Change Password Page

Return to the Unlock Account Page

Return to the Profile Edit Page

ReturnURL

The ReturnURL Access Mode is enabled by passing in a 'ReturnURL' argument that specifies a URL to return to when an action is completed or an inactivity timeout occurs. This mode is intended for use when myPassword is launched from another web page, such as the Outlook Web Access (OWA) Logon Page or a company portal. An optional argument 'ReturnPageName' may also be added to customize the text on the Timeout/Return button.

For example, the URL specified might be:

OWA Return

//<servername>/myPassword?ReturnURL=https://mail.acme.com/exchange&ReturnPageName=OWA Logon

Company Portal Return

//<servername>/myPassword?ReturnURL=http://portal.acme.com&ReturnPageName=ACME Portal

In this Access Mode, the user will always return to the URL specified by the ReturnURL argument when the action is completed or an inactivity timeout occurs.

The Timeout/Return button text displays 'Return to *<Return Page Name>* Now', where *<Return Page Name>* is either the value specified by the 'ReturnPageName' argument, or 'Home Page' if the 'ReturnPageName' argument is not specified.

NOTE: *The Return Page Name should be short (<20 characters) to avoid adversely affecting the page formatting.*

AutoClose

The AutoClose Access Mode is designed to be used when myPassword is accessed from the Windows Logon Form, and is enabled by passing in the argument '*AutoClose=true*' in the URL.

For example, the URL specified might be:

//<servername>/myPassword?AutoClose=true

In AutoClose mode, the inactivity timer is automatically added to the user's entry page. When an action is completed or an inactivity timeout occurs, the browser is closed and the user is returned to their Windows Logon Form.

Customizing the Web Client and Main Menu Landing Page

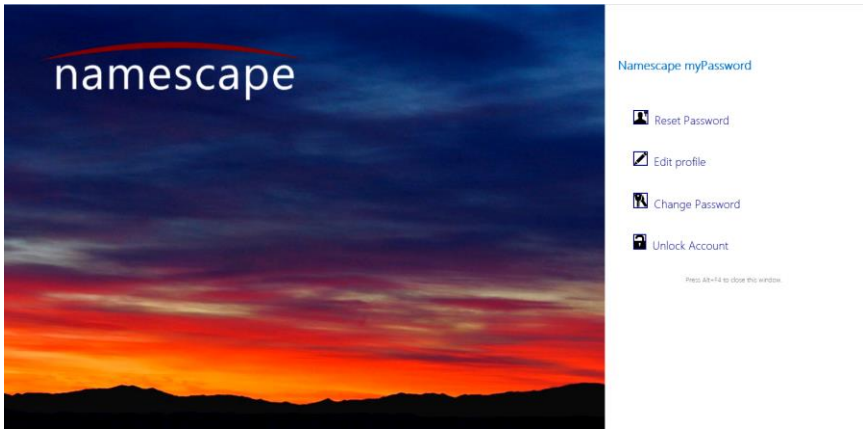
The myPassword client may be changed to display a different color theme, and the main menu landing page may be modified to display a custom landing page, based on your business needs.

To modify the default theme and main menu landing page layout, open the Namescape Designer and select *myPassword>General*. Under Appearance, the following settings are available:

Theme This setting allows you to choose which base theme will be used throughout the myPassword client. A number of color options are included.

NOTE: *Additional custom color combination packages may be developed and provided with the purchase of Namescape Professional Services hours.*

Landing Page This setting defines the main menu landing page layout. If the default main menu landing page is not desired, a number of templates are provided, including the Modern.html shown below. You may also modify the existing templates, or create your own landing page in *.html format.



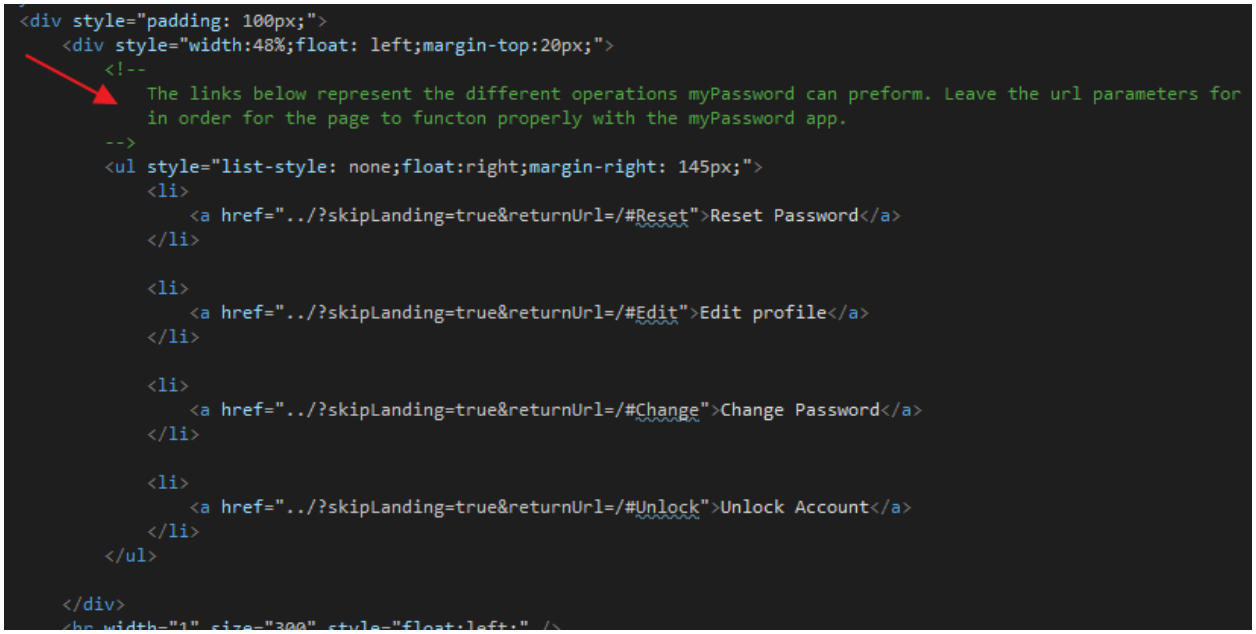
The Landing Page option reads any *.html file present in the /LandingPages folder, under the myPassword root directory. Selecting an option other than *–None-* will override the default myPassword page, and replace it with the selected template.

If you wish to use a landing page layout that you have created, verify that it is saved in *.html format, place it in the /LandingPages folder, select it in the designer, and click **Save.**

NOTE: *The landing page is a simple *.html overlay. All other myPassword features and functions remain isolated, and security is not compromised.*

NOTE: *Assistance creating custom landing pages is available with purchase of Namescape Professional Service hours.*

Additional help for each included template is included in the HTML files themselves. These notes will help you determine what changes to make, and where to make them, when customizing your landing page. To view the development notes, open the HTML template files with any HTML document editor.



```
<div style="padding: 100px;">
    <div style="width:48%;float: left;margin-top:20px;">
        <!--
            The links below represent the different operations myPassword can preform. Leave the url parameters for
            in order for the page to functon properly with the myPassword app.
        -->
        <ul style="list-style: none;float:right;margin-right: 145px;">
            <li>
                <a href="../?skipLanding=true&returnUrl=/#Reset">Reset Password</a>
            </li>

            <li>
                <a href="../?skipLanding=true&returnUrl=/#Edit">Edit profile</a>
            </li>

            <li>
                <a href="../?skipLanding=true&returnUrl=/#Change">Change Password</a>
            </li>

            <li>
                <a href="../?skipLanding=true&returnUrl=/#Unlock">Unlock Account</a>
            </li>
        </ul>

    </div>
```

For more information on theming myPassword, see *Appendix A – Customizing myPassword*

Using myPassword

To access the myPassword site once it is configured, enter the URL for myPassword into a browser. For example, if myPassword is installed as a virtual directory under the default website on a server, then the URL to access myPassword would be as follows:

http://<servername>/myPassword

The same URL is used for both Normal/Kiosk and Mobile views. The myPassword site will automatically display the appropriate view based on the detected device type.

