



Password Reset PRO INSTALLATION GUIDE

This guide covers the new features and settings available in Password Reset PRO.
Please read this guide completely to ensure a trouble-free installation.

January 2009
Version 1.4rc
Copyright SysOp Tools, Inc.

Contents

Contents	2
System Requirements	3
System Requirements for Installed Applications:	3
Installation Options (Single Tier or Two Tier)	3
Single Tier / Standalone (All on One Server)	3
Two Tier / High Security (Requires Two Separate Servers).....	3
Installation Prerequisites.....	4
Single-Tier Installation (Install everything on one server).....	4
Prerequisites.....	4
Two-Tier Installation (Install on Separate Servers)	4
Prerequisites - Master Service Installation Server	4
Prerequisites - Web Portal Installation Server	4
Prerequisites – Network / Firewall	4
Password Reset PRO Installation Steps.....	5
Password Reset PRO Configuration	10
Master Service Configuration Settings.....	10
Web Portal Configuration Settings	16
Testing the Web Portal.....	18
Post Installation Security Enhancements	19
Advanced Network Configuration & Firewall Settings	19
Firewall configuration	19
Web Portal Server Traffic (Extranet or DMZ)	19
Master Service Server Traffic (Intranet or LAN)	19
First Time Installing IIS on Server 2003? You may need to enable ASP.NET in IIS	20
Enable ASP.Net in IIS (Windows Server 2003 only – Server 2008 Skip This Step)	20
Reference Links for IIS and SSL Configuration.....	21
Enabling SSL:	21
Installing SSL Certificates:	21
Enabling or Re-Registering ASP.NET in IIS:	21

System Requirements

System Requirements for Installed Applications:

- Operating System Requirements:
 - Microsoft Windows Server 2003
 - Microsoft Windows Server 2003 x64
 - Microsoft Windows Server 2008
 - Microsoft Windows Server 2008 x64
- Microsoft [.Net Framework v2.0.50727 \(x86\)](#) or [Microsoft .Net Framework v2.0.50727 \(x64\)](#)
Must be Installed Before Installation of Application Components

The following requirements apply to specific application components:

- Web Portal Application
 - Microsoft Internet Information Server (IIS) 6.0 or above Must Be Installed
- Master Service Application
 - Active Directory domain member server located on the same subnet or SITE as your primary (FSMO) DCs. Direct installation on a domain controller is possible but strongly not recommended.
 - A domain\user account with Domain Admin or Enterprise Administrator permissions, or other appropriate delegated rights with read/write permissions on user objects within your licensed domain or organizational unit.
 - This domain\user account will be used to run the Master Service.

Installation Options (Single Tier or Two Tier)

Password Reset PRO can be installed in two configurations:

Single Tier / Standalone (All on One Server)

Both the Web Portal application and Master Service application are installed and run on the same physical or virtual domain member server. This server **MUST** be a member of the domain you have licensed! Choose this option if you are limited on physical server hardware, are not overly concerned with external security, or will not publish external (internet) user access to the Web Portal.

Two Tier / High Security (Requires Two Separate Servers)

The Web Portal application (Front End) and Master Service application (Back End) are installed on separate physical or virtual servers. The Web Portal server may reside in a DMZ or other extranet that is firewalled from the internal domain (LAN). The Web Portal server does not need to be a member of the domain and can be a simple workgroup server. The Master Service server must be installed on an Active Directory domain member server located on the same subnet or SITE as your primary (FSMO) DCs. The Web Portal server and the Master Service server will communicate to each other over a single port published through your firewall. Communication between servers is RSA secured and Blowfish encrypted.

****This is the RECOMMENDED installation if you will allow public (internet) user access to the self-service Web Portal.**

Installation Prerequisites

Follow the instructions below to install Password Reset PRO in a standalone “Single Tier” (Single Server) configuration or distributed “Two Tier” (Two Server) configuration (Preferred).

Single-Tier Installation (Install everything on one server)

Prerequisites

You will need the following before proceeding with installation:

1. A physical or virtual server running a supported Windows Server operating system and is a domain member-server (installation on domain controller not recommended).
2. Microsoft .Net v2.0.50727 installed
3. Microsoft Internet Information Server (IIS) 6.0 or above installed

Two-Tier Installation (Install on Separate Servers)

Prerequisites - Master Service Installation Server

You will need the following before proceeding:

1. A physical or virtual server running a supported Windows Server operating system and is a domain member-server (installation on domain controller not recommended).
2. Microsoft .Net v2.0.50727 installed

Prerequisites - Web Portal Installation Server

You will need the following before proceeding:

1. A physical or virtual server running a supported Windows Server operating system. The Web Portal server may reside in a DMZ or other extranet that is firewalled from the internal domain (LAN). The Web Portal server does not need to be a member of the domain and can be a simple workgroup server.
2. Microsoft .Net v2.0.50727 installed
3. Microsoft Internet Information Server (IIS) 6.0 or above installed

Prerequisites – Network / Firewall

1. Allow a single port to communicate between Web Portal Server and Master Service server through your firewall. The default port is 5000, however you may change this in the application configuration settings. Server to server communication is RSA secured and Blowfish encrypted.
2. Configuring external / public Web Portal access: Please refer to the Advanced Configuration section located at the end of this guide.

Next page, begin installation of Password Reset PRO

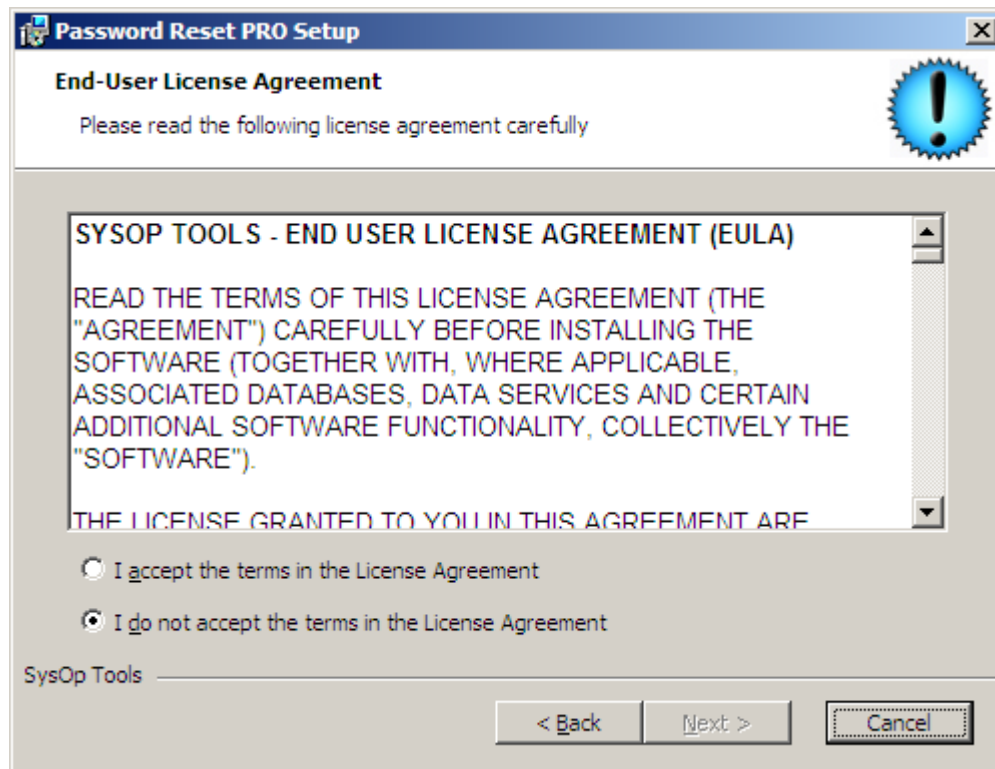
Password Reset PRO Installation Steps

Run the Password Reset PRO installation setup program:

