



# Rocket® LDAP Bridge

The Real-time LDAP Gateway to Mainframe Security Data

Provides bi-directional password synchronization between mainframe security database and the client

Uses TLS/SSL with Mutual Authentication and CRL checking

Provides LDAP change logging and audit logging

Provides alias management on user creation and deletion

## Configure and Audit Mainframe via LDAP

Whether you use RACF, CA ACF2, or CA Top Secret to store and enforce your mainframe security policy, Rocket LDAP Bridge allows deeper integration with your other enterprise security projects while reducing your dependence on mainframe-specific expertise. Relieve strain on your high-value mainframe security staff by using LDAP to automate help desk tasks. Rocket LDAP Bridge allows mainframe security data to be read and written over a secure LDAP connection, and offers a variety of special features through plug-ins. Take on new projects to streamline security management that just weren't technically feasible before.

## Make it Happen with Plug-Ins

Rocket LDAP Bridge serves as the foundation for a suite of plug-in products. Each plug-in adds features to the Rocket LDAP Bridge server, ranging from 'core' features (like reading and writing mainframe security information) to the exotic (like executing complex remote commands).

- ❖ racf2ldap, acf22ldap, tss2ldap: Provide automatic outbound synchronization from RACF, CA ACF2, or CA Top Secret to the LDAP Server.
- ❖ ldap2racf, ldap2acf2, ldap2tss: Provide inbound synchronization. These plug-ins are designed to allow you to update RACF, CA ACF2, or CA Top Secret fields.
- ❖ pticket: Provides RACF PassTicket credentials to sufficiently authorized LDAP clients. Idifsync: Provides a method for authorized LDAP clients to retrieve, in standard LDIF format, the changes that were made to the RACF, CA ACF2, or CA Top Secret database since the last Idifsync query.

- ❖ ldap2tso: Provides a method for authorized LDAP clients to issue non-interactive TSO commands, in the security context of the authenticated LDAP user.
- ❖ pwdsync: Provides a method for authorized LDAP clients to push passwords to the mainframe, or read the results of each user's most recent password change.

## How it Works

Based on OpenLDAP with LDAPv3 support, Rocket LDAP Bridge consists of a base product and a flexible set of optional plug-ins.

- ❖ Works with mainframe security database fields:
  - All RACF fields
  - All TSS fields including user-defined fields
  - All ACF2 logonid record fields as well as Access and Resource rules
- ❖ Provides bi-directional password synchronization between mainframe security database and the client
- ❖ Is constructed such that LDAP data and applications reside on the mainframe
- ❖ Uses TLS/SSL with Mutual Authentication and CRL checking
- ❖ Provides LDAP change logging and audit logging
- ❖ Provides alias management on user creation and deletion

## Reduce Costs Through Consolidation

Typically, separate security policy administration is required for mainframe and non-mainframe groups. Rocket LDAP Bridge streamlines all security policy

administration through one group. Managing security policies through a single group reduces the administrative burden, increases efficiency, and ultimately lowers costs while improving outcomes.

## System Requirements

- ❖ Any version of z/OS supported by IBM
- ❖ A version of CA Top Secret that is currently supported by CA (when working with CA Top Secret)
- ❖ A version of CA ACF2 that is currently supported by CA (when working with CA ACF2)