NOTE: *The following screen shots are taken in the Normal/Kiosk and Mobile Access modes using the Main Menu as the Entry Page.*

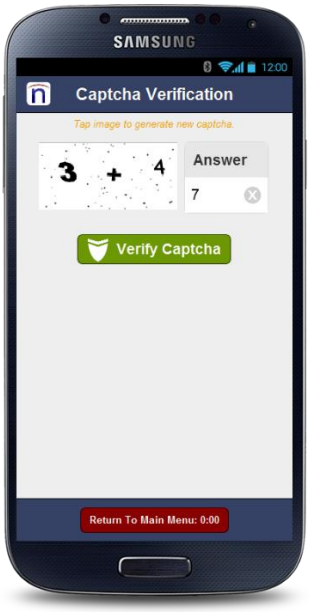
Main Page

If the Change Password, Password Reset, Unlock Account, and Password Profile Edit features are all enabled, then users accessing the main page of myPassword will see the choices shown below.

CAPTCHA

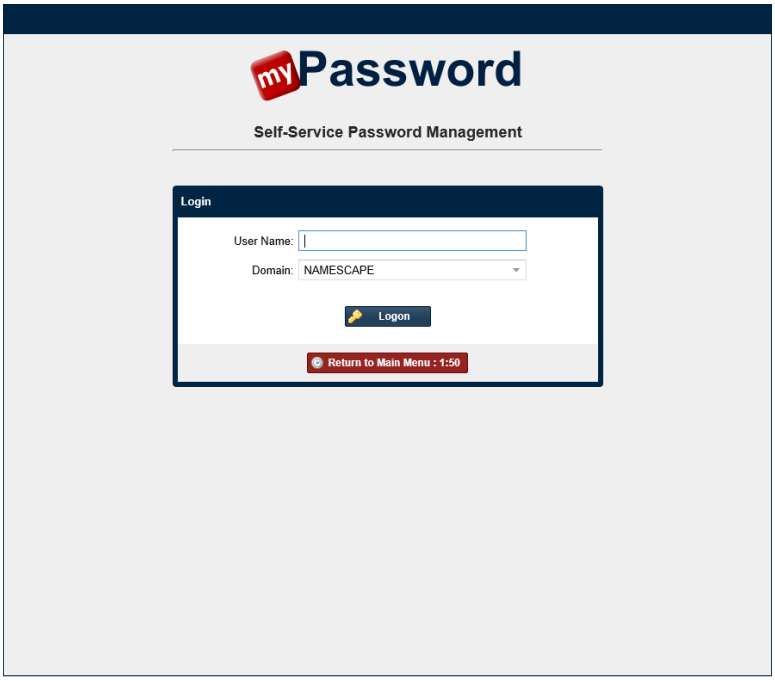
If enabled, a user will be presented with a CAPTCHA page prior to entering any personal information. On this page, a CAPTCHA will be generated that the user must correctly type into the box before they are allowed to proceed. If the user is unable to read the displayed CAPTCHA, they may click on the picture, and a new one will be generated.

Due to space limitations, the standard CAPTCHA is not practical on a mobile platform. Instead, a user will be asked to solve a simple math problem. If the user is unable to solve the presented problem, they may select to display a new problem.



Reset my Password

When a user selects **Reset my Password**, or otherwise lands on the Password Reset page, they are presented with the logon page shown below. On this page, users are asked to enter their Windows account name.

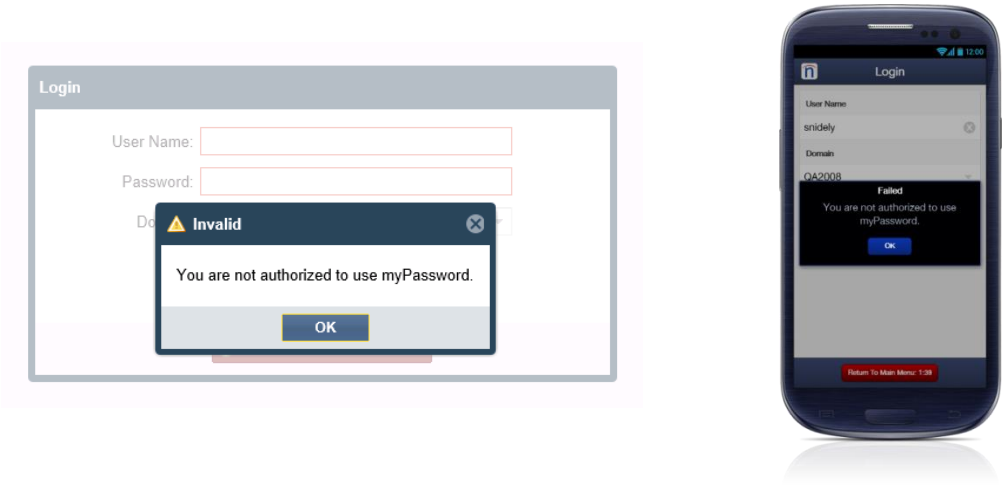


Denied Access Pages

After entering their logon name, users are denied access to myPassword if either of the following conditions exists:

1) The user is not allowed access by the myPassword Access Roles, or
2) The user has not filled in their Password Reset Profile in rDirectory and the Allow Reset without Profile if Vouched For option is not checked.

If the user is denied access based on myPassword Access Roles, they will be presented with an access denied dialogue and will not be allowed to proceed.



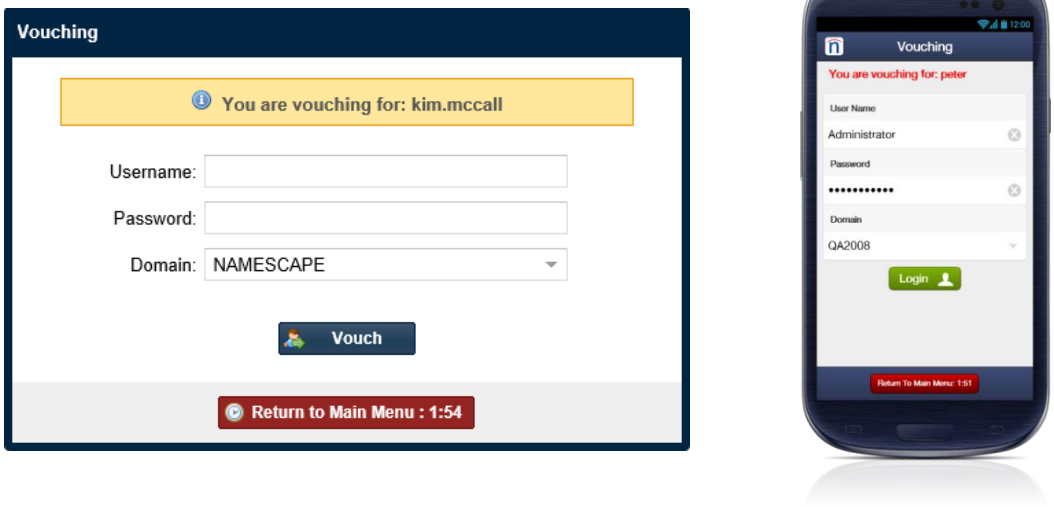
If the user has not filled in their Password Reset Profile, and the Vouching option is not enabled for users that have no profile, the error message below is shown:

Voucher Pages

After providing their logon name, a voucher is required if either of the following two conditions exist:

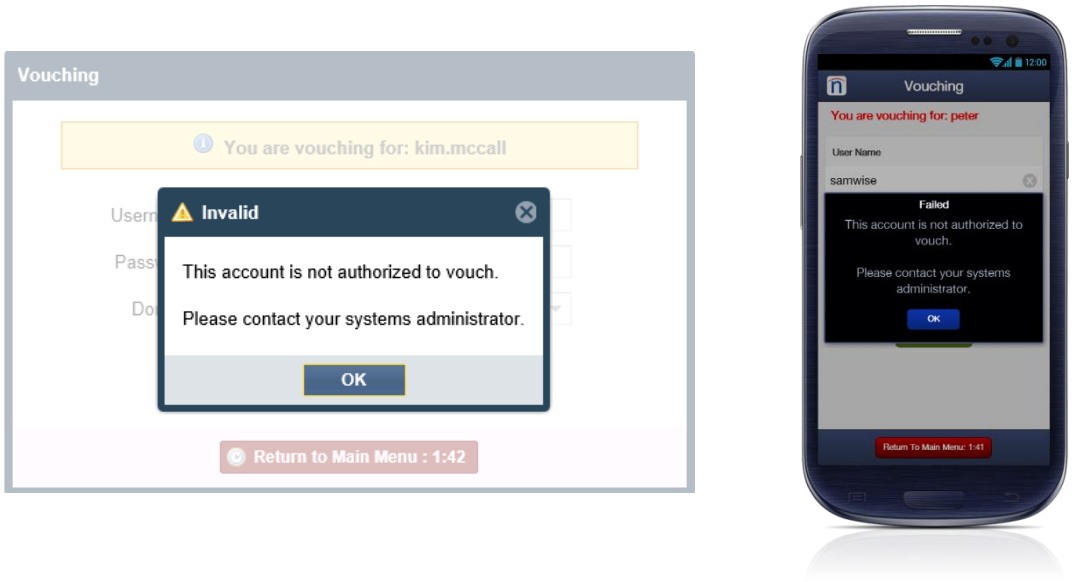
1) The user does not have a Password Reset Profile, and a voucher is allowed as an alternate means of validating the user's identity.
2) The user has a Password Reset Profile, and a voucher is required as an additional means of validating the user's identity.

