

SecureDomino

Authentication & Intrusion Prevention

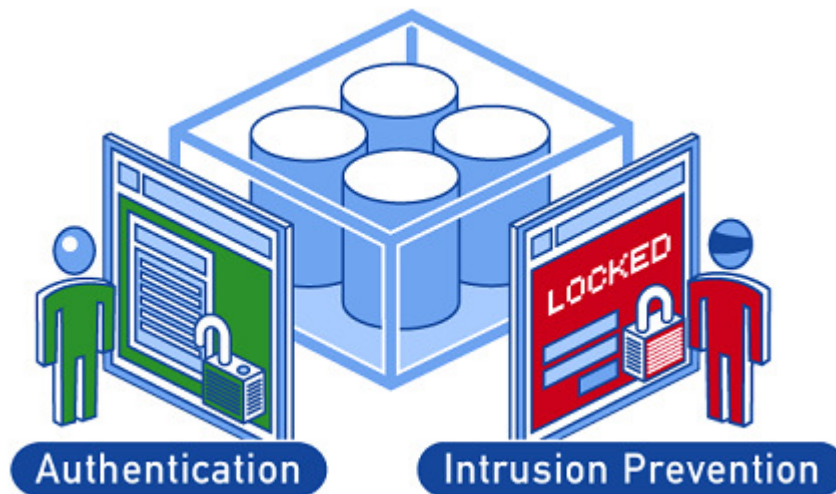
SECURE DOMINO

Authentication & Intrusion Prevention

SecureDomino is the universal authentication and security tool for Domino web servers.

By extending authentication options beyond the Domino Directory, SecureDomino allows a broader usage of Domino servers.

SecureDomino enhances data security and helps to enforce Sarbanes-Oxley compliance. Domino servers with activated HTTP task are protected by preventing unauthorized users from gaining access.



1	Product Overview	2
2	LDAP Authentication	4
3	Designated (SPNEGO) Authentication Server	5
4	Authentication Logging	6
5	IP-based Authentication	7
6	Logon Hours Definition - Time Controlled Login	7
7	Brute-Force and Password Guessing Prevention	8
8	HTTP-Access Limitation & Redirection	13
9	Forgotten Password Handling	14
10	License Fees	15
11	Appendix: TIMETOACT Background Information	16

Web Your
Business >>>

SecureDomino

Authentication & Intrusion Prevention

1 Product Overview

Authentication

Lotus Domino authentication has several shortcomings:

- Even with the Domino Directory Assistance and the Active Directory Synchronization users must still handle multiple passwords.
- Domino does not log authentication successfully and failed attempts efficiently.
- Domino does not support IP-based authentication.
- Domino does not allow the definition of log-on hours

SecureDomino Authentication Features:

- **LDAP Authentication**
Authenticate against Microsoft or any other LDAP directory and thus eliminate the need for users to remember multiple passwords.
- **Designated Authentication Server (new in R7!)**
Authenticate against a central Authentication Gateway that uses SPNEGO to fully automate logins. Minimizes the restriction to Windows and latest Domino Versions on the server side for the effective rollout of SPNEGO in your organization.
- **Authentication Logging**
Log sign-in attempts (either all, successful only or failed attempts only) for analysis, documentation and user-information.
- **IP-based Authentication**
Identify and authenticate users (and proxies) through their IP-address automatically.
- **Log-on Hours Definition**
Restrict signing in, e.g.: restrict log-in to business days and hours from 8am to 5pm.

Intrusion Prevention

Lotus Notes and Domino offer extensive and mature security architecture. Nevertheless, a Domino server in the Intra-, Extra- or Internet is exposed to many risks:

- Browser clients can endlessly attempt to sign in to a Domino Server. Retrieving a user's password is just a matter of time.
- Hackers can access sensitive data or cause a heavy server load by simply using hacking tools provided in the internet (Brute Force Attacks, Denial-of-Service).
- URL's like \$DefaultNav and \$DefaultView often reveal much more information than intended.
- Loading the HTTP-server task makes all databases accessible through browser-clients, not just the desired ones.

SecureDomino

Authentication & Intrusion Prevention

SecureDomino Intrusion Prevention Features:

- [Prevent Brute-Force Hacking and Password Guessing Attempts](#)
Effective protection against hacking and denial of service-attacks through HTTP lockout. IPs and user accounts are locked after a number of failed attempts. Unlock on a scheduled interval or have administrators unlock manually. [Forgotten Password Handling](#)
Users may request new http passwords and have them send to their Notes-mail accounts.
- [Access Restrictions](#)
Restrict http-access with white- and black-lists to directories and databases. Have all other databases accessed through Lotus Notes clients only.
- [Redirection](#)
Create redirections for custom and unwanted URL-commands like \$\$DefaultNav, \$\$DefaultView, %%Source%%. Works even with Unicode characters.

