BarTender System Security

Selecting the Best Security Measures for
Your BarTender Environment

WHITE PAPER

Contents

Overview

Whether you're a small business or a huge enterprise, protecting your BarTender documents and databases from unauthorized modification and printing is important. Your needs may be as simple as preventing accidental design changes by inexperienced users, or as complex as requiring document encryption and creating multiple user groups with different editing and printing rights. The purpose of this white paper is to tell you about the security measures available from BarTender, and to help you decide which of them are right for you and your business.

The following security options are covered in this white paper:

- Application-level security, including password protection for documents and for BarTender Designer
- BarTender's built-in security settings, where administrators can set up system-wide permission checks in Administration Console, require user log-in for specific actions, and encrypt BarTender documents
- Database Security, so that users can protect their data files and the BarTender System Database
- Revision Control to prevent multiple users from overwriting each other's changes to a file
- Printing Security to restrict and monitor a user's ability to print BarTender documents

BarTender Security and Government Standards

A variety of government agencies, both in the United States and internationally, require high standards in the area of electronic security and record-keeping. For example, the United States Food and Drug Administration (FDA) has published their 21 CFR, Part 11 guidelines with detailed description of the access control, logging standards and electronic signatures they want to see in a “secure” electronic record-keeping system. Other agencies, such as the Department of Defense, provide their own guidelines.

BarTender is almost always used as part of a larger software system. Simply installing it therefore does not in and of itself ensure compliance with any one security standard. For example, no printing software package is going to lock down your central database system for you, provide you with general network encryption, and in any way control the vulnerabilities of the other software running on your enterprise. However, BarTender provides the core security and record-keeping functions required in the area of document design and printing to support implementation of a secure printing system.

BarTender Application-based Security

BarTender includes some basic security measures that can easily be implemented in your environment, requiring little administrator input or continued administration. These measures are suggested for non-enterprise printing environments.

Print-Only Password

A “Print-Only Password” locks the design functionality of BarTender from being used by any person who does not have the password. This is the quickest security measure to set up, but it is also the most easily defeated.

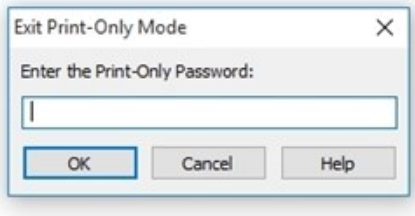
Once a password is set up, BarTender always starts in "Print-Only" mode. Any user who opens a document with that copy of BarTender can still view the template on screen and print it, but cannot modify template objects or use options in the **Administer** menu without knowing and entering the password.

This security measure is adequate for preventing accidental design changes by production personnel. However, it is not nearly as powerful as some of the other methods discussed in this white paper. For example, if you are using just the Print-Only Password for security, a user with a second copy of BarTender located on another computer could copy a BarTender document to their PC and change the design there.

The Print-Only Password is defined using the **Print-Only Password Setup** dialog, accessible from the **Administer** menu.

> **NOTE:** To enter Print-Only mode after setting the Print-Only Password for the first time, you must exit and then restart BarTender.

Once the Print-Only Password has been entered, BarTender will exit Print-Only mode. In order to reenter Print-Only mode, you must close and restart BarTender.



Who Should Use the Print-Only Password?

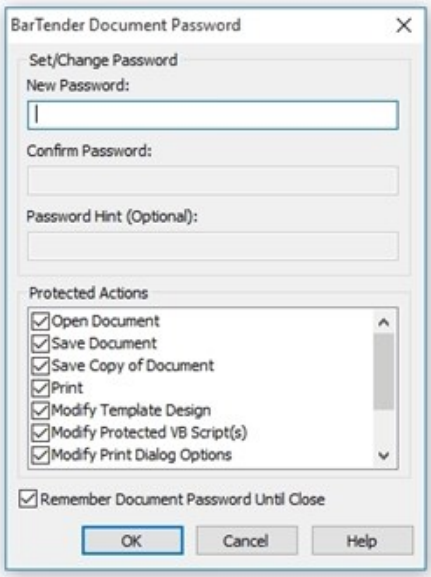
- Small businesses who have a single copy of BarTender and have no reason to expect malicious attacks from outside the company.

