



Password Reset Server User Guide

Table of Contents

Getting Started.....	3
Product Overview	3
Installation.....	3
Terminology	3
Security Policies.....	4
Overview	4
Administering Security Policies	4
Creating a New Security Policy	4
Modifying an Existing Security Policy	6
Configuring a Security Policy	6
Questions	11
Overview	11
Question Types.....	11
Setting up Questions.....	12
Creating a new Question.....	12
Modifying an Existing Question	12
Configuring a Question.....	12
Deleting Questions	14
Importing Question Answers	14
Windows Login Integration	16
Overview	16
Deployment.....	16
Configuring the Host Name.....	17
Configuration	18
General Configuration.....	18
Configuring SMTP Access	19
Username Recovery Configuration	20
Configuring TeleSign™	20
Configuring ProxStop™	21

Enrollment	22
Enrolling	22
Overview	22
Enrollment Process	23
Enrollment Reminders	25
Overview	25
Creating a New Reminder	27
Access Control.....	28
Overview	28
Defining Permissions	28
Default Roles	30
Administering Roles	30
Assigning Roles	31
By Role.....	32
By User or Group	32
Role Auditing	34
Overview	34
Role Audits.....	34
Role Assignment Audits	35
Domain and User Configuration	36
Overview	36
Administering Domains	36
Password Reset Server Encryption	37
Overview	37
AES-256 (Advanced Encryption Standard)	37
SHA-512 (Secure Hash Algorithm)	37
SSL/TLS (Secure Socket Layer)	37
Administrative Reports	38
Overview	38
Security Hardening Report	38
Backup / Disaster Recovery	39
Automatic Backups	39
System Log.....	39
Overview	39

Getting Started

Product Overview

Password Reset Server is a web-based application that allows users in your Microsoft Active Directory Domains to reset their password without the help of an Administrator. The Administrator chooses which users and Organizational Units are allowed to reset their passwords. These users then enroll in a list of questions that the Administrator chooses. When a user attempts to reset their password, they are prompted to answer all of their questions to verify their identity. Once the identity has been confirmed, Password Reset Server will reset and unlock the user's account.

Installation

Password Reset Server is distributed as an MSI or as a ZIP file of the web application. To install Password Reset Server and the software it depends on (such as SQL Server and Internet Information Services) please see our [Installation Guide](#).

Terminology

These terms are used to refer to specific features or concepts within Password Reset Server.

Administrator

Password Reset Server does not have a true "Administrator" or Administrative user, however within this guide an administrator refers to the user(s) who manage the system. Administrators have control over the global security and configuration settings.

Access Control (RBAC)

Password Reset Server uses role based access to determine which users and groups have access to specific features within the application. Access Control allows fine and granular permission for each user. For more information, see the section on

[ACCESS](#) Control.

Enrollment

Enrollment is when a domain user has successfully answered all of the questions for their Security Policy. Once a user has been enrolled, they are allowed to reset their password when they confirm their identity by successfully answering their questions. For more information, see the section on [ENROLLMENT](#).

Questions

Questions are answered by a user and must be answered to complete enrollment. For a user to enroll, they must answer each question that is part of their Security Policy which will confirm their identity to Password Reset Server. When the identity has been confirmed, the user is then prompted for their new password. For more information, please see the section on [QUESTIONS](#).

Security Policies

A Security Policy defines which questions a user or group of users must enroll in and will have to answer when they attempt to reset their password. For more information, please see the section on [SECURITY POLICIES](#).

Security Policies

Overview

A Security Policy is a set of questions defined by the administrator that the users must answer to complete their enrollment. Password Reset Server ships with a default Security Policy; however an administrator can change the Security Policy to meet the company or industry security requirements. Multiple policies can be created which allow different users to answer different sets of questions. This allows stronger policies to exist for more privileged domain accounts, or having different sets of questions per group if the Security Policy is specific to a group of people. A single user, group, or organizational unit can belong to only one Security Policy.

Administering Security Policies

An administrator can login to Password Reset Server and click the “Administration” link on the top navigation bar, then click “Security Policies”.

Creating a New Security Policy

From the Security Policies administrative page, click the “Create” button. You can then type the name of your new Security Policy, such as “Financial Users Policy” and a description that will help describe who this Security Policy applies to. Click “Create” to create the new Security Policy.

Create Security Policy

Name

Financial Users Policy *

Description

Policy for users that have access to sensitive fin

Cancel

Create

Modifying an Existing Security Policy

To modify an existing Security Policy, click “Administration” on the top navigation bar and then click “Security Policies”, and finally click the name of the policy that you would like to configure.

Configuring a Security Policy

After creating a new Security Policy or modifying an existing one, you can configure it and tailor it to meet your requirements.

To edit the description or name of a Security Policy, click the “Edit” button on the Security Policy overview page, or click “Activate” to enable the Security Policy. An inactive Security Policy means that users can no longer be assigned to it.

NOTE: A Security Policy cannot be activated unless at least one question is assigned to it. By default, new policies do not have any questions.

Configuring Questions

To view the assigned questions or modify them, click the “Questions” tab at the top of the overview of the Security Policy.

To modify which questions belong to the policy, click the “Edit” button. You can then move items between “Required” and “Available” by selecting the item and clicking the single arrow left or right.

The screenshot shows the configuration interface for a Security Policy, specifically the "Questions" tab. At the top, there are navigation tabs: "General", "Questions", "Users", "Security", "Alerts", and "Expiration". Below the tabs, there are two dropdown menus: "Minimum Questions for Enrollment" (set to 3) and "Minimum Correct Answers For Reset" (set to 2). The main area is divided into two columns: "Required" and "Available". The "Required" column contains a list of questions: "Name Question", "Parent Name Question", "Robot Question", and "Image Question". The "Available" column contains a list of questions: "Email Question", "Phone Question", and "SMS Question". Between the two columns are four arrow buttons: a double left arrow, a single left arrow, a single right arrow, and a double right arrow. At the bottom of the interface are two buttons: "Cancel" and "Save".

You can also move all questions from Required or Available by clicking the double arrow.

TIP: You can move multiple questions at once by holding the Control Key (Ctrl) and clicking more than one in the list, then clicking the left or right arrow.

To give your users flexibility, you can set how many questions must be answered for enrollment and password reset using the “Minimum Questions for Enrollment” and “Minimum Correct Answers For Reset” settings. For example, based on the image above users must enroll in three questions from the list in the Required box (Name, Parent Name, Robot, and Image). When they are answering these questions in order to reset their password, they must answer two of the three questions they enrolled in correctly.

Once you have your desired questions, click “Save”, or “Cancel” to abandon your changes.

