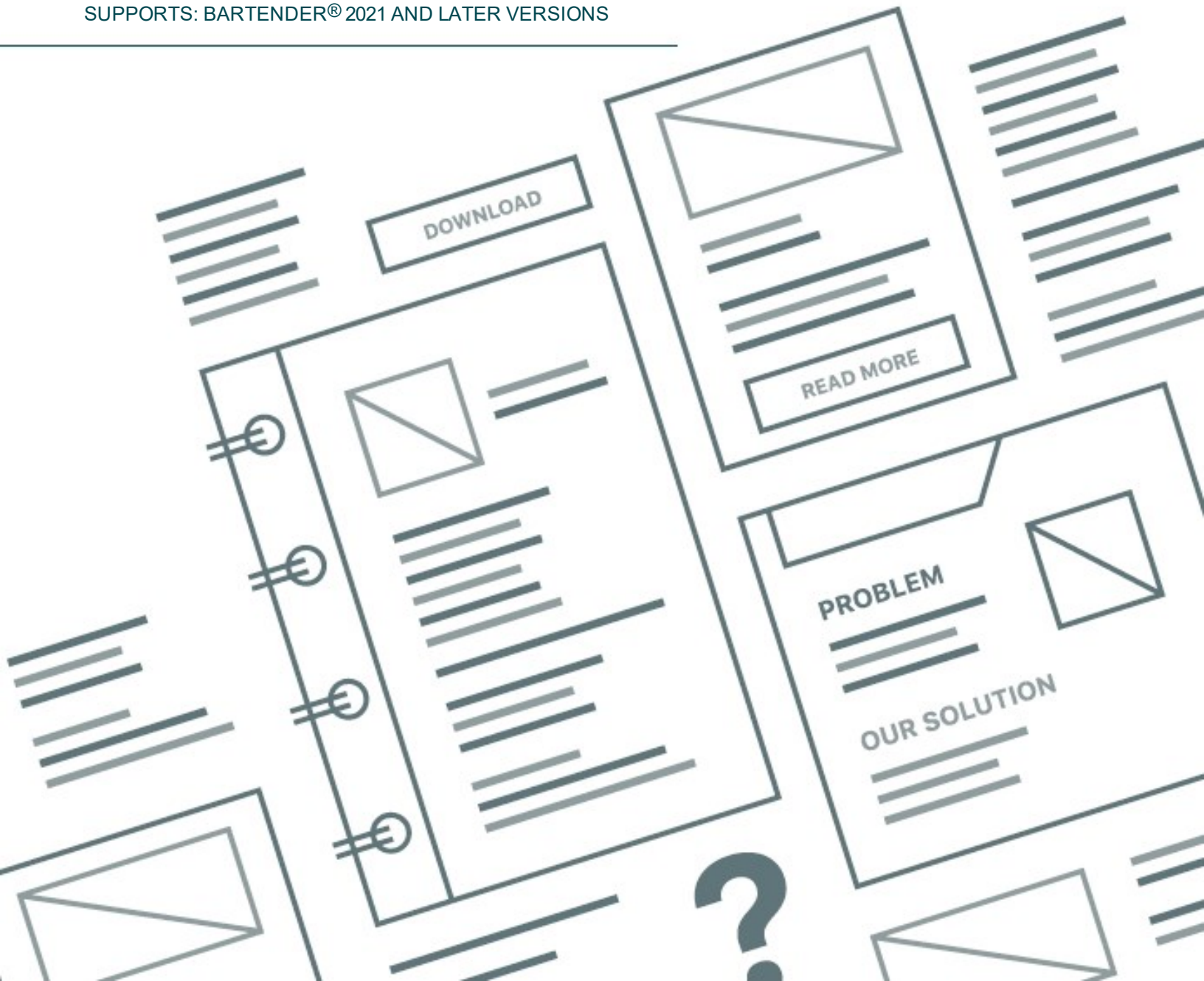
BarTender
BY SEAGULL SCIENTIFIC

Technical Document
English

BarTender System Security

SELECTING THE BEST SECURITY MEASURES FOR YOUR BARTENDER® ENVIRONMENT

SUPPORTS: BARTENDER® 2021 AND LATER VERSIONS



Contents

Overview

Whether you're running a small business or a huge enterprise, it's important to protect your BarTender documents and databases from unauthorized modification and printing. 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 that have different editing and printing permissions. This technical document describes the security measures that BarTender offers, so that you can decide which ones are right for you and your business.

