Delinea

Password Reset Server

Documentation 5.3.0

Table of Contents

This is the installation guide for Windows 8 and Windows Server 2012, as well as Windows 8.1 and Windows Server 2012 R2. If you are looking for the installation guide for Windows Server 2008 / 2008 R2, Vista, or Windows 7, please click here.

ASP.NET Website

Password Reset Server is installed as an ASP.NET website. The MSI will setup the website with the correct permissions and configure the appropriate settings in IIS. Once the website is set up, the installation will be completed by a process within the application itself.

SQL Server Database

Password Reset Server requires an instance of SQL Server for the database backend. The SQL Server database will require a SQL account with db_owner permission to complete the installation.

Administrative Access

Throughout the installation, you will be required to be an administrator to perform most of these actions. Please ensure that you are logged on to your system with a Windows account that has administrative permissions.

Introduction

Group Management Server is installed as an ASP.Net website. The setup.exe installer will setup the website with the correct permissions and configure the appropriate settings in IIS. Once the website is set up, the installation will be completed by a 5-step process within the application itself.

Group Management Server requires an instance of SQL Server for the database backend. The SQL Server database will require a SQL account with *db_owner* permission to complete the installation.

Throughout most of this installation, you will be required to be an administrator to perform most of these actions. Please ensure that you are logged on to your system with a Windows account that has administrative permissions.

Minimum requirements for installing Password Reset Server

Hardware Requirements

- **CPU**: Minimum of 2 cores, 2 Ghz or higher per core
- **RAM/Memory**: Minimum 4GB
- **Disk Space**: Minimum 20GB (mainly for the database, operating system, other applications/tools)

Please Note*: Hardware requirements depend on the target system and projected usage volume, and they are subject to change.*

Software Requirements

Please Note*:*

- *DO NOT install Password Reset Server on a domain controller, because Microsoft ASP.NET will not operate reliably.*
- *We do not recommend installing Password Reset Server as a Web Server on a client operating system for production use (testing purposes or proof of concept only). This includes all standard Windows operating systems (Vista 10 and later).*

Microsoft Windows Server

- 2008
- 2008 R2
- 2012
- 2016

Please Note*:*

- *Small Business Server (SBS) is not supported.*
- *The Essentials edition is not supported because it requires the domain controller role.*
- *The “Core” (GUI-less) role is only supported for Server 2012 and Server 2012 R2.*

Microsoft SQL Server

- 2005
- 2008
- 2008 R2
- 2012
- 2014
- 2016

Please Note*: Edition must be SQL Server Express or higher.*

Microsoft Internet Information Services (IIS)

- IIS 7
- IIS 8

Please note*: You must add IIS as a feature in Windows Server. See the information here.*

Microsoft .NET Framework

- .NET 4.5.1
- .NET 4.5.2

Database Size Recommendations

- 1 GB initial database size minimum.
- Typical database size for 1000 users is around 300 MB.
- Growth depends on the size of the domain (OUs, groups, users) and audit activity.

Important Notes

- Password Reset Server will operate in a virtual environment (VMware or Hyper-V).
- Windows Login Integration (GINA Hook) is compatible on Windows XP through Windows 10.
- You can run Password Reset Server on the same machine as other applications (Password Reset Server will require sufficient RAM and CPU to operate normally).
- For maximum security, you should install the application on dedicated systems or at least systems with applications with the same level of security/sensitivity. Access to these systems should then be restricted. While all sensitive data in Password Reset Server is either securely hashed or encrypted, it is a security best practice to limit any opportunities for foul play.
- Password Reset Server 3.3.000000 and higher requires the .NET Framework 4.5.1 to be installed on the web server prior to installation or upgrade.

SQL Server 2012 Express requires some software to be installed before it can be installed.

1. Windows PowerShell 2.0.
2. Microsoft .NET Framework 4.5.1.
3. Windows Installer (Windows Installer 5.0 is included by default in Windows 8 / Server 2012)

Only the Express Edition requires these components to be installed separately. If you are installing another edition of SQL, such as Standard or Enterprise, these components will be installed for you.

Please Note: Secret Server and Password Reset Server require SQL_Latin1_General_CP1_CI_AS to be the default collation for Microsoft SQL Server and its database. Using a different default collation will cause the installation to fail. See Microsoft SQL collation requirements and check your server collation settings before upgrading.

Installing PowerShell

Windows PowerShell is included by default in Windows 8, Windows 8.1, and Windows Server 2012 / R2.

Virtual Accounts

Virtual Accounts, or Managed Service Accounts, is a feature included in Windows 8 and Windows Server 2012. Windows will create a virtual account for the name of the application pool. Thus, if your application pool’s name is DefaultAppPool and its identity is set to ApplicationPoolIdentity, you would assign folder permissions to the account IIS AppPool\DefaultAppPool. This account can then optionally be used to connect Secret Server to the SQL database by adding db_owner access to the database as a Windows account. See *Adding a SQL Server User*. For more information on virtual accounts as application pool identities, see this article by Microsoft.

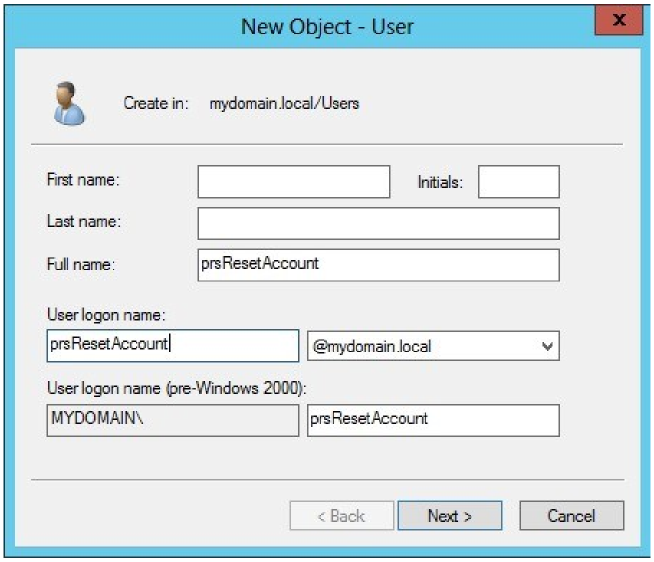
Creating a domain account to reset passwords

For Password Reset Server to reset passwords, it must be provided access to an account that is able to reset passwords for the domain users. Instructions for setting up the exact permissions are detailed below. We recommend creating a new domain account that will only be used by Password Reset Server for this purpose:

You must be a member of the Domain Admins group to perform these steps.

1. Open the Active Directory Users and Computers MMC snap-in and connect to your domain.
2. Right click Users under your domain and select New > User.
3. In the Full name and User logon name fields, enter a descriptive name and unique username, respectively (Figure A). Click Next.
4. Enter a strong password.
5. Uncheck the User must change password at next logon box.
6. Check the Password never expires and User cannot change password boxes (Figure B).

   We recommended choosing “Password never expires” because if the password expires and it is not changed, Password Reset Server will not be able to change passwords for domain users.
7. Click Next and Finish.



New Object - User

Create in: mydomain.local/Users

First name:

Initials:

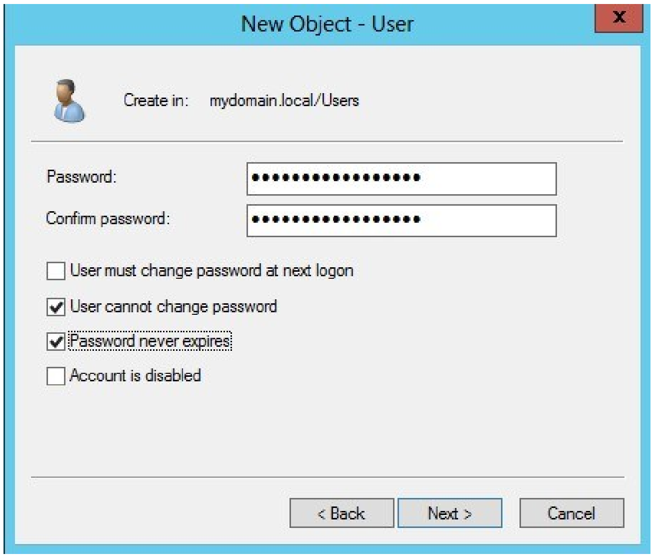
Last name:

Full name: prsResetAccount

User logon name: prsResetAccount @mydomain.local

User logon name (pre-Windows 2000): MYDOMAIN\ prsResetAccount

Figure A – Configure New User Account



New Object - User

Create in: mydomain.local/Users

Password: ●●●●●●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●●●●●●

□ User must change password at next logon

☑ User cannot change password

☑ Password never expires

□ Account is disabled

Figure B – Configure New User Password

The domain account used to synchronize and reset passwords for the domain must have the following permissions to reset a user's account: Change Password, Reset Password, Write lockoutTime*,* Write pwdLastSet.

8. Configure the Active Directory Users and Computers to display Advanced Features by clicking View from the top menu, and then Advanced Features (Figure C).

9. Select the top level domain node, right click, and select Delegate Control (Figure D).

   If desired, you may apply the permissions to specific Organizational Units instead of the entire domain. These actions must be repeated for each Organizational Unit.

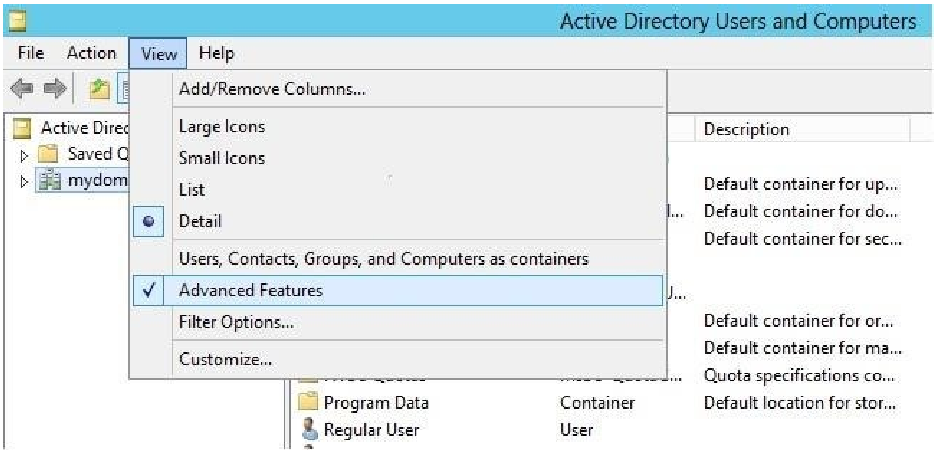

Active Directory Users and Computers
File
Action
View
Help
Add/Remove Columns...
Large Icons
Small Icons
List
Detail
Users, Contacts, Groups, and Computers as containers
Advanced Features
Filter Options...
Customize...
Active Direc
Saved Q
mydom
Description
Default container for up...
Default container for do...
Default container for sec...
Default container for or...
Default container for ma...
Quota specifications co...
Program Data
Container
Default location for stor...
Regular User
User

Figure C – View Advanced Features

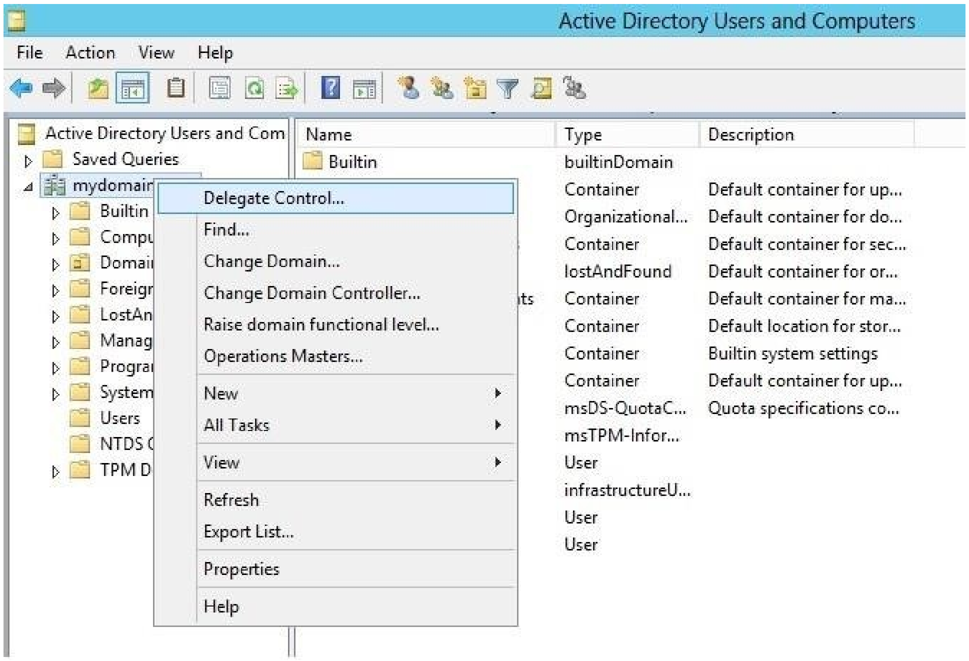
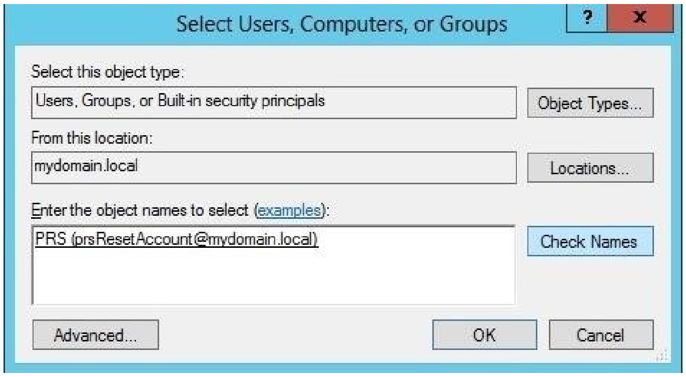


Figure D – Delegate Control

10. Once the Delegation of Control Wizard window opens, click Next.

11. On the Selected users and groups screen click Add.

12. Select the user created above (Figures E,F). Click Next.



Select Users, Computers, or Groups

Select this object type:

Users, Groups, or Built-in security principals

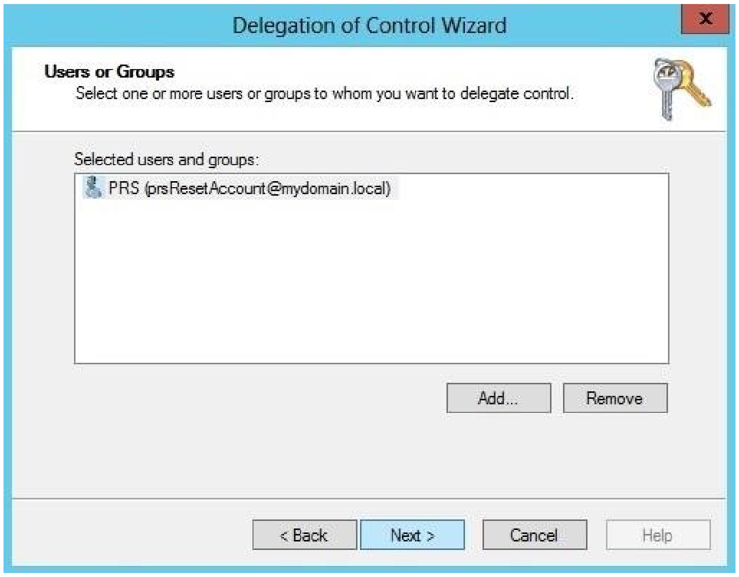
From this location:

mydomain.local

Enter the object names to select (examples):

PRS (prsResetAccount@mydomain.local)

Figure E – Select PRS Admin User



Delegation of Control Wizard

Users or Groups

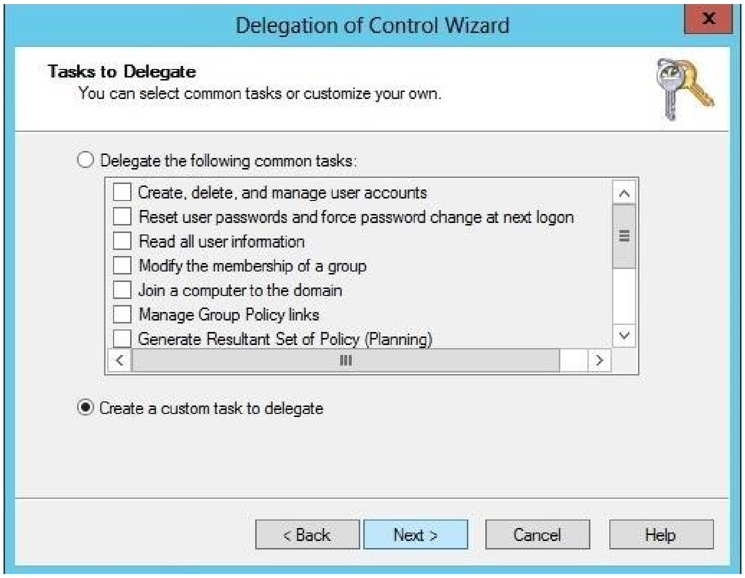
Select one or more users or groups to whom you want to delegate control.

Selected users and groups:

PRS (prsResetAccount@mydomain.local)

Figure F – Confirm Selection of PRS Admin User

13. In the next window, select the “Create a custom task…” bubble (Figure G). Click Next.
14. For Delegate control of, select the “Only the following…: option and check the User Objects box at the very bottom (Figure H). Click Next.



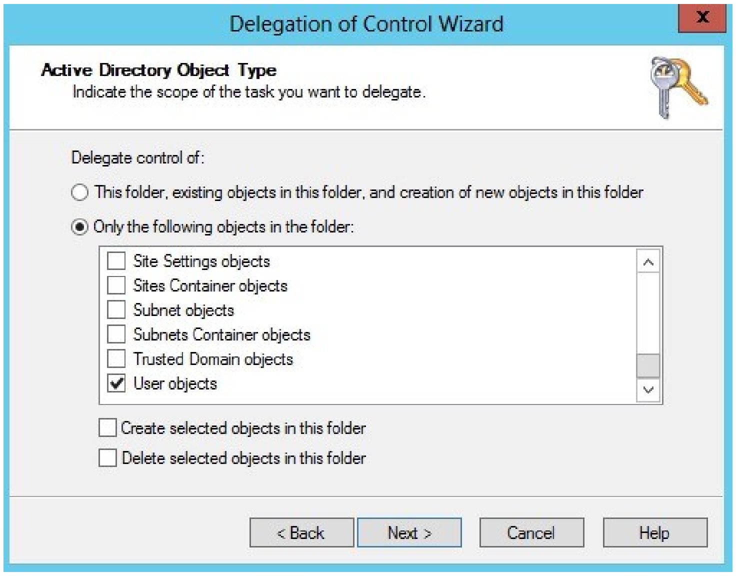
Tasks to Delegate
You can select common tasks or customize your own.

○ Delegate the following common tasks:

□ Create, delete, and manage user accounts
□ Reset user passwords and force password change at next logon
□ Read all user information
□ Modify the membership of a group
□ Join a computer to the domain
□ Manage Group Policy links
□ Generate Resultant Set of Policy (Planning)

● Create a custom task to delegate

Figure G – Create a custom task to delegate



Active Directory Object Type
Indicate the scope of the task you want to delegate.

Delegate control of:

○ This folder, existing objects in this folder, and creation of new objects in this folder

● Only the following objects in the folder:

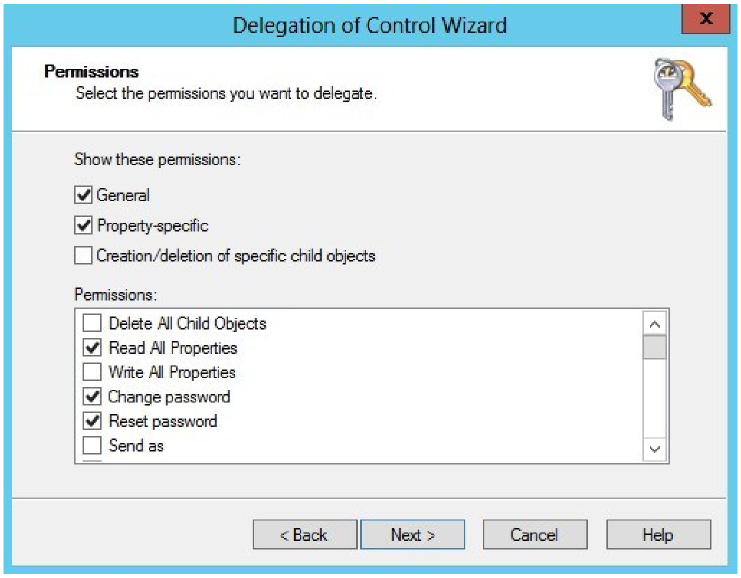
□ Site Settings objects
□ Sites Container objects
□ Subnet objects
□ Subnets Container objects
□ Trusted Domain objects
☑ User objects

□ Create selected objects in this folder
□ Delete selected objects in this folder

Figure H – Select User Objects

15. Leave the General box checked, and select the "Read All Properties," "Change password," and "Reset password" check boxes below (Figure I). **If you plan to allow users to update Active Directory attributes through Password Reset Server as well, you will also need to give this account "Write All Properties" or permission to write the specific attribute(s).** Click Next and Finish.

16. Repeat steps 9 through 14, then check only the Property-specific box and check the "**Write lockoutTime**" (Figure J), "**Write pwdLastSet**" (Figure K), and "**Write userAccountControl**" (Figure L) boxes. Click Next and Finish.



Delegation of Control Wizard

Permissions

Select the permissions you want to delegate.

Show these permissions:

☑ General

☑ Property-specific

☐ Creation/deletion of specific child objects

Permissions:

☐ Delete All Child Objects

☑ Read All Properties

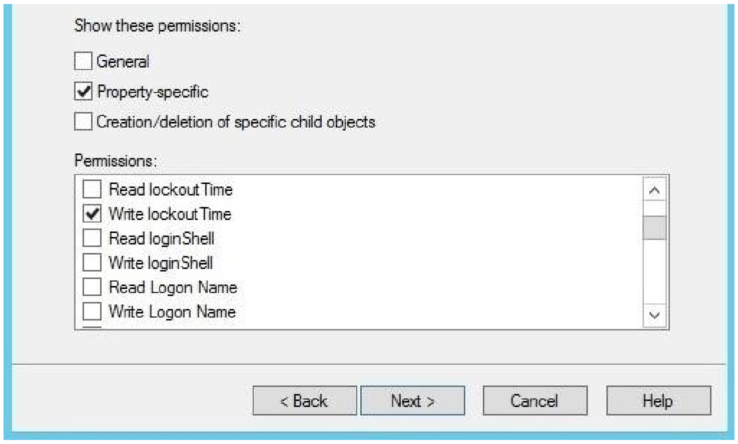
☐ Write All Properties

☑ Change password

☑ Reset password

☐ Send as

Figure I – Delegate Change & Reset Password Permissions



Show these permissions:

☐ General

☑ Property-specific

☐ Creation/deletion of specific child objects

Permissions:

☐ Read lockoutTime

☑ Write lockoutTime

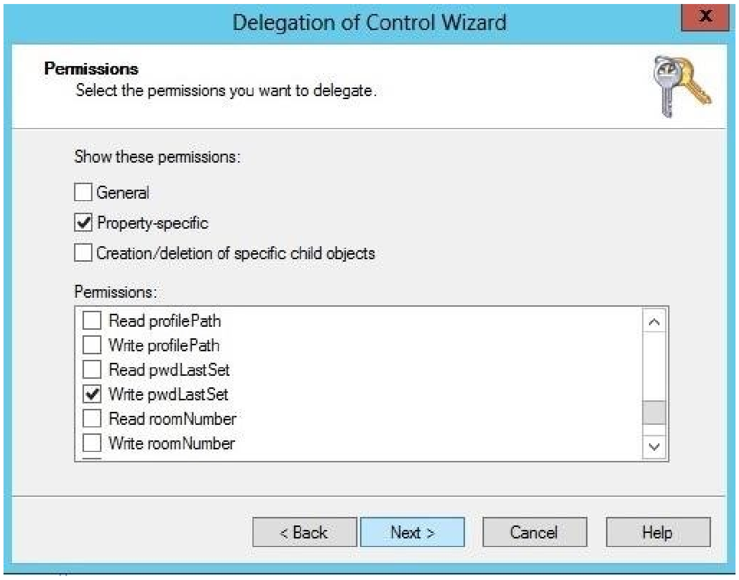
☐ Read loginShell

☐ Write loginShell

☐ Read Logon Name

☐ Write Logon Name

Figure J – Delegate Write lockoutTime Permission



Delegation of Control Wizard

Permissions
Select the permissions you want to delegate.

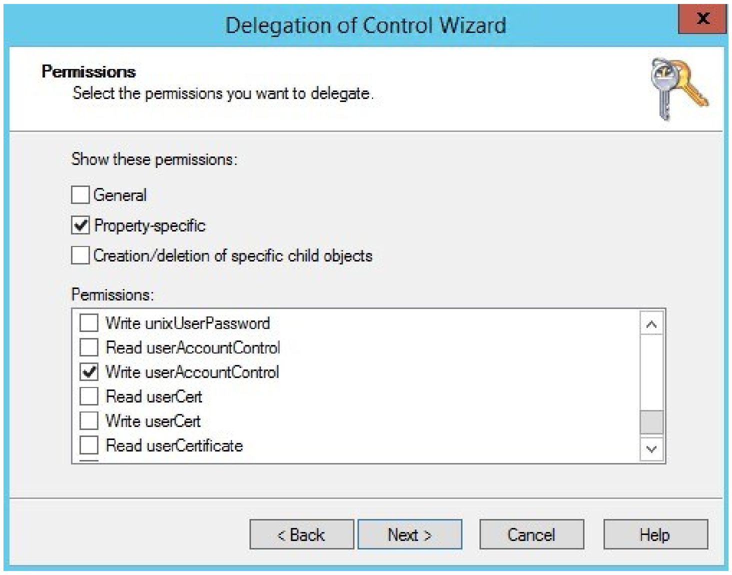
Show these permissions:

- ☐ General
- ☑ Property-specific
- ☐ Creation/deletion of specific child objects

Permissions:

- ☐ Read profilePath
- ☐ Write profilePath
- ☐ Read pwdLastSet
- ☑ Write pwdLastSet
- ☐ Read roomNumber
- ☐ Write roomNumber

Figure K – Delegate Write pwdLastSet Permission



Delegation of Control Wizard

Permissions
Select the permissions you want to delegate.

Show these permissions:

- ☐ General
- ☑ Property-specific
- ☐ Creation/deletion of specific child objects

Permissions:

- ☐ Write unixUserPassword
- ☐ Read userAccountControl
- ☑ Write userAccountControl
- ☐ Read userCert
- ☐ Write userCert
- ☐ Read userCertificate

Figure L - Delegate Write userAccountControl Permission

You can now use this account to reset passwords using Password Reset Server.

You may want to modify your domain Group Policy to deny local login for this account under User Rights Assignment.

SSL Certificate

What is an SSL Certificate?

An SSL (Secure Sockets Layer) Certificate greatly enhances the security between the user's browser and the server Password Reset Server is installed on. It encrypts all data between the server and the client's browser so if an attacker were to look at the data being transmitted between the two, they would not be able to decipher it.

Where can I obtain an SSL Certificate?

A certificate can be obtained from various companies such as Thawte or VeriSign. It is also possible to create your own, see Creating and installing your own.

Software Requirements

- One of the following operating systems:
  - Windows 8 or 8.1

    Note: Windows 8 and 8.1 are only supported for testing environments. Microsoft does not support either of these operating systems being used as a production server environment.
  - Window Server 2012 or 2012 R2

    Note: Both 32-bit and 64-bit editions of Windows Server are supported. You must install the proper version of the .NET Framework to support 64-bit.
- Microsoft SQL Server 2005, 2008 or 2012, including R2 (any edition)
- Microsoft **Internet Information Services** (IIS) (internal part of the operating system)
- **Microsoft .NET Framework 4.5.1 / 4.5.2** (both 32-bit and 64-bit editions are supported)

Note: Windows 8 / 8.1 and Windows Server 2012 / R2 come with the .NET Framework 4.5.1 already installed. If you are using Windows 8 or Windows Server 2012, you should already have .NET Framework 4.5 but will need to upgrade to .NET Framework 4.5.1 / 4.5.2. Find the installer provided by Microsoft here.

Domain Account Requirements

Each domain will need a domain account to synchronize the users and reset passwords. For instructions on setting up a domain account, please scroll up this page to the section named, **Creating a domain account to reset passwords**.

Additional Recommendations

- Run Microsoft Update on your server to make sure all components are up to date.

Beginning the Installation Process

Components should be installed in the following order:

1. Internet Information Services (IIS)
2. .NET Framework 4.5.1 / 4.5.2 (Windows 8 / Server 2012 Only)
3. SQL Server
4. Password Reset Server

Installing IIS

IIS is an internal part of the Microsoft Windows operating system. Installing it will vary depending on which version of the operating system you are using.

Windows Server 2012 / Windows Server 2012 R2

To install Internet Information Services on Windows Server 2012 or Windows Server 2012 R2, you will give your server the Web Server (IIS) role.

1. Begin by opening the Server Manager and clicking Manage, then Add Roles and Features:

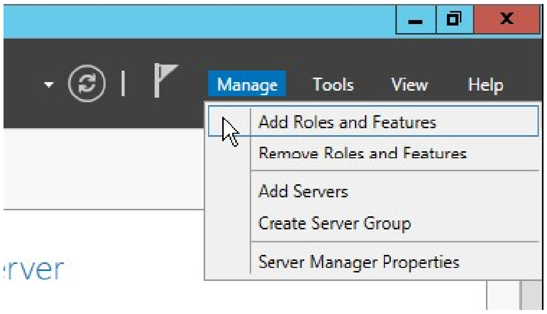


   Figure 1.1 – Add Roles and Features

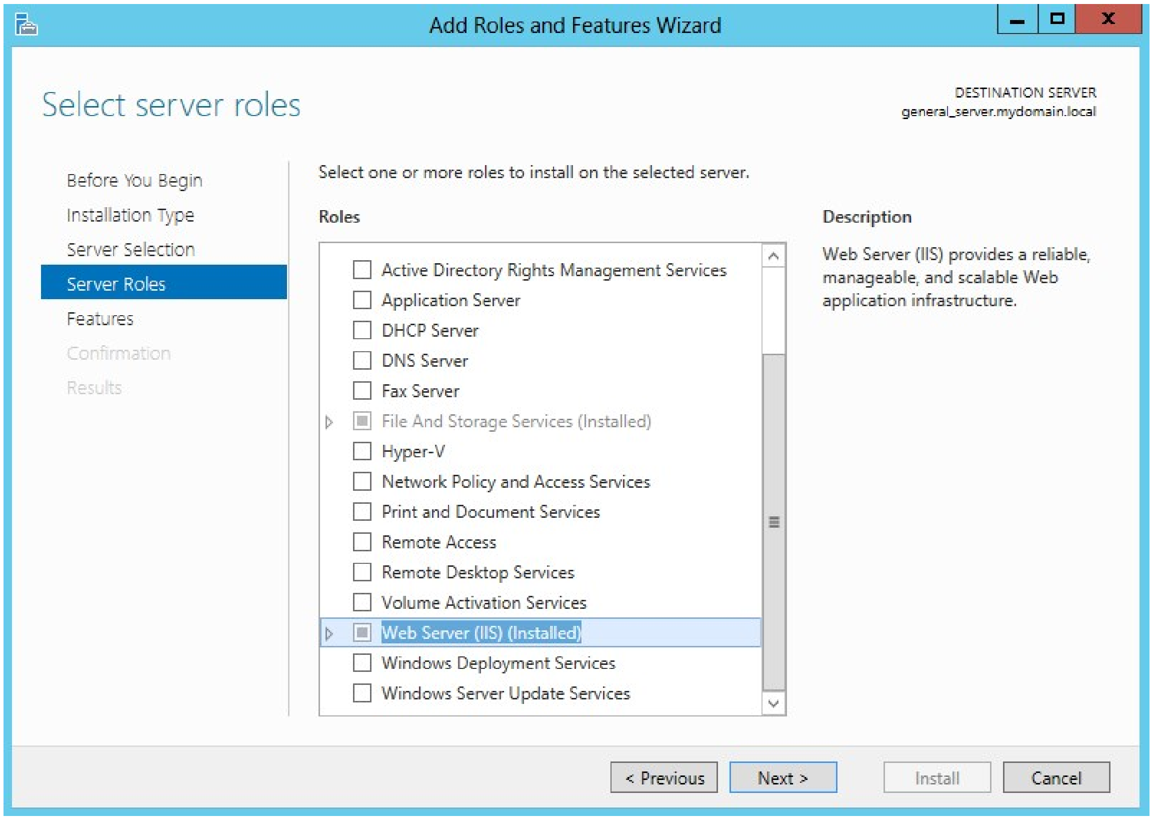
2. Click Next until reaching the Installation Type screen. Select Role-based or feature-based installation and click Next.

3. Select your Server (it should be selected by default) and click Next.

4. Check the Web Server (IIS) box, then expand the category (see Figure 2.2 on the following page).

5. Expand Web Server > Application Development and check the **ASP.NET 4.5** box (Figure 2.3).

6. Expand Common HTTP Features and ensure that the Static Content, Default Document, and HTTP Errors boxes are checked as well. Click Next, and then Add Features.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
general_server.mydomain.local

Select one or more roles to install on the selected server.

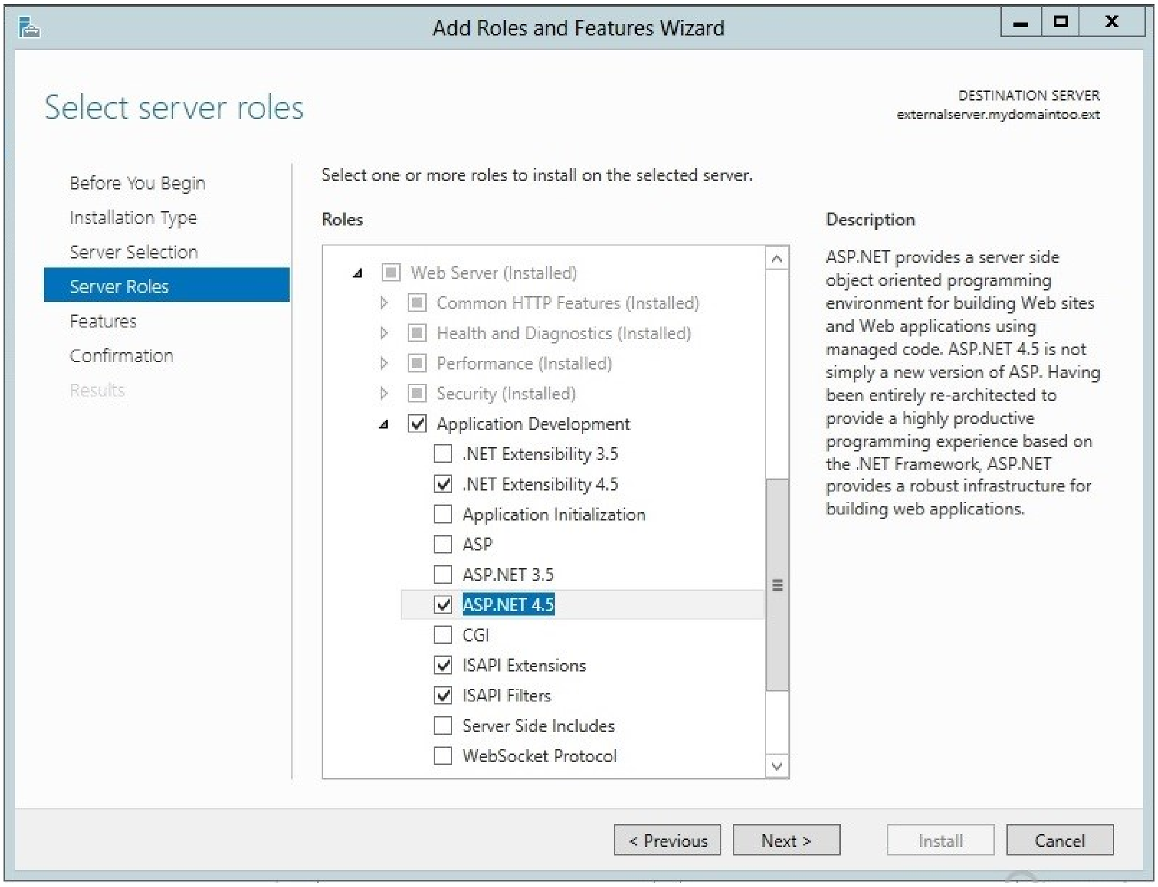
Roles

- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ▷ ▣ File And Storage Services (Installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ▷ ▣ Web Server (IIS) (Installed)
- ☐ Windows Deployment Services
- ☐ Windows Server Update Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

Figure 1.2 – Choose the IIS Role



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
externalserver.mydomaintoo.ext

Select one or more roles to install on the selected server.

Roles

- ▨ Web Server (Installed)
  - ▨ Common HTTP Features (Installed)
  - ▨ Health and Diagnostics (Installed)
  - ▨ Performance (Installed)
  - ▨ Security (Installed)
  - ☑ Application Development
    - □ .NET Extensibility 3.5
    - ☑ .NET Extensibility 4.5
    - □ Application Initialization
    - □ ASP
    - □ ASP.NET 3.5
    - ☑ ASP.NET 4.5
    - □ CGI
    - ☑ ISAPI Extensions
    - ☑ ISAPI Filters
    - □ Server Side Includes
    - □ WebSocket Protocol

Description

ASP.NET provides a server side object oriented programming environment for building Web sites and Web applications using managed code. ASP.NET 4.5 is not simply a new version of ASP. Having been entirely re-architected to provide a highly productive programming experience based on the .NET Framework, ASP.NET provides a robust infrastructure for building web applications.

Figure 1.3 – Select ASP.NET 4.5

Windows 8 / 8.1

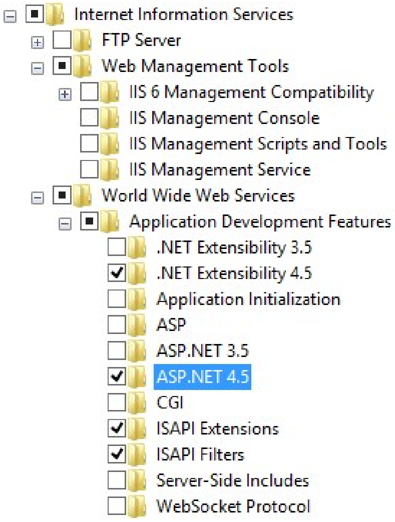
Please ensure you have your Windows installation disk available if the system asks for it. This disk should have been included with the System Manufacturer or the Administrator that installed Windows on that machine.

1. From the Desktop, start by tapping the Windows key, then type Control Panel and hit Enter.
2. Open the Programs Control Panel item, and then Programs and Features.
3. Click Turn Windows Features on or off.
4. A dialog will appear. It may take a moment or two for the system to load. Expanding Internet Information Services > World Wide Web Services > Application Development Features and checking **ASP.NET 4.5** will also check other needed dependencies (see Figure 1.1 on the following page).
5. Expand Common Http Features and check the following:
   1. Static Content (if this is not checked, the application images will not appear)
   2. Default Document
6. Ensure that .NET Framework 4.5 is already checked. If not, check this box as well.
7. Click OK. At this point, Windows will now install IIS (see Figure 1.2). It may ask you for your operating system's disk.

8. IIS is now installed. Depending on your operating system, Windows may ask you to restart your computer.

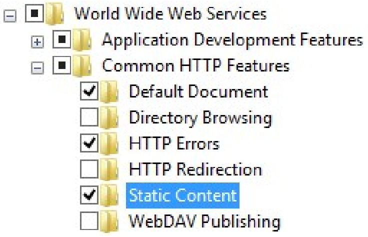
9. You can verify the installation of IIS by tapping the Windows key from your Desktop and typing IIS. Search results should return Internet Information Services (IIS) Manager.

10. We recommend running Windows Updates to receive the latest security patches for IIS once you have installed it.



- ⊟ ▣ Internet Information Services
  - ⊞ ☐ FTP Server
  - ⊟ ▣ Web Management Tools
    - ⊞ ☐ IIS 6 Management Compatibility
    - ☐ IIS Management Console
    - ☐ IIS Management Scripts and Tools
    - ☐ IIS Management Service
  - ⊟ ▣ World Wide Web Services
    - ⊟ ▣ Application Development Features
      - ☐ .NET Extensibility 3.5
      - ☑ .NET Extensibility 4.5
      - ☐ Application Initialization
      - ☐ ASP
      - ☐ ASP.NET 3.5
      - ☑ ASP.NET 4.5
      - ☐ CGI
      - ☑ ISAPI Extensions
      - ☑ ISAPI Filters
      - ☐ Server-Side Includes
      - ☐ WebSocket Protocol

Figure 2.1 – Selecting additional features



- ⊟ ▣ World Wide Web Services
  - ⊞ ▣ Application Development Features
  - ⊟ ▣ Common HTTP Features
    - ☑ Default Document
    - ☐ Directory Browsing
    - ☑ HTTP Errors
    - ☐ HTTP Redirection
    - ☑ Static Content
    - ☐ WebDAV Publishing

Figure 2.2 – Installing additional features

Installing ASP.NET 4.5 and the .NET Framework 4.5.1 / 4.5.2

For operating systems other than Windows 8.1 or Windows Server 2012 R2, .NET Framework 4.5.1 is not included by default. To install version 4.5.1, use the offline installer provided by Microsoft, found here.

If you installed IIS in the instructions above, then ASP.NET 4.5 should already be installed.

Microsoft has released an SP2 update for the .NET Framework which contains compatibility fixes for applications running on previous versions. It is recommended that this update is installed after the .NET Framework 4.5 has been installed. It can be downloaded here.

Installing and Configuring Microsoft SQL Server

We recommend using Microsoft SQL Server 2012. A free edition called Microsoft SQL Server Express is available to download.

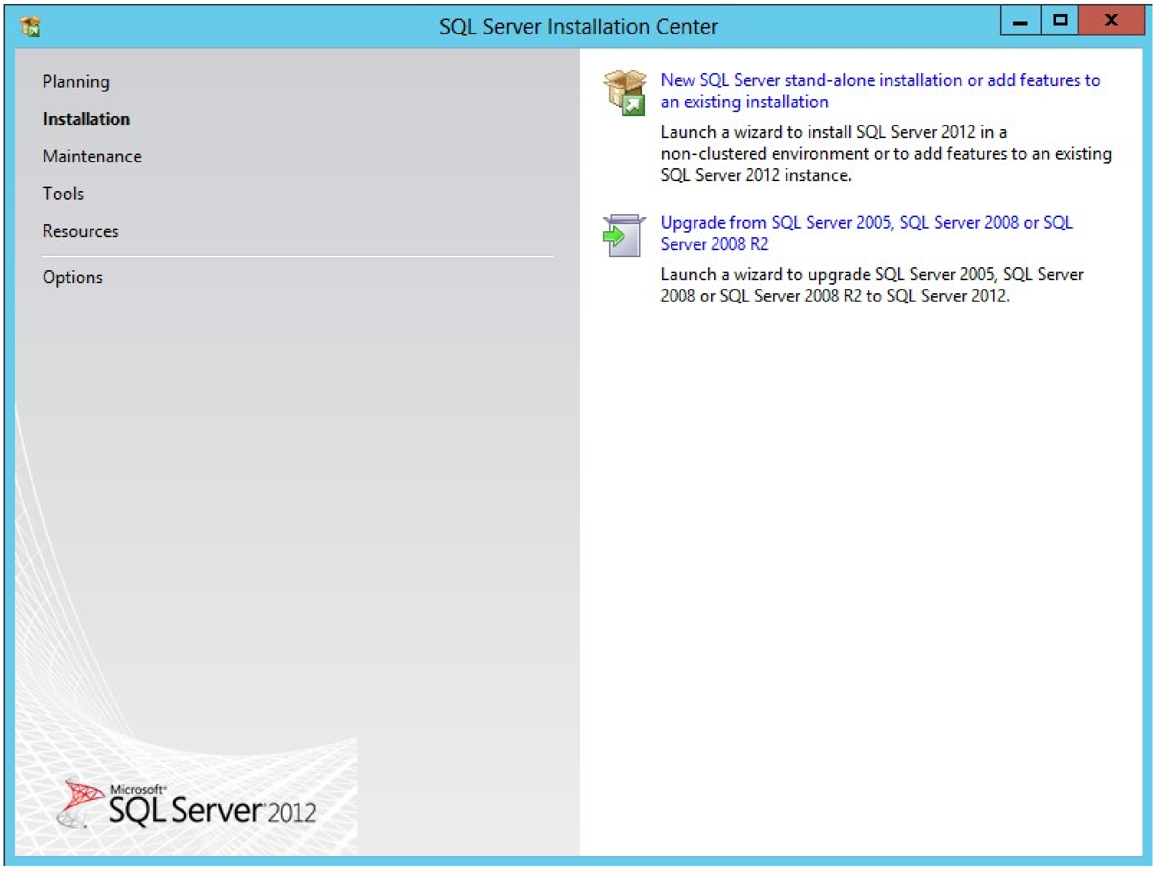
Please Note: Secret Server and Password Reset Server require SQL_Latin1_General_CP1_CI_AS to be the default collation for Microsoft SQL Server and its database. Using a different default collation will cause the installation to fail. See Microsoft SQL collation requirements and check your server collation settings before upgrading.

Installing Microsoft SQL Sever

The instructions given below are for Microsoft SQL Server 2012 Express Edition with Tools. The installation processes for other editions such as Enterprise or Standard may be similar, but not the same.

There are several editions of Microsoft SQL Server 2012 Express. We recommend downloading Microsoft SQL Server 2012 Express with Tools. This KB article has the link on Microsoft's site.

1. Download the installation package, right-click it and select Run as Administrator.
2. From the welcome screen, select Installation from the left menu.
3. Select the New SQL Server option (see Figure 1.1, on the following page).
4. SQL Server will then initialize your installation.
5. Accept the license terms and click Next.
6. Click Next once more to install the setup files.
7. In the following Window (Figure 1.2), ensure that Database Engine Services and Management Tools – Basic are both selected. Click Next.
8. In the Instance Configuration step, the default settings can be left (Named instance: SQLEXPRESS is the default). Click Next.
9. For Server Configuration, change the SQL Server Database Engine Account Name to NT AUTHORITY\NETWORK SERVICE. Click Next.



SQL Server Installation Center

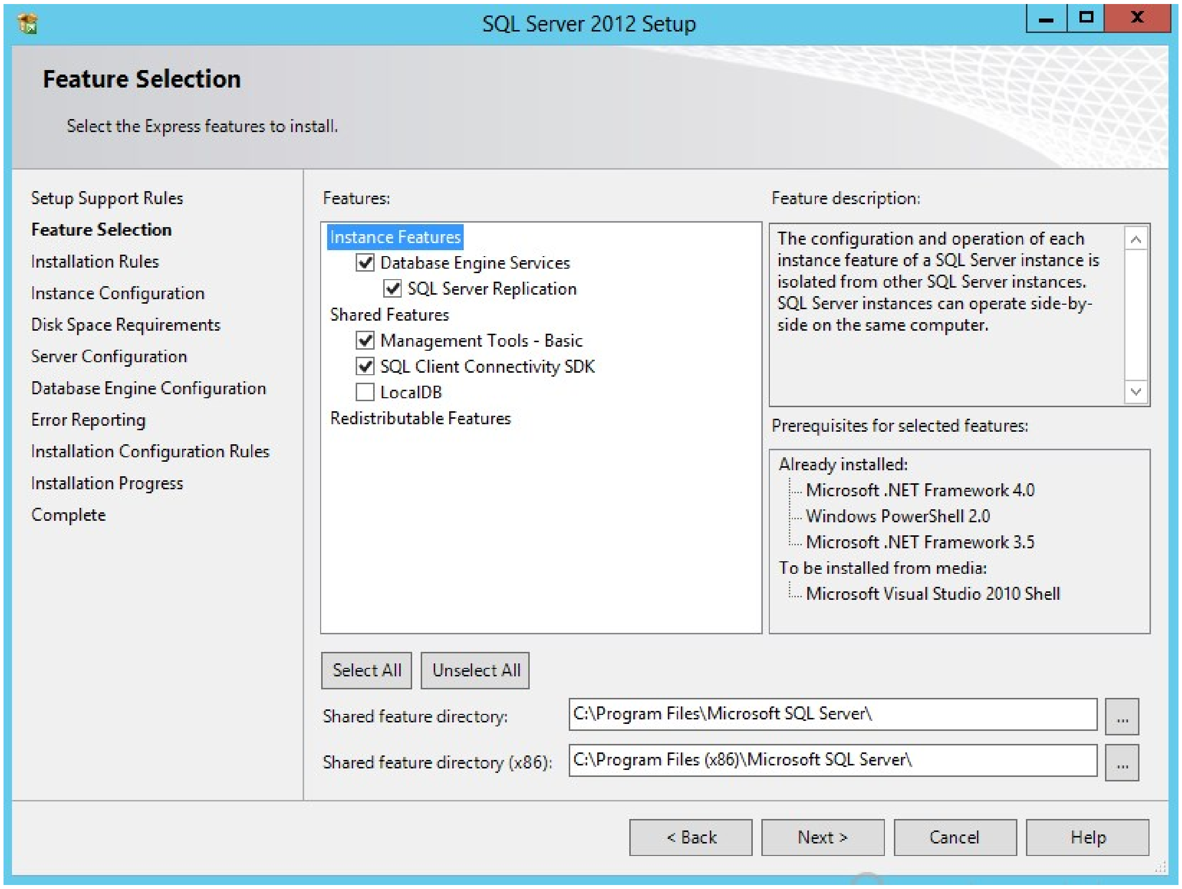
New SQL Server stand-alone installation or add features to an existing installation

Launch a wizard to install SQL Server 2012 in a non-clustered environment or to add features to an existing SQL Server 2012 instance.

Upgrade from SQL Server 2005, SQL Server 2008 or SQL Server 2008 R2

Launch a wizard to upgrade SQL Server 2005, SQL Server 2008 or SQL Server 2008 R2 to SQL Server 2012.

Figure 1.1 – SQL Server Installation Center



Feature Selection

Select the Express features to install.

Features:

Instance Features
- ☑ Database Engine Services
  - ☑ SQL Server Replication

Shared Features
- ☑ Management Tools - Basic
- ☑ SQL Client Connectivity SDK
- ☐ LocalDB

Redistributable Features

Feature description:

The configuration and operation of each instance feature of a SQL Server instance is isolated from other SQL Server instances. SQL Server instances can operate side-by-side on the same computer.

Prerequisites for selected features:

Already installed:
- Microsoft .NET Framework 4.0
- Windows PowerShell 2.0
- Microsoft .NET Framework 3.5

To be installed from media:
- Microsoft Visual Studio 2010 Shell

Shared feature directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory (x86): C:\Program Files (x86)\Microsoft SQL Server\

Figure 1.2 – SQL Server Feature Selection

10. For Database Engine Configuration, choose Mixed Mode or Windows mode:

- *Mixed Mode (recommended for easiest configuration)* - Mixed Mode is required if you intend on using a SQL Server account to authenticate Password Reset Server to your SQL Server. If you are doing an evaluation and using the Password Reset Server MSI, we recommend Mixed Mode with a SQL Authentication account. See [Creating the SQL Server User](#Adding a SQL Server User) (below) for instructions.