If the user has no Password Reset Profile, and a voucher is required, the user will see the screen below:



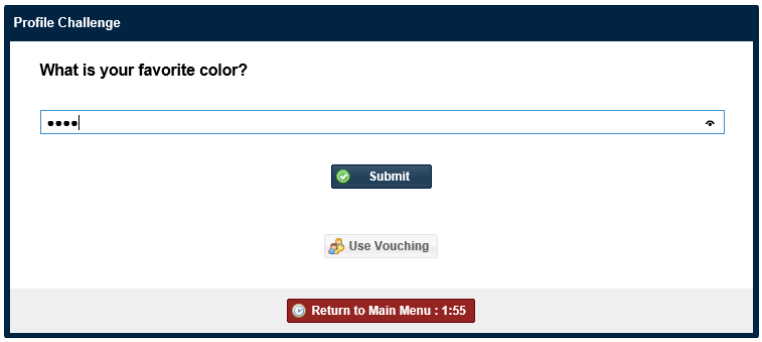
The message field ('You are vouching for: username) can be modified by editing the assigned header file associated with a voucher rule. For example, if you had a rule that required a user's manager to vouch for them, that rule might also specify a header message such as 'A Manager must vouch for you before your password can be reset'.

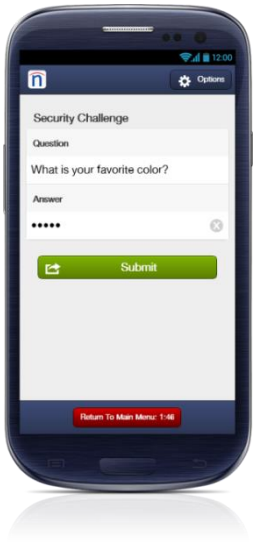
Each voucher rule may also specify the roles of those who are allowed to vouch for a given user. If the voucher is not authorized for the given user, the following screen appears:



Answering the Password Reset Profile Questions

If a user attempts to reset their password, and they have a previously completed Password Reset Profile, they will be asked to provide answers in order to continue. Only one question will be presented at a time, and the user is required to answer each question correctly before they are allowed to proceed to the next question.

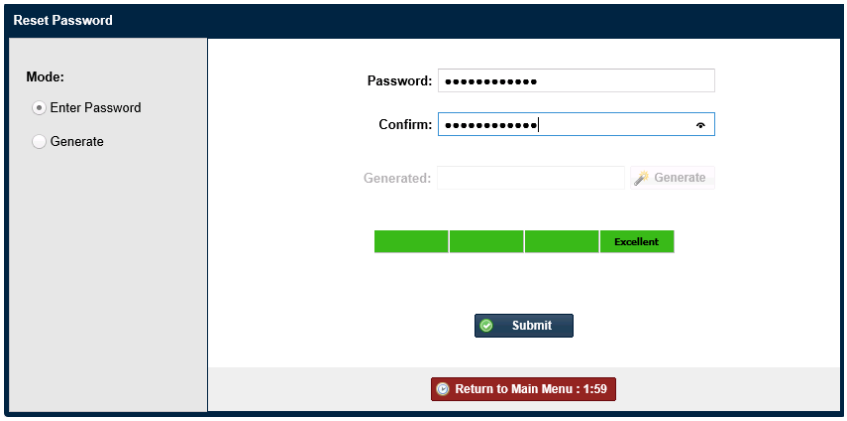


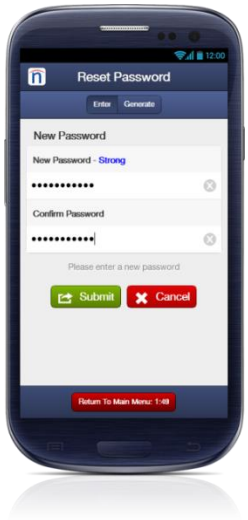


If an excessive number of incorrect answers are entered, an intrusion event will trigger that may be configured to block the originating account or IP address for a defined time period, as well as send an email to an administrator notifying them of a potential attack that may be under way.

Reset Password Page

After all Password Reset Profile questions have been answered correctly and/or the user has been successfully vouched for, the user will be allowed to reset their password. The user can be given the option to either manually enter a new password, or generate a password automatically. Additional configuration options may allow only a generated password and/or force the user to change their password at next logon.



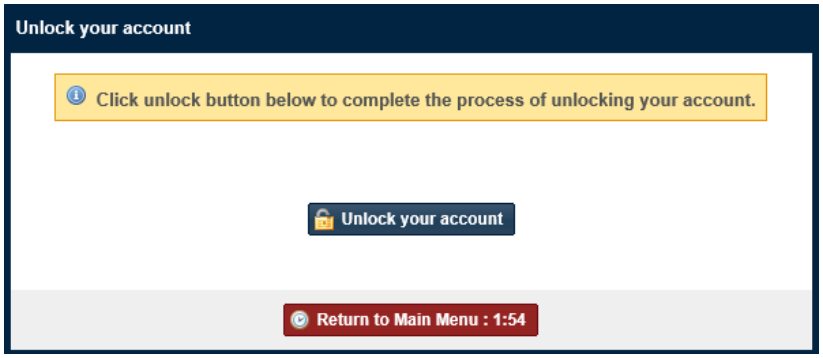


As a password is entered, the password strength meter will display **Weak, Average, Strong** or **Excellent,** depending on the complexity of the password. If you would like to automatically create a random password instead of manually entering one, select the **Generate** option. Each time the **Generate** button is clicked, a new password will be generated.

Once an appropriate password has been entered, click the **Submit** button to accept the new password.

Unlock my Account

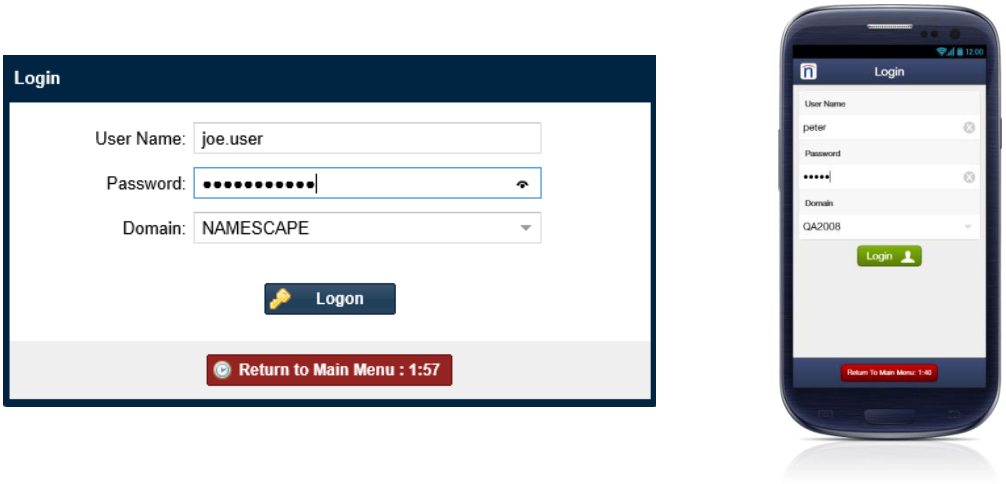
When a user selects **Unlock my Account**, or otherwise lands on the Account Unlock page, they are presented with the same set of pages that appear when they select the **Reset my Password** option. These pages include Logon, Vouch (if applicable), or a Question/Answer profile (if applicable). However, once a user is authenticated, they will be shown the following Account Unlock page rather than the Reset Password Page.



For security reasons, the locked status will not be presented until the account has been authenticated by either answering the associated profile questions or vouched for by an authorized user.

Change my Password

When a user selects **Change my Password** or otherwise lands on the Password Change page, they are first presented with the Logon page. On this page, users enter their Windows credentials in order to change their existing password.