1. Welcome Screen – click next.

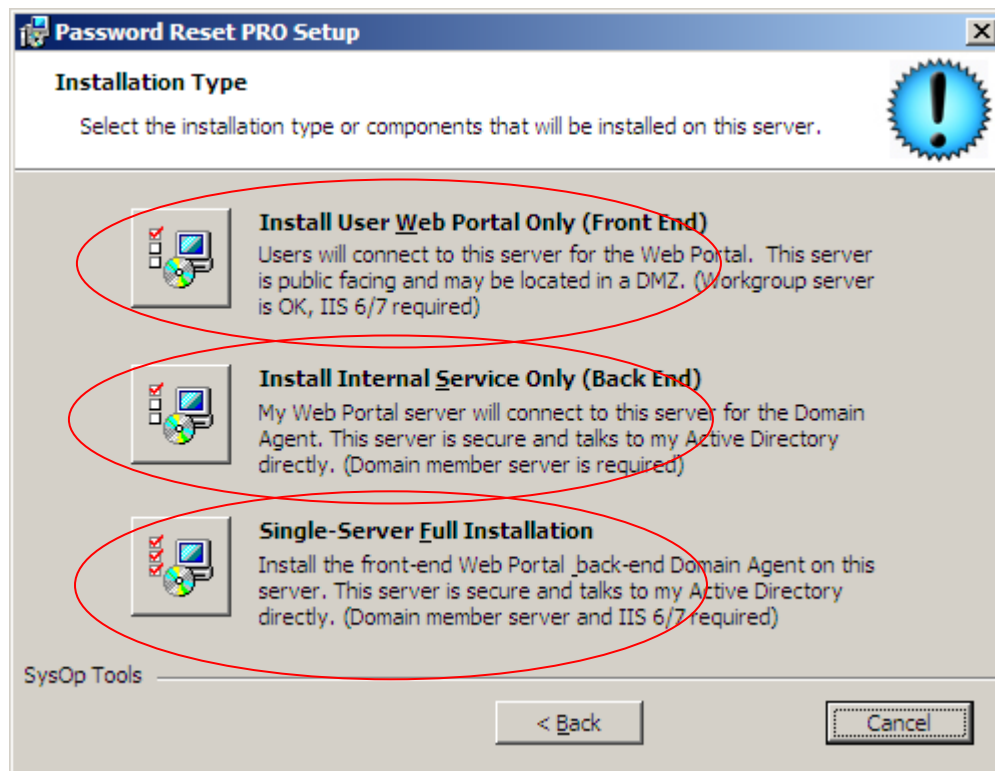


2. Read the entire license agreement and choose accept to continue



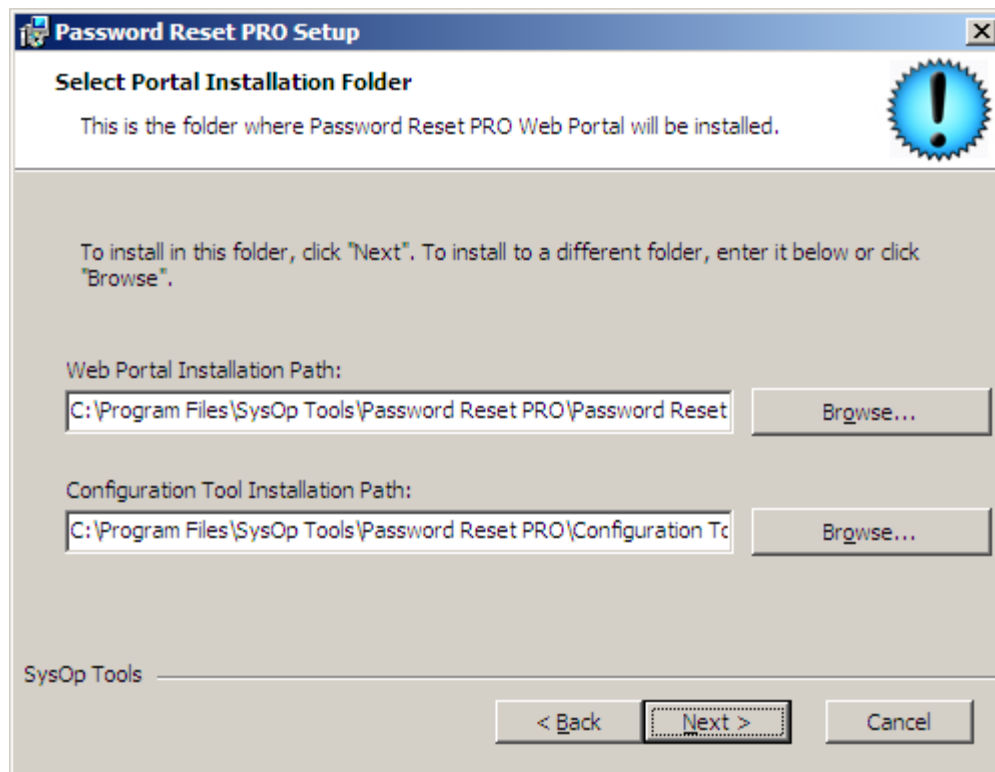
3. Installation choices:

- a. Choose “Single-Server Full Installation” to install the Web Portal and the Master Service on the same server.
- b. Choose “Install Internal Service Only” to install the Master Service on an internal domain member server. Select this option if you will install the Web Portal on a different server.
- c. Choose “Install User Web Portal Only” to install the Web Portal only. Choose this option if you will install the Master Service on a different server.

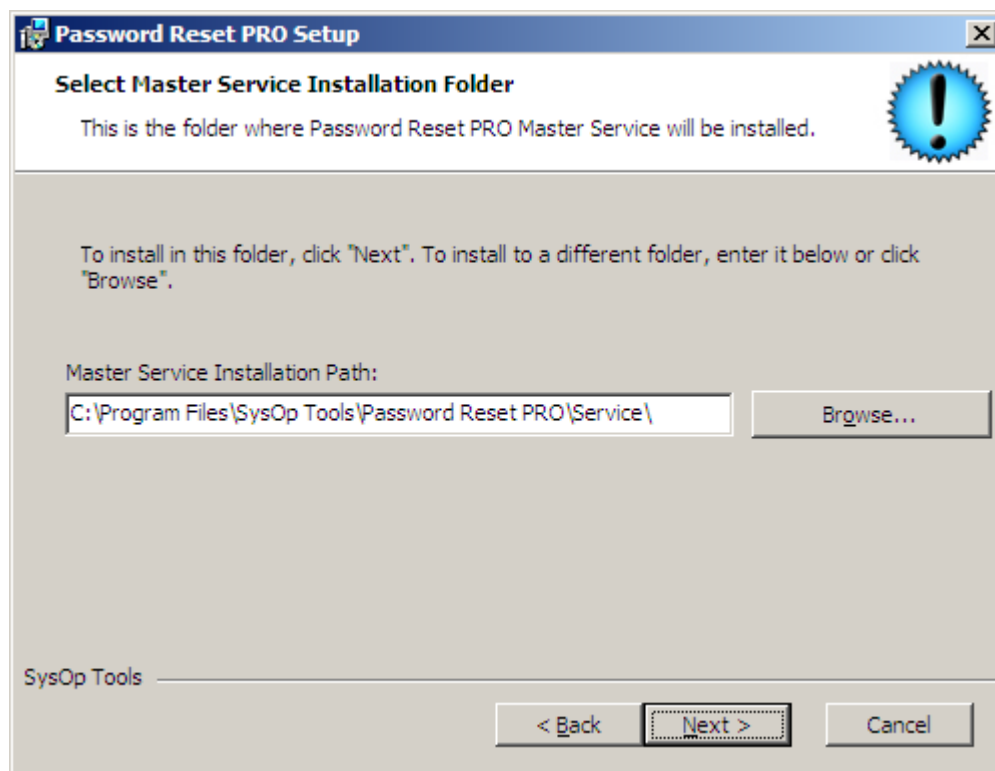


Continued on next page...