- *Windows Mode (recommended for best security)* - This will prevent SQL Server account authentication and requires a Windows Service account to run the Password Reset Server website. This will also require additional configuration in IIS once Password Reset Server is installed. This KB article walks through the advanced setup. This mode is recommended as a best practice.

11. Click Add Current User under the SQL Server administrators box. Click Next.

12. Click Next once more to complete the installation.

We recommend running Microsoft Update to get all of the latest service packs and fixes for SQL 2012.

Creating the Database

1. Open SQL Server Management Studio.

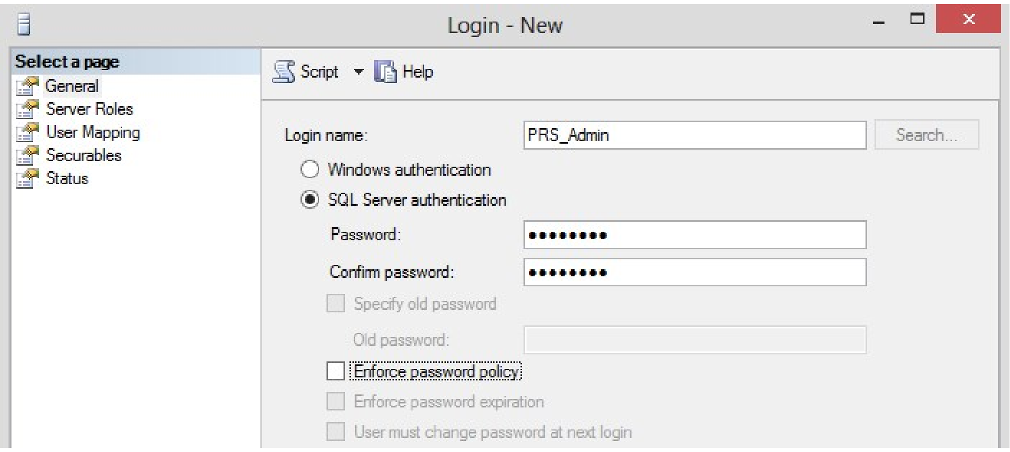
2. Connect to your SQL database.

3. Right click the Databases folder and select New Database.

4. Enter a database name and click OK.

Adding a SQL Server User

1. Open SQL Server Management Studio.
2. Connect to your SQL database.
3. Expand the Security folder.
4. Right click Logins and select New Login.
    1. To create a **local SQL account**, select SQL Server authentication (this requires Mixed Mode to be enabled).
        1. Enter a login name (username) and password.
        2. Uncheck the Enforce password policy box to prevent the account from expiring.
    2. To add a **Windows account**, select Windows authentication.
        1. Enter a login name in the form of domain\username, or click Search to search for the domain account.
5. Select the User Mappings from the left menu.
6. Check the checkbox next to your Password Reset Server database.
7. Check the db_owner box.
8. Click OK.



Login name: PRS_Admin

○ Windows authentication

● SQL Server authentication

Password: ••••••••

Confirm password: ••••••••

□ Specify old password

Old password:

□ Enforce password policy

□ Enforce password expiration

□ User must change password at next login

Figure 3.1 – Creating a SQL user

Make sure you have the *prerequisites* installed before attempting to setup Password Reset Server.

Download the latest version of Password Reset Server

To download the installation file for the newest version of Password Reset Server, go to our Support Community page, log in, and click the Password Reset Server panel. Follow the prompts to navigate to the new download page, where you can download the **Installer (.msi)** file for automated installation.

Running the MSI

When running the setup.exe file, your first option will be to choose Standard or Advanced.

Standard Option

This option installs Password Reset Server as a virtual directory under the Default Website. This is recommended if you have existing sites using the Default Website, and is also the fastest way to get up and running.

Advanced Option

This option installs Password Reset Server as a new website without using the Default Website. This allows you to specify a port number that the website will run under. Using this option assumes some knowledge of IIS and is often followed up by adding a DNS entry on the domain controller. This option must be used if there is no Default Website already present.

File Destination

This is the location where the application files will exist. The folder is typically C:\inetpub\wwwroot\PasswordResetServer but can be customized to follow your convention.

Application Name

Application name will be used when creating the Application Pool and either the website or the virtual directory, depending on the selected option above.

Completing Installation from Password Reset Server

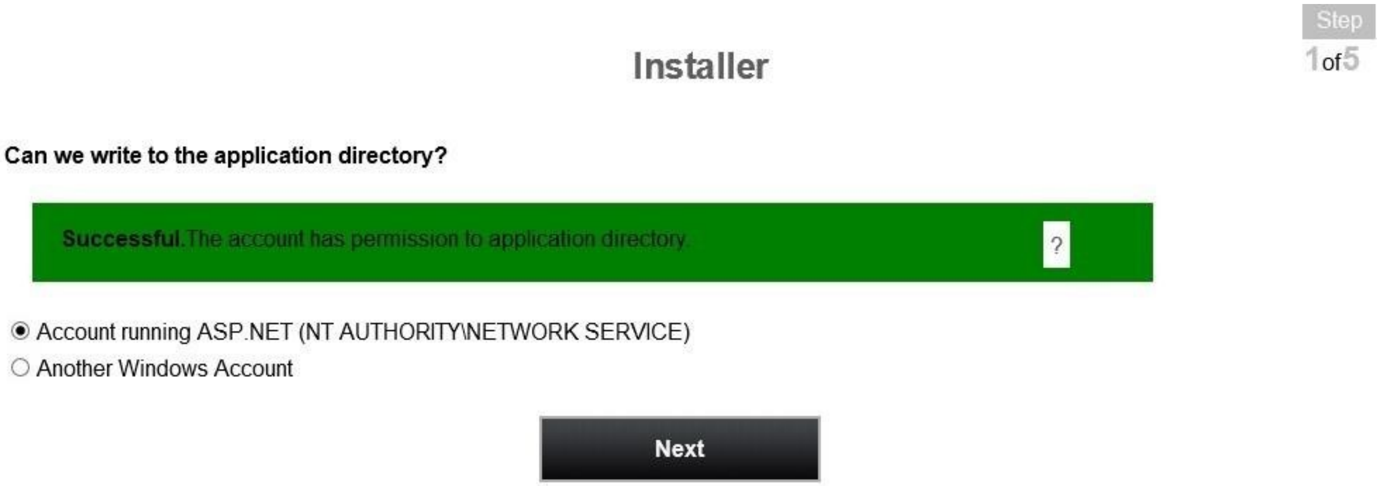
Once the MSI completes, the website will be set up with the correct permissions. The browser will open to allow you to complete the Password Reset Server installation from the webpage. The following section will guide you through this process.

Password Reset Server is now ready to begin installation through its installer. Open a browser and browse to where your Password Reset Server is located, for example:

http://localhost/passwordresetserver

Password Reset Server has a 5-step installation process:

1. Step 1 ensures that the identity running the Password Reset Server application pool has write access to the application directory. The account running the IIS application pool requires modify permission (this includes the write permission) to the application folder to continue.



Installer

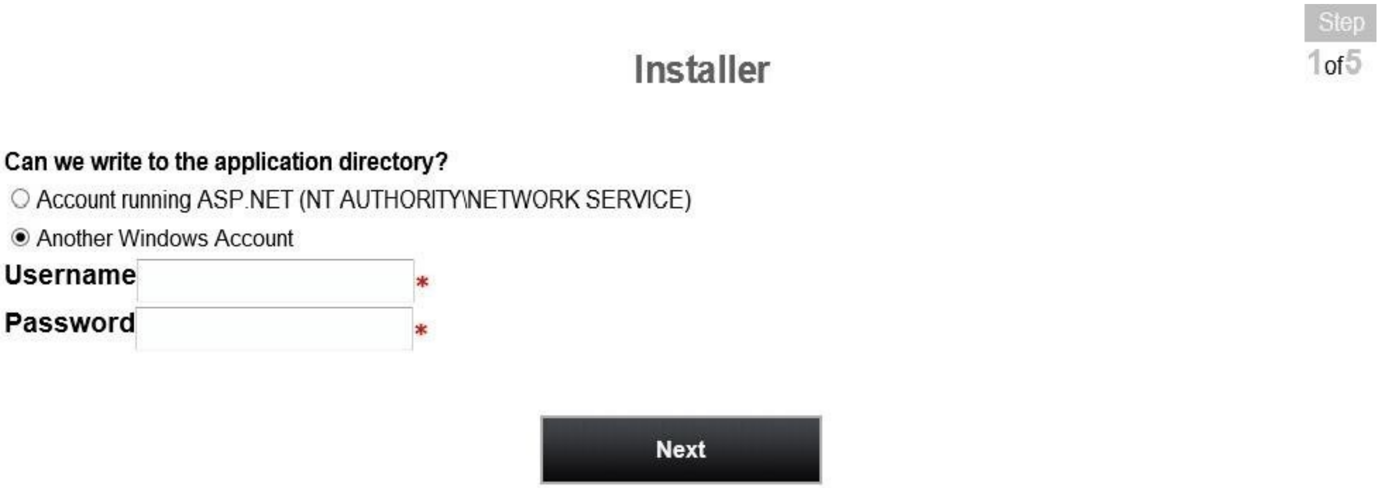
Step 1 of 5

Can we write to the application directory?

Successful. The account has permission to application directory.

● Account running ASP.NET (NT AUTHORITY\NETWORK SERVICE)
○ Another Windows Account

If you don't want to change the permissions of a folder, you can give Password Reset Server a Windows username and password that has modify permissions already, and Password Reset Server will "impersonate" as that user during the installation process.



Installer

Step 1 of 5

Can we write to the application directory?

○ Account running ASP.NET (NT AUTHORITY\NETWORK SERVICE)
● Another Windows Account

Username *

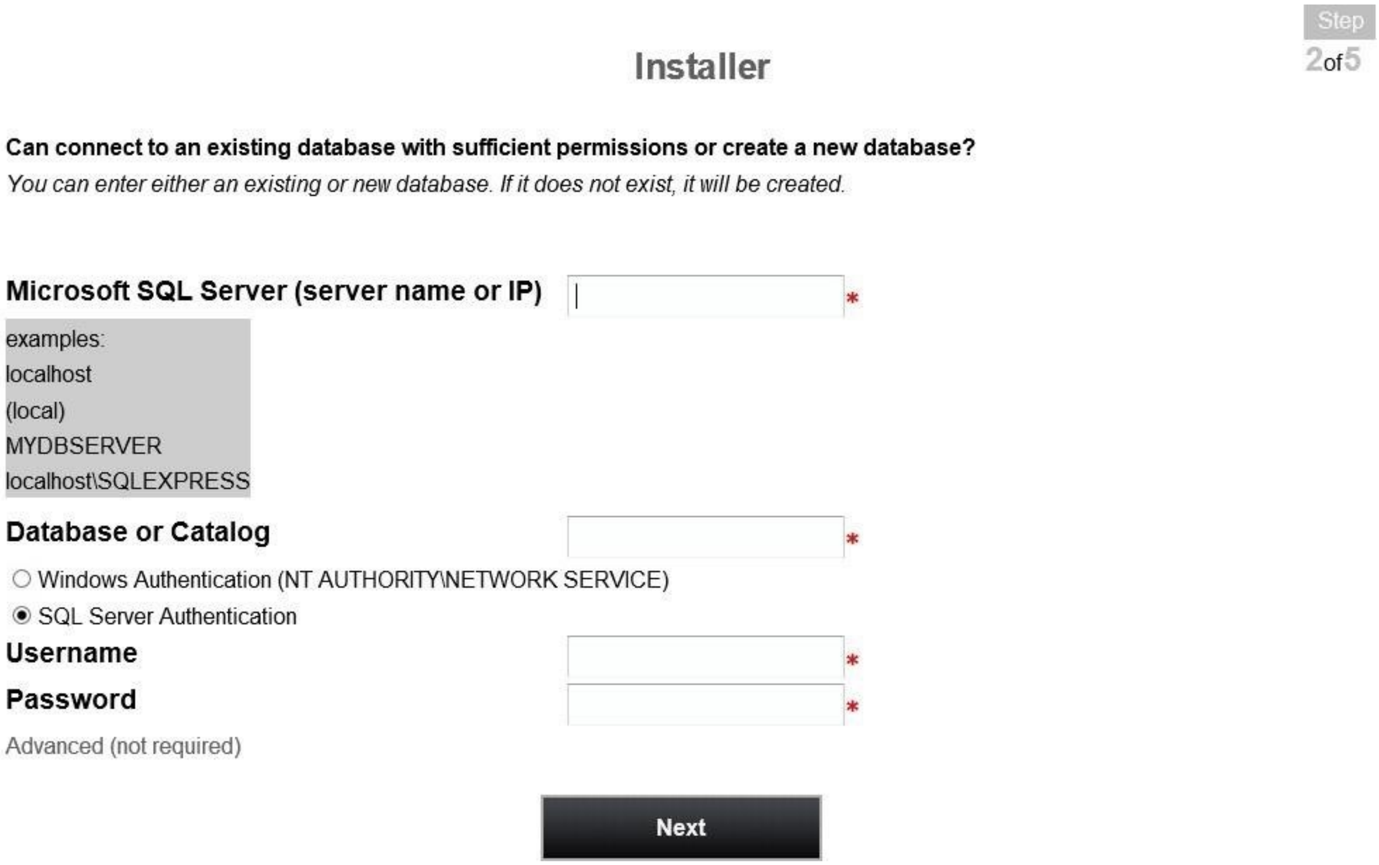
Password *

Password Reset Server only needs write permission during installation and upgrade. You can remove the write and modify permissions once the installation process is complete.

Once the permissions are set, click Next.

See the *Manual Installation* section for more information on account permissions.

2. In Step 2, specify the database. If Password Reset Server is installed on the same machine as SQL Server, you can type (local). If you are using a named instance of SQL, use a slash then the instance name, for instance: (local)\InstanceName. If you are not sure of the instance name, you can open SQL Server Management Studio and select Connect. The full instance name used here is the same one that will be used by Password Reset Server, for example THYCO1\SQLEXPRESS.



Step 2of5

Installer

Can connect to an existing database with sufficient permissions or create a new database?

You can enter either an existing or new database. If it does not exist, it will be created.

Microsoft SQL Server (server name or IP) | *

examples:
localhost
(local)
MYDBSERVER
localhost\SQLEXPRESS

Database or Catalog *

○ Windows Authentication (NT AUTHORITY\NETWORK SERVICE)

● SQL Server Authentication

Username *

Password *

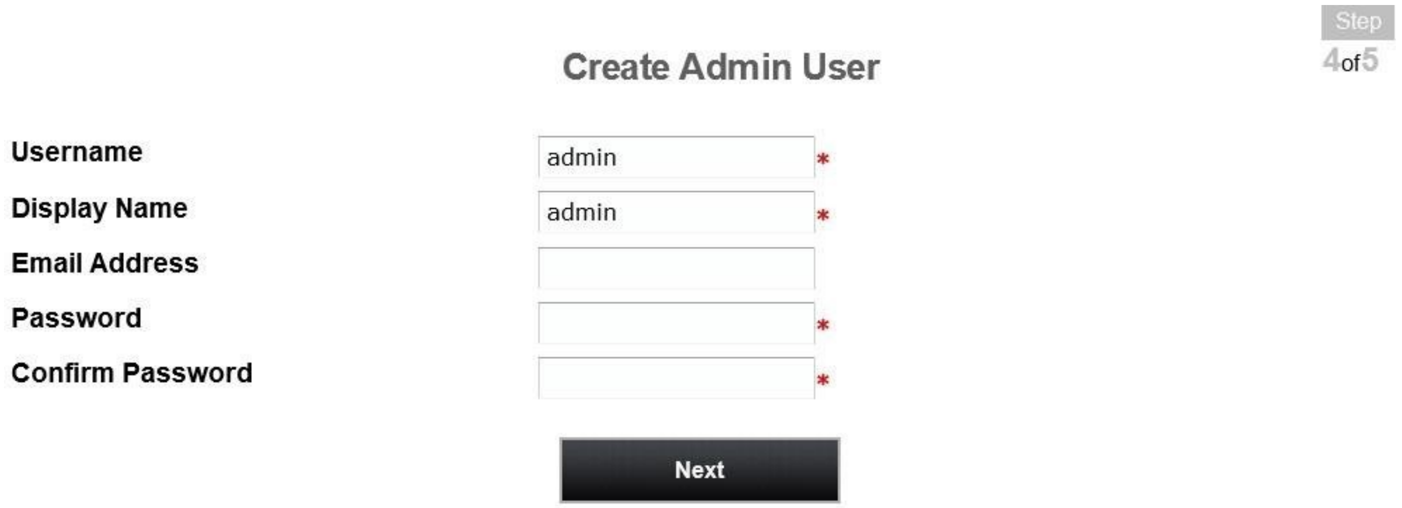
Advanced (not required)

Password Reset Server will create the database for you if it does not exist.

Enter the SQL Username and Password if using SQL Server Authentication, or select Windows Authentication. To create a SQL Server user, see *Creating the SQL Server User*.

3. Review the EULA and check the I Agree box, then click Continue to accept the agreement. Otherwise, Password Reset Server will not be installed.

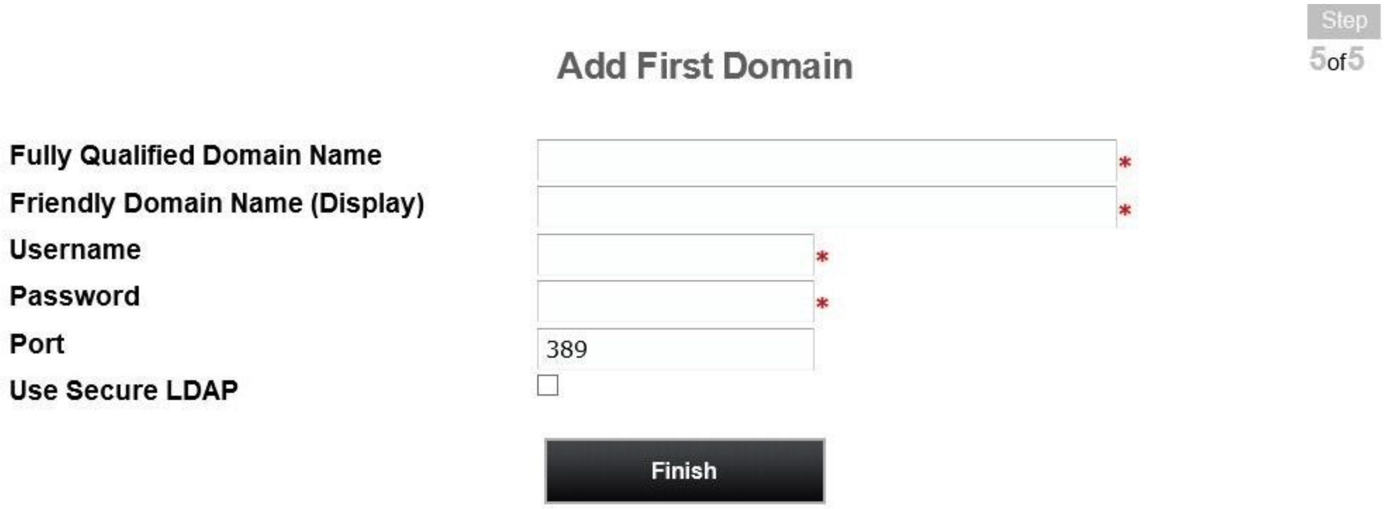
4. Password Reset Server will now ask you to create your first user. This user will be a local administrator that will be used to configure your Password Reset Server. We recommend choosing a strong password.



Create Admin User

Username	admin *
Display Name	admin *
Email Address	
Password	*
Confirm Password	*

5. Step 5 will prompt you to enter a domain and credentials for a domain account that has the required permissions to reset passwords on the domain. See *Creating a Domain Account to Reset Passwords*.



Add First Domain

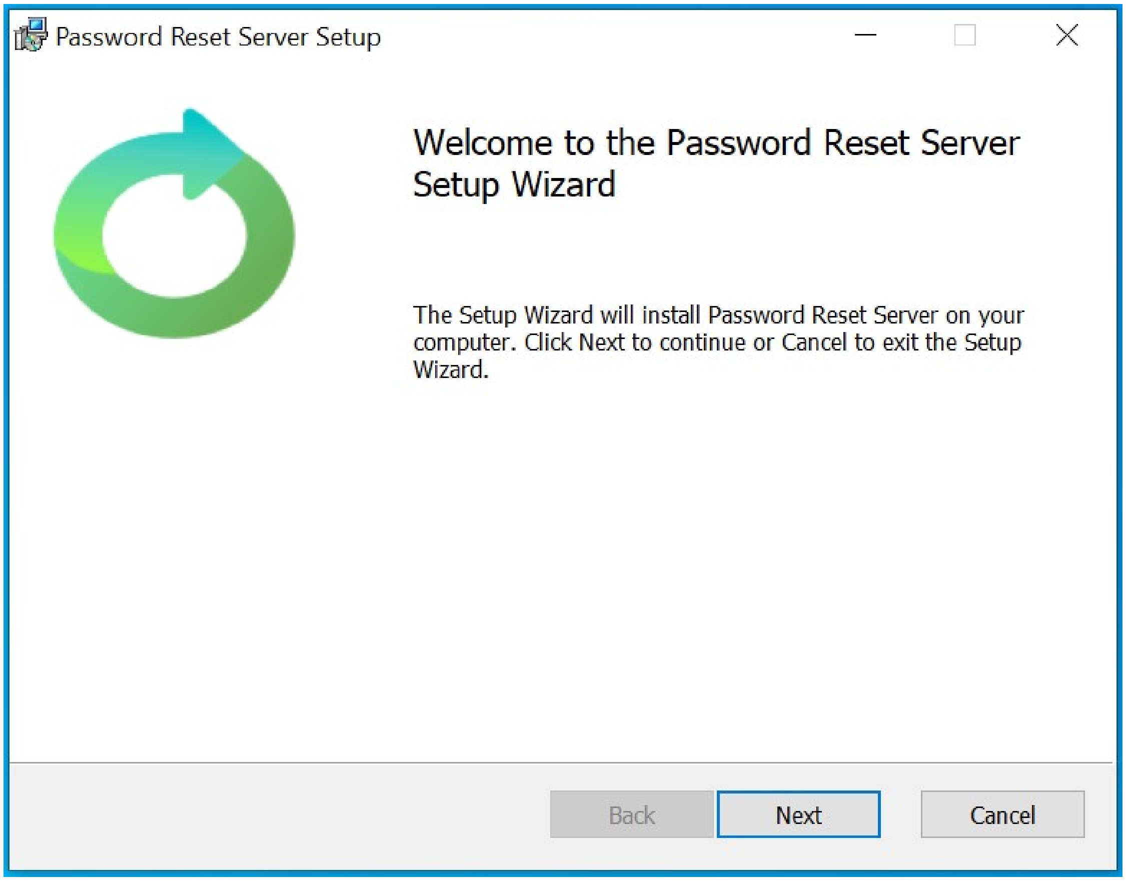
Fully Qualified Domain Name	*
Friendly Domain Name (Display)	*
Username	*
Password	*
Port	389
Use Secure LDAP	□

The domain name needs to be the Fully Qualified Domain Name (FQDN), for example: use *domain.thycotic.com* instead of *domain*.

Password Reset Server has now successfully been installed. For more information on configuring and maintaining your Password Reset Server, please see our User Guide.

The following covers the steps for the Password Reset Server installer for versions 5.2.0 and later. Ensure that IIS is enabled on the system you are installing Password Reset Server on.

1. Download the installer ZIP file and extract the contents for the MSI file.
    1. Go to our Support Community page, log in, and click the Password Reset Server panel.
    2. Follow the prompts to navigate to the new download page, where you can choose to download an MSI file for automated installation, or a zip file for manual installation.
2. Run the Installer file with Admin rights.
3. Click **Next**.

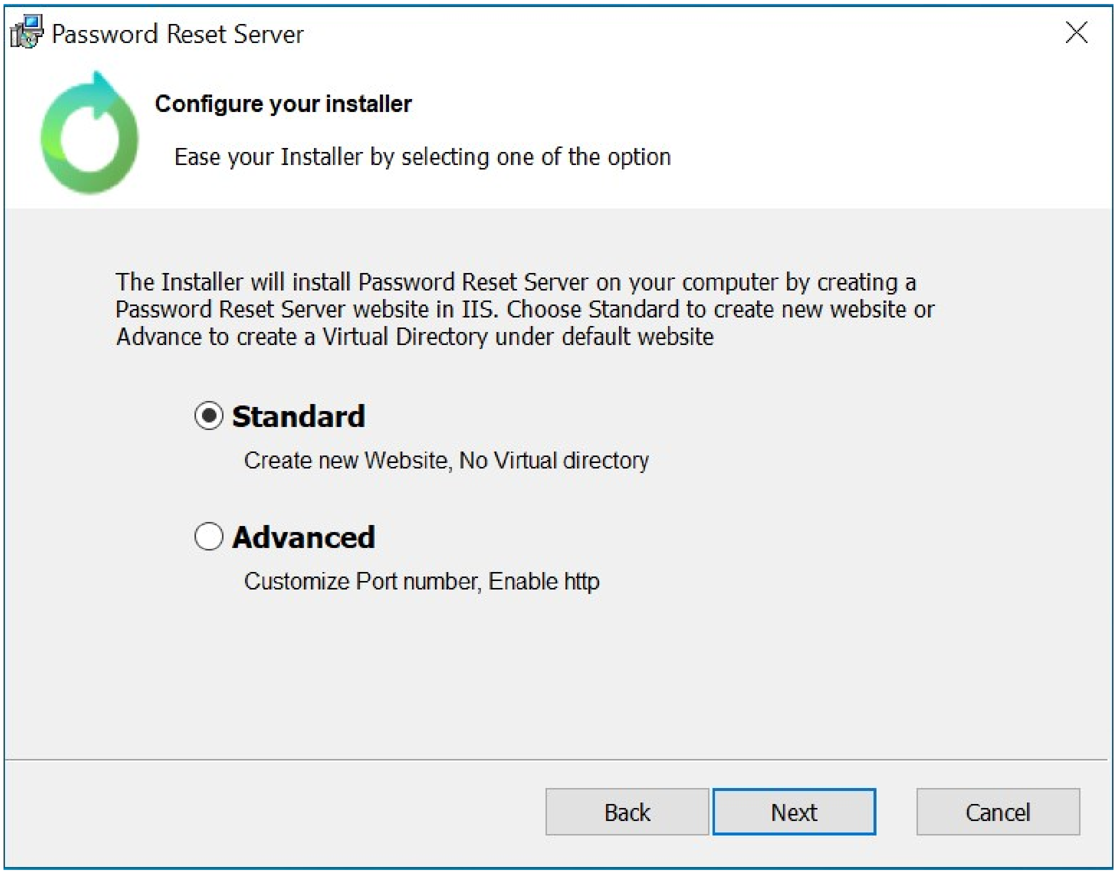


Password Reset Server Setup

Welcome to the Password Reset Server Setup Wizard

The Setup Wizard will install Password Reset Server on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

4. On the **Configure your installer** page you can choose one of the following options:



Password Reset Server

Configure your installer

Ease your Installer by selecting one of the option

The Installer will install Password Reset Server on your computer by creating a Password Reset Server website in IIS. Choose Standard to create new website or Advance to create a Virtual Directory under default website

● **Standard**

Create new Website, No Virtual directory

○ **Advanced**

Customize Port number, Enable http

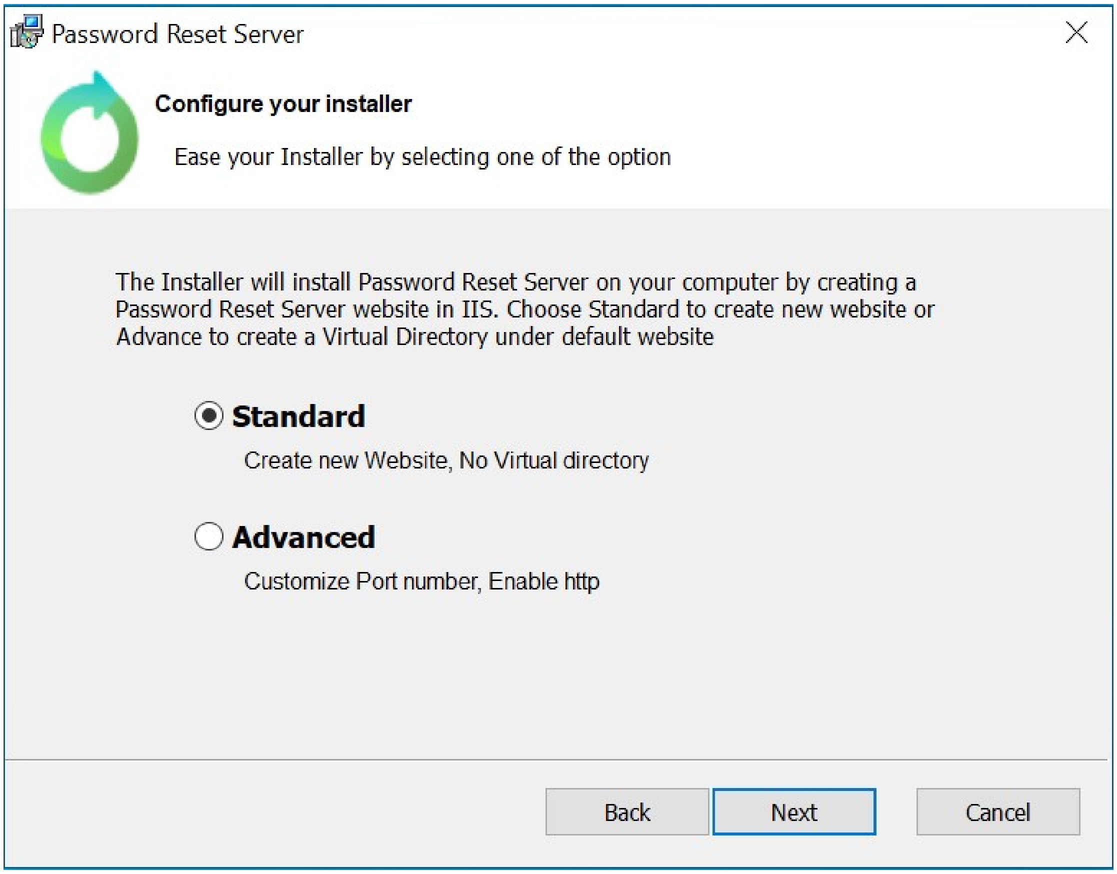
- **Standard:** This option installs Password Reset Server as a virtual directory under the Default Website. This is recommended if you have existing sites using the Default Website, and is also the fastest way to get up and running.
- **Advanced:** This option installs Password Reset Server as a new website without using the Default Website. This allows you to specify a port number that the website will run under. Using this option assumes some knowledge of IIS and is often followed up by adding a DNS entry on the domain controller. This option must be used if there is no Default Website already present.

5. Select the option you would like to use and click **Next**.

Standard Install

The following steps are for selecting the **Standard** option in the install wizard.

1. Select the Standard option and click **Next**.



Password Reset Server

Configure your installer

Ease your Installer by selecting one of the option

The Installer will install Password Reset Server on your computer by creating a Password Reset Server website in IIS. Choose Standard to create new website or Advance to create a Virtual Directory under default website

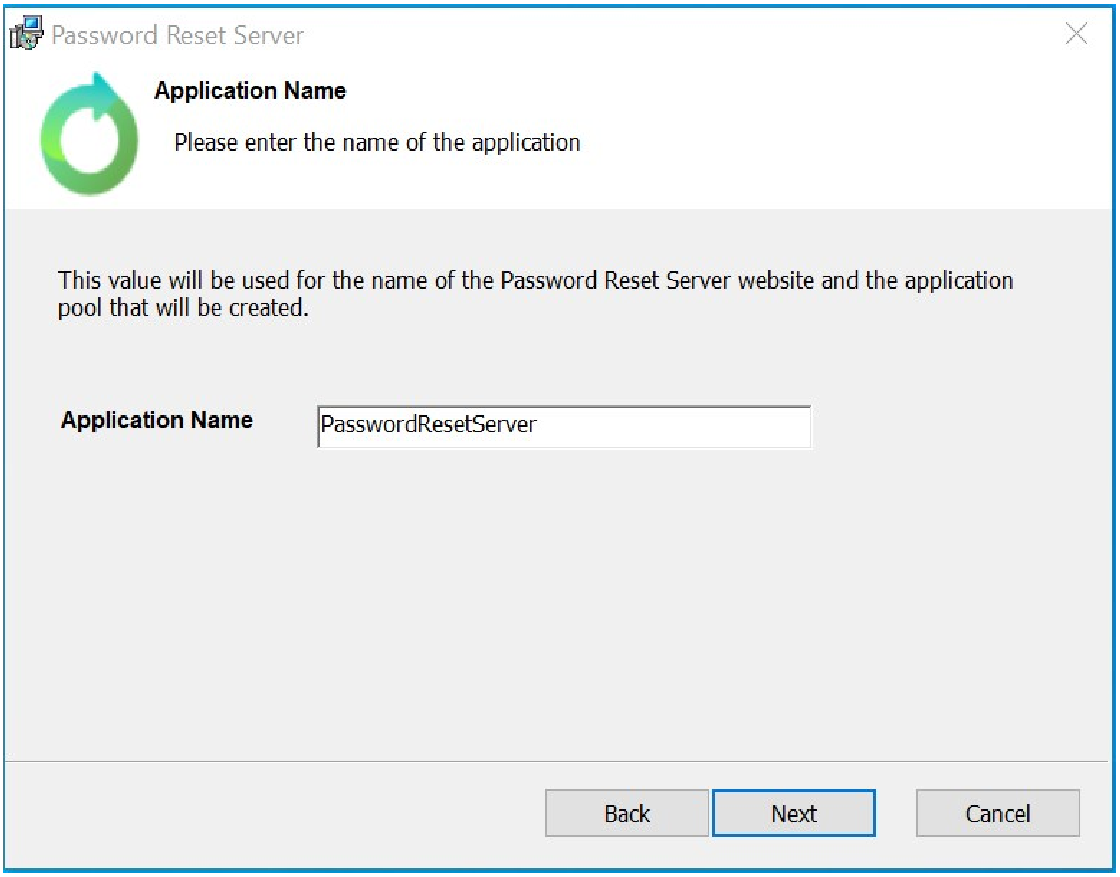
● **Standard**

Create new Website, No Virtual directory

○ **Advanced**

Customize Port number, Enable http

2. You can enter the **Application Name** value that will be used in IIS. By default this is set to **PasswordResetServer**. You can keep the default or change the value to something else. Once the value is entered, click **Next**.



Password Reset Server

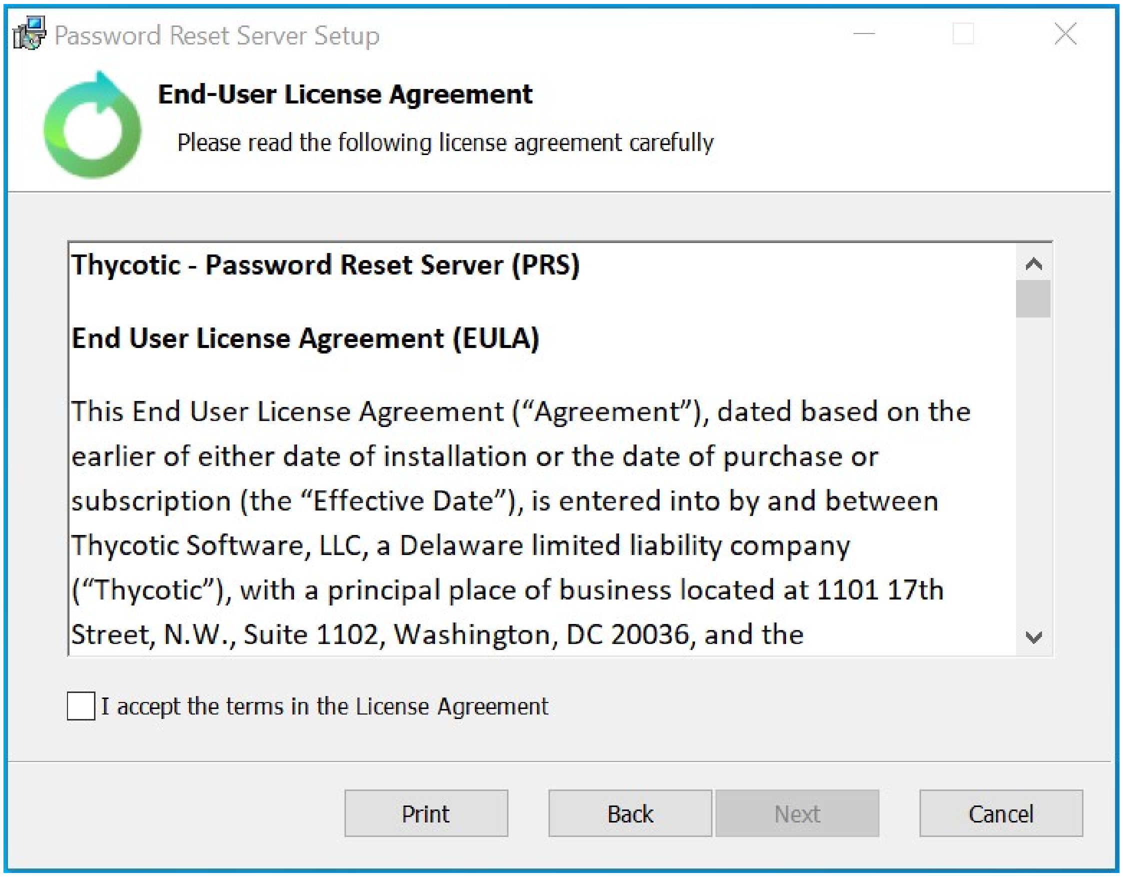
Application Name

Please enter the name of the application

This value will be used for the name of the Password Reset Server website and the application pool that will be created.

Application Name PasswordResetServer

3. Review the End-User License Agreement and click the **I accept the terms in the License Agreement** check-box if you agree to the terms.



End-User License Agreement

Please read the following license agreement carefully

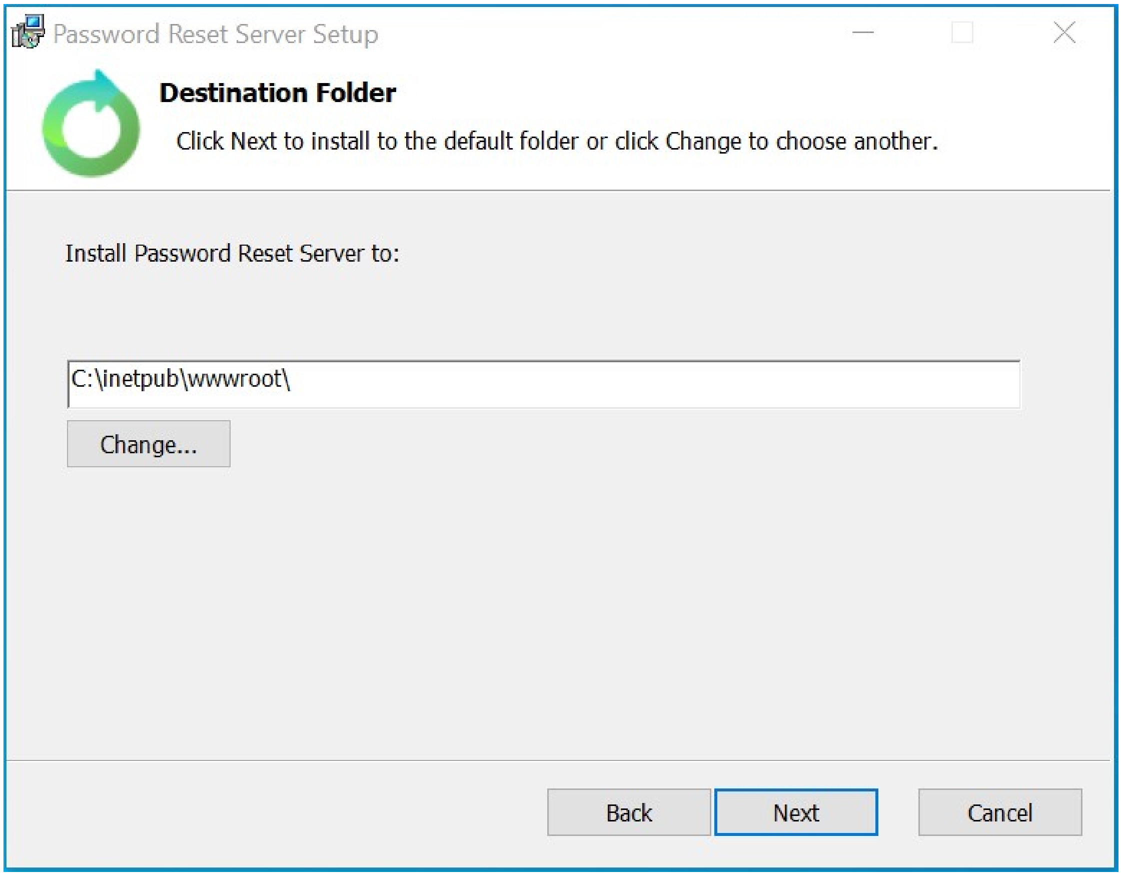
Thycotic - Password Reset Server (PRS)

End User License Agreement (EULA)

This End User License Agreement (“Agreement”), dated based on the earlier of either date of installation or the date of purchase or subscription (the “Effective Date”), is entered into by and between Thycotic Software, LLC, a Delaware limited liability company (“Thycotic”), with a principal place of business located at 1101 17th Street, N.W., Suite 1102, Washington, DC 20036, and the

□ I accept the terms in the License Agreement

4. Click **Next** after you agree to continue.
5. On the **Destination Folder** page you can select what folder to install PRS under for IIS.



Password Reset Server Setup

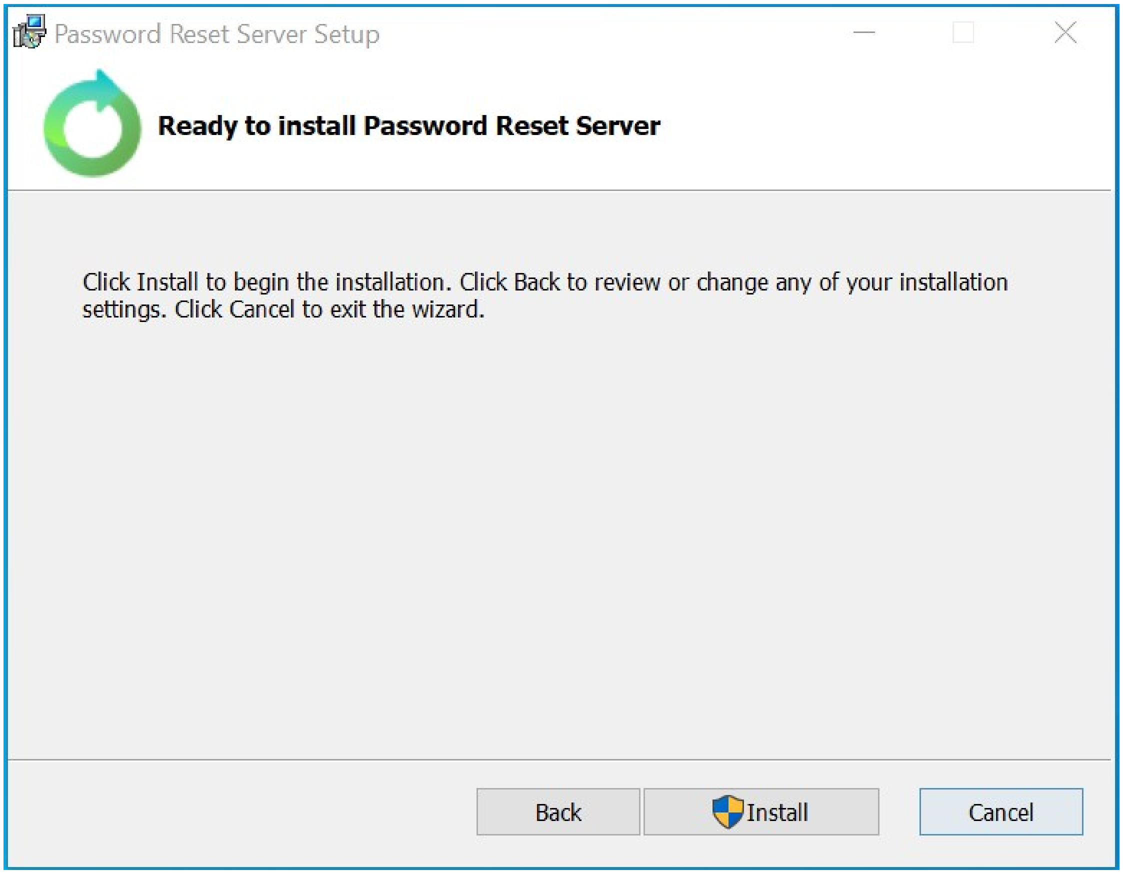
Destination Folder

Click Next to install to the default folder or click Change to choose another.

Install Password Reset Server to:

C:\inetpub\wwwroot\

6. You can either Change the root directory to install the PRS files under or leave the default value C:\inetpub\wwwroot\.
7. After you have selected the folder to install PRS under, click the **Next** button.
8. All of the Standard steps are now complete, and you are ready to install Password Reset Server.


Password Reset Server Setup

Ready to install Password Reset Server

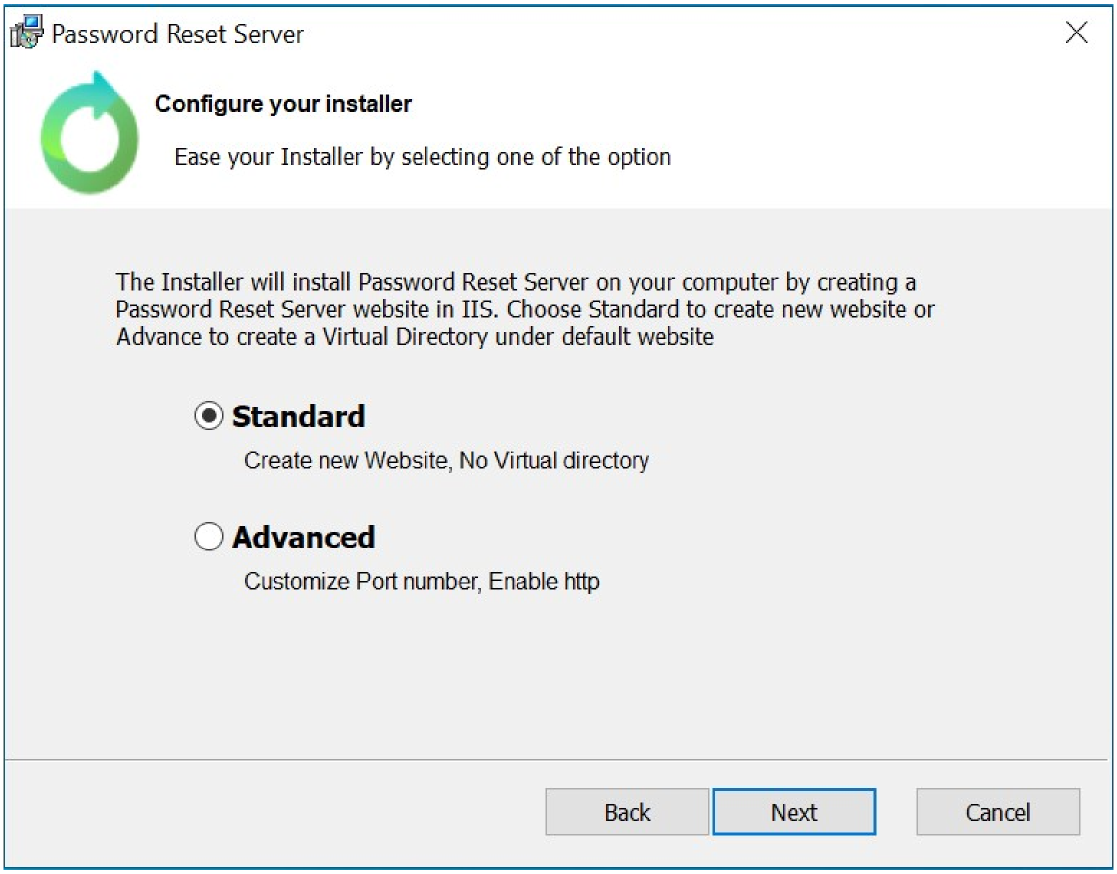
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

9. Click the **Install** button to finalize the install and begin the file creation on your system.

Advanced Install

The following steps are for selecting the Advanced option in the install wizard.

1. Select the Advanced option and click **Next** to proceed.



Password Reset Server

Configure your installer

Ease your Installer by selecting one of the option

The Installer will install Password Reset Server on your computer by creating a Password Reset Server website in IIS. Choose Standard to create new website or Advance to create a Virtual Directory under default website

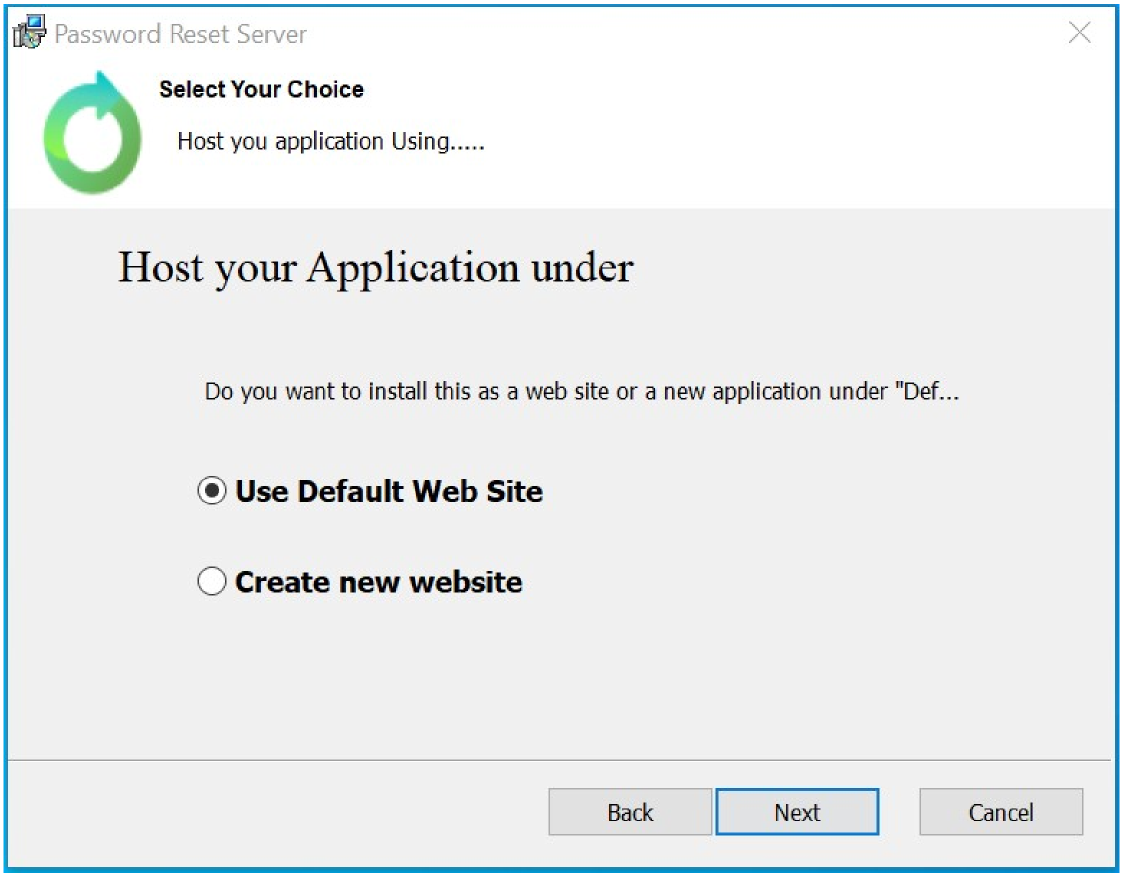
● **Standard**

Create new Website, No Virtual directory

○ **Advanced**

Customize Port number, Enable http

2. On the **Select your Choice** screen you can decide where to host the Password Reset Server application. There are two options:
   - **Use Default Web Site:** This will host the application under the default website in IIS. This includes defaulting to use HTTPS as well as using the default Port value.
   - **Create new website:** This will create a new website in IIS to host the application (for Password Reset Server), and the new website will not be under the default site in IIS.