Which Editions of BarTender Support It?

- The Professional, Automation and Enterprise Automation editions

BarTender Document Password Protection

A BarTender Document Password protects a specific BarTender document (as opposed to the Print-Only password, which locks all of BarTender's functionality). They offer a quick and easy way to protect specific attributes of selected BarTender documents from malicious or accidental modification, and to optionally prevent unauthorized printing.



The password that you set is unique for each BarTender document. Once you set a password, you can select the actions within that document that you wish to protect from unauthorized users.

BarTender Document Passwords cannot be breached just by copying the document to another computer. The password is encrypted, so that hackers can't read it out of the stored document. By setting a password, the system administrator or designer can protect access to all aspects of the document, or only selected capabilities without any dependency on or interaction with BarTender Security Center.

The BarTender Document Password is set using the **BarTender Document Password Setup** dialog, accessible from the **File** menu.

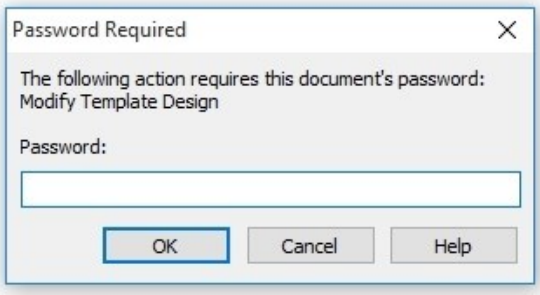
Protecting Individual Features

Once you have specified the password for your document, you can then set which actions you want to designate as "Protected Actions." When any of these check boxes are enabled, the user will be asked to enter the password before being allowed to perform that action.

For a complete list of actions protected by the document password, refer to the BarTender Document Password Dialog topic in the BarTender help system.

Supplying the Password to Access Protected Features

Once a Document Password has been specified and stored within a document, users are automatically prompted for the password when attempting to access a protected action.



Who should use Document Passwords?

- Any business with a need to password-protect individual documents to prevent unauthorized modification and printing.
- Designers with Administrator privileges who want to protect a document or aspects of a document they are working on.
- Businesses who want a higher level of security than is provided by Print-Only Passwords, but who don't want to get very technical to set up their security.
- Managers who want to specify which aspects of a document can be accessed by editors or print personnel.

Which Editions of BarTender Support It?

- The Professional, Automation and Enterprise Automation editions

BarTender Security Settings

BarTender's integrated security settings, defined in Administration Console, controls whether specific actions can be performed by individual users or groups of users for each application in the BarTender Suite. This allows system administrators to prevent both malicious users and well-intended curiosity seekers from making application configuration changes, modifying a document or document data, and even from printing.

These security options are included with both Automation editions of BarTender, with two features (Electronic Signatures and Logging) only available in the Enterprise Automation edition.

With Adminstration Console, you can:

- Set user permissions that define what actions a user can perform.
- Log attempts to modify BarTender documents or the application.
- Require the use of electronic signatures.
- Add encryption keys to BarTender documents.

For more information, refer to the Security section of the BarTender help system.

Initial Planning

Achieving a maximally secure environment with the least amount of effort requires careful planning prior to configuring your security settings. Here are some issues you should plan for in advance.

Limit Members of the Administrators Group

By default, all users that are members of a Windows computer's **Administrators** group have full control of Administration Console on that system and can therefore change security settings that they want, even disabling security completely. It is therefore important to ensure that the **Administrators** group is appropriately configured on any computer that can run BarTender or Administration Console. This caution is consistent with Microsoft's recommendation that general system users should not be part of the **Administrators** group.

