



## Features Comparison Guide:

PortalGuard and Domino R6/7/8/8.5

### ***About PortalGuard***

PortalGuard enhances the security of Domino by offering strong authentication functionality. PortalGuard addresses the increased security standards of industries handling highly sensitive data such as banking and financial services.

Your company's most valuable commodity is housed in its information systems. Keeping it secure is a top priority. At the center of any data security model is the password. It is the key that unlocks the doors to your company's data. In order to secure access to critical business applications and data, Administrators need to ensure access is granted only to those individuals who are authorized.

With the rising implementation of e-business applications and need to provide employees, vendors, and customers around the world with access to corporate intranets and extranets, it is becoming even more important for IT administrators to keep access secure. In addition, writes ePro magazine's Jim O'Donnell, "As system hackers get more sophisticated, network administrators have on their hands the increasingly tougher task of defending against unwanted intruders."

PortalGuard prevents multiple concurrent logins preventing multiple users from using the same login credentials. PortalGuard allows Administrators to set strike-out limits per user or group and send an alert email notification when those counts are exceeded.

The challenge for corporations today is implementing a cost-effective solution that will secure the password authentication process and lock down their data as well as minimize the Help Desk calls eating up support staff time and money.

PortalGuard makes it happen. PortalGuard offers dozens of password authentication features not available in Lotus Domino R6/7/8/8.5, including self-service password reset, strikeouts per domain, self-registration, auditing, site seal to help prevent phishing, and multi-password synchronization. This powerful solution allows end-users to easily manage their passwords directly from a Web browser, while providing administrators with functionality to meet or exceed your corporate security initiatives.

PortalGuard includes features that fall into three categories:

- **Security and Auditing** - Features that secure the authentication process.
- **Help Desk and End User Productivity** – Features that decrease Help Desk calls about forgotten passwords and password resets.
- **Corporate Branding and Awareness** – Features that allow customization of login screens for creating an interface that is user-friendly and consistent with your corporate look and messaging without use of Domino Designer.



## Security & Auditing Features

Feature	Feature Details	Domino R6/7/8/8.5	PortalGuard (PG)
<b>Prevent Multiple Logon Sessions</b>	Prevent users from using same login credentials concurrently on different machines.	Not Included	<b>NEW</b>
<b>Multiple Factor Authentication</b>	Username, password and a challenge question must be answered for successful login. Upon first logon user is prompted to set and answer set <i>n</i> challenge questions. After initial login user is then prompted to enter username, password and answer one of those challenge questions. Challenge questions are randomized upon every login.	Not Included	<b>NEW</b>
<b>Lockout User After <i>n</i> Days</b>	Lockout inactive users after <i>n</i> number of days, prevents dictionary attacks on inactive end-user accounts. The lockout removes the password from the existing user account in the Domino directory and requires the Help Desk to reinstate.	Not Included	<b>NEW</b>
<b>Alert Administrator When Strike-out Count Exceeded</b>	Email alert is sent to Group or People alerting of strike-out count exceeded. Limit is set by administrator. Alert contains: <ul style="list-style-type: none"> <li>• Username</li> <li>• Password used</li> <li>• Time and date</li> <li>• Client IP address</li> <li>• URL requested</li> <li>• Server</li> </ul>	Not Included	<b>NEW</b>
<b>Policy-based Settings</b>	Set strikeout limit and password rules per user, group or domain hierarchy. These rules previously were the same for all users of a server.	Limited	<b>NEW</b>
<b>Site Seal</b>	Prior to logging in end-user sets custom Site Seal (color and text) this information is stored on the server, NOT client. Upon setting, Site Seal is displayed after username is entered and before password is entered to help prevent phishing and ensure credentials are submitted to authentic site.	Not Included	<b>NEW</b>
<b>Restrict Time of Day Login</b>	Restrict end-users from logging in during certain hours, policy is set per user.	Not Included	<b>NEW</b>
<b>Password Limit</b>	Restrict the frequency which a previously used password can be re-used for login purposes. Does not allow passwords to be reused for <i>n</i> days.	Not Included	<b>NEW</b>

