



PolicyServer™ and DataArmor™

Deployment Best Practices



Table of Contents

Overview	1
Customer Preparation.....	1
Assigning a Project Team.....	1
Transferring Knowledge	2
Piloting the software	2
Communicating with the End-user Community	2
Product Architecture.....	3
PolicyServer.....	4
PolicyServer Components	4
PolicyServer Database	5
PolicyServer Log Database.....	5
PolicyServer MMC Plug-in	5
PolicyServer Active Directory Plug-in	6
PolicyServer Web Service	6
PolicyServer Windows Service.....	6
PolicyServer Blackberry Service	6
Prerequisites	7
Hardware.....	7
Software	8
Windows Server	8
Microsoft SQL Server.....	8
Microsoft .NET	8
VMware	8
Permissions	9
PolicyServer Database Setup	9
PolicyServer Windows Service.....	10
PolicyServer AD Plug-in.....	12
Scaling the PolicyServer	15
Application Server	15
Database.....	15
Installation Considerations	16
PolicyServer Database	17
PolicyServer Log Database.....	18
PolicyServer MMC Plug-in	18
PolicyServer Web Service	18
PolicyServer Windows Service.....	19
PolicyServer AD Plug-in	19
Initial Configuration	20
Enterprise Policies	20
Groups/Users	21



Group Policies.....	21
PolicyServer Administration.....	22
Active Directory	22
Active Directory Retrieval Wizard	23
Active Directory MMC Plug-in	23
Domain Authentication.....	23
Logging/Reporting	24
Known Issues.....	24
<i>DataArmor for PC.....</i>	<i>25</i>
DataArmor Components	25
DataArmor Operating System (DAOS)	26
DataArmor OS (DAOS) Startup Process	27
DataArmor Encryption Engine (MABACKFILE).....	28
DataArmor Windows Service (MobileSentinel).....	28
DataArmor Installation	30
Manual Installation	30
Automated Installation.....	30
Encryption	34
Domain Authentication.....	35
DataArmor Password Sync Utility	36
RSA SECURID Setup.....	36
RSA SecurID Two-factor Authentication Setup.....	37
RSA SecurID Domain Authentication/Single Signon Setup	37
Known Issues.....	37



Overview

The purpose of this document is to provide Mobile Armor customers with “best practices” from previous Mobile Armor deployments. While this guide may offer insights and tips to deploying the Mobile Armor security product suite, it is not a substitute for proper evaluation of the product or software training for administrators.

This document is intended for Senior Managers, Project Managers, Security Administrators, and Help Desk personnel responsible for deploying the Mobile Armor software suite within the enterprise.

Customer Preparation

The Mobile Armor product suite is designed to be managed at the enterprise level to ensure enterprise-wide security. As with any application that impacts all users within an organization, it is highly recommended that a project team and project plan be developed for managing this software deployment project.

The “Customer Preparation” section is designed to provide information that has been helpful in previous deployment experiences when internally facilitating a successful installation of the Mobile Armor product suite.

Assigning a Project Team

It is assumed that the reader of this document has performed a software evaluation of the Mobile Armor product suite and Mobile Armor’s product suite was selected to protect the integrity of your enterprise data.

Best Practice: A successful implementation of any software product deployment always includes maintaining continuity as well as achieving “buy-in” from the internal users. Maintaining continuity results from strong leadership in the project team and achieving buy-in results from structuring the “project team” to include one or more strategic members from the departments impacted by the software deployment.

At a minimum, it is recommended that the project team include one or more members from each of the following groups:

- Executive Management
- Enterprise Application Servers
- Enterprise Database Administrators
- Data Security
- Desktop Support
- Disaster Recovery



Transferring Knowledge

The Mobile Armor product suite is designed to be transparent from an end-user's perspective, requiring little or no training; however, it is highly recommended that organizations fully utilize the training opportunities available for Administrators and Desktop Support/Help Desk Personnel.

Best Practice: Many organizations have found Mobile Armor's "train-the-trainer" offering very successful for the Desktop Support/Help Desk Personnel. The most effective method of knowledge transfer for Administrators is Mobile Armor's three-day certification training course.

Piloting the software

Mobile Armor recommends that organizations run a pilot or "sample" group of users and machines before deploying Enterprise-wide which allows an organization to finalize the deployment methodology to use when installing the DataArmor software.

To be effective, the pilot group should span departments and target users and devices that are disparate. For example, if your organization supports ten different manufacturers of laptops and DataArmor will be installed on all ten device types, then each of those devices should be included in the pilot. Similarly, if certain high-profile groups are of particular concern, one or two members of the groups should be enlisted to participate in the pilot. In general, corrections, changes to the process and/or the ability to navigate through corporate approval methods are greatly enhanced when working as a pilot group.

Even after the initial pilot of the software if you are introducing new equipment into the environment you should pilot the hardware with the latest Mobile Armor software to ensure there are no issues with drivers for the network card or smart card reader at the pre-boot.

Communicating with the End-user Community

Mobile Armor strongly suggests that the executive sponsor of the data security software project send a message to the enterprise users communicating the importance of the project to the company and the benefits to the users.

Additionally, the use of a Virtualization Application to capture video for internal training of end user procedures for normal login, web token login, and password reset is also recommended for end user training and familiarization.



