Password Reset PRO: Summary Information on Component Architecture

Software version 3.x.x

The below summarizes the architecture of Password Reset PRO, which is comprised of two main components: The "Web Portal", which is a simple ASP.NET website designed to run with no domain credentials on an extranet DMZ server, and the "Master Service", which resides on an internal domain member server and contains primary settings and security credentials. The "database" in this architecture is Active Directory. We do not use an external database.

Both components can be installed on a single domain member server with IIS for testing or production, however we always recommend doing a "two tier" (two server) installation. It is the most secure and scalable option.

Network topology:

> Basic Network Architecture Diagram (pdf)
> Advanced Network Architecture Diagram (pdf)

Master Service component (must be located on a domain member server):

For the **Master Service** component (internal facing component of our software), this should be installed in the domain (LAN) secured network on a regular domain member server- Any tools / utility type of member server is fine, you do not need a dedicated server. The Master Service server holds the domain credentials, core settings, accepts encrypted communication from the Web Portal servers, and talks to your DCs to perform the password resets / changes / account unlocks. You can consider this a "middle tier" application, and the server does not need IIS or anything special installed.

The Master Service contains strict logic rules to only allow specific user account types to access the Web Portal, specifically, only your enabled password expiring user accounts. The domain\administrator, domain\guest, domain\krbtgt, system AD accounts, disabled accounts, 'Can't change password' accounts, logon-date expired accounts, and accounts set with 'password never expires' are automatically excluded from Web Portal access and licensing requirement. You will however need a 'domain\domainadmin' user account to run the installed Windows Service (Password Reset PRO Master Service). A delegated account can also be used, and we can provide security spec on the required rights delegations.

Web Portal component (server must have IIS installed and ASP.NET v2 registered in IIS):

For the **Web Portal** component (public facing component), this should ideally be installed on a non-domain member server (workgroup box) that sits in a perimeter DMZ outside of the LAN. The Web Portal server must have IIS installed since our software simply installs an ASP.NET website and .NET 2.0 application pool under IIS. If you have other web sites on the IIS server that is fine, the Web Portal site will co-exist per typical IIS settings. The Web Portal's sole purpose is to accept public user input, encrypt the input data, and send it via a single TCP port (port 5000) through your firewall to the Master Service server. The port traffic between the Web Portal and Master Service is encrypted at the packet level (Layer3) with AES, and an RSA key handshake / rolling code exchange sequence is used at the application layer for session state traffic between the Web Portal and Master Server. The default port for connectivity between Web Portal and Master Service is TCP 5000, however, you can use any port instead of 5000 if you prefer.

You can consider this component a "Web Tier" application. We assume that any public facing web server, no matter how secure, can eventually become compromised by a smart attacker. If this were to happen, our Web Portal exposes zero data about your LAN and provides no pathway inside. Using a domain member server for the Web Portal function increases your security risk since any domain member server contains data about the domain, DC location, and possibly domain credential account names. By using a non domain server, you eliminate this risk.

Data Tier:

The "Data Tier" in this architecture is Active Directory. Active Directory is already plumbed out to support this type of self service system. When a user enrolls in the self service Web Portal, the Master Service receives the user's enrollment selections and creates an encrypted token. The token is stored under the user's AD account in the 'altSecurityIdentities' schema field and looks like this: "RST:bdtbhaDTHAdtthXv45y77z==%7ASREDS11=-". This method ensures that user enrollment data is stored in a secure, replicated and redundant repository for complete HA and DR- and this is also why our software does not need to use a separate database.

DR / HA:

For scalability / failover, it is very simple to install additional Web Portal servers then place them behind a VIP for load balancing. You can connect multiple individual Web Portals to the single Master Service, or run completely separate side by side installs of Web Portal + Master Service. You'll essentially treat our software just like any other data driven web architecture such as MOSS or OWA, and there is nothing new or proprietary introduced by our product other than general software settings.

Lastly, it is a snap to back up the software settings or move software to another server. DR is assured by design with very quick recovery time if a server were lost. Enrollments are always safe within Active Directory, and cannot be lost.

Perimeter and Countermeasures:

There are countermeasures built into the Web Portal which prevent a malicious user from repeatedly attacking, socially engineering or brute forcing logon entry. Programmatic security checks are built in to prevent an external unauthorized calling application or bot from connecting to the .NET Remoting channel of the Web Portal server, with the goal of 'back door' entry to the middle tier server (Master Service). In most cases, the Master Service will issue an alert email if it detects anomalous behavior, containing the calling source IP and event detail.

There are no "central administrator" or "settings" pages directly in the Web Portal pages, which could be used to compromise domain security.

Basically, our product is designed from the ground up to be an externally deployable solution. It is easy to install, easy to use, highly secure and completely brandable.

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.