Configuring Security Policy Members

Users may be assigned to a Security Policy directly, or by Organizational Unit (OU) or Group. To view OUs, Groups, and Users that are part of the Security Policy, click the “Users” tab at the top of the overview of the Security Policy.

The screenshot shows a web interface for configuring security policy members. At the top, there are tabs for General, Questions, Users, Security, Alerts, and Expiration. The 'Users' tab is selected. Below the tabs, it says 'User Count: 20 Click to preview'. There are two main sections: 'Include In Security Policy' and 'Exclude From Security Policy'. The 'Include' section contains a list of items: 'Thycotic' and 'testparent\Administrators', each with a close button (x). Below this list is a 'Show Unavailable' link. The 'Exclude' section is currently empty. At the bottom, there are two input fields labeled 'Include' and 'Exclude', and two buttons: 'Save' and 'Cancel'.

To add new users, either directly or by group or OU, first click Users, then click Edit. Next, type the name of the object you want to include in the Include box. An autocomplete dropdown list will display showing you possible matches. Click the correct match or use the arrow keys and press Enter. To remove users, groups, or OUs click the (x) next to the object you want to remove. To save your changes, click Save.

Sometimes you may want to include only some of the members of a group or OU. To exclude users, type the name of the object you want to exclude (user, group, or OU) in the Exclude box. An autocomplete dropdown list will display showing you possible matches. Click the correct match or use the arrow keys and press Enter. This will exclude the selected item from this Security Policy. Excluding a group will exclude all of that group’s members. Excluding an OU will exclude all of the OU’s members.

Advanced: Password Reset Server allows you to create complex include / exclude structures. For example, you may include an OU, exclude groups which have members of the included OU as members, and then include specific users that are in the excluded group. The resolution for include/exclude conflicts is that rules for groups take precedence over rules for OUs and rules for users take precedence over rules for groups. Exclusions take precedence over inclusions.

For example: Sara is in the Managers group and resides in the Accounting Dept OU. A policy is set up for the Accounting department, so it includes the Accounting Dept OU. However, managers have their own policy, so the Managers group is excluded. Lastly, Sara opts in to the same policy as the rest of accounting, so her user is included.

Note that you can see the total number of included users next to User Count at the top of the page. To see which users are included, click the 'Click to Preview' link.

Configuring Security

To view or edit the security settings of a Security Policy, click the "Security" tab at the top of the policy overview.

General	Questions	Users	Security	Alerts	Expiration
Mask Answers		No			
Force Enrollment Test Run		No			
Grace Attempts		3			
Maximum Attempts		10			
Delay Interval (minutes)		10			
Delay Multiplier		2.000			
Forgiven Reset Interval (minutes)		1440			
Allow Unlock Without Password Reset		Yes			
Change Password After First Enrollment		No			

[Edit](#) [Back](#)

Mask Answers

When a user is enrolling in the questions for this Security Policy, all of the answers that they type will be masked instead of showing the real characters entered.

Force Enrollment Test Run

When a user completes the enrollment process for this Security Policy, they will be forced to do a dry test-run of the reset process without actually resetting their password. This ensures that the user is comfortable with answering the questions.

Grace Attempts

The number of successive failures a user can have when resetting their password before they are forced to wait before making another attempt. Forcing a user to wait between tries after they fail the number of grace attempts is to ensure a malicious person does not try to brute-force the reset by guessing common answers to questions.

Maximum Attempts

The maximum number of failures a user can have before they must wait for the Forgiven Reset Interval to pass.

Delay Interval

The time, in minutes, a user must wait before they are allowed to try again after they use all of their grace attempts. For example, given three grace attempts, the user will be forced to wait this many minutes before they are allowed to try a fourth time.

Delay Multiplier

The factor for which to increase the Delay Interval between each successive failure the user makes. For example, given a Delay Interval of twenty, a Delay Multiplier of two, and a grace attempt of three, the user will have to wait twenty minutes before being allowed to make a fourth attempt, 40 minutes before making a fifth attempt, and so on. Set the Delay Multiplier to one if you do not wish to use this feature.

Forgiven Reset Interval

The amount of time, in minutes, must occur for the number of failures to decrease. For example , given a Delay Interval of twenty, a Delay Multiplier of two, and a grace attempt of three, and a Forgiven Reset Interval of 1,440 (1 Day), and the user failed 5 times in a row resulting in an 80 minute delay, after 1 day a passes the delay will drop down to 40, then 20, etc.

Allow Unlock Without Password Reset

If this flag is 'Yes', after users prove their identity they can decide to unlock their account instead of resetting the password.

Change Password After First Enrollment

If this flag is 'Yes', after a user finishes enrolling, they are taken to a page where they can change their password.

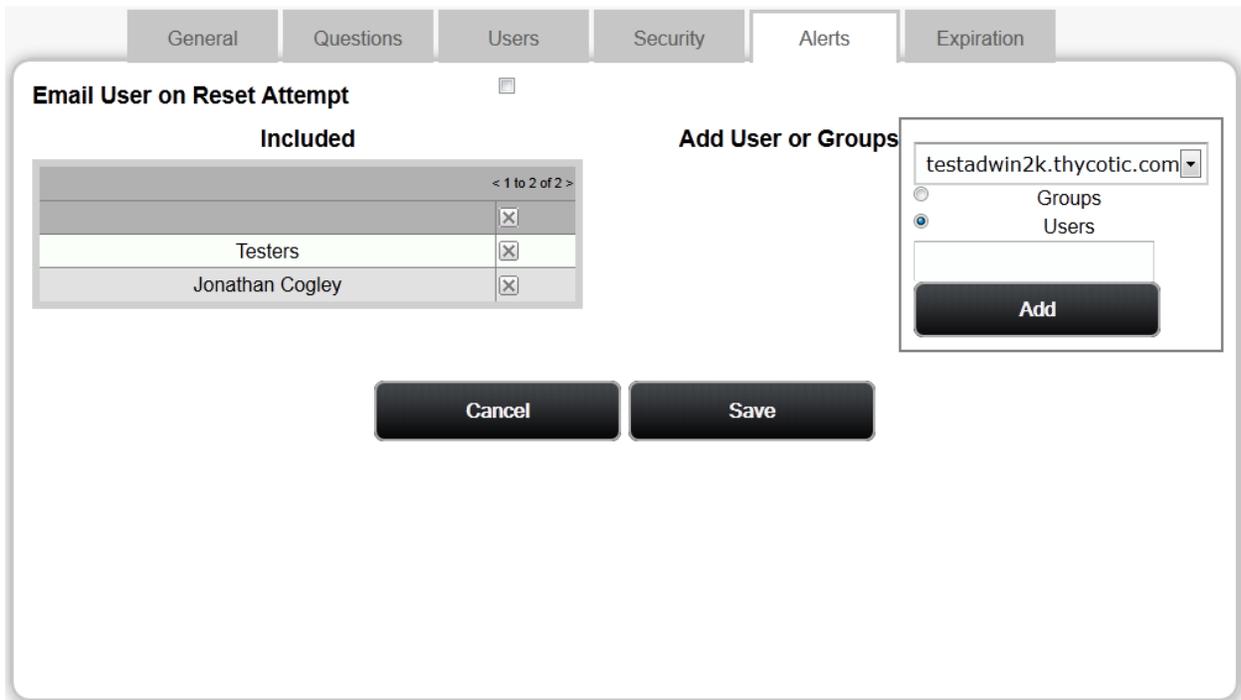
To edit these values, click the "Edit" button. From the Edit screen you can click "Save" to save your changes or "Cancel" to abort them.