SecureDomino benefits

- is widely tested and implemented by corporations (including IBM) and governments around the world.
- is a DSAPI-filter and can simply be plugged into any Domino server
- can be installed within minutes
- does not does require any modifications to the Domino directory or even a new Domino directory
- does not slow down the Domino server
- does not write into the Domino directory
- even works with strong password encryption
- is available on all relevant Domino platforms (Windows, Linux, AIX, Sun OS, others on request)

Platforms

SecureDomino is available for the following platforms:

- Windows NT/2000/2003
- Linux
- AIX
- Sun Solaris / Risc on request
- iSeries and zSeries on request

SecureDomino R7 requires an IBM Lotus Domino R7 (or higher) server.

SecureDomino

Authentication & Intrusion Prevention

SECURE DOMINO

Authentication & Intrusion Prevention

SecureDomino 7
Release 7.0

Authentication Log

Intrusion Log

Currently Blocked

Archive by Time

Archive by User

Archive by IP

Configuration

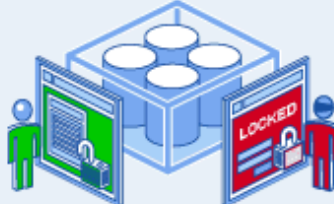
License Keys

Authentication + LDAP

Intrusion Prevention

Access + Redirection

Logon Hours



Protect Your Data!

MOBILE85

Unblock IP / User

Date / Time	Blocked IP/User ^	Username ^
11.03.2010 10:35:00	User Blocked	Linda Moll
11.03.2010 10:32:29	User Blocked	Susi Sorglos
11.03.2010 10:30:35	User Blocked	Emma Ginär
11.03.2010 10:28:34	User Blocked	Polly Ester
11.03.2010 10:08:03	User Blocked	Fritz
11.03.2010 10:05:50	User Blocked	Michael Gollmick/TimeToAct

Screenshot: SecureDomino Administration and Logging Database

2 LDAP Authentication

The LDAP Authentication works with Microsoft Active and other LDAP directories and thus eliminates the need for multiple passwords.

Of course Domino Directory Assistance already supports authentication against the Microsoft Active Directory (MSAD). However, MSAD authenticated users are then known to the Domino servers with their MSAD username, not their Domino username. Access rights will not work, as the MSAD username is generally a single text string and the Domino username is generally a full user name including first name, last name organizational units, organization and sometime even a country code.

SecureDomino

Authentication & Intrusion Prevention

Yes, "ADSync" supports synchronization of the MSAD and the Domino directory. However, companies tend to have strict policies for MSAD password expiration. Users therefore end up, at least temporarily, with several passwords. SecureDomino R7 eliminates the need for multiple passwords. It supports authentication against MSAD or any other LDAP. Any LDAP search string can be used for authentication. SecureDomino then maps the LDAP search string to a Domino username and authenticates the user with their Domino username. Access rights in groups and ACL's still work. And the second a password is updated in MSAD the same password works for Domino authentication as well.

LDAP Authentication

With LDAP authentication user / password may not be found in local Domino directory, i.e. HTTPPassword field must be empty.

<p>LDAP Server: <input type="text" value="DNS1.ACME.ORG"/></p> <p>LDAP Port: <input type="text" value=""/></p> <p>LDAP Options: <input checked="" type="checkbox"/> MS Active Directory <input type="checkbox"/> SSL</p> <p>LDAP Username: <input type="text" value="LDAPUser"/></p> <p>LDAP Password: <input type="password" value="Enter Password"/> 717F60666D6C7E80</p> <p>LDAP Base: <input type="text" value="DC=acme,DC=org"/></p> <p>LDAP Search: <input type="text" value="(sAMAccountName=%s)"/></p> <p>LDAP Field: <input type="text" value="sAMAccountName"/></p> <p>LDAP LookupView: <input type="text" value="(\$Users)"/></p>	<p>Enter the IP or hostname of the LDAP servers, which the Domino server uses to authenticate user. Multiple entries are allowed. The hosts will be tried in the order listed, stopping with the first one to which a successful connection is made.</p> <p>e.g.:</p> <p>dns1.acme.org dns2.acme.org</p> <p>Optional: Enter the LDAP port for the LDAP server above, default is 389 and 636 for SSL.</p> <p>Enter the name of the LDAP user, which the domino server uses to authenticate against the LDAP server. E.g. for Microsoft Active Directory: ACME\LDAPUserName</p> <p>Enter the password of the LDAP user above.</p> <p>e.g.: DC=timetoact,DC=de</p> <p>e.g. for Active Directory: (sAMAccountName=%s)</p> <p>Optional define LDAP attribute to be used for authentication instead of DN. e.g. for Active Directory: sAMAccountName</p> <p>Enter the name of the view, SecureDomino uses for looking up with the LDAP username to the corresponding Domino username. Default is "\$Users".</p>
--	---

Screenshot: Authentication Configuration

3 Designated (SPNEGO) Authentication Server

The Designated Authentication Server allows the redirection of the authentication process to another server. This is especially useful if you want to leverage Integrated Windows Authentication that comes with SPNEGO in Domino 8.5.1, but want to operate your Domino Servers on different Operating Systems than Windows or need to run Domino Servers before Domino R 8.5.1.

