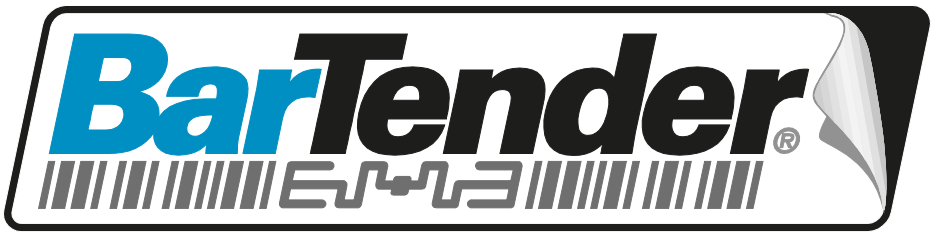


White Paper

Label System Security

Defining Permissions and Controlling Access within the BarTender Application Suite

SEAGULL SCIENTIFIC

Contents

Overview of BarTender Security

Properly protecting your label designs from unauthorized modifications and printing is essential in certain environments. However, in other circumstances, you may only need protection against accidental changes by careless users. Accordingly, as you consider the scope of your security requirements, you need to keep in mind that enabling *every* security feature currently available in the BarTender Application Suite requires time and careful planning. Such a project should only be performed by a "technical" individual, such as your System Administrator. On the other hand, some of BarTender's security features are quick and easy enough to be set by individuals with only casual system knowledge.

The five types of security available in the BarTender Application Suite are summarized below and explored in greater detail later in this document.

BarTender-based Security

Some measure of security can be introduced to an individual copy of BarTender using what we have long referred to as the "Print-only Password." This is the quickest security measure to set up, but it is also the most easily defeated.

Any one copy of BarTender can be forced into a "Print-only" mode just by using the **Password Setup** option in BarTender's **Administer** menu. Thereafter, any user that opens a label format using that copy of BarTender can still view the label on screen and print it. However, the user cannot modify label objects or use options in the Administer menu without knowing the password.

This security measure is adequate for preventing "accidental" label design changes by production personnel. However, it is not nearly as powerful as some of the methods described below. One reason is that a user armed with only basic Windows knowledge and a second copy of BarTender located elsewhere could copy a label format to another computer and change the label design there. (Available in Professional and both the Automation editions.)

Label Format-based Security

This is the second most powerful type of security available for BarTender and allows you to specify a unique password for each individual label format. The security in force when using label format passwords cannot be breached just by copying the label format to another computer. (The password is even encrypted, so that "hackers" can't just read it right out of the stored label format.) At the system administrator's option, the password can protect access to *all* aspects of the label format, or only selected capabilities. (Available in Professional and both Automation editions.)

User-based Security

The most powerful security features available in the BarTender Application Suite are provided by BarTender Security Center. This module was first introduced with BarTender version 9.1 in April of 2009. The Security Center allows system administrators to provide different users with different levels of access to just about every module and function in the entire BarTender Suite. (Available in the two Automation editions only, with some features limited to the Enterprise Automation edition.)

Label Format Encryption

The ability to encrypt a label format is actually part of BarTender Security Center. However, this function can be applied to the other two security methods listed above as well, thereby making them more secure. For example, by using Label Format Encryption in combination with the Print-only Password, an unauthorized individual can no longer gain access to a label format just by copying it to a non-secure location. (Available in both Automation editions.)

Event Logging and Auditing

Event logging itself is arguably not a "security feature" in that it doesn't actively *prevent* unauthorized activity. However, subsequent audits of event logs using History Explorer allow you to at least offer the threat of detecting these actions after they have occurred. For more information, please see the sections on Logging and History Explorer in the *What's New in BarTender 9.0 white paper*.

Introduction to BarTender Security Center

The BarTender Security Center application was added to the BarTender Application Suite in April 2009. It controls which actions can and cannot be performed by individual users and "groups" of users within each of the applications of the BarTender Suite. This allows system administrators to prevent both malicious users and well-intended curiosity seekers from making application configuration changes, modifying the label design or label data, and even from printing. BarTender Security Center is included with both Automation editions of BarTender, with two features (Electronic Signature and Logging, described below) only available in the Enterprise Automation edition.

About Compliance with CFR 21, Part 11 and Similar 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 CFR 21, 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 label 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 now provides the core security and record-keeping functions required in the area of label design and printing to support implementation of a secure labeling system.

For more detailed information on the relevant portion of the US FDA Regulations, please see:

http://www.fda.gov/ora/compliance_ref/Part11/

Introduction to User-based Permissions in BarTender Security Center

Security Center determines 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 is allowed to select a printer and launch a print job, but is not able to alter the design of a label format or the associated data sources.

Login Override

If you want to permit a supervisor to occasionally authorize users to perform actions that they are not ordinarily permitted to do, you can enable the **Login Override** feature. Thereafter, when a user attempts an action that he or she is not authorized to perform, a dialog will pop up inviting the entry of a login override name and password in order to allow the action to occur. (When properly configured, the **Login Override** dialog will require the name and password of the user's *supervisor*, rather than the actual user.)

For more details, please see the dedicated section later in this document.

Electronic Signature

If you have multiple people using a PC, especially if they sometimes share their login credentials for that PC, and you want to be sure to know which user is performing a particular action, you can enable the **Electronic Signature** feature for that action. This mandates entry of the user's name and password prior to that action being allowed, *regardless* of whether or not the currently logged-in user has already been configured within BarTender Security Center to have the appropriate permissions. Requiring an electronic signature protects you from the possibility of the currently logged-in user walking away from his or her workstation without locking it. Then, if another user with lower-level security rights attempts to perform security-sensitive actions, he or she will be asked to submit login credentials before being allowed to proceed. (This feature is only available in the Enterprise Automation edition.)

For more details, please see the dedicated section later in this document.

Logging of BarTender Security Center Permission Checks

If you need a record of authorization requests and their results, you can have Security Center log these permission checks to the BarTender System Database. This can be useful for both troubleshooting and auditing purposes. 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 CFR 21 Part 11 guidelines, which require that electronic signatures be captured for certain actions. (This feature is only available in the Enterprise Automation edition.)

For more details, please see the dedicated section later in this document.

Introduction to Label Format Encryption

The protection that BarTender Security Center provides can be defeated if someone is able to copy label formats from a PC on which Security Center has been installed and configured to an unsecured PC. A similar security breech occurs if somebody installs another copy of BarTender elsewhere on the network, but does not install Security Center on that computer. In both cases, an unauthorized individual could now possibly modify or print the previously secure label formats. In contrast, once label formats are *encrypted* using Security Center, they become unreadable accept when accessed by a user that is appropriately-authorized by a properly-configured Security Center to perform the desired actions.

WARNING: Guard Against Possible Loss of Your Label Formats!

In order to start encrypting label formats, you need to first enter an encryption "key" into BarTender Security Center, which it stores and then uses to automatically scramble and unscramble your label formats. Encryption keys are just text strings, somewhat similar to passwords. However, when you lose a password (such as to an on-line bank or e-mail account), you can usually get a new one. In contrast, if you lose an encryption key once it has been used to encrypt label formats, there is no way to get a replacement key. That means that, once you configure Security Center to encrypt label formats, losing the associated encryption key would likely prevent you from ever opening those label formats 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 BarTender Security Center's security file on the user's hard drive.

In any of the above circumstance, if your label formats were backed up or located on another computer, you would be able to retain use of your label formats 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 label formats 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
- You can set up one or more additional copies of BarTender on your network and configure the associated BarTender Security Center 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.)

Deploying BarTender Security Center

Achieving a maximally secure environment with the least amount of effort requires careful planning prior to configuring Security Center.

Initial Planning

Here are some issues you should plan for in advance.

