

# Why Self-Service Password Reset Is Essential for HCL Domino Environments

## Web Password Assistance for HCL Notes and Domino

### Secure Password Recovery — Without the Help Desk

#### White Paper

---

## Executive Summary

Passwords remain one of the most common causes of user-access problems in enterprise IT environments. When an employee forgets a password, becomes locked out, or cannot access their HCL Notes or Domino account, the traditional response is to contact the IT help desk.

For organizations running HCL Domino, this process can be particularly disruptive because Domino authentication is closely associated with Notes user IDs, the Domino ID Vault, server access, mail, applications, and other Domino services.

HCL Domino provides administrators with password-reset capabilities through the ID Vault and also provides a sample self-service password-reset application. However, implementing a convenient, user-friendly self-service experience requires appropriate authentication, password-reset authority, application configuration, and security controls. HCL documentation specifically notes that a custom application can be used to provide self-service password reset.

**Web Password Assistance (WPA)** provides a purpose-built web-based self-service password-reset experience for HCL Notes and Domino users. WPA allows users to reset forgotten passwords without contacting the help desk and incorporates one-time password verification and CAPTCHA into the recovery process.

The business case for SSPR is therefore straightforward:

**Users should be able to securely recover access to their Domino accounts without requiring an administrator to manually reset every forgotten password.**

This can reduce help-desk workload, shorten user downtime, improve the user experience, and provide a controlled password-recovery process.

---

## 1. The Password Problem in Domino Environments

Passwords are unavoidable in many enterprise environments, and forgotten passwords are equally unavoidable.

A typical password-reset scenario looks like this:

1. A user forgets their Domino password.
2. The user cannot authenticate to Notes, Nomad, or another Domino service.
3. The user contacts the help desk.
4. IT must verify the user's identity.
5. An administrator accesses Domino administration tools.
6. The administrator performs the password reset.
7. The user receives instructions for accessing the account again.
8. The administrator returns to other IT responsibilities.

Individually, this may appear to be a minor incident.

Across hundreds or thousands of users, however, password-reset requests become a recurring operational workload.

The problem becomes particularly important in organizations where Domino remains a critical platform for:

- Email and calendaring
- Business applications
- Workflow
- Document management
- Enterprise databases
- Automated processes
- Domino Web applications
- Nomad and Nomad Web
- Remote users

A password problem can therefore become more than an inconvenience—it can prevent an employee from performing normal business activities.

---

## 2. Why HCL Domino Makes Password Recovery Different

HCL Domino uses Notes user IDs as an important component of its security architecture.

The Domino ID Vault provides protected copies of Notes user IDs and enables authorized password-reset operations. HCL describes the ID Vault as providing capabilities including password resets, ID recovery, synchronization of ID copies, and support for custom password-reset applications. HCL states that use of the ID Vault is strongly recommended.

Domino also provides specific security mechanisms governing who or what is authorized to reset passwords.

HCL documentation explains that unauthorized password resets are protected through Password Reset Certificates. A custom password-reset application requires password-reset authority to be assigned to the identity under which the application operates and to the appropriate servers.

This is important because an enterprise SSPR solution should not simply provide a web page that changes passwords.

It must operate within Domino's security model.

---

## 3. HCL Provides the Technology—But Organizations Still Need the User Experience

HCL Domino includes a sample web-based self-service password-reset application called **PwdResetSample.nsf**.

HCL documentation explains that the sample application allows users whose IDs are stored in the ID Vault to reset their Notes passwords from a browser. However, the sample application is intended as an example that organizations can customize. Its deployment requires configuration of the database ACL, agent signing, server permissions, password-reset authority, and other settings.

HCL also explicitly documents the ability for developers to create custom password-reset applications using the `ResetUserPassword` method.

In other words, Domino provides the underlying capability.

Organizations still need to determine how they want to deliver that capability to their users.

This distinction is important:

**Domino password reset capability  $\neq$  complete end-user SSPR solution.**

An enterprise SSPR solution must address questions such as:

- How does the user prove their identity?
- How does the user request a reset?
- How is the verification process protected?
- How is automated abuse prevented?
- How does the user create a new password?
- How are successful resets recorded?
- How does the solution integrate with the Domino environment?
- How easy is the solution for employees to use?

---

## 4. The Business Case for Self-Service Password Reset

### 4.1 Reduce Help-Desk Workload

Password-reset requests are repetitive.