Create User Groups

If you have many BarTender users, you may find it useful to define "groups" of users using standard Windows Security. This way, you can create settings just once for that group, instead of repeatedly configuring settings for one individual user after another. You can create these groups locally on the PC or on the Windows domain. You should consider creating multiple groups, one each type of user. For example, you could create one group called DocumentEditors for those users who are authorized to create and modify documents, and another group called PrintOperators for those users who are only authorized to print. You create these groups using the standard Windows user and group management tools.

Configuring Your Security Settings

Once your planning and preparation is done, you are ready to run and configure your security settings using Administration Console.

Specifying the Data Storage Location

First, you need to activate BarTender's security settings on the **Security** page of Administration Console.

Separate security settings, including user permissions, electronic signatures and access logs, can be stored locally to a text file for each copy of BarTender on a network. With the Enterprise Automation edition, shared settings can be stored in a single location accessible to multiple BarTender users on the network or in a shared BarTender System Database.

Adding Users and Groups

In order for individuals and groups to be given rights within Administration Console, they must first be created as Windows users by their system administrator. After that, you can add users and/or groups to Administration Console and set what actions they can perform.

> **NOTE:** Once Administration Console is installed and enabled, any Windows user or group that you fail to include within the user list will automatically be denied permission to all actions in the BarTender Suite.

Disabling BarTender's Security Settings

To disable BarTender's integrated security settings:

1. Run Administration Console.
2. On the Security page, disable (uncheck) **Enable Security for this PC**.
3. Click **OK**.

This will disable all permission checks based on Administration Console's security settings.

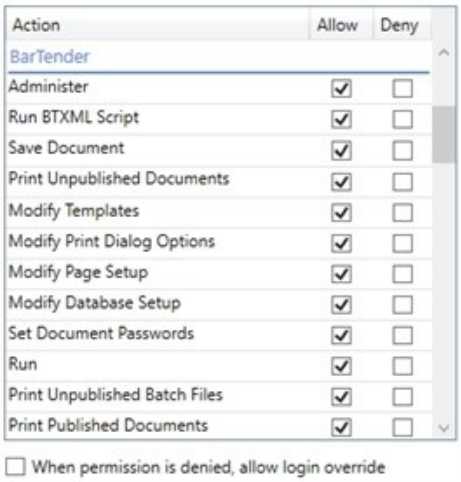
Turning Off Encryption for Existing Documents

Disabling your security settings does nothing to make encrypted documents readable again. To fix that problem, you need to temporarily enable your security settings again. Then, use the **Document Encryptor** utility on the **Encryption** page to set the encryption for the desired document to **<None>**. You can then disable security again.

User Permissions

By setting user permissions, you define what actions can be performed within the BarTender Suite based on the identity of the person logged into that PC. For example, you can specify that a given user or a member of a specific group is allowed to select a printer and launch a print job, but is not able to alter the design of a document or change any data in the document.

Once you have added the desired users and/or groups to Administration Console, you can individually set the permissions for any of a large number of available actions.



Check the appropriate box to define permissions for the selected user or leave both boxes blank to deny permissions. These permissions work exactly the same as they do for Window Security, which means that the absence of explicit permissions for a given action is equivalent to the **Deny** option being enabled.

The ability to leave the security settings blank (neither **Allow** nor **Deny** is enabled) for a selected action is an important part of supporting a security configuration in which an individual user is also a member of one or more user "groups." In this situation, the access rights of a given user to perform an action may depend on combining multiple sets of security settings. The following rules are used to resolve any permissions conflicts that may result:

- If the settings for an action are set to **Deny** for any security entity for which the user is a member, then the user will not be allowed to perform that action.
- If no **Deny** settings for an action are present in any security entities for which the user is a member, then the user will be allowed to perform that action.
- The absence of any **Allow** or **Deny** settings for an action within the security entities for which a user is a member is equivalent to a **Deny** status for access to that action.

