SONISWEB®

Scholastic ONline Information System

for the Web

Security Checklist

We don't re-invent what works well. Your Internet firewall, operating system and database security are the first line of defense. SONISWEB® follows them with access control for each group and each person. This manual illustrates how you tie the levels of security together to secure your system against inadvertent errors and malicious attacks.

March 2006

(SecurityTips.doc - 04/11/06 4:35 PM)

RJM Systems, Inc.

NEW IN THIS EDITION

- This edition is for SONISWEB® version 2.0.
- Figure 1 "SONISWEB® Configuration without Internet Connection", page 2.
- Figure 2 "IIS Help", page 4.
- Figure 3 "SONISWEB® Internet Connection", page 5.
- Figure 4 "Query for Security Articles and Experience", page 7.

SECURITY CHECKLIST

This paper contains a security checklist based on the RJM Systems, Inc. staff and contractor observations in implementing SONISWEB® in its development and test sites and with its customers. It's not comprehensive. It's a place to start in working out your security requirements.

RJM Systems, Inc. is not responsible for your security. You are expected to employ or contract with people who can knowledgeably advise you on your security needs and see to their implementation. This includes periodic tests of your system to see that it remains secure. By installing SONISWEB®, you agree to hold RJM Systems, Inc., harmless in this regard.

Local, LAN, and Physical Security

You don't have to connect to the Internet. If all of your users are connected by a campus local area network (LAN), you can connect it as shown in Figure 1.

Local Area Networks (LANs) are not protected by firewalls and encryption. You need physical barriers and passwords to protect against unauthorized access via your local Ethernet, dial-up access, and physical access.

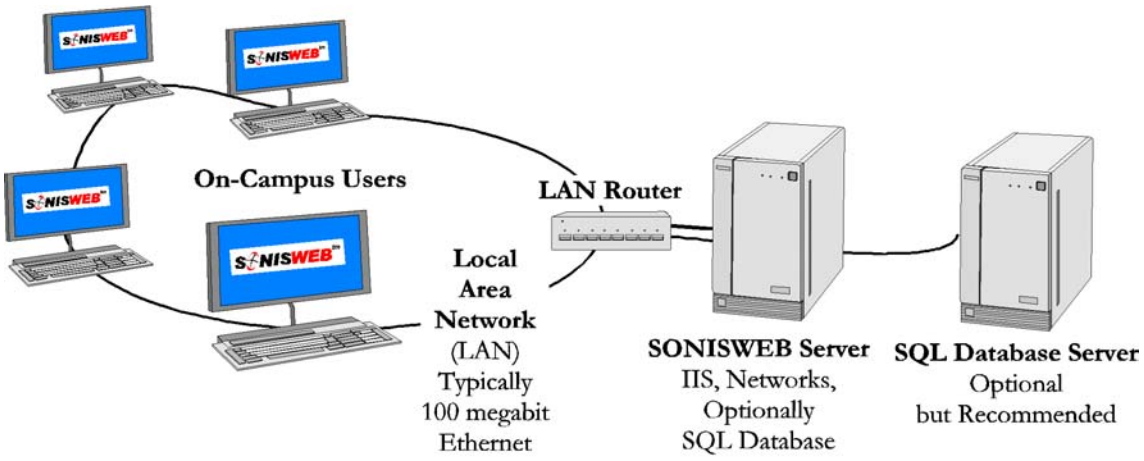


Figure 1 SONISWEB® Configuration without Internet Connection

(SONISWEB® can be installed on a single server ["SONISWEB Server" in Figure 1]. However RJM recommends that two servers be used. One hosts the SONISWEB® soft-

ware, IIS[1], ColdFusion™, the connection to the LAN, and the Report Builder. The second contains the SQL database. Separating these two functions improves the performance of SONISWEB® as seen by your users.)

These are the items to check when setting up the SONISWEB®-SQL servers and the LAN.