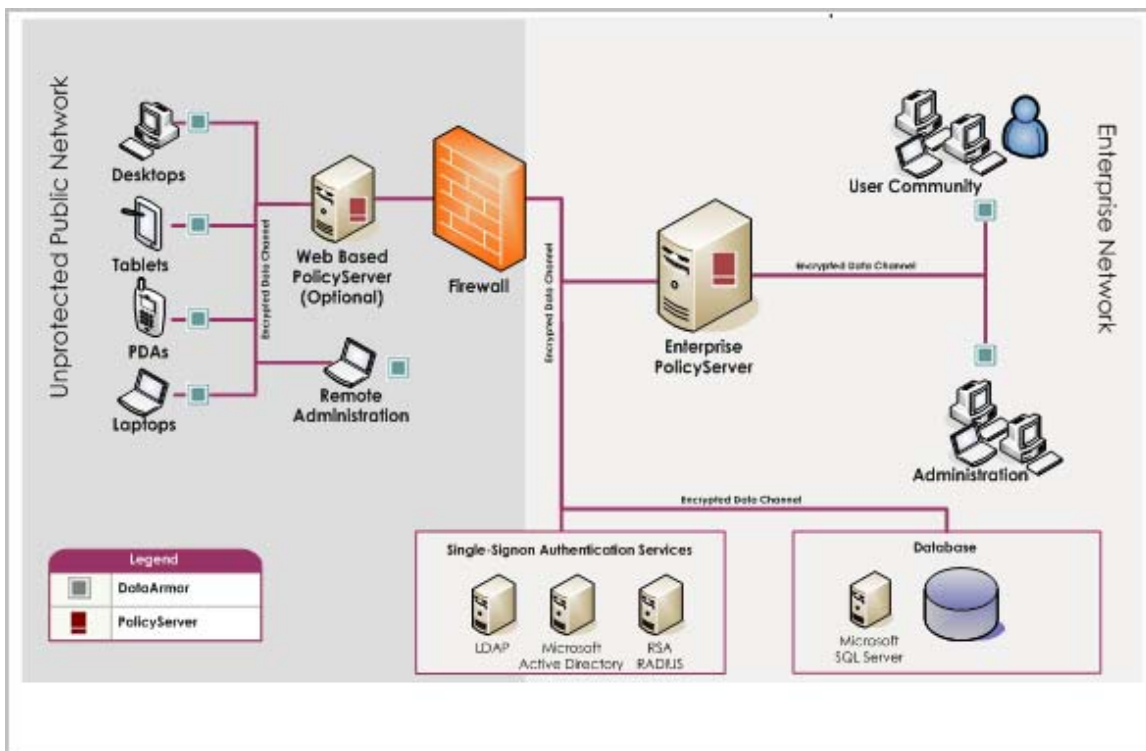
Product Architecture

From a deployment perspective, the Mobile Armor product suite has two components:

- PolicyServer
- Client applications

This guide focuses on PolicyServer and its relationship with Mobile Armor's pre-boot authentication and full-disk encryption client application — DataArmor.

The diagram below is just one many possible configurations for distributing the Mobile Armor products throughout an organization. If this diagram does not meet your needs, your Mobile Armor technical representative is available to assist you in designing a more suitable configuration for your enterprise.





As shown in the diagram, the Mobile Armor PolicyServer is configurable to run inside or outside the corporate firewall and can be managed from any number of locations. In addition,

- All communications between the DataArmor client software and the PolicyServer are encrypted.
- The PolicyServer database may exist on the same machine as the PolicyServer or in a separate location (not depicted).
- The PolicyServer platform is entirely web-services based and is designed to implement easily with other enterprise authentication mechanisms.

Also illustrated is the Authentication Services that are natively available, such as LDAP, Active Directory and RSA support.

PolicyServer

Administration is a principle concern with any software deployment, and even more so for security software. PolicyServer is the leading solution for extensible and scalable Enterprise Mobile Data Security (EMDS™) administration, and the centerpiece of Mobile Armor's product suite. Policy Server is a powerful tool that offers centralized policy management from a single self-service console across heterogeneous devices; allows delegation of administration for end users; and provides the capability to enforce and report on compliance across all deployed devices ensuring consistency, integrity and availability for your critical data.

All Mobile Armor products are integrated with PolicyServer's advanced security management framework. Utilizing this advanced framework empowers you to design and easily manage comprehensive security policies, maintaining consistent security policies across all types of data and devices.

PolicyServer Components

Mobile Armor's PolicyServer is comprised of the following components:

- PolicyServer Database
- PolicyServer Log Database (optional)
- PolicyServer MMC Plug-in
- PolicyServer Active Directory(AD) Plug-in (optional)
- PolicyServer Web Service
- PolicyServer Windows Service
- PolicyServer Blackberry service (optional)



PolicyServer Database

The PolicyServer Database stores all users, devices, and groups, and is the staging table for logs, in addition the database:

- Stores all keys that may be used for authentication or recovery in an encrypted state.
- Should be maintained by the SQL Server group just as any other database is within the organization.

Best practice: Perform nightly backups on the database once it is considered a production instance.

Many organizations also choose to replicate the SQL server in order to provide instant back-ups should a failure occur. Similarly, larger organizations choose to run the database in a cluster or a SQL farm to provide failover and recovery assistance. Mobile Armor supports all of these activities and recommends that organizations maintain the PolicyServer database in the same manner as they do all other Enterprise databases.

PolicyServer Log Database

The PolicyServer Log Database provides a repository for transactions such as user logins and user/group/device management. The Log Database is used for long-term storage and is managed by an administrator, with the capability to search the stored data for trends, such as security violations. It is recommended that organizations use the Log Database as the engine for enterprise reporting. The Log Database can be populated only by running the Windows Event named "Populate Log DataMart Event".

A log table exists in the PolicyServer Database. As an alternative to the Log Database reports may be run from that table. However, Mobile Armor recommends that all reports are run from the Log Database to avoid any performance degradation to the main database.

PolicyServer MMC Plug-in

The PolicyServer MMC Plug-in provides the capability to manage the enterprise security policies, groups, users, and devices. The MMC is designed to be installed on any machine that manages the enterprise. The MMC may administer the PolicyServer from the Enterprise or group level. The only prerequisite is that Microsoft .Net version 1.1.4322 is installed



PolicyServer Active Directory Plug-in

The Active Directory Plug-in provides an interface that allows administrators the capability to import groups and users from Active Directory to PolicyServer.

PolicyServer Web Service

The PolicyServer Web Service is an IIS based web service that communicates with the DataArmor clients via AES encrypted communications. The web service utilizes port 80 for all communications and no other port may be used for this purpose. The web service also communicates with the MMC and passes communications to the Windows Service.

PolicyServer Web Service and PolicyServer Windows Service **must** be installed on the same machine.

PolicyServer Windows Service

The PolicyServer Windows Service accesses the database and retrieves data in response to DataArmor client requests. The Windows Service is the main PolicyServer engine.

Please note:

- The PolicyServer Windows Service and the PolicyServer Web Service **must** be installed on the same machine.
- If using Domain Authentication (Single Sign-on), a new domain account **must** be set up for Windows Service.
- If Domain Authentication (Single Sign-on) is activated after the initial PolicyServer setup, PolicyServer Windows Service **must** be uninstalled and re-installed at that time.
- If installing Windows Service on a domain controller, the user specified **must** be an Enterprise Administrator. **Best practice:** is to not install the PolicyServer on a domain controller.
- The account used for the Windows Service should have a long, complex password and set never to expire.

PolicyServer Blackberry Service

The PolicyServer RSA Service is the conduit between the Blackberry BES Server and the Mobile Armor PolicyServer. The PolicyServer simply manages the policies of the Blackberry BES server.



Prerequisites

The prerequisites for the PolicyServer can be categorized as:

- Hardware
- Software
- Permissions

Hardware

Mobile Armor recommends the server intended to act as the application/web server meets or exceeds the minimum requirements for Windows Server 2003 (PolicyServer also supports the Windows Server 2000 platform).

To view the requirements, click on the link below.

<http://www.microsoft.com/windowsserver2003/evaluation/sysreqs/default.mspx>

Best practice has proven that using multiple web-servers configured with a load balancer or through a DNS lookup table has proven to be the most efficient and effective method for requests and providing failover assistance.

Mobile Armor recommends the server intended to act as the database server meets or exceeds the minimum requirements for Windows Server 2003 (PolicyServer also supports the Windows Server 2000 platform).

To view the requirements, click on the link below.