A denied action can be overridden by another user who has the appropriate permission.

For the full list of user permissions controllable with Administration Console, refer to Security Permissions List in the BarTender help system.

Who Should Use User Permissions?

- Businesses with enough employees and/or complex enough documents that controlling what aspects of BarTender a user or group can access is important. For example, you might want to allow your Document Design team to modify and save documents, but deny them access to Printer Maestro if printing is not part of their job. Likewise, you might want to allow your Print team access to Print Station, Printer Maestro and Reprint Console, but deny them permission to modify or save documents.
- Businesses with high security requirements. User-based permissions is the most powerful single security feature in Security Center.

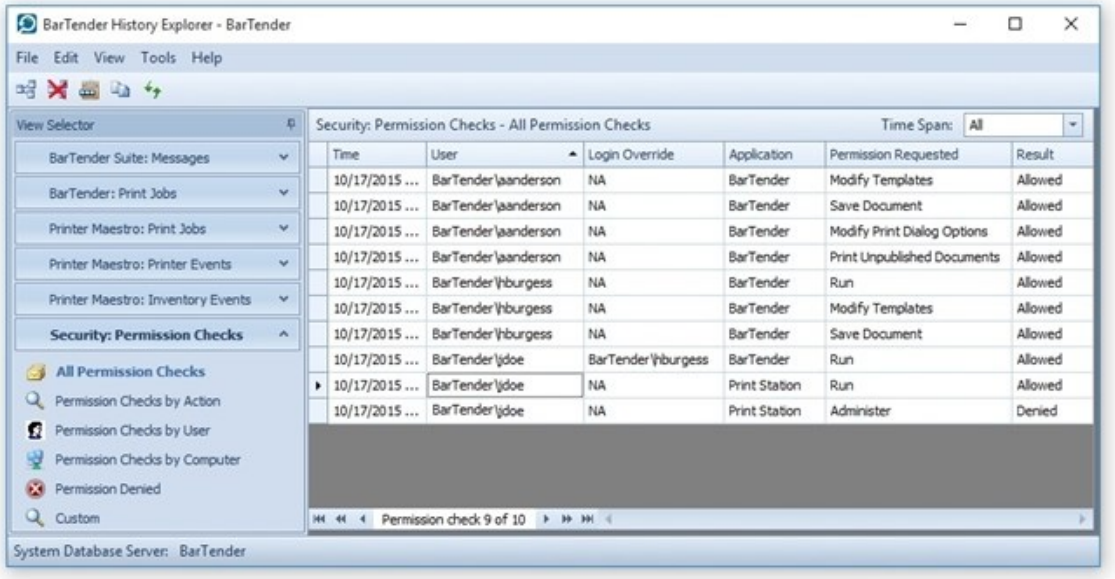
Which Editions of BarTender Support It?

- The Automation and Enterprise Automation editions

Logging Permission Checks

Some system administrators want to do more than simply set permissions that allow some users to perform certain actions that other users cannot. You may want to know who asked to perform certain actions, even if those users were never granted permission to do so. Administration Console can log these "permission checks" to the BarTender System Database. Later, you can view a list of permission checks using History Explorer.

When combined with the Electronic Signature feature, the logging of permission checks is a vital part of satisfying a number of high security standards, including the United States FDA's 21 CFR Part 11 guidelines, which require that electronic signatures be captured for certain actions.



Who Should Use Logging?

- Businesses with high security needs.
- Businesses held to government regulation security standards.
- Businesses who suspect attempted security breeches.

Which Editions of BarTender Support It?

- The Enterprise Automation edition

Electronic Signatures

Administration Console lets administrators require an electronic signature (or user login) for all users performing actions within the BarTender Suite. When users perform actions requiring an Electronic Signature, a dialog pops up requesting that they resubmit their Windows credentials. The electronic signature is nothing but a request for the user to resubmit his or her login credentials, similar to what is requested when first logging into Windows at the beginning of the day.

