

Cams IONA Customer Case Study

IONA provides over 5,000 customers worldwide with mission-critical infrastructure for demanding technical applications including large-scale manufacturing systems, high-end financial systems, telecommunications network management systems and federal computing initiatives. IONA's web site is a key resource to provide information and services to their customers. The IONA web site consists of clustered Sun ONE web servers on the front end, clustered JBoss J2EE servers hosting application functionality and an Oracle 9 database, which hosts the user directory and other application tables.

The Requirements

IONA had an internally developed web application security solution to protect customer service resources on their web site. However, there was no easy way for customers to self-register or manage their own accounts and passwords, for administrators to manage users or to leverage the web security solution over the entire site. High-level goals were identified by the IONA business units for a new site that would:

- Provide a platform to ease IONA product purchase and download
- Implement a single point of user registration for the entire web site
- Incorporate IONA customer service, tech zone and update centers under a common security infrastructure
- Track web usage by users to enable targeted marketing campaigns
- Consolidate user data into an accurate and comprehensive profiles for contact, lead and opportunity creation
- Provide a common infrastructure to manage product downloads

For example, IONA required fine-grained and flexible access controls for web site content such as PDF files. Specifically, the IONA marketing department wanted to secure PDF white papers such that:

- *One-time* access could be granted after specified contact information is provided.
- Unregistered users could gain access by providing required contact information (without registering).
- Contact information would be populated automatically for authenticated users.

Other specific feature requests from the business units included:

- Automatic assignment or removal of a user's roles and privileges based on the completeness of a user's identity.
- A "Yahoo-like" remember me to automatically, securely and transparently log users into the site on return visits.
- Requiring explicit login when automatically authenticated users access higher-value content, such as user profile updates or password changes.

As an overriding goal, IONA wanted web site security to drive personalization and facilitate IONA responsiveness to their customers rather than to impose strict security policies on their users. Additionally, the web security infrastructure needed to be flexible to easily adjust to changes in future business requirements.

The Solution

Cafésoft provided web application security professional services to assist IONA with developing a formal technical requirements specification. A use-case driven approach helped flush out system requirements and ensure mutual understanding of the desired features. Cafésoft's web application security expertise helped IONA to quickly and comprehensively gather requirements. A design was then devised by Cafésoft to implement the requirements using Cams as the web application security middleware and a customized implementation of Cams Identity mapped to IONA's existing user database schema. Additionally, the design required new Cams features to achieve the project goals. These features are included as of the Cams 2.1 release and include:

SQL Data Access Control Rule – A new, standard Cams access control rule that ensures the *existence* or *completeness* of required SQL database values (also called constraints). Each SQL constraint is evaluated and access is granted to a protected resource if all constraints are fulfilled. If any constraint is not fulfilled, then access is denied. This provides flexible support for context-sensitive SQL statements based on user identity and other request-specific values. For example, this feature enabled IONA to flexibly capture snapshot user identity data before granting one-time access to high-value white papers.

Obligations – This unique, powerful feature enables sites to change work flow based on an access control policy decision. For example, Cams web agents can be instructed to do an HTTP redirect based on a Cams access control decision, which also specifies the URL to use. For the IONA site, this feature is used in conjunction with a SQL data access control rule to redirect users to specified forms if an access control evaluation determines that a user needs to provide contact information. If the user is already authenticated, the form is populated with the user's current database values.



Automatic HTTP User Login – This is Cams “Yahoo-like” remember me feature. If the user chooses to be remembered and Cams is configured for automatic HTTP login, the Cams web agent creates a cookie with encrypted user name and password values and a configurable expiration period. Every time the user returns to the site, he is automatically authenticated. This feature also enables increased site personalization and improves analysis of user visits.

Authentication Types and Additional Authentication – Cams provides the ability to grant or deny users access to resources based on authentication type. Users can be required to provide additional credentials for higher value content. For example, this feature enabled IONA to require users authenticated with automatic authentication to be prompted for explicit login when they accessed high-value resources such as user profile updates and password changes.

Other Cams components were also created specific to IONA for this project. For example, IONA required flexible notification and reporting of specified access control events to appropriate personnel by logging these events to a database. IONA had previously deployed a JMS infrastructure and wanted to use it to handle these access control event notifications. To do so, Cafésoft implemented a JMS client access control valve, which was plugged into the Cams policy server's access control pipeline. When specified resources are accessed, the JMS client sends a notification message to the JMS server, which is programmed to store key information in a relational database for reports and follow-up.

Summary

IONA engaged Cafésoft with the need to implement a common, flexible web application security infrastructure on its mission critical web site. Working with Cafésoft professional services, they were able to quickly and efficiently define the security requirements and design a new web application security architecture based on Cams security middleware. The design required standard Cams features such as web single sign-on to Sun ONE and JBoss/Tomcat web applications and role-based access control. Additionally, new Cams features and custom Cams components as well as a customized implementation of Cams Identity were required. The pluggable, flexible and open Cams architecture enabled the new features and custom components to be quickly developed, tested and deployed into IONA's production environment. The new Cams features are included in Cams as of 2.1 release.

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



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

Cams Platform Support

Cams Policy Server

- Mac OS X and OS X Server
- Red Hat 9 and Red Hat Enterprise 3.4
- 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
- Apache 2.0.40 and 2.0.49-55 on Red Hat 9 and Enterprise 3
- Apache 2.0.49-55 on Windows 2003/2000 Server, XP Pro, 2000 Workstation
- J2EE Application Servers via Servlet Filter:
 - BEA WebLogic 8.1
 - IBM WebSphere 5.x
 - JBoss 3.2.x using Jetty or Tomcat
 - Jetty 4.2.x
 - JRun 4.x
 - Oracle 9iAS and 10g
 - Tomcat 4/5/5.5
 - *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
- Tomcat 4/5

User Directories

LDAP

- IBM Directory Server
- Microsoft Active Directory and ADAM
- Novell eDirectory
- OpenLDAP
- SunOne/iPlanet/Netscape Directory Server
- *Other LDAP v3 compliant directories*

Databases

- IBM DB2
- Microsoft SQL Server
- MySQL
- Oracle 9i/10g
- Sybase
- *Other databases with a JDBC 2.0 compatible driver*

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, Tomcat and Oracle 9iAS. 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.