- Proper security settings on the router such as network address translation and/or MAC layer address limits to exclude those who shouldn't access the system.
- Alerting your user community to the security issues described in the separate SONISWEB® text "Browser Settings". This prevents unauthorized users from accessing SONISWEB® from a connected computer while the user is absent.
- Control physical access to the SONISWEB® database and software server. Place your servers in locked spaces. Many commercial providers of server space put locked cages (indoor chain-link fences) around servers. They can see who is in the cage and there is adequate air flow to keep the servers cool.
- Control the LAN connection permissions by your local user computers. Pay special attention to computers in labs, libraries and other public places. SONISWEB® and other sensitive systems should reside on separate servers that exclude access by computers in public places. You can use MAC layer controls to exclude them.
- Keep backup copies of your SONISWEB® database and software in locked drawers. For safety from fire and building damage, professional server companies keep backup copies in another building in a fire-resistant safe.
- Use layered password protection. Although SONISWEB® provides user password or PIN protection for its functions (see "SONISWEB® Security", page 8), malicious users can use the "backdoors" in the operating system and database software to copy and/or destroy your data. The layers recommended:
  - Protect the SONISWEB® database through "SQL Authentication" (user-name and passwords) instead of "Windows Authentication".

Only the database administrator and his or her backup should have SQL Authentication. Everyone else needing access should use a developer copy process as described in "Custom Reports and Development" (page 5).

  - Set up the IIS[1] "Local Security Policy" tables to control access to IIS. That's the entry point for LAN users to access the server.
  - Check for the latest security information on IIS since it's the connection between your LAN users and SONISWEB®. A Web search such as this will get you Microsoft's recommendations and those of other users:

microsoft IIS security

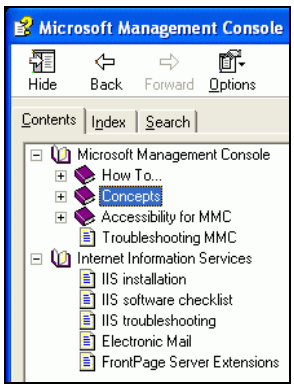
[1] Internet Information Services, a part of Microsoft® Windows™ server operating systems.

- Use "SQL Authentication" (not "Windows Authentication") to access the SQL Enterprise Manager and Query Analyzer. Windows-only authentication allows data to be extracted, destroyed or changed.
- Lock up the SONISWEB® directories-folders so that the programs, files, and applications cannot be added or changed. Allow read-only access, lock out all other access except by your trusted server administrator.

> If you allow write-change access to the SONISWEB® directories, a malicious user can write new ColdFusion™, Report Builder, or Crystal Reports™ - Crystal Enterpise[2] applications, install them in the directory, and get to your data that way. On most systems the directory you need to protect is inetpub\wwwroot.

- User a different server for development, as described in "Custom Reports and Development" on page 6.

A useful starting point for examining security is the IIS Help function. Start the IIS function (usually in Administrative Services) and click Help. Use the index tab to look up "passwords", "security", and "permissions".

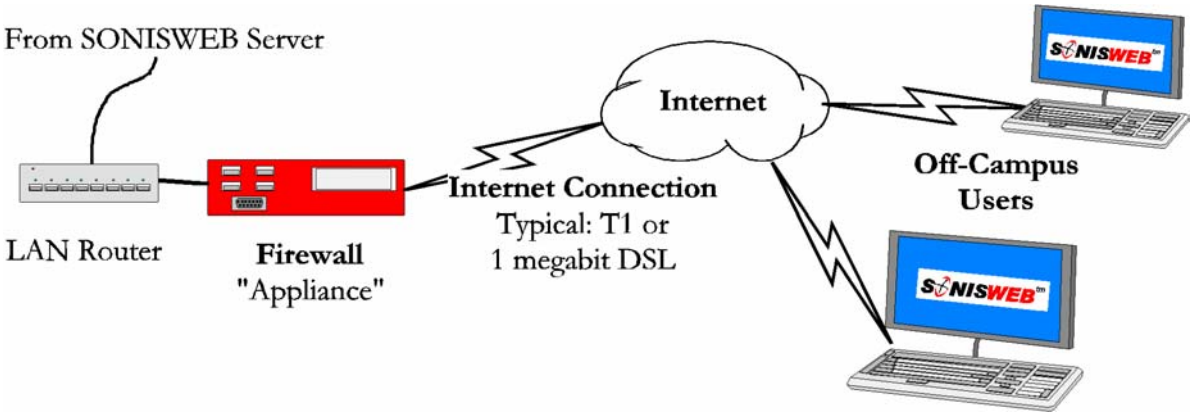


• Figure 2 IIS Help

[2] All new reports and enhancements to current reports are built with the ColdFusion™ Report Builder. You only need Crystal Enterprise if you want to run the old reports..