Feature	Feature Details	Domino R6/7/8/8.5	PortalGuard (PG)
<b>Timer Auto Logoff</b>	Automatically logoff inactive users after <i>n</i> minutes. Session is ended and redirected to logoff page to ensure the security.	Not Included	<b>NEW</b>
<b>Enforces Minimum Password Age</b>	Prevent users who were just forced to change their password from immediately changing it back to the previous password.	Not Included	✓
<b>Synchronizes Multiple Passwords via a Web Browser<sup>1</sup></b>	Allows end-users to synchronize Windows, HTTP, LDAP passwords and Notes ID File.  Password synchronization increases security because having only one password to commit to memory decreases the likelihood end-users will write it down and become a target for internal network intruders.	Not Included	✓
<b>Enables the Ability to Force an SSL (Secure Sockets Layer) Connection for Logins</b>	Ensures end-users credentials are submitted via SSL. If end-user tries to login through HTTP instead of HTTPS, PG forces login to HTTPS by redirecting the end-user to the HTTPS connection.	✓	✓
<b>Enables Dictionary Lookup Functionality</b>	Administrators can enable a dictionary lookup to prevent users from setting pre-specified (unacceptable or easily guessed) passwords, such as company name.	Not Included	<b>NEW</b>
<b>Check Password Strength During Login</b>	Verifies password complexity requirements are met prior to allowing login. PG will log the occurrence to the PG log database, immediately force the user to change their password or both.	Not Included	<b>NEW</b>
<b>Log Self-Service Password Reset Attempts</b>	Log when users leverage any of the recovery options within PortalGuard to reset their password. This information can be sent to the PG Log and additionally as an email alert to individuals or groups.	Not Included	<b>NEW</b>
<b>Checks Password Quality by Disqualifying Username as Password</b>	Administrators can prevent new passwords from containing variations of the end-user's username, a typical password choice that is easily guessed by network intruders.  These variants include: <ul style="list-style-type: none"> <li>• First name</li> <li>• Last name</li> <li>• Any entries in the shortname or fullname fields</li> <li>• The organization from the fully qualified Notes name</li> <li>• Any organizational units from the fully qualified Notes name</li> </ul>	Not Included	✓

<sup>1</sup> Password synchronization is supported on Microsoft Windows 2000, 2003 and 2008).

Feature	Feature Details	Domino R6/7/8/8.5	PortalGuard (PG)
<b>Checks Password Quality</b>	<p>Administrators can configure fully customizable password “strength” rules. Domino offers two rules: 1) minimum length and 2) minimum “quality” as defined by the @PasswordQuality formula.</p> <p>PortalGuard offers <b>11 password strength rules</b> that Administrators can easily enable or disable:</p> <ol style="list-style-type: none"> <li>1. Minimum length</li> <li>2. Password cannot contain username</li> <li>3. Passwords cannot be similar to current password</li> <li>4. Password must contain a configurable number of numeric characters</li> <li>5. Password must contain a “special” character (from a customizable list)</li> <li>6. Password must contain a configurable number of lower-case characters</li> <li>7. Password must contain a configurable number of upper-case characters</li> <li>8. Password cannot be a previously used password</li> <li>9. Password cannot be any variant of end-users username</li> <li>10. Password cannot be a dictionary word (used for lists of 10,000+ words)</li> <li>11. Minimum “quality” as defined by @PasswordQuality formula</li> </ol>	Limited	✓
<b>Maintains HTTP Password History</b>	Configurable history limit lets Administrators set how many times an end-user must choose a new password before they can reuse an old one, preventing the end-user from using the same password over and over again.	Not Included	✓
<b>Enables Configurable “Expire On First Login” Functionality</b>	Ensures that end-users will not continue to use the password issued by the Administrator when the end-user account was first set up.	✓	✓
<b>Enables Configurable Password Expiration Intervals</b>	Allows Administrators to set the intervals between end-users’ password resets (e.g. every 30 days).	✓	✓
<b>Enables Password Expiration Grace Period</b>	Lets Administrators select a grace period or a timeframe in which end-users must change their passwords.	✓	✓