The following security options are described:

- Application-level security, including password protection for documents and for BarTender Designer
- The BarTender built-in security settings, which administrators can use to set up systemwide permission checks in Administration Console, to require users to log on for specific actions, and to encrypt BarTender documents
- Database security to protect users' 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) published their 21 CFR, Part 11 guidelines, which include detailed descriptions of the access control, logging standards and electronic signatures that they want to see in a secure electronic record-keeping system. Other agencies, such as the US Department of Defense, provide their own guidelines.

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

BarTender Application-Based Security

BarTender includes some basic application-based security measures that can easily be implemented in your environment and that require little administrator input or continued administration. We recommend these measures for non-enterprise printing environments.

Print-Only Password

A print-only password prevents 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.

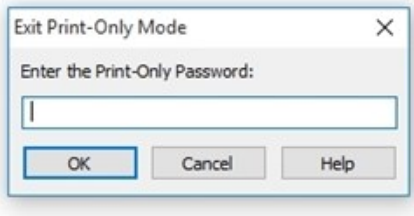
After you configure a password, BarTender always starts in "print-only" mode. Any user who opens a document in that copy of BarTender can still view the template on screen and print it but cannot modify template objects or use the **Administer** menu options without entering the password.

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 that this technical document describes. For example, if you are using only the print-only password for security, a user who is running another copy of BarTender that is located on another computer could copy a BarTender document to their computer and then change the design there.

You configure the print-only password by using the **Print-Only Password Setup** dialog, which you can access on the **Administer** menu.

To enter print-only mode after you configure the print-only password for the first time, you must exit and then restart BarTender.

After the user enters the print-only password, BarTender exits print-only mode. To re-enter print-only mode, the user must exit and then restart BarTender.



Who should use the print-only password?

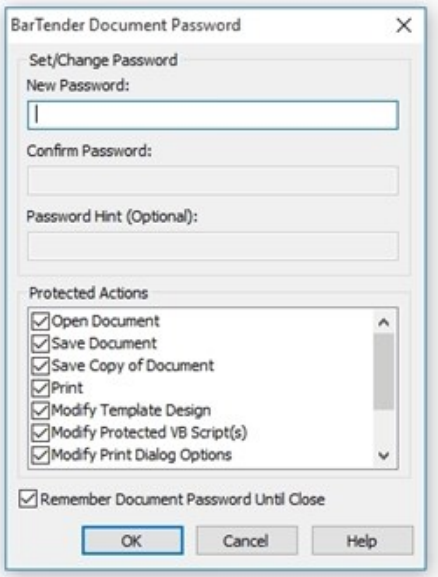
- Small businesses that have a single copy of BarTender and have no reason to expect malicious attacks from outside the company

Which editions of BarTender support it?

- Professional, Automation and Enterprise

BarTender Document Password Protection

A BarTender document password protects a specific BarTender document (as opposed to the print-only password, which locks all of the BarTender functionality). It offers a quick and easy way to protect specific aspects of selected BarTender documents from malicious or accidental modification and to optionally prevent unauthorized printing.



The password that you configure is unique for each BarTender document. After you configure a password, you can select the actions within that document that you want to protect from unauthorized users.

BarTender document passwords cannot be breached by copying the document to another computer. The password is encrypted, so that hackers cannot read it out of the stored document. By configuring a password, you can protect access to some or all aspects of the document.

You configure the BarTender document password by using the **BarTender Document Password Setup** dialog, which you can access on the **File** menu.