Password Reset Server

Select Your Choice

Host you application Using.....

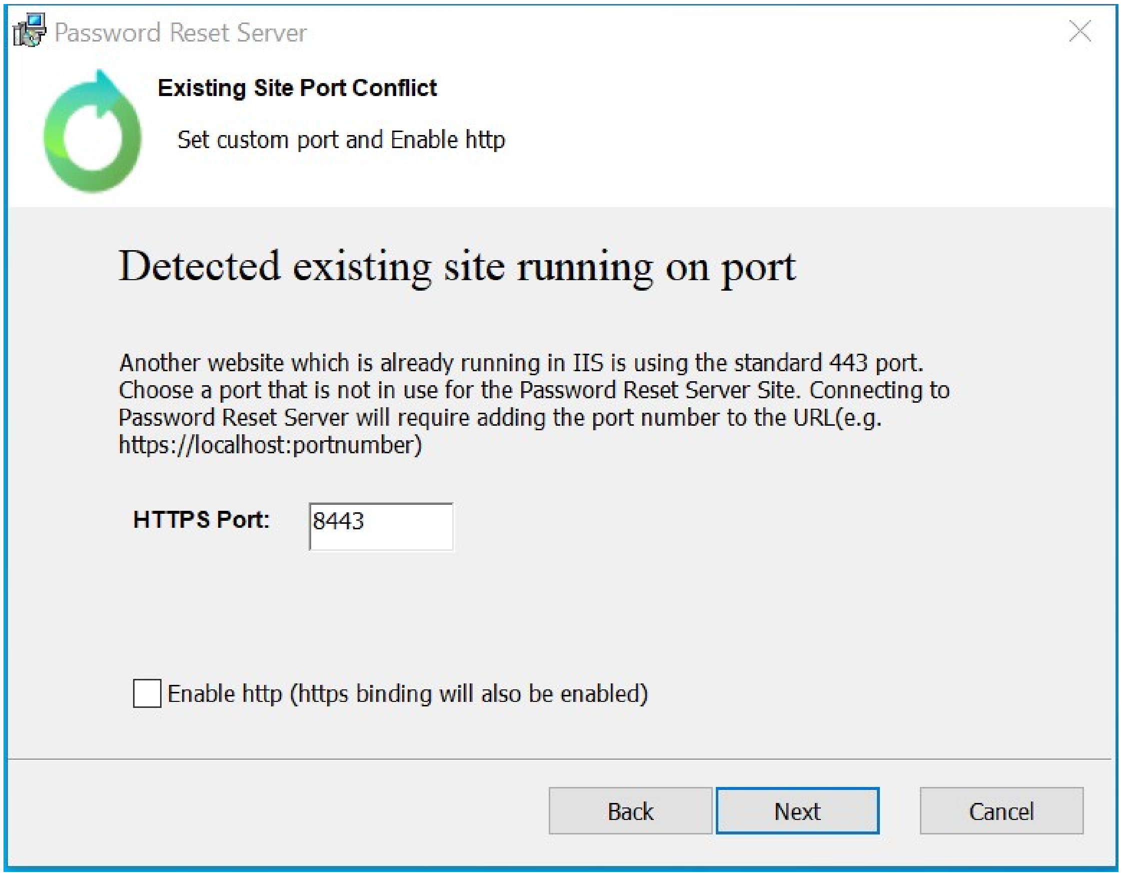
Host your Application under

Do you want to install this as a web site or a new application under "Def...

● **Use Default Web Site**

○ **Create new website**

3. Clicking the **Next** button when this option is selected will then take you to the **Existing Site Port Conflict** screen (if a site is already detected in IIS).



Password Reset Server

Existing Site Port Conflict

Set custom port and Enable http

Detected existing site running on port

Another website which is already running in IIS is using the standard 443 port. Choose a port that is not in use for the Password Reset Server Site. Connecting to Password Reset Server will require adding the port number to the URL(e.g. https://localhost:portnumber)

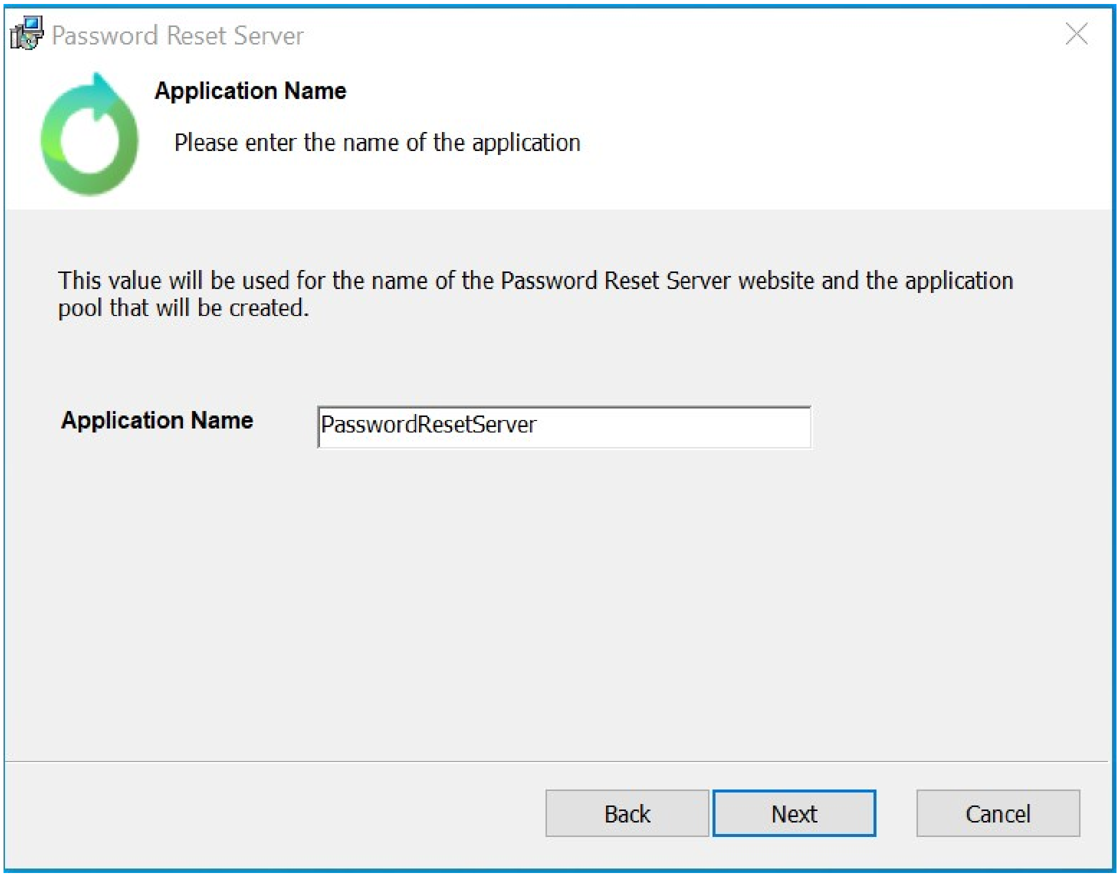
HTTPS Port: 8443

□ Enable http (https binding will also be enabled)

- Users can either manually enter a **HTTPS Port** value or they can use the value that is populated when they get to the page.
- There is also a check-box to allow the configuration to enable HTTP support (including setting the HTTP port number) instead of requiring HTTPS support for the URL.

4. Once these options have been set, click **Next** to continue.

5. After selecting the location to Host the application, you will be brought to the **Application Name** page.



Password Reset Server

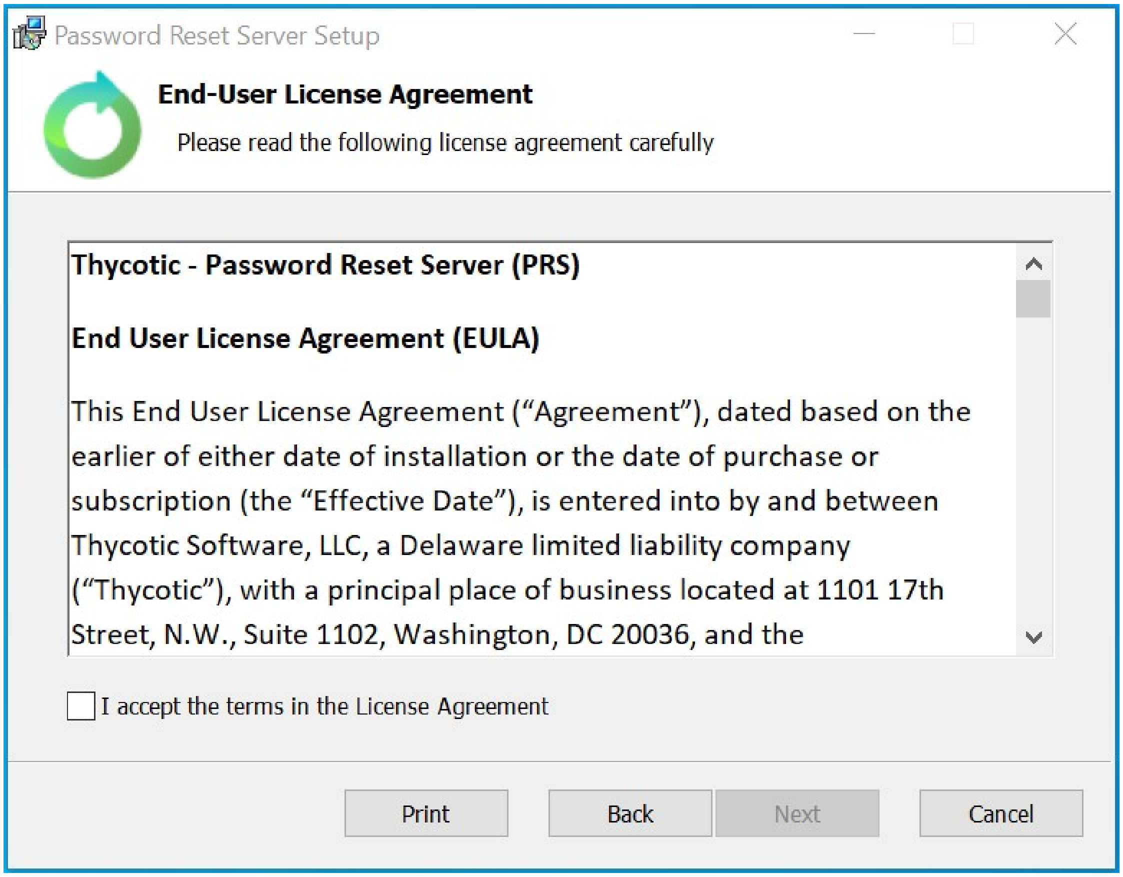
Application Name

Please enter the name of the application

This value will be used for the name of the Password Reset Server website and the application pool that will be created.

Application Name: PasswordResetServer

6. You can enter the **Application Name** value that will be used in IIS. By default this is set to **PasswordResetServer**. You can keep the default or change the value to something else. Once the value is entered, click **Next**.
7. Review the End-User License Agreement and click the **I accept the terms in the License Agreement** check-box if you agree to the terms and want to continue.



Password Reset Server Setup

End-User License Agreement

Please read the following license agreement carefully

Thycotic - Password Reset Server (PRS)

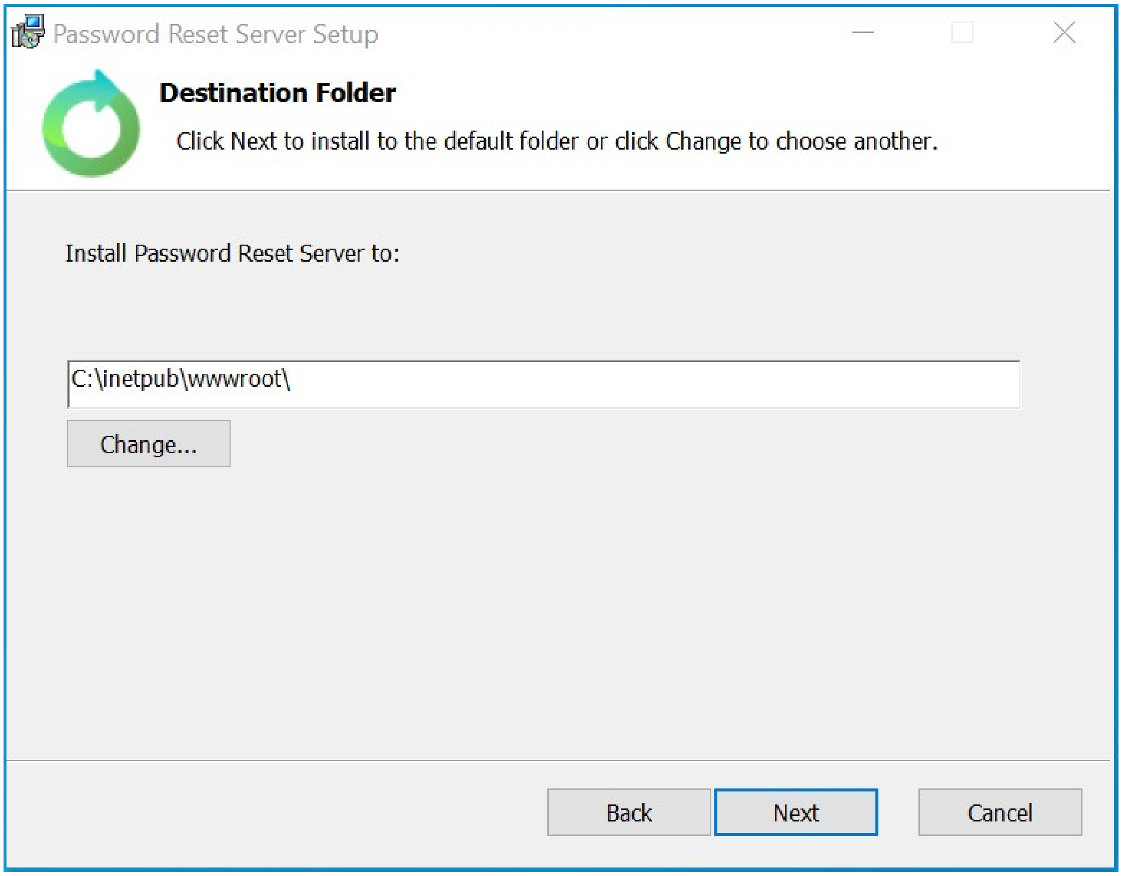
End User License Agreement (EULA)

This End User License Agreement ("Agreement"), dated based on the earlier of either date of installation or the date of purchase or subscription (the "Effective Date"), is entered into by and between Thycotic Software, LLC, a Delaware limited liability company ("Thycotic"), with a principal place of business located at 1101 17th Street, N.W., Suite 1102, Washington, DC 20036, and the

□ I accept the terms in the License Agreement

8. Click **Next** after you agree to continue.

9. On the **Destination Folder** page you can select what folder to install PRS under for IIS.



Password Reset Server Setup

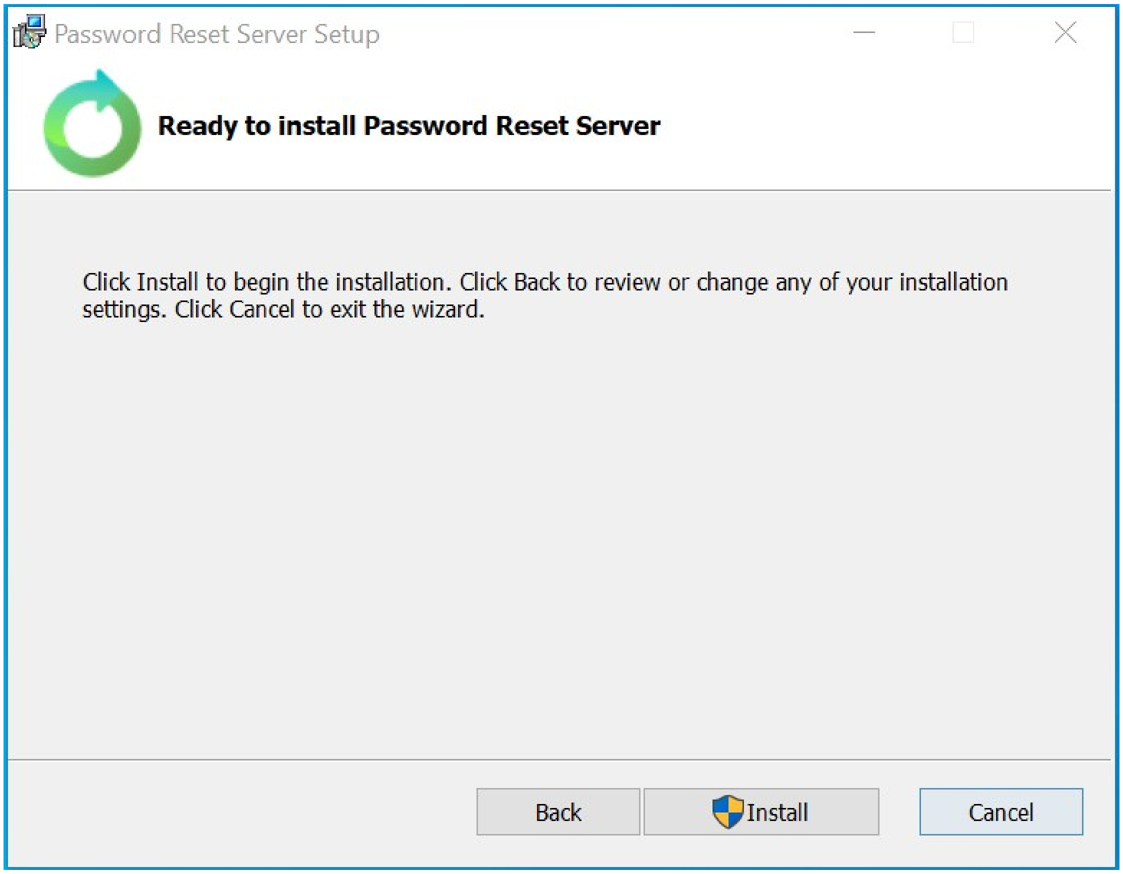
Destination Folder

Click Next to install to the default folder or click Change to choose another.

Install Password Reset Server to:

C:\inetpub\wwwroot\

10. You can either Change the root directory to install the PRS files under or leave the default value (C:\inetpub\wwwroot).
11. After you have selected the folder to install PRS under, click the **Next** button.
12. All of the Advanced steps are now complete, and you are ready to install Password Reset Server.



Password Reset Server Setup

Ready to install Password Reset Server

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

13. Click the **Install** button to finalize the install and begin the file creation on your system.

14. Once the install has run you will be prompted to finish the installer. You can close the Installer dialog by clicking the **Finish** button.

This part of the installation is complete. The website will be set up with the correct permissions and the browser will open to allow you to complete the Password Reset Server installation from the webpage.

This does not impact a fresh install and the following steps should only be used for upgrade purposes. Some servers have their file upload limits set too low. Before upgrading, be sure to check your IIS server and web application settings to ensure the upgrade process completes.

Steps before Upgrading

1. Stop the IIS Server
2. Go to the PRS install directory default path is C:\inetpub\wwwroot\PasswordResetServer. This is root of where Password Reset Server is installed.
3. Look for the web.config file.

   Note: It is suggested to create a back up before making any changes to the web.config file.
4. Open the web.config file in notepad and look for the system.webServer tag.
5. Add the following entry just below the system.webServer

```
<security>
 <requestFiltering>
  <requestLimits maxAllowedContentLength="131072000" />
 </requestFiltering>
</security>
```

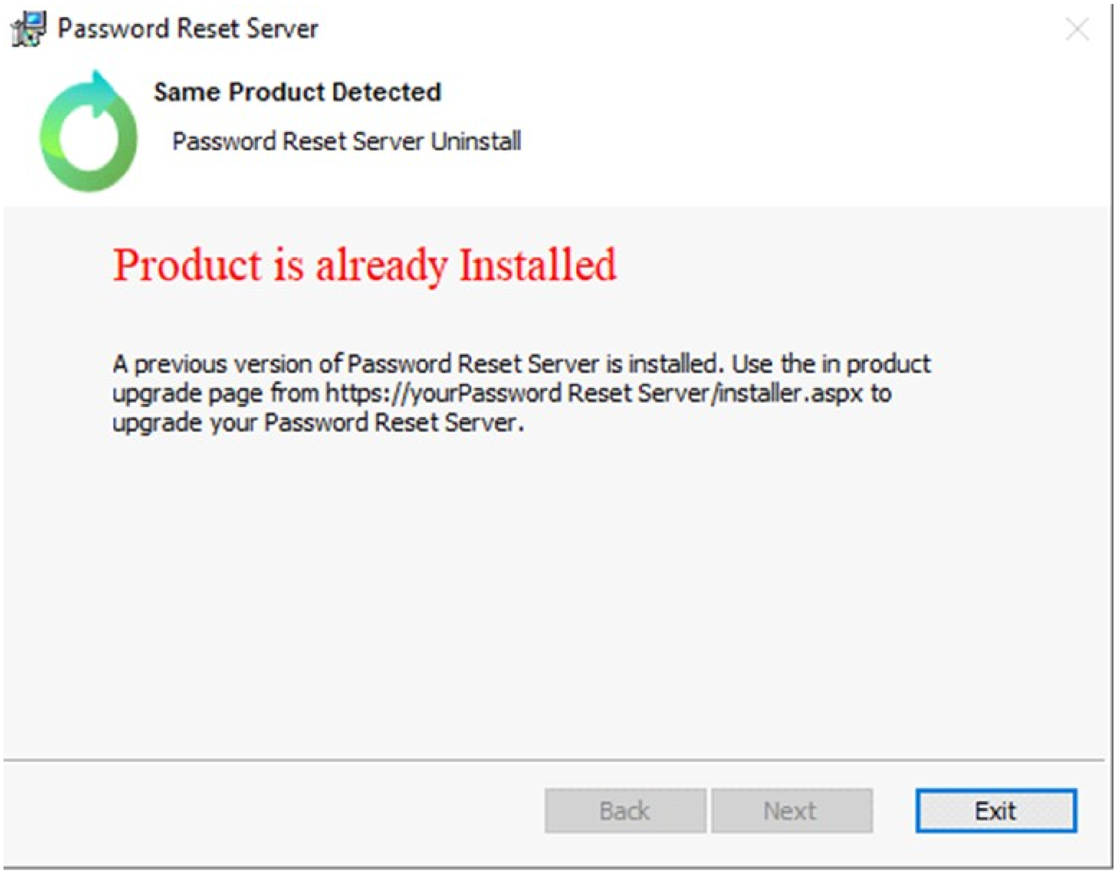
6. Search for the location path="InstallerCheckForUpdates.aspx" tag.
7. Inside this tag update the **maxRequestLength** value to "128000" and **execution timeout** value to 1100.

   Example: <httpRuntime maxRequestLength="128000" executionTimeout="1100"/>
8. Save the web.config file.
9. Restart **IIS**.
10. Use the normal upgrade process to upgrade Password Reset Server.

Upgrading from an older version of Password Reset Server

When upgrading from older version of Password Reset Server it is recommended to use the in-product upgrade page to begin this process. This page can be accessed from (depending on your permissions) “https://YourPasswordResetServerURL/installer.aspx".

If Password Reset Server is already installed in your environment and you attempt to re-run the installer, the installer process will try to detect if PRS is already configured and, if detected, will prompt you to perform the upgrade using the page above.



Password Reset Server

Same Product Detected

Password Reset Server Uninstall

Product is already Installed

A previous version of Password Reset Server is installed. Use the in product upgrade page from https://yourPassword Reset Server/installer.aspx to upgrade your Password Reset Server.

Manual Upgrade

Password Reset Server periodically polls our update server to detect for updates. However, if your Password Reset Server is on an internal network that does not have outbound access or goes through a proxy, it will not be able to perform updates.

As of 2.1.00000 (for older version please contact support), the recommended method is the using 'Advanced options' to manually select and upload the upgrade file.

If you are knowledgeable of IIS and would prefer to manually install the website without using the MSI, you can follow these instructions.

To download the installation file for the newest version of Password Reset Server, go to our Support Community page, log in, and click the Password Reset Server panel. Follow the prompts to navigate to the new download page, where you can download the **Application Files** (zip) for manual installation. Use this ZIP file for the instructions below.

Password Reset Server can be installed in a few different ways:

- As a virtual directory
- As a website
- As part of a website

Make sure you have the *required software* installed before attempting to setup Password Reset Server.

Installing as a virtual directory

1. Extract the contents of the ZIP file where you would like Password Reset Server to be located on your system.
2. Open the IIS Control Panel by going into the Control Panel, then Administrative Tools > Internet Information Services (IIS) Manager.
3. Highlight the Default Web Site, right-click it and select Add Virtual Directory (see Figure 1.1 below).
4. Select an alias for your Password Reset Server. The alias is what will be appended to the website. For instance, *http://myserver/PasswordResetServer*.
5. Select the physical directory for where you unzipped Password Reset Server.
6. In the tree, right-click the virtual directory and select Convert to Application. Click OK.
7. Click the Application Pools node, then highlight the application pool running Password Reset Server. Click Advanced Settings in the right pane. Under Process Model, set Identity to a Windows service account or leave the default ApplicationPoolIdentity (Figure 1.2).

   Windows 8 / Server 2012 will default the application pool to a virtual identity, ApplicationPoolIdentity. For easiest configuration, use either this or NETWORK SERVICE as the identity. For better security, you can specify your own Windows service account. See the *Appendix* for further information on using a virtual identity for Password Reset Server in IIS.

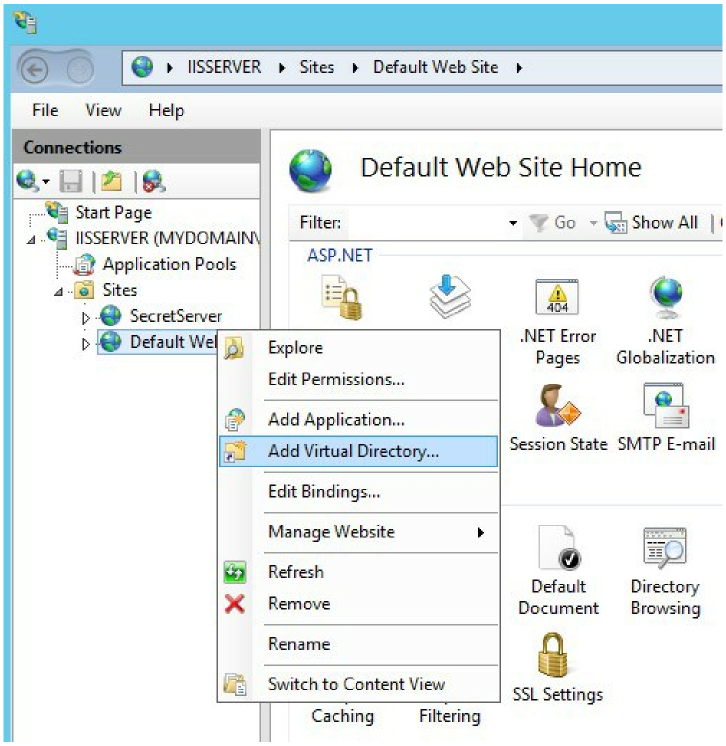


Figure 1.1 – Add Virtual Directory

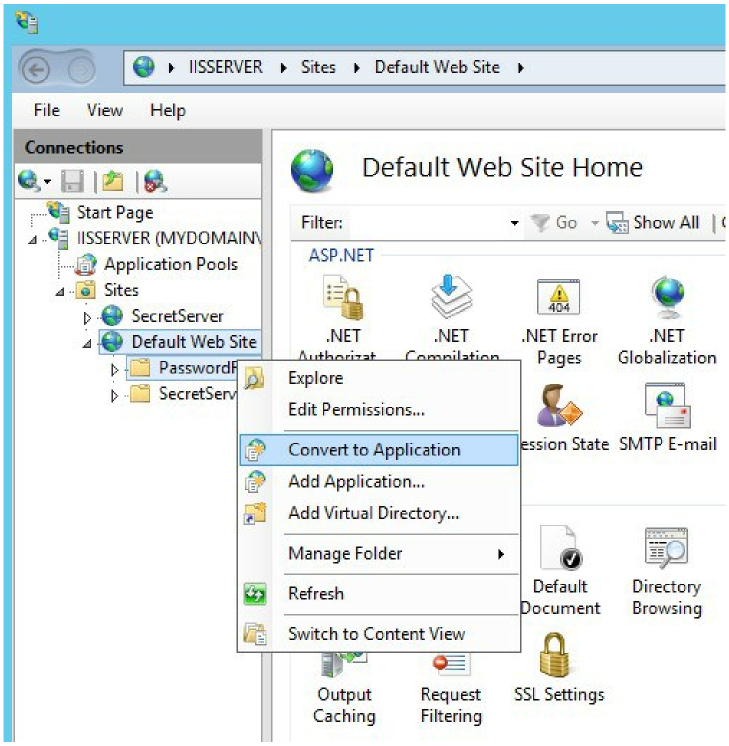


Figure 1.2 – Convert to Application

8. Ensure that the Password Reset Server folder has the proper permissions by checking that the account running the application pool in IIS has Modify permissions on the folder where Password Reset Server is installed.

Password Reset Server is now ready to be installed. See *Completing Password Reset Server installation*.

Installing as part of a website

1. Extract the contents of the ZIP file where you would like Password Reset Server to be located on your system (a common location is C:\inetpub\wwwroot).
2. Open the IIS Control Panel by going into the Control Panel, then Administrative Tools > Internet Information Services (IIS) Manager.
3. Expand the Default Website and locate the Password Reset Server folder. Right-click it, and select Convert to Application. Click OK.
4. Click the Application Pools node, then highlight the application pool running Password Reset Server. Click Advanced Settings in the right pane. Under Process Model, set Identity to a Windows service account or leave the default ApplicationPoolIdentity (Figure 1.2, see the previous page).

   Windows 8 / Server 2012 will default the application pool to a virtual identity, ApplicationPoolIdentity. For easiest configuration, use either this or NETWORK SERVICE as the identity. For better security, you can specify your own Windows service account. See the *Appendix* for further information on using a virtual identity for Password Reset Server in IIS.
5. Ensure that the Password Reset Server folder has the proper permissions by checking that the account running the application pool in IIS has Modify permissions on the folder where Password Reset Server is installed.

Password Reset Server is now ready to be installed. See *Completing Password Reset Server installation*.

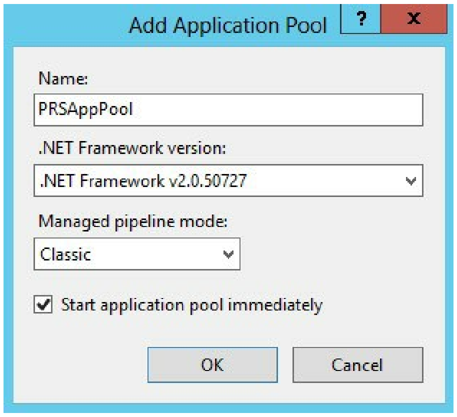
Configuring the pipeline

Password Reset Server is by default placed in the DefaultAppPool application pool, which may not be set to use the correct pipeline for Password Reset Server. PRS requires that the application pool's managed pipeline mode be set to Classic. This can be done by modifying the application pool settings or creating a new one.

It is recommended that you create a new application pool if you have other web applications running on the server. This will help avoid changing the configuration for another application.

Changing the Pipeline Mode

1. In the Internet Information Services (IIS) Manager, select the Application Pools node.
2. Double-click the DefaultAppPool.
3. Set Managed Pipeline Mode to Classic. Click OK.



Name:
PRSAppPool

.NET Framework version:
.NET Framework v2.0.50727

Managed pipeline mode:
Classic

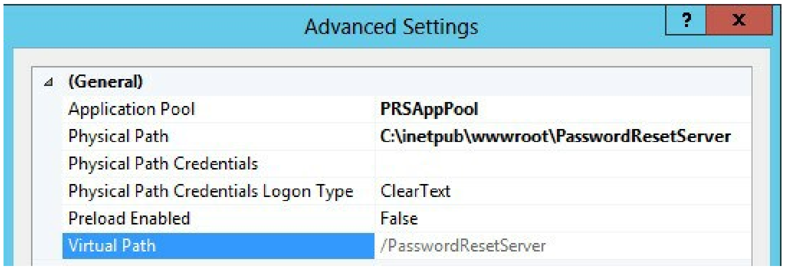
☑ Start application pool immediately

IIS Application Pool - Windows 8 IIS Application Pool - Windows 8.1

The Windows Server 2012 R2 and Windows 8.1 application pool window will appear slightly different than in Windows Server 2012 and Windows 8.

Creating a New Application Pool

1. In the Internet Information Services (IIS) Manager, right-click the Application Pools node and select Add Application Pool.
2. Enter a name for your application pool.
3. Ensure that the .NET Framework Version or CLR is set to .NET Framework v4.0.30319.
4. Set Managed Pipeline Mode to Classic. Click OK.
5. Right-click the virtual directory in IIS and select Manage Application > Advanced Settings.
6. In the new window, change Application Pool to the one we just created.



(General)	
Application Pool	**PRSAppPool**
Physical Path	**C:\inetpub\wwwroot\PasswordResetServer**
Physical Path Credentials	
Physical Path Credentials Logon Type	ClearText
Preload Enabled	False
Virtual Path	/PasswordResetServer

Figure 2.1 – Specify Application Pool

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.

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.

Default Roles

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

Administrator

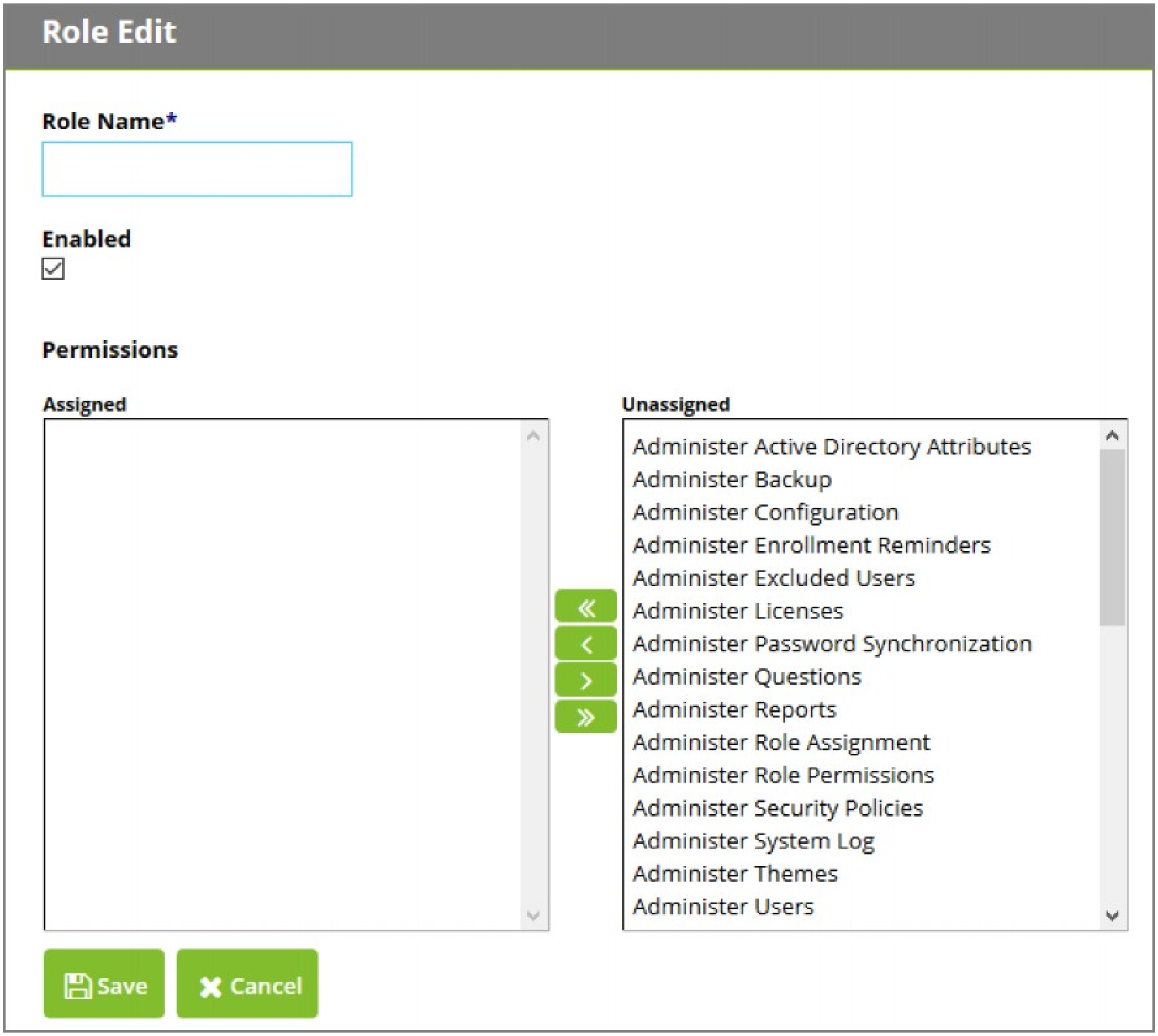
The Administrator role comes will all permissions. The first account created is placed in this role.

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, click the **Administration** link on the top navigation bar and select **Roles**, then **Create**.



Give your role a name. 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. Finally, click **Save**.

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

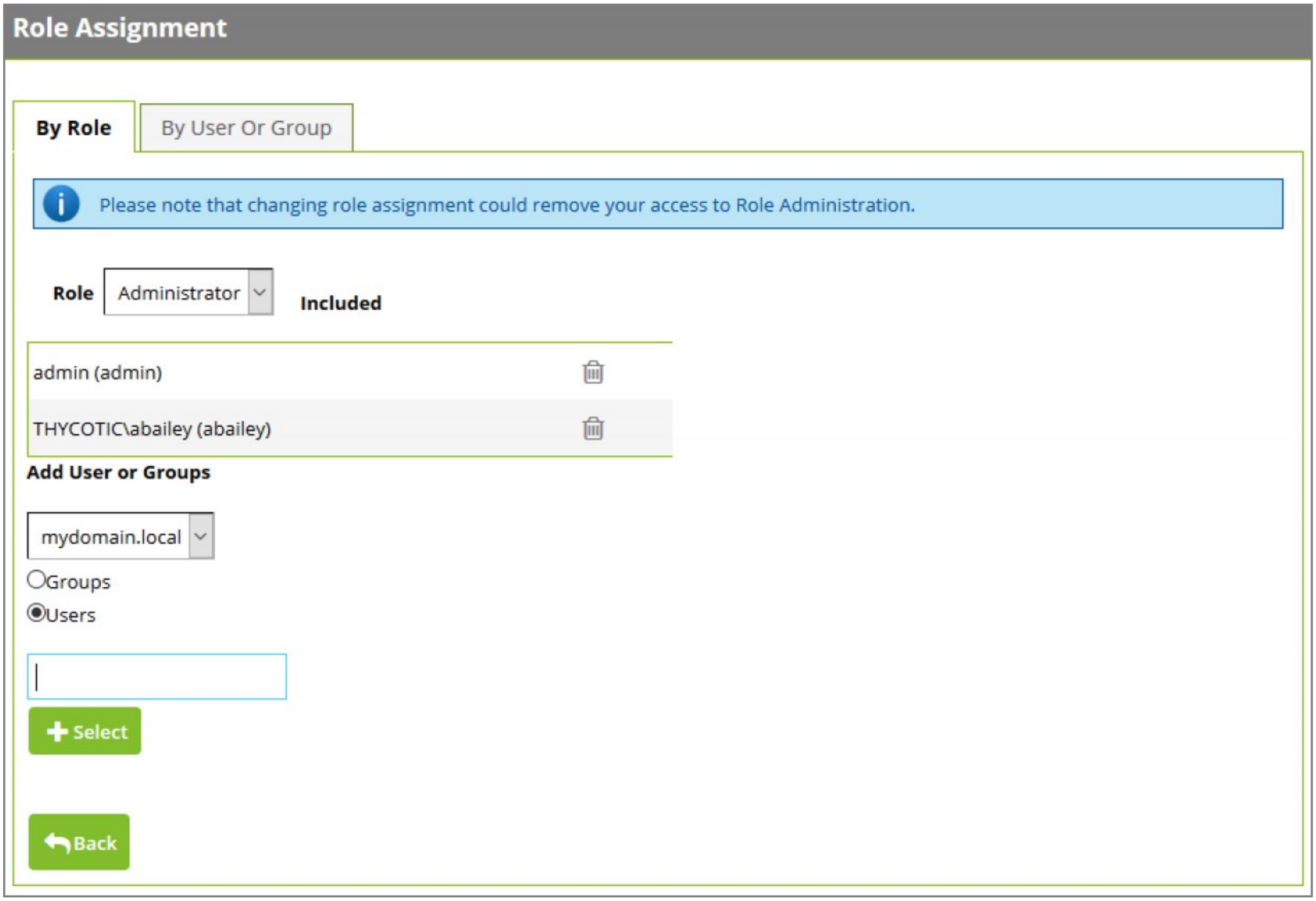
To edit a role, click the name of the role on the role overview screen. When editing a role, you can change the name, assign or un-assign permissions, or disable the role. A role cannot be deleted once created.

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. Click **Save Changes** when you are complete.



Role Assignment

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

Role: Administrator

Included

admin (admin)

THYCOTIC\abailey (abailey)

Add User or Groups

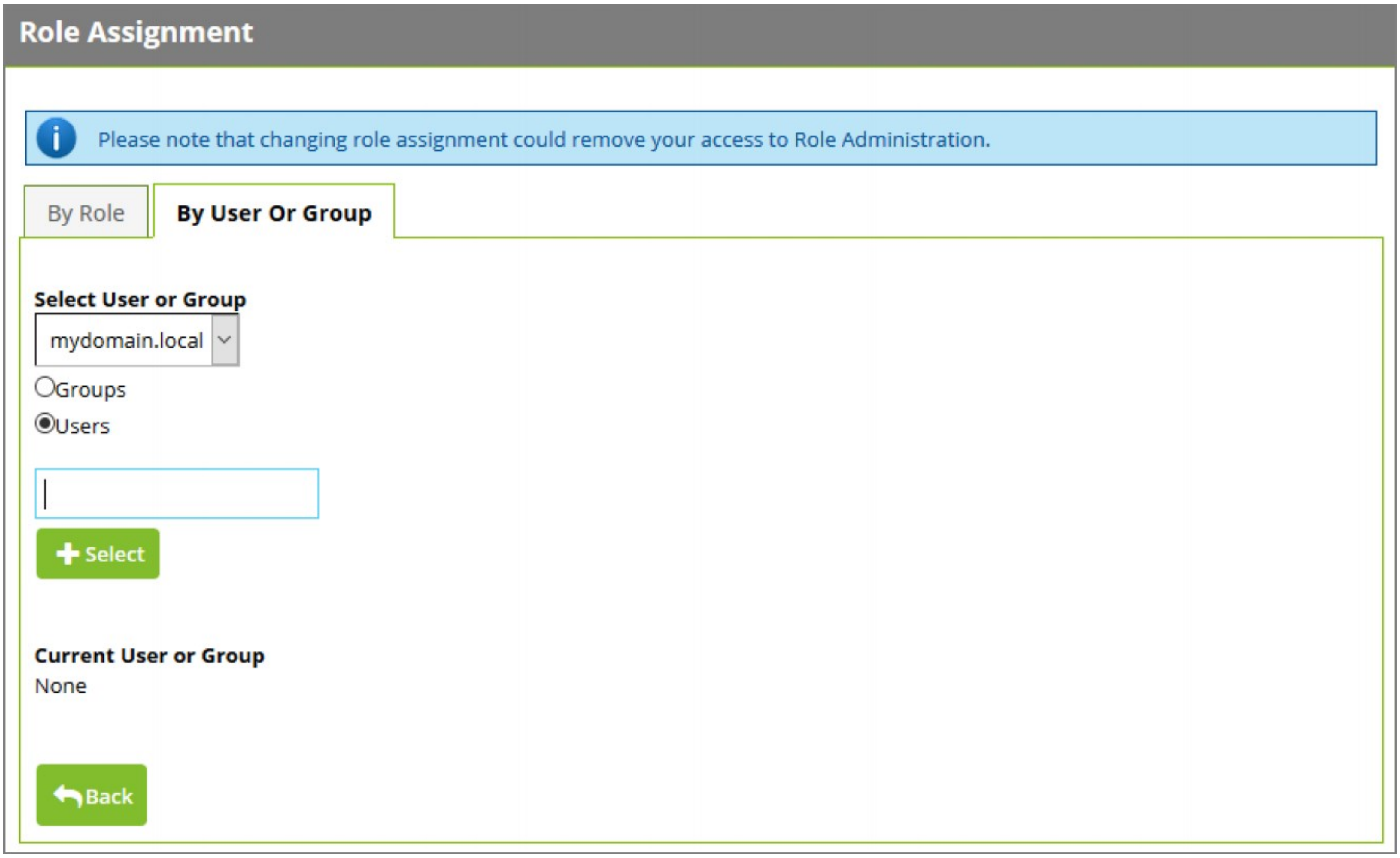
mydomain.local

○Groups

●Users

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. Click **Save Changes** when you are complete.


Role Assignment

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

Select User or Group

mydomain.local

○Groups

●Users

Current User or Group

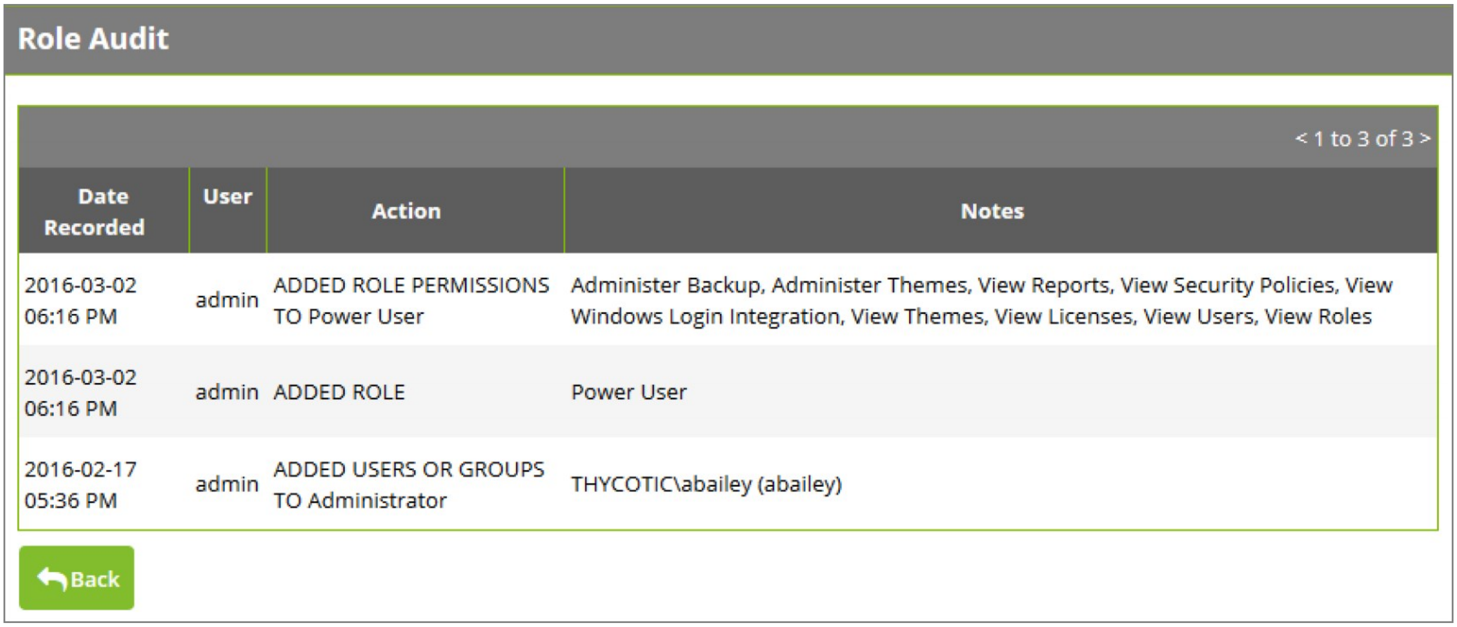
None

Role Auditing

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, such as renaming it, modifying its permissions, or assigning users to it, begin by clicking the **Administration** link on the top navigation bar and then clicking **Roles**, then the **View Audit** button. Action describes what was done and the **Notes** describe the details of the action.

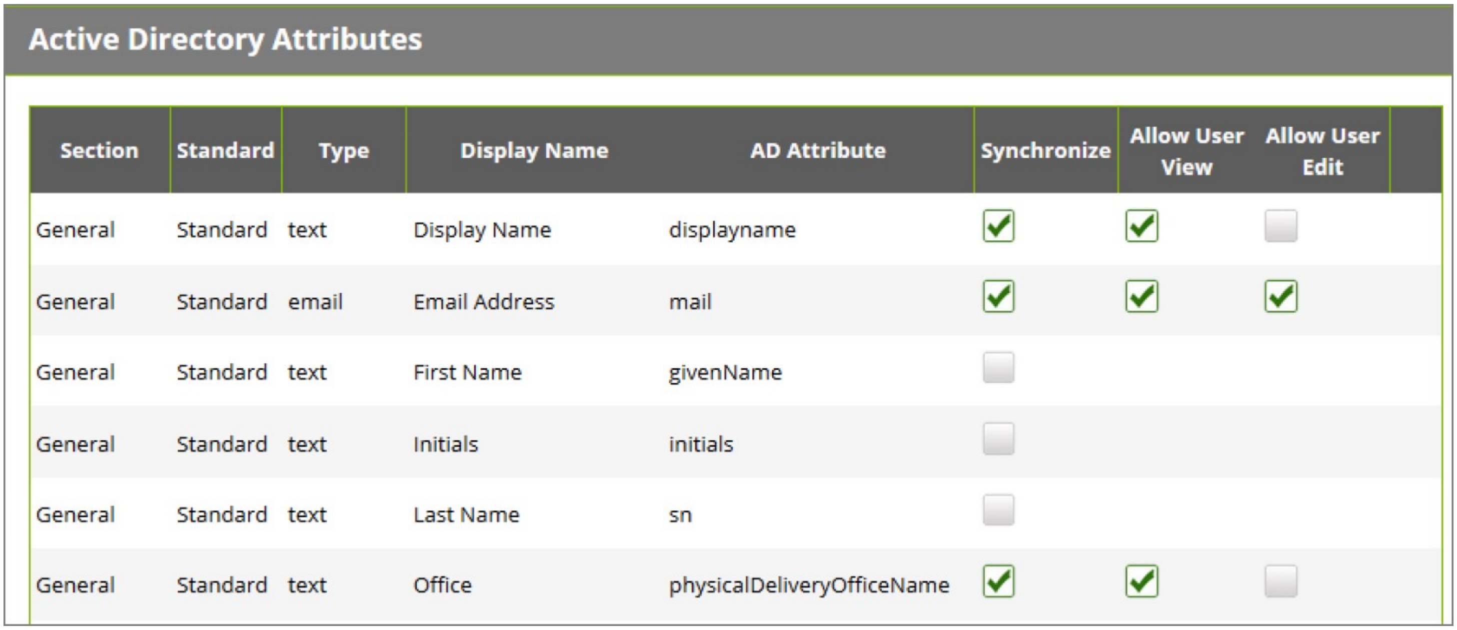


Role Audit

< 1 to 3 of 3 >

Date Recorded	User	Action	Notes
2016-03-02 06:16 PM	admin	ADDED ROLE PERMISSIONS TO Power User	Administer Backup, Administer Themes, View Reports, View Security Policies, View Windows Login Integration, View Themes, View Licenses, View Users, View Roles
2016-03-02 06:16 PM	admin	ADDED ROLE	Power User
2016-02-17 05:36 PM	admin	ADDED USERS OR GROUPS TO Administrator	THYCOTIC\abailey (abailey)

The Active Directory attributes settings allow Password Reset Server to synchronize additional information with Active Directory. By default, only display name and email address will be synced.