If you run your Domino Servers with Gateway Authentication, you may operate only one SPNEGO activated Domino Server in your domain. Once the Designated Authentication Server is activated on servers, unauthenticated HTTP requests are redirected to the central SPNEGO activated Domino server that was configured in the SecureDomino configuration database. The user authentication is performed on that machine. After a successful authentication the user is redirected back to the original server. The original request is issued

SecureDomino

Authentication & Intrusion Prevention

for a second time then. As the user is authenticated at this point, the original server knows the requests user identity and processes the request without challenging the user for a password. As this authentication roundtrip is very fast, the user may not even realize it but enjoys the comfort of being authenticated without a password challenge even after restarting the browser or the machine.

SecureDomino supports the configuration of multiple LTPA-Domains and encrypted connections.

Designated Authentication Server

With a designated authentication server the user may be authenticated via a server that handles the authentication request and redirects back to the original website.

Gateway Hostname:

Gateway Protocol: Normal (HTTP)
 SSL (HTTPS)

Enter the hostname of the gateway server that will handle authentication in your domain e.g.:
 auth.acme.org:

- all involved servers must be configured to use Multiple Server (SSO) session authentication (LTPA-Token)
- all involved servers must be in within the top and second level same domain, that is: .acme.org
- on the gateway server, please use "Domino Authentication"

Screenshot: Designated Authentication Server Configuration

4 Authentication Logging

Authentication logging allows recording of sign-in attempts (either all, successful only or failed attempts only).

- Who is actually using the (expensive) Extranet?
- When has XYZ last signed in?

These questions can easily be answered with SecureDomino R7. Authentication can either be logged to the SecureDomino database or to a separate or custom database.

Date / Time	UserName entered ^	User ^	PW ^	UserName authenticate ^
12.03.2010 12:54:41	EXGVZ	✖	✖	
12.03.2010 12:54:37	EXGVZ	✖	✖	
12.03.2010 12:54:32	EXGVZ	✖	✖	
12.03.2010 12:51:33	Polly Ester	✔	✖	Polly Ester
12.03.2010 12:30:11	susi sorglos	✔	✔	Susi Sorglos
12.03.2010 12:30:02	susi	✖	✖	
12.03.2010 12:28:58	mgo	✔	✔	Michael Gollmick/TimeToAct
12.03.2010 12:24:13	mgo	✔	✖	Michael Gollmick/TimeToAct

Screenshot: Authentication Log within the SecureDomino data base

Computed text message can inform the users about their last successful login, such as: "Hello Michael, Your last successful login was: Jan. 12th 2007 11:46 am."

SecureDomino

Authentication & Intrusion Prevention

5 IP-based Authentication

With SecureDomino users or organizations can be authenticated upon their IP-address without having to enter username and password. This functionality, seamless at first sight, allows using the Domino server in completely new situations. For example:

- Company A and company B have merged. They do not have an private network yet. Company A can therefore use an internet server and authenticate all employees of company B with the IP-address of their firewall. Employees of company B could therefore read the merger-information's without having to authenticate.
- Company X offers to their few but important customers a special information database. The offer would not be accepted, if users had to authenticate manually.
- System X is supposed to read a XML-export from a read-restricted database on a server with session based authentication.

Of course, the IP-based authentication can not be used in highly critical situations. But in many instances, IP-based authentication might be a helpful alternative to manual authentication using username and password.

IP Authentication

Automatic authentication of users through their IP-address without username and password.

```
IP List: 『 213.156.86.34 | Customer A
          134.216.145.73 | Customer B
          196.206.45.* | Partner 』
```

```
Example:
192.168.0.1 | UserName/Organisation
```

Screenshot: IP Authentication Configuration

6 Logon Hours Definition - Time Controlled Login

Do you have an application that users are only supposed to use during certain times? Would you like to stop people from tampering with your applications in the middle of the night? Not a problem with SecureDomino. It allows you create sign-in profiles for individual users. For example certain users are only allowed to sign-in workdays from 8 am to 5 pm?