Limit Members of the Administrators Groups

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

Create User Groups

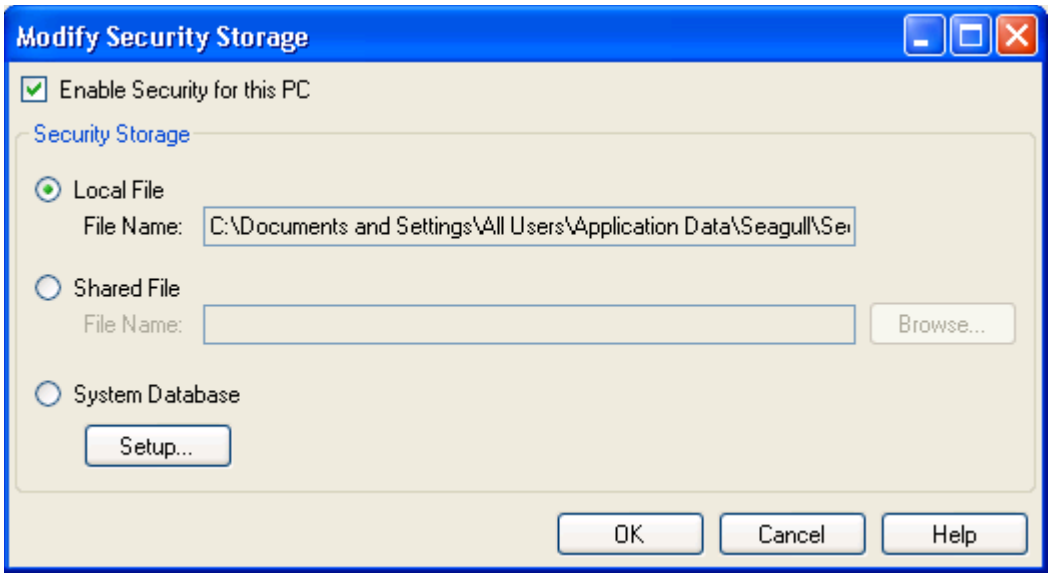
If you have many BarTender users, you may find it useful to define "groups" of users using standard Windows Security. This way, you can create settings just once for that group, instead of repeatedly configuring settings for one individual user after another. You can create these groups locally on the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

Configuring BarTender Security Center

Once your planning and preparation is done, you are ready to run and configure Security Center.

Specifying the Data Storage Location

The first time you run BarTender Security Center, it opens the **Modify Security Storage** dialog. Security Center starts out disabled by default. Use the topmost checkbox to enable Security.



Separate security settings can be stored local to each copy of BarTender on a network. Alternatively, shared settings can be stored in a single location accessible to multiple BarTender users.

The User Permissions, Electronic Signature, and Logging settings for any one copy of the BarTender Application Suite are stored together in any one of three locations:

- **Local File** - This setting is the simplest solution if you only have BarTender installed on one PC, or if you do not need to share security settings between computers.
- **Shared File** - This setting lets you specify a single security file for sharing security settings between multiple copies of the BarTender Application Suite.
- **System Database** - This setting stores your security configuration in the BarTender system database. If you are using the Automation edition, a system database will be created that is local to each copy of BarTender and is therefore not shared. Therefore, when Automation edition users want to specify shared security settings, they should use the **Shared File** setting instead of **System Database**. In contrast, if you are using the Enterprise Automation edition, you have the option of having multiple PCs access shared security settings within a single, shared BarTender System Database.

Once you have enabled Security Center and closed this dialog, you can change your security storage settings later using the **Modify Security Storage** button on the main Security Center window.

Security Vulnerability in Windows 2000 Systems

Windows 2000 does not support the features needed to properly secure the **Local File** security file. This means that any user that knows where to look can read the contents of that file if desired. The greatest threat that this poses is that a user could copy the file and install it on another PC where he or she is an administrator. BarTender Security Center could then be used to view any encryption keys that might be in use. We therefore recommend against use of Windows 2000 as part of any security solution in which label format encryption is essential. If you ignore this caution, you should at least take measures to control access to the network, e-mail, removable media, and any other means that could potentially allow a user to make a copy of the security file.

Special Considerations for Sharing the Security File or System Database

When the **Local File** storage option is chosen, the security file is automatically protected against unauthorized access. However, for the **Shared File** and **System Database** storage options, you must take extra steps to secure the data storage. In both cases you need to give all BarTender users the ability to read the data, but you only want to give write access to users that need to administer to BarTender Security Center.

To Protect Shared Security Files Stored on a Windows File Server:

To protect your shared security file on Windows, you simply use the standard Windows Properties dialog as follows:

1. Right-click on the file and select **Properties**
2. Open the **Security** tab
3. Give all BarTender users read access to the file, but reserve write access for Administrators only.

To Protect Shared Security Files on non-Windows File Servers:

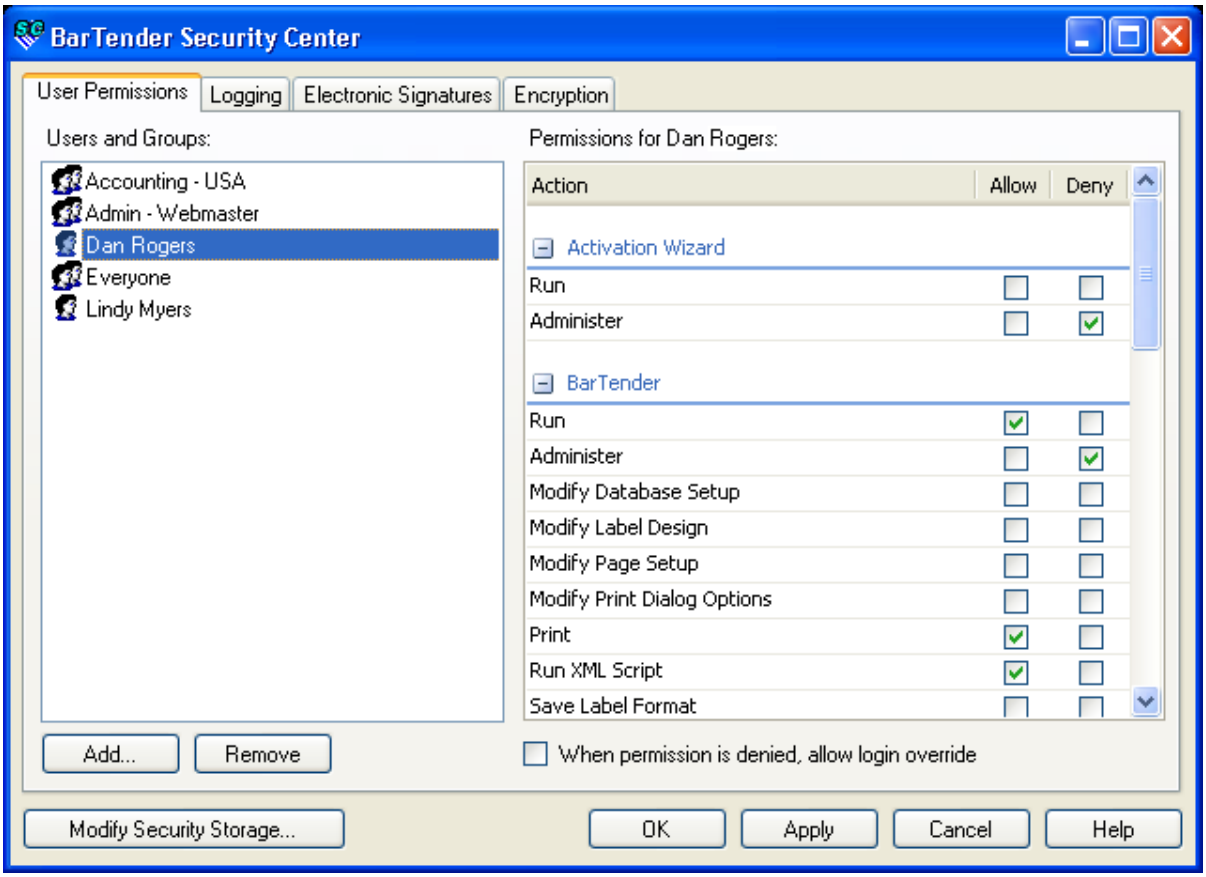
Methods will vary. Please consult the documentation for your file server operating system.