Alerts

To view or edit the alerts, click the "Alerts" tab at the top of the Security Policy overview.

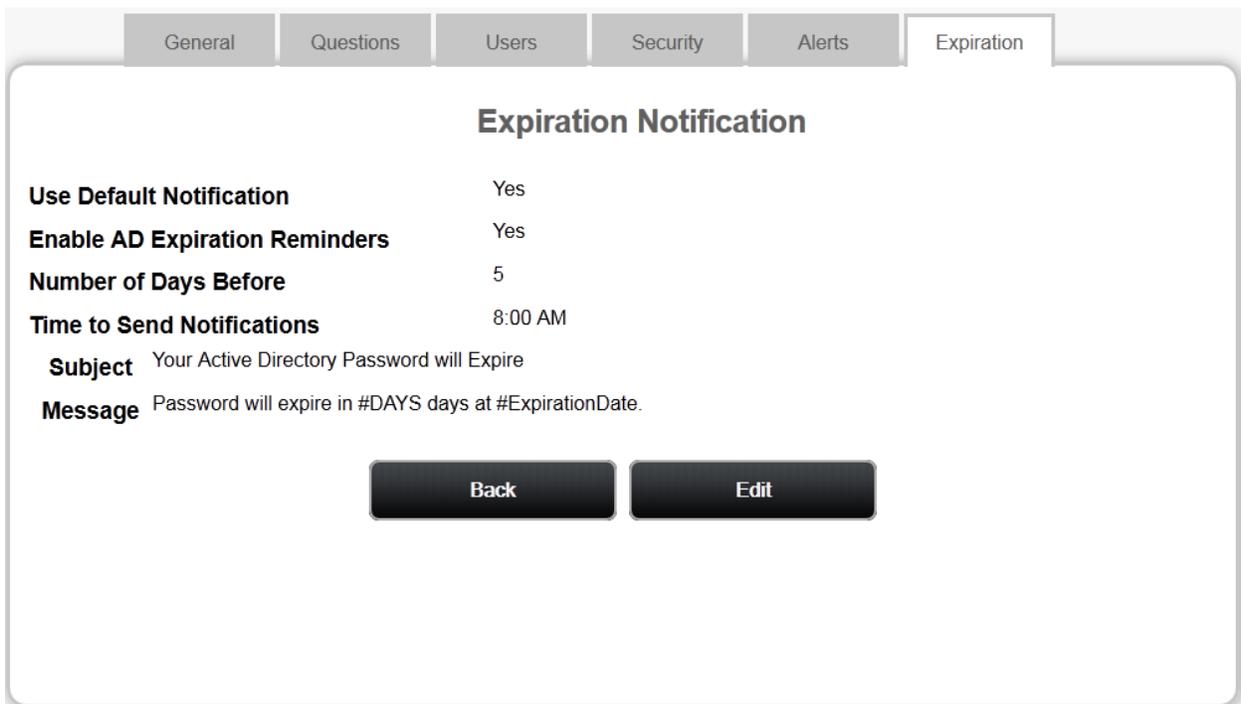
Alerts allow specific users or group members to receive an email when a user or group member that is assigned that Security Policy completes the enrollment or when they attempt to reset their password.

To make additional users and groups receive alerts, enter the user or group in the search box and click "Add". To stop users and groups from receiving alerts, click the "x" next to the user or group name.



Configuring Expiration Notifications

To view or edit the Expiration Notification settings of a Security Policy, click the “Expiration” tab at the top of the policy overview.



When Enable AD Expiration Reminders is set to true, members of this Security Policy will receive an email before their AD account's password expires. To adjust the time the email is sent, change the "Time to Send Notifications" setting. To set how many days before the expiration the email should be sent, change the "Number of Days Before" setting. Note, no email will be sent on the actual day of expiration. If the "Use Default Notification" setting is true, the standard email will be sent. To change the subject and body of the email, set "Use Default Notification" to false and change the Subject and Message values.

Questions

Overview

Password Reset Server uses questions to confirm the identity of a user before they can reset their password. As part of the enrollment process, a user will answer all of the questions that are a part of the Security Policy they are assigned. They must also answer all questions correctly before resetting their password.

Password Reset Server stores all of the answers to a question using an irreversible algorithm called [SHA-512](#). This ensures that all answers are kept confidential. Even a malicious user that has access to Password Reset Server's database will be unable to extract the users' answers.

Question Types

Password Reset Server supports multiple types of questions. This ensures variety to increase security.

Text Question

A text question is displayed in the form of text which the user must supply an answer for. For example, a text question could be "In which city have you lived in the longest?"

Text questions should be personal and not easy to guess, such as "What color is your car?" A malicious user could easily guess a common car color – or may even know the answer if they know the user personally.

Image Question

An image question is set of images which the user is given and will need to recall when resetting their password. During the enrollment process, the user will be shown a configurable number of images. During the password reset process, they will be asked to recall the images they were displayed.

Email Question

An email question will email the user a pin code during the password reset process. The user will then have to type in the pin the email provided. This is common for users that have access to email with a mobile device such as a smart phone.

Phone Question

A phone question will call the user and tell them a five digit code during the password reset process. They will then type in the five digit code to answer the question. During the enrollment process, the user will provide their phone number.

SMS Question

A phone question will send the user a PIN code SMS message during the password reset process. They will then type in the code to answer the question. During the enrollment process, the user will provide their phone number.

A phone or SMS question requires that Password Reset Server be configured with a phone provider. See the sections on [CONFIGURING TELESIGN™](#) or [Configuring ProxStop™](#) for additional information on configuration.

Setting up Questions

Creating a new Question

To create a new question, click the “Administration” link in the top navigation bar and click “Security Questions”, then select the question type you’d like to create from the drop down list.

Modifying an Existing Question

To modify an existing question, click the “Administration” link in the top navigation bar and click “Security Questions”, then click the name of the question that you would like to edit.