Feature	Feature Details	Domino R6/7/8/8.5	PortalGuard (PG)
<b>Stores Last Login Date and Time</b>	Administrators can track the date and time an end-user last logged in — data that is stored as a new field in the Person Document.	✓	✓
<b>Enables Strikeout Limit Functionality</b>	<p>Allows Administrators to set how many logon attempts can be made before the end-user strikes out, preventing dictionary attacks and identifying accounts that have been denied server access.</p> <p>Domino defines strikeout limits at the server-level and maintains separate strikeout databases for each server. This effectively gives users more strikes (which is a security concern) and can be confusing to users if they attempt login to a different server.</p> <p>PG has ability to define strikeouts per user, group or hierarchy. Strikeout limits also work correctly in multi-server environments.</p>	Limited	✓
<b>Enables Strikeout Message Functionality</b>	<p>Administrators can create a custom message for end-users when they strike out, minimizing confusion and subsequent Help Desk calls.</p> <p>Domino message is not configurable and is no different from the “invalid username/password” message which can cause confusion for end-users.</p> <p>PG message is configurable and will alert user as to the number of strikes they have remaining until account lock out. Optionally, Administrators can allow end-users to reset their password in this warning prior to end-users getting locked out of their account. This is done by adding a link in the to warning to the challenge question/ answer recovery page.</p>	Limited	✓
<b>Enables Strikeout Logging Functionality</b>	Strikeouts can be logged to database so Administrators can see who failed to login and when.	✓	✓
<b>Provides Strike Event Functionality</b>	Strike events can be logged to a database so Administrators see who successfully logged in and when.	Not Included	✓
<b>Stores “Set Password” Date and Time</b>	Administrators can track date and time an end-user last set their HTTP password — data stored as a new field in the Person Document.	✓	✓
<b>Logs Password Used</b>	Administrators can enable logging of ‘Password Used’ when a Strikeout, Strike or Invalid Username event is logged to the mail-in database.	Not Included	✓

Feature	Feature Details	Domino R6/7/8/8.5	PortalGuard (PG)
<b>Upgrades Access Level from Author to Editor</b>	Administrators can enable the isProtected property on the HTTP password field or all PortalGuard fields. Once this property is set, an end-user must have Editor-level access or higher to modify the field(s) in the Person Document. This prevents end-users from bypassing the security and auditing functionality enabled by the Administrator.	Not Included	✓
<b>Disables Internet Explorer Auto Complete</b>	Administrators can prevent Internet Explorer Auto Complete feature from offering a list of previously used entries. When enabled, this applies to all PortalGuard fields and only affects IS5.0 and higher. This feature prevents internal intruders from easily accessing the password from the drop-down menu of previously used passwords.	✓	✓
<b>Enables Console Logging</b>	Administrators can choose from three levels of console logging: <ul style="list-style-type: none"> <li>• Informational—enables activities to be logged</li> <li>• None—only errors get logged</li> <li>• Verbose—used for debugging purposes</li> </ul>	Not Included	✓
<b>Logs Invalid Usernames</b>	Administrator can enable logging of invalid usernames to the mail-in database.  This information includes: <ul style="list-style-type: none"> <li>• IP address of computer that made the request</li> <li>• URL requested by the user</li> <li>• Username used</li> <li>• Password given</li> <li>• The PG-specific function the user was trying to accomplish (i.e., login, set password)</li> <li>• The server on which the attempt occurred</li> <li>• The time the attempt occurred</li> </ul>	Not Included	✓
<b>Enables “Set Password” Logging</b>	Administrators can enable logging of successful ‘Set Password’ events to the mail-in database	Not Included	✓
<b>Prevents Similar Password Use</b>	“Prevent Similar Passwords” JavaScript Rule checking disallows use of similar passwords during passwords resets.	Not Included	✓
<b>Allows Extended Storage of Login Information</b>	Administrators can record more detailed information to be sent to the PG database, such as username, time/date, end-user’s IP address, URL requested and server name	Not Included	✓
<b>Confirmation Requirement for Self-registration</b>	An email is sent to end-users with a link to a confirmation page for self-registration. On this page, end-users are prompted for their email address, which affects creation of the Person Document in the Domino directory.	Not Included	✓