4. Accept default installation paths for the Web Portal (IIS site) and Configuration Tool:

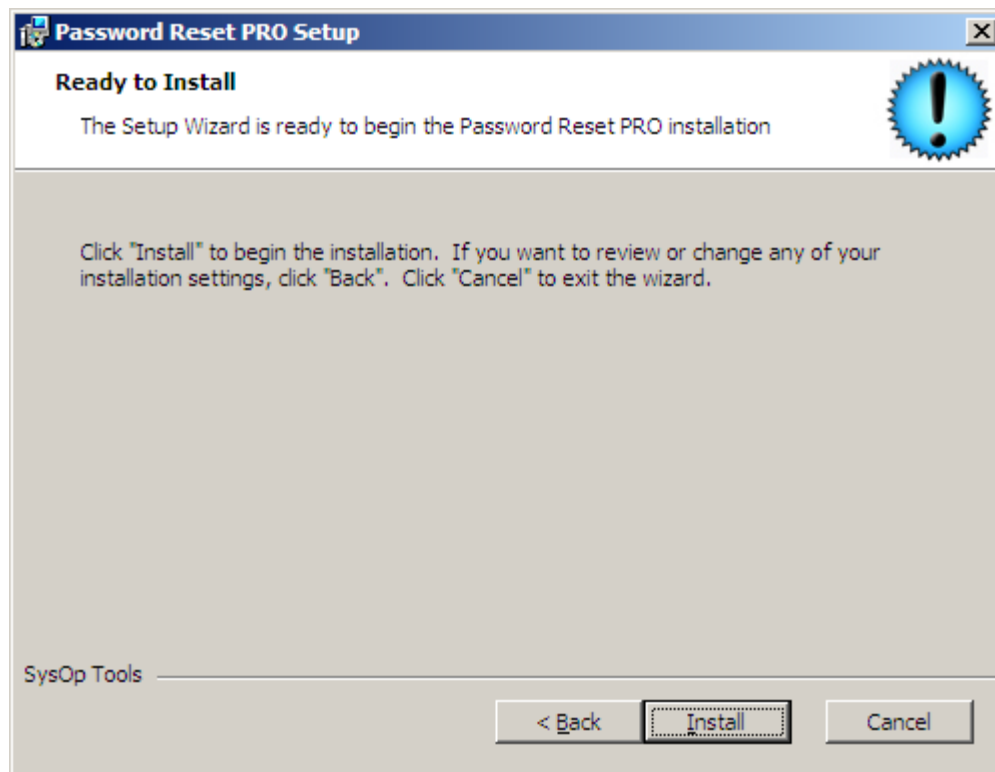


5. Accept the default installation path for the Master Service:

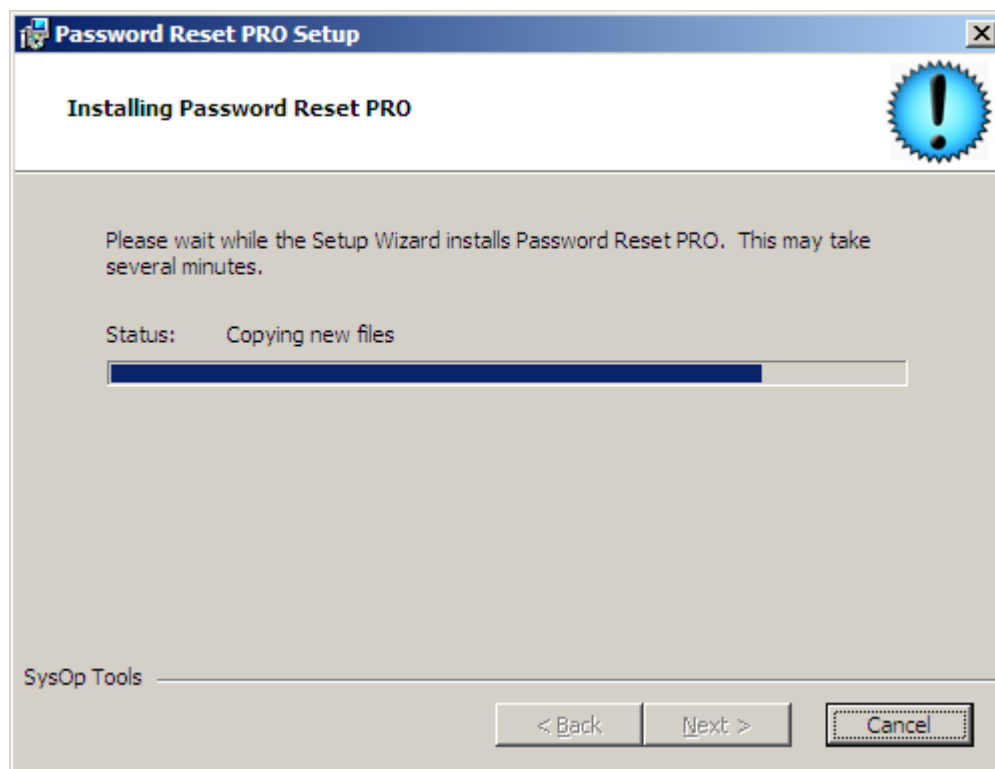


Continued on next page...

6. Choose Install to begin the installation:

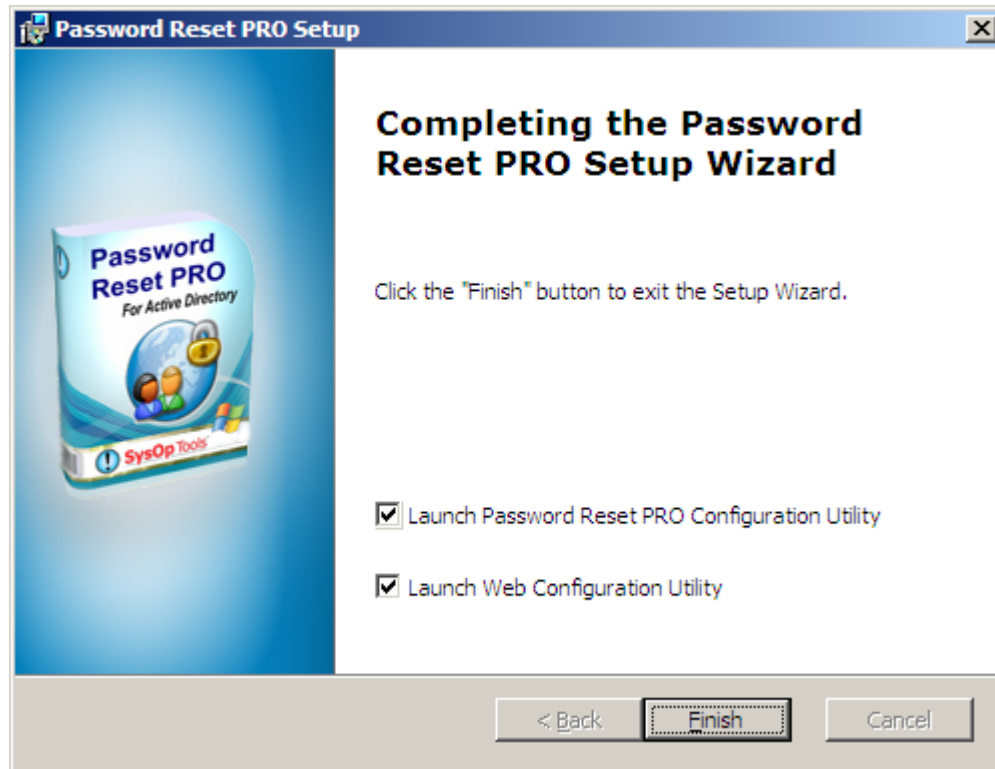


7. Please wait while the installation completes:



Continued on next page..

