Paper 059-2008

SAS® BI Web Application Security Configuration Primer

Heesun Park, SAS Institute Inc.
Brian English, SAS Institute Inc.

ABSTRACT

Securing Web-based resources is one of the biggest challenges for IT today. Virtually all IT organizations utilize security measures through authentication and authorization to protect their Web resources. Thus, it is vital for SAS® BI Web applications to integrate within a secure Web environment. This paper explores just that.

SAS BI Web applications are implemented based on SAS® Metadata Server, which typically is tied to the local OS for "host" authentication, but it can be integrated with external authentication mechanisms already in place for organizations' Web space. The latter is called "Web" (or "trusted") authentication. The most popular user registry for Web authentication is an LDAP directory server but it could also be a flat password file or DBMS.

Web-based authentication can occur in various Web components such as a Web (HTTP) server, reverse proxy security server, or application server. So the factors in Web security configuration include what authentication mechanism to use, where authentication challenge occurs, type of user registry that contains user information and in some cases, and single sign-on (SSO) capability through third-party security packages.

We will examine the pros and cons of various Web security configurations and how SAS BI Web applications operate within each one.

No paper was submitted for publication in the *Proceedings*. Check http://support.sas.com/rnd/papers/ or contact the author.

CONTACT INFORMATION

Heesun Park
SAS Institute Inc.
sashsp@sas.com