

## Air Force Materiel Command



### Solution Highlights

- Seamless integration of Internal and external users
- External user provisioning based on CAC card and ECA certificates.
- Kerberos authentication to SharePoint and integrated applications.
- Centralized control of site creation and publication
- Delegated management of users
- Terms and conditions govern user access
- Strong audit and reporting
- Conformance to Air Force IT policies

### Air Force Materiel Command Extends SharePoint Sites to Pentagon and Contractors

Air Force Materiel Command (AFMC) conducts research, development, test and evaluation, and provides acquisition management services and logistics support necessary to keep Air Force weapon systems ready for war. These mission elements require coordination with other Air Force units, the Pentagon and with contractors that supply products and technology to the Air Force.

Within AFMC, Microsoft SharePoint has been widely accepted as a document management, collaboration and secure communications platform. AFMC expected to achieve operational improvements and efficiencies if it could extend SharePoint to work with external parties.

#### Background and Requirements

Air Force Materiel Command (AFMC) needed to give external users access to AFMC-managed SharePoint sites. Some of the external users were Air Force employees stationed at the Pentagon. Others are other military personnel as well as contractors at companies like Lockheed Martin. In both cases, these external users did not have accounts in AFMC's Active Directory (AD) forest. Furthermore, any solution that provided access to these external users had to work within the following constraints:

- SharePoint is located behind an ISA server, which authenticates users via a CAC card for Air Force employees or an ECA certificate for contractors. This ISA server is capable of distinguishing between internal and external users and routing them to different SharePoint Web Front Ends (WFEs) as appropriate.
- ISA authentication requires a local AD account in a single AD forest for all users, both internal and external.
- URLs for internal and external users had to be consistent. In other words, a URL to a page or document in a SharePoint had to be resolvable by both internal and external users so they could be shared freely between the two groups.
- AFMC uses K2 as a workflow product with SharePoint. K2 required that a user authenticates to SharePoint using Kerberos authentication so that user impersonation could occur to the K2 server via Kerberos constrained delegation. AFMC expected to add additional SharePoint third-party components in the future with similar requirements.
- Timing and logistics of the project required zero lift at the Pentagon and contractors.
- Existing SharePoint sites are often available to internal AFMC users who are categorized in an Authenticated Users group. External users should generally not be considered part of this group.

## Key Business Benefits

- Site owners can efficiently add and remove external users
- Extensive auditing of extranet user access rights and activities
- Tight integration with Microsoft and USAF security infrastructure
- Improved communication and coordination with distributed USAF staff and contractors
- Lower IT cost of provisioning new extranet users
- Commercial-off-the-shelf solution

## Technology Environment

- Microsoft SharePoint
- Epok Federated Access Manager with CAC Support
- Microsoft Windows Server 2008
- Microsoft SQL Server
- Microsoft Active Directory
- Microsoft ISA

Given these constraints, AFMC wanted a solution that provisioned local AD accounts for external users based on the information encoded on the external users' CAC cards or ECA certificates. These AD accounts needed to be located in a child domain of the AFMC AD forest. External users would authenticate to these accounts via ISA using a CAC card or ECA certificate, then use Kerberos authentication from ISA to SharePoint to satisfy K2. Internal and external users needed to be able to access SharePoint on the same SharePoint zone (i.e. the default Windows-authenticated zone) to provide consistent URLs for both groups of users.

The ability to make a site externally accessible could only be available to IT. Site owners could then be empowered to add or remove individual users once the site is shared. Trusted agents on the partner side (at the Pentagon or at a contractor, for example) needed to be able to provision users and in some cases to add or remove users to a site, subject to the review and approval of the site owner.

Additionally, AFMC needed a solution that provided the following:

- Sites that may be shared with external parties had to be clearly marked as such via a banner on each page of the site.
- When external users enter the site, they had to review and agree to the terms and conditions that governed their site access.
- External users with access to many sites needed a page that listed all the sites within the AFMC SharePoint environment to which they had access.
- IT resources within AFMC required oversight, visibility and control over sharing relationships throughout AFMC, with the ability to initiate and revoke external access to sites throughout the AFMC SharePoint farm.
- IT resources needed tools to manage accounts and groups, including provisioning tools based on information extracted from a user's authentication certificates.
- Auditing and reporting capabilities had to be stronger than the default SharePoint audit logs provided including the ability to provide context about the authorization as well as subsequent access.

Any solution had to conform to the relevant Air Force IT policies.

