

Central console
for tracking, managing,
auditing, and securing
information assets
throughout an organization



Mobile Armor® PolicyServer™

In an environment of devastating security breaches, increasingly demanding privacy and security regulations, and on-the-go employees using stationary, mobile, and removable devices, enterprise and government organizations need the most technologically advanced, comprehensive, and scalable security policy management and compliance enforcement solution.

Mobile Armor has developed such a solution in the Web services-based PolicyServer which easily manages and enforces enterprise security policies for the entire suite of Enterprise Mobile Data Security™ solutions across desktops, laptops, PDAs, Smartphones, removable storage devices, and other critical computer systems.

Security administrators manage all users and devices through the PolicyServer Microsoft Management Console (MMC) using a Windows Explorer-like interface. They create security policies for users, groups, subgroups, and devices that transform business rules into an easily implemented security reality. Encrypted communication and policy updates are delivered over-the-air to mobile devices and on boot-up to networked devices with no impact to performance or intervention from the user.

Security applications traditionally have soaring password reset costs, which PolicyServer mitigates with several password reset choices that users can perform securely without administrator intervention.

PolicyServer provides audit trail, compliance, and system metric reports to management that help define the impact of the security management system and meet regulatory requirements.

Mobile Armor's PolicyServer is the centerpiece for a complete suite of security solutions that add multiple layers of security to protect an organization from the outside world. PolicyServer provides a single point for administrators to easily track, manage, and secure information assets throughout an organization and to provide compliance and performance reports.

Mobile Armor PolicyServer™ offers scalable, auditable, cross-platform enterprise security for multiple devices managed from a single console for a defensible security perimeter—especially as boundaries are pushed by mobile users ...

Benefits

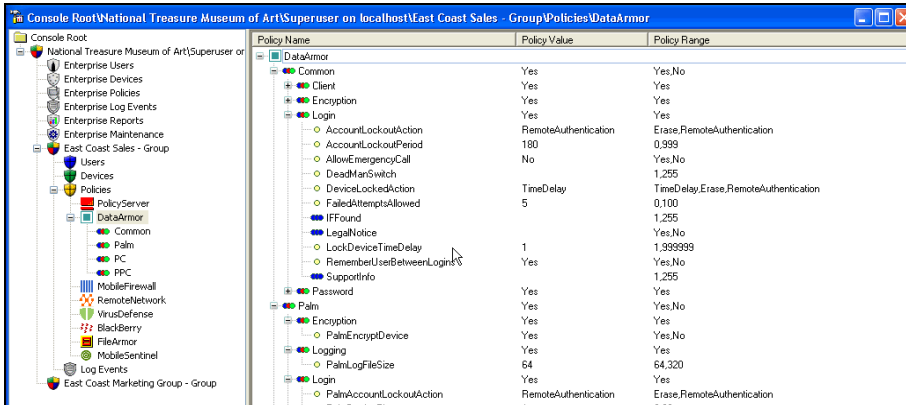
- Centralized administration through the PolicyServer Microsoft Management Console (MMC)
- Full visibility into which devices and users are connected to the network
- Automatic updates to non-compliant programs and assurance that only corporate-sanctioned software is installed
- Over-the-air security policy enforcement and device wipe to mitigate risk for lost or stolen devices
- Automatic or on-demand reporting to inform management and help administrators refine the system
- Event logging and compliance managed, monitored, and enforced across multiple devices, hardware, and operating systems
- Enterprise scalable, Service-oriented Architecture (SOA)—an ideal fit for large organizations with geographically diverse operations

Managed Service Provider

- Security and vulnerability management, threat management, secure content management, and identity and access management as part of a complete end-to-end mobile data security solution for enterprise customers
- Flexibility to offer enterprise customers administrative management at MSP's site

Enterprise

- Transparent deployment, protection, and usage for user
- Flexibility to install and manage PolicyServer management console on enterprise servers or at the MSP's site
- Seamless integration with widely accepted third-party software such as anti-virus, firewall, and VPN with minimal effort



PolicyServer Hierarchy

Administrators have a central view of all Mobile Armor applications from one management console through the PolicyServer Microsoft Management Console (MMC). Pictured above, the interface window has a tree structure on the left and a results window on the right.

The icons at the top of the tree structure are used to manage the enterprise and the colored icons are used to manage the groups and sub-groups. Administrators can set policies for each group and subgroup, add users, add devices, and enable and disable applications.