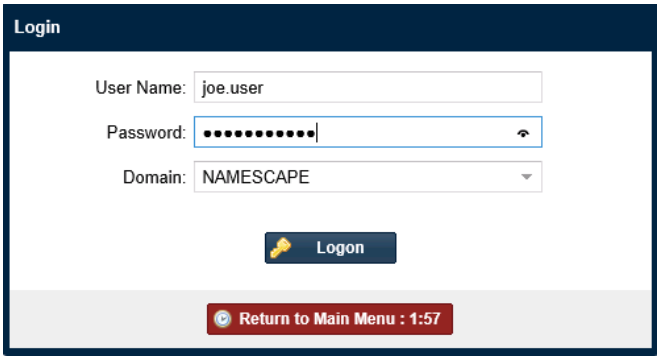
Because the user must provide valid credentials to change their password, vouching is not available on this page. Configured myPassword Access Roles, however, will still apply and accounts not authorized to use myPassword will be presented the Denied Access message.

Mandatory Profile Completion on Password Change

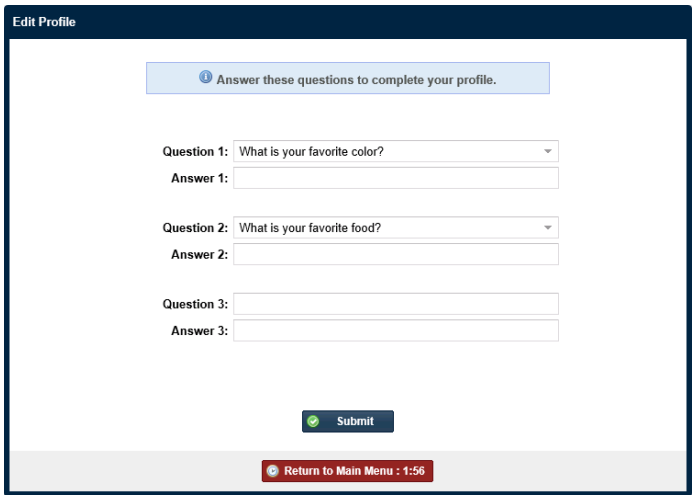
If a user has not filled out a Password Reset Profile, they will be forced to do so before proceeding to the Change Password page. This improved flow guarantees a profile is created for users who do not have access to a computer where the profile validator is installed, and simplifies the onboarding process when filling out a password profile is desired.

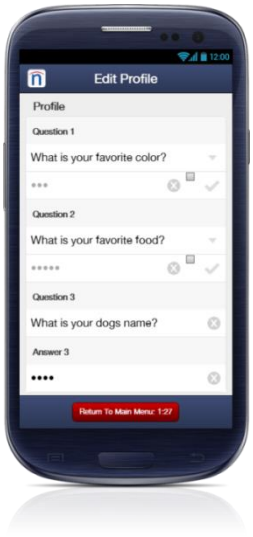
Edit my Profile

When a user selects **Edit my Profile** or otherwise lands on the Edit Profile page, they are first presented with the Logon page. On this page, users are required to enter their Windows credentials in order to edit their password profile.



Once authenticated, the user will be presented with a list of questions, as required by the assigned Password Profile Policy. A single, global Password Profile Policy may be configured for all users, or multiple Password Profile Policy Rules may be created in the Namescape Designer and assigned to different groups of users as desired.





After answers have been provided and any custom questions defined, click **Submit** to create the Password Reset Profile and return to the main menu.

Enforcing Enrollment

In addition to forcing enrollment in the **Change my Password** feature of myPassword, there are a number of other methods available that may be used to prompt a user to create a Password Reset Profile.

On rDirectory access

By using the integrated Enforce Profile Validation features within rDirectory, users can be required to fill in their Password Reset Profile when they access the rDirectory site. This feature may also enforce data validation rules for other attributes, including those with malformed or otherwise incorrect data.

For more details on the Enforce Profile Validation feature, please see the rDirectory online help.

On Logon with ProfileValidator.exe

The ProfileValidator.exe tool is designed to execute automatically during logon and request, or optionally require, the user complete or correct data in their Password Reset Profile.

If only myPassword is installed, the ProfileValidator.exe will check for an empty Password Reset Profile and require that it be completed at logon.

If rDirectory is installed and licensed in addition to myPassword, the ProfileValidator.exe can be configured to leverage the Enforce Profile Validation feature and require the user to certify or validate virtually any attribute associated with their Active Directory account.

See **Installation and Setup myPassword Optional Features.pdf** in the documentation folder for details configuring and deploying this tool via GPO policies.

Reporting in myPassword

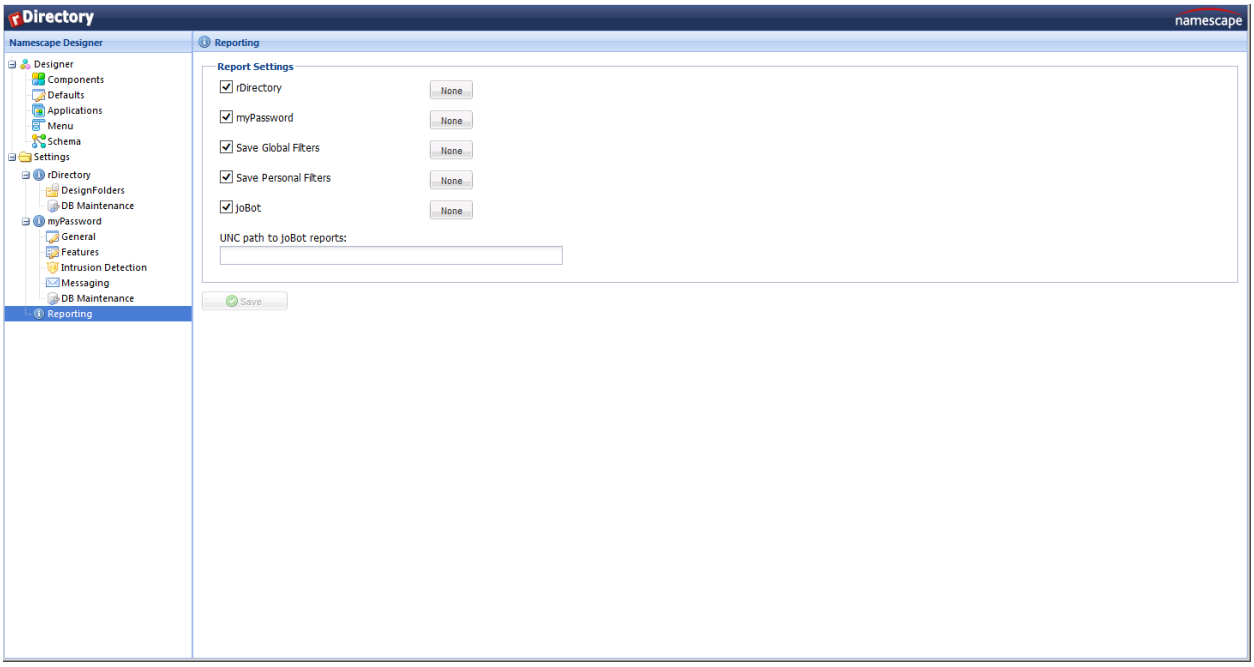
myPassword and rDirectory include a Report Console that allows you to search for specific user activity, view activity summaries, and generate and export activity reports in various formats. The report console may be accessed by granting the report access role in the Namescape Designer, and then selecting the Report Console button in the upper right corner of the rDirectory client.

Configuring Report Access

To add or change a role, open the Designer and select the Reporting node.

