Integration for CA Single Sign-On with Entrust® IdentityGuard

What It Does

EnTrust® IdentityGuard is a strong authentication solution. It performs this function very well, but it does not have an authorization function (authentication is verifying who you are, while authorization is verifying whether you are allowed to access a specific resource). CA Single Sign-On performs both the authentication and authorization functions. The Entrust® IdentityGuard for CA Single Sign-On solution allows our customers to utilize the Entrust® IdentityGuard authentication function with the Single Sign-On authorization function.

Entrust IdentityGuard can authenticate with many methods. The following methods are supported by the Entrust IdentityGuard for Single Sign-On solution:

1. Grid Authentication
2. Knowledge Based Authentication
3. Machine Authentication coupled with Grid Authentication
4. Machine Authentication coupled with Knowledge Based Authentication

Benefits That Deliver Value

For Customers that own Entrust IdentityGuard or acquire companies that owned Entrust IdentityGuard implementation of a new solution and retraining users can be a costly endeavor. On the other hand, not having authorization control over their resources introduces risk. By utilizing the Entrust IdentityGuard for Single Sign-On solution the end-user experience is stable while gaining the needed authorization control of the resources.

How It Works

The Entrust IdentityGuard for Single Sign-On solution is composed of two parts:

- a tailored CA Single Sign-On Authentication Scheme on the Policy Server
- and forms/jsps/js on the Web Server.

The tailored authentication scheme contains the logic. The logic is as follows:

1. A request is made for a protected resource on a Web Server protected by CA Single Sign-On. The particular authentication scheme is IdentityGuard Auth Scheme.

2. The User is prompted for UserId and Password
3. The tailored authentication scheme will validate the UserId and Password against the configured User Directories
4. If successful, CA Single Sign-On will call the Entrust IdentityGuard server for a challenge response, this response will be forwarded to the end user
5. The end user's answer will be forwarded back to the authentication scheme
6. The authentication scheme will forward the answer to the Entrust IdentityGuard server
7. The authentication scheme will take the response from the Entrust IdentityGuard server, and if successful the end user will be forwarded to the protected resource

When the IdentityGuard Machine Authentication is used in conjunction with a challenge authentication (Grid or Knowledge based), there is an added step at the beginning. This step is to authenticate the machine that the end user is logging in from. If the machine identity can be determined and is trusted then the challenge authentication is skipped. In this case only the UserId and Password is required.

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.