SecureDomino

Authentication & Intrusion Prevention

Logon Hours / Day - Time Restrictions

Time Controlled Login

<p>Use internal errorpage: <input checked="" type="radio"/> Yes <input type="radio"/> No</p> <p>Errorpage: <input type="text" value="Edit this errorpage"/></p> <p>Redirect URL: <input type="text"/></p> <p>Username: <input]"="" type="text" value="*"/> <input type="button" value="v"/></p> <p>Sign in on Weekdays: <input type="checkbox"/> Sunday <input checked="" type="checkbox"/> Monday <input checked="" type="checkbox"/> Tuesday <input checked="" type="checkbox"/> Wednesday <input checked="" type="checkbox"/> Thursday <input checked="" type="checkbox"/> Friday <input type="checkbox"/> Saturday</p> <p>Monday sign in times: <input type="text" value="08:00"/> to <input type="text" value="18:00"/></p> <p>Tuesday sign in times: <input type="text" value="08:00"/> to <input type="text" value="18:00"/></p> <p>Wednesday sign in times: <input type="text" value="08:00"/> to <input type="text" value="18:00"/></p> <p>Thursday sign in times: <input type="text" value="08:00"/> to <input type="text" value="18:00"/></p> <p>Friday sign in times: <input type="text" value="08:00"/> to <input type="text" value="18:00"/></p>	<p>Select whether you want to use the configurable SecureDomino errorpage, or a custom one.</p> <p>Edit the errorpage, which is presented to the users.</p> <p>Enter the URL for the redirection (e.g. http://WWW... for external addresses)</p> <p>Select the users you want allow to sign in during a specific time period.</p> <p>Select the weekdays.</p> <p>Choose the sign-in times for monday.</p> <p>Choose the sign-in times for tuesday.</p> <p>Choose the sign-in times for wednesday.</p> <p>Choose the sign-in times for thursday.</p> <p>Choose the sign-in times for friday.</p>
---	---

Screenshot: Logon Hours Configuration

7 Brute-Force and Password Guessing Prevention

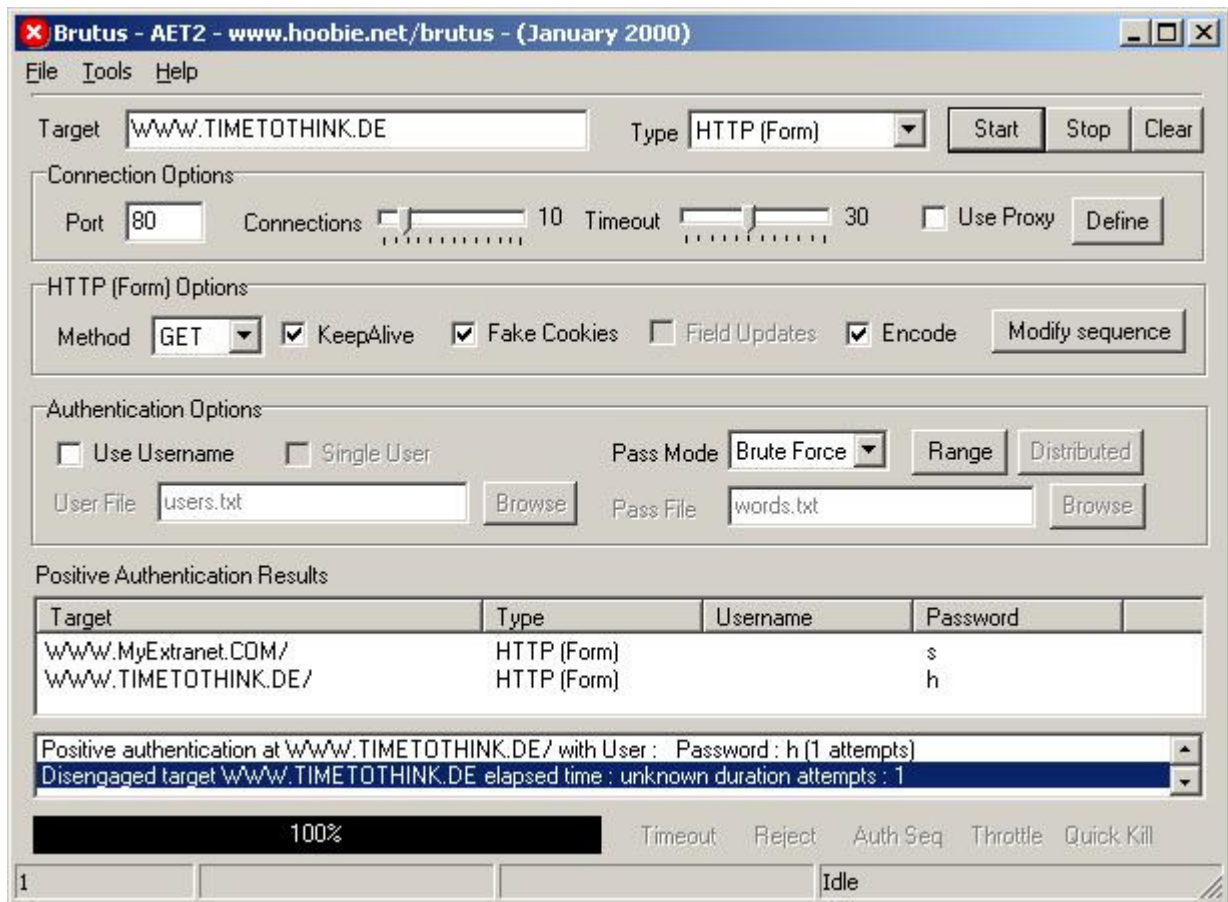
Protecting sensitive data published on the web via username and password authentication is not secure enough. Browser clients and so called "Password Recovery Tools", i.e. brute force tools, can endlessly attempt to log onto a Domino Server. Retrieving a user's password is just a matter of patience, or using brute force programs, just a matter of time. Domino does not offer any protection against brute force attacks whatsoever. HTTPS will not help. The options "more secure passwords" or "less name variations" will not help either.