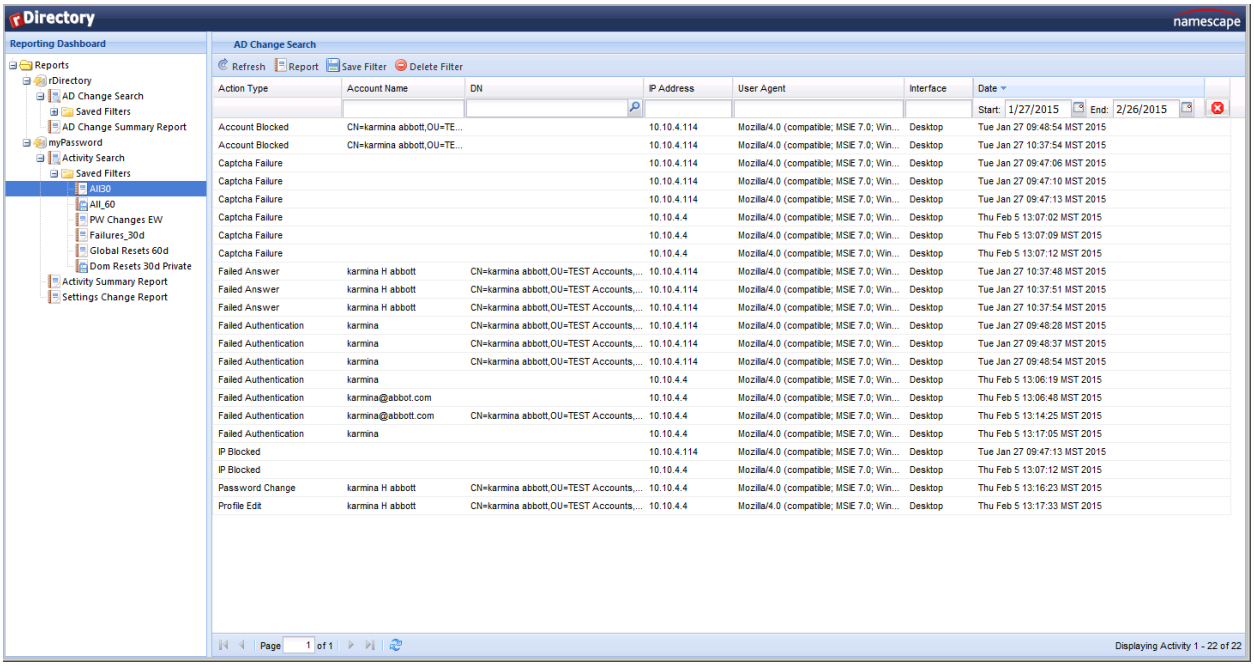
To set a role, select the Role button to open the Roles editor and add the desired claim or group to either allow or deny access to the selected component. Click **Save** when you have completed your changes.

> ***NOTE:*** *If roles are not defined, everyone will be granted Allow access by default.*



Saved Filters

The Report Console allows users granted the appropriate roles to create and save custom report filters. These filters let users quickly generate reports with the same filter parameters.



Two filter types are available.

Global Filters

When a Global filter is created, all other users who have been granted the appropriate role access to rDirectory, myPassword or joBot will be able to see the filter. The ability to create a Global filter can be limited by defining the *Save Global Filter* role under Report Settings..

Personal Filters

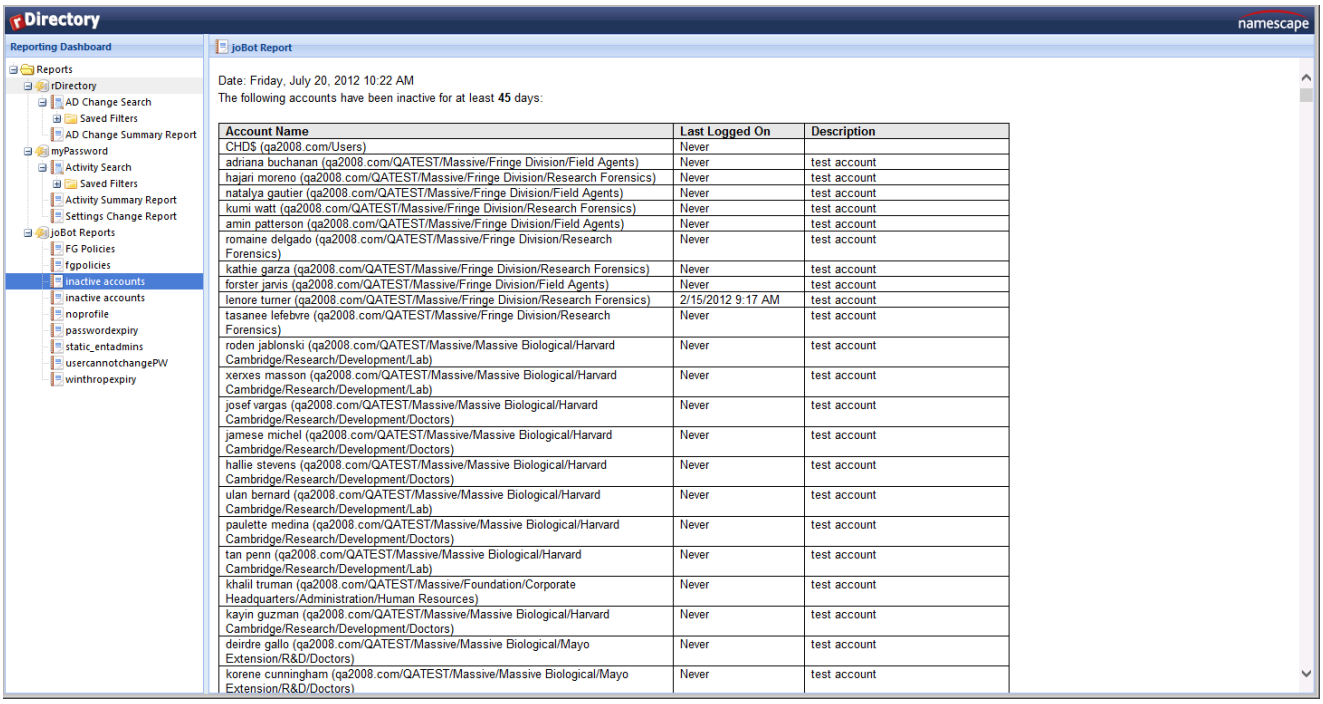
When a Personal Filter is created, only the user who created the filter may see it. The ability to create a Personal Filter can be limited by defining the *Save Personal Filters* role under Report Settings.

Enabling joBot Reports in the Report Console

The Report Console can display generated reports saved to a file share by joBot. To enable the display of joBot reports, select the *UNC path to joBot reports* setting and simply enter the UNC or file system path to the directory where the reports are saved.

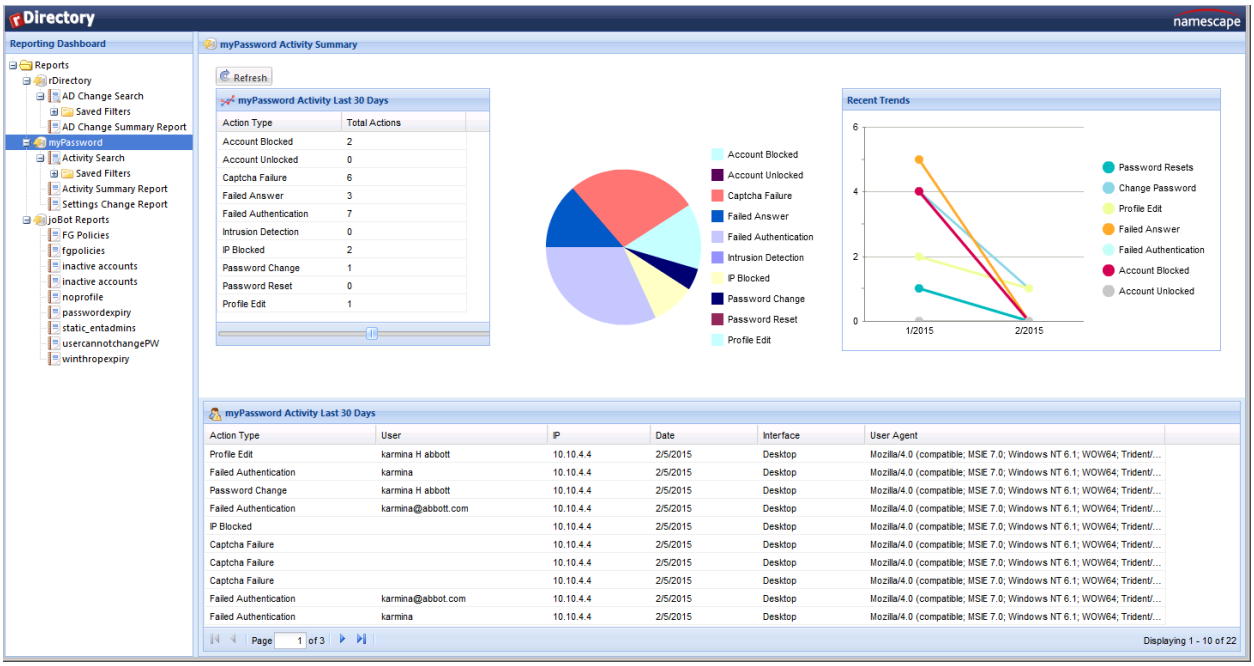
Once a valid path is entered, a new joBot node will appear in the Report Console, and any reports that have been generated in either HTML or text format will be displayed.