The following roles exist in PolicyServer:

- **Enterprise Administrator** – controls the entire enterprise and has administrative rights to all groups, subgroups, users, and policies
- **Group Administrator** – manages one or more groups when assigned as the administrator
- **Enterprise Authenticator** – assists with remote authentication for the entire enterprise
- **Group Authenticator** – assists with remote authentication for a specific group
- **User** – makes use of the system, but is not assigned administrative or authenticator duties or responsibilities

Features

- Central management and reporting on all components under a single management console
- Enterprise scalable, Service Oriented Architecture
- User-centric management
- Multiple operating systems and hardware configurations
- Extensible management of third-party software
- Password recovery option for users
- Active Directory integration

Device Support

- Desktops, laptops, and tablets
- PDAs, Smartphones, and Pocket PCs

Groups

A PolicyServer group compartmentalizes a group's users by restricting access to the data and information available to them by setting policy for the group. Setting policy at a group level and compartmentalizing the user minimizes the risk of loss due to accidental release of information or deliberate sabotage.

Adding a group at any level also adds the group icons for Users, Devices, Policies, Log Events, and Scheduled Events. Users must be added to a group to become members of a group. Each group added to a group is a subgroup. Each group displays the applications available, as is seen in the above screenshot, which shows those of the East Coast Sales Group.

Modules in PolicyServer

PolicyServer includes the following modules:

- **PolicyServer Database** – stores all users, devices, and groups, and is the staging table for logs. This module also includes the PolicyServer Log Database, which is used for long-term storage and allows the administrator to search the stored data for trends such as security violations.
- **PolicyServer MMC Plugin** – provides the capability to manage the enterprise security policies, groups, users, and devices
- **PolicyServer Web Service** – allows the DataArmor™ or FileArmor™ client to communicate with PolicyServer via the Internet or Intranet
- **PolicyServer Windows Service** – accesses the database and retrieves data in response to DataArmor or FileArmor client requests.
- **Active Directory** – provides an interface that allows administrators the capability to import groups and users from Active Directory to PolicyServer

Operating System Support

- Microsoft® Windows Server 2000 or 2003
- Microsoft Windows XP Professional, Tablet Edition
- Windows Mobile 2003, 5.0
- BlackBerry Enterprise Server 4.1

Hardware Requirements

- CPU make/speed required 1 GHz minimum
- 512 MB memory minimum
- 20 MB hard drive minimum

Software Requirements

- Fast strong encryption using AES or DES
- Internet Information Services (IIS) with ASP.NET installed, including latest Service Packs (SP)
- Microsoft® SQL Server 2000, SP4 or
- Microsoft® SQL Server 2005 SP2
- Microsoft® .NET Framework 2.0 SP1

Email Messaging Requirements (Optional)

- Microsoft Active Directory for Active Directory administration integration

RSA Server Requirements (Optional)

- RSA Authentication Manager 6.0

Administrator authentication

Security Administrators and Security Authenticators must authenticate to PolicyServer before access is granted. This authentication is separate from logging in to the computer. They can authenticate using fixed password, RSA SecurID, or Common Access Card.

Password reset

PolicyServer provides the following password reset methods for users to mitigate the normally high cost of password reset:

- **Microsoft Windows Active Directory** – recommended if the user has access to the Help Desk, network connectivity to PolicyServer, and Windows Single Sign-on (SSO) enabled.
- **PolicyServer MMC** – recommended when SSO is not being used. A one-time password is assigned within the PolicyServer MMC.
- **Remote Help** – designed for organizations that do not use X9.9 hardware tokens. The user contacts the Help Desk to obtain an X9.9 response. Remote Help allows the administrator to use either the Soft Token option or a hard token.
- **Reset Help** – similar to Remote Help, but does not allow for the administrator to use a hardware token.
- **Self Help** – provides QA (personal challenge), email, and combination QA/email options.
- **WebToken™** – designed to allow one-time access to a device when the user's password has been forgotten or the physical token is lost. This method requires network connectivity and may be used independently of Help Desk assistance.

Mobile Armor Security Suite

- *Comprehensive security suite*
Complete security for all mobile devices and platforms
- *Enterprise-class service oriented architecture*
Scalable and standards-based with centralized management
- *Revolutionary technology*
First 32-bit pre-boot authentication full-device encryption product, ensuring device data security through revolutionary authentication technology, advanced administration, and user transparent data encryption
- *Transparent operation*
- *Cross-platform user-centric management*
- *Comprehensive cross-platform support*
- Single-user security for multiple devices and applications
- *Integration with existing infrastructure*
- *Minimized operating cost*
- *Audit reporting*
- *Centralized administration*