Active Directory Attributes

Section	Standard	Type	Display Name	AD Attribute	Synchronize	Allow User View	Allow User Edit	
General	Standard	text	Display Name	displayname	☑	☑	☐	
General	Standard	email	Email Address	mail	☑	☑	☑	
General	Standard	text	First Name	givenName	☐			
General	Standard	text	Initials	initials	☐			
General	Standard	text	Last Name	sn	☐			
General	Standard	text	Office	physicalDeliveryOfficeName	☑	☑	☐	

To modify these settings, navigate to **Administration > Active Directory Attributes**. There are three settings that can be enabled by checking the box in each of the following columns:

Synchronize

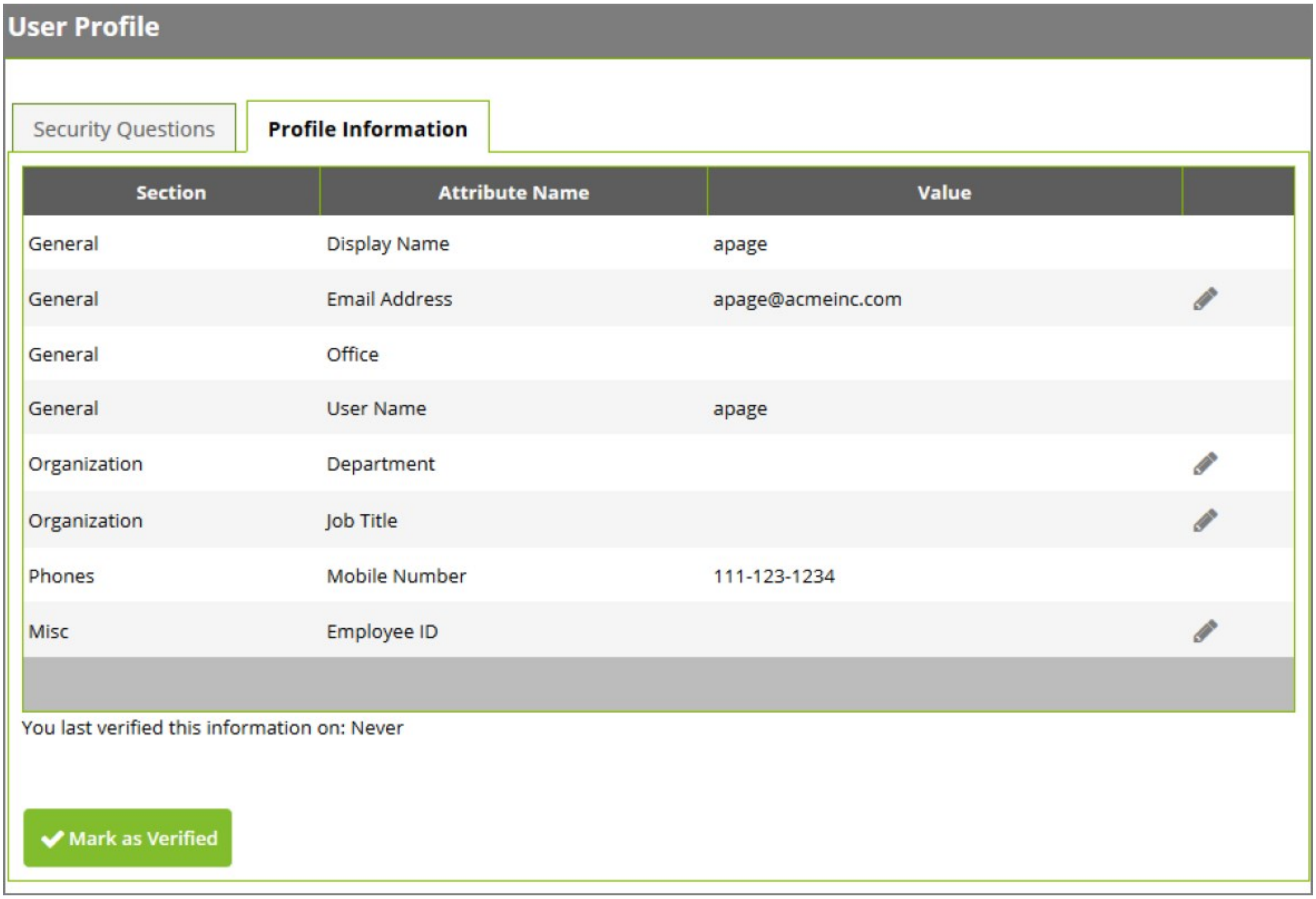
Synchronize an attribute from Active Directory. This value will be stored in the database after the next Active Directory sync.

Allow User View

Allow users to view the attribute value once they are logged into Password Reset Server under the **Profile Information** tab.

Allow User Edit

Allow users to update their attribute from Password Reset Server. When users log in and go to the Profile Information tab, they will see an “edit” icon at the end of the row for the attribute that they can click to change the value. Once the attribute is saved here, it will be immediately updated in Active Directory.



Section	Attribute Name	Value	
General	Display Name	apage	
General	Email Address	apage@acmeinc.com	✎
General	Office		
General	User Name	apage	
Organization	Department		✎
Organization	Job Title		✎
Phones	Mobile Number	111-123-1234	
Misc	Employee ID		✎

You last verified this information on: Never

If **Allow User View** is enabled, users will be able to verify that their information is correct by clicking **Mark as Verified** under the **Profile Information** tab when they log into PRS as a non-admin. This marks an audit in the database for internal purposes (see figure on the following page).

For environments that include additional or custom Active Directory attributes, Password Reset Server supports defining custom attributes to be synchronized. To add a custom attribute, select **Active Directory Attributes** from the **Administration** menu and then select the attribute type in the drop-down menu in the last row of the **Type** column. There are three options:

Text

An attribute that contains a text-based value. This type of attribute will be made available as an answer for any text-based question.

Phone

An attribute that will be formatted as a phone number. Phone type attributes are made available as answers for multifactor Phone and SMS questions.

Email

An attribute that will be formatted as an email address. Email type attributes are made available as answers for multifactor Email questions. In the **Display Name** field, fill in the name that you would like to reference the attribute by in Password Reset Server when configuring the attribute as an answer source. The **AD Attribute** column must include the name by which the attribute is referenced in Active Directory.

Client Password Validation

For Password Reset Server users, password requirements are typically managed by Active Directory Group Policy. If the password the user enters does not comply with the AD Group Policy, the user receives a general error and the reset request is not sent. Custom Client Password Validation allows administrators to set password requirements beyond what AD Group Policy can enforce.

Implementation

Custom Password Validation is implemented using an app setting, so you must log into the IIS host server and navigate to the installation directory, which is typically **C:\inetpub\wwwroot\PasswordResetServer**. Open the file named **web-appSettings.config** to add the **ClientPasswordValidation** key with regex statements like those below:

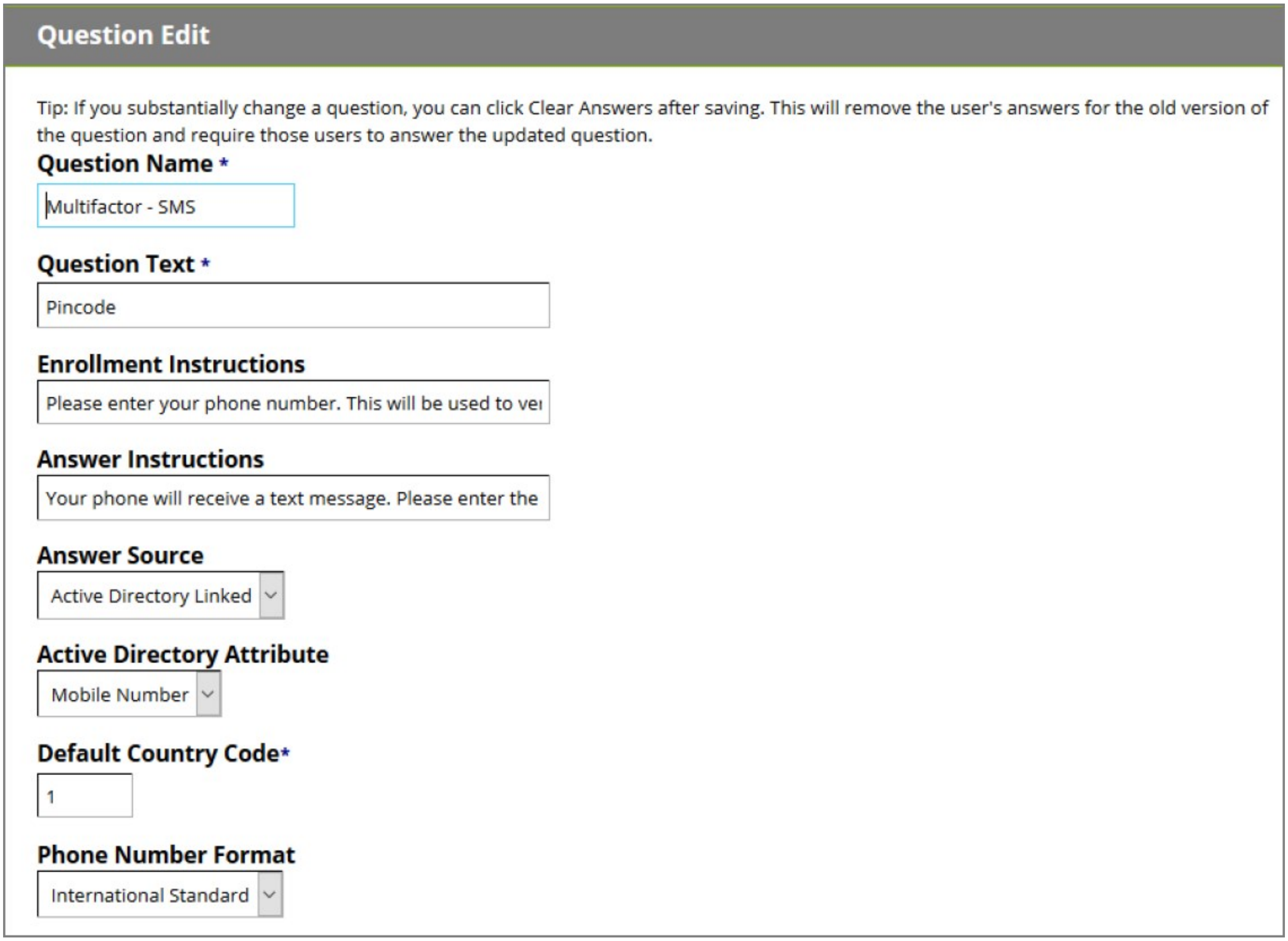
```
<?xml version="1.0" encoding="utf-8" ?>
  <appSettings>
    <add key="ChartImageHandler" value="Storage=memory;Timeout=10;Url=~/tempimages/;"/>
    <add key="ShouldValidateResetCredentials" value="True"/>
    <add key="IsDebugLoggingEnabled" value="False"/>
    <add key="UserErrorPage" value="~/CustomError.aspx"/>
    <add key="ClientPasswordValidation" value="{
       &quot;Please use at least one digit&quot; : &quot;\\d&quot;,
       &quot;Please use at least one letter&quot; : &quot;[a-zA-Z]&quot;,
       &quot;Please use at least one symbol&quot; : &quot;[!@#$%^&*]&quot;,
       &quot;Please use at least ten characters&quot; :  &quot;(\\w){10,}&quot;,
       &quot;Please use no repeating characters&quot; : &quot;^(?!.*(\\w).*\\1).+$&quot;}"

/>
```

Active Directory attributes that are synchronized with Password Reset Server can be used as answers for text-based and multifactor questions.

Specify an Attribute

To assign an attribute as an answer to a question, navigate to **Administration > Security Questions** and create a new question or click a question to modify it. Click the drop-down menu for **Answer Source** and select **Active Directory Linked**. Another drop-down menu will then appear – select the Active Directory attribute you would like to reference for the answer. Click **Save**.



Question Edit

Tip: If you substantially change a question, you can click Clear Answers after saving. This will remove the user's answers for the old version of the question and require those users to answer the updated question.

Question Name *: Multifactor - SMS

Question Text *: Pincode

Enrollment Instructions: Please enter your phone number. This will be used to vei

Answer Instructions: Your phone will receive a text message. Please enter the

Answer Source: Active Directory Linked

Active Directory Attribute: Mobile Number

Default Country Code*: 1

Phone Number Format: International Standard

Multifactor Phone and SMS Questions

In the case of multifactor Phone or SMS questions, several additional configuration options will also appear. Enter the country code for the phone number – this will only be used if it is not included in the attribute value.

If the phone number is in an International Standard format, choose this option for the **Phone Number Format** setting. Otherwise, you will need to select the **Custom** option and specify the **Regex** to be used to read the number from the attribute.

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 **Explain**.

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 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.

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.

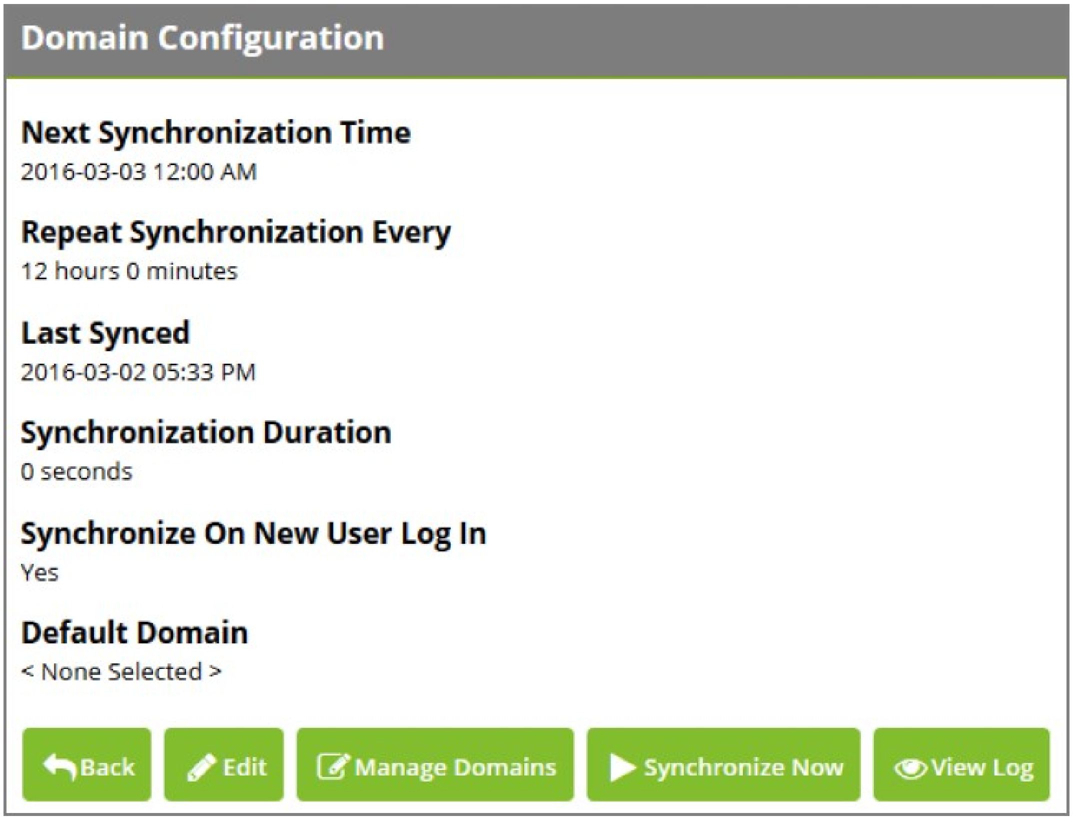
Password Reset Server supports automatic database and IIS directory backups.

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.

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.

To administer domains, click **Administration** on the top navigation bar, then click **Domain Configuration**.



Domain Configuration

Next Synchronization Time
2016-03-03 12:00 AM

Repeat Synchronization Every
12 hours 0 minutes

Last Synced
2016-03-02 05:33 PM

Synchronization Duration
0 seconds

Synchronize On New User Log In
Yes

Default Domain
< None Selected >

The **Next Synchronization Time** can be set manually to choose when Password Reset Server will synchronize with Active Directory. The **Repeat Synchronization Every** setting determines how long Password Reset Server will wait after the next synchronization is complete before starting another sync. Last Synced indicates the last time Password Reset Server finished synchronizing with Active Directory. Synchronization Duration shows the time it took to complete the last synchronization to give an idea of how long the next synchronization might take.

Synchronize on New User Login

Synchronize on New User Log In will cause Password Reset Server to automatically synchronize if a user logs in who has been added to Active Directory since the last synchronization. This setting is enabled by default. With this option enabled, when a new user tries to log in they will receive a message to wait while synchronization is occurring. After synchronization is complete, they will be taken back to the login page and prompted to log in again.

If this option is disabled Password Reset Server will then only sync when you kick off a sync manually or when it is scheduled. With this option disabled, when a new user attempts to log in they will receive a message like the following:

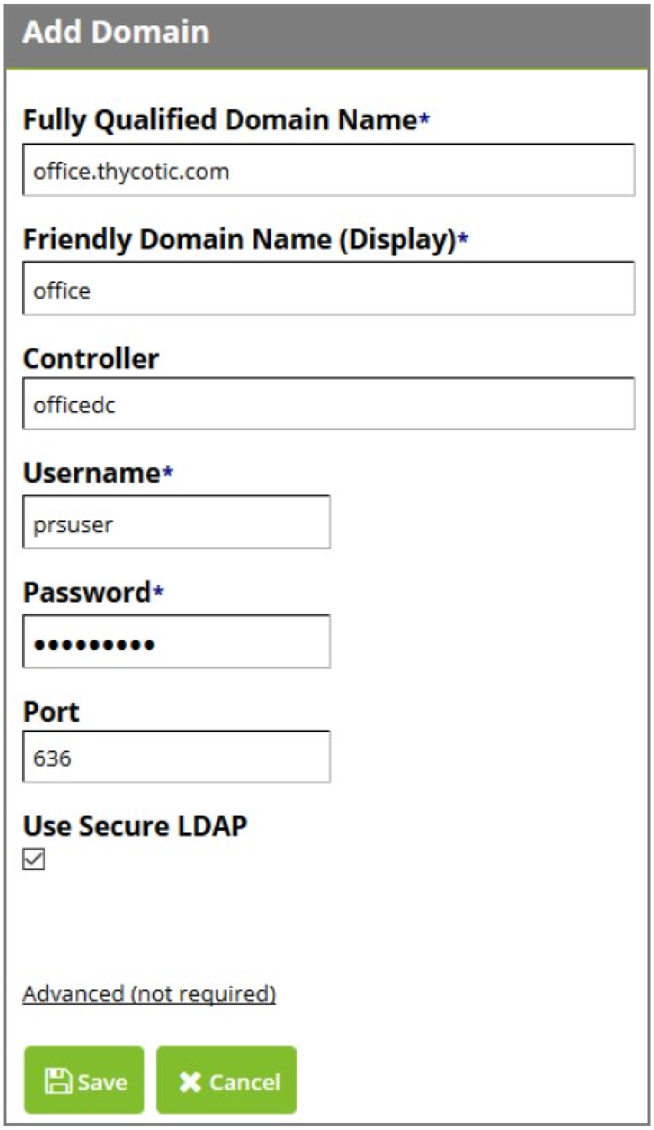
"The system will need to synchronize this user before logging in. Please try again after the next domain synchronization at 2015-07-08 01:00 AM."

This configuration option replaces what was previously the **PreventSyncForNewUser** key that could be added to the web-appSettings.config file. If you have already added this setting, it will take priority and the option on the **Domain Configuration** page will be disabled. Remove this setting from webappSettings.config to control it from the **Domain Configuration** page.

Default Domain

Default Domain allows you to specify which domain will appear on the Login, Change Password, and Reset Password pages by default the first time a user accesses any of these pages.

To add a domain, click **Add** from the domain management page.



Add Domain

Fully Qualified Domain Name*: office.thycotic.com

Friendly Domain Name (Display)*: office

Controller: officedc

Username*: prsuser

Password*: ••••••••••

Port: 636

Use Secure LDAP: ☑

Enter the **Fully Qualified Domain Name** (FQDN) along with the username and password of the domain user. If there is a domain controller you'd like to use, specify it in the **Controller** field. To use Secure LDAP, select the **Use Secure LDAP** check box. If using a non-standard port, change the port. Normally the port is 389 for LDAP or 636 for LDAPS.

Under **Advanced (not required)**, you can choose which LDAP layer you'd like to use – Pure or Negotiated. You may choose to specify a search base DN if you don't want to use the default one (the entire domain). Finish by clicking **Save**.

Editing Domains

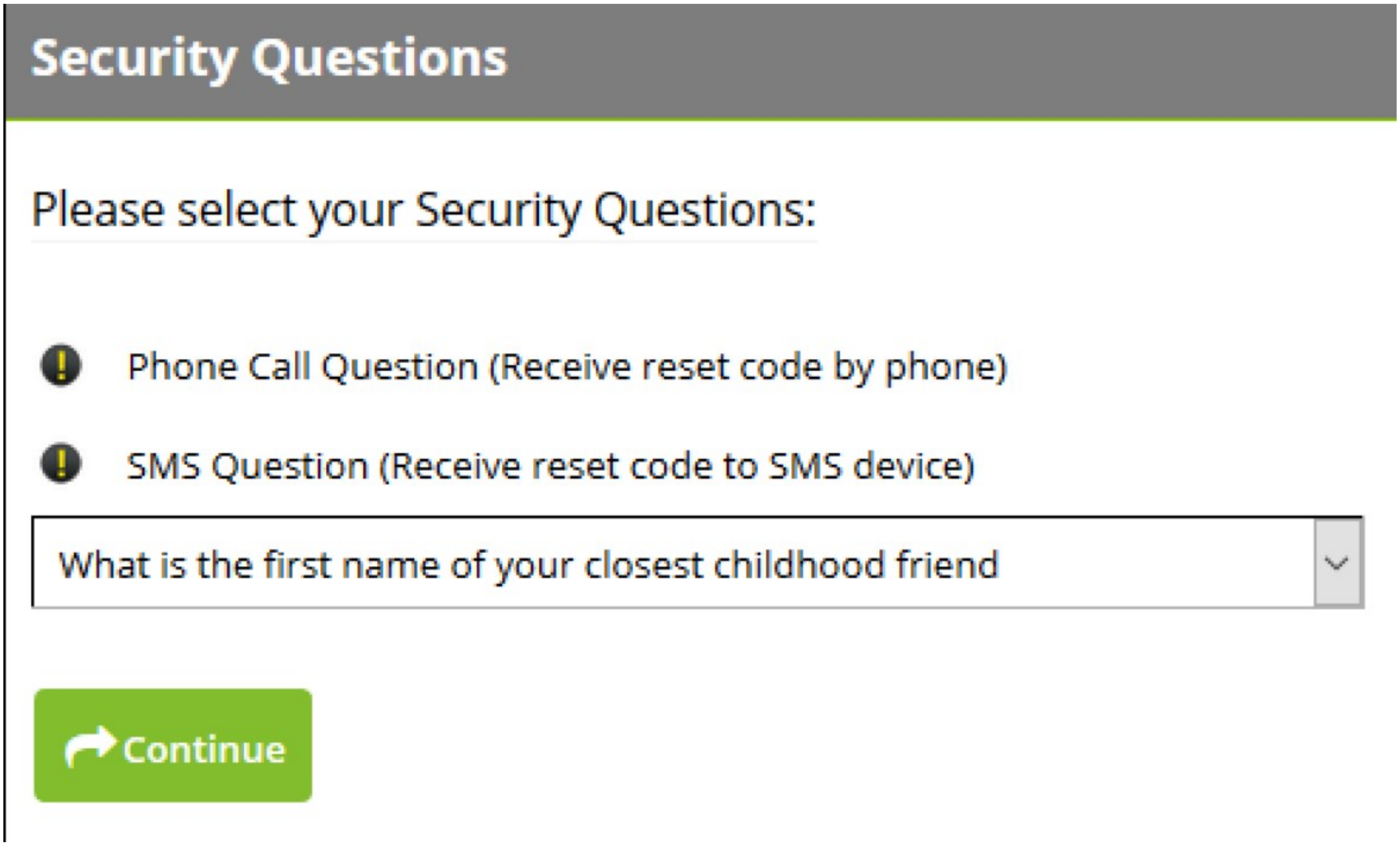
To edit or deactivate a domain, click the domain name in the domain overview and make the desired edits, and click **Save**.

Before a user can use Password Reset Server to reset their password, they must complete the enrollment process. A user logging into Password Reset Server whose Active Directory account has been marked “User must change password at next logon” will be taken to the **Change Password** page before they are able to enroll.

> **Note**: If the user was added to Active Directory, but Password Reset Server has not yet synced with Active Directory, Password Reset Server will initiate a sync to attempt to find the new user when they attempt to enroll. This setting can be disabled, if desired, via the **Synchronize on New User Login** setting on the **Domain Configuration** page.

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.

When a user clicks **Enroll**, they will first be asked to select be the questions they would like to answer from their security policy.



Security Questions

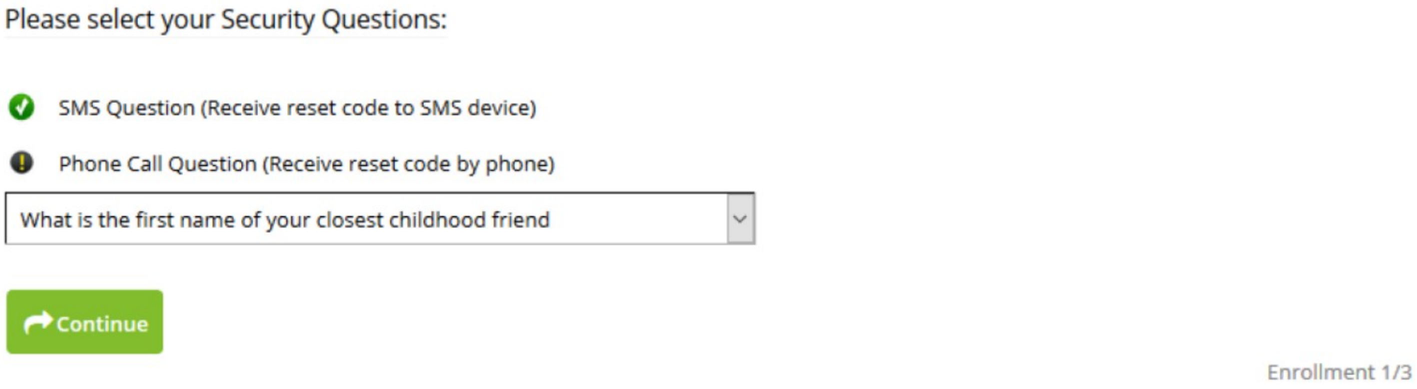
Please select your Security Questions:

! Phone Call Question (Receive reset code by phone)

! SMS Question (Receive reset code to SMS device)

What is the first name of your closest childhood friend

Questions using Active Directory attributes will display a icon next to the question title to indicate that the answer to the question is synced from Active Directory. The user will not be asked to answer the question during enrollment, however they will be required to answer it during a test run.



Please select your Security Questions:

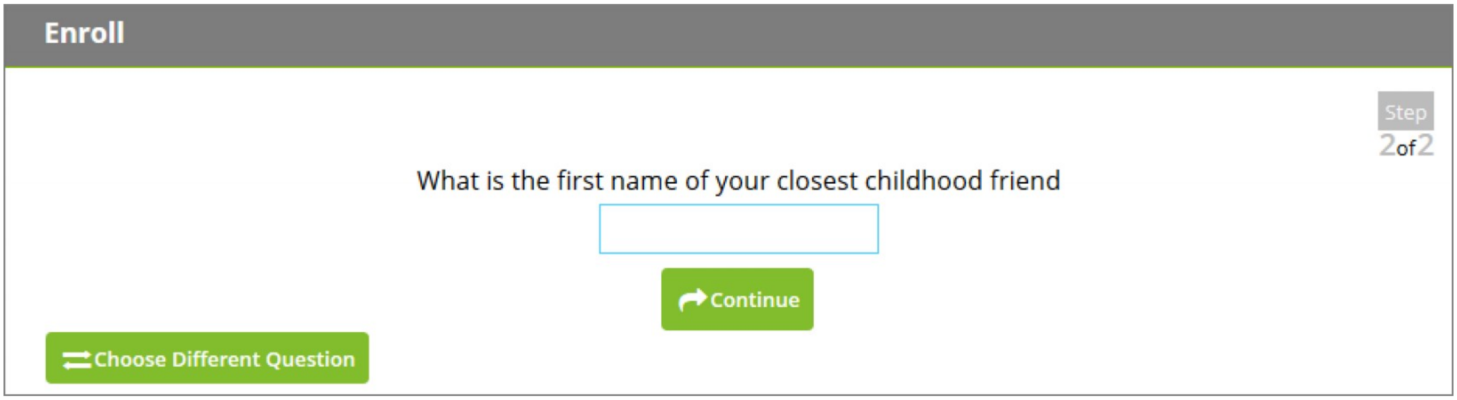
✓ SMS Question (Receive reset code to SMS device)

! Phone Call Question (Receive reset code by phone)

What is the first name of your closest childhood friend

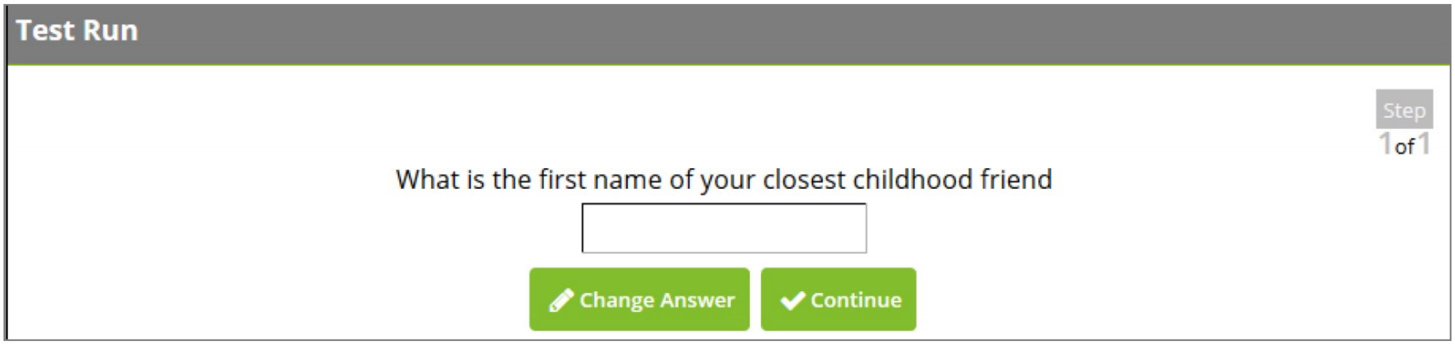
Enrollment 1/3

After choosing their security questions, the user will be asked each question in turn. To modify their selection of questions during the enrollment process, a user can click Choose Different Question.



What is the first name of your closest childhood friend

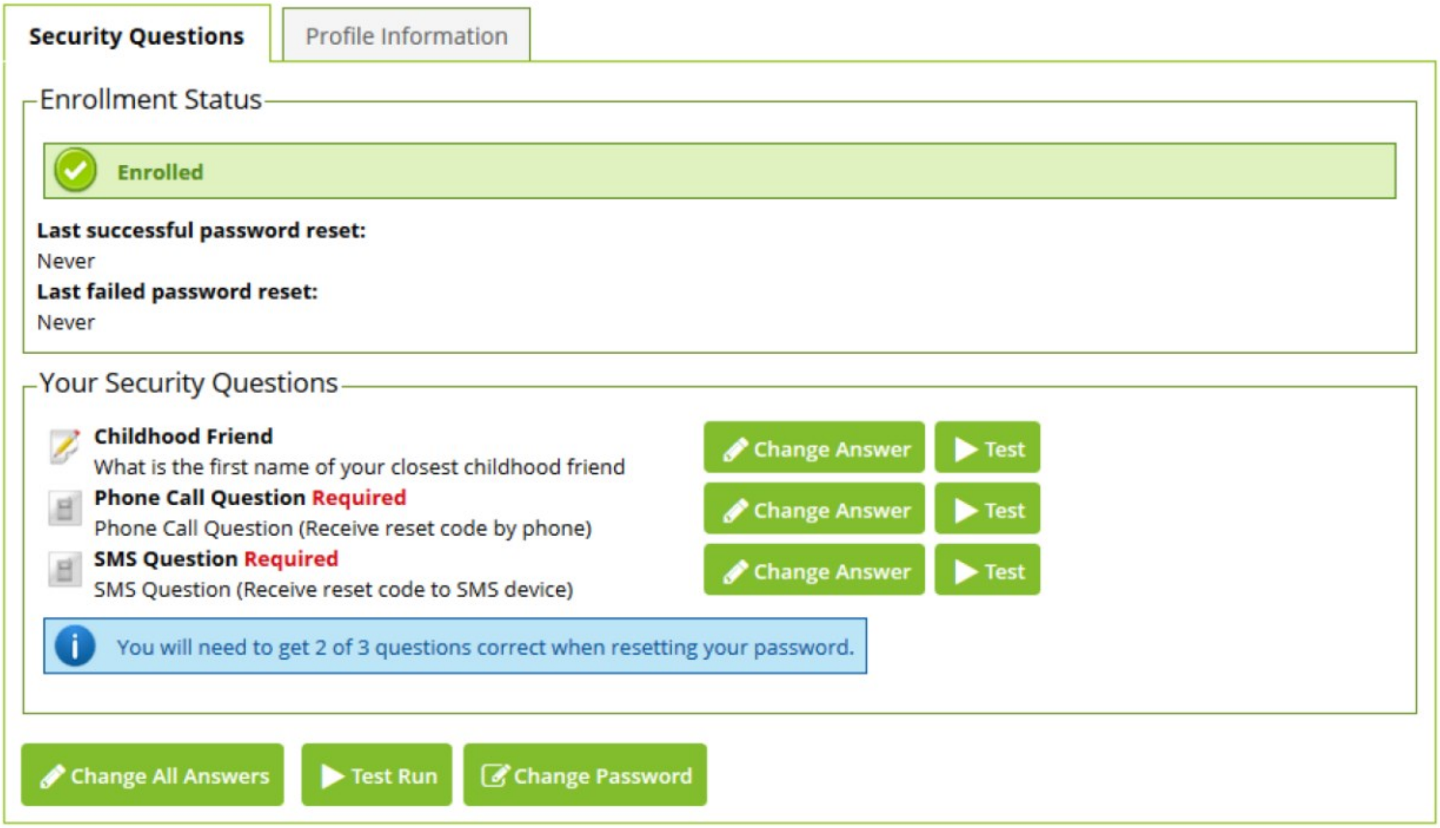
If a test run is required by the security policy, the user will next be required to answer all of their security questions a second time.



What is the first name of your closest childhood friend

Once their enrollment is complete, the user is directed to their home screen.

A user can return to this screen at any time by opening a browser and clicking **Enroll** to log into Password Reset Server with their current credentials. They can then 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.



Enrollment Status

✓ Enrolled

Last successful password reset:
Never
Last failed password reset:
Never

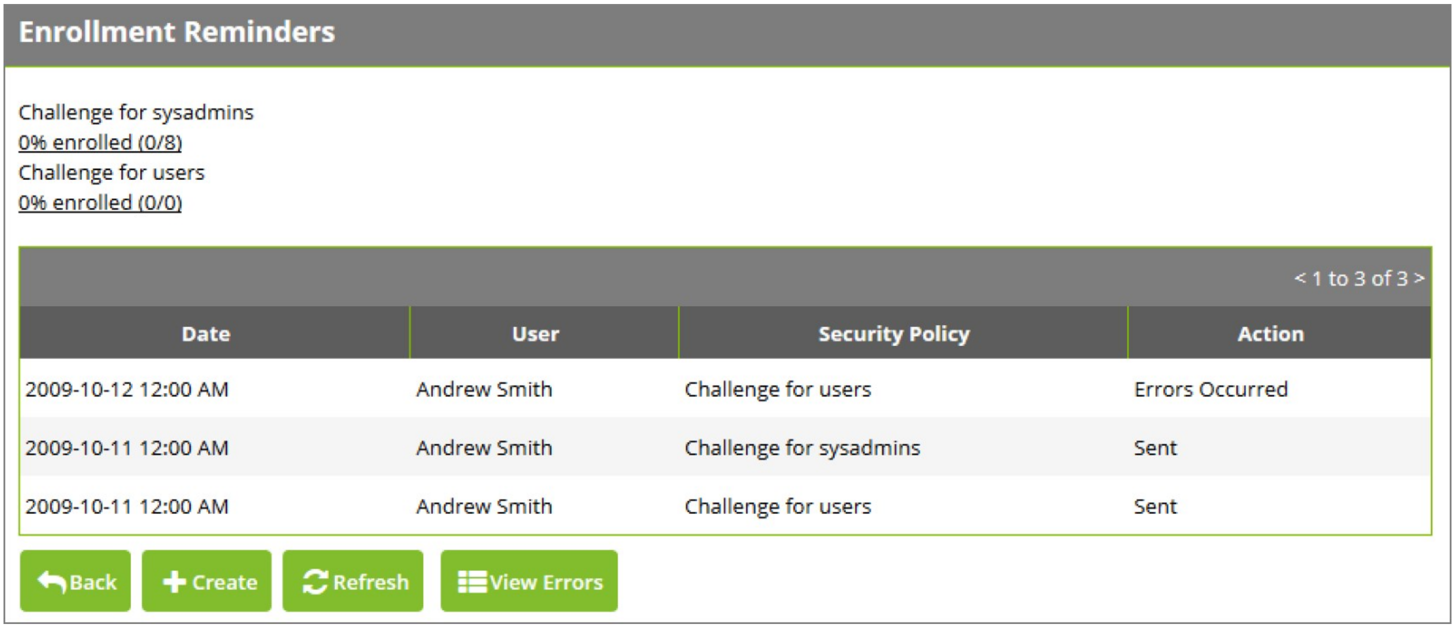
Your Security Questions

Childhood Friend
What is the first name of your closest childhood friend
Phone Call Question Required
Phone Call Question (Receive reset code by phone)
SMS Question Required
SMS Question (Receive reset code to SMS device)

You will need to get 2 of 3 questions correct when resetting your password.

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.

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.



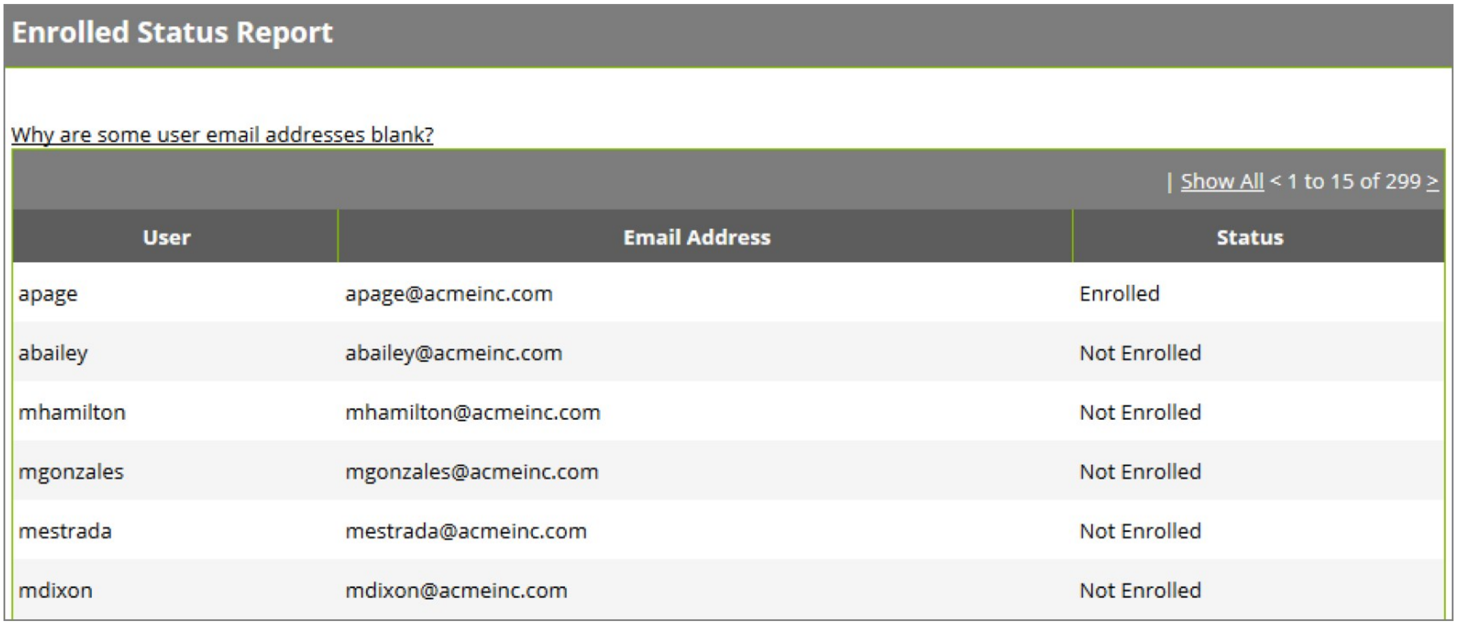
Enrollment Reminders

Challenge for sysadmins
0% enrolled (0/8)
Challenge for users
0% enrolled (0/0)

< 1 to 3 of 3 >

Date	User	Security Policy	Action
2009-10-12 12:00 AM	Andrew Smith	Challenge for users	Errors Occurred
2009-10-11 12:00 AM	Andrew Smith	Challenge for sysadmins	Sent
2009-10-11 12:00 AM	Andrew Smith	Challenge for users	Sent

Click **View Errors** to view the errors that have occurred while sending out the reminders. Click Refresh to **refresh** the grid.



Enrolled Status Report

Why are some user email addresses blank?

| Show All < 1 to 15 of 299 >

User	Email Address	Status
apage	apage@acmeinc.com	Enrolled
abailey	abailey@acmeinc.com	Not Enrolled
mhamilton	mhamilton@acmeinc.com	Not Enrolled
mgonzales	mgonzales@acmeinc.com	Not Enrolled
mestrada	mestrada@acmeinc.com	Not Enrolled
mdixon	mdixon@acmeinc.com	Not Enrolled

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.

Creating a New Reminder

To create a new reminder, click **Create** on the **Enrollment Reminders** screen.

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. The following options are available:

Subject

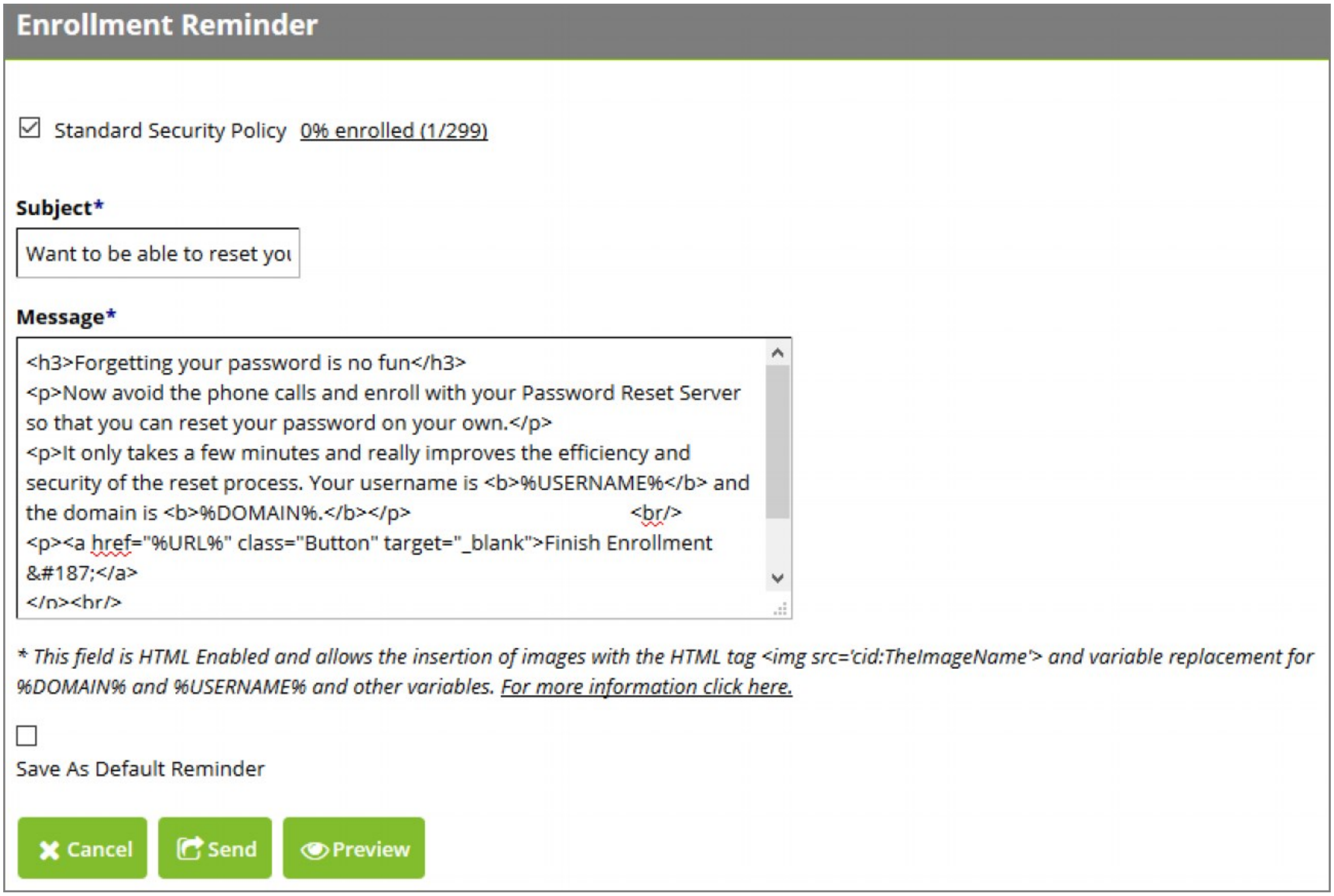
The subject of the email that users in the security policies will receive.

Message

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.



Enrollment Reminder

☑ Standard Security Policy 0% enrolled (1/299)

Subject*

Want to be able to reset you

Message*

```
<h3>Forgetting your password is no fun</h3>
<p>Now avoid the phone calls and enroll with your Password Reset Server
so that you can reset your password on your own.</p>
<p>It only takes a few minutes and really improves the efficiency and
security of the reset process. Your username is <b>%USERNAME%</b> and
the domain is <b>%DOMAIN%.</b></p>                    <br/>
<p><a href="%URL%" class="Button" target="_blank">Finish Enrollment
&#187;</a>
</p><br/>
```

* This field is HTML Enabled and allows the insertion of images with the HTML tag <img src='cid:TheImageName'> and variable replacement for %DOMAIN% and %USERNAME% and other variables. For more information click here.

□ Save As Default Reminder

Password Reset Server's configuration can be accessed by logging in as an administrator, clicking **Administration** in the top navigation bar, then selecting **Configuration**.

The following settings are available:

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 Password Reset Server.

Windows Client Language

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

Force HTTP/SSL

When this setting is on, requests coming in to Password Reset Server using HTTP will be redirected to use HTTPS.

Enable Email Sign In

When this setting is on, users will be able to log into Password Reset Server using their email addresses instead of their Active Directory usernames.

Enable Domain Selector Login

This setting determines what users see when they login or try to do a password reset.

- **Show Domain Drop Down:** Users see a drop down with all domains listed. This is the default behavior.
- **Show Domain Label:** Users see a label with the default domain.
- **Hide Domain Info:** Completely hides all domain info.

If the domain drop down is not used, the domain used will be the user's last used domain. If they are logging in for the first time it will be the default domain as specified under **Administration | Domain Configuration**. Users can specify a different domain than the default by using their UPN, email, or by specifying their username as DOMAIN\Username. To login as the local admin, use LOCAL\username or .\username.

URL for User Help Link

Set a custom help link in the Password Reset Server footer for end users to take them to an internal custom page describing your organization's password reset policies and procedures.

Email for User Error Submission

Set a custom email address for users to submit any exceptions they run into. This should be the IT owners of Password Reset Server so end user issues can be addressed.

Password Reset Server can log to a CEF or Syslog listener. When this is configured, all important system log entries are sent to the CEF or Syslog server entered in the configuration. The written events contain data such as user information, time, IP Address, and any other important details about the event.

When in **Administration > Configuration**, click the **Edit** button and select the **Enable Syslog/CEF Logging** check box. When you do this, three additional settings will appear:

Syslog/CEF Server

IP address or name of the server.

Syslog/CEF Port

Port that the events will be sent to the server on.

Syslog/CEF Protocol

Either UDP or TCP, the protocol used by your server.

Once you have entered these values, click **Save**. After enabling CEF, your server should start to receive messages right away if you entered the data correctly. In order to force an event to happen, perform a log out and then log back in. If the event does not appear on your CEF server soon after, there is something wrong with your configuration.

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

The following settings are available:

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” address 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.