## The Solution

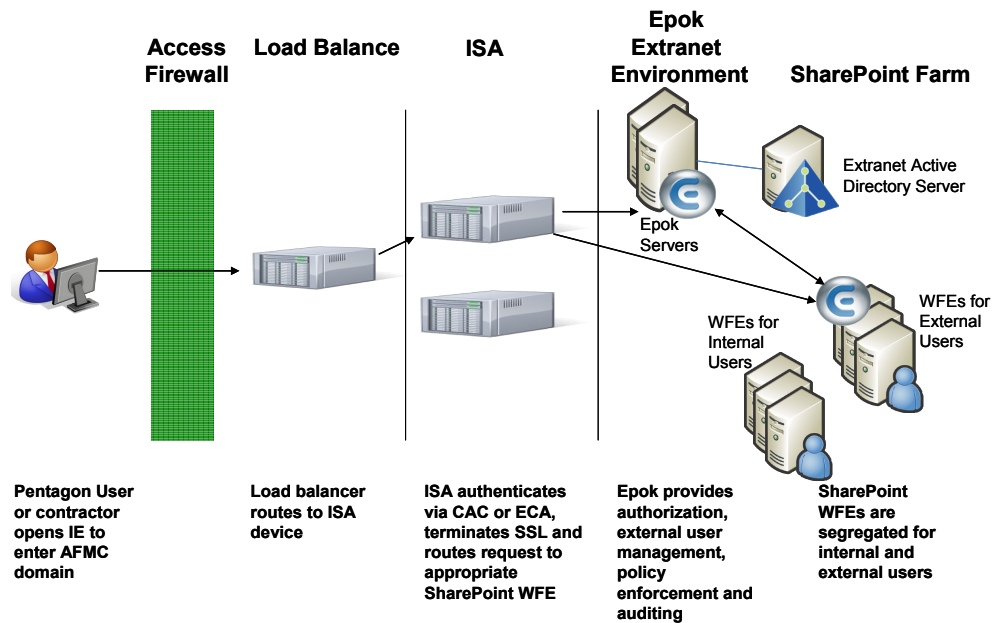
Epok's solution addressed AFMC's requirements as described above by providing a provisioning, operational management and reporting solution for external users accessing AFMC-managed SharePoint sites.

The provisioning system allowed IT administrators to provision external user accounts into a child domain of AFMC's AD forest based on information extracted from the external users' CAC or ECA certificates. The system also allowed accounts to be updated and for groups of users to be created and managed.

Sites that were eligible for sharing with external parties were clearly marked as such via a banner on each page of the site. Only IT administrators were allowed to initiate site sharing with external organizations. Once the site was shared, site owners were able to add or remove individual users to the site. At AFMC's discretion, trusted agents at the partner organization were also allowed to add or remove individual users, subject to review and approval by the site's owner. URLs for sites and site content were consistent for internal and external users so links could be freely shared between the two groups.

External users could authenticate to ISA using a CAC card or an ECA certificate, for Air Force employees at the Pentagon or for contractors, respectively. Authentication from ISA to SharePoint used Kerberos to satisfy K2 and other similar components that could be used in the future. External users have access to a page that lists all the sites within

# AFMC Solution Architecture



The Epok Server and Epok agents running on SharePoint WFEs provide user management, authorization and policy enforcement for AFMC's external SharePoint users

the AFMC SharePoint environment to which they have access. When an external user enters a site, the Air Force is able to require him/her to review and agree to the terms and conditions that govern that user's site access. If appropriate, the Air Force can also use additional tools included in the Epok solution, like document watermarking and the collection of the authorized purpose for a site visit, to establish the user's informed consent.

When an external user accesses a site or the contents of a site, Epok performs additional authorization to insure that the user has authorized access to the requested resource. If a site is available to the Authenticated Users group, for example, but not to a particular external user, access to that resource is blocked by Epok.

IT resources within AFMC have tools that provide oversight, visibility and control over sharing relationships for SharePoint sites throughout AFMC, with the ability to initiate and revoke external access to sites throughout the AFMC farm. IT resources also have tools to manage accounts and groups, including provisioning tools based on information extracted from a user's authentication certificate. Auditing and reporting capabilities provide access to audit logs maintained by Epok. Audit logs are stored in SQL Server and custom reports can be created by AFMC to meet additional reporting requirements.

The Epok solution is delivered by a combination of the Epok Edition for Microsoft SharePoint and new features and functions that were added to the product to address solution elements that were not part of the existing product.



This case study represents an active project Epok is implementing for AFMC that is targeted for completion in mid-2009.