## Help Desk & End User Productivity Features

Feature	Feature Details	Domino R6/7/8/8.5	PortalGuard (PG)
<b>Reset Forgotten Password via Browser</b>	Allow end-users to securely reset password from a browser.	Not Included	<b>NEW</b>
<b>Multiple Challenge Question and Answer Password Reset/ Recovery</b>	<p>End-user is presented with a configurable number of questions required to be answered correctly in order to reset their password without help desk intervention, this task can be performed from any browser.</p> <p>This feature stems potential security breaches that occur when Administrators e-mail or phone passwords to end-users.</p> <p>PG enables:</p> <ul style="list-style-type: none"> <li>• Customizable challenge questions</li> <li>• Customizable HTML on successful use of challenge questions</li> </ul>	Not Included	<b>NEW</b>
<b>Recovery/Reset of Active Directory Password</b>	Self-service recovery/reset of Active Directory password using multiple challenge questions and answers.	Not Included	<b>NEW</b>
<b>Enables Forced Challenge Question &amp; Answer Functionality</b>	Allows Administrators to force end-users to set their challenge question and answer before login, reducing Help Desk calls about forgotten passwords.	Not Included	✓
<b>Allows Alternate Login</b>	Allow end-user to login into Domino utilizing the Active Directory or Domino HTTP password.	Not Included	<b>NEW</b>
<b>Enables Self-Registration</b>	Allows end-users to create their own user accounts without administrators involvement.	Not Included	✓
<b>Enables E-mail Random Password Functionality</b>	<p>Allows Administrators to generate random passwords that are automatically emailed to new end-users. This is both an administrative time-saver as well as a security feature because the administrator never sees the password.</p> <p>PG enables:</p> <ul style="list-style-type: none"> <li>• Customizable e-mail fields, including From, Subject and Body</li> <li>• Customizable expiration options (separate from normal setting)</li> <li>• Customizable HTML on e-mail random password use</li> </ul>	Not Included	✓

Feature	Feature Details	Domino R6/7/8/8.5	PortalGuard (PG)
<b>Enables Single Sign-on</b>	<p>End-users only have to authenticate once to access multiple Domino domains (e.g., <code>sametime.pistolstar.com</code> and <code>sametime.pistolstar.us</code>).</p> <p>Domino allows single sign-on within single domain.</p>	Limited	✓
<b>Reduced Sign-on to Portals</b>	Enable end-users to login through Domino and access other portals such as SAP, WebSphere, SharePoint, Apache via ActiveX Control without receiving additional login prompts.	Not Included	<b>NEW</b>
<b>Graphical User Interface Simplifies Usability &amp; Self-Service Experience</b>	An organized and easy-to-use graphical interface allows Administrators to enable all features from an easy-to-configure set of preferences tabs without use/knowledge of Domino Designer. This save time and money because configuring PG does not require developer time	Not Included	✓
<b>Adds Help Desk Manager Utility</b>	<p>Help Desk personnel can manage end-user passwords without full access to PG's configuration data. This database includes six (6) action buttons:</p> <ol style="list-style-type: none"> <li><b>1. Unlock User Button</b>—Unlocks end-user accounts that have been locked out by PG's strikeout functionality.</li> <li><b>2. Email Random Password Button</b>—Generates random value passwords and emails them to the end-user. Can also be used to automatically send multiple end-users' blank passwords.</li> <li><b>3. Reset Password Button</b>—Resets the HTTP password to a new value when end-user does not have an HTTP password, has forgotten it, is unable to reset it themselves, and does not have a Notes Client.</li> <li><b>4. Expire Password Button</b>—Forces end-user(s) to change their HTTP password the next time they log in to Domino through a Web browser. Useful when password policies change.</li> <li><b>5. Reset PG Fields Button</b>—Resets end-user accounts as if they had never accessed PG.</li> <li><b>6. Set Expiration Date Button</b>—Provides a one-time override of PG's expiration functionality. Useful for exempting end-users from resetting a password.</li> <li><b>7. Unlock Agent</b>—Unlocks end-users automatically every x number of hours.</li> <li><b>8. Password Expiration Reminder Agent</b>—Emails users x days before their password expires.</li> </ol>	Not Included	✓

