User Context Gateway for CA Single Sign-On

What It Does

The User Context Gateway for CA Single Sign-On (UCG) Packaged Work Product provides the capability for password credential storage and replay within a CA Single Sign-On environment. This enables single sign-on integration between CA Single Sign-On and applications which manage their own sessions using a username and password. Applications which support the UCG integration avoid re-challenging the user for their application credentials, instead receiving them securely from the CA Single Sign-On Policy Server.

UCG consists of a number of independent components, working in concert, to manage, store, verify and provide user credentials to underlying applications. Users' credentials are saved securely within an attribute of the CA Single Sign-On user's directory record (the **UCG Attribute**), and are retrieved and provided to the application during application sign-on.

Credentials are stored through one of three different supported mechanisms:

- UCG Authentication Scheme
- UCG OnAuthAccept Active Response
- UCG Update Page

Credentials are delivered to the application through the UCG Web Server Module, inserting the username and password into the HTTP header, supporting either HTTP Basic authentication or through a separate HTTP header to support automatic population of forms. Clear text passwords are secure in a standard Web Agent deployment, existing only in web server memory.

Benefits That Deliver Value

The User Context Gateway for CA Single Sign-On provides the functionality required to automatically present user credentials such as username and password when interacting with a supported Web Server. It eliminates the need for the user to have to interact with the application to provide credentials as part of accessing the protected resources.

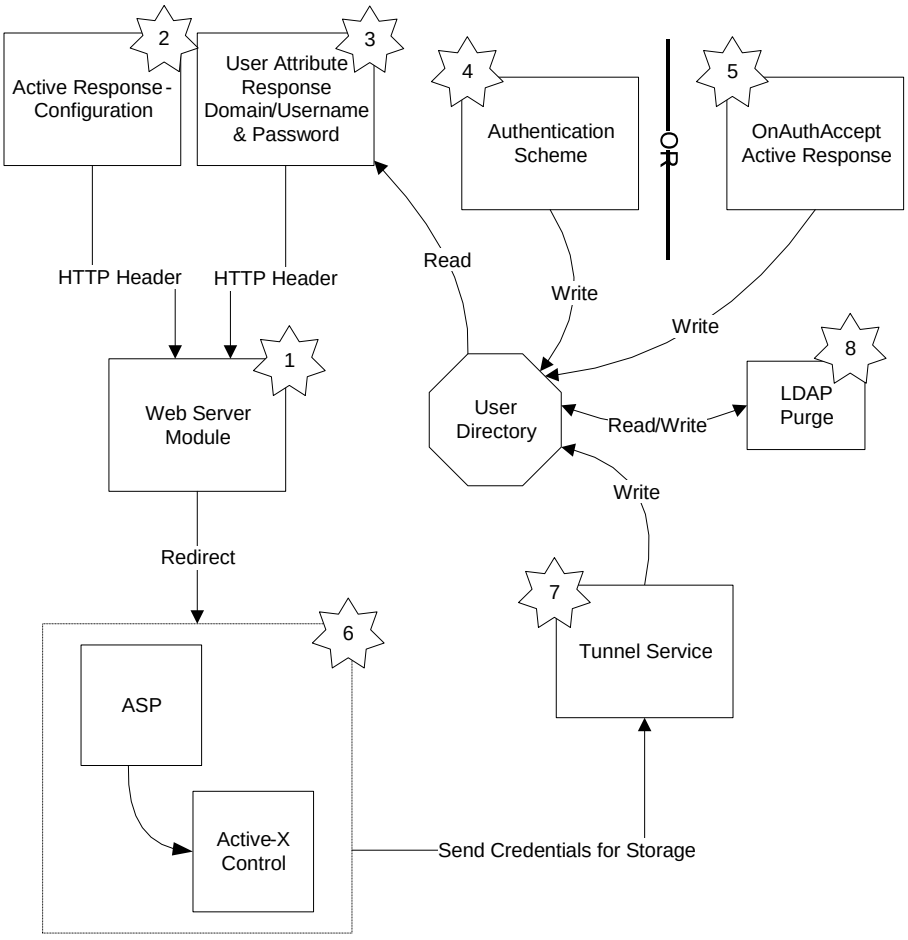
How It Works

The User Context Gateway for CA Single Sign-On supports the top-level use case described as "Credential storage and replay in a CA Single Sign-On environment", which is divided into two sub-cases:

- Credential Storage
- Credential Replay

Credential Storage is handled by one of either the UCG Authentication Scheme, the OnAuthAccept Active Response, or the Update Web Page. Credential Replay is handled by the UCG Web Server Module, and is controlled through the Configuration Active Response

UCG contains components which run both on the CA Single Sign-On Policy Server and on the application web server. Not all configurations using UCG will use all components.



Single Sign-On Flow Diagram

1. Web Server Module
2. Configuration Active Response

3. User Attribute Response
4. Authentication Scheme
5. OnAuthAccept Active Response
6. Update Web Page
7. Tunnel Service
8. LDAP Purge Utility

Note: Not all components are necessary for all configurations.

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.