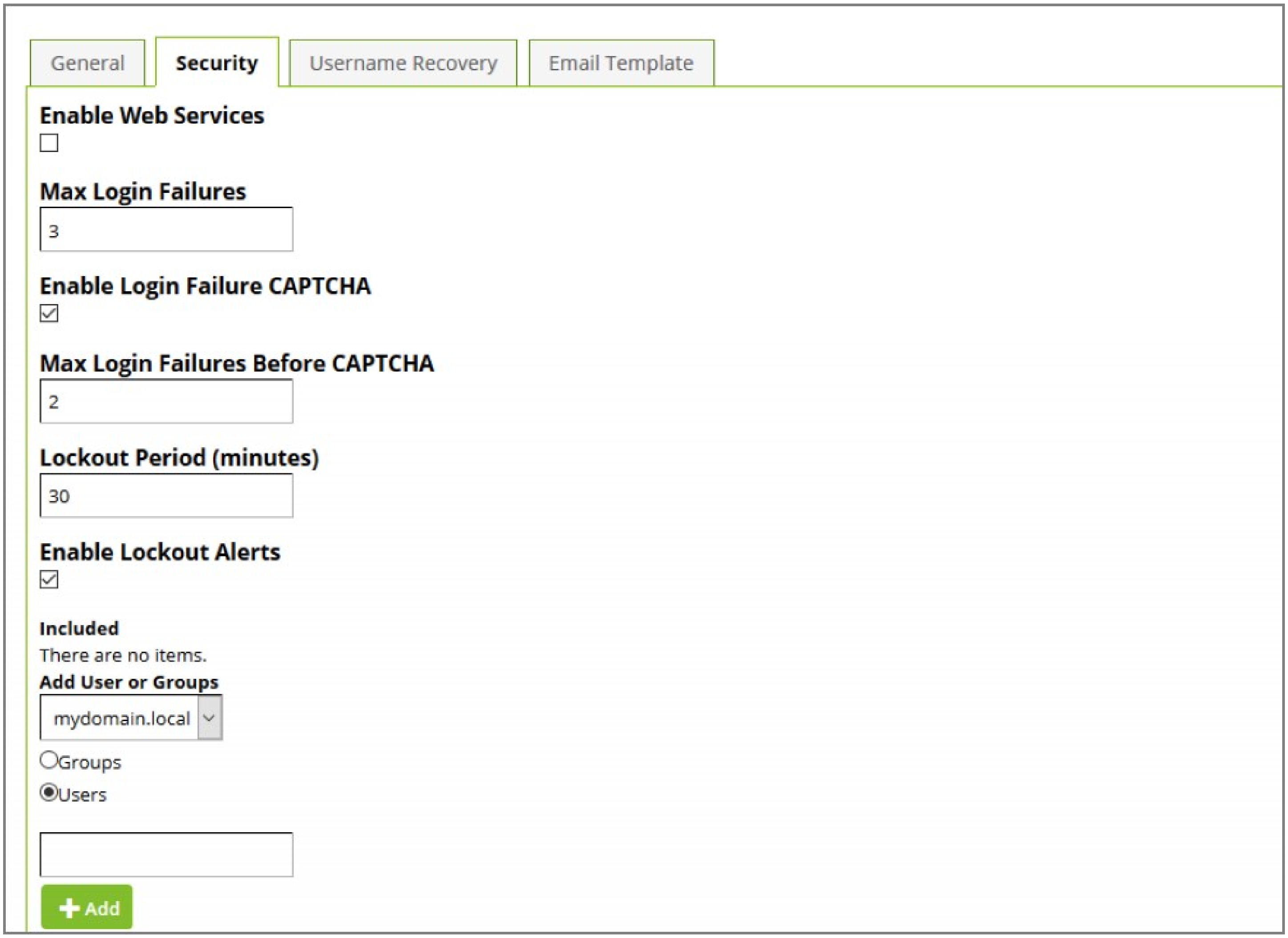
The following settings are available:

Enable Web Services

This will determine if web services can be used or not.

Max Login Failures

After providing an incorrect password this many times, the user's account will be locked out in Password Reset Server and they must then either reset their password or wait for the Lockout Period (listed below) to pass before they can attempt to log in again.



Enable Web Services
□

Max Login Failures
3

Enable Login Failure CAPTCHA
☑

Max Login Failures Before CAPTCHA
2

Lockout Period (minutes)
30

Enable Lockout Alerts
☑

Included
There are no items.
Add User or Groups
mydomain.local
○Groups
●Users

Enable Login Failure CAPTCHA When enabled, users will have to complete a CAPTCHA challenge in addition to providing the correct password when logging in after providing an incorrect password a certain number of times specified below. For added security, if this setting is enabled and there are 5 login failures from the same IP address in a one hour period, Password Reset Server will always require a CAPTCHA when the user attempts to log in.

Max Login Failures Before CAPTCHA When Enable Login Failure CAPTCHA is enabled, this setting specifies how many times a user can provide the incorrect password before a CAPTCHA must be completed on subsequent login attempts. This amount must be lower than Max

Login Failures.

Lockout Period (minutes)

This is the number of minutes a user must wait to log in if their account has been locked out as a result of exceeding the Max Login Failures value. This number must be an interval of 15.

Enable Lockout Alerts If enabled, specified users and groups will receive an email whenever a user's account is locked out of Password Reset Server.

The following settings are available:

Allow Username Recovery

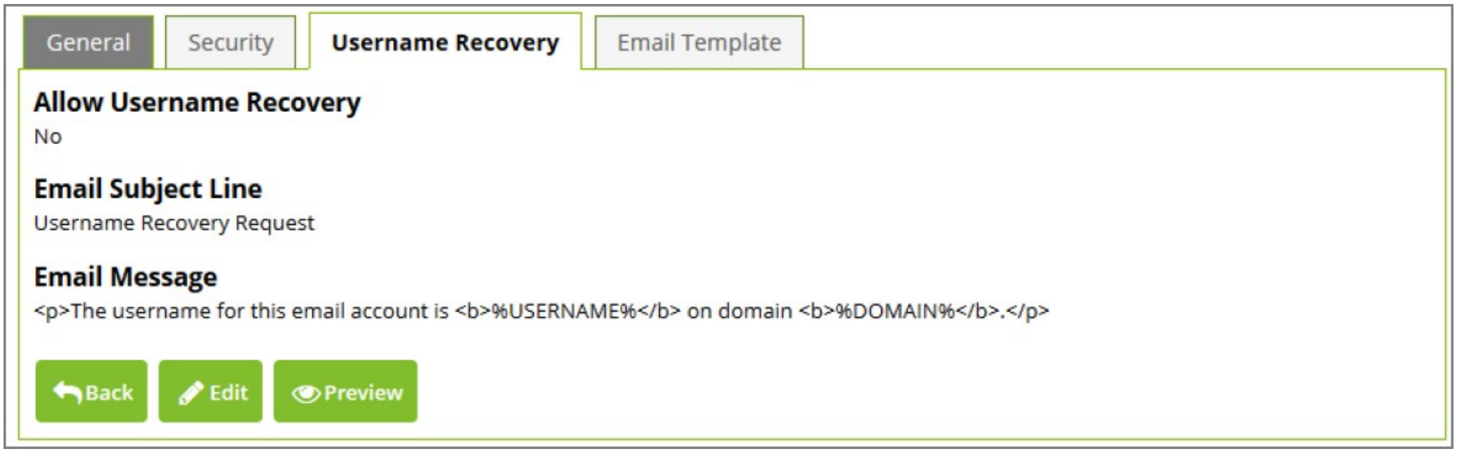
When this setting is on, there will be a link on the reset password page that takes users to a page where they can enter their email address and recover their username by email.

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 html and macro variables %USERNAME%, and %DOMAIN% which will be replaced with the actual values for the user.



Allow Username Recovery
No

Email Subject Line
Username Recovery Request

Email Message
<p>The username for this email account is <b>%USERNAME%</b> on domain <b>%DOMAIN%</b>.</p>

TeleSign is a service that Password Reset Server uses when making phone calls for Phone and SMSQuestions. 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**.

> **Note**: Testing the functionality will result in TeleSign charging your account.

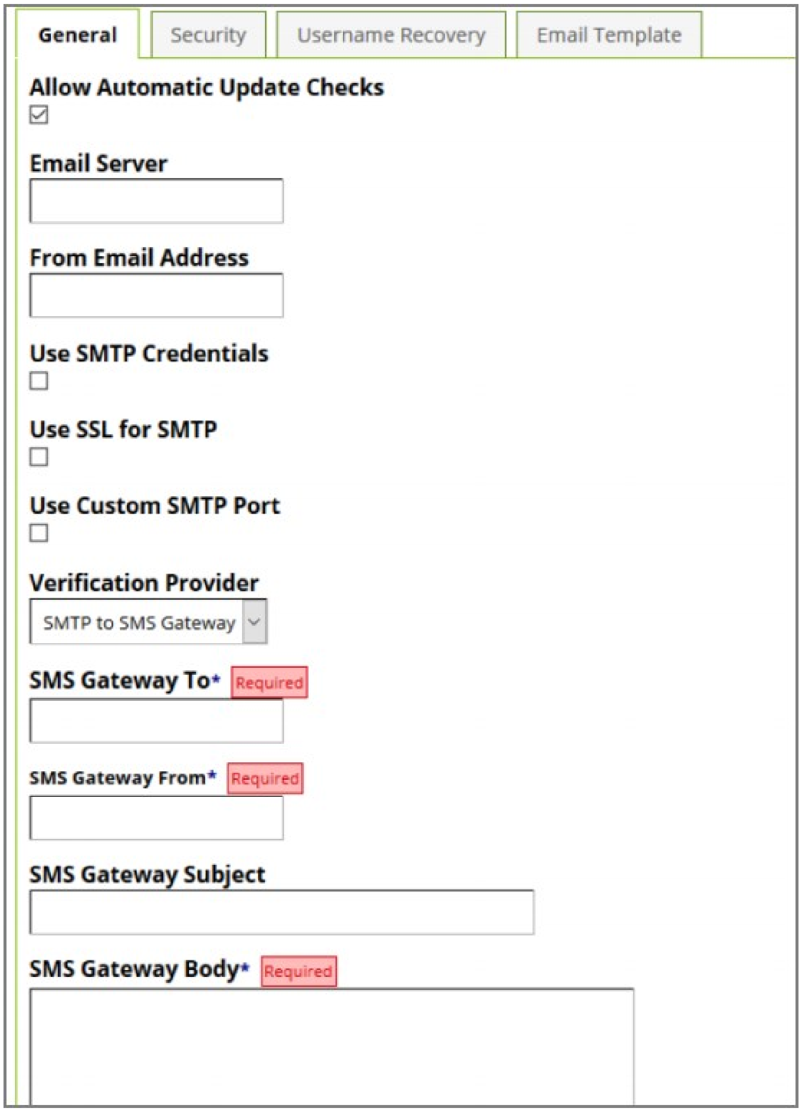
ProxStop is a service that Password Reset Server uses when making phone calls for Phone and SMS Questions. For more information on ProxStop and their services, please visit their website.

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**.

> **Note:** Testing the functionality will result in ProxStop charging your account.

SMTP to SMS Gateway allows for sending SMTP to SMS messages for the purpose of multifactor verification.



Allow Automatic Update Checks
☑

Email Server

From Email Address

Use SMTP Credentials
☐

Use SSL for SMTP
☐

Use Custom SMTP Port
☐

Verification Provider
SMTP to SMS Gateway

SMS Gateway To* Required

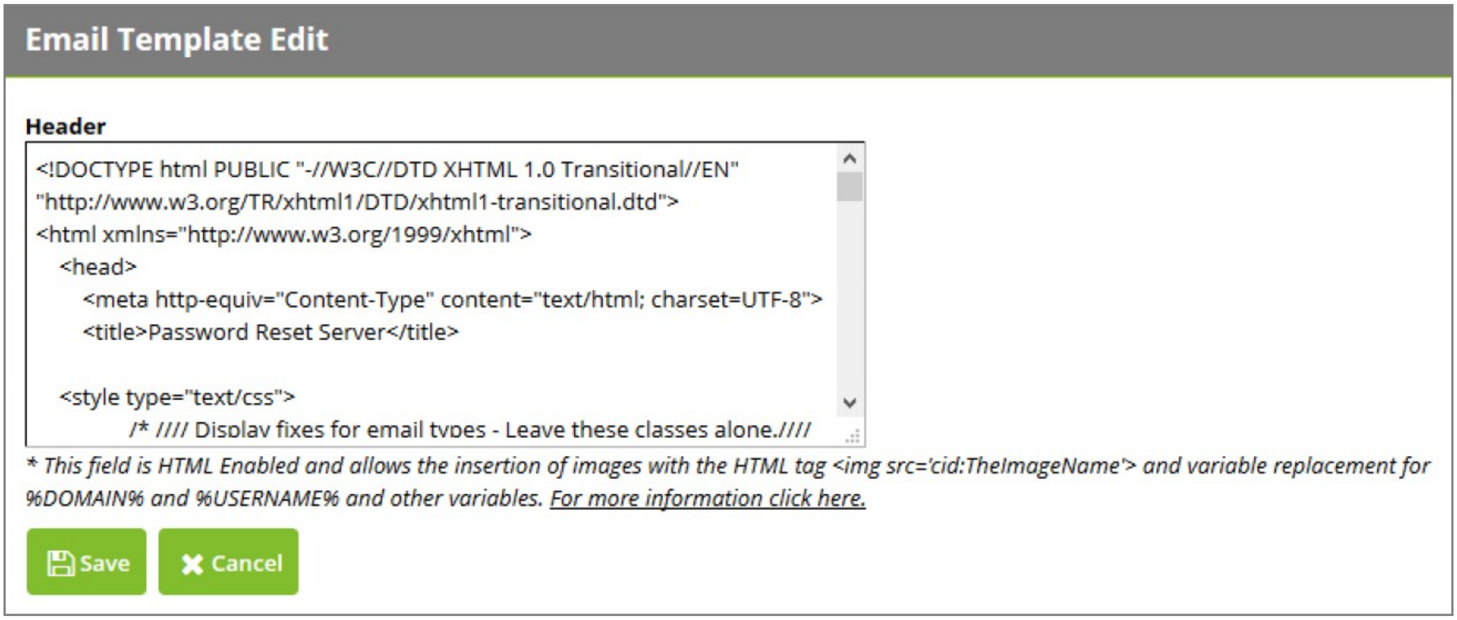
SMS Gateway From* Required

SMS Gateway Subject

SMS Gateway Body* Required

The Email Template tab under Administration > Configuration allows you to customize the header, footer, and logo used for email notifications such as enrollment reminders.

To modify the html for the header or footer, click the “edit” icon at the end of the corresponding row in the grid.



Email Template Edit

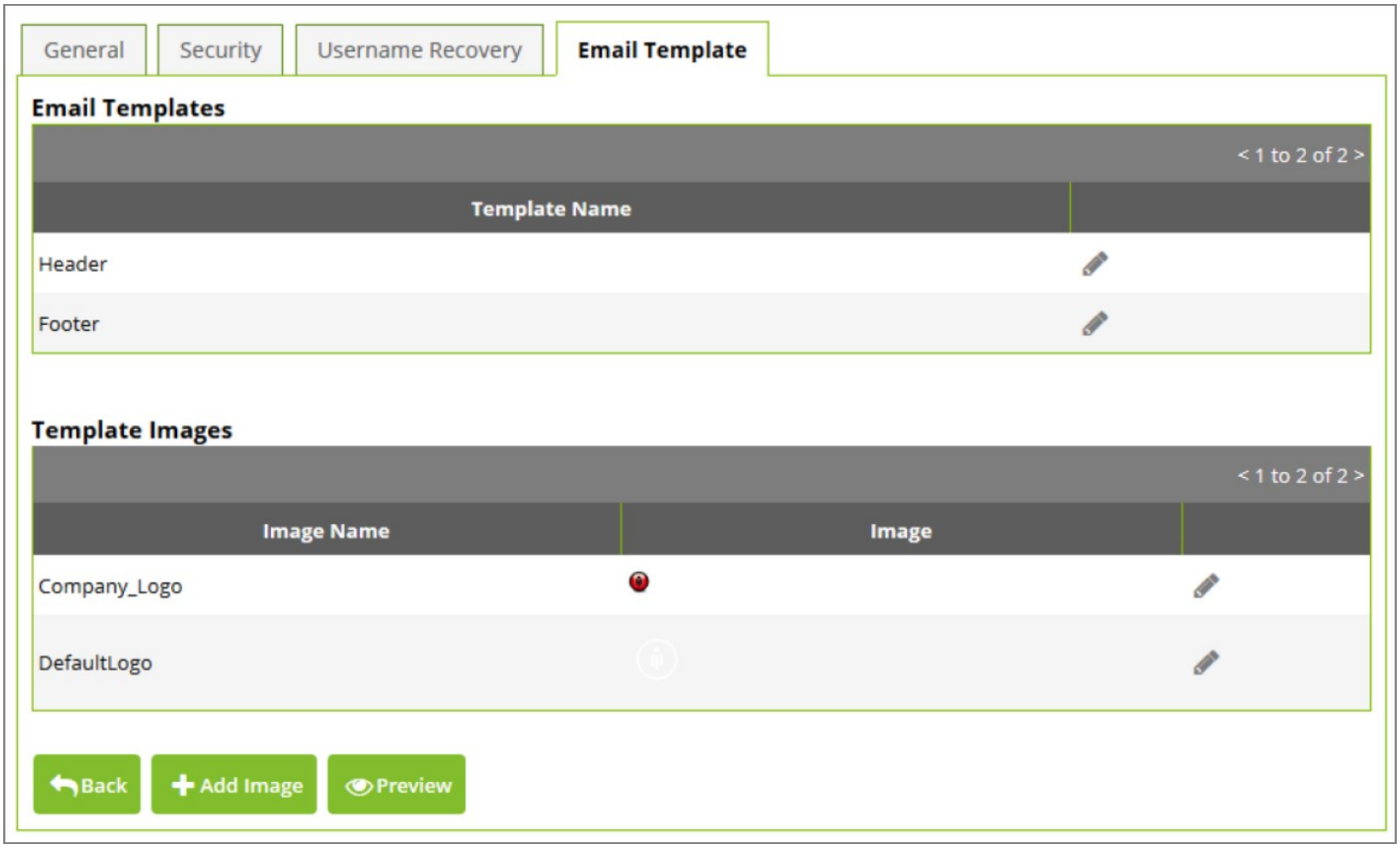
Header

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <title>Password Reset Server</title>

