



Security Notes

Copyright © 2005–2007 by Inmagic, Inc. All rights reserved.

Inmagic[®], the Inmagic logo, DB/Text[®], DB/TextWorks[®], BiblioTech[®], and BiblioTech PRO[®] are registered trademarks; and Inmagic.net[™], BibSpeed[™], IntelliMagic[™], and PowerPack[™] are trademarks of Inmagic, Inc.

Other brand and product names are trademarks or registered trademarks of their respective holders. Use of any other product name does not imply endorsement of that product by Inmagic, Inc.

The information in this document is subject to change without notice and should not be construed as a commitment by Inmagic, Inc., which assumes no responsibility for any errors that may appear in this document.

WARRANTY

INMAGIC, INC. MAKES NO WARRANTY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY AND FITNESS. INMAGIC, INC. SHALL NOT BE LIABLE FOR ANY LOST PROFITS OR ANY OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. IN PARTICULAR, INMAGIC, INC. SHALL HAVE NO LIABILITY FOR ANY DATA OR PROGRAMS STORED OR USED WITH THIS PRODUCT, INCLUDING THE COSTS OF RECOVERING SUCH PROGRAMS OR DATA.

U.S. GOVERNMENT: If Licensee is acquiring the software on behalf of any unit or agency of the U.S. Government, the following shall apply:

(a) For units of the Department of Defense: RESTRICTED RIGHTS LEGEND: Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data Clause at DFARS 252.227-7013. (b) For any other unit or agency: NOTICE - Notwithstanding any other lease or license agreement that may pertain to, or accompanying the delivery of, the computer software and accompanying documentation, the rights of the Government regarding its use, reproduction and disclosure are as set forth in Clause 52.227-19(c)(2) of the FAR.

Contractor/Manufacturer is Inmagic, Inc., 200 Unicorn Park Drive, Fourth Floor, Woburn, MA 01801, U.S.A.

Inmagic, Inc.
200 Unicorn Park Drive
Fourth Floor
Woburn, MA 01801 U.S.A.
Telephone: 781-938-4444 or 800-229-8398
Fax: 781-938-4446
<http://www.inmagic.com>

Contents

- Inmagic® Genie Security Notes..... 1**
 - Contacting Inmagic and Communicating with Other Users..... 1
 - Communicating with Other Users 1
- Security Models..... 2**
- GENIEKEY Textbase 3**
- Roles 4**
- Users 5**
 - Login/password examples..... 5
- Groups 6**
 - User login with groups..... 6
- End Users and Groups 7**
- Bypassing the Login Page 8**

Inmagic® *Genie* Security Notes

This document is intended for the Administrator of the *Genie* application. This document discusses security models and ways you may want to consider to set up security for the application. This document discusses the GENIEKEY textbase and tells you how security works in the application. It also tells you how you can manage roles, groups, and users who are members of the library staff. It also talks about security and end users. This document also tells you how you can bypass the login page for Windows users.

Note: Consider removing this document (InmagicGenieSecurityNotes.PDF) from the Documentation subfolder (which is where it is placed during the installation process) if you do not want others with access to that subfolder to be able to read it.

To administer security for the *Genie* application, use the Manage Security & Logins function (choose **Other>Manage Security & Logins**). Instructions for this function are provided on the graphical user interface (GUI) for it.

Contacting Inmagic and Communicating with Other Users

For help, you can contact Inmagic, Inc. or your local Inmagic dealer. You can also communicate with other Inmagic users.

If you have a maintenance agreement, please have your customer ID ready, and try to be at your computer when you call. If that is not possible, note exactly what you were doing when you encountered the problem, the exact text of any error messages you received, and your software version numbers and serial numbers. (For the *Genie* serial number, click the **About Genie** link on the *Genie* navigation bar. For the *Content Server* serial number, open CS/TextWorks and choose **Help>About CS/TextWorks**.) If you do not have a maintenance agreement, you can contact Inmagic Customer Service to purchase one.

Inmagic, Inc.

200 Unicorn Park Drive, Fourth Floor
Woburn, MA 01801
U.S.A.
Tel: 781-938-4444 or 800-229-8398
Fax: 781-938-4446
<http://www.inmagic.com>

support@inmagic.com	- technical support questions
CustomerSvc@inmagic.com	- general company, product, and services questions
sales@inmagic.com	- sales, product pricing, and custom solution questions
wishlist@inmagic.com	- feature requests

If your message is intended for a particular person at Inmagic, Inc. (for example, a Technical Support representative who is expecting the message or files), please include the name of that person in the subject and in the message.

Communicating with Other Users

You can participate in user-to-user discussions through an Inmagic forum on the Web. Note that the forums are not an official customer or technical support channel for Inmagic products. To participate in a forum, go to the Inmagic Customer Extranet at <http://support.inmagic.com/downloads/extranet.html>.

