

## MOVEIT DMZ: EXTERNAL AUTHENTICATION OPTION

This document describes how the MOVEit DMZ secure data transfer and storage server software from Ipswitch can authenticate users against one or more external databases, including Active Directory.

MOVEit DMZ server is an enterprise solution that enables the encrypted transfer and storage of files, messages, and Web form postings. It provides a secure portal for exchanging sensitive data using MOVEit and third-party clients that support either secure HTTP (HTTPS) used by Web browsers and most MOVEit clients, or secure FTP over SSH2 (SFTP and SCP2), or secure FTP over SSL (FTPS).

MOVEit DMZ has its own built-in secure database that it automatically authenticates users against. There is also an external authentication option that enables MOVEit DMZ to authenticate users against LDAP, Secure LDAP and RADIUS Server accessible sources, and ODBC-compliant databases. MOVEit DMZ licensees typically put their business partners and customers into its user database, and use the external authentication capabilities to enable MOVEit DMZ to also authenticate against one or more LDAP and/or RADIUS accessible sources that contain information on their employees. The external authentication option works with any combination of the following products.

**Active Directory (AD)** by Microsoft via LDAP or Secure LDAP

**Border Manager** by Novell via RADIUS

**eDirectory** by Novell via LDAP or Secure LDAP

**Internet Authentication Services (IAS)** by Microsoft via RADIUS

**iPlanet** by Sun Microsystems via LDAP or Secure LDAP

**Tivoli Access Manager** by IBM via LDAP

The external authentication option also includes a RADIUS:ODBC authentication service that enables MOVEit DMZ to authenticate against one or more ODBC-compliant databases that contain clear text usernames and passwords. (Note: Several methods exist for automatically importing usernames and passwords into the MOVEit DMZ built-in user database from ODBC-compliant databases.)

The following advanced capabilities are provided by the MOVEit DMZ external authentication option.

**User Replication.** Specific user properties can be looked up on an LDAP server and replicated on MOVEit DMZ during automatic user creation, user signon, and scheduled overnight processes.

**Group Replication.** LDAP user groups and membership can be automatically replicated on MOVEit DMZ, and access to it can also be either restricted or allowed by specific LDAP groups.

**User Expiration.** MOVEit DMZ can automatically expire users in its user database who are no longer visible on the LDAP server(s) that it is configured to authenticate users against.

**Custom Mapping.** Administrators can use a macro syntax to map the specific properties of their LDAP user records to various fields on a MOVEit DMZ user profile.

**Configuration Testing.** Step-by-step testing capabilities are built into MOVEit DMZ to assist administrators to correctly setup its LDAP and/or RADIUS configurations.

**SSO Intergration.** Enables “single sign-on” to the MOVEit DMZ Web interface for end-users who authenticate through either a CA eTrust SiteMinder portal authentication server or using Active Directory and a US Department of Defense (DoD) Common Access Card (CAC).

The MOVEit DMZ external authentication capabilities are part of the product’s commercial codebase, but are offered as a separately licensed and priced option and activated with a special license key.

Information about MOVEit DMZ licensing, and details on how to arrange a free online demo and/or a free online or onsite evaluation of the software, can be obtained by contacting Ipswitch directly. To learn more, please visit [www.ipswitchft.com](http://www.ipswitchft.com) or click on the purple link below for more contact information.



Contact Ipswitch’s File Transfer Division