To Protect the Security Settings Stored in the System Database:

To protect the security setting in the System Database, you must protect the "SystemData" table from being written to by non-administrators. All users need read-only access to that table, but only administrators need to write to it. See your SQL management tools documentation for details on how to secure a database or a table.

Adding Users and Groups

The **User Permissions** tab in BarTender Security Center allows you to import a list of users and groups previously defined using your Windows security settings. You then set these users' permissions to access various actions available within the BarTender Application Suite.



In order for individuals and groups to be given rights within BarTender Security Center, they must first be created as Windows users by their system administrator in the normal manner. After that, you can use the **Add** button in Security Center to select from your existing list of Windows users and groups. Once BarTender Security Center is installed and enabled, any Windows user or group that you fail to include within this BarTender Security Center list will automatically be denied permission to *all* actions in the BarTender Application Suite.

Specifying User Permissions

Once you have added the desired users and/or groups to BarTender Security Center, you can individually set the permissions for any of a large number of available actions to:

- Allow
- Deny
- Or, it can be left blank

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 checked.

Resolving Contradictory Allow and Deny Settings

If you are new to Windows security, you may wonder, "Why are the **Allow** and **Deny** options *both* available for a given user or group?" It is *not* so that you can select them both at the same time, but because this is the easiest way to optionally offer the ability to leave the security settings blank for a selected action. Being able to do so 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.
- Otherwise, if no **Deny** settings for an action are present in any security entities for which the user is a member *and* there is at least one **Allow** setting present for that action, 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.

Extensive List of User Permissions

For the full list of user permissions controllable by BarTender Security Center, please see *Appendix A*.

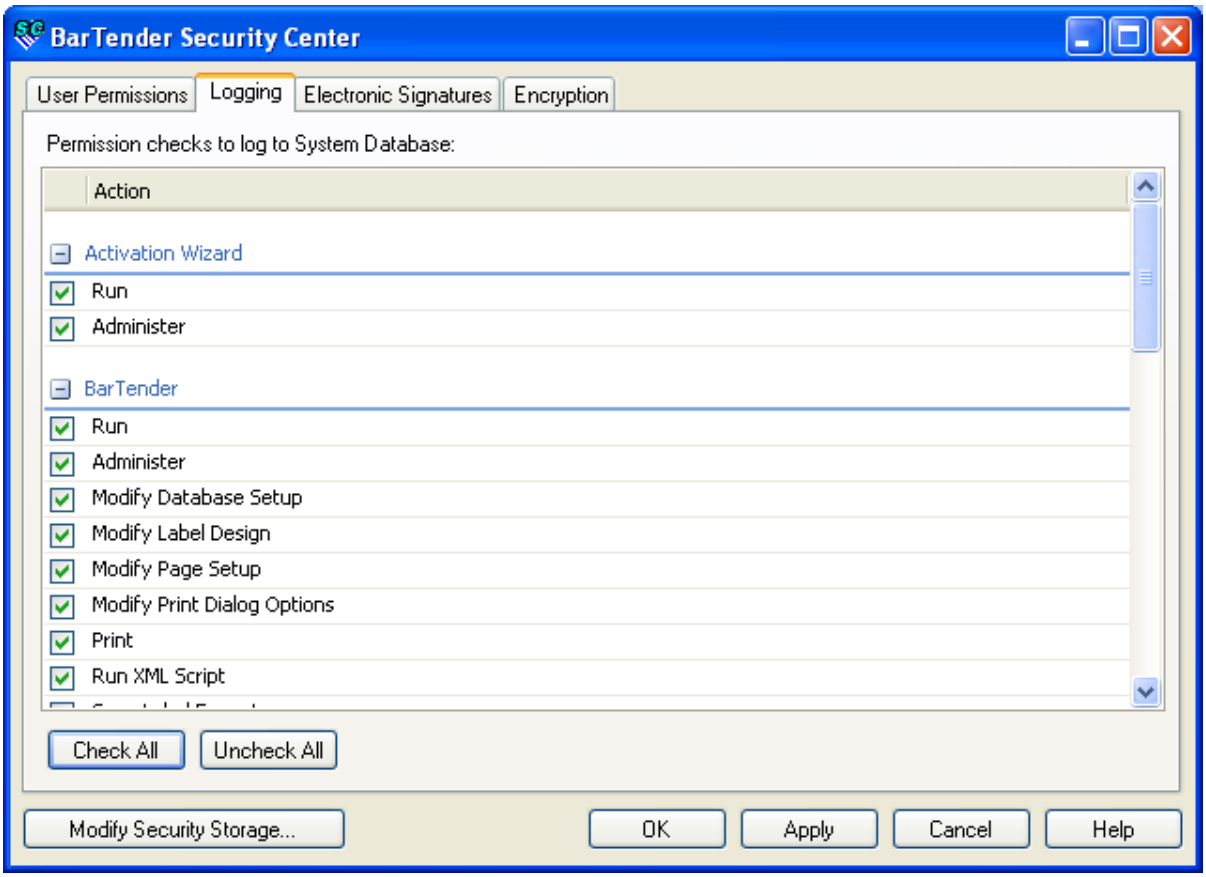
Enabling the "Login Override Required" Option

Underneath the **Permissions** list of the **User Permissions** tab is a checkbox that says, "When permission is denied, allow login override." If this checkbox has been enabled, when a user is denied permission to access a feature, a dialog displays requesting a "Login Override." This allows for another user that has rights to use the desired feature to type in their user name and password. Such a "Login Override" provides one-time access to the desired feature.

If a user is denied access to a feature or function when "Login Overrides" are enabled, the user has the option of having someobody with higher-level security credentials enter in a temporary override.

