

Application Password Management Module

e-DMZ Security's Application Password Management (APM), part of the TPAM Suite of privileged user and access control solutions, provides a solution to replace embedded passwords that are hard-coded in scripts, procedures and programs with simple CLI/API calls. Often overlooked, embedded passwords create back-door access accounts to target systems and applications that can easily be exploited. Replacing these hard-coded passwords with programmatic calls that dynamically retrieve the account credential removes this often overlooked exposure. APM comes standard with our Password Auto Repository™ (PAR) appliance, or as an optional add-on bundled with our Privileged Password Management (PPM) module for eGuardPost™ appliance. Key features include:

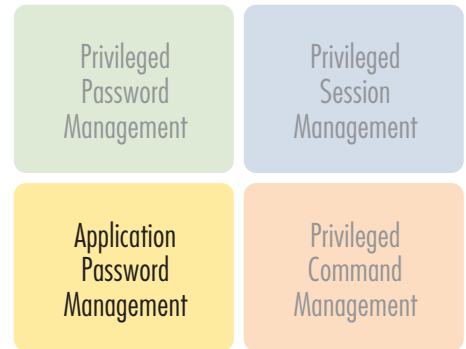
Programmatic Access: APM supports both Command Line Interface (CLI) access and Application Program Interface (API) for C++, Java, .NET and Perl. Connectivity is via SSH with DSS key exchange.

Role Based Access: As with interactive access, APM supports role-based access for CLI/API, added as "programmatic" user with either a "basic" access (eg. Requestor) or "admin" access. With basic access, the CLI/API is granted permission to request account passwords for authorized target(s)/account(s). With admin access, the CLI/API is able to perform administrative tasks.

Extensive Command Set: e-DMZ Security offers the most extensive command set via the CLI/API. Beyond just "Get Password" commands for replacing hard-coded passwords, APM supports extensive admin level commands to support tight integration with existing enterprise tools and workflows.

The types of commands available include:

AddAccount	DeleteAccount	ListGroupMemberShip	SetPermission
AddAlias	DeleteSystem	ListPermissions	TestSystem
AddCollectionMember	DeleteUser	ListRequest	UnlockUser
AddGroupMember	DropCollectionMember	ListRequestDetails	UpdateAccount
AddUser	DropGroupMember	ListSystems	UpdateAlias
Aprove	GetPassword	ListUsers	UpdateSystem
Cancel	GrantPermission	Retrieve	UpdateUser
ChangeUserPassword	ListAccounts	RetrieveWithTicket	
CheckPassword	ListCollectionMembership	RevokePermission	



APM Highlights:

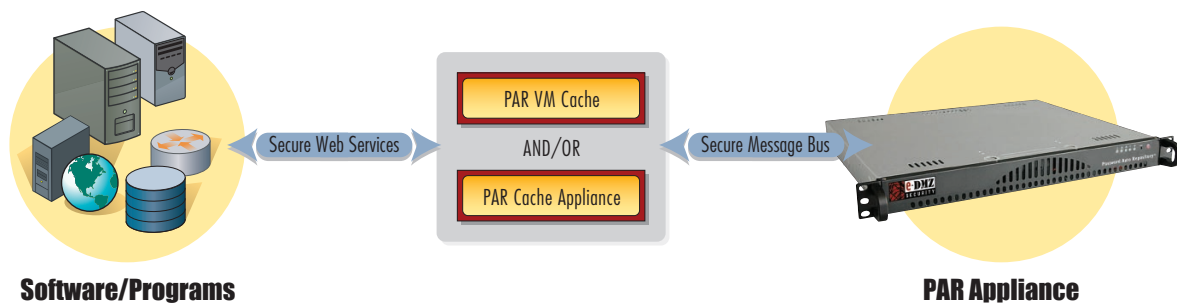
- Command Line Interface (CLI)
- Application Interface (API) including:
 - C++
 - Java
 - .NET
 - Perl
- Role based secure programmatic access
- Extensive command support
- Supports integration with existing workflows
- Optional Cache to support high-demand A2A/A2DB

Application Password Management Module

Performance: Depending on the execution characteristics of the script/program, performance requirements can vary – for programs that execute once, retrieve required credential(s) and store them in local memory, performance requirements of the programmatic interface are minimal. Other programs may execute at a higher frequency requiring performance in the tens or hundreds of calls per second. The most demanding applications can require tens or hundreds of calls to “get password” per second.

The CLI/API can natively handle call requests in the 100 per minute range. For those application requirements that require enhanced performance, we provide an optional PAR Cache add-on.

PAR Cache: PAR Cache is an optional add-on to APM. Deployed as an external appliance or VM based cache, each PAR Cache is able to support over 1,000 password requests per second. This level of performance is able to meet the requirements of the most demanding applications.



Key architectural features of PAR Cache include:

- Physical or Virtual Appliance
- Hardened Linux O/S (JeOS)
- J2EE Server
- DBMS, used for temporary storage
- Full disk encryption with boot encryption
- Secure bus for communication to/from PAR
- Client/application access via Secure Web Services