

Advanced Certificate Authentication for CA Single Sign-On



What It Does

The Advanced Certificate Authentication for CA Single Sign-On enables customers to specify LDAP search filters to map data from their certificates to data in their user store in order to determine which account in the user store to associate with the session being authenticated.

- The mapping is configured via the CA Single Sign-On Admin GUI, using the certificate's custom mapping attribute.
- The mapping string is an LDAP search filter. If the search returns one distinguished name (DN), mapping is successful, indicating that the cert part of authentication is successful.
- If the StepUp authentication feature is being used, then optionally the same client certificate can be shared by multiple users.
- Supports the following Cert fields as macros in the filter string:
 - Subject DN or any component of it
 - Issuer DN or any component of it
 - Serial number
 - Subject Key ID
 - Subject Alternate Name extension – RFC822Name and/or Principal Name
- Supports the following Cert, cert+basic, certorbasic, cert+forms, and certorforms variations
 - For cert+forms and cert+basic, disambiguation is by basic/form credentials.
 - Password & Cert are validated for authentication; DN returned by Cert filter search must match disambiguated DN.
- Supports StepUp authentication
- Supports using an SSL Accelerator that terminates the SSL connection before it reaches the web server
- Example Mapping Strings:
 - DNsearch=%{DN} – This is how to search for a user entry whose DN matches the Subject DN of the certificate.
 - certSubjectDn=%{DN} – The certificate's Subject DN matches the value stored in the certSubjectDn custom attribute in the user's LDAP user entry.

Benefits That Deliver Value

The Advanced Certificate Authentication for CA Single Sign-On provides:

- Flexibility in search and query methods
- Flexibility in certificate disambiguation

How It Works

The Advanced Certificate Authentication for CA Single Sign-On is implemented as a Single Sign-On Authentication scheme and the user experience is similar to the out of the box CA Single Sign-On Certification Authentication. This component only supports LDAP based user directories.

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.