8. Finish the installation and launch the Web Portal Configuration Utility and Master Service Configuration Utility.



Installation Complete!

Next section: Configuring Password Reset PRO...

Password Reset PRO Configuration

Master Service Configuration Settings

1. Configure the Master Service FIRST.

Open the Master Service Configuration Utility.

- Enter your license keys under “*Add License Key*”.
- Web Portal Deny List*: Enter accounts you want to exclude from accessing the Web Portal. We STRONGLY recommend adding all “well known” accounts such as “Guest” and “Administrator”, and other sensitive user accounts. As a security feature of our software, all non-password-expiring user accounts and “System” accounts are denied Web Portal login access.
- Refresh User Accounts*: Password Reset PRO refreshes its list of Active Directory users every 5 hours by default. You can change this interval or click “refresh now” to do an immediate update. If you just created several new user accounts and want them to use the Web Portal immediately, click “refresh now” to update Password Reset PRO.

Master Service Configuration Screen

Password Reset PRO Master Configuration

License and Access Settings | Network and Service Settings | Profile Security Settings | Web Portal Settings | Report and Email Settings | About

License Keys

Add License Key: Add Key

Domain	Users	Expiration Date
--------	-------	-----------------

Licensed User Accounts Cache

Refresh User Accounts Every: 5 h 0 m Refresh Cache Now

Web Portal Deny List

Select Users...

Help for This Tab

License Keys
Copy / Paste your license key into the "Add License Key" field, then click "Add Key". You must have a valid license key for Password Reset PRO to function in your domain. Make sure to paste the entire key string otherwise you will receive a license key error. You can remove a license key by clicking the red X to the right of an added license key.

Licensed User Accounts Cache
Checks Active Directory for current list of domain user accounts. Use the "Refresh" setting to tell Password Reset PRO how often to update its list of cached domain user accounts. **Newly created domain user accounts will not be able to access the Web Portal until the User Cache has been updated. Click "Refresh Now" to immediately update the cache.

Web Portal Deny List
Click the "Browse" button to select domain user accounts that will be denied access to the web portal. Typically, you will want to deny sensitive domain user accounts within the \Builtin OU of Active Directory. **At very least, you should deny access to the "Administrator" and "Guest" domain

Save Changes Close

Continued on next page...

2. Set the IP address of your Web Portal server and select TCP communication port.

Web Portal IP Address:

- a. Single Tier (single server) installation: Enter 127.0.0.1 (localhost) as the IP address of the Web Portal.
- b. Two Tier (separate server) installation: Enter the IP address of the server on which you installed the Web Portal application.

Tip** If you want to allow access to the Master Service from multiple Web Portal servers, you can enter the additional external server's IP addresses separated by a semicolon (;). This is great for failover or capacity planning.

Service Port:

- a. Select the TCP network port to be used for connecting the Master Service server to the Web Portal Server. You **MUST** allow this port access through your firewall if the servers are separated by the firewall. Change the port number as needed.
- b. For Single-Tier installations with both Web Portal and Master Service on the same server, it is OK to leave the port setting as-is.

Master Service Configuration:

Password Reset PRO Master Configuration

License and Access Settings | **Network and Service Settings** | Profile Security Settings | Web Portal Settings | Report and Email Settings | About

Web Portal Connection

Web Portal IP Address: 127.0.0.1

Master Service Configuration

Service Port: 5000

Service Status: Stopped Refresh

Service Credentials: LocalSystem **Service must use a domain\user account with domain administrator rights**

Startup Mode: Manual

Service Configuration: Open Windows Services

Service Control: Start Service Stop Service

Help for This Tab

Web Portal Connection

Web Portal IP Address: Specify the IP address of your Web Portal server. For single-tier installations with the Web Portal and Internal Master Service installed on same server, use 127.0.0.1. For two-tier installations with the Web Portal installed on a physically separate server from the Internal Master Service, enter the IP of the Web Portal server. **If this field is not set properly, the Web Portal will fail to connect to the Internal Master Service.

Master Service Configuration

Service Port: Used for secure communication between the Web Portal server and the internal Master Service server. Choose any unused network port between 1025 and 56656. **If your Web Portal server is located in an external DMZ zone or on a different network subnet than the Master Service server, you may need to adjust firewall rules to allow bi-directional port traffic. Service Port connection is RSA secured and communication is Blowfish encrypted.

Service Status: Operational state of the Internal Master Service. Use controls to start / stop the Master Service. If the service is stopped, users will not be able to access the Web Portal.

Save Changes Close

Continued on next page...

3. Configure the Installed Windows Service:

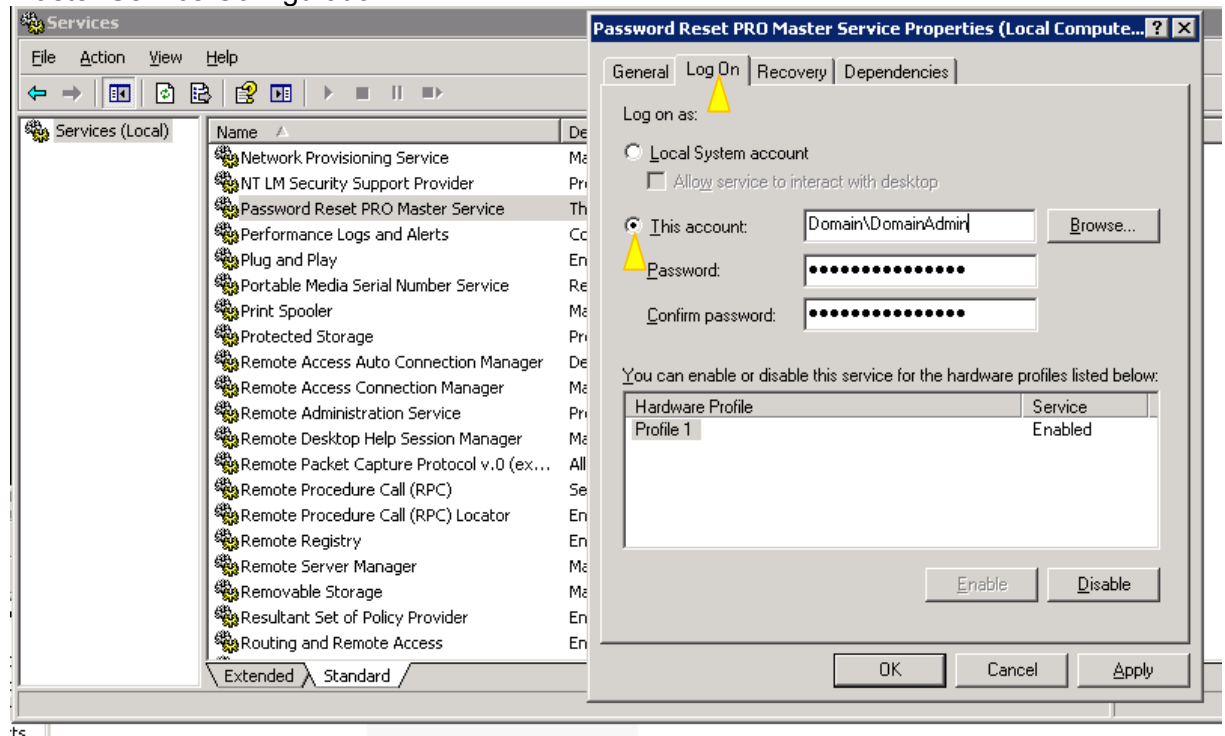
The installed service is extremely important to configure correctly. If you do not grant the service appropriate domain permissions or start the service, users will not be able to log in to the Web Portal and will not be able to create a Portal Logon Identity.