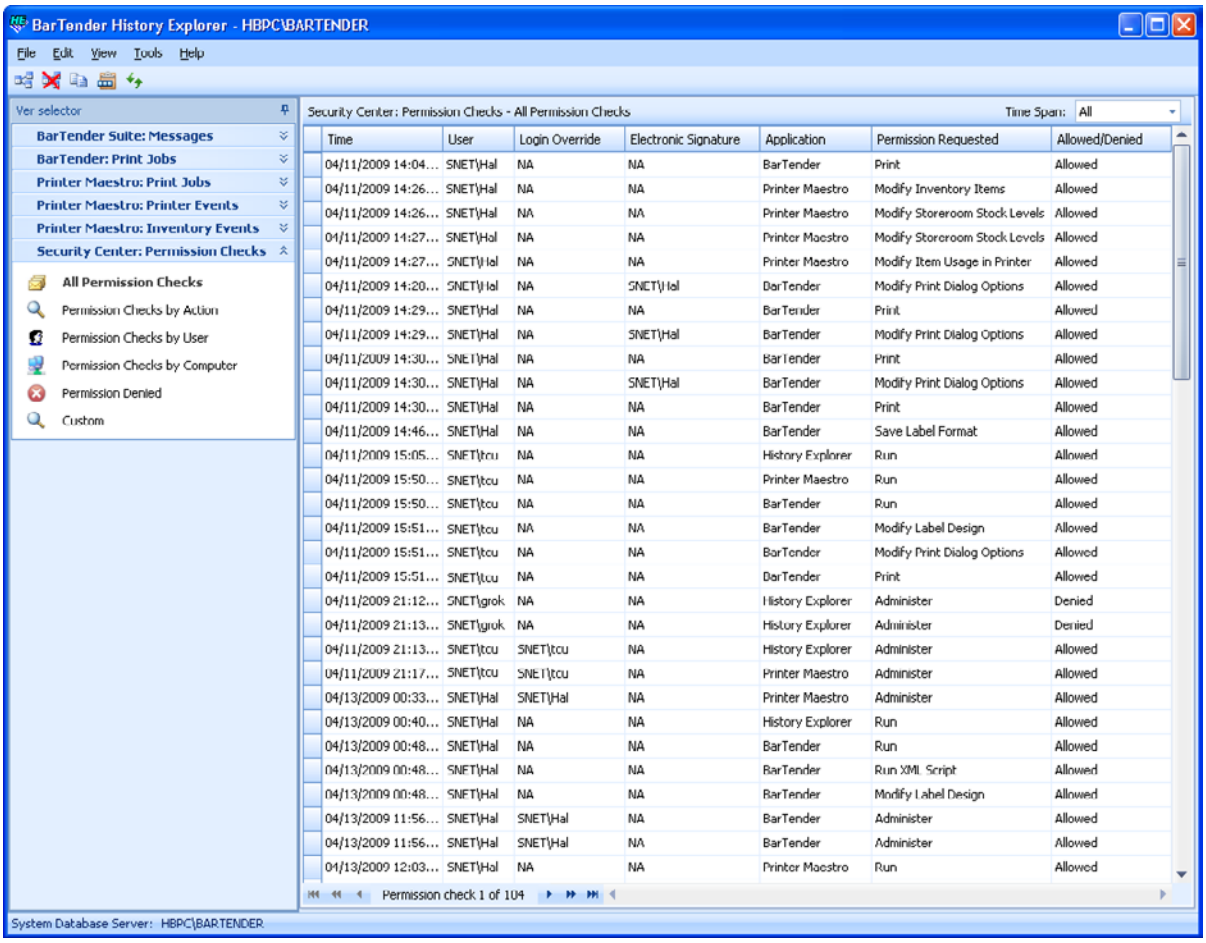
Logging Permission Checks

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 even want to know who asked to perform certain actions, even if those users were never granted permission to do so. The **Logging** tab makes it very easy to log any (or all) possible permission checks. (The available **Action** list is the same as the **Permissions** list in the **User Permissions** tab.) Simply click on the checkbox in front of the actions for which you want to log the permission checks. Alternatively, you can click on the **Check All** button to specify logging of *all* permission checks.



The Logging tab lets you record permission checks and whether or not the permission was granted.

Once the logging of permission checks has been enabled, you can audit the list of permission checks that have been performed within your BarTender Application Suite by running the separate History Explorer application. In the **View Selector** on the left side of the History Explorer screen, simply select the **Security Center: Permissions Checks** view, an example of which is shown below:



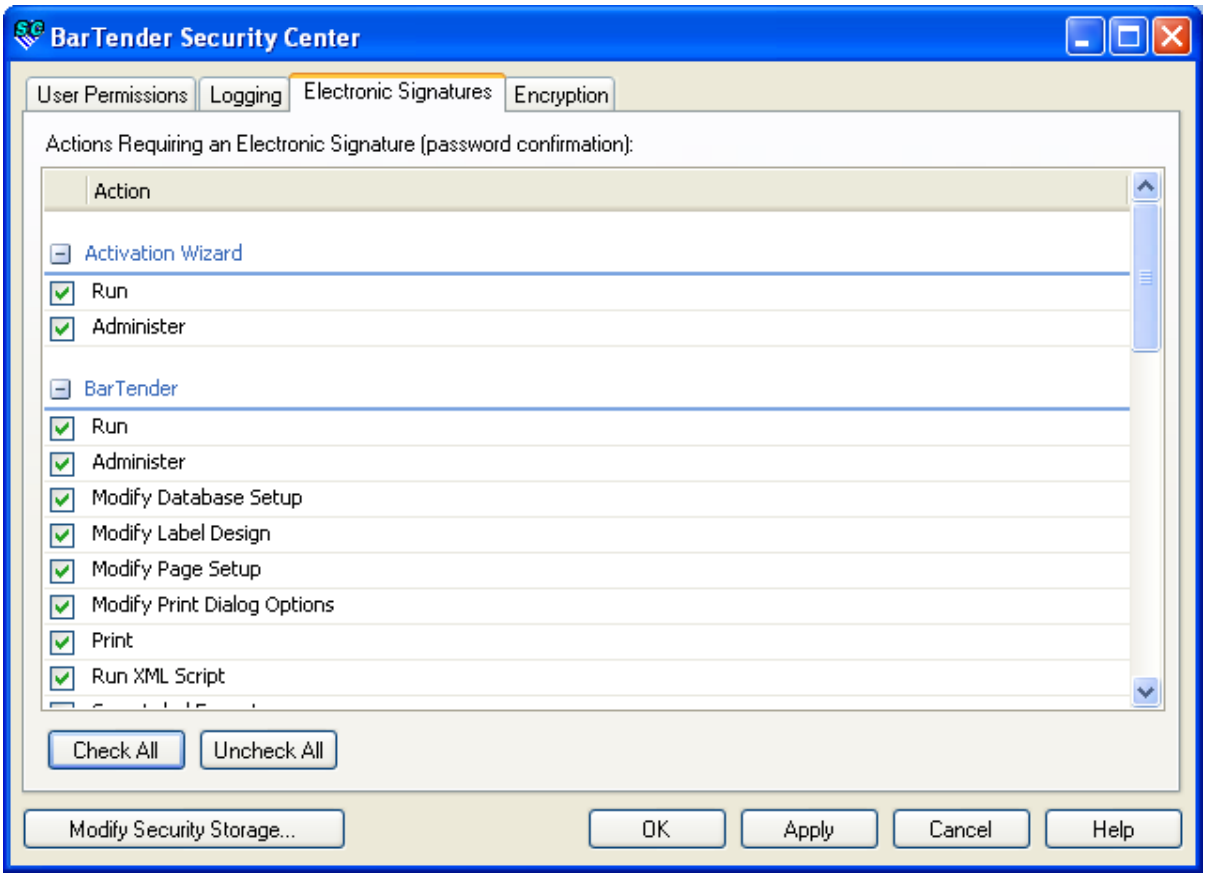
The "Security Center: Permissions Checks" view in History Explorer lets you audit who has attempted to access which features, and whether or not permission was granted.

Enabling Requests for an "Electronic Signature"

The **Electronic Signatures** tab provides you with an easy way to ensure that the user that originally logged into the computer that is running the BarTender Application Suite did not walk away from his or her computer, thereby leaving it vulnerable to control by an unauthorized intruder.

On the **Electronic Signatures** tab, you can specify that individual actions require an "electronic signature" prior to access being granted. (You can even use the **Check All** button to specify that *all* actions require an electronic signature.) The subsequently-requested 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.

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 tab.



Electronic Signatures let you define actions for which users must resubmit their Windows login credentials before proceeding. This tab displays the same action list shown on the User Permissions tab.

When users perform actions that require an Electronic Signature, a dialog pops up requesting that they resubmit their Windows credentials.