Electronic signatures require the entry of a user's name and password *regardless of whether or not the currently logged-in user has already been configured in Administration Console to have the appropriate permissions*. Suppose a user walks away from his or her workstation without locking it, and another user with lower-level security rights attempts to perform security-sensitive actions. With Electronic Signatures enabled, that user will be asked to submit login credentials before being allowed to proceed.

In order for an electronic signature to be associated with a given user action, you must also ensure that the user (or his or her group) has been granted permission to that action on the **User Permissions** page.

Combined with Administration Console's logging capabilities, electronic signatures can keep track of who requests what actions in BarTender.

Who Should Use Electronic Signatures?

- Businesses that have multiple people using a PC, especially if they sometimes share their login credentials for that PC.
- Businesses held to government regulation security standards, some of which require the use of electronic signatures.
- Businesses who suspect attempted security breaches.

Which Editions of BarTender Support It?

- The Enterprise Automation edition

Document Encryption

The protection that BarTender provides can be defeated if someone copies a document from a computer with security enabled to an unsecured workstation. A similar security breach occurs if somebody installs another copy of BarTender elsewhere on the network, but does not install Administration Console on that computer. In both cases, an unauthorized individual could now possibly modify or print the previously secure documents.

To fix this dilemma, you can encrypt BarTender documents using Administration Console. Once a document is encrypted, it becomes unreadable except when it is accessed by an authorized user on a properly-configured PC. If encrypted documents are moved to a different PC, they cannot be read unless Administration Console is installed there *and* somebody knows what security keys to specify.

You only have to enter encryption keys into Administration Console at setup time – you will never be asked to type them in while loading a document. Once you enable the document encryption and define at least one encryption key in Administration Console, the encryption is performed automatically as each document is saved during normal use. Similarly, the decryption is performed automatically as the documents are opened (which they have to be in order to be printed).

Any instance of Administration Console can optionally store multiple encryption keys in order to allow decryption of documents encrypted by multiple sources.

You can always change, add or remove encryption keys from documents you've already encrypted. For more information, refer to the Managing Encryption topic in the BarTender help system.

WARNING: Guard Against Possible Loss of Your Documents!

In order to start encrypting documents, you need to first enter an encryption "key" into Administration Console, which it stores and then uses to automatically scramble and unscramble your documents. Encryption keys are just text strings, somewhat similar to passwords. However, when you lose a password (such as to an on-line bank or email account), you can usually get a new one. In contrast, if you lose an encryption key once it has been used to encrypt templates, there is no way to get a replacement key. That means that, once you configure Administration Console to encrypt documents, losing the associated encryption key would likely prevent you from ever opening those documents again. You would "lose" the copy of the key(s) located on an individual computer if:

- The computer is stolen.
- The computer incurs damage to its hard drive that causes the associated copy of BarTender to be destroyed or otherwise lose access to its encryption key(s).
- A member of the Administrators group deletes Administration Console's security file on the user's hard drive.

In any of the above circumstance, if your documents were backed up or located on another computer, you would be able to retain use of your documents as long as you had recorded and stored the value of your key(s) in a secure location. Therefore, to minimize the likelihood that you could ever be left with documents that you cannot read, we suggest one or more of the following precautions:

- When backing up your computer's hard drive, make sure that you back up your local security file, stored by default at: C:\Documents and Settings\All Users\Application Data\Seagull Security\SecuritySettings.xml.
- Set up one or more additional copies of BarTender on your network and configure the associated Administration Console to use (and therefore store) the same key value.
- System administrators can also simply write down key values on paper. (In order to keep from nullifying the benefits of encryption, information about your keys obviously has to be stored in a location not readily available to others.)

Who Should Use Encryption?