NOTE: *For the best possible display, we recommend generating joBot reports in HTML format.*



Using the Report Console

To view activity for a specific product, expand the **Reports** node and select the product on which you wish to generate a report. You will be presented with the product specific **Activity Summary** view.

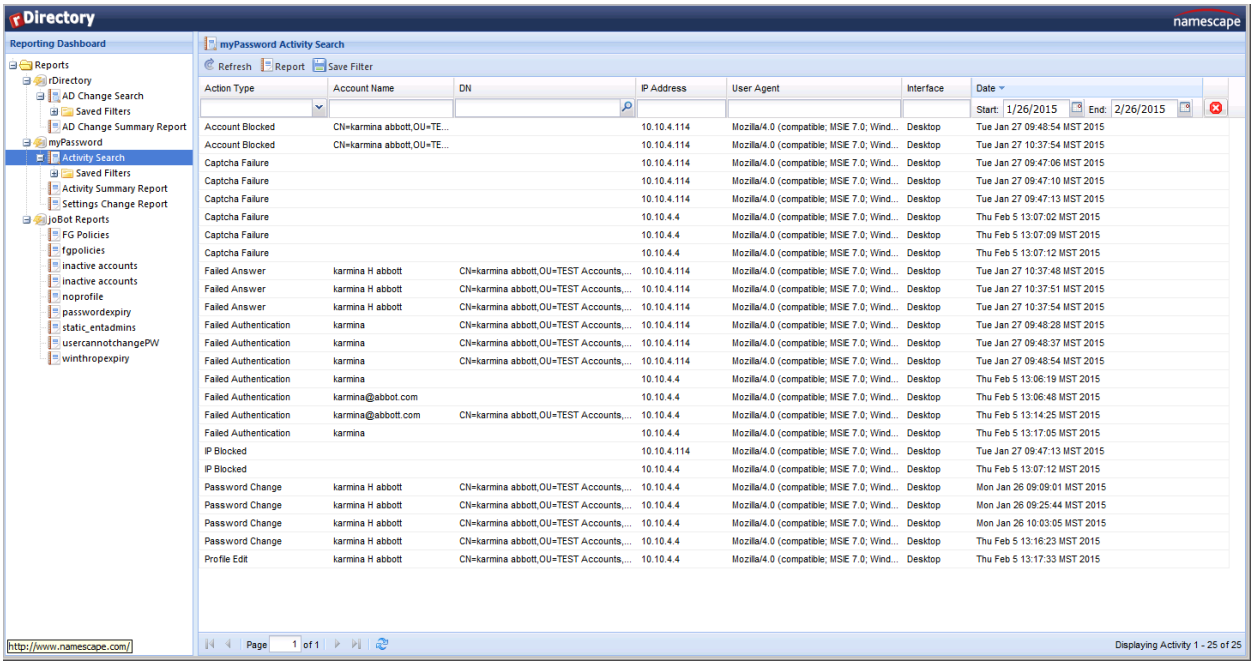


In this view, you have the ability to display all activity for a given time period, as well as charts showing activity count and trending information. To change the time period displayed, simply move the slider to the left or right. The graph, summary, and detail views will update automatically.

In addition to the summary view, there are a number of included reports that can be generated, ensuring a simple and effective way to audit events in your environment.

Activity Search

The **Activity Search** (*AD Change Search* in rDirectory) view provides a filterable display containing detailed activity information in your environment. It allows you to filter down a list of actions, including *Action Type, Account Name, DN (Distinguished Name), IP address*, *User Agent, Interface type* and *Start\End Date* , and generate a report based on those results that can be exported to various formats, including Excel, PDF and Word.



The data shown in the Activity Search window can be displayed however you desire. Columns may be moved, sorted, added and hidden to fit your needs.

Options include:

Sort Ascending or Descending

Click the column header to sort the list of activity by ascending or descending order within that column. Click once for ascending order and again for descending order, or select **Sort Ascending** or **Sort Descending** from the drop down list of options.

Drop Down List of Options

Click the down arrow that displays next to each column header when selected to see a list of available options, including Sort Ascending, Sort Descending and Columns.

Columns

Select the **Columns** option from the drop down list to show or hide specific columns in the display window.

Page

Use the arrow keys at the bottom of the screen to advance the report results by page.

Refresh

Click the **Refresh** icon at either the top or bottom of the screen to update the filtered results and redisplay the entire list in descending date order.

Report

Selecting the **Report** button will generate an exportable report based on your filtered activity search results. This report can then be exported in Excel, PDF or Word formats.

Filtering Results

Each column in the Activity Search represents a different filter used to narrow down the activity data search results.

Action Type

Click the drop down to display all action types available. Place a check in the box next to the action or actions you wish to include in the filtered results.

Account Name

This column allows you to filter activity data based on the account that performed the action. To apply an account name search filter, simply begin typing in the name of the account, and if myPassword finds a partial match, the activity results will dynamically update based on the characters as they are typed in.

DN (Distinguished Name)

This column filters activity data based on the DN (Distinguished Name) of the account that performed an action. Be aware that certain activity will only display the Naming Context, and not the full DN, of the account that performed the action. To select an account DN, click the magnifying glass to the right of the field to open the object selector dialogue box. Locate and click on the desired account, and click **Select** to filter the activity results.

IP Address

This column allows you to filter activity data based on the originating IP address.

User Agent

This column will display information about the browser used to perform the password action

Interface

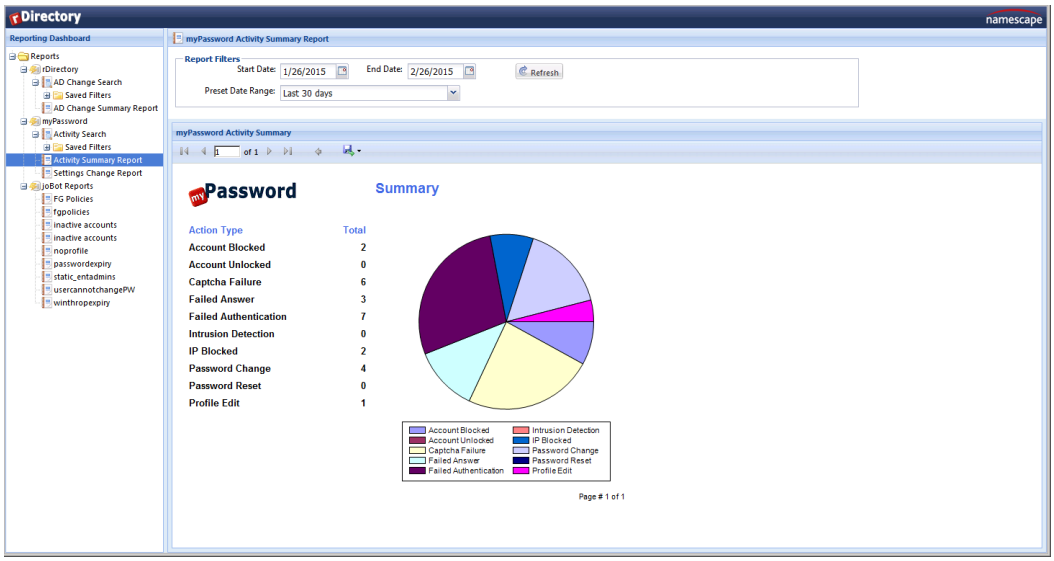
This column will display the originating type of device used to perform the password action. Possible values include Desktop, Mobile or Tablet.

Start and End Date

Click the calendar icon in the Date entry box to display the Calendar object. Select a date from this calendar to display all activities for a defined start and end date. The filter defaults to the last 30 days of activity.