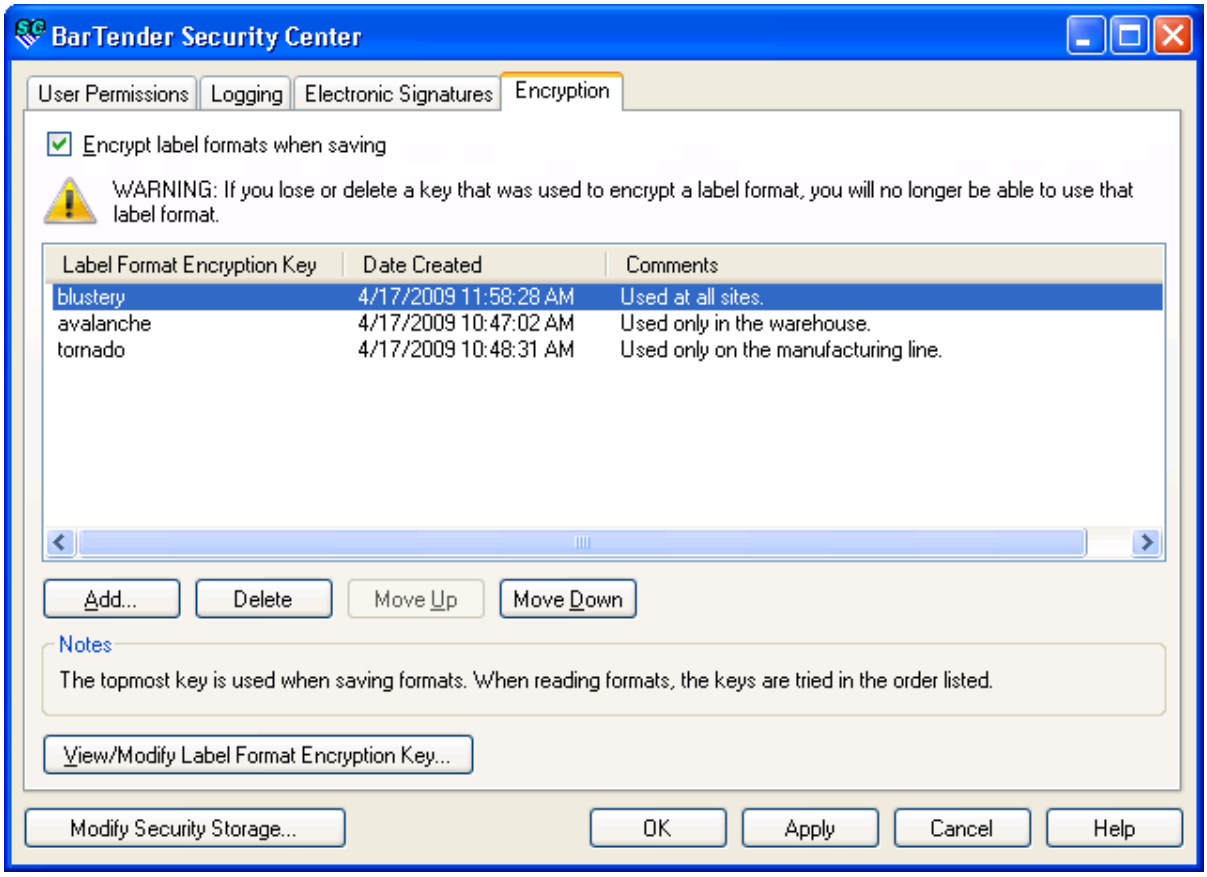
Configuring Label Format Encryption

If there is any possibility that a user could either copy your label formats to a PC that does not have BarTender Security Center enabled or install an unsecured copy of BarTender onto a PC, then your label formats are at risk for being modified and/or printed by users that are not authorized to do so. One way to significantly reduce such unauthorized activity is to encrypt your label formats so that they will not be readable on other PCs.

The encryption key(s) you enter into BarTender Security Center are stored on the individual PC being secured. That means that, if your encrypted label formats are moved to a different PC, they cannot be read unless there is also a copy of BarTender Security Center installed there *and* somebody knows what security keys to specify.

To Enable Label Format Encryption:

1. To enable the automatic encryption of label formats as they are saved, first click on the checkbox at the top of the Encryption tab in BarTender Security Center.
2. Next, use the Add button below the list of encryption keys to define one or more keys.



Any instance of BarTender Security Center can optionally store multiple encryption keys in order to allow decryption of label formats encrypted by multiple sources.

Encrypting and Decrypting is Normally Automatic

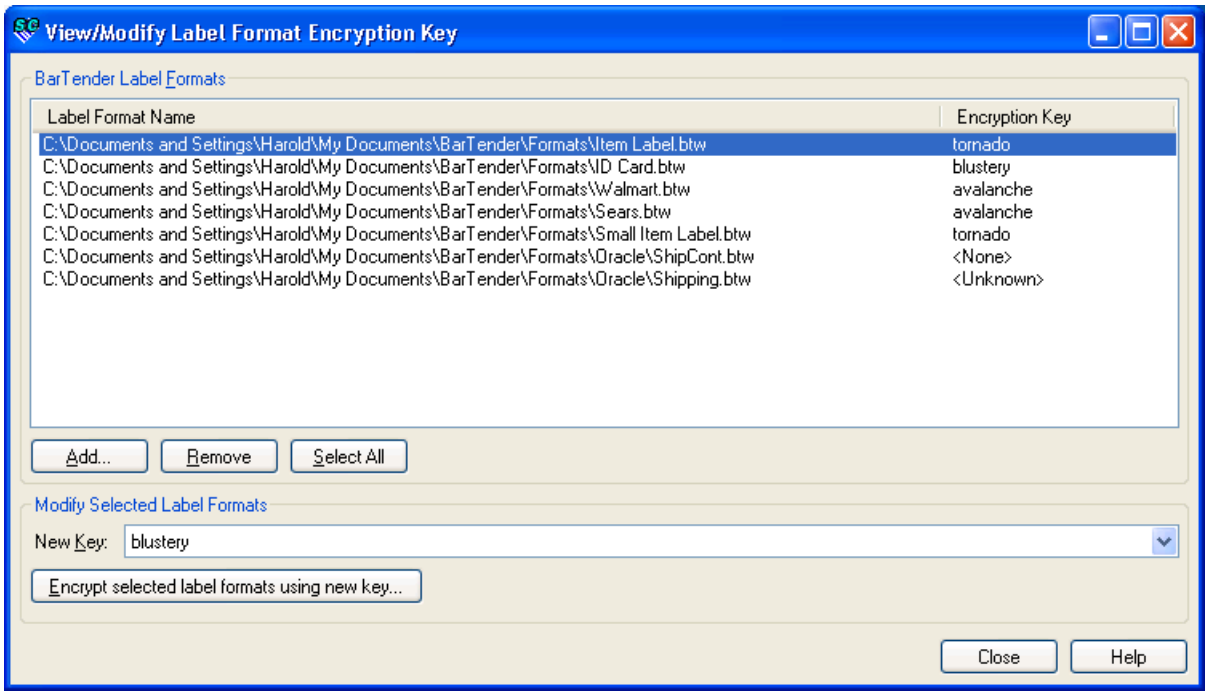
You only have to enter encryption keys into BarTender Security Center at setup time – you will never be asked to type them in while loading a label format. This is because, once you enable the encryption of label formats and define at least one encryption key in BarTender Security Center, the encryption is performed *automatically* as each label format is saved during normal use. Similarly, the decryption is performed automatically as the label formats are opened (which they have to be in order to be printed).

Encrypting Already-Saved but Non-Encrypted Label Formats

Because label formats are normally encrypted during the saving process, if you enable BarTender Security Center after you have already created and started to use some label formats, those label formats will not magically on their own become encrypted while sitting unused on a hard drive. That's fine, if you don't mind waiting until the next time those label formats are saved for them to become encrypted. However, at your option, you may wish to encrypt one or more label formats without bothering to manually load and resave them using BarTender. Alternatively, you may want to view or change the encryption key used for one or more already-encrypted label formats. You may even want to *remove* encryption. All of these actions can be performed using the **View/Modify Label Format Encryption Key** button in BarTender Security Center.

Viewing the Encryption Key(s) used in Existing Label Formats

To visually inspect the encryption keys used in one or more existing label formats, click the **View/Modify Label Format Encryption Key** button in BarTender Security Center. The associated dialog provides you with an **Add** button for the purpose of viewing the encryption status of as many existing label formats as you wish. (When you inspect a label format that uses a key that is not entered into your copy of BarTender Security Center, the value in the Encryption Key column will display as "Unknown.")