Configuring a Question

After creating a new question or modifying an existing one, you can configure it with additional options. Depending on the question type, there are different configuration options.

Text Question

Question Name

This is the name of the question that will be displayed during the enrollment process and allow you to refer back to it.

Question Text

This contains the question that will be displayed to the user during the password reset process and must also provide an answer for during the enrollment process.

Minimum Length

This is minimum length of an answer that the user supplies during the enrollment process.

Answer Instructions

Any additional instructions that should be displayed to the user during the enrollment and password reset process.

Image Question

Question Name

This is the name of the question that will be displayed during the enrollment process and allow you to refer back to it.

Image Set

Image set is the set of images that are used during the enrollment process and password reset process. Each set contains sixteen images.

Order Matters

During the password reset process, Order Matters specifies if they user must pick their images in a specified order or not. Picking the images in the wrong order means the user did not answer the question correctly.

Position Randomly

During the password reset process, Position Randomly specifies if the images in the image set are displayed in a different, random order each time.

Enrollment Instructions

Enrollment Instructions are additional instructions to be displayed to the user during the enrollment process.

Answer Instructions

Answer Instructions are additional instructions to be displayed to the user during the password reset process.

Email Question**Question Name**

This is the name of the question that will be displayed during the enrollment process and allow you to refer back to it.

Question Text

This is the question text field which is optional information for the administrator.

Enrollment Instructions

Enrollment Instructions are additional instructions to be displayed to the user during the enrollment process.

Answer Instructions

Answer Instructions are additional instructions to be displayed to the user during the password reset process.

Phone Question**Question Name**

This is the name of the question that will be displayed during the enrollment process and allow you to refer back to it.

Question Text

This is the question text which is optional information for the administrator.

Enrollment Instructions

Enrollment Instructions are additional instructions to be displayed to the user during the enrollment process.

Answer Instructions

Answer Instructions are additional instructions to be displayed to the user during the password reset process.

SMS Question

Question Name

This is the name of the question that will be displayed during the enrollment process and allow you to refer back to it.

Question Text

This is the question text field which is optional information for the administrator.

Enrollment Instructions

Enrollment Instructions are additional instructions to be displayed to the user during the enrollment process.

Answer Instructions

Answer Instructions are additional instructions to be displayed to the user during the password reset process.

After completing a question, click the “Save” button to save the question and return to the questions overview, or click “Save and Add New” to save the question and add another of the same type.

Deleting Questions

You can delete a question as long as there are no Security Policies that use that question. You can delete a question by clicking “Administration”, “Security Questions”, clicking the name of a question, and clicking the “Delete” button.

An error will occur if the question is in use by a Security Policy. The error will indicate which policies are using the question.

Importing Question Answers

Answers to questions can be loaded for users through the Administration->Import Answers page. Answers can be imported in CSV or XML format. Imported answers will not overwrite answers that users have entered already. Import information is logged and can be accessed from the “Import Answers” page by clicking “View Audit”.

Bulk Answer Import

1. Select import format

- CSV Import
Explain
- XML Import
Explain

2. Select import file

Back

View Audit

Import

Windows Login Integration

Overview

Password Reset Server allows integrating into the logon screen of the Windows Operating System. This allows enrolled users to reset their password directly from the logon screen by clicking “Forgot Password?” The desktop logon application will work on the Windows XP operating system or higher.



This functionality utilizes the Credential Provider infrastructure that is built into Windows. It is installed by copying the dynamic link library to the machine and modifying the registry. For technical information, please refer to the appendix.

Deployment

The recommended method of deployment is via MSI. To download the MSI, click “Administration” and then “Windows Login Integration”. At this point the MSI may be downloaded via the “Download Installer” button. The [KB article](#) linked from this page provides instructions on installing the MSI through Group Policy.

MSI Installation Directly or Through Group Policy

The MSI can be installed directly or through group policy and runs on both 32 and 64 bit systems. A reboot may be necessary on certain operating systems. For full instructions on installing from an MSI through Group Policy, see the following KB article: [Client MSI Installation](#)

After installing the Windows Login hook, clients will connect to host [www.passwordreset.mycompany.com] for password resets. To connect to a different host, such as http://myhost/prs_qa/, click [here](#).

Download Installer

Back

Configuring the Host Name

During Password Reset Server's installation, a host name is chosen that will be used when Windows Login Integration clients connect to the server. To change the host name, first click on "Administration", then click the "Windows Login Integration" button, and finally click the 'here' link at the end of the message. This will take you to the following page, where you can change the host name.

Application URL Configuration

These are the current values for use in enrollment reminders and the desktop login. They may be changed by clicking the Edit button.

Host	www.passwordreset.mycompany.com
Application Path	/passwordresetserver/

Edit

Back

Configuration

Password Reset Server's configuration can be accessed by logging in as an administrator and click "Administration" in the top navigation bar and clicking "Configuration". Configuration settings are split between two tabs – General and Username Recovery

General	Username Recovery
Allow Automatic Update Checks	Yes
Email Server	
From Email Address	secret@acme.com
Use SMTP Credentials	No
Use SSL for SMTP	No
Use Custom SMTP Port	No
Verification Provider	Not Set
Default Theme	PasswordResetServer - Default
Default Date Format	M/d/yyyy - 1/31/1980
Default Time Format	hh:mm tt - 09:09 PM
Windows Client Language	English ↕
Force HTTPS/SSL	No
Enable Domain Selector on Login	Yes

[Edit](#) [Back](#)

General Configuration

Allow Automatic Update Checks

When automatic update checks is on, Password Reset Server will perform background checks to see if there are any updates available for download. If updates are available, there will be a notice and link at the top of the page to download the updates. When automatic updates is off, the background check is not done and no notice about updates will be shown on the page.

Default Theme

Password Reset Server ships with two themes, a default theme, and a red theme. The theme setting will apply to all users.

Default Date Format

The default date format controls how dates are formatted in PRS.

Windows Client Language

This setting determines the language which is displayed when using the Windows integration client.

Force HTTP/SSL

When this setting is on, requests coming in to PRS using http will be redirected to use HTTPS.

Enable Domain Selector Login

When this setting is on, there will be a domain selector on the login screen that allows the user to choose his domain.

Configuring SMTP Access

Password Reset Server requires a valid SMTP server to send emails. Please contact your mail server administrator for determining your SMTP server address.

Email Server

The SMTP Server or IP Address provided by your IT administrator.

From Email Address

The email address that Password Reset Server will send emails from. This will appear as the "From" when users receive emails from Password Reset Server. Depending on your email configuration, you may have to use a specific address. Contact your IT administrator for more information.

Use SMTP Credentials

Select this option if the SMTP Server requires specific credentials for access. When this option is selected, the Domain, Username, and Password can be provided.

