Override Authentication Login for CA Single Sign-On

What It Does

Many times, customers first implement CA Single Sign-On using simple, user name and password-based authentication schemes. In their initial implementations, it is also common for customers to make use of the SM_USER header variable to identify users to their web applications.

As they expand their site, customers may identify new requirements for authentication, such as the need for NTLM authentication or more secure authentication schemes like Certificate Based Authentication. Implementing these schemes poses a problem because the CA Single Sign-On Certificate Authentication scheme does not provide a value for SM_USER, and NTLM changes the format of SM_USER to domain\loginID. This causes web applications or other backend applications to fail because they are not getting the type of user loginID expected.

Override Authentication for CA Single Sign-On solves this problem by providing a mechanism to automatically and securely re-authenticate users with a configurable loginID value which gets set as the value of SM_USER.

Benefits That Deliver Value

Override Authentication for CA Single Sign-On allows customer to make use of new authentication mechanisms that don't populate SM_USER in the standard way without having to modify applications that rely on the SM_USER value.

How It Works

A sample use case would be:

- User 1 logs into a web site using an X.509 certificate.
- CA Single Sign-On authenticates User 1 based on the certificate. CA Single Sign-On opens a session for User 1 and creates a cookie, which contains user DN and timeout values, as well as a unique session id. The SM_USER header variable contains no value.
- A configured active response redirects the user's browser to a special resource protected by the Override Authentication Scheme. The active response obtains a loginID value from a configured attribute of the user's profile and provides it as the user's new LoginID value.
- An active response tied to the special resource generates an encrypted token to act as the user's password during the following re-authentication process.

- The Override Authentication scheme re-authenticates the user, using the new LoginID and encrypted token as credentials, creating a new cookie which contains the user's new LoginID, user DN and timeout values, as well as a new session id.
- The user's browser is redirected to the original resource requested by the user. This and all subsequent resources will have the SM_USER header variable delivered to them containing the value of the new LoginID.

Technical Prerequisites

A list of technical prerequisites for this packaged work product can be found at **CA Support online**. This is a central repository that will help you identify CA Technologies product compatibility with operating systems, other third-party software products, as well as with certification standards and regulations. **Contact** your CA Services representative for further assistance with purchasing this component.