Security Models

The *Genie* security features were designed to fit a range of security requirements an organization might have. The following lists the basic ways in which you can set up *Genie* security:

- **Role login.** This is the simplest model, and matches the security available in previous versions of the application. A login name and password are set for at least one and at most three permission levels. A login name and password are required for the Administrators role. They are optional for the Catalogers and Staff roles, as some libraries do not need to differentiate between levels of access granted to library staff. With this model, no Users or Groups are set up, and passwords are clearly visible on the Login Search Results page (which can only be accessed by someone with the Administrators role).
- **User login.** User login names are entered by the Administrator, who also associates each user with a Role. Users create their own passwords the first time they log in to the *Genie* application. Passwords are encrypted in the GENIEKEY textbase and appear as asterisks on the Login Search Results page. Use this model if you want to be able to separate the login credentials from the access permissions granted to a particular user. If a user leaves the company, for example, that user can be removed from the textbase and there is no need to change passwords to protect access to the application.
- **User login with Constraints.** This model was designed to meet the security requirements of some multi-branch libraries. A third type of record called a Group is created, associated with a Constraint and a Role. Users are then assigned to groups instead of roles. The constraints can limit a user's access to the titles located in a specific branch. Constraints can also be implemented to limit access to other subsets of the entire collection, such as documents belonging to a specific department. Note that "user" here can refer to library staff as well as end users. Constraints are always enforced; a user with a constraint will never see noncompliant titles in the catalog. (For an alternative to a constraint, see the "Adding a Location Drop-down List to the Catalog and OPAC Search Pages" topic in the MyGenie.CONFIG File section of the *Inmagic Genie Technical Notes*.)
- **Bypassing the login screen.** This model is closest to User login (with or without constraints), except that the user's Windows credentials are checked against the GENIEKEY textbase, and if found, used to bypass the login screen.

GENIEKEY Textbase

Genie security is supported through the GENIEKEY textbase. This textbase supports all of the security models described on page 1. We strongly recommend that you assign a master password to this textbase at your earliest convenience. Do the following:

- **Assign a password to the textbase.** This prevents Windows users from opening the textbase. To assign a password to a textbase, you must use Inmagic® CS/TextWorks. For instructions on how to assign a password, look up the “Master Password” topic in the CS/TextWorks online help.
- **Include the same password in the applicable section of the Web.CONFIG file.** Doing this means that the *Genie* application can use it to open the textbase. Every user logging in to the application is checked against the records in this textbase, so the Administrator cannot use directory permissions or SQL Server permissions to block people from opening the GENIEKEY textbase. Include the password you assigned to the textbase in the following section of the Web.CONFIG file (which is located in the main *Genie* installation folder; for example, C:\Program Files\Inmagic\Genie), in the `value` attribute.

```
<!-- GenieKey password -->
<add key="GenieKeyAccess" value="" />
```

For example, if you assign a password of `baseball` to the textbase, this section of the Web.CONFIG file would look like this:

```
<!-- GenieKey password -->
<add key="GenieKeyAccess" value="baseball" />
```

Roles

Genie security, at the most basic level, is role-based. The following roles control access to specific *Genie* functions:

- The **Public** role can search and see Catalog records; may be able to see information about items, loans, and/or reserves if support for this has been set up; cannot edit anything or search any other textbases; and, by default, does not have to log in.
- The **Staff** role can search all textbases; can add and edit records in any textbase except CATALOG, ITEMS, or ORDERS; and cannot delete records.
- The **Catalogers** role has all of the capabilities of the Staff role with the added ability to add and edit Catalog, Item, and Order records; delete records in any textbase; and set up e-mail information.
- The **Administrators** role has all of the capabilities of the Catalogers role with the added ability to set up security, logins, and passwords.

These roles are available out-of-the-box. Access to them is controlled by the login/password combinations for each role, which are entered on the login page; except for the Public role, which by default bypasses the login page. If you prefer to have users log in as themselves, see “End Users and Groups” on page 7.

Out of the box, these are the role/login/password combinations. For a role login, each individual logging in to the application has to log in with one of these login/password combinations.

Role	Login	Password
Staff	Staff	staff
Catalogers	Cataloger	cataloger
Administrators	Admin	admin

We strongly recommend that you change the passwords at your earliest convenience. Alternatively, if you prefer one of the other security models listed on page 1, remove the login names and passwords for the roles. For example, to change the password for the Administrators role:

1. Choose **Other>Manage Security & Logins**.
2. Select the role option button, then click the **Submit Query** button.
3. Click the **Edit** link for the Administrators role.
4. Change the password, then click the **Update** link.