The "View/Modify Label Format Encryption Key" dialog lets you review the encryption keys currently in use by selected label formats, as well as change or even remove the encryption for selected formats.

Changing, Adding and Removing Encryption Keys from Existing Label Formats

You can add encryption to non-encrypted label formats and change (or remove) the key used by already-encrypted label formats using the exact same method:

1. If you have just added or deleted encryption keys on the main **Encryption** tab, be sure to press the **Apply** button before proceeding so that you will have proper access to the most current list of encryption keys.
2. Press the **View/Modify Format Encryption Key** button to load the associated dialog.
3. Use the **Add** button as many times as you want to load the path to and name of all of the label formats whose keys you want to inspect or change.
4. Click on the label format whose key you want to change. (You can use the CTRL and SHIFT keys in the traditional Windows manner to select multiple label formats.)
5. Using the **New Key** dropdown list, select the new key value that you want to use (or select "None" to remove encryption from the selected label formats).
6. Click on the **Encrypt selected formats using new key** button to complete your encryption change.

Understanding How and When Multiple Encryption Keys are Used

When you start out with a brand new copy of the BarTender Application Suite and it is the first copy on your network, there is a good chance that you will not yet have *any* encrypted label formats on your network. In this situation, once you enable BarTender Security Center and the **Encrypt label formats when saving** option, you only need to supply Security Center with a single key value.

Suppose that you subsequently install a second copy of the BarTender Application Suite on your network and that you also decide to use Security Center and label format encryption on that computer as well. If you decide to use the same encryption key value for this second system, then the users of the two copies of BarTender will be able to read each other's label formats and you would still only have one BarTender label format encryption key in use on your network.

In contrast, if you decide to use a *different* key value for the second system, then the users of the two copies of BarTender would by default *not* be able to read each other's label formats. Another way that you might end up with more than one encryption key in use on a network is if you simply decided to add a second key to at least one of your BarTender Security Center installations in order to encrypt all *new* label formats created on that computer using a new key value. (At your option, you could use Security Center to update your existing formats to use the new key instead of the old one, or you could continue to use the old key for the old label formats.)

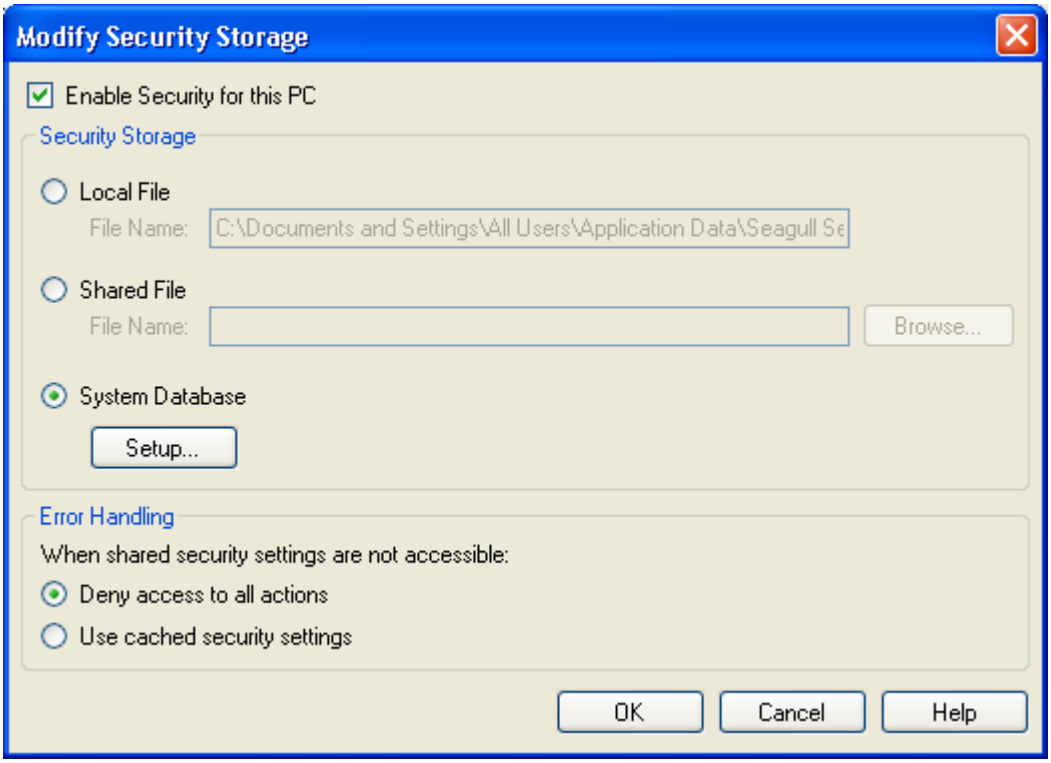
If you do decide to use multiple encryption keys for different copies of BarTender Security Center, you may want to designate at least one copy of Security Center on your network to be able to use *multiple* encryption keys. (For example, you might want to do this for a system administrator.) This allows the associated copy of BarTender to load different label formats that may be encrypted using different keys.

When an instance of Security Center has been configured to use more than one encryption key, decryption is attempted using each key in the same sequence in which it is listed in Security Center until either the label format has been successfully decrypted and loaded or Security Center has run out of available keys that it knows about. However, when saving label formats, the topmost key in the **Format Encryption Key** list is always used. (This applies regardless of whether you are saving a new label format or an existing one that may previously have been encrypted using a different key.)

Enabling BarTender Security Center on Multiple Computers to use Shared Security Settings

When the BarTender Application Suite is first installed on a PC, BarTender Security Center by default starts out disabled. That means that you need to explicitly run BarTender Security Center at least once on any PC for which you want to offer Security Center protection. When

you start BarTender Security Center on a PC for the first time, the Modify Security Storage dialog is displayed.



The Modify Security Storage dialog displays automatically the first time Security Center is run. Once you enable security, there are two options for sharing security settings among multiple computers.

Click the checkbox at the top of the dialog to enable security and then specify the shared data location (using either a Shared File or the System Database). When you press **OK** to close this dialog, the main Security Center window will display.

Special Considerations for Label Format Encryption

Even on a network with multiple copies of BarTender Security Center set to share common security settings, when encryption keys are used by a given copy of Security Center, the keys are always stored in the Local File on that PC (and not in the Shared File or System Database). You must therefore manually type encryption key(s) into each copy of Security Center that needs to be able to read encrypted label formats. (The reason for this extra precaution is that the Shared File and System Database are readable by *all* BarTender users. This would unnecessarily make your keys visible to intruders with possibly malicious intent. In contrast, the Local File is locked down so that only system administrators and the local copy of Security Center can read it.)

Disabling BarTender Security Center

To disable BarTender Security Center:

1. Run BarTender Security Center.
2. Press the **Modify Security Storage** button in the lower left corner.
3. Uncheck the **Enable Security** checkbox.
4. Press **OK**.

This will disable all permission checks based on Security Center settings.

Turning Off Encryption for Existing Label Formats

Disabling BarTender Security Center does nothing to make encrypted label formats readable again. To fix that problem, you need to temporarily enable Security Center again. Then, use the **View/Modify Format Encryption Key** dialog of the **Encryption** tab to set the encryption for the desired label formats to **<none>**. You can then disable your Security Center again.