- Businesses with multiple computers and who don't want to make documents readable, writable or printable by users of all computers.
- Businesses held to government regulation security standards, some of which require the use of encryption.
- Businesses who suspect attempted security breaches.

Which Editions of BarTender Support It?

- The Automation and Enterprise Automation editions

Database Security

A "database" in BarTender can be one of two things:

- A database file that is the source of text or image data in your BarTender document.
- The BarTender System Database, which is a SQL database used by applications in the BarTender Suite to store print job information, application messages and security permission checks.

You can protect both database files and the BarTender System Database in a variety of ways.

Protecting Database Files

If your goal is simply to protect the database files connected to your document from unauthorized modification by select users or groups, you can:

- Protect a database file on a single computer from modification using the Windows **Properties** dialog to make the file read-only.
- Password-protect the database file in the application it is written or stored in (such as Microsoft Access, SQL Server or Oracle).
- Check the database into Librarian, then restrict access to specific users or groups using Administration Console's **User Permissions** page.

  > **NOTE:** Denying access to Librarian does not just restrict the users or groups from editing database files, it restricts them from editing *any* file in Librarian.

- Protect the modification or addition of databases to a particular document using BarTender's **Document Password** security feature or from the **User Permissions** page in Administration Console.

  > **NOTE:** These settings will not prevent a user from opening a database file from outside of BarTender and modifying it.

Protecting the BarTender System Database

A certain amount of protection is built in to the BarTender System Database setup and modification process. When you set up the BarTender System Database for the first time, you will be asked for Windows authentication or the proprietary system database (SQL, Oracle, etc.) authentication. Anyone trying to modify the BarTender System Database on that computer will be asked for authentication as well. If they don't have authentication rights to the computer or to the copy of the database on the computer, they will be unable to modify the database.

Non-technical employees can inadvertently wreak havoc on the BarTender System Database by misusing powerful companion applications like Integration Builder and Seagull License Server. The easiest way to prevent this is to limit access to these applications on a user-by-user or group-by-group basis using Administration Console.

Who Should Use Database Protection?

- Businesses with enough employees or teams that accidental modification, deletion, or

overwriting of databases is a possibility.

- Businesses with multiple people using one copy of BarTender.
- Businesses who want to protect the BarTender System Database from accidental modification, or malicious attacks. Note that accidental modification can happen only if multiple people have Administrator rights.

Which Editions of BarTender Support It?

- Windows Security is not related to BarTender and is available on any Windows-based PC.
- Administration Console is included with both the Automation and Enterprise Automation editions of BarTender.
- Librarian comes with the Enterprise Automation edition of BarTender only.

Revision Control

Revision control isn't exactly security, but it is an excellent way to prevent multiple users from editing the same file at the same time and to keep track of who has modified documents and when. BarTender comes with its native revision control system, Librarian. (Of course, your company may use another form of revision control system that operates outside of BarTender.)

Overview of Librarian

Librarian is a revision control system for BarTender documents, images and related files. Once you have added files to Librarian, they are stored in a centralized repository. Files must be checked out of Librarian to be edited, eliminating the possibility of multiple users editing the same file at once. When the changes are complete, the files are checked back into the repository. Librarian keeps track of all revisions, noting the date and time of a modification, as well as the user who checked the file into the repository.

Librarian stores its files in the BarTender System Database, so that all users of the BarTender Suite have access to them. Users (who have permission in Administration Console) have access to Librarian revision information, so that they can easily identify and keep track of revisions.

Revisions of a file are identified by consecutive numbers. The initial addition of a file to the repository is "revision 1". When the first change is made to a file, the subsequent check-in is "revision 2", and so on. At any point, a user can roll back to a previous revision of a file, or even restore a deleted file.

Librarian also allows you to use workflows to track changes made to a file, using configurable states. (Examples of workflow states might be "First Draft", "Editor Review", "Stakeholder Review", and so on.) By assigning a state to a file, you can identify the progress of a file towards a goal.