Note: The privileges associated with these roles cannot be changed, the role names cannot be changed, and additional roles cannot be created. However, the Administrator (the person with the Administrators role) can change the login name and password associated with each role (except the Public role).

Users

Optionally, you can set up user logins. Users, in this case, are members of the library staff. In this model, users have individual login names and passwords, and each user must be assigned to one of the roles listed on page 4.

Note that the Administrator cannot specify or see the password for users. After you add a new user record, the password for that user is empty. At the initial login, the user will have to provide and confirm a password of his or her choosing at that time. The application will capture the password and store it, encrypted (appears as ****), with the corresponding entry in the GENIEKEY textbase.

Once you have set up user logins, users will have to use their login/password combination to access the *Genie* application.

If a user forgets his or her password, the Administrator can reset the password by clicking the **Clear** link in the **Password** box for that user record. When the user next accesses the *Genie* application, he or she can provide and confirm another password at that time.

Login/password examples

In this example, the Administrators, Catalogers, and Staff roles do not have login names assigned, thereby disabling role login. The following are examples of login/password/role combinations assigned to four users. Notice that user Mary has not yet logged in and set her password.

Login	Password	Role
joan	****	Administrator
fred	****	Catalogers
mary		Catalogers
beth	****	Staff

For example, to add new user Ken:

1. Choose **Other>Manage Security & Logins**.
2. Select the **user** option button, then click the **Submit Query** button.
3. Click the **Add** button.
4. Enter a user name and select a role, then click the **Update** link.

Groups

Groups are also optional. Groups provide a way to implement query constraints, which are hidden search criteria added to every query into the CATALOG textbase. An example of such a constraint would be to limit the records retrieved to those located in a particular branch of the library.

If the Administrator implements groups for the *Genie* application, each group has a unique name, a query constraint, and an assigned role. You then assign users to groups rather than roles.

User login with groups

In this example, the Administrators, Catalogers, and Staff roles do not have login names assigned, thereby disabling role login.

When entering a constraint, use this format: TextbaseName, Boolean, Field, SearchArgument, as shown in the table below. Note that only one constraint is permitted in this release, which may only be applied to the CATALOG textbase.

These are examples of groups:

Group	Constraint	Role
WoburnCat	Catalog, AND, CatLocation, =Woburn	Catalogers
WoburnStaff	Catalog, AND, CatLocation, =Woburn	Staff
StonehamCat	Catalog, AND, CatLocation, =Stoneham	Catalogers

These are examples of users assigned to groups:

Login	Password	Role OR Group
joan	****	Administrators role
fred	****	WoburnCat group
mary		StonehamCat group
beth	****	WoburnStaff group

For example, to add group BostonCat:

1. Choose **Other>Manage Security & Logins**.
2. Select the **group** option button, then click the **Submit Query** button.
3. Click the **Add** button.
4. Enter a group name and a query constraint, select a role from the drop-down list, then click the **Update** link.

End Users and Groups

The discussion and examples above cover login options for members of the library staff. End users, by default, can search your catalog without having to log in (they bypass the login page). The MyGenie.CONFIG file (which is located in the ConfigFiles subfolder of the main *Genie* installation folder; for example, C:\Program Files\Inmagic\Genie\ConfigFiles) lists the pages that can be accessed without login, such as Opac.ASPX.

If your organization wants to implement query constraints for end users, follow these steps. This means that end users will no longer bypass the login page.

1. Choose **Other>Manage Security & Logins**.
2. Add a group with a query constraint and assign the group to the Public role.
3. Add user records and assign them to that group.
4. Remove the list of pages accessible without login.

For example:

1. In the MyGenie.CONFIG file, comment out (as shown in the following example) or delete the elements between the <OpacPages> </OpacPages> elements.

```
<OpacPages>
  <! -- <OpacPage>opac.aspx</OpacPage> -->
  <! -- <OpacPage>opac_report.aspx</OpacPage> -->
</OpacPages>
```

2. Create groups, as shown in the following example:

Group	Constraint	Role
WoburnPublic	Catalog, AND, CatLocation, =Woburn	Public
StonehamPublic	Catalog, AND, CatLocation, =Stoneham	Public

3. Create users, as shown in the following example:

Login	Password	Group
joe		WoburnPublic
jane		StonehamPublic

Bypassing the Login Page

If you selected the Windows Authentication option during the installation of the *Genie* application, you can bypass the login page for Windows users. If you did not, there are some changes you will need to make in the Web.CONFIG file in your *Genie* installation folder, as well as corresponding changes to make using IIS. They are described in “To set up the *Genie* application to bypass the login” below.