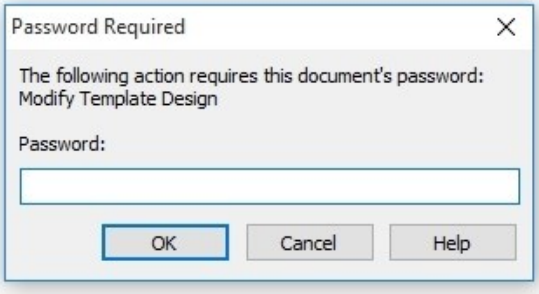
Protecting individual features

After you configure the password for your document, you can specify which actions you want to designate as "protected actions." When any of these check boxes are selected, users are prompted to enter the password before they can perform those actions.

For a complete list of actions that can be 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

After you specify and store a document password within a document, users are automatically prompted for the password when they try to perform a protected action.



Who should use document passwords?

- Any business that needs to password-protect individual documents to prevent unauthorized modification and printing
- Designers who have Administrator privileges who want to protect a document or aspects of a document that they are working on
- Businesses that want a higher level of security than is provided by print-only passwords but still want an easy process for setting up their security environment
- Managers who want to specify which aspects of a document can be accessed by editors or print personnel

Which editions of BarTender support it?

- Professional, Automation and Enterprise

BarTender Security Settings

The BarTender built-in security settings control whether specific actions can be performed by individual users or groups of users for each application in the BarTender Suite. By using these settings, system administrators can prevent both malicious users and well-intended curiosity seekers from making application configuration changes, modifying a document or document data, and printing documents.

The integrated security settings are managed by using the Security module in Administration Console. The Security module is available for every BarTender edition, but certain functionality depends on the edition that you have installed, as follows:

- The Professional edition supports the user and group permissions feature, which you can use to configure user permissions that specify the actions that each user or user group can perform.
- The Enterprise edition supports the electronic records and signatures feature, which you can use to configure the following:
    - Logging of permission checks when you want BarTender to log users' attempts to perform certain actions, whether the user has permission to perform the action or not
    - Electronic signatures that require users to submit their logon credentials before access is granted to the user for specific actions
    - Encryption keys for BarTender documents

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

Initial Planning

To achieve a maximally secure environment with the least amount of effort, carefully plan your security settings before you configure them. For example, you should plan in advance to address the following considerations.

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. Therefore, they can change security settings and even turn off security completely. Because of this, you must ensure that the **Administrators** group is appropriately configured on any computer that can run BarTender or Administration Console.

This caution is consistent with the Microsoft 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 by using standard Windows Security features. When you do this, you can create or modify settings for all users in that group at one time instead of repeatedly configuring settings for one user after another.

You can create these groups locally on the computer or on the Windows domain. We recommend that you consider creating multiple groups, one for each type of user. For example, you could create one group that is called DocumentEditors for those users who are authorized to create and modify documents and another group that is called PrintOperators for those users who are authorized only to print. You create these groups by using the standard Windows user and group management tools.

Configuring Your Security Settings

After your planning and preparation are done, you are ready to run and configure your security settings by using Administration Console. The first step is to click to select the **Enable Security for this computer** check box on the **Security** page of Administration Console to make the BarTender security settings available.

Specifying the data storage location

You can store separate security settings, including user permissions, electronic signatures and access logs, locally in a text file for each BarTender installation. When you run the Enterprise edition, shared settings can be stored in a single location in a shared BarTender System Database.

Adding users and groups

To give individuals and groups rights in Administration Console, the system administrator must first create them as Windows users. Then, you can add them to Administration Console and then configure the actions that they can perform.

After Administration Console is installed and security turned on, any Windows users or groups that you do not include in the user list are automatically denied permission to all actions in the BarTender Suite.

Turning Off the BarTender Security Settings

To turn off the BarTender security settings, follow these steps:

1. Run Administration Console.
2. On the **Security** page, click to clear the **Enable Security for this computer** check box.
3. Click **OK**.

When you do this, all permission checks that are based on the Administration Console security settings are turned off.

