WASS

Web Access Security Subsystem Overview

Senior Team Members

Gary Faeth (PIH Security Officer)
Dallas Blair (IT Project Manager)
Amalio Escobar (Project Manager)
Ajit Sowdas (Senior Developer)

What does it do?

- Protects system resources from unauthorized use
- Provides single sign-on to multiple applications (over 25)
- Authenticates (identifies the user)
- Authorizes (determines what the user can do)
- Delegates authorization functions to coordinators and system administrators
- Logs user activities

WASS Components

- WASS administration
- SiteMinder
  - Web Agent
  - Policy Server
  - Policy Server Store
- User Repositories
  - LDAP (for external users)
  - Active Directory (for internal users)

Authentication Service

- Provides controlled, granular access to any HTTP or HTTPS content servers
- Allows remote users to connect to the Web Service, which then allows authorized user to access resources
- Hides the true location of the resources, as the users never access the content server directly

Policy Server

- Interacts both with the organization's user stores—(Active Directory and LDAP in our case) and with defined access policies
- Authenticates the user, and assuming all is well, returns user profile and entitlement information which can then be passed to the originally requested application

Authentication & Authorization

- Supports single sign-on to multiple data sources
- Supports specific access control to content based on the authenticated user's authorization information
- Authorization is performed by configuring Roles and Actions such that content is available to members of those groups only

Process Flow

- The Web agent checks which authentication method is required for a resource. Credentials are userID and password.
- The Web agent challenges the user for credentials.
- The user responds with the appropriate credentials.
- The Web agent passes the credentials to the Policy Server, which determines whether or not the credentials are correct.
- If the user passes the authentication phase, the Policy Server determines whether or not the user is authorized to access the resource. After the Policy Server grants access, the Web agent allows the access request to proceed to the Web server.

E-Authentication

E-Authentication – Background

- Launched in 2002 as the and is part of the President's Management Agenda. E-Authentication assists Federal agencies in meeting two primary goals:
  1. Mitigate the security and privacy risks associated with electronic government by allowing government agencies to develop trust relationships among user communities.
  2. Control costs associated with authenticating the identity of a large number of end users by eliminating the need for each agency to create and maintain a separate credentialing system for each of their online applications.

E-Authentication – Assurance Levels

- Level 1 – Verification of user identity not needed
- Level 2 – Identity must be known. Credential passed identifies user as one that has been verified by credential issuer.
- Level 3 – Identity must be verified and additional token passed. L2 requirements and need to pass additional token (usually a PKI certificate or additional log-in with different PIN of password). Additional token can also be smart card.
- Level 4 – Known individual, additional token passed, verify identity. L3 requirements and verification of that person's identity using biometrics, usually a retina scan or fingerprint scan.

E-Authentication and WASS

- New interface for Users to log into WASS/Secure Systems.
  - http://asc.gsa.gov/portal/template/FindCredentialServices.vm?csid=0&aaid=3459
  - https://csp.orc.com/portal.jsp?aaid=3459

- Existing interfaces still intact for internal and external users.

E-Authentication – How do I get a Federated ID?

- Go to: https://csp.orc.com/reg/index.jsp
- Fill out form.
  - Important Note: Make certain that checkbox for “If you wish to obtain Level 2 access check here” is checked.
- Print Registration Form
- Get Registration Form Notarized
- Send Form via Certified Mail to ORC
- After receipt of form, ORC will provide Level 2 access confirmation via email.

E-Authentication – What does it do for ME?

- Makes ID management easier
- Use one ID across several agencies.
  - Department of Labor
  - Small Business Administration
  - Department of Agriculture
  - Department of Education
  - Environmental Protection Agency
  - Many more agencies besides…
- Well tested security

Limit Concurrent Logins

Limit Concurrent Logins

- What is this all about?
- Why limit concurrent sessions?

Limit Concurrent Logins

- Security!
- Security!
- Security!

Limit Concurrent Logins – What it Does

- Allows one user to use one ID with one system and one WASS session.
- Explicitly eliminates concurrent usage or sharing of a single user ID.
- Ensures users are adhering to the terms of use as presented to users on a yearly basis when logging into WASS, specifically that users will not share an ID with another person.
- Can alert users if their ID has been stolen or compromised, by alerting them when their session has been terminated.

Limit Concurrent Logins – What it Does Not Do

- Does not prohibit a user on a single machine from logging into the system and using multiple instances of a live session.
- Does not interfere with the workflow of a single user since sessions are not limited when using the same browser.
- Does not allow users to log into the system a second time from the same machine, even if using the same browser, without killing the previous session.

Limit Concurrent Logins – Impacts

- Organizations that share an ID (or ID's) will need to get ALL users registered.
- Will kill sessions of users who are accustomed to using multiple machines at the same time. (We believe this is a minority.)
- Will create a more secure environment for business transactions by ensuring ID's are being used by the person entitled to use that ID.

Contact Information

- Gary Faeth
  - gary.faeth@hud.gov
  - 202.475.8730
- Dallas Blair
  - dallas.c.blair@hud.gov
  - 202.475.8699
- Amalio Escobar
  - amalio.x.excobar@hud.gov
  - 202.475.8666

Questions?