Label Format Passwords

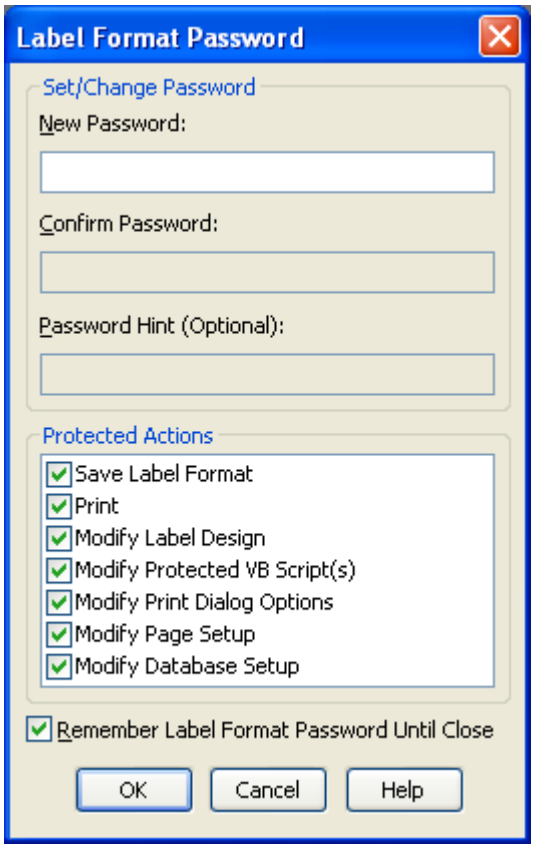
The Label Format Password option is available in the Professional and both the Automation editions. This option offers a quick and easy way to protect specific attributes of selected label formats from malicious or accidental modification and to optionally prevent unauthorized printing. Label Format Passwords are created, requested and validated without any dependency on or interaction with BarTender Security Center.

You enable the **Label Format Password** option for a given label format simply by setting a password (as described below). You can specify a different password for each label format and individually select the actions within that label format that you wish to protect from unauthorized users.

If you need to secure additional actions or other applications in the BarTender Suite, consider using BarTender Security Center. Alternatively, BarTender's Print-Only Password option, discussed later in this document, offers some very basic security with very little implementation effort.

Setting the Label Format Password

Within BarTender's **File** menu, select the **Label Format Password** option. The following dialog will appear.



Enter the password that you want to use and type it in a second time in the **Confirm Password** field. You can also provide an optional **Password Hint**, which will be available to you later whenever you are asked to provide the password. Then click on **OK**.

Protecting Individual Features

Once you have specified the password for your label format, you can then specify which actions you want to designate as "Protected Actions." When any of these checkboxes are marked, the user will be asked to enter the password before being allowed to perform that action.

- If the **Remember Label Format Password Until Close** checkbox is set, then a user will only be asked to enter the password once. Then, until the label format is closed, he or she will be able to perform all of the protected actions as many times as desired without having to reenter the password.
- If the **Remember Label Format Password Until Close** checkbox is empty, then the user will be prompted to enter the password each and every time a protected action is attempted.

The full list of protected actions is described in *"Appendix B: Actions Protected using the Label Format Password."*

Supplying the Password to Access Protected Features

Once the Label Format Password has been specified and stored within a label format, users are automatically prompted for the password as follows when attempting to access a protected action.

The BarTender-based Print-Only Password

Within any given copy of BarTender, you can specify a "Print-Only Password." Thereafter, BarTender will always start in "Print-Only Mode." Users then have to supply the Print-Only Password in order to either modify objects in the label design area or to access any of the options in the **Administer** menu. However, users without the Print-only Password can still print labels.

The Print-only Password is a quick and easy way to make it harder for production users to make accidental or casual changes to the configuration of BarTender. However, setting a Print-only Password is a relatively low-security measure for protecting label formats from alteration by motivated intruders. That is because this protection can be defeated just by copying any desired label formats to another computer that has a different copy of BarTender installed (unless that copy is already configured to use the same Print-only password). In contrast, the **Label Format Password** option (previously discussed) is not nearly as easily defeated just by copying label formats to another computer. It also offers granular control over which individual BarTender actions the password controls access to. For the most granular control over user actions and the very highest degree of security, you should enable and use BarTender Security Center. (This is a more technical tool recommended for use by System Administrators only.)

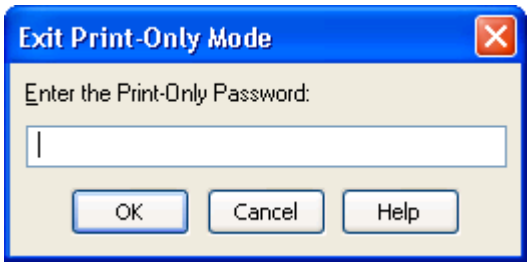
Specifying a Print-only Password

The Print-Only Password is specified using the **Print-Only Password Setup** option in the **Administer** menu, as shown here:

After you first specify a Print-Only password, your copy of BarTender will continue to run normally without any features being protected because BarTender knows that you are the one that set the password. In order to enter the Print-only Mode after first setting the Print-only Password, you must exit from and then restart BarTender.

Supplying the Password to Access Protected Features

Once the Print-Only Password has been set and BarTender has been exited from one time, the dialog below is displayed when a user attempts to modify objects in the label design area or access options in the **Administer** menu for the first time in any given BarTender user session.



Once the Print-Only Password has been supplied to this dialog, BarTender will exit its Print-Only Mode. In order to reenter Print-Only Mode, you must exit from and restart BarTender.

Other Security Issues

In addition to the various security features built into the BarTender Application 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 labeling system.

Using Windows Security as Part of your Security Solution

To use Windows-based security to selectively allow or deny individual users access to specific label formats and printers:

1. Right-click on either the printer (in the Windows **Printers and Faxes** folder) or the file (in any Windows Explorer window).
2. Select the **Properties** option.
3. Click on the **Security** tab.
4. Specify the desired permissions for your Windows users and groups.

Appendix A: User Permissions Available using Security Center

This appendix lists applications in the BarTender Application Suite and the controllable permissions available for control within each one at the time BarTender 9.1 was released. Although this list will be updated periodically, there may be times when BarTender Security Center itself displays a more current list than the one shown here.

Permissions in Activation Wizard

- **Run** - Determines whether or not a user can run this application.
- **Administer** - Determines whether or not a user can Activate or Deactivate their software license. Without this permission, a user can only view the Activation state.

Permissions in BarTender

- **Run** - Determines whether or not a user can run this application.
- **Administer** - Determines whether or not a user can use any of the options in the Administer menu.
- **Modify Database Setup** - Determines whether or not a user can open and/or change options in the Database Setup dialog.
- **Modify Label Design** - Determines whether or not a user can change the appearance or position of objects in the label design area. If a user does not have this permission, a padlock is shown in the label design area and the user cannot modify the label objects.
- **Modify Page Setup** - Determines whether or not a user can open and/or change options in the Page Setup dialog.

- **Modify Print Dialog Options** - Determines whether or not a user can change options in the Print dialog. Users that do not have this permission can still open the Print dialog but will not be able to change any of the options.
- **Print** - Determines whether or not a user can print.
- **Run XML Script** - Determines whether or not a user can use the Run XML Script option from either the File menu or from the Automation interface.
- **Save Label Format** – Determines whether or not users can save Label Formats. Users that have the ability to modify label formats obviously need this permission enabled in order to save their changes. Even users that do not have permission to modify label formats themselves may need permission to save them. For example, if they have permission to print label formats and their label formats use Prompting or Serialization, then their Screen Data sub-strings (which are part of the label format) need to be preserved at the end of the label job. Otherwise, their next label job will not start out with properly updated data values in place.
- **Set Label Format Passwords** - Determines whether or not a user can set or change the Label Format Password on any format. Remember that users that have this permission can lock other users out of a format by giving it a password that nobody else knows.

Permissions in BarTender System Database Setup

- **Run** - Determines whether or not a user can run this application.
- **Administer** - Determines whether or not a user can change any of the options in System Database Setup. Users that have Run permission but not Administer permission can only view the current settings.