Security Note: The service account credentials and password used by Password Reset PRO are ONLY stored natively by Windows, nowhere else! This ensures native Windows security remains intact when installing our software.

- Click 'Open Windows Services' button. The Windows Services snap-in opens.
- Find 'Password Reset PRO Master Service' and choose properties.
- In the 'Log On' tab of the service properties, set the 'Log on as' to a valid domain\user account that has Domain Admin or Enterprise Admin rights, or delegated permissions to modify user objects including password change, password reset, account unlock, and write properties.
- Click Apply, then start or restart the service for the settings to take effect.
- Make sure the Startup Mode is set to "Automatic"

Tech Note: When a user creates a Portal Logon Identity in the Web Portal, their identity information is written to an existing attribute within their Active Directory user account. This identity information allows a domain user to access the Web Portal when their password is expired or when their account is locked out. Therefore, it is imperative for the service to have permissions to write the identity information to the AD user object.

Master Service Configuration:



Continued on next page...

4. Review the Profile Security options and make appropriate selections. These settings affect Web Portal user ID profile setup and Web Portal login.
 - a. *Domain Logon Security*: “Max Failed Login Attempts” sets how many incorrect login attempts a user is allowed before being denied further access to the Web Portal. A user must close / re-open their browser to try again if they exceed the limit. We recommend setting this limit to one less than your domain lockout policy. If your domain lockout policy is set to 3 invalid attempts, set this value to 2.
 - b. *Profile Security Word Settings*: Sets a level of complexity for Web Portal users creating or changing their Profile ID security word. By adding complexity, this keeps users from using overly-simple words for their security word.
 - c. *Min Length*: Sets the minimum length of the security word. We recommend setting this to the same length as your domain password policy setting.
 - d. *Banned Words*: Add words to the list that you do not want your users to use as part of their security word. The default list of words includes words that may be easy to guess when compared to the table of security images, and also includes the variable “%username%” which excludes use of their domain user name. We recommend not removing any of the default words.

Master Service Configuration:

The screenshot shows the 'Password Reset PRO Master Configuration' window with the 'Profile Security Settings' tab selected. A yellow arrow points to the 'Profile Security Settings' tab. The 'Domain Logon Security' section has 'Max Failed Domain Login Attempts' set to 2. The 'Profile Security Word Settings' section has 'Security Word Complexity' set to 'Letters + Number', 'Security Word Min Length' set to 6, and a list of 'Banned Words' including 'teapot, island, shoe, boot, blueman, horse, heart, motorcycle, lemon, fish, flower, people, dinosaur, rex, car, coffee, pig, pepper, castle, mansion, radio, shopping, cart, butterfly, ski, snowboard, boat, parrot, bird, barrel, wheel, %username%'. A red oval highlights the 'Max Failed Domain Login Attempts' and the 'Profile Security Word Settings' section. A 'Help for This Tab' pane on the right provides detailed explanations for these settings. At the bottom right are 'Save Changes' and 'Close' buttons.

Continued on next page...

5. Customize messages that appear to users in the Web Portal.

- a. Change the “*Domain Password Requirement Text*” to match your internal domain change password policy. Users will see this text when changing or resetting their domain password in the Web Portal. We have provided example text here to help get you started. This text should match your domain password policy settings.
- b. *Help Request Page*: Within the Web Portal, users have an option to send a help request email to an administrator or help desk. This message is displayed on the “Help Request” page for the user. We have provided default text to get you started.
- c. *Contact Admin Page*: If a Web Portal user is denied access or encounters an error, they are diverted to a “Contact Admin” page to request help. This message is displayed on the “Contact Admin” page for the user. We have provided default text to get you started.

Tech Note: You can use basic HTML markup tags to improve the looks of the web portal messages. Do not include scripts or image tags as they will not work.

Master Service Configuration:

The screenshot shows the 'Password Reset PRO Master Configuration' window with the 'Web Portal Settings' tab selected. The 'Domain Password Requirement Text' field is circled in red. The 'Help Request Page' and 'Contact Admin Page' fields are also visible. The right pane shows 'Header and Footer Settings' and 'Web Portal Messages'.

Web Portal Messages (HTML tags allowed)

Domain Password Requirement Text:

Choosing a new domain password: Your password must be at least 6 characters long and contain at least 1 capital letter and one number or non-letter character. Also, your password cannot contain any part of your user name or last five passwords. Example passwords which meet this criteria are "P@ssw0rd", "H3llo2u", "Myd0gSp0t", or "!!W33kend". Make it fun, think of something memorable and personable.

Help Request Page:

Welcome to the help request page.
Using the contact form below, you can send a message to IT support staff and request assistance with any issues you may be encountering with your domain user account, password or web portal. Your domain account information will be sent with the request automatically, if you would like to be contacted at a specific email address or phone number please include that information in the provided areas below. You will receive a response to your help

Contact Admin Page:

Welcome to the contact admin page.
Using the contact form below, you can send a message to IT support staff and request assistance with any issues you may be encountering with your domain user account, password or web portal. Your domain account information will be sent with the request automatically, if you would like to be contacted at a specific email address or phone number please include that information in the provided areas below. You will receive a response to your help

Help for This Tab

Header and Footer Settings

Header: Enter the url of an image that you would like to use as the Web Portal banner for all pages. Image dimensions cannot be larger than 90px high by 600px wide. If no image is specified the default "Password Reset PRO" banner will be used.
Example:

Footer: You may enter footer text for the Web Portal. For example, links to your company's privacy policy or other information. Images are not allowed in the footer, only text and hyperlinks.

Web Portal Messages

Domain Password Requirement Text: Inform users of your domain's password change complexity requirements. They will see this text when changing or resetting their domain password within the Web Portal. We have provided default text to help get you started.

Help Request Page: Specify a message to users who want to submit a help request. Users will see this message when they arrive at the "Submit Help Request" page within the Web Portal.

Save Changes Close

Continued on next page...

6. Select the log file path, SMTP server and admin email settings.
- Choose a local SMTP relay server for sending administrator alerts and daily summary report emails. Make sure your Exchange server virtual SMTP relay is set to allow connection and relay from the IP of the Master Service server.
**** If you do not set up email connectivity to your relay server correctly, you will not receive any emails or reports from Password Reset PRO!**
 - Send Immediate Emails to:* Add an email address for receiving "immediate alerts" such as account unlock events and system errors. Immediate alerts are sent in real-time as they happen and should be sent to an IT Administrator.
 - Send Help Request emails to:* Add an email address for receiving user help requests from the Web Portal. You may want these emails to go to your helpdesk group or ticketing system.
 - Send Daily Reports to:* Add an email address for receiving the Daily Summary Report email. This report contains a summary of all Web Portal events for the last 24hr period. Typically this email should go to an helpdesk group or UT administrator group for daily review.
 - Audit Reports:* Export a list of all active password expiring user accounts that do not have a logon profile established on the Web Portal. The user's name, domain account and email address are exported to an XML-based Excel spreadsheet (Excel 2003 or later required) for easy review. Extract the email addresses from the exported data and send a reminder email to your users, encouraging them to create a profile on the Web portal.

Tech Note - Disabling Emails: If you leave an email address field blank, the feature will be disabled. Testing email delivery: Use the "Test" button to test and verify email connectivity. You should receive a test email to the specific address.