Use SSL for SMTP

Select this option if the SMTP Server requires access using SSL.

Use Custom SMTP Port

Select this option if the SMTP Server should be accessed through a non-default port (port 25 or ports 465/587 for SSL).

To test your email configuration, click "Save" and then click "Send Test Email". Password Reset Server will send an email to your address using the provided configuration. You should receive an email address if the configuration setup properly.

Username Recovery Configuration

General	Username Recovery
Allow Username Recovery	No
Email Subject Line	Username Recovery
Email Message	The username for this email account is %USERNAME% on domain %DOMAIN%.

Allow Username Recovery

When this setting is on, there will be a link on the reset password page that takes users to a page where they can enter their email address and recover their username by email.

Email Subject Line

The subject line of the email that is sent to users for username recovery.

Email Message

The message that will be sent to users for email recovery. The message body can contain macro variables %USERNAME%, and %DOMAIN% which will be replaced with the actual values for the user.

Configuring TeleSign™

TeleSign is a service that Password Reset Server uses when making phone calls for Phone and SMS Questions. For more information on TeleSign and their services, please visit their [website](#).

To configure TeleSign for Password Reset Server, you must sign up for their service through their website. Once you have signed up, you will be given a CustomerId and an AuthenticationId. Enter these IDs into the Configuration Edit screen and click "Save".

To test the phone functionality, click the “Send Test Phone Call” and when prompted enter your phone number. To test the SMS functionality, click “Send Test SMS”.

WARNING: Testing the functionality will result in TeleSign charging your account.

Configuring ProxStop™

ProxStop is a service that Password Reset Server uses when making phone calls for Phone and SMS Questions. For more information on ProxStop and their services, please visit their [website](#).

To configure ProxStop for Password Reset Server, you must sign up for their service through their website. Once you have signed up, you will be given an API key. Enter this key into the Configuration Edit screen and click “Save”.

To test the phone functionality, click the “Send Test Phone Call” and when prompted enter your phone number. To test the SMS functionality, click “Send Test SMS”.

WARNING: Testing the functionality will result in ProxStop charging your account.

Enrollment

Enrolling

Overview

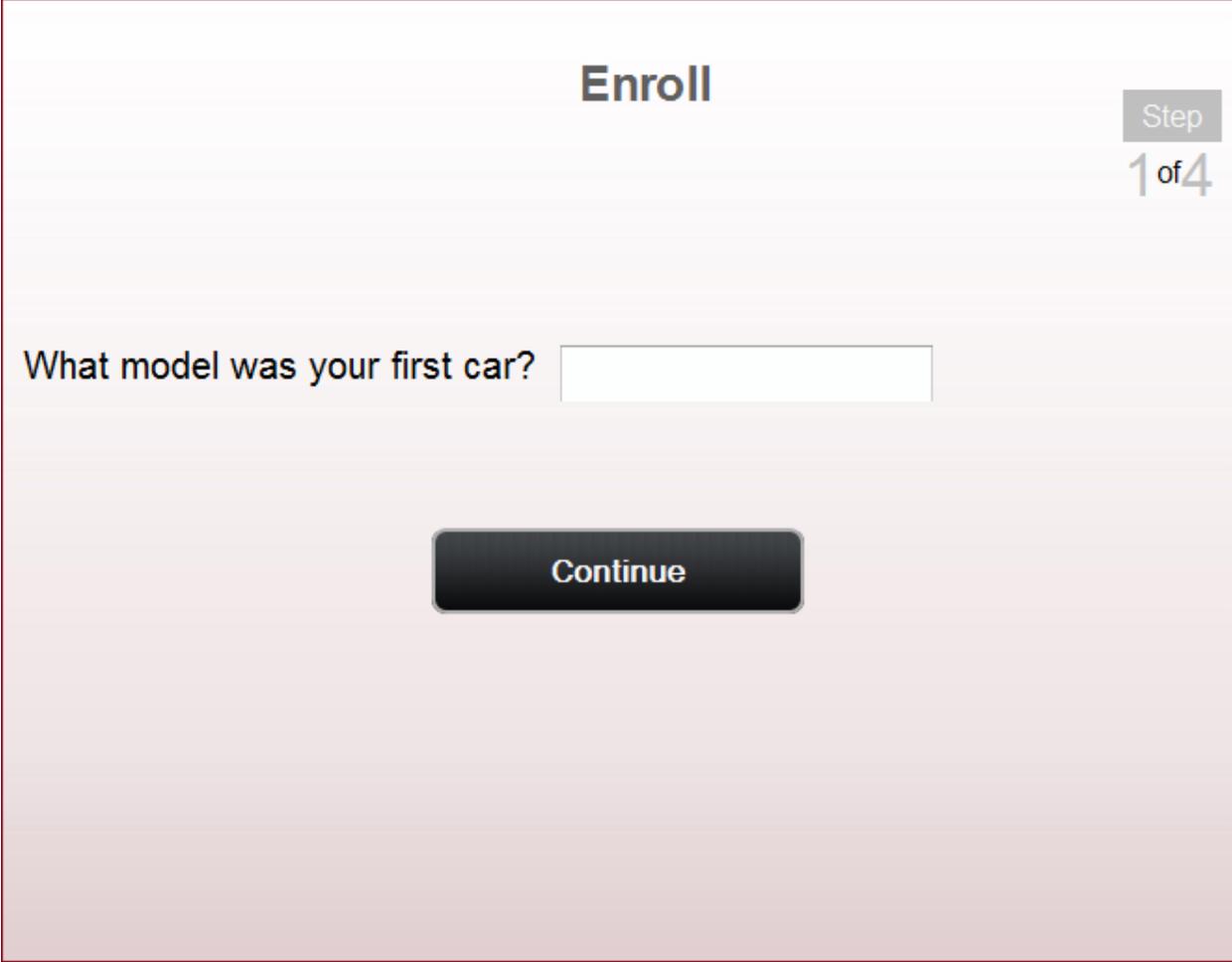
Before a user can use Password Reset Server to reset their password, they must complete the enrollment process. A user can begin the enrollment process by opening Password Reset Server and entering their Active Directory username, selecting their domain, and entering their current password.