  <style type="text/css">
        /* //// Display fixes for email types - Leave these classes alone.////
```

** This field is HTML Enabled and allows the insertion of images with the HTML tag <img src='cid:TheImageName'> and variable replacement for %DOMAIN% and %USERNAME% and other variables. For more information click here.*

Click the “edit” icon in the Template Images grid to upload a new image from your filesystem. To add an additional image, click Add Image.



Email Templates

< 1 to 2 of 2 >

Template Name	
Header	✎
Footer	✎

Template Images

< 1 to 2 of 2 >

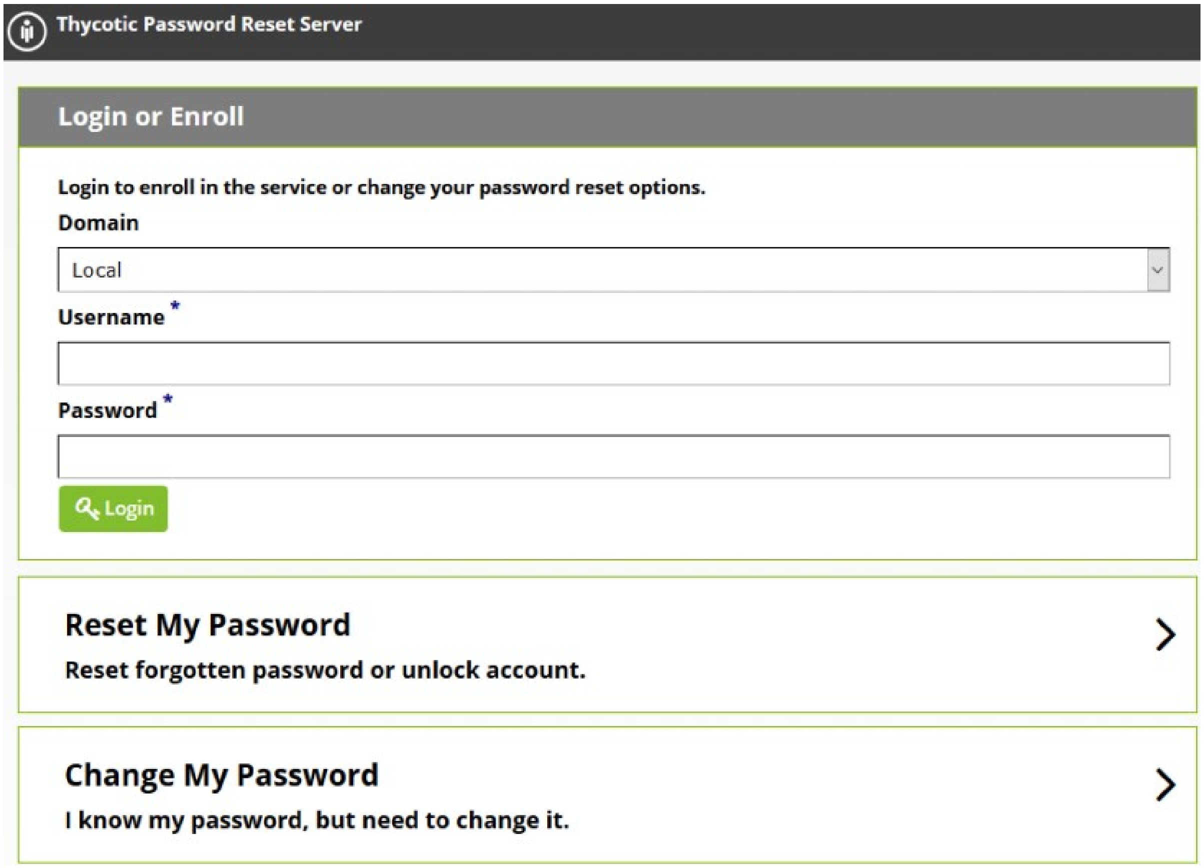
Image Name	Image	
Company_Logo	●	✎
DefaultLogo		✎

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 Installation.

ACCESSING PASSWORD RESET SERVER

Password Reset Server presents three options to users on the main page: Login or Enroll, Reset My Password, and Change My Password.



Thycotic Password Reset Server

Login or Enroll

Login to enroll in the service or change your password reset options.

Domain: Local

Username *

Password *

Reset My Password

Reset forgotten password or unlock account.

Change My Password

I know my password, but need to change it.

Clicking **Login** will allow users to log into the system. If they have not yet enrolled, they will be required to complete the enrollment process. Otherwise, they will be presented with a screen displaying information on their security questions. See User **Home Screen** for details. Administrators will be presented with the administration dashboard.

Users can log in with their AD username or their UPN. Additionally email logins can be set up in **Administration | Configuration**.

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**.

Password Reset Server utilized two cryptographic algorithms for storing its data: 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: 3eeee1d0 e11733ef 152a6c29 503b3ae2 0c4f1f3c da4cb26f 1bc1a41f 91c7fe4a b3bd8649 4049e201 c4bd5155 f31ecb7a 3c860684 3c4cc8df cab7da11 c8ae5045

SSL/TLS (Secure Socket Layer)

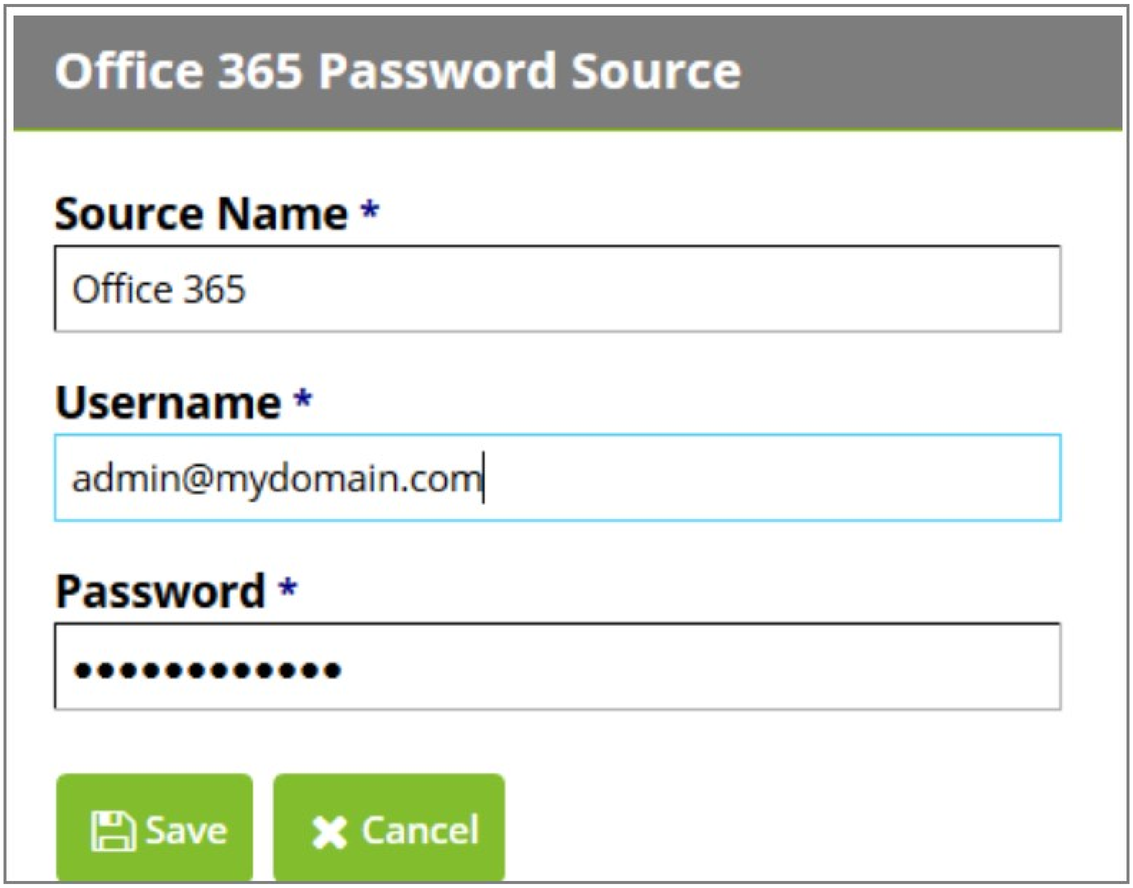
Password Reset Server can be configured to run SSL certificates. It is strongly recommended that Password Reset Server installations run using SSL. Not using SSL will significantly reduce the security of the contents of Password Reset Server since browsers viewing the site will not be using an encrypted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

Creating a New Password Source

You can use password sources to define additional Office 365 domains that will be used to change an additional password for a user when a password change or password reset is performed.

By default, password sources will always contain an Active Directory password source once you define a domain in PRS. To add a new password source, click **Add** and then select your **Source Type** (currently either Active Directory Domain or Office 365).

If you choose **Active Directory Domain**, you will prompted to add domain information (see **Domain Configuration**). If you choose Office 365 Domain you will need to complete the following form:



Office 365 Password Source

Source Name *

Office 365

Username *

admin@mydomain.com

Password *

●●●●●●●●●●●●●

Source Name:

The display name of the source.

Username:

The Office 365 administrator user that will be used to change the end user’s password during the reset process. This user must be an Office 365 administrator

Password:

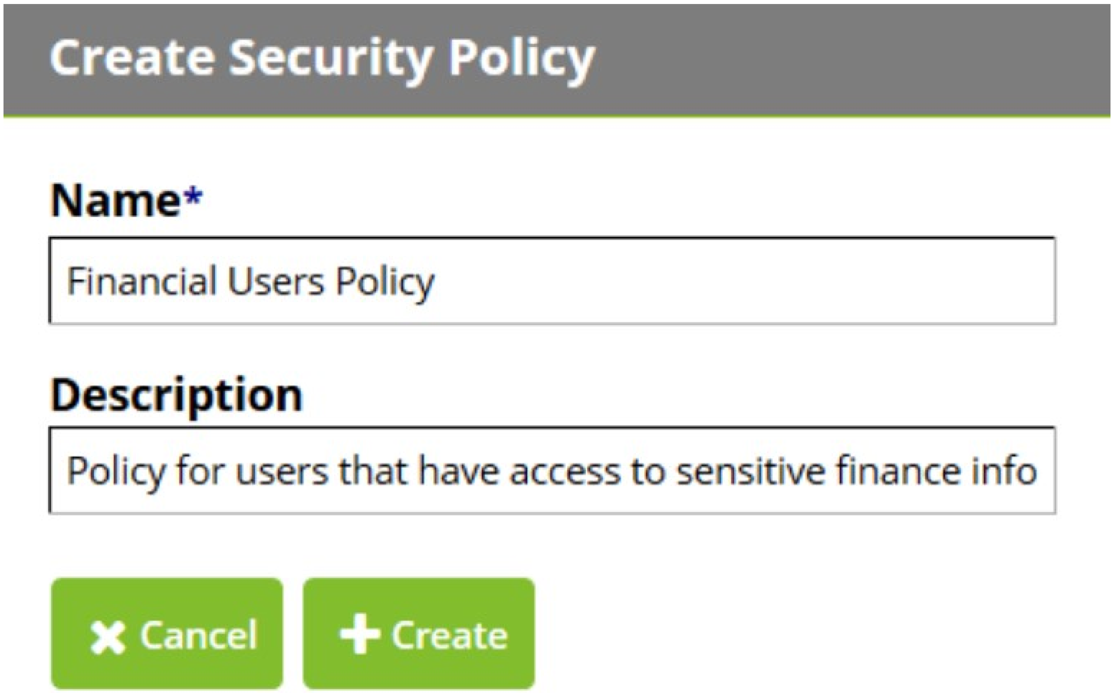
The password of the Office 365 administrator.

A security policy is a set of questions defined by the administrator that 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 only belong to one security policy at a time.

An administrator can view or modify security policies by logging into Password Reset Server and selecting **Security Policies** from the **Administration menu**.

Creating a new Security Policy

From the **Security Policies** administrative page, click **Create**. 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 finance info

Modifying an Existing Security Policy

To modify an existing security policy, select **Security Policies** from the **Administration** menu and then click the name of the policy you would like to configure.

Configuring a Security Policy

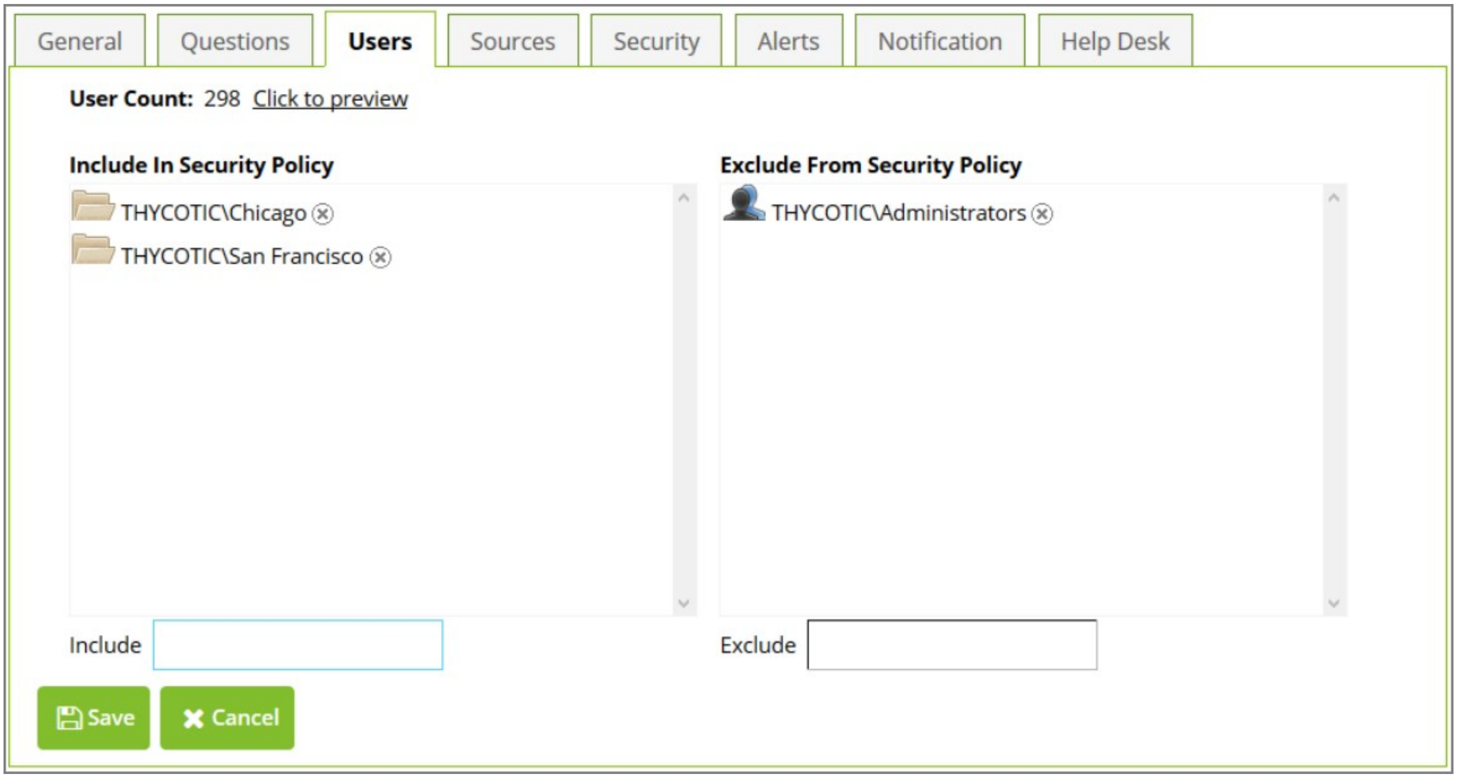
After creating a new security policy or modifying an existing one, you can configure it and tailor it to meet your requirements.

To edit the description or name of a security policy, click **Edit** 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.

Users may be assigned to a security policy directly, by Organizational Unit (OU), or by group. To view OU's, groups, and users that are part of the security policy, click the **Users** tab at the top of the overview of the security policy.

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 OU's click the **X** next to the object you want to remove. To save your changes, click **Save**.



User Count: 298 Click to preview

Include In Security Policy

THYCOTIC\Chicago ⊗

THYCOTIC\San Francisco ⊗

Exclude From Security Policy

THYCOTIC\Administrators ⊗

Include

Exclude

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.

Password Reset Server also 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.

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:** 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.

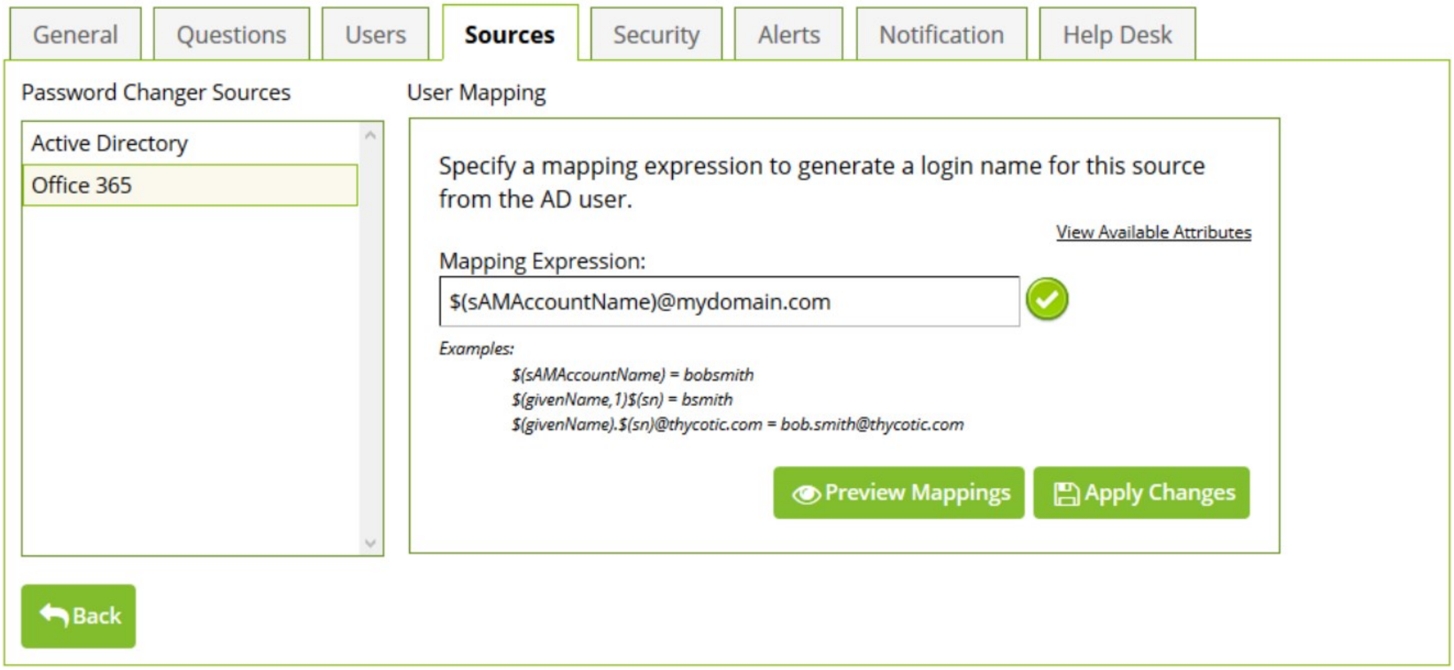
Active Directory

The Active Directory password source represents the user's domain. By default all security policies have an Active Directory password source assigned. You can remove this source if you want only Office 365 sources (no Active Directory password resets).

Office 365

Once an Office 365 password source has been created, then you may use it on a security policy. To do so, open the security policy and then select the **Source tab**. The following screen is displayed:

Click **Add** to add a new password source to the security policy. Select the source you want to add to this security policy, then click **OK**. Then under **Password Changer Sources** click on the source you want to map and **User Mapping** for that source will be displayed.



Specify a mapping expression to generate a login name for this source from the AD user.

Mapping Expression: $(sAMAccountName)@mydomain.com

Examples:

$(sAMAccountName) = bobsmith
$(givenName,1)$(sn) = bsmith
$(givenName).$(sn)@thycotic.com = bob.smith@thycotic.com

The mapping expression maps Active Directory Attributes to credentials used to create the login name for the Office 365 user. Mapping expressions can be any combination of Active Directory Attributes and actual text. Also Active Directory Attributes can be set to a specific length with the addition of a ',' (comma) and the number of characters to include.

> **Note:** For Office 365, the default mapping expression is the user's email address $(mail).

View Available Attribute

This will show a list of available Active Directory Attributes that are defined (see **Active Directory Attributes**). You may select any attribute with a double click to place it in the mapping expression.

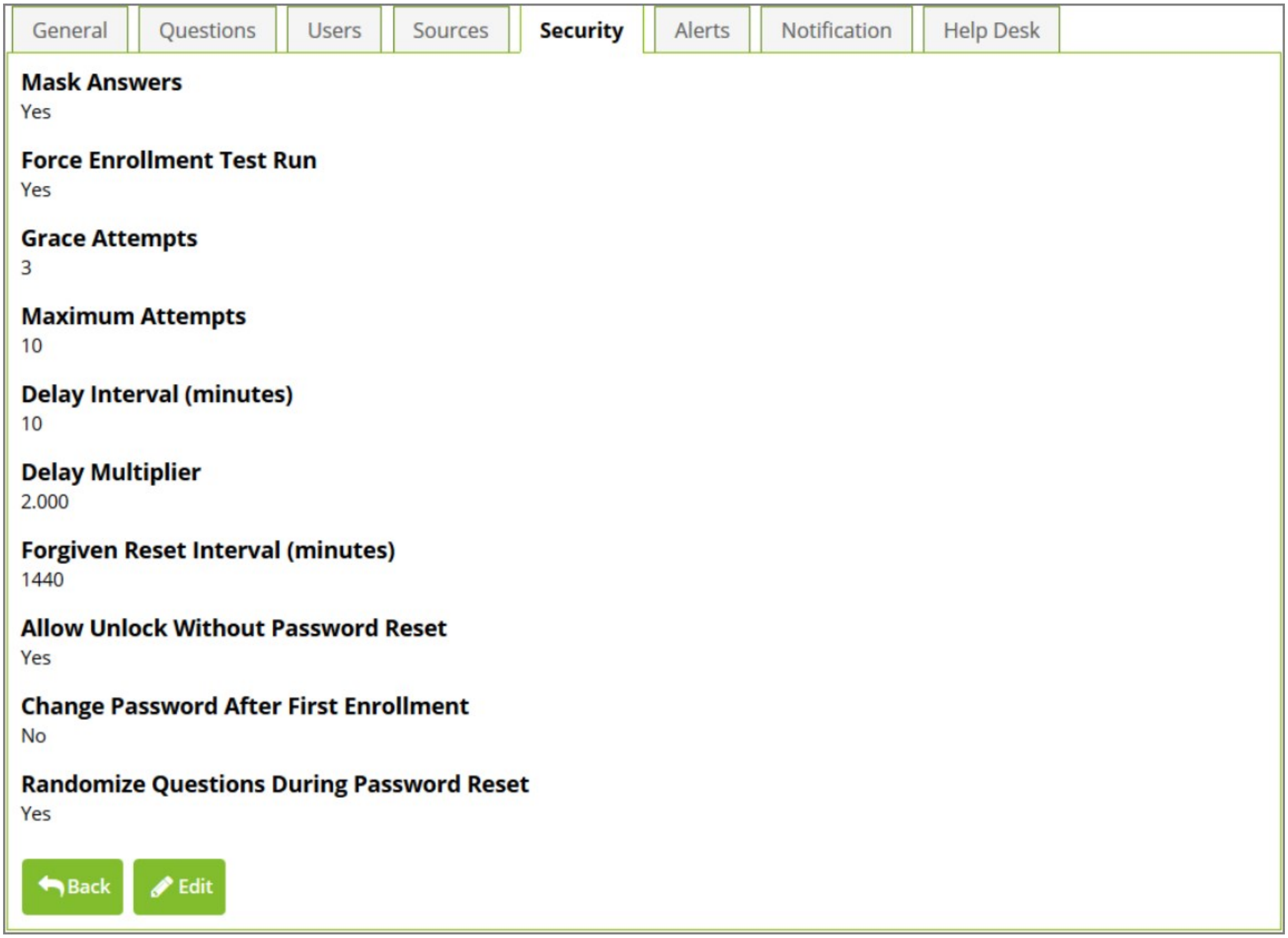
Preview Mappings

This will preview a list of up to 25 users, with the mapping expression evaluated.

Apply Changes

This will save the changes to the mapping expression associated the password source.

To view or edit the security settings of a security policy, click the **Security** tab at the top of the policy overview. To edit these values, click the **Edit button**. From the Editscreen you can click **Save** to save your changes or **Cancel** to abort them.



Mask Answers
Yes

Force Enrollment Test Run
Yes

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

Randomize Questions During Password Reset
Yes

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. Set the **Delay Multiplier** to 1 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.

Configuring the reset attempt:

The **Grace Attempts, Maximum Attempts, Delay Interval, Delay Multiplier**, and **Forgiven Reset Interval** fields control how many times a user can try to reset their password and what happens when their reset attempts fail.

The following process occurs when a user attempts to reset their password based on the values of these fields:

1. The user is prompted for their account name.
2. PRS checks if there are any reset attempt failures since the last successful reset. If there are and the number of failed attempts is less than the number of Grace Attempts defined in the Security Policy (or Grace Attempts is zero) the user is allowed to proceed. (See below for the process if the number of failed attempts is not less than the number of Grace Attempts). The current release allows the user to try one more time than the Grace Attempts. So, if the Grace Attempts is set to three, the user can actually attempt a password reset four times before the procedure below kicks in. This will be fixed in the next release.
3. If validated, the user is prompted for their security question or questions.
4. If the answers meet the minimum requirements defined in the Security Policy, the user is allowed to reset their password. Otherwise, the user receives a message that their identity could not be verified and that they can try again.

If the number of failed attempts is not less than the number of Grace Attempts AND Grace Attempts is not zero, then:

1. The user will be informed that they have exceeded the number of retries and that they must wait until a time calculated as number of minutes specified by the Delay Interval defined in the Security Policy past the last failed retry.
2. After the Delay Interval has passed the user can attempt to reset their password again. If they fail to answer the security questions again they will need to wait until a time calculated as the Delay Interval x Delay Multiplier past the last failed retry before attempting to log in again.
3. Each subsequent retry failure will increase the time before they can try again by the Delay Multiplier (see example, below).
4. If the user attempts to reset their password more than the Maximum Attempts defined in the Security Policy they will be blocked from trying to reset their password until the number of minutes defined in the Forgiven Reset Interval has passed. After that interval has passed, the system resets and the user gets the Grace Attempts number of retries again before the Delay Interval and Multiplier are applied.

Example If the following settings are configured in the security policy:

- Grace Attempts: 3
- Delay Interval: 10
- Delay Multiplier: 2
- Maximum Attempts: 6
- Forgiven Reset Interval: 1,440

When a user attempts to reset their password but does not know their security answers, the following will happen:

1. The user will be given three tries to answer their security question or questions.
2. The fourth time the attempt to reset their password they will be informed that they must wait 10 minutes from the time of their third failed attempt before trying again. So, if their third attempt occurred at 2:30 PM and they are trying for the fourth time at 2:34 PM they must wait six more minutes.
3. If they retry again at 2:45 PM and fail again, they will not be allowed to try again until 3:05 PM (2:45 PM plus 10x2 minutes).
4. If they try a fifth time at 3:15 PM and fail again they will not be allowed to try again until 3:55 PM (3:15 PM plus 10x2x2 minutes).
5. If they try a sixth time at 4:00 PM and fail again they will have tried the maximum allowed number of times. They will not be allowed to try resetting their password until 4:00 PM the following day (the Forgiven Reset Interval of 1440 minutes = 1 day).
6. After 4:00 PM the following day they will be able to try resetting their password again. All previous failures are forgiven so they will have three grace attempts again. Then the process described above will repeat.

   Note: : If **Grace Attempts** is set to zero all delaying strategies are disabled, including the **Maximum Attempts** and **Forgiven Reset Interval**. Setting **Grace Attempts** to zero is not advised since it allows a malicious person an unlimited number of attempts to gain access to a user's account by brute-force guessing common answers to questions.

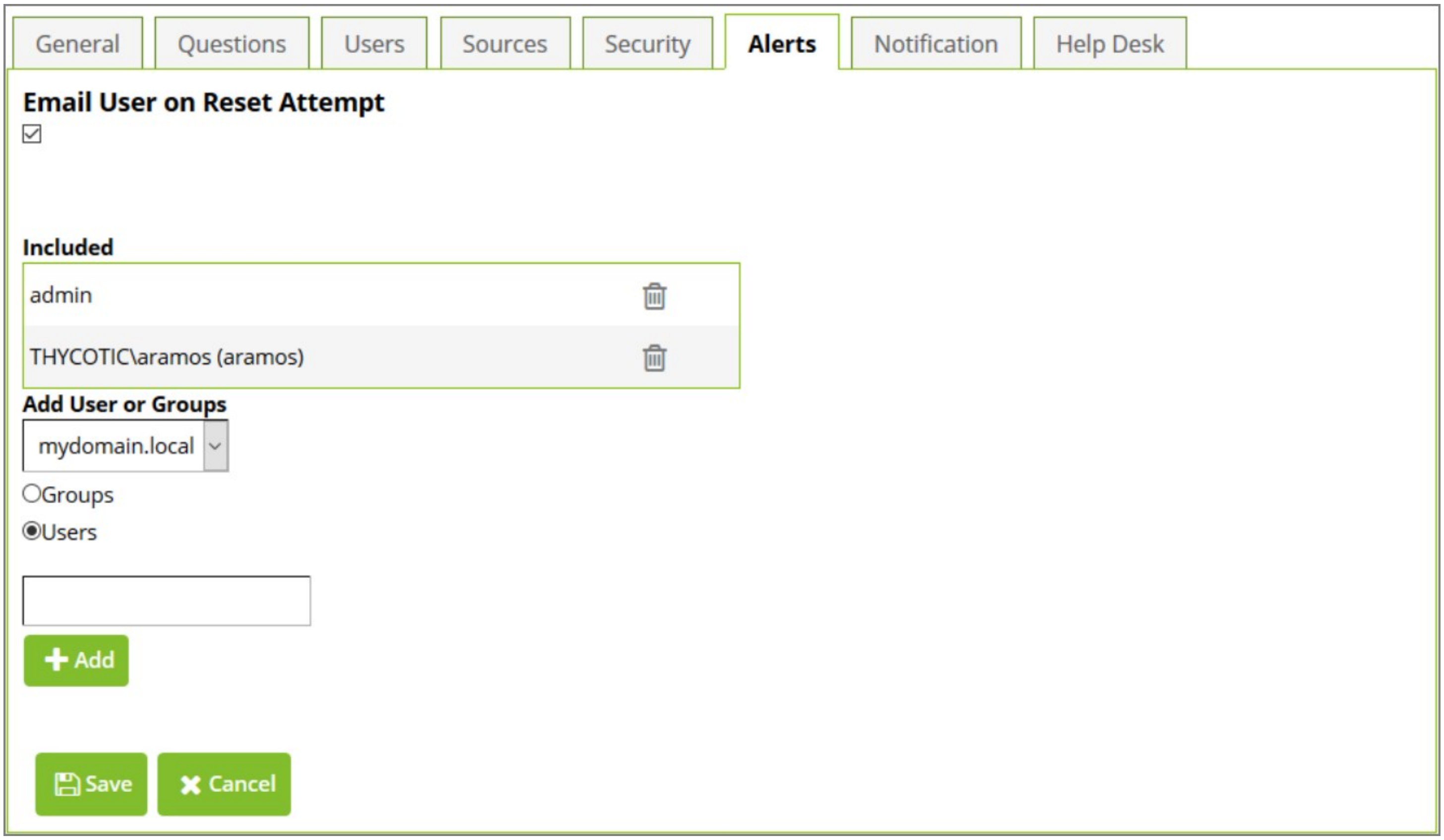
Allow Unlock Without Password Reset

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

Randomize Questions During Password Reset

If 'Yes', questions will be presented to the user in random order during a password reset and enrollment.

To view or edit the alerts, click the **Alerts** tab at the top of the security policy overview.



Email User on Reset Attempt

☑

Included

admin

THYCOTIC\aramos (aramos)

Add User or Groups

mydomain.local

○Groups

●Users

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.

To view the assigned questions or modify them, click **Questions** at the top of the security policy overview.

To modify which questions belong to the policy, click **Edit**. You can then select or deselect the **Include** check box for each question to add or remove it from the policy. Select the question status from the Status drop-down menu. The three options are as follows:

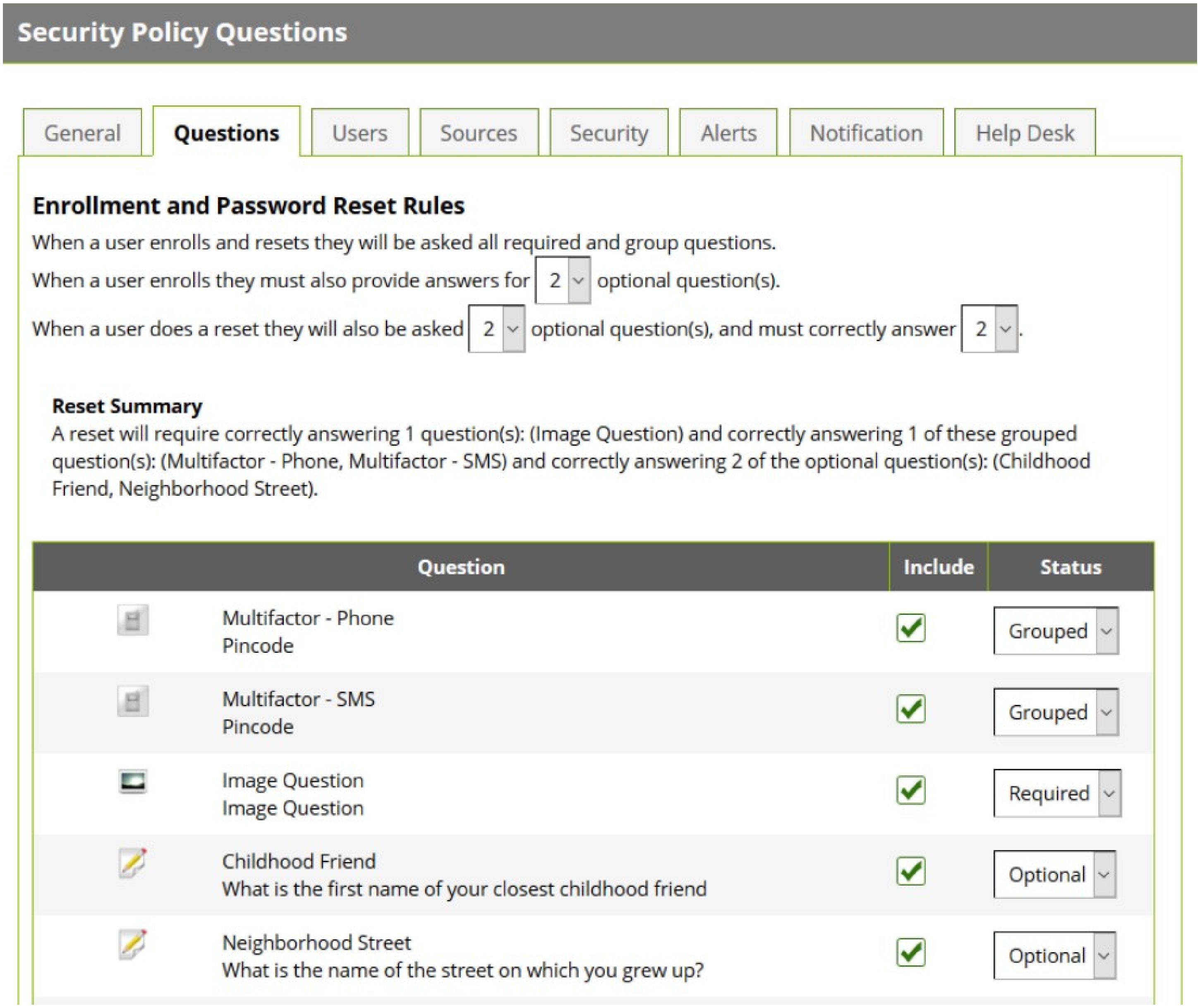
Optional:

The question will be available, but not required, to answer during enrollment, a reset, and when the user updates the answers to their questions.

Required:

The question will be required to answer during enrollment and during a reset.

Grouped: The question will be required to answer during enrollment. Upon a reset, the user will be required to answer one of the grouped questions correctly.



Security Policy Questions

Enrollment and Password Reset Rules

When a user enrolls and resets they will be asked all required and group questions.

When a user enrolls they must also provide answers for 2 optional question(s).

When a user does a reset they will also be asked 2 optional question(s), and must correctly answer 2.

Reset Summary

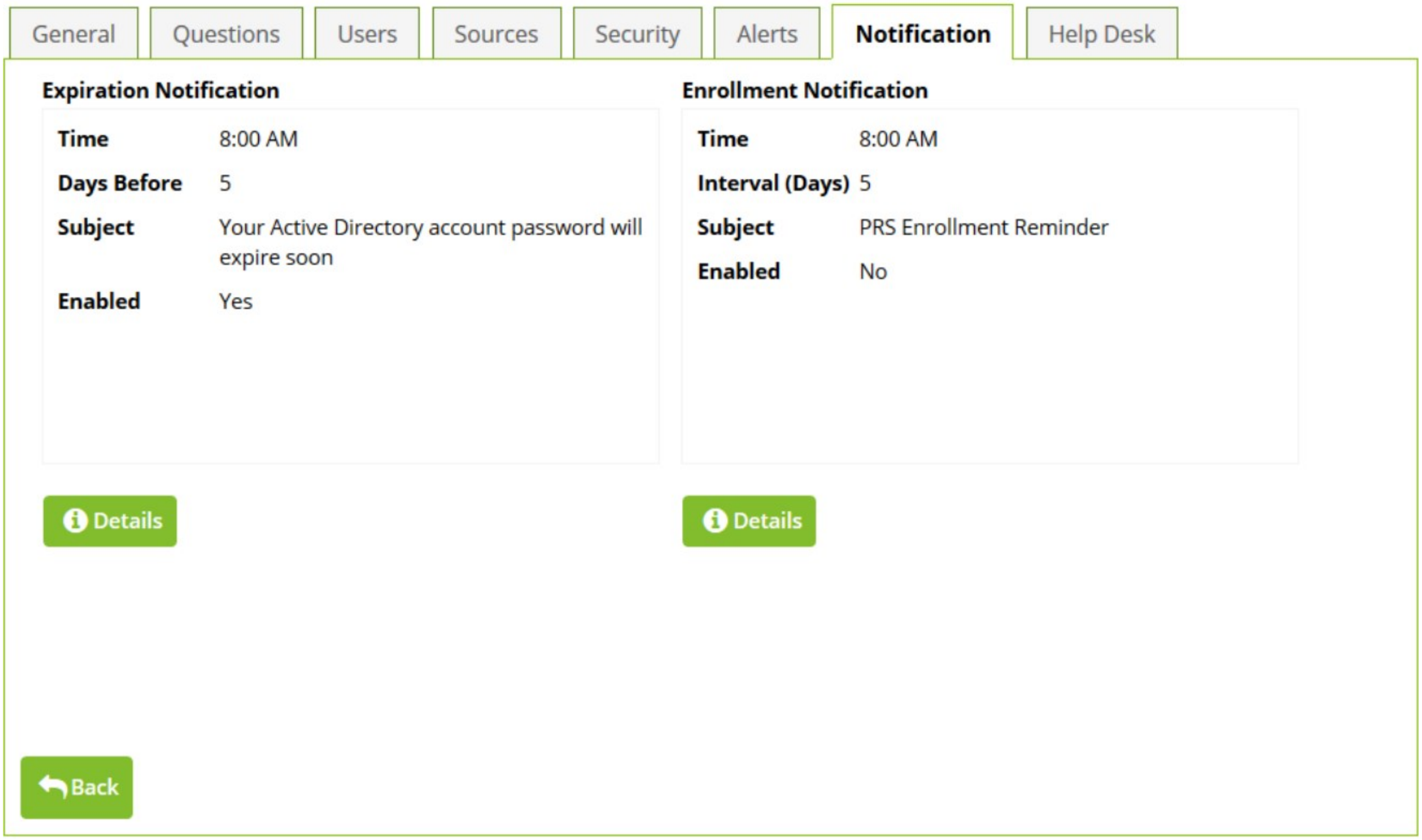
A reset will require correctly answering 1 question(s): (Image Question) and correctly answering 1 of these grouped question(s): (Multifactor - Phone, Multifactor - SMS) and correctly answering 2 of the optional question(s): (Childhood Friend, Neighborhood Street).

	Question	Include	Status
	Multifactor - Phone Pincode	☑	Grouped
	Multifactor - SMS Pincode	☑	Grouped
	Image Question Image Question	☑	Required
	Childhood Friend What is the first name of your closest childhood friend	☑	Optional
	Neighborhood Street What is the name of the street on which you grew up?	☑	Optional

To give your users flexibility, you can set how many questions must be answered for enrollment and password reset using the drop-down menus at the top of the window. For example, in the image above, users must enroll in three questions (First Car, Childhood Friend, and Employee Phone Number). When answering these questions to reset their passwords, they must answer two of the three questions they enrolled in correctly.

View the **Reset Summary** for an overview of the questions and settings you've chosen. Once you have your desired questions, click **Save**, or **Cancel** to abandon your changes.

To view or edit the Expiration Notification or Enrollment Notification settings of a security policy, click the **Notification** tab at the top of the policy overview.



Expiration Notification

Time	8:00 AM
Days Before	5
Subject	Your Active Directory account password will expire soon
Enabled	Yes

Enrollment Notification

Time	8:00 AM
Interval (Days)	5
Subject	PRS Enrollment Reminder
Enabled	No

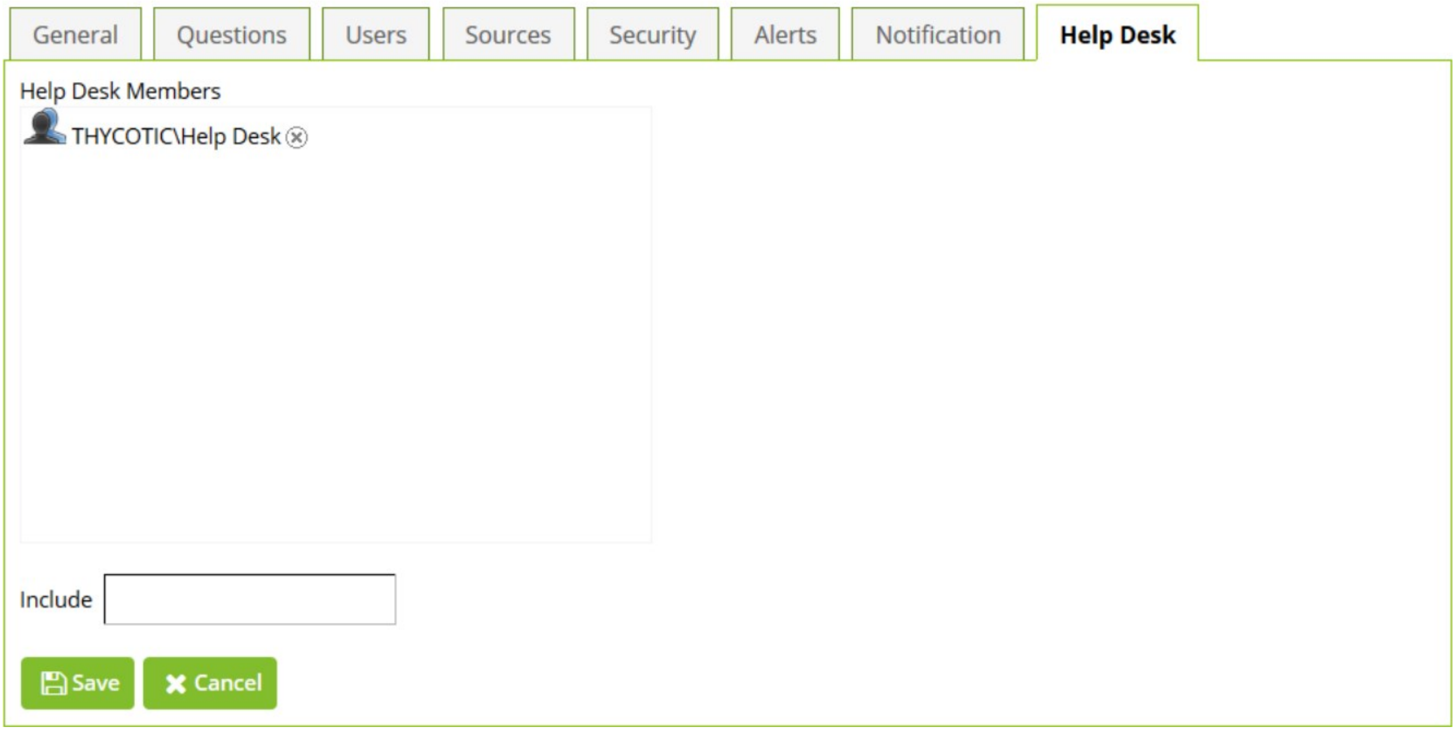
Clicking the **Details** button under either will take you to the main configuration page for the selectednotification type.

When the current **Expiration** Notification is enabled, 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** setting. To set how many days before the expiration the email should be sent, change the **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.

When the current **Enrollment** Notification is enabled, members of this security policy will receive an email if they are not yet enrolled in Password Reset Server. To adjust the time the email is sent, change the **Time setting**. To set how many days should pass in between Enrollment Reminders before the next one is sent, change the **Interval (Days)** setting.

On the **Help Desk** tab of any security policy, type a user or group name in the search field and an autocomplete drop-down list will display possible matches.



Help Desk Members

THYCOTIC\Help Desk

Include

Note: Any user added to a help desk for a security policy will be able to reset the passwords of any user in that security policy. Any user who is a member of a group assigned to a help desk of a security policy will be able to reset the passwords of any user in that security policy.

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 SHA512. 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.

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.

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 may be additional configuration options.

The following settings are present in all questions:

Email Question, Phone Question, 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

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

Enrollment Instructions

Additional instructions to be displayed to the user during the enrollment process.

Answer Instructions

Additional instructions to be displayed to the user during the password reset process. Text and Image questions contain additional configuration options:

Text Question

Minimum Length

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

Image Question

Image Set

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. 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.

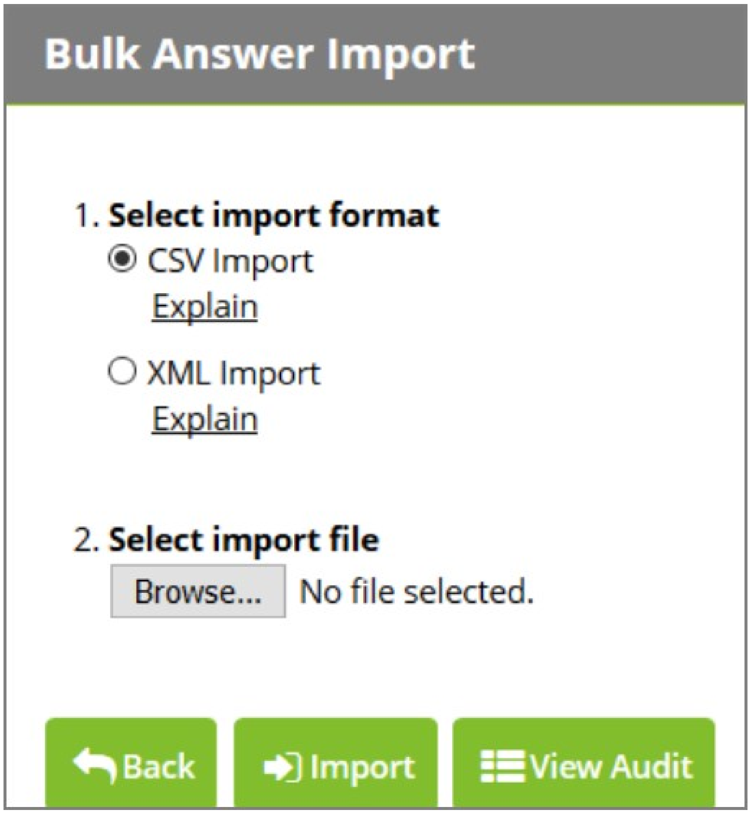
Deleting Questions

You can delete a question as long as there are no security policies that use that question. You can delete a question by navigating to **Administration > Security Questions**, clicking the name of a question, and clicking **Delete**.

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**.



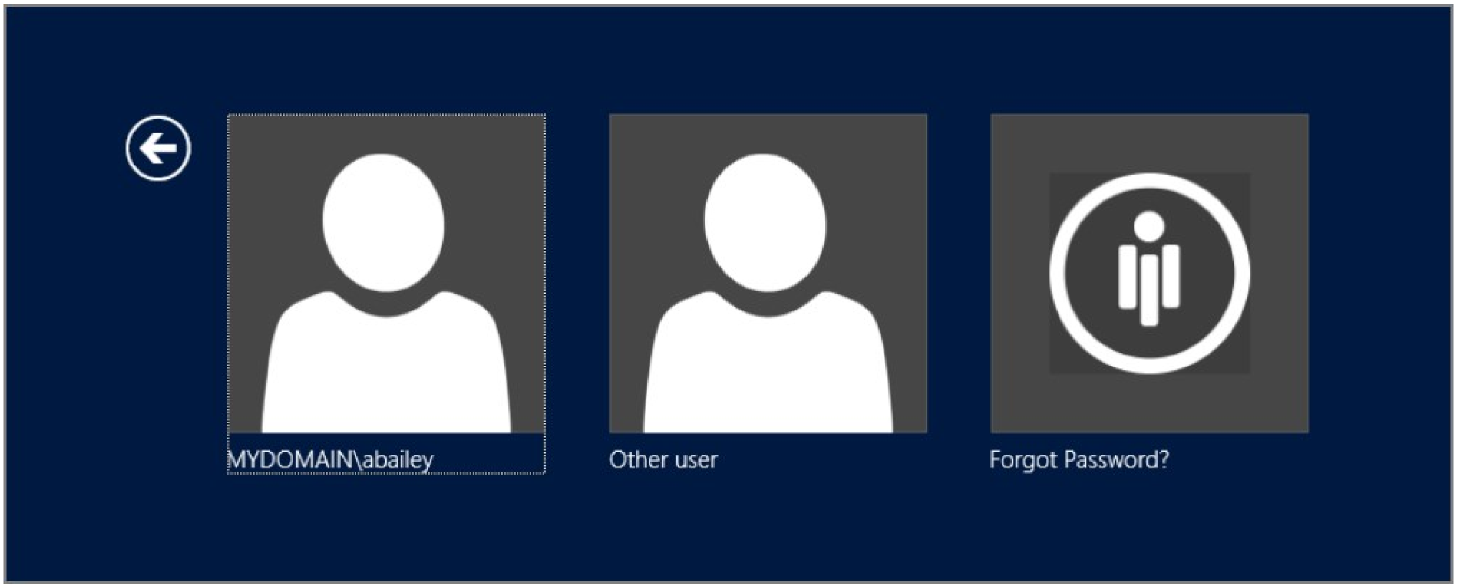
Bulk Answer Import

1. **Select import format**
   - ● CSV Import
     Explain