<http://www.microsoft.com/sql/editions/enterprise/sysreqs.mspx>

PolicyServer does not require a stand-alone server and may run alongside other applications, provided the server is robust enough to satisfy the traffic requests. The PolicyServer data repository has no reported issues when running on the same server as other SQL applications or as part of enterprise clusters. In short, organizations are able to configure their SQL configuration as they would any other enterprise database application.



Software

The following section details the software that **must** be installed for PolicyServer and DataArmor to function correctly.

Windows Server

Mobile Armor supports Windows Server 2000 or Windows Server 2003 and recommends that companies use Windows Server 2003 if available.

- Since Mobile Armor is a web-services based architecture, it is required that the server be configured in an “Application Server” role.
- Similarly, ASP.Net pages **must** be enabled for the server to communicate properly.

For more information on setting up the Windows Server for initial use please see the “Pre-Installation Checklist” appendix of the PolicyServer Administrator manual.

Microsoft SQL Server

Mobile Armor requires Microsoft SQL Server 2000/2005 with the latest Service Packs. The SQL Server **must** be configured in “Mixed Mode” and allowed to start up each time the operating system restarts.

Note: SQL 2000 MSDE and SQL 2005 Express can be used to evaluate the software but are not recommended for a production environment.

Microsoft .NET

Mobile Armor requires Microsoft .NET version 1.1.4322 be installed on all Servers and Clients running Mobile Armor software. Microsoft .NET 2.0 may be used provided version 1.1.4322 is installed as well. Systems running only Microsoft .NET 2.0 are not supported at this time.

VMware

The Mobile Armor PolicyServer may be installed and managed utilizing virtualization software, such as VMware, as the host. However, VMware, especially as it pertains to networking, contains many configurations that may adversely affect the network performance of the Mobile Armor PolicyServer. Mobile Armor may not support issues that pertain to VMware; however, Mobile Armor can suggest VMware settings that have worked in other instances upon customer request.



Permissions

The Mobile Armor PolicyServer contains permission-based functionality that **must** be properly configured to perform as designed.

- PolicyServer Database Setup
- PolicyServer Windows Service
- PolicyServer AD Plug-in

PolicyServer Database Setup

The PolicyServer Database Setup program installs the primary database. This database retains the keys, user information, device information and other pertinent information as it relates to the PolicyServer application.

During the installation of the Mobile Armor Database, the software requests the Server Administrator (SA) account for the SQL database. This or any other SQL administrator account **must** be provided to allow the tables to be created properly. Please note that during the database setup an opportunity to create a new SQL account to manage the Mobile Armor database is provided.

To maintain consistency in the database setup, the team responsible for deployments should involve at least one member of the group that manages the organization's SQL Servers to participate in the "project team".



PolicyServer Windows Service

The PolicyServer Windows Service allows the Mobile Armor PolicyServer to communicate with Microsoft's Active Directory or other LDAP controllers. Both Mobile Armor and Microsoft require specific credentials to perform properly.

Mobile Armor's PolicyServer Windows Service requires a valid AD/LDAP account for performing such actions as:

- Password verifications
- Password resets

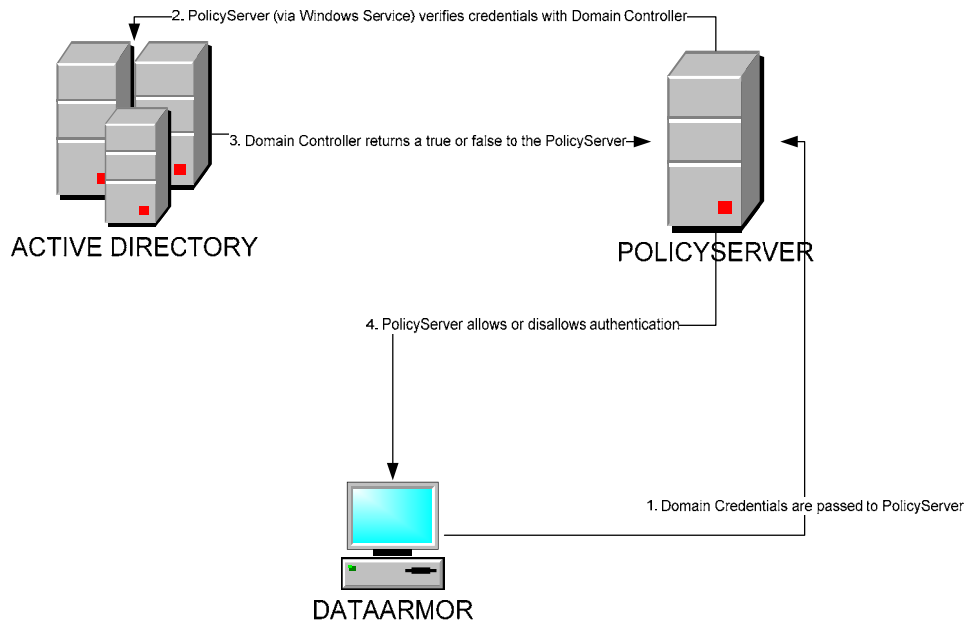
Microsoft requires credentials to:

- Query Active Directory
- Receive responses from Active Directory
- Establish a password change process with Active Directory
- Disable accounts through Active Directory

Depending on how an organization has configured their environment, different user types may provide different results. The PolicyServer Windows Service is the proxy for all those types of requests coming from DataArmor clients and therefore, it is important that the appropriate credentials be granted to the service itself. **Best practice** is to create an account that is granted Domain Administrator privileges to avoid any issues with Active Directory permissions.

Mobile Armor recommends that organizations create a "service account" for the PolicyServer Windows Service. An example of this is adding a user to the Active Directory named "Mobile Armor". The account used for the Windows Service should have a long, complex password and set to not expire.

Note: In some instances, an account lower than domain administrator may be used, i.e. OU Administrator or Department Administrator; provided they have the appropriate privileges. However, using a domain user is not recommended as it is rare that a domain user would have sufficient privileges.



As outlined in the diagram above

1. The DataArmor client passes the credentials entered at pre-boot to the PolicyServer.
2. PolicyServer (with SSO enabled) acts as a proxy to the Domain Controller via the PolicyServer Windows Service validating the user credentials with the domain. *Again, it is necessary for the service to contain domain administrator privileges to make such a request.*
3. The PolicyServer again acts as a proxy and returns either an approved or failed message to the DataArmor client.
4. PolicyServer allows or disallows authentication.



PolicyServer AD Plug-in

The PolicyServer Active Directory plug-in is designed to allow administrators to add/remove users and groups from Active Directory using the PolicyServer MMC. This plug-in should be installed on every machine that maintains the users and groups in PolicyServer.

To install on a machine, the user account logged into the machine must be logged in as an account that **has** permission to modify the Forest Root of Active Directory. In some configurations of Group Policies you may be able to do this as a Domain Admin account. If that does not work you will have to use an Enterprise Administrator account to complete the installation. It is important to note that the Enterprise Admin is not always needed to use the AD Plug-in but only needed for the initial installation. The functions used to modify these pages are shown below.