Brute Force Attacks:

The threat of brute force attacks is very real. There are lots of free allegedly "Password Recovery" tools or tools that help administrators detect security holes. These programs can be used in the internet or in the intranet alike.

SecureDomino

Authentication & Intrusion Prevention



Screenshot: Typical "Passwort Recovery", i.e. Brute Force Tool

From the application description:

"With just a few clicks of the mouse, the program tests the security and robustness of Internet servers, via remote brute-force attack. Designed for the novice to intermediate-level user with little experience in security applications, the program is extremely easy to use. It is also fast and flexible enough for site administrators and security professionals."

<p><i>Features include:</i> <i>Internal word generator with character set selection</i> <i>Supports all major wordlist formats</i> <i>Coordinates attacks across multiple machines</i> <i>Supports HTTP proxy servers</i> <i>Track attack history in easy-to-read logs</i> <i>Automatic save and filtering functions</i> <i>Much, much more!"</i></p>	<p>Excerpts from another feature list <i>"Testing of websites that use basic authentication, html-form based logins or single pass protection schemes (AVS)</i> <i>Running up to 100 bots</i> <i>Proxy- and SOCKS-proxy support and proxy rotation</i> <i>Wordlist support for all wordlist formats</i> <i>advanced and customizable on-the-fly wordlist manipulations</i> <i>Wordlist tools such as duplicates remover, passleecher and list queue</i> <i>Advanced, customizable and fast security test tools</i> <i>Autopilot"</i></p>
--	--

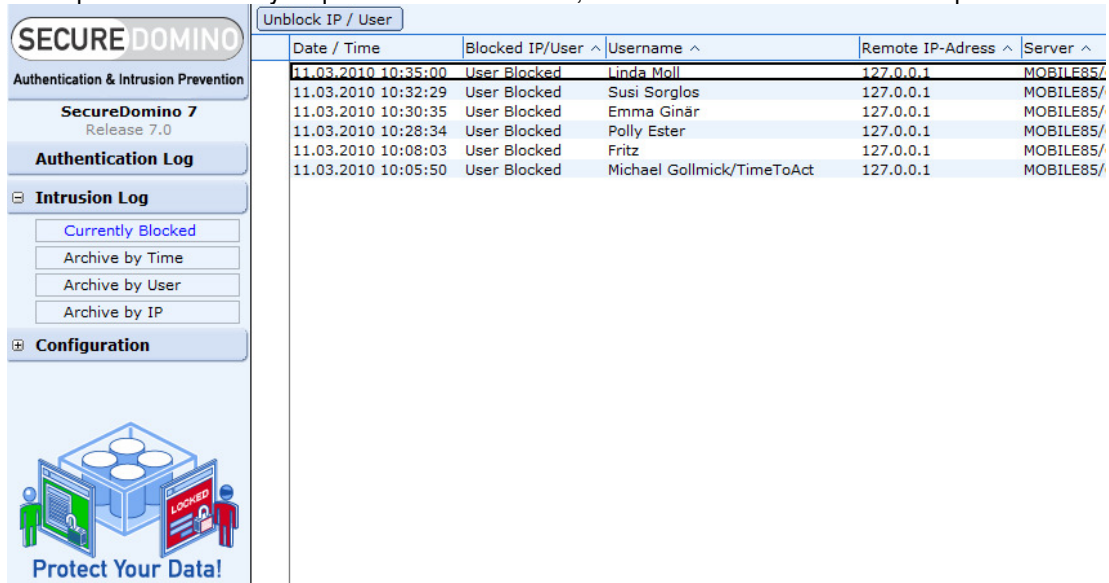
SecureDomino

Authentication & Intrusion Prevention

Intrusion Prevention

SecureDomino supplies an additional security to Domino servers with activated HTTP task through limiting the number of failed login attempts. After the defined number of unsuccessful login attempts, SecureDomino blocks the hacker's IP-address and / or the user name and logs that information in a data base. SecureDomino then informs the administrator about the hack attempt. SecureDomino works even with strong http-password encryption and LDAP-directories. An automatic logout can also be provided for basic authentication.

With SecureDomino, Domino servers can be utilized in environments that would be either to risky without additional protection or may require X509 certificates, intensive administration and expensive add-ons.



