

Lotus Notes Integration

Simplifying Lotus Notes Management

Lotus Notes ID files and passwords use a complicated combination of encryption and data replication. This complexity makes Lotus Notes expensive to manage and support.

The Hitachi ID Management Suite simplifies user setup, password synchronization, password resets, managing security entitlements in the Notes environment and user deactivation.

Hitachi ID automation and self-service reduce the cost of managing and supporting Lotus Notes.



The Challenge

Managing Lotus Notes ID files and passwords is a challenge for most organizations. ID files are physically distributed, with some users having multiple copies on their PC hard drive, network share or even a USB flash drive. Passwords are applied to both ID files and server-based, distributed database on mail servers. To make matters worse, ID files are encrypted with the user's current password, making administrative password resets impossible.

Onboarding

Activating new users on Lotus Notes is harder than on other platforms. Users need to get a mail box, an entry in the name and address book (NAB), a new ID file and software must be installed on their PC. This is much more complex than creating a new account on a typical directory or application.

Password expiration and synchronization

Routine password changes on Lotus Notes must be coordinated between the user's ID file(s), the user's entry in the Notes directory and other systems, such as Active Directory. This is too hard for users to manage.

Forgotten passwords and intruder lockouts

If users forget their Notes password, they require extraordinary assistance from the help desk. Since a simple, administrative password reset is not possible on Lotus Notes, the help desk must use one of several complex and expensive processes:

- Key recovery
- Deleting the user's account and creating a new one
- Recovering the user's old (and possibly outdated) ID file from a database

In any case, the new or recovered ID file must somehow be installed on the user's PC.

Moving and deactivating users

Moving users from one location or department to another may require their ID file to be moved as well as their mail folder. This is more complex than simply moving a user's object to a new OU in a directory, for example. Deactivating Notes users requires that their public key be added to a certificate revocation list -- a complexity that arises because of the public key infrastructure (PKI) built into Lotus Notes.

The Solution

The Hitachi ID Management Suite includes both extensive user lifecycle management automation and advanced integration with Lotus Notes. This combination helps organizations to reduce the total cost of ownership of the Lotus Notes platform:

User Lifecycle Management Automation

An unattended process can monitor one or more systems of record and automatically create or delete user accounts on Lotus Notes and other systems.

A self-service request entry and approvals system allows business users to request updates to their profiles (e.g., new phone number) and entitlements (e.g., add user to security group). These requests are validated, routed, approved and executed without IT involvement.



The Hitachi ID Management Suite

Password synchronization and self-service password reset

Hitachi ID Password Manager can intercept “native” password changes on systems including Lotus Notes and Active Directory and automatically set all of that user’s other passwords to the same new value. It also provides a user interface where users who forgot their password or triggered a lockout can authenticate with something other than their password (for example, answering personal questions) and can then choose a new password. This is accessible from a web browser, the login prompt, a smart phone or a telephone.

Simplified application login

Hitachi ID Login Manager can capture a user’s Windows login ID and password when the user signs into his workstation and can automatically insert those credentials into other applications that the user launches, such as Lotus Notes. This complements password synchronization with single signon.

Integration with Lotus Notes ID files and User Directories

The Hitachi ID Identity Management Suite includes advanced technology for creating, distributing and managing ID files, as well as user entries in the Lotus Notes directory (Name and Address Book / NAB). This includes collecting ID files and passwords from user PCs and storing them in a secure database as well as pushing out updated ID files back to user PCs or network shares. In fact, the Hitachi ID architecture for managing ID files works so well that IBM copied it in the Lotus Notes 8.5 release.

Impact

Deploying Hitachi ID Password Manager reduces the cost and complexity of managing users and passwords in the Lotus Notes environment:

- User setup is simpler and faster.
- Passwords are automatically synchronized between Lotus Notes and Active Directory
- Users can reset their own forgotten passwords.
- Security entitlements can be managed and reviewed by business users
- Access deactivation is automatic and reliable.

Technical Specifications

TARGET SYSTEM INTEGRATION

Directory:

Windows domains, Active Directory, eDirectory, Novell NDS, any LDAP

File/Print:

Windows 2000, 2003, 2008; Novell NetWare, Samba

Databases:

Oracle, Sybase, SQL Server, DB2/UDB, Informix

Unix:

Linux, Solaris, HP/UX, AIX, Tru64, Irix, Unisys, SCO, DG; passwd, shadow, TCB, Kerberos, NIS, NIS+

Mainframes:

z/OS, VM/ESA, Unisys, Siemens

Minis:

iSeries OS400, OpenVMS, Tandem

Applications:

Oracle eBusiness Suite, PeopleSoft, SAP R/3, JD Edwards

Groupware:

Microsoft Exchange, Lotus Notes, Novell GroupWise

Networking:

Cisco ACS, RADIUS, TACACS+, etc.

Flexible Agents:

API, Web services, command-line, SSH, Telnet, TN3270, TN5250, SQL injection, LDAP attributes, Web services, web forms

SUPPORT INTEGRATION

Automatically create/update/close incidents:

- Axios Assyst
- BMC Remedy AR System
- BMC Service Desk Express
- CA Unicenter Service Desk
- Clarify eFrontOffice
- FrontRange HEAT
- HP Service Manager
- Tivoli Service Desk

Additional integrations through e-mail, ODBC, web services, web forms, SQL injection, LDAP attributes and command-line.

Hitachi ID Systems, Inc.

500, 1401 - 1 Street SE
Calgary AB Canada T2G 2J3
Tel: 1.403.233.0740 Fax: 1.403.233.0725
E-Mail: info@Hitachi-ID.com