CN=groupdisplay,CN=409,CN=DisplaySpecifiers,CN=Configuration,DC=*Domain*,DC=com
Attribute: adminPropertyPages

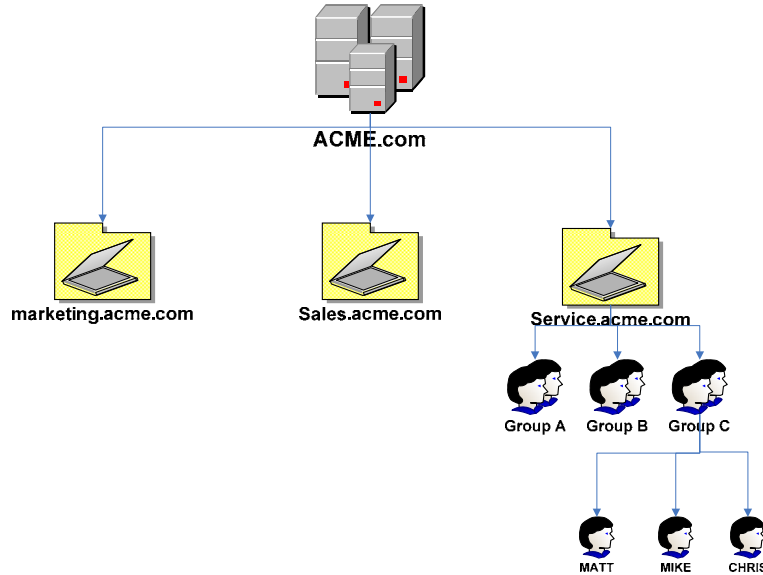
Function	Description
CN=groupdisplay	Indicates that the plug-in intends to modify the property for Active Directory group container(s)
CN=409	Indicates the change will be in the English language
CN=DisplaySpecifiers	Indicates the plug-in will add a tab to the property page display
CN=Configuration	Indicates the plug-in will configure the property page
DC=Domain	Indicates the domain in which the local machine is a member
DC=com	Translated as .com to the DC=Domain parameter as in XYZ.com
Attribute:Adminpropertypages	Indicates that the attribute to modify is the adminpropertypages



CN=user-Display,CN=409,CN=DisplaySpecifiers,CN=Configuration,DC=Domain,DC=com
Attribute: adminPropertyPages

Function	Description
CN=user-display	Indicates that the plug-in intends to modify the property for Active Directory user container(s)
CN=409	Indicates the change will be in the English language
CN=DisplaySpecifiers	Indicates that the plug-in intends to add a tab to the property page display
CN=Configuration	Indicates that the plug-in intends to configure the property page
DC=Domain	Indicates the domain in which the local machine is a member
DC=com	Translated as .com to the DC=Domain parameter as in XYZ.com
Attribute:Adminpropertypages	Indicates that the attribute to modify is the adminpropertypages

Please note that the Active Directory plug-in does not modify the Active Directory schema; however, the plug-in modifies the property pages of the machine where it is installed. Therefore, if it is installed on HelpDeskPC1 and not on HelpDeskPC2, only HelpDeskPC1 will have the ability to import groups and users via AD.



In the figure above, user MATT is an Administrator for the Service.acme.com Organizational Unit (OU) for Acme Corporation. MATT is attempting to install the Active Directory plug-in and receives a message that his permission is not sufficient to do so. It is very important to realize that the change the Active Directory plug-in is requesting is at the domain level or Acme.com. Unless the user has permission to make changes at the domain level, the plug-in will not be allowed to continue. MATT has full access to the OU of the domain but not the domain itself. Therefore he is not allowed to make the required changes.

MATT **must** find an administrator for the acme.com domain to install the plug-in for him. That administrator's credentials are only required for the initial installation.

Please contact your Active Directory administrator if questions remain regarding individual permission levels.



Scaling the PolicyServer

When considering an Enterprise application such as Mobile Armor's security suite, a discussion point should certainly be scalability. Mobile Armor is the most scalable solution in the marketplace today. Our data security suite has two main components:

- Application server
- Database

Application Server

Mobile Armor's PolicyServer is built on web-services architecture and in many ways the PolicyServer can be scaled much like an enterprise web-site. The PolicyServer is designed so that as the load increases an organization can simply add more application servers to handle the increased traffic. This allows organizations to quickly and inexpensively react to changing conditions. In general, an enterprise class application server can handle approximately 20,000 client devices before performance begins to diminish.

An enterprise class server is defined as:

- Dual Processor (or more) Pentium 4
- 100 GB+ HD
- 4+ GB RAM

Results may differ depending on the strength of the server being used as the application server. However, if performance decreases, it is best practice to add another application server and bridge it with the existing server either through the use of a load balancer or through DNS addressing.

Database

The PolicyServer database is built upon the Microsoft SQL Server 2000 platform. Therefore, any functionality that natively exists in SQL Server 2000 such as distributed databases and clustering is natively supported by the PolicyServer. In general, the concern of the SQL Administrator is the size of the database. Administrators may use the following calculation when sizing the database(s):

$$(((\text{Number of Users} * 5366) + (\text{Number of Devices} * 2471) + (\text{Number of Groups} * 3392))/1024)/1024 = \text{Mobile Armor Database in Megabyte (MB)}$$

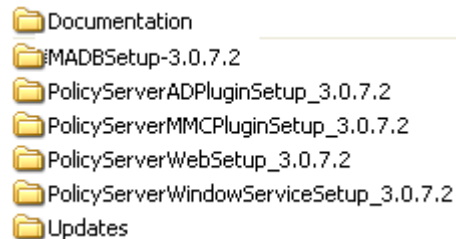
For the Log database a similar calculation may be used to size the database. That calculation is:

$$(((\text{Number of Users} * 2) * 3951) * \text{Number of days logs are kept})/1024)/1024 = \text{Mobile Armor Log Database in Megabyte (MB)}$$



Installation Considerations

The software folders required to properly install the PolicyServer are illustrated below. If one or more of the defined folders are not available in the software package you received please contact your Mobile Armor representative.



Note 1: The software **must** be copied from the CD/Network Share/Removable Media onto the server and run from the local C Drive. If run from the CD/Network Share/Removable Media, the installation packages attempt to write a temp file to the software directory and will fail.

In general there is no order of installation outside of the database being installed first. However, one installation order has proven more efficient than any other:

1. MADBSetup – Installs both the primary & log databases (**required**)
2. PolicyServer AD Plug-in & MMC on remote clients
3. PolicyServer MMC Plug-in. Server only, remote clients are typically installed last. (**required**)
4. PolicyServer WebSetup (**required**)
5. PolicyServer Windows Service (Requires a reboot) (**required**)

Note 2: PolicyServer Blackberry, RSA, and AD Plug-in are optional components. Installation should be performed as described in the PolicyServer Administrator guide if needed.

Note 3: The AD Plug-in is the Best Practice way to import users from AD into the Policy Server. However if the AD Plug-in cannot be installed there is a built in component in the Policy Server MMC which can be used.