To access the *Genie* application without having to log in, library staff will need their Windows login names entered in the GENIEKEY textbase, but no passwords are required or requested. Their login names then need to be assigned to a role or group.

End users who access the OPAC pages in the *Genie* application do not need to be in the GENIEKEY textbase unless you want them to have query constraints applied when they search. In that case, they do need to be in the textbase, assigned to a group with the appropriate constraint and the role of “Public.”

A user accessing the *Genie* application, who is not present in the GENIEKEY textbase or who does not have Windows credentials, is redirected to the *Genie* login page, where he or she must enter a user name and password present in the textbase.

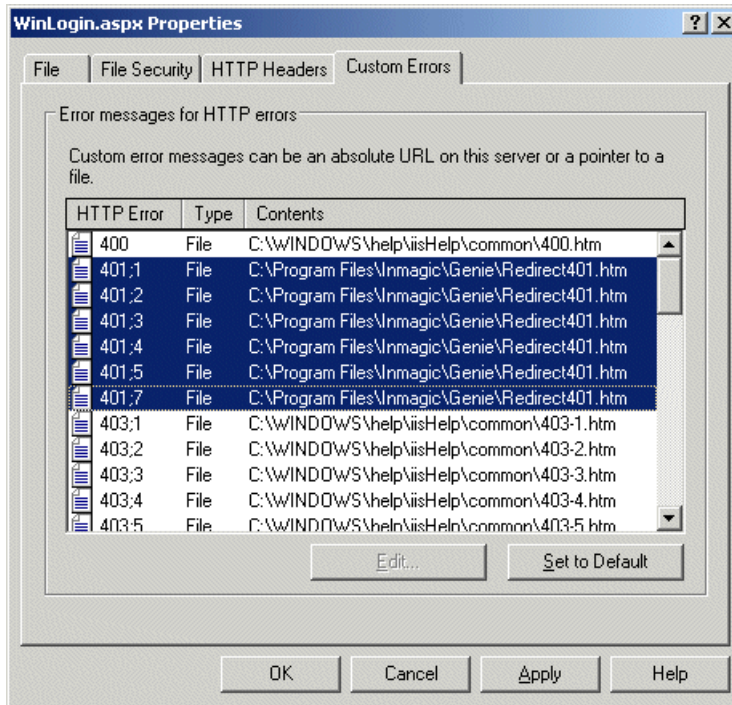
To set up the *Genie* application to bypass the login page

1. Open the Web.CONFIG file located in the main *Genie* installation folder.
2. Find the following line: `<add key="Genie eAuth" value="Anonymous" />`
and change the `value` attribute to `value="Windows"`.
3. Find the following line:

```
<forms name="Genie eAuth" path="/" loginUrl="Login.aspx" protection="All"
    timeout="600">
```


and change the `loginUrl` attribute to `loginUrl="WinLogin.aspx"`.
4. Configure IIS Windows security with the IIS Manager:
 - a. Navigate to and right-click the InmagicGenie Web site and select **Properties** from the shortcut menu; on the Directory Security tab, click the **Edit** button; on the Authentication Methods dialog box, optionally, clear the **Enable anonymous access** check box, and select the **Integrated Windows authentication** check box; then click **OK** twice.
 - b. Navigate to and right-click the ICS-WPD virtual directory and select **Properties** from the shortcut menu; on the Directory Security tab, click the **Edit** button; on the Authentication Methods dialog box, ensure that both the **Enable anonymous access** and **Integrated Windows authentication** check boxes are selected; then click **OK** twice.
 - c. Navigate to and right-click the InmagicBrowse virtual directory and select **Properties** from the shortcut menu; on the Directory Security tab, click the **Edit** button; on the Authentication Methods dialog box, ensure that both the **Enable anonymous access** and **Integrated Windows authentication** check boxes are selected; then click **OK** twice.

5. Configure the IIS Custom 401 Errors handler. When Integrated Windows security fails, the user gets a 401 error. To catch the error and redirect to the *Genie* login page, do the following:
 - a. Using the IIS Manager, navigate to the InmagicGenie Web site.
 - b. Right-click the WinLogin.ASPX file, and select **Properties** from the shortcut menu to open a dialog box.
 - c. On the Custom Errors tab, edit each 401 error to assign it to the Redirect401.HTM page provided in the main *Genie* installation folder (for example, C:\Program Files\Inmagic\Genie), as shown in the following illustration.



6. Restart IIS (the World Wide Web Publishing Service) using the Services option through the Computer Management window. We recommend that you do this when no one is accessing the *Genie* application. If logged-in users are using the application when IIS is restarted, they will get an "Access Denied" page. They will have to log in to the *Genie* application again. For your OPAC users, who typically do not have to log in, restarting IIS will discard the contents of their InfoCart.

End of document