Active Directory Authentication for CA Identity Manager

What It Does

CA Identity Manager comes with an out of box authentication module that authenticates the user against the directory configured for the environment. However, if the user needs to be authenticated against an external Active Directory, this PWP is designed to facilitate the authentication.

The Packaged Work Product contains a servlet filter based authentication invoked by a login page that then connects to the configured Active Directory and authenticates the user. The following steps are performed:

1. The user types a username and a password in the login page, and the Component authenticates the user using the credentials.
2. The Component supports a configurable list of Active Directory domain servers in failover mode.
3. The SSL connection to the Active Directory is supported.
4. The following exception messages are handled and displayed on the page:
   a. User Not Authenticated
   b. User Not Found
   c. Internal Error Accessing Active Directory Service
   d. Account Locked
   e. Password Expired

Benefits That Deliver Value

Active Directory Authentication for CA Identity Manager provides:

- Centralized external authentication via an Active Directory source
- Secure, Reliable, and Scalable
- Simplicity of support

How It Works

The Packaged Work Product consists of two primary features:

Disambiguation of the User

The Component queries the CA Identity Manager User Repository to find the user. If the user is not found, the Component will return an error. If the user is found, then the user is authenticated.

Optionally, an attribute in the CA Identity Manager user repository may be used to properly map the username for the Active Directory (if the username in the CA Identity Manager user repository and Active Directory are different).

Authenticating the User

Upon successful disambiguation of the user, the Component will authenticate the user with respect to Active Directory. In the case where the ids are different the authentication module will use the mapped username to authenticate against the Active Directory.

If the user is not authenticated for some reason, the proper exception will be caught and passed to the login page as a user friendly message.

If the user is successfully authenticated then the authorization is handled by CA Identity Manager itself, based on the privileges within the CA Identity Manager user repository.

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.