   - ○ XML Import
     Explain
2. **Select import file**
   Browse... No file selected.

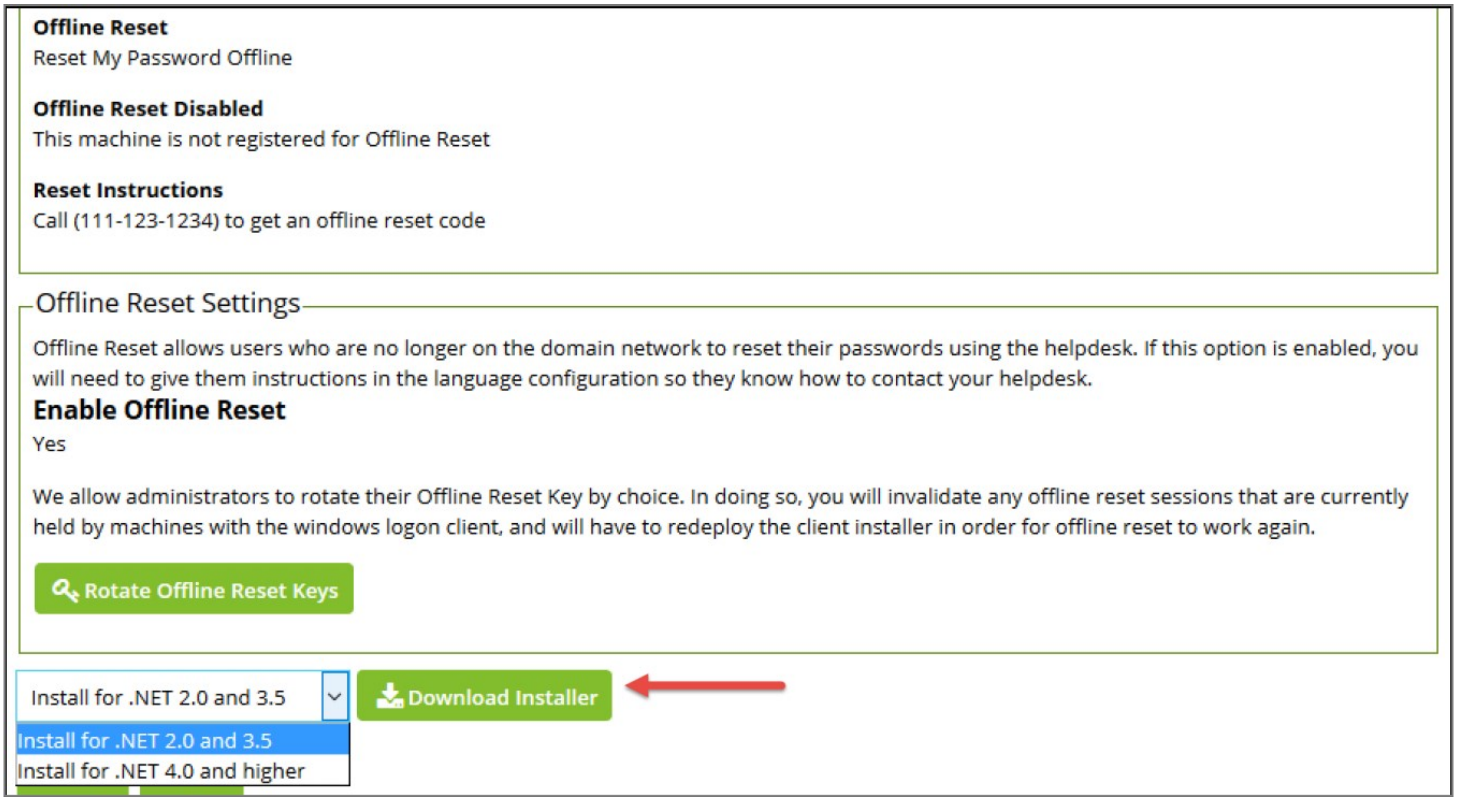
The system log allows you to diagnose issues with Password Reset Server, such as issues with querying your Active Directory domain, backups, etc. For information on sending System Log events to a SIEM tool, see the Configuration section.

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.

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. The Windows Login Integration is required for a user to be able to perform an offline reset on their machine.



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. Select the .NET framework that applies to the version of the Windows operating system you are running in your environment before clicking Download Installer.



Offline Reset
Reset My Password Offline

Offline Reset Disabled
This machine is not registered for Offline Reset

Reset Instructions
Call (111-123-1234) to get an offline reset code

Offline Reset Settings

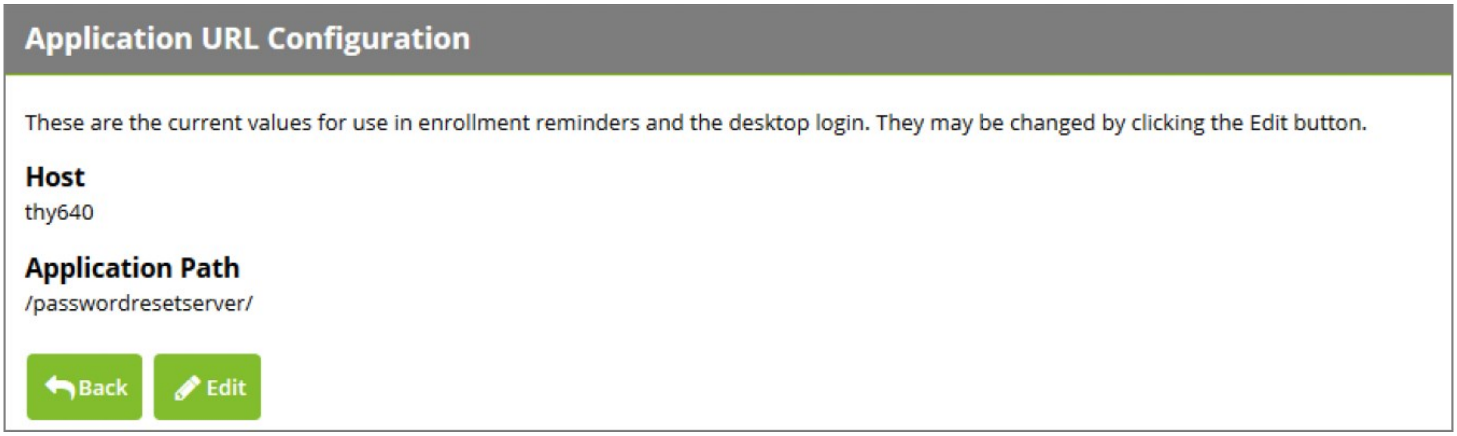
Offline Reset allows users who are no longer on the domain network to reset their passwords using the helpdesk. If this option is enabled, you will need to give them instructions in the language configuration so they know how to contact your helpdesk.

Enable Offline Reset
Yes

We allow administrators to rotate their Offline Reset Key by choice. In doing so, you will invalidate any offline reset sessions that are currently held by machines with the windows logon client, and will have to redeploy the client installer in order for offline reset to work again.

Rotate Offline Reset Keys
Install for .NET 2.0 and 3.5
Download Installer
Install for .NET 2.0 and 3.5
Install for .NET 4.0 and higher

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.



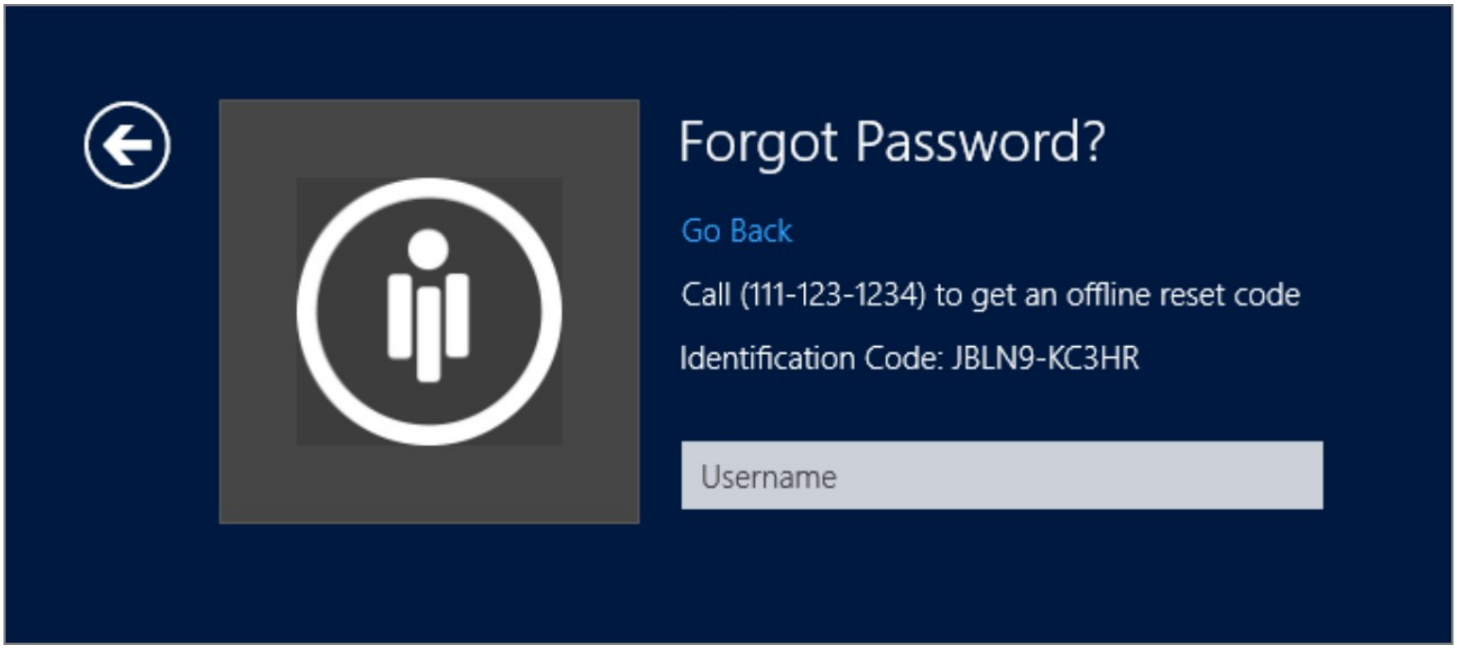
Application URL Configuration

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

Host
thy640

Application Path
/passwordresetserver/

An offline reset works by the end user starting the reset process through the Windows Login Integration UI and getting an identification code. This identification code will be entered during a normal password reset on Password Reset Server, either through a self-reset or via a helpdesk reset. When the reset is finished, a Reset Code will be displayed, and the user will use this, along with their new password, to reset their password on the Windows machine.



Forgot Password?

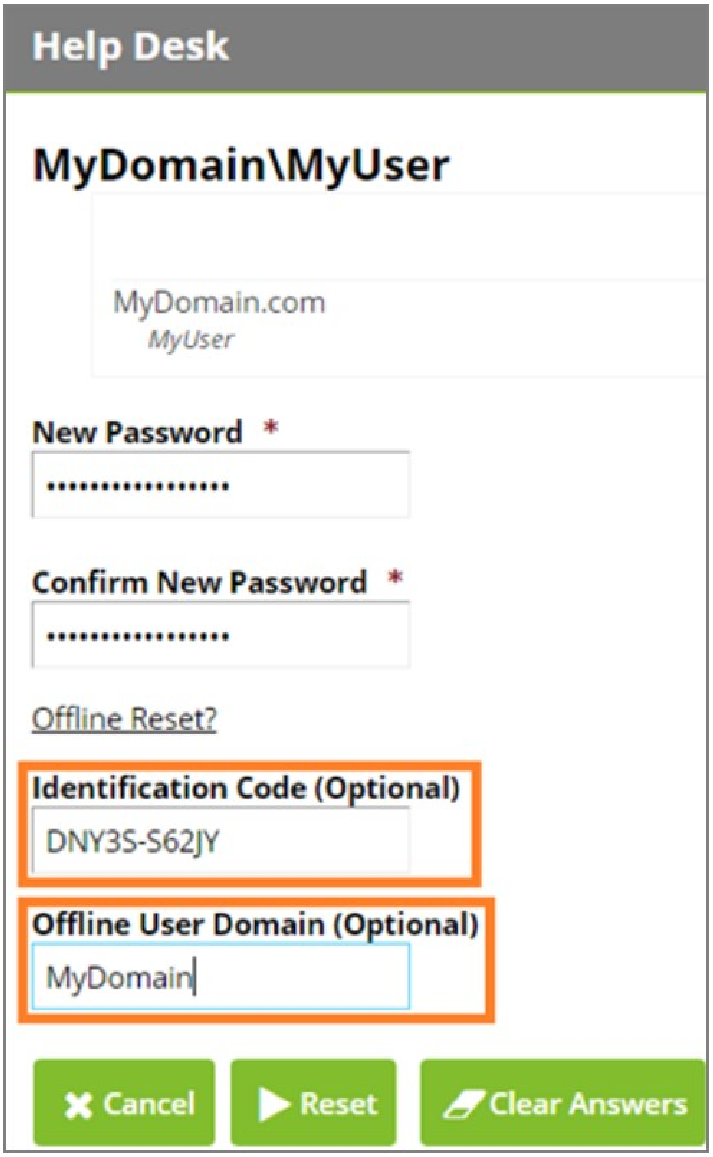
Call (111-123-1234) to get an offline reset code

Identification Code: JBLN9-KC3HR

The Identification Code is unique per machine. Each machine will get a unique encryption key that will be used to retrieve the password from the reset code generated by the server. If these keys need to be regenerated click the **Rotate Offline Reset Keys** which will invalidate and recreate the keys. This will require the Windows Login Integration redeployment for the offline reset to work again.

Help Desk Offline Reset

A help desk user will reset the end users password as normal. But the end user will need to provide the Identification Code. The Offline User Domain needs to match the user's domain on the Windows machine. If left blank it will default to the first part of the FQDN.



Help Desk

MyDomain\MyUser

MyDomain.com
MyUser

New Password *
•••••••••••••••••

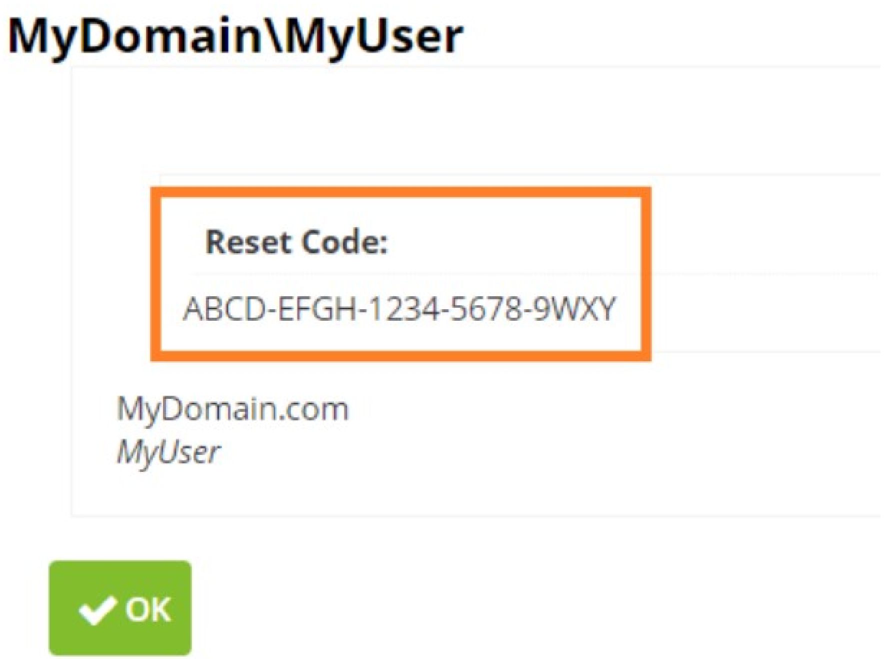
Confirm New Password *
•••••••••••••••••

Offline Reset?

Identification Code (Optional)
DNY3S-S62JY

Offline User Domain (Optional)
MyDomain

After resetting the users password the help desk user will be given a reset code to give to the end user.



MyDomain\MyUser

Reset Code:

ABCD-EFGH-1234-5678-9WXY

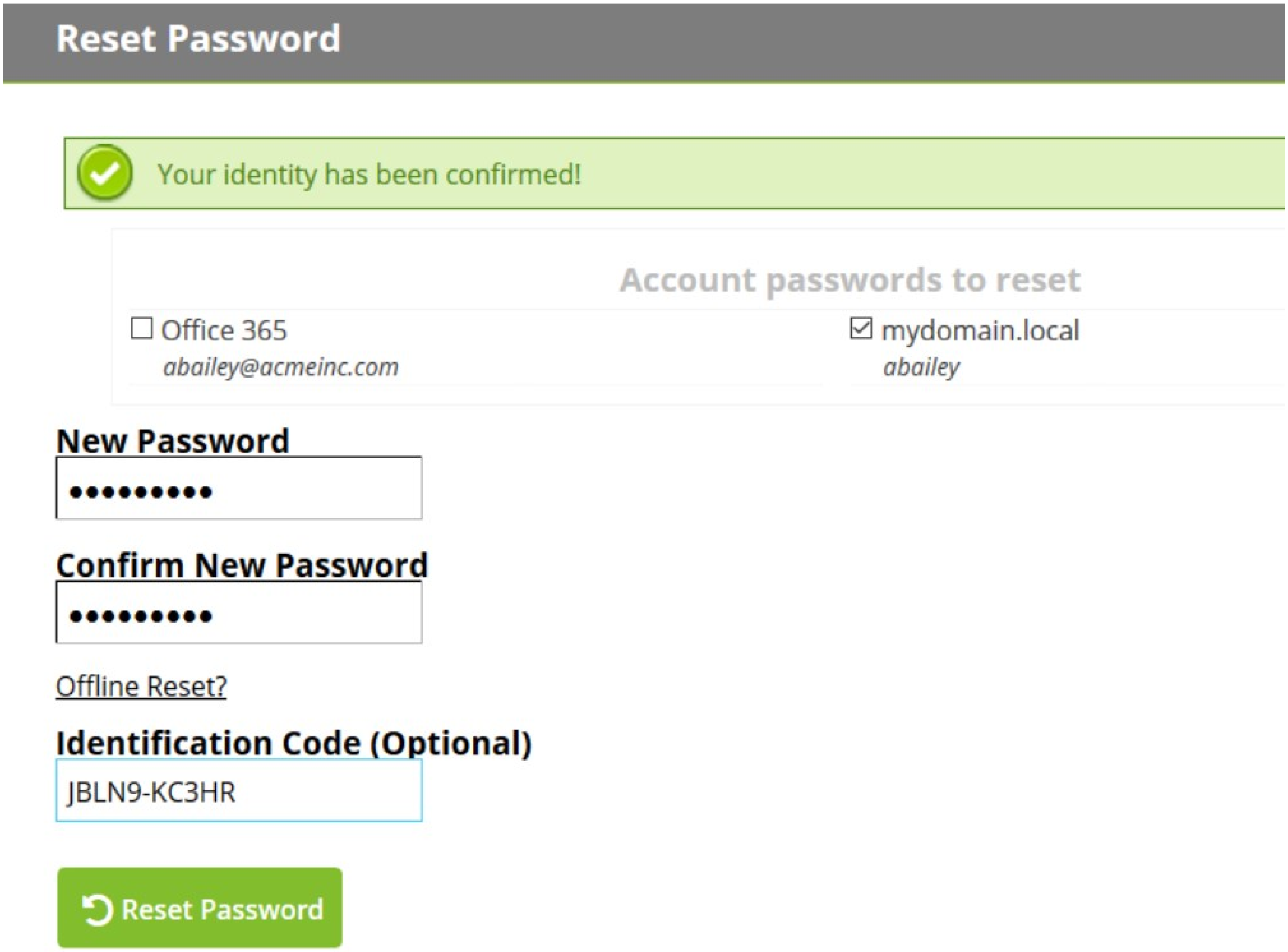
MyDomain.com

MyUser

Self Service Offline Reset

The end user can perform a self-service password reset as normal through the web browser. This requires Password Reset Server to be publicly accessible so the end user can reset using their phone or another internet connected device.

At the end of the reset process the user will have to provide their Identification Code.



Reset Password

Your identity has been confirmed!

Account passwords to reset

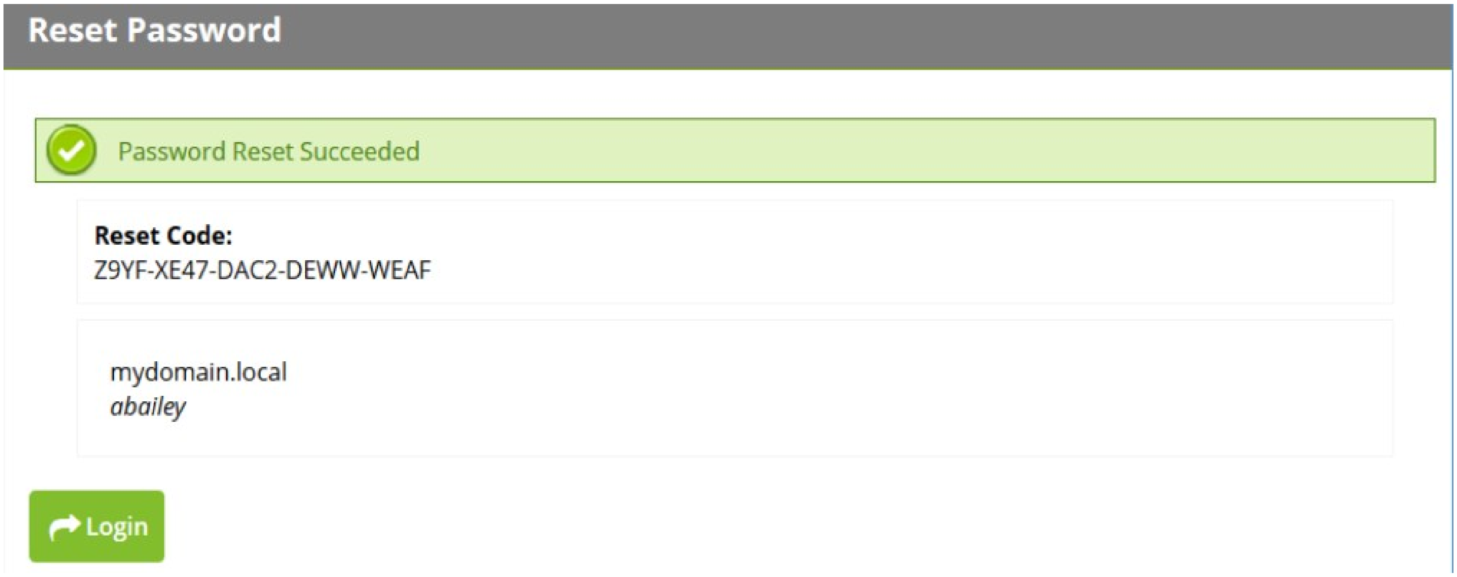
☐ Office 365 *abailey@acmeinc.com*	☑ mydomain.local *abailey*

New Password: ••••••••••

Confirm New Password: ••••••••••

Offline Reset?

Identification Code (Optional): JBLN9-KC3HR



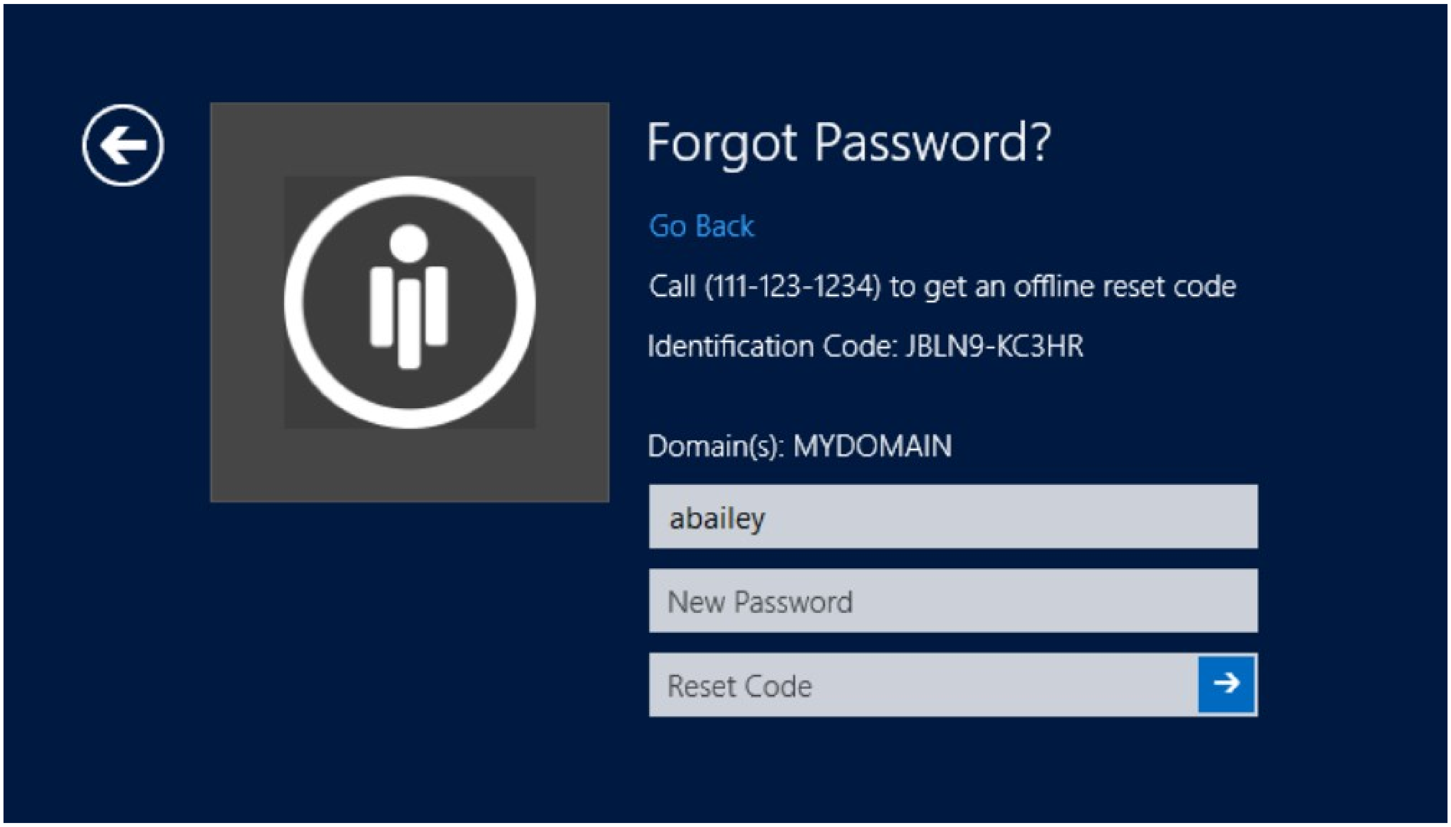
Reset Password

Password Reset Succeeded

Reset Code:
Z9YF-XE47-DAC2-DEWW-WEAF

mydomain.local
abailey

After the user resets their password they will need to enter their reset code, username, and their new password into the windows login integration.



Forgot Password?

Go Back

Call (111-123-1234) to get an offline reset code

Identification Code: JBLN9-KC3HR

Domain(s): MYDOMAIN

abailey

New Password

Reset Code

The user will be able to login as normal with their new password.

User Guide

This section includes information on how a user can enroll and change their password in Password Reset Server.

- Getting Started
- User Information
- Test Run
- Confirmation

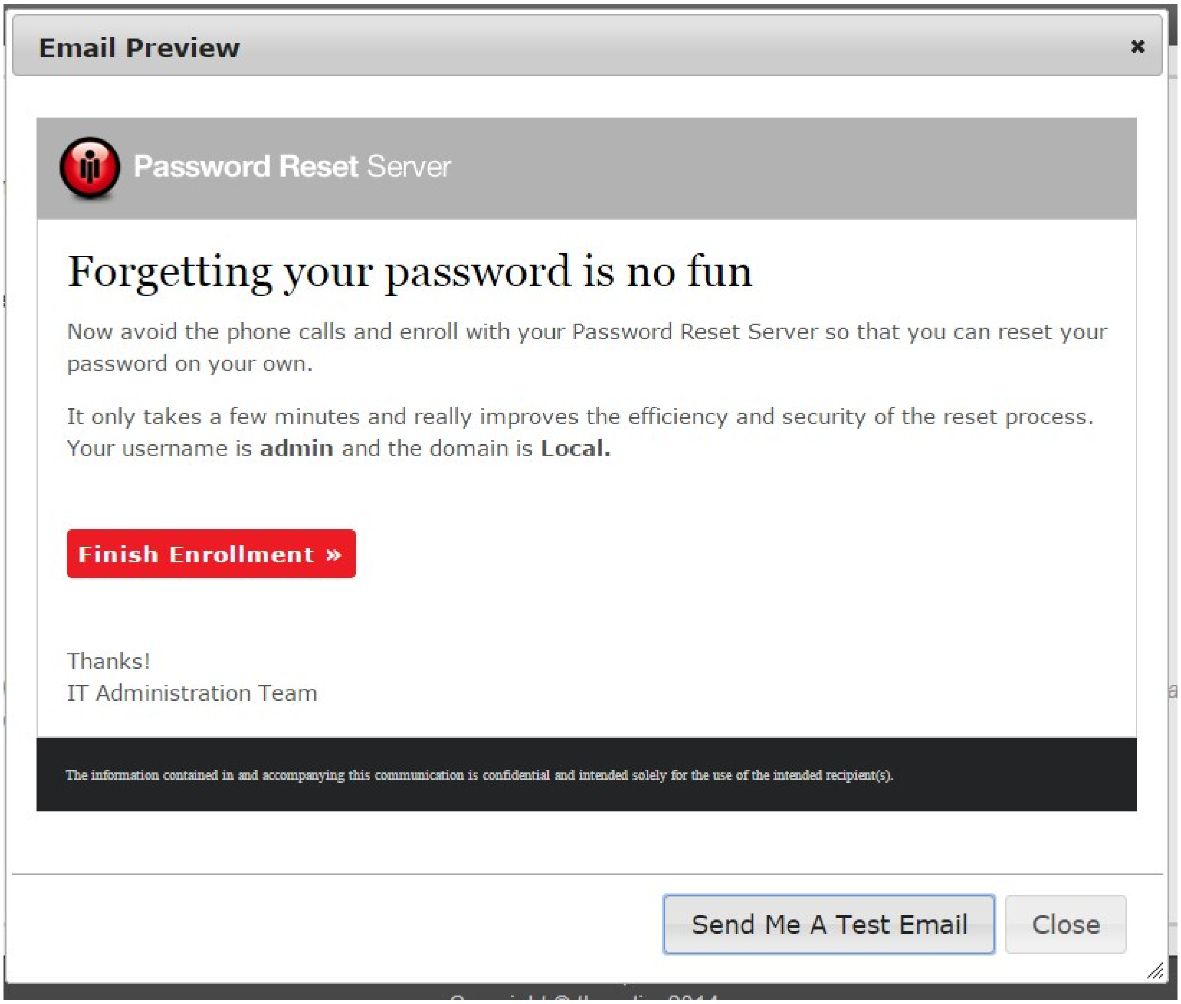
- Getting Started
- Answering Security Questions
- Confirmation
- Offline Reset

This section contains the steps on how to enroll a user in Password Reset Server.

- Getting Started
- User Information
- Test Run
- Confirmation

Getting Started

Begin by clicking the enrollment link sent to you by email or by going to the Password Reset Server URL (*see system administrator).



Forgetting your password is no fun

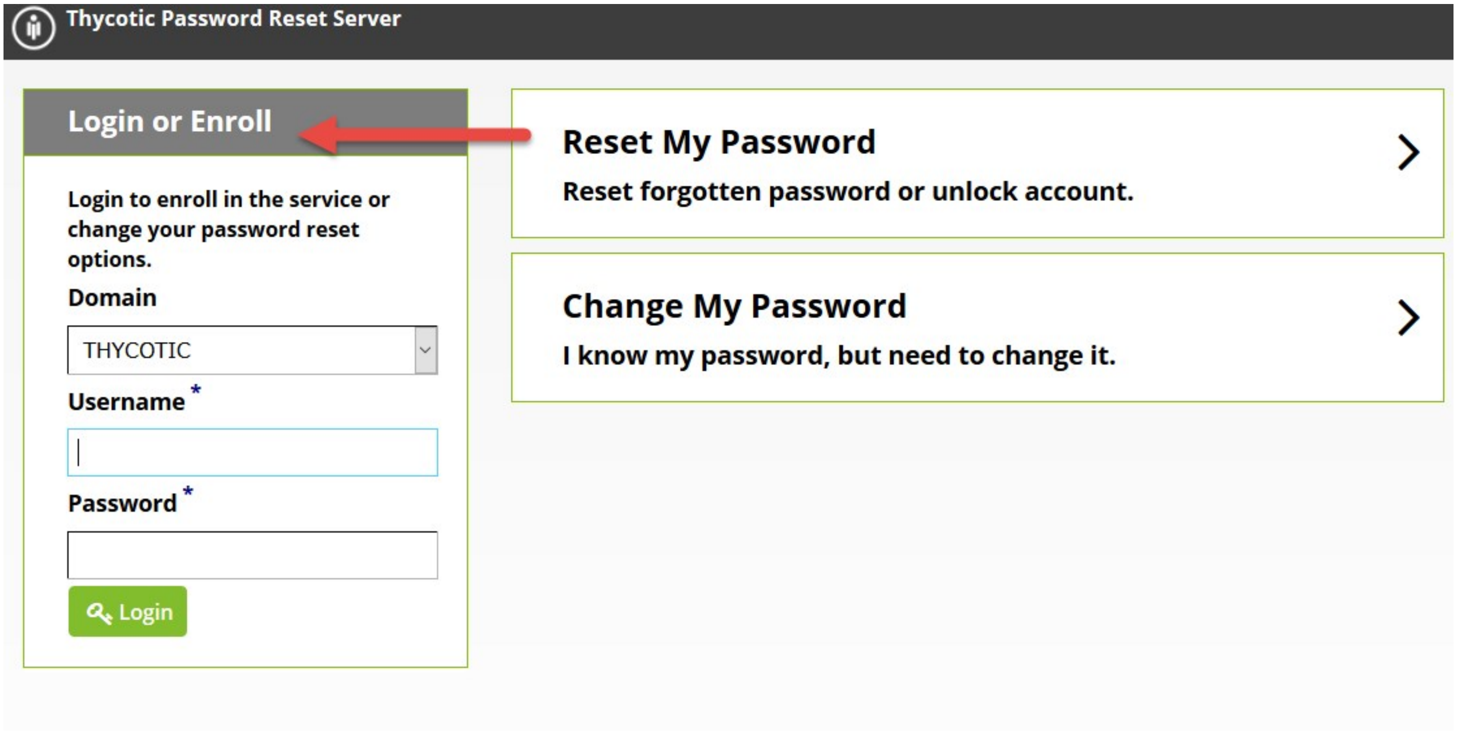
Now avoid the phone calls and enroll with your Password Reset Server so that you can reset your password on your own.

It only takes a few minutes and really improves the efficiency and security of the reset process. Your username is **admin** and the domain is **Local.**

Thanks!
IT Administration Team

The information contained in and accompanying this communication is confidential and intended solely for the use of the intended recipient(s).

Click **Enroll**, then select the domain that you normally log onto and enter your current username and password. Click **Log In**.



Login to enroll in the service or change your password reset options.

Domain: THYCOTIC

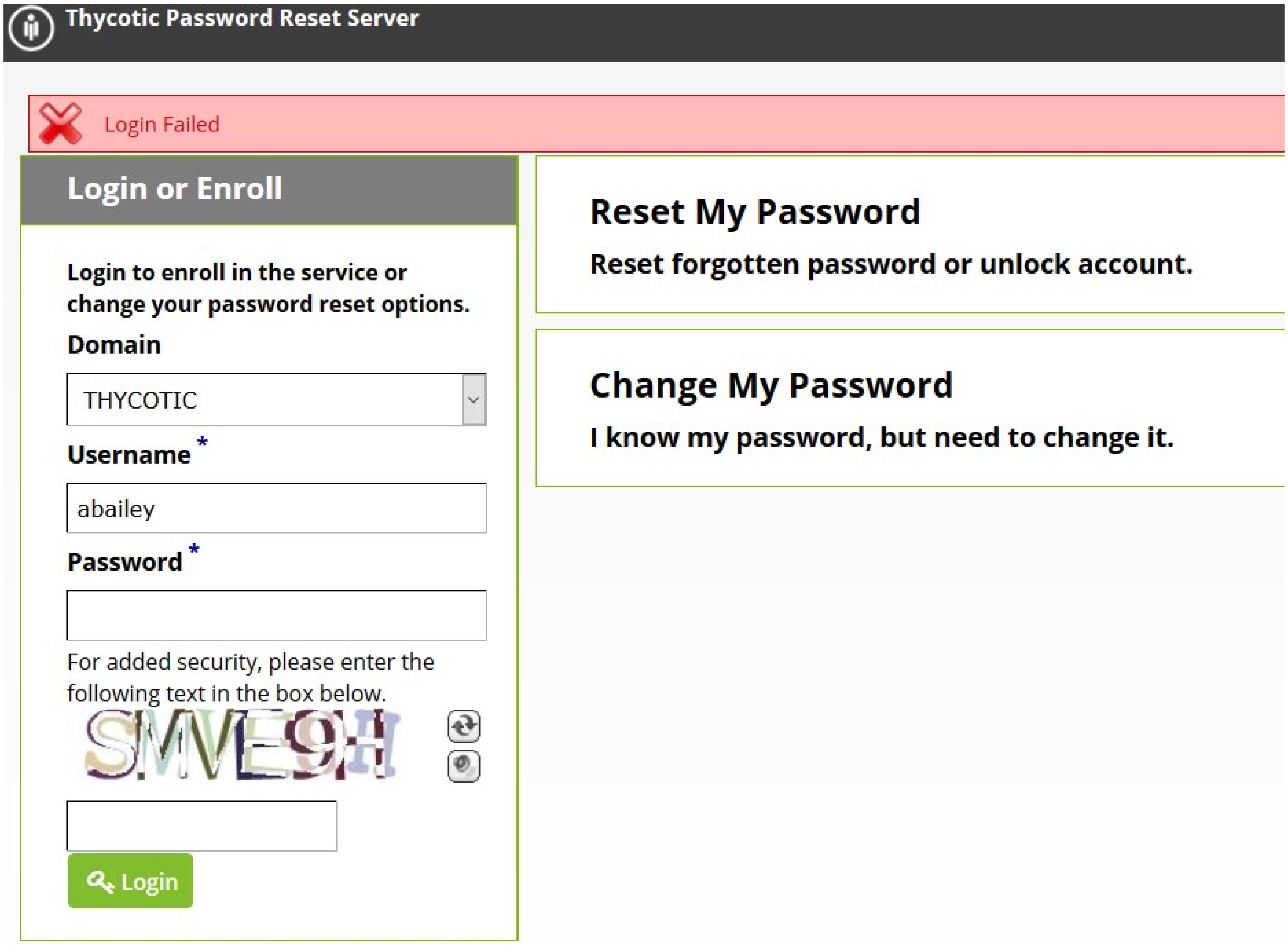
Reset My Password

Reset forgotten password or unlock account.

Change My Password

I know my password, but need to change it.

If you enter an incorrect username and/or password multiple times, you may be required to complete a CAPTCHA challenge in order to log in or enroll.



Thycotic Password Reset Server

Login Failed

Login or Enroll

Login to enroll in the service or change your password reset options.

Domain

THYCOTIC

Username *

abailey

Password *

For added security, please enter the following text in the box below.

Reset My Password

Reset forgotten password or unlock account.

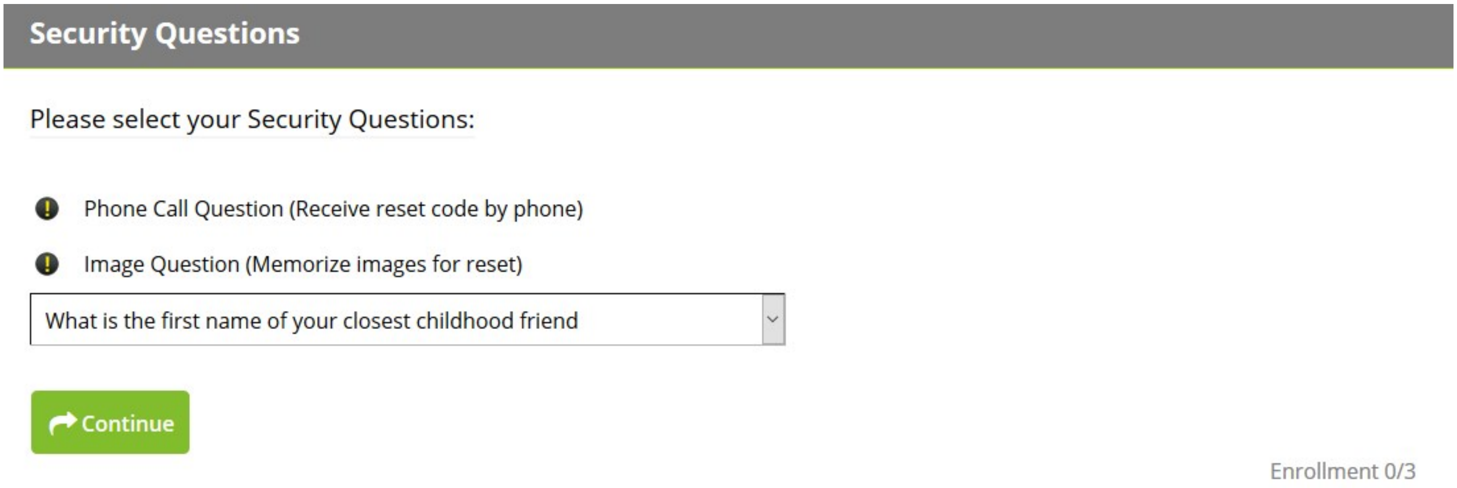
Change My Password

I know my password, but need to change it.

If you continue entering an incorrect password for your username, your account may be locked out and you will need to wait a period of time determined by your administrator before you may attempt to log in or enroll again. If you are already enrolled, you may go through the password reset process to unlock your account.

User Information

Now you will start enrollment by answering the security questions as they appear on screen (i.e. Question/Graphic/Phone).



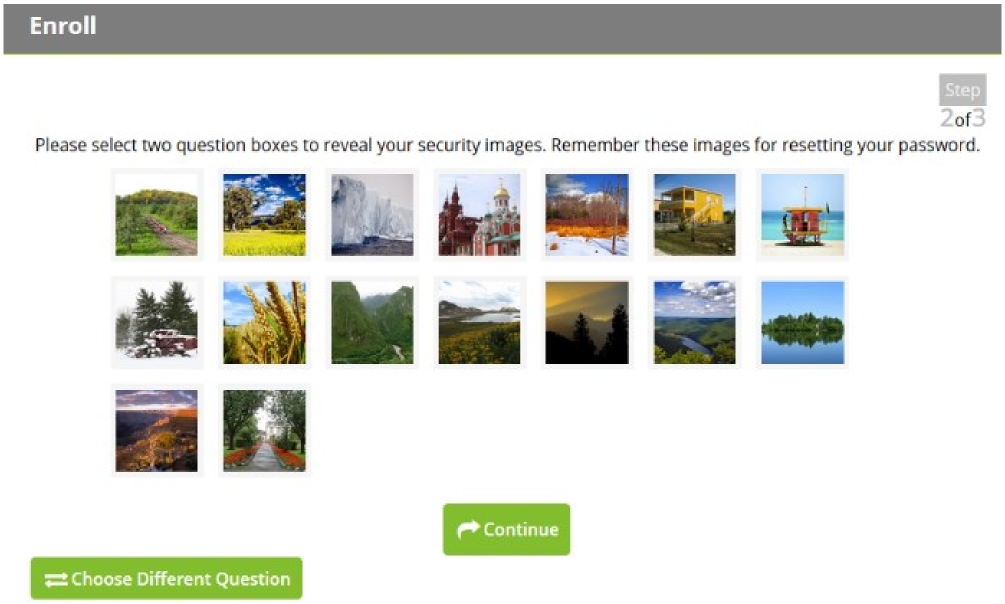
Security Questions

Please select your Security Questions:

- Phone Call Question (Receive reset code by phone)
- Image Question (Memorize images for reset)

What is the first name of your closest childhood friend

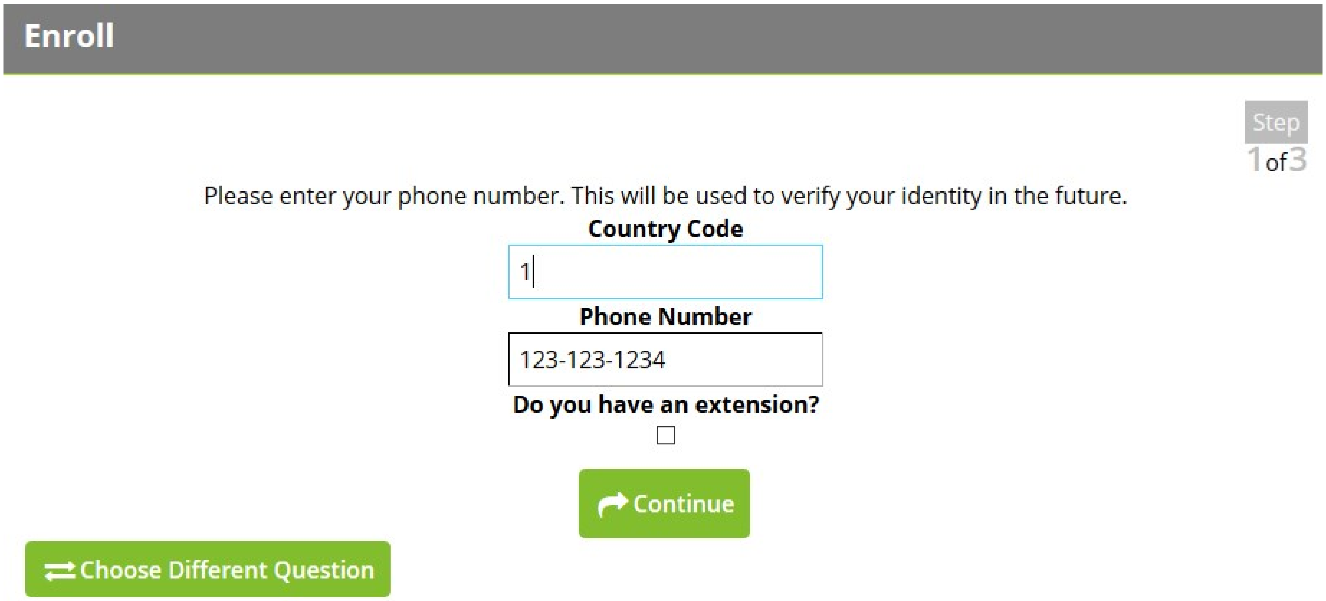
Enrollment 0/3



Enroll

Step 2 of 3

Please select two question boxes to reveal your security images. Remember these images for resetting your password.



Enroll

Step 1 of 3

Please enter your phone number. This will be used to verify your identity in the future.

Country Code

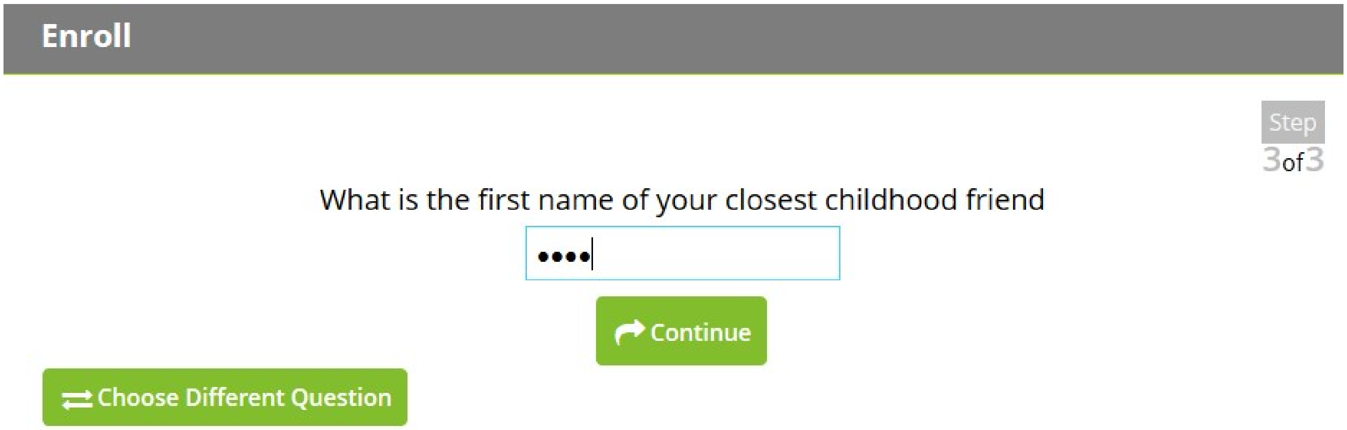
1

Phone Number

123-123-1234

Do you have an extension?

□



Enroll

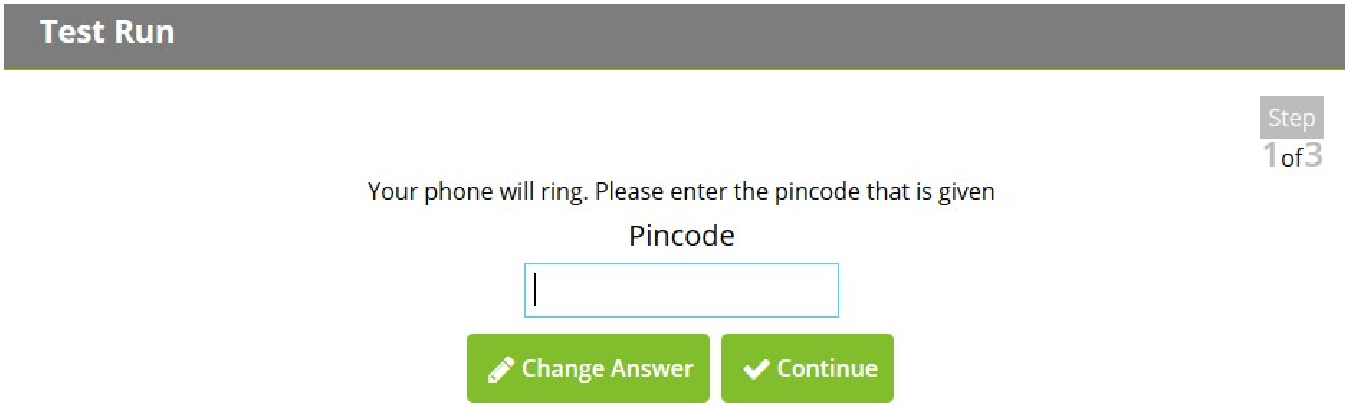
Step 3 of 3

What is the first name of your closest childhood friend

••••

Test Run

Next, you may be prompted to go through a test run.



Test Run

Step 1 of 3

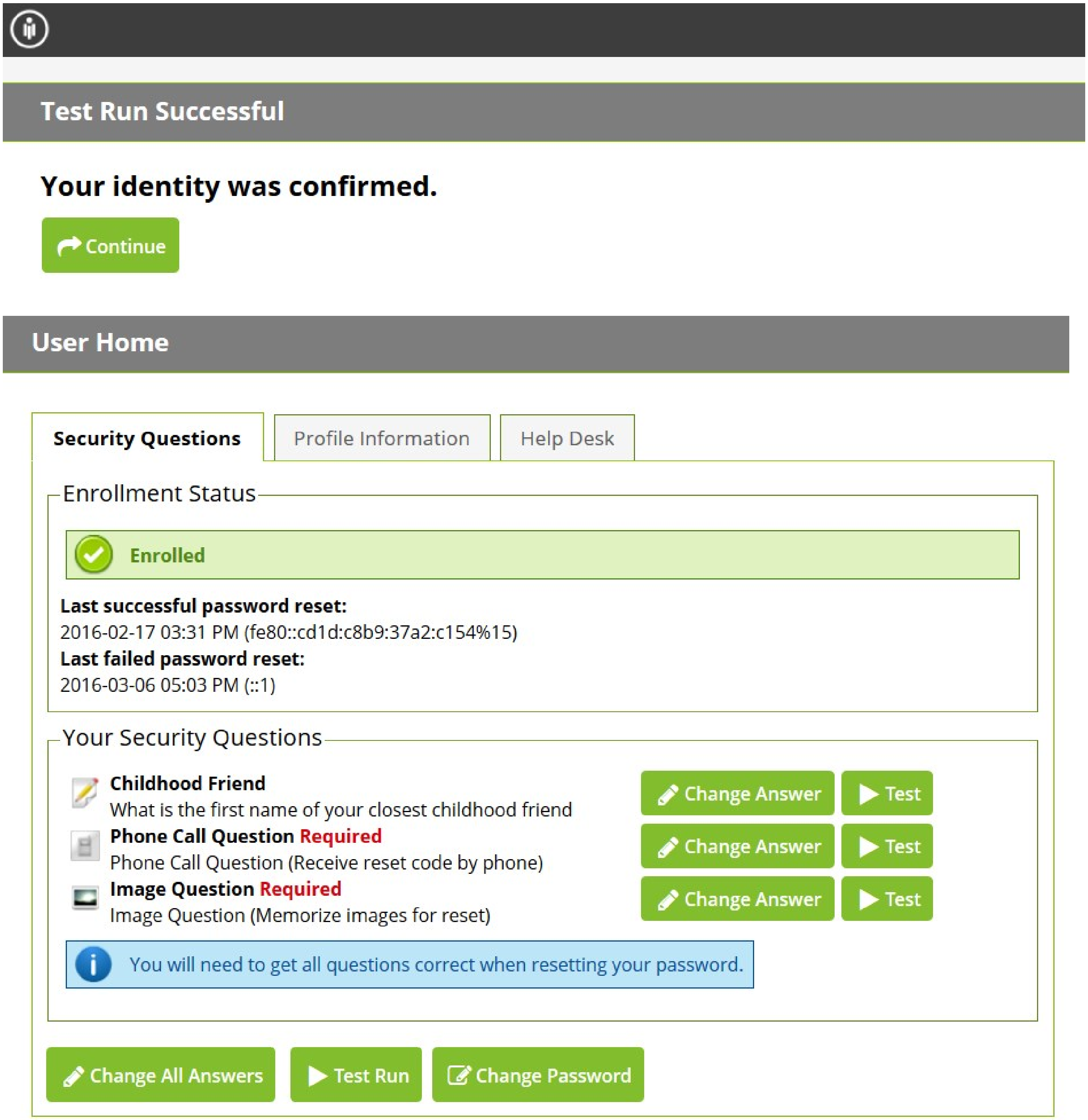
Your phone will ring. Please enter the pincode that is given

Pincode

Note: If you forget the answer to any question during the test run, you can change the answer by clicking the **Change Answer** button.

Confirmation

After successfully completing the test run, your identity will be confirmed and you will be enrolled in Password Reset Server.



Test Run Successful

Your identity was confirmed.

User Home

Enrollment Status

Enrolled

Last successful password reset:
2016-02-17 03:31 PM (fe80::cd1d:c8b9:37a2:c154%15)
Last failed password reset:
2016-03-06 05:03 PM (::1)

Your Security Questions

Childhood Friend
What is the first name of your closest childhood friend

Phone Call Question Required
Phone Call Question (Receive reset code by phone)

Image Question Required
Image Question (Memorize images for reset)

You will need to get all questions correct when resetting your password.

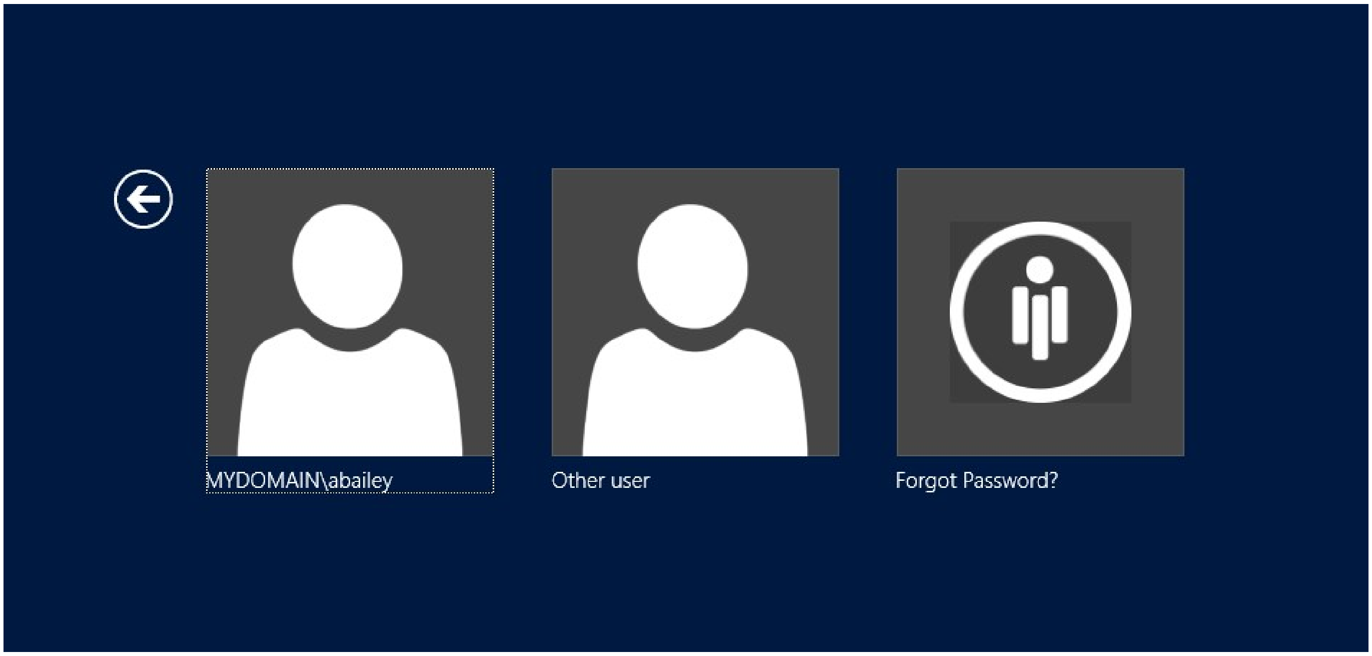
Note: At this screen you will be able to see your security questions and change your answers.

This section contains the steps on how to change your password in Password Reset Server.

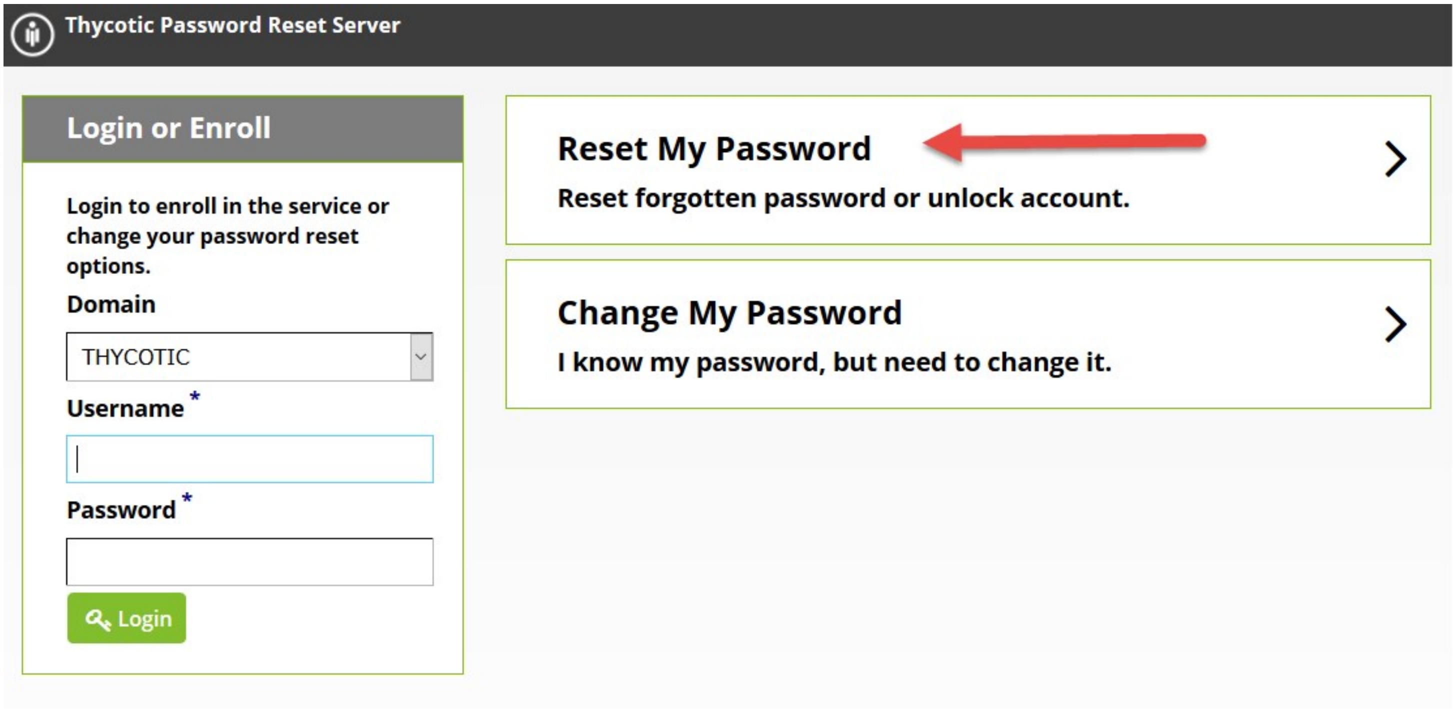
- Getting Started
- Answering Security Questions
- Confirmation
- Offline Reset

Getting Started

To begin you can click on the **Forgot Password** button on the windows login screen.



You can also reset your password through the web interface by going to the Password Reset Server URL (*see system administrator) and clicking the **Reset Password** button. You may receive reminder emails when your password is going to expire.



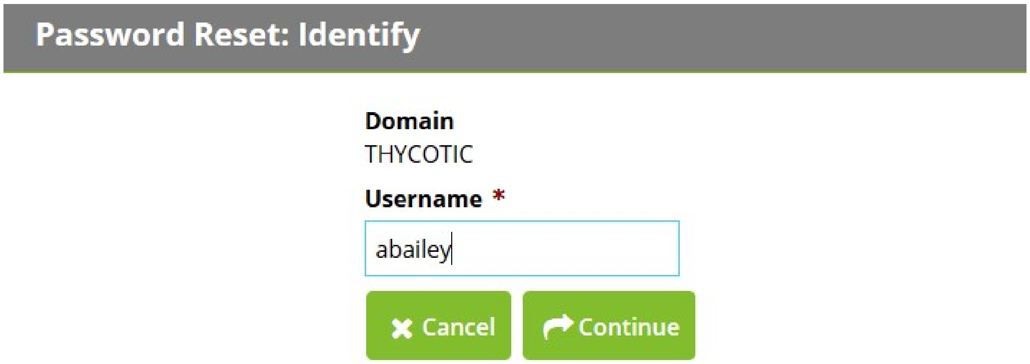
Login to enroll in the service or change your password reset options.

Reset forgotten password or unlock account.

I know my password, but need to change it.

Answering Security Questions

Enter your username.

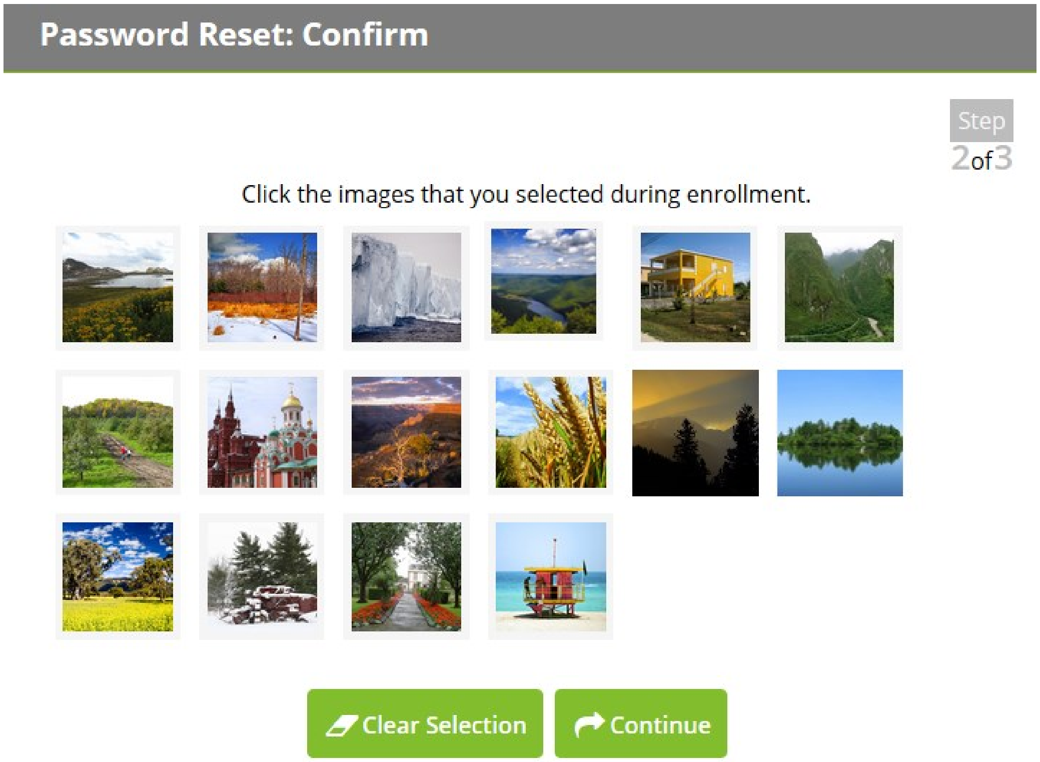


Password Reset: Identify

Domain
THYCOTIC

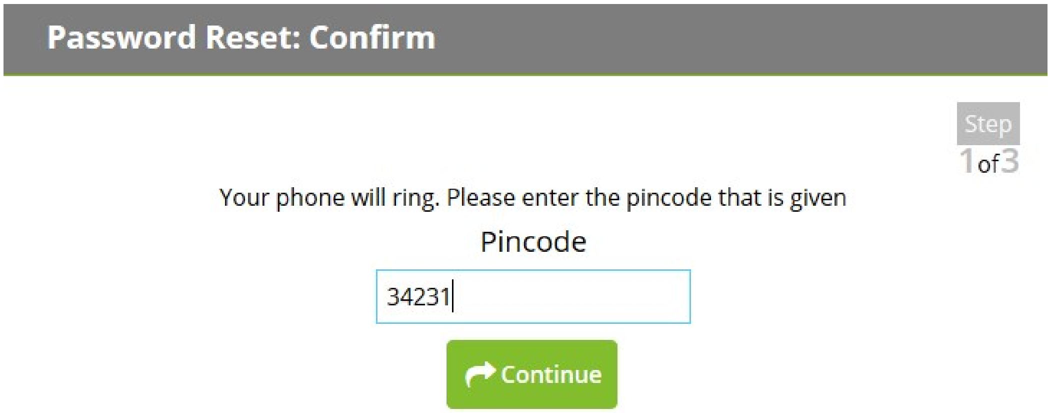
Username *
abailey

Provide the answers to the security questions as they appear.



Password Reset: Confirm

Click the images that you selected during enrollment.



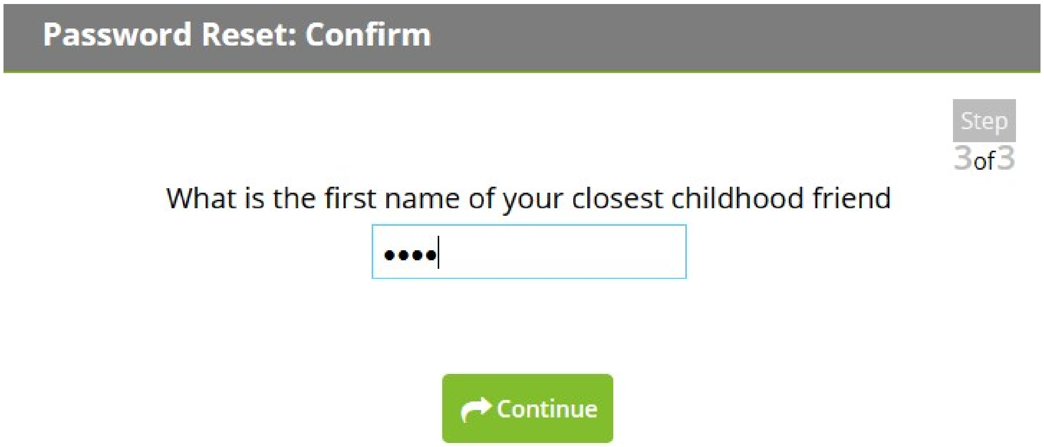
Password Reset: Confirm

Step 1 of 3

Your phone will ring. Please enter the pincode that is given

Pincode

34231



Password Reset: Confirm

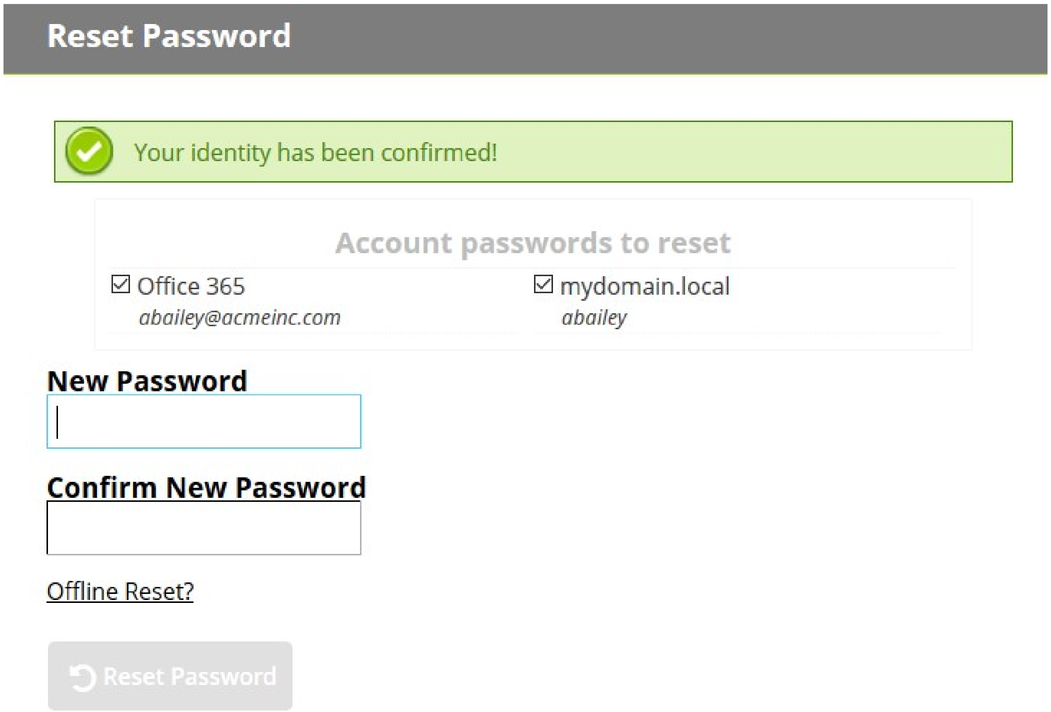
Step 3 of 3

What is the first name of your closest childhood friend

••••

Confirmation

After you have successfully answered your security questions, you will be prompted to create a new password. If your administrator has allowed the option, you will also be able to unlock your account without resetting your password. If your account has been configured to allow reset of password in multiple systems, you can select the systems on which you would like to reset your password.



Reset Password

Your identity has been confirmed!

Account passwords to reset

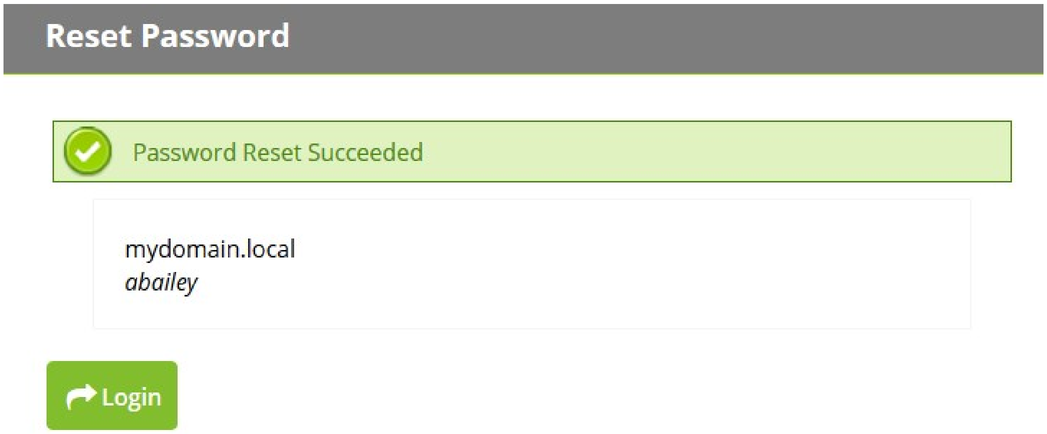
☑ Office 365
abailey@acmeinc.com

☑ mydomain.local
abailey

New Password

Confirm New Password

Once your password has been changed, close the window by clicking the **X** button in the top-right corner of the window.



Reset Password

Password Reset Succeeded

mydomain.local
abailey

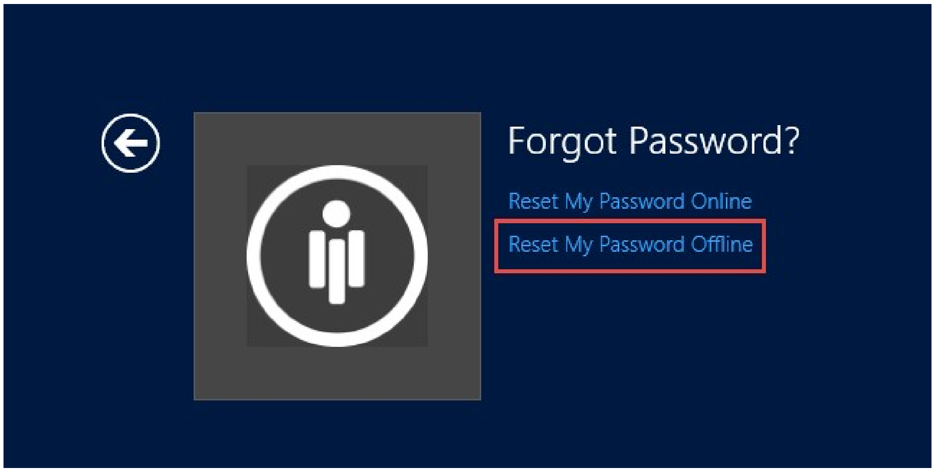
Log in to your account using the new password you created.

Offline Reset

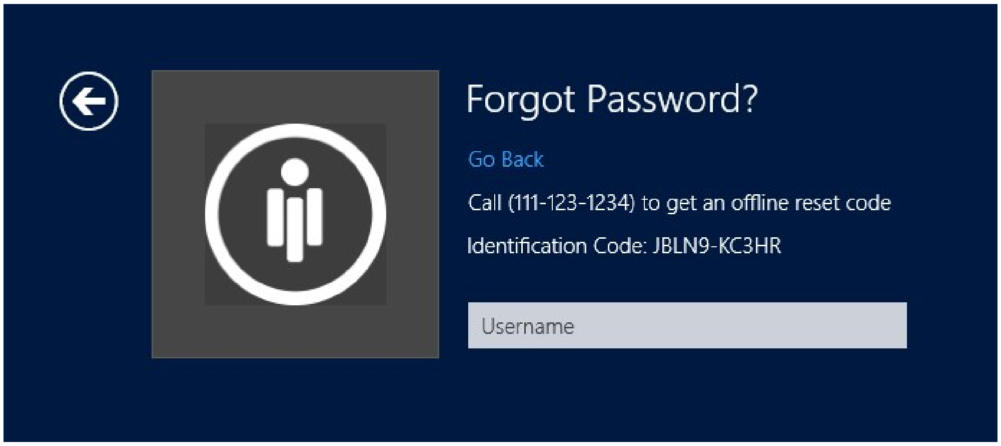
Offline password reset allows you to reset your password when you are traveling or not connected to the company domain.

To reset your password on your computer you will first need a reset code. You can get your reset code by either calling the help desk, or logging into the password reset server portal through your smartphone or an internet connected computer.

To start the offline reset, click the Forgot Password icon on your computer logon screen and click **Reset My Password Offline**



You will be given an identification code to provide to the help desk or the Password Reset Server website.



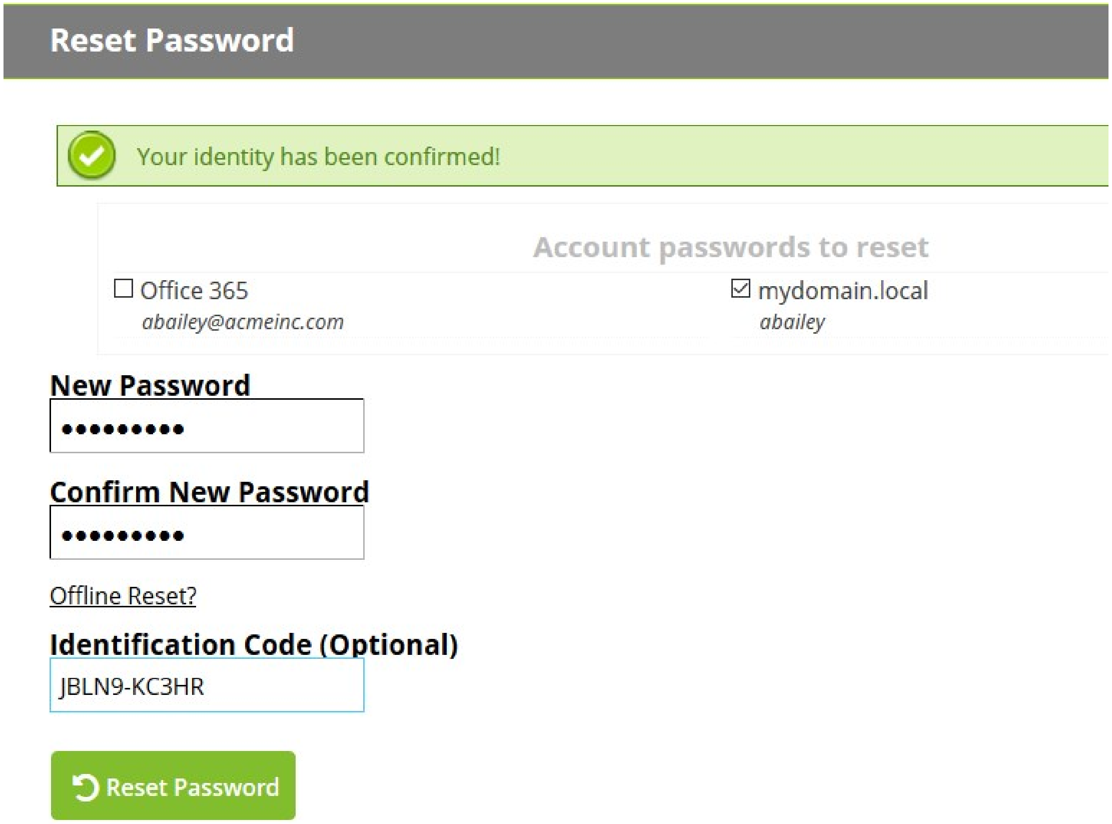
Call (111-123-1234) to get an offline reset code

Identification Code: JBLN9-KC3HR

You can either call the help desk to get your offline reset code, or answer your reset questions by navigating to the Password Reset Server website from your phone or an internet connected computer.

Web Portal

After answering your reset questions, expand the offline reset link to put in your identification code.



Reset Password

Your identity has been confirmed!

Account passwords to reset

☐ Office 365
abailey@acmeinc.com

☑ mydomain.local
abailey

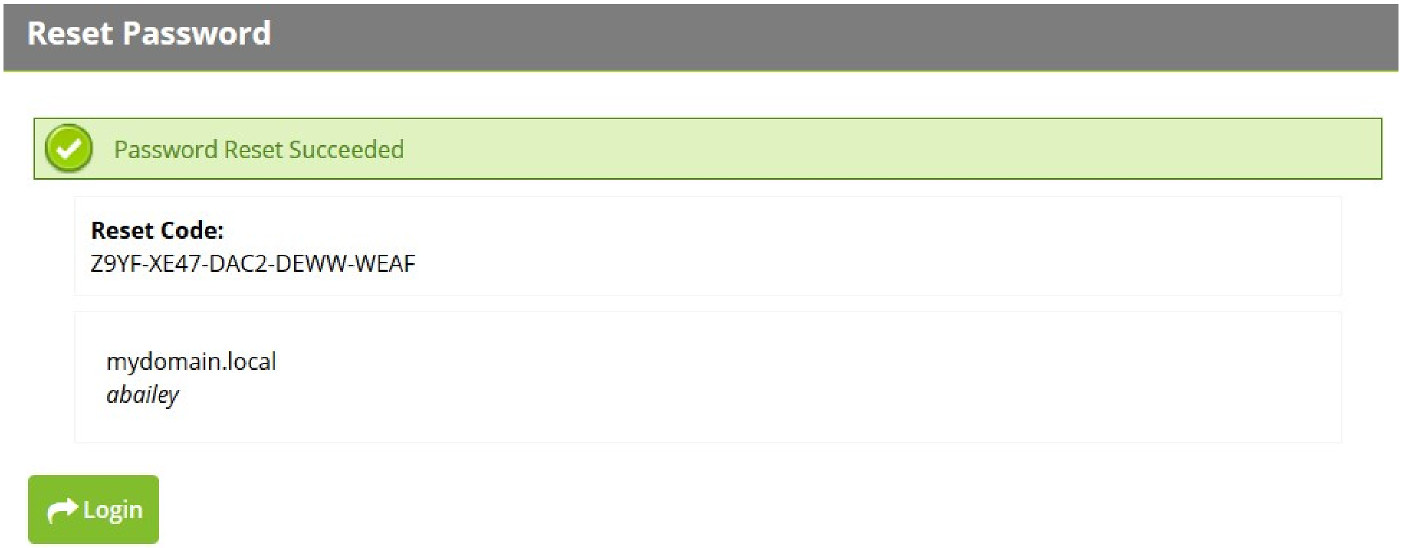
New Password: •••••••••

Confirm New Password: •••••••••

Offline Reset?

Identification Code (Optional): JBLN9-KC3HR

You will be given a reset code



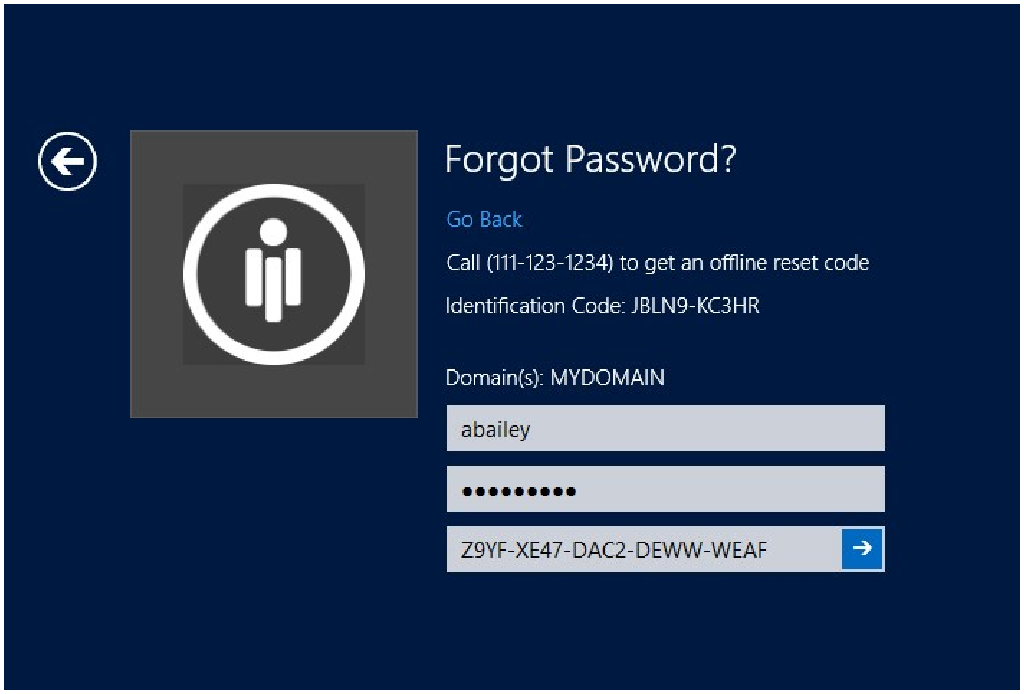
Reset Password

Password Reset Succeeded

Reset Code:
Z9YF-XE47-DAC2-DEWW-WEAF

mydomain.local
abailey

Enter the reset code into the windows logon screen along with your new password



Forgot Password?

Go Back

Call (111-123-1234) to get an offline reset code

Identification Code: JBLN9-KC3HR

Domain(s): MYDOMAIN

abailey

●●●●●●●●●●

Z9YF-XE47-DAC2-DEWW-WEAF

After changing your password you will be able to log in as normal.

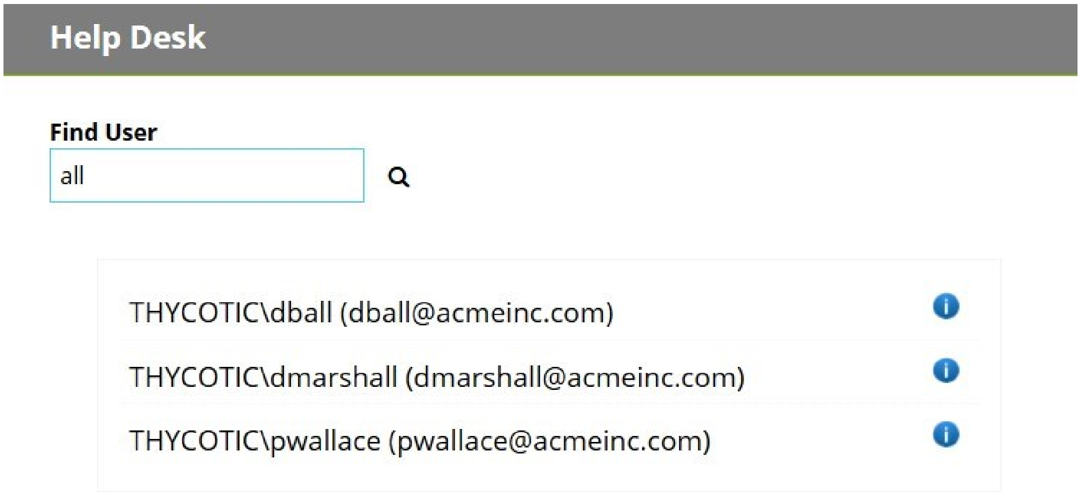
Help Desk Guide

Any user who is assigned to a help desk on a security policy will have access to the help desk interface of Password Reset Server. A user can be placed in the help desk of multiple security policies, and they will be able to reset the password of any user in all policies that they are assigned to.

Note: The local administrator account will not be assignable to any help desk and will not have access to the help desk functionality.

Using Help Desk

First, log into Password Reset Server with your Active Directory credentials by clicking **Enroll** from the main Password Reset Server page. Search for a user by typing in the **Find User** search field. You can search by a user's display name or email address. Select a user from the results and you will be taken to the page where you can select which password sources you wish to change.



Help Desk

Find User

all

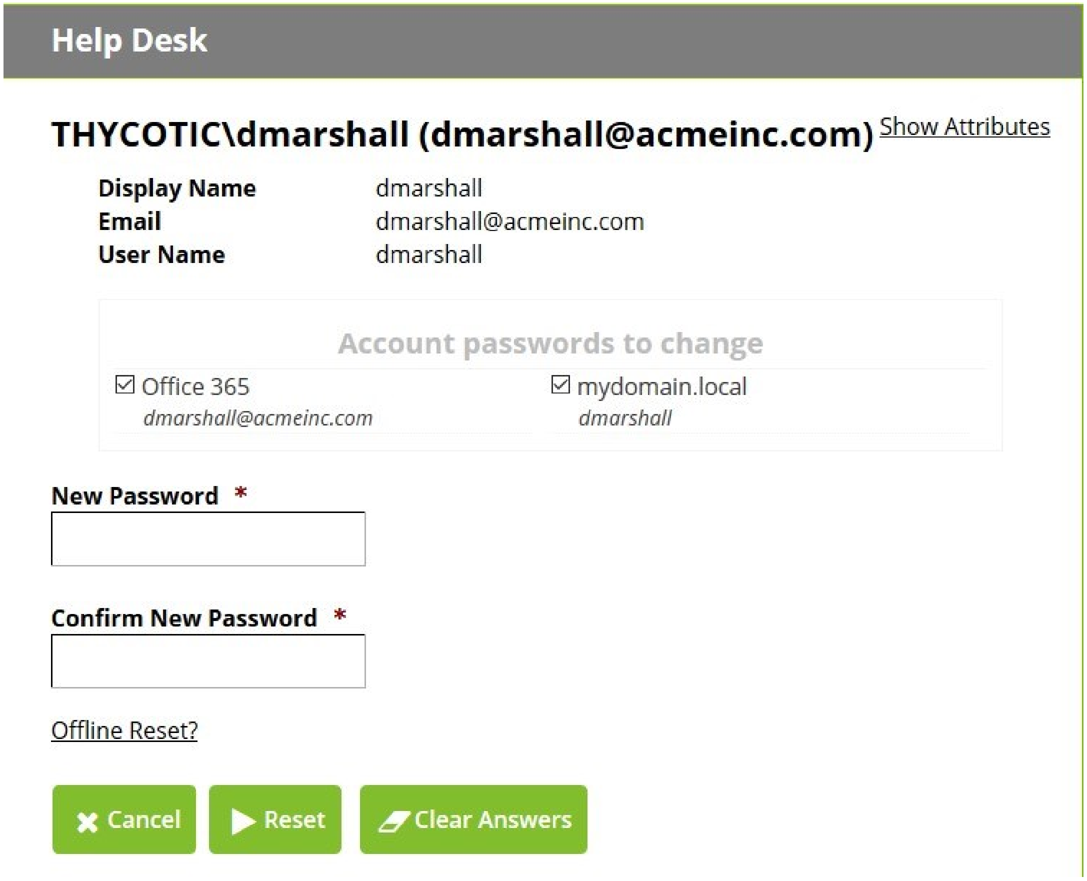
THYCOTIC\dball (dball@acmeinc.com)

THYCOTIC\dmarshall (dmarshall@acmeinc.com)

THYCOTIC\pwallace (pwallace@acmeinc.com)

Click **Reset** to reset the user's password. Click **Clear Answers** to make the user re-enroll. Click **Cancel** to return to the previous page. Any synced Active Directory attributes will be displayed for a user to act as an identity verification after clicking **Show Attributes**.

Note: If you would like additional attributes to be displayed, please contact your Password Reset Server administrator.



Help Desk

THYCOTIC\dmarshall (dmarshall@acmeinc.com) Show Attributes

Display Name	dmarshall
Email	dmarshall@acmeinc.com
User Name	dmarshall

Account passwords to change

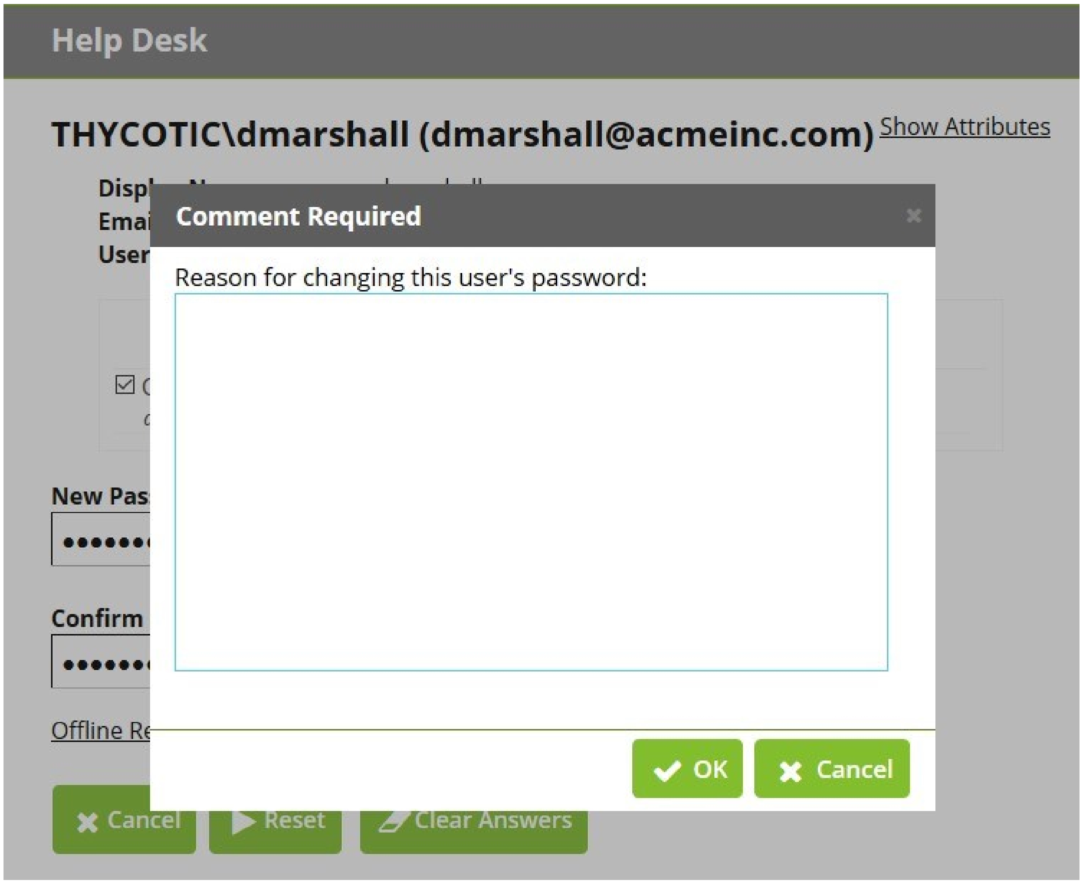
☑ Office 365 *dmarshall@acmeinc.com*

☑ mydomain.local *dmarshall*

New Password *

Confirm New Password *

When attempting to reset a password through this screen, the help desk user will be prompted for a comment which will be added to Password Reset Server reports.



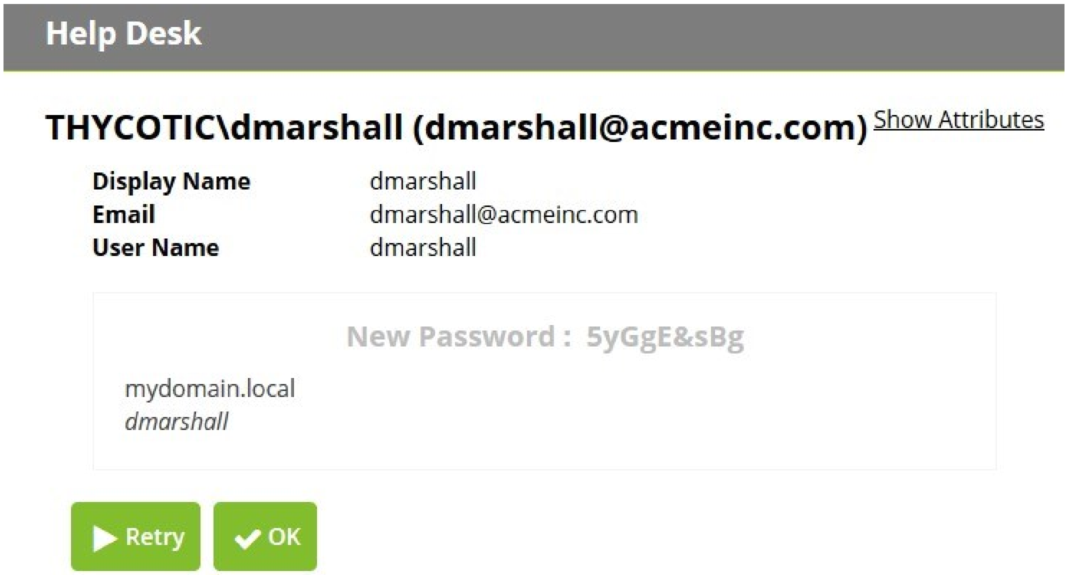
Help Desk

THYCOTIC\dmarshall (dmarshall@acmeinc.com) Show Attributes

Comment Required

Reason for changing this user's password:

After a user's password is reset by the help desk, the help desk user can read the user their new passwords. When the user next logs in, they will be forced to change their password.



Help Desk

THYCOTIC\dmarshall (dmarshall@acmeinc.com) Show Attributes

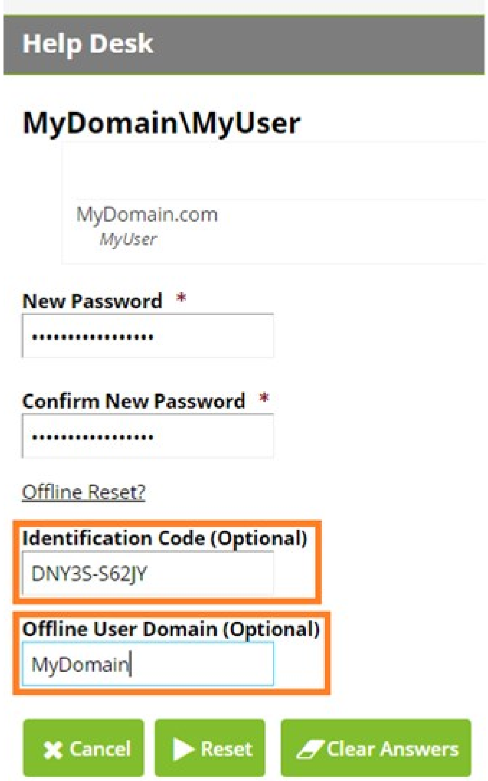
Display Name	dmarshall
Email	dmarshall@acmeinc.com
User Name	dmarshall

New Password : 5yGgE&sBg

mydomain.local
dmarshall

If a user's machine is not connected to the corporate domain they won't be able to perform a standard reset and use the new password on the domain. In order to reset their password on their machine they need to do an offline reset.

Each machine with the Password Reset Server Windows Login Integration will have an Identification Code that will need to be provided to the help desk use. Enter this Identification Code into the Help Desk reset process to get a reset code.



Help Desk

MyDomain\MyUser

MyDomain.com
MyUser

New Password * ••••••••••••••••

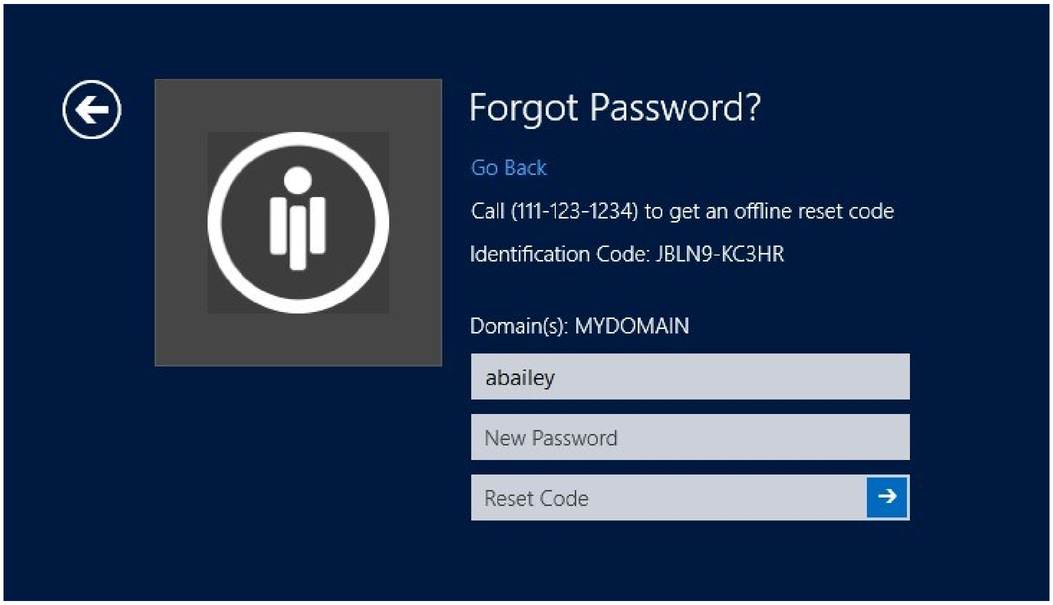
Confirm New Password * ••••••••••••••••

Offline Reset?

Identification Code (Optional): DNY3S-S62JY

Offline User Domain (Optional): MyDomain

The Offline Reset User Domain needs to match what the user's domain is shown as in the Windows Login Integration.



Forgot Password?

Go Back

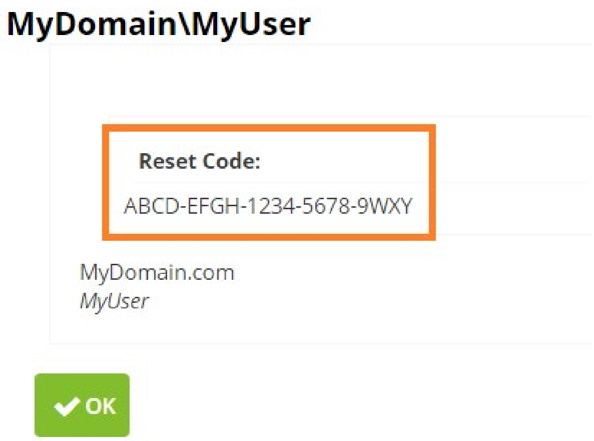
Call (111-123-1234) to get an offline reset code

Identification Code: JBLN9-KC3HR

Domain(s): MYDOMAIN

abailey

After resetting the user’s password on the domain, give them the reset code which they can enter along with their new password.


MyDomain\MyUser

Reset Code:

ABCD-EFGH-1234-5678-9WXY

MyDomain.com

MyUser

Syslog Integration

Leveraging Password Reset Server event data with SIEM and Log Management solutions can give organizations insight into self-service reset attempts by users, and potentially malicious attacks on usernames.

Note: Terminology used in this document is based on the SANS Glossary of Security Terms, available at http://www.sans.org/security-resources/glossary-of-terms/

Table 1 is a complete list of events in Password Reset Server's Syslog. Both the Event Name and Event ID are contained in the log as well as the data fields that apply to the event.

Table 2 is a complete list of data fields in Password Reset Server's Syslog. Only Data Fields relevant to the Event ID are included in the log. Some log entries may differ in terms of their field content, see examples below.

Example Event 1

In this event, a user has started the reset process:

```
May 15 09:39:55 THY364 CEF:0\|Thycotic Software\|Password Reset
Server\|4.1.000001\|10007\|USER - START RESET\|2\|msg=[PasswordResetServer]
Event: [User] Action: [Start Reset] By User:
test.thycotic.com\\\\THYCOTICTESTUSER Item Name:
test.thycotic.com\\\\THYCOTICTESTUSER Details THYCOTICTESTUSER suid=173
suser=test.thycotic.com\\\\THYCOTICTESTUSER cs4= duser=
test.thycotic.com\\\\THYCOTICTESTUSER duid=173 fname=
test.thycotic.com\\\\THYCOTICTESTUSER fileType=User fileId=173 src=::1 rt=May 15
2015 09:39:55
```

Example Event 2

In this event, an administrator has edited a report.

```
May 15 09:29:12 THY364 CEF:0\|Thycotic Software\|Password Reset
Server\|4.1.000001\|10003\|REPORT - REPORT_EDIT\|2\|msg=[PasswordResetServer]
Event: [Report] Action: [Report Edit] By User: admin Details User Param suid=1
suser=admin cs4= src=::1 rt=May 15 2015 09:29:12
```

Table 1

System Log	500
USER - CREATE	1
USER - DISABLE	2
USER - ENABLE	3
USER – LOCKOUT	4

USER - ADDEDTOGROUP	5
USER - REMOVEDFROMGROUP	6
FOLDER - CREATE	7
FOLDER - DELETE	8
ROLE - CREATE	9
ROLE - ASSIGNUSERORGROUP	10
ROLE - UNASSIGNUSERORGROUP	11
ROLEPERMISSION - ADDEDTOROLE	12
ROLEPERMISSION - REMOVEDFROMROLE	13
FOLDER - EDITPERMISSIONS	14
CONFIGURATION - EDIT	15
USER - LOGIN	16
USER - LOGOUT	17
USER - LOGINFAILURE	18
USER - PASSWORDCHANGE	19
AD_ATTRIBUTE – ATTRIBUTE_CHANGE	10001
AD_ATTRIBUTE – SETTING_CHANGE	10002
REPORT - REPORT_EDIT	10003
REPORT - REPORT_RENAME	10004
REPORT - REPORT_CREATE	10005
USER - USER_IMPORTANSWER	10006
USER - START RESET	10007
USER - RESET SUCCESS	10008
USER - RESET FAILURE	10009
USER - UNLOCK FAILURE	10010

USER - UNLOCK SUCCESS	10011
USER - RESET UPDATE SUCCESS	10012
USER - RESET UPDATE FAILURE	10013
REPORT - REPORT_DELETE	10014
LICENSING - LICENSING INVALID	10015
USER - HELP DESK RESET UPDATE SUCCESS	10016
USER - HELP DESK RESET UPDATE FAILURE	10017

Table 2

User ID being viewed or changed	duid
User name being viewed or updated	duser
User ID of user performing action	suid
Username of user performing action *	suser
Description of audit action	msg
Current Version of Password Server	Version
Human readable name of event	Name
The Priority of event	Priority
Name of company	Vendor
Name of product	Product
Description of audit action	Message
Time of event	rt
IP Address of client machine	src
Name of item action was taken on	fname
Type of item action was taken on	fileType
ID of item action was taken on	fileId

Name of Role modified	cs1
"Role"	cs1label
Name of User or Group added to role	cs2
"Group" or "User"	cs2label
Name of Folder containing Secret	cs3
"Folder"	cs3label
Display name of user performing action *	cs4
"suser Display Name" *	cs4label

Disaster Recovery

Disaster Recovery is a primary concern of nearly every System Administrator. Establishing a set of procedures to recover data from (or maintain operations during) failing hardware, natural disasters, or unforeseen circumstances is a requirement in most businesses and institutions. Password Reset Server can help System Administrators by storing and securing critical infrastructure data including admin-level credentials and important documents or files. Password Reset Server has several features specifically designed to aid restore processes as well as methods for achieving business continuity during disaster scenarios.

Note: This document is designed to assist System Admins to integrate Password Reset Server with their Disaster Recovery Plan. Electrical, connectivity, and similar concerns are out of the scope of this document. The assumptions made below are not intended to fit every situation, merely to serve as a guide for Password Reset Server administrators.

Password Reset Server Disaster Recovery Features

There are many factors to a solid disaster recovery plan. Physical hardware, network connectivity, power requirements, Operating System configuration, and similar concerns are out of the scope of Password Reset Server. However, Password Reset Server can help with the management of and access to the user answers saved in the application database. It is worth noting that Password Reset Server performs well in virtual environments, integrating Password Reset Server into your virtualization solution is recommended.

This is a complete list of Disaster Recovery Features built in to the Password Reset Server application.

- Manual Web Application Backup
- Manual Application Database Backup
- Automated Application Database Backup
- Automated Web Application Backup
- Microsoft SQL Mirroring

Manual Web Application Backup

This is a configurable "one-click" process that creates a backup of the folder containing of the Password Reset Server application. Using this file in conjunction with a valid Password Reset Server Application Database, functionality can typically be restored in less than 30 minutes.

Manual Application Database Backup

This is a configurable "one-click" process that creates a backup of the Password Reset Server Application Database. Restoring this database backup and reconnecting the web application to the database typically requires less than 30 minutes (depending on the size of the database being restored).

Automated Web Application Backup

This is a scheduled version of the Manual Web Application Backup feature. This can be automated in conjunction with the backup of the Application Database.

Automated Application Database Backup

This is a scheduled version of the Manual Application Database Backup feature. This can be automated in conjunction with the backup of the Web Application.

Microsoft SQL Mirroring

Password Reset Server support Synchronous and Asynchronous mirroring in Microsoft SQL Server. Log File Shipping is not supported in Password Reset Server.

Maintaining Password Reset Server in a Disaster

The framework of a solid Password Reset Server Disaster Recovery Plan should follow these methods of maintaining operations. Thycotic Software recommends geographic redundancy when and where economically feasible. Multiple sites are not required by any means, but work to ensure network, power and hardware replication between Password Reset Server instances.

Password Reset Server can operate on typical modern servers and even workstations in the simple configurations without requiring high-end hardware.

Password Reset Server System Requirements

By design, Password Reset Server's installation is a quick and easy process. Keeping the installation process quick and easy was a goal from the very first release of Password Reset Server (as a security product it should be very easy to upgrade should security fixes need to be applied). This serves as a viable fallback option should redundancy plans fail. In a worst-case scenario where the host server fails, a mirror fails, and the other backup plans fail, Password Reset Server can be installed from scratch quickly and data imported from various methods. Users familiar with Microsoft SQL and IIS can typically install Password Reset Server in about 30-45 minutes on a prepared server.

Review the installation guides on our Support page.

Password Reset Server natively supports local and network backups. By configuring locations for the application folder and Microsoft SQL database, Password Reset Server backs up this data based on a highly-configurable user-defined schedule with detailed logging. Please refer to the following documentation for Automated Backup configuration:

Backing up to a Network Share

Backup Configuration File Path Settings

Manual Backup Procedures

Restoring Password Reset Server's web application folder is as simple as copying the contents of the last available zipped backup file back into folder. Microsoft SQL database restores are simple as well but require several steps depending on the backup scenario.

Password Reset Server supports Synchronous/Asynchronous Microsoft SQL Mirroring. Mirroring database instances is an important part of any high-availability Business Continuity Plan. Adding geographic redundancy to this plan is recommended for customers with multiple sites, for that added layer of protection. To use a mirrored database with Password Reset Server, ensure that the Failover Partner is set in the database configuration installation step.

See the Microsoft documentation here.

Disaster Recovery Recommendations

When using a configuration without multiple servers, making frequent backups is the best solution. However, using a virtual server is the preferable choice when using the single server approach. Virtual servers allow the System Administrator to make a full backup of the server in addition to backups within Password Reset Server. They also allow for the server to be transferred to different hardware quickly. Regardless of using a physical server or virtual server, suggestions for Disaster Recovery Plans are listed below.

Make frequent (at least daily) backups. Password Reset Server supports creating backups manually and on a schedule. To make a backup within Password Reset Server, login in as an Administrator. Then, click on Administration > Backup. Choose a location for the backup.

Note: In single server configurations, it is highly recommended to save the backup files for Password Reset Server on a different device. This will isolate sensitive files from a hardware failure on that server.

When restoring from backup in the single-server configurations, be certain to make copies of the Password Reset Server backup files on a different device or media.

Start by preparing a server for installation as the Installation Guide instructs. When the server is prepared, restore the application and database. This guide below will explain the procedure of restoring the database. Some specific web configurations may be needed to match the previous IIS settings. If you are unable to restore Password Reset Server after following these steps, please contact Technical Support. It is recommended to configure a second server or Virtual Machine after setting up the primary server. Then the process of restoring from the Password Reset Server backups is simply a matter of copying the files to the pre-configured server and restoring them.

Moving the location of the database to a different server adds an additional layer of reliability.

Password Reset Server supports several features that allow the uninterrupted operation of the application. Using Microsoft SQL Mirroring, the Password Reset Server Application Database can be automatically replicated to a second database server. Make use of multiple servers when logistically and economically feasible.

Use mirroring if at all possible. Mirrored databases are a reliable method of maintaining operations when servers fail. Password Reset Server supports both Asynchronous and Synchronous Mirroring. However, Log File Shipping is not supported. To enable Microsoft SQL Mirroring in Password Reset Server, use the following article:

Microsoft SQL Server Mirroring

The Web Application does not support clustered installations at this time. The recommended configuration is to configure a secondary web server and copy over a production backup of the Password Reset Server application folder and configure the site. Once it is pointed at the mirror, the site can be switched off in IIS. If the primary web server goes down, then an application backup can be restored onto the pre-configured server and the site enabled. Since it would be pointing to a mirror, there would be no need to restore a database backup in this scenario thus reducing downtime.

Summary

The integration of Password Reset Server into our customers' Business Continuity Planning should not present any unique challenges beyond normal server and database recovery. If your organization already has DR plans for servers and databases, Password Reset Server and its Microsoft SQL database should fit within your organization's current framework. Using server virtualization to assist with Business Continuity and Disaster Recovery in terms of snapshots, replication, and other 3rd party features are recommended where applicable.

API Guide

Password Reset Server provides web services to allow for 3rd party developers to interact with Password Reset Server in a developer-friendly way while maintaining security.

The web services use a standard messaging format called Simple Object Access Protocol (SOAP for short). SOAP is an XML based message exchange protocol to exchange information over a standard HTTP connection.

Password Reset Server is built using version 1.2 of the SOAP protocol.

For technical details of the SOAP protocol, please refer to the W3C here.

Accessing Web Services

Password Reset Server's web services can be accessed with the following URL:

http://yourpasswordresetserverinstallation/webservices/webservice.asmx

For getting the WSDL definition, append *?wsdl* to the end of the URL:

http://yourpasswordresetserverinstallation/webservices/webservice.asmx?wsdl

Concepts

Password Reset Server requires the use of a token for most of the web service methods. A token can be acquired using the Authenticate methods.

This token is then passed to other web service methods that require it. The token contains information from when it was initially acquired, such as the date it was created for expiration purposes. Password Reset Server verifies that the token is still valid on the web service methods that use it.

The token should be persisted to storage if authentication sessions go beyond the lifetime of your application. If the token is no longer valid, you must re-authenticate to acquire a new token.

Password Reset Server web service methods that can fail will return a web service type that includes an Errors property, which is a collection of strings. If there is one or more string in the Errors collection, the service method is assumed to have failed. The Errors collection contains details of the nature of the failure.

For service methods that return a type without an Errors property, the service method should succeed in all cases unless otherwise noted.

Web service methods, which require a token, may return the following error in addition to web service specific errors.

- "Bad token."
  The token is no longer valid.

Web Service Methods

This method is used to authenticate a username and password, and gives a token if the authentication was successful.

Return Type

Token

Parameters

- domain
  Type: string
  Required: no
  The domain, if attempting to authenticate using a domain account. For non-domain accounts, passing null, empty string, or "(local)" indicates it is not a domain account.

- username
  Type: string
  Required: yes
  The username for authentication.

- password
  Type: string
  Required: yes
  The password for authentication.

Errors

- "Login failed."
  The credentials specified are not valid, or the account is disabled, or locked out.

This method is used to automatically fill out a question for a user. It allows enrollment to happen automatically.

ReturnType

WebServiceResult

Parameters

- token
  Type: string
  Required: Yes
  The authentication token returned by the Authenticate method.

- domain
  Type: string
  Required: Yes
  Domain of the user to enroll for this question.

- username
  Type: string
  Required: Yes
  User to enroll for this question.

- questionName
  Type: string
  Required: Yes
  Question to enroll the user for.

- answer
  Type: string
  Required: Yes
  Answer for the question the user is being enrolled in.

- countryCode
  Type: string
  Required: No
  Code for the country – used by Phone and SMS questions.

- extension
  Type: string
  Required: No
  Optional extension for Phone questions.

Errors

- "The user needs Administer Users and Bulk Import Answers permissions."
  The user whose token is being used for the question import does not have the Administer Users or Bulk Import Answers permissions. Assign these permissions on the Role Assignment or Role Edit pages under Administration > Roles.

This method is used to check whether a particular user has successfully enrolled.

Return Type

bool

Parameters

- domain
  Type: string
  Required: no
  The domain of the user to check.

- username
  Type: string
  Required: yes
  The username of the user to check the enrollment status of.

Web Service Types

WebServiceResult is a generic result that does not return any information except Errors.

Members

- Errors
  Type: string array
  SOAP Type: ArrayOfString. A complex type of a sequence of strings with an unbounded number of occurrences.
  One or more errors that occurred during the operation.

Troubleshooting

Administrators can enable end-to-end encryption with the SQL database by using an Encrypted connection. This is a feature that is built into Microsoft SQL Server and Password Reset Server supports. It can be enabled in the 2nd step of the installer by checking the "Enable Encryption" check box.

SQL Server must be pre-configured to support encryption. This Microsoft TechNet article explains how to configure the SQL Server environment for encryption:

http://technet.microsoft.com/en-us/library/ms191192.aspx

Login failed for user

A severe error occurred on the current command. The results, if any, should be discarded.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Login failed for user. A severe error occurred on the current command. The results, if any, should be discarded.

This sudden failure may be because the "Enforce Password Expiration" setting is turned on for the SQL Login Account for Secret Server. In SQL Server Management Studio, turn off this setting by right clicking and selecting "Properties" on the user under the "Security\Logins" folder. On the properties page, uncheck the "Enforce password expiration" checkbox and save.

Performance issues

Note that using this setting can adversely affect performance. http://technet.microsoft.com/en-us/library/ms189067.aspx

There are two file path settings on the Admin > Backup page (ConfigurationBackup.aspx). The "Backup File Path" setting corresponds to the application backup. The "Backup Database Path" setting corresponds to the SQL server backup.

Generally, the "Backup File Path" setting can be set to a path local to the application server for backing up of application files. If Secret Server is running under an account that does not have permission to write to a local path, then a network share can be used.

If the SQL server is located on the same server as the web application server, the "Backup Database File Path" setting can be set to a local path. If the SQL server is not located on the same server as the web application server then a network share should be used. The account under which SQL server service is running either must have modify rights to that path or must be a member of a group with modify rights to that path. You must use UNC (Universal Naming Convention) notation to write to a network path (ie. \TESTVM0\c$\backupDirectory).

If you are getting an error stating "Cannot open backup device. Operating system error 3", this is often due to an invalid path value.

If you see an error similar to below, then the machine running Password Reset Server is having trouble using the Password Reset Server database:

This error is caused when Password Reset Server tries to a run a database query, but the query times out before completion. To diagnose the issue, please follow these steps:

- Check the task manager on the machine running your Password Reset Server database. Make sure no process is taking up too much ram or CPU power. If it is, stop the process or move the Password Reset Server database to another machine.
- Check the hard drive space on the machine running your Password Reset Server database. Make sure there is at least 3 gigabytes of free space.
- Try restarting the SQL Service.

Password Reset Server supports setting up the database in a disaster recovery environment by using Microsoft SQL AlwaysOn or the mirroring capabilities in SQL Server 2005 and SQL Server 2008. This allows you to have a copy of your Password Reset Server database on another server and automatically start using the backup server should your primary database server fail.

Click here for a detailed guide to configuring Password Reset Server for database mirroring:

Windows 7

- Run services.msc and ensure Windows "Management Instrumentation" service Startup Type is set to Automatic.
- In Firewall settings, click on the "Advanced settings" link. For the Inbound Rules, ensure "Windows Management Instrumentation (WMI-In)" is Enabled and Allowed for the Profile called Domain.

Vista

- Run services.msc and ensure "Windows Management Instrumentation" service Startup Type is set to Automatic.
- In Firewall settings, click on the "Change Settings" link. In the Windows Firewall Settings dialog, click the Exceptions tab. Enable the "Windows Management Instrumentation (WMI)" exception.

Windows XP

- Run services.msc and ensure "Windows Management Instrumentation" service Startup Type is set to Automatic.
- From the command prompt, run the following command: "netsh firewall set service RemoteAdmin enable"
- From the command prompt, run the following command: "netsh firewall add portopening protocol=tcp port=135 name=DCOM_TCP135"
- From the command prompt, run the following command: "netsh firewall set portopening tcp 445 smb enable"

In Password Reset Server, email addresses used for password expiration notifications and enrollment reminders are retrieved from Active Directory. When you enter a domain and perform a synchronization, Password Reset Server will create all users that exist in AD and use their AD email addresses. If an email address in Password Reset Server appears as blank, this means the email address is also blank in Active Directory.

To fix this, an administrator can edit the user in Active Directory, add an email address, and then force a synchronization or wait for a scheduled synchronization to occur. To force synchronization in PRS, an admin can log in through the web portal, click on "Administration", then on "Domain Configuration", and click "Synchronize Now".

This error occurs when too much data is sent to the server on a request. This can be caused by a large file attachment.

To fix this, first locate the page on which this occurred. Then, edit the web.config file that exists in your Password Reset Server installation directory. Next, search for the tag that contains the page on which the error occurred. For example, if you received this error on the CreateUser.aspx, you would want to look for the following section:

```
<location path="CreateUser.aspx">
        <system.web>
            <authorization>
                <allow users="*"/>
            </authorization>
        </system.web>
</location>
```

If you located the tag, then add the following line directly above the closing < /system.web > tag:

```
<httpRuntime maxRequestLength="20480" executionTimeout="600" />
```

So, in this case, your CreateUser node should look like this:

```
<location path="CreateUser.aspx">
        <system.web>
            <authorization>
                <allow users="*"/>
            </authorization>
            <httpRuntime maxRequestLength="20480" executionTimeout="600" />
        </system.web>
</location>
```

In some cases, this tag may not exist in your web.config file. When this occurs, create a new section right before the closing in the file. This closing tag usually is on the last line of the file. For example, if you received the error on DomainSynchronize.aspx, add the following lines to your web.config file above the closing tag:

```
<location path="DomainSynchronize.aspx">
        <system.web>
            <authorization>
                <allow users="?"/>
            </authorization>
            <httpRuntime maxRequestLength="20480" executionTimeout="600" />
        </system.web>
 </location>
```

ASP .NET applications will throw a System.OutOfMemoryException error if they cannot allocate physical memory or reserve sufficient virtual memory to meet an allocation request. By default, the addressable virtual memory space that is available is 2 GB. If this is used, the operating system can't allocate additional memory.

This can also occur if other processes on the server are using most of the ram.

To troubleshoot the problem, follow these steps:

- Connect to the machine running your web application and open up task manager (start->run->taskmgr). Make sure other processes are not using up most of the RAM on the server. If they are, close them, migrate your application to another machine, or increase the amount of RAM available. Note that ASP .NET applications will appear as the w3wp.exe process.
- If most of the RAM is not being used, your application pool may be limited to a small amount of memory. You can increase this amount

by opening the IIS manager (start->run->inetmgr), expanding the server node on the left pane, clicking on "Application Pools", right clicking on the application pool running your application, selecting "Advanced Settings", and changing the Private Memory Limit and Virtual Memory Limit in the recycling section.

Symptom

After upgrading Password Reset Server to 4.0.000000 and changing the CLR version, when attempting to load Password Reset Server, you receive the following error in Internet Explorer:

HTTP Error 404.17 - Not Found The requested content appears to be script and will not be served by the static file handler.

Resolution

This error can be caused by ASP.NET 4.5 not being correctly registered on the server.

Windows Server 2012 / 2012 R2 Use the Server Manager to install ASP.NET 4.5.

1. Open the Server Manager, select "Manage" and "Add Roles and Features".
2. Select Role based or feature based installation for your server.
3. Under "Web Server (IIS)", expand "Web Server", then "Application Development".
4. Check ASP.NET 4.5.
5. Finish the wizard to complete the installation.

Please visit the following link for more information on TeleSign.

Please visit the following link for more information on ProxStop

Release Notes

This section includes the most recent PRS Release Notes.

- 5.3.0 Release Notes
- 5.2.1 Release Notes
- 5.2.0 Release Notes
- 5.1.000006 and previous releases Release Notes

Password Reset Server Release Notes 5.3.0

- Thycotic encourages all customers to upgrade to PRS 5.3.0, the newest version of Password Reset Server, at your earliest opportunity. To download the installation file, go to our Support Community page, log in, and click the Password Reset Server panel. Follow the prompts to navigate to the new download page, where you can choose to download an MSI file for automated installation, or a zip file for manual installation.
- We also recommend changing the password on your Domain Admin account used by PRS to connect to AD.
- Thycotic thanks Brian Fox from Booz Allen for identifying the security issues leading to this release.

High Priority Security Fix

Addressed potential credential disclosure issues.

Common Vulnerability Scoring System (CVSS) v3.1:

- **Score**: 10 (Critical)
- **Vector**: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Best Practices for Hardening PRS Communication to the LDAP Server

To prevent opening a security vulnerability for Password Reset Server, especially when PRS is installed in the DMZ or is exposed to the public internet, outgoing requests over ports 389 and 636 should be blocked by an outbound firewall rule, except those intended for the legitimate LDAP server.

On the Password Reset Server host, this configuration can be accomplished by creating two custom outbound rules in a specific order. You must create and execute the **Allow** rule first, and then create and execute the **Block** rule.

1. **Allow**. First, create an outbound rule to allow PRS to connect to your internal LDAP server over LDAP ports 389 and 636 only.
2. **Block**. Then, create a second outbound rule to block PRS from connecting to other LDAP servers/endpoints on LDAP ports 389 and 636.

Offline reset setup failed. Some users, while installing PRS client in some environments, received an exception message of “Too many automatic re-directions were attempted.” The exception blocked offline reset functionality, and the user received an error message reading, “Offline reset setup failed, verify application host URL is reachable and re-install PRS Windows Login Client.” The issue has been fixed in this release.

Server not reachable. After making changes in the custom resources folder, some users received an error message of, “Server not reachable.” The message was worded generically to protect the user from potential security vulnerabilities. But the server was always reachable, and the issue has been fixed in this release.

PRS client 5.1.6 is not compatible with PRS server 5.2.00000 and higher.

Customers on PRS client 5.1.6 must upgrade to PRS client 5.1.7 before they can upgrade to PRS server 5.2.00000 and higher. Click Password Reset Server 5.1.7 to download the installation file directly.

Upgrade Path: If you have 5.1.6 installed, upgrade to 5.1.7 and roll out the client that comes with 5.1.7 (client 5.3). Once the client rollout is complete, you can upgrade to any version.

If you have 5.1.5 or earlier installed, or 5.2 and later, you can upgrade directly to PRS 5.3.

PRS Version Compatibility Table

5.1.6	5.1.6	Yes
5.1.6	5.3	Yes
5.1.7	5.1.6	Yes
5.1.7	5.3	Yes
5.2.0	5.3	Yes
5.2.0	5.2.0	Yes
5.2.00001	5.3	Yes
5.2.00001	5.2.0	Yes
5.2.00001	5.2.00001	Yes
5.3	5.3	Yes
5.2.0	5.1.6	**No**
5.2.00001	5.1.6	**No**

Phone Verification Method

During phone verification if your phone does not ring, please ensure that the following line is **not** in your web.config file:

```
<add key="PhoneQuestionCaller.TypeName" value="Thycotic.Usizo.Business.MockPhoneQuestionsCaller"/>
```

You might have to restart IIS after removing the line above.

Configuration File

- For PRS 5.1.000006 and earlier, use the web-appSettings.config file to configure application settings.
- For PRS 5.1.000007 and later, use the web.config file to configure application settings
- When upgrading from a version of PRS that uses web-appSettings.config to a version that uses web.config, please ensure that your values in the new web.config file match the values you had in the old web-appSettings.config file.

SQL Timeout Settings

Microsoft recommends that SQL timeout be set to 15 seconds. However in some environments this may not be optimal and could cause latency issues. If you have seen latency or database timeout issues on your PRS installation, you could change this value from 15 seconds to 300 seconds or longer as needed. If the SQL timeout setting `<add key="SQLTimeout" value ="15"/>` is missing (absent or removed) the default timeout will be set to 60 seconds.

Password Reset Server Release Notes 5.2.1

December 15th, 2020:

- Fixed a possible cross site scripting issue with the image upload function.
- Fixed potential code injection issue when uploading the answer file.

Password Reset Server Release Notes 5.2.0

Note: The Password Reset Server MSI has been updated. Some servers have their file upload limits set too low. Before upgrading, be sure to check your IIS server and web application settings to ensure the upgrade process completes. Click here for the steps to complete before upgrading.

- Improved standardization around the Maximum login attempts message when users login fails beyond configured max attempts limit.
- Increased digit length for SMS PIN codes.
- Updated PRS installer file to run with modern wizard user flow.
- Fixed a vulnerability in GINA client which could lead to remote code execution and was only present if attacker had control over network communications.
- Fixed a vulnerability in GINA client which could lead to remote code execution Security, the issue was discovered by:
  - **Barrett Adams** (Lead Researcher) of Specter Ops and **Rick Romo**, **Angel Flores** and **Marcus Sailler** of Capital Group Companies.
- CRC validation added to all resources downloaded by the client.

- Addressed the issue with the **Forgot Password** text not being displayed correctly when on the Windows login screen after a reboot.
- Resolved issue for UI dialog for Offline key rotation that caused the dialog to still be open after user interaction.
- Resolved an issue that returned a “Please wait” message if the new password and confirm password values didn’t match.
- Resolved issue that returned an error if the display name for a user contained “{“ or “}” characters when it tried to sync back with the system.
- Resolved issue that prevented user from logging when the Windows Login Integration client is configured but the SSL certificate for the PRS site is untrusted.
- Resolved an issue on the Application URL Configuration page where clicking on the “Back” button would redirect an Admin user to the wrong page.

Password Reset Server Release Notes for 5.1.000006 and Previous

Upgrade Notes

Password Reset Server Version 5.1.000006 September 9, 2020

Security:

- Fixed a vulnerability in GINA client which could lead to remote code execution and was only present if the attacker had control over network communications.
- Fixed a vulnerability in GINA client which could lead to remote code execution. Security Issue Discovered by:
  - **Barrett Adams** (Lead Researcher) of Specter Ops and **Rick Romo**, **Angel Flores**, and **Marcus Sailler** of Capital Group Companies.

September 24, 2019

To take advantage of updates to the Windows logon integration (WLI) desktop application in this release, you will need to uninstall and re-install your WLI files after upgrading PRS. Before doing so, perform the workaround steps listed below.

Known Issue: After installing Windows logon integration, customers may see the message "This machine is not registered for offline reset" on the Windows logon screen even though they have enabled offline reset.

Workaround: Before installing or re-installing Windows logon integration, the installer files may need updating by making a change in the configuration:

> **Note;** Administrator permissions are necessary to make these changes.

1. Go to CreateConfigurationFiles.aspx.
2. Click the **Edit** button.
3. Do not change anything
4. Click the **Save** button.
5. Download and reinstall Windows login integration.

Enhancements and Security

Updated JQuery Libraries

Updated JQuery libraries to JQuery version 3.4.1., eliminating an XSS vulnerability.

SQL Security Vulnerability

Fixed a SQL injection security vulnerability

Support for Special Characters Used in XML

Updated the PRS configuration setting “App Host URL” and all Windows-logon-integration localized text settings to support XML special characters and address an XML vulnerability.

Modern SSL Protocols

Updated Windows logon integration desktop application to allow communications over modern SSL protocols, including TLS 1.1 and TLS 1.2. This addressed a reported issue where PRS attempted to make calls over HTTP instead of HTTPS. This issue could occur when PRS and the machine hosting the Windows logon integration fail to find a common secure protocol. In addition:

- All customers should verify that the PRS certificate is valid and works in Internet Explorer because the issue may be environmental.
- Windows 7 customers (and those using .NET 2.0) should verify that registry settings to support TLS 1.1 and TLS 1.2 are in place on the local machine.

General

No Longer Force Users to Reset Their Password After Reset

Added a new “ResetWithoutChangeOnNextLogon” application setting that allows administrators to change the default Password Reset Server (PRS) behavior where users are prompted to change passwords at next logon immediately after performing an offline password reset.

Typically, when a user performs a password reset through PRS, it sets an attribute in Active Directory that forces them to change their password on their next logon. After setting the new “ResetWithoutChangeOnNextLogon” setting to “True,” PRS users can use the newly set password until the normally configured expiration time. To set this new app setting to True, follow these steps:

> **Note:** Administrator permissions are necessary to change app settings.

1. Open Windows File Explorer or another file manager.
2. Navigate to your PRS installation directory, which is usually `C:\inetpub\wwwroot\PasswordResetServer\`.
3. Right click the web-appSettings.config file, and select Open With, and select Notepad or other text editor. The XML file opens.
4. Type the following text inside the `<appSettings>` brackets: `<add key="ResetWithoutChangeOnNextLogon" value="True" />`
5. Save the file.
6. Restart IIS on the server.

Do Not Differentiate “Too Many Attempts” Login Errors

Updated PRS behavior to allow masking logon error differences between valid and invalid usernames during failed logons. The default behavior in PRS provides users with a new “Login Failed” message after hitting the maximum number of logon attempts for their username.

The regular logon failure message states:

Login Failed

The “too many attempts” message states:

“You have reached the maximum number of login attempts. Please try again later. If you have forgotten your password, please utilize the “Reset My Password” function below."

This can be undesirable because it implies that the username the user entered is in fact a valid username because PRS had to associate a username with the logon to count the attempts.

If you want to avoid this and display the same message for all users, regardless of reaching the maximum logon attempts, we now provide a “MaximumLoginAttemptsHaveBeenReachedJustLockedOut” setting to allow for customizing the “maximum attempts” error message, so you can now set it to the exact same message as the regular logon error message, eliminating the username inference.

To configure this behavior, follow these steps:

> **Note:** Administrator permissions are necessary to make these changes.

1. Open Windows File Explorer or another file manager.

2. Navigate to the ninth PRS resource directory, which is usually `C:\inetpub\wwwroot\PasswordResetServer\resources\9`.

   > **Note:** he number representing the final subdirectory can vary, depending on the languages you set up.

3. Right click the pages.xml file, and select Open With, and select Notepad or other text editor. The XML file opens.

4. Ensure the LoginFailed, MaximumLoginAttemptsHaveBeenReachedJustLockedOut, and MaximumLoginAttemptsHaveBeenReachedsettings are all set to “Login Failed,” or any consistent message according to your company’s preference.

5. Save the file.

6. Restart IIS on the server.

Bug Fixes

Custom Images

Fixed an issue where custom images were not properly loading in PRS and in emails.

Customer-provided images were not loading in e-mail templates because they did not contain a valid organization ID. Now the organization ID defaults to 1 for every image uploaded, since multiple-organizations are not supported in PRS.

Also enhanced logging and logic flow so it will report which images failed to load and if a substitute image was used in the case of a company logo.

Active Directory Passwords

Fixed a bug where Active Directory (AD) users with expired passwords attempted to logon to PRS received an “Access Denied” message and their AD passwords would automatically set to “Never Expire.”

To resolve this issue, code was removed that set the user’s PwdLastSetAttribute in AD to a value other than 1 or 0. Only Windows itself can change PwdLastSet to a value other than 1 or 0.

Grayed Out Reset Button Issues

Fixed a bug during the password reset process where the “Reset” button remained grayed out on the page but was still active. Clicking the button changed the user’s password, and clicking anywhere else on the page activated the button.

> **Note:** This issue was resolved for users accessing PRS through supported Web browsers, but when accessing PRS through the Windows logon integration desktop application, users must still click anywhere on the page before the “Reset” button looks activated.

Windows Logon Integration Desktop Application Offline Reset

Fixed an issue in the Windows logon integration desktop application where offline reset remained enabled, even after re-installing the application.

The issue occurred because the offline reset is enabled via registry keys. Previously those keys were added with every install. Now, before the keys are added, there is a check to make sure if offline reset is enabled. If it is not, the keys are not added. Also, the registry values are now removed upon uninstall.

Erroneous Error Message for Failed PRS Agent Connection

Updated error messaging to be “Offline Reset Agent Configuration Issue” when PRS agents are unable to connect with the server. This error previously displayed “Offline Reset Disabled,” which was misleading.

New Error Messages for Offline Reset

Added error messaging for when the Windows logon Integration desktop application fails to receive information from the PRS server regarding whether the registry keys need to enable offline reset or not.

We added a third offline reset localization string to the PRS Web client called “Offline Reset Setup Failure.” It contains text explaining a setup error occurred and instructs users they should verify the application host URL is reachable and then re-install the PRS logon client. Offline Reset installation states now include: Enabled, Disabled, and Setup Failure.

Custom Port Connections to Windows Logon Integration

Updated the Windows logon integration desktop application to respect a custom port when entered as part of the host on the Application URL Configuration page. This update only applies to HTTPS connections

Change Log

- Added 5.3.0 Release Note

- Added 5.2.1 Release Note

- Added 5.2. Release Note

Best Practices for Hardening PRS Communication to the LDAP Server

To prevent opening a security vulnerability for Password Reset Server, especially when PRS is installed in the DMZ or is exposed to the public internet, outgoing requests over ports 389 and 636 should be blocked by an outbound firewall rule, except those intended for the legitimate LDAP server.

On the Password Reset Server host, this configuration can be accomplished by creating two custom outbound rules in a specific order. You must create and execute the **Allow** rule first, and then create and execute the **Block** rule.

1. **Allow**. First, create an outbound rule to allow PRS to connect to your internal LDAP server over LDAP ports 389 and 636 only.

2. **Block**. Then, create a second outbound rule to block PRS from connecting to other LDAP servers/endpoints on LDAP ports 389 and 636.