Web and Internet Connections

For your Web (Internet) connected users, install "firewalls", encryption, and server isolation. An Internet connection, shown in Figure 3, simply adds to the LAN system shown in Figure 1.



• Figure 3 SONISWEB® Internet Connection

A typical configuration is illustrated in Figure 3:

- A Firewall to prevent unauthorized access from the Internet. Usually this is a "firewall appliance", a small, separate special-purpose computer that serves that single function. You can use firewall software on your SONISWEB® server instead. That can absorb significant capacity, so it isn't advised unless you expect the user load on that server to be low to moderate.
- Proper setting of the Firewall "policies" to assure you keep out those who should not connect to SONISWEB®.
- A secure socket link (SSL) from a company like VeriSign®. In this method, Internet traffic (page requests) are passed through the Firewall using port 443.
- Alerting your Internet users to the security issues described in the separate SONISWEB® text "Browser Settings". This prevents unauthorized users from accessing SONISWEB® from a connected computer while the user is absent.

CUSTOM REPORTS AND DEVELOPMENT

RJM recommends that you use a "development" computer separate from your production server. You can put copies of SONISWEB® and your database on this "development" computer. That prevents inadvertent errors by developers affecting your production copy of SONISWEB® and your database.

This is how RJM uses development computers. We have several development and testing systems consisting of laptops with Windows 2000 Professional or XP Professional, IIS, SQL, ColdFusion™ run-time modules, and Report Builder installed. Two of our sites have testing servers. These isolate the production SONISWEB® software and data from the test environment.

- Password protect the start-up of these development computers. This protection is often called "Power-on Password".
- Set up screen savers to require a password to go from screen-saver to operation. Right-click an open space on the desktop and choose Properties to set this screen-saver option.

> Although this is just test data and test software, your copy of the production database tables will contain the same private and sensitive data as the production server.

- Define and use an inspection process to move newly developed software and files to the production server. A formal checklist is often used to make sure the production system is not compromised.

GETTING SECURITY UPDATES

At least monthly, Microsoft issues security updates for its products. Less frequently, ColdFusion™ and Crystal Reports™2 issue security updates. Your staff or your security contractor need to track these updates then download and install the appropriate ones.

- For Windows 2000-2003 and XP, Microsoft offers an automatic update service you can set up in Windows on your computer. It checks periodically for any updates.
- You can check for Windows 2000 and XP and for IIS and SQL security directly. As of this writing, you can access them at:

http://windowsupdate.microsoft.com/

http://www.microsoft.com/sql/downloads/default.asp

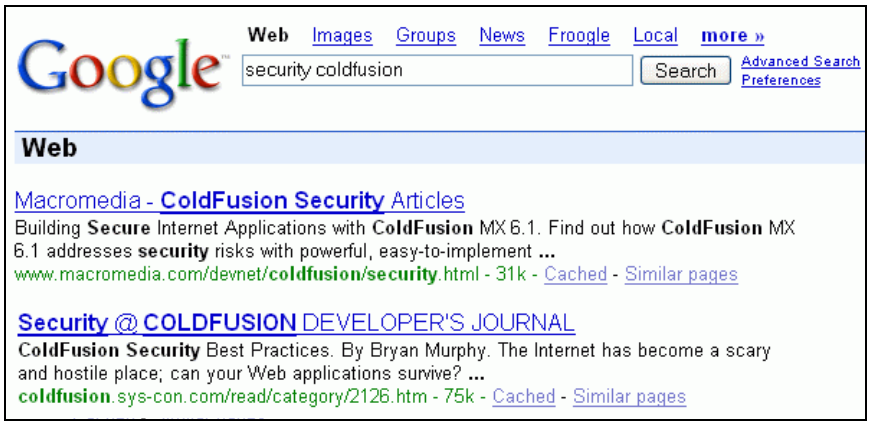
- For ColdFusion™ and its Report Writer, Macromedia® has a security Web page that links to their offerings. It has best-practices advice and white papers. Presently you can access it through:

http://www.macromedia.com/v1/developer/SecurityZone/AlertUs.cfm

- You can sign up for ColdFusion™ security e-mail notification at:

  http://www.macromedia.com/devnet/security/security_zone/notification_service.html