Feature	Feature Details	Domino R6/7/8/8.5	PortalGuard (PG)
<b>Enables Customized HTML</b>	Administrators can write custom messages to end-users to prompt them through the login process, reducing end-user confusion and subsequent Help Desk calls.  Customized messages can be written in the following situations: <ul style="list-style-type: none"> <li>• When end-user is attempting to set their password to a previously used password (i.e., Stored Passwords)</li> <li>• When end-user's password has expired</li> <li>• When end-user's password is expired, but within the grace period (if applicable)</li> </ul>	Not Included	✓
<b>Supports Multiple Hub Servers</b>	Allows end-users to be authenticated against a backup hub server if the primary hub server goes down, preventing Web browser users from being locked out of applications on a Domino server.	Not Included	✓
<b>Supports Multiple Servers</b>	Supports Hub & Spoke topology in real time <sup>4</sup> .	Not Included	✓
<b>Supports Localization</b>	Administrators can configure <b>all</b> UI screens in any language <b>without</b> use/knowledge of Domino Designer. Administrators can easily modify logon screens in any language, ensuring that customized messages and prompts are understood by the end-user. Localization reduces Help Desk calls by minimizing end-user confusion.	Not Included	✓

<sup>4</sup> **Doesn't Domino 6/7/8/8.5 support hub & spoke topology?** With Domino 6/7/8/8.5, reads occur on the local server or the server where the login is being executed. Domino writes occur on the user's home or mail server through AdminP, a task that takes requests and performs them asynchronously. Because tasks are performed on the local server, data will be out of synch for as long as it takes to replicate throughout your entire topology. Password changes will be synchronized across servers eventually, *but not in real time*. If a person modifies their Person Document on different spoke servers, Domino does not prevent replication conflicts from occurring.

PortalGuard helps prevent replication conflicts by notifying users that their passwords are currently out of synch. With The PortalGuard, all reads and writes occur on the hub server regardless of where login is executed. All password changes are made in real-time.

Feature	Feature Details	Domino R6/7/8/8.5	PortalGuard (PG)
<b>Recovers Passwords Without Admin Level Intervention—PG Unlock Utility</b>	<p>PG's strikeout functionality (see description under "Security &amp; Auditing") is an important part of securing the authentication process. When enabled, the end-user is no longer able to log in after a pre-set number of attempts. The PG Unlock Utility allows Help Desk personnel who do not have Editor-level access to the Domino directories to unlock end-users who have struck out.</p> <p>Companies can now delegate unlocking of strikeouts to Help Desk personnel with less security clearance. This is especially beneficial to companies with employees in different time zones, when employing Help Desk personnel with a high-level of security clearance around the clock is costly. The end-user doesn't have to wait for support and the company can maintain security by granting Editor-level access to fewer personnel.</p>	Not Included	✓