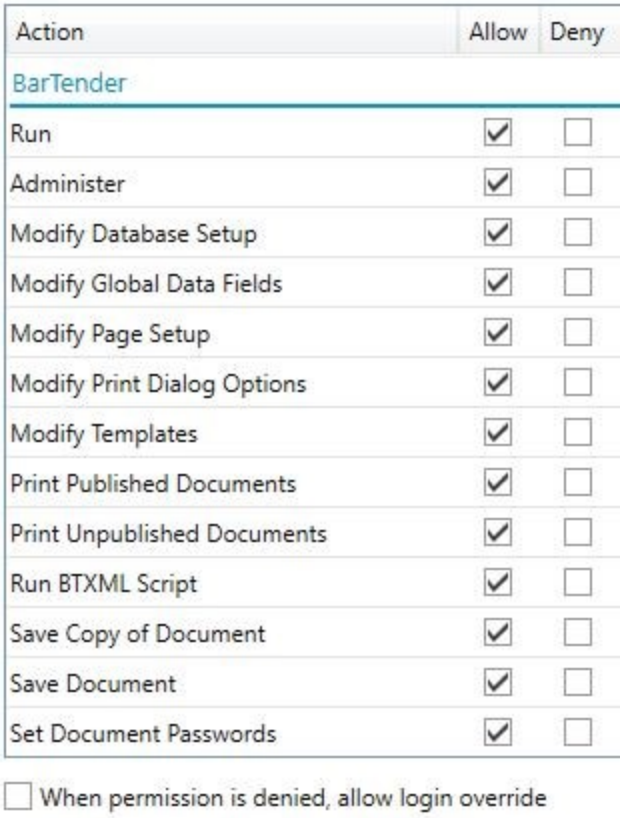
Turning off encryption for existing documents

Turning off your security settings does not make encrypted documents readable again. To make encrypted documents readable, you must temporarily turn on your security settings again. Then, use the **Document Encryptor** tool on the **Encryption** page to set the encryption for the documents to **<None>**. You can then turn security off again.

User Permissions

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

After you add the users and groups that you want to Administration Console, you can individually configure the permissions for any of a large number of available actions.



Click to select the appropriate check box to define permissions for the selected user, or leave both check boxes blank to deny permissions. These permissions work exactly the same as they do for Windows Security, which means that the absence of explicit permissions for a given action is the same as selecting the **Deny** option.

The ability to leave the security settings blank (so that neither **Allow** nor **Deny** is selected) for an action is an important way that BarTender supports 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 specific user to perform an action may depend on the combination of 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 is not 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 is 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 the same as 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 that can be controlled by using Administration Console, refer to the User Permissions Page topic in the BarTender help system.

Who should use user permissions?

- Businesses that have enough employees and/or complex enough documents that it is important to control which aspects of BarTender a user or group can access. 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 that have high security requirements. The user-based permissions feature is the single most powerful security feature in BarTender.

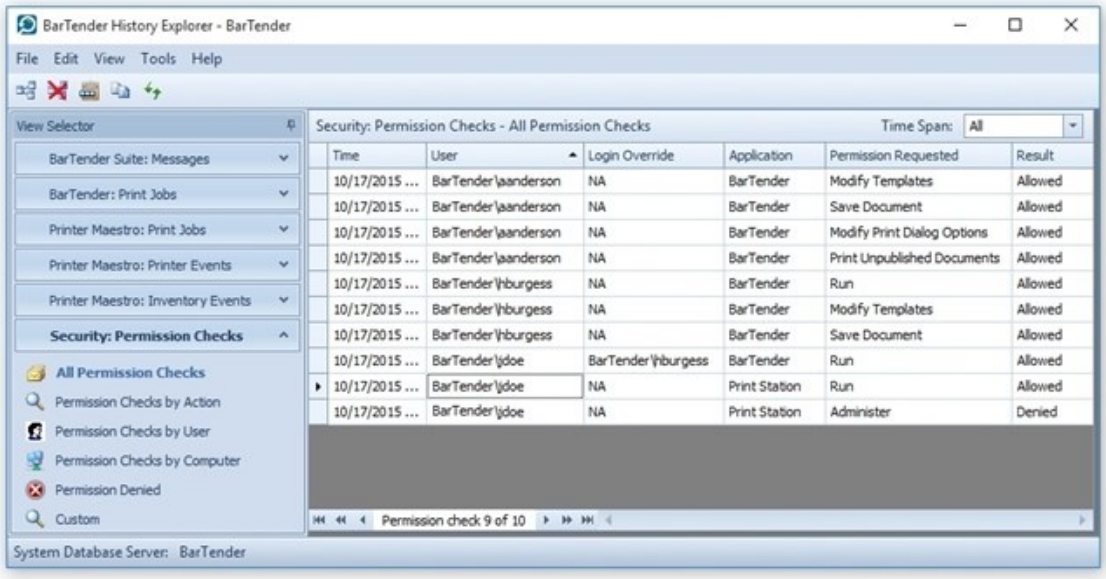
Which editions of BarTender support it?