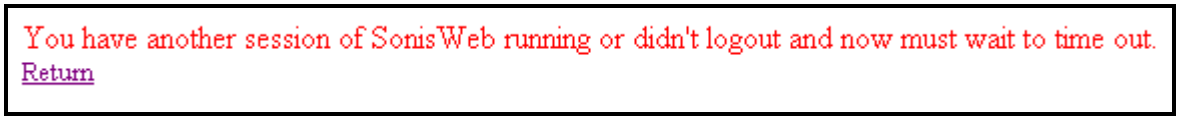
- Periodically, you can do a broad security search for your installed software using a search engine as illustrated in Figure 4.



• Figure 4 Query for Security Articles and Experience

BROWSER AND NORTON SECURITY INTERACTION

SONISWEB® customers have reported to us that the message shown in Figure 5 is caused by an interaction between Norton Internet Security™ (NIS) and the Internet Explorer (IE) browser. (The RJM Systems staff has not observed the problem.)



• Figure 5 "You have another session..." Error Message

If you are certain that another browser is not open with access to SONISWEB®, this NIS-IE interaction is suspect. The solution is to change the Norton Privacy Control settings:

1. Log off SONISWEB® and close your Web browser
2. Start Norton
3. Click "Privacy Control" (it's on the left)
4. Select "Configure"
5. Select "Custom Levels"
6. Turn off "Enable Browser Privacy" by clicking until the checkbox is empty
7. Exit Norton
8. Clear your browser's cookies
9. Log on to SONISWEB®.

A review of Web sites on the subject implies that Norton Personal Firewall™ (NPF) may cause the same problem. The Web references imply that Netscape® Navigator is affected also. These have not been reported to RJM Systems.

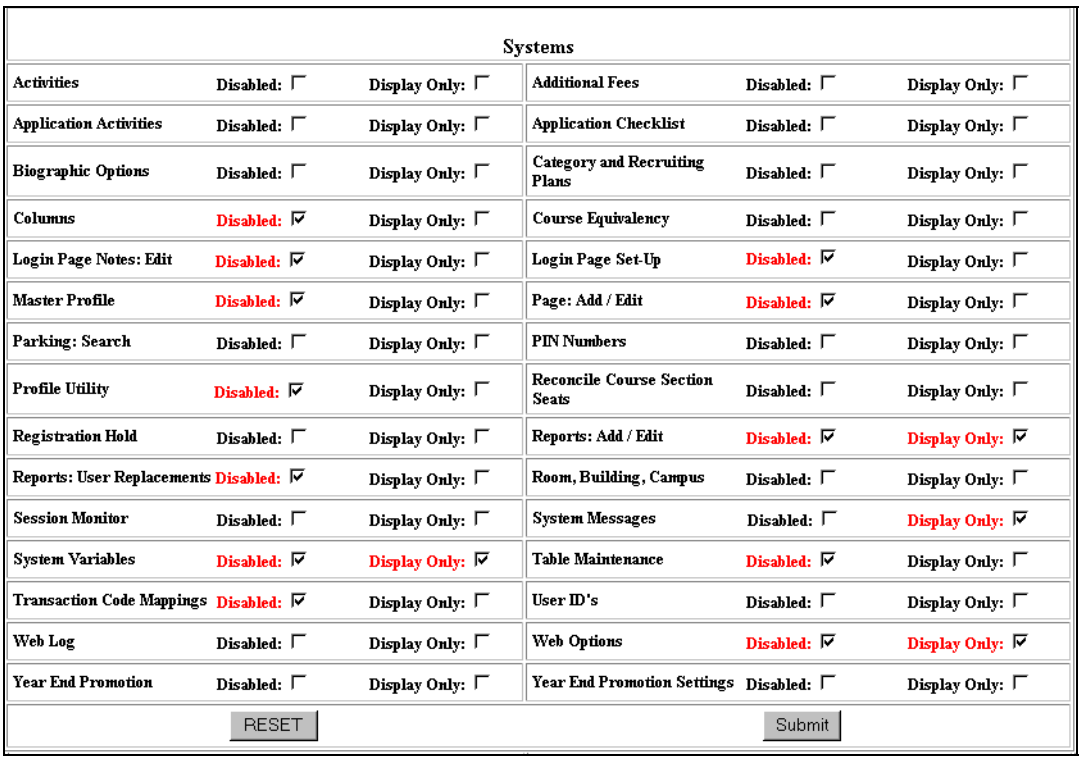
You should evaluate the privacy and security implications of this change before making it.

