Integration for CA Single Sign-On with Microsoft Windows Web Server Identity

What It Does

Integration for CA Single Sign-On with Microsoft Windows Web Server Identity (WWSI) enables Integrated Windows Authentication (IWA) based applications to be protected by CA Single Sign-On (CA SSO) security and utilize its single sign-on capabilities while using the applications' existing security model.

WWSI provides protocol transition, the ability to create one type of session based on the state of a different system's session, from a CA SSO session to a Windows security context. After decoding and validating a user's CA SSO session, WWSI will receive the user's Kerberos User Principal Name (UPN) as a CA SSO response, and then create a security token to be used by the web server as the user context for the specified user for the request.

The security token is passed to the web server through its authentication API, making the user context created by WWSI compatible with those created by the web server's IWA module. This enables applications designed to work with IWA to receive an equivalent security context, but still provide the flexibility and strength of the CA SSO platform.

With CA SSO and WWSI, users can be authenticated by any CA SSO authentication scheme, sensitive resources can be restricted to require stronger authentication, and the application will continue to function with a real Windows security context.

Benefits That Deliver Value

- Single sign-on for IWA environments that allow for CA SSO authentication schemes
- Protocol Transition from CA SSO to Windows security context
- Integration with the following platforms:
  - IIS
  - OWA
  - SharePoint (in Classic mode)

How It Works

WWSI consists of two components: a web server module and a token service. The token service creates the security contexts, and the web server module provides the security contexts to the web server. The two WWSI components have external dependencies, discussed below.

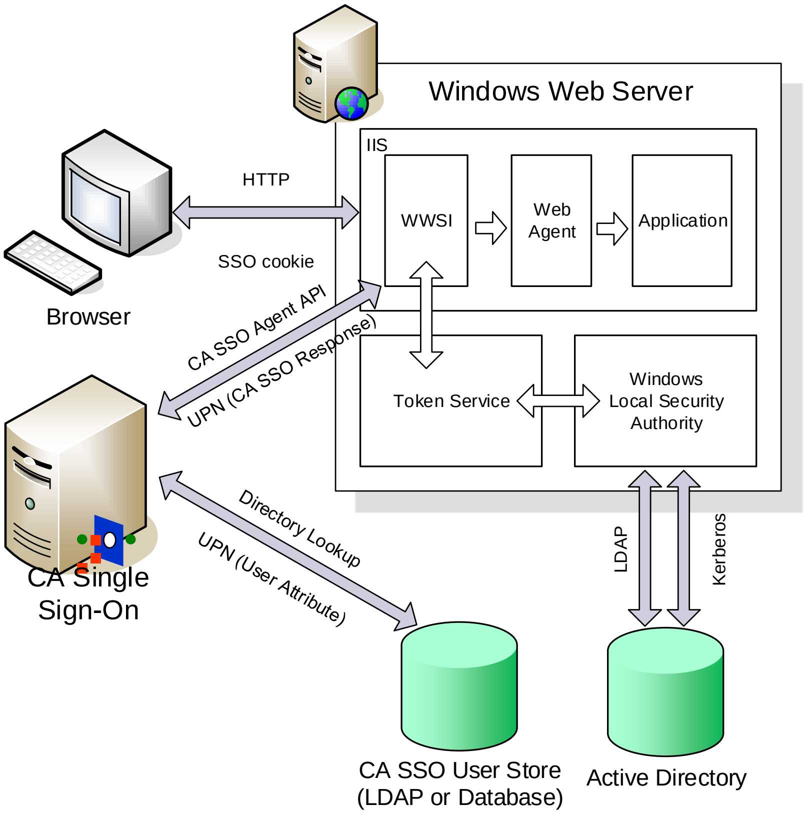

Figure 1- WWSI Component Diagram

WWSI Token Service

The WWSI token service creates Windows security contexts requested for a specified UPN by WWSI. Security contexts are created using S4U logon via the Windows Local Security Authority (LSA). This is a privileged operation, and to provide a secure architecture, the token service runs separately from the web server worker processes, protecting against privilege escalation vulnerabilities.

