Extended NTLM Authentication for CA Single Sign-On

What It Does

Extended NTLM Authentication for CA Single Sign-On is an authentication scheme plug-in for the CA Single Sign-On Policy Server.

While CA Single Sign-On has a built-in Windows authentication scheme, the scheme expects that user login IDs are unique across all Active Directory (AD) domains that are represented as CA Single Sign-On User Directories. If a user's login ID is not unique then it will be unable to successfully authenticate that user since the disambiguation phase will not map to a single User Directory object.

This Packaged Work Product can be used to successfully authenticate users in this use case because it can be configured with a mapping of domain names versus User Directories, and thus given the user's domain and login ID as input can uniquely locate the user's LDAP entry.

Benefits That Deliver Value

- Single sign-on for multi-domain IWA environments where users are not uniquely identified across domains.

How It Works

When a user accesses a resource protected with this authentication scheme, it instructs the CA Single Sign-On web agent to redirect to a Microsoft Internet Information Services (IIS) web server resource configured to trigger the IIS Integrated Windows Authentication process (IWA, also known as NTLM authentication). After IIS has completed its IWA, it returns control to the CA Single Sign-On Web Agent and provides only a username field formatted as <domain>\<loginID>. No password or Kerberos ticket is provided to the CA Single Sign-On web agent. The CA Single Sign-On Web Agent in turn sends a login message containing the username field to the CA Single Sign-On Policy Server to be processed by this authentication scheme.

The authentication scheme uses information from a configuration file to find the CA Single Sign-On User Directory associated with the <domain> name found in the username field, and then disambiguates (locates the user's entry) in the User Directory based on the loginID value from the username field. The authentication scheme then declares the user authenticated and a CA Single Sign-On SMSESSION cookie is issued. Since this authentication scheme only attempts to disambiguate the user in the User Directory that their LDAP entry is known to exist in, there is no requirement for the user's login ID to be unique across multiple domains.

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.