Enrolled:	No
Last successful password reset:	Never
Last failed password reset:	Never

Enroll

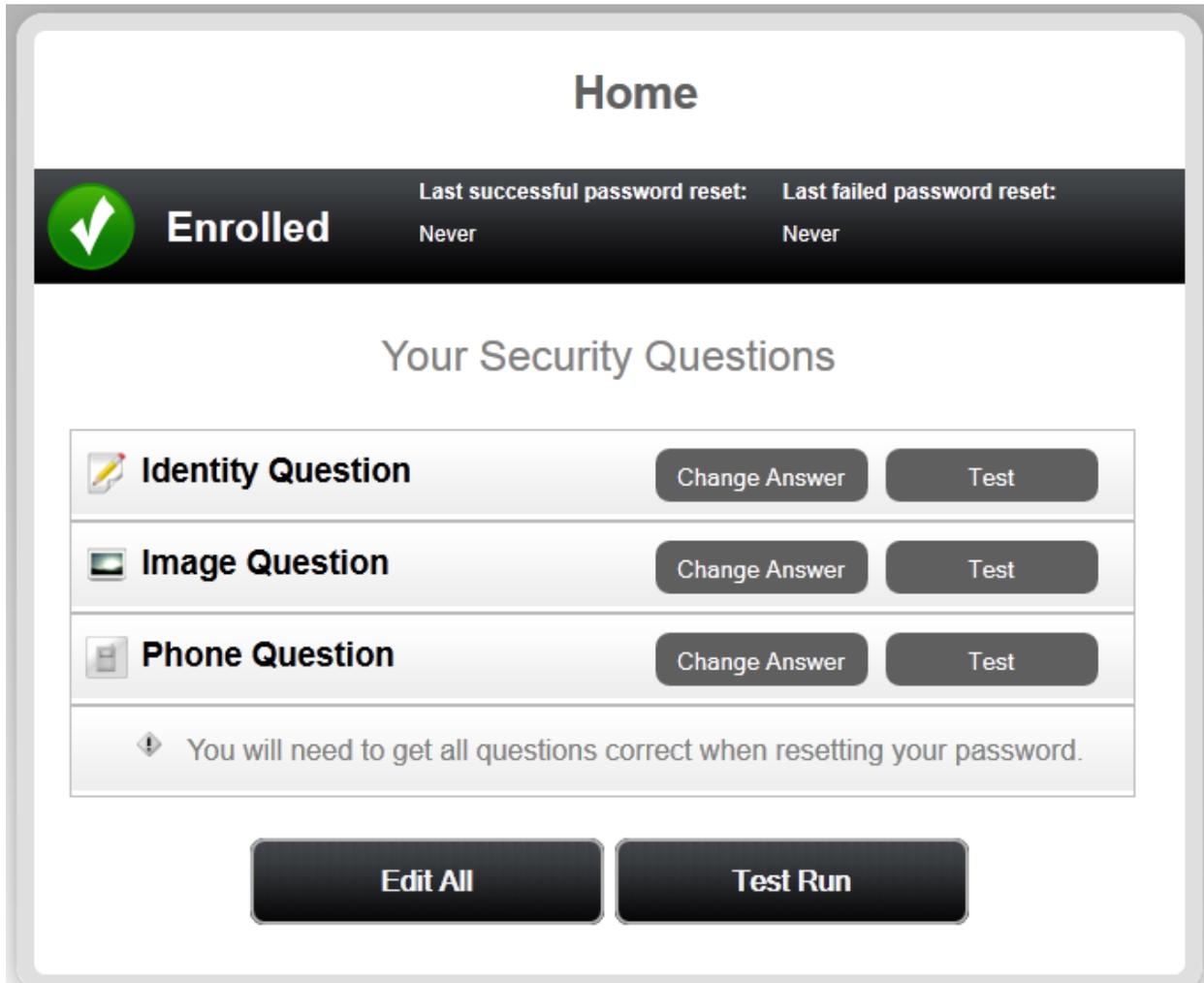
Enrollment Process

When a user clicks the “Enroll” button, they will be taken through the questions of their Security Policy.



The screenshot shows a mobile application interface for an enrollment process. At the top center, the word "Enroll" is displayed in a large, bold, dark font. In the top right corner, there is a grey rectangular box containing the text "Step 1 of 4". Below the title, the question "What model was your first car?" is presented in a dark font. To the right of the question is a white rectangular input field. At the bottom center of the screen, there is a dark grey rounded rectangular button with the word "Continue" written in white text.

Once their enrollment is complete, they are able to reset their password. They can test the process by clicking the “Test Run” button.



A user can return to this screen at any time by opening a browser and logging into Password Reset Server and entering their current username and password. Once on this screen, they can change an answer by clicking “Change Answer” next to a question. They can also test a single question by using the “Test” button, and test all questions by clicking “Test Run”. The note at the bottom tells them how many questions they need to answer correctly when confirming their identity.

After proving their identity, users can reset their password or unlock their account.

Enrollment Reminders

Overview

Password Reset Server can send reminders to your users for enrolling and also see a percentage of how many users have enrolled in a particular Security Policy.

Enrollment Reminders

Challenge for sysadmins [50% enrolled \(2/4\)](#)

Challenge for users [33% enrolled \(1/3\)](#)

Financial Users Policy [0% enrolled \(0/0\)](#)

< 1 to 3 of 3 >			
Date	User	Security Policy	Action
10/12/2009 12:00 AM	Kevin Jones	Challenge for users	Errors Occurred
10/11/2009 12:00 AM	Kevin Jones	Challenge for sysadmins	Sent
10/11/2009 12:00 AM	Kevin Jones	Challenge for users	Sent

To view the Enrollment Reminders, click “Administration” in the top navigation bar then “Enrollment Reminders”.

The grid shows previous reminders sent out and if there were any errors.

Date

Date is the date and time the enrollment reminder was sent out.

User

User is the name of the user which sent out the Enrollment Reminder.

Security Policy

Security Policy is the name of the policy that the reminder was sent out for.

Action

Action indicates the results from sending out the policy. “Sent” indicates the reminders were successfully sent.

Click the “View Errors” button to view and errors that have occurred while sending out the reminders. Click the “Refresh” button to refresh the grid.

The top shows each Security Policy and how many of them have enrolled. Click the name of the Security Policy for additional information regarding enrollment. This allows you to see which users have or have not enrolled in that particular Security Policy.

Enrolled Status Report

< 1 to 4 of 4 >		
User	Email Address	Status
Jonathan Cogley	jcogley@acmeinc.com	Enrolled
Kevin Jones	kjones@acmeinc.com	Not Enrolled
Ben Yoder	byoder@acmeinc.com	Not Enrolled
Tucker Croft	tcroft@acmeinc.com	Enrolled

[Back](#)

Creating a New Reminder

To create a new reminder, click the “Create” button on the Enrollment Reminders screen.

Enrollment Reminder

- Challenge for sysadmins 50% enrolled (2/4)
- Challenge for users 33% enrolled (1/3)
- Financial Users Policy 0% enrolled (0/0)

Subject

Message

Forgetting your password is no fun - now avoid the phone calls and enroll with your Password Reset Server so that you can reset your password on your own.