IT personnel frequently spend time performing tasks that do not require specialized troubleshooting skills:

- Identifying the user
- Verifying identity
- Finding the user's account
- Performing the password reset
- Communicating the result
- Helping the user reconnect

An SSPR solution moves much of this process from IT to the user while maintaining appropriate authentication and security controls.

Instead of:

**User → Help Desk → Administrator → Domino → User**

the process becomes:

**User → Secure SSPR Portal → Domino → User**

This allows IT personnel to concentrate on higher-value work such as infrastructure, security, applications, troubleshooting, and strategic projects.

---

## 5. Reduce User Downtime

A forgotten password can occur at any time.

It may happen:

- Before work
- After business hours
- During weekends
- While traveling
- While working remotely
- During a holiday
- When the help desk is closed

Traditional password recovery introduces a dependency on IT availability.

Self-service removes much of that dependency.

A user can access a web-based password recovery process without waiting for an administrator to become available.

The result is a shorter path from:

**"I cannot log in."**

to:

"I am back to work."

---

## 6. Improve Security Through Controlled Recovery

Self-service password reset should not mean unrestricted password changes.

The opposite is true.

A properly designed SSPR system should provide controlled identity verification before allowing a password reset.

HCL explicitly identifies **trust in the identity of the user whose password is being reset** as one of the key security considerations for password-reset applications. HCL also states that the application is responsible for verifying the identity of users who use it.

Web Password Assistance addresses this requirement through a web-based verification workflow.

WPA includes:

- One-time password (OTP) verification
- CAPTCHA
- Account verification
- Verification-code email
- New-password creation
- Password-change confirmation
- Password-reset logging

The published WPA workflow shows these stages on the product page.

These controls help establish a structured recovery process rather than simply exposing a password-change function.

---

## 7. One-Time Password Verification

A significant component of the WPA recovery process is the use of a one-time verification code.

The basic concept is:

**Identify Account → Send Verification Code → Verify Code → Create New Password**

The verification code provides an additional step in establishing that the person attempting the reset has access to the designated verification channel.

This is particularly useful for forgotten-password scenarios because the user may no longer know the existing password.

The recovery process therefore does not need to depend exclusively on the user's existing password.

---

## 8. CAPTCHA and Automated Abuse

Password-reset endpoints can themselves become targets for automated abuse.

For example, attackers may attempt to:

- Enumerate user accounts
- Submit repeated reset requests
- Abuse verification mechanisms
- Automate requests against a password-reset page

Web Password Assistance incorporates CAPTCHA into its password-recovery workflow.

CAPTCHA can provide an additional barrier against automated activity.

It should be viewed as one component of a broader security architecture rather than as a replacement for authentication, network security, monitoring, or other enterprise controls.

---

## 9. The Domino ID Vault Provides the Foundation

An SSPR solution does not replace the Domino ID Vault.

It works with the Domino security architecture.

HCL describes the ID Vault as a server-based database containing protected copies of Notes user IDs. Among its benefits are the ability for authorized personnel to reset passwords and support for custom password-reset applications.

HCL's current documentation also explains that a Domino environment must establish password-reset authority when configuring the ID Vault.

This provides an important security boundary:

**The web application requests a password reset; Domino's security architecture determines whether the operation is authorized.**

That separation is important in an enterprise environment.

---

# 10. Why a Dedicated SSPR Application Can Be Preferable to Manual Administration

Without SSPR, the password-reset process is administrator-centric.

An administrator must intervene every time a user forgets a password.

With SSPR, the organization can move routine password recovery toward a user-centric model.

| Traditional Process                 | SSPR Process                                      |
|-------------------------------------|---------------------------------------------------|
| User contacts help desk             | User opens web portal                             |
| IT verifies request                 | Automated verification workflow                   |
| Administrator performs reset        | Authorized application performs reset             |
| User waits for assistance           | User completes recovery process                   |
| IT handles repetitive task          | IT remains available for higher-value work        |
| Recovery depends on IT availability | Recovery can be available through a web interface |

The objective is not to eliminate IT involvement in security.

The objective is to eliminate unnecessary IT involvement in routine password recovery.

---

# 11. Support for Modern Domino Environments

Domino environments are no longer limited to the traditional Notes desktop client.

Organizations may use a combination of:

- HCL Notes
- Domino Web applications
- Domino Workspace
- Nomad
- Nomad Web
- Browser-based applications
- Windows clients
- macOS clients
- Mobile and remote users

WPA supports Notes and Domino, Domino Workspace and Nomad Web, and modern browsers including Chrome, Edge, Firefox, and Safari. It also lists Windows and macOS desktop platforms and Windows, Linux, and AIX server platforms.