Who Should Use Librarian?

- Businesses with multiple document designers, database programmers, writers or other employees who are likely to accidentally overwrite each other's work.
- Businesses with a formal editing and review process.

Which Editions of BarTender Support It?

- The Enterprise Automation edition

For more information, refer to the Librarian section of the BarTender help system, as well as the **Librarian** and **Revision Control** white papers:

http://www.seagullscientific.com/support/white-papers

Restricting and Monitoring the Printing Environment

If your company is larger than a handful of employees, monitoring the print environment can be very important. You want to make sure that only authorized personnel modify print settings and start and/or stop print jobs. You can control print access from BarTender on a per-document level or from Administration Console at an administrative level.

You can also monitor and/or control printing using the companion applications Print Station, Printer Maestro and History Explorer.

Limit Printing Access at the Document Level

In each BarTender document, you can add a document password that prevents unauthorized users from printing *that particular document*. By setting up this security measure, users will need to enter the password in order to print the document and/or modify any of its print settings (like printer, number of copies, printer optimizations or caching options).

For more information, refer to the Document Password Protection section of this white paper.

Limit Printing Access for Users and Groups using Administration Console

Alternatively, you can restrict users or groups from printing *any* BarTender document through Administration Console. Administration Console also provides a number of other printing rights that grant you more control over your printing environment, such as:

- Modifying the options in the Print dialog
- Printing "Published" batch files and documents from Librarian
- Printing "Unpublished" batch files and documents

Limit Modification of Documents with Print Station

Print Station lets users browse and quickly print BarTender documents (*.btw), batch files (*.btbat), and BTXML Script files (*.btxml) with a single click.

Users of Print Station essentially have no access to modify the documents -- from the application, users can only print them. System administrators can also set up certain security measures for the application such as selectively disabling features, limiting the number of open documents, or requiring an Administration Password to modify Print Station's settings.

With Print Station, you can:

- Browse BarTender documents and command files in thumbnail and verbose views.
- Print documents and command files with a single mouse click.
- Prevent users from changing settings using password authentication.
- Preview BarTender documents before they are printed.

Who should use Print Station?

- Print Station is appropriate for businesses of all sizes who quickly need to locate and print a document.

Which Editions of BarTender Support It?

- All editions

For more information, refer to the Print Station section of the BarTender help system, as well as the **Print Station** white paper:

http://www.seagullscientific.com/support/white-papers

Limit the Ability to Print with BarTender Print Portal

BarTender Print Portal is a web-based application that provides an interface for selecting and printing BarTender documents. As with Print Station, users of Print Portal do not have the ability to modify the documents they view --they can only print them. Administrators can set which printing permissions to allow.

The **Administration** page of Print Portal is for use by system administrators only, and is not accessible by print-time users. It can be accessed using the Windows **Start** menu on the web server, or directly using the URL http://localhost/bt-wps/BtAdmin.aspx. From the **Administration** page, you can:

- Allow or disable standard Windows printing, and define which printers will be supported.
- Allow or disable PDF printing.
- Allow or disable Queue-based Internet printing.
- Specify the Internet printing methods, client-side print module and printer models that will be supported.

Who Should Use Print Portal?

- Any large enterprise with the need to browse, select, and print BarTender documents from any operating system or platform that can run a web browser.

Which Editions of BarTender Support It?

- The Enterprise Automation edition only

For more information, refer to the **BarTender Print Portal** white paper:

http://www.seagullscientific.com/support/white-papers

Monitor Printing with Printer Maestro

The Printer Maestro application is a powerful tool for monitoring printers and print jobs on your network. Printer Maestro can be configured to send you notifications via email, instant message or text message for a variety of events, including printer errors or warnings and inventory use thresholds. Using Printer Maestro, you can:

- Monitor the status of all the computers in your network.
- Monitor the status of all the printers in your network and view their properties.
- Monitor print jobs in your networks, including details such as who started the print job, the computer where the print request originated and print job progress.
- View recent print jobs and the job's properties.
- Reprint a recent print job.
- Track all events that affect computers, printers, print jobs and inventory items system-wide.
- Configure a print management system for a cluster (a set of connected computers that work together like a single system)

Who should use Printer Maestro?