Date / Time	Blocked IP/User	Username	Remote IP-Address	Server
11.03.2010 10:35:00	User Blocked	Linda Moll	127.0.0.1	MOBILE85/
11.03.2010 10:32:29	User Blocked	Susi Sorglos	127.0.0.1	MOBILE85/
11.03.2010 10:30:35	User Blocked	Emma Ginär	127.0.0.1	MOBILE85/
11.03.2010 10:28:34	User Blocked	Polly Ester	127.0.0.1	MOBILE85/
11.03.2010 10:08:03	User Blocked	Fritz	127.0.0.1	MOBILE85/
11.03.2010 10:05:50	User Blocked	Michael Gollmick/TimeToAct	127.0.0.1	MOBILE85/

Intrusion Log

SecureDomino Configuration:

Configuration is done easily with a database, where you can define:

- the databases or directories to be monitored,
- the amount of unsuccessful login attempts per account,
- the amount of unsuccessful login attempts per ip-address,
- the automatic unblocking time
- the error page viewed by a blocked user,
- the names of the administrators to be informed

SecureDomino

Authentication & Intrusion Prevention

Intrusion Prevention Configuration (IP/User Blocking)

General configuration

Servernames: (* - includes all servers)

Blocking

Block options: Choose your desired blocking options.

Notice: If the Domino server is 'behind' a reverse proxy, i.e. if all requests to the Domino server are from the same IP-address, IP-address blocking should be disabled.

User information: Display errorpage Display an errorpage if a user or an IP is blocked.

IP based blocking

Login attempts: Enter the number for the maximum of false login attempts from one IP-address.

Use internal error page: Yes No Select whether you want to use the SecureDomino errorpage or a custom one.

Error page: Edit the errorpage, which is presented to the users, for IP based blocking.

User based blocking

Login attempts user-account: We recommend ≥ 3 . Sometimes IE submits one authentication request twice.

Use internal error page: Yes No Select whether you want to use the SecureDomino errorpage, or a custom one.

Errorpage for blocked users: Edit the errorpage, which is presented to the user, for user based blocking.

Unblocking

Unblock blocked users after: Minutes If this field is empty users will not be unblocked automatically.

Unblock blocked IPs after: Minutes If this field is empty IP-addresses will not be unblocked automatically.

Mail Information

Messages: Send Memo Send an email when a user or IP is blocked.

To: Choose the recipients for the email.

Subject: Enter the subject for the email.

Content: Type a short and informative text.

User: {~UserName~}
IP-Address: {~RemoteAddr~}

Password request

Allow password request: Yes No Allow users to request a new password.

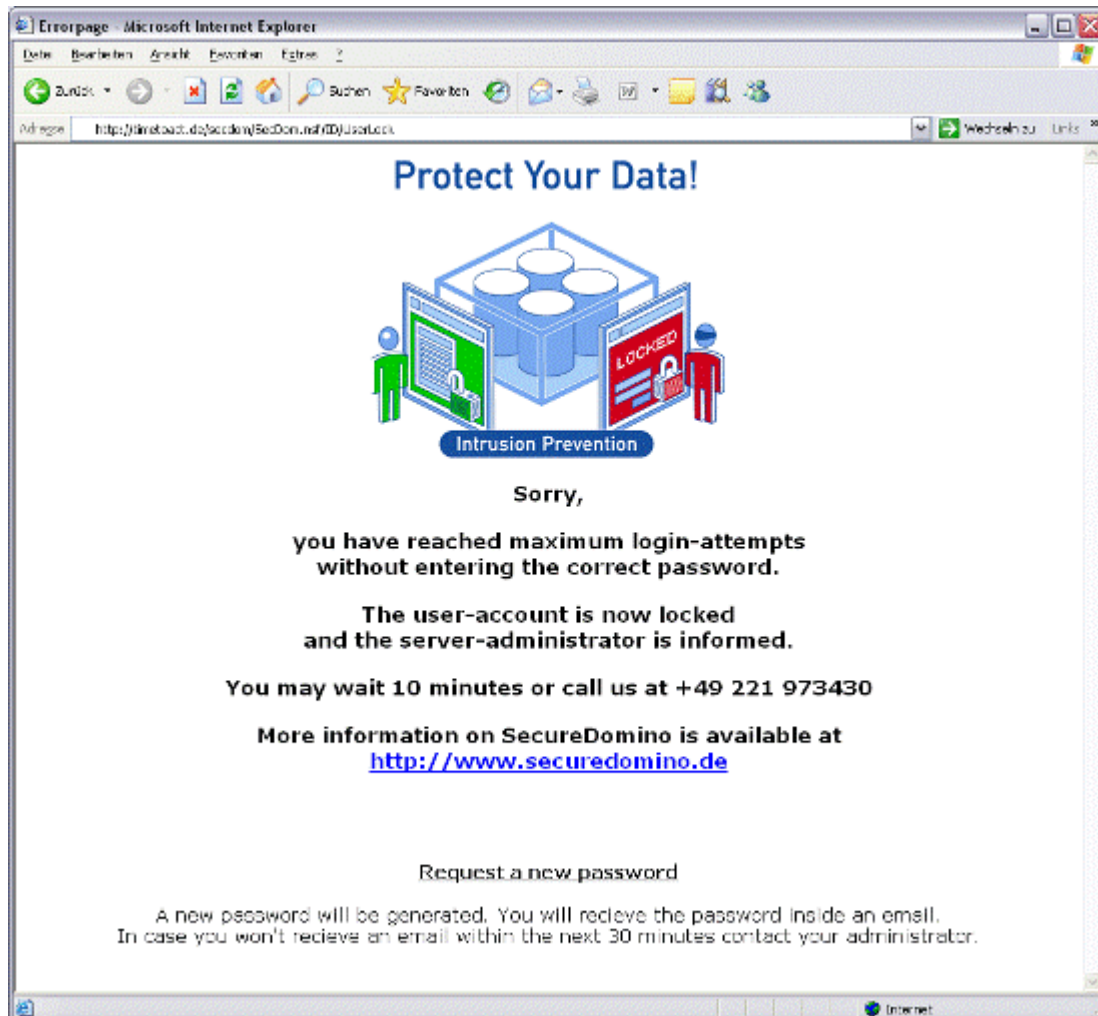
Screenshot: Intrusion Prevention Configuration