Master Service Configuration:

Password Reset PRO Master Configuration

License and Access Settings | Network and Service Settings | Profile Security Settings | Web Portal Settings | **Report and Email Settings** | About

Report Log Location: C:\Program Files\SysOp Tools\Password Reset PRO\Logs [Browse..]

Mail Configuration

SMTP Server: 192.168.1.10 [Test]

Send Immediate Emails to: admin@yourdomain.com [Test]

Send Help Request Emails to: helpdesk@yourdomain.com [Test]

Daily Summary Report Settings

Report Subject Line: Password Reset PRO Daily Summary for %domain%

Send Daily Reports to: admin@yourdomain.com [Test]

Audit Reports

Licensed Users Without a Web Portal Profile: [Export]

Help for This Tab

Email Configuration

SMTP Server: Password Reset PRO sends "real time" message alerts and a daily activity summary report to you via email. Enter the mail.server.com name or IP address of your internal mail relay server. **If you are using Microsoft Exchange, make sure you set the "Relay" and "Connection" settings on the Exchange Virtual SMTP server to allow SMTP relay from the IP address of this server. Also, make sure any anti-spam filters are set to "white list" email from this server.

Send Immediate Emails to: Enter the email address of the person or group that should receive "immediate" real-time alerts from the Web Portal. This includes system error alerts, unlock domain account events, and (Scott what else?). **Use the "Test" button to check deliverability of the email address entered. A test email will be sent to the specified email address.

Send Help Request Emails to: Enter the email address of the person or group that should receive Help Request and Contact Admin emails from the Web Portal. The Help Request and Contact Admin emails include user account data, message from

[Save Changes] [Close]

Web Portal Configuration Settings

7. Open the Web Portal Configuration Utility. Begin by entering the Master Service Server IP address.

Master Service Server IP Address:

- a. For Single Tier (all on same server) installation, enter 127.0.0.1 (localhost).
- b. For Two Tier (separate server) installation, enter the IP address of the server where you installed the Master Service.
- c. **Service Port:** Set the Service Port to the same port you specified in the Master Service Configuration.
- d. Use the “Test” button to test the connection and ensure it is working properly.
- e. **IIS Web Server Status:** Shows you the current state and settings of the Web Portal on your server. These settings can be changed through the IIS manager.

Tech Note: If the port number does not match in the Master Service configuration and the Web Portal configuration settings, the connection will fail. If you have a firewall or router between the Web Portal Server and the Master Service Server, make sure you allow bi-directional port traffic for this port between the two servers.

Web Portal Configuration Settings

Password Reset PRO Web Portal Settings

Network and Server Settings | **Web Portal Settings** | About

Master Service Connection

Master Service Server IP Address:

Service Port of Master Service Server:

Test Connection:

IIS Web Server Status

IIS Website Name: Password Reset Pro Web Portal (Running)

Launch Portal: <http://localhost:8080>

IIS Network Bindings

IP Address	Port	Host Header
All Unassigned	8080	

SSL Enabled: No

IIS Application Pool: DefaultAppPool

Help

Master Service Connection

Master Service Server IP Address: Specify the IP address of your Master Service server. For single-tier installations where you have installed the Web Portal and the Master Service on the same server, use 127.0.0.1 as the IP. For two-tier installations where the Web Portal is installed on a physically separate server from the Master Service server, enter the IP of the Master Service server.

****If the IP address is not set properly, the Web Portal will fail to connect to the internal Master Service.**

Service Port of Master Service Server: Used for secure communication between the Web Portal server and the internal Master Service server. Enter the Service Port number that you specified in the Master Service configuration settings.

****If your Web Portal server is located in an external DMZ zone or on a different network subnet than the Master Service server, you may need to adjust firewall rules to allow bi-directional port traffic.**

****If the Service Port is not set properly, the Web Portal will fail to connect to the internal Master Service.**

Continued on next page...

8. Brand your Web Portal! You may optionally change the Web Portal page title, image header and add footer text / hyperlinks. Max header image size is 800px by 150px.

Web Portal Configuration Settings

Password Reset PRO Web Portal Settings

Network and Server Settings | **Web Portal Settings** | About

Web Portal Title Bar Text

Title Text: Password Reset PRO Identity Management Portal

Header and Footer Settings

Header Image (HTML for Header Image - max 800w x 150h - .jpg, .gif, .png, .bmp):

``

Browse...

Footer:

Help

Header / Footer

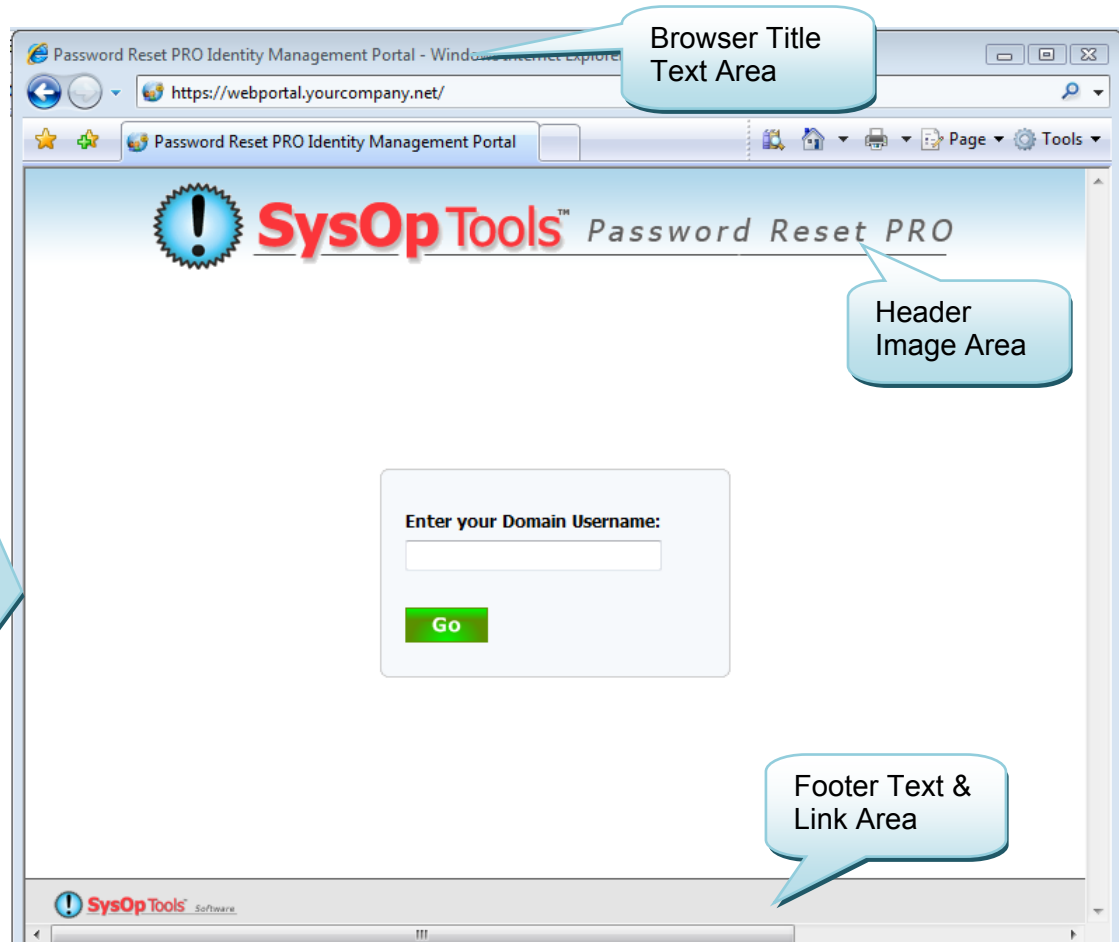
Header Image: Specifies a custom banner image to use on Web Portal pages. Use the "File > Browse" button to choose an image stored on your computer (jpg, gif, png, bmp formats only). The image will be saved in the 'images' directory of the web portal application install directory. Alternatively, you can use an external url of an image hosted on another server. **Image cannot be wider than 800px or taller than 150px.