A browser-based recovery mechanism is therefore particularly relevant to organizations with geographically distributed or remote users.

---

## 12. Directory Integration

Large Domino environments may contain more than a single straightforward directory configuration.

Organizations can use:

- Domino Directory
- Directory Assistance
- Multiple Domino domains
- Organizational units
- Complex enterprise directory structures

WPA supports the Domino Directory and Directory Assistance.

This can be important for organizations where a simple single-directory assumption does not accurately represent the production environment.

---

## 13. Operational Visibility

A password-reset system should provide administrators with visibility into password-recovery activity.

WPA app includes a **Log** as part of its workflow.

Logging can provide useful operational information such as:

- Password-reset activity
- Successful recovery operations
- Failed attempts
- Troubleshooting information
- Administrative visibility

Organizations should incorporate SSPR logging into their broader monitoring, auditing, and security policies.

---

## 14. SSPR and the Modern Security Model

Modern security programs increasingly recognize that passwords alone are not sufficient protection for sensitive systems.

CISA recommends multifactor authentication because it makes unauthorized access more difficult even when passwords have been compromised.

SSPR should therefore be considered part of a larger identity-security strategy.

A mature Domino security architecture may combine:

## **User Identity**



## **Identity Verification**



## **SSPR**



## **Domino ID Vault**



## **Password Reset Authority**



## **Notes / Domino / Web / Nomad Access**

SSPR does not replace MFA, endpoint security, network security, or other security controls.

Instead, it provides a controlled mechanism for recovering access when the user's existing password is unavailable.

---

# **15. The Cost of Doing Nothing**

The cost of password resets is not limited to help-desk labor.

There can also be indirect costs:

### **Lost employee productivity**

The employee cannot access required systems while waiting for assistance.

### **Help-desk interruption**

IT personnel must repeatedly stop other work to process password-reset requests.

### **After-hours support**

Organizations may need to provide support outside normal business hours for users who cannot work.

### **Administrative overhead**

Every manual reset creates another administrative transaction.

## User frustration

Repeated dependency on IT for routine account recovery creates unnecessary friction.

## Security risk

Poorly controlled manual recovery processes can create opportunities for social engineering if identity verification is inconsistent.

SSPR addresses these issues by creating a standardized recovery workflow.

---

# 16. Why Web-Based SSPR Matters

A browser-based password-reset application has a significant practical advantage:

**The user does not need the application they are currently locked out of in order to begin recovery.**

If a user cannot authenticate to the Notes client, a browser-based recovery portal can provide an alternative path to account recovery.

This is particularly useful for remote employees.

The recovery experience can be reduced to:

### Open Browser



### Verify Domino Account



### Receive Verification Code



### Enter Verification Code



### Create New Password



### Return to Work

This is the core value proposition of Web Password Assistance.

---

## 17. Web Password Assistance

NotesMail's **Web Password Assistance (WPA)** is designed specifically around this Domino password-recovery use case.

The product describes itself as a Domino web self-service password-reset application that enables users to reset forgotten passwords without contacting the help desk.

Its published capabilities include:

- Self-service password recovery
- OTP verification
- CAPTCHA
- Domino Directory support
- Directory Assistance support
- Notes and Domino compatibility
- Domino Workspace compatibility
- Nomad Web compatibility
- Chrome, Edge, Firefox and Safari support
- Windows and macOS desktop environments
- Windows, Linux and AIX server environments
- Password-reset logging
- Simple installation
- No DLL requirement
- Modern web implementation rather than legacy XPages

The product therefore addresses both sides of the password-reset problem:

### **Business requirement:**

Reduce the operational burden of routine password recovery.

### **Technical requirement:**

Provide a controlled web-based interface that works with the Domino password-reset infrastructure.

---

## 18. A Practical ROI Model

Organizations can estimate the potential value of SSPR using a simple calculation.

### **Annual Help-Desk Cost**

**Number of password-reset incidents per year**

×

**Average IT minutes per incident**

÷ 60

×

**Fully burdened hourly IT cost**

=

**Annual password-reset labor cost**

For example, an organization experiencing 1,000 password-reset incidents annually at an average of 15 minutes per incident would spend approximately:

**250 IT hours per year**

on password-reset activity.

At a hypothetical fully burdened IT cost of \$75/hour:

**250 × \$75 = \$18,750**

This does not include employee downtime, after-hours support, interruption costs, or the administrative overhead associated with manual processing.