WWSI Module

The WWSI module interfaces with a web server's authentication API to provide the protocol transition between a CA SSO session and a Windows security context. The WWSI Module is a CA SSO agent, requiring resources to be protected by CA SSO, and for the user to be authorized to access the resource. WWSI requires policies be configured to return a response containing the user's UPN.

WWSI works in conjunction with a CA SSO Web Agent. The Web Agent performs CA SSO authentication, session creation and management, single sign-on, and resource-level access protection. WWSI utilizes the CA SSO session cookie which is created by the Web Agent to create a Windows security context.

WWSI uses CA SSO policies to determine the specific user context to use for the application. The user context is specified within a response variable returned from CA SSO upon authorization to the application.

Upon receipt of a request, WWSI will:

- Determine resource protection
- Authorize the session for the requested resource to get the UPN response
- Call token service to convert UPN to Windows security context
- IIS authentication is set to the security context returned from the token service

For unprotected resources, WWSI will perform no action and return control back to the web server. For protected resources with no session, WWSI will pass control to the Web Agent to perform authentication. This is normally achieved by WWSI providing the application pool identity (the anonymous user context) to IIS, which will then allow the Web Agent to perform a challenge. If the Web Agent is configured to support inline IWA authentication for resources protected with the CA SSO Windows Authentication scheme, WWSI can be configured to support this feature by instead performing no action and allowing IIS to perform its own authentication.

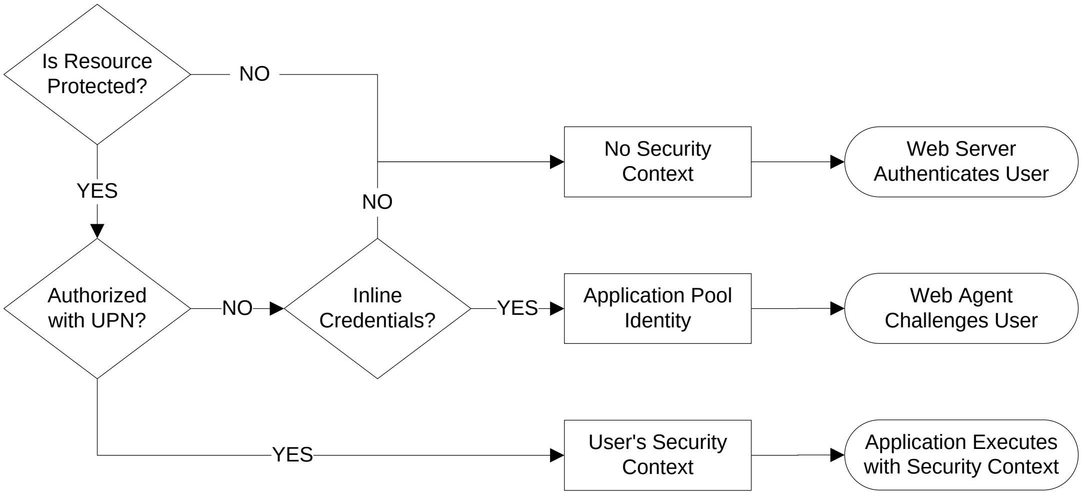
Is Resource Protected?
NO
YES
NO
No Security Context
Web Server Authenticates User
Authorized with UPN?
NO
Inline Credentials?
YES
Application Pool Identity
Web Agent Challenges User
YES
User's Security Context
Application Executes with Security Context

Figure 2- WWSI User Context Decision Diagram

CA SSO URI resource protection, end user authentication, single sign-on and session management are all performed by the CA SSO Web Agent. Applications are protected with CA SSO in the standard fashion. Other than the UPN response no specific requirements are imposed on CA SSO policy design.

Technical Prerequisites

A list of technical prerequisites for this packaged work product can be found in **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.