PolicyServer Database

When installing the PolicyServer database:

- The SQL Server Administrator account (SA) **must** be used for initial installation.
- The machine where the MADB Setup is Ran from the logged in user must have permission to write to the C:\Windows\System32 directory.
- PolicyServer allows administrators to create a unique SQL administrator account for the PolicyServer database(s) only.
- The database may be installed on any distributed database or server cluster.
- The database may be installed on the default or any named instance.
- The database installation may be “run” from any machine as long as the proper database is entered in the database location fields.
- The database is approximately 12 MB in size but may grow significantly if logs are not cleared.
- The database may be queried but sensitive fields such as passwords and encryption keys are stored in an encrypted state.
- If you are installing on a SQL named instance, you must provide the SERVERNAME\INSTANCE name for the install to work properly.

Best practice is to perform a nightly backup of this database.



PolicyServer Log Database

When installing the PolicyServer Log Database:

- The installation of the Log Database requires the same parameters as the main database.
- The Log Database is only populated by running the Windows Event named “Populate Log DataMart Event”.
- While built-in reporting tools exist on the MMC plug-in, more robust reporting may be obtained by using a tool such as Crystal Reports.
- The database supports any reporting tool that has the ability to query a SQL database.

Best practice is to offload the Log Database every 60 days to network storage and run the Windows Event “Remove Logs Event” to eliminate any old logs.

PolicyServer MMC Plug-in

When installing the PolicyServer MMC Plug-in:

- The MMC may be installed on any Windows 2000 SP4+ or higher machine.
- If installed remotely, access to the PolicyServer is required either via network or VPN connectivity.
- The MMC communicates over Port 80 via an encrypted channel. No other port may be used for this purpose.
- The MMC Plug-in requires that the Microsoft.Net 1.1.4322 framework is installed on the host PC.

Note: Microsoft .NET 2.0 may be used provided version 1.1.4322 is installed as well. Systems running only Microsoft .NET 2.0 are not supported at this time.

PolicyServer Web Service

When installing the PolicyServer Web Service:

- The Web Service **must** be installed on the server functioning as the Application Server.
- The Web Service and Windows Service **must** be installed on the same physical machine.
- The virtual directory “MAWEBSERVICE2” should not be changed.
- The MMC communicates over Port 80 via an encrypted channel. No other port may be used for this purpose.



PolicyServer Windows Service

When installing the PolicyServer Windows Service:

- The Windows Service **must** be installed on the server functioning as the Application Server.
- The Policy Server Windows Service and Web Service **must** be installed on the same physical machine.
- If using Domain Authentication, a new domain account **must** be created and used for installation of the Windows Service. It is highly recommended that this account has domain administrator privileges and has a long complex password set not to expire.
- If Domain Authentication is enabled *after* the initial installation, the Windows Service **must** be uninstalled and reinstalled for domain authentication to perform properly.
- It may be necessary to access the service and enable rights to start the service at OS boot. Please see the PolicyServer Administrator Guide for details on this action.

Best practice is to install the Windows Service on a *non*-domain controller. However, if the Windows Service is installed on a domain controller the account used to install the Windows Service **must** be that of Enterprise Administrator.

PolicyServer AD Plug-in

A few points to consider when installing the PolicyServer AD Plug-in:

- The AD Plug-in should be installed on the machine where the server administration takes place. The plug-in is not designed to be installed on the server only, but rather a distributed tool.
- The permission required to use the PolicyServer AD plug-in is domain administrator.

Note: In some configurations of Group Policies you may be able to do this as a Domain Admin account. If that does not work you will have to use an Enterprise Administrator account to complete the installation. It is important to note that the Enterprise Admin is not always needed to use the AD Plug-in but only needed for the initial installation.

- Receiving an access denied error message indicates that the user attempting to install the plug-in does not have sufficient privileges to do so.

Best practice is to install the PolicyServer AD Plug-in tool on a limited number of machines, as it is very powerful in its ability to make modifications to the PolicyServer and Active Directory. Therefore, care should be taken when choosing which roles in the organization are allowed to utilize the functionality.



Initial Configuration

Once PolicyServer and its subcomponents installation is completed, the initial configuration may take place.

Best practice is to configure the PolicyServer in the following order:

1. Enterprise Policies
2. Groups/Users
3. Group Policies
4. Reports/Windows Events

Enterprise Policies

The Mobile Armor PolicyServer enables organizations to set broad policies at the Enterprise level and further define those policies in the granularity desired through the addition of groups. Mobile Armor recommends that the Enterprise Administrator should (1) configure the Enterprise policies first so that all new groups will inherit the base set of policies providing immediate protection and (2) the Enterprise policies should be generic in nature.

Further restrictions to the Enterprise policies may be enacted at the group level. For example, many organizations have different standards for length or complexity of password. The enterprise level policies should allow less restrictive measures, permitting the group level administrators to set stronger password restrictions for the group policy when appropriate.

Please note that a policy change at the enterprise level does not propagate to existing groups; in this same scenario, new groups added to the enterprise will inherit any new settings from the enterprise level. However, once the groups are added to the PolicyServer, an administrator cannot make an enterprise policy change and expect that change to propagate to the groups. Any existing groups requiring the new policies **must** be modified individually to reflect the changes.



Groups/Users

After configuring the Enterprise policies, the next step is to configure the Groups and Users. **Best practice** is to define groups and users in the following manner:

1. Identify Enterprise Administrators and Authenticators
2. Import/create the Enterprise Administrators and Authenticators
3. Identify the Groups
4. Import/create the Groups
5. Identify the Group Administrators and Authenticators
6. Import/create the Group Administrators and Authenticators
7. Identify the Users to be assigned to each Group
8. Import/create the users to each Group

The PolicyServer allows users and groups to be added on a singular basis. This, in general, is acceptable for test scenarios but many organizations desire the ability to import users from Active Directory. For those administrators importing using Active Directory please see the section “Active Directory” in this document.

To minimize access to computers/devices within a group and ensure a more secure environment, **Best Practice** is that organizations create more than one group to classify users. A single group with all users as members allows any member access to any device in that group. In this scenario, anyone with a valid domain account can access any machine in the enterprise. Mobile Armor also recommends that groups are either created by department or organizational unit. Further, a properly defined Active Directory schema is a good template for defining the PolicyServer schema.

Group Policies

As groups are added to the PolicyServer, either manually or from Active Directory, they inherit the policy values set at the enterprise level. If the “generic” set of Enterprise policies provides the required protection for a specific group, it is not necessary to reconfigure that group’s policies.

Many organizations find it important to further restrict policies relating to communication thresholds, password reset timelines and the like for groups with sensitive members, such as an executive group. Mobile Armor recommends that all informational fields (Support info, If Found, Self Help) be configured at the group level. This allows organizations to fine tune user-based information to make it more useful. However, if the organization uses only one help desk and provides only one support number no matter who the user is, then this should be entered at the Enterprise level and inherited by the groups.



