StepUp Authentication Integration for CA Single Sign-On

What It Does

StepUp Authentication Integration for CA Single Sign-On (SmStepUpAuth) provides a user friendly way to protect resources with dual authentication schemes, typically combining HTML Forms or IWA authentication for the low security level authentication, and then a stronger authentication mechanism.

The “user friendly” aspect comes into play when a user first accesses some resource that only requires the low security level authentication, and then later accesses a resource protected with the SmStepUpAuth scheme shim (wrapping the stronger authentication mechanism). In this use case, the user is not re-prompted for their lower level credentials, they are only prompted for the strong authentication credentials. However, when an unauthenticated user accesses a resource protected with the SmStepUpAuth shim (wrapping the stronger authentication mechanism), they are first prompted to enter the credentials for the low security level authentication mechanism, and then prompted for the strong authentication credentials.

Benefits That Deliver Value

This module allows two authentication schemes to be chained together while providing the convenience of not requiring user’s to duplicate the entry of credentials to the lower security level authentication scheme if they are already authenticated when accessing SmStepUpAuth protected resources.

How It Works

StepUp Authentication Integration for CA Single Sign-On works by protecting both the resource that displays the prompt for the strong auth credentials and the credential collector file that the credentials are posted to (these may be the same resource) with the low security level authentication mechanism. This enables the user to be first authenticated at the lower security level before they are allowed to authenticate at the higher security level. When the strong auth credentials are posted to the protected fcc file, upon authorization an active response is executed to provide an encrypted token that is passed to the authentication scheme along with the strong auth credentials. This encrypted token ensures that the user doesn’t switch identities when authenticating at the higher security level. When SMStepUpAuth receives the credentials, it first disambiguates the user and validates the encrypted

token, then passes the strong auth credentials to the strong auth scheme it is configured to execute for credential validation.

This module is not guaranteed to be able to work with all strong authentication schemes, but it should be able to work with just about any strong auth scheme that collects its credentials with an FCC file. For StepUp to Client Certificate authentication, it is recommended that the Advanced Certificate Authentication for CA Single Sign-On (ACA) packaged work product be purchased instead of SMStepUpAuth. ACA has the StepUp functionality built into it, as does the Knowledge Based Authentication for CA Single Sign-On (KBA) packaged work product.

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.