- Professional, Automation and Enterprise

Logging Permission Checks

In some cases, system administrators need to do more than simply set permissions that allow some users to perform certain actions that other users cannot. You might want to know which users try to perform certain actions when they were not granted permission to do so. Administration Console can log these permission checks to the BarTender System Database, and then later, you can view a list of permission checks by using History Explorer.

The combination of permission checks logging and the electronic signature feature is an important part of satisfying a number of high security standards, including the US FDA 21 CFR Part 11 guidelines, which require that electronic signatures be captured for certain actions.



Who should use logging?

- Businesses that have high security needs
- Businesses that are held to government regulation security standards
- Businesses that suspect or anticipate attempted security breaches

Which editions of BarTender support it?

- Enterprise

Electronic Signatures

By using Administration Console, administrators can require an electronic signature (or user logon credentials) for all users who perform actions within the BarTender Suite. When users perform actions that require an electronic signature, a dialog is displayed to request that they resubmit their Windows credentials. This is similar to what is requested when users first log on to Windows at the beginning of the day.

Electronic signatures require that a user's name and password be entered regardless of whether the currently logged-on user has already been configured in Administration Console to have the appropriate permissions. This configuration provides an extra layer of security. For example, suppose that a user walks away from his or her workstation without locking it and another user who has lower-level security rights tries to perform security-sensitive actions. When electronic signatures are used, that user is prompted to submit logon credentials before being allowed to proceed.

For an electronic signature to be associated with a specific 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 the Administration Console 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 computer, especially if they sometimes share their logon credentials for that computer
- Businesses that are held to government regulation security standards, some of which require the use of electronic signatures
- Businesses that suspect or anticipate attempted security breaches

Which editions of BarTender support it?

- Enterprise

Document Encryption

The protection that BarTender provides can be defeated if someone copies a document from a computer that has 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 possibly modify or print the previously secure documents.

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

You must enter encryption keys into Administration Console only at setup time. You are never prompted to enter them while you load a document. After you enable 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 (and they must be opened before they can be printed).

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

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

Keep track of your encryption keys. If you lose or delete an encryption key that was used to encrypt a document, you can no longer use that document.

Guarding against possible loss of your documents

To start encrypting documents, you must first enter an encryption key into Administration Console. The key is stored in Administration Console and then used to automatically encrypt and decrypt your documents.

Encryption keys are text strings, somewhat similar to passwords. The difference is that when you lose a password (such as for an online banking or email account), you can usually get a new one, but if you lose an encryption key after it has been used to encrypt documents, there is no way to get a replacement key. This means that if you lose the associated encryption key after you configure Administration Console to encrypt documents, you are likely to be prevented from ever opening those documents again.

You could lose the copy of encryption keys that are located on a computer under the following circumstances:

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

In any of these circumstances, if your documents were backed up or located on another computer, you could still use them as long as you had previously recorded and stored the values of your keys in a secure location. Therefore, to minimize the likelihood that you could be left with documents that you cannot read, we recommend that you take one or more of the following precautions:

- Back up your local security file whenever you back up your computer's hard drive. By default, the local security file is stored in the following location:

C:\Program Data\Seagull Security\SecuritySettings.xml

- Set up one or more additional copies of BarTender on your network, and then configure the associated copy of Administration Console to use (and therefore store) the same key value.
- Write the key values down on paper and then store them in a location that is not readily available to others.