### Corporate Branding & Awareness Features

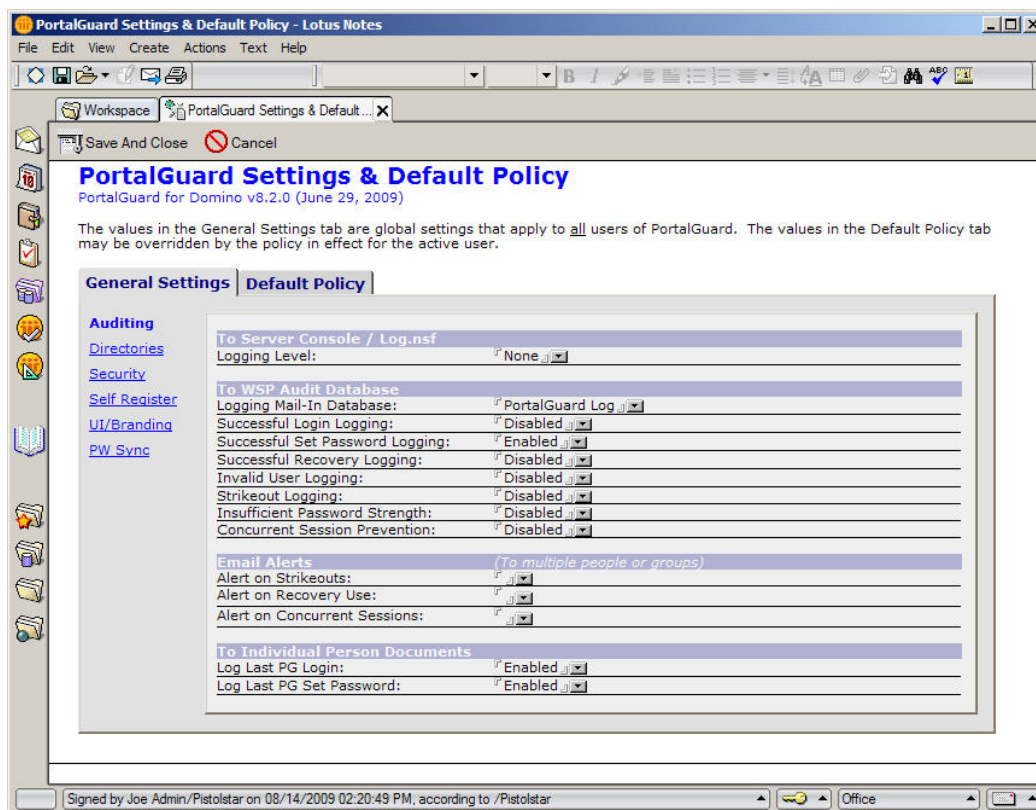
Feature	Feature Details	Domino R6/7/8/8.5	PortalGuard (PG)
<b>Supports Cascading Style Sheets on UI Screens</b>	Enables the ability to use cascading style sheets for all end-user login and set password screens.	✓	✓
<b>Enables Customized Disclaimer Messages</b>	<p>Administrators can create a disclaimer message that the end-user sees prior to performing three actions:</p> <ul style="list-style-type: none"> <li>• Login</li> <li>• 'Set Password'</li> <li>• 'Set Challenge'</li> </ul> <p>This feature can be used to display corporate network usage instructions for sensitive Websites and resources (i.e., password protected).</p>	Not Included	✓
<b>Easily Configurable User Interface</b>	All screens seen by the end-user are configurable <b>without</b> knowledge/use of Domino Designer. Through a user-friendly interface, c\screens can be modified with logo insertion, font and color selection, and editing of HTML seen by user.	Not Included	✓

## Using PortalGuard

PortalGuard comes with a default configuration that can be used as soon as it is installed. Most likely, you will want to customize the settings according to your own password policies.

- **PortalGuard is easy to install and configure.**

Figure 1: Most PortalGuard features can be easily enabled or disabled.



- **PortalGuard requires no client-side software**—PG is a non-invasive solution for the end-user. Because it is a server-side solution, it does not require end-user setup. Help Desk calls related to deployment are minimal to non-existent.
- **PortalGuard System Requirements:**
  - IBM Lotus Domino R6 or Higher
  - Supports IBM System i, IBM AIX 5.1 or higher, Linux, Sun Solaris Ultra SPARC, Microsoft Windows Server 2008/2003/2000

###