The actual financial benefit will vary substantially by organization, user population, incident volume, and labor costs.

---

## 19. Recommended SSPR Architecture

A typical Domino SSPR deployment should include:

### 1. Domino ID Vault

Provides the protected repository and password-reset infrastructure.

### 2. Password Reset Authority

Defines which identity or application is authorized to perform password resets.

### 3. Web Password Assistance

Provides the user-facing recovery interface.

### 4. Identity Verification

Establishes that the person requesting the reset is authorized to perform it.

### 5. OTP / Verification Controls

Provides an additional verification mechanism.

## 6. CAPTCHA

Helps reduce automated abuse.

## 7. Logging and Monitoring

Provides visibility into recovery activity.

## 8. TLS/HTTPS

Protects communications between users and the web application.

This layered architecture helps separate **user convenience** from **security authority**.

---

# 20. Implementation Considerations

Organizations considering SSPR should evaluate:

- Domino version
- ID Vault configuration
- User registration and vault coverage
- Password-reset authority
- Directory configuration
- Directory Assistance
- SMTP/email availability for verification
- HTTPS/TLS configuration
- Network accessibility
- Firewall rules
- Logging requirements
- Security policies
- Password complexity requirements
- User communication
- Help-desk procedures
- Backup and recovery procedures

HCL documentation emphasizes that password-reset applications must appropriately establish trust in both the reset application and the identity of the user requesting the reset.

SSPR should therefore be implemented as part of the organization's overall identity and access-management strategy.

---

# 21. Frequently Asked Questions

## **Is SSPR mandatory for HCL Domino?**

No. Domino provides administrator-based password-reset functionality, and organizations can choose whether to implement self-service recovery.

However, SSPR becomes highly valuable when organizations want to reduce routine help-desk password-reset activity and allow users to recover access without waiting for IT.

## **Does Domino support self-service password reset?**

Yes.

HCL provides a sample web-based self-service password-reset application and documents APIs and mechanisms that developers can use to create custom password-reset applications.

## **Does SSPR replace the Domino ID Vault?**

No.

The ID Vault remains an important component of Domino's identity infrastructure. HCL specifically documents support for custom password-reset applications using the ID Vault.

## **Is self-service password reset secure?**

Security depends on implementation.

HCL identifies user identity verification and application trust as important security considerations for password-reset applications.

An SSPR implementation should therefore use appropriate authentication, verification, authorization, TLS, logging, and operational controls.

## **What happens if the user forgets their password outside business hours?**

With an appropriately deployed web-based SSPR system, the user can initiate the recovery process without waiting for a help-desk administrator.

This is one of the principal operational advantages of self-service recovery.

---

## **22. Conclusion**

HCL Domino provides a robust security architecture for managing Notes user IDs and password resets. The Domino ID Vault provides the underlying infrastructure for password recovery, while HCL also provides mechanisms for building self-service password-reset applications.

The remaining challenge is delivering that capability in a convenient, secure, user-friendly experience.

That is where SSPR fits.

A properly implemented self-service password-reset solution can:

**Reduce help-desk workload**

**Reduce employee downtime**

**Provide faster account recovery**

**Standardize the password-recovery process**

**Provide identity-verification controls**

**Reduce dependence on manual administrator intervention**

**Improve the user experience**

**Support modern browser-based work environments**

For organizations that depend on HCL Domino for email, applications, workflow, and business operations, password recovery is not merely an administrative task. It is an availability and productivity issue.

Web Password Assistance addresses this problem by providing a dedicated web-based SSPR experience designed for HCL Notes and Domino.

**Secure password recovery — without the help desk.**

---

## About Web Password Assistance

**Web Password Assistance (WPA)** is a web-based self-service password-reset solution for HCL Notes and Domino.

WPA is designed to enable users to recover access to their Domino accounts through a browser-based verification and password-reset workflow while reducing the need for routine help-desk intervention.

NotesMail is an HCLSoftware Business Partner providing Domino solutions since 1994.

**Product website:**

<https://www.notesmail.com/Web-Password-Assistance>

**HCL Domino documentation:**

HCL documents both ID Vault password-reset capabilities and custom/self-service password-reset applications.

---

## Disclaimer

This white paper is intended for informational and product-marketing purposes. Actual security, availability, regulatory, and cost benefits depend on an organization's environment, configuration, policies, user population, and implementation. Organizations should evaluate their own security requirements and conduct appropriate testing before deploying an SSPR solution in production.