PolicyServer Administration

The PolicyServer is administered via the MMC plug-in. This application may be run on any Windows 2000 SP4, XP or higher desktop where Microsoft .Net framework version 1.1.4322 is installed. Similarly, the PolicyServer may be administered from any location with access to the PolicyServer such as a remote location with a VPN.

After the initial installation, administrator accounts associated with specific individuals should be created to provide a better audit trail of administrative changes. The initial Enterprise Administrator account should only be used in case of emergency when other accounts are no longer available. In all cases, the Enterprise account for the PolicyServer should be known by a select number of people. To ensure the highest level of security, Mobile Armor recommends that the enterprise account be split across two or more individuals, i.e. an 18-character password is assigned — Individual A knows the first 6 characters, Individual B the second 6 characters and Individual C the final 6 characters. In this instance three individuals are required to login when making any changes to the Enterprise. In general, very few changes should be made at the enterprise level once the production environment has been setup. Additional groups may be required although organizations do not typically modify the enterprise level past the initial configuration.

Group level administration is much more common. Activities such as password resets, log queries, groups additions/deletes are activities typically performed by group administrators. It is important to stress that group administrators are properly defined in the PolicyServer. A group administrator should be permitted to modify only the specific group for which he/she is responsible. It is not recommended to create 'generic' group administrator accounts.

It is also at the group level that the role of Authenticator becomes useful. The Authenticator role is designed for help desk personnel who are allowed to view the PolicyServer and reset user passwords. Essentially the Authenticator role is read-only with the ability to modify the password fields only. This role should be assigned to any Level 1 support personnel who is responsible for light troubleshooting related to a user's inability to access their PC/Handheld.

Active Directory

PolicyServer contains the following methods for adding users and groups from Active Directory.

- Active Directory Retrieval Wizard
- Active Directory MMC Plug-in



Active Directory Retrieval Wizard

The Active Directory Retrieval Wizard is designed for organizations that elect not to use the Active Directory Plug-in. The AD Retrieval Wizard polls Active Directory for the groups and users contained within, and as such it consumes more processor and bandwidth cycles than the AD Plug-in.

Many organizations choose to use this feature to avoid changing domain permissions for administrators; specifically, organizations that assign PolicyServer management to a group without control over Active Directory may find using the Retrieval Wizard a more efficient process.

Active Directory MMC Plug-in

The Active Directory Plug-in is the quickest and most efficient way to manage users and groups within the PolicyServer product. The plug-in is simply a MMC snap-in that makes use of Active Directory Users and Computers components. AD Users and Computers **must** be available on the machine where the plug-in is installed. The ADMINPAK.MSI located on a Windows Server 2003 CD installs the necessary AD components required by the plug-in.

In some configurations of Group Policies you may be able to do this as a Domain Admin account. If that does not work you will have to use an Enterprise Administrator account to complete the installation. It is important to note that the Enterprise Admin is not always needed to use the AD Plug-in but only needed for the initial installation. The AD plug-in requires the credentials be allowed to change the Active Directory property pages for the local computer.

Domain Authentication

Domain Authentication, often referred to as Single Sign-On, is the ability for a DataArmor installed client to use a Windows Domain Credential to authenticate to the pre-boot and automatically be presented to the Windows desktop without the need to enter credentials at the Windows GINA. From a server standpoint there are only two settings: Enable Domain Authentication and provide the proper hostname. The value that should be populated in the hostname is the domain name such as "mobilearmor".

Note: The addition of ".com", ".net", ".org" or similar will cause Domain Authentication to fail.



Logging/Reporting

The PolicyServer contains logs on **all** activity that occurs in the enterprise as it relates to DataArmor software. Care **must** be taken with the log files so as not to let them grow too large. The logs should be archived per organizational directive and should be deleted once the archive is established. To ensure the correct log file is selected for any report, it is highly recommended that administrators review the log descriptions contained in the PolicyServer Administrators Guide — Appendices.

Reporting may be performed within the log view by clicking on the reports button. This method is designed for ad hoc reports that are generated via raw SQL statements.

The following SQL statement example allows the administrator to run a report from the main database for all encrypted PC's in the enterprise by name:

```
SELECT DeviceName, Other  
FROM [Log]  
WHERE (MessageID = '400008')  
ORDER BY DeviceName
```

An entire log database also exists where queries can be run without any impact to the user community.

Known Issues

For the complete list of known issues, please visit:

www.mobilearmor.com/support

The credentials provided by Mobile Armor Technical Support for accessing this site are required.



DataArmor for PC

DataArmor provides mandatory authentication services and full disk encryption on all types of laptop, tablets and desktop PC's. This service requires that each user is properly authenticated prior to accessing a device. This includes the operating system (such as Windows), and all stored data and programs.

DataArmor secures not only the data files, but also all programs, registry settings, temporary files, print spoolers, etc. DataArmor encryption protects each sector of the hard drive and does not require a separate partition be created to encrypt the entire hard disk.

The Mobile Armor product suite has been tested extensively on a wide range of devices and manufacturers. However, in deployments, some older machines required a BIOS upgrade or change or a driver update for DataArmor to operate effectively.

DataArmor Components

DataArmor consists of the following main components.

- DataArmor Operating System (DAOS)
- DataArmor encryption engine (MABACKFILE)
- DataArmor Windows Service (MobileSentinel)



DataArmor Operating System (DAOS)

The DataArmor Operating System (DAOS) is the pre-boot authentication engine for the DataArmor product. The DAOS is a full 32-bit operating system which enables the DAOS to establish network connections, and support a wide range of network, video, and USB devices.

At installation the DAOS is installed on the hard disk in contiguous space and is immediately encrypted. Once the encryption takes place the authentication engine starts and the user is presented with the DAOS graphical user interface. If networked, user credentials are validated against the PolicyServer (if SSO is disabled) or the Domain controller (if SSO is enabled). If non-networked, the credentials are validated against the cached credentials stored in encrypted space on disk.

The DAOS itself is comprised of the following components:

Components	Description	Process
Stage 1 boot loader	16-bit driver	The machine powers up and calls the Stage 1 boot loader and the Stage 1 boot loader passes control over to the Stage 2 boot loader.
Stage 2 boot loader	32-bit driver	The Stage 2 boot loader starts up MAKERNEL.
MAKERNEL	Program that controls the authentication engine	MAKERNEL reads the data from the scratch space
DAOS Scratch Space	contains machine details, i.e. which security policies are enabled, valid credentials and other pertinent data for successful authentication	



DataArmor OS (DAOS) Startup Process

Once the PC is powered on, the following process takes place.

