100% USA Sales / Support / Service

Password Reset PRO: Migrate or Back up Password Reset PRO v3 Settings
Software version 3.x.x

Use this guide for multiple domain installations, moving software components to new servers, or backing up production settings for quick disaster recovery of a failed server. Basically you will export the installation and configuration data and then import it into the other domain installs, or to new servers. You will save the data to a safe backup location off the production servers. This will cut down your install / config / migration / recovery time considerably.

Current Servers: Back up your configuration data and Web Portal customizations

1. Saving Application Configuration Settings: Open the Master Service Configuration application and the Web Portal Configuration application. On the "Support" tab of each application, there is a "Save" button. Use this to back up the application configurations to a backup file. Save these two files for the new server installations, as they contain all of your input configurations on the various tabs.

2. User enrollments in the self service portal are always safe; the user's enrolled information is stored as an encrypted token under their AD user account in altSecurityIdentities schema field. Users can access your migrated or recovered Password Reset PRO installation without having to re-enroll. Nice!

3. There are a few items that will <u>not</u> be backed up automatically such as your license key, service account settings, IIS-specific settings (SSL cert, IP, Port, etc), manual changes made to the Web Portal .aspx pages, and custom images added to the Web Portal.

    a. Saving custom Web Portal page changes: Make note of any manual changes you've made to the Web Portal pages (.aspx files and .css file). By "Manual" changes, we mean any changes you've made with an HTML editor such as adding or modifying text on the pages directly. You must copy these modified pages to your new server. Also, you'll need to copy image changes you've made such as your global top banner file, buttons, custom security thumb images, etc, which are stored under the "\Images" and "\Images\Icons" directory. **You can make a backup copy of the entire '\Password Reset PRO Web Portal\' directory and store it off of the production Web Portal server in a safe location, BUT do NOT include the "\BIN" folder (you don't need this folder and it may mess up your recovery installation).**

    b. Make note of the domain\user account used to run the Password Reset PRO Master Service

    c. Make note of any IIS-specific settings in IIS Manager for the Web Portal site such as IP, Host Header, Port, SSL cert.

    d. Keep a copy of your license key. You can always obtain a copy of your license key by logging on to your customer account on our website.

Done – Go on to the next section.

Recovery or Migration: After installing Password Reset PRO software on new servers

The below steps apply to recovery installations, server migrations, and replicating installations in multiple domains. For multiple domains, you will need the correct key for that domain.

1. Restoring Software application configuration settings:

    a. Open the Master Service configuration and add your license key.

    b. Configure the Password Reset PRO Master Service under Windows Services and start the Master Service

    c. Open the Master Service configuration application and the Web Portal configuration application, use the "Support" tab and "Import" button to import your saved configuration backup files into the configuration applications. Note that the Web Portal and Master Service each have their own specific backup file to import. Do not save changes yet.

    d. In the **Web Portal configuration** application on the first tab, change the IP address of the Master Service server to the correct IP, if the IP of your new Master Server has changed.
    Save changes to commit.

    e. In the **Master Service configuration** application, go to the "Network and Service Settings" tab, click the "Edit" icon next to your listed Web Portal to open the 'Web Portal Editor', and edit the IP address of your Web Portal server if the IP of your new Web Portal server has changed. (Since you are on new servers now, the IPs will be different for both your Master Server and Web Portal servers).
    Click OK on the Web Portal Editor menu after updating the IP, then click Save Changes in the Master Service application to commit.

2. Restoring custom Web Portal page changes and custom images (skip this step if not applicable):

    a. Copy any modified aspx pages to the Web Portal server's installation directory and replace any default .aspx files with your modified aspx files.

    b. Copy your custom banner image file (and any other custom images) to the "\Images" directory. Copy your modified CSS to the \App_Themes" directory.

    c. Recycle the IIS application pool for Password Reset PRO through IIS manager.

3. Restoring IIS manager settings: Open IIS Manager and perform any final configuration settings to the Password Reset PRO Web Portal site (SSL cert, SSL settings, IP, Host Header, Port, etc)

4. Launch the Web Portal and confirm operation. The 1st-time page load will take a few seconds while the web page code is compiled. Log on with an enrolled account or enroll a new user account.

5. If you receive any initial errors, make sure you have configured your LAN firewall to allow port communication between the Web Portal server and the Master Service server. Also make sure your mail server will allow SMTP relay from the Master Service server.

Have more questions? Contact our knowledgeable Sales & Support Teams

1-877-SYSOPTOOLS (USA) or +1-213-995-5060 (Direct & Int'l)
Support Team Hours: M-F 8am-6pm PST | Sales Team Hours: M-F 9am-6pm PST

Additional Resources:

📄 **Purchase Information** | 📄 **Reference Material and Knowledge Base**
📄 **Support Information** | 📄 **>>Sign up and Download Password Reset PRO Software**

SysOp Tools, Inc. is a privately held company located in Los Angeles, California – Software sales, support and development are handled by experienced in-house staff. We do not outsource any of our operations.