Who should use encryption?

- Businesses that have multiple computers and that do not want to make documents readable, writable or printable by users of all computers
- Businesses that are held to government regulation security standards, some of which require the use of encryption
- Businesses that suspect or anticipate attempted security breaches

Which editions of BarTender support it?

- Enterprise

Database Security

In BarTender, a database can be one of the following things:

- A database file that is a data source in your BarTender document
- The BarTender System Database, which is a Microsoft SQL Server-based database that is 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 to protect only the database files that are connected to your document from unauthorized modification by certain users or groups, you can do one or more of the following:

- Protect a database file on a single computer from modification by 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, Microsoft SQL Server or Oracle).
- Check the database in to Librarian, and then restrict access to specific users or groups by using the Administration Console **User Permissions** page.

When you deny access to Librarian to specific users or groups, you not only prevent them from editing database files, but you also prevent them from editing any file in Librarian.

- Prevent a document from being modified or databases from being added to a document by using the BarTender **Document Password** security feature or the **User Permissions** page in Administration Console.

These settings do not prevent a user from opening a database file 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 are prompted for Windows authentication or proprietary system database (such as SQL Server and Oracle) authentication. Any users who try to modify the BarTender System Database on that computer are also prompted for authentication. If they do not have authentication rights to the computer or to the copy of the database on the computer, they cannot modify the database.

Non-technical employees can inadvertently wreak havoc on the BarTender System Database by misusing powerful companion applications such as Integration Builder. The easiest way to prevent

this is to use Administration Console to limit access to these applications on a user-by-user or group-by-group basis.

Who should use database protection?

- Businesses that have enough employees or teams that accidental modification, deletion, or overwriting of databases is a possibility
- Businesses that have multiple people who are using one copy of BarTender
- Businesses that 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 computer.
- Configuring user permissions by using Administration Console is supported by the Professional, Automation and Enterprise editions.
- Librarian is supported only by the Enterprise edition.

Revision Control

Although revision control is not technically a security feature, it is an excellent way to prevent multiple users from editing the same file at the same time and to keep track of who modified a document and when. Your company might use a form of revision control system that operates outside of BarTender, but the Enterprise edition of BarTender does include its own native revision control system: Librarian.

Overview of Librarian

Librarian is a revision control system for BarTender documents, images and other kinds of files. After you add files to Librarian, they are stored in a centralized repository. To edit files, users must check them out of Librarian, which eliminates the possibility of multiple users editing the same file at a time. When the changes are complete, users check the files back in to the repository. Librarian keeps track of all revisions, logs the date and time of a modification, and logs the user who checked the file in to 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 the appropriate 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 serial numbers. When a file is first added to the repository, it is called "revision 1." When the first change is made to a file, the subsequent checked-in file is called "revision 2," and so on. At any time, a user can revert to a previous revision of a file or even restore a deleted file.

In Librarian, you can use configurable workflow states to track changes that are made to a file. (For example, your 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. For more information about how to use workflows in Librarian, refer to the *Understanding Librarian Workflows* technical document:

https://www.seagullscientific.com/resources/white-papers/

Who should use Librarian?

- Businesses that have multiple document designers, database programmers, writers or other employees who might accidentally overwrite each others' work
- Businesses that have a formal editing and review process

Which editions of BarTender support it?

- Enterprise

For more information, refer to the Librarian section of the BarTender help system and to the *Librarian* and *Revision Control* technical documents:

https://www.seagullscientific.com/resources/white-papers/

Restricting and Monitoring the Printing Environment

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

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

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. When you configure this security measure, users must enter the password to print the document and/or modify any of its print settings (such as printer, number of copies, printer optimizations or caching options).

For more information, refer to the Document Password Protection section of this technical document.