Step	Component	Process
1.	Stage 2 boot loader	Stage 2 boot loader loads MAKERNEL into memory.
2.	MAKERNEL	MAKERNEL compresses itself and initializes a minimal set of hardware (i.e., CPU/memory) and clears the screen to all black at a resolution of 1024x768@16-bit color.
3.	MAKERNEL	MAKERNEL loads any disk drivers necessary to locate the DAOS on the system.
4.	DAOS	If this is the first time the DAOS has been loaded, the DAOS encrypts itself with a new key for that system.
5.	DAOS	Start the window sub-system at a resolution of 1024x768@16-bit color.
6.	DAOS	Check for any DAOS updates and apply them.
7.	DAOS	Install device drivers for network, PCMCIA, and other necessary devices the DAOS may need to authenticate the user.
8.	DAOS	Start attempting to get a DHCP lease (if not a static IP network).
9.	DAOS	Start any smart card programs/drivers.
10.	DAOS	Start the authentication program and wait for the user.
11.	DAOS	User successfully authenticates.
12.	DAOS	Shut down all components.
13.	DAOS	Reboot.



DataArmor Encryption Engine (MABACKFILE)

Encryption begins, once the initial authentication takes place; and on a PC, it begins once the encryption service “MABACKFILE” starts in Windows. Typically this occurs about the same time the Windows GINA is presented to the user. Two processes are termed MABACKFILE: (1) the encryption engine is the service running as a system process; (2) the GUI that is accessible through the system tray icon is the service running as a user process.

In general, encryption on a 60GB Pentium 4 laptop takes approximately two hours. Performance degrades if the user is occupying processor cycles. The encryption engine is designed to throttle down or up depending on how many cycles the user is occupying. However, the typical user experience while the encryption engine is running is similar to a virus scan. The user notices some degradation in performance but it does not prevent them from performing ordinary tasks.

DataArmor Windows Service (MobileSentinel)

MobileSentinel is the compliance and remediation agent for the DataArmor product. MobileSentinel maintains the health of all DataArmor subcomponents; retrieves updates from the PolicyServer; transfers logs back to the server; and maintains security over peripheral devices attempting to communicate with the PC (such as PDAs).

Continued on the following page ...



MobileSentinel maintains the following files which reside in Windows/System32 (except for MAKERNEL which resides in the root directory of the OS):

File	Description
ACTSLRV	DataArmor's Windows service responsible for communicating with PolicyServer and applying updates.
MAKERNEL	The DAOS operating system (pre-boot operating system).
DA_LISI.XML	The current authenticated user information. This corresponds to the SystemInfo.xml file residing in DAOS.
DAEL.XML	The log file containing all log information to be sent to the PolicyServer
DAPAF.XML	Administrator, authenticator and/or other authenticated user information/credentials.
DAPOL.XML	The policy file implemented on the device
DAUPDATELOG.XML	Information on updates and/or patches applied to the system
MABACKFILE.EXE	DataArmor encryption/decryption service and GUI
MACLIENTENDLL.DLL	Encryption/Decryption functionality for MAClient communications
MAFIPS.DLL	Managed encryption wrapper for FIPS certification modules
MASCMON.EXE/DLL	DataArmor smartcard monitor
MAWHDD	DataArmor encryption/decryption driver



DataArmor Installation

Most organizations use an automated installation for DataArmor software; the installation may be accomplished manually, as well. However, for evaluations and pilot programs the manual installation is the most efficient.

Manual Installation

Manual installations require that a person installs the DataArmor software. This may be accomplished either by copying the files from the CD or running them from the CD.

Note: To install the software properly, the “Start Here” command **must** be run; simply double-clicking the .msi file does not install the software properly.

Automated Installation

Automated installations require that a software package installs the DataArmor software. DataArmor is compliant with SMS, Tivoli, LANDesk and all of the automated software delivery tools.

DataArmor installation **Best Practice:** Mobile Armor considers the following procedure as Best Practice as for large organizations when installing DataArmor; many of Mobile Armor’s DataArmor customers have adopted it as well.

Continued on the following page ...



Automated Installation (*continued*)

Step		Description
1.	Identify the targeted Recipients.	<p>Automated installation requires a project plan that includes the organizations involved and the deployment schedule. To ensure a successful deployment, Mobile Armor suggests:</p> <ul style="list-style-type: none">• Identify the groups that will receive the software.• Notify the groups well in advance of deployment to provide ample time for managers to properly inform the organization of the pending changes and schedule pilot programs.
2.	Identify any potential conflicts.	<p>As with any software product, potential conflicts may exist between DataArmor and other applications. Many desktop security agents such as Cisco Security Agent, Proventia and the like will flag DataArmor as nefarious. In most cases, this is because DataArmor is accessing and modifying the registry and the Windows/System 32 file.</p> <p>Mobile Armor recommends that DataArmor be added to the trusted applications folder of any desktop security agent. Simply disabling the desktop agents during installation may not prove beneficial.</p>

Continued on the following page ...



Automated Installation (*continued*)

Step	Description
3.	<p>Prepare a script.</p> <p>Organizations that intend to “push” the software to devices must prepare an automated script for the automated tool to push down.</p> <p>Script switches:</p> <ul style="list-style-type: none"> • REQCRED=NoPrompt – This command uses the credentials from the command line to sign-onto the PolicyServer. • REQCRED=Password – This command uses the host and user name from the command line and prompt only for the install password. • REQCRED=Prompt – This command prompts for user name, password, and host address. This command uses the default from the command line as well. • ALLOWCANCEL=YES – Allow users to cancel install – Default value is NO. • USER=<Username> - Default user name. If this command is not populated, the username defaults to the Windows user name. • PASSWORD=<Password> - This is either a domain password (if using SSO) or the one time password assigned to the user via the PolicyServer. • HOST=<Host IP or Name> - This is the name or IP address of the PolicyServer. <p>Examples:</p> <p>Msiexec /i <Install Dir>\DA_Setup.msi REQCRED=NoPrompt USER=<Username> PASSWORD=<Password> HOST=<PS Name/IP></p> <p>An example install of the user “Matt” to the 192.168.2.130 PolicyServer, an administrator would use: Msiexec /i C:\DataArmor_v3.0.7.2\DataArmor_v3.0.7.2 \Bin\Packages\pc\DA_Setup.msi REQCRED=NoPrompt USER=Matt PASSWORD=123456 HOST=192.168.2.130</p> <p>To prompt the user for their password and default to the user’s windows user name: Msiexec /i <Install Dir>\DA_Setup.msi REQCRED=Password HOST=192.168.2.130</p>



Automated Installation (continued)

Step	Description
<p>3. Prepare a script. (continued)</p>	<p>In conjunction with the automated scripts many organizations choose to use the auto-login program DAAUTOLOGIN to bypass the initial authentication. The DAAUTOLOGIN program is run after the DataArmor software is installed as part of the installation script. The DAAUTOLOGIN program is located in the Tools folder of the DataArmor CD.</p> <p>An example script with DAAUTOLOGIN is:</p> <pre>Msiexec /i <Install Dir>\DA_Setup.msi REQCRED=NoPrompt USER=<Username> PASSWORD=<Password> HOST=<PS Name/IP> DAAutoLogin.exe <Administrator> <Password></pre> <p>If you wanted to do Single Sign-On (SSO) along with the DAAUTOLOGIN program you would use:</p> <pre>DAAutologin.exe <Administrator> <Password> <Domain> <User> <Password></pre> <p>DAAUTOLOGIN requires the use of an administrator or authenticator credential. Many organizations choose to create an “installer” account to perform the automated install. This installer account is an enterprise authenticator that is given a password in the PolicyServer. The Installer account is not required to be a member of the domain. The installation packages then use the installer credentials to install the software.</p> <p>The net effect of using an automated script with DAAUTOLOGIN allows the administrator to silently install the software; reboot without user intervention; bypass the DataArmor pre-authentication engine; boot to the Windows GINA where the machine will begin encrypting. When the user arrives in the morning they will sign into Windows to a fully encrypted machine. This method allows for very low user impact. The next time a user reboots he/she will be presented with the DAOS where he/she will enter his/her Windows Domain credentials.</p>

Continued on the following page ...