It only takes a few minutes and really improves the efficiency and security of the reset process.
%LINK%

Thanks!
IT Administration Team

To add a link to the enrollment page in your email, please type in %LINK%.

Save As Default Reminder

Check the Security Policies you would like to send a reminder out for. You may not check a Security Policy if all of its users are enrolled.

Subject

The Subject is the subject of the email that users in the Security Policies will receive.

Message

The Message is the body of the email that users in the Security Policies will receive. You can place the text %LINK% anywhere in the message. Password Reset Server will replace it with a link that users may click to start the enrollment process.

Save As Default Reminder

If checked, clicking “Send” will cause your current Subject and Message to become the defaults when creating new reminders.

Access Control

Overview

Access Control is Password Reset Server's method of regulating permission to system access. Each User and Group must be assigned to a role. Password Reset Server ships with two roles: Administrator and User. Each role contains various permissions to match the job function of the user. With Access Control strict granular access to Password Reset Server is ensured.

Defining Permissions

Administer Active Directory

- Change domain information for synchronization.

Administer Backup

- View Backup Configuration
- Edit Backup Configuration

Administer Configuration

- View Configuration
- Edit Configuration

Administer Enrollment Reminders

- View previously sent reminders
- Send new reminders
- View Enrollment Statistics

Administer Excluded Users

- Edit global exclusion list for users (deprecated – as of version 2.3.000000 users are encouraged to use the built-in Include and Exclude lists on the Security Policy).

Administer Licenses

- View installed licenses
- Add a license
- Remove a license
- Update a license

Administer Questions

- View questions
- Add a question
- Update a question
- Remove a question

Administer Reports

- Create new reports and edit created reports.

Administer Role Assignment

- Assign users or groups to a role
- Assign roles to a user or group

Administer Role Permissions

- View Roles
- Create a new Role
- Assign permissions to an existing role
- View permissions on an existing role

Administer Security Policies

- View existing Security Policies
- Add a new Security Policy

Administer System Log

- View the System Log
- Clear the System Log

Administer Users

- Grants access to the Users page.

Bulk Import Answers

- Allows answers to be imported for users.

Clear Answers

- Allows all answers for a specific question to be cleared.

View Backup

- View backup configuration

View Configuration

- View configuration

View Enrollment Reminder Reports

- View enrollment reminder reports

View Enrollment Reminders

- View enrollment reminders

View Group Roles

- View audit of Role assignment changes and Role permission changes.

View Licenses

- View currently installed licenses

View Questions

- View questions

View Reports

- View reports

View Roles

- View roles

View Security Policies

- View Security Policies

View System Log

- View the System Log

View Users

- Grants access to the Users page.

Default Roles

Password Reset Server comes pre-configured with two roles. These can be edited or disabled if necessary.

Administrator

The Administrator role comes with all permissions. The first account created is placed in this role.

User

The User role has no permissions. It is the default role. All users will be added to this role by default.

Administering Roles

To add a role, begin by clicking the "Administration" link on the top navigation bar and then clicking "Roles", then the "Create Button".

Role Edit

Role Name*

Enabled

Created

Permissions

Assigned		Unassigned
	<div style="display: flex; flex-direction: column; gap: 10px;"> ⏪ ⏩ ⏴ ⏵ </div>	<ul style="list-style-type: none"> Administer Active Directory Administer Backup Administer Computers Administer Configuration Administer Enrollment Reminders Administer Folders Administer Groups Administer IP Addresses Administer Languages Administer Licenses Administer Questions Administer Role Assignment Administer Role Permissions Administer Security Policies Administer System Log

Give your role a name, such as "Security Policy and Question Maintenance".

You can then move permissions between "Assigned" and "Unassigned" by selecting the item and clicking the single arrow left or right, or moving all items to the left or right by clicking the double arrow.

TIP: You can move multiple users or groups at once by holding the Control Key (Ctrl) and clicking more than one in the list, then clicking the left or right arrow.

Finally, click "Save".

To edit a role, click the name of the role on the role overview screen. When editing a role, you can change the name, assign or un-assign permissions, or disable the role. A role cannot be deleted once created.

Assigning Roles

To assign a role to users or groups, begin by clicking the "Administration" link on the top navigation bar and then clicking "Roles", then the "Assign Roles" button.

By Role

If you have a specific role you want to assign users and groups to, click the "By Role" tab and select the role you would like to assign users and groups to. Modify the assigned users or groups by clicking them, then the left or right arrows.

Role Assignment

⚠ Please note that changing role assignment could remove your access to Role Administration.

By RoleBy User Or Group

Role Administrator

Included

< 1 to 3 of 3 >	
Bryant Smith (bryant@thycotic.com)	✕
John Morales (john@thycotic.com)	✕
Idapserveritest (test)	✕

Add User or Groups

testparent.thycotic.com

Groups

Users

Select

Save Changes

Discard Changes

Click "Save Changes" when you are complete.

By User or Group

If you have a specific user or group you would like to assign roles to, click the "By User or Group" tab and select the user or group you would like to assign users and groups to. Modify the assigned roles by clicking them, then the left or right arrows.

Role Assignment

⚠ Please note that changing role assignment could remove your access to Role Administration.

By Role

By User Or Group

Selected User/Group

testparent\Ken Ober (ken.ober)

Assigned

Unassigned

User

Administrator



Save Changes

Discard Changes

Click "Save Changes" when you are complete.

Role Auditing

Overview

All actions taken on roles are fully audited. This includes assigning a user or group to a role, renaming a role, disabling a role, etc. This helps ensure your company is meeting any auditing requirements imposed by industry or other standards.

Role Audits

To view changes to a role itself, such as renaming it, disabling it, or modifying its permissions, begin by clicking the "Administration" link on the top navigation bar and then clicking "Roles", then the "View Audit" button. The action describes what was done and the Notes describe the details of the action.

Role Audit			
< 1 to 2 of 2 >			
Date Recorded	User	Action	Notes
10/20/2009 10:28 AM	Jonathan Cogley	ADDED ROLE PERMISSIONS TO Security Policy and Question Maintenance	View Security Policies, Administer Security Policies, Administer Questions, View Questions
03/23/2008 12:00 AM	Jonathan Cogley	ADDED ROLE PERMISSIONS TO Administrator	Unlimited Administrator

[Back](#)

Role Assignment Audits

To view which users and groups have been assigned and un-assigned from a role, begin by clicking the "Administration" link on the top navigation bar and then clicking "Roles", then the "View Assignment Audit" button. The action describes what was done and the Notes describe the details of the action.