SecureDomino

Authentication & Intrusion Prevention

Error page

Once the defined threshold of failed login attempts has been reached, an error page can be displayed informing the user that the user / the IP-address has been blocked. Of course the page can be customized and may e.g. contain advice to call helpdesk.



Screenshot: Informing user about his locked account

Password Reset

Optionally, the [page can contain a link to request a new password](#). The new password could be retrieved by the user through Lotus Notes or a Blackberry and subsequently be used to authenticate without having to bother the IT support.

Denial-of-service attacks

A Domino server can be heavily loaded through a brute force attack, the response time quickly rises to several minutes. With SecureDomino, attackers will be logged out, and Domino servers will perform normally. SecureDomino can be configured to unblock the IP -address and / or the username after a predefined time.

SecureDomino

Authentication & Intrusion Prevention

8 HTTP-Access Limitation & Redirection

Administrators often do not like to mix Notes and browser access to one Domino server. Either they have not tested all Notes databases with browser access or they do not want the extra load on a server. Domino Servers are therefore often dedicated to either Notes or browser access. But especially in small locations, separating Notes from browser access mean higher costs: double hardware, software and maintenance are required.

Use Domino servers a better way: Notes- and browser-clients on one server. With SecureDomino, administrators can expose only specific databases or directories to http access. Administrators can therefore allow browser access only to specific applications and not to the mail files or only to the mail files and not to the applications.

Black and White Lists

HTTP-access to internet servers can be limited to the databases that make up the website (white list). HTTP-access to all other databases, like the Domino directory or the databases catalog can be prohibited (black list). That also may act as an additional protection in case of incorrect set up ACL.

Redirection

HTTP DB / Directory Access & Access Deny List

Servername: <input type="text" value="*"/>	(* - includes all servers)
Access list: <input type="text" value="Mail*"/> <input type="text" value="WWW*"/>	Enter the database and directories which are allowed to be accessed via HTTP. Examples given: * - includes all databases Icons HTML Apps* Mail* c1256aa3004320b8*
No access list: <input type="text" value="Catalog.nsf"/> <input type="text" value="CRM*"/>	Enter the database and directories which are <u>not</u> allowed to be accessed via HTTP. Examples given: adminp.nsf catalog.nsf *XYZ.nsf Note: Session based authentication requires access to the names.nsf !!

Redirection

Target: <input checked="" type="radio"/> Errorpage <input type="radio"/> URL	Select the redirection target
Errorpage: <input type="button" value="Edit errorpage"/>	Edit the errorpage, the user is redirected to.

Screenshot: HTTP Access and Redirection Configuration

Preventing smart force attacks

Domino based websites often offer more information than intended by the administrators. Inaccurate developed Domino-based applications may allow hackers to easily retrieve confidential information like personal data or database configuration settings. SecureDomino protects the entire server against spying out.

For example: The URL command \$DefaultNav will open a database with a default navigator that displays all available views and folders. Even views designed for Notes administrators or for the content- or webmaster will be displayed, unless the Domino-designer explicitly hides all views from web browser. But who is perfect? Other critical URL commands include \$DefaultView, \$DefaultForm and ?ReadViewEntries. After the hacker has retrieved the names and addresses of the domino objects, he might even try to tamper the database with other URL commands like "?DeleteDocument" or "?SaveForm".

SecureDomino

Authentication & Intrusion Prevention

URL-Filtering / Redirection

With SecureDomino you can block these specific commands. Hackers trying an illegal URL will be forwarded to a specific page or to any other URL. SecureDomino can not be cheated with coding the URL commands in Unicode and is therefore much safer than entering a simple redirection mapping in the Domino directory. Prove it: [/Names.nsf/\\$DefaultNav?open](#)

SecureDomino additionally allows custom redirections. A very helpful feature in database-development or after a migration of a static website to a Domino-based one.

