Impersonation for CA Single Sign-On

What It Does

The Impersonation module extends the functionality of CA Single Sign-On to enable one set of users to ‘impersonate’ another set of users (Customer Service Rep use case, CSR), or to enable a user who has multiple accounts to switch between accounts, without having to re-submit authentication credentials (Persona use case). When switching accounts, a SMSESSION cookie containing the DN of the new user account is issued, and as far as the CA Single Sign-On solution is concerned, the impersonator is the user who is being impersonated. Because this is a very powerful privilege, a combination of policies for CA Single Sign-On and special logic in the Impersonation module will restrict use of this function.

The Impersonation Authentication Scheme will:

1. Allow a user authenticated and/or authorized in one user directory to impersonate a user whose authentication/authorization data is in the same or another directory.
2. Optionally enable a header variable or cookie to be generated that contains the login-ID or DN of the impersonator. This is not available for the personas use case.
3. Optionally provide an event handler logging mechanism that will provide an audit log of all impersonation authentication events and all the protected resources accessed during the impersonation session.
4. Requires the impersonator to authenticate via any of the authentication schemes supported by CA Single Sign-On and be authorized as an impersonator before being able to access the impersonation function. This is accomplished via the Realm, Rule, and Policy definitions of CA Single Sign-On.
5. Provides multiple mechanisms for authorizing groups of impersonators to impersonate certain groups of users (CSR use case):
    a. A grouping mechanism to restrict each impersonator to only be able to impersonate users in assigned groups or roles. Impersonators will have a multi-valued attribute with a name like ImpRights that will list the group names they can impersonate. Impersonatees will have a multi-valued attribute with a name like ImpRoles that will list the names of the groups they belong to. An impersonator will only be able to impersonate an impersonatee if the impersonatee’s list of group names is a subset of the impersonator’s list of group names. From the point of view of the impersonation authentication scheme these group names are

simply text strings that are compared and can represent any kind of role, group, or even the ID of an individual user.

   b. Allow impersonators to impersonate anyone.
   c. Allow impersonators to impersonate anyone who is a peer in the LDAP DIT. That is anyone who has the same DN except for their uid.
   d. Allow impersonators to impersonate anyone who is a subordinate in the DIT. That is anyone who is below them in the DIT.
   e. Allow impersonators to impersonate anyone whose user entry is in a particular branch of the LDAP DIT.
   f. Allow impersonators to impersonate anyone who belongs to a specified group defined in the user store.

6. Personas use case: User's primary account contains an attribute containing a default secondary account login ID, plus a multi-valued attribute containing a complete list of the user's secondary account login IDs. The user is only allowed to switch between their master account and the accounts whose login IDs are listed in the multi-valued attribute.

Benefits That Deliver Value

Impersonation for CA Single Sign-On:

- Simplifies the authentication process
- Provides flexibility to users with specific privileges
- Maintains security of impersonators by role and group

How It Works

The packaged work product consists of two policy server plugins, one for impersonation and one for logging.

Two configuration files control the behavior of the two plugins.

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.