Footer: You can provide text and links in the Web Portal bottom footer area. For example, links to your company's privacy or use policy. Only text, hyperlinks and basic HTML style tags are allowed, no images or scripts. Any URL links specified in the footer will open in a new browser window when clicked.

Web Portal Title Bar Text

Title Text: Enter the title text that you would like to appear in the top bar of the Web Portal user's client browser.

Save Changes Close

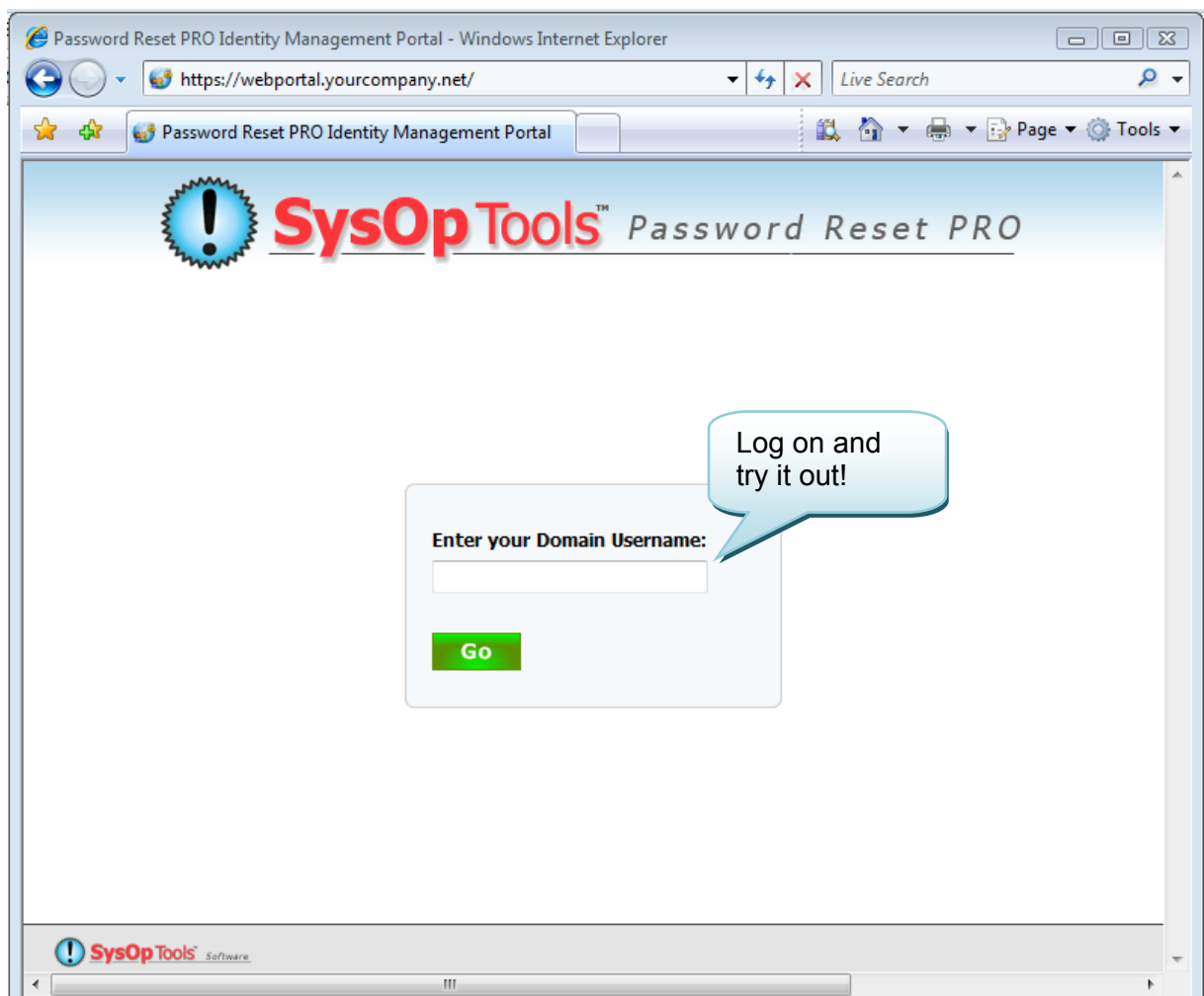


Configuration of your Password Reset PRO Installation should now be complete!

Testing the Web Portal

By default, the installation configured your Password Reset PRO web portal to use port 8080. You can change the port settings in the IIS manager. We strongly urge only allowing SSL connections and port 443 for external (internet) user access.

1. Log on to the server where you installed the Web Portal application. Open your browser and type <http://localhost:8080> . The Web Portal will take about 30 seconds to “compile” the ASP.NET code and then display the main logon page. The “compile” time occurs the very first time you load the portal. Users accessing the Web Portal will not experience this delay after the 1st-time compile.
2. Try accessing the web portal from another server or workstation on the LAN by typing: <http://www.YourServerName.com:8080> . If the page displays, this means you have everything operational now.
3. Log on to the portal with an active password expiring user account and set up an ID profile. Log off the Web Portal and then log back on with your new Profile ID. This will give you an understanding for how the process works and what your users will see.



Post Installation Security Enhancements

Follow the optional Post Installation Steps to further configure your Web Portal installation and strengthen security.

By now your Password Reset PRO Self Service Portal is operational. If you plan on making the Web Portal publically accessible to your remote users via the internet, we urge you to strongly consider the following steps for strengthening perimeter security:

- Configure IIS and the Web Portal with a public IP and only allow Port 443
- Allow SSL connections only to the Web Portal (disable Port 80 access)
- Install a trusted SSL certificate from a Certificate Authority such as Verisign

Advanced Network Configuration & Firewall Settings

Password Reset PRO may be used in a high security environment by placing the Web Portal application on a separate non-domain server in a DMZ or extranet, physically separated from your domain / intranet (LAN) by a firewall. Install the Master Service application on a domain member server located inside the internal network (LAN) within the same subnet or SITE container as your primary Active Directory Domain Controllers.

Firewall configuration

Firewall rules should be configured as follows for a Two Tier (Separate Server) Installation:

Web Portal Server Traffic (Extranet or DMZ)

Description	In/Outbound	Protocol	Port
External user HTTP/S connectivity from Internet	Inbound	TCP	443 (or other port specified in your IIS configuration as needed)
Internal connectivity to / from Master Service server	Outbound	TCP	5000 or alternate port configured in the Master Service Configuration (Network and Service Settings tab)

Master Service Server Traffic (Intranet or LAN)