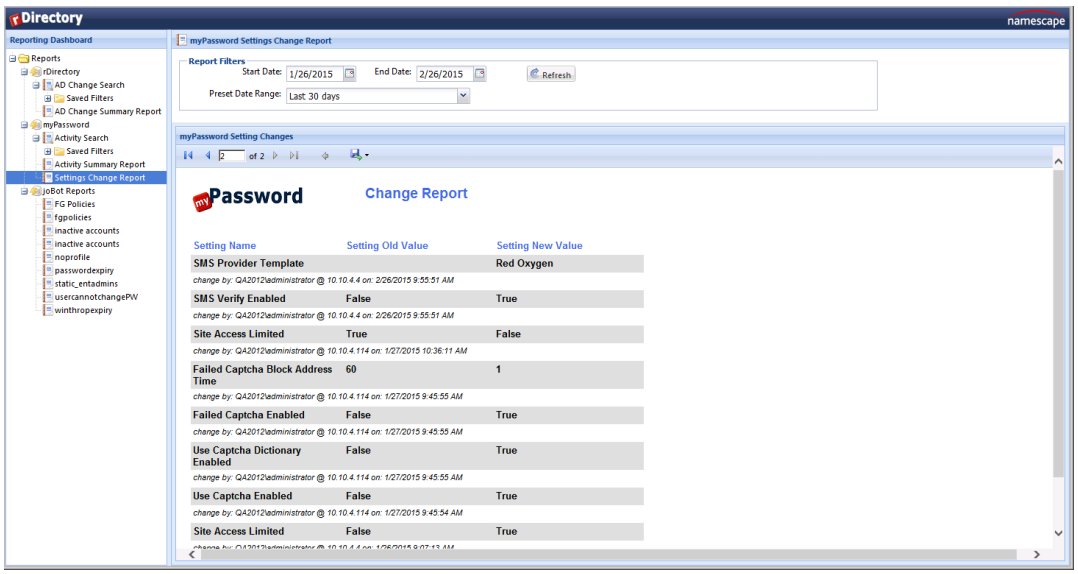
Activity Summary Report

The **Activity Summary Report** (*AD Change Summary Report* in rDirectory) view shows a static summary, with corresponding pie graph, of all myPassword activity for a defined time period.



Settings Change Report

The Settings Change Report displays any settings that have been modified within myPassword for a defined time period, listing the original value and the new value for each setting. The first page of the report displays a summary and follows with a breakdown of changes.



Start and End Date

Click the calendar icon in the Date entry box to display the Calendar object. Select a date from this calendar to display all activities for a defined start and end date. The filter defaults to the last 30 days of activity.

Report Options

Once the report has been generated, you can navigate through the pages of the report by using the arrow keys. You may also expand or shrink the report display size by using the zoom dropdown.

To export the generated report, select the desired format from the drop down list. Currently available formats are Excel, PDF and Word.

Appendix A – Customizing myPassword

Customizing myPassword has changed significantly from previous versions of the product. The 2.x and 3.x versions of myPassword allowed direct access to the underlying HTML. In 4.x versions of the product, other than a custom landing page, this is no longer possible as all content is dynamically generated. This means certain customization options available previously may not be possible without the assistance of Namescape Professional Services.

NOTE: *myPassword customization/training is not included as part of the standard product support package. Professional Services are available for purchase if additional assistance beyond this documentation is required.*

Client Customization

A limited number of styles within myPassword are customizable by an administrator through the Namescape Designer, or by modifying files in the installation directory.

The look of the myPassword client is based on the currently defined theme, located in the *\myPassword\App_Themes* directory. Each selectable theme will have a contents subfolder containing its own unique set of files and images.

The ***myPassword.css*** file in each theme folder defines major CSS classes which control styles such as background color, font, and elements of the main menu page. In most cases, selecting an existing theme in the Namescape Designer and then modifying the *myPassword.css* file should achieve the desired effect.

NOTE: *The **myPassword-all.css** file is a minified version of all styles necessary for the base components of the application. Editing this CSS file is not recommended, and is not supported by Namescape.*

If the only customization desired is replacing the myPassword logo with your own branded logo, simply rename your custom png image to ***myPassword.png*** and replace the existing ***myPassword.png*** file in the root of the myPassword website directory.

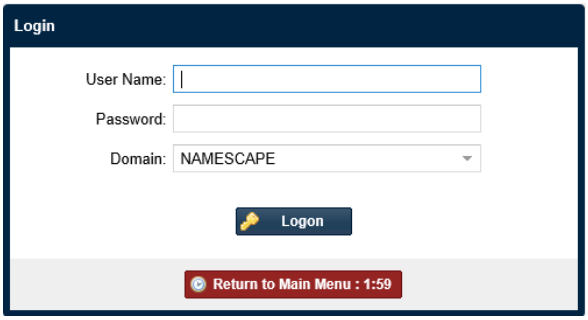
Themes

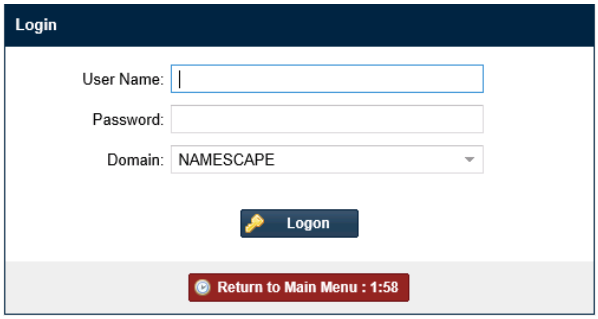
The majority of the CSS that controls the look and feel of myPassword is part of a predefined theme. The currently selected theme can be changed in the Namescape Designer under myPassword | General | Appearance. Changing a theme will alter the colors of all elements within the client, but will not affect text or the logo graphic.

NOTE: *If you are unable to achieve a desired look with the options provided, Namescape Professional Services are available for purchase to assist you with creating a custom theme to fit your needs.*

Use Classic Dialogue Style

In addition to selecting a theme, you also have the option to make dialogue boxes appear similar to those in previous versions of the product. By enabling this setting, the dialogue boxes will appear with a thinner border and have squared corners, rather than rounded.



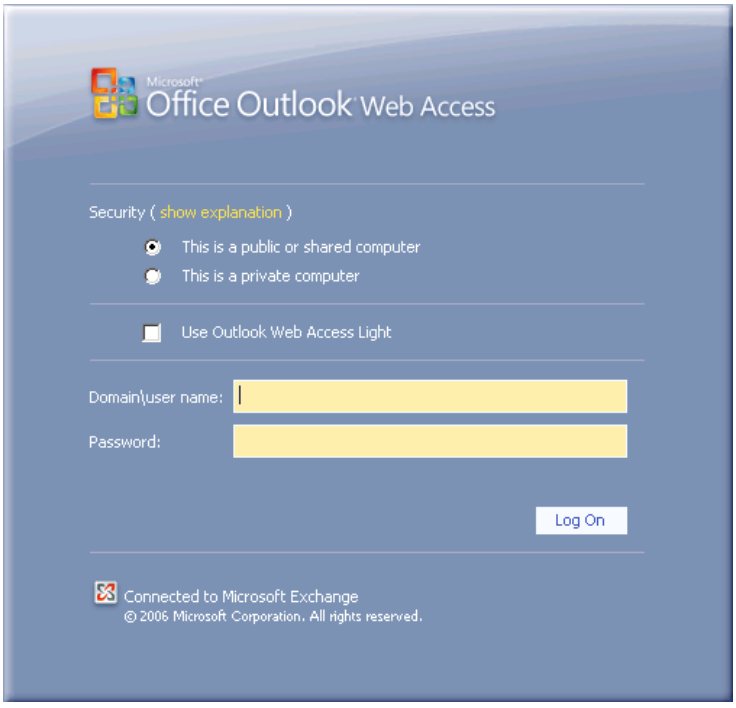


Adding a myPassword link to the Outlook Web Access Logon Page

NOTE: *Customizing the Outlook Web Access (OWA) Logon Screen may require advanced customization techniques not included in this document. Professional Services are available for purchase if additional assistance beyond this documentation is required.*

The procedures included in this document have been confirmed to work with Outlook 2003 and Outlook 2007.

By default, the Outlook Web Access logon screen should look similar to the picture below:



To include a direct link to myPassword on this screen, complete the following steps:

NOTE: *Please make a backup of any files before modifying them.*

1. On the server hosting OWA 2003 or 2007, navigate to the following directory:

Outlook 2003 - [%Program Files%]\Exchsrvr\exchweb\bin\auth\[Country subdirectory]
Outlook 2007 - [%Program Files%]\Microsoft\Exchange Server\ClientAccess\Owa\auth

Example:

OWA 2003 - C:\Program Files\Exchsrvr\exchweb\bin\auth\usa
OWA 2007 - C:\Program Files\Microsoft\Exchange Server\ClientAccess\Owa\auth

2. In this directory, you will find the file logon.asp (or logon.aspx). Create a copy or backup of this file before proceeding. Once a backup copy has been made, open the logon.asp or logon.aspx file with a text editor such as Notepad.
3. Find the following section of HTML markup:

For Outlook Web Access 2003:

```
<TR>
<TD NOWRAP width="1%"><P><LABEL for="password"><%=L_Password_Text
%></LABEL></P></TD>
<TD width="98%"><INPUT type="password" autocomplete="off" style="width:100%"
id="password" name="password" size="25" maxlength="256"
onfocus="g_fDoFocus=false;"></TD>
<TD width="1%"><INPUT type="submit" value="<%=L_LoginButton_Text %>"
id="SubmitCreds" name="SubmitCreds"></TD>
</TR>
```

Insert the following lines right after the closing </TR> above :

```
<tr>
<td> </td>
</tr>
<tr>
<td align="center" colspan=4 style="width:100%">
<a href="[myPassword URL]?[OWA URL]">Forget your password? Click here to reset it
using myPassword.</a></td>
</tr>
<tr>
<td> </td>
</tr>
```

Replace the [myPassword URL] with the URL of your myPassword website and replace the section [OWA URL] with the URL of your OWA website.