- Large enterprises with complex printing systems.

Which Editions of BarTender Support It?

- The Enterprise Automation edition. Partially supported in the Automation edition.

For more information, refer to the Printer Maestro section of the BarTender help system, as well as the **Printer Maestro** white paper:

http://www.seagullscientific.com/support/white-papers

Monitor Printing with History Explorer

History Explorer is a utility that displays information stored in the BarTender System Database, such as print job information for items that are printed by BarTender, application messages, security permission checks and inventory levels. History Explorer provides a configurable interface that allows you to monitor data in the BarTender System Database. With History Explorer, you can:

- View BarTender print jobs and messages.
- View Printer Maestro print jobs and events.
- View and filter print job records.
- View Security Center permission checks.

Who should use History Explorer?

- Large businesses who need to monitor activity in the BarTender System Database for security reasons.
- Managers who want to track BarTender and Printer Maestro activity.

- Print teams who need to view and track print job records.

Which Editions of BarTender Support It?

- The Enterprise Automation edition. Partially supported in the Automation edition.

For more information, refer to the History Explorer section of the BarTender help system, as well as the **History Explorer** white paper:

http://www.seagullscientific.com/support/white-papers

Other Security Issues

In addition to the various security features built into the BarTender Suite, Windows itself offers security features for protecting any file (as opposed to just BarTender files) and printers from unauthorized use. Although these features are not documented in detail here, they should be familiar to any Windows system administrator. Knowledge and use of these capabilities, as well as knowledge of the security functions available in any software controlling BarTender, are all important to creating a secure printing system.

Security Methods Quick Reference

Security Type	BarTender Edition	Protects Documents	Protects Printing	Monitors Printing	Protects Application	Protects Seagull License Server	Protects BarTender System Database	Protects Shared Files	Revision Control	High Security
Print Only Password	Professional Automation Enterprise Automation	Yes	Yes	No	Yes	Yes	No	No	No	No
Document Password	Professional Automation Enterprise Automation	Yes	Yes	No	No	No	No	No	No	No
User Permissions	Automation Enterprise Automation	Yes	Yes	No	Yes	Yes	Yes	No	No	Yes
Logging Permission Checks	Enterprise Automation	No	No	Yes	No	No	No	No	No	Yes*
Electronic Signatures	Enterprise Automation	Yes	Yes	No	Yes	Yes	Yes	No	No	Yes*
Document Encryption	Automation Enterprise Automation	Yes	Yes	No	No	No	No	No	No	Yes
Librarian	Enterprise Automation	Yes	No	No	No	No	No	Yes	Yes	Yes*
Printer Maestro	Automation** Enterprise Automation	No	Yes	Yes	No	No	No	No	No	Yes*
Print Station	All	No	Yes	No	No	No	No	No	No	No
BarTender Print Portal	Enterprise Automation	No	Yes	No	No	No	No	No	No	No
History Explorer	Automation** Enterprise Automation	No	No	Yes	No	No	No	No	No	Yes*
Windows Security	N/A	Yes	Yes	No	No	No	Yes	No	No	No

*High security when combined with other security measures.

**Partially supported in the Automation edition.

Related Documentation

White Papers and Manuals

- Administration Console
- BarTender Print Portal
- History Explorer
- Librarian
- Print Station
- Printer Maestro
- Revision Control

For downloadable versions, visit:

http://www.seagullscientific.com/support/white-papers

BarTender Help Topics

- Configuring BarTender Security
- BarTender Document Password Dialog
- Administration Console: Security
- Librarian

BarTender® BY SEAGULL SCIENTIFIC