Lightweight SSO Ticket Authentication for CA Single Sign-On

What it does

The Lightweight SSO Ticket Authentication for CA Single Sign-On Packaged Work Product is designed to seamlessly log on a user into a CA Single Sign-On environment when they already have an authenticated session in a "trusted" non-CA Single Sign-On environment. The use cases that this was designed for are:

1. A customer already has non-CA Single Sign-On environments that authenticates their end users and want/need to keep this non-CA Single Sign-On environment while protecting additional resources by CA Single Sign-On.
2. A customer has a set of partners that they want to grant access to a resource(s). This solution allows for a trust to be established so that partner users can access resources.

In both cases the requirement is to have the user's logon once and achieve access to both environments.

Benefits that Deliver Value

Lightweight SSO Ticket Authentication for CA Single Sign-On delivers the following benefits:

- Seamless logon of users based on trusted non-CA Single Sign-On session
- End-users can experience their current logon experience, even for CA Single Sign-On protected users
- Provides a way to federate with a partner who does not currently have SAML capabilities
- Disambiguation is based on one or two user attributes
- Ability to set up multiple Secure Ticket Generators, each with its' own secret

How it works

The solution works based on a trust set up between CA Single Sign-On and another environment. This environment can be a non-CA Single Sign-On environment or another separate CA Single Sign-On environment.

When a user attempts to access a resource protected by the Lightweight SSO Authentication Scheme for CA Single Sign-On, they are forwarded to the Web Application that generates the Lightweight SSO Ticket. The Web Application generates the ticket based on the existence of the user's identity within

the HTTP Session. Only authenticated and/or authorized users in the non-CA Single Sign-On environment are allowed access to this Web Application. Once a ticket is automatically generated, it is exchanged for a CA Single Sign-On SSO token. The user is then forwarded on to the CA Single Sign-On protected resource. The ticket is authenticated, and the authorization step verifies the user is allowed access to the resource.

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.