



The DiscoveryGate® content platform *Security, privacy and confidentiality*

*DiscoveryGate protects
your information.*

The DiscoveryGate® content platform from Elsevier MDL integrates, indexes and links information underlying scientific discovery to give immediate access to compounds and related data, reactions, original journal articles, patents and authoritative reference works on synthetic methodologies, pharmacology and drug safety.

Elsevier MDL recognizes the critical importance of the security and integrity of information that transits the DiscoveryGate system. Elsevier MDL manages DiscoveryGate data transmission using industry-standard security systems, strict user password rules and encryption technology. Systems are maintained in a secure site location to ensure around-the-clock protection.

Committed to protecting your data

This paper describes the security measures implemented in the DiscoveryGate system.

- All DiscoveryGate client-server traffic is encrypted using SSL technology
- All results are securely returned to the client browser

Actions logged by DiscoveryGate that help ensure security or assist in customer support include:

- Successful login
- Unsuccessful login
- Change of user password
- Permission retrieval
- Promotion signup
- Promotion use

The technologies, methodologies and protocols that enable DiscoveryGate security are described below.

How DiscoveryGate security is implemented

Forced password protection

When users are created or imported through the DiscoveryGate administration interface, passwords are machine-generated and not created by the administrator. The administrator must identify the email address of the user, and the machine-generated password is emailed to the user. Before entering DiscoveryGate, the user is forced to change the password according to the following rules:

- Password must meet a minimum length criterion
- Password must contain a minimum number of non-letter (number or symbol) characters
- Password must not match any of several easily guessed values related to the user's personal information

Declarative security

To provide secure access and authorization control for DiscoveryGate, Elsevier MDL uses declarative security as defined within the Servlet 2.2 specification from the Java Community Process. The use of declarative security prevents any user from accessing the application without first having specified a valid username/password and "permissions" for the Web resource.



Elsevier MDL

2440 Camino Ramon, Suite 300
San Ramon, CA 94583
Phone: +1 (925) 543-5400
Fax: +1 (925) 543-5401

About Elsevier MDL

Elsevier MDL provides informatics, database and workflow solutions that accelerate successful life sciences R&D by improving the speed and quality of scientists' decision making. Academic and industrial life sciences researchers around the world depend on Elsevier MDL for innovative and reliable discovery informatics software solutions augmented by 400 Elsevier chemistry and life sciences journals and related products. For more information, visit www.mdl.com.

Elsevier is a world-leading publisher of scientific, technical and medical information products and services. Working in partnership with the global science and health communities, Elsevier publishes more than 2,000 journals and 1,900 new books per year, in addition to offering a suite of innovative electronic products and online reference works. For more information, visit www.elsevier.com.

MDL and DiscoveryGate are registered trademarks of MDL Information Systems, Inc. ('Elsevier MDL') in the United States and/or other countries. Equifax is a registered trademark of Equifax, Inc. Java and all Java-related marks are trademarks or registered trademarks of Sun Microsystems, Inc. Oracle is a registered trademark of the Oracle Corporation in the United States and other countries. All other product and company names mentioned herein may be trademarks or registered trademarks of their respective holders.

© Copyright 2006 Elsevier MDL.
All rights reserved.
PPWP/11-06/500

Based on this specification, the servlet runner is responsible for ensuring that the user has the correct credentials to access the application. When the user tries to access a secure resource, the servlet container intercepts the request and displays a login page. The user enters the username and password into the login page. If the username and password are those of a user who has a role that is allowed to access the application, the resource is displayed. Only users with the correct role can access the application; all others are blocked at the servlet container level.

Password Encryption

DiscoveryGate uses coding based on state of the art algorithms for encryption of passwords. User passwords are not stored directly in the authentication database; instead we hold a digest value calculated from the password plus an undisclosed salt value. The digest method is thought to be irreversible. The login process calculates the equivalent digest from the submitted password and allows authentication only if the two match. The password submitted during login is immediately discarded.

Secure Sockets Layer (SSL) protocol

All data exchanged between DiscoveryGate and a DiscoveryGate user are enciphered and transmitted via SSL. The SSL protocol is an industry-standard method for protecting Web communications and ensuring secure client/server communications. Using the SSL protocol, an SSL-enabled server can authenticate itself to an SSL-enabled client and the client can authenticate itself to the server, thereby establishing an encrypted connection between both machines. This encrypted connection provides "channel security," which has three basic properties:

- **The channel is private:** encryption is used for all messages after a simple handshake defines a secret key. The initial key exchange is protected by Public Key Encryption.
- **The channel is authenticated:** the server endpoint of the conversation is always authenticated.

- **The channel is reliable:** the message transport includes a message integrity check.

An SSL connection provides a high degree of confidentiality by requiring that all information sent between a client and a server is encrypted by the sending software and decrypted by the receiving software. Any tampering with data sent over an encrypted SSL connection is automatically detected by a mechanism that determines whether the data have been altered in transit.

SSL connections for DiscoveryGate are managed by Elsevier MDL. SSL encryption is validated by the certificating authority Equifax, Inc. Equifax issues a digital certificate, or electronic credential, confirming that Elsevier MDL is the owner of the DiscoveryGate client connections and enabling secure communications between client and server. For more information on Equifax digital certificates, refer to: http://www.equifax.com/DigitalCertificates/dc_index.html.

Industry-standard measures supporting the security, privacy and confidentiality of customer information transiting the DiscoveryGate system include machine-generated passwords, state-of-the-art password encryption technology, strict permissions implemented at the servlet container level and secure communications utilizing the SSL protocol.

Elsevier MDL is committed to maintaining the confidence and trust of customers with respect to the information collected from them. Refer to the Elsevier MDL corporate privacy policy at www.discoverygate.com (Privacy) for a description of the information collected about customers, how this information is used and the choices customers have about how this information is used.