Example:

Replace: <a href="[myPassword URL]?ReturnURL=[OWA URL]"> With:

<a href="http://myserver/mypassword.aspx?ReturnURL=https://myserver/exchange">

> ***NOTE:*** *The above change adds 3 rows to the HTML table and puts the myPassword link in the middle row in the center.*

For Outlook Web Access 2007

Highlight the </td>, </tr> and </table> in the file, as shown below in the first figure. This is right below <% } %> and right above <table class="mid tblConn"> of the logon.aspx file.

```
</td>
                        </tr>
                    </table>
                    <table class="mid tblConn">
```

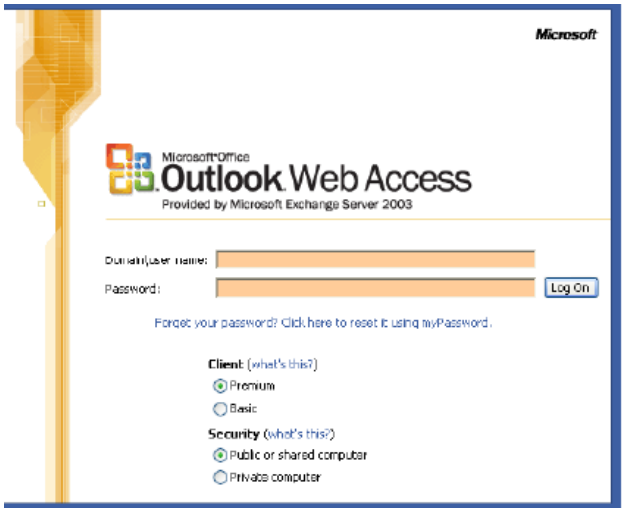
Replace the highlighted section with this:

```
                                <% } %>
                                </td>
                        </tr>
                    </table>
                    <table class="mid">
                        <tr>
                    <tdalign="center">
                    <a
href="http://myserver/mypassword.aspx?ReturnURL=https://myserver/exchange">Forgot your password? Click here to reset using myPassword.</a>
                                </td>
                        <\tr>
                    </table>
```

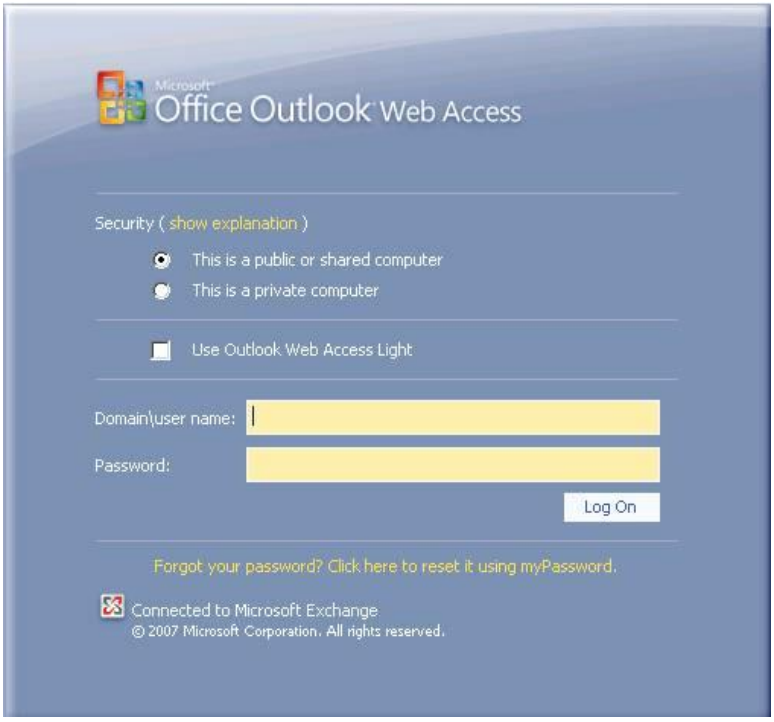
4. Once the version appropriate changes have been made, save the file and test by reloading the Outlook Web Access site.

You should now see a new myPassword link displayed below the password entry field on the logon page. It will look similar to this:

OWA 2003



OWA 2007



Redirecting the IWA failed logon page to the myPassword site

This section of the document describes how to redirect users to the main myPassword site in the event of a failed logon from any website using Integrated Windows Authentication (IWA), including SharePoint.

1. Using Notepad, edit the 401-1.htm file, by default found under:

   C:\Inetpub\custerr\en-US\

2. Find the following section of HTML markup:

```
</STYLE>
</HEAD><BODY><TABLE width=500 border=0 cellspacing=10><TR><TD>


<h1>You are not authorized to view this page</h1>
You do not have permission to view this directory or page using the credentials that you supplied.
<hr>
<p>Please try the following:</p>
```

3. Modify the <BODY> element to include **onload="redirect()">**

```
</STYLE>
</HEAD><BODY>onload="redirect()"> <TABLE width=500 border=0 cellspacing=10><TR><TD>


<h1>You are not authorized to view this page</h1>
You do not have permission to view this directory or page using the credentials that you supplied.
<hr>
```

```
<p>Please try the following:</p>
```

4. Now find the following section of HTML markup at the bottom of the file:

```
<ul>
<li>Go to <a href="http://go.microsoft.com/fwlink/?linkid=8180">Microsoft Product Support
Services</a> and perform a title search for the words <b>HTTP</b> and <b>401</b>.</li>
<li>Open <b>IIS Help</b>, which is accessible in IIS Manager (inetmgr),
 and search for topics titled <b>Authentication</b>, <b>Access Control</b>, and <b>About
Custom Error Messages</b>.</li>
</ul>

</TD></TR></TABLE></BODY></HTML>
```

5. Insert the following lines right after </BODY> and before </HTML>

```
<script language = "javascript">
function redirect(){
window.location = "http://mp1";
}
</script>
```

It should read as follows:

```
</TD></TR></TABLE></BODY>
<script language = "javascript">
function redirect (){
window.location = "http://mp1;
}
</script>
</HTML>
```

Where 'http://mp1' is replaced with the URL of your myPassword website.

Example:

Replace:

```
window.location = "http://mp1";
```

With:

```
window.location = "http://[myPassword URL]";
```

6. Save the file and test.

How to change the language in myPassword

NOTE: *This section describes how to manually configure the language support in myPassword. The product ships with German, Spanish and French already translated. For those languages, simply change your browser language setting.*

In addition to the included languages, myPassword may be configured to display any other custom language desired. Namescape is not responsible for translation errors resulting from the following procedure.

Setting up the directory infrastructure

The example we will use will demonstrate how to create a sub-folder structure for the Italian language.

1. Locate the Resources folder, located by default at:

   C:\inetpub\wwwroot\myPassword\Resources

2. Create a new folder under the \Resources folder named '**it**' for Italian
3. Open the \en-us folder under \Resources and copy all the folders and files to the new \it folder.
4. Copy the DefaultResource.xml from the \Resources folder and paste it in the new \it folder
5. Rename the DefaultResource.xml in the \it directory to Resource.xml
6. In the \it folder, open the resource.xml and change the item key value that corresponds with the object that you want to display in Italian.

NOTE: *Use extreme caution when making changes to the Resource.xml file. If this file is modified incorrectly, the desired changes will not take effect and may cause further problems for the page display. Namescape Support does not include assisting with customizations.*

The following edits will change the Product Description text:

Before

<item key="productdescription">Self-Service Password Management</item>

After

<item key="productdescription"> Self-Service parola d'ordine gestione</item>

7. Restart IIS
8. Change the language in your web browser to 'it' for Italian
9. Launch the myPassword website. The product description should now display the Italian text.

By modifying the key values in the resources.xml file, you can change any text for a language specific page that is triggered by the browser default language settings.

namescape