

Cams US Army Customer Case Study

The US Army's Aberdeen Proving Ground Edgewood Area (APGEA) has been a center for chemical warfare research and development since it was established. From the trenches of France and Belgium in World War I to the desert battlefields of Iraq, the work at APGEA has contributed to the defense and safety of American forces threatened by chemical weapons.

The Requirements

The information technology department at APGEA manages mission critical web applications for a community of 3,800 internal users. Most of these web applications were developed using ColdFusion though other CGI scripting languages are also in use. Web applications are deployed on Apache 2.0 web servers running on Solaris and Windows with Microsoft IIS on some servers. A cluster of Sun ONE directory servers provides user identity management services. A Sun ONE certificate authority server provides X.509 certificate management.

APGEA required a web single sign-on solution to provide consolidated authentication services and single sign-on for secure web applications and files. Existing web applications used a variety of SQL database tables for user authentication primarily through Apache's HTTP BASIC security implementation. HTTP BASIC was considered to be insecure as it passes the user credentials in cleartext with each request after a user authenticated. Other limitations included lacking way to logout and no easy way to centralize logging, audits and security policy management. APGEA also knew that strong authentication using the Common Access Card (CAC) would be required later to comply with the DODI 8500.1 and HSPD-12 directives.

The Solution

A Cams policy server cluster was integrated to provide the security infrastructure to protect all web-based applications. APGEA information technology personnel worked with Cafésoft to configure and integrate authentication with the Sun ONE directory server. Specifically, this required configuring a secure LDAP connection (LDAPS) between the Cams policy server and the Sun ONE directory server. This configuration guaranteed that the user's credentials would be encrypted using SSL/TLS between the user's HTTP browser and the web server; then, by Cams when sending credentials from the Cams web agent to the Cams policy server; and, finally by the secure LDAP connection when transmitted by the Cams policy server to the Sun ONE directory server for verification.

APGEA web developers inventoried the mission critical ColdFusion web applications. They determined that the web applications could use Cams security without modification if the Cams Apache 2.0 web agent was enhanced to populate the REMOTE_USER HTTP request header using the authenticated Cams user name. These web applications used the REMOTE_USER HTTP request header through ColdFusion CGI calls to make fine-grained web application security decisions. The Cams Apache web agents were enhanced with this feature by Cafésoft professional services. The feature was included with the standard product distribution starting with the Cams 2.1 release. Populating this value also had the additional benefit of writing the authenticated user name to the standard Apache logs for each request submitted by a Cams authenticated user.

With the release of Cams 3.0, the X.509 certificate infrastructure was in place to support the integration of the US Department of Defense Common Access Card (CAC) for authentication to web applications. CAC was already in use at APGEA for facility access as well as desktop system authentication and was now required for web application authentication by the DODI 8500 and HSPD-12 directives. Using the Cams 3.0 X.509 infrastructure, Cafésoft was able to work with APGEA to quickly implement a strong authentication solution that supports CAC according to their requirements.

Summary

APGEA engaged Cafésoft with the requirement to implement web single sign-on for its mission critical web applications. Working with minimal assistance from Cafésoft professional services, APGEA's information technology staff was able to quickly integrate, test and deploy Cams as the access management security middleware for their site. The deployment required use of standard Cams features such as web single sign-on to Apache and IIS servers and use of secure LDAP connections to ensure user credentials are always encrypted when transmitted. A new feature was added to Cams 2.1 to allow unmodified porting of existing mission critical ColdFusion web applications to the Cams security environment. After initial deployment, the new Cams 3.0 X.509 digital certificate authentication feature enabled easy integration of the CAC card at APGEA.

With this Cams web application security infrastructure in place, APGEA has a secure, powerful and flexible web application security platform to comply with mandated standards, incorporate business policy changes and securely move into the future.



Cams is secure, flexible and affordable web application security middleware that provides cross-platform web single sign-on, access control and session management services. The Cams policy server deploys on Linux, Solaris and Windows to secure files and web applications on Apache, IIS and Sun ONE web servers, and J2EE application servers such as BEA WebLogic, IBM WebSphere, JBoss, and Tomcat.

Cams Identity is a companion product to Cams that provides user provisioning and management features like user self-registration, password reset and administrator management of users and groups.

Cams Platform Support

Cams Policy Server

- Mac OS X and OS X Server
- Red Hat Enterprise Linux 3/4/5
- Solaris 8/9/10
- SuSE 9/10
- Windows 2003/2000 Server, XP Pro, 2000 Workstation
- Other operating systems with Java JRE 1.4 or 1.5

Cams Web Agents

- Apache 1.3 on Red Hat 9 and Enterprise 3 (Cams 2.1 only)
- Apache 2.0 and 2.2 on Red Hat Enterprise Linux 3/4/5
- Apache 2.0 and 2.2 on Solaris 8/9/10 32/64-bit servers
- Apache 2.0 on Windows 2003/2000 Server, XP Pro, 2000 Workstation
- J2EE Application Servers via Servlet Filter:
 - BEA WebLogic 8.1
 - IBM WebSphere 5.x
 - JBoss 3/4
 - Oracle 9iAS and 10g
 - Tomcat 4/5/5.5/6
 - *Other J2EE servers that support Servlet API 2.3/2.4*
- Microsoft IIS 5 and 6
- Sun ONE 6.x on Solaris 8/9/10 32/64 bit
- Tomcat 4/5/5.5/6

User Directories

LDAP

- IBM Directory Server
- Microsoft Active Directory and ADAM
- Novell eDirectory
- OpenLDAP
- Red Hat Directory Server
- SunONE Directory Server
- *Other LDAP v3 compliant directories*

Databases

- IBM DB2
- Microsoft SQL Server
- MySQL
- Oracle
- Sybase
- *Other databases with a JDBC 2.0 compatible driver*



AMERICA

phone: +1.858.268.5100
fax: +1.858.384.3330
e-mail: info@cafesoft.com

EMEA

phone: +07531.36598 00
fax: +07531.36598 11
e-mail: info@sientenbau.com