Permissions in Commander

- **Run** - Determines whether or not a user can run this application.
- **Administer** - Determines whether or not a user can Start and Stop Detection of triggers, load Task Lists, and Add, Delete, and Modify Tasks. If a user has Run permission, but not Administer, her or she can only view the current status of Commander, but not change any of its options.

Permissions in History Explorer

- **Run** - Determines whether or not a user can run this application.
- **Administer** - Determines whether or not a user can use any of the options in the Administer menu.
- **Reprint** - Determines whether or not a user can use History Explorer's Reprint feature.

Permissions in Seagull License Server

- **Run** - Determines whether or not a user can run this application.
- **Administer** - Determines whether or not a user can use any of the features in Seagull License Server (SLS). Users that have Run permission but not Administer permission can only view the current status of SLS but not change any of its options.

Permissions in Printer Maestro

- **Run** - Determines whether or not a user can run this application.
- **Administer** - Determines whether or not a user can use any of the options in the Administer menu.
- **Modify Inventory Items** - Determines whether or not a user can Add, Delete, or Modify inventory items.
- **Modify Item Usage in Printer** - Determines whether or not a user can perform the following inventory actions: "Drag" inventory items and "drop" them on printers, remove items from printers, or modify the properties of items once they have been dropped on a printer.
- **Modify Storeroom Stock Levels** - Determines whether or not a user can modify the stock level and Receive or Use Inventory items.
- **Reprint** - Determines whether or not a user can use Printer Maestro's Reprint feature.

Permissions in Reprint Console

- **Run** - Determines whether or not a user can run this application.
- **Administer** - Determines whether or not a user can use any of the options in the Administer menu.
- **Reprint** - Determines whether or not a user can use the Reprint feature.

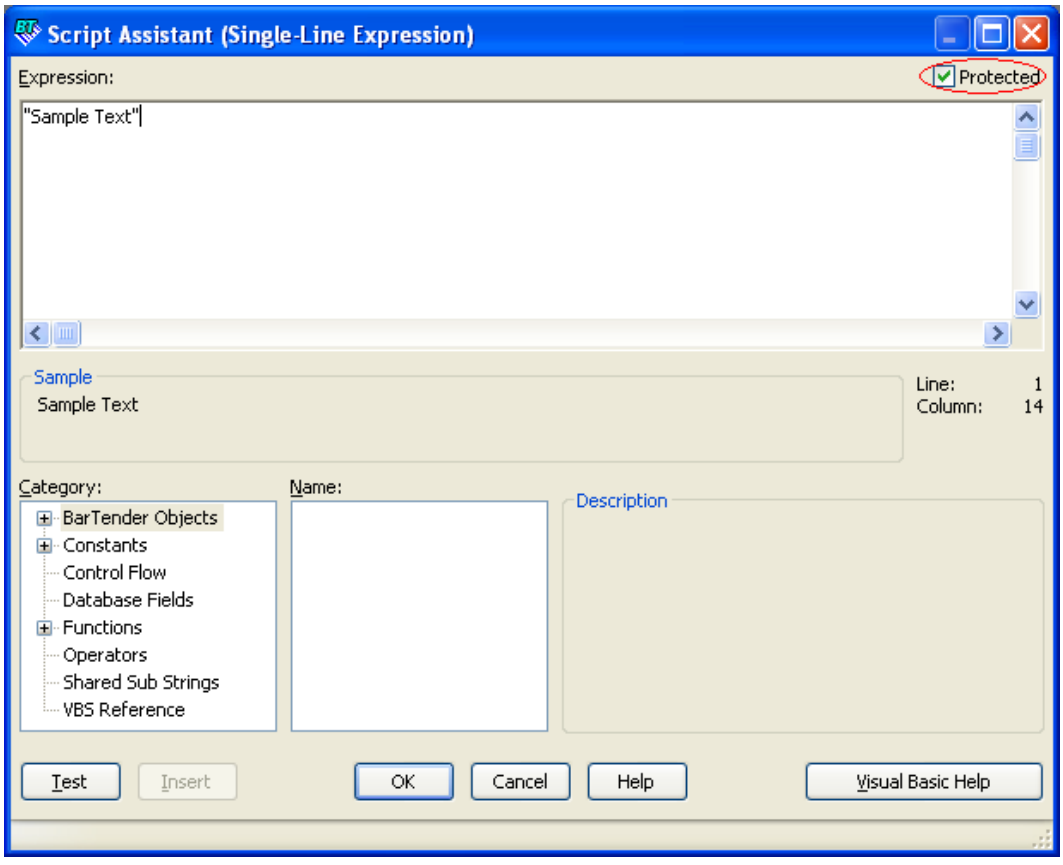
Appendix B: Actions Protected using the Label Format Password

Users can optionally create Label Format Passwords within any one copy of BarTender (Professional or better) for storage within individual label formats. Once defined, the Label Format Password can optionally protect any or all of the following actions from being performed by users that do not know the password. (The Label Format Password option has nothing to do with the Print-only Password.)

- **Save Label Format** – Determines whether or not users can save Label Formats. Users that have the ability to modify label formats obviously need this permission enabled in order to save their changes. Even users that do not have permission to modify label formats themselves may need permission to save them. For example, if they have permission to print label formats and their label formats use Prompting or

Serialization, then their Screen Data sub-strings (which are part of the label format) need to be preserved at the end of the label job. Otherwise, their next label job will not start out with the properly updated data values in place.

- **Print** - Protects the ability to print the Label Format.
- **Modify Label Design** - Protects the ability to change the appearance or position of objects in the label design area. When protected, a padlock is shown in the label design area and, when if user attempts to modify any label objects, her or she will be prompted by the display of the Exit Print-only Mode dialog to enter a password. Once the password has been supplied, it will not need to be entered again until the next time the label format is opened (regardless of the setting for "Remember Label Format Password Until Close").
- **Modify Protected VB Script(s)** – Preserves the ability to modify any VB Scripts in the label format that have their "Protected" checkbox set. This allows label designers to protect their proprietary VB Script code from viewing and modification.



The "Protected" checkbox in the upper right-hand corner of the VB Script Assistant allows a label designer to protect his or her VS Scripts from viewing and modification by others. The "Modify Protected VB Script(s)" option offered by BarTender's Label Format Password feature allows approved label designers to retain editing rights.

- **Modify Print Dialog Options** - Protects the ability to change options in the Print dialog. When enabled, users can still open the print dialog but they will not be able to change any of the options.
- **Modify Page Setup** - Protects the ability to open and/or change options in the Page Setup dialog.
- **Modify Database Setup** - Protects the ability to open and/or change options in the Database Setup dialog.

Available Seagull White Papers

General White Papers

- The Advantage of Drivers by Seagull

Companion Applications

- Printer Maestro: Enterprise Print Management
- Librarian
- BarTender Security Center
- BarTender Web Print Server

Recent Upgrades

- What's New in the Latest BarTender

Integration White Papers

- Integration Overview
- Commander
- Commander Examples
- BarTender's .NET SDKs
- BarTender's ActiveX Automation Interface
- Exporting Printer Code Templates
- Using BarTender with Remote Desktop Services and Citrix XenApp
- Integration with Oracle's WMS and MSCA
- Integration with IBM WebSphere Sensor Events
- Integration with SAP

Miscellaneous White Papers

- Weighing Scales
- Dynamically Changing Objects at Print-Time using VB Script
- GHS Labeling
- Licensing for BarTender's Automation Editions
- Printing International Characters Using BarTender
- BarTender Software Activation
- Using BarTender's Application Identifier Wizard
- Optimizing Label Printing Performance
- Status Monitor Overview
- Silent Install

For downloadable versions, visit:

www.seagullscientific.com/aspx/white-papers.aspx

SEAGULL SCIENTIFIC

www.seagullscientific.com

Version:2011-10-10 13:13 Copyright © 2011 Seagull Scientific, Inc.