SONISWEB® SECURITY

After you close all of the security "holes" in the operating system, the server, SQL, ColdFusion™, the Report Writer, and Crystal Reports™ (if you need it[2]), you depend on SONISWEB® security. The text "User Authorization and Profiles" tells you how to set up SONISWEB® security.

Briefly, here's an outline of SONISWEB® security:

- Unattended workstation: SONISWEB® logs out users who are logged on but have been idle for a time you set in Web Options. See the SONISWEB® manual "Web Options" for setting the time-out period.
- Local computer: you can tighten security by setting up your users' computer screen-savers for password protection and shortening the inactivity timeout. Adding start-up passwords ("Power-on Password") to your users' computers adds the final layer.
- SONISWEB® PIN and Password security: issue these to the appropriate people and revoke them when their status changes. The SONISWEB® text "Semester and Year End Preparation Guide" recommends this at least at the end of each semester.
- Limit the "Master Profile" to one or two of your most trusted staff. For all others, provide role-specific profiles that carefully limit what records and what functions those users can access and edit. Figure 6 below shows some of the SONISWEB® functions that can disable the system if misused.



Systems

Activities	Disabled: ☐	Display Only: ☐	Additional Fees	Disabled: ☐	Display Only: ☐
Application Activities	Disabled: ☐	Display Only: ☐	Application Checklist	Disabled: ☐	Display Only: ☐
Biographic Options	Disabled: ☐	Display Only: ☐	Category and Recruiting Plans	Disabled: ☐	Display Only: ☐
Columns	Disabled: ☑	Display Only: ☐	Course Equivalency	Disabled: ☐	Display Only: ☐
Login Page Notes: Edit	Disabled: ☑	Display Only: ☐	Login Page Set-Up	Disabled: ☑	Display Only: ☐
Master Profile	Disabled: ☑	Display Only: ☐	Page: Add / Edit	Disabled: ☑	Display Only: ☐
Parking: Search	Disabled: ☐	Display Only: ☐	PIN Numbers	Disabled: ☐	Display Only: ☐
Profile Utility	Disabled: ☑	Display Only: ☐	Reconcile Course Section Seats	Disabled: ☐	Display Only: ☐
Registration Hold	Disabled: ☐	Display Only: ☐	Reports: Add / Edit	Disabled: ☑	Display Only: ☑
Reports: User Replacements	Disabled: ☑	Display Only: ☐	Room, Building, Campus	Disabled: ☐	Display Only: ☐
Session Monitor	Disabled: ☐	Display Only: ☐	System Messages	Disabled: ☐	Display Only: ☑
System Variables	Disabled: ☑	Display Only: ☑	Table Maintenance	Disabled: ☑	Display Only: ☐
Transaction Code Mappings	Disabled: ☑	Display Only: ☐	User ID's	Disabled: ☐	Display Only: ☐
Web Log	Disabled: ☐	Display Only: ☐	Web Options	Disabled: ☑	Display Only: ☑
Year End Promotion	Disabled: ☐	Display Only: ☐	Year End Promotion Settings	Disabled: ☐	Display Only: ☐

RESET Submit

• Figure 6 Compressed Section of a Profile with High-risk Functions Disabled

Figure 6 is a "telescoped" display of Systems functions in a profile. The highest risk functions have been marked as disabled as an illustration of how you might set up your profiles.

You should look beyond the functions in Figure 6. Who should see the students' financial ledgers or financial aid records? Who may see the faculty salary record? Questions like these are critical to setting up each group's profile to maintain security and privacy.