Assignment Audit			
< 1 to 4 of 4 >			
Date Recorded	User	Action	Notes
03/26/2008 12:00 AM	Bryant Smith	REMOVED ROLE FROM User Two	Administrator
03/26/2008 12:00 AM	Jonathan Cogley	REMOVED ROLE FROM User One	Administrator
03/26/2008 12:00 AM	Jonathan Cogley	REMOVED ROLE FROM Developers	Administrator
03/23/2008 12:00 AM	Jonathan Cogley	ADDED ROLE TO Bryant Smith	Administrator

[Back](#)

Domain and User Configuration

Overview

Password Reset Server can integrate with multiple domains and import users. During installation, you will be asked to provide the first domain and a user that will be used to reset passwords. This user must be on the same domain that it will reset passwords on. For more information about creating and configuring one of these accounts, please see our [Installation Guide](#).

When you add a domain, Password Reset Server will begin reading your domain's groups, users, organization units and configuration in the background. Until this processing is complete, all information may not be available.

Administering Domains

To add a domain, click "Administration" on the top navigation bar, then click "Domain Configuration" followed by "Add Domain".

The screenshot shows a web form titled "Domain" with the following fields and values:

Fully Qualified Domain Name	office.thycotic.com	*
Friendly Domain Name (Display)	office	*
Username	pruser	*
Password	••••••••	*
Port	389	
Active	<input checked="" type="checkbox"/>	
Use Secure LDAP	<input type="checkbox"/>	

At the bottom of the form are two buttons: "Save" and "Cancel".

Enter the Fully Qualified Domain Name (FQDN) along with the username and password of the domain user. To use Secure LDAP, check the 'Use Secure LDAP' box. If using a non-standard port, change the port. Normally the port is 389 for LDAP or 636 for LDAPS. For more information on how this password is stored, please see the section on encryption.

Finish by clicking "Save" or cancelling by clicking "Cancel".

To edit or deactivate a domain, click the domain name in the domain overview and make the desired edits, and click "Save".

Password Reset Server Encryption

Overview

Password Reset Server utilized two cryptographic algorithms for storing its data. It uses AES-256 and SHA-512.

AES-256 (Advanced Encryption Standard)

Password Reset Server uses the government standard AES-256 algorithm for storing domain passwords. When entering the password for a domain account that will be used for changing passwords, Password Reset Server will encrypt it using the AES-256 algorithm. For more information on AES, please see the [official standard](#).

SHA-512 (Secure Hash Algorithm)

Password Reset Server utilized SHA-512, an irreversible data transformation to securely store local account passwords and answers to questions. Hashing algorithms are mathematical functions to replace inputted text values with numerical ones. If the input text is the same, the final hashed value will also be the same. The input text of "fox" will always produce the same hashed value. Minor changes in the input value will radically alter the hashed output, as shown in the examples below.

Example input text: "The quick brown fox jumps over the lazy dog"

Hashed value: 07e547d9 586f6a73 f73fbac0 435ed769 51218fb7 d0c8d788 a309d785
436bbb64 2e93a252 a954f239 12547d1e 8a3b5ed6 e1bfd709 7821233f a0538f3d b854fee6

Example input text, with 'dog' changed to 'cog':
"The quick brown fox jumps over the lazy cog".

Hashed value: 3e0001d0 e11733ef 152a6c29 503b3ae2 0c4f1f3c da4cb26f 1bc1a41f
91c7fe4a b3bd8649 4049e201 c4bd5155 f31ecb7a 3c860684 3c4cc8df cab7da11 c8ae5045

SSL/TLS (Secure Socket Layer)

Password Reset Server can be configured to run SSL certificates. It is strongly recommended that Password Reset Server installations run using SSL. Not using SSL will significantly reduce the security of the contents of Password Reset Server since browsers viewing the site will not be using an encrypted connection.

Administrative Reports

Overview

Password Reset Server has reports available to administrators to help get a demographic for adoptions, usages, etc. To view these reports, click the "Administration" link on the top navigation bar and then click "Administration Reports".

For an explanation of each report and what it represents, click the "Explain" link.

Security Hardening Report

The Security Hardening Report checks aspects of Password Reset Server to ensure security best practices are being implemented. While Password Reset Server will run with all of the items failing, administrators should be aware of possible security issues within an installation.

Below is an explanation of the different values:

- **SQL Server Authentication Password Strength** - SQL Server Authentication requires a Username and password. The password must be a strong password to get a pass result. Strong passwords are 8 characters or longer and contain lowercase, uppercase, numbers and symbols. The SQL Server Authentication Credentials in use can be changed by going to the installer (installer.aspx) and changing them on Step 3. A pass result is also given if Windows Authentication is used to authenticate to SQL Server.
- **SQL Server Authentication Username** - The SQL Server Authentication Username should not be obvious - the use of "sa", "prs" or "passwordresetserver" will give a fail result. The SQL Server Authentication Credentials in use can be changed by going to the installer (installer.aspx) and changing them on Step 3. A pass result is also given if Windows Authentication is used to authenticate to SQL Server.
- **Windows Authentication to Database** - Windows Authentication takes advantage of Windows Security to provide secure authentication to SQL Server. The SQL Server Authentication options can be changed by going to the installer (installer.aspx) and changing them on Step 3. Please see page 19 of the Installation Guide for instructions on configuring Windows Authentication to SQL Server.
- **Require SSL** - Secure Sockets Layer (SSL) is required to ensure that all communication between the web browser and Password Reset Server is encrypted and secure. Once the SSL certificate is installed, Force HTTPS/SSL in Configuration to get a pass result. Please see the

[Installing a Self-Signed SSL/HTTPS Certificate](#) Knowledge Base article for instructions on installing and configuring SSL certificates.

- **Using SSL** - SSL needs to be running with at least a 128 bit key size to get a pass result. A warning result indicates your key size is less than 128 bits. A fail result indicates you are not using SSL.

- **Note: Use of SSL is highly recommended for Password Reset Server.**

Backup / Disaster Recovery

Automatic Backups

Password Reset Server supports automatic database and IIS directory backups.

From the Backup page, specify the correct folder paths for the IIS Password Reset Server file directory and the database backups to go. The backup path must be local to the server where the Password Reset Server database or file directory exists. The folders must also have the proper permissions to allow Password Reset Server to automatically place backups in them. The account that needs permissions will be displayed as an alert on the page.

There are numerous options to consider when backing up Password Reset Server. Backups can be scheduled to run on a specific time interval. To prevent the directory from growing too large, the number of backups to keep can be defined as well. Depending on size constraints or preferences of the DBA who would be administrating a disaster recovery scenario, the database backup can either truncate the transaction log or keep it intact.

System Log

Overview

The system log allows you to diagnose issues with Password Reset Server, such as issues with querying your Active Directory Domain, Backups, etc.

The system log can be accessed by clicking "Administration" on the top navigation bar and then clicking "System Log".

To clear the System Log, click the "Clear" button.