XauthRADIUS Integration for CA Single Sign-On

What It Does

In a typical deployment of CA Single Sign-On for use in an extranet or consumer portal, users have a single login based on a single entry in a centralized user directory, typically LDAP. CA Single Sign-On provides basic username and password-based authentication along with whatever authorization is required. For many organizations, this is a sufficient level of security, but for others, where data security is more critical, passwords are not a sufficient mechanism to authenticate users. In environments where a higher degree of confidence in the identity of the user is necessary, 2-factor tokens, certificates, biometrics, and other authentication products may be employed.

Vendors of authentication systems frequently include an API that allows for the inclusion of support for their authentication product in other vendors' products. These APIs typically offer a limited set of functionality, but are often effective for some level of integration. To enable others to implement additional authentication schemes, the CA Single Sign-On solution provides an API which can be used to add ancillary authentication methods to the core CA Single Sign-On product.

Through the use of this API and other vendors' APIs, CA Single Sign-On comes with a set of standard authentication schemes. These include SecurID, SafeWord Certificates and others. To aid in the deployment of CA Single Sign-On and simplify the development of custom authentication schemes, the XauthRADIUS Integration for CA Single Sign-On an authentication scheme that can be used to authenticate through other products via the Remote Authentication Dial In User Service (RADIUS) protocol. It provides a generic interface to authenticate users to a number of authentication products that support RADIUS and has been successfully tested with RSA's SecurID, Axent's Defender, Secure Computing's SafeWord and others.

Benefits That Deliver Value

XauthRADIUS Integration for CA Single Sign-On delivers:

- Flexibility in implementing robust authentication
- Simplify the development of custom authentication schemes
- Extended capabilities beyond the CA Single Sign-On RADIUS offering

"Out of the Box" RADIUS Authentication Scheme vs. XauthRADIUS

CA Single Sign-On includes a RADIUS Authentication Scheme in the default installation. The XauthRADIUS Authentication Scheme can provide the same functionality as the product Authentication Scheme, but also includes additional functionality. The main differences between these two Authentication Schemes are shown in the table below:

Feature	OOTB	XauthRADIUS
Basic style authentication	Yes	Yes
HTML Forms-based authentication	No	Yes
RADIUS server Failover	No	Yes
RADIUS server intelligent routing	No	Yes
Directory Password plus RADIUS password	No	Yes
One-shot Authentication support	Yes	Yes
Challenge/Response support	No	Yes
RADIUS over IPv6	No	Yes

How It Works

The packaged work product is deployed as an authentication scheme, active response, and credential collector for the CA Single Sign-On solution based on HTML forms templates which are used to collected credentials for validation against a RADIUS-enabled back end authentication server.

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.