Automated Installation (continued)

Step		Description
4.	Pilot.	<p>Mobile Armor recommends that organizations perform a pilot program on a small, but diverse number of users within the organization. Ideally, the pilot should test the automated script that was created. Also, the pilot group should assist in piloting the software on different makes and models of PC's.</p> <p>Best practice is to choose 4-5 members from each targeted department and pilot the software to that group for 20 to 30 days. During the pilot, administrators can tweak and tailor their implementation strategy to make the DataArmor deployment as effortless and silent as possible.</p>

Encryption

Once the user has authenticated to the device, initial encryption begins. As stated before, a typical machine (Pentium 4, 60GB HD, 1GB RAM) encrypts in approximately two hours. The user notices some system degradation during the initial encryption process. However, the degradation does not prevent the user from performing their normal tasks.

When encryption is complete, the user notices no performance impact. The on-the-fly encryption/decryption process takes less than 100 milliseconds to complete; therefore, the user does not notice any delay in decrypting or encrypting a file during normal use.

Currently, DataArmor encrypts the primary drive only. Any slave or secondary drives are not encrypted. DataArmor encrypts all partitions of a drive and there is no limit to the number of partitions that can be created. If unallocated space is allocated after initial encryption has taken place, DataArmor automatically encrypts the newly allocated space after the next reboot.



Domain Authentication

Domain authentication, or commonly known as Single Sign On (SSO) enables a user to enter his/her Windows credentials in the DataArmor authentication screen and go to the Windows desktop without having to re-enter those credentials at the Windows GINA. To accomplish this functionality, DataArmor “chains” the Windows GINA but does **NOT** replace the Windows GINA. Simply put, the DAOS passes the credentials to the Windows GINA during startup allowing the user to bypass the Windows GINA.

By chaining the GINA, DataArmor is compliant with any Microsoft certified GINA replacement, such as RSA. Similarly, any native functionality of the Windows GINA (smartcards, change password, etc) is not affected by the installation of DataArmor. SSO does not currently work in cases where Windows is configured for smartcard only authentication. This is because the smartcard PIN is not passed to the OS (the most conservative approach to security). Organizations requiring smartcard SSO should notify their sales representatives.

When SSO is enabled, DataArmor makes the following changes to the system:

1. Addition of:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\dawinlogon to the Windows registry

The above key should have the following string values:

String	Data
Dllname	dawinlogon.dll
Logon	WLEventLogon
Startup	WLEventStartu
Unlock	WLEventUnlock
StopScreenSaver	WLEventStopScreenSave
StartShell	WLEventStartShell
StartScreenSaver	WLEventStartScreenSaver
Shutdown	WLEventShutdown
Lock	WLEventLock
Logoff	WLEventLogoff

2. Within the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon** there should exist an **AUTOADMINLOGON** key.
Note: The Autoadminlogon key should have a value of 1 (one).



3. Addition of **DAWINLOGIN.DLL** in the WINDOWS/SYSTEM32 folder. The version of the .DLL should match the currently installed version of DataArmor.

When enabling Domain Authentication, organizations should ensure their group policy does not interfere with the process outlined above. Group policy, on occasion, has shown to not permit the population of the WINLOGON keys. If you receive strange behavior at the Windows GINA, investigate the interaction between the registry settings that DataArmor has completed and Group Policy.

DataArmor Password Sync Utility

If a user password is reset or is expired and the device is then disconnected from the network before it has been restarted, DataArmor is unaware of the password change. Afterwards, if that device is booted without network connectivity to the PolicyServer (i.e., a laptop using a VPN), the previous (cached) password is required to logon. Once network connectivity is established, the Windows and DataArmor passwords may be synchronized by the user using the Password Sync utility:

- Step 1: Run the program DataArmor Password Sync.exe located in the <Drive>/Program Files/MobileArmor/DataArmor directory.
- Step 2: Enter the domain/username and domain password of the user to be synchronized and select "Continue". The domain and DataArmor passwords are now synchronized.

RSA SECURID Setup

RSA SecurID tokens are considered among the most secure authentication methods available for user identification. The RSA SecurID token is based on an internal cryptographic key that generates a unique password in periodic intervals, eliminating the need for complex passwords.

The following steps are required for using RSA SecurID tokens as an authentication method:



RSA SecurID Two-factor Authentication Setup

1. Install the RSA Authentication Manager or the RSA ACE-Agent on the same machine as the PolicyServer.
2. Ensure communication with the PolicyServer from the DAOS (RSA SecurID will not work if disconnected).
3. Within the PolicyServer, the following Policies **must** be set:
 - a. Policies >> DataArmor >> Password >> AllowedAuthenticationMethods >> RSA
 - b. Policies >> DataArmor >> RSAOfflineAllowed >> Yes/No
4. At the first login to the DAOS, the users will select Authentication Methods >> RSA SecurID and enter the PIN + code from their RSA SecurID token and be logged to the Windows GINA.

RSA SecurID Domain Authentication/Single Signon Setup

1. Install the RSA Authentication Manager or the RSA ACE-Agent on the same machine as the PolicyServer.
2. Ensure the Windows GINA is being used and that the RSA GINA is not installed.
3. Ensure communication with the PolicyServer from the DAOS (RSA SecurID does not work if disconnected).
4. Within the PolicyServer, the following Policies **must** be set:
 - a. Policies >> DataArmor >> Password >> AllowedAuthenticationMethods >> RSA
 - b. Policies >> DataArmor >> RSAOfflineAllowed >> Yes/No
5. With the first login to the DAOS, users are required to login using their Windows credentials.
6. At the next login, at the DAOS, the users select Authentication Methods >> RSA SecurID and enter the PIN + code from their RSA SecurID token and are logged into Windows.

Known Issues

For a complete list of known issues please visit:
www.mobilearmor.com/support.

The credentials provided by Mobile Armor Technical Support for accessing this site are required.



Support:

If you have any questions or require technical support, please contact Mobile Armor Technical Support:

Mobile Armor, Inc.

400 S Woods Mill Rd, Suite 300

Chesterfield, MO 63017

Telephone: (314) 590-0925

Email: support@mobilearmor.com Website: <http://www.mobilearmor.com/support>