Limit Printing Access for Users and Groups by Using Administration Console

You can use Administration Console to prevent users or groups from printing any BarTender document. Administration Console also provides several other printing rights that grant you more control over your printing environment, such as the following:

- Modifying the options in the **Print** dialog
- Printing "published" files and documents from Librarian
- Printing "unpublished" files and documents

Limit Modification of Documents with Print Station

By using Print Station, users can browse to and quickly print BarTender documents (*.btw), process files (*.btproc), and BarTender XML (BTXML) script files (*.btxml) with a single click.

In Print Station, users have no access to modify the documents; they can only print them. System administrators can set up certain security measures for the application, such as selectively turning features off, limiting the number of open documents, or requiring an administration password to modify the Print Station settings.

By using Print Station, you can do the following:

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

Who should use Print Station?

- Businesses of all sizes that need to quickly locate and print a document

Which editions of BarTender support it?

- Professional, Automation and Enterprise

For more information, refer to the Print Station section of the BarTender help system and the *Print Station* technical document:

https://www.seagullscientific.com/resources/white-papers/

Limit the Ability to Print with Print Portal

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 cannot modify the documents they view; they can only print them.

As an administrator, you can configure Print Portal so that users must log on by using their Windows accounts. To do this, you must first enable security and configure permissions in Administration Console and then enforce these permissions by enabling authentication on the **Advanced** property page of the **Administrative Setup** page of Print Portal. You can access this page by entering the following URL into a web browser:

http://localhost/BarTender/Settings

On the **Advanced** property page of the **Administrative Setup** page, you can do the following:

- Enable authentication
- Specify that users are automatically logged out after a certain amount of time elapses with no activity
- Require that users enter a password before they can access the **Administrative Setup** page

Who should use Print Portal?

- Businesses that need to browse to, select, and print BarTender documents from any operating system or platform that can run a web browser

Which editions of BarTender support it?

- Enterprise

For more information, refer to the *BarTender Print Portal* technical document:

https://www.seagullscientific.com/resources/white-papers/

Monitor Printing with Printer Maestro

Printer Maestro is a powerful tool for monitoring printers and print jobs on your network. You can configure Printer Maestro 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. By using Printer Maestro, you can do the following:

- 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 the user who started the print job, the computer from which the print request originated and the progress of the print job
- 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 systemwide
- Configure a print management system for a cluster (which is a set of connected computers that work together like a single system)

Who should use Printer Maestro?

- Large enterprises that have complex printing systems

Which editions of BarTender support it?

- Enterprise

For more information, refer to the Printer Maestro section of the BarTender help system and the *Printer Maestro* technical document:

https://www.seagullscientific.com/resources/white-papers/

Monitor Printing with History Explorer

History Explorer displays information that is stored in the BarTender System Database, such as print job information for items that BarTender prints, application messages, security permission checks and inventory levels. History Explorer provides a configurable interface that you can use to monitor data in the BarTender System Database. By using History Explorer, you can do the following:

- View BarTender print jobs and messages
- View Printer Maestro print jobs and events
- View and filter print job records
- View security permission checks

Who should use History Explorer?

- Large businesses that 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?

- Automation (limited) and Enterprise

For more information, refer to the History Explorer section of the BarTender help system and the *History Explorer* technical document:

https://www.seagullscientific.com/resources/white-papers/

Other Security Issues

In addition to the various security features that are built into the BarTender Suite, Windows itself offers security features for protecting any file (not only BarTender files) and printers from unauthorized use. This document does not describe these features, but they should be familiar to any Windows system administrator. To create a secure printing system, it is important to know and use these features and the security features that are available in any software that controls BarTender.

Related Documentation

Technical Documents

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

To view and download technical documents, visit:

https://www.seagullscientific.com/resources/white-papers/

User Guides

- *Getting Started with BarTender*
  https://support.seagullscientific.com/hc/categories/200267887

BarTender Help System

- Configuring Document and Application Security
- BarTender Document Password Dialog
- Security
- Librarian
- User Permissions Page

Other Resources

Please visit the BarTender website at *https://www.seagullscientific.com*.