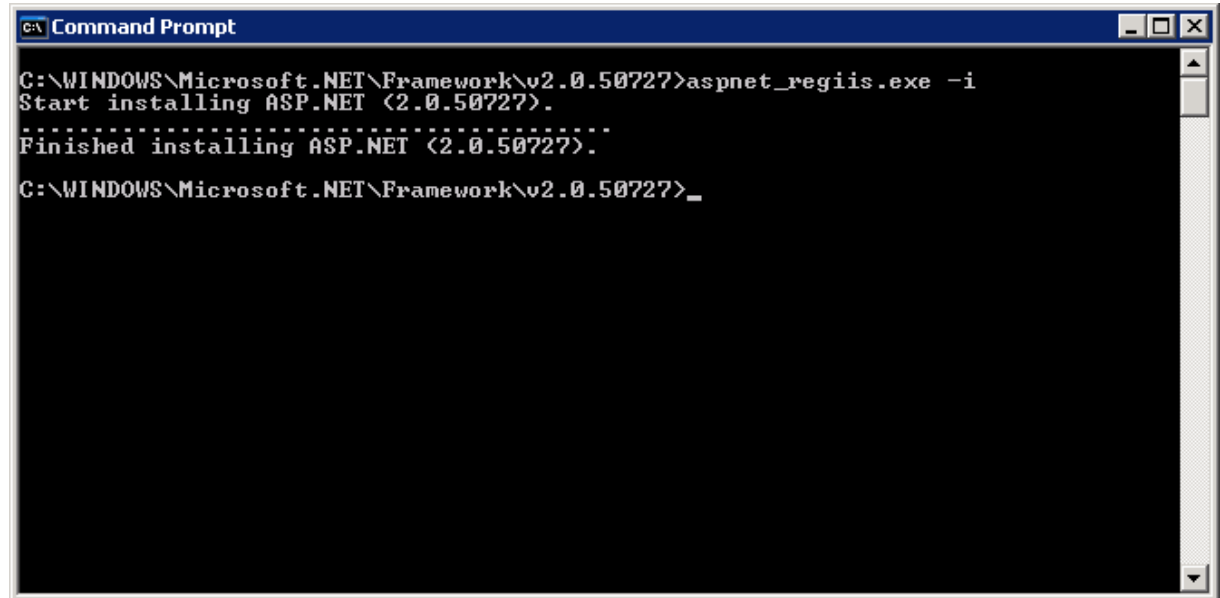
Description	In/Outbound	Protocol	Port
Internal connectivity to / from Web Portal	Inbound	TCP	5000 (default) or other port configured in the Master Service Configuration > Network and Service Settings tab
Internal connectivity to Active Directory Domain Controller	Outbound	TCP	Full LAN / domain connectivity

First Time Installing IIS on Server 2003? You may need to enable ASP.NET in IIS

Enable ASP.Net in IIS (Windows Server 2003 only – Server 2008 Skip This Step)

If you have not already configured your IIS server to run ASP.Net applications, perform the following step to enable ASP.NET in IIS. Note that this is not required if you are running Windows Server 2008:

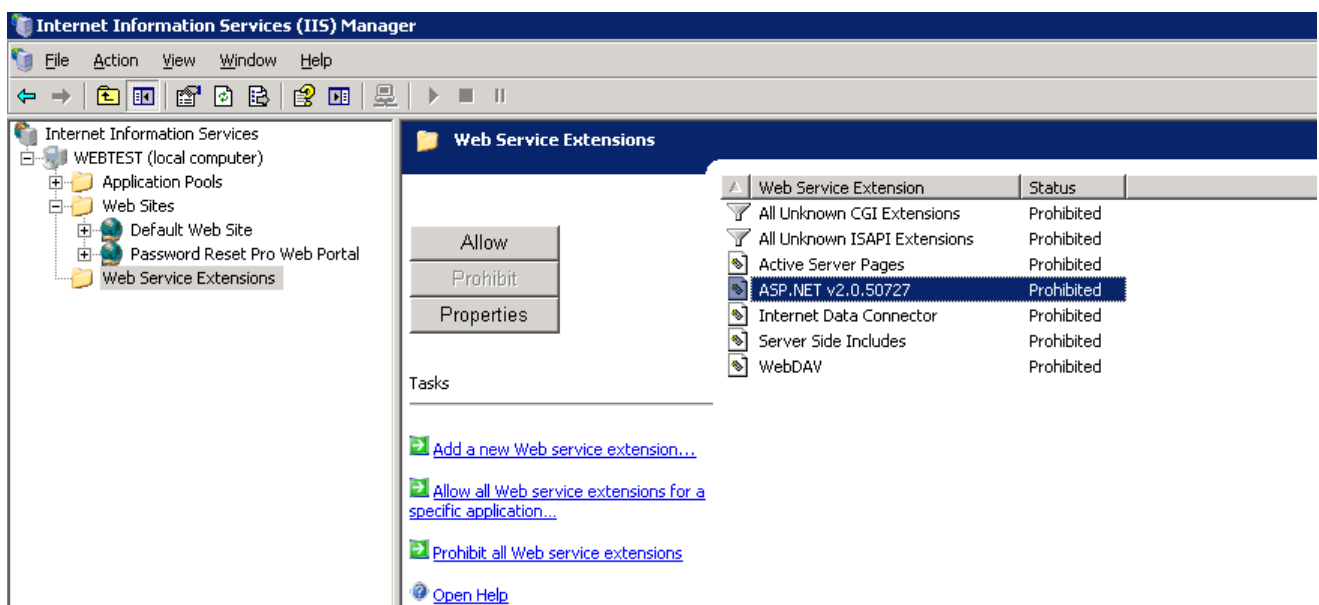
1. Install ASP.NET by opening a Command Prompt and running the following command:
C:\Windows\Microsoft.NET\Framework\v2.0.50727>aspnet_regiis.exe -i



```
C:\> Command Prompt

C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727>aspnet_regiis.exe -i
Start installing ASP.NET <2.0.50727>.
.....
Finished installing ASP.NET <2.0.50727>.
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727>_
```

2. Enable the ASP.Net Web Service Extension by opening IIS Manager and choosing Web Service Extensions, selecting ASP.Net v2.0.50727 and clicking 'Allow'.



Reference Links for IIS and SSL Configuration

The below resource links are provided for your convenience. Please be advised these links are outside of the control of SysOp Tools, Inc. SysOp Tools takes no responsibility for the accuracy, completeness, availability or content of information obtained through the below resource links.

If you find yourself stuck on the installation / setup of Password Reset PRO, please contact our Support Team through the "Contact Us" page on our website located at: <http://www.sysoptools.com> . We'll do our best to help!

Enabling SSL:

Set up SSL Protocol in Server 2003 IIS6

<http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/56bdf977-14f8-4867-9c51-34c346d48b04.mspx?mfr=true>

Set up SSL Protocol in Server 2008 IIS7

<http://learn.iis.net/page.aspx/144/how-to-setup-ssl-on-iis-7/>

<http://learn.iis.net/page.aspx/378/configuring-ssl-in-iis-manager/> (Video Tutorial)

*Disable port 80 to ensure only secure connections to the web portal

Installing SSL Certificates:

Install Certificate Authority SSL Cert in Server 2003 IIS6

http://www.verisign.ch/support/ssl-certificate-support/page_ch_en_dev020193.html

Install Certificate Authority SSL Cert in Server 2008 IIS7

<https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=so9071>

Enabling or Re-Registering ASP.NET in IIS:

Enable ASP.NET 2.0 Protocol in Server 2003 IIS6

aspx pages not displaying? Make sure you have enabled the .aspx protocol.

<http://msdn.microsoft.com/en-us/library/aa560277.aspx>

Enable ASP.NET 2.0 in Server 2008 IIS7

In order to enable .aspx pages to be served under IIS7, you must install ASP.NET 2.0 through the Windows setup interface available from the Control Panel > Programs applet. This will create the appropriate handler mappings you need at the global IIS level to serve your .aspx pages and other asp.net content.

Re-Registering ASP.NET in IIS

Sometimes you may need to re-register ASP.NET 2.0 with IIS6 or IIS7 in order for IIS to see the available 2.0 .NET version.

This can happen if you installed ASP.NET 2.0 before installing IIS6 or IIS7.

Register ASP.NET 2.0 in Server 2003 IIS6 or Server 2008 IIS7

Open a command prompt and run

"C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis.exe -i -enable".

Open IIS manager again and .NET 2.0 should now be a selectable option for the web application.

Make sure to enable ASP.NET as an allowed protocol.

<< End of Installation Guide >>