Redirection Mapping

The URLs "DefaultNav", "DefaultForm" and "DefaultView" might reveal more information from databases than desired. Filtering these URLs is not likely to have any side-effects.

The URL "ReadViewEntries" reveals the document unique ID of documents, which might be used to read documents even when not intended by the database designer. When the URL "ReadViewEntries" is filtered, views with Java-Applets will not work.

The URL "DeleteDocument" is used to delete documents. The ACL-setting "Delete documents" is global and can not be restricted to specific documents. Filtering this URL can be used to prohibited document deletion with URLs without having to disable document deletion altogether.

The URL "SecureDominoRedirectionTest" can be used the test redirection functionality, even if SecureDomino runs in Demonstration-mode.

Filtered URLs:	<input checked="" type="checkbox"/> *DefaultForm*	Select the URLs you want to be filtered.
	<input checked="" type="checkbox"/> *DefaultNav*	
	<input checked="" type="checkbox"/> *DefaultView*	
	<input checked="" type="checkbox"/> *DeleteDocument*	
	<input checked="" type="checkbox"/> *OpenAbout*	
	<input checked="" type="checkbox"/> *OpenHelp*	
	<input checked="" type="checkbox"/> *OpenIcon*	
	<input type="checkbox"/> *ReadDesign*	
	<input type="checkbox"/> *ReadEntries*	
	<input type="checkbox"/> *ReadViewEntries*	
	<input type="checkbox"/> *SecureDominoRedirectionTest*	
	<input checked="" type="checkbox"/> *%%object%%*	
	<input checked="" type="checkbox"/> *%%source%%*	

Note:

- iNotes requires "ReadViewEntries"
- Quickplace requires "\$DefaultView"

Custom URL Redirection Mapping: The custom URL redirection can be used to redirect any URL to any other URL. E.g.: A static HTML website has been migrated to a Domino database. Map all static HTML directories to the database, so that old bookmarks / search engines will not result in a "404 File not found" error.

Screenshot: URL commands Redirection Configuration

9 Forgotten Password Handling

SecureDomino creates new random http-passwords for blocked users. The new password is mailed to the user's Notes mail accounts. Thus users can retrieve their new http-password using their Notes client without having to bother system administration.

Password request

Allow password request: Yes No

Allow users to request a new password.

Mail Settings

Default Recipients:

This email address will be supplemented in the standard recipients field.

Default Subject:

This subject will be used, if no other subject is specified.

Message Body:

This is the message body. Use the following substitution to insert dynamic values.

{0} Username
{1} New password
{2} Current date

Screenshot: Password Request Configuration

SecureDomino

Authentication & Intrusion Prevention

10 License Fees

SecureDomino is available on a 'per server' basis (with volume discount) and under a company license.

License Cost including 1. Year Software Maintenance		Authentication Features	Intrusion Prevention Features	Authentication Features and Intrusion Prevention Features
1st Server	=	3.125,00 €	3.125,00 €	5.000,00 €
2nd Server - 25%	=	2.343,75 €	2.343,75 €	3.750,00 €
3rd Server - 40%	=	1.875,00 €	1.875,00 €	3.000,00 €
4th Server - 50%	=	1.562,50 €	1.562,50 €	2.500,00 €
5th Server - 50%	=	1.562,50 €	1.562,50 €	2.500,00 €
company license	=	12.500,00 €	12.500,00 €	20.000,00 €

License conditions:

- Software maintenance cost for the consecutive years is 24% of the license cost.
- The company license is limited to one Notes organization.
- Volume discount applies only for purchases within three months.
- Software Reinstatement costs 65% of the license cost.
- All prices exclude value added tax.

For orders please contact:

TIMETOACT Software & Consulting GmbH
Im Mediapark 2
50670 Cologne
Germany

Tel.: +49 221 97343 0
Tel.: +49 700 TIMETOACT
Fax: +49 221 97343 20
Sales: <mailto:sales@TIMETOACT.DE>

SecureDomino

Authentication & Intrusion Prevention

11 Appendix: TIMETOACT Background Information

TIMETOACT is specialized in consulting and development on the basis of IBM Lotus and WebSphere software, Eclipse rich client platform and open standards. Key aspects of activity are web content management, portals, application- and system-architecture. TIMETOACT develops out-of-the-box products as well as customized solutions for the intra-, extra- and internet.

Content Management
Collaboration & Commerce >>>

Web Your Business !

TIMETOWEB
Web Content Management

Employee Pages
Corporate Transparency >>>

Map Your Company !

TIMETONET
Consulting & Solutions

Consulting
Development & Solutions >>>

Web Your Business
>>>

TIMETOACT
Software & Consulting GmbH

Authentication & Intrusion Prevention >>>

Protect Your Data !

SECUREDOMINO
Authentication & Intrusion Prevention

Authorized IBM Training Partner >>>

Extend Your Skills !

Authorized **IBM** Training

IBM **Lotus** software
IBM **WebSphere** software